

Microsoft®

Vademecum administratora

Windows Server® 2008

William R. Stanek

Vademecum administratora Windows Server® 2008
Edycja polska Microsoft Press

Tytuł oryginału: Windows Server® 2008 Administrator's Pocket Consultant

Original English language edition copyright © 2008 by William R. Stanek

Polish edition by APN PROMISE Sp. z o.o. Warszawa 2008

APN PROMISE Sp. z o.o., biuro: 00-108 Warszawa, ul. Zielna 39

tel. (022) 351 90 00, faks (022) 351 90 99

e-mail: mspress@promise.pl

Wszystkie prawa zastrzeżone. Żadna część niniejszej książki nie może być powielana ani rozpowszechniana w jakiegokolwiek formie i w jakikolwiek sposób (elektroniczny, mechaniczny), włącznie z fotokopiowaniem, nagrywaniem na taśmy lub przy użyciu innych systemów bez pisemnej zgody wydawcy.

Microsoft, Microsoft Press, Active Directory, Authenticode, Internet Explorer, Jscript, SharePoint, SQL Server, Visual Basic, Visual C#, Win32, Windows, Windows CardSpace, Windows NT, Windows PowerShell, Windows Server oraz Windows Vista są zarejestrowanymi znakami towarowymi Microsoft Corporation.

Wszystkie inne nazwy handlowe i towarowe występujące w niniejszej publikacji mogą być znakami towarowymi zastrzeżonymi lub nazwami zastrzeżonymi odpowiednich firm odnośnych właścicieli.

Przykłady firm, produktów, osób i wydarzeń opisane w niniejszej książce są fikcyjne i nie odnoszą się do żadnych konkretnych firm, produktów, osób i wydarzeń. Ewentualne podobieństwo do jakiegokolwiek rzeczywistej firmy, organizacji, produktu, nazwy domeny, adresu poczty elektronicznej, logo, osoby, miejsca lub zdarzenia jest przypadkowe i niezamierzone.

APN PROMISE Sp. z o.o. dołożyła wszelkich starań, aby zapewnić najwyższą jakość tej publikacji. Jednakże nikomu nie udziela się rękoma ani gwarancji. APN PROMISE Sp. z o.o. nie jest w żadnym wypadku odpowiedzialna za jakiegokolwiek szkody będące następstwem korzystania z informacji zawartych w niniejszej publikacji, nawet jeśli APN PROMISE została powiadomiona o możliwości wystąpienia szkód.

ISBN: 978-83-7541-019-8

Przekład: Arkadiusz Czajkowski, Dominik Daniewski, Alicja Kahn, Marek Włodarz

Redakcja: Marek Włodarz

Korekta: Magdalena Kalina Swoboda

Skład i łamanie: MAWart Marek Włodarz

Spis treści

Wprowadzenie	xvi
Część I Podstawy administracji Windows Server 2008	
1 Wprowadzenie do administracji Windows Server 2008	3
Windows Server 2008 i Windows Vista	3
Poznanie systemu Windows Server 2008	5
Narzędzia i protokoły sieciowe	7
Istota opcji sieciowych	7
Korzystanie z protokołów sieciowych	8
Kontrolery domeny, serwery członkowskie i usługi domenowe	9
Korzystanie z Active Directory	9
Korzystanie z kontrolerów domeny tylko do odczytu	11
Korzystanie ze wznawialnych usług katalogowych Active Directory	11
Usługi rozwiązywania nazw	12
Korzystanie z Domain Name System (DNS)	13
Korzystanie z Windows Internet Name Service (WINS)	14
Korzystanie z mechanizmu Link-Local Multicast Name Resolution (LLMNR)	16
Często używane narzędzia	18
Korzystanie Windows PowerShell	18
2 Wdrażanie Windows Server 2008	21
Role serwera, usługi roli oraz rozszerzenia systemu Windows Server 2008	22
Instalacja pełna i Server Core systemu Windows Server 2008	28
Instalowanie Windows Server 2008	31
Wykonywanie czystej instalacji	31
Wykonywanie uaktualnienia	33
Wykonywanie dodatkowych zadań administracyjnych podczas instalacji	34
Zarządzanie rolami, usługami roli i rozszerzeniami	41
Przeglądanie skonfigurowanych ról i usług roli	41
Dodawanie i usuwanie ról	43
Przeglądanie i modyfikowanie usług roli na serwerze	45
Dodawanie i usuwanie rozszerzeń Windows Server 2008	45
3 Zarządzanie serwerami systemu Windows Server 2008	47
Wykonywanie wstępnych zadań konfiguracyjnych	48
Zarządzanie serwerami	50
Zarządzanie właściwościami systemu	53
Zakładka Computer Name	55
Zakładka Hardware	56
Zakładka Advanced	56
Zakładka Remote	65
Zarządzanie bibliotekami DLL	65

4 Monitorowanie procesów, usług i zdarzeń	67
Zarządzanie aplikacjami, procesami i wydajnością	67
Task Manager	68
Zarządzanie aplikacjami	68
Administrowanie procesami	69
Przeglądanie usług systemowych	72
Wyświetlanie i zarządzanie wydajnością systemu	73
Przeglądanie i zarządzanie wydajnością sieci	75
Przeglądanie i zarządzanie sesjami użytkowników	76
Zarządzanie usługami systemowymi	77
Uruchamianie, zatrzymywanie i wstrzymywanie usług	79
Konfigurowanie uruchamiania usług	79
Konfigurowanie logowania usługi	80
Konfigurowanie odzyskiwania usług	81
Wyłączanie niepotrzebnych usług	83
Rejestrowanie i przeglądanie zdarzeń	83
Uzyskiwanie dostępu i korzystanie z dzienników zdarzeń	85
Filtrowanie dzienników	87
Określanie opcji dzienników zdarzeń	89
Czyszczenie dzienników zdarzeń	90
Archiwizowanie dzienników zdarzeń	90
Monitorowanie wydajności i aktywności serwera	92
Po co monitorować serwery?	92
Przygotowanie do monitorowania	93
Korzystanie z konsoli Reliability And Performance	93
Wybieranie liczników do monitorowania	96
Rejestrowanie wydajności	98
Przeglądanie raportów modułów zbierających dane	101
Konfigurowanie alertów liczników wydajności	102
Dostrajanie wydajności systemu	103
Monitorowanie i dostrajanie wykorzystania pamięci	103
Monitorowanie i dostrajanie wykorzystania procesora	105
Monitorowanie i dostrajanie dyskowego podsystemu wejścia/wyjścia	106
Monitorowanie i dostrajanie pasma sieciowego i możliwości połączeń	107
5 Automatyzacja zadań administracyjnych, zasady i procedury	109
Istota Zasad grupy	112
Podstawy Zasad grupy	112
Kolejność stosowania wielu obiektów zasad	113
Kiedy zasady grupy są stosowane?	113
Uwarunkowania Zasad grupy i zgodność wersji	114
Przeglądanie zmian w Zasadach grupy	115
Zarządzanie zasadami lokalnymi	117
Lokalne obiekty zasad grupy	117
Uzyskiwanie dostępu do lokalnych ustawień zasad najwyższego poziomu	118
Ustawienia LGPO	119
Uzyskiwanie dostępu do obiektów zasad administratorów, nie-administratorów oraz specyficznych dla użytkownika	120

Zarządzanie zasadami dla lokacji, domeny i jednostki organizacyjnej	121
Istota domyślnych zasad domenowych	121
Korzystanie z narzędzia Group Policy Management Console	122
Poznanie edytora zasad	124
Korzystanie z szablonów administracyjnych do ustawiania zasad	125
Tworzenie centralnego magazynu	126
Tworzenie i łączenie GPO	127
Tworzenie i korzystanie ze startowych GPO	128
Delegowanie uprawnień do zarządzania zasadami grupy	128
Blokowanie, zastępowanie i wyłączanie zasad	130
Konserwacja i rozwiązywanie problemów z zasadami grupy	133
Odświeżanie zasad grupy	133
Konfigurowanie interwału odświeżania dla innych komputerów	135
Modelowanie zasad grupy do celów planowania	136
Kopiowanie, wklejanie i importowanie obiektów zasad	138
Tworzenie kopii zapasowych i przywracanie obiektów zasad	139
Ustalanie bieżących ustawień zasad grupy i stanu odświeżania	140
Wyłączanie nieużywanej części zasad grupy	140
Zmianianie preferencji przetwarzania zasad	140
Konfigurowanie wykrywania powolnych łączy	141
Usuwanie łączy i obiektów zasad	144
Rozwiązywanie problemów z zasadami grupy	144
Naprawianie obiektu Default Group Policy	145
Zarządzanie użytkownikami i komputerami przy użyciu zasad grupy	146
Scentralizowane zarządzanie folderami specjalnymi	146
Zarządzanie skryptami użytkowników i komputerów	150
Rozpowszechnianie oprogramowania za pośrednictwem zasad grupy	153
Automatyczne żądania certyfikatów dla komputerów i użytkowników	158
Zarządzanie aktualizacjami automatycznymi	158
6 Podnoszenie zabezpieczeń komputerów	163
Korzystanie z szablonów zabezpieczeń	163
Korzystanie z przystawek Security Templates oraz Security Configuration And Analysis	165
Przeglądanie i zmienianie ustawień szablonów	166
Analizowanie, przeglądanie i aplikowanie szablonów zabezpieczeń	172
Wdrażanie szablonów zabezpieczeń na wielu komputerach	175
Korzystanie z narzędzia Security Configuration Wizard	176
Tworzenie zasad zabezpieczeń	176
Edytowanie istniejących zasad zabezpieczeń	180
Stosowanie istniejących zasad zabezpieczeń	180
Wycofywanie ostatnio zaaplikowanej zasady	181
Rozpowszechnianie zasady zabezpieczeń na wielu komputerach	181

Część II **Administrowanie usługą katalogową Windows Server 2008**

7 Korzystanie z Active Directory	185
Wprowadzenie do Active Directory	185
Active Directory i DNS	185
Wdrażanie kontrolerów domeny tylko do odczytu	186
Windows Server 2008 i Windows NT 4.0	187
Budowanie struktury domenowej	187
Domeny	188
Lasy i drzewa domen	189
Jednostki organizacyjne	191
Lokacje i podsieci	192
Używanie domen Active Directory	193
Korzystanie z komputerów systemu Windows 2000 i wersji późniejszych a Active Directory	193
Korzystanie z poziomów funkcjonalnych domen	194
Podnoszenie poziomu funkcjonalnego domeny i lasu	197
Istota struktury katalogu	198
Poznawanie magazynu danych	199
Poznawanie wykazu globalnego	199
Buforowanie członkostwa w grupach uniwersalnych	200
Replikacja i Active Directory	201
Active Directory i LDAP	202
Istota ról wzorców operacji	202
8 Podstawy administracji Active Directory	205
Narzędzia zarządzania Active Directory	205
Narzędzia administracyjne Active Directory	205
Narzędzia wiersza polecenia Active Directory	206
Pomocnicze narzędzia Active Directory	207
Korzystanie z narzędzia Active Directory Users And Computers	208
Poznawanie narzędzia Active Directory Users And Computers	208
Łączenie się z kontrolerem domeny	209
Łączenie się z domeną	210
Wyszukiwanie kont i udostępnionych zasobów	211
Zarządzanie kontami komputerów	212
Tworzenie kont komputerów dla stacji roboczych lub serwerów	212
Tworzenie kont komputerów w konsoli Active Directory Users And Computers	213
Wyświetlanie i edytowanie właściwości kont komputerów	214
Usuwanie, wyłączanie i włączanie kont komputerów	214
Resetowanie zablokowanego konta komputera	214
Przenoszenie kont komputerów	215
Przyłączanie komputera do domeny lub grupy roboczej	216
Zarządzanie kontrolerami domeny, rolami i katalogami	217
Instalowanie i odłączanie kontrolerów domeny	217
Przeglądanie i transferowanie ról domenowych	218
Wyświetlanie i przenoszenie roli wzorca nazw domen	220

Wyświetlanie i przenoszenie roli wzorca schematu	220
Przenoszenie ról przy użyciu wiersza polecenia	221
Przechwytywanie ról w trybie wiersza polecenia	222
Konfigurowanie wykazów globalnych	223
Konfigurowanie buforowania członkostwa grup uniwersalnych	224
Zarządzanie jednostkami organizacyjnymi	224
Tworzenie jednostek organizacyjnych	224
Przemianowywanie i usuwanie jednostek organizacyjnych	225
Przenoszenie jednostek organizacyjnych	225
Zarządzanie lokacjami	225
Tworzenie lokacji	226
Tworzenie podsiaci	226
Przypisywanie kontrolerów domeny do lokacji	227
Konfigurowanie łączy lokacji	228
Konfigurowanie mostków łączy lokacji	230
Konserwacja Active Directory	231
Korzystanie z narzędzia ADSI Edit	231
Badanie topologii międzylokacyjnej	233
Rozwiązywanie problemów z Active Directory	234
9 Istota kont użytkowników i grup	237
Model zabezpieczeń Windows Server 2008	237
Protokoły uwierzytelniające	237
Kontrola dostępu	238
Różnice pomiędzy kontami użytkowników i grup	239
Konta użytkowników	239
Konta grup	241
Domyślne konta użytkowników i grup	245
Wbudowane konta użytkowników	245
Wstępnie zdefiniowane konta użytkowników	246
Wbudowane i wstępnie zdefiniowane grupy	247
Grupy niejawne i tożsamości specjalne	247
Możliwości kont	248
Przywileje	248
Prawa logowania	252
Możliwości wbudowane grup w Active Directory	253
Korzystanie z grup domyślnych	258
Grupy używane przez administratorów	258
Tożsamości specjalne	259
10 Tworzenie kont użytkowników i grup	261
Planowanie i uporządkowanie kont	261
Reguły nazw kont	261
Zasady haseł i kont	263
Konfigurowanie zasad kont	265
Konfigurowanie zasad haseł	265
Konfigurowanie zasad blokady konta	267
Konfigurowanie zasad protokołu Kerberos	269

Konfigurowanie zasad praw użytkowników	270
Globalne konfigurowanie praw użytkowników	270
Lokalne konfigurowanie praw użytkowników	272
Dodawanie konta użytkownika	273
Tworzenie domenowych kont użytkowników	273
Tworzenie lokalnych kont użytkowników	275
Dodawanie konta grupy	276
Tworzenie grup domenowych	277
Tworzenie grupy lokalnej i przypisywanie członków	277
Zarządzanie członkostwem w grupach domenowych	278
Zarządzanie indywidualnym członkostwem grup	279
Zarządzanie członkostwem grupy	279
Określanie grupy podstawowej dla użytkowników i komputerów	280
11 Zarządzanie istniejącymi kontami użytkowników i grup	281
Zarządzanie informacjami kontaktowymi	281
Ustawianie informacji kontaktowych	281
Wyszukiwanie użytkowników i grup w Active Directory	283
Konfigurowanie ustawień środowiskowych użytkownika	284
Systemowe zmienne środowiskowe	285
Skrypty logowania	286
Przypisywanie folderów macierzystych	287
Określanie opcji i ograniczeń konta	288
Zarządzanie godzinami logowania	288
Definiowanie dozwolonych stacji roboczych	290
Definiowanie przywilejów telefonowania i VPN	291
Definiowanie opcji zabezpieczeń konta	292
Zarządzanie profilami użytkowników	293
Profile lokalne, mobilne i obowiązkowe	294
Wykorzystanie narzędzia System do zarządzania profilami lokalnymi	296
Aktualizowanie kont użytkowników i grup	300
Przemianowywanie kont użytkowników i grup	300
Kopiowanie domenowych kont użytkowników	301
Importowanie i eksportowanie kont	302
Kasowanie kont użytkowników i grup	303
Zmianie i resetowanie haseł	304
Włączanie kont użytkowników	304
Zarządzanie wieloma kontami użytkowników	305
Ustawianie profili dla wielu kont	306
Definiowanie godzin logowania dla wielu użytkowników	306
Określanie dozwolonych komputerów logowania dla wielu kont	307
Definiowanie opcji konta dla wielu kont	307
Rozwiązywanie problemów związanych z logowaniem	308
Przeglądanie i ustawianie uprawnień Active Directory	309

Część III **Administrowanie danymi w Windows Server 2008**

12 Zarządzanie systemami plików i napędami	313
Zarządzanie rolą usługi plików	313
Dodawanie dysków twardych	318
Dyski fizyczne	318
Przygotowanie dysku fizycznego do pracy	320
Korzystanie z narzędzia Disk Management	320
Wymienne narzędzia magazynujące	323
Instalowanie i sprawdzanie nowego napędu	324
Znaczenie stanu dysku	325
Praca z dyskami podstawowymi i dynamicznymi	326
Zastosowanie dysków podstawowych i dynamicznych	327
Cechy szczególne dysków podstawowych i dynamicznych	328
Zmiana typu napędu	328
Uaktywnianie ponowne dysków dynamicznych	330
Skanowanie ponowne dysków	330
Przenoszenie dysku dynamicznego do nowego systemu	330
Praca z dyskami podstawowymi i partycjami	332
Podstawy partycjonowania	332
Tworzenie partycji i woluminów prostych	333
Formatowanie partycji	335
Zarządzanie istniejącymi partycjami i dyskami	336
Przydzielanie liter dysku i ścieżek	337
Zmiana lub usuwanie etykiety woluminu	338
Kasowanie partycji i napędów	338
Konwertowanie woluminu do NTFS	339
Zmiana rozmiaru partycji i woluminów	340
Naprawa błędów dysku i niespójności	342
Defragmentacja dysków	344
Kompresowanie dysków i danych	346
Szyfrowanie napędów i danych	348
Znaczenie szyfrowania i szyfrowanie systemu plików	348
Praca z zaszyfrowanymi plikami i folderami	350
Konfigurowanie zasady odzyskiwania	351
13 Administrowanie zestawami woluminów i macierzami RAID	353
Woluminy i zestawy woluminów	353
Podstawowe informacje o woluminach	354
Istota zestawów woluminów	355
Tworzenie woluminów i ich zestawów	357
Usuwanie woluminów i zestawów woluminów	359
Zarządzanie woluminami	359
Poprawianie wydajności i odporności na błędy w technologii RAID	360
Implementowanie macierzy RAID w systemie Windows Server 2008	361
Implementowanie RAID 0: przeplatanie dysków	361
Implementowanie RAID 1: dublowanie dysku	362
Implementowanie RAID 5: dysk rozłożony z parzystością	364

Zarządzanie macierzami RAID i przywracanie w razie awarii	365
Dzielenie zestawu dublowania	365
Ponowna synchronizacja i naprawa zestawu dublowania.	365
Naprawa dublowanego woluminu systemowego, aby umożliwić rozruch	366
Usuwanie zestawu dublowania	367
Naprawa zestawu rozłożonego bez parzystości.	367
Regenerowanie zestawu rozłożonego z parzystością	367
Zarządzanie jednostkami LUN w sieciach SAN.	368
Konfigurowanie połączeń sieci SAN Fibre Channel	369
Konfigurowanie połączeń interfejsu iSCSI dla sieci SAN	370
Dodawanie i usuwanie celów.	371
Tworzenie, rozszerzania, przypisywanie i usuwanie jednostek LUN	371
Definiowanie klastra serwerów w narzędziu Storage Manager For SANs	371
14 Zarządzanie osłonami plików i raportami magazynowymi	373
Znaczenie osłon plików i raportów magazynowania	373
Zarządzanie osłonami plików i raportami magazynowymi	377
Ustawienia globalne zasobu plików	377
Zarządzanie grupami plików w osłonach	380
Zarządzanie szablonami osłon plików	381
Tworzenie osłon plików	384
Definiowanie wyjątków osłony plików.	384
Tworzenie i planowanie raportów magazynowych	384
15 Udostępnianie danych, zabezpieczenia i inspekcja	387
Włączanie i korzystanie z udostępniania plików	388
Konfigurowanie standardowego udostępniania plików	391
Przeglądanie istniejących udziałów	391
Tworzenie folderów udostępnionych.	393
Tworzenie dodatkowych udziałów na istniejącym udziale	396
Zarządzanie uprawnieniami udziału	396
Uprawnienia udziału	396
Przeglądanie uprawnień udziału.	397
Konfigurowanie uprawnień udziału	397
Modyfikowanie istniejących uprawnień udziału.	398
Usuwanie uprawnień udziału dla użytkowników i grup	399
Zarządzanie istniejącymi udziałami	399
Istota udziałów specjalnych	399
Podłączanie do udziałów specjalnych	400
Przeglądanie sesji użytkowników i komputerów	401
Zatrzymywanie udostępniania plików i folderów	403
Konfigurowanie udostępniania NFS.	403
Wykorzystanie kopii w tle	405
Istota kopii w tle	405
Tworzenie kopii w tle	406
Odtwarzanie kopii w tle	406
Odtwarzanie całego woluminu do poprzedniej kopii w tle	407
Usuwanie kopii w tle.	407

Wyłączanie kopii w tle	407
Podłączanie się do dysków sieciowych	408
Mapowanie dysku sieciowego	408
Odłączanie dysku sieciowego	409
Dziedziczenie, własność i zarządzanie obiektami	409
Obiekt i menedżer obiektu	409
Własność i transfer obiektu	409
Dziedziczenie obiektu	411
Uprawnienia folderów i plików	411
Istota uprawnień folderów i plików	412
Konfiguracja uprawnień folderów i plików	415
Inspekcja zasobów systemu	416
Konfiguracja zasad inspekcji	416
Inspekcja plików i folderów	418
Inspekcja rejestru	420
Inspekcja obiektów usługi Active Directory	420
Wykorzystanie, konfiguracja i zarządzanie przydziałami dysków w systemie NTFS	421
Istota i sposób wykorzystania przydziałów dysku w systemie NTFS	422
Konfigurowanie zasad przydziałów dysku w systemie NTFS	423
Włączanie przydziałów dysku na woluminach z systemem plików NTFS	426
Przeglądanie wpisów przydziałów dysku	427
Tworzenie wpisów przydziałów dysku	428
Usuwanie wpisów przydziałów dysku	429
Eksportowanie i importowanie ustawień przydziałów dysku NTFS	430
Wyłączanie przydziałów NTFS	430
Wykorzystanie, konfiguracja i zarządzanie Resource Manager Disk Quotas	431
Istota przydziałów dysku Resource Manager	431
Zarządzanie szablonami przydziałów dysku	432
Tworzenie przydziałów dysku Resource Manager	434
16 Tworzenie kopii zapasowych i przywracanie danych	435
Tworzenie planu wykonywania kopii zapasowych i odzyskiwania danych	435
Tworzenie planu ratunkowego	435
Podstawowe typy kopii zapasowych	436
Kopie różnicowe i przyrostowe	437
Nośniki i urządzenia kopii zapasowych	438
Najczęstsze rozwiązania	438
Zakup i zastosowanie nośników kopii zapasowych	439
Wybór narzędzia kopii zapasowej	440
Zasadnicze kwestie dotyczące kopii zapasowych	441
Instalowanie kopii zapasowej systemu Windows i narzędzi odzyskiwania	441
Rozpoczęcie pracy z Windows Server Backup	442
Rozpoczęcie pracy z narzędziem kopii zapasowej z wiersza poleceń	444
Polecenia Wbadmin	446
Polecenia ogólne	446
Polecenia zarządzania kopiami zapasowymi	446
Polecenia zarządzania przywracaniem danych	447

Kopie zapasowe serwera	448
Konfigurowanie harmonogramu kopii zapasowych	449
Modyfikowanie i usuwanie harmonogramów kopii zapasowych	451
Tworzenie i planowanie kopii zapasowych przez Wbadmin	453
Ręczne tworzenie kopii zapasowej	454
Odzyskiwanie serwera po awarii sprzętu lub błędzie podczas rozruchu	455
Uruchamianie serwera w trybie awaryjnym	458
Przywracanie po awarii podczas uruchamiania	459
Zabezpieczanie i odtwarzanie stanu systemu	459
Odzyskiwanie Active Directory	460
Przywracanie systemu operacyjnego i pełnego systemu	461
Odzyskiwanie aplikacji, woluminów niesystemowych, plików i folderów	463
Zarządzanie zasadą odzyskiwania szyfrowania	464
Istota certyfikatów szyfrowania i zasady odzyskiwania	464
Konfigurowanie zasady odzyskiwania EFS	465
Tworzenie kopii zapasowych i odzyskiwanie zaszyfrowanych danych i certyfikatów	466
Tworzenie kopii zapasowych certyfikatów szyfrowania	467
Odzyskiwanie certyfikatów szyfrowania	467

Część IV Administrowanie siecią w Windows Server 2008

17 Zarządzanie sieciami TCP/IP	471
Nawigowanie w sieci w systemie Windows Server 2008	471
Nowoczesne opcje sieciowe w systemach Windows Vista i Windows Server 2008	474
Instalowanie obsługi sieci TCP/IP	476
Konfigurowanie sieci TCP/IP	477
Konfigurowanie statycznych adresów IP	478
Konfigurowanie dynamicznych adresów IP oraz alternatywnego adresowania IP	479
Konfigurowanie wielu bram	480
Zarządzanie połączeniami sieciowymi	481
Sprawdzanie statusu, prędkości i aktywności połączeń lokalnych	481
Wyłączanie i włączanie połączeń lokalnych	482
Zmianie nazw połączeń lokalnych	482
18 Zarządzanie drukarkami sieciowymi i usługami drukowania	483
Zarządzanie rolą usługi drukowania	483
Urządzenia do drukowania	483
Ważne kwestie dotyczące drukowania	484
Konfigurowanie serwerów wydruku	485
Włączanie i wyłączanie udostępniania drukarek	486
Podstawy zarządzania drukowaniem	487
Instalowanie drukarek	488
Zastosowanie funkcji automatycznego instalowania dostępnych przez Print Management	489
Instalowanie i konfigurowanie podłączonych fizycznie drukarek	489
Instalowanie drukarek podłączonych do sieci	492
Podłączanie utworzonych drukarek do sieci	494

Wdrażanie połączeń drukarki	495
Konfigurowanie ograniczeń trybu Wskaż i drukuj.	497
Przenoszenie drukarek do nowego serwera wydruku.	499
Automatyczne monitorowanie drukarek i kolejek.	500
Rozwiązywanie problemów buforowania	501
Konfigurowanie właściwości drukarki	502
Dodawanie komentarzy i informacji o lokalizacji.	502
Wyświetlanie drukarek w Active Directory	502
Zarządzanie sterownikami drukarek.	502
Konfigurowanie strony separatora i zmiana trybu urządzenia do drukowania.	503
Zmiana portu drukarki	504
Planowanie i priorytety zadań drukowania.	504
Uruchamianie i zatrzymywanie udostępniania drukarek	506
Konfigurowanie uprawnień dostępu do drukarki.	506
Inspekcja zadań drukowania	507
Konfigurowanie ustawień domyślnych dokumentów	508
Konfigurowanie właściwości serwera wydruku	508
Umiejscowianie foldera buforu i włączanie drukowania w NTFS.	508
Zarządzanie dużą ilością wydruków.	509
Zapisywanie zdarzeń drukowania.	509
Włączanie powiadamiania o błędach zadań drukowania.	509
Zarządzanie zadaniami drukowania na drukarkach zdalnych i lokalnych.	509

19 Korzystanie z mechanizmu DHCP	513
Istota mechanizmu DHCP	513
Wykorzystanie i konfiguracja dynamicznego adresowania IPv4	513
Wykorzystanie i konfiguracja dynamicznego adresowania IPv6	514
Sprawdzanie nadania adresów IP	517
Istota zakresów.	517
Instalowanie serwera DHCP.	518
Instalowanie komponentów DHCP.	518
Korzystanie z konsoli DHCP.	521
Podłączanie się do zdalnych serwerów DHCP	522
Uruchamianie i zatrzymywanie serwera DHCP.	522
Autoryzowanie serwera DHCP w Active Directory.	522
Konfigurowanie serwerów DHCP	523
Wiązanie serwera DHCP wyposażonego w wiele kart sieciowych z określonym adresem IP.	523
Aktualizowanie statystyk DHCP.	524
Prowadzenie inspekcji DHCP i rozwiązywanie problemów.	524
Integrowanie DHCP i DNS	525
Integrowanie DHCP i NAP	526
Unikanie konfliktów adresów IP	529
Zapisywanie i przywracanie konfiguracji DHCP	530
Zarządzanie zakresami DHCP	530
Zarządzanie zakresami	530
Zarządzanie superzakresami	539

Zarządzanie pulami adresów, dzierżawami i zastrzeżeniami	540
Przeglądanie statystyk zakresu	540
Definiowanie nowego przedziału wykluczeń	540
Usuwanie przedziału wykluczeń	540
Rezerwowanie adresów DHCP.	541
Modyfikowanie właściwości zastrzeżenia	542
Usuwanie dzierżaw i zastrzeżeń	542
Tworzenie kopii zapasowej i przywracanie bazy danych DHCP	543
Wykonywanie kopii zapasowej bazy danych DHCP.	543
Przywracanie bazy danych DHCP z kopii zapasowej.	544
Wykorzystanie kopiowania i przywracania do przenoszenia bazy danych DHCP na nowy serwer.	544
Wymuszanie regeneracji bazy danych przez usługę DHCP Server	544
Uzgodnianie dzierżaw i zastrzeżeń.	545
20 Optymalizacja DNS	547
Istota DNS	547
Integracja Active Directory i DNS	548
Włączanie DNS w sieci	549
Konfigurowanie rozwiązywania nazw na klientach DNS	551
Instalowanie serwerów DNS	553
Instalowanie i konfigurowanie usługi DNS Server	553
Konfigurowanie podstawowego serwera DNS	555
Konfigurowanie pomocniczego serwera DNS	557
Konfigurowanie wyszukiwania wstecznego.	558
Konfigurowanie nazw globalnych.	560
Zarządzanie serwerami DNS	560
Dodawanie serwerów zdalnych do konsoli DNS	561
Usuwanie serwera z konsoli DNS	561
Uruchamianie i zatrzymywanie usługi DNS Server	562
Tworzenie domen podrzędnych wewnątrz stref	562
Tworzenie domen podrzędnych w oddzielnych strefach	562
Usuwanie domeny lub podsieci	563
Zarządzanie rekordami DNS	564
Dodawanie rekordów adresów i wskaźników	564
Dodawanie aliasów nazw DNS za pomocą rekordu CNAME	566
Dodawanie serwerów wymiany poczty	566
Dodawanie serwerów nazw	568
Przeglądanie i aktualizowanie rekordów DNS	569
Aktualizowanie właściwości strefy i rekordu SOA	569
Modyfikowanie rekordu SOA.	569
Dopuszczanie i ograniczanie transferów stref.	571
Powiadamianie serwerów pomocniczych o zmianach.	572
Określanie typu strefy.	573
Włączanie i wyłączanie aktualizacji automatycznych	573
Zarządzanie konfiguracją i zabezpieczeniami serwera DNS	573
Włączanie i wyłączanie adresów IP używanych przez serwer DNS.	574
Kontrolowanie dostępu do serwerów DNS poza organizacją	574

Włączanie i wyłączanie rejestrowania zdarzeń	576
Wykorzystanie rejestrowania debugowania do śledzenia aktywności DNS.	576
Monitorowanie serwera DNS.	577
Indeks	579

Rozdział 1

Wprowadzenie do administracji Windows Server 2008

W tym rozdziale:

Windows Server 2008 i Windows Vista	3
Poznanie systemu Windows Server 2008	5
Narzędzia i protokoły sieciowe	7
Kontrolery domeny, serwery członkowskie i usługi domenowe	9
Usługi rozwiązywania nazw	12
Często używane narzędzia	18

Windows Server 2008 to wydajny, elastyczny i w pełni funkcjonalny system operacyjny, zbudowany w oparciu o usprawnienia, które firma Microsoft wprowadziła w dodatku Service Pack 1 oraz w wersji Release 2 systemu Windows Server 2003. Systemy Windows Server oraz Windows Vista mają wiele wspólnych cech, gdyż obydwa powstały w ramach jednego projektu programistycznego. Funkcje te wykorzystują wspólny kod źródłowy i rozciągają się na wiele obszarów obu systemów operacyjnych, takich jak zarządzanie, zabezpieczenia, obsługa sieci i przechowywanie danych. Oznacza to, że znaczna część znanych już informacji dotyczących Windows Vista będzie miała zastosowanie także w systemie Windows Server 2008.

Rozdział ten zawiera omówienie podstawowych zagadnień związanych z wykorzystywaniem systemu Windows Server 2008 i ukazuje zmiany w architekturze, które mają wpływ na stosowanie i zarządzanie systemem. Zarówno w tym rozdziale, jak i w pozostałych częściach książki Czytelnik znajdzie szczegółowe omówienie zmian wprowadzonych w mechanizmach zabezpieczeń. Zostaną przedstawione techniki, które pozwalają usprawnić bezpieczeństwo systemu we wszystkich aspektach, poczynając od bezpieczeństwa fizycznego, przez ochronę informacji, aż po zabezpieczenia sieci. Wprawdzie głównym obszarem zainteresowań tej książki jest administrowanie systemem Windows Server 2008, jednak omówione tu wskazówki i techniki będą przydatne dla każdego, kto obsługuje, projektuje aplikacje lub po prostu pracuje z systemem Windows Server 2008.

Windows Server 2008 i Windows Vista

Podobnie jak system Windows Vista, Windows Server 2008 wykorzystuje rewolucyjną architekturę o następujących cechach:

Budowa modułowa, zapewniająca niezależność wersji językowych oraz mechanizm obrazów dysków zapewniający niezależność sprzętową Modułowa budowa oznacza, że każdy składnik systemu operacyjnego został zaprojektowany jako odrębny blok, który

można łatwo dodać lub usunąć. Funkcjonalność ta zapewnia podstawy nowej architektury konfiguracyjnej Windows Server 2008. Firma Microsoft rozpowszechnia system Windows Server 2008 na nośnikach zawierających obrazy dysków w formacie Windows Imaging Format (WIM), które dzięki kompresji i przechowywaniu tylko pojedynczych wystąpień plików pozwalają znacząco zmniejszyć wielkość plików obrazów.

