

IDŹ DO

PRZYKŁADOWY ROZDZIAŁ



SPIS TREŚCI

KATALOG KSIĄŻEK

KATALOG ONLINE

ZAMÓW DRUKOWANY KATALOG

TWÓJ KOSZYK

DODAJ DO KOSZYKA

CENNIK I INFORMACJE

ZAMÓW INFORMACJE
O NOWOŚCIACH

ZAMÓW CENNIK

CZYTEL尼亚

FRAGMENTY KSIĄŻEK ONLINE

Microsoft Small Business Server 2003. Księga eksperta

Autor: Eriq Neale

Tłumaczenie: Paweł Gonera

ISBN: 83-246-0651-3

Tytuł oryginału: [Microsoft Small Business Server 2003 Unleashed](#)

Format: B5, stron: około 688

oprawa twarda



Wszystostronny przewodnik po platformie Small Business Server 2003

- Zainstaluj pakiet Small Business Server 2003 i naucz się nim administrować
- Zapewnij bezpieczeństwo serwera i stacji roboczych
- Usprawnij współpracę w swojej firmie

Microsoft Small Business Server 2003 to kompletny pakiet oprogramowania przeznaczony do zarządzania danymi w małych firmach. W jego skład wchodzi serwer sieciowy, rozbudowany klient poczty elektronicznej, mechanizmy udostępniania zasobów, liczne funkcje zapewniające ochronę danych i sieci oraz inne narzędzia, które umożliwiają wydajne działanie przedsiębiorstwa i współpracę zatrudnionych osób. Trzeba jednak pamiętać, że pakiet Small Business Server 2003 to coś więcej niż tylko zestaw programów biurowych, dlatego do sprawnego korzystania z niego wymagana jest pewna wiedza.

Dzięki książce „Microsoft Small Business Server 2003. Księga eksperta” szybko nauczysz się zarządzać tym pakietem na różnych poziomach zaawansowania. Poznasz możliwości wszystkich podstawowych funkcji Small Business Server, ich domyślne ustawienia, zaawansowaną konfigurację, a także sposoby skutecznego rozwiązywania problemów. Dowiesz się, jak integrować usługi, obsługiwać serwer IIS, zapewniać zdalny dostęp do serwera, zabezpieczać dane i stacje robocze, zarządzać firmową pocztą i wykonywać wiele innych zadań związanych z administracją Small Business Server 2003. W książce znajdziesz również szereg praktycznych przykładów wdrożenia tego pakietu oraz przeczytasz o korzyściach, jakie dało firmom jego zastosowanie.

- Instalowanie i konfigurowanie Small Business Server
- Integrowanie usług DNS, DHCP i Active Directory
- Administrowanie serwerem IIS
- Dostęp zdalny
- Korzystanie z usług terminalowych
- Zabezpieczanie danych i stacji roboczych
- Zarządzanie pocztą elektroniczną
- Współpraca przez internet
- Zarządzanie klientami
- Administrowanie i zarządzanie oprogramowaniem Small Business Server
- Praktyczne zastosowania pakietu

Jeśli jesteś administratorem Small Business Server, ta książka pomoże Ci zaoszczędzić mnóstwo czasu i rozwiązać wiele problemów.

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



Spis treści

Wstęp	25
Część I Profil pakietu Microsoft Small Business Server 2003	27
Rozdział 1. Opis technologii SBS	29
Rozwój i dojrzewanie SBS	31
Pierwsza wersja — SBS 4.0	33
Druga wersja — SBS 4.5	35
Trzecia wersja — SBS 2000	37
Czwarta wersja — SBS 2003	39
Wersje SBS 2003	41
SBS 2003 Standard Edition	41
SBS 2003 Premium Edition	42
SBS 2003 SP1	42
Podsumowanie	43
Rozdział 2. Przykłady zastosowań biznesowych dla SBS	45
Definicja małej firmy	45
Definicja mikrofirmy (jako podzbioru małej)	46
Firma jednoosobowa	46
Nakładające się potrzeby korporacji i małych firm	47
Wyjątkowe tendencje	47
Marketing w świecie małych firm	47
Wpływ sprzedaży na świat małych firm	48
Technologia i właściciel małej firmy	48
Finanse i przepływy pieniężne dla zarządzających małymi firmami	49
Lista potrzeb z priorytetami	49
Jak SBS spełnia te potrzeby	50
SBS w działaniu — analiza przypadków	50
Calvert Technologies	50
HeadNETWORKS, LLC	51
Interprom Computer Technologies	52
Rehab Designs, Inc	53
Correct Solutions Pty Ltd	54
JD Fogg Technology	55
The Norwich Group	56

