Microsoft®

Active Directory®
Windows® Server® 2008

Resource Kit

Stan Reimer, Conan Kezema,
Mike Mulcare i Byron Wright
oraz Microsoft Active Directory Team

Active Directory® Windows® Server® 2008 Resource Kit
Edycja polska Microsoft Press
Original English language edition © 2008 by Stan Reimer and Mike Mulcare
Tytuł oryginału: Windows® Server® 2008 Active Directory® Resource Kit

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) 355-16-00; fax (022) 355-16-99
e-mail: mspress@promise.pl

Wszystkie prawa zastrzeżone. Żadna część niniejszej książki nie może być powielana ani rozpowszechniana w jakiejkolwiek 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, ActiveX, Internet Explorer, MSDN, Outlook, SQL Server, Visual Basic, Visual Studio, Windows, Windows Media, 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 jakiejkolwiek 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 rękojmi ani gwarancji.
APN PROMISE Sp. z o.o. nie jest w żadnym wypadku odpowiedzialna za jakiekolwiek szkody będące następstwem korzystania z informacji zawartych w niniejszej publikacji, nawet jeśli APN PROMISE została powiadomiona o możliwości wystąpienia szkód.

ISBN: 978-83-7541-031-0

Przekład: Leszek Biolik,
Arkadiusz Czajkowski, Andrzej Bańkowski,
Dominik Daniewski, Bartłomiej Ożóg
Redakcja: Marek Włodarz
Korekta: Ewa Swędrowska
Skład i łamanie: MAWart Marek Włodarz

Spis treści

Podziękowania xv

Wstęp xvii

Omówienie książki xviii
Konwencje używane w tekście xx
Korzystanie z obrazu dysku CD xxii
Wyszukiwanie dodatkowych informacji w trybie online xxiii
Pomoc techniczna dla zbioru Resource Kit xxiv

Część I Omówienie usługi Windows Server 2008 Active Directory

1 Nowości w usłudze Active Directory dla systemu Windows Server 2008 3

Nowości w usługach AD DS (Active Directory Domain Services) 3
Kontrolery RODC (Read-Only Domain Controllers) 3
Inspekcja usług AD DS (Active Directory Domain Services) 6
Dokładne zasady haseł 7
Możliwość ponownego uruchamiania usług AD DS (Active Directory Domain Services) 9
Narzędzie instalowania bazy danych 10
Udoskonalenia interfejsu użytkownika 10
Dodatkowe role usług Active Directory Service 12
Rola AD CS (Active Directory Certificate Services) 12
Rola AD FS (Active Directory Federation Services) 14
Rola AD LDS (Active Directory Lightweight Directory Services) 16
Rola AD RMS (Active Directory Rights Management Services) 17
Podsumowanie 19

2 Składniki usług AD DS 21

Struktura fizyczna usług AD DS 21
Magazyn danych katalogu 22
Kontrolery domeny 25
Serwery wykazu globalnego 25
Kontrolery domeny przeznaczone tylko do odczytu 28
Wzorce operacji 31
Transfer ról wzorców operacji 35
Schemat 35
Struktura logiczna usług AD DS 44
Partycje usług AD DS 45
Domeny 49

Lasy ... 53
Relacje zaufania ... 55
Lokacje ... 58
Jednostki organizacyjne ... 61
Podsumowanie ... 64
Źródła dodatkowe ... 64
Narzędzia ... 65
Zasoby znajdujące się na dysku CD ... 65
Powiązane tematy modułów Pomoc ... 65

3 Usługi AD DS i DNS ... 67

Integracja systemu DNS i usług AD DS ... 68
Rekordy zasobu lokalizacji usługi (SRV) ... 68
Rekordy SRV zarejestrowane przez kontrolery domen usług AD DS ... 70
Usługa lokalizacji DNS ... 73
Automatyczne pokrycie lokacji ... 76
Zintegrowane strefy usługi AD DS ... 80
Korzyści używania stref zintegrowanych z usługami AD DS ... 80
Domyślne partycje aplikacji dla DNS ... 81
Zarządzanie strefami zintegrowanymi z usługami AD DS ... 83
Integracja przestrzeni nazw DNS i domen usług AD DS ... 87
Delegowanie w systemie DNS ... 87
Usługa przesyłania dalej i wskazówki dotyczące serwerów głównych ... 89
Rozwiązywanie problemów związanych z integracją systemu DNS i usług AD DS ... 94
Rozwiązywanie problemów systemu DNS ... 94
Rozwiązywanie problemów związanych z rejestracją rekordu SRV ... 97
Podsumowanie ... 97
Porady praktyczne ... 98
Źródła dodatkowe ... 98
Informacje pokrewne ... 98
Narzędzia ... 99
Zasoby znajdujące się na dysku CD ... 100
Powiązane tematy modułów Pomoc ... 100

4 Replikacja usług AD DS ... 101

Model replikacji usług AD DS ... 102
Proces replikacji ... 103
Typy aktualizacji ... 103
Replikowanie zmian ... 105
Replikowanie katalogu SYSVOL ... 112
Replikacja wewnątrz lokacji i pomiędzy lokacjami ... 113
Replikacja wewnątrz lokacji ... 113
Replikacja pomiędzy lokacjami ... 115
Opóźnienie replikacji ... 116
Pilne replikacje ... 117

Generowanie topologii replikacji ... 117
KCC (Knowledge Consistency Checker) ... 118
Obiekty połączenia ... 119
Topologia replikacji wewnątrz lokacji ... 120
Replikacja wykazu globalnego ... 125
Topologia replikacji pomiędzy lokacjami ... 126
Kontrolery RODC a topologia replikacji ... 127
Konfigurowanie replikacji pomiędzy lokacjami ... 129
Tworzenie dodatkowych lokacji ... 130
Łącza lokacji ... 131
Mosty łączy lokacji ... 135
Protokoły transportu replikacji ... 136
Konfigurowanie serwerów czołowych ... 137
Rozwiązywanie problemów dotyczących replikacji ... 140
Proces rozwiązywania problemów awarii replikacji usług AD DS ... 140
Narzędzia przeznaczone do rozwiązywania problemów replikacji usług AD DS 142
Podsumowanie ... 145
Porady praktyczne ... 145
Źródła dodatkowe ... 146
Informacje pokrewne ... 146
Narzędzia ... 147
Zasoby znajdujące się na dysku CD ... 148
Powiązane tematy modułów Pomocy ... 148

Część II Projektowanie i implementacja usługi Windows Server 2008 Active Directory

5 Projektowanie struktury usług AD DS ... 151

Definiowanie wymagań usługi katalogowej ... 152
Definiowanie wymagań biznesowych i technicznych ... 153
Dokumentowanie aktualnego środowiska ... 158
Projektowanie struktury lasu ... 165
Projekt lasów i usług AD DS ... 165
Pojedynczy las lub wiele lasów ... 168
Projektowanie lasów dla bezpieczeństwa usług AD DS ... 170
Modele projektu lasu ... 172
Definiowanie własności lasu ... 175
Zasady kontroli zmian lasu ... 175
Projektowanie integracji wielu lasów ... 176
Projektowanie relacji zaufania pomiędzy lasami ... 176
Projektowanie integracji katalogu pomiędzy lasami ... 180
Projektowanie struktury domeny ... 181
Określanie liczby domen ... 183
Projektowanie domeny głównej lasu ... 185
Projektowanie hierarchii domeny ... 186
Drzewa domen i relacje zaufania ... 187

Zmiana hierarchii domen po zainstalowaniu ... 189
Definiowanie własności domeny ... 190
Projektowanie poziomów funkcjonalnych domeny i lasu ... 190
Funkcje włączane na poziomach funkcjonalnych domeny ... 190
Funkcje włączane na poziomach funkcjonalnych lasu ... 192
Implementowanie poziomu funkcjonalnego domeny i lasu ... 193
Projektowanie infrastruktury systemu DNS ... 194
Projektowanie przestrzeni nazw ... 194
Projektowanie struktury jednostki organizacyjnej ... 202
Jednostki organizacyjne a projekt usług AD DS ... 203
Projektowanie struktury jednostki organizacyjnej ... 204
Tworzenie projektu jednostek organizacyjnych ... 206
Projektowanie topologii lokacji ... 208
Projekt lokacji i usług AD DS ... 209
Projektowanie lokacji ... 209
Projekt replikacji ... 212
Projektowanie lokalizacji serwerów ... 217
Podsumowanie ... 226
Porady praktyczne ... 226
Źródła dodatkowe ... 227
Informacje pokrewne ... 227
Zasoby znajdujące się na dysku CD ... 228

6 Instalowanie usług AD DS ... 229

Wymagania wstępne instalowania usług AD DS ... 229
Wymagania dotyczące miejsca na dysku twardym ... 230
Połączenia sieci ... 231
DNS ... 232
Uprawnienia administracyjne ... 232
Kompatybilność systemu operacyjnego ... 233
Działanie opcji instalacji usług AD DS ... 234
Kreator zadań konfiguracji początkowej i dostosowywania serwera ... 234
Server Manager ... 235
Instalacja usług AD DS (Active Directory Domain Services) ... 236
Instalacja nienadzorowana ... 237
Używanie programu Active Directory Domain Services Installation Wizard ... 237
Konfiguracja instalacji ... 238
Nadanie nazwy domenie ... 239
Definiowanie poziomów funkcjonalnych systemu Windows Server 2008 ... 240
Dodatkowe opcje kontrolera domeny ... 245
Lokalizacja plików ... 246
Dokończenie instalacji ... 247
Sprawdzanie instalacji usług AD DS ... 248
Przeprowadzanie nienadzorowanej instalacji ... 249
Instalowanie z nośnika ... 250
Instalowanie kontrolerów RODC ... 251

Instalacja typu Server Core w systemie Window Server 2008 ... 252
Instalowanie kontrolera RODC ... 252
Usuwanie usług AD DS ... 253
Usuwanie dodatkowych kontrolerów domeny ... 254
Usuwanie ostatniego kontrolera domeny ... 255
Nienadzorowane usunięcie usług AD DS ... 256
Wymuszone usunięcie kontrolera domeny systemu Windows Server 2008 ... 256
Podsumowanie ... 257
Źródła dodatkowe ... 258
Informacje pokrewne ... 258
Narzędzia ... 259

7 Migracja do usług AD DS ... 261

Ścieżki migracji ... 262
Ścieżka migracji aktualizowania domeny ... 263
Restrukturyzacja domeny ... 264
Określanie ścieżki migracji ... 266
Aktualizowanie domeny ... 268
Aktualizowanie z systemu Windows 2000 Server i Windows Server 2003 ... 269
Restrukturyzacja domeny ... 271
Migracja pomiędzy lasami ... 272
Migracja wewnątrz lasu ... 280
Konfigurowanie relacji zaufania pomiędzy lasami ... 281
Podsumowanie ... 283
Porady praktyczne ... 283
Źródła dodatkowe ... 284
Informacje pokrewne ... 284
Narzędzia ... 285

Część III Administracja usługi Windows Server 2008 Active Directory

8 Zabezpieczenia usług AD DS ... 289

Podstawy zabezpieczeń usług AD DS ... 290
Podmioty zabezpieczeń ... 290
Listy kontroli dostępu ... 290
Żetony dostępu ... 294
Uwierzytelnienie ... 294
Autoryzacja ... 295
Zabezpieczenia protokołu Kerberos ... 296
Wprowadzenie do protokołu Kerberos ... 297
Uwierzytelnienie Kerberos ... 299
Delegowanie uwierzytelnienia ... 307
Konfigurowanie protokołu Kerberos w systemie Windows Server 2008 ... 310
Integracja z infrastrukturą klucza publicznego ... 311
Integracja za pomocą kart inteligentnych ... 314
Współpraca z innymi systemami Kerberos ... 315

Rozwiązywanie problemów protokołu Kerberos ... 316
Uwierzytelnienie NTLM ... 320
Implementacja zabezpieczeń kontrolerów domeny ... 323
Ograniczanie możliwości ataków na kontrolery domeny ... 323
Konfigurowanie domyślnej zasady kontrolerów domeny ... 326
Konfigurowanie narzędzia SYSKEY ... 337
Zalecenia praktyczne dotyczące administrowania zabezpieczeniami ... 337
Podsumowanie ... 340
Porady praktyczne ... 341
Źródła dodatkowe ... 341
Informacje pokrewne ... 341
Narzędzia ... 342
Zasoby znajdujące się na dysku CD ... 343
Powiązane tematy modułów Pomocy ... 343

9 Delegowanie administracji usług AD DS ... 345

Zadania administracyjne usług Active Directory ... 346
Uzyskiwanie dostępu do obiektów usług Active Directory ... 347
Sprawdzenie wpisów ACE (zezwalaj i odmów) w liście DACL ... 348
Uprawnienia obiektu usługi Active Directory ... 349
Uprawnienia standardowe ... 350
Uprawnienia specjalne ... 352
Dziedziczenie uprawnień ... 357
Uprawnienia czynne ... 361
Własność obiektów usług Active Directory ... 364
Delegowanie zadań administracyjnych ... 366
Inspekcja użycia uprawnień administracyjnych ... 370
Konfigurowanie zasady inspekcji dla kontrolerów domeny ... 370
Konfigurowanie inspekcji dla obiektów usług Active Directory ... 373
Narzędzia delegowania administracji ... 375
Dostosowywanie konsoli MMC (Microsoft Management Console) ... 376
Planowanie delegowania administracji ... 377
Podsumowanie ... 378
Źródła dodatkowe ... 378
Informacje pokrewne ... 378

10 Zarządzanie obiektami usług Active Directory ... 381

Zarządzanie użytkownikami ... 381
Obiekty użytkowników ... 382
Obiekt inetOrgPerson ... 388
Obiekty kontaktów ... 389
Konta usług ... 390
Zarządzanie grupami ... 390
Typy grup ... 391
Zakres grupy ... 392
Grupy domyślne w usłudze Active Directory ... 396

Tożsamości specjalne ... 399
Projektowanie grup zabezpieczeń ... 399
Zarządzanie komputerami ... 402
Zarządzanie obiektami drukarek ... 405
Publikowanie drukarek w usługach Active Directory ... 405
Śledzenie lokalizacji drukarek ... 408
Zarządzanie opublikowanymi folderami udostępnionymi ... 410
Automatyzacja zarządzania obiektami usług Active Directory ... 411
Narzędzia wiersza polecenia dotyczące zarządzania usługą Active Directory ... 412
Stosowanie narzędzi LDIFDE i CSVDE ... 413
Korzystanie z języka VBScript do zarządzania obiektami usług Active Directory ... 415
Podsumowanie ... 421
Porady praktyczne ... 422
Źródła dodatkowe ... 423
Informacje pokrewne ... 423
Narzędzia ... 424
Zasoby znajdujące się na dysku CD ... 424

11 Omówienie zasad grupy ... 425

Przegląd zasad grupy ... 426
Działanie zasad grupy ... 428
Nowości zasad grupy w systemie Windows Server 2008 ... 430
Składniki zasad grupy ... 432
Kontener zasad grupy GPC ... 432
Składniki szablonu zasad grupy ... 434
Replikacja składników obiektu zasad grupy ... 436
Przetwarzanie zasad grupy ... 436
Sposób przetwarzania obiektów GPO przez systemy klienckie ... 437
Początkowe przetwarzanie obiektu GPO ... 440
Odświeżanie w tle obiektów GPO ... 442
Historia GPO a odświeżanie zasad grupy ... 443
Wyjątki dotyczące domyślnych interwałów przetwarzania ... 444
Implementowanie zasad grupy ... 450
Omówienie konsoli GPMC ... 451
Używanie konsoli GPMC do tworzenia obiektów GPO i tworzenia połączeń tych obiektów ... 452
Modyfikowanie zakresu przetwarzania obiektu GPO ... 454
Delegowanie administracji obiektów GPO ... 463
Implementowanie zasad grupy pomiędzy domenami i lasami ... 465
Zarządzanie obiektami zasad grupy ... 466
Tworzenie kopii zapasowych i przywracanie obiektów GPO ... 466
Kopiowanie obiektów zasad grupy ... 468
Importowanie ustawień obiektu zasad grupy ... 469
Modelowanie i raportowanie wyników zasad grupy ... 469
Tworzenie skryptów zarządzania zasadami grupy ... 474

Planowanie implementacji zasad grupy ... 479
Rozwiązywanie problemów zasad grupy ... 480
Podsumowanie ... 482
Źródła dodatkowe ... 482
Informacje pokrewne ... 482

12 Zarządzanie pulpitem użytkownika za pomocą zasad grupy ... 485

Zarządzanie pulpitem przy użyciu zasad grupy ... 487
Zarządzanie danymi użytkowników i ustawieniami profilu ... 490
Zarządzanie profilami użytkowników ... 490
Zarządzanie mobilnymi profilami użytkowników za pomocą zasad grupy ... 497
Przekierowanie folderu ... 502
Szablony administracyjne ... 511
Działanie plików szablonów administracyjnych ... 512
Zarządzanie plikami szablonów odnoszących się do domeny ... 515
Zalecane działania dotyczące zarządzania plikami szablonów ADMX ... 516
Używanie skryptów do zarządzania środowiskiem użytkownika ... 518
Instalowanie oprogramowania przy użyciu zasad grupy ... 520
Technologia Windows Installer ... 520
Instalowanie aplikacji ... 521
Używanie zasad grupy do dystrybucji aplikacji, które nie są instalowane za pomocą technologii Windows ... 525
Konfigurowanie właściwości pakietów oprogramowania ... 526
Stosowanie zasad grupy do konfigurowania programu Windows Installer ... 534
Planowanie instalacji oprogramowania przy użyciu zasad grupy ... 537
Ograniczenia w korzystaniu z zasad grupy do zarządzania oprogramowaniem 538
Omówienie funkcji preferencji zasad grupy ... 540
Preferencje zasad grupy w porównaniu do ustawień zasad ... 540
Ustawienia preferencji zasad grupy ... 541
Opcje preferencji zasad grupy ... 544
Podsumowanie ... 547
Źródła dodatkowe ... 547
Informacje pokrewne ... 548
Zasoby znajdujące się na dysku CD ... 548

13 Korzystanie z zasad grupy do zarządzania zabezpieczeniami ... 549

Konfigurowanie zabezpieczeń domeny za pomocą zasad grupy ... 550
Omówienie domyślnej zasady domeny ... 550
Omówienie domyślnej zasady kontrolerów domen ... 556
Ponowne tworzenie domyślnych obiektów GPO dla domeny ... 566
Szczegółowe zasady haseł ... 567
Wprowadzanie zasad ograniczeń oprogramowania przy użyciu zasad grupy ... 574
Zasady ograniczeń oprogramowania ... 576
Konfigurowanie zabezpieczeń sieci za pomocą zasad grupy ... 580
Konfigurowanie zabezpieczeń sieci przewodowych ... 582
Konfigurowanie zabezpieczeń sieci bezprzewodowych ... 584

Konfigurowanie zasad zapory systemu Windows i zabezpieczeń IPsec 584
Konfigurowanie ustawień zabezpieczeń za pomocą szablonów 587
Instalowanie szablonów zabezpieczeń 588
Podsumowanie 591
Źródła dodatkowe 592
Informacje pokrewne 592

Część IV Konserwacja usługi Windows Server 2008 Active Directory

14 Monitorowanie i konserwacja usług Active Directory 595

Monitorowanie usług Active Directory 595
Uzasadnienie monitorowania usług Active Directory 597
Monitorowanie wydajności i niezawodności serwera 598
Metody monitorowania usług Active Directory 606
Obszary monitorowania 615
Monitorowanie replikacji 617
Konserwacja bazy danych usług Active Directory 619
Usuwanie zbędnych elementów 619
Defragmentacja w trybie online 621
Defragmentacja w trybie offline bazy danych usług Active Directory 622
Zarządzanie bazą danych usług Active Directory przy użyciu narzędzia Ntdsutil 623
Podsumowanie 625
Źródła dodatkowe 626
Informacje pokrewne 626

15 Przywracanie usługi Active Directory po awarii 627

Planowanie operacji przywracania po awarii 628
Magazyn danych usług Active Directory 629
Tworzenie kopii zapasowej usługi Active Directory 631
Potrzeba tworzenia kopii zapasowych 633
Czas istnienia obiektów reliktowych 634
Częstotliwość tworzenia kopii zapasowych 635
Przywracanie usługi Active Directory 635
Przywracanie usługi Active Directory poprzez utworzenie nowego kontrolera domeny 636
Wykonywanie nieautorytatywnego przywracania usługi Active Directory 639
Przeprowadzanie autorytatywnego przywracania usługi Active Directory 643
Przywracanie członkostwa grupy 646
Reanimacja obiektów reliktowych 650
Korzystanie z narzędzia instalowania bazy danych usługi Active Directory 652
Przywracanie informacji folderu SYSVOL 655
Przywracanie serwerów wzorców operacji i wykazu globalnego 656
Podsumowanie 659
Porady praktyczne 659
Źródła dodatkowe 660

Informacje pokrewne ... 660
Narzędzia ... 661

Część V Zarządzanie tożsamościami i dostępem za pomocą usługi Active Directory

16 Usługi AD LDS ... 665

Omówienie usług AD LDS ... 665
Cechy usług AD LDS ... 666
Scenariusze instalowania usług AD LDS ... 666
Architektura i składniki usług AD LDS ... 668
Serwery usług AD LDS ... 668
Instancje usług AD LDS ... 670
Partycje katalogu ... 671
Replikacja usług AD LDS ... 676
AD LDS Security ... 680
Implementacja usług AD LDS ... 687
Konfigurowanie instancji i partycji aplikacji ... 687
Narzędzia zarządzania usługami AD LDS ... 690
Konfigurowanie replikacji ... 696
Tworzenie kopii zapasowych i przywracanie usług AD LDS ... 699
Konfigurowanie synchronizacji usług AD DS i AD LDS ... 703
Podsumowanie ... 706
Porady praktyczne ... 706
Źródła dodatkowe ... 706
Narzędzia ... 707
Zasoby znajdujące się na dysku CD ... 707
Pokrewne tematy pomocy ... 707

17 Usługi Active Directory Certificate Services ... 709

Omówienie usług AD CS (Active Directory Certificate Services) ... 709
Składniki infrastruktury klucza publicznego ... 710
Urzędy certyfikacji ... 716
Scenariusze instalacji usług certyfikatów ... 718
Implementowanie usług AD CS ... 719
Instalowanie głównych urzędów certyfikacji usług AD CS ... 719
Instalowanie podrzędnych urzędów certyfikacji usług AD CS ... 722
Konfigurowanie rejestrowania w sieci Web ... 722
Konfigurowanie odwoływania certyfikatów ... 723
Zarządzanie archiwizacją i odzyskiwanie kluczy ... 730
Zarządzanie certyfikatami w usługach AD CS ... 734
Konfigurowanie szablonów certyfikatów ... 734
Konfigurowanie automatycznej rejestracji certyfikatów ... 739
Zarządzanie akceptowaniem certyfikatu za pomocą zasad grupy ... 741
Konfigurowanie mobilnego dostępu do poświadczeń ... 742
Projektowanie implementacji usług AD CS ... 744

Projektowanie hierarchii urzędu certyfikacji ... 744
Projektowanie szablonów certyfikatów ... 747
Projektowanie dystrybucji i odwoływania certyfikatu ... 749
Podsumowanie ... 750
Porady praktyczne ... 751
Źródła dodatkowe ... 751
Informacje pokrewne ... 751
Narzędzia ... 752

18 Usługi Active Directory Rights Management Services ... 753

Omówienie usług AD RMS ... 754
Funkcje usług AD RMS ... 754
Składniki usług AD RMS ... 756
Działanie usług AD RMS ... 759
Scenariusze instalowania usług AD RMS ... 763
Implementacja usług AD RMS ... 765
Analiza wstępna instalacji usług AD RMS ... 765
Instalowanie klastrów usług AD RMS ... 766
Konfigurowanie punktu połączenia usługi AD RMS ... 770
Praca z klientami usług AD RMS ... 771
Administracja usług AD RMS ... 776
Zarządzanie zasadami zaufania ... 777
Zarządzanie szablonami zasad uprawnień ... 783
Konfigurowanie zasad wykluczeń ... 789
Konfigurowanie zasad zabezpieczeń ... 789
Przeglądanie raportów ... 792
Podsumowanie ... 793
Źródła dodatkowe ... 793
Informacje pokrewne ... 793

19 Usługi Active Directory Federation Services ... 795

Omówienie usług AD FS ... 796
Federacja tożsamości ... 796
Usługi sieci Web ... 797
Składniki usług AD FS ... 799
Projekty wdrożenia usług AD FS ... 803
Implementacja usług AD FS ... 809
Wymagania instalacji usług AD FS ... 809
Implementowanie usług AD FS w projekcie Federation Web SSO ... 817
Konfigurowanie usługi federacyjnej partnera kont ... 824
Konfigurowanie składników usług AD FS partnera zasobów ... 833
Konfigurowanie usług AD FS dla aplikacji korzystających z żetonu systemu Windows NT ... 838
Implementowanie projektu Web SSO ... 840
Implementowanie projektu Federated Web SSO with Forest Trust ... 841
Podsumowanie ... 843

Porady praktyczne ... 843
Źródła dodatkowe ... 843
Zasoby znajdujące się na dysku CD ... 844
Pokrewne temat modułów Pomoc ... 844

Indeks ... 845

O autorach ... 882

Wymagania systemowe ... 884

Podziękowania

Stan Reimer (dla zespołu):

Przede wszystkim chciałbym podziękować współautorom za ich trud włożony w opracowanie tej książki. Kiedy po raz pierwszy zostałem poproszony o poprowadzenie tego projektu, zacząłem się rozglądać za odpowiednimi osobami, z którymi mógłbym napisać tę książkę – teraz widzę, że nie mogłem zebrać lepszego zespołu.

Po drugie, chciałbym podziękować ludziom z Microsoft Press. Ten zespół, wliczając w to Martina DelRe – dyrektora programowego, który tak usilnie nas przekonywał, aż zgodziliśmy się zrealizować ten projekt, Karen Szall i Maureen Zimmerman. Jestem przekonany, że wynikające z naszej winy problemy z zachowaniem harmonogramu powodowały u tych osób bóle głowy, ale wszyscy oni byli niezwykle pomocni i wspierali nas na każdym kroku. Maureen miała niezwykły talent przypominania nam bez zadręczania, by materiały były przygotowywane na czas.

Podziękowania kieruję do Boba Dean, korektora technicznego, za jego wartościowe komentarze. Produkcja książki była profesjonalnie obsługiwana przez firmę Custom Editorial Productions Inc. i Lindę Allen jako menedżera produktu, Cecilię Munzenmaier jako redaktora i wiele innych osób, którzy poświęcili wiele czasu, aby książka ta mogła powstać i musieli jeszcze długo pracować, kiedy my, autorzy, już mogliśmy się cieszyć z zakończenia zadania.

Zbiór Resource Kit nie powstałby bez sporej interakcji ze strony grup osób zajmujących się produktami firmy Microsoft, jak również ekspertów technicznych, takich jak Directory Services MVP. Wszystkie rozdziały tej książki zostały sprawdzone przez ekspertów, a wielu z nich opracowało treść ramek *Porady ekspertów*, *Sprawdzone w praktyce* czy *Zasada działania*, które uprzyjemniają czytanie tej książki. Wspomniane osoby to:

James McColl, Mike Stephens, Moon Majumdar, Judith Herman, Mark Gray, Linda Moore, Greg Robb, Barry Hartman, Christiane Soumahoro, Gautam Anand, Michael Hunter, Alain Lissoir, Yong Liang, David Hastie, Teoman Smith, Brian Lich, Matthew Rimer, David Fisher, Bob Drake, Rob Greene, Andrej Budja, Rob Lane, Gregoire Guetat, Donovan Follette, Pavan Kompelli, Sanjeev Balarajan, Fatih Colgar, Brian Desmond, Jose Luis Auricchio, Darol Timberlake, Peter Li, Elbio Abib, Ashish Sharma, Nick Pierson, Lu Zhao i Antonio Calomeni.

Conan Kezema:

Specjalne podziękowania kieruję do współautorów za ich ciężką pracę nad książką. Pragnę także podziękować Stanowi za stwarzane przez lata możliwości; jest wspaniałym przyjacielem i mentorem.

Wstęp

Zapraszamy do zapoznania się z książką *Windows Server 2008 Active Directory Resource Kit*, kompletnym źródłem informacji potrzebnych do zaprojektowania i zaimplementowania usługi Active Directory w systemie Windows Server 2008.

Książka *Windows Server 2008 Active Directory Resource Kit* jest pełnym źródłem informacji technicznych dotyczących planowania, instalowania, utrzymywania i rozwiązywania problemów infrastruktury usługi Active Directory w systemie Windows Server 2008. Chociaż książka ta przeznaczona jest dla doświadczonych pracowników działów IT organizacji średniej i dużej wielkości, jest także wartościowym źródłem wiedzy dla każdego, kto chce poznać metody implementacji i zarządzania usługą Active Directory w systemie Windows Server 2008.

Nowa zmiana w usłudze Windows Server 2008 Active Directory polega na tym, że obecnie pojęcie *Active Directory* obejmuje dużo większy obszar, niż było to w poprzedniej wersji usługi katalogowej. To co poprzednio nazywane było usługą Active Directory w systemie Windows 2000 i Windows Server 2003, obecnie jest nazywane usługami AD DS (Active Directory Domain Services), a pojęcie Active Directory obejmuje teraz szereg dodatkowych składników usługi katalogowej. Składniki te to usługi AD LDS (Active Directory Lightweight Directory Services), AD CS (Active Directory Certificate Services), AD RMS (Active Directory Rights Management Services) i AD FS (Active Directory Federation Services).

W zbiorze Resource Kit znaleźć można szczegółowe informacje techniczne opisujące działanie usługi Active Directory w systemie Windows Server 2008. Ponadto zamieszczono poradniki dokładnie opisujące zadania związane z implementacją i utrzymaniem infrastruktury usługi Active Directory. W wielu ramkach informacyjnych tej książki – opracowanych przez członków zespołów produktu Active Directory, ekspertów firmy Microsoft i MVP w dziedzinie usług katalogowych – przedstawiono wnikliwą analizę działania usługi Active Directory, praktyczne porady dotyczące projektowania i implementacji usługi Active Direktory oraz nieocenione wskazówki dotyczące rozwiązywania problemów. Ponadto na dołączonym do książki dysku CD zapisane zostały narzędzia instalowania, szablony i wiele przykładowych skryptów, które mogą być używane i dostosowywane w celu zautomatyzowania różnych aspektów zarządzania usługą Active Directory w środowiskach przedsiębiorstw.