Środowisko przedinstalacyjne i przeduruchomieniowe Środowisko przedinstalacyjne Windows Preinstallation Environment 2.0 (Windows PE 2.0) zastępuje MS-DOS jako środowisko instalacyjne i zapewnia rozruchowe otoczenie początkowe dla zadań instalacji, wdrażania, przywracania systemu lub rozwiązywania problemów. Środowisko przeduruchomieniowe Windows Pre-Boot Environment zapewnia środowisko z menedżerem rozruchu, który pozwala wybrać aplikację startową, która ma zostać uruchomiona w celu załadowania systemu operacyjnego. W komputerach z zainstalowanymi kilkoma systemami operacyjnymi można uzyskać dostęp do systemów starszych niż Windows Vista, wybierając wpis wcześniejszego systemu operacyjnego.

Kontrola kont użytkowników i podnoszenie uprawnień Mechanizm kontroli kont użytkowników (User Account Control – UAC) podnosi bezpieczeństwo systemu komputerowego dzięki zapewnieniu rzeczywistej separacji standardowych kont użytkowników od kont administratorów. Dzięki UAC wszystkie aplikacje są wykonywane przy użyciu albo uprawnień kont standardowych, albo administracyjnych, przy czym użytkownik jest domyślnie informowany (przez monit zabezpieczeń) za każdym razem, gdy próbuje uruchomić aplikację wymagającą przywilejów administratora. Sposób działania tego monitu zależy od ustawień zawartych w Zasadach grupy (Group Policy). Przy zalogowaniu na wbudowane konto administratora monity te zazwyczaj nie są wyświetlane.

Funkcje wspólne dla Windows Vista i Windows Server 2008 używają identycznych interfejsów zarządzających. W istocie niemal każde narzędzie Panelu sterowania, które jest dostępne w Windows Server 2008, jest identyczne lub niemal takie samo, jak jego odpowiednik w systemie Windows Vista. Istnieją oczywiście wyjątki dotyczące domyślnych ustawień standardowych. Ponieważ Windows Server 2008 nie używa ocen wydajnościowych, serwery Windows nie zawierają danych Windows Experience Index. System Windows Server 2008 nie korzysta z trybu uśpienia (Sleep) ani podobnych, nie występuje w nim funkcjonalność pozwalająca na uśpienie, hibernację czy przywrócenie działalności systemu. Także funkcje zarządzania zasilaniem zwykle nie są potrzebne w serwerach, tak więc Windows Server 2008 ma tylko ograniczony zestaw opcji tego rodzaju. Co więcej, w systemie Windows Server 2008 nie są stosowane rozszerzenia Windows Aero (Aero Glass, Flip, 3D Flip i tak dalej), funkcje Windows Sidebar, Windows Gadgets ani inne usprawnienia wyglądu. Przyczyna takiego stanu rzeczy leży w tym, że Windows Server 2008 zaprojektowany został w celu osiągnięcia optymalnej wydajności zadań serwerowych i nie przewiduje się w nim rozbudowanego personalizowania wyglądu pulpitu.

Ponieważ wspólne cechy Windows Vista i Windows Server 2008 są tak bardzo podobne, nie będziemy tu tracić czasu na omawianie zmian interfejsu, których dokonano w stosunku do poprzednich wersji systemu operacyjnego, analizę działania mechanizmu UAC i tak dalej. Szczegółowe omówienie tych funkcji zawiera publikacja *Microsoft Windows Vista Administrator's Pocket Consultant* (Microsoft Press, 2007)*, z której warto korzystać łącznie z niniejszą pozycją. Oprócz omówienia szerokiego zakresu zadań administracyjnych, książka ta przedstawia dostosowywanie systemu operacyjnego i środowiska Windows,

* Wydanie polskie: *Vademecum administratora Microsoft Windows Vista* (APN Promise, 2007)

konfigurowanie urządzeń sprzętowych i sieciowych, zarządzanie dostępem użytkowników i ustawieniami globalnymi, konfigurowanie komputerów przenośnych oraz sieci bezprzewodowych, korzystanie z funkcji zdalnego zarządzania i pomocy zdalnej, rozwiązywanie problemów systemowych i wiele, wiele innych zagadnień. W tej książce zaś skoncentrujemy się na administrowaniu usługą katalogową, sieciami i systemami magazynowania danych.

Poznawanie systemu Windows Server 2008

Rodzina systemów operacyjnych Windows Server 2008 obejmuje kilka wydań dostosowanych do różnych typów zastosowań: Windows Server 2008, Standard Edition; Windows Server 2008, Enterprise Edition, oraz Windows Server 2008, Datacenter Edition.

Windows Server 2008, Standard Edition Wydanie to bezpośrednio zastępuje Windows Server 2003 i zostało zaprojektowane do udostępniania usług i zasobów dla innych systemów pracujących w sieci. System operacyjny dysponuje wielką liczbą funkcji i opcji konfiguracyjnych. Wersja Windows Server 2008, Standard Edition zapewnia obsługę do czterech procesorów w trybie SMP (*symmetric multiprocessing*) i do 4 gigabajtów (GB) pamięci w wersji 32-bitowej lub 32 GB w systemach 64-bitowych.

Windows Server 2008, Enterprise Edition Wydanie Enterprise Edition rozszerza funkcjonalność oferowaną przez wersję Standard Edition, zapewniając większą skalowalność i oferując dodatkowe funkcje, takie jak usługa klastrowania (Cluster Service) oraz Active Directory Federated Services. Zapewnia wsparcie dla modułów pamięci wymienianych na gorąco (w systemach 64-bitowych) oraz niejednorodnego dostępu do pamięci (Non-uniform Memory Access – NUMA). Serwery wersji Enterprise mogą używać do 32 GB RAM przy procesorach x86 lub do dwóch terabajtów (TB) RAM w systemach 64-bitowych i do 8 procesorów.

Windows Server 2008, Datacenter Edition Jest to najbardziej rozbudowana wersja serwera Windows. Dysponuje ulepszonymi funkcjami klastrowania i obsługą bardzo wielkich pamięci – do 64 GB RAM w systemach x86 lub do dwóch TB RAM w wersji 64-bitowej. Minimalna obsługiwana konfiguracja to 8 procesorów, zaś maksymalna liczba procesorów wynosi 64.

Windows Web Server 2008 Jest to odpowiednik wydania Web Edition dla Windows Server 2008. Ponieważ wersja ta zaprojektowana została w celu zapewnienia tylko usług Web dla witryn i aplikacji internetowych lub intranetowych, wspiera tylko funkcje związane z tym zastosowaniem. W szczególności edycja ta zawiera Microsoft .NET Framework, Microsoft Internet Information Services (IIS), ASPNET, funkcje serwera aplikacji i równoważenia obciążenia sieciowego. Wydanie to jest za to pozbawione wielu innych funkcji, w tym Active Directory. Windows Web Server 2008 może obsłużyć do 2 GB pamięci RAM oraz dwa procesory.

Uwaga Poszczególne wydania systemu zawierają te same bazowe funkcje i narzędzia administracyjne. Oznacza to, że techniki omawiane w tej książce mogą być stosowane bez względu na to, która wersja Windows Server 2008 jest używana. Trzeba jednak zauważyć, że ponieważ w wydaniu Web nie można zainstalować Active Directory, nie można wypromować serwera używającego Windows Web Server 2008 do roli kontrolera domeny. Serwer ten może jednak być częścią domeny Active Directory.

Wskazówka Przetwarzanie 64-bitowe bardzo rozwinęło się od czasu, gdy zostało po raz pierwszy wprowadzone w systemach operacyjnych Windows. Mówiąc o przeznaczonych dla architektury x86 będziemy mówić o systemach 32-bitowych, zaś systemy zaprojektowane dla architektury x64 określać będziemy terminem 64-bitowych. Wsparcie dla procesorów Itanium 64-bit (IA-64) nie jest już standardową cechą systemów operacyjnych Windows. Firma Microsoft opracowała oddzielną wersję Windows Server 2008 dla komputerów opartych na procesorach Itanium, przy czym wydanie to ma na celu udostępnić szczególne funkcje serwerowe. W rezultacie niektóre role serwera i funkcjonalności nie są wspierane w systemach IA-64.

Podczas instalacji systemu Windows Server 2008 wykonuje się konfigurację stosownie do roli, jaką system ten ma odgrywać w sieci, zgodnie z poniższymi wskazówkami:

- Serwery mogą być częścią grupy roboczej lub domeny.
- Grupa robocza to luźny związek komputerów połączonych siecią, przy czym każdy komputer zarządzany jest niezależnie od pozostałych.
- Domena to zbiór komputerów, którymi można zarządzać zbiorowo za pośrednictwem kontrolerów domeny, czyli komputerów systemu Windows Server 2008 sterujących dostępem do sieci, katalogowej bazy danych i zasobów udostępnionych.

Uwaga W tej książce zarówno termin „Windows Server 2008”, jak i „rodzina Windows Server 2008” oznacza rodzinę czterech produktów: Windows Server 2008, Standard Edition; Windows Server 2008, Enterprise Edition; Windows Server 2008, Datacenter Edition oraz Windows Web Server 2008. Poszczególne wydania serwera wspierają tę samą podstawową funkcjonalność i narzędzia administracyjne.

Wszystkie wersje Windows Server 2008 udostępniają dwa widoki menu Start:

Klasyczne menu Start Jest to widok używany we wcześniejszych wersjach Windows. W tej wersji kliknięcie przycisku Start wyświetla wyskakujące okno zapewniające bezpośredni dostęp do menu i programów.

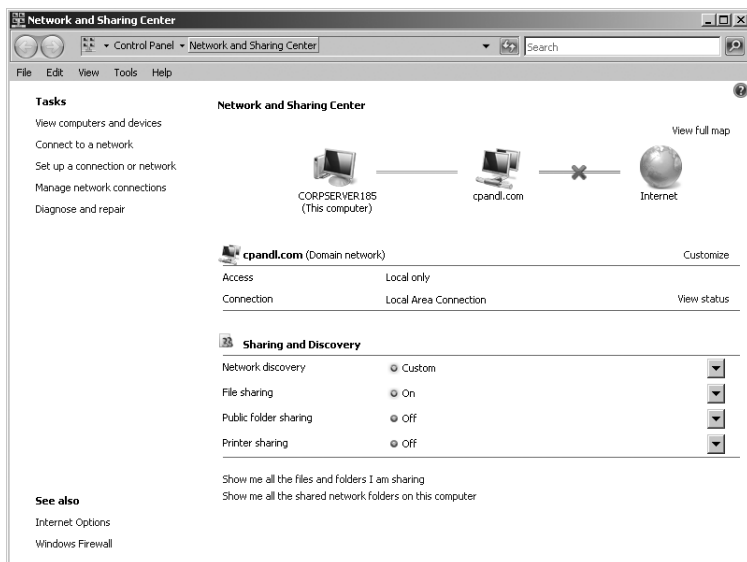
Przy korzystaniu z klasycznego menu Start dostęp do narzędzi administracyjnych można uzyskać klikając Start, wskazując Programs (Programy), a następnie klikając Administrative Tools (Narzędzia administracyjne). W celu otwarcia Panelu sterowania należy kliknąć Start, wskazać Settings (Ustawienia), po czym kliknąć Control Panel (Panel sterowania).

Proste menu Startu Zapewnia bezpośredni dostęp do często używanych programów i pozwala bezpośrednio wykonać typowe zadania. Można na przykład kliknąć Start, a następnie Computer (Komputer), aby uzyskać dostęp do dysków i napędów wymiennych zainstalowanych w serwerze.

Przy korzystaniu z prostego menu Start dostęp do narzędzi administracyjnych można uzyskać klikając Start, a następnie Administrative Tools. Analogicznie w celu wyświetlenia Panelu sterowania należy kliknąć Start i następnie Control Panel.

Narzędzia i protokoły sieciowe

Podobnie jak Windows Vista, Windows Server 2008 zawiera nowy zestaw narzędzi sieciowych, w tym Network Explorer (Eksplorator sieci), Network And Sharing Center (Centrum sieci i udostępniania), Network Map (Mapa sieci) oraz Network Diagnostics (Diagnozowanie sieci). Rysunek 1-1 ukazuje narzędzie Network And Sharing Center.



Rysunek 1-1 Narzędzie Network And Sharing Center zapewnia szybki dostęp do opcji udostępniania, wyszukiwania w sieci i konfigurowania usług sieciowych.

Istota opcji sieciowych

Opcje konfiguracyjne dostępne w narzędziu Network And Sharing Center sterują podstawowymi ustawieniami sieci. Jeśli ustawienia odkrywania sieci są włączone i serwer jest przyłączony do sieci, będzie on mógł dostrzec inne komputery i urządzenia w sieci, a zarazem sam będzie w niej widoczny. Przy włączaniu lub wyłączeniu ustawień udostępniania różnorodne opcje stają się dostępne lub nieosiągalne. Opcje udostępniania obejmują udostępnianie plików, folderów publicznych, drukarek oraz udostępnianie zabezpieczone hasłem. Zagadnienia te stanowią treść rozdziału 15, „Udostępnianie danych, zabezpieczenia i inspekcja”.

W systemach Windows Vista oraz Windows Server 2008 sieci są klasyfikowane jako należące do jednego z następujących typów:

Sieć domenowa Sieć, w której komputery są członkami domeny przedsiębiorstwa. Domyślnie w sieciach domenowych odkrywanie jest dozwolone, co zmniejsza liczbę ograniczeń i pozwala komputerom w sieci lokalizować inne komputery i urządzenia w tej sieci.

Sieć prywatna Sieć, w której komputery są skonfigurowane jako członkowie grupy roboczej i nie są bezpośrednio połączone z Internetem. Domyślnie w sieci prywatnej odkrywanie jest dozwolone, co zmniejsza liczbę ograniczeń i pozwala komputerom w sieci lokalizować inne komputery i urządzenia w tej sieci.

Sieć publiczna Sieć dostępna publicznie (w takim miejscu, jak kawiarenka internetowa, port lotniczy itp.), w której komputery mogą być bezpośrednio połączone z Internetem. W sieciach publicznych odkrywanie sieci jest domyślnie zablokowane, co zwiększa bezpieczeństwo, gdyż powstrzymuje komputery przed ujawnianiem swoich zasobów, ale ogranicza możliwość wyszukiwania innych komputerów i urządzeń w tej sieci.

Ponieważ system zapamiętuje ustawienia oddzielnie dla każdej kategorii sieci, można zastosować różne ustawienia blokowania i zezwalania w każdej z nich. Przy pierwszym połączeniu z siecią użytkownik zobaczy okno dialogowe, które pozwala określić kategorię sieci – publiczną lub prywatną. Jeśli po wybraniu opcji sieci prywatnej komputer ustali, że został przyłączony do domeny, której jest członkiem, kategoria sieci zostanie samoczynnie zmieniona na sieć domenową.

Korzystanie z protokołów sieciowych

Aby serwer mógł połączyć się z siecią, konieczne jest zainstalowanie w nim karty sieciowej oraz obsługi Transmission Control Protocol/Internet Protocol (TCP/IP). Windows Server 2008 wykorzystuje TCP/IP jako domyślny protokół sieci rozległej (WAN). Zazwyczaj obsługa sieci jest instalowana podczas instalacji systemu operacyjnego. Obsługę protokołów TCP/IP można również włączyć przez właściwości lokalnego połączenia sieciowego.

Protokoły TCP i IP pozwalają komputerom na komunikowanie się przez różne sieci i Internet za pośrednictwem kart sieciowych. Podobnie jak w systemie Windows Vista, Windows Server 2008 dysponuje dwupoziomą architekturą IP, w której zaimplementowane są zarówno Internet Protocol w wersji 4 (IPv4), jak i Internet Protocol w wersji 6 (IPv6), oraz wspólnymi warstwami transportową i ramki. Podczas gdy IPv4 używa adresów 32-bitowych i jest podstawową wersją protokołu stosowaną w większości sieci, w tym w Internecie, IPv6 używa adresów 128-bitowych i jest następną generacją protokołu IP.

32-bitowe adresy IPv4 są zazwyczaj przedstawiane jako cztery wartości dziesiętne rozdzielane kropkami, na przykład 127.0.0.1 lub 192.168.10.52. Liczby te są często nazywane oktetami, gdyż każda z nich reprezentuje 8 bitów pełnej 32-bitowej liczby. Przy standardowych adresach emisji pojedynczej (*unicast*) IPv4 część adresu o zmiennej długości określa identyfikator (adres) sieci, zaś pozostała część określa identyfikator hosta. Nie występuje żadna korelacja pomiędzy adresem hosta protokołu IPv4 i wewnętrznym adresem sprzętowym (MAC) używanym przez kartę sieciową.

128-bitowe adresy protokołu IPv6 są podzielone na osiem 16-bitowych bloków rozdzielanych dwukropkami. Każdy blok jest wyrażany w postaci szesnastkowej, na przykład FEC0:0:0:02BC:FF:BECB:FE4F:961D. W przypadku standardowych adresów emisji pojedynczej pierwsze 64 bity reprezentują identyfikator sieci, zaś pozostałe – interfejs sieciowy. Ponieważ wiele bloków adresu IPv6 wynosi 0, ciągły zbiór takich bloków można oznaczyć jako „::”, co określa się terminem „notacji podwójnego dwukropka (*double-colon notation*). Przy użyciu tej notacji dwa bloki zerowe w poprzednim przykładzie można skompresować do postaci FEC0::02BC:FF:BECB:FE4F:961D. W ten sam sposób można skompresować trzy i więcej bloków zerowych. Na przykład adres FFE8:0:0:0:0:0:1 można zapisać jako FFE8::1.

Po wykryciu sprzętu sieciowego podczas instalowania systemu operacyjnego obydwa protokoły (IPv4 i IPv6) są włączane domyślnie. Nie zachodzi zatem potrzeba instalowania dodatkowego składnika, aby umożliwić obsługę IPv6. Zmodyfikowana architektura IP w systemach Windows Vista i Windows Server 2008 jest określana terminem Next Generation TCP/IP (TCP/IP następnej generacji) i zawiera wiele rozszerzeń, które usprawniają korzystanie z protokołów IPv4 i IPv6.

Kontrolery domeny, serwery członkowskie i usługi domenowe

Podczas instalowania Windows Server 2008 na nowym komputerze można skonfigurować go tak, aby był serwerem członkowskim, kontrolerem domeny lub serwerem autonomicznym. Różnice pomiędzy tymi typami serwerów są niezwykle ważne. Serwery członkowskie stanowią część domeny, ale nie przechowują informacji katalogowych. Kontrolery domeny różnią się od serwerów członkowskich tym, że przechowują informacje katalogowe i zapewniają uwierzytelnianie oraz usługi katalogowe komputerom w domenie. Serwery autonomiczne nie są częścią domeny. Ponieważ serwery takie zawierają własne bazy danych użytkowników, niezależnie uwierzytelniają żądania logowania.

Korzystanie z Active Directory

Podobnie jak w Windows 2000 i Windows Server 2003, w systemie Windows Server 2008 nie są rozróżniane podstawowe (główne) i pomocnicze kontrolery domeny. Zamiast tego Windows Server 2008 wspiera model replikacji o wielu wzorcach. W modelu tym każdy kontroler domeny może przetwarzać zmiany w katalogu i następnie zreplikować je automatycznie do pozostałych kontrolerów domeny. Stanowi to różnicę w stosunku do modelu replikacji pojedynczego wzorca stosowanego w systemie Windows NT, w którym podstawowy kontroler domeny przechowywał główną (edytowalną) wersję katalogu, zaś pomocnicze kontrolery utrzymywały kopię głównej bazy. Ponadto w Windows NT dystrybucji podlegała tylko baza danych menedżera kont zabezpieczeń (Security Account Manager – SAM), podczas gdy w wersji Windows 2000 i późniejszych edycjach Windows Server replikowany jest pełny katalog informacji zwany magazynem danych (*data store*). Magazyn danych zawiera zbiory obiektów reprezentujących konta użytkowników, grup i komputerów, a także udostępniane zasoby, takie jak serwery, pliki czy drukarki.

Domeny wykorzystujące usługę katalogową Active Directory określane są terminem *domen Active Directory*, co odróżnia je od domen Windows NT. Jakkolwiek domeny Active Directory mogą funkcjonować dysponując tylko jednym kontrolerem domeny, można i należy stosować kilka kontrolerów domeny. W ten sposób w razie awarii jednego z kontrolerów można nadal zapewnić obsługę uwierzytelniania i innych krytycznych zadań przez pozostałe kontrolery domeny.

Firma Microsoft dokonała wielu fundamentalnych zmian w wersji Active Directory zastosowanej w Windows Server 2008. W szczególności ujednotliciono funkcjonalność usługi katalogowej i utworzono rodzinę powiązanych usług, w tym:

Active Directory Certificate Services (AD CS) Usługi certyfikatów Active Directory zapewniają funkcje niezbędne dla wystawiania i odwoływania certyfikatów dla użytkowników, komputerów klienckich i serwerów. AD CS wykorzystuje Urzędy certyfikacji (Certificate Authority – CA), które są odpowiedzialne za potwierdzanie tożsamości użytkowników

i wystawianie certyfikatów dla tych tożsamości. Domeny mogą zawierać główne CA przedsiębiorstwa, które są serwerami certyfikatów dla korzenia (początku) łańcucha hierarchii certyfikatów i najbardziej zaufanymi serwerami w strukturze, oraz podrzędne CA, które są członkami odpowiednich szczebli hierarchii przedsiębiorstwa. Grupy robocze mogą zawierać autonomiczne główne serwery certyfikacji wraz z podrzędnymi CA, zapewniając podobną hierarchiczną strukturę, ale bez środowiska domenowego.

Active Directory Domain Services (AD DS) Usługi domenowe Active Directory zapewniają podstawowe usługi niezbędne do utworzenia domeny, w tym magazyn danych przechowujący informacje o obiektach w sieci i udostępniający je użytkownikom. AD DS wykorzystuje kontrolery domeny do zarządzania dostępem do zasobów sieci. Gdy użytkownik uwierzytli się logując się w domenę, jego poświadczenia mogą zostać użyte do uzyskiwania dostępu do zasobów sieciowych. Ponieważ AD DS jest podstawową częścią Active Directory i jest niezbędny dla funkcjonowania aplikacji i rozwiązań opartych na katalogu, zazwyczaj określa się go po prostu terminem Active Directory, a nie Active Directory Domain Services lub AD DS.

Active Directory Federation Services (AD FS) AD FS uzupełnia funkcje uwierzytelniania i zarządzania dostępem oferowane przez AD DS przez ich rozszerzenie na sieć World Wide Web. AD FS wykorzystuje agentów Web do zapewniania użytkownikom dostępu do wewnętrznie utrzymywanych aplikacji sieci Web oraz proxy, obsługujące dostęp klientów. Po skonfigurowaniu AD FS użytkownicy mogą użyć swoich cyfrowych identyfikatorów do uwierzytelniania w sieci Web i dostępu do wewnętrznych aplikacji Web, używając przeglądarki takiej jak Internet Explorer.

Active Directory Lightweight Directory Services (AD LDS) AD LDS udostępnia magazyn danych dla aplikacji wykorzystujących usługi katalogowe, który nie wymaga AD DS i nie musi być instalowany na kontrolerach domeny. AD LDS nie jest usługą systemu operacyjnego i może być wykorzystywana zarówno w środowisku domenowym, jak i grupy roboczej. Każda aplikacja uruchomiona na serwerze może mieć swój własny magazyn danych zaimplementowany za pośrednictwem AD LDS.

Active Directory Rights Management Services (AD RMS) AD RMS zapewnia warstwę ochrony dla informacji organizacyjnych, którą można rozszerzyć poza granice przedsiębiorstwa, umożliwiając zabezpieczenie wiadomości e-mail, dokumentów, intranetowych stron Web i wielu innych form informacji przed nieautoryzowanym dostępem. AD RMS wykorzystuje usługi certyfikatów do wydawania certyfikatów uprawnień, identyfikujących zaufanych użytkowników, grupy lub usługi. Drugim elementem jest usługa licencjonowania, zapewniająca uwierzytelnionym użytkownikom, grupom i usługom dostęp do chronionych informacji. Trzecim składnikiem jest usługa rejestrująca, która monitoruje i zarządza usługą zarządzania uprawnieniami. Po ustanowieniu relacji zaufania użytkownicy dysponujący certyfikatem uprawniającym mogą uzyskać prawa dostępu do informacji. Uprawnienia te pozwalają kontrolować, którzy użytkownicy mogą mieć dostęp do danych, a także co mogą z nimi zrobić. Szyfrowanie gwarantuje, że dostęp do informacji chronionych jest kontrolowany zarówno wewnątrz, jak i na zewnątrz przedsiębiorstwa.

Korzystanie z kontrolerów domeny tylko do odczytu

Windows Server 2008 zawiera wsparcie dla kontrolerów domeny tylko do odczytu (Read-Only Domain Controllers – RODC) oraz wznawialnych usług domenowych Active Directory. RODC jest dodatkowym kontrolerem domeny, utrzymującym replikę magazynu danych Active Directory tylko do odczytu. RODC doskonale odpowiadają potrzebom biur oddziałowych, w których nie jest możliwe zagwarantowanie bezpieczeństwa kontrolera domeny. Z wyjątkiem hasel RODC przechowuje te same obiekty i atrybuty, które są dostępne w zwykłym, „zapisywalnym” kontrolerze domeny. Obiekty te i ich atrybuty są kopiowane do RODC za pośrednictwem jednokierunkowej replikacji z zapisywalnego kontrolera domeny, pełniącego funkcję partnera replikacji.

Ponieważ RODC domyślnie nie przechowują hasel ani poświadczeń innych, niż swojego własnego konta komputera oraz konta Kerberos Target (krbtgt), weryfikują poświadczenia użytkowników i komputerów, odwołując się do zapisywalnego kontrolera domeny pracującego pod kontrolą systemu Windows Server 2008. Jeśli zasada Password Replication Policy (Zasada replikacji hasel) zostanie włączona na zapisywalnym kontrolerze domeny, RODC pobiera i buforuje poświadczenia w miarę konieczności, dopóki nie nastąpi ich zmiana. Ponieważ RODC przechowuje tylko podzbiór poświadczeń, ogranicza to ryzyko ich ujawnienia lub nadużycia.

Wskazówka Każdy użytkownik domeny może zostać delegowany jako lokalny administrator RODC bez konieczności przyznawania mu jakichkolwiek innych praw w domenie. RODC nie może odgrywać roli serwera wykazu globalnego ani żadnej roli wzorca operacji. Jakkolwiek RODC mogą pobierać informacje z kontrolerów domeny pracujących pod kontrolą systemu Windows Server 2003, aktualizacje partycji katalogu dla danej domeny mogą być pobierane tylko z zapisywalnego kontrolera domeny systemu Windows Server 2008, zlokalizowanego w tej samej domenie.

Korzystanie ze wznawialnych usług katalogowych Active Directory

Wznawialne usługi katalogowe (Restartable Active Directory Domain Services) to funkcja, która umożliwia zatrzymywanie i ponowne uruchamianie usługi AD DS. Na kontrolerach domeny w konsoli Services (Usługi) dostępna jest usługa Active Directory Domain Services, co pozwala na proste zatrzymanie i wznowienie AD DS, tak samo jak każdej innej usługi na tym serwerze. Po zatrzymaniu AD DS można wykonać zadania konserwacyjne, które w innym wypadku wymagałyby ponownego uruchamiania serwera, takich jak defragmentacja bazy danych Active Directory, instalowanie poprawek systemu operacyjnego lub zainicjowanie przywracania autorytatywnego. Podczas wstrzymania usługi AD DS obsługę uwierzytelniania i logowania użytkowników przejmują inne kontrolery domeny. Również poświadczenia buforowane, karty inteligentne i mechanizmy logowania oparte na biometrii nadal są obsługiwane. Jeżeli nie jest dostępny inny kontroler domeny i nie da się zastosować żadnej z wymienionych metod, można nadal zalogować się na serwerze, używając konta i hasła Directory Services Restore Mode.

Wszystkie kontrolery domeny pracujące pod kontrolą systemu Windows Server 2008 wspierają tryb Restartable Active Directory Domain Services – także RODC. Administrator może uruchomić lub zatrzymać usługę AD DS, posługując się wpisem Domain Controller

w konsoli Services. Ze względu na funkcję Restartable Active Directory, kontrolery domeny systemu Windows Server 2008 mogą znajdować się w jednym z trzech możliwych stanów:

Active Directory Started Usługa Active Directory jest uruchomiona i kontroler domeny jest aktywny – stan ten odpowiada stanowi działającego kontrolera domeny systemu Windows 2000 Server lub Windows Server 2003. W tym trybie kontroler domeny zapewnia usługi uwierzytelniania i logowania dla domeny.

Active Directory Stopped Usługa Active Directory jest zatrzymana i kontroler domeny nie obsługuje uwierzytelniania w domenie. W tym trybie serwer łączy część charakterystyki serwera członkowskiego i kontrolera domeny w trybie przywracania usług katalogowych (Directory Services Restore Mode – DSRM). Tak jak serwer członkowski, serwer jest przyłączony do domeny. Użytkownik może się na nim zalogować interaktywnie, posługując się poświadczeniami buforowanymi, kartą inteligentną lub urządzeniami biometrycznymi. Możliwe jest również zwykle zalogowanie przez sieć, o ile dostępny jest inny kontroler domeny. Tak jak w przypadku DSRM, baza danych Active Directory (Ntds.dit) przechowywana na tym kontrolerze znajduje się w stanie offline. Oznacza to, że możliwe jest wykonanie operacji wymagających stanu offline, takich jak defragmentacja bazy danych czy instalacja poprawek zabezpieczeń bez konieczności ponownego uruchamiania serwera.

Directory Services Restore Mode Tryb przywracania usług katalogowych jest analogiczny do tego trybu w systemie Windows Server 2003. Umożliwia on wykonanie autorytatywnego lub nieautorytatywnego przywracania bazy danych Active Directory.

Należy pamiętać, że przełączenie usługi AD DS w stan Stopped powoduje również zatrzymanie wszystkich usług zależnych. Oznacza to, że usługi File Replication Service (FRS), Kerberos Key Distribution Center (KDC) i Intersite Messaging zostają zatrzymane przed zatrzymaniem Active Directory, a nawet gdyby były uruchomione, zostaną zrestartowane, gdy usługa Active Directory zostanie ponownie uruchomiona. Ponadto wprowadzić można uruchomić kontroler domeny w stanie Directory Services Restore Mode, jednak nie jest możliwe uruchomienie go w stanie zatrzymania usługi katalogowej Active Directory. W celu przejścia do stanu Stopped należy najpierw uruchomić kontroler domeny zwyczajnie, po czym dopiero zatrzymać usługę AD DS.

Usługi rozwiązywania nazw

Systemy operacyjne Windows wykorzystują mechanizmy rozwiązywania nazw, aby ułatwić komunikowanie się z innymi komputerami w sieci. Rozwiązywanie nazw przypisuje nazwom komputerów ich numeryczne adresy IP, używane do komunikacji w sieci. Dzięki temu zamiast długich łańcuchów cyfr użytkownicy mogą łączyć się z komputerami za pomocą przyjaznych, łatwych do zapamiętania nazw.

Windows Vista i Windows Server 2008 wspierają trzy systemy rozwiązywania nazw:

- Domain Name System (DNS)
- Windows Internet Name Service (WINS)
- Link-Local Multicast Name Resolution (LLMNR)

Systemy te omówione zostały w kolejnych podrozdziałach.

Korzystanie z Domain Name System (DNS)

DNS jest usługą rozwiązywania nazw, która przekształca nazwy komputerów na adresy Internet Protocol (IP). Przy użyciu DNS w pełni kwalifikowana nazwa hosta, na przykład `computer84.cpandl.com`, może zostać przekształcona na odpowiadający mu adres IP, co umożliwi przesłanie pakietu do tego komputera. DNS działa w oparciu o stos protokołów TCP/IP i może zostać zintegrowana z usługami WINS, Dynamic Host Configuration Protocol (DHCP) oraz Active Directory Domain Services.

DNS łączy grupy komputerów w domeny, które są następnie porządkowane w strukturę hierarchiczną, definiowaną na poziomie całego Internetu lub w skali przedsiębiorstwa w przypadku sieci prywatnych (nazywanych też intranetami i ekstranetami). Różne poziomy hierarchii identyfikują poszczególne komputery, domeny organizacyjne, aż do domen najwyższego poziomu (*top-level domains*). W przypadku w pełni kwalifikowanej nazwy hosta `computer84.cpandl.com`, `computer84` odpowiada nazwie indywidualnego komputera, `cpandl` jest domeną organizacyjną, zaś `com` jest domeną najwyższego poziomu.

Domeny najwyższego poziomu stanowią korzeń (*root*) hierarchii DNS, są więc czasem nazywane *domenami korzenia*. Domeny te są uporządkowane na podstawie geografii (przynależności państwowej), typu organizacji lub funkcji. Zwykle domeny, takie jak `cpandl.com`, nazywane są domenami nadrzędnymi (*parent domains*). Nazwa ta wynika z faktu, że są one nadrzędne dla struktury organizacyjnej. Domeny nadrzędne mogą być podzielone na poddomeny, które mogą odpowiadać grupom lub oddziałom wewnątrz organizacji.