Specyficzne nisze małych firm	56
Gabinety medyczne	56
Usługi profesjonalne	57
Wycena przedsiębiorstw	57
Detal	58
Podsumowanie	58

Część II Instalacja SBS 2003 59

Rozdział 3. Planowanie nowej instalacji SBS 61

Zapoznanie się z bazą kliencką	61
Planowanie prawidłowego licencjonowania	62
Kiedy korzystać z licencji użytkowników	62
Kiedy korzystać z licencji urządzeń	63
Licencje CAL serwera terminali	63
Planowanie sieci	64
Podłączenie do internetu	65
Jedna czy dwie karty sieciowe	65
Zakresy adresów IP	68
Konfiguracja DHCP	70
Publiczne i prywatne nazwy domen	70
Bezprzewodowy dostęp do sieci	71
Planowanie układu pamięci dyskowej	72
Odporność na awarie	73
Wiele partycji czy wiele osi	75
Technologie wykonywania kopii zapasowych	77
Podsumowanie	78
Podsumowanie najlepszych praktyk	78

Rozdział 4. Instalowanie SBS 2003 SP1 na nowym serwerze 81

Instalowanie systemu Small Business Server	81
Instalacja podstawowego systemu operacyjnego Windows Server 2003	82
Zintegrowana instalacja SBS	83
Instalacja komponentów SBS	86
Konfiguracja SBS — lista czynności do wykonania, część 1.	88
Podłączenie do internetu	88
Konfiguracja zdalnego dostępu	94
Aktywacja serwera	95
Dodawanie licencji klienckich	95
Konfiguracja instalacji — lista czynności do wykonania, część 2.	95
Dodawanie drukarek	96
Dodawanie użytkowników i komputerów	96
Konfiguracja usług faksowych	96
Konfigurowanie monitorowania	97
Konfigurowanie kopii zapasowej	97
Konfiguracja aktualizacji automatycznych	98
Rozwiązywanie problemów z instalacją	99
Podsumowanie	103
Podsumowanie najlepszych praktyk	104

Część III Sieć SBS 2003 105

Rozdział 5. Integracja usług DNS, DHCP oraz Active Directory 107

Przegląd integracji usług Active Directory oraz DNS	107
Co to jest DNS	107
Jak działa DNS	108
Jak Active Directory korzysta z DNS	108
Konfiguracja DNS dla sieci wewnętrznej	110
Standardowa konfiguracja serwera DNS	110
Standardowa konfiguracja DNS stacji roboczej	111
Konfiguracja DNS do rozpoznawania publicznych adresów internetowych	113
Wykorzystanie usługi przesyłania dalej serwera DNS w konsoli Zarządzanie systemem DNS	113
Wykorzystanie wskazówek dotyczących serwerów głównych w konsoli Zarządzanie systemem DNS	114
Konfiguracja DHCP dla sieci wewnętrznej	115
Co to jest DHCP	115
Domyślne ustawienia DHCP w SBS	117
Modyfikowanie ustawień DHCP	117
Rozwiązywanie problemów z usługami DNS, DHCP oraz Active Directory	120
Rozwiązywanie problemów z wewnętrznym wyszukiwaniem w DNS	121
Rozwiązywanie problemów z zewnętrznym wyszukiwaniem w DNS	125
Rozwiązywanie problemów z DHCP	127
Rozwiązywanie problemów Active Directory związanych z DNS	128
Podsumowanie	131
Podsumowanie najlepszych praktyk	131

Rozdział 6. Usługa IIS 133

Usługa IIS a Small Business Server	133
Technologie Web w SBS	133
Komponenty IIS	134
Konfiguracja domyślnych witryn	138
Ustawienia dla domyślnej witryny sieci Web	138
Ustawienia dla witryny Companyweb	142
Ustawienia witryny Administracja programu Microsoft SharePoint	145
Ustawienia witryny Administracja centralna programu SharePoint	145
Konfiguracja dodatkowych witryn	146
Tworzenie kopii zapasowej konfiguracji IIS	146
Tworzenie nowej witryny	148
Zarządzanie katalogami wirtualnymi	150
Instalowanie usług sieciowych innych firm	150
Udostępnianie w internecie bezpiecznych witryn przy wykorzystaniu certyfikatów SSL firm zewnętrznych	152
Rozwiązywanie problemów z IIS	157
Anatomia strony błędu	157
Usługa niedostępna	158
Ograniczenia adresów IP	160
Podsumowanie	161
Podsumowanie najlepszych praktyk	162