Omówienie książki

Niniejsza książka została podzielona na pięć części, które zawierają następujące rozdziały:

Część I – Omówienie usługi Windows Server 2008 Active Directory

- **Rozdział 1 – „Nowości w usłudze Active Directory dla systemu Windows Server 2008"** W rozdziale zamieszczono przegląd nowych funkcji udostępnionych w systemie Windows Server 2008. Jeśli Czytelnik zna usługę Windows Server 2003 Active Directory, w tym miejscu znajdzie krótki przegląd nowego materiału umieszczonego w prezentowanej książce.
- **Rozdział 2 – „Składniki usługi AD DS"** Rozdział stanowi przegląd usług AD DS (Active Directory Domain Services) – jeśli Czytelnik słabo zna usługę Active Directory, warto by rozpoczął od tego rozdziału, zapoznając się z pojęciami i koncepcją budowy usług AD DS.
- **Rozdział 3 – „Usługi AD DS i DNS"** Jednym z najważniejszych składników potrzebnych do sprawnego działania usług AD DS jest prawidłowo zaimplementowana infrastruktura systemu DNS. W rozdziale zamieszczono informacje, w jaki sposób można zrealizować to zadanie.
- **Rozdział 4 – „Replikacja usług AD DS"** Aby korzystać z usług AD DS, należy zrozumieć działanie replikacji. W rozdziale znajdują się wszystkie szczegółowe informacje na temat działania i konfigurowania replikacji usług AD DS.

Część II – Projektowanie i implementacja usługi Windows Server 2008 Active Directory

- **Rozdział 5 – „Projektowanie struktury usługi AD DS"** Przed wdrożeniem usług AD DS należy utworzyć projekt spełniający wymagania danej organizacji. W rozdziale zamieszczono szczegółowe informacje potrzebne do przeprowadzenia procesu planowania.
- **Rozdział 6 – „Instalowanie usługi AD DS"** Instalowanie usług AD DS w systemie Windows Server 2008 jest dość proste, ale instalację można przeprowadzać różnymi sposobami. W rozdziale opisano wszystkie opcje i powody, dla których poszczególne z nich są wybierane.
- **Rozdział 7 – „Migracja usługi AD DS"** W wielu organizacjach jest wykorzystywana poprzednia wersja usługi Active Directory. W rozdziale przedstawiono, w jaki sposób w takim środowisku instalować kontrolery domeny systemu Windows Server 2008 oraz w jaki sposób przeprowadzić migrację środowiska usługi Active Directory do systemu Windows Server 2008.

Część III – Administracja usługi Windows Server 2008 Active Directory

- **Rozdział 8 – „Bezpieczeństwo usługi AD DS"** W wielu organizacjach podstawowe usługi dotyczące uwierzytelniania i autoryzacji w sieci udostępniane są przez usługi AD DS. W rozdziale opisano sposób działania zabezpieczeń usług AD DS oraz operacje, jakie należy przedsięwziąć, aby zabezpieczyć środowisko usług AD DS.
- **Rozdział 9 – „Delegowanie administracji usługi AD DS"** Jedną z opcji instalacji usług AD DS jest możliwość delegowania wielu zadań administracyjnych do innych administratorów bez konieczności przydzielania im uprawnień na poziomie domeny. W rozdziale omówiono działanie uprawnień w usługach AD DS oraz sposób ich przekazywania.
- **Rozdział 10 – „Zarządzanie obiektami usługi Active Directory"** Administrator usług AD DS największą cześć czasu poświęca zarządzaniu obiektów usługi AD DS, takich jak użytkownicy, grupy i jednostki organizacyjne. W rozdziale omówiono sposoby zarządzania poszczególnymi obiektami, ale także opisane zostały sposoby zarządzania dużą liczbą obiektów przy użyciu skryptów.
- **Rozdział 11 – „Omówienie zasad grupy"** Centralnym składnikiem systemu zarządzania siecią Windows Server 2008 są zasady grupy (Group Policy). Za pomocą zasad grupy można zarządzać wieloma ustawieniami pulpitu, jak również można konfigurować zabezpieczenia. Rozdział rozpoczyna się od wyjaśnienia, czym są obiekty zasad grupy, a następnie przedstawione zostają sposoby stosowania i filtrowania tych obiektów.
- **Rozdział 12 – „Zarządzanie pulpitem użytkownika za pomocą zasad grupy"** Jednym z ważniejszych zadań wykonywanych przez administratora za pomocą zasad grupy jest konfigurowanie pulpitów użytkowników. W systemie Windows Server 2008 i Windows Vista istnieje kilka tysięcy ustawień zasad grupy. W rozdziale przedstawiono sposoby stosowania zasad, a także wskazano, które zasady są najważniejsze.
- **Rozdział 13 – „Zarządzanie zabezpieczeniami za pomocą zasad grupy"** Innym ważnym zadaniem wykonywanym za pomocą zasad grupy jest stosowanie ustawień zabezpieczeń. Dotyczy to ustawień stosowanych do wszystkich użytkowników i komputerów w domenie, jak również ustawień stosowanych do poszczególnych komputerów lub użytkowników. W rozdziale zamieszczono dokładne informacje na temat sposobów konfigurowania zabezpieczeń za pomocą zasad grupy.

Część IV – Konserwacja usługi Windows Server 2008 Active Directory

- **Rozdział 14 – „Monitorowanie i konserwacja usługi Active Directory"** W rozdziale znajdują się informacje dotyczące zadań związanych z utrzymaniem infrastruktury usługi Active Directory po jej zainstalowaniu, takie jak monitorowanie środowiska usług AD DS czy metody konserwacji kontrolerów domen usług AD DS.
- **Rozdział 15 – „Przywracanie po awarii usługi Active Directory"** Ponieważ w wielu korporacjach usługi AD DS pełnią centralną rolę, dla administratora istotna jest wiedza, w jaki sposób przygotować się na awarie i w jaki sposób przywracać systemy w środowisku usług AD DS. Tematyka ta jest przedmiotem rozdziału 15.

Część V – Zarządzanie tożsamością i dostępem za pomocą usługi Active Directory

- **Rozdział 16 – „Usługi AD LDS"** Usługi AD LDS są nową rolą serwera, która ujęta została w systemie Windows Server 2008 w obszarze usługi Active Directory. Usługi AD LDS zostały tak zaprojektowane, by stanowić katalog aplikacji – omawiany rozdział opisuje, w jaki sposób można instalować i zarządzać środowiskiem usługi AD LDS.
- **Rozdział 17 – „Usługi AD CS"** Usługi AD CS stanowią infrastrukturę klucza publicznego udostępniającą certyfikaty cyfrowe, które są bardzo istotne dla wielu implementacji zabezpieczeń sieci. W rozdziale przedstawiono sposoby planowania i implementacji usług AD CS.
- **Rozdział 18 – „Usługi AD RMS"** Usługi AD RMS udostępniają narzędzia stosowania trwałych zasad dotyczących informacji, które to zasady pozostają dołączone do informacji, nawet jeśli są one przenoszone w obrębie organizacji lub poza nią. W rozdziale opisano sposoby implementacji usług AD RMS.
- **Rozdział 19 – „Usługi AD FS"** Usługi AD FS umożliwiają użytkownikom dostęp do wielu aplikacji opartych na sieci Web w swojej organizacji i poza nią za pomocą jednokrotnego uwierzytelnienia. W rozdziale omówiono scenariusze instalacji usług AD FS i sposoby ich implementacji.

Konwencje używane w tekście

Poniżej wymieniono symbole graficzne i konwencje tekstowe, które wyróżniają ważne informacje, funkcje i sposób użycia:

Notki ostrzegawcze

Poniższe symbole używane są w całej książce w celu zwrócenia uwagi na przydatne informacje:

Ikona	Notka	Znaczenie
	**Uwaga**	Podkreślenie ważności danego pojęcia lub wyróżnienie specjalnych przypadków, które nie muszą mieć zastosowania w każdej sytuacji.
	**Ważne**	Zwrócenie uwagi na istotne informacje, które nie powinny zostać pominięte.
	**Ostrzeżenie**	Ostrzeżenie o możliwości awarii lub unikaniu określonych czynności, które mogą spowodować poważne problemy dla użytkowników, systemów, integralności danych itp.
	**Na dysku CD**	Symbol zwraca uwagę na powiązany z tekstem skrypt, narzędzie, szablon lub pomoce zamieszczone na dysku CD, które ułatwiają wykonanie zadań opisanych w tekście.

Ikona	Notka	Znaczenie
	**Dodatkowe informacje**	Symbole wskazuje witryny sieci Web lub inne materiały, w których znajdują się informacje dodatkowe, dotyczące tematów opisywanych w tekście.
	**Alert zabezpieczeń**	Podkreślenie informacji lub zadań, które są istotne dla utrzymania bezpiecznego środowiska lub zidentyfikowania zdarzeń wskazujących na potencjalne zagrożenia.

Ramki

W książce można spotkać ramki zawierające spostrzeżenia, wskazówki i porady praktyczne dotyczące usługi Windows Server 2008 Active Directory:

Ramka	Znaczenie
Porady ekspertów	Teksty opracowane przez ekspertów firmy Microsoft w celu zaprezentowania punktu widzenia „najbliższego źródła" poprzez przekazanie spostrzeżeń na temat działania usługi Active Directory w systemie Windows Server 2008, zaleceń praktycznych dotyczących planowania i implementacji ról serwera usługi Active Directory oraz wskazówek dotyczących rozwiązywania problemów.
Sprawdzone w praktyce	Teksty opracowane przez specjalistów MVP w zakresie usługi katalogowej w celu udostępnienia najlepszych rozwiązań praktycznych związanych z planowaniem i implementacją usługi Active Directory oraz w celu przekazania wskazówek dotyczących rozwiązywania problemów.
Zasada działania	Krótkie spojrzenie na funkcje usługi Windows Server 2008 Active Directory i ich działanie.

Przykłady wiersza polecenia

Poniżej przedstawiono konwencję używaną w książce do prezentowania przykładów działania narzędzi wiersza polecenia:

Styl	Znaczenie
czcionka wytłuszczona	Czcionka używana do zaznaczenia poleceń wprowadzanych przez użytkownika (znaki należy wprowadzać tak, jak są przedstawione).
kursywa	Czcionka używana do określania zmiennych, za które należy podstawiać konkretne wartości (na przykład ***filename*** może odnosić się do dowolnej poprawnej nazwy pliku).
`czcionka stałopozycyjna`	Czcionka o stałej szerokości używana jest w przykładach kodów i danych wyjściowych okna wiersza polecenia.
%SystemRoot%	Składnia używana dla zmiennych środowiskowych.

Korzystanie z obrazu dysku CD

Obraz dysku CD towarzyszącego książce jest dostępny na stronie wydawcy przy opisie książki w zakładce Dodatkowe informacje, pod adresem:

http://www.ksiazki.promise.pl/aspx/produkt.aspx?pid=47323

Na podstawie tego obrazu można wykonać fizyczny dysk CD lub zainstalować go jako napęd wirtualny. Wiele narzędzi i zasobów opisywanych w rozdziałach zostało zamieszczonych na tym dysku; dostęp do innych narzędzi i zasobów można uzyskać za pośrednictwem odnośników zapisanych na dysku CD. Plik Readme.txt zawiera opis strukturę tego dysku CD.

Skrypty zarządzania

Na dysku CD dołączony został zestaw skryptów umożliwiających zarządzanie usługą Active Directory. Oprócz tych skryptów dołączone zostały również skrypty pozwalające na uzyskanie informacji o obiektach usługi Active Directory i skrypty umożliwiające tworzenie i modyfikowanie tych obiektów. Do uruchamiania skryptów potrzebna jest powłoka Windows PowerShell. Poniżej wymienione zostały skrypty dołączone do dysku CD:

- **AddUserToGroup.ps1** Dodawanie konta użytkownika do grupy w tej samej jednostce organizacyjnej.
- **CreateAndEnableUserFromCSV.ps1** Tworzenie włączonego konta użytkownika poprzez odczytanie pliku csv.
- **CreateGroup.ps1** Tworzenie grupy w usłudze Active Directory w określonej jednostce organizacyjnej i domenie.
- **CreateObjectInAD.ps1** Tworzenie obiektu usługi Active Directory.
- **CreateOU.ps1** Tworzenie jednostki organizacyjnej w usłudze Active Directory.
- **CreateUser.ps1** Tworzenie konta użytkownika w usłudze Active Directory.
- **EnableDisableUserSetPassword.ps1** Włączenie lub wyłączenie konta użytkownika i ustawienie hasła.
- **GetDomainPwdSettings.ps1** Uzyskanie ustawień zasady haseł dla domeny.
- **GetModifiedDateFromAD.ps1** Wyświetlenie ostatnio zmodyfikowanych danych określonego użytkownika w lokalnej lub zdalnej domenie.
- **ListUserLastLogon.ps1** Wyświetlenie ostatniej daty logowania określonego użytkownika w lokalnej lub zdalnej domenie.
- **LocateDisabledUsers.ps1** Zlokalizowanie wyłączonych kont użytkowników w lokalnej lub zdalnej domenie.
- **LocateLockedOutUsers.ps1** Zlokalizowanie zablokowanych kont użytkowników w lokalnej lub zdalnej domenie.
- **LocateOldComputersNotLogon.ps1** Zlokalizowanie kont komputerów lokalnej lub zdalnej domeny, które nie logowały się przez określoną liczbę dni.

- **LocateOldUsersNotLogOn.ps1** Wyszukanie w lokalnej lub zdalnej domenie kont użytkowników, które nie były zalogowane w domenie przez dłuższy okres czasu, określony przez wyspecyfikowaną liczbę dni.
- **ModifyUser.ps1** Modyfikowanie atrybutów użytkownika usługi Active Directory.
- **QueryAD.ps1** Kwerenda w usłudze Active Directory dotycząca obiektów, takich jak użytkownicy, grupy, komputery itp.
- **UnlockLockedOutUsers.ps1** Odblokowanie aktualnie zablokowanych kont użytkowników.

Oprócz odniesień do tych skryptów w wielu rozdziałach zamieszczone są odniesienia do dodatkowych skryptów, wykonujących zadania zarządzania opisywane w danym rozdziale.

W pliku Readme.txt znaleźć można pełny opis zawartości i struktury dysku CD dołączonego do książki.

Korzystanie ze skryptów

Na dołączonym do książki dysku CD znajdują się skrypty napisane za pomocą narzędzia VBScript (rozszerzenie pliku vbs) i Windows PowerShell (rozszerzenie pliku ps1).

Skrypty VBScript identyfikowane są poprzez rozszerzenie vbs. W celu uruchomienia tych skryptów należy dwukrotnie kliknąć skrypt lub wykonać go bezpośrednio w wierszu polecenia.

Skrypty Windows PowerShell wymagają zainstalowania powłoki Windows PowerShell i skonfigurowania jej tak, aby uruchamiane były niepodpisane skrypty. Skrypty powłoki Windows PowerShell można uruchamiać w systemie Windows XP SP2, Windows Server 2003 SP1, Windows Vista lub Windows Server 2008. Aby skrypty mogły działać, wszystkie komputery muszą należeć do domeny systemu Windows Server 2008.



Uwaga Informacje dotyczące wymagań systemowych związanych z uruchamianiem skryptów znajdujących się na dysku CD znaleźć można w części Wymagania systemowe na końcu książki.

Wyszukiwanie dodatkowych informacji w trybie online

Po opublikowaniu nowych bądź zaktualizowanych materiałów, będących uzupełnieniem niniejszej książki, można je będzie uzyskać w witrynie Microsoft Press Online Windows Server and Client Web. Bazując na finalnej wersji systemu Windows Server 2008 materiały te mogą dotyczyć aktualizacji treści książki, artykułów, odnośników, poprawek zauważonych błędów itp. Te witryny sieci Web będą wkrótce dostępne pod adresem *http://www.microsoft.com/learning/books/online/serverclient* i będą okresowo aktualizowane.

Pomoc techniczna dla zbioru Resource Kit

Dołożono wszelkich starań dla zapewnienia dokładności książki i zawartości na dołączonym dysku. Firma Microsoft Press wprowadza poprawki do książki za pośrednictwem witryny sieci Web pod adresem:

http://www.microsoft.com/learning/support/search.asp.

Wszelkie komentarze, pytania lub pomysły odnoszące się do tej książki lub zawartości dołączonego do niej dysku CD bądź odnoszące się do pytań, na które nie można znaleźć odpowiedzi w Bazie Wiedzy (Knowledge Base), prosimy kierować do wydawnictwa Microsoft Press, korzystając z jednej z poniższych metod:

E-mail:
rkinput@microsoft.com

Pocztą tradycyjną:
Microsoft Press
Attn: Windows Server 2008 Active Directory Resource Kit
One Microsoft Way
Redmond, WA 98052-6399

Prosimy zwrócić uwagę, że pod żadnym z wymienionych adresów nie jest udzielana pomoc techniczna. W celu uzyskania takiej pomocy należy odwiedzić witrynę Microsoft Product Support pod adresem: *http://support.microsoft.com*

Część I

Omówienie usługi Windows Server 2008 Active Directory

W tej części:

1 Nowości w usłudze Active Directory dla systemu Windows Server 2008 3
2 Składniki usług AD DS 21
3 Usługi AD DS i DNS 67
4 Replikacja usług AD DS 101

Rozdział 1

Nowości w usłudze Active Directory dla systemu Windows Server 2008

W tym rozdziale:

Nowości w usługach AD DS (Active Directory Domain Services) 3
Dodatkowe role usług Active Directory Service 12
Podsumowanie. 19

Nowości w usługach AD DS (Active Directory Domain Services)

Chociaż większość tematów potrzebnych do zarządzania domeną usługi Active Directory pozostaje taka sama, jak w poprzednich wersjach implementacji usługi katalogowej (w systemie Windows 2000 czy Windows Server 2003), kilka nowych i uzupełnionych funkcji umożliwia administratorowi większą kontrolę i zapewnienie lepszego bezpieczeństwa środowiska domeny. W niniejszym rozdziale omówiono ogólnie sześć nowych udoskonaleń usług AD DS (Active Directory Domain Service), jak również zaprezentowano cztery nowe role, które mogą spełniać w przedsiębiorstwie usługi Active Directory.

Kontrolery RODC (Read-Only Domain Controllers)

Jedną z nowych funkcji w systemie Windows Server 2008 jest możliwość instalowania kontrolerów domeny przeznaczonych tylko do odczytu (Read-Only Domain Controller – RODC). Tak jak sugeruje nazwa tego nowego typu kontrolera domeny, jego rola polega na utrzymywaniu partycji bazy danych usługi Active Directory przeznaczonej tylko do odczytu.

Kontroler RODC umożliwia organizacjom łatwiejsze instalowanie kontrolerów domeny w sytuacjach, gdzie nie można zagwarantować bezpieczeństwa fizycznego (na przykład w lokalizacjach biur oddziałowych), gdzie lokalny magazyn wszystkich haseł domeny stanowi główne miejsce zagrożenia (na przykład w roli określanej przez aplikację) lub jeśli kontroler używany jest w instalacji systemu Windows 2008 Server Core.

W organizacji, gdzie można zagwarantować fizyczne bezpieczeństwo oddziałowego kontrolera domeny, można również instalować kontrolery RODC, ponieważ zmniejszone

zostają wymagania związane z zarządzaniem poprzez udostępnienie takich funkcji, jak separacja roli administratora.

Ponieważ administracja kontrolera RODC może być delegowana do użytkownika domeny lub grupy zabezpieczeń, kontroler RODC dobrze nadaje się do lokacji, w których nie ma użytkowników należących do grupy Domain Admins (Administratorzy domeny). Poniżej wymienione zostały główne cechy kontrolerów RODC.

Baza danych usługi AD DS przeznaczona tylko do odczytu

Za wyjątkiem haseł kont kontroler RODC przechowuje większość obiektów i atrybutów usługi Active Directory przechowywanych na typowym (z możliwością zapisu) kontrolerze domeny. Nie istnieje jednak możliwość wprowadzania zmian w bazie danych przechowywanej na kontrolerze RODC. Zmiany muszą być wprowadzane na kontrolerze domeny z możliwością zapisu, a następnie muszą być replikowane do kontrolera RODC.

Aplikacje lokalne wymagające dostępu Read (Odczyt) do katalogu mogą uzyskać taki dostęp. Aplikacje LDAP (Lightweight Directory Application Protocol), które żądają dostępu Write (Zapis), odbiorą odpowiedź LDAP przeznaczoną do rozpatrzenia, która przekierowuje aplikację do kontrolera domeny z możliwością zapisu, zazwyczaj w lokacji centralnej.

Zestaw filtrowanych atrybutów kontrolera RODC

Do kontrolera RODC replikowane są tylko niektóre atrybuty. Zestaw atrybutów może być dynamicznie konfigurowany (zestaw filtrowanych atrybutów kontrolera RODC) tak, aby atrybuty zestawu nie były replikowane do kontrolera RODC. Atrybuty zdefiniowane w zestawie filtrowanych atrybutów kontrolera RODC nie będą replikowane do żadnego kontrolera RODC w lesie.

Złośliwy użytkownik, który uzyskał dostęp do kontrolera RODC, może próbować skonfigurować go w taki sposób, aby kontroler próbował replikować atrybuty zdefiniowane w zestawie filtrowanych atrybutów kontrolera RODC. Jeśli kontroler RODC próbuje replikować te atrybuty z kontrolera systemu Windows Server 2008, żądanie replikacji zostanie odrzucone. I dlatego, ze względów bezpieczeństwa, jeśli planowane jest konfigurowanie zestawu filtrowanych atrybutów kontrolera RODC, należy zapewnić, aby w lesie używany był poziom funkcjonalny systemu Windows Server 2008. Jeśli w lesie używany jest poziom funkcjonalny systemu Windows Server 2008, kontroler RODC, którego zabezpieczenia zostały złamane, nie może być w ten sposób wykorzystany, ponieważ w takim lesie nie są dopuszczone kontrolery domen działające pod kontrolą systemu Windows Server 2003.

Jednokierunkowa replikacja

Ponieważ bezpośrednio na kontrolerze RODC nie są zapisywane zmiany, to na tym kontrolerze zmiany nie są też generowane. I również kontrolery domeny z możliwością zapisu, które są partnerami replikacji, nie muszą pobierać zmian z kontrolerów RODC. Oznacza to, że jakiekolwiek zmiany lub uszkodzenia, które mogą być wykonane przez złośliwych użytkowników w lokacjach oddziałowych, nie mogą przenosić się z kontrolera RODC do pozostałych części lasu. Cecha ta zmniejsza również obciążenie serwerów czołowych w koncentratorze i nakłady związane z monitorowaniem replikacji.

Jednokierunkowa replikacja kontrolera RODC dotyczy zarówno replikacji usług AD DS, jak i replikacji systemu DFS (Distributed File System). Kontroler RODC przeprowadza zwykłą replikację przychodzącą dla zmian w usługach AD DS i replikacji systemu DFS.

Buforowanie poświadczeń

Buforowanie poświadczeń jest magazynem poświadczeń użytkownika lub komputera, wliczając w to hasła użytkownika wyrażone jako szereg kodowanych wartości. Domyślnie kontroler RODC nie przechowuje poświadczeń użytkownika lub komputera. Wyjątkiem jest konto komputera kontrolera RODC i specjalne (i unikalne) konto krbtgt, które istnieje na każdym kontrolerze RODC.

Buforowanie poświadczeń na kontrolerze RODC można konfigurować poprzez modyfikowanie zasady replikacji hasła (Password Replication Policy) dla określonego kontrolera domeny. Przykładowo, jeśli kontroler RODC ma buforować poświadczenia wszystkich użytkowników w biurze oddziału, którzy normalnie logują się w lokacji biura, to można dodać wszystkie konta użytkowników (użytkowników w biurze oddziału) do zasady replikacji hasła. W ten sposób użytkownicy będą mogli logować się do kontrolera domeny, nawet jeśli niedostępne jest połączenie sieci WAN (Wide Area Network) do kontrolera domeny z możliwością zapisu. Podobnie można dodać wszystkie konta komputerów biura oddziału tak, aby konta te mogły uwierzytelniać się w kontrolerze RODC, nawet jeśli nie działa łącze WAN. W obu poprzednich sytuacjach połączenie WAN do kontrolera domeny z możliwością zapisu musi być dostępne podczas pierwszego logowania dla wprowadzenia poświadczeń, które mają być buforowane na kontrolerze RODC.

Separacja roli administratora

Lokalne uprawnienia administracyjne dla kontrolera RODC mogą być delegowane do każdego użytkownika domeny bez przydzielania użytkownikowi praw do domeny czy innych kontrolerów domeny. Dzięki temu użytkownik oddziału lokalnego może logować się do kontrolera RODC i przeprowadzać konserwację serwera, na przykład aktualizację sterownika. Użytkownik oddziału nie może jednak logować się do dowolnego kontrolera domeny lub wykonywać innych zadań administracyjnych w domenie. W ten sposób możliwość efektywnego zarządzania kontrolerem RODC w biurze oddziału może być przekazana użytkownikowi tego biura bez ujawniania zabezpieczeń pozostałej domeny.

System DNS tylko do odczytu

Na kontrolerze RODC można zainstalować usługę DNS Server. Kontroler RODC może replikować wszystkie partycje katalogu aplikacji używane przez system DNS, wliczając w to ForestDNSZones i DomainDNSZones. Jeśli serwer DNS zostanie zainstalowany na kontrolerze RODC, klienci mogą przesyłać do niego zapytania dotyczące rozpoznawania nazw w taki sam sposób, jak pytania kierowane do innych serwerów DNS.

Serwer DNS na kontrolerze RODC jednak nie obsługuje bezpośrednio aktualizacji klienta. W konsekwencji kontroler RODC nie zarejestruje rekordów zasobu NS (nazwa serwera) dla żadnej przechowywanej strefy zintegrowanej z usługą Active Directory. Jeśli klient próbuje zaktualizować swój rekord DNS w kontrolerze RODC, serwer zwraca odpowiedź polecającą. Następnie klient może spróbować aktualizacji w serwerze DNS wskazanym w odpowiedzi polecającej. W tle, serwer DNS na kontrolerze RODC próbuje replikować

zaktualizowany rekord z serwera DNS, który przeprowadzał aktualizację. Takie żądanie replikacji dotyczy tylko pojedynczego obiektu (rekordu DNS). Całe listy zmienionych danych strefy lub domeny nie będą replikowane podczas tego specjalnego żądania replikacji pojedynczego obiektu. W celu zwiększenia bezpieczeństwa kontroler RODC w biurze oddziału musi rejestrować swoje rekordy DC (takie jak czas serwera, host ldap, host kdc itp.) w kontrolerze domeny systemu Windows Server 2008. Jeśli następnie zostaną złamane zabezpieczenia kontrolera RODC, nie będzie możliwości zmiany rekordów DNS i przedstawiać się będzie jako inny kontroler domeny lub ogłaszać się klientom poza ich własną lokacją.

Inspekcja usług AD DS (Active Directory Domain Services)

W celu lepszego zarządzania usługami AD DS w organizacji przydatna jest nie tylko wiedza o tym, które obiekty zostały zmodyfikowane, ale także informacje o bieżących i poprzednich wartościach. W poprzednich wersjach usług AD DS była tylko jedna zasada inspekcji: Inspekcja dostępu do usługi katalogowej. W systemie Windows Server 2008 są dodatkowe podkategorie inspekcji usługi katalogowej. Funkcja ta oferuje więcej informacji dotyczących rejestrowania zdarzeń zakończonych powodzeniem lub niepowodzeniem w usłudze AD DS. W systemie Windows Server 2008 zasada inspekcji dostępu do usługi katalogowej została podzielona na cztery podkategorie:

- Directory Service Access (Dostęp do usługi katalogowej)
- Directory Service Changes (Zmiany usługi katalogowej)
- Directory Service Replication (Replikacja usługi katalogowej)
- Detailed Directory Service Replication (Szczegóły replikacji usługi katalogowej)

Ta globalna zasada inspekcji jest domyślnie włączona w systemie Windows Server 2008. Podkategoria Directory Service Changes jest również domyślnie włączona i ustawiona na rejestrowanie jedynie zdarzeń zakończonych powodzeniem. Które operacje będą poddane inspekcji, można kontrolować poprzez modyfikowanie listy kontroli dostępu do systemu (SACL) dla odpowiednich obiektów usługi katalogowej. W celu przeprowadzenia inspekcji zmian usługi katalogowej obecnie dostępne są następujące możliwości:

- Jeśli wykonywana jest pomyślna operacja modyfikowania atrybutu obiektu, usługi AD DS rejestrują poprzednie i bieżące wartości atrybutu. Jeśli atrybut ma kilka wartości, rejestrowane są tylko wartości, które zostały zmodyfikowane wskutek tej operacji.
- Jeśli tworzony jest nowy obiekt, rejestrowane są wartości atrybutów, które zostały opublikowane w momencie tworzenia. Jeśli podczas operacji tworzenia dodawane są atrybuty, to rejestrowane są te nowe wartości atrybutu.
- Jeśli obiekt jest przenoszony wewnątrz domeny, rejestrowana jest poprzednia i nowa lokalizacja (w postaci nazwy wyróżniającej). Jeśli obiekt jest przenoszony do innej domeny, generowane jest zdarzenie dotyczące tworzenia na kontrolerze domeny w domenie docelowej.
- Jeśli obiekt jest przywracany po usunięciu, rejestrowana jest lokalizacja, do której obiekt jest przenoszony. Ponadto, jeśli podczas tej operacji są dodawane, modyfikowane lub usuwane atrybuty, to również rejestrowane są wartości tych atrybutów.



Uwaga Pomimo że globalna zasada inspekcji – Inspekcja dostępu do usługi katalogowej – jest włączana przy użyciu konsoli Group Policy Management (Zarządzanie zasadami grupy), to w systemie Windows Server 2008 nie jest dostępny interfejs GUI do przeglądania lub ustawiania podkategorii zasad inspekcji usługi AD DS. W tym celu należy korzystać z narzędzia wiersza polecenia Auditpol.exe. Informacje dodatkowe na temat używania narzędzia Auditpol.exe do włączania poszczególnych podkategorii znaleźć można w rozdziale 8 „Zabezpieczenia usług AD DS (Active Directory Domain Services)", jak również w poradniku „Windows Server 2008 Auditing AD DS Changes Step-by-Step Guide" dostępnym pod adresem *http://technet2.microsoft.com/windowsserver2008/en/library/a9c25483-89e2-4202-881c-ea8e02b4b2a51033.mspx?mfr=true*.

Dokładne zasady haseł

W systemie Windows Server 2000 i Windows Server 2003 zasady hasła i ustawienia blokowania konta dla wszystkich użytkowników domeny są kontrolowane przez domyślną zasadę domeny (Default Domain Policy). W celu utworzenia oddzielnych zasad hasła lub ustawień blokady konta dla określonego użytkownika domeny wymagane było utworzenie dodatkowych domen lub filtrów hasła. W usłudze AD DS systemu Windows Server 2008 są obecnie dostępne dokładne zasady haseł (*fine-grained password policies)*, które określają wiele zasad haseł wewnątrz jednej domeny. Dzięki temu członkowie grupy Domain Admins (Administratorzy domeny) mogą tworzyć oddzielne zasady haseł i ustawienia blokady konta dla różnych typów użytkowników domeny. Na przykład administrator domeny może utworzyć silniejszą zasadę hasła dla grupy użytkowników uprzywilejowanych, którzy mają większe uprawnienia dostępu oraz słabszą zasadę hasła dla innych użytkowników.