Poddomeny są często nazywane domenami podrzędnymi (*child domains*). Na przykład w pełni kwalifikowana nazwa domenowa (Fully Qualified Domain Name – FQDN) komputera należącego do oddziału przedsiębiorstwa może mieć postać `jacob.hr.cpandl.com`. W tym przykładzie `jacob` jest nazwą hosta, `hr` jest domeną podrzędną, zaś `cpandl.com` – domeną nadrzędną.

Domeny Active Directory wykorzystują DNS do implementacji struktury nazewniczej i hierarchii. Active Directory i DNS są ściśle zintegrowane, tak bardzo, że konieczne jest zainstalowanie DNS w sieci, zanim będzie możliwe zainstalowanie w niej pierwszego kontrolera domeny wykorzystującego Active Directory. W trakcie instalacji pierwszego kontrolera domeny administrator ma możliwość automatycznego zainstalowania usługi DNS, jeśli w sieci nie można znaleźć serwera DNS. Może on również określić, czy DNS i Active Directory powinny być w pełni zintegrowane. W większości wypadków właściwym wyborem jest akceptacja obu żądań. Przy pełnej integracji informacje DNS są przechowywane bezpośrednio w bazie danych Active Directory. Daje to możliwość skorzystania z możliwości oferowanych przez usługę katalogową. Różnica pomiędzy integracją częściową i pełną jest bardzo istotna.

Integracja częściowa W tym trybie informacje DNS przechowywane są w plikach tekstowych z rozszerzeniem `.dns`, które domyślnie zlokalizowane są w katalogu `%SystemRoot%\System32\Dns`. Zmiany w DNS są obsługiwane za pośrednictwem pojedynczego autorytatywnego serwera DNS. Serwer ten jest określony jako główny (*primary*) serwer DNS dla konkretnej domeny lub obszaru wewnątrz domeny, zwanego strefą (*zone*). Komputery kliencie, które używają dynamicznych aktualizacji DNS przez DHCP, muszą zostać skonfigurowane tak, aby używały głównego serwera DNS dla strefy. W przeciwnym wypadku ich informacje DNS nie będą aktualizowane. Dodatkowo dynamiczne aktualizacje przez DHCP nie będą wykonywane, jeśli główny serwer DNS nie będzie dostępny.

Pełna integracja Przy pełnej integracji informacje DNS są przechowywane w katalogu Active Directory i są dostępne za pośrednictwem kontenera obiektu `dnsZone`. Ponieważ informacje te są częścią Active Directory, każdy kontroler domeny ma dostęp do tych

danych, a ponadto można wykorzystać replikację o wielu wzorcach do realizacji aktualizacji dynamicznych. Pozwala to każdemu kontrolerowi domeny, na którym uruchomiona jest usługa DNS Server, do obsługi aktualizacji dynamicznych. Co więcej, komputery klienckie używające aktualizacji dynamicznych przez DHCP mogą korzystać z dowolnego serwera DNS w danej strefie. Dodatkową korzyścią integracji jest możliwość wykorzystania mechanizmu zabezpieczeń katalogu do kontrolowania dostępu do informacji DNS.

Przeglądając się sposobom, jakimi informacje DNS są replikowane w sieci, można zauważyć więcej korzyści z pełnej integracji z Active Directory. Przy integracji częściowej informacje DNS są przechowywane i replikowane niezależnie od Active Directory. Konieczność utrzymania dwóch oddzielnych struktur zmniejsza sprawność zarówno DNS, jak i Active Directory, a zarazem powoduje, że administracja jest bardziej złożona. Ponieważ mechanizmy replikacji DNS są mniej wydajne, niż Active Directory, może to również powodować zwiększenie ruchu sieciowego i wydłużenie czasu niezbędnego na powielenie zmian w DNS w całej sieci.

W celu uaktywnienia DNS w sieci konieczne jest skonfigurowanie klientów i serwerów DNS. Podczas konfigurowania klientów DNS należy podać im adresy IP serwerów DNS. Przy użyciu tych adresów klienci będą mogli porozumieć się z serwerami DNS w dowolnym miejscu sieci, nawet jeśli serwery te znajdują się w innych podsieciach.

Jeśli sieć wykorzystuje DHCP, należy skonfigurować tę usługę, aby współpracowała z DNS. W tym celu należy ustawić opcje zakresów DHCP: 006 DNS Servers oraz 015 DNS Domain Name, zgodnie ze opisem zawartym w podrozdziale „Ustawianie opcji zakresów” w rozdziale 19. Ponadto, jeśli komputery w sieci mają być dostępne z innych domen Active Directory, konieczne będzie utworzenie dla nich rekordów w DNS. Rekordy DNS uporządkowane są w strefy, przy czym strefa jest po prostu obszarem wewnątrz domeny. Konfigurowanie serwera DNS omówione zostało w podrozdziale „Konfigurowanie głównego serwera DNS” w rozdziale 20.

Jeśli usługa DNS Server zostanie zainstalowana na RODC, serwer ten jest w stanie pobierać replikę tylko do odczytu wszystkich partycji aplikacji katalogu używanych przez DNS, w tym ForestDNSZones oraz DomainDNSZones. Komputery klienckie mogą następnie przesyłać zapytania do serwera RODC, jak do każdego innego serwera DNS. Jednak podobnie jak w przypadku zmian katalogu, serwer DNS zainstalowany na RODC nie będzie wspierał bezpośrednich zmian. Oznacza to, że RODC nie rejestruje rekordów zasobu serwera nazw (NS) dla żadnej utrzymywanej przez siebie strefy zintegrowanej z Active Directory. Gdy klient spróbuje uaktualnić swój rekord DNS na serwerze RODC, serwer ten zwróci odsyłacz do serwera DNS, którego ten klient może użyć w tym celu. Następnie serwer DNS na RODC odbierze zaktualizowany rekord z serwera DNS, który obsłużył aktualizację, używając specjalnego żądania replikacji pojedynczego obiektu, wykonywanego jako proces w tle.

Korzystanie z Windows Internet Name Service (WINS)

WINS jest usługą rozwiązywania nazw, przekształcającą nazwy komputerów na ich adresy IP. Przy użyciu WINS nazwa komputera, taka jak COMPUTER84, może zostać przekształcona na jego adres IP, co pozwala komputerom w sieci Microsoft na odnajdywanie się wzajemnie i przekazywanie informacji. WINS jest niezbędne do obsługi systemów starszych niż Windows 2000 oraz starszych aplikacji, które wykorzystują protokół Network Basic Input/Output System (NetBIOS) over TCP/IP, takich jak narzędzia wiersza polecenia NET. Jeśli sieć nie zawiera systemów starszych niż Windows 2000 i nie są stosowane takie aplikacje, nie ma potrzeby instalowania i konfigurowania WINS.

WINS funkcjonuje najlepiej w środowisku typu klient-serwer, w którym klienci tej usługi wysyłają zapytania do serwerów WINS, które rozwiązują je i odsyłają odpowiedź. Do przesyłania zapytań WINS i innych informacji komputery wykorzystują protokół NetBIOS, zapewniający interfejs programowania aplikacji (API), który pozwala na komunikowanie się komputerów w sieci. Aplikacje NetBIOS opierają się na mechanizmie WINS lub lokalnym pliku LMHOSTS do rozwiązywania nazw komputerów na adresy IP. W sieciach starszych niż Windows 2000 WINS stanowił podstawową usługę rozwiązywania nazw. Od momentu wprowadzenia Windows 2000 główną usługą rozwiązywania nazw stała się DNS, zaś WINS ma inną funkcję. Jest nią umożliwienie starszym niż Windows 2000 systemom przeglądania listy zasobów sieciowych oraz wyszukiwanie przez komputery systemu Windows 2000 i późniejszych zasobów NetBIOS.

W celu włączenia rozwiązywania nazw WINS w sieci należy skonfigurować klientów i serwery WINS. Podczas konfigurowania klientów WINS należy podać im adresy IP serwerów WINS. Przy użyciu tych adresów klienci będą mogli porozumieć się z serwerami WINS w dowolnym miejscu sieci, nawet jeśli serwery te znajdują się w innych podsięciach. Klienci WINS mogą również porozumiewać się przy użyciu metody rozgłaszania, w której klient wysyła komunikat do innych komputerów w lokalnym segmencie sieci, żądając podania ich adresów IP. Ponieważ komunikaty są rozgłaszane, serwer WINS nie jest używany. Każdy klient nieużywający WINS, który wspiera ten typ rozgłaszania komunikatów, może użyć tej metody do rozwiązywania nazw komputerów na adresy IP.

Gdy klienci komunikują się z serwerami WINS, tworzą sesję połączenia składającą się z następujących głównych części:

Rejestracja nazwy W trakcie rejestrowania nazwy klient przekazuje do serwera swoją nazwę i adres IP i żąda dodania do bazy danych WINS. Jeśli określona nazwa i adres nie są jeszcze używane w sieci, serwer WINS akceptuje żądanie i rejestruje klienta w swojej bazie danych.

Odnowienie nazwy Rejestracja nazwy nie jest trwała. Zamiast tego klient otrzymuje nazwę do użycia przez określony czas, zwany dzierzwą (*lease*). Ponadto otrzymuje informację o okresie, w którym nazwa musi zostać odnowiona, zwanym interwałem odnowy (*renewal interval*). Klient musi ponownie zarejestrować się na serwerze WINS podczas interwału odnowy.

Zwolnienie nazwy Jeśli klient nie odnowi dzierżawy, rejestracja nazwy zostaje zwolniona, co pozwala innemu komputerowi w sieci na użycie tej samej nazwy, adresu IP lub obydwu. Nazwa zostaje zwolniona również wtedy, gdy klient WINS zostanie wyłączony.

Po utworzeniu sesji połączenia z serwerem WINS klient może żądać usług rozwiązywania nazw. Metoda używana do rozwiązywania nazw na adresy IP zależna jest od konfiguracji sieci. Dostępne są następujące metody:

B-node (rozgłaszanie) Wykorzystuje komunikaty rozgłaszania do rozwiązywania nazw komputerów na adresy IP. Komputery, które muszą rozwiązać nazwę, wysyłają komunikat rozgłaszania do wszystkich hostów w sieci lokalnej, żądając podania adresu IP dla danej nazwy. W dużej sieci zawierającej setki czy tysiące komputerów komunikaty takie mogą zużyć znaczącą część pasma sieciowego.

P-node (peer-to-peer) Wykorzystuje serwery WINS do rozwiązywania nazw komputerów. W tym trybie, gdy klient musi rozwiązać nazwę komputera na adres IP, wysyła zapytanie do serwera, który odsyła komunikat z odpowiedzią.

M-node (mieszany) Łączy tryby *b-node* oraz *p-node*. W tym trybie klient WINS najpierw wykonuje rozgłaszanie. Jeśli próba się nie powiedzie, klient używa trybu *p-node*. Ponieważ rozgłaszanie wykonywane jest najpierw, metoda ta powoduje te same problemy z pasmem sieciowym, które występują w trybie *b-node*.

H-node (hybrydowy) Również łączy tryby *b-node* i *p-node*. W tym wypadku jednak klient najpierw próbuje uzyskać odpowiedź z serwera WINS (tryb *p-node*). Jeśli próba zakończy się niepowodzeniem, klient rozgłasza zapytanie. Ponieważ podstawową metodą jest zapytanie do serwera, metoda ta zapewnia najlepszą wydajność w większości sieci. Jest to również domyślna metoda rozwiązywania nazw WINS.

Jeśli w sieci dostępne są serwery WINS, klienci systemu Windows używają metody *p-node*. Przy braku serwerów WINS używana będzie metoda rozgłaszania *b-node*. Dodatkowo komputery Windows do rozwiązywania nazw mogą wykorzystywać również DNS oraz lokalne pliki LMHOSTS i HOSTS. Konfigurowanie serwerów DNS jest omówione w rozdziale 20, „Optymalizacja DNS”.

Przy korzystaniu z DHCP do dynamicznego przydzielania adresów IP można określić metodę rozwiązywania nazw przez klientów. W tym celu należy skonfigurować opcję zakresów DHCP 046 WINS/NBT Node Type, zgodnie z opisem zawartym w podrozdziale „Ustawianie opcji zakresów” w rozdziale 19. Zalecaną metodą jest tryb hybrydowy, który zapewnia najlepszą wydajność i pozwala zmniejszyć nadmiarowy ruch w sieci.

Korzystanie z mechanizmu Link-Local Multicast Name Resolution (LLMNR)

Mechanizm rozgłoszeniowego rozwiązywania nazw łączy lokalnego (LLMNR) powstał w celu zaspokojenia potrzeb bezpośredniego rozwiązywania nazw przez urządzenia używające IPv4, IPv6 lub obu typów adresów. Pozwala on na wzajemne rozwiązywanie nazw przez urządzenia IPv4 lub IPv6 zlokalizowane w tej samej podsieci – możliwość, której ani WINS, ani DNS nie mogą w pełni zapewnić. Wprawdzie WINS umożliwia rozwiązywanie nazw – tak w trybie klient-serwer, jak i bezpośrednim (*peer-to-peer*) – dla protokołu IPv4, nie wspiera jednak adresów IPv6. Z drugiej strony DNS wprawdzie obsługuje adresy obu protokołów, ale jest zależny od istnienia i konfiguracji dedykowanych serwerów, zapewniających usługi rozwiązywania nazw.

Wsparcie dla LLMNR zapewnia zarówno system Windows Vista, jak i Windows Server 2008. LLMNR przeznaczony jest dla klientów sieci IPv4 oraz IPv6, gdy inne mechanizmy rozwiązywania nazw nie są dostępne, a zatem w takich sytuacjach, jak:

- Sieci domowe lub małych firm
- Sieci ad hoc
- Sieci przedsiębiorstw, gdy usługi DNS nie są dostępne

LLMNR został zaprojektowany, aby uzupełnić DNS przez umożliwienie rozwiązywania nazw w sytuacjach, w których konwencjonalne rozwiązywanie nazw DNS nie jest możliwe. Wprawdzie LLMNR może zastąpić potrzebę WINS w przypadku, gdy NetBIOS nie jest wymagany, nie jest jednak zamiennikiem DNS, gdyż może działać tylko w lokalnej podsieci. Ponieważ ruch LLMNR nie rozprzestrzenia się przez routery, nie może spowodować przypadkowego „zalanía” sieci nadmiarowym ruchem.

LLMNR jest domyślnie włączony na wszystkich komputerach systemu Windows Vista lub Windows Server 2008, przy czym komputery te użyją tego mechanizmu jedynie wtedy,

gdy wszystkie próby wyszukania nazwy hosta przez DNS zakończą się niepowodzeniem. W rezultacie w systemach tych rozwiązywanie nazw przebiega następująco:

1. Komputer wysyła zapytanie do skonfigurowanego na nim głównego serwera DNS. Jeśli nie otrzyma odpowiedzi lub odbierze komunikat o błędzie, próbuje kolejno pozostałe, alternatywne serwery DNS. Jeżeli host ten nie ma skonfigurowanych serwerów DNS lub nie może się połączyć z żadnym z nich, mechanizm rozwiązywania nazw przełącza się na tryb LLMNR.
2. Komputer wysyła zapytanie w postaci komunikatu emisji wielokrotnej (*multicast*) przy użyciu protokołu User Datagram Protocol (UDP), żądając podania adresu IP dla poszukiwanej nazwy. Zapytanie to jest ograniczone do lokalnej podsieci (określonej również terminem łącza lokalnego).
3. Każdy komputer w sieci lokalnej, który wspiera LLMNR i został skonfigurowany tak, aby odpowiadał na przychodzące zapytania, odbiera komunikat i porównuje żądaną nazwę z własną nazwą hosta. Jeśli nazwy nie pasują, komputer odrzuca żądanie. Jeśli nazwa jest prawidłowa, komputer odsyła komunikat emisji pojedynczej zawierający swój adres IP do źródłowego hosta.

LLMNR można wykorzystać także do mapowania odwrotnego. W takim wypadku komputer wysyła komunikat emisji pojedynczej do wskazanego adresu IP, żądając podania nazwy hosta komputera docelowego. Komputer z włączoną obsługą LLMNR, który otrzyma takie żądanie, odeśle odpowiedź zawierającą nazwę do komputera źródłowego.

Funkcjonowanie LLMNR wymaga, aby nazwy komputerów były unikatowe w obrębie podsieci lokalnej. W większości wypadków komputer sprawdza unikatowość nazwy podczas uruchamiania, gdy jest przywracany ze stanu wstrzymania lub gdy wystąpi zmiana ustawień interfejsu sieciowego. Jeżeli komputer jeszcze nie ustalił, czy jego nazwa jest unikatowa, musi zaznaczyć ten warunek podczas odpowiadania na zapytanie o nazwę.

W praktyce

LLMNR jest domyślnie włączone automatycznie na wszystkich komputerach systemu Windows Vista i Windows Server 2008. Wyłączenie tego mechanizmu możliwe jest przez edycję rejestru.

W celu wyłączenia LLMNR dla wszystkich interfejsów sieciowych należy utworzyć następującą wartość rejestru i ustawić jej wartość na 0 (zero): HKLM/SYSTEM/CurrentControlSet/Services/Dnscache/Parameters/EnableMulticast. W celu wyłączenia LLMNR dla wybranego interfejsu sieciowego, należy utworzyć następującą wartość rejestru i ustawić jej wartość na 0 (zero): HKLM/SYSTEM/CurrentControlSet/Services/Tcpip/Parameters/AdapterGUID/EnableMulticast, gdzie *AdapterGUID* jest globalnie unikatowym identyfikatorem (GUID) tej karty sieciowej.

LLMNR można włączyć ponownie w dowolnym momencie, zmieniając tę wartość rejestru na 1. Włączanie lub wyłączenie LLMNR jest również możliwe za pośrednictwem Zasad grupy.

Często używane narzędzia

System Windows Server 2008 zawiera wiele narzędzi przydatnych dla administratorów. Do najczęściej używanych należą następujące:

Control Panel (Panel sterowania) Zbiór narzędzi do zarządzania konfiguracją systemu. Zawartość panelu można uporządkować na różne sposoby, zależnie od używanego widoku. Domyślnym widokiem jest widok kategorii, pozwalający na dostęp do narzędzi przez kategorie, narzędzia i kluczowe zadania. Widok klasyczny prezentuje każde narzędzie odrębnie, uporządkowane według nazw.

Graficzne narzędzia administracyjne Podstawowe narzędzia zarządzania sieciami komputerami i ich zasobami. Narzędzia te zebrane są w podmenu Administrative Tools (Narzędzia administracyjne).

Kreatory administracyjne Narzędzia zaprojektowane do zautomatyzowania kluczowych zadań administracyjnych. Dostęp do nich zapewnia konsola Server Manager – centralna konsola administracyjna Windows Server 2008.

Narzędzia wiersza polecenia Większość programów narzędziowych można uruchomić w trybie wiersza polecenia. Oprócz tych narzędzi Windows Server 2008 udostępnia także inne programy, które mogą być przydatne przy obsłudze systemu.

Informacje o składni narzędzi wiersza polecenia NET można uzyskać wpisując **NET HELP <nazwa>**, gdzie <nazwa> jest konkretnym poleceniem, np. NET HELP SEND.

Korzystanie Windows PowerShell

Dodatkową elastyczność i automatyzację za pomocą skryptów można osiągnąć instalując Windows PowerShell. Jest to pełnowartościowa powłoka trybu wiersza polecenia (znakowego), wykorzystująca wbudowane polecenia zwane *cmdlets* oraz techniki programistyczne, jak również zwykłe programy narzędziowe. Wprawdzie PowerShell nie jest instalowany domyślnie, jednak rozszerzenie to można zainstalować wykonując następujące czynności:

1. Kliknąć przycisk Server Manager (Menedżer serwera) w pasku szybkiego uruchamiania. Alternatywnie można kliknąć Start, wskazać Administrative Tools, po czym kliknąć Server Manager.
2. W narzędziu Server Manager wybrać węzeł Features (Funkcjonalność), po czym kliknąć Add Features (Dodaj funkcje).
3. W oknie dialogowym Windows Features wybrać select Windows PowerShell.
4. Kliknąć Next (Dalej), a następnie Install (Instaluj).

Ponieważ dołączona do pakietu instalacyjnego wersja PowerShell może nie być najnowszą dostępną, warto upewnić się, czy w witrynie Microsoft Download nie jest dostępna nowsza edycja. Po zainstalowaniu PowerShell w menu Start pojawi się skrót do programu. Jeśli zachodzi potrzeba uruchomienia PowerShell w trybie wiersza polecenia, należy pamiętać, że plik wykonywalny (powershell.exe) zlokalizowany jest w katalogu %SystemRoot%\System32\WindowsPowerShell\Version, gdzie *Version* jest numerem zainstalowanej wersji narzędzia, na przykład v1.0 lub v1.11. Ścieżka do katalogu zawierającego ostatnio zainstalowaną wersję powinna być dołączona domyślnie do zmiennej środowiskowej *path*. Pozwala to zagwarantować, że możliwe będzie uruchomienie PowerShell z wiersza polecenia bez konieczności wpisywania całej ścieżki lub przechodzenia do odpowiedniego katalogu.

Po uruchomieniu Windows PowerShell można wpisać nazwę *cmdlet* po znaku zachęty i polecenie zostanie wykonane podobnie, jak typowe komendy. Wykonanie *cmdlet* może nastąpić także z wnętrza skryptu. Polecenia *cmdlet* mają nazwy w postaci par czasownik-rzeczownik. Czasownik określa ogólną czynność wykonywaną przez polecenie. Rzeczownik wskazuje, czego dotyczy dane polecenie. Na przykład polecenie **get-variable** (bez parametrów) zwróci nazwy i wartości wszystkich zmiennych środowiskowych Windows PowerShell, a uzupełnione nazwą zmiennej – wartość tej zmiennej. Najczęściej występujące czasowniki używane w nazwach poleceń *cmdlet* to:

Get- (Pobierz) Zapytuje wskazany obiekt lub zbiór obiektów, na przykład konkretną skrzynkę pocztową lub wszystkich użytkowników poczty.

Set- (Ustaw) Zmienia wskazane ustawienie obiektu lub obiektów.

Enable- (Włącz) Uaktywnia ustawienie lub włącza obsługę poczty dla odbiorcy.

Disable- (Wyłącz) Wyłącza aktywne ustawienia lub wyłącza obsługę poczty dla odbiorcy.

New- (Nowy) Tworzy nową instancję obiektu, na przykład nową skrzynkę pocztową.

Remove- (Usuń) Usuwa istniejącą instancję obiektu, na przykład skrzynkę pocztową.

Pełną listę poleceń *cmdlet* można uzyskać wpisując **help *-*** po znaku zachęty Windows PowerShell. Aby uzyskać informacje na temat konkretnego polecenia, należy wpisać **help** uzupełnione o nazwę, na przykład **help get-variable**.

Dla każdego polecenia można skonfigurować aliasy, które działają jak skróty. Aby wyświetlić listę istniejących aliasów, należy wpisać **get-item -path alias:** po znaku zachęty PowerShell. Można również utworzyć własny alias wywołujący dane polecenie, używając następującej składni:

```
new-item -path alias:AliasName -value:FullCommandPath
```

gdzie *AliasName* jest nazwą tworzonego aliasu, a *FullCommandPath* jest pełną ścieżką do danego polecenia, na przykład:

```
new-item -path alias:sm -value:c:\windows\system32\compmgmtlauncher.exe
```

Przykład ten tworzy alias *sm* uruchamiający narzędzie Server Manager. Aby go użyć, wystarczy wpisać **sm** i nacisnąć Enter w oknie poleceń PowerShell.

Automatyzacja zadań administracyjnych, zasady i procedury

W tym rozdziale:

Istota Zasad grupy	112
Przeglądanie zmian w Zasadach grupy	115
Zarządzanie zasadami lokalnymi	117
Zarządzanie zasadami dla lokacji, domeny i jednostki organizacyjnej	121
Konserwacja i rozwiązywanie problemów z zasadami grupy	133
Zarządzanie użytkownikami i komputerami przy użyciu zasad grupy	146

Codzienne wykonywanie rutynowych zadań, zajmowanie się konfigurowaniem zasad dla komputerów i przeprowadzanie użytkowników przez podstawy systemu nie jest najlepszym sposobem wykorzystania czasu administratora. Znacznie lepszą efektywność można osiągnąć, automatyzując codzienne czynności i poświęcając czas zagadnieniom, które są bardziej istotne. Wszelkie usługi pomocnicze służą zwiększeniu produktywności i skoncentrowaniu się na ważnych problemach, bez potrzeby marnowania czasu na trywialne codzienne czynności.

Microsoft Windows Server 2008 obejmuje wiele ról, usług roli i rozszerzeń, które ułatwiają obsługę instalacji serwerowych. Niektóre z tych komponentów można bez wysiłku zainstalować i od razu zacząć używać. Jeśli potrzebne jest narzędzie administracyjne do zarządzania rolą lub rozszerzeniem na komputerze zdalnym, można wybrać je do zainstalowania w ramach rozszerzenia Remote Server Administration Tools (Narzędzia administracji zdalnej). Jeżeli serwer zawiera bezprzewodową kartę sieciową, można zainstalować rozszerzenie Wireless Networking, aby włączyć obsługę połączeń bezprzewodowych. Połączenia takie w systemie Windows Server 2008 działają identycznie jak w systemie Windows Vista.

Oprócz tych i innych elementarnych komponentów pomocniczych dostępne są inne składniki wspierające pracę administratora, w tym:

Aktualizacje automatyczne Składnik ten jest odpowiedzialny za wykonywanie aktualizacji systemu operacyjnego. Pozwala to zagwarantować, że system zawiera najświeższe poprawki zabezpieczeń i aktualne wersje krytycznych plików. Rozszerzenie serwera ze standardowego trybu Windows Update do trybu Microsoft Update pozwala na uzyskiwanie aktualizacji dla dodatkowych produktów. Domyślnie aktualizacje automatyczne na komputerach systemu Windows Server 2008 są zainstalowane, ale nieuruchomione. Konfigurację aktualizacji automatycznych umożliwia narzędzie Windows Update, dostępne w Panelu sterowania. W celu jego uruchomienia należy kliknąć Start, następnie Control Panel (Panel sterowania), Security (Zabezpieczenia) i na koniec Windows Update.

Szyfrowanie BitLocker Zapewnia dodatkowy poziom zabezpieczeń, umożliwiając ochronę dysków twardych serwera przed napastnikiem, który ma fizyczny dostęp do serwera. Szyfrowania BitLocker można użyć zarówno na serwerach wyposażonych w mechanizm Trusted Platform Module (TPM), jak i na pozostałych. Po zainstalowaniu tej funkcji za pomocą kreatora Add Features Wizard można nią zarządzać przy użyciu narzędzia BitLocker Drive Encryption w Panelu sterowania.

Remote Assistance (Pomoc zdalna) Udostępnia funkcję pomocy zdalnej, pozwalającej na wysyłanie zaproszeń pomocy do bardziej zaawansowanego administratora. Po zaakceptowaniu zaproszenia administrator ten może uzyskać wgląd w pulpit użytkownika i czasowo przejąć kontrolę nad komputerem, aby rozwiązać problem. Po zainstalowaniu rozszerzenia na serwerze można nim zarządzać posługując się opcjami dostępnymi na zakładce Remote (Zdalny) okna dialogowego System Properties. W celu wyświetlenia tych opcji należy uruchomić narzędzie System And Maintenance w Panelu sterowania, kliknąć System, a następnie kliknąć Remote Settings w sekcji Tasks (Zadania).

Remote Desktop (Pulpit zdalny) Udostępnia mechanizm łącznościowy, który umożliwia zdalne połączenie z serwerem i zarządzanie nim z innego komputera. Pulpit zdalny jest domyślnie zainstalowany, ale nie włączony na komputerach systemu Windows Server 2008. Zarządzanie konfiguracją pulpitu zdalnego umożliwiają opcje dostępne na zakładce Remote (Zdalny) okna dialogowego System Properties. W celu wyświetlenia tych opcji należy uruchomić narzędzie System And Maintenance w Panelu sterowania, kliknąć System, a następnie kliknąć Remote Settings w sekcji Tasks (Zadania). Aby utworzyć połączenie przy użyciu narzędzia Remote Desktop Connection (Połączenie pulpitu zdalnego) należy kliknąć Start, następnie All Programs, Accessories i na koniec Remote Desktop Connection.

Task Scheduler (Harmonogram zadań) Pozwala na zaplanowanie jednokrotnego lub powtarzalnego wykonania pewnego zadania, na przykład w celu przeprowadzenia rutynowej konserwacji. Podobnie jak Windows Vista, Windows Server 2008 intensywnie wykorzystuje funkcjonalność zaplanowanych zadań. Przeglądanie, tworzenie i modyfikowanie zaplanowanych zadań można wykonać przy użyciu konsoli Server Manager. W tym celu należy rozwinąć kolejno węzły Configuration (Konfiguracja), Task Scheduler (Harmonogram zadań) oraz Task Scheduler Library (Biblioteka harmonogramu zadań), aby wyświetlić aktualnie skonfigurowane zadania.

Windows Defender Pozwala ochronić serwer przed programami spyware i innymi niepożądanymi programami. Narzędzie Windows Defender można uruchamiać ręcznie w miarę potrzeb lub skonfigurować jego automatyczne uruchamianie zgodnie z zaplanowanym harmonogramem. Domyślnie w instalacjach serwerowych narzędzie Windows Defender nie jest aktywne. Po zainstalowaniu narzędzia Windows Defender jako części rozszerzenia Desktop Experience można je uruchomić przy użyciu menu All Programs.

Desktop Experience Instaluje dodatkowe funkcje pulpitu Windows Vista na serwerze. Rozszerzenia tego należy użyć wówczas, gdy Windows Server 2008 ma pełnić funkcję systemu operacyjnego stacji roboczej. Po dodaniu tego rozszerzenia za pomocą kreatora Add Features Wizard funkcje pulpitu zostają rozszerzone do poziomu zbliżonego do Windows Vista, przy czym instalowane są również następujące programy: Windows Calendar, Windows Defender, Windows Mail, Windows Media Player, Windows Photo Gallery, Windows Sidebar oraz Windows SideShow.

Windows Firewall (Zapora systemu Windows) Pozwala chronić komputer przed atakami pochodzącymi z sieci. Windows Server 2008 zawiera podstawową zaporę ogniową (osobistą) o nazwie Windows Firewall oraz zaawansowaną zaporę o nazwie Windows Firewall With Advanced Security. Domyślnie zapory te nie są uaktywnione w instalacjach serwerowych. W celu uzyskania dostępu do konfiguracji zapory podstawowej należy kliknąć Windows Firewall (Zapora systemu Windows) w sekcji Network And Internet (Sieć i Internet) Panelu sterowania. Dostęp do zaawansowanych funkcji zapory umożliwia narzędzie Windows Firewall With Advanced Security obecne w menu Administrative Tools (Narzędzia administracyjne).

Windows Time (Czas systemu Windows) Synchronizuje czas systemowy z wzorcem czasu w sieci w celu zagwarantowania jego dokładności. Synchronizacja może odbywać się względem wskazanego serwera czasu. Metoda działania usługi Windows Time zależy od tego, czy komputer jest członkiem domeny, czy grupy roboczej. W środowisku domeny jako wzorce czasu służą kontrolery domeny, przy czym funkcjonalnością tą można zarządzać za pośrednictwem zasad grupy. W środowisku grupy roboczej synchronizacja odbywa się względem internetowych serwerów czasu, zaś zarządzanie funkcjonalnością umożliwia narzędzie Date And Time.

Konfiguracja i zarządzanie tymi komponentami pomocniczymi odbywa się dokładnie w taki sam sposób w obydwu systemach: Windows Vista i Windows Server 2008. Szczegółowe omówienie tych składników zawiera publikacja *Vademecum Administratora Microsoft Windows Vista* (wydanie polskie APN Promise, Warszawa 2007).

Również wiele innych komponentów systemowych udostępnia usługi pomocnicze. Jednak te dodatkowe usługi potrzebne są tylko w szczególnych scenariuszach. Można na przykład wykorzystać Windows System Resource Manager do zarządzania wykorzystaniem procesorów i pamięci serwera, gdy dąży się do zapewnienia najlepszej dostępności intensywnie wykorzystywanego serwera. Usługi terminalowe umożliwiają uruchamianie aplikacji na serwerze przez użytkowników zdalnych. Mechanizm Windows Deployment Services pozwala zrealizować automatyczne wdrażanie systemów operacyjnych Windows. Tym narzędziem pomocniczym, które jest zawsze w użyciu i którego obsługa musi być doprowadzona do perfekcji, aby skutecznie administrować systemem Windows Server 2008, są Zasady grupy.

Uwaga Ustawienia Zasad grupy w systemie Windows Server 2008 uległy znaczącym zmianom w porównaniu do wcześniejszych wersji Windows. W gałęziach Computer Configuration (Konfiguracja komputera) oraz User Configuration (Konfiguracja użytkownika) znaleźć można dwa nowe węzły: Policies (Zasady) oraz Preferences (Preferencje). Ustawienia ogólne zasad zostały umieszczone w węźle Policies. Ustawienia dotyczące ogólnych preferencji zebrane zostały w węźle Preferences. Przy omawianiu ustawień zawartych w węźle Policies będziemy używać skróconego odnośnika, takiego jak User Configuration\Administrative Templates\Windows Components zamiast pełnej ścieżki User Configuration\Policies\Administrative Templates: Policy Definitions\Windows Components. W tym wypadku skrócony odnośnik informuje, że omawiane ustawienie zasad znajduje się w gałęzi User Configuration i można je zlokalizować w podwęźle Administrative Templates\Windows Components.