Rozdział 7. Routing i dostęp zdalny, VPN oraz zapory sieciowe 163

Podstawy usługi Routing i dostęp zdalny (RRAS)	163
Zastosowanie zapory sieciowej RRAS	164
Kreator CEICW a zapora sieciowa RRAS	165
Konfiguracja zapory sieciowej RRAS	166
Podstawy zdalnego dostępu	170
Opcje zdalnego dostępu	170
Konfiguracja zdalnego dostępu	173
Konfigurowanie serwera	173
Konfiguracja klientów	175
Rozwiązywanie problemów z routingiem i dostępem zdalnym	177
Usługa nie jest dostępna zdalnie	177
Chcemy skorzystać zdalnie z serwera, ale dostępne są tylko dynamiczne adresy IP	178
Nie można podłączyć się zdalnie za pomocą VPN — błąd 721	179
Udało się podłączyć do VPN, ale nie można skorzystać z żadnego zasobu	179
Nie można zestawić więcej niż pięciu jednoczesnych połączeń VPN	179
Po podłączeniu do VPN dostęp do internetu jest powolny lub zablokowany	180
Połączenie VPN rozłącza się po określonym czasie bezczynności	180
Więcej zasobów pomocnych w rozwiązywaniu problemów	180
Podsumowanie	181
Podsumowanie najlepszych praktyk	181

Rozdział 8. Usługi terminalowe 183

Przegląd trybów działania usług terminalowych	183
Tryb zdalnej administracji	183
Tryb aplikacji	184
Instalowanie i konfigurowanie serwera terminali	185
Instalowanie usług terminalowych	185
Konfigurowanie usługi licencjonowania serwera terminali	186
Zarządzanie serwerami terminali	187
Instalowanie aplikacji	187
Konfiguracja usług terminalowych	188
Działanie konsoli Menedżer usług terminalowych	190
Rozwiązywanie problemów z usługami terminali	192
Konfiguracja zwiększonych zabezpieczeń programu Internet Explorer	192
Serwer terminali nie pojawia się w usłudze Zdalne miejsce pracy w sieci Web	193
Użytkownicy nie mogą zalogować się na serwerze terminali	193
Podsumowanie	194
Podsumowanie najlepszych praktyk	194

Część IV Bezpieczeństwo 197**Rozdział 9. Bezpieczeństwo serwera 199**

Bezpieczeństwo fizyczne	199
Bezpieczeństwo na poziomie systemu plików	200
Uprawnienia plików NTFS	200
Stosowanie uprawnień NTFS	201
Szyfrowanie systemu plików	206
Bezpieczeństwo na poziomie udziałów	208

Bezpieczeństwo haseł	211
Konfiguracja zasad haseł	212
Obiekt zasad haseł domeny Small Business Server	214
Rozwiązywanie problemów z zabezpieczeniami	215
Częste problemy z dostępem	216
Czynne uprawnienie	217
Podsumowanie	218
Podsumowanie najlepszych praktyk	219

Rozdział 10. Bezpieczeństwo stacji roboczych221

Windows XP Service Pack 2	222
Zapora systemu Windows	223
Internet Explorer	225
Outlook Express	228
Zapobieganie wykonywaniu danych (DEP)	228
Aktualizacje automatyczne	228
Centrum zabezpieczeń systemu Windows	228
Lokalni administratorzy	229
Konfiguracja grup zabezpieczeń	231
Narzędzia antywirusowe	235
Narzędzia antyspyware	237
Sieć zarządzana	239
Nie zapominajmy o Office	240
Szkolenie użytkowników końcowych i proces przeglądów bezpieczeństwa	242
Zabezpieczanie danych przed dostępem z wewnątrz firmy	244
Rozwiązywanie problemów z bezpieczeństwem stacji roboczych	246
Podsumowanie	250
Podsumowanie najlepszych praktyk	250