Dokładne zasady haseł w systemie Windows Server 2008 mogą być stosowane do obiektów użytkowników lub do globalnych grup zabezpieczeń. Zasady nie mogą być bezpośrednio stosowane do jednostek organizacyjnych (OU). W celu utworzenia odrębnej zasady haseł dla członków jednostki organizacyjnej należy zastosować zasadę hasła do globalnej grupy zabezpieczeń, która jest logicznie zamapowana do jednostki organizacyjnej (*shadow group*). Jeśli użytkownik przenoszony jest z jednej jednostki organizacyjnej do drugiej, należy zaktualizować członkostwo w grupie typu shadow, o ile użytkownik ma być kontrolowany przez zasadę hasła nowej jednostki organizacyjnej (lub zasada starej jednostki nie ma być już dłużej stosowana do użytkownika).

Przechowywanie dokładnych zasad haseł

W schemacie usługi AD DS zostały utworzone nowe klasy obiektów w celu przechowywania dokładnych zasad haseł: Password Settings Container (PSC) (Kontener ustawień hasła) i Password Settings (Ustawienia hasła). Obiekty PSO (Password Settings Object) są przechowywane w kontenerze PSC. Kontener PSC jest domyślnie tworzony w domenie w kontenerze System – nie może być przenoszony, usuwany i nie może być zmieniana jego nazwa. Obiekt PSO ma atrybuty dla wszystkich ustawień, które mogą być definiowane w domyślnej zasadzie domeny (Default Domain Policy), za wyjątkiem ustawień protokołu Kerberos. Ustawienia te obejmują atrybuty dla następujących ustawień hasła:

- Enforce password history (Wymuszaj tworzenie historii haseł)

- Maximum password age (Maksymalny okres ważności hasła)
- Minimum password age (Minimalny okres ważności hasła)
- Minimum password length (Minimalna długość hasła)
- Passwords must meet complexity requirements (Hasło musi spełniać wymagania co do złożoności)
- Store passwords using reversible encryption (Zapisz hasła korzystając z szyfrowania odwracalnego)

Ustawienia te obejmują również atrybuty dla następujących ustawień blokowania konta:

- Account lockout duration (Czas trwania blokady konta)
- Account lockout threshold (Próg blokady konta)
- Reset account lockout after (Wyseruj licznik blokady konta po)

Ponadto obiekt PSO ma następujące dwa nowe atrybuty:

- **PSO link (Łącze PSO)** Atrybut o wielu wartościach, który jest powiązany z użytkownikami i/lub obiektami grup.
- **Precedence (Priorytet)** Wartość całkowita używana do rozwiązywania konfliktów w sytuacji, kiedy kilka obiektów PSO jest stosowanych do użytkownika lub grupy.



Uwaga Podczas dodawania kontrolera domeny systemu Windows Server 2008 do istniejącej domeny usługi Active Directory, należy upewnić się, czy uruchomione było narzędzie Adprep w celu rozszerzenia schematu usługi Active Directory o dwie nowe klasy obiektów, co jest wymagane przez dokładne zasady hasła. Narzędzie wiersza polecenia Adprep przygotowuje schemat pod kątem zmian wymaganych do obsługi usług AD DS w systemie Windows Server 2008. Informacje dodatkowe na temat korzystania z narzędzia Adprep znaleźć można w rozdziale 6 „Instalowanie usług AD DS (Active Directory Domain Services)", jak również w poradniku „Step-by-Step Guide for Fine-Grained Password and Account Lockout Policy Configuration" dostępnym pod adresem *http://technet2.microsoft.com/windowsserver2008/en/library/2199dcf7-68fd-4315-87cc-ade35f8978ea1033.mspx*.

Wynikowy zestaw zasad dla dokładnej zasady hasła

Ustawienia dokładnej zasady hasła mogą być stosowane do obiektów użytkowników i do globalnych grup zabezpieczeń. Wynikowy zestaw zasad RSOP (Resultant Set of Policy) może być obliczany jedynie dla obiektu użytkownika. Jeśli kilka obiektów PSO jest powiązanych z użytkownikiem lub grupą, stosowany wynikowy zestaw zasad PSO określany jest w następujący sposób:

1. Obiekt PSO bezpośrednio powiązany z obiektem użytkownika jest wynikowym zestawem zasad (PSO). Jeśli kilka obiektów PSO jest powiązanych bezpośrednio do obiektu użytkownika, w dzienniku zdarzeń zarejestrowane zostanie ostrzeżenie, a obiekt PSO o najniższym priorytecie będzie wynikowym obiektem PSO.
2. Jeśli żaden obiekt PSO nie jest powiązany z obiektem użytkownika, porównywane jest członkostwo w globalnej grupie zabezpieczeń użytkownika i wszystkie obiekty PSO,

które stosowane są do użytkownika w oparciu o te członkostwa w grupach globalnych. Obiekt PSO o najniższej wartości priorytetu jest wynikowym obiektem PSO (jeśli istnieje kilka takich obiektów, identyfikator PSO GUID będzie używany do definiowania kolejności stosowania obiektów).

3. Jeśli żaden obiekt PSO nie zostaje wskazany poprzez spełnienia warunków opisanych w punkcie 1 i 2, stosowana jest domyślna zasada domeny.

Istnieją trzy ustawienia stosowane bezpośrednio do obiektu użytkownika, które zawsze zastępują ustawienia stosowane za pośrednictwem dokładnej zasady hasła. Bity te można ustawiać w atrybucie *userAccountControl obiektu użytkownika*:

- Reversible password encryption required (wymagane hasło przy użyciu szyfrowania odwracalnego)
- Password not required (hasło nie jest wymagane)
- Password does not expire (hasło nie wygasa)

Bity te zastępują ustawienia wynikowego obiektu PSO stosowanego do obiektu użytkownika (tak jak bity te zastępują ustawienia domyślnej zasady domeny systemu Windows 2000 i Windows Server 2003).

Możliwość ponownego uruchamiania usług AD DS (Active Directory Domain Services)

Możliwość ponownego uruchamiania usług AD DS w systemie Windows Server 2008 pozwala administratorom na wykonywanie funkcji, które realizowane są w trybie offline bez konieczności ponownego uruchamiania kontrolera domeny. W poprzednich wersjach systemu Windows Server funkcje trybu offline, takie jak defragmentacja bazy danych, wymagały ponownego uruchomienia kontrolera domeny w trybie Directory Services Restore (Przywracanie usługi katalogowej). W systemie Windows Server 2008 można zatrzymać usługi AD DS i wykonać potrzebne aktualizacje, kiedy w tym samym czasie inne usługi uruchomione na serwerze (jak na przykład DHCP) kontynuują swoje działania i są dostępne dla użytkowników. Należy pamiętać, że usługi zależne, takie jak DNS czy KDC, nie będą funkcjonować bez usługi AD DS; podczas zatrzymywania usług AD DS zatrzymywane są również usługi zależne.

Poniżej wymienione zostały trzy możliwe stany kontrolera domeny systemu Windows Server 2008:

- **AD DS Started (Uruchomione usługi AD DS)** W tym stanie usługi AD DS są uruchomione. Dla klientów i innych usług uruchomionych na serwerze kontroler domeny systemu Windows Server 2008 funkcjonujący w tym stanie jest takim samym kontrolerem domeny, jak kontroler działający w systemie Windows 2000 Server lub Windows Server 2003.
- **AD DS Stopped (Zatrzymane usługi AD DS)** W tym stanie usługi AD DS są zatrzymane. Chociaż jest to unikalny tryb, serwer charakteryzuje się pewnymi cechami trybu przywracania usługi katalogowej (Directory Services Restore Mode) i serwera członkowskiego domeny.

- **Directory Services Restore Mode (Tryb przywracania usług katalogowych)** W porównaniu do systemu Windows Server 2003, tryb ten nie został zmieniony.

Usługi AD DS można w prosty sposób zatrzymywać lub uruchamiać za pomocą składnika Services (Usługi) przystawki konsoli MMC (Computer Management) lub przy użyciu innych metod zatrzymywania bądź uruchamiania usług uruchomionych lokalnie na serwerze.

Narzędzie instalowania bazy danych

Narzędzie instalowania bazy danych (Dsamain.exe) umożliwia przeglądanie obrazów (snapshot) i kopii zapasowych danych usług AD DS w celu określenia, które kopie czy obrazy zawierają dane odpowiednie do przywracania. Poprzednio we wcześniejszych wersjach usług AD DS, administratorzy musieli przywracać wiele zestawów kopii zapasowych, aby określić, który zestaw zawiera potrzebne dane. Proces ten wymagał ponownego uruchamiania kontrolera domeny w trybie Directory Services Restore Mode i nie umożliwiał porównania danych przechowywanych w kopiach zapasowych wykonanych w różnych okresach czasu. Pomimo że narzędzie instalowania bazy danych nie może być używane do przywracania danych usługi AD DS, może być używane do uproszczenia procesu identyfikacji zmodyfikowanych informacji i wybrania odpowiedniej kopii zapasowej bez wydłużania okresu przerw pracy usługi.

Narzędzie instalowania bazy danych używane jest do ujawnienia woluminu obrazu (snapshot), utworzonego przy użyciu narzędzia Ntdsutil lub Volume Shadow Copy Service, jako pliku AD.dit. Następnie korzystając z narzędzia LDAP, takiego jak program LDP.exe (dołączonego do systemu Windows Server 2008), można przeglądać obraz tak, jak każdy uruchomiony kontroler domeny.

Udoskonalenia interfejsu użytkownika

W systemie Windows Server 2008 wprowadzonych zostało szereg udoskonaleń interfejsu usług AD DS. Program instalacyjny, Active Directory Domain Services Installation Wizard, zawiera obecnie zaawansowane opcje w celu lepszej obsługi instalacji kontrolerów RODC. Proces instalacji usług AD DS został uproszczony. Ponadto narzędzia zarządzania, jak przystawka Active Directory Sites and Services (Lokacje i usługi Active Directory), umożliwiają kontrolę nowych funkcji usług AD DS (na przykład zasady replikacji hasła dla kontrolerów RODC).

Udoskonalenia programu AD DS Installation Wizard

Pomimo że można korzystać z nowego programu Add Roles Wizard (Kreator dodawania ról) do konfigurowania serwera dla roli usług AD DS i do instalowania potrzebnych plików w celu uruchomienia instalacji usług AD DS, to nadal przy użyciu polecenia Dcpromo.exe trzeba będzie uruchamiać program AD DS Installation Wizard (Kreator instalacji usługi AD DS). W systemie Windows Server 2008, na stronie powitalnej programu AD DS Installation Wizard Welcome pojawiła się nowa opcja umożliwiająca uruchomienie kreatora w trybie Advanced (Zaawansowany), zamiast używania przełącznika */adv podczas wprowadzania polecenia* Dcpromo.exe w wierszu polecenia lub polu Run (Uruchom).

Poniżej wymienione zostały dodatkowe opcje instalacji trybu zaawansowanego:

- Utworzenie nowego drzewa domeny;
- Używanie nośnika kopii zapasowej z istniejącego kontrolera domeny w tej samej domenie w celu zmniejszenia ruchu w sieci związanego z początkową replikacją;
- Wybór dla instalacji źródłowego kontrolera domeny, co umożliwia określenie, który kontroler domeny jest używany do początkowej replikacji danych o domenie do nowego kontrolera domeny;
- Definiowanie dla kontrolera RODC zasady replikacji hasła (Password Replication Policy);

Nowy program instalacyjny Active Directory Domain Services Installation Wizard zawiera ponadto następujące udoskonalenia:

- Domyślnie kreator używa obecnie poświadczeń użytkownika, który jest aktualnie zalogowany. W razie potrzeby użytkownik będzie poproszony o podniesienie uprawnień.
- Podczas tworzenia dodatkowego kontrolera domeny w domenie podrzędnej kreator wykrywa obecnie, czy rola wzorca infrastruktury jest utrzymywana na serwerze katalogu globalnego tej domeny i kreator będzie monitował administratora o przetransferowanie roli wzorca infrastruktury do tworzonego kontrolera domeny, jeśli kontroler ten nie będzie serwerem katalogu globalnego. Dzięki temu uniknąć można niepotrzebnych przemieszczeń roli wzorca infrastruktury.
- Na stronie podsumowania można obecnie wyeksportować wybrane ustawienia do odpowiedniego pliku odpowiedzi, który może być wykorzystywany w kolejnych operacjach (instalowania czy odinstalowania). W porównaniu do ręcznego tworzenia plików instalacji nienadzorowanej metoda ta pozwala uniknąć pomyłek.
- Obecnie w pliku odpowiedzi można pomijać hasło administratora. Zamiast hasła w pliku odpowiedzi można wpisać **password=***, aby zapewnić, że użytkownik będzie monitowany o podanie poświadczeń konta.
- Istnieje możliwość wstępnego podawania parametrów dla programu instalacyjnego poprzez określanie niektórych z nich w wierszu poleceń, co zmniejsza liczbę interakcji ze strony użytkownika wymaganych przez kreator. Parametry wiersza polecenia są również wymagane podczas instalowania usług AD DS w systemie Windows Server 2008 Server Core.
- Obecnie można wymusić degradację kontrolera domeny, który uruchomiony został w trybie przywracania usługi katalogowej (Directory Services Restore Mode).

Udoskonalenia narzędzi zarządzania usługami AD DS

Wprowadzonych zostało szereg udoskonaleń w przystawce Active Directory Sites and Services (Lokacje i usługi Active Directory), które upraszczają zarządzanie usługami AD DS. Po pierwsze dodana została nowa zakładka Password Replication Policy (Zasada replikacji hasła) na stronie Properties (Właściwości) kontrolera domeny, która może być używana do przeglądania, jakie hasła zostały wysłane do kontrolera RODC i które hasła są aktualnie przechowywane na kontrolerze RODC. Na zakładce tej wskazane jest również, które konta zostały uwierzytelnione na kontrolerze RODC w celu określenia, czy jest, czy też nie jest

dopuszczona replikacja hasła. Ponadto do paska narzędzi oraz do menu Action (Akcja) dodane zostało polecenie Find (Znajdź). Dzięki niemu administratorzy mogą określić, w jakiej lokacji znajduje się kontroler domeny, co ułatwia rozwiązywanie problemów replikacji.

Kilka narzędzi, takich jak Ldp, Repadmin czy Nltest, które były częścią narzędzi pomocniczych lub były dostępne w zestawie Windows Server 2003 Resource Kit, zostały obecnie dołączone do standardowej instalacji systemu Windows Server 2008 i są dostępne po zainstalowaniu ról kontrolera domeny. Te same narzędzia mogą być używane do zarządzania usługami AD DS i AD LDS, poprzednio nazywanymi ADAM (Active Directory Application Mode). Istnieje opcja, aby narzędzia te były instalowane jedynie podczas instalacji.

Dodatkowe role usług Active Directory Service

Oprócz usług AD DS na komputerze systemu Windows Server 2008 można instalować cztery dodatkowe role usług Active Directory:

- Rola AD CS (Active Directory Certificate Services)
- Rola AD FS (Active Directory Federation Services)
- Rola AD LS (Active Directory Lightweight Services)
- Rola AD RMS (Active Directory Rights Management Services)

W niniejszym rozdziale skrótowo opisano funkcje dostępne po skonfigurowaniu tych ról usług AD serwera. W ostatnim rozdziale czytelnik zapoznany zostanie z implikacjami projektowymi instalowania wielu ról usług na pojedynczym komputerze systemu Windows Server 2008, jak również informacjami szczegółowymi każdej roli usługi.

W celu zainstalowania ról usług na komputerze z systemem operacyjnym Windows Server 2008 należy skorzystać z konsoli Server Manager (Menedżer serwera). Kilka z tych ról usług wymaga, aby serwer był najpierw skonfigurowany jako kontroler domeny, a inne wymagają, aby serwer był instalowany w istniejącym lesie usługi Active Directory.

Rola AD CS (Active Directory Certificate Services)

Rola AD CS jest używana do tworzenia, dystrybucji i zarządzania certyfikatami kluczy publicznych, które zabezpieczają zasoby sieci. Certyfikaty klucza publicznego mogą być wydawane użytkownikom, urządzeniom lub komputerom, usługom i funkcjom usług AD CS w celu powiązania tożsamości osoby, urządzenia lub usługi z odpowiednim kluczem prywatnym, który jest unikalny dla tego obiektu.

W usługach AD CS systemu Windows Server 2008 pojawiło się kilka udoskonaleń dotyczących zarządzania i odwoływania certyfikatów w skalowalnych środowiskach:

- **Cryptography Next Generation (CNG)** Funkcja CNG (kryptografia następnej generacji) udostępnia zestaw interfejsów API używanych do wykonywania podstawowych operacji kryptograficznych, takich jak tworzenie skrótów (hash) czy deszyfrowanie danych. Funkcja jest również używana do tworzenia, przechowywania i pobierania kluczy kryptograficznych.
- **Rejestrowanie w sieci Web** Funkcja rejestrowania w sieci Web pozwala użytkownikom łączyć się z urzędem certyfikacji (CA) za pomocą przeglądarki sieci Web w celu

żądania certyfikatów, pobierania list odwołań certyfikatów CRL (Certificate Revocation List) i wykonywania rejestracji certyfikatów kart inteligentnych.

- **Usługa Online Responder** Usługa Online Responder umożliwia klientom sprawdzenie stanu odwołania certyfikatu przy użyciu protokołu OCSP (Online Certificate Status Protocol), a nie za pomocą list odwołań certyfikatów CRL (Certificate Revocation Lists). Kiedy klient żąda informacji o stanie odwołania certyfikatu z usługi Online Responder, serwer sprawdza stan certyfikatu i zwraca podpisaną odpowiedź zawierającą informacje o stanie żądanego certyfikatu. Podczas korzystania z listy CRL cała lista odwołanych certyfikatów pobierana jest do systemu klienckiego.
- **Network Device Enrollment Service (NDES)** Usługa NDES (rejestrowanie urządzeń sieci) umożliwia uzyskanie certyfikatów routerom, przełącznikom i innym urządzeniom sieci, które nie mają kont sieci.
- **Enterprise PKI (PKIView)** Narzędzie PKIView jest przystawką MMC dostępną w usługach AD CS dla systemu Windows Server 2008 i jest używana do monitorowania i rozwiązywania problemów związanych z kondycją wszystkich urzędów certyfikacji (CA) infrastruktury klucza publicznego (PKI). Przystawka PKIView graficznie przedstawia kondycję i stan wszystkich urzędów certyfikacji w danym środowisku.
- **Ograniczony agent rejestrowania** Ograniczony agent rejestrowania jest nową funkcją systemu Windows Server 2008, która ogranicza uprawnienia, które mają użytkownicy wyznaczeni jako „agenci rejestrowania" do rejestrowania certyfikatów kart inteligentnych w imieniu innych użytkowników. Funkcja ta jest dostępna tylko dla systemu Windows Server 2008 Enterprise.
- **Ustawienia zasad grupy dotyczące certyfikatów** W usługach AD CS pojawiły się nowe ustawienia zasad grupy dotyczące certyfikatów, które mogą być zarządzane przy użyciu konsoli zarządzania zasadami grupy GPMC (Group Policy Management). Ustawienia te mogą być używane do:
  - Instalowania certyfikatów pośrednich urzędów certyfikacji (CA) na komputerach klienckich.
  - Zapobiegania instalowaniu aplikacji przez użytkowników, które zostały podpisane przez niezatwierdzony certyfikat publikatora.
  - Konfigurowania limitów czasu sieci dla dużych list CRL, jak również do wydłużania wygasania list CRL.

W usłudze AD CS może być instalowany urząd certyfikacji przedsiębiorstwa (Enterprise CA) lub autonomiczny urząd certyfikacji. Enterprise CA jest ściśle zintegrowany z usługami AD DS, dzięki czemu można zautomatyzować wiele zadań dotyczących rejestrowania i odnawiania certyfikatów. Urząd certyfikacji przedsiębiorstwa musi być instalowany na komputerze systemu Windows Server 2008, który należy do domeny usługi AD DS.

Składniki usług AD CS mogą być instalowane na pojedynczym serwerze lub rozproszone na kilku serwerach. W niewielkim przedsiębiorstwie wszystkie role, za wyjątkiem usługi Online Responder, mogą być instalowane na pojedynczym komputerze, a jeden komputer może być wyznaczony do świadczenia usługi Online Responder. W dużych przedsiębiorstwach o skomplikowanych wymaganiach certyfikatów cyfrowych, na oddzielnych komputerach można instalować kilka urzędów certyfikacji, wliczając w to podrzędne urzędy i komputery usługi Online Responder. Liczba instalowanych serwerów zależy od kilku

zmiennych, a w tym liczby żądań certyfikatów, liczby i lokalizacji urzędów certyfikacji i liczby aplikacji żądających certyfikatów. Aplikacje te dotyczą rozszerzeń S/MIME (Secure/Multipurpose Internet Mail Extensions), bezpiecznych sieci wirtualnych, prywatnych sieci wirtualnych (VPN), IPsec (Internet Protocol security), systemu EFS (Encrypting File System), logowania kart inteligentnych, protokołów SSL/TLS (Secure Socket Layer/Transport Layer Security) i podpisów cyfrowych.

W celu zwiększenia elastyczności obsługi infrastruktury PKI usługa Online Responders może być instalowana na pojedynczym komputerze lub na kilku komputerach. Kilka komputerów usług Online Responder może być instalowanych, aby obsługiwać jeden lub kilka urzędów certyfikacji, a jeden komputer usługi Online Responder może obsługiwać kilka urzędów CA. Dla zapewnienia większej odporności na uszkodzenia i dla zapewnienia obsługi zdalnych żądań odwoływania certyfikatów (scenariusze biur oddziałowych), usługa Online Responder może być instalowana jako macierz. Jeden członek macierzy musi być wyznaczony jako kontroler macierzy. Pomimo że każdy komputer usługi Online Responder w macierzy może być konfigurowany i zarządzany niezależnie, w przypadku konfliktów konfiguracja macierzy zastąpi konfigurację pozostałych członków macierzy.

Rola AD FS (Active Directory Federation Services)

Usługi AD FS (Active Directory Federation Services) pełnią rolę serwera w systemie operacyjnym Windows Server 2008, która używana jest do rozszerzenia funkcjonalności uwierzytelnienia kont usług AD DS poza granice lasu usług AD FS i na wielu platformach, wliczając w to środowiska systemów Windows i innych systemów. Usługi AD FS są dobrze dostosowane do aplikacji internetowych lub dowolnego środowiska, gdzie pojedyncze konto użytkownika wymaga dostępu do zasobów w różnych sieciach. W takich sytuacjach użytkownicy mogą być monitowani o poświadczenia, ilekroć próbują uzyskać dostęp do aplikacji, która korzysta z innych źródeł uwierzytelnienia (na przykład w innej organizacji lub w innym lesie, tak jak las sieci obwodowej w tej samej organizacji).

Podczas implementowania usług AD FS można wprowadzać zaufania federacyjne pomiędzy dwoma różnymi organizacjami lub pomiędzy dwoma różnymi lasami. To zaufanie federacyjne umożliwia użytkownikom używanie bezpiecznych poświadczeń ze swojego własnego lasu podczas uzyskiwania dostępu do aplikacji znajdującej się poza lasem użytkownika. Zaufanie federacyjne jest konfigurowane pomiędzy organizacjami zasobów (organizacje, które posiadają zasoby bądź aplikacje i nimi zarządzają oraz które są dostępne z Internetu lub sieci innych dostawców) a organizacjami kont (organizacje, które posiadają konta użytkowników i nimi zarządzają oraz do których to kont przydzielany jest następnie dostęp do zasobów w organizacjach zasobów). W takim scenariuszu usługi AD FS oferują dostęp o pojedynczej rejestracji (SSO; Ssingle Sign-On) do zasobów w organizacji zasobów dla użytkowników, którzy zostali uwierzytelnieni w organizacji kont. Usługa SSO umożliwia użytkownikom zalogowanie się w lokalnej sieci i odebranie tokenu zabezpieczeń, umożliwiającego im dostęp do zasobów w innych sieciach, które zostały skonfigurowane tak, aby ufać tym kontom. Nawet wewnątrz pojedynczej organizacji o oddzielnych sieciach i granicach zabezpieczeń użytkownicy będą doceniali zalety usługi SSO do uzyskiwania dostępu do wszystkich odpowiednich zasobów sieci. Usługi AD FS nadają się do stosowania zarówno wewnątrz dużych organizacji z oddzielnymi organizacjami zasobów i kont, jak i poza zaporą: usługi AD FS są skalowane do sieci Internet w celu zapewnienia obsługi

żądań dostępu, generowanych przez użytkowników uzyskujących dostęp do zasobów przy użyciu przeglądarek sieci Web.

Usługi AD FS w systemie Windows Server 2008 składają się z kilku składników:

- **Federation Service (Usługi federacyjne)** Usługa federacyjna składa się z jednego lub kilku serwerów federacyjnych, które współużytkują wspólną zasadę zaufania. Serwery federacyjne używane są do przekierowania żądań uwierzytelnienia generowanych przez konta użytkowników w innych organizacjach lub przez klientów, którzy mogą znajdować się gdzieś w sieci Internet.
- **Federation Service Proxy (Proxy usług federacyjnych)** Federation Service Proxy jest usługą proxy dla usług federacyjnych w sieci obwodowej (nazywaną również strefą zdemilitaryzowaną i podsiecią ekranującą). Usługa Federation Service Proxy korzysta z protokołów WS-F PRP (WS-Federation Passive Requestor Profile) do gromadzenia informacji o poświadczeniach użytkowników klientów i w ich imieniu przesyła je do usługi federacyjnej.
- **Claims-aware agent (Agent obsługujący oświadczenia)** Agent obsługujący oświadczenia na serwerze sieci Web utrzymującej aplikacje obsługujące oświadczenia jest używany do umożliwienia generowania zapytań o oświadczenia dotyczące tokenu zabezpieczeń usług AD FS. Aplikacją obsługującą oświadczenia jest aplikacja platformy Microsoft ASP.NET, która używa oświadczeń prezentowanych w tokenie zabezpieczeń usług AD FS do podejmowania decyzji dotyczących autoryzacji i do personalizacji aplikacji.
- **Windows token-based agent (Agent bazujący na tokenie systemu Windows)** Agent bazujący na tokenie zabezpieczeń systemu Windows na serwerze sieci Web, który utrzymuje aplikację korzystającą z tokenu systemu Windows NT do obsługi konwersji tokenu zabezpieczeń wystawianego przez usługę AD FS do poziomu spersonifikowanego tokenu dostępu systemu Windows NT. Aplikacją używającą tokenu systemu Windows NT jest aplikacja, która korzysta z mechanizmów autoryzacji bazujących na systemie Windows.

Jednym z kilku udoskonaleń usługi AD FS w systemie Windows Server 2008 jest proces instalacji. Inaczej niż w przypadku usług AD FS w systemie Windows Server 2003 R2, gdzie do zainstalowania usług AD FS trzeba użyć apletu Add Or Remove Programs (Dodaj lub usuń programy), w systemie Windows Server 2008 usługi AD FS są instalowane podobnie jak inne role serwera – przy użyciu programu Server Manager (Menedżer serwera). Usługi AD FS wymagają usługi katalogowej i mogą korzystać z usług AD DS lub AD LDS (Active Directory Lightweight Directory Services) jako katalogu. Dodatkowym usprawnieniem w systemie Windows Server 2008 jest ścisła integracja pomiędzy usługami AD FS a programem Office SharePoint Server 2007 w kontekście członkostwa i dostawców roli oraz usługami AD RMS dla współużytkowania chronionej zawartości z zaufanymi partnerami zewnętrznymi.

Po zainstalowaniu usług AD FS mogą one być zarządzane przy użyciu konsoli MMC (Microsoft Management Console). Do zarządzania usługami ról Federation Service i Federation Service Proxy używana jest przystawka Active Directory Federation Services.

Rola AD LDS (Active Directory Lightweight Directory Services)

Rola AD LDS (Active Directory Lightweight Directory Services), poprzednio nazywana Active Directory Application Mode (ADAM), jest usługą katalogową protokołu LDAP (Lightweight Directory Access Protocol), która w niektórych sytuacjach może zastąpić funkcje usług AD DS lub może być instalowana razem z usługami AD DS. Usługi AD LDS są specyficznie używane w celu zapewnienia usług katalogowych do instalowania aplikacji używających katalogu, bez zależności od usług AD DS. Korzystając z usług AD LDS można zainstalować uproszczone usługi katalogowe bez domen i lasów (które są wymagane w usługach AD DS) i można obsługiwać oddzielne schematy dla każdej instancji zainstalowanych usług AD LDS. Usługi AD DS są ograniczone do pojedynczego schematu w całym lesie.

Poniżej wymienione zostały sytuacje, w których instalowane są usługi AD LDS:

- **Udostępnienie magazynu katalogu przedsiębiorstwa** Usługi AD LDS są używane do przechowywania danych specyficznych dla aplikacji, które są istotne tylko dla aplikacji przedsiębiorstwa. Informacje te mogą być przechowywane na tym samym serwerze co aplikacja lub mogą być replikowane do wielu serwerów usług AD LDS w całym przedsiębiorstwie. Usługi AD LDS mogą przechowywać tylko dane konfiguracji aplikacji przedsiębiorstwa, podczas gdy usługi AD DS mogą być używane do przechowywania głównych danych zabezpieczeń – co zmniejszy w sieci ilość baz danych kont użytkowników specyficznych dla aplikacji.
- **Udostępnienie magazynu uwierzytelnienia sieci zewnętrznej (extranet)** Usługi AD LDS dobrze nadają się na ten magazyn uwierzytelnienia, ponieważ mogą przechowywać dane konta użytkownika, które nie są podmiotami zabezpieczeń systemu Windows, ale mogą być uwierzytelniane za pomocą prostych powiązań protokołu LDAP. Klienci sieci Web mogą uzyskiwać dostęp do aplikacji opartych na portalach przy użyciu prostych usług katalogowych LDAP.
- **Udostępnianie magazynu konfiguracji dla aplikacji rozproszonych** W tym scenariuszu instancja usług AD LDS, służąca jako magazyn konfiguracji aplikacji, jest powiązana z aplikacją rozproszoną. W ten sposób projektanci aplikacji nie muszą obawiać się o dostępność usługi katalogowej przed instalacją aplikacji – mogą dołączyć usługi AD LDS jako część procesu instalacji aplikacji, aby zapewnić, że aplikacja będzie miała dostęp do usługi katalogowej zaraz po zainstalowaniu. Następnie aplikacja konfiguruje i zarządza usługami AD LDS całkowicie lub częściowo dla swoich potrzeb w zależności od poziomu odsłonięcia się dla funkcji zarządzania usług AD LDS i używa usług AD LDS do wypełniania różnych wymagań dotyczących danych.