Istota Zasad grupy

Zasady grupy upraszczają administrację w średnich i dużych przedsiębiorstwach, pozwalając administratorom na scentralizowanie zarządzania przywilejami, uprawnieniami i możliwościami tak użytkowników, jak i komputerów. Za pośrednictwem zasad grupy można wykonać takie zadania, jak:

- Kontrola dostępu do składników Windows, zasobów systemowych, zasobów sieci, narzędzi Panelu sterowania, pulpitu i menu Start. Zagadnienia te omówione są w podrozdziale „Korzystanie z szablonów administracyjnych do ustawiania zasad”.
- Utworzenie centralnie zarządzanych katalogów mieszczących foldery specjalne, takie jak foldery Documents użytkowników. Te zagadnienia omawia podrozdział „Scentralizowane zarządzanie folderami specjalnymi”.
- Definiowanie skryptów użytkowników i komputerów, uruchamianych w określonym czasie lub okolicznościach. Problematykę tę omawia podrozdział „Zarządzanie skryptami użytkowników i komputerów”.
- Konfigurowanie zasad dotyczących blokad kont, haseł, inspekcji, przypisywania praw użytkowników i zabezpieczeń. Tematykę tę omawia część II tej książki, „Administracja usługami katalogowymi Windows Server 2008”.

Kolejne podrozdziały ukazują sposoby korzystania z zasad grupy w celu lepszego zobrazowania działania i sposobów stosowania zasad grupy.

Podstawy Zasad grupy

Zasady grupy można w uproszczeniu nazwać zbiorem reguł, które pozwalają zarządzać użytkownikami i komputerami. Zasady mogą być stosowane na najróżniejszych poziomach struktury – wobec kilku domen, pojedynczych domen, podgrup w obrębie domeny lub nawet indywidualnych systemów. Zasady dotyczące indywidualnych komputerów określane są mianem *lokalnych zasad grupy* i są przechowywane tylko w systemie lokalnym. Zasady stosowane na innych poziomach są połączone jako obiekty w magazynie danych usługi katalogowej Active Directory.

W celu zrozumienia zasad grupy trzeba znać przynajmniej podstawy struktury Active Directory. Strukturą „geograficzną” położoną powyżej poziomu domeny są *lokacje*, zaś „podgrupy” wewnątrz domen nazywane są *jednostkami organizacyjnymi* (*organizational units* – OU). Innymi słowy, sieć może zawierać lokacje o nazwach NewYorkMain, CaliforniaMain i WashingtonMain. Wewnątrz lokacji WashingtonMain mogą istnieć domeny o nazwach SeattleEast, SeattleWest, SeattleNorth oraz SeattleSouth. Wreszcie domena SeattleEast może zawierać jednostki organizacyjne o nazwach Information Services (IS), Engineering i Sales.

Zasady grupy mogą być stosowane tylko do komputerów pracujących pod kontrolą systemów Windows 2000, Windows XP Professional, Windows Vista, Windows Server 2003 oraz Windows Server 2008. W przypadku systemu Windows NT 4.0 zasady można zaaplikować przy użyciu narzędzia System Policy Editor (Poedit.exe). Wobec komputerów systemów Windows 95 i Windows 98 konieczne jest posłużenie się narzędziem System Policy Editor dołączonym do każdego z nich i skopiowanie pliku zasad do udziału Sysvol na kontrolerze domeny.

Ustawienia Zasad grupy przechowywane są w obiektach zasad grupy (Group Policy Object –GPO). GPO można traktować jako pojemnik na zasady, które mają zostać zastosowane. Wobec pojedynczego obiektu Active Directory (lokacji, domeny lub jednostki organizacyjnej) można zastosować wiele obiektów zasad. Ponieważ Zasady grupy używają pojęcia

obiektów, zastosowanie ma wiele koncepcji projektowania obiektowego. Ktoś, kto zetknął się z programowaniem zorientowanym obiektowo, może zatem spodziewać się takich mechanizmów, jak zależności pomiędzy obiektem nadrzędnym (rodzicielskim) i podrzędnym (potomnym) oraz dziedziczenie – i będzie miał słuszość.

Terminem *kontenera* określa się obiekt, który może zawierać inne obiekty. Dzięki dziedziczeniu zasady zastosowane do kontenera nadrzędnego są przejmowane przez obiekty w nim zawarte – także inne kontenery. Uściślając, oznacza to, że ustawienie zasad zaaplikowane do obiektu nadrzędnego jest przekazywane w dół przez kolejne poziomy obiekty podrzędnych. Na przykład ustawienie zasad zaaplikowane na poziomie domeny zostanie odziedziczone przez wszystkie jednostki organizacyjne w tej domenie. W tym wypadku GPO powiązany z domeną jest obiektem nadrzędnym, a GPO powiązane z jednostkami organizacyjnymi (o ile istnieją) – obiektami podrzędnymi.

Porządek dziedziczenia jest następujący:

Lokacja → Domena → Jednostka organizacyjna

Oznacza to, że ustawienia Zasad grupy dla lokacji są przekazywane do domen w tej lokacji, zaś ustawienia dla domen do jednostek organizacyjnych wewnątrz odpowiedniej domeny.

Jak można się spodziewać, dziedziczenie można zablokować. W tym celu należy na niższym poziomie kontenerów przypisać ustawienie, które znosi ustawienie zastosowane na wyższym poziomie. O ile zastępowanie zasad jest dozwolone (to znaczy nie jest zablokowane), ustawienie niższego poziomu będzie ostatecznym (wynikowym). Blokowanie zastępowania zostało omówione w podrozdziale „Blokowanie, zastępowanie i wyłączanie zasad”.

Kolejność stosowania wielu obiektów zasad

Na każdym komputerze i dla każdego użytkownika Zasady grupy są stosowane w następującej kolejności:

1. Lokalne ustawienia zasad
2. Zasady grupy dla lokacji
3. Zasady grupy dla domeny
4. Zasady grupy dla jednostki organizacyjnej
5. Zasady grupy dla podrzędnych jednostek organizacyjnych (o ile istnieją)

W razie wystąpienia konfliktu pomiędzy ustawieniami zasad pierwszeństwo mają zasady zaaplikowane później, które zastępują wcześniej narzucone ustawienia. Oznacza to na przykład, że zasady jednostek organizacyjnych mają pierwszeństwo przed zasadami dla domen. Jak można się spodziewać, także od tej reguły mogą istnieć wyjątki, które zostały omówione w podrozdziale „Blokowanie, zastępowanie i wyłączanie zasad”.

Kiedy zasady grupy są stosowane?

Jak można szybko zauważyć, ustawienia zasad grupy dzielą się na dwie ogólne kategorie:

- Te, które są stosowane do komputerów
- Te, które dotyczą użytkowników

Zasady dotyczące komputerów są w normalnym trybie aplikowane podczas uruchamiania systemu, zaś zasady użytkowników podczas logowania. Dokładna sekwencja zdarzeń jest często ważna przy rozwiązywaniu problemów z zachowaniem systemu. Zdarzenia, które mają miejsce podczas procedury rozruchowej i logowania są następujące:

1. Sieć zostaje uruchomiona, po czym system operacyjny (na przykład Windows Server 2008) stosuje zasady dotyczące komputera. Domyślnie zasady komputera aplikowane są po jednej na raz, we wcześniej ustalonej kolejności. W czasie przetwarzania zasad komputera nie jest wyświetlany żaden interfejs użytkownika.
2. System wykonuje skrypty rozruchowe. Także te skrypty są wykonywane po jednym na raz, przy czym uruchomienie kolejnego skryptu następuje po zakończeniu poprzedniego (lub przekroczeniu czasu oczekiwania). Wyniki skryptów nie są wyświetlane dla użytkownika, o ile nie określono inaczej.
3. Pojawia się interfejs użytkownika, który naciska Ctrl+Alt+Del w celu zalogowania. Po weryfikacji tożsamości Windows Server 2008 łąduje profil użytkownika.
4. Windows Server 2008 aplikuje zasady dotyczące użytkownika. Domyślnie zasady są stosowane po jednej na raz we wcześniej ustalonej kolejności. W trakcie przetwarzania zasad wyświetlany jest interfejs użytkownika.
5. Windows Server 2008 wykonuje skrypty logowania. Skrypty zdefiniowane w Zasadach grupy są domyślnie wykonywane równolegle. Wykonywanie skryptu nie jest demonstrowane użytkownikowi, o ile nie zostanie jawnie włączone. Skrypty zawarte w udziale Netlogon są wykonywane w ostatniej kolejności w zwykłym oknie trybu wiersza polecenia.
6. Windows Server 2008 wyświetla początkowy interfejs powłoki skonfigurowany w Zasadach grupy.
7. Domyślnie Zasady grupy odświeżane są podczas wylogowywania użytkowników lub ponownego uruchamiania komputera. Zachowanie to można zmienić definiując interwał odświeżania Zasad grupy, zgodnie z omówieniem zawartym w podrozdziale „Odświeżanie Zasad grupy”. Można również ręcznie odświeżyć Zasady grupy, wykonując polecenie **gpupdate**.

W praktyce

Niektóre ustawienia użytkownika, takie jak Folder Redirection (Przekierowanie folderów), nie mogą zostać zaktualizowane, dopóki użytkownik jest zalogowany. W celu zaaplikowania tych ustawień użytkownik musi się wylogować i zalogować ponownie. Można użyć polecenia **gpupdate /logoff**, aby wymusić automatyczne wylogowania użytkownika po odświeżeniu zasad. Również niektóre ustawienia komputera mogą być zastosowane tylko podczas rozruchu systemu. W takim wypadku można użyć polecenia **gpupdate /boot**, aby wymusić ponowne uruchomienie komputera po odświeżeniu zasad.

Uwarunkowania Zasad grupy i zgodność wersji

Zasady grupy zostały wprowadzone w systemie Windows 2000 i mają zastosowanie tylko do komputerów (stacji roboczych i serwerów) pracujących pod kontrolą systemu Windows 2000 i późniejszych. Jak można się spodziewać, każda nowsza wersja systemu Windows dodaje pewne zmiany w mechanizmie Zasad grupy. Zmiany te niekiedy powodują, że dotychczasowe zasady stają się przestarzałe w nowszych wersjach systemu. W takim wypadku ustawienia zasad działają tylko na konkretnych wersjach systemu Windows, na przykład tylko w Windows XP Professional lub Windows Server 2003.

Jednak najogólniej ujmując, większość zasad jest kompatybilnych w przód. Oznacza to, że zasady wprowadzone w systemie Windows 2000 w większości wypadków mogą być używane w Windows 2000, Windows XP Professional, Windows Server 2003, Windows Vista i Windows Server 2008. Oznacza to również, że zasady, które pojawiły się w Windows

XP Professional, na ogół nie będą możliwe do zastosowania w Windows 2000, a tych, które wprowadzono wraz z Windows Vista, nie da się zaaplikować do Windows 2000 ani Windows XP Professional.

Ustawień zasad, które nie są obsługiwane przez daną wersję systemu Windows, nie można wymusić na komputerach używających tej wersji systemu operacyjnego.

Jak można ustalić, czy dana zasada jest obsługiwana przez konkretną wersję Windows? To proste. Okno dialogowe właściwości dla każdej zasady na zakładce Settings (Ustawienia) zawiera pole Supported On (Obsługiwane w). To pole tekstowe zawiera listę systemów zgodnych z daną zasadą. Wybranie zasady w rozszerzonym trybie wyświetlania w dowolnym edytorze Zasad grupy również pokazuje wpis Requirements (Wymagania), który zawiera tę samą listę.

Nowe zasady mogą pojawiać się przy instalowaniu pakietów serwisowych, aplikacji Windows lub dodatkowych składników systemu.

Przeglądanie zmian w Zasadach grupy

Dążąc do uporządkowania technik zarządzania Zasadami grupy firma Microsoft usunęła funkcje zarządzające z narzędzi Active Directory i przeniosła je do podstawowej konsoli o nazwie Group Policy Management Console – GPMC (Konsola zarządzania zasadami grupy). Konsolę tę można dodać jako rozszerzenie do dowolnej instalacji systemu Windows Server 2008. GPMC jest również dołączona do systemu Windows Vista, a ponadto można ją pobrać z witryny Microsoft. Po dodaniu GPMC do serwera można ją uruchomić za pośrednictwem menu Administrative Tools.

Próba edytowania GPO w konsoli GPMC powoduje uruchomienie Group Policy Management Editor (Edytora zarządzania zasadami grupy), umożliwiającego modyfikowanie ustawień zasad. Gdyby Microsoft ograniczył się tylko do tych dwóch narzędzi, mielibyśmy doskonale i łatwe w użyciu środowisko zarządzania zasadami. Niestety, istnieje jeszcze kilka innych edytorów o niemal identycznej funkcjonalności, w tym:

Group Policy Starter GPO Editor Edytor pozwalający na utworzenie i zarządzanie startowymi obiektami zasad. Jak można wywnioskować z nazwy, startowe GPO mają na celu zapewnienie punktu wyjściowego dla nowych obiektów zasad, które mają być używane w organizacji. Przy tworzeniu nowego obiektu zasad można wskazać startowy GPO jako źródło czy też podstawę dla nowego obiektu.

Local Group Policy Object Editor (Edytor lokalnego obiektu zasad) Edytor ten umożliwia tworzenie i zarządzanie obiektami zasad komputera lokalnego. Zgodnie z nazwą, lokalne GPO mają na celu dostarczenie ustawień zasad dla konkretnego komputera w odróżnieniu od ustawień narzucanych całej lokacji, domenie lub jednostce organizacyjnej.

Osoby, które używały wcześniejszych wersji serwerów Windows, mogą już znać narzędzie Group Policy Object Editor – GPOE (Edytor obiektów zasad grupy). W systemie Windows Server 2003 i wcześniejszych GPOE był podstawowym narzędziem edytowania ustawień zasad. Group Policy Object Editor, Group Policy Management Editor, Group Policy Starter GPO Editor oraz Local Group Policy Object Editor są zasadniczo identyczne – różnią się tylko zbiorem obiektów, do których można uzyskać dostęp. Z tego względu, a także dlatego, że zarządzanie poszczególnymi obiektami zasad odbywa się w każdym z nich w taki sam sposób, nie będziemy rozróżniali ich od siebie, o ile nie będzie to konieczne. Wszystkie te narzędzia będziemy nazywać wspólnym mianem *edytorów zasad*. Niekiedy może pojawić

się akronim GPOE jako ogólne wskazanie edytorów zasad, gdyż jest on łatwiejszy do odróżnienia od skrótu nazwy konsoli zarządzającej, czyli GPMC.

Ustawieniami zasad specyficznych dla systemów Windows Vista i Windows Server 2008 można zarządzać tylko z komputerów jednego z tych systemów. Przyczyną takiego stanu rzeczy jest fakt, że w systemach tych dostępne są nowe wersje GPOE oraz GPMC, zaktualizowanych w celu umożliwienia korzystania z nowego, opartego na XML formacie szablonów administracyjnych o nazwie ADMX.

Uwaga Szablonów ADMX nie można przetwarzać w edytorach zasad starszych wersji. Obiekty zasad wykorzystujące pliki ADMX mogą być edytowane tylko na komputerach pracujących pod kontrolą systemu Windows Vista lub Windows Server 2008.

Firma Microsoft miała wiele powodów, aby wprowadzić nowy format. Do kluczowych przyczyn należy zaliczyć zwiększoną elastyczność i rozszerzalność. Ponieważ pliki ADMX są w istocie plikami XML, są one w pełni strukturalne, dzięki czemu łatwiejsze i znacznie szybsze jest ich przetwarzanie podczas inicjowania. Pozwala to podnieść wydajność przetwarzania Zasad grupy podczas faz rozruchu, logowania, wylogowywania i zamykania systemu, a także w trakcie odświeżania zasad. Ponadto ścisła struktura plików ADMX ułatwia dalsze działania firmy Microsoft w kierunku umiędzynarodowienia oprogramowania.

Pliki ADMX dzielą się na pliki neutralne językowo z rozszerzeniem .admx oraz pliki specyficzne dla języka z rozszerzeniem .adml. Pliki neutralne gwarantują, że obiekt zasad zawiera identyczne zasady (jeśli chodzi o ich sens). Pliki językowe pozwalają na wyświetlanie zasad w wielu językach. Ponieważ to pliki neutralne zawierają właściwe ustawienia, zasady można edytować w dowolnym języku skonfigurowanym na danym komputerze, co oznacza, że jeden użytkownik może przeglądać i edytować zasady w języku angielskim, a inny na przykład w hiszpańskim. Mechanizmem determinującym użycie języka jest pakiet językowy zainstalowany na komputerze.

Na komputerach systemów Windows Vista lub Windows Server 2008 neutralne językowo pliki ADMX instalowane są w folderze %SystemRoot%\PolicyDefinitions. Pliki specyficzne dla języka umieszczane są w folderze %SystemRoot%\PolicyDefinitions\LanguageCulture. Każdy podfolder nosi nazwę zgodną z zalecaną przez International Organization for Standardization (ISO), na przykład EN-US oznacza *US English*.

Podczas uruchamiania edytora zasad odczytuje on automatycznie pliki ADMX z folderów definicyjnych. Dzięki temu można udostępnić dodatkowe pliki ADMX po prostu kopiując je do odpowiednich folderów definicji zasad. Jeśli pliki zostaną skopiowane przy uruchomieniu edytora, w celu ponownego odczytania plików konieczne będzie zamknięcie edytora i uruchomienie go ponownie.

W środowisku domeny pliki ADMX mogą być przechowywane w centralnym magazynie – katalogu wspólnym dla całej domeny, utworzonym wewnątrz katalogu Sysvol (%SystemRoot%\Sysvol\Domain\Policies). W tym wypadku szablon administracyjny nie są już zapisywane wraz z każdym GPO. Zamiast tego GPO zawiera tylko bieżący stan ustawienia, zaś pliki ADMX są przechowywane centralnie. Pozwala to zredukować wielkość miejsca zajmowanego w miarę wzrostu liczby GPO, a także zmniejszyć liczbę danych replikowanych pomiędzy kontrolerami domeny w przedsiębiorstwie. Dopóki edycja GPO będzie wykonywana tylko przy użyciu Windows Vista lub Windows Server 2008, nowe obiekty zasad nie będą zawierały ani plików ADM, ani ADMX. Więcej informacji zawiera podrozdział „Tworzenie magazynu centralnego”.

Przy korzystaniu z poziomu funkcjonalności domeny Windows Server 2008 implementowany jest nowy mechanizm replikacji Zasad grupy, zwany Distributed File System (DFS)

Replication Service. Przy replikacji DFS kopiowane są tylko zmiany dokonane w obiektach zasad, tym samym eliminując potrzebę replikowania całego GPO po modyfikacji.

W odróżnieniu od Windows Server 2003, Windows Server 2008 wykorzystuje usługę Group Policy Client (Klient Zasad grupy) w celu odizolowania powiadamiania i przetwarzania Zasad grupy od procesu logowania Windows. Rozdzielenie tych procesów zmniejsza wielkość zasobów wymaganych dla przetwarzania zasad w tle, przy jednoczesnym podniesieniu ogólnej wydajności i umożliwieniu dostarczania i aplikowania nowych plików Zasad grupy jako części procesu aktualizacji, bez wymagania ponownego uruchamiania komputerów.

Windows Server 2008 nie wykorzystuje funkcjonalności śledzenia dzienników zawartej w bibliotece userenv.dll, zapisując zamiast tego zdarzenia dotyczące Zasad grupy w dzienniku systemowym. Co więcej, dziennik operacyjny Zasad grupy zastępuje wcześniejszy mechanizm rejestrowania Userenv. Podczas rozwiązywania problemów dotyczących Zasad grupy należy posługiwać się raczej szczegółowymi komunikatami o zdarzeniach zawartych w dzienniku operacyjnym, zamiast dziennika Userenv. Dziennik operacyjny jest dostępny w narzędziu Event Viewer (Podgląd zdarzeń) w gałęzi Applications And Services Logs\Microsoft\Windows\GroupPolicy.

Windows Server 2008 wykorzystuje mechanizm Network Location Awareness (Rozpoznawanie lokalizacji w sieci) zamiast protokołu ICMP (ping). Przy korzystaniu z Network Location Awareness komputer rozpoznaje typ sieci, z którą jest aktualnie połączony i może również reagować na zmiany w stanie systemu lub konfiguracji sieci. Przy użyciu Network Location Awareness klient zasad grupy może rozpoznać stan komputera, stan sieci i dostępne pasmo sieciowe w celu wykrywania powolnych łączy.

Zarządzanie zasadami lokalnymi

Windows Server 2008 umożliwia stosowanie wielu lokalnych obiektów zasad grupy (Local Group Policy Object – LGPO) na jednym komputerze (o ile komputer ten nie jest kontrolerem domeny). We wcześniejszych wersjach systemu komputery zawierały tylko jeden LGPO. Windows Server 2008 pozwala na przypisanie innego LGPO dla każdego lokalnego użytkownika lub ogólnego typu użytkownika. Pozwala to na bardziej elastyczne stosowanie zasad i obsługę szerszego zakresu rozwiązań implementacyjnych.

Lokalne obiekty zasad grupy

W przypadku komputerów w konfiguracji autonomicznej (które nie są członkami domeny) możliwość zastosowania kilku LGPO jest bardzo użyteczna, gdyż na przykład nie zachodzi już potrzeba jawnego wyłączenia lub usuwania ustawień, które mogłyby zakłócać możliwość zarządzania komputerem przed wykonaniem zadań administracyjnych. Zamiast tego można zastosować jeden obiekt LGPO dla administratorów, a inny dla pozostałych (nieadministracyjnych) użytkowników. W konfiguracji domenowej nie należy raczej stosować licznych obiektów lokalnych. W takim środowisku większość komputerów i użytkowników już ma przypisanych kilka obiektów Zasad grupy – dodawanie do tej już złożonej mieszanki jeszcze kilku lokalnych obiektów zasad może skrajnie skomplikować zarządzanie zasadami.

System Windows Server 2008 zawiera trzy warstwy lokalnych obiektów zasad:

Local Group Policy (Lokalne zasady grupy) Jest to jedyny LGPO umożliwiający stosowanie zarówno ustawień konfiguracji komputera, jak i konfiguracji użytkownika, które dotyczą wszystkich użytkowników tego komputera.

Administrators and Non-Administrators Local Group Policy (Lokalne zasady grupy dla administratorów i nie-administratorów) Obiekty te zawierają tylko ustawienia konfiguracji użytkownika. Zasady stosowane są zależnie od tego, czy użytkownik jest członkiem lokalnej grupy Administrators.

User-specific Local Group Policy (Lokalne zasady grupy specyficzne dla użytkownika) Obiekty te zawierają tylko ustawienia konfiguracji użytkownika. Zasady te są stosowane wobec indywidualnych użytkowników lub grup.

Poszczególne warstwy lokalnych obiektów zasad grupy są przetwarzane w następującej kolejności: lokalne zasady grupy, następnie zasady dla administratorów i nie-administratorów, a na końcu zasady specyficzne dla użytkowników.

Ponieważ ustawienia gałęzi konfiguracji użytkownika są identyczne dla wszystkich lokalnych obiektów zasad, ustawienia zawarte w jednym GPO mogą być sprzeczne z ustawieniami w innym GPO. W takiej sytuacji ustawienia kolejnego odczytywanego obiektu zastępują wcześniejsze. Przy rozwiązywaniu konfliktów pod uwagę brane są tylko ustawienia włączone lub wyłączone – jeśli ustawienie ma wartość Not Configured (Nieskonfigurowane), nie ma to wpływu na stan tego ustawienia pochodzący z wcześniejszego obiektu zasad. W celu uproszczenia administrowania domeną można wyłączyć przetwarzanie lokalnych obiektów zasad grupy na komputerach systemu Windows Server 2008, włączając ustawienie Turn Off Local Group Policy Objects Processing (Wyłącz przetwarzanie lokalnych obiektów zasad grupy) w domenowym obiekcie zasad. Ustawienie to jest zlokalizowane w gałęzi Computer Configuration\Administrative Templates\System\Group Policy.

Uzyskiwanie dostępu do lokalnych ustawień zasad najwyższego poziomu

Z wyjątkiem kontrolerów domeny wszystkie komputery pracujące pod kontrolą systemu Windows 2000 i wersji późniejszych zawierają edytowalny lokalny obiekt zasad grupy. Najszybszą metodą dostępu do LGPO na komputerze lokalnym jest wpisanie następującego polecenia:

```
gpedit.msc /gpcomputer: "%ComputerName%"
```

Polecenie to uruchamia GPOE w konsoli Microsoft Management Console (MMC), przy czym edytowane są ustawienia lokalnego komputera. *%ComputerName%* jest zmienną środowiskową, która zawiera nazwę komputera lokalnego i musi być zawarta w podwójnych cudzysłowach, jak w powyższym przykładzie. Aby uzyskać dostęp do zasad lokalnych na komputerze zdalnym należy wpisać polecenie:

```
gpedit.msc /gpcomputer: "RemoteComputer"
```

gdzie *RemoteComputer* jest nazwą hosta lub w pełni kwalifikowaną nazwą domenową komputera zdalnego. Także i tu nazwę tę należy ująć w podwójne nawiasy:

```
gpedit.msc /gpcomputer: "corpsvr82"
```

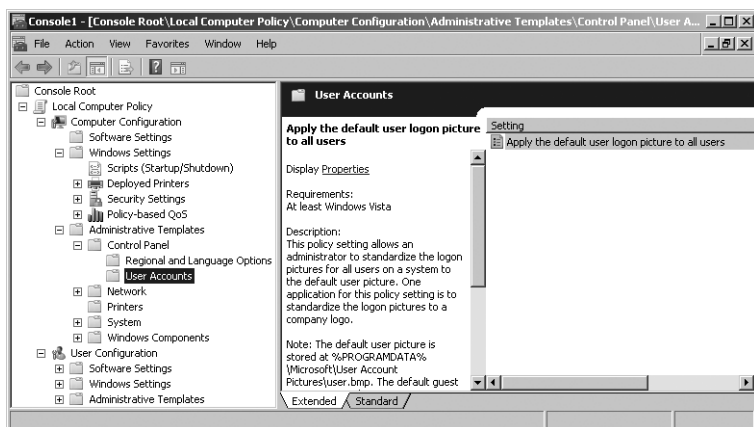
Alternatywnie można zarządzać zasadami lokalnymi najwyższego poziomu na komputerze lokalnym, wykonując następującą procedurę:

1. Kliknij Start, wpisz **mmc** w polu Search, po czym naciśnij Enter.

2. W konsoli Microsoft Management Console kliknij File (Plik), a następnie Add/Remove Snap-In (Dodaj/usuń przystawkę).
3. W oknie dialogowym Add Or Remove Snap-Ins kliknij Group Policy Object Editor (Edytor obiektów zasad grupy), po czym kliknij Add (Dodaj).
4. W oknie dialogowym Select Group Policy Object (Wybierz obiekt zasad grupy) kliknij Finish (Zakończ), gdyż domyślnym obiektem jest komputer lokalny, po czym kliknij OK.

Jak widać na rysunku 5-1, można następnie zarządzać ustawieniami lokalnymi używając udostępnionych opcji.

Wskazówka Ta sama przystawka MMC umożliwia zarządzanie więcej niż jednym lokalnym obiektem grupy. W oknie dialogowym Add Or Remove Snap-Ins można dodać kolejną instancję Local Group Policy Object Editor dla każdego obiektu zasad.



Rysunek 5-1 Edytor zasad umożliwia zarządzanie lokalnymi ustawieniami zasad.

Ustawienia LGPO

Lokalne zasady grupy przechowywane są w folderze %SystemRoot%\System32\GroupPolicy na każdym komputerze systemu Windows Server 2008. Można w nim znaleźć następujące podfoldery:

- Machine** Zawiera skrypty komputera w folderze Script oraz informacje zasad dotyczące rejestru (przeznaczone dla gałęzi HKEY_LOCAL_MACHINE – HKLM) w pliku Registry.pol file.
- User** Zawiera skrypty użytkownika w folderze Script oraz informacje zasad dotyczące rejestru dla gałęzi HKEY_CURRENT_USER (HKCU) w pliku Registry.pol.

Ostrzeżenie Nie należy próbować bezpośredniego edytowania zawartości tych folderów i plików. Zamiast tego należy posłużyć się odpowiednimi funkcjami jednego z narzędzi zarządzania zasadami grupy. Domyślnie pliki te i foldery są ukryte. W celu wyświetlenia ukrytych plików i folderów w Eksploratorze Windows należy wybrać polecenie Folder Options (Opcje folderów) z menu Tools (Narzędzia), kliknąć zakładkę View (Widok), zaznaczyć pole wyboru Show Hidden Files And Folders (Wyświetlaj ukryte pliki i foldery), wyczyścić pole wyboru Hide Protected Operating System Files (Recommended) (Ukryj chronione pliki systemu operacyjnego), w ostrzegawczym oknie dialogowym kliknąć Yes, po czym kliknąć OK.

Uzyskiwanie dostępu do obiektów zasad administratorów, nie-administratorów oraz specyficznych dla użytkownika

Domyślnie na każdym komputerze istnieje tylko jeden obiekt zasad – jest to Local Group Policy Object. Można jednak utworzyć i wykorzystać inne obiekty lokalne w miarę potrzeb. W celu utworzenia lub uzyskania dostępu do obiektu zasad grupy dla administratorów (lub nie-administratorów), wykonaj następującą procedurę:

1. Kliknij Start, wpisz **mmc** w polu Search, po czym naciśnij Enter. W konsoli Microsoft Management Console kliknij File, a następnie kliknij Add/Remove Snap-In.
2. W oknie dialogowym Add Or Remove Snap-Ins kliknij Group Policy Object Editor, po czym kliknij Add.
3. W oknie dialogowym Select Group Policy Object kliknij Browse (Przeglądaj), po czym w oknie dialogowym Browse For A Group Policy Object (Przeglądanie w poszukiwaniu obiektu zasad grupy) zakładkę Users.
4. Wpisy w kolumnie Group Policy Exists (Istniejące zasady grupy) określają, czy dla danego użytkownika (klasy użytkowników) utworzono obiekt zasad. Można tu wykonać jedno z poniższych:
 - Zaznaczyć grupę Administrators, aby utworzyć lub uzyskać dostęp do lokalnego obiektu zasad dla administratorów.
 - Zaznaczyć klasę Non-Administrators (Nie-administratorzy), aby utworzyć lub uzyskać dostęp do lokalnego obiektu zasad dla użytkowników nieadministracyjnych.
 - Zaznaczyć użytkownika lokalnego, dla którego zamierza się utworzyć lub edytować lokalny obiekt zasad.
5. Kliknij OK. Jeśli wybrany obiekt dotychczas nie istniał, zostanie utworzony. W innym wypadku istniejący obiekt zostanie otwarty do edycji.

Ustawienia zasad dla administratorów, nie-administratorów oraz indywidualnych użytkowników są przechowywane w folderze %SystemRoot%\System32\GroupPolicyUsers na każdym komputerze systemu Windows Server 2008. Ponieważ te LGPO aplikują tylko ustawienia konfiguracji użytkownika, folder %SystemRoot%\System32\GroupPolicyUsers zawiera tylko podfolder User, w którym znajduje się folder Script ze skryptami użytkownika oraz dane rejestru dla gałęzi HKEY_CURRENT_USER (HKCU) w pliku Registry.pol.

Zarządzanie zasadami dla lokacji, domeny i jednostki organizacyjnej

Po wdrożeniu Active Directory Domain Services można wykorzystać Zasady grupy usługi katalogowej Active Directory. Każda lokacja, domena i jednostka organizacyjna może mieć jeden lub więcej obiektów zasad grupy. Zasady wymienione na wyższej pozycji listy Zasad mają pierwszeństwo przed zasadami umieszczonymi na dalszych miejscach listy. Gwarantuje to, że zasady są stosowane we właściwym porządku w odpowiednich lokacjach, domenach i jednostkach organizacyjnych.

Istota domyślnych zasad domenowych

Zapoznając się z Zasadami grupy w usłudze katalogowej Active Directory można zauważyć, że każda domena zawiera dwa domyślne GPO:

Default Domain Controllers Policy GPO Domyślny GPO utworzony i połączony z jednostką organizacyjną Domain Controllers (Kontrolery domeny). Obiekt ten stosowany jest do wszystkich kontrolerów domeny (o ile nie zostaną one przeniesione do innej jednostki organizacyjnej). Służy on do zarządzania ustawieniami zabezpieczeń kontrolerów domeny.

Default Domain Policy GPO Domyślny GPO utworzony i połączony z samą domeną Active Directory. Obiekt ten pozwala określić bazową konfigurację różnorodnych ustawień zasad, które są stosowane do wszystkich użytkowników i komputerów w domenie.

Zazwyczaj Default Domain Policy GPO jest obiektem o najwyższym priorytecie połączonym na poziomie domeny, zaś Default Domain Controllers Policy GPO jest obiektem najwyższego poziomu przypisanym do kontenera Domain Controllers. Zarówno na poziomie domeny, jak kontenera Domain Controllers można dołączyć kolejne obiekty zasad. W takim wypadku ustawienia GPO o wyższym priorytecie zastępują ustawienia zawarte w obiektach zasad niższego poziomu. Te GPO nie mają na celu ogólnego zarządzania zasadami grupy.

Default Domain Policy GPO służy tylko do zarządzania domyślnymi ustawieniami konta (Account Policies), a w szczególności trzema szczególnymi dziedzinami tych ustawień: Password Policy (Zasady haseł), Account Lockout Policy (Zasady blokady konta) oraz Kerberos Policy (Zasadami protokołu Kerberos). Ponadto GPO ten zarządza czterema wybranymi opcjami zabezpieczeń. Są to Accounts: Rename Administrator Account (Konta: Zmień nazwę konta administratora), Accounts: Rename Guest Account (Konta: Zmień nazwę konta gościa), Network Security: Force Logoff When Logon Hours Expire (Zabezpieczenia sieciowe: Wymuś wylogowanie użytkowników po upływie czasu logowania) oraz Network Access: Allow Anonymous SID/Name Translation (Dostęp sieciowy: zezwalaj na anonimową translację identyfikatorów SID/nazw). Jedną z metod zmiany tych ustawień jest utworzenie nowego GPO z odmiennymi ustawieniami i połączenie go z kontenerem domeny z wyższym poziomem priorytetu.