Część V Serwer Exchange251

Rozdział 11. Połączenia klienckie253

Wykorzystanie programu Outlook	253
Instalacja programu Outlook	254
Tryb buforowy programu Exchange	255
Konfiguracja programu Outlook poprzez internet lub RPC po HTTP	257
Konfiguruj Outlook poprzez internet na kliencie	260
Wykorzystanie Outlook Web Access	261
Outlook Web Access podstawowy	264
Outlook Web Access zaawansowany	264
Outlook Web Access zaawansowany z ActiveX	266
Ustawienia zabezpieczeń Outlook Web Access	267
Wykorzystanie Outlook Mobile Access (OMA)	270
Wykorzystanie ActiveSync	273
Wersje ActiveSync	273
Urządzenia przenośne	273
Synchronizacja	274
Rozwiązywanie problemów z połączeniami klienckimi	277
Rozwiązywanie problemów z trybem buforowanym programu Exchange	277
Rozwiązywanie problemów z programem Outlook poprzez internet	279

Rozwiązywanie problemów z Outlook Web Access	280
Rozwiązywanie problemów z Outlook Mobile Access (OMA)	280
Rozwiązywanie problemów z ActiveSync	281
Podsumowanie	283
Podsumowanie najlepszych praktyk	283

Rozdział 12. Zarządzanie serwerem Exchange 285

Zarządzanie konfiguracją domyślnej skrzynki pocztowej	285
Niechciana poczta i wirusy	286
Filtrowanie odbiorców i funkcja tar pit	287
Exchange Intelligent Message Filter (IMF)	289
Dostarczanie poczty pomimo funkcji antyspamowych	291
Łącznik POP3	296
Jak działa łącznik POP3	297
Ograniczenia łącznika POP3	298
Konfiguracja łącznika POP3	298
Kierowanie poczty z konta globalnego	299
Kierowanie poczty do kont indywidualnych	300
Odbieranie poczty z wielu domen	301
Dodawanie kolejnych adresów e-mail	301
Zasady odbiorców	302
Usługa Recipient Update Service	304
Kierowanie poczty do strefy nieautorytatywnej	305
Rozwiązywanie problemów z konfiguracją Exchange	305
Rozwiązywanie problemów z pocztą wychodzącą	306
Rozwiązywanie problemów z IMF	309
Rozwiązywanie problemów z łącznikiem POP3	310
Podsumowanie	312
Podsumowanie najlepszych praktyk	312

Rozdział 13. Przywracanie Exchange po awarii 313

Opis struktury bazy danych Exchange	314
Grupy pamięci masowej Exchange	315
Bazy danych Extensible Storage Engine (ESE)	316
Pliki dzienników	318
Plik punktu kontrolnego	320
Transakcje	321
Opis wymagań i metod tworzenia kopii zapasowych w Exchange	322
Kopia zapasowa w trybie online	322
Kopia zapasowa w trybie offline	324
Uprawnienia	325
Tworzenie kopii zapasowej Exchange za pomocą kreatora konfiguracji kopii zapasowych	325
Zastosowanie programu NTBackup	328
Zastosowanie ExMerge	329
Zastosowanie rozwiązań innych firm	331
Przywracanie baz danych Exchange z kopii zapasowej	332
Zdarzenia wymagające przywracania Exchange	334
Proces odtwarzania	334
Zastosowanie kreatora przywracania SBS do odtwarzania	335
Zastosowanie programu NTBackup do odtwarzania	335

Użycie Recovery Storage Group	338
Zastosowanie programu ExMerge do odtwarzania	342
Zastosowanie rozwiązań innych firm do odtwarzania	344
Naprawianie uszkodzonej bazy danych Exchange	344
ESEUTIL /r	346
ESEUTIL /p	346
ISINTEG	347
Przywracanie 16-gigabajtowej bazy danych	348
Rozwiązywanie problemów z przywracaniem po awarii Exchange	350
Podsumowanie	350
Podsumowanie najlepszych praktyk	351

Część VI Technologie Web353

Rozdział 14. SharePoint oraz witryna Companyweb355

Przegląd usług Windows SharePoint	355
Przegląd implementacji witryny Companyweb dla SBS	356
Domyślne lokalizacje plików w Companyweb	357
Domyślne uprawnienia dla Companyweb	358
Dostosowywanie interfejsu Companyweb	363
Stosowanie motywów do interfejsu Companyweb	363
Tworzenie i zarządzanie obiektami oraz listami	363
Tworzenie nowych widoków dla obiektów oraz list	365
Tworzenie stron personalizowanych	367
Korzystanie ze składników Web Part	367
Tworzenie nowych witryn w SharePoint	369
Tworzenie nowych podwitryn wewnątrz Companyweb	369
Tworzenie nowych witryn najwyższego poziomu w SharePoint	371
Tworzenie kopii i przywracanie danych SharePoint	374
Rozszerzanie witryny Companyweb za pomocą FrontPage	377
Korzystanie z wielu języków w SharePoint	380
Rozwiązywanie problemów z SharePoint	380
Kompletny przewodnik na temat usuwania i przeinstalowywania witryny Companyweb	382
Podsumowanie	384
Podsumowanie najlepszych praktyk	384