Uwaga Rola Edge Transport Server w programie Exchange Server 2007 jest przykładem aplikacji, która korzysta z usług AD LDS. Podczas instalowania tej roli serwera usługi są automatycznie instalowane i konfigurowane tak, by obsługiwały tę rolę serwera.

- **Migracja starszych aplikacji korzystających z katalogu** Usługi AD LDS można zainstalować w celu zapewnienia obsługi starszych aplikacji, które zależne są od nazewnictwa standardu X.500, podczas gdy usługi AD DS mogą być używane w przedsiębiorstwie do zapewnienia współużytkowanej infrastruktury zabezpieczeń. Metakatalog lub konfiguracja synchronizacji pomiędzy usługami AD LDS a AD DS może być używana

do zautomatyzowania synchronizacji danych w usługach AD DS i AD LDS dla zapewnienia bezproblemowej migracji.

Po dodaniu roli serwera usług AD LDS za pomocą programu Server Manager, przy użyciu programu instalacyjnego Active Directory Lightweight Directory Services Setup Wizard, tworzone będą instancje usługi AD LDS i partycje aplikacji. Na jednym serwerze można tworzyć kilka instancji usług AD LDS, a każda instancja może korzystać z innego schematu. W każdej instancji można skonfigurować wiele partycji aplikacji. Po utworzeniu instancji i partycji są one zarządzane za pomocą narzędzi LDAP, takich jak przystawka ADSI Edit MMC lub program LDP.exe.

Rola AD RMS (Active Directory Rights Management Services)

Rola AD RMS (Active Directory Rights Management Services) używana jest do rozszerzenia istniejących w organizacji rozwiązań zabezpieczeń poprzez udostępnienie obiektowej zasady o trwałym stosowaniu. Usługi AD RMS rozszerzają rozwiązanie zabezpieczeń dołączając zasady o trwałym użyciu, które mogą chronić ważne dane korporacji, takie jak dokumenty tekstowe, dane klientów, wiadomości e-mail czy dane finansowe. Zabezpieczenia dotyczące określonego pliku „podążają" za dokumentem, jeśli jest przenoszony, i nie są przypisane do kontenera, w którym dokument jest przechowywany (inaczej jest w przypadku list ACL).

Korzystając z usług AD RMS użytkownicy sieci mogą zabraniać kopiowania, drukowania lub przesyłania ważnych danych. Dzięki temu można przesłać poufną wiadomość e-mail tak, aby odbiorca mógł otworzyć i przeczytać wiadomość, ale nie mógł wyciąć, skopiować lub przekazać tej wiadomości do innych odbiorców, wliczając w to załączniki wiadomości. Poufna komunikacja w korporacji pozostaje poufna poprzez ograniczenie odbiorcom wiadomości e-mail możliwości przekierowywania chronionej komunikacji. Usługi AD RMS wyłączają również możliwość kopiowania danych chronionych za pomocą uprawnień, a następnie wklejania ich do niechronionego dokumentu lub wiadomości e-mail.

W systemie Windows Server 2008 wprowadzono kilka udoskonaleń usługi AD RMS w odniesieniu do usług RMS (Windows Rights Management Services), które usprawniają administrację usługi i rozszerzają jej funkcjonalność poza organizacją:

- **Udoskonalona instalacja i administracja** Usługi AD RMS zostały dołączone do systemu Windows Server 2008 i są instalowane jako rola serwera. Poprzednie wersje usług RMS były dostarczane jako oddzielna instalacja udostępniana w witrynie Microsoft Download Center. Ponadto obecnie administracja usług AD RMS jest realizowana poprzez przystawkę konsoli MMC, co jest prostszą metodą niż korzystanie z interfejsu sieci Web stosowanego w poprzednich wersjach usług RMS. Wraz z dołączeniem ról administracji usług AD RMS konsola AD RMS wyświetla jedynie te części, do których użytkownik może uzyskać dostęp. Na przykład użytkownik, który pełni rolę AD RMS Template Administrators (Administratorzy szablonów usług AD RMS), będzie mógł wykonywać zadania dotyczące szablonów AD RMS, a pozostałe zadania administracyjne nie będą dla niego dostępne w konsoli AD RMS.
- **Automatyczne rejestrowanie klastra usług AD RMS** Klaster usług AD RMS może być zarejestrowany bez konieczności łączenia się z usługą Microsoft Enrollment Service. Dzięki używaniu samo-rejestrującego się certyfikatu serwera proces rejestracji jest

całkowicie wykonywany na komputerze lokalnym. Ta nowa funkcja eliminuje zależność operacyjną od usługi rejestrowania, a także pozwala usługom AD RMS działać w sieci, która jest zupełnie odizolowana od Internetu.

- **Integracja z usługami AD FS** Usługi AD RMS i AD FS zostały zintegrowane tak, aby w przedsiębiorstwach można było korzystać z istniejących zależności federacyjnych do współpracy z partnerami zewnętrznymi. W poprzednich wersjach usług RMS opcje współużytkowania zawartości chronionej uprawnieniami były ograniczone do identyfikatora Windows Live ID (poprzednio Microsoft Passport). Zintegrowanie usług AD FS i AD RMS umożliwia ustanawianie tożsamości federacyjnych pomiędzy organizacjami i współużytkowanie chronionych zawartości, bez konieczności instalowania usług AD RMS w obu miejscach.
- **Nowe role administracyjne usług AD RMS** Możliwość delegowania zadań dotyczących usług AD RMS do innych administratorów jest potrzebna w każdym przedsiębiorstwie i funkcje takie zostały dołączone do aktualnej wersji usług AD RMS. Utworzyć można trzy role administracyjne: AD RMS Enterprise Administrators (Administratorzy usług AD RMS w przedsiębiorstwie), AD RMS Template Administrators (Administratorzy szablonów usług AD RMS) i AD RMS Auditors (Audytorzy usług AD RMS). Nowe role administracyjne usług AD RMS umożliwiają delegowanie zadań dotyczących usług AD RMS bez przekazywania pełnej kontroli administracyjnej nad całym klastrem usług AD RMS.

Klient korzystający z usług AD RMS musi mieć przeglądarkę z włączoną obsługą AD RMS lub aplikację, taką jak Microsoft Word, Outlook czy PowerPoint w pakiecie Microsoft Office 2007. Aby utworzyć zawartość chronioną przez uprawnienia, wymagana jest wersja oprogramowania Microsoft Office 2007 Enterprise, Professional Plus lub Ultimate. System Windows Vista dołącza domyślnie klienta usług AD RMS, ale w innych systemach operacyjnych klient usług RMS musi być instalowany. Klient usług RMS z dodatkiem Service Pack 2 (SP2) może być pobrany z witryny Microsoft Download Center i oprogramowanie to działa w klienckich systemach operacyjnych wcześniejszych niż systemy Windows Vista i Windows Server 2008. W celu zapewnienia dodatkowego bezpieczeństwa usługi AD RMS mogą być zintegrowane z innymi technologiami, takimi jak karty inteligentne.



Uwaga Odbiorcy wiadomości chronionych przez uprawnienia, korzystający z aplikacji pocztowych, które nie obsługują takich wiadomości, jak na przykład Microsoft Office 2003 czy Microsoft Office 2007, mogą przeglądać te wiadomości poprzez pobranie dodatku Rights Management dla programu Internet Explorer z witryny Microsoft Download Center pod adresem *http://www.microsoft.com/downloads/details.aspx?FamilyId=B48F920B-5AF0-46B4-994F-2F62582CC86F&displaylang=en*. Oprogramowanie to jest przykładowo potrzebne dla odbiorców korzystających z aplikacji pocztowych w sieci Web.

Usługi AD RMS są instalowane na komputerze systemu Windows Server 2008. Podczas instalowania roli serwera AD RMS instalowane są wymagane usługi. Wymaganą usługą jest IIS (Internet Information Services). Usługi AD RMS wymagają również bazy danych, na przykład Microsoft SQL Server, która może być uruchamiana na tym samym serwerze co usługi AD RMS lub na serwerze zdalnym znajdującym się w tym samym lesie co usługi AD DS. Ponadto usługi AD RMS i AD FS zostały zintegrowane, by umożliwiać korzystanie

z istniejących zależności federacyjnych do współużytkowania i zabezpieczania informacji wraz z partnerami zewnętrznymi.

Podsumowanie

W rozdziale omówiono skrótowo nowe funkcje usług AD DS, jak również role serwera udostępnione w systemie Windows Server 2008. Zrozumienie działania tych nowych funkcji i ról serwera pozwoli administratorom usług katalogowych ocenić proces migracji do systemu Windows Server 2008 i usługi Active Directory oraz zaplanować w organizacji wykorzystanie nowych funkcji udostępnianych przez system Windows Server 2008.

Rozdział 2

Składniki usług AD DS

W tym rozdziale:

Struktura fizyczna usług AD DS **21**
Struktura logiczna usług AD DS **44**
Podsumowanie. **64**
Źródła dodatkowe **64**

Administrator usług AD DS (Active Directory Domain Services) wiele czasu musi przeznaczyć na konfigurowanie kont użytkowników i grup, które znajdują się w jednostkach organizacyjnych lub obiektach kontenerów w domenie. Podczas konfigurowania tych obiektów w rzeczywistości przeprowadzane są zmiany w pliku bazy danych przechowywanym na dysku twardym kontrolera domeny. W większości sytuacji administrator bezpośrednio nie używa fizycznej bazy danych usługi AD DS; posługuje się przeważnie narzędziami zarządzania usługami AD DS w celu zmodyfikowania obiektów przechowywanych w bazie danych.

Usługi AD DS w systemie Microsoft Windows Server 2008 obejmują składnik fizyczny i organizację logiczną obiektów katalogu. W odniesieniu do pojęcia struktury fizycznej usługi AD DS składają się z pojedynczego pliku bazy danych na dysku twardym każdego kontrolera domeny, który utrzymuje usługę. Struktura logiczna usług AD DS składa się z kontenerów używanych do przechowywania obiektów usługi katalogowej (takich jak partycje katalogów, domeny czy lasy) w przedsiębiorstwie. W niniejszym rozdziale Czytelnik zapoznany zostanie ze składnikami fizycznymi, które tworzą usługę AD DS. Następnie przedstawiona zostanie struktura logiczna implementacji usług AD DS. Dokładne zrozumienie struktury fizycznej usługi katalogowej jest istotną kwestią, ale zrozumienie struktury logicznej ma zasadnicze znaczenie dla prawidłowego zaimplementowania i zarządzania infrastrukturą usługi katalogowej. Wykonując codzienne zadania administrator właśnie oddziałuje na strukturę logiczną.

Struktura fizyczna usług AD DS

Dane usług AD DS są przeważnie przechowywane jako pojedynczy plik bazy danych. Plik bazy danych jest przechowywany na kontrolerach domen, które umożliwiają dostęp do bazy danych dla administratorów i udostępniają funkcje usług katalogowych, takie jak uwierzytelnienie i autoryzacja innym użytkownikom i komputerom. Podczas implementowania usług AD DS można dodawać kontrolery domen tak, aby spełnione zostały potrzeby danej organizacji.

Wszystkie kontrolery domen w domenie udostępniają w zasadzie te same usługi. Istnieje jednak pięć specyficznych ról, które mogą być w danym momencie umieszczane tylko na jednym kontrolerze domeny. Role te nazywane są *flexible single-master operation (elastyczne operacje z jednym wzorcem)*. Usługi AD DS włączają również unikalne role kontrolera

domeny dla serwerów wykazu globalnego i kontrolerów domeny przeznaczonych tylko do odczytu. W tym podrozdziale opisany został magazyn danych usług AD DS i kontrolery domen, które go utrzymują.

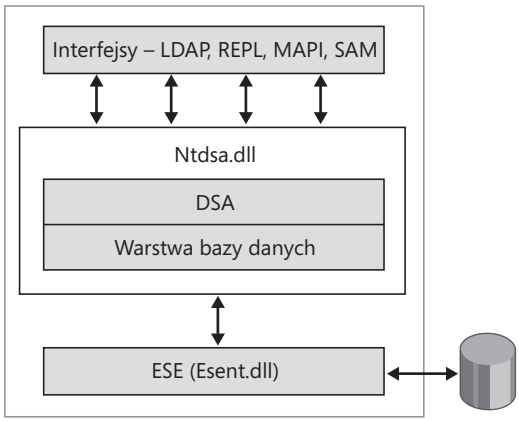
Magazyn danych katalogu

Wszystkie dane bazy danych usług AD DS przechowywane są w pliku nazwanym Ntds.dit, a dzienniki transakcji na kontrolerze domeny. Te pliki danych są przechowywane domyślnie w folderze %SystemRoot%\NTDS na kontrolerze domeny. Pliki te przechowują wszystkie informacje o katalogu domeny, jak również informacje, które są współużytkowane przez wszystkie kontrolery domen w danej organizacji. Serwery wykazu globalnego w tych samych plikach przechowują ponadto dane wykazu globalnego.



Uwaga Chociaż rzadko zachodzi potrzeba bezpośredniej interakcji z plikami danych usługi AD DS, warto wiedzieć, w jaki sposób usługi AD DS zarządzają bazą danych, ponieważ pliki te mogą być potrzebne podczas przywracania usługi po awarii. Informacje dodatkowe na temat utrzymywania i przywracania bazy danych usług AD DS znaleźć można w rozdziale 14 „Monitorowanie i konserwacja usługi Active Directory" i w rozdziale 15 „Przywracanie po awarii usługi Active Directory".

Magazyn danych usług AD DS zainstalowany jest na każdym kontrolerze domeny w danym lesie. Magazyn danych usług AD DS składa się z kilku składników, które zaprezentowane zostały na rysunku 2-1.



Rysunek 2-1 Składniki magazynu danych usług AD DS.

W tabeli 2-1 zamieszczony został opis składników magazynu danych.

Tabela 2-1 Składniki magazynu danych

Składnik	Opis
Interfejsy	Komputery klienckie, administratorzy i inne kontrolery domen nie mogą komunikować się bezpośrednio z bazą danych. Magazyn danych obsługuje następujące interfejsy dla klientów katalogu i innych serwerów katalogu w celu komunikowania się z magazynem danych: ■ **Lightweight Directory Access Protocol (LDAP)** Protokół LDAP v3 jest najczęściej używanym interfejsem przez klientów katalogu do zlokalizowania informacji w magazynie katalogu. Protokół LDAP v3 jest zgodny z poprzednią wersją LDAP v2. Klienci mogą korzystać z portu 389 (standardowy port LDAP port), portu 636 (protokół LDAP zabezpieczony przez SSL), portu 3268 (dla wyszukiwań wykazu globalnego) oraz z portu 3269 (globalny wykaz LDAP zabezpieczony przez SSL) do uzyskania dostępu do interfejsu LDAP. Klienci mogą również użyć portu 389 protokołu UDP zarówno dla LDAP, jak i dla Netlogon (interfejs ten jest używany do zlokalizowania kontrolerów domen). ■ **Interfejs zarządzania replikacją (REPL) i kontrolerem domeny** Interfejs zarządzania REPL jest używany przez narzędzia zarządzania usług AD DS oraz podczas replikacji pomiędzy kontrolerami domen. Interfejs ten udostępnia funkcje wyszukiwania danych o kontrolerach domen, konwersji nazw obiektów sieci występujących w różnych formatach i funkcje obsługi głównych nazw usługi SPN (Service Principal Name) i agentów DSA. Interfejs ten jest dostępny poprzez wywołania RPC (Remote Procedure Call) i protokół SMTP (jedynie dla replikacji opartych na SMTP). ■ **Messaging API (MAPI)** Interfejs MAPI jest używany przez klientów przekazywania wiadomości, takich jak program Outlook, do uzyskania dostępu do danych programu Microsoft Exchange Server przechowywanych w magazynie danych. Program Exchange Server 2000 i jego późniejsze wersje korzysta z magazynu danych usług AD DS do przechowywania wszystkich informacji o odbiorcy, a interfejs MAPI umożliwia klientom pocztowym uzyskanie dostępu do globalnej listy adresów GAL (Global Address List). Interfejs MAPI używa komunikacji RPC. ■ **Security Accounts Manager (SAM)** Program SAM jest interfejsem opracowanym przez firmę Microsoft służącym połączeniom do DSA w imieniu klientów korzystających z systemu Windows NT 4.0 lub wcześniejszych systemów. Te systemy klienckie używają interfejsów API sieci systemu Windows NT 4.0 do połączenia się z DSA poprzez interfejs SAM. Komunikacja interfejsu SAM również korzysta z komunikacji RPC.

Ciąg dalszy na stronie następnej

Tabela 2-1 Składniki magazynu danych

Ciąg dalszy ze strony poprzedniej

Składnik	Opis
Directory Service Agent (DSA) (Ntdsa.dll)	Agent usługi katalogowej DSA (uruchamiany jako biblioteka Ntdsai.dll na każdym kontrolerze domeny) udostępnia interfejsy dostępu do magazynu danych. Ponadto agent DSA wymusza semantykę katalogu, utrzymuje schemat, gwarantuje tożsamość obiektu i wymusza typy danych dla atrybutów. Kiedy klienci lub inne kontrolery domen potrzebują uzyskać dostęp do magazynu danych, korzystają z jednego z obsługiwanych interfejsów do połączenia (powiązania) z agentem DSA, a następnie wyszukują, odczytują i zapisują informacje w obiektach i atrybutach usług AD DS.
Warstwa bazy danych	Warstwa bazy danych znajduje się w pliku Ntdsai.dll i udostępnia wewnętrzny interfejs pomiędzy DSA a bazą danych katalogu. Agent DSA nie może bezpośrednio łączyć się z bazą danych; aplikacje przechodzą przez warstwę bazy danych. Warstwa bazy danych umożliwia również przeglądanie obiektów bazy danych katalogu, przez co dane stają się dostępne dla DSA jako zestaw hierarchicznych kontenerów. Warstwa bazy danych jest także odpowiedzialna za tworzenie, uzyskiwanie i usuwanie poszczególnych rekordów (obiektów), atrybutów wewnątrz rekordów i wartości wewnątrz atrybutów.
ESE (Esent.dll)	Mechanizm ESE (Extensible Storage Engine) jest składnikiem systemu Windows używanym przez usługi AD DS, jak również przez kilka innych składników systemu Windows jako interfejs do bazy danych. Składnik ESE jest odpowiedzialny za indeksowanie danych w pliku bazy danych i za transfer danych do/z bazy danych. Składnik ten utrzymuje także wiersze i kolumny, z których składa się baza danych, i jego zadaniem jest umożliwienie aplikacjom przechowywanie i uzyskiwanie danych. Składnik ESE implementuje również proces transakcji przekazywania zmian w bazie danych.
Pliki bazy danych	Magazyn danych przechowuje informacje o katalogu w pojedynczym pliku bazy danych. Ponadto magazyn danych korzysta także z plików dziennika transakcji, w których zapisuje tymczasowo zadysponowane i niezadysponowane zmiany przed przekazaniem ich do bazy danych.



Uwaga Druga kopia pliku Ntds.dit znajduje się na każdym kontrolerze domeny w strukturze folderu %SystemRoot%\System32. Ta wersja pliku jest kopią dystrybucyjną (kopia domyślna) bazy danych katalogu i jest używana tylko do zainstalowania usług AD DS. Plik ten jest kopiowany do serwera podczas instalowania systemu Microsoft Windows Server 2008 tak, aby serwer mógł być promowany do roli kontrolera domeny bez konieczności używania nośnika instalacyjnego. Podczas działania programu instalacyjnego Active Directory Domain Services Installation Wizard (Dcpromo.exe) plik Ntds.dit jest kopiowany z folderu System32 do folderu NTDS. Kopia przechowywana w folderze NTDS staje się następnie kopią magazynu danych katalogu. Jeśli komputer ten nie jest w domenie pierwszym kontrolerem domeny, plik ten będzie aktualizowany z innych kontrolerów domeny za pośrednictwem procesu replikacji.

Kontrolery domeny

Zgodnie z definicją, każdy komputer systemu Windows Server 2008 utrzymujący kopię bazy danych usługi AD DS jest kontrolerem domeny. Kontrolery domeny udostępniają dla domeny usługi uwierzytelnienia, jak również usługi wyszukiwania katalogu. Za wyjątkiem kilku różnic, które opisane są szczegółowo w dalszej części rozdziału, wszystkie kontrolery domeny są tworzone jednakowo. Przy użyciu procesu replikacji z wieloma wzorcami (multimaster), opisanego w rozdziale 4 „Replikacja usług AD DS", każdy kontroler domeny w domenie utrzymuje aktualną kopię bazy danych domeny i może modyfikować bazę danych.

Oprócz kontrolerów domen, które utrzymują usługi AD DS, można wyróżnić kilka kontrolerów domen specjalnego przeznaczenia, które są potrzebne usługom AD DS do wykonywania niektórych funkcji. Są to serwery wykazu globalnego i wzorce operacji. Ponadto w systemie Windows Server 2008 obsługiwane są kontrolery domen przeznaczone tylko do odczytu (RODC).

Serwery wykazu globalnego

Wykaz globalny jest częściową repliką przeznaczoną tylko do odczytu wszystkich pozostałych partycji katalogu domeny w lesie. Dodatkowe partycje katalogu domeny są częściowe, ponieważ dla każdego obiektu dołączany jest tylko ograniczony zestaw atrybutów. Poprzez dołączenie tylko tych atrybutów, które są najczęściej używane do wyszukiwania, każdy obiekt w każdej domenie lasu może być reprezentowany w bazie danych pojedynczego serwera wykazu globalnego. Wykaz globalny umożliwia efektywną lokalizację obiektów z każdej domeny, nawet jeśli las zawiera wiele domen i drzew domen. Wyszukiwania korzystające z wykazu globalnego są szybsze, ponieważ nie wywołują odwołań do różnych kontrolerów domen.

Wykaz globalny przechowywany jest na kontrolerach domen, które zostały wyznaczone jako serwery wykazu globalnego i jest dystrybuowany za pośrednictwem replikacji z wieloma wzorcami.

To, czy atrybut jest replikowany do wykazu globalnego, określa schemat. Atrybuty dołączone do wykazu globalnego są identyfikowane w schemacie jako częściowy zestaw atrybutów (PAS). Zestaw PAS jest identyfikowany za pomocą atrybutu *isMemberOfPartialAttributeSet*: jeśli atrybut ten ma wartość *true,* atrybut będzie dołączany do wykazu globalnego.

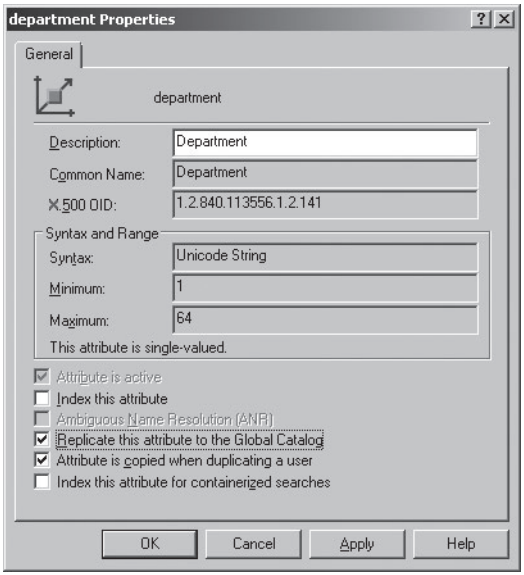
Administratorzy mogą dodawać atrybuty do wykazu globalnego przy użyciu przystawki Active Directory Schema (Schemat usługi Active Directory). Atrybut warto dodać do wykazu globalnego, jeśli przewidujemy, że użytkownicy będą wyszukiwać obiekty w wielu domenach przy użyciu tego określonego atrybutu. Na przykład, domyślnie atrybut *Department* nie jest dodawany do wykazu globalnego. Jeśli zachodzi potrzeba, aby możliwe było wyszukiwanie użytkowników według działów, warto rozważyć dodanie tego atrybutu do wykazu globalnego.

W celu dodania atrybutu do wykazu globalnego należy uzyskać dostęp do właściwości atrybutu w przystawce Active Directory Schema i wybrać opcję Replicate This Attribute To The Global Catalog (Replikuj ten atrybut do wykazu globalnego). Operacja ta ustawi wartość parametru *isMemberOfPartialAttributeSet* dla atrybutu jako *true*. Na rysunku 2-2

pokazano interfejs używany do skonfigurowania atrybutu tak, aby należał do zestawu częściowego atrybutów (PAS).



Ostrzeżenie Należy uważnie dodawać atrybuty do wykazu globalnego. Po dodaniu atrybutu do wykazu globalnego wykaz ten musi być ponownie obliczony we wszystkich domenach lasu, a zaktualizowane dane muszą być replikowane do wszystkich serwerów wykazu globalnego. Ma to szczególne znaczenie, jeśli w środowisku znajdują się kontrolery domen systemu Windows 2000. Jeśli na kontrolerze domeny systemu Windows 2000 nowy atrybut jest dodawany do wykazu globalnego lub z niego usuwany, kontroler domeny będzie przebudowywał i ponownie replikował cały wykaz globalny. Kontrolery domeny systemu Windows Server 2003 i późniejsze wersje replikują jedynie modyfikacje (to znaczy ten atrybut, który został dodany lub usunięty z zestawu PAS). W dużej organizacji o wielu domenach operacja taka może wiązać się ze znaczącym wykorzystaniem procesora i sieci. W większości przypadków zmiany zestawu PAS będą wykonywane, tylko jeśli wymaga tego określona aplikacja. Na przykład instalowanie programu Exchange 2000 Server lub jego późniejszej wersji spowoduje dodanie wielu nowych atrybutów do wykazu globalnego.



Rysunek 2-2 Przy użyciu przystawki Active Directory Schema konsoli MMC można dodać atrybut *Department* do wykazu globalnego.

Pierwszy kontroler domeny zainstalowany w lesie zostaje automatycznie skonfigurowany jako serwer wykazu globalnego. Dodatkowe kontrolery domeny mogą być wyznaczane jako serwery wykazu globalnego podczas instalowania usług AD DS lub poprzez zaznaczenie opcji Global Catalog Server (Serwer wykazu globalnego) w narzędziu administracyjnym Active Directory Sites and Services (Lokacje i usługi Astice Directory).



Uwaga W większości przypadków serwer wykazu globalnego powinien być konfigurowany w każdym biurze, które zostało skonfigurowane jako lokacja usługi AD DS. Dzięki temu w takim biurze zoptymalizowany zostanie proces logowania użytkowników. W rozdziale 5 „Projektowanie struktury usług AD DS (Active Directory Domain Services)" zamieszczono porady dotyczące liczby serwerów wykazu globalnego, które należy zainstalować i informacje o zalecanych lokalizacjach tych serwerów.

Serwery wykazu globalnego mają istotne znaczenie z kilku powodów. Jednym z nich jest usprawnienie wyszukiwań w usłudze AD DS. Bez wykazu globalnego żądania wyszukiwania odbierane przez kontroler domeny dotyczące innego obiektu domeny powodowałyby na tym kontrolerze domeny generowanie zapytania do kontrolera domeny w domenie szukanego obiektu. Wyszukiwanie byłoby możliwe, tylko jeśli kwerenda wyszukiwania obejmowałaby domenę, gdzie obiekt jest zlokalizowany. Ponieważ wykaz globalny zawiera pełną listę obiektów lasu, serwer wykazu globalnego może odpowiadać na wszystkie zapytania przy użyciu atrybutu, który został replikowany do wykazu globalnego bez konieczności odnoszenia się do innego kontrolera domeny.



Uwaga Kwerendy wykazu globalnego są identyczne, jak inne kwerendy protokołu LDAP wysyłane do kontrolera domeny systemu Windows Server 2008. Jedyną różnicą jest to, że kwerenda wykazu globalnego korzysta z portu 3268 protokołu TCP, a nie z portu 389, który jest standardowym portem LDAP. Jeśli kontroler domeny jest również serwerem wykazu globalnego, to odbiera kwerendy na porcie 389 i nie będzie przeszukiwał wykazu globalnego w innych domenach.

Serwery wykazu globalnego są również używane podczas przetwarzania logowania użytkownika. Ilekroć użytkownik loguje się w domenie, następuje kontakt z serwerem wykazu globalnego. Dzieje się tak, ponieważ kontroler domeny wykazu nie-globalnego nie zawiera informacji o członkostwie w grupach uniwersalnych. Grupy uniwersalne mogą zawierać konta dowolnej domeny danego lasu. Ponieważ członkostwo w grupie uniwersalnej dotyczy całego lasu, informacje o członkostwie mogą być znalezione jedynie przez kontroler domeny, który posiada informacje o katalogu całego lasu, czyli informacje wykazu globalnego. W celu wygenerowania dokładnego tokenu zabezpieczeń dla użytkownika żądającego uwierzytelnienia wykaz globalny musi być użyty do określenia członkostwa w grupach uniwersalnych.



Uwaga System Windows Server 2008 obsługuje funkcję nazwaną *universal group membership caching* (buforowanie członkostwa grupy uniwersalnej), która umożliwia zalogowanie się do sieci systemu Windows Server 2008 bez połączenia z wykazem globalnym. Członkostwo w grupie uniwersalnej może być buforowane na kontrolerach domeny wykazu nie-globalnego po zalogowaniu się użytkownika do tego kontrolera domeny. Po uzyskaniu tych informacji z wykazu globalnego, są one stale buforowane na kontrolerze domeny lokacji i są okresowo aktualizowane (domyślnie co 8 godzin). Włączenie tej funkcji powoduje skrócenie czasu logowania użytkowników w lokacjach zdalnych, jeśli uwierzytelniające kontrolery domen nie mają dostępu do wykazu globalnego. W rozdziale 5 zamieszczono bardziej szczegółowe informacje na temat planowania i konfigurowania funkcji buforowania członkostwa w grupie uniwersalnej.

Serwer wykazu globalnego potrzebny jest również do przetworzenia logowania użytkownika, jeśli użytkownik korzysta z głównej nazwy użytkownika UPN (User Principal Name). Nazwy UPN umożliwiają użytkownikom logowanie się do komputerów w dowolnej domenie lasu przy użyciu spójnej nazwy użytkownika. Format nazwy UPN jest następujący: *nazwa_użytkownika@nazwa_domeny*, ale nazwa domeny nie musi być domeną, w której znajduje się konto użytkownika. W celu zidentyfikowania domeny użytkownika nazwa UPN musi być rozpoznana w wykazie globalnym.

Kontrolery domeny przeznaczone tylko do odczytu

Kontrolery domen przeznaczone tylko do odczytu (RODC) są jeszcze innym rodzajem kontrolerów domen dostępnych w usługach AD DS systemu Windows Server 2008. Kontrolery RODC utrzymują wersję bazy danych usług AD DS przeznaczoną tylko do odczytu i udostępniają wszystkie usługi dotyczące uwierzytelniania i autoryzacji oferowane przez inne kontrolery domen.