Obiekt Default Domain Controllers Policy zawiera szczególne ustawienia User Rights Assignment (Przypisywanie praw użytkownika) oraz Security Options (Opcje zabezpieczeń), ograniczające sposoby korzystania z kontrolerów domeny. Także w tym wypadku zalecaną metodą zmiany tych ustawień jest utworzenie nowego GPO z innymi ustawieniami i połączenie go z kontenerem Domain Controllers z jednoczesnym ustawieniem wyższego priorytetu.

W celu zarządzania innymi obszarami zasad należy stworzyć nowe GPO i łączyć je z kontenerem domeny lub odpowiednimi jednostkami organizacyjnymi w obrębie domeny.

Zasady grupy dla lokacji, domeny i jednostek organizacyjnych są przechowywane w folderze %SystemRoot%\Sysvol\Domain\Policies na kontrolerach domeny. Folder ten zawiera podfolder dla każdego obiektu zasad zdefiniowanego na kontrolerze domeny. Nazwą folderu zasad jest globalnie unikatowy identyfikator obiektu (GUID). W celu ustalenia GUID konkretnego obiektu zasad należy sprawdzić stronę Properties (Właściwości) na zakładce General (Ogólne) w ramce podsumowania. Wewnątrz folderów poszczególnych zasad można znaleźć następujące podfoldery:

Machine Przechowuje skrypty komputera w folderze Script oraz informacje rejestru zasady przeznaczone dla gałęzi HKEY_LOCAL_MACHINE (HKLM) w pliku Registry.pol.

User Przechowuje skrypty użytkownika w folderze Script oraz informacje rejestru zasady przeznaczone dla gałęzi HKEY_CURRENT_USER (HKCU) w pliku Registry.pol.

Ostrzeżenie Nie należy próbować bezpośredniego edytowania tych folderów ani plików. Zamiast tego należy posłużyć się odpowiednimi funkcjami jednego z narzędzi zarządzania zasadami grupy.

Korzystanie z narzędzia Group Policy Management Console

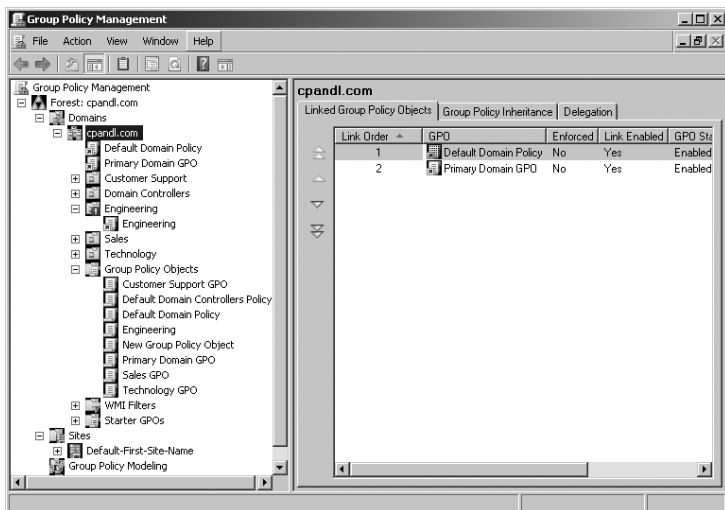
W celu uruchomienia narzędzia GPMC należy kolejno kliknąć Start, All Programs (Wszystkie programy), Administrative Tools (Narzędzia administracyjne), a na koniec Group Policy Management Console. Jak widać na rysunku 5-2, węzeł korzenia konsoli ma etykietę Group Policy Management, zaś bezpośrednio podrzędny węzeł nosi nazwę Forest (Las@@@). Węzeł ten reprezentuje las Active Directory, z którym aktualnie połączona jest konsola – nosi on nazwę głównej domeny tego lasu. Dysponując odpowiednimi uprawnieniami można utworzyć połączenia do innych lasów. W tym celu należy kliknąć prawym klawiszem myszy węzeł Group Policy Management, po czym wybrać polecenie Add Forest (Dodaj las). Następnie w oknie dialogowym Add Forest trzeba wpisać nazwę domeny głównej lasu w polu tekstowym Domain i kliknąć OK.

Po rozwinięciu węzła Forest ujrzymy następujące węzły:

Domains (Domeny) Zapewnia dostęp do ustawień zasad w poszczególnych domenach odpowiedniego lasu. Domyślnie konsola połączona jest z domeną, w której zalogowany jest użytkownik. Dysponując odpowiednimi uprawnieniami można dodać połączenia do innych domen. W tym celu należy kliknąć prawym klawiszem myszy węzeł Domains i następnie wybrać polecenie Show Domains (Pokaż domeny). Następnie w oknie dialogowym Show Domains należy zaznaczyć pola wyboru przy nazwach domen, które chce się dołączyć, po czym kliknąć OK.

Sites (Lokacje) Zapewnia dostęp do ustawień zasad dla lokacji wybranego lasu. Lokacje są domyślnie ukryte. Przyłączenie lokacji do konsoli wymaga odpowiednich uprawnień. W tym celu należy kliknąć prawym klawiszem myszy węzeł Sites i wybrać polecenie Show Sites (Pokaż lokacje). Następnie w oknie dialogowym Show Sites należy zaznaczyć pola wyboru przy odpowiednich lokacjach, po czym kliknąć OK.

Group Policy Modeling (Modelowanie zasad grupy) Zapewnia dostęp do kreatora Group Policy Modeling Wizard, ułatwiającego planowanie wdrożenia zasad i umożliwiającego symulację działania ustawień w celach testowych. Możliwe jest również zapisywanie modeli w celu ich dalszej analizy lub zastosowania w rzeczywistości.



Rysunek 5-2 GPMC umożliwia obsługę obiektów zasad w różnych lokacjach, lasach i domenach.

Group Policy Results (Wyniki zasad grupy) Zapewnia dostęp do kreatora Group Policy Results Wizard. Umożliwia on sprawdzenie faktycznych ustawień zasad pochodzących z każdego GPO dla każdej domeny i jednostki organizacyjnej, z którą konsola jest połączona.

Obiekty zasad wymienione w kontenerach domeny, lokacji lub jednostki organizacyjnej w GPMC są w rzeczywistości połączeniami GPO, a nie samymi GPO. Bezpośredni dostęp do rzeczywistych obiektów zasad umożliwia kontener Group Policy Objects (Obiekty zasad grupy) dla wybranej domeny. Warto zauważyć, że ikony połączeń GPO zawierają małe strzałki w lewym dolnym rogu, podobnie jak ikony skrótów, podczas gdy ikony samych GPO strzałek tych nie zawierają.

Po uruchomieniu GPMC konsola łączy się domyślnie z usługą Active Directory uruchomioną na kontrolerze domeny odgrywającym rolę emulatora PDC w domenie logowania i pobiera listę wszystkich obiektów zasad oraz jednostek organizacyjnych (OU) w tej domenie. W celu uzyskania dostępu do magazynu katalogu wykorzystywany jest protokół LDAP, a do odczytania zawartości katalogu Sysvol protokół Server Message Block (SMB). Jeśli emulador PDC nie jest dostępny, na przykład z powodu czasowego wyłączenia, GPMC wyświetla monit pozwalający pobrać ustawienia zasad z kontrolera domeny, z którym komputer jest aktualnie połączony (tego, który wykonał uwierzytelnienie) albo wskazać inny dostępny kontroler domeny. Można również zmienić kontroler domeny, z którym konsola jest połączona. W tym celu należy kliknąć prawym klawiszem myszy węzeł domeny, z której zamierzamy wybrać kontroler domeny, po czym wybrać polecenie Change Domain Controller (Zmień kontroler domeny). Aktualnie połączony kontroler domeny zostanie wyświetlony na liście Current Domain Controller w oknie dialogowym Change Controller. Należy wskazać odpowiedni kontroler domeny używając opcji dostępnych w sekcji Change To (Zmień na) i kliknąć OK.

Poznananie edytora zasad

W celu edycji obiektu zasad należy kliknąć go prawym klawiszem myszy w konsoli GPMC, po czym wybrać Edit z menu podręcznego. Jak widać na rysunku 5-3, edytor zasad zawiera dwa główne węzły:

Computer Configuration (Konfiguracja komputera) Umożliwia definiowanie zasad, które mają być stosowane do komputera bez względu na to, kto (i czy w ogóle) jest na nim zalogowany.

User Configuration (Konfiguracja użytkownika) Pozwala określać zasady, które mają być stosowane do użytkowników bez względu na to, na jakim komputerze się logują.

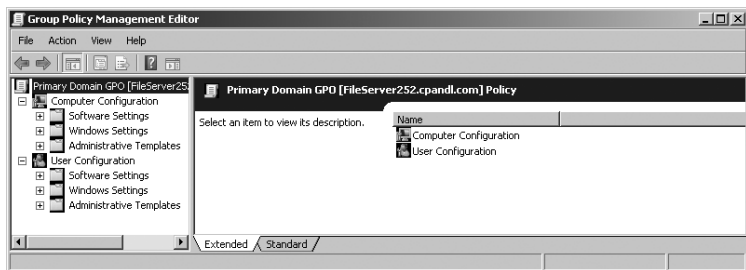
Konkretne ustawienia obu węzłów zależą od zainstalowanych dodatków, a także od typu edytowanej lub tworzonej zasady. Tym niemniej zazwyczaj w obu miejscach można znaleźć następujące podwęzły:

Software Settings (Ustawienia oprogramowania) Obejmują zasady dotyczące ustawień i instalacji oprogramowania. Podczas instalowania różnych programów w części tej mogą pojawiać się nowe podwęzły.

Windows Settings (Ustawienia systemu Windows) Zawiera zasady określające przekierowanie folderów, skrypty i ustawienia zabezpieczeń.

Administrative Templates (Szablony administracyjne) Zawiera zasady dla systemu operacyjnego, składników systemu Windows i innych programów. Szablony administracyjne są konfigurowane przez pliki szablonów. Pliki te można dodawać lub usuwać w dowolnym momencie.

Uwaga Szczegółowe omówienie dostępnych opcji wykracza poza zakres tematyczny tej książki. Kolejne podrozdziały skupiają się na konfigurowaniu przekierowania folderów i korzystaniu z szablonów administracyjnych. Zagadnienia dotyczące skryptów omówione są w podrozdziale „Zarządzanie skryptami użytkownika i komputera”. Zagadnienia zabezpieczeń omawia Część II tej książki.



Rysunek 5-3 Konfiguracja edytora zasad zależy od typu tworzonej zasady i zainstalowanych rozszerzeń.

Korzystanie z szablonów administracyjnych do ustawiania zasad

Szablony administracyjne zapewniają łatwy dostęp do ustawień zasad dotyczących rejestrów, które można konfigurować. Edytor zasad zawiera domyślny zestaw szablonów administracyjnych, tak dla użytkowników, jak i dla komputerów. Można również dołączać lub usuwać szablony. Dowolne zmiany dokonywane w zasadach za pośrednictwem szablonów są zapisywane w rejestrze komputera. Ustawienia dotyczące konfiguracji komputera zapisywane są w gałęzi HKEY_LOCAL_MACHINE (HKLM) rejestru, zaś ustawienia użytkownika w gałęzi HKEY_CURRENT_USER (HKCU).

Dostępne szablony zawiera węzeł Administrative Templates w edytorze zasad. Węzeł ten zawiera zasady, które można zastosować wobec systemów lokalnych, jednostek organizacyjnych domen lub lokacji. Warto zauważyć, że węzły Computer Configuration oraz User Configuration zawierają odmienne zestawy szablonów. Można również ręcznie dodać nowe szablony zawierające nowe ustawienia zasad. Nowe szablony mogą się również pojawić po zainstalowaniu dodatkowych składników systemu Windows.

Szablony administracyjne umożliwiają zarządzanie następującymi elementami systemu:

Control Panel (Panel sterowania) Określają dostępne opcje i konfigurację samego Panelu sterowania oraz narzędzi w nim zawartych.

Desktop (Pulpit) Konfigurują pulpit systemu Windows oraz dostępne opcje.

Network (Sieć) Konfigurują ustawienia sieci i opcje klienta sieci, takie jak pliki trybu offline, ustawienia DNS i połączenia sieciowe.

Printers (Drukarki) Konfigurują ustawienia drukarek, przeglądanie, buforowanie i opcje katalogów.

Shared folders (Udostępnione foldery) Umożliwiają publikowanie folderów udostępnionych oraz punktów źródłowych rozproszonego systemu plików (DFS).

Start menu and taskbar (Menu Start i pasek zadań) Sterują dostępnymi opcjami i konfiguracją menu Start i paska zadań.

System Konfigurują ustawienia systemowe, takie jak przydziały dysku, profile użytkowników, logowanie użytkowników, odzyskiwanie systemu, raportowanie błędów i tak dalej.

Windows components (Składniki systemu Windows) Określają dostępne opcje i konfigurację różnych składników Windows, w tym narzędzia Event Viewer, przeglądarki Internet Explorer, narzędzi Task Scheduler, Windows Installer oraz Windows Updates. Najlepszą metodą ustalenia, jakie są dostępne szablony, jest przejrzanie odpowiednich węzłów Administrative Templates. Podczas przeglądania szablonów można zauważyć, że zasady mogą mieć jeden z trzech stanów:

Not Configured (Nieskonfigurowana) Zasada nie jest używana i żadne jej ustawienia nie są zapisywane w rejestrze (nie są zmieniane ewentualne wcześniejsze ustawienia).

Enabled (Włączona) Zasada jest aktywnie wymuszana i jej ustawienia zostają zapisane w rejestrze.

Disabled (Wyłączona) Zasada jest nieaktywna i nie jest wymuszana, o ile nie zostanie zastąpiona. Ustawienie to jest zapisywane w rejestrze, anulując ewentualne wcześniejsze włączenie ustawień.

W celu włączenia, wyłączenia i skonfigurowania zasad wykonaj następującą procedurę:

1. Otwórz folder Administrative Templates (Szablony administracyjne) w węzle Computer Configuration lub User Configuration odpowiednio do typu modyfikowanej zasady w edytorze zasad.
2. W lewym panelu edytora wybierz podfolder zawierający zasady, które mają być modyfikowane. Odpowiednie zasady pojawiają się w prawym panelu edytora.
3. Kliknij podwójnie wybraną zasadę lub kliknij ją prawym klawiszem myszy i wybierz polecenie Properties (Właściwości), aby wyświetlić odpowiednie okno dialogowe Properties.
4. Kliknij zakładkę Explain (Wyjaśnij), aby wyświetlić opis zasady. Opis taki jest dostępny jedynie pod warunkiem, że został zdefiniowany w odpowiednim pliku szablonu.
5. W celu ustawienia stanu zasady kliknij zakładkę Settings (Ustawienia), po czym wybierz jeden z przycisków opcji, aby zmienić stan:
 - Not Configured** Zasada będzie nieskonfigurowana (ignorowana).
 - Enabled** Zasada zostanie włączona.
 - Disabled** Zasada zostanie wyłączona.
6. Po włączeniu zasady należy określić ewentualne dodatkowe parametry wymienione na zakładce Settings, po czym kliknij OK.

Uwaga W normalnej konfiguracji Windows Server 2008 zasady komputera mają pierwszeństwo przed ustawieniami użytkownika. W razie wystąpienia konfliktu pomiędzy ustawieniami komputera i użytkownika zastosowane zostaną zasady komputera.

Tworzenie centralnego magazynu

Magazyn centralny jest zbiorem folderów utworzonym w katalogu Sysvol na kontrolerze domeny, replikowanym do wszystkich kontrolerów domeny w organizacji. W celu umieszczenia plików ADMX w scentralizowanej lokalizacji należy utworzyć magazyn centralny na jednym kontrolerze domeny w każdej domenie. Zawartość tego magazynu zostanie następnie powielona przez usługę replikacji do pozostałych kontrolerów domeny. Ponieważ replikacja w dużej sieci może zająć trochę czasu, zalecane jest wykorzystanie do tego celu kontrolera domeny działającego jako emulator PDC, gdyż narzędzia GPOE oraz GPMC domyślnie łączą się z tym właśnie kontrolerem domeny.

Centralny magazyn może utworzyć każdy administrator będący członkiem grupy Domain Admins w domenie. W tym celu wykonaj następującą procedurę:

1. Po zalogowaniu się na kontrolerze domeny użyj Eksploratora Windows, aby utworzyć główny folder magazynu centralnego w katalogu %SystemRoot%\Domain\Policies.
2. Utwórz podfolder %SystemRoot%\Domain\Policies\PolicyDefinitions dla każdego języka, którego mają używać administratorzy zasad. Poszczególne podfoldery powinny mieć nazwy zgodne ze standardem nazewnictwa zdefiniowanym przez International Organization for Standardization (ISO), na przykład EN-US dla języka US English.
3. Następnie należy umieścić w magazynie pliki ADMX dystrybuowane z systemem Windows Vista. W tym celu zaloguj się na należącem do domeny komputerze systemu Windows Vista Business lub wyższej wersji z zainstalowanym najnowszym pakietem serwisowym. Potem wykonaj następujące czynności:
 - Skopiuj wszystkie neutralne językowo pliki ADMX z folderu %SystemRoot%\PolicyDefinitions na tym komputerze do magazynu centralnego na kontrolerze domeny (%SystemRoot%\Domain\Policies\PolicyDefinitions).

- Skopiuj specyficzne dla języka pliki ADMX z folderów %SystemRoot%\PolicyDefinitions\LanguageCulture do odpowiednio nazwanych folderów w centralnym magazynie na kontrolerze domeny. Na przykład w celu skopiowania plików ADMX dla wersji US English należy skopiować pliki z folderu %SystemRoot%\PolicyDefinitions\EN-US na komputerze administratora do folderu %SystemRoot%\Domain\Policies\PolicyDefinitions\EN-US na kontrolerze domeny.
- 4. W następnym kroku należy przenieść do magazynu centralnego pliki ADMX rozpowszechniane z systemem Windows Server 2008. W tym celu zaloguj się na komputerze należącym do domeny, pracującym pod kontrolą systemu Windows Server 2008 z zainstalowanym najnowszym pakietem serwisowym i powtórz czynności opisane dla systemu Windows Vista w punkcie poprzednim.
- 5. Skopiowane pliki zostaną następnie powielone na innych kontrolerach domeny w ramach zwykłej replikacji katalogu Sysvol. W dużej sieci proces ten może trwać nawet kilka godzin. W razie potrzeby należy proces ten powtórzyć w innych domenach, aby także w nich utworzyć magazyny centralne.

Tworzenie i łączenie GPO

Tworzenie obiektu Zasad grupy i łączenie go z konkretnym kontenerem w strukturze Active Directory to dwa oddzielne zadania. Można utworzyć GPO bez łączenia z jakimkolwiek kontenerem (domeną, lokacją lub OU). Później można w razie potrzeby połączyć ten obiekt z konkretną domeną, lokacją lub OU. Można również utworzyć GPO, automatycznie łącząc go z wybranym kontenerem Active Directory. Wybrana technika zależy głównie od przyzwyczajień oraz tego, jak dany GPO ma być wykorzystany. Należy pamiętać, że po utworzeniu i połączeniu GPO z kontenerem lokacji, domeny lub OU ustawienia zawarte w tym obiekcie zasad zostaną zastosowane do obiektów kont i komputerów znajdujących się w danym kontenerze, zgodnie z opcjami sterującymi dziedziczeniem Active Directory, ustawieniami pierwszeństwa i innymi ustawieniami.

W celu utworzenia i następnie połączenia GPO z lokacją, domeną lub OU wykonaj następującą procedurę:

1. W GPMC rozwiń wpis odpowiadający wybranemu lasowi, po czym rozwiń odpowiedni węzeł Domains, kolejno klikając podwójnie odpowiednie węzły.
2. Kliknij prawym klawiszem myszy Group Policy Objects (Obiekty zasad grupy), po czym wybierz polecenie New (Nowy). W oknie dialogowym New GPO wpisz opisową nazwę tworzonego obiektu zasad, na przykład **Secure Workstation GPO**. Aby użyć startowego GPO jako źródła wstępnych ustawień, wybierz odpowiedni obiekt z listy rozwijanej Source Starter GPO (Źródłowy startowy obiekt zasad). Po kliknięciu OK nowy GPO zostanie dodany do kontenera Group Policy Objects (Obiekty zasad grupy).
3. Kliknij prawym klawiszem myszy nowy GPO i wybierz Edit (Edytuj). W edytorze zasad skonfiguruj odpowiednie ustawienia, po czym zamknij edytor.
4. W konsoli GPMC zaznacz lokację, domenę lub OU. W prawym panelu konsoli na zakładce Linked Group Policy Objects (Połączone obiekty zasad grupy) ukazują listę GPO połączonych aktualnie z wybranym kontenerem (o ile istnieją).
5. Kliknij prawym klawiszem myszy lokację, domenę lub OU, z którą ma być połączony nowy GPO, po czym wybierz polecenie Link An Existing GPO (Połącz istniejący obiekt zasad). Wybierz odpowiedni GPO w oknie dialogowym Select GPO, po czym kliknij OK. Po odświeżeniu zasad grupy dla komputerów i użytkowników zawartych w wybranym kontenerze ustawienia zasad zawarte w tym GPO zostaną zastosowane.

Możliwe jest również utworzenie i połączenie GPO w pojedynczej operacji:

1. W konsoli GPMC kliknij prawym klawiszem myszy domenę lub OU, dla której ma być utworzony nowy GPO, po czym wybierz **Create A GPO In This Domain, And Link It Here** (Utwórz obiekt GPO w tej domenie i utwórz tu łącze).
2. Kliknij prawym klawiszem myszy **Group Policy Objects** (Obiekty zasad grupy), po czym wybierz polecenie **New (Nowy)**. W oknie dialogowym **New GPO** wpisz opisową nazwę tworzonego obiektu zasad, na przykład **Secure Workstation GPO**. Aby użyć startowego GPO jako źródła wstępnych ustawień, wybierz odpowiedni obiekt z listy rozwijanej **Source Starter GPO** (Źródłowy startowy obiekt zasad). Po kliknięciu **OK** nowy GPO zostanie dodany do kontenera **Group Policy Objects** (Obiekty zasad grupy) i połączony z uprzednio wybraną domeną lub jednostką organizacyjną.
3. Kliknij prawym klawiszem myszy nowy GPO i wybierz **Edit**. W edytorze zasad skonfiguruj odpowiednie ustawienia, po czym zamknij edytor. Po odświeżeniu zasad grupy dla komputerów i użytkowników zawartych w wybranym kontenerze ustawienia zasad zawarte w tym GPO zostaną zastosowane.

Tworzenie i korzystanie ze startowych GPO

Podczas tworzenia nowego GPO w konsoli GPMC pojawia się opcja oparcia tego obiektu na startowym obiekcie GPO. Ponieważ ustawienia zawarte w startowym GPO są wówczas importowane do tworzonego obiektu, pozwala to na zdefiniowanie bazowych ustawień konfiguracyjnych dla każdego nowego GPO. W dużej organizacji przydatnych może być kilka różnych kategorii startowych GPO, opartych na rodzajach użytkowników lub komputerów, dla których będą przeznaczone, lub na różnych wymaganiach konfiguracji zabezpieczeń.

W celu utworzenia startowego GPO wykonaj następującą procedurę:

1. W konsoli GPMC rozwiń wpis lasu, po czym kliknij podwójnie odpowiadający mu węzeł **Domains**.
2. Prawym klawiszem myszy kliknij **Starter GPO**, po czym wybierz **New**. W oknie dialogowym **New Starter GPO** wpisz opisową nazwę tworzonego obiektu, na przykład **General Management User GPO**. W razie potrzeby można także dodać komentarz opisujący przeznaczenie tego obiektu. Kliknij **OK**.
3. Prawym klawiszem myszy kliknij nowy GPO i wybierz **Edit**. Skonfiguruj odpowiednie ustawienia zasad, po czym zamknij edytor zasad.

Delegowanie uprawnień do zarządzania zasadami grupy

W środowisku Active Directory wszyscy administratorzy dysponują pewnym poziomem uprawnień do wykonywania zadań związanych z zarządzaniem zasadami grupy. Dzięki delegowaniu także inne osoby mogą otrzymać przywileje wykonywania wybranych lub wszystkich spośród poniższych zadań:

- tworzenie obiektów GPO i zarządzanie utworzonymi przez siebie obiektami,
- wyświetlanie i modyfikowanie ustawień, usuwanie obiektów zasad i zmienianie ustawień zabezpieczeń,
- zarządzanie łączami do istniejących GPOs lub generowanie raportów wynikowego zestawu zasad (Resultant Set of Policy – RSoP).

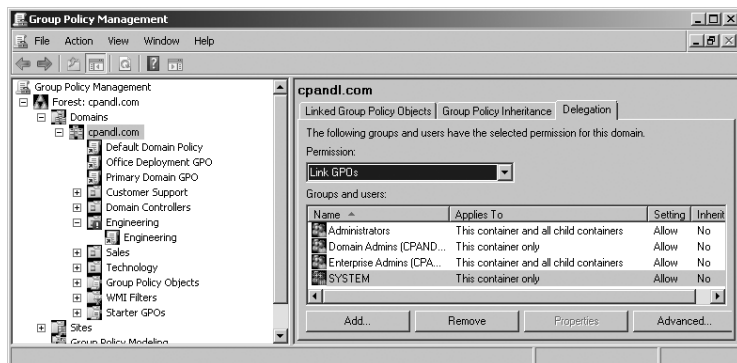
Domyślnie administratorzy mogą tworzyć GPO, zaś każdy twórca obiektu ma uprawnienia do zarządzania tym GPO. Przy użyciu konsoli GPMC można określić, kto w domenie może tworzyć nowe obiekty GPO, wybierając węzeł Group Policy Objects i następnie klikając zakładkę Delegation. Zawiera ona listę grup i użytkowników, którzy mają uprawnienia do tworzenia obiektów zasad w tej domenie. W celu przyznania użytkownikowi lub grupie prawa do tworzenia GPO należy kliknąć Add (Dodaj), po czym wskazać odpowiednie konto użytkownika lub grupy w oknie dialogowym Select User, Computer, Or Group (Wybieranie: użytkownik, komputer lub grupa) i kliknąć OK.

Konsola GPMC zapewnia kilka sposobów ustalenia, kto ma prawa dostępu do zarządzania zasadami grupy. W przypadku uprawnień dotyczących domeny, lokacji lub OU należy wybrać odpowiedni kontener, po czym kliknąć zakładkę Delegation w prawym panelu, pokazaną na rysunku 5-4. Następnie należy wybrać uprawnienie, które ma być sprawdzane, z listy Permission (Uprawnienia). Dostępne są następujące opcje:

Link GPOs (Połącz obiekty zasad grupy) Wyświetla użytkowników i grupy, którzy mogą tworzyć i zarządzać połączeniami pomiędzy analizowanym kontenerem a obiektami zasad grupy.

Perform Group Policy Modeling Analyses (Przeprowadź analizę modelowania zasad grupy) Wyświetla użytkowników i grupy, które dysponują uprawnieniami do tworzenia raportów RSoP w celu planowania (modelowania zasad).

Read Group Policy Results Data (Odczytaj dane wyników zasad grupy) Wyświetla użytkowników i grupy, którzy mogą określić rzeczywiste wyniki RSoP dla faktycznie zastosowanych zasad.



Rysunek 5-4 Przeglądanie uprawnień do zarządzania zasadami grupy.

W celu przyznania uprawnień w domenie, lokacji lub OU wykonaj następującą procedurę:

1. Wybierz domenę, lokację lub OU w konsoli GPMC, po czym kliknij zakładkę Delegation w prawym panelu.
2. Wybierz pożądane uprawnienie z listy Permission.
3. Kliknij Add, po czym wskaż odpowiedniego użytkownika lub grupę w oknie dialogowym Select User, Computer, Or Group i następnie kliknij OK.
4. W oknie dialogowym Add Group Or User (Dodawanie użytkownika lub grupy) określ, jak uprawnienie ma być stosowane. W celu zastosowania uprawnienia do bieżącego

kontenera i wszystkich kontenerów w nim zawartych należy wybrać opcję This Container And All Child Containers (Ten kontener i wszystkie kontenery podrzędne). Aby zastosować uprawnienia tylko do bieżącego kontenera należy wybrać opcję This Container Only (Tylko ten kontener). Kliknij OK.

Aby określić uprawnienia dla indywidualnego GPO, należy zaznaczyć ten obiekt w konsoli GPMC, po czym kliknąć zakładkę Delegation w prawym panelu. Pokazuje ona uprawnienia przypisane użytkownikom lub grupom. Dostępne są następujące możliwości:

Read (Odczyt) Oznacza, że użytkownik (grupa) ma prawo do przeglądania właściwości GPO i jego ustawień.

Edit Settings (Edytuj ustawienia) Oznacza, że użytkownik (grupa) może przeglądać i modyfikować ustawienia zawarte w GPO. Uprawnienie to jednak nie pozwala na usuwanie obiektu ani modyfikowanie jego właściwości zabezpieczeń.

Edit Settings, Delete, Modify Security (Edytuj ustawienia, usuń, modyfikuj zabezpieczenia) Uprawnienia Edit Settings uzupełnione o możliwość usunięcia GPO lub zmiany jego ustawień zabezpieczeń.

Aby przyznać uprawnienia do obiektu zasad grupy, wykonaj następującą procedurę:

1. W konsoli GPMC zaznacz domenę, lokalację lub OU zawierającą dany obiekt grupy, następnie zaznacz ten obiekt, po czym kliknij zakładkę Delegation w prawym panelu. Kliknij Add.
2. W celu przyznania uprawnień do tego GPO użytkownikowi lub grupie kliknij Add. W oknie dialogowym Select User, Computer, Or Group wybierz odpowiedniego użytkownika lub grupy, po czym kliknij OK.
3. W oknie dialogowym Add Group Or User wybierz poziom uprawnień i kliknij OK.

Blokowanie, zastępowanie i wyłączenie zasad

Dziedziczenie powoduje, że każdy obiekt komputera lub użytkownika w domenie, lokalacji czy też OU otrzymuje odpowiednie ustawienia zasad grupy. Większość zasad dysponuje trzema opcjami konfiguracyjnymi: Not Configured (Niezdefiniowane), Enabled (Włączone) lub Disabled (Wyłączone). Domyślnym ustawieniem początkowym dla większości zasad jest stan niezdefiniowany. Jeśli zasada zostanie włączona, ustawienie to zostaje wymuszone i zastosowane dla wszystkich użytkowników lub komputerów, które podlegają działaniu tej zasady wprost lub wskutek dziedziczenia. Wyłączenie zasady powoduje, że ustawienie to *nie* jest stosowane dla wszystkich takich użytkowników i komputerów.

Istnieją cztery metody zmiany funkcjonowania mechanizmu dziedziczenia:

- Zmiana kolejności i priorytetu łączy obiektów zasad grupy
- Zastąpienie dziedziczenia (o ile nie występuje wymuszenie dziedziczenia)
- Zablokowanie dziedziczenia (całkowicie przerywa dziedziczenie zasad)
- Wymuszenie dziedziczenia (wyklucza zastępowanie lub blokowanie dziedziczenia)

W przypadku zasad grupy kolejność stosowania zasad (a zatem kolejność dziedziczenia ustawień) biegnie od poziomu lokalacji przez poziom domeny do kolejnych zagnieżdżonych jednostek organizacyjnych. Należy tu pamiętać o następujących regułach:

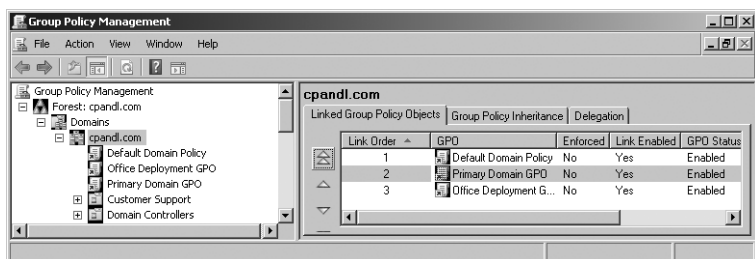
- Jeśli na danym poziomie połączonych jest kilka obiektów zasad, kolejność ich stosowania określana jest przez kolejność połączeń. Najpierw przetwarzane są obiekty o niższym

rankingu, po czym kolejno następują obiekty o coraz wyższym rankingu, potencjalnie zastępując ustawienia wynikające z wcześniej zaaplikowanych obiektów (o ile nie zostało zastosowane wymuszanie lub blokowanie dziedziczenia zasad).

- Jeśli kilka obiektów zasad może zostać odziedziczonych z wyższego poziomu, kolejność ta określa dokładnie, jak będą one przetwarzane. Podobnie jak w przypadku kolejności łącz, obiekty o niższym rankingu (bardziej odległe) przetwarzane są wcześniej. Ostateczne ustawienia są determinowane przez ostatni przetwarzany obiekt zasad, o ile nie zostanie zastosowane blokowanie lub wymuszanie dziedziczenia.

W celu zmiany kolejności łączy obiektów zasad (a tym samym ich priorytetów) wykonaj następującą procedurę:

1. Zaznacz odpowiedni kontener lokacji, domeny lub OU w konsoli GPMC.
2. W prawym panelu konsoli zakładka Linked Group Policy Objects (Połączone obiekty zasad grupy) powinna być wybrana domyślnie (rysunek 5-5). Zaznacz obiekt zasad, którego pozycję na liście chcesz zmienić, klikając go.