Kontrolery RODC są głównie przeznaczone do instalowania w biurach oddziałowych, gdzie nie może być zapewnione bezpieczeństwo fizyczne kontrolera lub w sytuacjach, gdzie zachodzi obawa o bezpieczeństwo magazynu lokalnego haseł domeny. Kontrolery RODC mogą także zawierać przeznaczoną tylko do odczytu wersję stref DNS zintegrowanych z usługami AD DS i mogą być konfigurowane jako serwery wykazu globalnego.



Uwaga W celu zapewnienia dodatkowego bezpieczeństwa warto przeanalizować instalowanie kontrolerów RODC w systemie Windows Server 2008 Server Core. Ta opcja instalacji nie udostępnia żadnego graficznego narzędzia administracji. Ponadto, ponieważ kontrolery RODC mogą być instalowane w lokacjach uważanych za niebezpieczne, w takich lokacjach nie należy instalować zwykłych kontrolerów domen.

Buforowanie poświadczeń na kontrolerach RODC

Jedną z opcji konfiguracji dostępnych dla kontrolera RODC jest funkcja buforowania poświadczeń. Buforowanie poświadczeń dotyczy magazynu haseł, który jest skojarzony z podmiotami zabezpieczeń. Wszystkie kontrolery domen z możliwością zapisu mają dostęp do wszystkich poświadczeń podmiotów zabezpieczeń. W celu zapewnienia dodatkowego bezpieczeństwa dla kontrolera RODC można określać, które poświadczenia zostaną buforowane na kontrolerze RODC.

Domyślnie żadne poświadczenia inne niż konto komputera RODC i specjalne konto krbtgt nie są przechowywane na kontrolerze RODC. Oznacza to, że kontroler RODC musi mieć udostępnione połączenie z kontrolerem domeny z możliwością zapisu, o ile użytkownicy lub komputery uwierzytelniają się na tym kontrolerze RODC. Kiedy kontroler RODC odbiera żądanie uwierzytelnienia, przekierowuje żądanie do kontrolera domeny z możliwością zapisu.

Poprzez konfigurowanie zasady replikacji haseł (Password Replication Policy) dla kontrolera RODC można modyfikować domyślną konfigurację buforowania poświadczeń. Na przykład można utworzyć taką konfigurację tej zasady, aby poświadczenia wszystkich kont użytkowników, komputerów i usług w biurze oddziału były buforowane na kontrolerze RODC. Modyfikując zasadę replikacji haseł trzeba pamiętać, że hasła będą buforowane

na kontrolerze RODC po pierwszym pomyślnym zalogowaniu podmiotu zabezpieczeń zidentyfikowanego przez zasadę. Po pomyślnym uwierzytelnieniu konta kontroler RODC próbuje skontaktować się z kontrolerem domeny z możliwością zapisu w lokacji centralnej i żąda kopii odpowiednich poświadczeń. Kontroler domeny z możliwością zapisu rozpoznaje, że żądanie przesłane zostało przez kontroler RODC i sprawdza informacje w zasadzie replikacji haseł. Jeśli zasada (Password Replication Policy) pozwala, kontroler domeny z możliwością zapisu replikuje poświadczenia do kontrolera RODC, a ten będzie je buforował. Po zbuforowaniu poświadczeń na kontrolerze RODC, kontroler RODC może bezpośrednio obsługiwać żądania logowania użytkownika, chyba że następuje zmiana poświadczeń lub zasady replikacji haseł.

Ograniczając buforowanie poświadczeń na kontrolerze RODC można ograniczać potencjalne ujawnienie poświadczeń w przypadku kradzieży kontrolera RODC. Zazwyczaj tylko mały zestaw użytkowników domeny ma poświadczenia buforowane przez dany kontroler RODC. Z tego względu, w przypadku kradzieży kontrolera RODC, potencjalnie ujawnione zostają tylko poświadczenia buforowane na tym kontrolerze. W takim przypadku w prosty sposób można posłużyć się konsolą Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory) do zidentyfikowania, które poświadczenia są buforowane na serwerze i zresetować hasła dla wszystkich tych kont.

Aby obsługiwać zasadę replikacji haseł kontrolera RODC, w usługach AD DS systemu Windows Server 2008 dołączono nowe atrybuty przypisane do kontrolera RODC:

- ***msDS-Reveal-OnDemandGroup*** Atrybut ten identyfikuje grupę, której członkowie mogą mieć buforowane poświadczenia na kontrolerze RODC.
- ***msDS-NeverRevealGroup*** Atrybut ten identyfikuje grupę charakterystyczną tym, że poświadczenia dla jej członków nie mogą być buforowane na kontrolerze RODC. Domyślnie atrybut ten zawiera wszystkie konta administratorów. Atrybut ten nie wpływa na możliwości tych podmiotów zabezpieczeń w zakresie uwierzytelniania przy użyciu kontrolera RODC.
- ***msDS-RevealedList*** Atrybut ten jest listą podmiotów zabezpieczeń, dla których kontroler RODC buforuje poświadczenia.
- ***msDS-AuthenticatedToAccountList*** Atrybut ten zawiera listę podmiotów zabezpieczeń domeny lokalnej, które zostały uwierzytelnione w kontrolerze RODC. Można określić, które komputery i użytkownicy korzystają z kontrolera RODC do logowania poprzez uzyskanie dostępu do właściwości kontrolera RODC w konsoli Active Directory Users and Computers. Dzięki temu można dostosowywać zasadę replikacji haseł (Password Replication Policy) dla kontrolera RODC.

Delegowanie uprawnień administracyjnych do kontrolera RODC

Inną funkcją udostępnianą przez kontrolery RODC jest separacja roli administratora (Administrator Role Separation), która umożliwia konfigurowanie dla kontrolera RODC delegowanego administratora lokalnego bez przydzielania żadnych uprawnień na poziomie domeny. Delegowany administrator może zalogować się do kontrolera RODC w celu wykonania zadań konserwacji serwera, takich jak aktualizacja sterownika. Delegowany administrator nie może jednak zalogować się do innego kontrolera domeny lub wykonywać inne zadania administracyjne w domenie. Delegowanie uprawnień administracyjnych do kontrolera

RODC warto przeanalizować, jeśli kontroler domeny jest zlokalizowany w biurze oddziałowym, w którym nie pracuje żaden administrator domeny dla tej lokacji.



Alert zabezpieczeń Delegowani administratorzy lokalni kontrolera RODC mają bezpośredni dostęp do plików bazy danych usług AD DS i w związku z tym potencjalnie mogą zdobyć wszystkie informacje przechowywane na kontrolerze RODC, wliczając w to buforowane poświadczenia. Delegowani administratorzy lokalni powinni być osobami o najwyższym zaufaniu.



Uwaga Delegowanego administratora lokalnego dla kontrolera RODC można dodawać podczas działania programu instalacyjnego usługi AD DS (Active Directory Domain Services Installation Wizard). Podczas delegowania uprawnień administratora lokalnego, konto użytkownika nie jest dodawane do żadnej dodatkowej grupy zabezpieczeń. Zamiast tego, nazwa użytkownika lub grupy przechowywana jest w atrybucie obiektu komputera RODC w usługach AD DS, który jest używany, kiedy użytkownik próbuje zalogować się do kontrolera RODC. Należy zwrócić uwagę, że poświadczenia delegowanego administratora lokalnego nie są domyślnie buforowane na kontrolerze RODC. Oznacza to, że delegowany administrator lokalny nie będzie mógł zalogować się do kontrolera RODC, jeśli nie jest dostępny kontroler domeny z możliwością zapisu. Należy przeanalizować to ustawienie, jeśli administrator lokalny będzie potrzebny do obsługi kontrolera RODC w sytuacji awarii łącza WAN. Aby dodać administratorów lokalnych do grupy administracyjnej kontrolera RODC po skonfigurowaniu usług AD DS, należy użyć narzędzia wiersza polecenia Dsmgmt.exe. Dokładne informacje na ten temat znaleźć można w rozdziale 6 „Instalowanie usług AD DS (Active Directory Domain Services)".

Ograniczenia kontrolera RODC

Niektóre opcje kontrolera domeny (dostępne dla kontrolera domeny z możliwością zapisu) nie są dostępne dla kontrolera RODC. Kontroler RODC nie może:

- **Pełnić roli wzorca operacji** System pełniący rolę wzorca operacji musi mieć możliwość zapisu informacji do bazy danych usług AD DS. Na przykład dla wzorca schematu musi istnieć możliwość zapisu definicji nowych klas obiektów i atrybutów. Identyfikator względny (RID) wzorca musi mieć możliwość zapisu wartości pul identyfikatorów RID, które są przypisane do innych kontrolerów domen. Ze względu na to, że kontroler RODC może tylko odczytywać bazę danych usług AD DS, nie może działać jako wzorzec operacji.
- **Pełnić funkcji serwera czołowego (bridgehead)** Serwery typu bridgehead są serwerami przeznaczonymi do replikowania zmian pomiędzy lokacjami. Ponieważ za pośrednictwem procesu replikacji kontrolery RODC mogą tylko odbierać zmiany, a nie mogą przesyłać aktualizacji replikacji, to nie mogą działać jako serwery czołowe lokacji. Jeśli kontroler RODC jest instalowany w lokacji wraz z innym kontrolerami domen w tej samej domenie lub lesie, jeden z innych kontrolerów domeny zostanie skonfigurowany dla lokacji jako serwer czołowy.



Na dysku CD Skrypt ListDomainControllers.ps1 powłoki Windows PowerShell (znajdujący się na dołączonym dysku CD) może być używany do utworzenia listy kontrolerów domeny danej domeny i listy serwerów wykazu globalnego w lesie. Jeśli powłoka Windows PowerShell uruchomiona jest w systemie Windows Server 2008, trzeba skonfigurować zasadę wykonywania skryptu PowerShell tak, aby dopuścić niepodpisane certyfikaty (uruchamiając polecenie Set-ExecutionPolicy RemoteSigned). Ponadto podczas uruchamiania skryptu powłoki PowerShell należy wprowadzać pełną ścieżkę.

Przykłady skryptów języka Visual Basic Scripting Edition (VBScript), które można używać do uzyskania informacji usług AD DS, znaleźć można w witrynie Script Center pod adresem *http://www.microsoft.com/technet/scriptcenter/scripts/default.mspx?mfr=true*.

Wzorce operacji

Usługi AD DS zostały zaprojektowane jako system replikacji z wieloma wzorcami (multimaster), co wiąże się z wymaganiem, aby wszystkie kontrolery, inne niż kontrolery RODC, miały uprawnienie Write (Zapis) do bazy danych katalogu. System ten funkcjonuje dobrze dla większości operacji katalogowych, ale dla niektórych operacji wymagany jest pojedynczy serwer autorytatywny. Kontrolery domen, które spełniają określone role, są nazywane wzorcami operacji, a każdy spełnia rolę elastycznych operacji pojedynczego wzorca FSMO (Flexible Single-Master Operations; wymowa *fizz-mo*). Kontrolery domen, które utrzymują rolę wzorca operacji, są przeznaczone do wykonywania określonych zadań w celu zapewnienia spójności i wyeliminowania wpisów w bazie danych AD DS, które potencjalnie powodują konflikty. W usługach AD DS rozróżnianych jest pięć ról wzorca operacji:

- Wzorzec schematu
- Wzorzec nazw domen
- Wzorzec RID
- Emulator PDC
- Wzorzec infrastruktury

Dwie pierwsze role, wzorzec schematu i nazw domen, są rolami odnoszonymi do lasu, co oznacza, że w danym lesie może być tylko jeden wzorzec schematu i tylko jeden wzorzec nazw domen. Pozostałe trzy role odnoszone są do domeny – dla każdej domeny w lesie istnieje jeden z tych wzorców operacji. Podczas instalowania usług AD DS i tworzenia w lesie pierwszego kontrolera domeny, kontroler ten spełniać będzie wszystkie pięć ról. Podobnie, jeśli do lasu dodawana jest domena, pierwszy kontroler domeny w każdej nowej domenie będzie także uzyskiwał rolę wzorca operacji odnoszących się do domeny. Dodając kontrolery domeny do domeny można transferować te role do innych kontrolerów domeny.

Wzorzec schematu

Wzorzec schematu jest jedynym kontrolerem domeny, który ma uprawnienia Write (Zapis) do schematu katalogu. W celu zmodyfikowania schematu administrator (który musi być członkiem grupy zabezpieczeń Schema Admins) musi być podłączony do wzorca schematu. Nie powiedzie się próba modyfikacji schematu na kontrolerze domeny innym, niż wzorzec

schematu. Po wprowadzeniu zmian w schemacie aktualizacje schematu są replikowane do wszystkich pozostałych kontrolerów domen w lesie.

Wzorzec schematu jest identyfikowany poprzez wartość atrybutu *fSMORoleOwner* obiektu katalogu głównego (root) partycji schematu. Domyślnie pierwszy kontroler domeny zainstalowany w lesie obejmuje rolę wzorca schematu. Rola ta może być przekazywana w dowolnym momencie przy użyciu przystawki Active Directory Schema (Schemat usługi Active Directory) lub przy użyciu narzędzia wiersza polecenia Ntdsutil.

Wzorzec nazw domen

Wzorzec nazw domen jest kontrolerem domeny, który zarządza dodawaniem i usuwaniem wszystkich partycji katalogu w hierarchii lasu. Kontroler domeny pełniący tę rolę musi być dostępny podczas:

- **Dodawania lub usuwania domen** Podczas tworzenia lub usuwania domeny podrzędnej lub nowego drzewa domeny program instalacyjny kontaktuje się ze wzorcem nazw domen i żąda dodania lub usunięcia. Wzorzec nazw domen jest odpowiedzialny za to, aby nazwy domen nie powtarzały się. Jeśli wzorzec nazw domen nie jest dostępny, w lesie nie można dodać lub usunąć domeny.
- **Dodawania lub usuwania partycji katalogu aplikacji** Partycje katalogu aplikacji są specjalnymi partycjami, które mogą być tworzone na kontrolerach domen systemu Windows Server 2003 lub Windows Server 2008 w celu udostępnienia magazynu dla dynamicznych danych aplikacji. Jeśli kontroler domeny spełniający rolę wzorca operacji nazw domeny nie jest dostępny, w lesie nie jest możliwe dodanie lub usunięcie partycji katalogu aplikacji.
- **Dodawania lub usuwania obiektów wzajemnych odwołań** Podczas tworzenia nowego lasu, na pierwszym kontrolerze domeny w lesie tworzony jest schemat, konfiguracja i partycja katalogu domeny. Dla każdej partycji katalogu w kontenerze Partitions (Partycje) w partycji konfiguracji katalogu (*CN=partitions,CN=configuration, DC=forestRootDomain*) tworzony jest obiekt wzajemnych odwołań (cross-reference object). Jeśli tworzone są nowe domeny lub partycje katalogu aplikacji, to w kontenerze Partitions tworzony jest także skojarzony obiekt odwołań wzajemnych. Jeśli wzorzec nazw domen nie jest dostępny, nie będzie możliwe dodawanie lub usuwanie obiektów odwołań wzajemnych.
- **Walidacji instrukcji zmiany nazwy domeny** Podczas używania narzędzia zmiany nazwy domeny, Rendom.exe, aby zmienić nazwę domeny usługi AD DS, narzędzie musi mieć możliwość uzyskania dostępu do wzorca operacji nazw domen. W trakcie działania tego narzędzia skrypt języka XML zawierający instrukcje zmiany nazwy domeny wprowadza zapisy w atrybucie *msDS-UpdateScript* w obiekcie kontenera Partitions *(CN=partitions,CN=configuration,DC=ForestRootDomain)* w partycji konfiguracji katalogu. Ponadto nowa nazwa DNS każdej domeny, dla której zmieniana jest nazwa, jest również zapisywana przez narzędzie Rendom.exe do atrybutu *msDS-DnsRootAlias* obiektu wzajemnych odwołań (klasa *crossRef*) dotyczącego tej domeny. Oba te obiekty przechowywane są w kontenerze Partitions, a kontener może być tylko aktualizowany na kontrolerze domeny spełniającym w lesie rolę wzorca operacji nazw domeny.

Wzorzec nazw domeny jest identyfikowany poprzez wartość atrybutu *fSMORoleOwner* obiektu kontenera Partitions. Domyślnie pierwszy kontroler domeny zainstalowany w lesie obejmuje rolę wzorca nazw domen. Rola ta może być przekazywana w dowolnym momencie przy użyciu przystawki Active Directory Domains and Trusts (Domeny i relacje zaufania usługi Active Directory) lub przy użyciu narzędzia wiersza polecenia Ntdsutil.

Wzorzec RID

Wzorzec RID jest rolą wzorca operacji odnoszącym się do domeny. Jest używany do zarządzania pulą identyfikatorów RID w celu utworzenia nowych podmiotów zabezpieczeń w całej domenie, takich jak użytkownicy, grupy i komputery. Dla każdego podmiotu zabezpieczeń wydawany jest unikalny identyfikator zabezpieczeń SID (security identifier), który zawiera identyfikator domeny (identyczny dla wszystkich identyfikatorów SID w domenie) i względny identyfikator RID (relative identifier), który jest unikalny dla każdego podmiotu zabezpieczeń. Ponieważ podmioty zabezpieczeń mogą być tworzone na dowolnym kontrolerze domeny zawierającym kopie katalogu z możliwością jej zapisu, to wzorzec RID jest używany do uniemożliwienia wydania tego samego identyfikatora RID przez dwa kontrolery domeny. Wzorzec RID wydaje blok identyfikatorów RID (nazywanych pulą identyfikatorów RID) każdemu kontrolerowi domeny w danej domenie. Jeśli na kontrolerze domeny liczba dostępnych identyfikatorów RID w puli zmniejsza się (mniej więcej poniżej 100), do wzorca RID generowane jest żądanie uzyskania następnego bloku identyfikatorów RID. W takiej sytuacji wzorzec RID wydaje pulę około 500 identyfikatorów RID.

Jeśli wzorzec RID jest niedostępny przez pewien okres czasu, proces tworzenia nowych kont na określonym kontrolerze domeny może zostać przerwany. Mechanizm żądania nowego bloku identyfikatorów RID został tak zaprojektowany, aby opisywana sytuacja nie miała miejsca, ponieważ żądanie jest generowane zanim w puli wyczerpią się wszystkie dostępne identyfikatory RID. Jednakże, jeśli wzorzec RID jest w trybie offline, a kontroler domeny zużyje wszystkie dostępne mu identyfikatory, to utworzenie kona nie powiedzie się. W celu ponownego umożliwienia tworzenia kont system spełniający rolę wzorca RID musi zacząć pracować w trybie online lub rola ta musi zostać przeniesiona do innego kontrolera domeny.

Wzorzec RID jest identyfikowany poprzez wartość atrybutu *fSMORoleOwner* obiektu partycji domeny, którego klasa to *rIDManager*. Domyślnie pierwszy kontroler domeny instalowany w nowej domenie obejmuje rolę wzorca RID. Rola ta może być transferowana w dowolnym momencie przy użyciu przystawki Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory) lub przy użyciu programu narzędziowego wiersza polecenia Ntdsutil.

Emulator PDC

System spełniający rolę emulatora PDC funkcjonuje jako główny kontroler domeny PDC (primary domain controller) dla systemów operacyjnych wcześniejszych niż system Windows 2000. Serwery członkowskie systemu Windows NT i komputery klienckie muszą mieć możliwość komunikowania się z kontrolerem PDC w celu przetworzenia zmian haseł. Oprócz udostępniania usług dla starszych klientów emulator PDC pełni także ważną rolę w replikowaniu haseł.



Uwaga W usługach Active Directory systemów Windows 2000 i Windows 2003 jedną z ważnych ról emulatora PDC jest rola kontrolera PDC dla starszych (systemy Microsoft Windows NT 3.51 lub Windows NT 4.0) kontrolerów kopii zapasowych BDC (backup domain controller). Ponieważ system Windows Server 2008 nie obsługuje „koegzystencji" z kontrolerami domen systemów starszych niż system Windows 2000, funkcja ta straciła na znaczeniu.

Nawet jeśli w domenie nie istnieją serwery członkowskie systemu Windows NT lub komputery klienckie, emulator PDC ma do spełnienia rolę w utrzymaniu aktualizacji haseł. Wszystkie modyfikacje haseł przeprowadzone na innych kontrolerach domen w domenie są przesyłane do emulatora PDC przy użyciu pilnej replikacji. Jeśli uwierzytelnienie nie powiedzie się na kontrolerze domeny innym niż emulator PDC, proces uwierzytelnienia jest ponownie przeprowadzany na emulatorze PDC. Jeśli emulator PDC zaakceptował ostatnie zmiany hasła danego konta, uwierzytelnienie przeprowadzone zostanie pomyślnie. Jeśli użytkownik pomyślnie uwierzytelni się na kontrolerze domeny, na którym poprzednio nie powiodła się próba uwierzytelnienia, kontroler domeny powiadomi emulator PDC o pomyślnym uwierzytelnieniu. Powiadomienie to zeruje licznik blokady konta na emulatorze PDC w przypadku, kiedy inny klient będzie próbował sprawdzić to samo konto przy użyciu innego kontrolera.

Emulator PDC identyfikowany jest poprzez wartość atrybutu *fSMORoleOwner* obiektu katalogu głównego (root) partycji domeny. Domyślnie pierwszy kontroler domeny zainstalowany w nowej domenie obejmuje rolę emulatora PDC. Rola ta może być transferowana w dowolnym momencie przy użyciu przystawki Active Directory Users and Computers (Użytkownicy i komputery usług Active Directory) lub narzędzia wiersza polecenia Ntdsutil.

Wzorzec infrastruktury

Wzorzec infrastruktury jest odpowiedzialny za aktualizację pomiędzy domenami odniesień typu grupa-użytkownik. Ta rola wzorca operacji zapewnia, że modyfikacje nazw obiektów (zmiany atrybutu nazwy pospolitej, *cn*) zostają odzwierciedlone w informacjach o członkostwie w grupach dla grup znajdujących się w innych domenach. Wzorzec infrastruktury utrzymuje aktualną listę tych odniesień, a następnie replikuje te informacje do wszystkich innych kontrolerów domeny w domenie. Jeśli wzorzec infrastruktury nie jest dostępny, to pomiędzy domenami nie będą aktualne odniesienia typu grupa-użytkownik.

Wzorzec infrastruktury jest identyfikowany poprzez wartość atrybutu *fSMORoleOwner* kontenera Infrastructure partycji domeny (*CN=Infrastructure, DC=domain*). Domyślnie pierwszy kontroler domeny zainstalowany w nowej domenie obejmuje rolę wzorca infrastruktury. Rola ta może być transferowana w dowolnym momencie przy użyciu przystawki Active Directory Users and Computers (Użytkownicy i komputery usług Active Directory) lub narzędzia wiersza polecenia Ntdsutil.



Na dysku CD W celu wyświetlenia, które kontrolery domen w danym lesie i domenie pełnią rolę FSMO, należy uruchomić skrypt ListFSMOs.ps1 w powłoce Windows PowerShell znajdujący się na dołączonym dysku CD.

Transfer ról wzorców operacji

Role wzorców operacji mogą być przenoszone pomiędzy kontrolerami domen w celu zoptymalizowania wydajności kontrolera domeny lub zastąpienia kontrolera domeny, jeśli dany system staje się niedostępny. Proces transferu zależny jest od roli, która ma być przenoszona. W tabeli 2-2 wymienione zostały narzędzia używane do transferu ról wzorców operacji.

Tabela 2-2 Narzędzia zarządzania wzorcami operacji

Rola wzorca operacji	Narzędzie administracji
Wzorzec schematu	Active Directory Schema (Schemat usługi Active Directory)
Wzorzec nazw domen	Active Directory Domains And Trusts (Domeny i relacje zaufania usługi Active Directory)
Wzorzec RID, emulator PDC i wzorzec infrastruktury	Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory)

W celu przeniesienia roli wzorca operacji musi być zapewniona łączność z bieżącym i proponowanym kontrolerem domeny. W przypadku awarii serwera, serwer aktualnie pełniący rolę może nie być dostępny, to rola może zostać przejęta. Przejmowanie ról wzorca operacji nie jest zalecaną opcją i powinno być wykonywane, tylko jeśli jest to absolutnie konieczne, czyli jeśli wiadomo, że kontroler domeny pełniący tę rolę będzie niedostępny przez długi okres czasu. Dodatkowe informacje na temat przejmowania ról wzorców operacji znaleźć można w rozdziale 15.



Uwaga Role wzorców operacji mogą być przenoszone do dowolnego kontrolera domeny w danej domenie. Jedyne ograniczenie przemieszczania wzorca operacji wiąże się z rolą wzorca infrastruktury, która nie powinna być instalowana na kontrolerze domeny będącym również serwerem wykazu globalnego, jeśli las zawiera wiele domen, chyba że każdy kontroler domeny w domenie jest również serwerem wykazu globalnego. Domyślnie pierwszy kontroler domeny w lesie jest zarówno serwerem wykazu globalnego, jak i wzorcem infrastruktury. Podczas instalowania drugiego kontrolera domeny, który nie jest serwerem wykazu globalnego, w trakcie instalowania usług AD DS program instalacyjny Active Directory Domain Services Installation Wizard monituje administratora o przeniesienie wzorca infrastruktury do nowego kontrolera domeny.

Schemat

Schemat definiuje każdą klasę i atrybut, który może być przechowywany w usługach AD DS. Każdy obiekt usług AD DS jest instancją klasy. Przykładami klas jest „user” czy „group”. Zanim obiekt może być utworzony w usługach AD DS, jego klasa musi być wcześniej zdefiniowana w schemacie. Schemat wymusza również kilka reguł dotyczących tworzenia obiektów w bazie danych.

Do jednego lasu odnosi się jeden schemat. Kopie schematu są jednak replikowane do każdego kontrolera domeny w lesie. W ten sposób każdy kontroler domeny ma szybki

dostęp do wszystkich definicji klas lub atrybutów, które mogą być potrzebne, a także dzięki temu podczas tworzenia danego obiektu każdy kontroler domeny posługuje się tą samą definicją. Magazyn danych bazuje na schemacie w celu udostępnienia definicji klas i atrybutów i używa ich do wymuszenia spójności danych. Dzięki temu wszystkie obiekty tworzone są jednolicie i bez znaczenia jest fakt, który kontroler domeny utworzył bądź zmodyfikował obiekt, ponieważ wszystkie kontrolery domen korzystają z tego samego schematu.

Składniki schematu

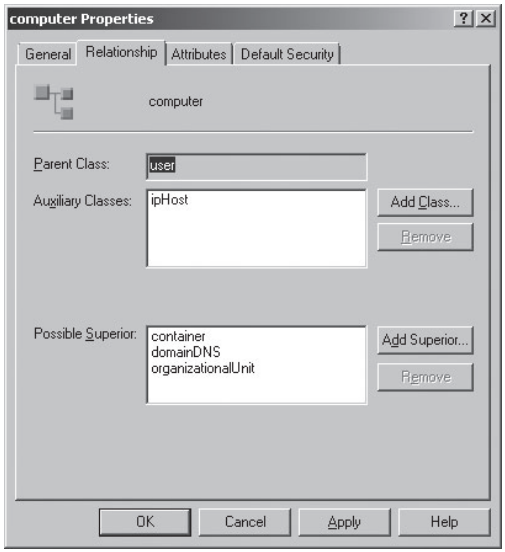
Schemat zbudowany jest z obiektów *classSchema* i *attributeSchema*. Obiekty *classSchema* są definicjami przechowywanymi w schemacie i używanymi do definiowania klas. Klasy definiują grupy atrybutów, które łączą pewne podobieństwa. Przykładem klasy jest klasa *User*, która obejmuje różne atrybuty, wliczając w to nazwę logowania użytkownika, nazwisko, imię i hasło. Ilekroć tworzone jest nowe konto użytkownika, katalog używa klasy *User* do zdefiniowania sposobu skonfigurowania obiektu. Ustawienia określone przez klasę *User* obejmują atrybuty, które obiekt może i musi mieć, oraz określają, które klasy mogą być nadrzędnymi obiektu w hierarchii usług AD DS. Każdy utworzony obiekt użytkownika używa tych atrybutów.

Schemat definiuje również atrybuty, które mogą być przechowywane dla każdej klasy. Atrybuty są definiowane globalnie w usługach AD DS jako obiekty *attributeSchema,* a każda klasa może korzystać z wielu globalnie zdefiniowanych atrybutów. Na przykład obiekt konta użytkownika ma kilka atrybutów, które są używane do przechowywania różnych fragmentów danych odnoszących się do konta użytkownika, takich jak atrybut nazwy logowania czy atrybut hasła. Każdy z tych atrybutów jest definiowany przez obiekty atrybutów, które mają również swoje własne definicje specyfikujące informacje, takie jak typ przechowywanych danych czy minimalna bądź maksymalna długość lub wartość. Usługa katalogowa używa obiektów *attributeSchema* do definiowania typu danych przechowywanych w atrybutach dla każdego obiektu danej klasy i do wymuszania ograniczeń zdefiniowanych w obiekcie *attributeSchema* (na przykład zakres długości łańcucha).

Obiekt *classSchema specyfikuje atrybuty* skojarzone z obiektem. Specyfikacja obejmuje wszystkie atrybuty, które mogą być skojarzone z obiektem i które są podzielone na cztery kategorie:

- *mustContain* – kategoria obejmuje wymagane atrybuty, które muszą być prezentowane w każdym obiekcie będącym instancją tej klasy
- *mayContain* – kategoria obejmuje opcjonalne atrybuty, które mogą znaleźć się w obiekcie będącym instancją tej klasy
- *systemmayContain* – kategoria obejmuje opcjonalne atrybuty skonfigurowane podczas tworzenia obiektu i które nie mogą być modyfikowane po utworzeniu obiektu
- *systemmustContain* – kategoria obejmuje wymagane atrybuty skonfigurowane podczas tworzenia obiektu i które nie mogą być modyfikowane po utworzeniu obiektu

Oprócz tego obiekt *classSchema* specyfikuje reguły hierarchii, które określają możliwe katalogi nadrzędne w drzewie katalogu obiektu, który jest instancją klasy. Na przykład, zgodnie z rysunkiem 2-3, obiekt komputera może być tylko utworzony w obiektach *container, domainDNS lub organizationUnit*.



Rysunek 2-3 Schemat definiuje, gdzie obiekty mogą być tworzone w usługach AD DS.

Na koniec, typ danych, które mogą być przechowywane w usługach AD DS dla każdego atrybutu, jest definiowany w schemacie składnia atrybutu. Klasa *User* zawiera atrybut nazwany *displayName*, a składnia atrybutu została zdefiniowana jako ciąg wartości, który akceptuje dowolne znaki alfanumeryczne. Wartość każdego atrybutu zawarta w instancji klasy musi spełniać wymagania składni tego atrybutu.

Schemat usług AD DS obsługuje dziedziczenie klas. Wszystkie obiekty schematu są zorganizowane hierarchicznie. Ze względu na tę hierarchiczną strukturę każda klasa może dziedziczyć wszystkie charakterystyki swojej klasy nadrzędnej. Na przykład (rysunek 2-3) klasa *Computer* jest w rzeczywistości podklasą klasy *User*. I w takim przypadku klasa *Computer* dziedziczy wszystkie atrybuty skojarzone z klasą *User*. Klasa *Computer* zostaje następnie skojarzona z atrybutami specyficznymi dla kasy *User*. Korzystając z przystawki Active Directory Schema (Schemat usługi Active Directory) można przeglądać organizację dziedziczenia klas i hierarchię klas obiektów. Ten system dziedziczenia jest znacznie łatwiejszy dla administratorów przy tworzeniu nowych klas obiektów, ponieważ nie muszą definiować każdego atrybutu skojarzonego z nową klasą. Nowy obiekt po prostu dziedziczy wszystkie skojarzenia atrybutów odpowiedniej klasy nadrzędnej.

Modyfikowanie schematu

Schemat usług AD DS zawiera najczęściej używane klasy i atrybuty potrzebne do obsługi implementacji usług katalogowych przedsiębiorstwa. Aby obsługiwać aplikacje, które wymagają przechowywania informacji w schemacie usług AD DS, projekt schematu zakłada możliwość jego rozszerzania. Inaczej mówiąc, schemat może być modyfikowany lub rozszerzany, aby objąć nowe obiekty klas i atrybutów, które mogą być potrzebne w organizacji.

Schemat jest najczęściej rozszerzany, aby spełnić potrzeby aplikacji korzystających z usług Active Directory. Dobrym tego przykładem jest aplikacja Microsoft Exchange Server 2007, która przeprowadza ponad tysiąc modyfikacji schematu, dzięki którym usługi AD DS mogą obsługiwać program Exchange Server.



Uwaga Przed zainstalowaniem programu Exchange 2000, Exchange 2003 lub Exchange 2007 należy zmodyfikować schemat. Pliki instalacji programu Exchange obejmują kilka plików LDIF, które podczas importowania przeprowadzają odpowiednie zmiany schematu. Jeśli instalowana jest inna aplikacja, która wymaga modyfikacji schematu, schemat powinien być modyfikowany jedynie za pomocą plików LDIF, które zostały rzetelnie przetestowane, co pozwala uniknąć pomyłek przy modyfikowaniu schematu.

Zasada działania: Indeksowanie w celu optymalizacji wyszukiwań

Magazyn danych katalogu może być indeksowany, co poprawia efektywność wyszukiwań. Indeksowanie zostało wyspecyfikowane jako część definicji schematu atrybutu (takiego jak *Description* lub *givenName*). Podczas indeksowania atrybutu, wszystkie wystąpienia tego atrybutu zostaną dołączone do indeksu. Niektóre atrybuty są indeksowane zgodnie z ustawieniami domyślnymi, a administrator może określać dodatkowe atrybuty, które mają być indeksowane. Dostępnych jest wiele typów indeksowania, w zależności od tego, w jaki sposób atrybut będzie używany podczas wyszukiwań:

- **Indeksy podstawowe** Wartość (lub wartości) atrybutu zostają indeksowane tak, aby szybciej działały kwerendy żądające obiektów o określonej wartości tego atrybutu.
- **Indeksy konteneryzowane** Indeksowanie jest podobne do podstawowego, z tym że obiekty są również indeksowane według kontenera. Dzięki temu zapytanie może szybko sprawdzić wszystkie obiekty podrzędne w kontenerze, aby określić, które są zgodne z żądaną wartością atrybutu.
- **Indeksy krotkowe** Używane dla ciągu atrybutów tak, aby podciąg wyszukiwań określony dla tego atrybutu działał szybciej. Na przykład, zastosowanie indeksu krotkowego do atrybutu *Description* umożliwi efektywniejsze działanie zapytaniom, takim jak „zwróć wszystkie obiekty, których atrybut *Description* w dowolnym miejscu zawiera ciąg Fabrikam”. Utrzymywanie indeksów krotkowych może pochłaniać dużą ilość zasobów, tak więc metoda powinna być włączana oszczędnie.
- **Indeksy poddrzewa** Umożliwiają szybsze wykonanie specjalnego typu wyszukiwania usługi Active Directory, znanego jako przeglądanie listy wirtualnej. Mechanizm podobny jest do indeksów konteneryzowanych, z tym że obejmuje nie tylko bezpośrednio podrzędne kontenery, ale także wszystkie zagnieżdżone głębiej. Podobnie jak indeksy krotek, indeksy poddrzewa mogą pochłaniać dużo zasobów.

Administratorzy mogą włączać indeksowanie atrybutów, które domyślnie nie są indeksowane, opierając się na potrzebach danej organizacji. Indeksy podstawowe i konteneryzowane mogą być włączane przy użyciu przystawki Active Directory Schema. Indeksy krotki i poddrzewa jednak wymagają ręcznego ustawienia wartości atrybutu *searchFlags* dla obiektów *attributeSchema* definiujących atrybuty, które mają być indeksowane.

Indeksowanie krotki i sposób włączania tej funkcji omówiono bardziej szczegółowo w artykule dostępnym pod adresem *http://msdn2.microsoft.com/en-us/library/ms676931.aspx*. Atrybut *searchFlags* zawierający wartości ustawiające indeksy krotki i poddrzewa zostały omówione w artykule dostępnym pod adresem *http://msdn2.microsoft.com/en-us/library/ms679765.aspx*.

Matthew Rimer
Senior SDE, US-Directory and Service Business

Za wyjątkiem sytuacji dotyczących aplikacji korzystających z usług Active Directory, administratorzy mogą rozszerzać schemat przy użyciu różnych innych metod. Schemat może być rozszerzany w trybie wsadowym przy użyciu narzędzi administracyjnych wiersza polecenia, a w tym narzędzia LDIFDE (LDAP Data Interchange Format Directory Exchange) i CSVDE (Comma Separated Value Directory Exchange). Schemat może być również rozszerzany programowo przy użyciu skryptów interfejsu ADSI (Active Directory Service Interfaces) programu Microsoft Visual Basic.

Na koniec schemat można modyfikować z interfejsu użytkownika systemu Windows Server 2008 przy użyciu przystawki Active Directory Schema (Schemat usługi Active Directory). Na przykład w organizacji może zachodzić potrzeba zachowywania rekordów dotyczących początkowych dat zatrudnienia. Daty te można przechowywać jako atrybut obiektu użytkownika w usługach AD DS. Domyślnie usługi AD DS nie obejmują tego atrybutu. Aby udostępnić ten atrybut podczas tworzenia nowego obiektu użytkownika, atrybut należy najpierw zdefiniować w schemacie.

Aby używać przystawki Active Directory Schema, należy ją najpierw zarejestrować poprzez wykonanie polecenia Regsvr32 Schmmgmt.dll w wierszu polecenia, a następnie należy dodać przystawkę w konsoli MMC. W celu zmodyfikowania schematu przy użyciu tego interfejsu użytkownik musi należeć do globalnej grupy Schema Admins (Administratorzy schematu).



Ostrzeżenie Pomimo że można dezaktywować zmiany przeprowadzone w schemacie, to nie można usuwać nowych klas i atrybutów utworzonych w schemacie. Modyfikacje schematu należy przeprowadzać tylko po uważnym zaplanowaniu i przetestowaniu w lesie. Należy upewnić się, że modyfikacje schematu są zgodne z aktualnymi i przyszłymi aplikacjami, które wymagają zmian schematu.

Tworzenie nowego atrybutu Aby zastosować przystawkę Active Directory Schema (Schemat usługi Active Directory) do dodania nowego atrybutu do schematu i skojarzenia go z obiektem klasy *User*, należy wykonać następujące operacje:

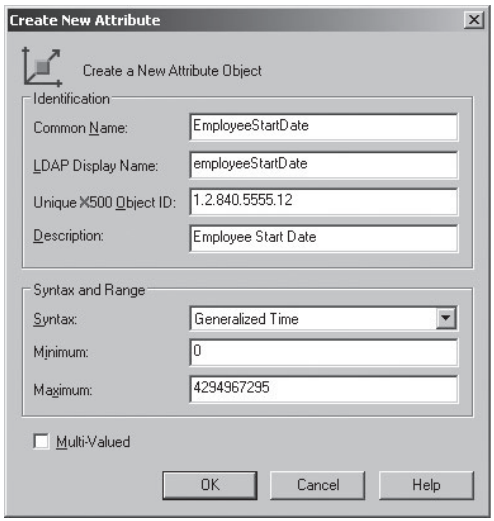
1. Otworzyć przystawkę Active Directory Schema.
2. W oknie drzewa konsoli zaznaczyć folder Attributes (Atrybuty).
3. W menu Action (Akcja) kliknąć polecenie Create Attribute (Utwórz atrybut).
4. W oknie dialogowym Schema Object Creation (Tworzenie obiektu schematu) zawierającym ostrzeżenie o nieodwracalności operacji tworzenia obiektów schematu kliknąć przycisk Continue (Kontynuuj).

5. W oknie dialogowym Create New Attribute (Tworzenie nowego atrybutu) wprowadzić informacje w ramce Identification (Identyfikacja):
   - ❑ Common Name (Nazwa pospolita)
   - ❑ LDAP Display Name (Wyświetlana nazwa LDAP)
   - ❑ Unique X500 Object ID (Unikatowy identyfikator obiektu X500)
   - ❑ Description (Opis)
6. W ramce Syntax and Range (Składnia i zakres) wprowadzić informacje w następujących polach:
   - ❑ Syntax (Składnia)
   - ❑ Minimum
   - ❑ Maximum
   - ❑ Zaznaczyć, czy nowy atrybut jest lub nie jest wielowartościowy (opcja Multi-Valued).



Uwaga Dodatkowe informacje na temat zawartości każdego pola dostępne są poprzez zaznaczenie danego pola tekstowego i naciśnięcie klawisza funkcyjnego F1.

Na rysunku 2-4 zaprezentowany został sposób tworzenia nowego atrybutu przy użyciu przystawki Active Directory Schema.



Rysunek 2-4 Tworzenie atrybutu *EmployeeStartDate* w usługach AD DS.

7. Po utworzeniu nowego atrybutu należy skojarzyć go z obiektem klasy. W tym celu w oknie drzewa konsoli zaznaczyć folder Classes (Klasy).
8. Wyszukać klasę, do której atrybut ma być dodany, kliknąć obiekt prawym przyciskiem myszy, a następnie kliknąć przycisk Properties (Właściwości).
9. Na zakładce Attributes kliknąć przycisk Add (Dodaj) i dodać nowo utworzony atrybut.



Uwaga Dodanie nowego atrybutu do schematu nie oznacza, że atrybut będzie automatycznie dostępny w każdym narzędziu administracyjnym. Narzędzia administracyjne, takie jak Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) dla każdej klasy pokazują niektóre atrybuty, a nie wszystkie atrybuty, które zostały dodane. Jeśli nowy atrybut ma być wyświetlany w narzędziu administracyjnym, należy zmodyfikować istniejące narzędzie lub utworzyć własne. Informacje na temat modyfikowania lub tworzenia narzędzi administracyjnych znaleźć można w artykule „Extending the User Interface for Directory Objects" udostępnionym pod adresem *http://msdn2.microsoft.com/en-us/library/ms676902.aspx*. *Program* ADSIEdit wyświetla nowe atrybuty, ponieważ lista dostępnych atrybutów obiektu jest dynamicznie ładowana ze schematu.

Porady ekspertów: Implementacja aktualizacji schematu

Po utworzeniu nowych atrybutów, nie należy oczekiwać, że nowe atrybuty będą natychmiast dostępne w schemacie. Atrybuty i klasy schematu wewnętrznie określają strukturę bazy danych. Utworzenie nowych klas bądź atrybutów ma znacznie większe oddziaływanie na wydajność kontrolera domeny niż inne zwykle operacje. Ze względu na ważność schematu dla systemu, cała zawartość schematu jest zawsze buforowana w pamięci. Jeśli schemat jest aktualizowany, buforowana kopia schematu musi zostać zaktualizowana, zanim udostępnione będą nowe atrybuty lub klasy. Domyślnie usługi AD DS oczekują pięć minut po wykonaniu ostatnich zmian schematu, zanim zaktualizują bufor schematu.

Główny scenariusz rozszerzeń schematu zakłada instalowanie oprogramowania korzystającego z nowego katalogu (na przykład podczas instalowania oprogramowania Exchange Server bądź uruchomienia programu Adprep w celu zaktualizowania drzewa systemu Windows 2000 lub 2003 do przygotowania dla systemu Windows Server 2008). W takich sytuacjach w schemacie przeprowadzanych jest wiele zmian w krótkim okresie czasu. W wielu przypadkach zmiany schematu powiązane są różnymi zależnościami – na przykład jedna zmiana schematu może tworzyć nowy atrybut, a inna modyfikacja będzie przypisywać ten nowy atrybut do klasy.

Podczas tworzenia plików LDIF w celu aktualizacji schematu zaleca się, aby projektant rozszerzenia schematu dołączał sygnalizację do usług AD DS w celu odświeżenia bufora schematu, zanim użyte zostaną odniesienia do właśnie utworzonych atrybutów lub klas. Zadanie to można zrealizować poprzez ustawienie na wartość 1 atrybutu *schemaUpdateNow* obiektu *rootDSE*. Większość plików sch*.ldf, które używają narzędzia Adprep, realizuje tę operację. Na przykład plik sch43.ldif aktualizuje bufor schematu po utworzeniu nowego atrybutu, a przed użyciem odniesień do tego atrybutu przez nowe klasy. W celu zaktualizowania bufora schematu należy w pliku zamieścić następujące wiersze:

```
DN:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-
```

Elbio Abib, SDE II

Identyfikatory obiektów X.500

Przestrzeń nazw *X.500 OID* jest hierarchiczną strukturą nazewnictwa, która w usłudze katalogowej identyfikuje unikalną liczbę dla każdego obiektu *classSchema* i *attributeSchema*. Przy użyciu identyfikatora OID X.500 (Object Identifier) każdy obiekt w każdej strukturze usług katalogowych może być jednoznacznie identyfikowany. Definicje przestrzeni nazw *X.500 OID* obejmują katalogi inne niż usługi AD DS, ale AD DS jest usługą katalogową bazującą na standardzie X.500.

Ta przestrzeń nazw może być przedstawiana w notacji kropkowej (numerycznie) lub w notacji ciągu. Na przykład, klasa obiektów organizacji (o nazwie wyświetlania LDAP *organization*) jest identyfikowana przez identyfikator X.500 OID równy 2.5.6.4. Numeryczne przedstawienie tej klasy obiektów identyfikuje jednoznacznie ten obiekt wewnątrz hierarchii X.500.

W celu wyświetlenia identyfikatora X.500 OID można użyć przystawki Active Directory Schema (Schemat usługi Active Directory) lub przystawki ADSI Edit (Edytor ADSI). W celu wyświetlenia identyfikatora X.500 OID dla obiektu *Organization classSchema* należy użyć przystawki ADSI Edit do otwarcia kontenera schematu i przewinąć w dół wyszukując nazwę wyróżniającą *classSchema*: *CN=Organization*.

Jedną z obaw dotyczących modyfikowania schematu jest możliwość tego, że dwie aplikacje wykonają niekompatybilne modyfikacje polegające na próbie dodania obiektów klasy lub atrybutu o tej samej nazwie lub identyfikatorze OID. Celem identyfikatora jest jednoznaczna identyfikacja wszystkich obiektów lub atrybutów w usługach AD DS i zapewnienie, aby żaden inny obiekt schematu nie używał tego samego identyfikatora OID.

W celu zrealizowania takiej identyfikacji organizacje planujące tworzenie nowych identyfikatorów OID powinny rejestrować je w organizacji ISO (International Standards Organization), ANSI (American National Standards Institute) lub firmie Microsoft. Podczas rejestrowania firmy zajmujące się standaryzacją lub firma Microsoft przypisują daną organizację jako część przestrzeni OID, która może być później rozszerzana tak, by spełniała określone potrzeby. Na przykład do danego przedsiębiorstwa może zostać przydzielona liczba w postaci 1.2.840.*xxxx*. Liczba ta jest uporządkowana hierarchicznie i może być podzielona w następujący sposób:

1 – ISO

2 – ANSI

840 – United States

xxxx – Unikalna liczba identyfikująca przedsiębiorstwo

Po przydzieleniu liczby można zarządzać własnym fragmentem hierarchii. Przykładowo, jeśli tworzony jest nowy atrybut nazwany *Employee Start Date*, można przypisać mu liczbę 1.2.840.*xxxx*.12.

Usługi AD DS są dostosowane do standardów OID. Na przykład identyfikator OID dla kontaktów w usługach AD DS to 1.2.840.113556.1.5.15. Pierwsze trzy części liczby zostały odpowiednio przypisane do ISO, ANSI i United States. Organizacja ANSI przypisała następnie numer 113556 do firmy Microsoft, która to z kolei przypisała liczbę 1 do usług Active Directory, 5 do klas usług Active Directory, a 15 do klasy *Contact*.



Ważne Należy zapewnić, aby wszystkie zmiany wprowadzane w schemacie miały unikalny identyfikator OID tak, aby modyfikacje te były zgodne z przyszłymi zmianami. Jednym ze sposobów zapewnienia unikalności jest uzyskanie dla przedsiębiorstwa unikalnego identyfikatora. Innym atrybutem, który musi być unikalny podczas modyfikowania schematu, jest atrybut *LdapDisplayName*. Przed wprowadzeniem zmian w schemacie należy upewnić się, że zrozumiałe są wszystkie reguły związane z wprowadzaniem tych zmian.

Dezaktywowanie obiektów schematu

Pomimo że rozszerzanie schematu jest prostą operacją, zanim zmiany te zostaną wprowadzone, należy uważnie je zaplanować. Po rozszerzeniu schematu lub zmodyfikowaniu istniejących klas bądź atrybutów nie będzie można wycofać się z tych zmian. Obiekty schematu nie mogą być usuwane. Jeśli podczas rozszerzania schematu został popełniony błąd, dany obiekt można wyłączyć (dezaktywować). W systemie Windows Server 2008 dezaktywowane obiekty schematu mogą być w razie potrzeby użyte ponownie, a nowe obiekty schematu mogą być tworzone przy użyciu tej samej nazwy wyświetlania LDAP lub tego samego identyfikatora OID, co dezaktywowany obiekt.

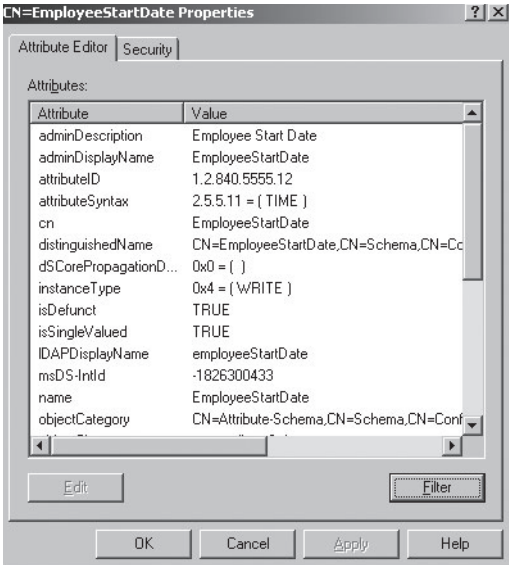
W odniesieniu do dezaktywacji obiektów klas i atrybutów schematu należy pamiętać o kilku kwestiach. Po pierwsze nie można dezaktywować obiektów *Category 1* lub *base schema*. Po drugie nie można dezaktywować atrybutu należącego do klasy, która nie została dezaktywowana. Ograniczenie to zapobiega tworzeniu nowych instancji niedezaktywowanej klasy, jeśli dezaktywowany atrybut jest atrybutem wymaganym.



Uwaga Jeśli las używa poziomu funkcjonalnego systemu Windows Server 2003, można utworzyć nowy obiekt, który używa tych samych wartości identyfikacji atrybutu (to znaczy *attributeID*, *governsID*, *lDAPDisplayName*, *mAPIID* lub *schemaIDGUID*), co „martwy" obiekt schematu, o ile unikalna jest nowa nazwa wyróżniająca obiektu. Dzięki temu można dezaktywować obiekt schematu, a następnie utworzyć całkiem nowy obiekt schematu tak, jakby stary obiekt zastał usunięty.

W celu dezaktywowania klasy lub atrybutu należy dla wartości logicznej atrybutu *isDefunct* obiektu schematu określić wartość *true*. Zadanie to można zrealizować przy użyciu narzędzia, takiego jak ADSI Edit. Na rysunku 2-5 przedstawiono sposób dezaktywowania atrybutu *EmployeeStartDate* utworzonego w poprzednim przykładzie. Atrybut usługi AD DS może być również dezaktywowany poprzez usunięcie zaznaczenia pola wyboru Attribute Is Active (Atrybut jest aktywny) widocznego podczas przeglądania właściwości atrybutu w przystawce Active Directory Schema.

Po dezaktywowaniu obiektu schematu pod każdym względem atrybut jest traktowany tak, jakby nie istniał. Komunikaty o błędach zwracane podczas prób utworzenia nowej instancji dezaktywowanej klasy bądź atrybutu są takie same, jak w przypadku nieistniejącej klasy czy nieistniejącego atrybutu. Jedyną modyfikacją, jaką można wykonać w odniesieniu do dezaktywowanego obiektu schematu jest jego ponowna aktywacja. W tym celu należy po prostu ustawić wartość atrybutu *isDefunct* jako *false* lub zaznaczyć pole wyboru Attribute Is Active (Atrybut jest aktywny). Po ponownej aktywacji obiektu schematu obiekt może być ponownie używany do tworzenia nowych instancji klasy bądź atrybutu. Nie istnieją inne „efekty uboczne" tego procesu aktywacji/dezaktywacji.



Rysunek 2-5 Używanie programu ADSIEdit.msc do dezaktywowania atrybutu schematu.

Struktura logiczna usług AD DS

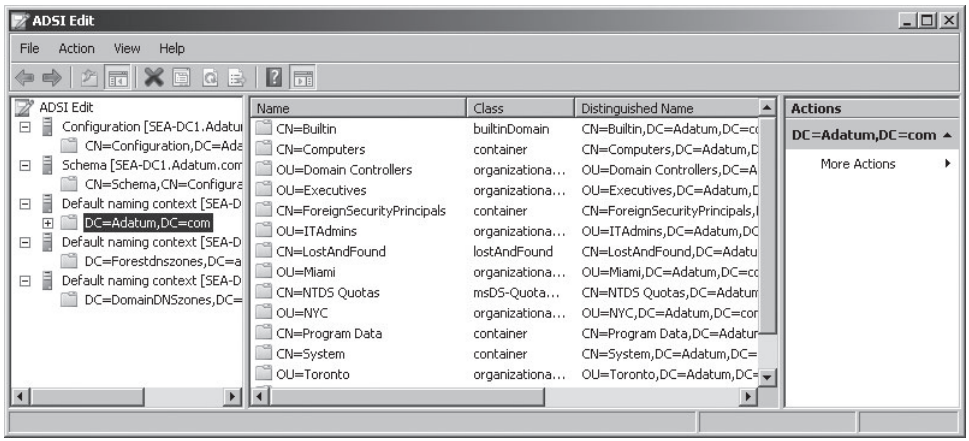
Po zainstalowaniu w środowisku sieci usług AD DS i rozpoczęciu implementowania odpowiedniego projektu tych usług zgodnego z potrzebami biznesu konfigurowana będzie logiczna struktura usług AD DS. Logiczna struktura prezentuje konfiguracje domen, jednostek organizacyjnych i innych obiektów AD DS w sposób, który jest niezależny od składników fizycznych usług AD DS, takich jak kontrolery domen lub magazyn danych usług AD DS znajdujący się na każdym kontrolerze domeny. Struktura logiczna usług AD DS składa się z następujących składników:

- Partycje
- Domeny
- Drzewa domen
- Lasy
- Lokacje
- Jednostki organizacyjne

W niniejszym podrozdziale składniki te zostały opisane w sposób ogólny. W podrozdziale omówiono również pojęcia zaufania, które są używane do umożliwienia dostępu do zasobów dla podmiotów zabezpieczeń przechowywanych w różnych domenach. W rozdziale 5 opisano, w jaki sposób i z jakich przyczyn te składniki strukturalne są używane do zrealizowania specyficznych celów biznesowych (jak na przykład bezpieczny dostęp do zasobów) i do zoptymalizowania wydajności sieci.

Partycje usług AD DS

Zgodnie z poprzednim opisem, baza danych usług AD DS jest przechowywana w jednym pliku bazy danych na dysku twardym każdego kontrolera domeny. Informacje przechowywane w bazie danych katalogu są podzielone na wiele partycji logicznych, a każda partycja przechowuje inne typy informacji. Partycje usług AD DS są również nazywane kontekstami nazw NC (*naming contexts*). Partycje usług AD DS są widoczne za pomocą narzędzi, takich jak Ldp.exe czy ADSI Edit (rysunek 2-6).



Rysunek 2-6 Partycje usług AD DS można przeglądać przy użyciu programu ADSIEdit.msc.

Usługi AD DS i protokół LDAP

Protokół LDPA (Lightweight Directory Access Protocol) jest w usługach AD DS systemu Windows Server 2008 zarówno protokołem dostępu, jak i modelem identyfikacji obiektów. Jako model identyfikacji obiektów protokół LDAP używa hierarchicznego formatu do zidentyfikowania każdego obiektu usługi AD DS. Ten hierarchiczny format rozpoczyna się od poziomu partycji katalogu i obejmuje każdy składnik logiczny hierarchii, aby możliwe było jednoznaczne rozpoznanie każdego obiektu. Mechanizm ten znany jest jako nazwa wyróżniająca. Na przykład konto użytkownika może być identyfikowane przy użyciu następującej nazwy wyróżniającej LDAP:

CN=Yvonne McKay,OU=Marketing,OU=Miami, DC=ADatum,DC=com

Każda część nazwy LDAP jest identyfikowana przez typ obiektu. Te fragmenty znane są jako względne nazwy wyróżniające (RDN), a typ obiektu jest nazywany atrybutem nazwy RDN. Na przykład, *cn* odnosi się do nazwy pospolitej, *ou* do jednostki organizacyjnej, a *dc* do domeny. Stosując tę konwencję nazywania można specyficznie odnosić się do obiektów i uzyskiwać do nich dostęp w usłudze katalogowej zgodnej z LDAP, takiej jak usługi AD DS. Protokół LDAP i model katalogu (ale nie składnia nazewnictwa) zostały zdefiniowane w specyfikacji RFC 2251 „Lightweight Directory Access Protocol (v3)" dostępnej pod adresem *http://www.ietf.org/rfc/rfc2251.txt*.

Ciąg dalszy na stronie następnej

Ciąg dalszy ze strony poprzedniej

Protokół LDAP jest również protokołem dostępu i interfejsem API (Application Programming Interface) do uzyskiwania informacji w usługach AD DS. Jako interfejs API, protokół LDAP został zaimplementowany w usługach AD DS systemu Windows Server 2008 w pliku Wldap32.dll. Wewnątrz aplikacji lub skryptu można uzyskać dostęp do każdego obiektu usługi AD DS przy użyciu ścieżki LDAP. Na przykład, aby odnieść się do określonej jednostki organizacyjnej w skrypcie powłoki Windows PowerShell, należy posłużyć się następującą składnią:

```
$objADSI = [ADSI]"LDAP://OU=Marketing,OU=Miami,DC=ADatum,DC=com"
```

W celu administrowania usługami AD DS przy użyciu protokołu LDAP można posługiwać się narzędziami administracyjnymi zgodnymi z protokołem LDAP, takimi jak program Ldp.exe, który jest zainstalowany w systemie Windows Server 2008. Za pomocą programu Ldp.exe można powiązać lub połączyć się z usługami AD DS poprzez jego numer portu TCP (Transmission Control Protocol) i pokazać nazwę wyświetlania LDAP każdego atrybutu, klasy i obiektu. W celu podłączenia się do usługi AD DS za pomocą narzędzia Ldp.exe i wyświetlenia atrybutów obiektu użytkownika należy podłączyć się do kontrolera domeny usług AD DS przy użyciu portu 389 TCP, rozwinąć kontener lub jednostkę organizacyjną, a następnie dwukrotnie kliknąć nazwę wyróżniającą użytkownika.

Partycja katalogu domeny

Partycja katalogu domeny zawiera wszystkie informacje o domenie, wliczając w to użytkowników, grupy, komputery i kontakty. Zasadniczo wszystko to, co może być przeglądane za pomocą narzędzia administracyjnego Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory), jest przechowywane w partycji katalogu domeny.

Partycja katalogu domeny jest w domenie automatycznie replikowana do wszystkich kontrolerów domeny. Partycja zawiera informacje, które każdy kontroler domeny potrzebuje do uwierzytelnienia użytkowników.

Partycja katalogu konfiguracji

Partycja katalogu konfiguracji zawiera informacje o konfiguracji całego lasu. Na przykład wszystkie informacje o lokacjach, łączach lokacji i połączeniach replikacji są przechowywane w partycji katalogu konfiguracji. Inne aplikacje mogą również przechowywać informacje w partycji konfiguracji. Na przykład program Exchange Server 2007 przechowuje wszystkie swoje informacje o konfiguracji w partycji katalogu konfiguracji usług AD DS, a nie we własnej usłudze katalogowej.

Ponieważ partycja katalogu konfiguracji zawiera informacje o całym lesie, jest replikowana w całym lesie. Każdy kontroler domeny zawiera kopię partycji katalogu konfiguracji z możliwością zapisu, a zmiany tej partycji mogą być wykonywane na dowolnym kontrolerze domeny w organizacji. Oznacza to, że informacje o konfiguracji są następnie replikowane do wszystkich innych kontrolerów domeny. Jeśli replikacja jest w pełni zsynchroni-

zowana, każdy kontroler domeny w lesie będzie dysponował tymi samymi informacjami o konfiguracji.

Partycja katalogu schematu

Partycja katalogu schematu zawiera schemat całego lasu. Zgodnie z wcześniejszym opisem, schemat jest zestawem reguł precyzującym, jakie typy obiektów mogą być tworzone w usługach AD DS, jak również jest zestawem reguł opisujących każdy typ obiektu.

Partycja katalogu schematu jest replikowana do wszystkich kontrolerów domen w całym lesie. Jednak tylko na jednym kontrolerze domeny – będącym wzorcem schematu – przechowywana jest kopia partycji katalogu schematu z możliwością zapisu. Wszystkie zmiany schematu muszą być przeprowadzane na wzorcu schematu; zmiany są następnie replikowane do wszystkich kontrolerów domen.