Rysunek 5-5 Zmianianie kolejności przetwarzania obiektów zasad.

3. Kliknij odpowiednio przycisk Move Link Up (Przenieś łącze w górę) lub Move Link Down (Przenieś łącze w dół), aby zmienić pozycję wybranego obiektu zasad na liście.
4. Po zakończeniu modyfikowania kolejności łączy upewnij się, że obiekty będą przetwarzane w zaplanowanej kolejności, sprawdzając ich porządek na zakładce Group Policy Inheritance.

Zastępowanie odziedziczonych ustawień jest podstawową techniką zmieniania sposobu działania dziedziczenia. Jeśli jakaś zasada jest włączona w obiekcie przypisanym na wyższym poziomie, można zastąpić jej ustawienia wyłączając ją w obiekcie połączonym na niższym poziomie i odwrotnie – wyłączone ustawienie można ponownie włączyć w później przetwarzanym obiekcie zasad. Tak długo, jak długo nie są wykorzystywane opcje blokowania lub wymuszania dziedziczenia, technika ta pozwala osiągnąć zamierzony efekt.

W niektórych sytuacjach pożądane jest zablokowanie dziedziczenia, aby ustawienia pochodzące z obiektów połączonych z kontenerami wyższego poziomu nie były stosowane wobec użytkowników i komputerów w pewnym szczególnym kontenerze. Po zablokowaniu dziedziczenia stosowane są tylko ustawienia skonfigurowane dla tego kontenera, a żadne ustawienia pochodzące z wyższych poziomów nie są dziedziczone (o ile nie zostanie użyte wymuszenie zasad).

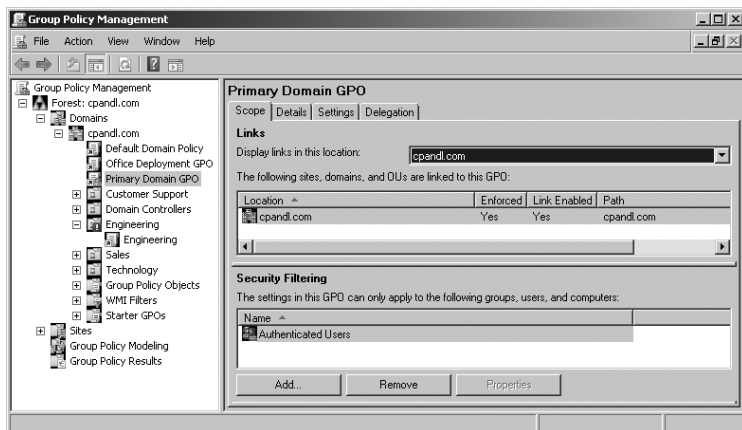
Administratorzy domen mogą użyć blokowania dziedziczenia, aby zablokować ustawienia dziedziczone z poziomu lokacji. Analogicznie administratorzy jednostek organizacyjnych mogą wykorzystać ten sam mechanizm, aby zablokować ustawienia dziedziczone z poziomu lokacji i domeny. Blokowanie zapewnia zatem autonomię domeny lub OU,

zapewniając ich administratorom pełną kontrolę nad zasadami, które są stosowane wobec komputerów i użytkowników znajdujących się w ich kompetencji.

Przy użyciu GPMC można zablokować dziedziczenie zasad klikając prawym klawiszem myszy domenę lub jednostkę organizacyjną, która nie powinna otrzymywać ustawień z kontenerów wyższego poziomu i wybierając polecenie Block Inheritance (Zablokuj dziedziczenie). Jeśli opcja ta jest już włączona, wybranie tego polecenia wyłącza ją. Po zablokowaniu dziedziczenia ikona węzła kontenera w lewym panelu konsoli GPMC zostaje wyróżniona symbolem wykrzyknika w niebieskim kółku.

Możliwe jest również powstrzymanie administratorów zarządzających danym kontenerem przed zastępowaniem lub blokowaniem dziedziczonych ustawień. Mechanizm ten nosi nazwę wymuszenia dziedziczenia. W takim wypadku wszystkie ustawienia z obiektu zasad połączonego na wyższym poziomie hierarchii są dziedziczone bez względu na ustawienia zasad zdefiniowane na poziomie tego kontenera. Innymi słowy, wymuszanie dziedziczenia pozwala wykluczyć zastępowanie lub blokowanie ustawień zasad. Typowym zastosowaniem tego mechanizmu może być narzucenie ogólnych wymagań zabezpieczeń na poziomie lokalacji lub domeny. Co warto podkreślić, wymuszanie dziedziczenia definiowane jest dla poszczególnych obiektów zasad, a nie dla całego kontenera.

W celu włączenia wymuszania dziedziczenia zasad należy w konsoli GPMC rozwinąć kontener zawierający odpowiedni obiekt zasad, kliknąć ten obiekt prawym klawiszem myszy, po czym wybrać polecenie Enforced (Wymuszone). Na przykład w celu zagwarantowania, że obiekt GPO na poziomie domeny będzie dziedziczony przez wszystkie jednostki organizacyjne w tej domenie należy rozwinąć kontener domeny, prawym klawiszem myszy kliknąć odpowiedni GPO i wybrać polecenie Enforced. Jeśli opcja ta jest już włączona, wybranie jej ponownie spowoduje jej wyłączenie. W konsoli GPMC można łatwo ustalić, które zasady są dziedziczone i których dziedziczenie jest wymuszone. W tym celu należy zaznaczyć obiekt zasad i wyświetlić odpowiadającą mu zakładkę Scope (Zakres) w prawym panelu. W przypadku zasady wymuszanej kolumna Enforced (Wymuszone) na liście poniżej tytułu Links (Łącza) będzie zawierała wpis Yes (Tak), jak na rysunku 5-6.



Rysunek 5-6 Wymuszanie dziedziczenia zasad gwarantuje, że ustawienia zostaną zaaplikowane we wszystkich podrzędnych kontenerach Active Directory.

Po zaznaczeniu obiektu zasad można kliknąć prawym klawiszem myszy lokalizację na zakładce Scope, aby wyświetlić menu skrótowe pozwalające zarządzać połączeniami obiektu i wymuszaniem dziedziczenia.

Konserwacja i rozwiązywanie problemów z zasadami grupy

Zasady grupy stanowią rozległy obszar zadań administracyjnych, które wymagają starannego zarządzania. Podobnie jak dla każdego innego zagadnienia administracyjnego, konieczna jest również odpowiednia obsługa oraz eliminowanie występujących problemów. Rozwiązywanie problemów dotyczących zasad grupy wymaga dobrego rozumienia mechanizmów odświeżania i przetwarzania zasad.

Odświeżanie zasad grupy

Po dokonaniu zmian w zasadach grupy zostają one natychmiast uaktywnione. Nie następuje jednak ich automatyczna propagacja. Komputery klienckie żądają danych zasad w następujących okolicznościach:

- Podczas uruchamiania komputera.
- Podczas logowania użytkownika.
- Gdy aplikacja lub użytkownik zażąda odświeżenia zasad.
- Po upływie interwału odświeżania zasad grupy.

Ustawienia zawarte w gałęzi Computer Configuration są stosowane podczas uruchamiania systemu operacyjnego. Ustawienia z gałęzi User Configuration są aplikowane podczas logowania użytkownika. Ponieważ ustawienia użytkownika są stosowane później niż ustawienia komputera, mają one domyślnie wyższy priorytet niż ustawienia komputera. Oznacza to, że w razie wystąpienia sprzecznych ustawień zastosowane zostaną ustawienia zawarte w konfiguracji użytkownika.

Po zastosowaniu ustawień zasad są one automatycznie odświeżane w celu zagwarantowania aktualności. Domyślny interwał odświeżania dla kontrolerów domeny wynosi 5 minut. Dla wszystkich innych komputerów domyślny interwał to 90 minut z losowym odchyleniem do 30 minut – pozwala to uniknąć przeciążenia kontrolerów domeny zbyt licznymi jednoczesnymi żądaniami klienckimi. Oznacza to, że wynikowe okno odświeżania dla komputerów, które nie są kontrolerami domeny, wynosi od 90 do 120 minut.

Podczas odświeżania zasad grupy komputer kliencki łączy się z dostępnym kontrolerem domeny we własnej lokacji. Jeśli więcej niż jeden obiekt zasad zdefiniowany w domenie uległ zmianie, kontroler domeny udostępni listę wszystkich obiektów zasad stosujących się do danego komputera i aktualnie zalogowanego użytkownika. Kontroler domeny wykonuje to bez względu na to, czy numery wersji wszystkich zwracanych obiektów zasad się zmieniły, czy nie. Domyślnie komputer przetwarza obiekty zasad jedynie wtedy, gdy przynajmniej jeden numer wersji uległ zmianie. Jeśli jednak zmieniona zostanie choć jedna zasada, przetwarzane są wszystkie obiekty zasad ze względu na zależności związane z dziedziczeniem i wzajemnymi uwarunkowaniami między zasadami.

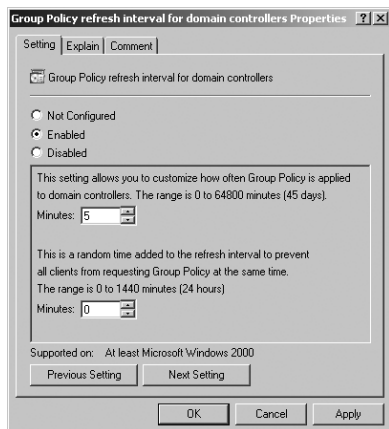
Istnieje jeden znaczący wyjątek od powyższych reguł – ustawienia zabezpieczeń. Są one odświeżane co 16 godzin (960 minut) bez względu na to, czy obiekty zasad uległy zmianie, czy nie. Do powyższego interwału dodawane jest losowe przesunięcie do 30 minut w celu uniknięcia przeciążenia kontrolerów domeny (co daje efektywne okno odświeżania od 960

do 990 minut). Ponadto jeśli komputer kliencki stwierdzi, że łączy do kontrolera domeny jest powolne, informuje o tym kontroler domeny i przesyłane są tylko ustawienia zabezpieczeń oraz szablony administracyjne. Oznacza to, że domyślnie przy powolnych łączach na komputerach klienckich stosowane są jedynie ustawienia zabezpieczeń i szablony administracyjne. Sposób działania wykrywania powolnych łączy można skonfigurować za pomocą zasad.

Należy starannie dobrać częstotliwość odświeżania do faktycznej częstości zmian zasad. Jeśli zmiany w zasadach następują rzadko, wygodne może być wydłużenie interwału odświeżania w celu zredukowania zużycia zasobów. Można na przykład zmienić interwał odświeżania do 20 minut na kontrolerach domeny i do 180 minut na pozostałych komputerach.

Interwał odświeżania zasad grupy można zdefiniować dla poszczególnych obiektów zasad. Aby zmienić interwał odświeżania dla kontrolerów domeny, wykonaj następującą procedurę:

1. Kliknij prawym klawiszem myszy obiekt zasad grupy, który ma być modyfikowany, po czym wybierz Edit. Ten GPO powinien być połączony z kontenerem zawierającym obiekty komputerów kontrolerów domeny.
2. Kliknij podwójnie zasadę Group Policy Refresh Interval For Domain Controllers (Interwał odświeżania zasad grupy dla kontrolerów domeny) w folderze Computer Configuration\Administrative Templates\System\Group Policy (Konfiguracja komputera\Szablony administracyjne\System\Zasady grupy). Pojawi się okno dialogowe właściwości zasady pokazane na rysunku 5-7.
3. Zdefiniuj zasadę, wybierając opcję Enabled i ustawiając podstawową wartość interwału odświeżania w pierwszym polu Minutes (Minuty). Dla kontrolerów domeny zalecane są wartości pomiędzy 5 a 59 minutami.
4. W drugim polu Minutes określ minimalny i maksymalny czas odchylenia dla interwału odświeżania. Kliknij OK.



Rysunek 5-7 Konfigurowanie interwału odświeżania zasad grupy.

Uwaga Większa częstotliwość odświeżania zwiększa szanse na to, by komputer miał najświeższą konfigurację zasad. Niższa częstotliwość zmniejsza obciążenie sieci i kontrolerów domeny, ale zarazem sprawia, że komputery mogą nie mieć najnowszych ustawień zasad.

Konfigurowanie interwału odświeżania dla innych komputerów

Aby określić interwał odświeżania zasad dla serwerów członkowskich i stacji roboczych, wykonaj następującą procedurę:

1. Kliknij prawym klawiszem myszy obiekt zasad grupy, który ma być modyfikowany, po czym wybierz Edit. Ten GPO powinien być połączony z kontenerem zawierającym obiekty komputerów.
2. Kliknij podwójnie zasadę Group Policy Refresh Interval For Computers (Interwał odświeżania zasad grupy dla komputerów) w folderze Computer Configuration\Administrative Templates\System\Group Policy (Konfiguracja komputera\Szablony administracyjne\System\Zasady grupy). Pojawi się okno dialogowe właściwości zasady podobne do pokazanego wcześniej na rysunku 5-7.
3. Zdefiniuj zasadę, wybierając opcję Enabled i ustawiając podstawową wartość interwału odświeżania w pierwszym polu Minutes (Minuty). Najczęściej stosowane wartości mieszczą się w przedziale od 60 do 240 minut.
4. W drugim polu Minutes określ minimalny i maksymalny czas odchylenia dla interwału odświeżania. Odchylenie to pozwala zredukować przeciążenie sieci i kontrolerów domeny i uniknąć sytuacji, w której wielu klientów równocześnie żądałoby odświeżenia zasad. Kliknij OK.

W praktyce

Zazwyczaj należy dążyć do tego, aby aktualizacja zasad nie odbywała się zbyt często, ale jednak wystarczająco często, aby spełnić wymagania firmowe. Zbyt częste odświeżanie zasad generuje nadmierny i niepotrzebny ruch w sieci. Oznacza to, że w wielkich instalacjach należy stosować dłuższe okresy odświeżania. W przypadku stabilnych, rzadko modyfikowanych konfiguracji zasad można rozważyć wykonywanie odświeżania raz dziennie lub nawet raz w tygodniu.

Administrator musi niekiedy wykonać ręczne odświeżenie zasad. Sytuacja taka może wystąpić, gdy nie chce się czekać na automatyczne odświeżenie albo podczas rozwiązywania problemów z konfiguracją zasad. Ręczne odświeżenie zasad umożliwia narzędzie wiersza polecenia Gpupdate.

Odświeżanie zasad można zainicjować kilkoma sposobami. Wpisanie **gpupdate** w wierszu polecenia odświeża zarówno ustawienia komputera, jak i użytkownika na komputerze lokalnym. Polecenie to powoduje przetworzenie i zastosowanie tylko tych ustawień, które uległy zmianie od poprzedniego odświeżenia. W celu wymuszenia odświeżenia wszystkich ustawień zasad można użyć parametru */Force*.

Możliwe jest również oddzielne odświeżanie ustawień konfiguracji komputera i użytkownika. W celu odświeżenia tylko ustawień komputera należy posłużyć się poleceniem **gpupdate /target:computer**. Analogicznie polecenie **gpupdate /target:user** spowoduje odświeżenie tylko ustawień użytkownika.

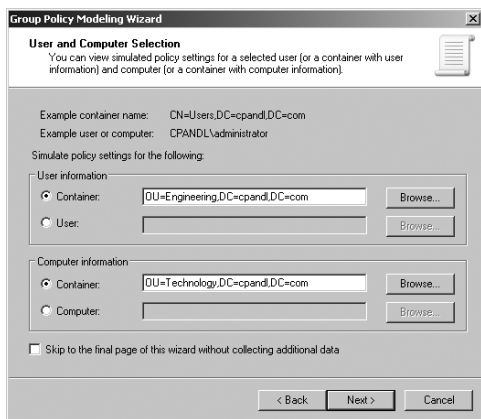
Narzędzie Gpupdate umożliwia również wymuszenie wylogowania użytkownika lub ponowne uruchomienie komputera po odświeżeniu zasad. Opcja ta jest przydatna, gdyż niektóre zasady mogą być aplikowane tylko podczas logowania użytkownika lub uruchamiania komputera. Wylogowanie użytkownika po odświeżeniu zasad powoduje parametr */Logoff*. Ponowne uruchomienie komputera wywoła parametr */Boot*.

Modelowanie zasad grupy do celów planowania

Modelowanie zasad grupy jest funkcją umożliwiającą przetestowanie najrozmaitszych wariantów implementacyjnych i konfiguracyjnych. Można na przykład wymodelować efekt przetwarzania pętli zwrotnej lub wykrywania powolnego łącza. Można także sprawdzić efekt przeniesienia użytkowników lub komputerów do innego kontenera Active Directory albo skutki zmiany członkostwa w grupach zabezpieczeń.

Każdy administrator domeny lub przedsiębiorstwa ma uprawnienia do modelowania zasad grupy, podobnie jak osoby, które otrzymały delegowane uprawnienie Perform Group Policy Modeling Analyses (Przeprowadź analizę modelowania zasad grupy). Modelowanie zasad wymaga wykonania następującej procedury:

1. Prawym klawiszem myszy kliknij węzeł Group Policy Modeling (Modelowanie zasad grupy) w konsoli GPMC, wybierz polecenie Group Policy Modeling Wizard, po czym kliknij Next.
2. Na stronie Domain Controller Selection (Wybieranie kontrolera domeny) wybierz domenę, w której ma być wykonane modelowanie, z listy Show Domain Controllers In This Domain (Pokaż kontrolery domeny z tej domeny). Domyślnie wykonywana będzie symulacja zasad na dowolnym dostępnym kontrolerze domeny. Można również użyć wybranego kontrolera domeny, zaznaczając opcję This Domain Controller (Ten kontroler domeny) i następnie klikając odpowiedni kontroler. Kliknij Next.
3. Strona User And Computer Selection (Wybieranie użytkownika i komputera), pokazana na rysunku 5-8, pozwala na wykonanie symulacji w oparciu o kontener Active Directory lub konkretne konto użytkownika czy komputera.

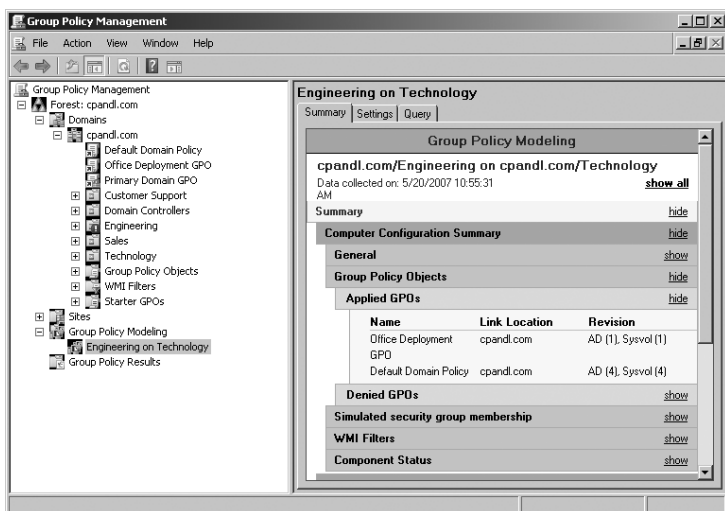


Rysunek 5-8 Wybieranie kontenerów lub kont do celów symulacji.

Użyj jednej z poniższych technik wybierania kont, po czym kliknij Next:

- Wybór kontenera pozwala zasymulować zmiany dokonywane w konfiguracji całych jednostek organizacyjnych. Poniżej tytułu User Information (Informacje o użytkowniku) zaznacz Container (Kontener), po czym kliknij Browse (Przeglądaj), aby wyświetlić okno dialogowe Choose User Container (Wybieranie kontenera użytkowników), w którym możliwe jest wybranie dowolnego kontenera użytkowników w bieżącej domenie. Analogiczną metodą można wybrać kontener komputerów.

- Wybór konkretnych kont pozwala zasymulować skutki zmian wobec konfiguracji wybranego użytkownika i komputera. W tym celu należy poniżej tytułu Under User Information zaznaczyć opcję User, po czym kliknąć Browse, by wyświetlić okno dialogowe Select User (Wybieranie użytkownika). Analogiczna metoda pozwala wskazać konkretny komputer.
- 4. Strona Advanced Simulation Options (Zaawansowane opcje symulacji) pozwala określić dodatkowe opcje, takie jak Slow Network Connections (Powolne łącza sieciowe), Loopback Processing (Przetwarzanie pętli zwrotnej) oraz Site (Lokacja). Po dokonaniu wyborów kliknij Next.
- 5. Strona User Security Groups (Grupy zabezpieczeń użytkowników) pozwala zasymulować zmiany członkostwa użytkowników w grupach zabezpieczeń. Zmiany wykonane na tej stronie dotyczą wcześniej wybranego użytkownika lub kontenera użytkowników. Na przykład w celu sprawdzenia, co się stanie, gdy użytkownik ze wskazanego kontenera będzie członkiem pewnej grupy zabezpieczeń, należy dodać tę grupę do listy Security Groups. Po dokonaniu wyborów kliknij Next.
- 6. Strona Computer Security Groups (Grupy zabezpieczeń komputerów) pozwala zasymulować zmiany członkostwa kont komputerów w grupach zabezpieczeń. Opcje dostępne na tej stronie są analogiczne do opcji dotyczących użytkowników ze strony poprzedniej. Po dokonaniu wyborów kliknij Next.
- 7. Obiekty zasad grupy można powiązać z filtrami WMI. Domyślnie wybierani użytkownicy i komputery powinni spełniać wszystkie wymagania ustawionych filtrów WMI, co w większości wypadków jest ustawieniem pożądanym. Kliknij Next dwukrotnie, aby zaakceptować opcje domyślne.
- 8. Przejrzyj dokonane wybory i kliknij Next. Gdy kreator zgromadzi informacje o zasadach, kliknij Finish. Po zakończeniu generowania raportu stanie się on dostępny w lewym panelu konsoli, zaś w prawym pojawią się wyniki (rysunek 5-9).



Rysunek 5-9 Przeglądanie raportu modelowania zasad.

Kopiowanie, wklejanie i importowanie obiektów zasad

Konsola GPMC dysponuje wbudowanymi mechanizmami kopiowania, wklejania i importowania obiektów. Korzystanie z funkcji kopiowania i wklejania jest proste. Opcje Copy (Kopiuj) oraz Paste (Wklej) dostępne są po kliknięciu obiektu GPO prawym klawiszem myszy. Pozwalają one na skopiowanie obiektu zasad wraz ze wszystkimi ustawieniami z jednej domeny do innej. Źródłowa i docelowa domena mogą być dowolnymi domenami, z którymi można się połączyć i w których użytkownik ma uprawnienia do zarządzania obiektami zasad. W domenie źródłowej wymagane jest co najmniej uprawnienie do odczytu, zaś w docelowej potrzebne jest uprawnienie do zapisu, aby możliwe było zapisanie skopiowanego obiektu. Przywilej ten domyślnie mają administratorzy oraz osoby, które otrzymały delegowane uprawnienie do tworzenia obiektów zasad.

Kopiowanie obiektów zasad pomiędzy domenami działa sprawnie, o ile istnieje połączenie między domenami i dysponuje się wymaganymi uprawnieniami. Jednak administrator w zdalnym biurze (lub osoba z delegowanymi uprawnieniami) może nie mieć dostępu do domeny źródłowej, aby móc skopiować obiekt zasad. W takim przypadku inny administrator może wykonać kopię zapasową obiektu i przesłać ją do lokalizacji zdalnej. Po otrzymaniu takiej przesyłki administrator może zaimportować kopię obiektu do swojej domeny, aby utworzyć nowy obiekt z tymi samymi ustawieniami.

Operację importu może wykonać każdy użytkownik dysponujący uprawnieniem Edit Settings Group Policy (Edytuj ustawienia zasad grupy). Importowanie zastępuje wszystkie ustawienia w obiekcie zasad wybranym jako docelowy. W celu zaimportowania kopii zapasowej obiektu zasad wykonaj następującą procedurę:

1. W konsoli GPMC kliknij prawym klawiszem myszy węzeł Group Policy Objects, po czym wybierz New. W oknie dialogowym New GPO wpisz opisową nazwę nowego obiektu i kliknij OK.
2. Nowy GPO pojawi się na liście w kontenerze Group Policy Objects. Kliknij prawym klawiszem myszy nowy obiekt i wybierz Import Settings (Importuj ustawienia). Uruchomi się kreator Import Settings Wizard (Kreator importu ustawień).
3. Kliknij Next dwukrotnie, aby pominąć stronę Backup GPO (Wykonaj kopię zapasową obiektu zasad grupy). Nie ma potrzeby tworzenia kopii tego obiektu, gdyż jest to nowy obiekt.
4. Na stronie Backup Location (Lokalizacja kopii zapasowej) kliknij Browse (Przejrząj) i zlokalizuj folder zawierający kopię zapasową obiektu, który ma zostać zaimportowany, po czym kliknij OK. Kliknij Next, aby kontynuować.
5. Jeśli wskazany folder zawiera kilka kopii zapasowych, na stronie Source GPO (GPO źródła) pojawi się ich lista. Kliknij ten, którego chcesz użyć, po czym kliknij Next.
6. Kreator Import Settings Wizard przeskanuje obiekt zasad w poszukiwaniu odwołań do podmiotów zabezpieczeń lub ścieżek UNC, które mogłyby wymagać modyfikacji. Jeśli wpisy takie zostaną odkryte, pojawi się możliwość utworzenia tabeli migracji lub użycia już istniejącej tabeli.
7. Przejdź przez pozostałe strony kreatora klikając Next, a na koniec Finish, aby rozpocząć proces importu. Po zakończeniu importowania kliknij OK.

Tworzenie kopii zapasowych i przywracanie obiektów zasad

Jednym z okresowych zadań administracyjnych jest tworzenie kopii zapasowych obiektów zasad. Konsola GPMC umożliwia wykonanie kopii zapasowych poszczególnych obiektów albo wszystkich obiektów w domenie:

1. Rozwiń i następnie zaznacz węzeł Group Policy Objects w konsoli GPMC. Jeśli zamierzasz wykonać kopię wszystkich obiektów zasad w tej domenie, kliknij prawym klawiszem myszy węzeł Group Policy Objects, po czym wybierz polecenie Back Up All (Kopia zapasowa wszystkich). W celu skopiowania tylko wybranego obiektu zasad kliknij go prawym klawiszem myszy i wybierz polecenie Back Up (Kopia zapasowa).
2. W oknie dialogowym Back Up Group Policy Object (Kopia zapasowa obiektu zasad grupy) kliknij Browse i wskaż albo utwórz folder, w którym kopia zapasowa ma zostać utworzona.
3. W polu Description (Opis) wpisz jednoznaczny opis zawartości kopii zapasowej, po czym Backup, aby rozpocząć kopiowanie.
4. Postęp operacji i status wyświetlany jest w oknie dialogowym Backup (Kopia zapasowa). Po zakończeniu tworzenia kopii kliknij OK. Jeśli operacja zakończy się niepowodzeniem, sprawdź uprawnienia do obiektów zasad i folderu, w którym kopie są zapisywane. Wymagane jest uprawnienie Read (Odczyt) wobec obiektu zasad i Write (Zapis) w folderze kopii zapasowych. Domyślnie członkowie grup Domain Admins oraz Enterprise Admins dysponują tymi uprawnieniami.

Przy użyciu GPMC można przywrócić obiekt zasad do stanu, w jakim był w momencie wykonania kopii zapasowej. Konsola GPMC śledzi kopie zapasowe dla każdego obiektu oddzielnie, nawet jeśli wykonano kopię wszystkich obiektów jednocześnie. Ponieważ rejestrowana jest również informacja o wersji, a także sygnatura czasowa i opis, można przywrócić ostatnią wersję każdego obiektu lub konkretną (wcześniejszą) wersję.

W celu przywrócenia obiektu zasad wykonaj następującą procedurę:

1. W konsoli GPMC kliknij prawym klawiszem myszy węzeł Group Policy Objects i wybierz polecenie Manage Backups (Zarządzaj kopiami zapasowymi), aby wyświetlić okno dialogowe Manage Backups.
2. Kliknij Browse w sekcji Backup Location (Lokalizacja kopii zapasowych), aby wskazać folder zawierający kopie zapasowe, po czym kliknij OK.
3. Wszystkie kopie zapasowe obiektów zasad znajdujące się we wskazanym folderze zostaną wyświetlone w sekcji Backup Policy Objects. Aby wyświetlić tylko najnowsze wersje obiektów zasad (zgodnie z sygnaturą czasową), zaznacz pole wyboru Show Only The Latest Version Of Each GPO (Pokaż tylko najnowszą wersję każdego obiektu GPO).
4. Zaznacz GPO, który ma być przywrócony. Przycisk View Settings (Wyświetl ustawienia) pozwala przejrzeć i zweryfikować ustawienia zawarte w danym obiekcie zasad. W celu rozpoczęcia przywracania kliknij Restore (Przywróć) i potwierdź chęć odtworzenia ustawień z kopii zapasowej, klikając OK w wyświetlonym monicie.
5. Okno dialogowe Restore (Przywróć) ukazuje postęp operacji i jej status. Jeśli przywracanie zakończy się niepowodzeniem, należy sprawdzić uprawnienia do obiektu zasad i folderu, w którym znajduje się kopia zapasowa. Przywrócenie GPO wymaga posiadania uprawnienia Edit Settings, Delete, and Modify Security wobec obiektu zasad oraz co najmniej uprawnienia Read w folderze zawierającym kopię. Uprawnienia te domyślnie powinni mieć członkowie grup Domain Admins oraz Enterprise Admins.

Ustalanie bieżących ustawień zasad grupy i stanu odświeżania

Mechanizm modelowania zasad grupy można wykorzystać do zarejestrowania wynikowego zestawu zasad (Resultant Set of Policy – RSoP). Dzięki takiemu wykorzystaniu modelowania można przejrzeć wszystkie obiekty zasad, które zostały zastosowane wobec komputera przy ostatnim przetwarzaniu (odświeżaniu) zasad. Wszyscy administratorzy domen i przedsiębiorstwa mają uprawnienia do rejestrowania wyników zasad. Prawa te mają również osoby, którym delegowano uprawnienie Read Group Policy Results Data. W celu wygenerowania wynikowego zestawu zasad należy w konsoli kliknąć prawym klawiszem myszy węzeł Group Policy Results (Wyniki zasad grupy), po czym wybrać polecenie Group Policy Results Wizard (Kreator wyników zasad grupy). Po uruchomieniu kreatora należy postępować zgodnie z wyświetlanymi wskazówkami.

Wyłączanie nieużywanej części zasad grupy

Inną metodą wyłączenia zasad jest wyłączenie nieużywanej części obiektu zasad. W ten sposób można zablokować część ustawień konfiguracji komputera, użytkownika lub obydwu – zasady w wyłączonych częściach nie będą stosowane. Dodatkowo wyłączenie nieużywanej części zasad przyspiesza aplikację GPO.

W celu włączenia lub wyłączenia części zasad wykonaj następującą procedurę:

1. W konsoli GPMC zaznacz odpowiedni kontener (lokacji, domeny lub jednostki organizacyjnej), zawierający obiekt zasad, który chcesz zmodyfikować.
2. Zaznacz wybrany obiekt zasad i kliknij zakładkę Details (Szczegóły) w prawym panelu konsoli.
3. Wybierz jedno z poniższych ustawień na liście GPO Status (Stan obiekt GPO), po czym kliknij OK w monicie potwierdzenia zmiany stanu:

All Settings Disabled (Wszystkie ustawienia wyłączone) Blokuje przetwarzanie obiektu zasad i jego wszystkich ustawień.

Computer Configuration Settings Disabled (Ustawienia konfiguracji komputera wyłączone) Wyłącza przetwarzanie ustawień zawartych w części Computer Configuration (Konfiguracja komputera). Oznacza to, że przetwarzane będą tylko ustawienia konfiguracji użytkownika.

Enabled (Włączone) Zezwala na przetwarzanie wszystkich ustawień zawartych w obiekcie zasad.

User Configuration Settings Disabled (Ustawienia konfiguracji użytkownika wyłączone) Wyłącza przetwarzanie ustawień zawartych w części User Configuration (Konfiguracja użytkownika). Oznacza to, że przetwarzane będą tylko ustawienia komputera.

Zmianianie preferencji przetwarzania zasad

Ustawienia zawarte w części Computer Configuration są przetwarzane, gdy komputer zostanie uruchomiony i połączony z siecią. Ustawienia z części User Configuration są przetwarzane, gdy użytkownik zaloguje się w sieci. W razie wystąpienia konfliktu pomiędzy ustawieniami komputera i użytkownika pierwszeństwo mają jednak ustawienia komputera. Należy przy tym pamiętać, że ustawienia komputera pochodzą z obiektu zasad właściwego dla lokalizacji konta komputera w strukturze Active Directory, zaś ustawienia użytkownika – z lokalizacji konta tego użytkownika.

W niektórych sytuacjach zachowanie takie nie jest pożądane. W przypadku komputera współdzielonego chcielibyśmy, aby ustawienia użytkownika pochodziły z obiektu zasad właściwego dla tego komputera, ale chcielibyśmy również pozwolić na zastosowanie ustawień z obiektu specyficznego dla użytkownika. W zabezpieczonym laboratorium lub środowisku ograniczonym pożądane byłoby zastosowanie tylko ustawień pochodzących z GPO komputera, aby zagwarantować zgodność ze ścisłymi regułami zabezpieczeń. Osiągnięcie takiego zachowania umożliwia mechanizm przetwarzania zwrotnego zasad grupy.