Partycja wykazu globalnego

Partycja wykazu globalnego nie jest partycją w takim samym znaczeniu, jak pozostałe partycje. Partycja wykazu globalnego jest przechowywana w bazie danych tak, jak inne partycje, ale administratorzy nie mogą bezpośrednio wprowadzać informacji do tej partycji. Wykaz globalny jest partycją przeznaczoną tylko do odczytu na wszystkich serwerach wykazu globalnego i zbudowany jest z zawartości baz danych domen. Każdy atrybut schematu ma wartość logiczną nazwaną *isMemberOfPartialAttributeSet*. Jeśli wartość ta określona jest jako *true*, atrybut jest replikowany do wykazu globalnego.

Partycje katalogu aplikacji

Ostatnim typem partycji w usługach AD DS systemu Windows Server 2008 jest partycja katalogu aplikacji lub kontekst NDNC (Non-Domain Naming Context). Partycje katalogu aplikacji są używane do przechowywania informacji specyficznych dla aplikacji. Zaletą korzystania a partycji katalogu aplikacji, a nie z jednej z pozostałych partycji usług AD DS, jest to, że dla partycji katalogu aplikacji może być kontrolowany zakres replikacji. Jeśli partycja jest używana do przechowywania informacji o katalogu, informacje te mogą być dość dynamiczne. Poprzez definiowanie, które kontrolery domen będą utrzymywać replikę partycji katalogu aplikacji, można ograniczać wielkość ruchu powstającego w sieci i związanego z replikacją. Kontrolery domen, które odbierają replikę partycji katalogu aplikacji, mogą znajdować się w dowolnej domenie lub lokacji lasu.

Partycje katalogu aplikacji mogą przechowywać dowolne typy obiektów usług AD DS, za wyjątkiem podmiotów zabezpieczeń. Ponadto, ponieważ partycje katalogu aplikacji są tworzone po to, by kontrolować, dokąd dane będą replikowane, żaden z obiektów partycji katalogu aplikacji nie może być replikowany do partycji wykazu globalnego.

Domyślnie żadna partycja katalogu aplikacji nie jest tworzona w usługach AD DS. Jeśli jednak podczas instalowania usług AD DS do zainstalowania na pierwszym kontrolerze domeny w lesie wybrany zostanie system DNS (Domain Name System), dla usługi serwera DNS utworzone zostaną dwie partycje katalogu aplikacji nazwane ForestDnsZones i DomainDnsZones. Oprócz partycji katalogu aplikacji tworzonych dla systemu DNS administrator może także tworzyć partycje dla innych aplikacji.



Informacje dodatkowe Informacje dodatkowe na temat tych partycji katalogu aplikacji DNS znaleźć można w rozdziale 3 „Usługi AD DS (Active Directory Domain Services) i system DNS (Domain Name System)".

Schemat nazw dla partycji katalogu aplikacji jest taki sam, jak dla innych partycji katalogu usług AD DS, na przykład nazwa LDAP dla partycji katalogu konfiguracji w lesie ADatum.com to: *CN=Configuration,DC=ADatum,DC=com*. Jeśli utworzona zostanie partycja katalogu aplikacji nazwana AppPartition1 w domenie ADatum.com, to jej nazwa DNS ma postać: *DC=AppPartition1,DC=ADatum,DC=com*. Partycje katalogu aplikacji są dość elastyczne w odniesieniu do miejsca, gdzie można tworzyć partycje lub bardziej dokładne w odniesieniu do tego, jaki będzie kontekst nazw partycji. Na przykład można utworzyć dodatkową partycję katalogu aplikacji poniżej partycji AppPartition1 tworząc partycje nazwane *DC=AppPartition2 DC=AppPartition1,DC=ADatum,dc=com*. Można nawet utworzyć partycję katalogu aplikacji o nazwie DNS, która nie jest zgodna z żadną domeną lasu. Można utworzyć partycję katalogu aplikacji w domenie ADatum.com, której nazwa DNS to *DC=AppPartition*. W rezultacie powstaje nowe drzewo lasu.



Uwaga Wybranie nazwy DNS dla przestrzeni nazw aplikacji w żaden sposób nie wpływa na funkcjonalność partycji katalogu aplikacji. Jedyna różnica dotyczyć będzie konfiguracji klienta LDAP, który uzyskuje dostęp do partycji. Partycje katalogu aplikacji są przeznaczone do uzyskiwania dostępu protokołu LDAP, tak więc klient musi zostać skonfigurowany, by wyszukiwał na serwerze odpowiednią przestrzeń nazw.

Podczas tworzenia partycji katalogu aplikacji jednym z bardziej skomplikowanych czynników jest konserwacja uprawnień do obiektów partycji. Przy użyciu partycji domyślnych usług AD DS uprawnienia są przypisywane automatycznie. Kiedy obiekt jest tworzony w partycji katalogu domeny, do grupy Domain Admins (Administratorzy domeny) automatycznie przypisywane są pełne uprawnienia do obiektu. Jeśli obiekt tworzony jest w partycji katalogu konfiguracji lub schematu, uprawnienia są przypisywane do kont użytkowników i grup domeny głównej lasu. Ponieważ partycja katalogu aplikacji może być replikowana do dowolnych domen w lesie, nie jest stosowany ten domyślny sposób przypisywania uprawnień. Chociaż prostą metodą jest przypisanie pełnej kontroli do obiektów partycji grupie, takiej jak Domain Admins, to w metodzie tej nie jest oczywiste, która domena jest domeną domyślną. Aby rozwiązać tę kwestię, partycje katalogu aplikacji są zawsze tworzone wraz z domeną odniesienia deskryptora zabezpieczeń. Domena ta staje się domeną domyślną używaną do przypisywania uprawnień do obiektów w partycji katalogu aplikacji. Jeśli partycja katalogu aplikacji zostaje utworzona poniżej partycji katalogu domeny, domena nadrzędna jest używana jako domena odniesienia deskryptora zabezpieczeń, co w rezultacie tworzy dziedziczność uprawnień. Jeśli partycja katalogu aplikacji tworzy nowe drzewo lasu, domena główna lasu jest używana jako domena odniesienia.



Uwaga Zazwyczaj partycje katalogu aplikacji będą tworzone poprzez instalację aplikacji, która wymaga korzystania z partycji katalogu aplikacji. Ponadto procedura instalacji aplikacji powinna zezwalać na tworzenie dodatkowych replik na innych kontrolerach. Pomimo że można tworzyć partycje katalogu aplikacji za pomocą narzędzia Ntdsutil, metoda ta nie jest zalecana w środowisku produkcyjnym. Procedury zarządzania partycjami katalogu aplikacji zostały opisane w module Pomoc i obsługa techniczna systemu Windows Server 2008. Informacje dodatkowe na temat partycji katalogu aplikacji, wliczając w to programowe metody dostępu do partycji, znaleźć można w artykule „Application Directory Partitions" dostępnym pod adresem *http://msdn2.microsoft.com/en-us/library/ms675020.aspx*.

Domeny

Domena jest najbardziej podstawowym blokiem konstrukcji modelu usług AD DS. Podczas instalowania usług AD DS na pierwszym komputerze systemu Windows Server 2008 tworzona jest domena. Domena służy jako granica administracyjna i definiuje także granice niektórych zasad zabezpieczeń. Struktura domeny powinna bazować na wymaganiach administracyjnych organizacji, takich jak delegowanie urzędów administracji i wymagania operacyjne, jak na przykład potrzeby związane z kontrolą replikacji. Przykładowo, w domenie wszyscy członkowie grupy Domain Admins (Administratorzy domeny) mają pełny administracyjny dostęp do wszystkich obiektów w tej domenie, ale domyślnie nie mają administracyjnego dostępu do obiektów w innych domenach.

W usługach AD DS domeny definiują następujące granice:

- **Granice replikacji** Granice domeny są granicami replikacji dla partycji katalogu domeny i dla informacji o domenie przechowywanych w folderze Sysvol na wszystkich kontrolerach domeny. Podczas gdy inne partycje katalogu, takie jak partycja katalogu schematu, konfiguracji czy wykaz globalny (GC), są replikowane w całym lesie, to partycja katalogu domeny jest replikowana tylko wewnątrz jednej domeny. W bardzo dużych organizacjach poprzez podział (partycjonowanie) danych na wiele domen tego samego lasu można zarządzać ruchem replikacji pomiędzy kontrolerami domen. Informacje przechowywane w partycji domeny są replikowane do wszystkich innych kontrolerów domen w danej domenie, ale nie są replikowane do kontrolerów domen w innych domenach.
- **Granice zasad zabezpieczeń** Niektóre zasady zabezpieczeń mogą być ustawiane tylko na poziomie domeny. Zasady te, jak na przykład zasady haseł, blokady konta czy biletu Kerberos, stosowane są do wszystkich kont domeny.



Uwaga W systemie Windows Server 2008 można definiować dokładne zasady hasła, które zastępują domyślne zasady konta domeny dla określonych użytkowników. Dokładne zasady haseł nie mogą być jednak stosowane do obiektu kontenera tylko do poszczególnych kont użytkowników lub grup zabezpieczeń.

- **Granice dostępu do zasobów** Granice domeny są również granicami dla usług uwierzytelnienia i autoryzacji. Domena udostępnia usługi uwierzytelniania dla wszystkich swoich kont w celu ułatwienia procesu logowania i kontroli rejestracji jednokrotnej dla dostępu do udostępnianych zasobów wewnątrz granic domeny. Domyślnie użytkownicy

w jednej domenie nie mogą uzyskać dostępu do zasobów w innej domenie, chyba że wprost przypisane im zostały odpowiednie uprawnienia.

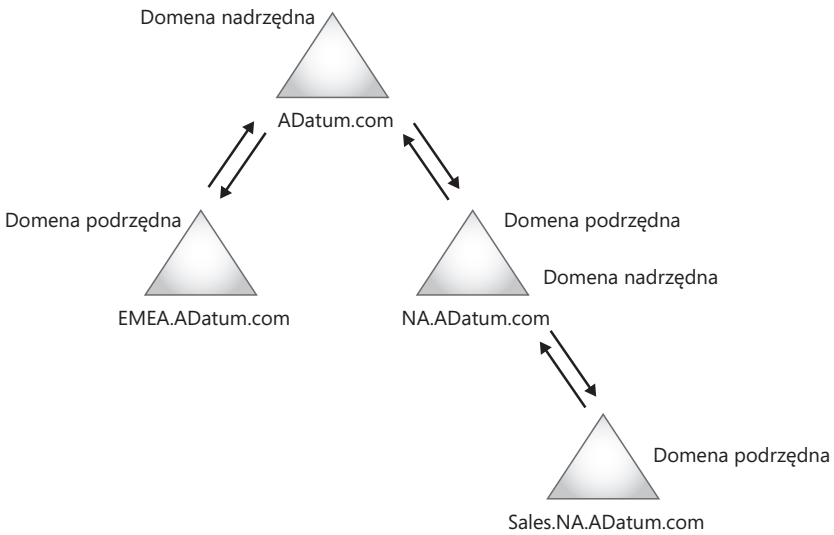
- **Granice zaufania** Domena jest najmniejszym kontenerem wewnątrz usług AD DS, który może być używany w relacjach zaufania. Zaufania są używane do zrealizowania usług uwierzytelnienia i autoryzacji tak, aby użytkownicy jednej domeny mogli uzyskać dostęp do zasobów innej domeny. Wewnątrz lasu relacje zaufania są automatycznie tworzone z jednej strony pomiędzy główną domeną lasu a wszystkimi domenami głównymi drzewa i z drugiej strony pomiędzy wszystkimi domenami podrzędnymi, które są podrzędne dla głównej domeny lasu.



Alert zabezpieczeń Granice domeny nie są granicami zabezpieczeń – operacje wykonywane przez administratora w jednej domenie mogą wpływać na wszystkie pozostałe domeny w lesie. W celu utworzenia granicy bezpieczeństwa trzeba tworzyć oddzielne lasy. Więcej informacji na ten temat znaleźć można w rozdziale 5.

Domeny usługi AD DS wewnątrz lasu są uporządkowane hierarchicznie. Pierwsza domena w przedsiębiorstwie nazywana jest główną domeną lasu (*forest root domain)* i jest punktem początkowym przestrzeni nazw usług AD DS. Na przykład pierwszą domeną w organizacji A. Datum jest domena ADatum.com. Ta pierwsza domena może być dedykowaną lub niededykowaną domeną główną. Dedykowany katalog główny (*dedicated root* lub *empty* root) jest pustym miejscem początkowym usług AD DS. Jedynie konta, które znajdują się w dedykowanej domenie głównej są domyślnymi kontami użytkowników i grup domeny, takimi jak konto Administrator czy globalna grupa Domain Admins (Administratorzy domeny). Niededykowana domena główna jest jedną z domen, w której rzeczywiście tworzone są konta użytkowników i grup. Kwestie związane z wyborem dedykowanego lub niededykowanego katalogu głównego lasu omówione zostały w rozdziale 5.

Wszystkie pozostałe domeny lasu istnieją jako partnerzy (*peers)* domeny głównej lub jako domeny podrzędne. Domeny podrzędne *współużytkują* tę samą przestrzeń nazw usług AD DS, co domena nadrzędna (domena główna). Przykładowo, jeśli pierwsza domena w organizacji A. Datum nazwana została ADatum.com, domena podrzędna w tej strukturze może zostać nazwana NA.ADatum.com. Domena NA.ADatum.com mogła być utworzona do zarządzania wszystkimi podmiotami zabezpieczeń dla lokacji w Ameryce Północnej organizacji A. Datum. Jeśli organizacja jest odpowiednio duża lub złożona, mogą być wymagane dodatkowe domeny podrzędne, takie jak Sales.NA.ADatum.com. Na rysunku 2-7 przedstawiona została hierarchia domeny dla organizacji ADatum.

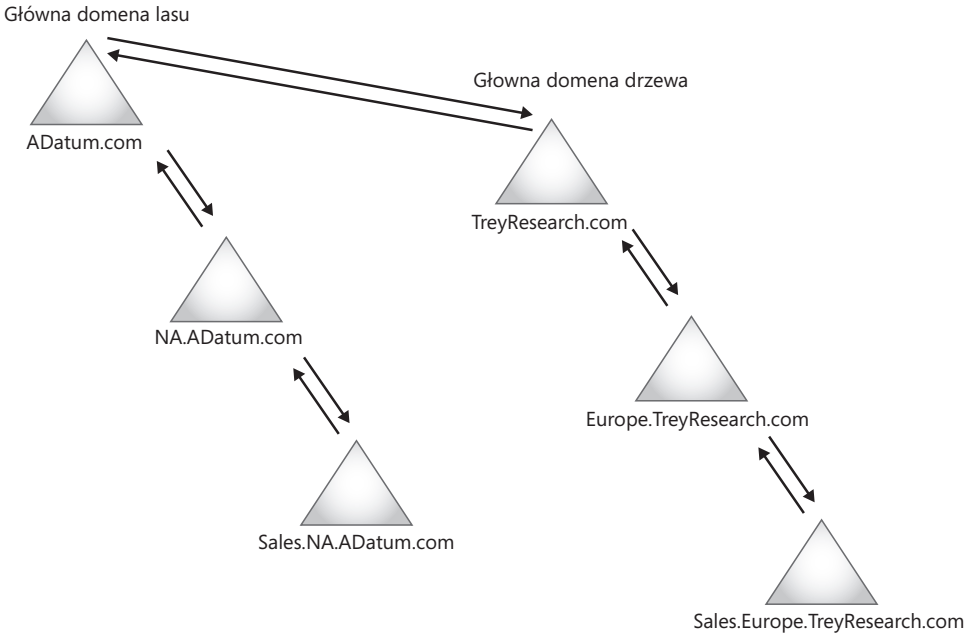


Rysunek 2-7 Model domeny (podrzędna-nadrzędna) dla organizacji A. Datum Corporation.

Jeśli domeny instalowane są w konfiguracji typu nadrzędna-podrzędna, otrzymany model nazywany jest drzewem domen. Drzewo domen to jedna lub więcej domen, które współużytkują ciągłą przestrzeń nazw. W lesie ADatum.com, domena NA.Adatum.com współużytkuje przestrzeń nazw Adatum.com z domeną główną lasu.

W tym samym lesie można implementować dodatkowe drzewa domen. Podczas tworzenia nowego drzewa domen dodawane są domeny do lasu, który nie współużytkuje tej samej ciągłej przestrzeni nazw. Na przykład organizacja A. Datum może mieć filię nazwaną Trey Research, dla której potrzebna jest oddzielna domena. Domenę TreyResearch.com można dodać do lasu ADatum.com i utworzyć nowe drzewo domen. W tym scenariuszu domena TreyResearch.com jest domeną główną drzewa domen.

Jeśli do spełnienia wymagań filii Trey Research potrzebne są dodatkowe domeny, mogą być utworzone jako domeny podrzędne w drzewie domen TreyResearch. Na rysunku 2-8 przedstawiono organizację ADatum w wieloma drzewami domen.



Rysunek 2-8 Korporacja A. Datum z wieloma drzewami domen.

Niezależnie od tego, czy używana jest pojedyncza przestrzeń nazw (jedno drzewo domen), czy jest używanych wiele przestrzeni nazw (wiele drzew domen), dodatkowe domeny w tym samym lesie funkcjonują dokładnie w ten sam sposób. Wszystkie domeny nadal są częścią tego samego lasu i wszystkie domeny współużytkują przechodnie relacje zaufania z wszystkimi innymi domenami w lesie. Utworzenie dodatkowych drzew domen jest decyzją czysto organizacyjną i związaną z nazewnictwem, nie wpływającą na funkcjonalność. Używanie wielu drzew, a nie domen podrzędnych, nie wpływa na konfigurację systemu DNS (co omówione zostało w rozdziale 3).

Lokalizacja obiektów w innych domenach

Ponieważ informacje każdej partycji domeny są replikowane do innych kontrolerów domen w tej samej domenie, to kontrolery domen muszą mieć pewien mechanizm umożliwiający lokalizację obiektów w innych domenach. Na przykład, jeśli użytkownik w jednej domenie próbuje uzyskać dostęp do udostępnionego folderu w innej domenie w lesie, kontroler domeny w domenie użytkownika musi mieć możliwość określenia, czy inna domena istnieje i musi być w stanie zlokalizować kontrolery domen w tej domenie. Usługi AD DS stosują odwołania wzajemne (cross-references), dzięki którym każdy kontroler domeny ma nie tylko informacje dotyczące swojej domeny, ale także ma informacje o wszystkich innych domenach i partycjach katalogów danego lasu.

Odwołania wzajemne są przechowywane jako obiekty katalogu klasy *crossRef*, które identyfikują istnienie i lokalizację wszystkich partycji katalogu. Ponadto obiekty te zawierają informacje używane przez usługi AD DS do konstruowania hierarchii drzewa katalogu. Klasa *crossRef* obejmuje następujące atrybuty:

- ***nCName*** Nazwa wyróżniająca partycji katalogu, do którego odnosi się obiekt *crossRef* (prefiks *nC* oznacza kontekst nazwy, który jest synonimem partycji katalogu). Kombinacja wszystkich właściwości atrybutu *nCName* w lesie definiuje całe drzewo katalogu, wliczając w to podrzędne i nadrzędne relacje pomiędzy partycjami.
- ***dNSRoot*** Nazwa DNS domeny, gdzie można znaleźć serwery przechowujące daną partycję katalogu.

Dla każdej partycji katalogu w lesie istnieje wewnętrzny obiekt odwołania wzajemnego przechowywany w kontenerze Partitions (Partycje) (*CN=Partitions,CN=Configuration,DC=ForestRootDomain*). Ponieważ obiekty odwołań wzajemnych znajdują się w kontenerze Configuration (Konfiguracja), to są replikowane do każdego kontrolera domeny w lesie i z tego względu każdy kontroler domeny ma informacje o nazwie każdej partycji w lesie. Dzięki korzystaniu z obiektów odwołań wzajemnych każdy kontroler domeny może generować odniesienia do dowolnej innej domeny lasu.

Lasy

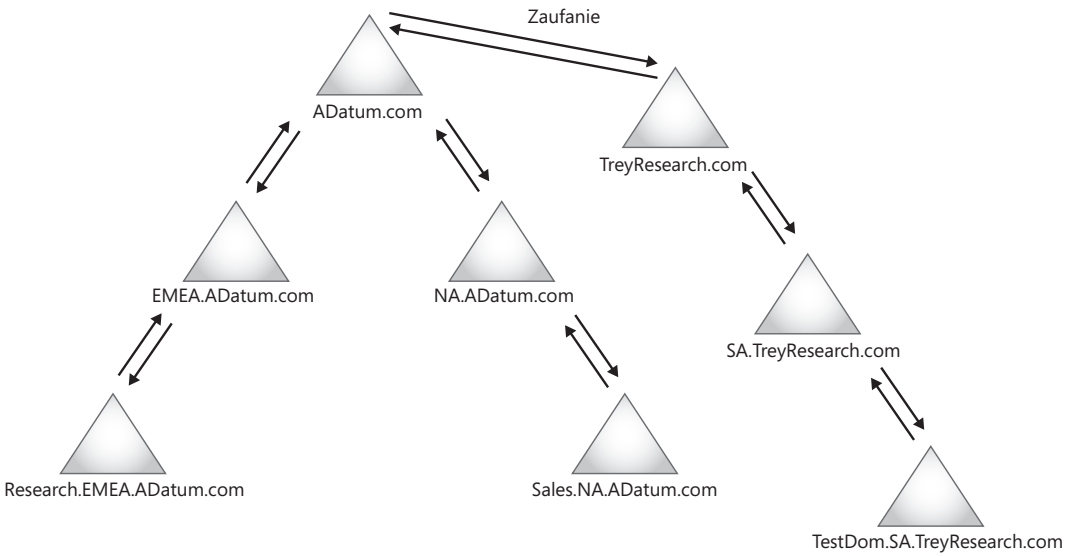
Las jest najwyższym poziomem hierarchii struktury logicznej usług AD DS. Las usług AD DS przedstawia pojedynczy samodzielny katalog. Las stanowi granice replikacji i zabezpieczeń przedsiębiorstwa. Wszystkie domeny i drzewa domen istnieją w lesie usług AD DS.

Las usług AD DS może być definiowany poprzez elementy współużytkowane przez wszystkie kontrolery domen lasu. Poniżej wymienione zostały te współużytkowane składniki:

- **Wspólny schemat** Wszystkie kontrolery domeny w lesie będą miały ten sam schemat. W usługach AD DS schemat jest przechowywany w partycji katalogu schematu i jest replikowany w lesie do wszystkich kontrolerów domen. Jedynym sposobem zainstalowania w organizacji dwóch różnych schematów jest zainstalowanie dwóch oddzielnych lasów.

- **Wspólna partycja katalogu konfiguracji** Wszystkie kontrolery domen w lesie mają ten sam kontener konfiguracji. Partycja konfiguracji zawiera informacje o topologii lasu i innych ustawieniach lasu, domen i kontrolerów domen. Te dane o konfiguracji obejmują listę wszystkich domen, drzew i lasów oraz informacje o lokalizacji kontrolerów domen i wykazów globalnych. Partycja katalogu konfiguracji jest również intensywnie używana przez aplikacje korzystające z usług Active Directory, takie jak program Exchange Server.
- **Wspólny wykaz globalny** Wykaz globalny zawiera informacje o wszystkich obiektach całego lasu. Dzięki temu efektywniejsze jest wyszukiwanie obiektów lasu i możliwe jest logowanie się użytkowników w dowolnej domenie przy użyciu nazwy UPN.
- **Wspólny w całym lesie zestaw wzorców operacji i administratorów** Wzorce nazw domen i schematu są konfigurowane na poziomie lasu. Każdy las ma tylko jeden wzorzec schematu i tylko jeden wzorzec nazw domen. Ponadto w domenie głównej lasu tworzone są dwie grupy zabezpieczeń o unikalnych uprawnieniach. Grupa Schema Admins (Administratorzy schematu) jest jedyną grupą, która ma uprawnienia do modyfikowania schematu, a grupa Enterprise Admins (Administratorzy przedsiębiorstwa) jest jedyną grupą, która ma prawa do wykonywania operacji na poziomie lasu, takich jak dodawanie lub usuwanie domen lasu. Grupa Enterprise Admins jest także automatycznie dodawana do każdej lokalnej grupy Administrators na kontrolerach domen w każdej domenie lasu.
- **Współużytkowana konfiguracja konfiguracji relacji zaufania** Wszystkie domeny lasu zostają automatycznie skonfigurowane, by ufać wszystkim innym domenom lasu.

Na rysunku 2-9 przedstawiono las organizacji A. Datum.



Rysunek 2-9 Las może zawierać wiele domen i drzew.



Na dysku CD W celu wyświetlenia informacji o lesie usługi AD DS i domenach wewnątrz tego lasu należy uruchomić skrypt ListADDSDomains.ps1 powłoki Windows PowerShell znajdujący się na dołączonym dysku.

Relacje zaufania

Jeśli nie zostały skonfigurowane żadne relacje zaufania, w organizacji granicą dostępu do zasobów jest domena. Za pomocą odpowiednich uprawnień dowolnego podmiotu zabezpieczeń (na przykład konta użytkowników czy grup) mogą uzyskać dostęp do zasobów udostępnianych w tej samej domenie. Aby możliwe było uzyskanie dostępu do zasobów udostępnianych poza domeną własną podmiotu zabezpieczeń, wykorzystywane są relacje zaufania usług AD DS. Zaufanie jest połączeniem uwierzytelnienia pomiędzy dwiema domenami, poprzez które podmioty zabezpieczeń mogą autoryzować dostęp do zasobów w innej domenie.

Jeśli pomiędzy dwiema domenami skonfigurowana jest relacja zaufania, mechanizm uwierzytelniania każdej domeny ufa mechanizmowi uwierzytelniania wszystkich innych zaufanych domen. Jeśli użytkownik lub aplikacja zostaje uwierzytelniona przez jedną domenę, uwierzytelnienie to jest akceptowane przez wszystkie inne domeny, które ufają domenie przeprowadzającej uwierzytelnienie. Użytkownicy w zaufanej domenie mają dostęp do zasobów w domenie ufającej, podlegają kontroli dostępu, która jest stosowana w domenie ufającej.



Uwaga Relacje zaufania są automatycznie konfigurowane pomiędzy wszystkimi domenami w lesie i nie mogą być usuwane.

Poniżej wymienionych zostało kilka typów relacji zaufania:

- Przechodnie dwukierunkowe relacje zaufania
- Relacje zaufania skrótu
- Relacje zaufania lasów
- Zewnętrzne relacje zaufania
- Relacje zaufania obszaru

Przechodnie dwukierunkowe relacje zaufania

Wszystkie domeny lasu utrzymują przechodnie, dwukierunkowe relacje zaufania z każdą inną domeną tego lasu. W przykładzie przedstawionym poprzednio, kiedy domena NA-.ADatum.com utworzona została jako domena podrzędna głównej domeny ADatum.com, to automatycznie pomiędzy domenami NA.ADatum.com i ADatum.com utworzona została dwukierunkowa relacja zaufania. Dzięki temu zaufaniu każdy użytkownik w domenie NA-.ADatum.com może uzyskać dostęp do każdego zasobu w domenie ADatum.com (jeśli ma przydzielone odpowiednie uprawnienia). Podobnie każdy podmiot zabezpieczeń istniejący w domenie ADatum.com uzyska dostęp do zasobów w domenie NA.ADatum.com.

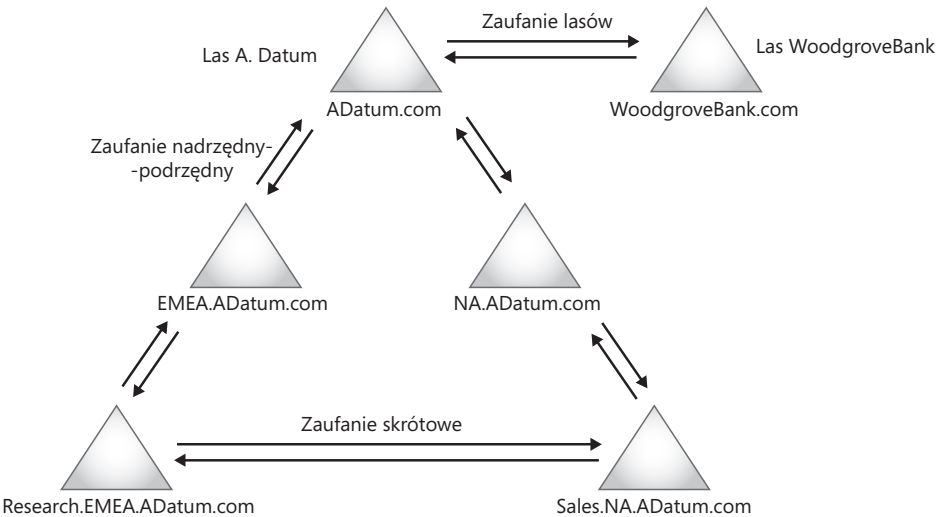
Wewnątrz lasu relacje zaufania są ustawiane jako zaufania typu nadrzędny-podrzędny lub jako główne zaufania drzewa. Przykładem zaufania typu nadrzędny-podrzędny jest relacja zaufania pomiędzy domeną NA.ADatum.com a domeną ADatum.com. Główne

zaufania drzewa to relacja zaufania pomiędzy dwoma drzewami lasu, na przykład pomiędzy ADatum.com a TreyResearch.com.

Wszystkie relacje zaufania pomiędzy domenami w lesie są także przechodnie. Przechodniość zaufania oznacza, że wszystkie domeny w lesie ufają sobie wzajemnie. Jeśli domena ADatum.com ufa domenie NA.ADatum., a domena EMEA.ADatum.com ufa domenie ADatum.com, to dzięki przechodniości domena EMEA.ADatum.com również ufa domenie NA.ADatum.com. Z tego względu użytkownicy w domenie NA.ADatum.com mogą uzyskać dostęp do zasobów w domenie EMEA.ADatum.com i odwrotnie. Przechodnie relacje zaufania są również stosowane do głównych zaufań drzewa. Domena NA.ADatum.com ufa domenie ADatum.com, a domena ADatum.com ufa domenie TreyResearch.com. Z tego względu domeny NA.ADatum.com i TreyResearch.com również współdzielą przechodnie relacje zaufania.

Relacje zaufania skrótu

Oprócz automatycznie utworzonych dwukierunkowych, przechodnich relacji zaufania, powstających podczas dodawania nowej domeny podrzędnej, pomiędzy domenami w lesie można tworzyć relacje zaufania skrótu. Zaufania skrótu są używane do zoptymalizowania wydajności podczas uzyskiwania dostępu do zasobów pomiędzy domenami, które są połączone poprzez przechodnie relacje zaufania. Zaufanie skrótu jest przydatne, jeśli często uzyskiwany jest dostęp do zasobów pomiędzy domenami, które są zdalnie podłączone poprzez drzewo domeny lub las. Na przykład relacje zaufania w organizacji A. Datum mogłyby być skonfigurowane tak, jak przedstawiono to na rysunku 2-10.



Rysunek 2-10 Relacje zaufania w lesie ADatum.

Jeśli grupa zabezpieczeń w domenie Research.EMEA.ADatum.com często uzyskuje dostęp do udostępnianych zasobów w domenie Sales.NA.ADatum.com, to przy korzystaniu jedynie z przechodnich relacji zaufania pomiędzy domenami użytkownicy domeny Research.EMEA.ADatum.com muszą odnosić się do każdego kontrolera domeny w każdej domenie drzewa, które znajdują się pomiędzy nimi a domeną zawierającą zasoby. Metoda ta nie

jest efektywna, jeśli dostęp jest często potrzebny. Relacja zaufania skrótu jest relacją bezpośredniego zaufania, dzięki której użytkownicy domeny Sales.EMEA.ADatum.com mogą efektywnie odwoływać się do kontrolera domeny w domenie Research.NA.ADatum.com – bez przechodzenia przez całe drzewo katalogu. Na rysunku 2-10 przedstawiono tę relację zaufania skrótu. Relacje zaufania skrótu mogą być konfigurowane jako zaufania jedno lub dwukierunkowe i nie są przechodnie.

Relacje zaufania lasów

Relacja zaufania lasów jest przechodnią, dwukierunkową relacją zaufania pomiędzy dwoma oddzielnymi lasami. Korzystając z tej relacji zaufania podmioty zabezpieczeń w jednym lesie mogą uzyskiwać dostęp do zasobów w domenie innego lasu. Ponadto użytkownicy mogą logować się w każdej domenie obu lasów przy użyciu tej samej nazwy UPN. Na rysunku 2-10 przedstawiono relację zaufania lasów pomiędzy lasem ADatum.com a lasem WoodgroveBank.com.



Uwaga W celu skonfigurowania relacji zaufania lasów oba lasy muszą korzystać z poziomu funkcjonalnego systemu Windows Server 2003 lub z wyższego poziomu.

Relacje zaufania lasów mogą być bardzo przydatne w środowisku systemu Windows Server 2008. Jeśli z przyczyn politycznych lub technicznych organizacja wymaga kilku lasów, korzystanie z relacji zaufania lasów oznacza prostą metodę przypisywania dostępu do zasobów we wszystkich domenach, niezależnie od tego, w jakim lesie znajduje się użytkownik czy zasób. W dwóch przedsiębiorstwach, mających zainstalowane lasy systemu Windows Server 2008, można lasy te logicznie połączyć przy użyciu relacji zaufania.

Chociaż relacje zaufania lasów są doskonałym rozwiązaniem, mają również kilka ograniczeń:

- Relacje zaufania lasów nie są przechodnie. Przykładowo, jeśli dla lasu ADatum.com określona została relacja zaufania z lasem WoodgroveBank.com, a las WoodgroveBank.com ma relacje zaufania z lasem Fabrikam.com, to automatycznie las ADatum.com nie ma relacji zaufania z lasem Fabrikam.com.
- Relacje zaufania lasów pomiędzy lasami umożliwiają jedynie uwierzytelnienie; nie udostępniają żadnej innej funkcjonalności. Na przykład każdy las będzie nadal miał unikalny wykaz globalny, schemat i partycję katalogu konfiguracji. Pomiędzy dwoma lasami nie są replikowane żadne informacje – relacje zaufania lasów umożliwiają tylko przypisywanie dostępu do zasobów.
- W niektórych przypadkach może zachodzić potrzeba, aby nie wszystkie domeny jednego lasu miały relacje zaufania z wszystkimi domenami innego lasu. W takiej sytuacji w dwóch oddzielnych lasach należy konfigurować jednokierunkowe, nieprzechodnie zewnętrzne relacje zaufania pomiędzy poszczególnymi domenami. Jako rozwiązanie alternatywne można również skonfigurować selektywne uwierzytelnienie dla relacji zaufania lasów, co oznacza, że dla użytkowników zaufanej domeny trzeba wprost włączać dostęp do zasobów na serwerze w domenie ufającej.



Informacje dodatkowe Informacje dodatkowe na temat planowania relacji zaufania lasów znaleźć można w rozdziale 5.

Zewnętrzne relacje zaufania

Zewnętrzna relacja zaufania jest relacją, która może być utworzona pomiędzy domenami usług AD DS znajdującymi się w różnych lasach lub pomiędzy domeną usługi AD DS a domeną systemu Windows NT 4.0 lub wcześniejszego systemu. Zewnętrzne relacje zaufania mogą być używane do umożliwienia dostępu do zasobów w domenie na zewnątrz lasu, który nie jest jeszcze połączony poprzez relacje zaufania lasów lub do utworzenia bezpośrednich relacji zaufania pomiędzy dwiema domenami, które są połączone relacjami zaufania lasów. Zewnętrzna relacja zaufania różni się od relacji zaufania lasów tym, że skonfigurowana jest pomiędzy dowolnymi dwiema domenami obu lasów, a nie tylko pomiędzy głównymi domenami lasów. Poniżej wymienione zostały dodatkowe cechy charakterystyczne zewnętrznych relacji zaufania:

- Zewnętrzne relacje zaufania nie są przechodnie. Tylko dwie domeny uczestniczą w relacji zaufania.
- Konfigurować należy obie strony relacji zaufania. Jeśli zachodzi potrzeba skonfigurowania dwukierunkowej relacji zaufania, relację należy skonfigurować dla każdego kierunku.
- Domyślnie w systemie Windows Server 2008 zewnętrzne relacje zaufania wymuszają filtrowanie identyfikatora SID. Filtrowanie identyfikatora SID jest używane do sprawdzenia, czy przychodzące żądania uwierzytelnienia, wygenerowane przez podmioty zabezpieczeń w zaufanej domenie, zawierają tylko identyfikatory SID podmiotów zabezpieczeń w zaufanej domenie. Filtrowanie SID zapewnia, że administratorzy w zaufanej domenie nie mogą użyć atrybutu *SIDHistory* do uzyskania dostępu do zasobów w domenie ufającej.

Relacje zaufania obszaru

Ostatni typ relacji zaufania to relacje zaufania obszaru. Relacje te konfigurowane są pomiędzy domeną lub lasem systemu Windows Server 2008 a implementacją obszaru protokołu Kerberos v5 inną niż w systemie Windows. Zabezpieczenia protokołu Kerberos bazują na otwartym standardzie i z tego względu istnieje kilka innych implementacji systemów zabezpieczeń opartych na protokole Kerberos. Relacje zaufania obszaru mogą być tworzone pomiędzy dowolnymi obszarami Kerberos, które obsługują standard Kerberos v5. Relacje te mogą być jedno lub dwukierunkowe, a także można je skonfigurować tak, by były przechodnie lub nieprzechodnie.

Lokacje

Wszystkie omawiane właśnie składniki logiczne usług AD DS są prawie całkowicie niezależne od fizycznej infrastruktury sieci. Na przykład podczas projektowania struktury domeny korporacji, gdzie lokalizacja użytkowników nie jest najważniejszą kwestią projektu, wszyscy użytkownicy domeny mogą być zlokalizowani w pojedynczym biurowcu lub mogą znajdować się biurach na całym świecie. Ta niezależność składników logicznych od infrastruktury sieci powstaje przede wszystkim jako wynik stosowania lokacji w usługach AD DS.

Lokacje udostępniają połączenie pomiędzy logicznymi składnikami usług AD DS a fizyczną infrastrukturą sieci. Lokacja jest zdefiniowana jako obszar sieci, gdzie wszystkie kontrolery domen są połączone poprzez szybkie i niezawodne łącze sieci. W większości przypadków lokacja zawiera jedną lub kilka podsieci protokołu IP (Internet Protocol) w sieci lokalnej (LAN) lub w bardzo szybkiej sieci rozległej (WAN) i połączona jest z resztą sieci poprzez wolne łącza WAN.



Na dysku CD W celu wyświetlenia informacji o lokacjach lasu usług AD DS należy uruchomić skrypt ListADDSSites.ps1 Windows PowerShell, znajdujący się na dołączonym dysku CD.

Głównym powodem tworzenia lokacji jest możliwość zarządzania dowolnym ruchem sieci, który musi korzystać z wolnych połączeń. Lokacje są używane do kontrolowania ruchu sieci wewnątrz sieci systemu Windows Server 2008 za pomocą trzech metod:

- **Replikacja** Jedną z najważniejszych metod optymalizacji ruchu sieci za pomocą lokacji jest zarządzanie ruchem replikacji pomiędzy kontrolerami domen. Na przykład, wewnątrz lokacji modyfikacje katalogu będą replikowane w ciągu kilku minut. Harmonogram replikacji pomiędzy lokacjami może być zarządzany tak, aby ruch replikacji nie występował często lub pojawiał się poza godzinami pracy. Domyślnie ruch replikacji pomiędzy lokacjami jest kompresowany, co zmniejsza zapotrzebowanie na pasmo sieci, natomiast wewnątrz lokacji ruch replikacji nie jest kompresowany. W rozdziale 4 zamieszczono bardziej szczegółowy opis różnic pomiędzy replikacją wewnątrz i na zewnątrz lokacji.
- **Uwierzytelnienie** Podczas logowania się użytkownika w domenie Windows Server 2008 z systemu klienckiego Windows 2000, Windows XP Professional lub Windows Vista, komputer kliencki zawsze próbuje połączyć się do kontrolera domeny w tej samej lokacji, w której się znajduje. Zgodnie z opisem zamieszczonym w rozdziale 3, każdy kontroler domeny rejestruje rekordy lokalizacji usługi (SRV) specyficzne dla lokacji – kiedy komputer kliencki próbuje zlokalizować kontroler domeny, zawsze będzie pytał serwery DNS o te rekordy lokacji. Oznacza to, że ruch związany z logowaniem klienta będzie pozostawał wewnątrz lokacji.
- **Usługi sieci rozpoznające lokacje** Trzecia metoda oszczędzania pasma sieci polega na oszczędzaniu pasma sieci poprzez ograniczanie połączeń systemów klienckich do aplikacji i usług obsługujących lokacje. Na przykład przy wykorzystywaniu systemu DFS (Distributed File System) można tworzyć wiele replik folderu w różnych lokacjach sieci. Ponieważ system DFS został tak zaprojektowany, by obsługiwać konfiguracje lokacji, komputery klienckie zawsze próbują uzyskać dostęp do repliki DFS w swojej własnej lokacji, zanim przeprowadzą próbę uzyskania potrzebnych informacji poprzez łącze WAN w innej lokacji. Podobnie program Exchange Server 2007 rozpoznaje konfigurację lokacji usług AD DS w celu zdefiniowania topologii routingu wiadomości wewnątrz organizacji. Wiadomości wysłane pomiędzy serwerami Exchange w tej samej lokacji zawsze będą przesyłane bezpośrednio ze źródłowego serwera do docelowego serwera, nawet jeśli wiadomość ma być przesłana do kilku serwerów w tej samej lokacji. W różnych lokacjach pomiędzy serwerami Exchange przesyłane są tylko pojedyncze kopie wiadomości, nawet jeśli wiadomość przeznaczona jest dla użytkowników kilku różnych serwerów Exchange w lokacji docelowej.

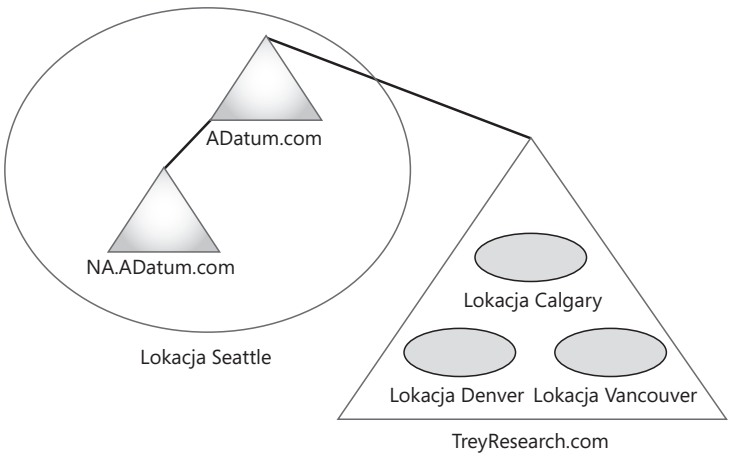
Każdy komputer w sieci systemu Windows Server 2008 przypisany zostaje do lokacji. Podczas instalowania usług AD DS w środowisku systemu Windows Server 2008 tworzona jest lokacja domyślna nazwana Default-First-Site-Name, a wszystkie komputery lasu będą przypisywane do tej lokacji, chyba że utworzone zostaną dodatkowe lokacje. Podczas tworzenia dodatkowych lokacji lokacje są łączone z podsieciami IP. Jeśli rola serwera systemu Windows Server 2008 zostaje podniesiona do roli kontrolera domeny, kontroler domeny automatycznie zostaje przypisany do lokacji, która odpowiada adresowi IP komputera. W razie potrzeby kontrolery domen mogą także być przenoszone pomiędzy lokacjami przy użyciu narzędzia administracji Active Directory Sites and Services (Lokacje i usługi Active Directory).

Komputery klienckie określają swoje lokacje podczas pierwszego uruchomienia i zalogowania się w domenie. Ponieważ komputer kliencki nie wie, do której należy domeny, będzie łączył się do dowolnego kontrolera domeny w danej domenie. Jako część początkowego procesu logowania, kontroler domeny będzie informował klienta, do której należy lokacji, a klient będzie buforował te informacje i używał je przy następnym logowaniu.



Uwaga Jeśli kontroler domeny lub komputer kliencki ma adres IP, który nie jest powiązany z określoną lokacją, komputer ten będzie umieszczany w lokacji Default-First-Site-Name. Każdy komputer, który jest częścią domeny systemu Windows Server 2008, musi należeć do lokacji.

Jak nadmieniono poprzednio w tym rozdziale, nie istnieją bezpośrednie połączenia pomiędzy lokacjami i innymi logicznymi składnikami usługi AD DS. Jedna lokacja może zawierać wiele domen, a jedna domena może rozciągać się w wielu lokacjach. Na przykład (rysunek 2-11), lokacja Seattle zawiera domenę ADatum.com i NA.ADatum.com. Domena TreyResearch.com rozciąga się w wielu lokacjach.



Rysunek 2-11 Lokacje i domeny wewnątrz lasu AD DS.

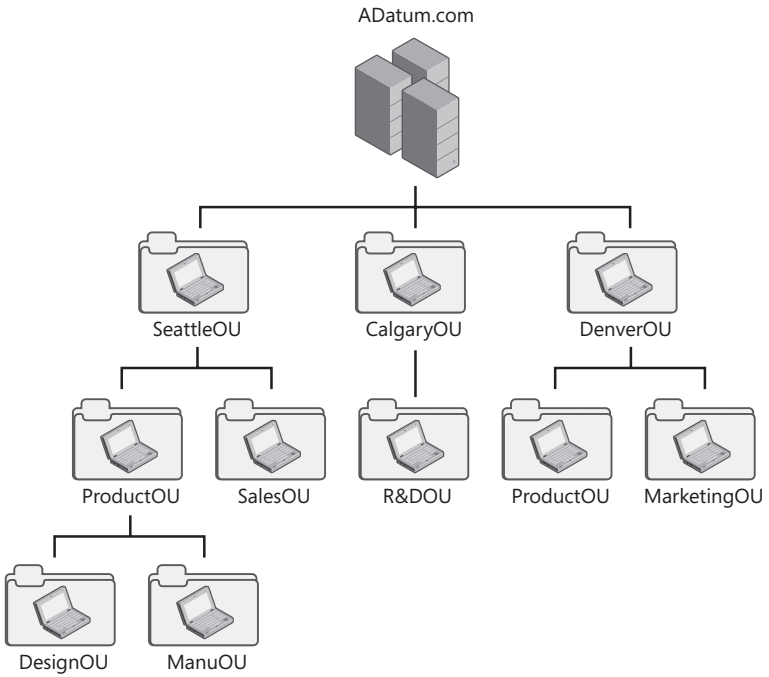


Uwaga Lokacje omawiane są bardziej szczegółowo w kilku innych rozdziałach tej książki. W rozdziale 3 szczegółowo omawiana jest rola DNS i lokacji dla procesu logowania klienta. W rozdziale 4 opisano rolę lokacji w procesie replikacji oraz metody tworzenia i konfigurowania lokacji. Z kolei w rozdziale 5 przedstawiono szczegółowe informacje na temat projektowania optymalnej konfiguracji lokacji lasu usług AD DS.

Jednostki organizacyjne

Poprzez zaimplementowanie wielu domen w lesie, w postaci pojedynczego drzewa lub wielu drzew, usługi AD DS systemu Windows Server 2008 mogą udostępniać usługi katalogowe praktycznie dla sieci o dowolnej wielkości. Wiele składników usług AD DS, takich jak wykaz globalny czy automatyczne przechodnie relacje zaufania, zostały zaprojektowane tak, aby używanie i zarządzanie katalogiem przedsiębiorstwa było efektywne, niezależnie od wielkości katalogu.

Jednostki organizacyjne OU (Organizational Uunit) zostały zaprojektowane, by ułatwić administrowanie usług AD DS w mniejszej skali. Jednostki organizacyjne umożliwiają bardziej efektywne zarządzanie pojedynczymi domenami. Domena może zawierać dziesiątki tysięcy obiektów (lub nawet miliony). Zarządzanie tak wieloma obiektami jest bardzo trudne bez metody ich uporządkowania poprzez logiczne grupowanie. Jednostki organizacyjne są używane do utworzenia struktury hierarchicznej wewnątrz domeny. Na rysunku 2-12 zaprezentowano, jak może wyglądać przykładowa struktura jednostek organizacyjnych organizacji A. Datum.



Rysunek 2-12 Struktura jednostek organizacyjnych może być wielowarstwowa.

Jednostki organizacyjne są obiektami kontenerów, zawierających kilka typów obiektów usług katalogowych:

- Komputery
- Kontakty
- Grupy
- Konta inetOrgPerson
- Drukarki
- Użytkownicy
- Foldery udostępnione
- Jednostki organizacyjne

Jednostki organizacyjne są używane do grupowania obiektów dla celów administracyjnych z dwóch powodów: w celu delegowania praw administracyjnych i w celu zarządzania grupą obiektów w postaci pojedynczej jednostki.

Używanie jednostek organizacyjnych do delegowania praw administracyjnych

Jednostki organizacyjne mogą być używane do delegowania praw administracyjnych. Na przykład, użytkownikowi można przydzielać prawa do wykonywania zadań administracyjnych dla określonej jednostki organizacyjnej. Prawa te mogą być prawami najwyższego poziomu, dzięki którym użytkownik ma pełną kontrolę na jednostką organizacyjną i wszystkimi jej obiektami lub prawa te mogą być bardzo ograniczone i specyficzne (na przykład, mogą umożliwiać jedynie resetowanie haseł użytkowników danej jednostki organizacyjnej). Zgodnie z ustawieniami domyślnymi użytkownik, któremu przydzielone zostały prawa administracyjne do jednostki organizacyjnej, nie ma żadnych praw administracyjnych poza jednostką organizacyjną.

W kontekście przypisywania praw (nazywanych również uprawnieniami w wielu oknach dialogowych i ekranach Właściwości systemu Windows) obiektom wewnątrz jednostki organizacyjnej struktura jednostek jest bardzo elastyczna. Sama jednostka organizacyjna ma listę kontroli dostępu (ACL), gdzie można przypisywać prawa do tej jednostki organizacyjnej. Każdy obiekt jednostki organizacyjnej, w rzeczywistości każdy atrybut każdego obiektu, ma również listę ACL. Oznacza to, że można mieć bardzo szczegółową kontrolę praw administracyjnych w jednostce organizacyjnej. Na przykład można grupie Help Desk przydzielić prawa do zmiany haseł użytkowników jednostki organizacyjnej, bez możliwości zmiany jakichkolwiek innych właściwości kont użytkowników, lub można przydzielić działowi kadr prawa modyfikowania informacji osobowych wszystkich kont użytkowników we wszystkich jednostkach organizacyjnych, bez przypisywania żadnych innych praw do pozostałych atrybutów kont użytkowników czy praw do innych obiektów. Można także przydzielać prawa poszczególnym obiektom wewnątrz jednostki organizacyjnej, jeśli znajdują się tam niektóre obiekty, które mają mieć inne prawa niż pozostałe obiekty w jednostce organizacyjnej.

Wykorzystanie jednostek organizacyjnych do administracji grupami obiektów

Innym powodem, dla którego używane są jednostki organizacyjne, jest grupowanie obiektów tak, aby obiekty te mogły być administrowane w ten sam sposób. Przykładowo, jeśli zachodzi potrzeba administrowania w ten sposób wszystkimi stacjami roboczymi w danym dziale (takimi jak ograniczanie, którzy użytkownicy mają prawo logować się na stacjach roboczych), to można zgrupować wszystkie stacje robocze w jednostce organizacyjnej i konfigurować uprawnienie Logon Locally (Logowanie lokalne) na poziomie jednostki organizacyjnej. Uprawnienie to zostanie zastosowane do wszystkich stacji roboczych tej jednostki organizacyjnej. Jeśli dla grupy użytkowników należy stosować tę samą standardową konfigurację pulpitu i ten sam zestaw aplikacji, to użytkownicy mogą zostać zgrupowani w jednostce organizacyjnej, a następnie można posłużyć się zasadami grupy do skonfigurowania pulpitu i do zarządzania instalacją aplikacji.

W wielu przypadkach obiekty w jednostce organizacyjnej będą zarządzane za pomocą zasad grupy. Zasady grupy mogą być używane do blokowania pulpitów użytkowników, do udostępniania użytkownikom standaryzowanego pulpitu, do udostępniania skryptów logowania i wylogowania czy umożliwienia przekierowania folderów. W tabeli 2-3 zamieszczona została skrótowa lista typów ustawień dostępnych w zasadach grupy.

Tabela 2-3 Typy ustawień zasad grupy

Typy ustawień	Wyjaśnienie
Szablony zabezpieczeń	Używane do zarządzania parametrami opartymi na rejestrze w celu konfigurowania ustawień aplikacji i pulpitu użytkownika, wliczając w to dostęp do składników systemu operacyjnego, dostęp do panelu sterowania czy konfiguracji plików trybu offline.
Zabezpieczenia	Używane do zarządzania ustawieniami zabezpieczeń komputera lokalnego, domeny i sieci, wliczając w to kontrolowanie dostępu użytkownika do sieci, konfigurowanie zasad konta i praw użytkownika.
Instalacja oprogramowania	Używane do scentralizowanego zarządzania instalacjami oprogramowania i konserwacją.
Skrypty	Używane do określania, które skrypty mogą być uruchamiane podczas uruchamiania bądź zamykania komputera lub podczas logowania bądź wylogowania użytkownika.
Przekierowanie folderu	Używane do przechowywania na serwerze w sieci niektórych folderów profilu użytkownika. Foldery te, takie jak folder My Documents, prezentowane są tak, jakby były przechowywane lokalnie, ale w rzeczywistości są przechowywane na serwerze, dzięki czemu można do nich uzyskać dostęp z dowolnego komputera czy sieci.

Tabela 2-3 Typy ustawień zasad grupy

Typy ustawień	Wyjaśnienie
Preferencje	Używane do zarządzania opcjami dotyczącymi ustawień systemu Windows lub Panelu sterowania, wliczając w to mapowanie dysków, zmienne środowiskowe, udziały sieci, użytkownicy i grupy lokalne, usługi, urządzenia i wiele innych.

Obiekty zasad grupy będą najczęściej przypisywane na poziomie jednostki organizacyjnej. Takie podejście ułatwia wykonywanie zadań związanych z administracją użytkowników jednostki organizacyjnej, ponieważ do jednostki organizacyjnej można przypisywać jeden obiekt zasad grupy (na przykład zasady szablonu administracyjnego), stosowanie którego jest następnie wymuszane dla wszystkich użytkowników i komputerów należących do tej jednostki organizacyjnej.



Uwaga Jednostki organizacyjne nie są podmiotami zabezpieczeń. Oznacza to, że nie można używać jednostek organizacyjnych do przypisywania uprawnień do zasobów, a następnie założyć, że wszyscy użytkownicy tej jednostki organizacyjnej automatycznie dziedziczyć będą te uprawnienia. Jednostki organizacyjne są używane w celach administracyjnych, natomiast grupy zabezpieczeń są używane do przydzielania dostępu do zasobów.

Podsumowanie

W niniejszym rozdziale ogólnie opisane zostały podstawowe fizyczne i logiczne składniki usług AD DS systemu Windows Server 2008. Pomimo że istotną kwestią jest zrozumienie roli składników fizycznych (w szczególności przy zarządzaniu bazami danych, rozmieszczaniu kontrolerów domen i zarządzaniu schematem), większa część pracy administratora usług AD DS dotyczyć będzie składników logicznych. Pozostała część książki w większości dotyczy struktury logicznej usług AD DS.

Źródła dodatkowe

- Rozdział 5 „Projektowanie struktury usług AD DS (Active Directory Domain Service)” – szczegółowy opis projektowania logicznej i fizycznej konfiguracji usług AD DS.
- Dokument „The Domain and Forest Trusts Technical Reference” udostępniony pod adresem *http://technet2.microsoft.com/windowsserver/en/library/92b3b6cb-9eb3-4dd7-b5f6-3fa9be8080821033.mspx?mfr=true* omawia szczegółowo relacje zaufania w usłudze Active Directory. Dokument ten odnosi się do systemu Windows Server 2003, ale sposób, w jaki relacje zaufania zostały zaimplementowane w systemie Windows Server 2008, nie zmienił się istotnie.
- Repozytorium skryptów: witryna sieci Web usługi Active Directory pod adresem *http://www.microsoft.com/technet/scriptcenter/scripts/default.mspx?mfr=true* zawiera kilka skryptów, które mogą być używane do wyświetlania i modyfikowania obiektów usług AD DS.

Narzędzia

W systemie Windows Server 2008 udostępniono kilka narzędzi, które mogą być używane do zarządzania logicznymi i fizycznymi składnikami usług AD DS. Niektóre z tych narzędzi zostały wymienione w tabeli 2-4.

Tabela 2-4 Narzędzia zarządzania usługami AD DS

Nazwa	Opis i sposób użycia
Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory)	Używane do konfigurowania domen usług AD DS, wliczając w to konfigurowanie i zarządzanie jednostkami organizacyjnymi i wszystkimi innym obiektami domeny.
Active Directory Domains and Trusts (Domeny i relacja zaufania usługi Active Directory)	Używane do konfigurowania relacji zaufania usług AD DS.
Active Directory Sites and Services (Lokacje i usługi Active Directory)	Używane do konfigurowania lokacji i replikacji.
Ntdsutil.exe lub Dsbutil.exe	Używane do zarządzania plikami magazynu danych usług AD DS i do przenoszenia ról FSMO pomiędzy kontrolerami domen.
ADSI Edit	Używane do przeglądania i modyfikowania zawartości partycji usług AD DS.

Zasoby znajdujące się na dysku CD

- Skrypt ListDomainControllers.ps1 w powłoce Windows PowerShell wyświetla wszystkie kontrolery domen w danej domenie i serwery wykazu globalnego w lesie.
- Skrypt ListFSMOs.ps1 w powłoce Windows PowerShell wyświetla wszystkie serwery wzorców operacji w lesie i domenie.
- Skrypt ListADDSDomains.ps1 w powłoce Windows PowerShell wyświetla informacje o wszystkich domenach w lesie.
- Skrypt ListADDSSites.ps1 w powłoce Windows PowerShell wyświetla informacje o wszystkich lokacjach w lesie.

Powiązane tematy modułów Pomoc

- „Managing Trusts” w module Pomoc przystawki Active Directory Domains and Trusts.

- „Managing Forest Trusts” w module Pomoc przystawki Active Directory Domains and Trusts.
- „Understanding Domains” w module Pomoc przystawki Active Directory Users and Computers.

Rozdział 3

Usługi AD DS i DNS

W tym rozdziale:

Integracja systemu DNS i usług AD DS 68
Zintegrowane strefy usługi AD DS 80
Integracja przestrzeni nazw DNS i domen usług AD DS 87
Podsumowanie. 97
Porady praktyczne. 98
Źródła dodatkowe. 98

Usługi AD DS (Active Directory Domain Services) w systemie Microsoft Windows Server 2008 wymagają systemu DNS (Domain Name System) do zlokalizowania zasobów w sieci. Bez niezawodnie działającej infrastruktury DNS nie byłaby możliwa replikacja usług AD DS pomiędzy kontrolerami domen, klienci systemów Microsoft Windows XP i Windows Vista nie mogliby zalogować się w sieci, a serwery oprogramowania Microsoft Exchange Server 2007 nie mogłyby wysyłać wiadomości e-mail. W zasadzie, jeśli system DNS nie jest stabilny i dostępny, to nie działa sieć systemu Windows Server 2008. Oznacza to, że administrator powinien posiadać rzetelną wiedzę na temat systemu DNS i implementacji DNS w systemie Windows Server 2008, jeśli zamierza zarządzać środowiskiem usług AD DS w systemie Windows Server 2008.

Usługi AD DS w różny sposób są ściśle zintegrowane z systemem DNS. Przede wszystkim wszystkie komputery systemu Microsoft Windows 2000 i kolejnych systemów korzystają z usługi DNS do zlokalizowania kontrolerów domen w środowisku usług AD DS – są to próby zalogowania się do sieci przeprowadzane przez komputery klienckie, próby połączeń z partnerami replikacji dokonywane przez kontrolery domen czy wyszukiwania w usługach AD DS informacji o odbiorcach wiadomości e-mail przeprowadzane przez program Exchange Servers. Dopiero po nieudanym wyszukiwaniu systemu DNS komputery te będą próbowały rozpoznać nazwy NetBIOS przy użyciu systemu Windows Internet Name Service (WINS), rozgłoszeń lub plików LMHosts. Po drugie, dane strefy systemu DNS można przechowywać w magazynie danych usług AD DS, co usprawnia funkcjonalność i poprawia bezpieczeństwo. Ponadto nazwy domen usług AD DS są nazwami systemu DNS. Jeśli w lesie usług AD DS znajduje się kilka domen w konfiguracji hierarchicznej (nadrzędne-podrzędne) lub w konfiguracji partnerskiej (kilka drzew domen), to implementacja systemu DNS powinna odpowiadać implementacji domen usług AD DS.



Ważne Ponieważ system DNS ma zasadnicze znaczenie dla usług AD DS, administrator musi znać pojęcia związane z systemem DNS i sposobem jego implementacji. Doskonałym źródłem informacji o systemie DNS jest witryna firmy Microsoft, DNS Technical Reference, udostępniona pod adresem *http://technet2.microsoft.com/WindowsServer/en/Library/6e45e81e-fb44-4a20-a752-ebe740e2acc61033.mspx*.