Aby zmienić sposób działania przetwarzania zwrotnego zasad grupy, wykonaj następujące czynności:

1. W konsoli GPMC kliknij prawym klawiszem myszy obiekt zasad grupy, który ma być modyfikowany, po czym wybierz Edit.
2. Kliknij podwójnie zasadę User Group Policy Loopback Processing Mode (Tryb przetwarzania sprzężenia zwrotnego zasad grupy użytkownika) w folderze Computer Configuration\Administrative Templates\System\Group Policy (Konfiguracja komputera\Szablony administracyjne\System\Zasady grupy). Pojawi się okno dialogowe Properties dla tej zasady.
3. Zdefiniuj zasadę, wybierając Enabled (Włączone), po czym wybierz jeden z poniższych trybów przetwarzania z listy Mode (tryb) i kliknij OK:

Replace (Zamień) Opcja ta powoduje, że ustawienia użytkownika zdefiniowane w obiektach zasad grupy komputera zastępują ustawienia użytkownika stosowane zwykle względem użytkownika.

Merge (Scal) Opcja powoduje, że ustawienia użytkownika zdefiniowane w obiektach zasad grupy komputera oraz ustawienia użytkownika stosowane zwykle względem użytkownika zostają połączone. Po włączeniu tej opcji najpierw przetwarzane są ustawienia użytkownika zawarte w obiektach GPO komputera, następnie ustawienia z obiektów GPO użytkownika, po czym ustawienia z obiektów komputera są stosowane ponownie. Technika ta pozwala połączyć obydwa zestawy niekonfliktowych ustawień, gwarantując jednocześnie, że w razie konfliktu zostaną użyte ustawienia z GPO komputera.

Konfigurowanie wykrywania powolnych łączy

Mechanizm wykrywania powolnych łączy polega na rejestrowaniu zwiększonych opóźnień w ruchu sieciowym i jest wykorzystywany przez klientów zasad grupy do podejmowania odpowiednich działań korygujących, aby zmniejszyć ryzyko, że przetwarzanie zasad grupy dodatkowo przeciąży sieć. Po wykryciu powolnego łącza klienci zasad grupy zmniejszają intensywność komunikacji sieciowej, ograniczając liczbę przetwarzanych zasad, a tym samym zmniejszając całkowite obciążenie ruchem sieciowym.

Domyślnie po zauważeniu, że prędkość łącza jest mniejsza niż 500 kilobitów na sekundę, komputer kliencki stwierdza, że połączenie jest powolne i powiadamia o tym kontroler domeny. W rezultacie podczas odświeżania zasad kontroler domeny przesyła do klienta tylko ustawienia zabezpieczeń oraz szablony administracyjne zawarte w odpowiednich obiektach zasad.

Wykrywanie powolnych łączy można skonfigurować za pomocą zasady Group Policy Slow Link Detection (Wykrywanie powolnego łącza zasad grupy), zlokalizowanej w folderze Computer Configuration\Administrative Templates\System\Group Policy (Konfiguracja komputera\Szablony administracyjne\System\Zasady grupy). Wyłączenie lub nieskonfigurowanie tej zasady powoduje, że klienci będą używali domyślnej wartości 500 kilobitów na sekundę jako proggu powolnego łącza. Po włączeniu tej zasady można określić inną wartość

progową, na przykład 384 kbps. Możliwe jest również całkowite wyłączenie wykrywania powolnych łączy. W tym celu należy określić wartość Connection Speed (Szybkość połączeń) na 0. Ustawienie takie powoduje, że klienci nie próbują wykrywać powolnych łączy i wszystkie połączenia uznają za szybkie.

Można zoptymalizować wykrywanie powolnych łączy dla różnych obszarów zasad grupy. Domyślnie po wykryciu powolnego łącza nie są przetwarzane następujące klasy zasad:

- Zasady przydziałów dysku
- Zasady przywracania EFS
- Zasady przekierowania folderów
- Zasady konserwacji programu Internet Explorer
- Zasady zabezpieczeń protokołu IP
- Skrypty zasad
- Zasady instalacji oprogramowania
- Zasady sieci bezprzewodowej

Przy korzystaniu z powolnych łączy automatycznie przetwarzane są tylko zasady zabezpieczeń. Domyślnie zasady te są odświeżane są co 16 godzin nawet wtedy, gdy nie zostały zmienione. Jediną metodą powstrzymania wymuszonego odświeżania jest takie skonfigurowanie przetwarzania zasad zabezpieczeń, aby nie były aplikowane podczas okresowych odświeżeń. W tym celu należy włączyć ustawienie zasad Do Not Apply During Periodic Background Processing (Nie stosuj podczas okresowego przetwarzania w tle). Ponieważ jednak zasady zabezpieczeń są tak ważne, ustawienie to oznacza tylko, że przetwarzanie zasad zabezpieczeń zostaje wstrzymane, gdy użytkownik jest zalogowany i używa komputera. Jediną przyczyną, dla której można w ogóle rozważać wyłączenie odświeżania zasad zabezpieczeń, może być awaria aplikacji następująca podczas odświeżania zasad.

W celu skonfigurowania wykrywania powolnych łączy i odpowiadającego mu przetwarzania zasad wykonaj następujące czynności:

1. Prawym klawiszem myszy kliknij obiekt zasad, który chcesz zmienić, po czym wybierz polecenie Edit.
2. Kliknij podwójnie zasadę Group Policy Slow Link Detection (Wykrywanie powolnych łączy zasad grupy) w folderze Computer Configuration\Administrative Templates\System\Group Policy (Konfiguracja komputera\Szablony administracyjne\System\Zasady grupy).
3. Zaznacz Enabled (Włączone), aby zdefiniować zasadę (rysunek 5-10), po czym wpisz prędkość, która ma posłużyć jako próg wykrywania powolnego łącza. Kliknij OK.

W celu skonfigurowania przetwarzania zasad w tle w razie wystąpienia powolnego łącza wykonaj następujące czynności:

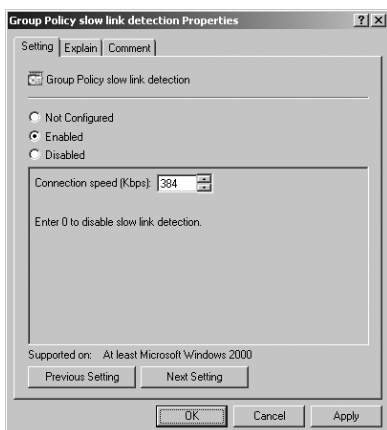
1. Prawym klawiszem myszy kliknij obiekt zasad, który chcesz modyfikować, po czym wybierz Edit.
2. Rozwiń folder Computer Configuration\Administrative Templates\System\Group Policy.
3. Kliknij podwójnie zasadę przetwarzania, którą chcesz skonfigurować. W celu włączenia zasady zaznacz pole Enabled (rysunek 5-11), po czym dokonaj odpowiednich wyborów konfiguracyjnych. Opcje te mogą się nieznacznie różnić dla poszczególnych zasad i mogą zawierać następujące możliwości:

Allow Processing Across A Slow Network Connection (Zezwalaj na przetwarzanie przez powolne połączenie sieciowe) Powoduje przetwarzanie odpowiednich zasad nawet w przypadku wykrycia powolnego łącza.

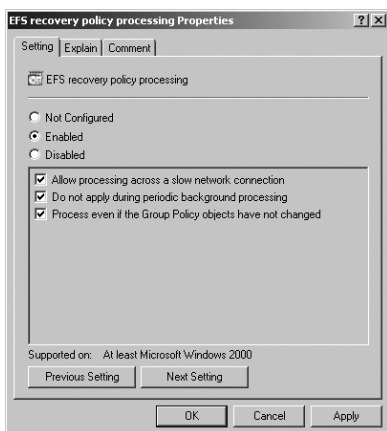
Do Not Apply During Periodic Background Processing (Nie stosuj podczas okresowego przetwarzania w tle) Blokuję odświeżanie zasad, jeśli zmiany ustawień nastąpią po uruchomieniu komputera lub zalogowaniu się użytkownika.

Process Even If The Group Policy Objects Have Not Changed (Przetwarzaj nawet jeżeli obiekty zasad grupy nie zostały zmienione) Wymusza przetworzenie ustawień danej klasy podczas odświeżania, nawet jeśli nie wystąpiły żadne zmiany.

4. Kliknij OK, by zapisać ustawienia.



Rysunek 5-10 Konfigurowanie wykrywania powolnych łącz.



Rysunek 5-11 Konfigurowanie przetwarzania zasad przez powolne łącza.

Usuwanie łączy i obiektów zasad

Istnieją dwie metody zaprzestania korzystania z obiektu GPO:

- Usunięcie łącza do tego obiektu, ale nie samego GPO.
- Trwale usunięcie obiektu GPO i wszystkich jego łączy.

Usunięcie łącza do GPO wstrzymuje korzystanie z zawartych w nim ustawień przez domenę, lokację lub OU, ale obiekt nadal istnieje. Dzięki temu obiekt ten może być nadal połączony z innym kontenerem Active Directory. W konsoli GPMC można usunąć łącze do obiektu GPO klikając prawym klawiszem myszy łącze obiektu w kontenerze, z którym jest połączony i wybierając polecenie Delete (Usuń). Operację trzeba potwierdzić w wyświetlonym monicie. Po usunięciu wszystkich łączy do tego obiektu nadal będzie on istniał w folderze Group Policy Objects, ale jego ustawienia nie będą miały żadnego wpływu na komputery i użytkowników w organizacji.

Trwale usunięcie GPO usuwa ten obiekt i wszystkie jego łącza. Jediną metodą odtworzenia usuniętego GPO jest przywrócenie go z kopii zapasowej (o ile takowa istnieje). W celu usunięcia obiektu zasad i wszystkich jego łączy należy w węzle Group Policy Objects kliknąć obiekt prawym klawiszem myszy i wybrać polecenie Delete, po czym w monicie potwierdzenia, że obiekt i wszystkie jego łącza mają być rzeczywiście usunięte, kliknąć OK.

Rozwiązywanie problemów z zasadami grupy

Jeśli okaże się, że zasady nie są stosowane zgodnie z oczekiwaniem, miejscem, od którego należy rozpocząć poszukiwanie przyczyn takiego stanu rzeczy powinno być sprawdzenie wynikowego zestawu zasad dla użytkownika lub komputera, dla których występuje problem. Pozwala to określić obiekty zasad, których ustawienia są stosowane, wykonując następującą procedurę:

1. W konsoli GPMC kliknij prawym klawiszem myszy węzeł Group Policy Results, po czym wybierz polecenie Group Policy Results Wizard (Kreator wyników zasad grupy). Po uruchomieniu kreatora kliknij Next (Dalej).
2. Strona Computer Selection (Wybór komputera) umożliwia wskazanie komputera, dla którego mają być gromadzone informacje. Opcja This Computer (Ten komputer) spowoduje wyświetlenie informacji o komputerze lokalnym. Aby przejrzeć informacje dla komputera zdalnego, należy wybrać opcję Another Computer (Inny komputer), po czym kliknąć Browse (Przejrząj). W oknie dialogowym Select Computer (Wybieranie: Komputer) wpisz nazwę komputera i kliknij Check Names (Sprawdź nazwy). Po wybraniu właściwego konta komputera kliknij OK.
3. Na stronie User Selection (Wybór użytkownika) wskaż użytkownika, dla którego mają być zgromadzone informacje o zasadach. Można wyświetlić informacje dla dowolnego użytkownika zalogowanego na poprzednio wybranym komputerze. Kliknij Next.
4. Przejrzyj dokonane wybory i kliknij Next. Po zgromadzeniu przez kreator informacji o zasadach kliknij Finish (Zakończ). Po zakończeniu generowania raportu pojawi się on w lewym panelu konsoli, zaś jego treść w prawym panelu.
5. Przejrzyj raport w celu ustalenia zaaplikowanych ustawień. Informacje o zasadach komputera i użytkownika są wymienione oddzielnie w sekcjach zatytułowanych odpowiednio Computer Configuration Summary (Podsumowanie konfiguracji komputera) oraz User Configuration Summary (Podsumowanie konfiguracji użytkownika).

Raport RSoP można także uzyskać przy użyciu narzędzia wiersza polecenia Gpresult. Narzędzie to udostępnia następujące informacje szczegółowe:

- Zastosowanie szczególnych ustawień dla przekierowania folderów, instalacji oprogramowania, przydziałów dysku, IPsec oraz skryptów.
- Czas ostatniego zastosowania (odświeżenia) zasad grupy.
- Nazwę kontrolera domeny, z którego zostały pobrane zastosowane zasady, oraz członkostwo w grupach zabezpieczeń konta komputera i zalogowanego użytkownika.
- Pełną listę obiektów GPO, które zostały zastosowane, a także listę obiektów, które zostały pominięte z powodu użycia filtrów.

Narzędzie Gpresult używa następującej składni:

```
gpresult /s ComputerName /user Domain\UserName
```

gdzie *ComputerName* jest nazwą komputera, dla którego gromadzone są dane o wynikach zasad grupy, zaś *DomainUserName* wskazuje odpowiedniego użytkownika. Na przykład w celu wyświetlenia RSoP dla komputera CorpPC85 i użytkownika tedg należącego do domeny CPANDL należy wpisać następujące polecenie:

```
gpresult /s corp85 /user cpandl\tedg
```

Bardziej szczegółowy wynik narzędzia można uzyskać za pomocą jednej z dwóch opcji rozszerzającej wyniki. Parametr */v* włącza szczegółowe wyświetlanie wyników, przy czym wyświetlane są tylko te zasady, które zostały faktycznie zastosowane. Parametr */z* dodatkowo wyświetla także inne GPO, które zawierały ustawienia zasad, ale które zostały zastąpione lub pominięte z powodu filtrów lub ustawień dziedziczenia. Wynik działania narzędzia Gpresult może być dość długi, zatem warto przekierować go do pliku HTML przy użyciu parametru */H* lub pliku XML przy użyciu parametru */X*. Poniższe przykłady wykorzystują te parametry:

```
gpresult /s corp85 /user cpandl\tedg /h gpreport.html
```

```
gpresult /s corp85 /user cpandl\tedg /x gpreport.xml
```

Naprawianie obiektu Default Group Policy

Obiekty GPO Default Domain Policy oraz Default Domain Controller Policy są krytycznymi elementami zdrowia Active Directory Domain Services. Jeśli te obiekty z jakiegoś powodu zostaną uszkodzone, zasady grupy nie będą funkcjonowały poprawnie. W celu rozwiązania tego problemu należy posłużyć się konsolą GPMC w celu przywrócenia tych obiektów z kopii zapasowej. W skrajnej sytuacji, gdy nie są dostępne żadne kopie zapasowe Default Domain Policy ani Default Domain Controller Policy, można wykorzystać narzędzie DCGPOFIX do odtworzenia ustawień zabezpieczeń w tych obiektach zasad. Stan przywracany przez narzędzie DCGPOFIX zależy od tego, jak zostały zmodyfikowane ustawienia kontrolera domeny przed uruchomieniem tego programu. Do uruchomienia narzędzia DCGPOFIX wymagane jest członkostwo grupy Domain Admins lub Enterprise Admins.

Uruchomienie narzędzia DCGPOFIX powoduje przywrócenie ustawień podstawowych w obiektach zasad Default Domain Policy oraz Default Domain Controller Policy do ich stanu domyślnego, zatem wszystkie zmiany dokonane w tych obiektach zostaną utracone. Niektóre ustawienia rozszerzone są jednak obsługiwane oddzielnie i zostają zachowane. Należą do nich Remote Installation Services (Usługi instalacji zdalnej), Security Settings (Ustawienia zabezpieczeń) oraz Encrypting File System (EFS). Różne od domyślnych

ustawienia zabezpieczeń nie są jednak zachowywane, co może oznaczać również utratę innych zmienionych ustawień zasad. Wszystkie inne ustawienia rozszerzeń zostają przywrócone do wartości domyślnych, zatem wszelkie dokonane zmiany zostaną utracone.

W celu uruchomienia narzędzia DCGPOFIX należy zalogować się na kontrolerze domeny, po czym wpisać **dcgpofix** w oknie wiersza polecenia z podniesionymi uprawnieniami. DCGPOFIX sprawdza numer wersji schematu Active Directory w celu zapewnienia zgodności pomiędzy używaną wersją DCGPOFIX i konfiguracją schematu Active Directory. Jeśli wersje te nie są zgodne, DCGPOFIX zakończy działanie bez naprawiania domyślnych obiektów zasad grupy. Przy użyciu parametru */Ignoreschema* można wymusić działanie narzędzia DCGPOFIX z różnymi wersjami Active Directory. W takim wypadku jednak domyślne obiekty zasad mogą nie zostać przywrócone do ich stanu oryginalnego. Z tego względu należy zawsze posługiwać się wersją narzędzia DCGPOFIX zainstalowaną wraz z aktualnym systemem operacyjnym.

Istnieje także możliwość naprawy tylko GPO Default Domain Policy albo Default Domain Controller Policy. W celu naprawy tylko obiektu zasad Default Domain Policy należy użyć polecenia **dcgpofix/target: domain**. Naprawę tylko obiektu Default Domain Controller Policy umożliwia polecenie **dcgpofix/target: dc**.

Zarządzanie użytkownikami i komputerami przy użyciu zasad grupy

Zasady grupy umożliwiają zarządzanie użytkownikami i komputerami na kilka różnych sposobów. W kolejnych podrozdziałach przyjrzymy się pewnym szczególnym obszarom zarządzania, w tym:

- Przekierowaniem folderów.
- Skryptami komputerów i użytkowników.
- Rozpowszechnianiem oprogramowania.
- Wystawianiem certyfikatów dla komputerów i użytkowników.
- Ustawieniami aktualizacji automatycznych.

Scentralizowane zarządzanie folderami specjalnymi

Mechanizm przekierowania folderów pozwala na scentralizowane zarządzanie folderami używanymi przez system Windows Server 2008. Polega to na przeniesieniu tych folderów do jednej lokalizacji w sieci zamiast korzystania z licznych domyślnych lokalizacji na poszczególnych komputerach. W przypadku Windows XP Professional i wcześniejszych wersji Windows tymi folderami specjalnymi są Application Data (Dane aplikacji), Start Menu, Desktop (Pulpit), My Documents (Moje dokumenty) oraz My Pictures (Moje obrazy). W systemie Windows Vista i późniejszych wersjach Windows zarządzać można następującymi folderami: AppData(Roaming), Desktop (Pulpit), Start Menu, Documents (Dokumenty), Pictures (Obrazy), Music (Muzyka), Videos (Wideo), Favorites (Ulubione), Contacts (Kontakty), Downloads (Pobieranie), Links (Łącza), Searches (Wyszukiwania) i Saved Games (Zapisane gry).

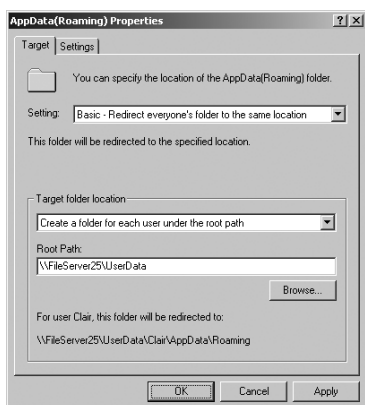
Dostępne są dwie ogólne opcje przekierowania folderów. Można przenieść folder specjalny do tej samej lokalizacji sieciowej dla wszystkich użytkowników albo określić lokalizację na podstawie członkostwa użytkowników w grupach zabezpieczeń. W każdym wypadku należy zadbać o to, aby wybrana lokalizacja sieciowa była dostępna jako udział sieciowy.

Więcej informacji na temat udostępniania lokalizacji sieciowych zawiera rozdział 15 „Udostępnianie danych, zabezpieczenia i inspekcja”.

Przekierowywanie folderu specjalnego do pojedynczej lokalizacji

W celu przeniesienia folderów specjalnych do pojedynczej lokalizacji w sieci wykonaj następującą procedurę:

1. W konsoli GPMC kliknij prawym klawiszem myszy obiekt GPO dla lokacji, domeny lub jednostki organizacyjnej, po czym wybierz Edit. Spowoduje to otwarcie tego obiektu w edytorze zasad.
2. Rozwiń następujące węzły w edytorze zasad: User Configuration (Konfiguracja użytkownika), Windows Settings (Ustawienia systemu Windows) oraz Folder Redirection (Przekierowanie folderów).
3. Prawym klawiszem myszy kliknij folder specjalny, który chcesz zmodyfikować, na przykład AppData(Roaming), po czym wybierz Properties (Właściwości) z menu skrótowego. Pojawi się okno dialogowe podobne do przedstawionego na rysunku 5-12.



Rysunek 5-12 Określanie opcji przekierowania przy użyciu okna dialogowego właściwości folderu.

4. Ponieważ zamierzamy przekierować folder do pojedynczej lokalizacji, należy wybrać opcję Basic – Redirect Everyone’s Folder To The Same Location (Podstawowe – Przekierowuj wszystkie foldery do tej samej lokalizacji) z listy Setting (Ustawienie) na zakładce Target (Miejsce docelowe).
5. Sekcja Target Folder Location (Lokalizacja folderu docelowego) zawiera kilka opcji. Dostępne możliwości zmieniają się zależnie od aktualnie modyfikowanego folderu i mogą zawierać następujące opcje:

Redirect To The User’s Home Directory (Przekieruj do katalogu domowego użytkownika) Wybranie tej opcji powoduje przeniesienie folderu do podkatalogu wewnątrz katalogu domowego użytkownika. Lokalizację katalogu domowego można określić, definiując zmienne środowiskowe %HomeDrive% oraz %HomePath%.

Create A Folder For Each User Under The Root Path (Utwórz folder dla każdego użytkownika w ścieżce katalogu głównego) Opcja ta powoduje utworzenie folderu dla każdego użytkownika wewnątrz lokalizacji wprowadzonej w polu Root

Path (Ścieżka katalogu głównego). Nazwy poszczególnych folderów są nazwami użytkowników, określonymi przez zmienną %UserName%. Innymi słowy, jeśli wybrana ścieżka katalogu głównego to \\Zeta\UserDocuments, folder dla użytkownika WilliamS zostanie umieszczony w \\Zeta\UserDocuments\WilliamS.

Redirect To The Following Location (Przekieruj do poniższej lokalizacji) Po wybraniu tej opcji folder zostanie przeniesiony do lokalizacji wpisanej w polu Root Path. Przy podawaniu folderu można użyć zmiennej środowiskowej w celu dostosowania położenia folderu dla każdego użytkownika. Na przykład można użyć takiej wartości, jak \\Zeta\UserData%\%UserName%\docs.

Redirect To The Local Userprofile Location (Przekieruj do lokalnej lokalizacji profilu użytkownika) Opcja ta przekierowuje folder do podkatalogu w katalogu profilu użytkownika. Przy podawaniu lokalizacji profilu można użyć zmiennej środowiskowej %UserProfile%.

6. Kliknij zakładkę Settings, aby skonfigurować dodatkowe opcje korzystając z poniższych pól, po czym kliknij OK, aby zakończyć proces.

Grant The User Exclusive Rights To (Udziel użytkownikowi praw wyłączności do [nazwa_folderu]) Przyznaje użytkownikowi pełne i wyłączne prawa dostępu do zawartości folderu specjalnego.

Move The Contents Of [x] To The New Location (Przenieś zawartość [nazwa_folderu] do nowej lokalizacji) Przenosi dane zawarte w folderze specjalnym z indywidualnych systemów do centralnego folderu(ów).

Przekierowywanie folderu specjalnego w oparciu o członkostwo grup

W celu przekierowania folderu specjalnego w oparciu o członkostwo grup zabezpieczeń wykonaj następującą procedurę:

1. W konsoli GPMC kliknij prawym klawiszem myszy obiekt GPO dla lokacji, domeny lub jednostki organizacyjnej, po czym wybierz Edit. Spowoduje to otwarcie tego obiektu w edytorze zasad.
2. Rozwiń następujące węzły w edytorze zasad: User Configuration (Konfiguracja użytkownika), Windows Settings (Ustawienia systemu Windows) oraz Folder Redirection (Przekierowanie folderów).
3. Prawym klawiszem myszy kliknij folder specjalny, który chcesz zmodyfikować, na przykład AppData(Roaming), po czym wybierz Properties (Właściwości) z menu skrótowego.
4. Na zakładce Target (Miejsce docelowe) wybierz opcję Advanced—Specify Locations For Various User Groups (Zaawansowane – Określaj lokalizacje dla różnych grup użytkowników). Jak widać na rysunku 5-13, w oknie dialogowym pojawi się panel Security Group Membership (Członkostwo w grupie zabezpieczeń).
5. Kliknij Add (Dodaj), aby wyświetlić okno Specify Group And Location (Określanie grupy i lokalizacji).
6. Wpisz nazwę grupy zabezpieczeń w polu Security Group Membership lub kliknij Browse, aby zlokalizować odpowiednią grupę.
7. Podobnie jak przy przekierowaniu podstawowym, dostępne opcje są zależne od folderu, który jest przekierowywany, i mogą zawierać następujące możliwości:

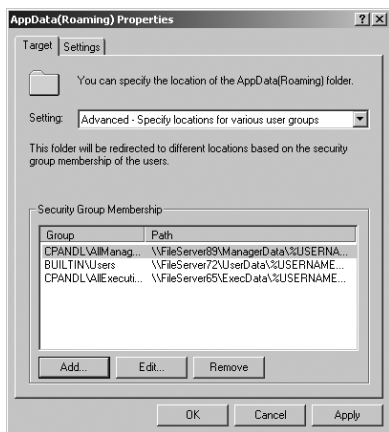
Redirect To The User's Home Directory (Przekieruj do katalogu domowego użytkownika) Wybranie tej opcji powoduje przeniesienie folderu do podkatalogu wewnątrz katalogu domowego użytkownika. Lokalizację katalogu domowego można określić definiując zmienne środowiskowe %HomeDrive% oraz %HomePath%.

Create A Folder For Each User Under The Root Path (Utwórz folder dla każdego użytkownika w ścieżce katalogu głównego) Opcja ta powoduje utworzenie folderu dla każdego użytkownika wewnątrz lokalizacji wprowadzonej w polu Root Path (Ścieżka katalogu głównego). Nazwy poszczególnych folderów są nazwami użytkowników, określonymi przez zmienną %UserName%. Innymi słowy, jeśli wybrana ścieżka katalogu głównego to \\Zeta\UserDocuments, folder dla użytkownika WilliamS zostanie umieszczony w \\Zeta\UserDocuments\WilliamS.

Redirect To The Following Location (Przekieruj do poniższej lokalizacji) Po wybraniu tej opcji folder zostanie przeniesiony do lokalizacji wpisanej w polu Root Path. Przy podawaniu folderu można użyć zmiennej środowiskowej w celu dostosowania położenia folderu dla każdego użytkownika. Na przykład można użyć takiej wartości, jak \\Zeta\UserData\%UserName%\docs.

Redirect To The Local Userprofile Location (Przekieruj do lokalnej lokalizacji profilu użytkownika) Opcja ta przekierowuje folder do podkatalogu w katalogu profilu użytkownika. Przy podawaniu lokalizacji profilu można użyć zmiennej środowiskowej %UserProfile%.

8. Kliknij OK. Następnie powtórz kroki 5–7 dla innych grup, które chcesz skonfigurować.
9. Po zakończeniu tworzenia wpisów dla grup kliknij zakładkę Settings i skonfiguruj dodatkowe opcje, analogiczne do omówionych przy przekierowaniu podstawowym. Kliknij OK, aby zakończyć proces.



Rysunek 5-13 Konfigurowanie zaawansowanego przekierowania przy użyciu panelu Security Group Membership.

Usuwanie przekierowania

Niekiedy konieczne jest usunięcie przekierowania wybranego folderu specjalnego. W tym celu wykonaj następujące czynności:

1. W konsoli GPMC kliknij prawym klawiszem myszy obiekt GPO dla lokacji, domeny lub jednostki organizacyjnej, po czym wybierz Edit. Spowoduje to otwarcie tego obiektu w edytorze zasad.

2. Rozwiń następujące węzły w edytorze zasad: User Configuration (Konfiguracja użytkownika), Windows Settings (Ustawienia systemu Windows) oraz Folder Redirection (Przekierowanie folderów).
3. Prawym klawiszem myszy kliknij folder specjalny, który chcesz zmodyfikować, po czym wybierz Properties (Właściwości) z menu skrótowego.
4. Kliknij zakładkę Settings (ustawienia) i upewnij się, że wybrana jest odpowiednia opcja Policy Removal (Usuwanie zasad). Dostępne są dwie możliwości:

Leave The Folder In The New Location When Policy Is Removed (Kiedy zasady zostaną usunięte, pozostaw folder w nowej lokalizacji) Opcja powoduje, że folder i cała jego zawartość pozostaje w dotychczasowej (przekierowanej) lokalizacji, zaś dotychczasowi użytkownicy nadal mają prawa dostępu do swoich folderów i ich zawartości.

Redirect The Folder Back To The Local Userprofile Location When Policy Is Removed (Kiedy zasady zostaną usunięte, przekieruj folder z powrotem do lokalnej lokalizacji profilu użytkownika) Opcja ta powoduje, że folder i jego zawartość zostaje skopiowana ponownie do lokalizacji oryginalnej. Tym niemniej zawartość nie jest usuwana z poprzedniej lokalizacji.

5. Jeśli opcja Policy Removal została zmieniona, kliknij Apply (Zastosuj), zanim klikniesz zakładkę Target. W innym wypadku po prostu otwórz zakładkę Target.
6. W celu usunięcia wszystkich przekierowań tego folderu wybierz opcję Not Configured (Nieskonfigurowane) na liście Setting (Ustawienia).
7. Aby usunąć przekierowanie dla wybranej grupy zabezpieczeń, wybierz tę grupę w panelu Security Group Membership i kliknij Remove (Usuń), po czym kliknij OK.

Zarządzanie skryptami użytkowników i komputerów

Przy korzystaniu z systemu Windows Server 2008 można skonfigurować cztery typy skryptów:

Rozruchowe komputera Wykonywane podczas uruchamiania systemu.

Zamykania komputera Wykonywane przed zamknięciem systemu.

Logowania użytkownika Wykonywane podczas logowania użytkownika.

Wylogowania użytkownika Wykonywane podczas wylogowywania się użytkownika.

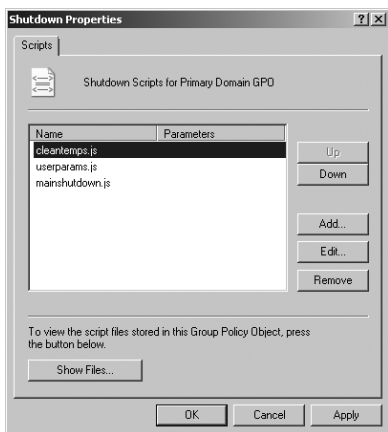
Skrypty te mogą być plikami wsadowymi powłoki wiersza poleceń (z rozszerzeniem .bat lub .cmd) lub skryptami wykorzystującymi środowisko Windows Script Host (WSH). WSH jest rozszerzeniem systemu Windows Server 2008, które pozwala na wykorzystanie skryptów napisanych w zaawansowanym języku skryptowym (takim jak VBScript), bez konieczności wstawiania go do strony sieci Web. W celu zapewnienia środowiska skryptowego dla różnych zastosowań WSH opiera się na silnikach skryptowych. Silnik skryptowy jest komponentem, który definiuje podstawową składnię i strukturę wybranego języka. Windows Server 2008 wyposażony jest domyślnie w silniki skryptowe dla języków VBScript oraz JScript. Dostępne są również silniki skryptowe dla innych języków.

Przypisywanie skryptów rozruchowych i zamykania komputera

Skrypty rozruchu i zamykania komputera są przypisywane jako część zasad grupy. W ten sposób wszystkie komputery będące członkami lokacji, domeny lub jednostki organizacyjnej wykonują skrypty automatycznie podczas uruchamiania lub zamykania systemu.

W celu przypisania skryptu rozruchu lub zamykania komputera wykonaj następującą procedurę:

1. W celu uproszczenia zarządzania skopij skrypty, których chcesz użyć, do folderu Machine\Scripts\Startup albo Machine\Scripts\Shutdown odpowiedniej zasady. Zasady przechowywane są na kontrolerach domeny w folderze %SystemRoot%\Sysvol\Domain\Policies.
2. W konsoli GPMC kliknij prawym klawiszem myszy odpowiedni obiekt GPO dla lokacji, domeny lub jednostki organizacyjnej, po czym wybierz Edit. Obiekt zostanie otwarty w edytorze zasad.
3. W węźle Computer Configuration (Konfiguracja komputera) kliknij podwójnie folder Windows Settings (Ustawienia systemu Windows), a następnie Scripts (Skrypty).
4. Aby zdefiniować skrypty rozruchowe, kliknij prawym klawiszem myszy Startup (Autostart), po czym wybierz Properties. W celu zdefiniowania skryptów zamykania kliknij prawym klawiszem myszy Shutdown (Zamknięcie) i wybierz Properties. Pojawi się okno dialogowe podobne do pokazanego na rysunku 5-14.
5. Kliknij Show Files (Pokaż pliki). Jeśli skrypty zostały skopiowane do właściwej lokalizacji w folderze Policies, powinny pojawić się w wyświetlonym oknie.
6. Kliknij Add (Dodaj), aby przypisać skrypt. Pojawi się okno dialogowe Add A Script (Dodaj skrypt). W polu Script Name (Nazwa skryptu) wpisz nazwę skryptu skopiowanego wcześniej do folderu Machine\Scripts\Startup lub Machine\Scripts\Shutdown, zależnie od wybranej zasady. W polu Script Parameters (Parametry skryptu) wpisz wymagane argumenty wiersza polecenia, które powinny być przekazane do interpretera skryptu lub do WSH. Powtórz ten krok dla innych skryptów.



Rysunek 5-14 Dodawanie, edytowanie lub usuwanie skryptów zamykania komputera.

7. Podczas rozruchu lub zamykania komputera skrypty będą wykonywane w tej kolejności, w jakiej są wyświetlane w oknie dialogowym Properties. Przyciski Up (W górę) i Down (W dół) w razie potrzeby umożliwiają zmianę kolejności.
8. W celu edycji przypisanego skryptu lub zmiany parametrów należy zaznaczyć skrypt na liście i kliknąć Edit.
9. Aby usunąć skrypt, zaznacz go na liście i kliknij Remove.

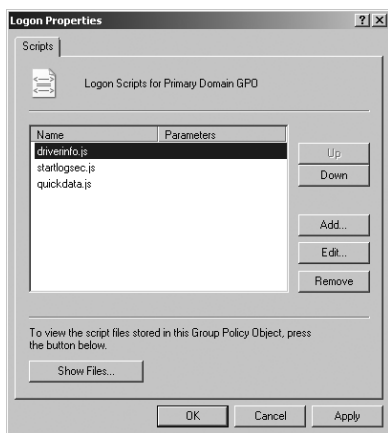
Przypisywanie skryptów logowania i wylogowywania się użytkowników

Skrypty użytkowników można przypisać jedną z poniższych metod:

- Przy użyciu zasad grupy. W ten sposób dla wszystkich użytkowników należących do odpowiedniej lokalacji, domeny lub jednostki organizacyjnej skrypty zostaną wykonane automatycznie w trakcie procedury logowania lub wylogowywania.
- Skrypty logowania mogą zostać przypisane indywidualnie za pośrednictwem konsoli Active Directory Users And Computers (Użytkownicy i komputery Active Directory). Tą metodą można przypisać oddzielne skrypty dla poszczególnych użytkowników lub grup. Szczegóły zawiera podrzdział „Konfigurowanie ustawień środowiskowych użytkowników” w rozdziale 11.
- Skrypty logowania mogą zostać również przypisane jako zadania zaplanowane, definiowane za pomocą Scheduled Task Wizard (Kreatora harmonogramu zadań).

W celu przypisania skryptu logowania lub wylogowywania za pomocą zasad grupy wykonaj następującą procedurę:

1. W celu uproszczenia zarządzania skopiuj skrypty, których chcesz użyć, do folderu User\Scripts\Logon albo User\Scripts\Logoff odpowiedniej zasady. Zasady przechowywane są na kontrolerach domeny w folderze %SystemRoot%\Sysvol\Domain\Policies.
2. W konsoli GPMC kliknij prawym klawiszem myszy odpowiedni obiekt GPO dla lokalacji, domeny lub jednostki organizacyjnej, po czym wybierz Edit. Obiekt zostanie otwarty w edytorze zasad.
3. Kliknij podwójnie folder Windows Settings (Ustawienia systemu Windows) w węzle User Configuration (Konfiguracja użytkownika), po czym kliknij Scripts (Skrypty).
4. Aby zdefiniować skrypty logowania, kliknij prawym klawiszem myszy węzeł Logon (Logowanie) i wybierz polecenie Properties. Analogicznie w celu zdefiniowania skryptów wylogowywania kliknij prawym klawiszem myszy Logoff (Wylogowywanie) i wybierz Properties. Pojawi się okno dialogowe podobne do pokazanego na rysunku 5-15.



Rysunek 5-15 Dodawanie, edytowanie i usuwanie skryptów logowania użytkownika.

5. Kliknij Show Files (Pokaż pliki). Jeśli skrypty zostały skopiowane do właściwej lokalizacji w folderze Policies, powinny pojawić się w wyświetlonym oknie.
6. Kliknij Add (Dodaj), aby przypisać skrypt. Pojawi się okno dialogowe Add A Script (Dodaj skrypt). W polu Script Name (Nazwa skryptu) wpisz nazwę skopiowanego wcześniej skryptu. W polu Script Parameters (Parametry skryptu) wpisz wymagane argumenty wiersza polecenia, które powinny być przekazane do interpretera skryptu lub do WSH. Powtórz ten krok dla innych skryptów.
7. Podczas logowania lub wylogowywania użytkownika skrypty będą wykonywane w tej kolejności, w jakiej są wyświetlane w oknie dialogowym Properties. Przyciski Up (W górę) i Down (W dół) w razie potrzeby umożliwiają zmianę kolejności.
8. W celu edycji przypisanego skryptu lub zmiany parametrów należy zaznaczyć skrypt na liście i kliknąć Edit.
9. Aby usunąć skrypt, zaznacz go na liście i kliknij Remove.

Rozpowszechnianie oprogramowania za pośrednictwem zasad grupy

Mechanizm zasad grupy zawiera podstawową funkcjonalność umożliwiającą rozpowszechnianie oprogramowania pod nazwą Software Installation (Instalacja oprogramowania). Wprawdzie zasada ta nie ma na celu zastąpienia rozwiązań klasy przedsiębiorstwa, takich jak Systems Management Server (SMS), można wykorzystać ją do zautomatyzowania wdrażania i konserwacji oprogramowania w organizacji niemal dowolnych rozmiarów przy założeniu, że wszystkie komputery pracują pod kontrolą biznesowych edycji systemów Windows w wersji Windows 2000 lub późniejszej.

Zapoznavanie się z zasadą instalacji oprogramowania

Zasady grupy umożliwiają wdrażanie oprogramowania dla komputerów lub dla użytkowników. Aplikacje rozpowszechnione dla komputerów są dostępne dla wszystkich użytkowników danego komputera i są konfigurowane w węźle Computer Configuration\Software Settings\Software Installation (Konfiguracja komputera\Ustawienia oprogramowania\Instalacja oprogramowania). Aplikacje przypisane użytkownikom są dostępne dla wskazanych użytkowników i są konfigurowane w węźle User Configuration\Software Settings\Software Installation (Konfiguracja użytkownika\Ustawienia oprogramowania\Instalacja oprogramowania).

Wdrożenie oprogramowania można wykonać jedną z trzech kluczowych metod:

Przypisanie do komputera Przypisuje oprogramowanie komputerom klienckim, co powoduje jego instalację podczas uruchamiania komputera. Technika ta wprawdzie nie wymaga żadnej interwencji użytkownika, wymaga jednak ponownego uruchomienia komputera w celu zainstalowania oprogramowania. Zainstalowane programy są następnie dostępne dla wszystkich użytkowników komputera.

Przypisanie do użytkownika Powoduje zainstalowanie oprogramowania w trakcie logowania użytkownika. Metoda ta nie wymaga interwencji użytkownika, ale wymaga wylogowania i ponownego zalogowania się użytkownika. Programy takie są przypisane do użytkowników, nie zaś do komputerów.

Publikowanie dla użytkowników Publikuje oprogramowanie, dzięki czemu użytkownicy mogą zainstalować je ręcznie za pośrednictwem narzędzia Programs And Features (Programy i funkcje). Technika ta wymaga udziału użytkownika podczas instalacji. Oprogramowanie jest powiązane tylko z użytkownikiem.

Przy korzystaniu z przypisania lub publikowania dla użytkowników można także ogłosić program, który wówczas zostanie zainstalowany przy pierwszej próbie użycia. Automatyczna instalacja ogłoszonego oprogramowania następuje w następujących sytuacjach:

- Gdy użytkownik próbuje otworzyć dokument wymagający danego oprogramowania.
- Gdy użytkownik otworzy skrót do aplikacji.
- Gdy inna aplikacja wymaga danego komponentu.

Do skonfigurowania zasady Software Installation zazwyczaj nie wykorzystuje się istniejących obiektów GPO. Zamiast tego zalecane jest utworzenie nowego GPO konfigurującego instalację oprogramowania i połączenie go z odpowiednimi kontenerami zasad grupy. Metoda ta znacznie upraszcza ponowne wdrażanie oprogramowania lub stosowanie uaktualnień.

Po utworzeniu nowego GPO do celów wdrożenia oprogramowania należy przygotować punkt dystrybucji. Jest to udostępniony folder, który jest osiągalny dla użytkowników i komputerów, dla których oprogramowanie ma zostać wdrożone. W przypadku prostych aplikacji przygotowanie punktu dystrybucji sprowadza się do skopiowania pliku pakietu instalatora i wszystkich wymaganych plików aplikacji do udziału sieciowego i skonfigurowanie uprawnień, aby pliki te były dostępne. Dla innych aplikacji, takich jak Microsoft Office, punkt dystrybucyjny jest tworzony w drodze administracyjnej instalacji w wybranym udziale sieciowym. W przypadku Microsoft Office można to osiągnąć uruchamiając program Setup z parametrem */a* i wskazując udział jako lokalizację instalacji. Przewagą instalacji administracyjnej jest to, że oprogramowanie może zostać później łatwo uaktualnione i ponownie rozpowszechnione za pośrednictwem zasady instalacji oprogramowania.

Aktualizację aplikacji rozpowszechnionych przy użyciu zasady instalacji oprogramowania wykonuje się albo za pomocą pakietu aktualizacyjnego (serwisowego), albo przez wdrożenie nowej wersji aplikacji. Każde z tych zadań wykonywane jest w nieco inny sposób.

Wdrażanie oprogramowania w organizacji

Zasada instalacji oprogramowania wykorzystuje albo pakiety instalatora Windows (.msi), albo pakiety aplikacji niskopoziomowych ZAW (.zap). Pakiety .msi można rozpowszechnić każdą z trzech dostępnych metod. W przypadku publikowania dla użytkowników można także wykorzystać pakiety ZAW (pliki .zap). W każdym wypadku konieczne jest określenie odpowiednich uprawnień do pakietu instalacyjnego, aby odpowiednie konta komputerów lub użytkowników miały prawo odczytu.

Ponieważ zasada instalacji oprogramowania jest stosowana tylko podczas jawnego przetwarzania ustawień zasad, wdrożenie aplikacji dla komputerów jest wykonywane tylko podczas rozruchu komputerów, zaś wdrożenie dla użytkowników podczas logowania. Możliwe jest również dostosowanie instalacji przy użyciu plików transformacji (.mst). Pliki te modyfikują proces instalacyjny zgodnie z ustawieniami zdefiniowanymi dla wybranych komputerów lub użytkowników.

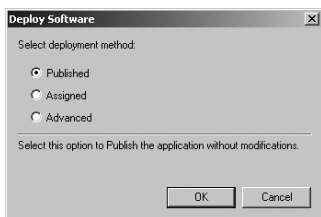
W celu wdrożenia oprogramowania wykonaj następujące czynności:

1. W konsoli GPMC kliknij prawym klawiszem myszy obiekt GPO, którego chcesz użyć do tego celu, po czym wybierz Edit.
2. W edytorze zasad otwórz odpowiednio węzeł Computer Configuration\Software Settings\Software Installation albo User Configuration\Software Settings\Software Installation, stosownie do wybranego typu wdrożenia.
3. Prawym klawiszem myszy kliknij Software Installation (Instalacja oprogramowania) i wybierz New z menu podręcznego, po czym kliknij Package (Pakiet).

4. W oknie dialogowym Open (Otwieranie) przejdź do udziału sieciowego zawierającego przygotowany pakiet, kliknij go i następnie kliknij Open (Otwórz).

Uwaga Na liście Files Of Type (Pliki typu) domyślnie wybrana jest opcja Windows Installer Packages (.msi) (Pakiety instalatora Windows). Przy wykonywaniu rozpozszczenia w drodze publikacji dla użytkowników można także wybrać typ ZAW Down-Level Application Packages (Pakiety aplikacji niskopoziomowych ZAW).

5. W oknie dialogowym Deploy Software (Rozmieszczanie oprogramowania), pokazanym na rysunku 5-16, wybierz jedną z poniższych metod instalacji, po czym kliknij OK:
 - Published (Opublikowany)** Aplikacja zostanie opublikowana bez modyfikacji.
 - Assigned (Przypisany)** Aplikacja zostanie przypisana bez modyfikacji.
 - Advanced (Zaawansowane)** Umożliwia wdrożenie aplikacji przy użyciu zaawansowanych opcji konfiguracyjnych.



Rysunek 5-16 Wybieranie metody rozmieszczania oprogramowania.

Konfigurowanie opcji wdrażania oprogramowania

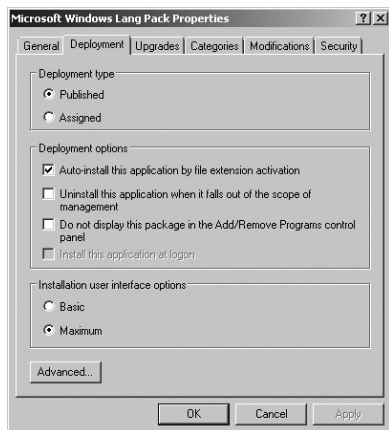
W celu przejrzania i ustawienia ogólnych opcji pakietu oprogramowania wykonaj następujące czynności:

1. W konsoli GPMC kliknij prawym klawiszem myszy obiekt GPO, który ma zostać użyty do rozmieszczania oprogramowania, po czym wybierz Edit.
2. W edytorze zasad otwórz odpowiednio węzeł Computer Configuration\Software Settings\Software Installation albo User Configuration\Software Settings\Software Installation, stosownie do wybranego typu wdrożenia.
3. Kliknij podwójnie pakiet instalacji oprogramowania. Pojawi się okno dialogowe Properties.
4. Zakładka Deployment (Rozmieszczanie), ukazana na rysunku 5-17, umożliwia zmianę typu rozmieszczania i skonfigurowanie następujących opcji:

Auto-Install This Application By File Extension Activation (Wykonaj autoinstalację tej aplikacji przez aktywację rozszerzenia pliku) Ogłasza rozszerzenia plików skojarzone z tym pakietem na potrzeby instalacji przy pierwszym użyciu. Opcja ta jest wybrana domyślnie.

Uninstall This Application When It Falls Out Of The Scope Of Management (Odinstaluj tę aplikację, gdy znajdzie się poza zasięgiem zarządzania) Usuwa aplikację, jeśli nie ma już zastosowania dla użytkownika.

Do Not Display This Package In The Add/Remove Programs Control Panel (Nie wyświetlaj tego pakietu w aplecie Dodaj/Usuń programy Panelu sterowania) Powoduje, że aplikacja nie jest wyświetlana w aplecie Dodaj/Usuń programy, tym samym powstrzymując użytkownika przed usunięciem aplikacji.



Rysunek 5-17 Opcje rozmieszczania oprogramowania.

Install This Application At Logon (Zainstaluj tę aplikację podczas logowania)

Powoduje wykonanie pełnej instalacji – zamiast ogłaszania – aplikacji podczas logowania się użytkownika. Opcja ta jest niedostępna, jeśli pakiet jest publikowany.

Installation User Interface Options (Opcje interfejsu użytkownika instalacji)

Steruje sposobem wykonywania instalacji. Przy domyślnym ustawieniu Maximum (Maksymalne) użytkownik widzi wszystkie ekrany instalatora i komunikaty wyświetlane podczas instalacji. Opcja Basic (Podstawowe) powoduje wyświetlanie tylko komunikatów o błędach (o ile wystąpią) oraz komunikatu o zakończeniu instalacji.

5. Kliknij OK.

Aktualizowanie wdrożonego oprogramowania

Jeśli aplikacja wykorzystuje pakiet instalatora Windows, można zastosować do niej poprawki lub pakiet serwisowy, wykonując następującą procedurę:

1. Po uzyskaniu pliku .msi albo .msp zawierającego poprawkę lub pakiet serwisowy skopiuj go wraz innymi wymaganymi plikami instalacyjnymi do folderu zawierającego oryginalny plik .msi. Zastąp wszystkie duplikujące się pliki w razie potrzeby.
2. W konsoli GPMC kliknij prawym klawiszem myszy obiekt GPO, którego chcesz użyć do tego celu, po czym wybierz Edit.
3. W edytorze zasad otwórz odpowiednio węzeł Computer Configuration\Software Settings\Software Installation albo User Configuration\Software Settings\Software Installation, stosownie do wybranego typu wdrożenia.
4. Kliknij prawym klawiszem myszy pakiet, który ma zostać uaktualniony, po czym w menu skrótowym All Tasks (Wszystkie zadania) i następnie Redeploy Application (Rozmieść ponownie aplikację).
5. Kliknij Yes (Tak) w monicie potwierdzenia operacji. Aplikacja zostanie ponownie zainstalowana dla wszystkich użytkowników lub komputerów, zgodnie z zasięgiem wybranego GPO.

Jeśli aplikacja używa pakietu instalacyjnego innego typu, można zainstalować jej aktualizację wykonując następujące czynności:

1. W konsoli GPMC kliknij prawym klawiszem myszy obiekt GPO, którego chcesz użyć do tego celu, po czym wybierz Edit.
2. W edytorze zasad otwórz węzeł User Configuration\Software Settings\Software Installation.
3. Kliknij pakiet prawym klawiszem myszy. W menu skrótowym wybierz All Tasks, po czym kliknij Remove (Usuń). Kliknij OK, aby zaakceptować domyślną opcję natychmiastowego usunięcia.
4. Skopiuj nowy plik .zap i wszystkie powiązane pliki do udziału sieciowego i ponownie розмісь aplikację.

Instalowanie nowej wersji rozmieszczonego oprogramowania

W celu zainstalowania nowej wersji wcześniej rozmieszczonego oprogramowania wykonaj następujące czynności:

1. Uzyskaj plik instalatora Windows dla nowej wersji oprogramowania i skopiuj go wraz ze wszystkimi wymaganymi plikami do udziału sieciowego. Alternatywnie możesz wykonać instalację administracyjną w tym udziale.
2. W konsoli GPMC kliknij prawym klawiszem myszy obiekt GPO, którego chcesz użyć do wdrożenia, po czym wybierz Edit.
3. W edytorze zasad otwórz odpowiednio węzeł Computer Configuration\Software Settings\Software Installation albo User Configuration\Software Settings\Software Installation, stosownie do wybranego typu wdrożenia.
4. Kliknij prawym klawiszem myszy Software Installation. Wybierz New z menu skrótowego, po czym kliknij Package. Następnie przypisz lub opublikuj nową wersję aplikacji, używając pliku instalatora Windows.
5. Kliknij prawym klawiszem myszy pakiet aktualizacji i wybierz polecenie Properties. Na zakładce Upgrades (Uaktualnienia) kliknij Add. W wyświetlonym oknie dialogowym Add Upgrade Package (Dodawanie pakietu uaktualniającego) wykonaj jedno z poniższych:
 - Jeśli oryginalna aplikacja i uaktualnienie znajdują się w bieżącym obiekcie GPO, wybierz Current Group Policy Object (Bieżący obiekt zasad grupy), po czym zaznacz wcześniej wdrożoną aplikację na liście Package To Upgrade (Pakiet do uaktualnienia).
 - Jeśli oryginalna aplikacja i uaktualnienie znajdują się w różnych GPO, wybierz A Specific GPO (Określony obiekt GPO), kliknij Browse, po czym wskaż właściwy obiekt GPO. Następnie zaznacz wcześniej wdrożoną aplikację na liście.
6. Wybierz opcję uaktualnienia. Jeżeli nowa wersja wymaga całkowitej reinstalacji aplikacji, wybierz opcję Uninstall The Existing Package, Then Install The Upgrade Package (Odinstaluj istniejący pakiet, a następnie zainstaluj pakiet uaktualniający). Jeśli aplikacja może zostać uaktualniona na miejscu przez zastąpienie poprzedniej wersji, wybierz opcję Package Can Upgrade Over The Existing Package (Pakiet może uaktualnić na istniejącym pakiecie).
7. Kliknij OK, aby zamknąć okno dialogowe Add Upgrade Package. Jeśli nowa wersja ma być wymaganą aktualizacją, zaznacz pole wyboru Required Upgrade For Existing Packages (Wymagane uaktualnienie dla istniejących pakietów), po czym kliknij OK, aby zamknąć okno dialogowe.

Automatyczne żądania certyfikatów dla komputerów i użytkowników

Serwer odgrywający rolę urzędu certyfikacji (Certificate Authority – CA) jest odpowiedzialny za wystawianie certyfikatów cyfrowych i zarządzanie listami odwołań certyfikatów (Certificate Revocation list – CRL). Funkcję tę mogą pełnić serwery systemu Windows Server 2008 po zainstalowaniu roli Active Directory Certificate Services. Komputery i użytkownicy wykorzystują certyfikaty do celów uwierzytelniania i szyfrowania danych.

W środowisku przedsiębiorstwa wykorzystuje się urzędy certyfikacji przedsiębiorstwa do automatycznego rejestrowania certyfikatów. Oznacza to, że autoryzowani użytkownicy i komputery mogą żądać wydania certyfikatów, które to żądania są następnie automatycznie przetwarzane przez CA, dzięki czemu komputery i użytkownicy praktycznie natychmiast mogą zainstalować otrzymany certyfikat.

Zasady grupy pozwalają na sterowanie mechanizmem automatycznej rejestracji. Po zainstalowaniu CA przedsiębiorstwa zasad automatycznej rejestracji zostają domyślnie włączone. Zasada sterująca rejestracją certyfikatów nosi nazwę Certificate Services Client–AutoEnrollment Settings (Ustawienia automatycznego żądania certyfikatów) i jest zlokalizowana w węźle Computer Configuration\Windows Settings\Security Settings\Public Key Policies (Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zasady kluczy publicznych) lub User Configuration\Windows Settings\Security Settings\Public Key Policies – odpowiednio dla komputerów i użytkowników.

W celu skonfigurowania automatycznych żądań certyfikatów wykonaj następującą procedurę:

1. W konsoli GPMC kliknij prawym klawiszem myszy obiekt GPO, którego chcesz użyć, po czym wybierz Edit.
2. W edytorze zasad przejdź do węzła Public Key Policies (Zasady kluczy publicznych) w konfiguracji komputera lub użytkownika.
3. Kliknij podwójnie Certificate Services Client–Auto–Enrollment. W celu wyłączenia automatycznego przetwarzania żądań wybierz opcję Disabled (Wyłączone) z listy Configuration Model (Model konfiguracji), kliknij OK i pomiń pozostałe kroki procedury. Aby włączyć automatyczne przetwarzanie żądań, wybierz opcję Enabled (Włączone).
4. Aby automatycznie odnawiać certyfikaty, których ważność wygasła, zaktualizować oczekujące certyfikaty i usunąć certyfikaty odwołane, zaznacz odpowiednie pole wyboru.
5. Aby zagwarantować, że używane są najnowsze wersje szablonów certyfikatów, zaznacz pole wyboru Update Certificates That Use Certificate Templates (Uaktualnij certyfikaty używające szablonów certyfikatów).
6. Aby powiadamiać użytkowników, że ważność ich certyfikatów się kończy, zaznacz pole wyboru Expiration Notification (Powiadamianie o wygaśnięciu) i określ czas wysyłania powiadomień. Domyślnie powiadomienia wysyłane są w momencie, gdy do końca ważności pozostanie 10 procent całego okresu ważności.
7. Kliknij OK, aby zapisać ustawienia.

Zarządzanie aktualizacjami automatycznymi

Aktualizacje automatyczne ułatwiają zapewnienie, że systemy operacyjne używają najnowszych wersji poprawek i uzupełnień. Wprawdzie możliwe jest skonfigurowanie tego mechanizmu na poszczególnych komputerach, jednak znacznie wygodniejsze i bardziej efektywne jest zrealizowanie tego zadania za pośrednictwem zasad grupy.

Konfigurowanie aktualizacji automatycznych

Zarządzając aktualizacjami automatycznymi przez mechanizm zasad grupy można określić dowolną z następujących opcji:

Auto Download And Schedule The Install (Pobierz automatycznie i zaplanuj instalację)

Aktualizacje są pobierane automatycznie i instalowane zgodnie z określonym harmonogramem. Po pobraniu aktualizacji system operacyjny powiadamia użytkownika, który może następnie przejrzeć aktualizacje, które mają zostać zainstalowane. Użytkownik może wówczas zainstalować aktualizację lub zaczekać na zaplanowany czas instalacji.

Auto Download And Notify For Install (Pobierz automatycznie i powiadom o instalacji)

System operacyjny pobiera wszystkie aktualizacje, gdy staną się dostępne, po czym informuje użytkownika, że są one gotowe do instalacji. Użytkownik może następnie zaakceptować lub odrzucić aktualizację. Zaakceptowane aktualizacje są instalowane, zaś odrzucone nie, ale nadal pozostają dostępne w systemie i mogą zostać zainstalowane w późniejszym terminie.

Notify For Download And Notify For Install (Powiadom o pobieraniu i powiadom o instalacji) System operacyjny informuje użytkownika przed pobraniem dowolnych aktualizacji. Jeśli użytkownik zdecyduje się na pobranie aktualizacji, będzie miał nadal możliwość zaakceptowania jej lub odrzucenia. Aktualizacje odrzucone nie są instalowane, ale pozostają w systemie i można je zainstalować w późniejszym terminie.

Allow Local Admin To Choose Setting (Zezwalaj lokalnemu administratorowi na wybór ustawień) Pozwala na konfigurowanie ustawień aktualizacji automatycznych przez administratora lokalnego komputera. Warto zauważyć, że użycie dowolnego innego ustawienia powoduje, że lokalni użytkownicy i administratorzy nie mają możliwości zmiany konfiguracji aktualizacji automatycznych.

W celu skonfigurowania aktualizacji automatycznych w zasadach grupy wykonaj następującą procedurę:

1. W konsoli GPMC kliknij prawym klawiszem myszy obiekt GPO, którego chcesz użyć, po czym wybierz Edit.
2. W edytorze zasad otwórz węzeł Computer Configuration\Administrative Templates\Windows Components\Windows Update (Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Windows Update).
3. Kliknij podwójnie wpis Configure Automatic Updates (Konfiguruj aktualizacje automatyczne). W oknie dialogowym Properties można następnie włączyć lub wyłączyć zarządzanie mechanizmem aktualizacji przez zasady grupy.
4. Wybierz odpowiednią opcję konfiguracyjną z listy Configure Automatic Update.
5. Jeśli wybraną opcją jest Auto Download And Schedule The Install, należy następnie określić dzień i godzinę wykonania instalacji, używając dostępnych list rozwijanych. Kliknij OK, aby zapisać ustawienia.

Optymalizowanie aktualizacji automatycznych

Mówiąc ogólnie, większość aktualizacji jest instalowanych podczas zamykania i ponownego uruchamiania komputera. Niektóre aktualizacje mogą być zainstalowane natychmiast bez przerywania działania usług systemowych i nie wymagają ponownego uruchomienia komputera.

W celu upewnienia się, że aktualizacje takie zostaną zainstalowane natychmiast, wykonaj następujące czynności:

1. W konsoli GPMC kliknij prawym klawiszem myszy obiekt GPO, którego chcesz użyć, po czym wybierz Edit.
2. W edytorze zasad otwórz węzeł Computer Configuration\Administrative Templates\Windows Components\Windows Update (Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Usługa Windows Update).
3. Kliknij podwójnie zasadę Allow Automatic Updates Immediate Installation (Zezwalaj na natychmiastową instalację aktualizacji automatycznych). W oknie dialogowym Properties zaznacz Enabled, po czym kliknij OK.

Domyslnie tylko użytkownicy z uprawnieniami lokalnego administratora otrzymują powiadomienia o aktualizacjach. Można jednak zezwolić na otrzymywanie tych powiadomień przez dowolnego zalogowanego użytkownika, wykonując następujące działania:

1. W konsoli GPMC kliknij prawym klawiszem myszy obiekt GPO, którego chcesz użyć, po czym wybierz Edit.
2. W edytorze zasad otwórz węzeł Computer Configuration\Administrative Templates\Windows Components\Windows Update (Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Usługa Windows Update).
3. Kliknij podwójnie zasadę Allow Non-Administrators To Receive Update Notifications (Zezwalaj, aby użytkownicy inni niż administratorzy otrzymywali powiadomienia aktualizacji). W oknie dialogowym Properties zaznacz Enabled, po czym kliknij OK.

Spośród innych użytecznych zasad dotyczących aktualizacji automatycznych można wymienić:

Windows Automatic Updates (Automatyczne aktualizacje systemu Windows) Za każdym razem, gdy użytkownik łączy się z Internetem, Windows wyszukuje poprawki pasujące do tego komputera. Włączenie tej zasady pozwala zablokować wyszukiwanie poprawek. Zasada ta jest zlokalizowana w folderze User Configuration\Administrative Templates\System (Konfiguracja użytkownika\Szablony administracyjne\System).

Turn Off Automatic Update Of ADM Files (Wyłącz automatyczne aktualizowanie plików ADM) Zasady grupy mogą zostać zmodyfikowane przez proces aktualizacji automatycznych. Zazwyczaj oznacza to instalację nowych zasad, które stają się dostępne przy kolejnym użyciu edytora zasad. Włączenie tej zasady blokuje automatyczne aktualizowanie zasad grupy. Jest ona zlokalizowana w User Configuration\Administrative Templates\System\Group Policy (Konfiguracja użytkownika\Szablony administracyjne\System\Zasady grupy), przy czym ustawienie to jest ignorowane, jeśli zostanie włączona zasada Always Use Local ADM Files For The Group Policy Object Editor (Zawsze używaj lokalnych plików ADM w Edytorze obiektów zasad grupy).

Remove Access To Use All Windows Update Features (Usuń dostęp do używania wszystkich funkcji witryny Windows Update) Zabrania dostępu do wszystkich funkcji Windows Update. Włączenie tej zasady usuwa wszystkie funkcje aktualizacji automatycznych. Dotyczy to odpowiedniej zakładki w narzędziu System, łączy Windows Update w menu Start oraz menu Tools przeglądarki Internet Explorer, a także łączy aktualizacji sterowników w narzędziu Device Manager. Zasada ta zlokalizowana jest w folderze User Configuration\Administrative Templates\Windows Components\Windows Update (Konfiguracja użytkownika\Szablony administracyjne\Składniki systemu Windows\Usługa Windows Update).

Korzystanie z intranetowych lokalizacji usługi aktualizacyjnej

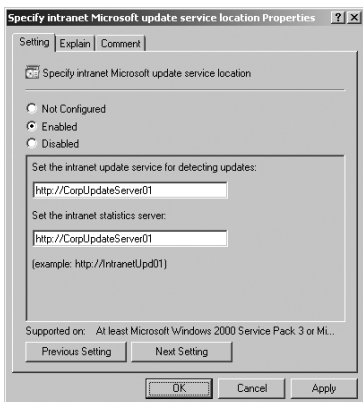
W sieciach zawierających setki lub tysiące komputerów proces aktualizacji automatycznych mógłby pochłonąć znaczącą część dostępnego pasma sieciowego, zaś wymaganie, aby wszystkie te komputery łączyły się z witryną w Internecie w celu pobrania poprawek, nie ma sensu. Zmiał tego należy posłużyć się zasadą Specify Intranet Microsoft Update Service Location (Określ intranetową lokalizację usługi aktualizującej), która nakazuje poszczególnym komputerom sprawdzanie wybranego serwera wewnętrznego w poszukiwaniu poprawek.

Na serwerze tym musi być uruchomiony składnik Windows Server Update Services (WSUS). Oznacza to, że musi być on skonfigurowany jako serwer Web z uruchomionym składnikiem Microsoft Internet Information Services (IIS), a ponadto musi być w stanie obsłużyć dodatkowe obciążenie, które może być znaczące w dużych sieciach podczas szczytowego użycia. Ponadto serwer aktualizacji musi mieć dostęp do sieci zewnętrznej przez port 80. Zastosowanie zapory ogniowej lub serwera proxy nie powinno nasręczać żadnych problemów.

Proces aktualizacji śledzi również informacje o konfiguracji i statystykach dla każdego komputera. Informacje te są niezbędne dla właściwego funkcjonowania procesu aktualizacji i mogą być przechowywane na odrębnym serwerze statystyk (wewnętrznym serwerze z uruchomionym składnikiem IIS) albo na samym serwerze aktualizacji.

W celu wskazania wewnętrznego serwera aktualizacji wykonaj następujące czynności:

1. Po zainstalowaniu i skonfigurowaniu serwera aktualizacji otwórz obiekt GPO, w edytorze zasad, po czym rozwiń węzeł Computer Configuration\Administrative Templates\Windows Components\Windows Update (Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Usługa Windows Update).
2. Kliknij podwójnie zasadę Specify Intranet Microsoft Update Service Location (Określ lokalizację intranetową usługi aktualizującej firmy Microsoft), po czym w oknie dialogowym Properties wybierz opcję Enabled.
3. Wpisz adres URL serwera aktualizacji w polu Set The Intranet Update Service For Detecting Updates (Ustaw intranetową usługę aktualizującą do wykrywania aktualizacji). W większości wypadków będzie to adres typu *http://servername*, na przykład *http://CorpUpdateServer01* (rysunek 5-18).



Rysunek 5-18 Wykorzystanie intranetowego serwera aktualizacji w celu scentralizowania procesu aktualizowania systemów i zmniejszenia zewnętrznego ruchu sieciowego.

4. Wpisz adres URL serwera statystyk w polu tekstowym Set The Intranet Statistics Server (Ustaw serwer statystyk intranetowych). Nie musi to być oddzielny serwer – w polu tym można podać adres serwera aktualizacji.
5. Kliknij OK. Po odświeżeniu tego obiektu zasad grupy systemu wykorzystujące Windows 2000 z dodatkiem Service Pack 3 lub późniejszym, Windows XP z dodatkiem Service Pack 1 lub późniejszym, Windows Server 2003, Windows Vista, oraz Windows Server 2008 będą sprawdzały dostępność aktualizacji na wskazanym serwerze. Zalecane jest dokładne monitorowanie serwerów aktualizacji i statystyk przez kilka dni lub tygodni w celu upewnienia się, że mechanizm funkcjonuje zgodnie z zamierzeniami.