Rozdział 15. Zdalne miejsce pracy w sieci Web387

Przegląd interfejsu Zdalne miejsce pracy w sieci Web	387
Widok administratora	388
Widok klienta	388
Użycie aplikacji Zdalne miejsce pracy w sieci Web	390
Podłączanie do RWW	391
Podłączanie do OWA	392
Podłączanie do Companyweb	393
Łączenie z pulpitemi serwera	394
Łączenie z pulpitemi klienta	395
Informacje techniczne na temat RWW	396
Lokalizacje plików RWW oraz ustawienia rejestru	396
Konfiguracja IIS dla RWW	397

Dostosowywanie interfejsu Zdalne miejsce pracy w sieci Web	397
Zmiana wyglądu i działania RWW	397
Zwiększanie domyślnych wartości czasu bezczynności w RWW	398
Wykluczanie systemów z listy zdalnego sterowania	399
Uniemożliwienie użytkownikom podłączania napędów lokalnych do zdalnych komputerów	399
Rozwiązywanie problemów z aplikacją Zdalne miejsce pracy w sieci Web	400
Nie można podłączyć się do RWW	401
Nie można otworzyć Companyweb z poziomu RWW	402
Nie można zdalnie sterować stacjami roboczymi poprzez RWW	402
Podsumowanie	403
Podsumowanie najlepszych praktyk	403

Część VII Połączenia klienckie 405

Rozdział 16. Użytkownicy i komputery 407

Zarządzanie użytkownikami w SBS 2003	407
Dostęp administratorów i użytkowników zaawansowanych	407
Dodawanie użytkowników	408
Zastosowanie konsoli Użytkownicy i komputery usługi Active Directory	410
Zmiana uprawnień użytkownika	411
Tworzenie i modyfikowanie limitów użytkowników	414
Praca z grupami zabezpieczeń i dystrybucyjnymi	418
Zarządzanie komputerami w SBS 2003	419
Dodawanie komputerów do sieci	420
Dodawanie serwerów	428
Rozwiązywanie problemów z użytkownikami i komputerami	429
Podsumowanie	431
Podsumowanie najlepszych praktyk	431

Rozdział 17. Integracja komputerów Macintosh ze środowiskiem Small Business Server 2003 433

Udostępnianie plików komputerom Macintosh przez serwer SBS	434
Podłączanie za pomocą Usług dla komputerów Macintosh (Mac OS 9 lub Mac OS X)	434
Podłączanie z użyciem SMB (tylko Mac OS X 10.3)	442
Dostęp do bezpiecznej witryny	450
Eksportowanie certyfikatu SSL z SBS	451
Importowanie certyfikatu SSL do magazynu certyfikatów komputera Macintosh	451
Dostęp do Exchange z komputerów Macintosh	452
Włączenie IMAP na SBS	453
Exchange	460
Narzędzia zdalnego dostępu dla Macintosha	466
Zdalne miejsce pracy w sieci Web (RWW)	466
Podłączanie się do sieci SBS z użyciem VPN	468
Połączenia pulpitu zdalnego	469
Podsumowanie	470
Podsumowanie najlepszych praktyk	471

Część VIII Administracja i zarządzanie473

Rozdział 18. Tworzenie kopii zapasowej Small Business Server475

Zagadnienia związane z kopiami zapasowymi	475
Przywracanie plików	476
Archiwizacja	476
Przywracanie systemu	476
Sprzęt i nośniki	477
Plan wykonywania kopii zapasowych	478
Lokacje i bezpieczeństwo	479
Typy kopii zapasowych	480
Harmonogram kopii zapasowej	482
Rotacja nośników	482
Zastosowanie kreatora kopii zapasowych SBS	484
Ograniczenia kreatora kopii zapasowych SBS	485
Ustawienia wygenerowane przez kreator	486
Wykluczanie danych z kreatora kopii zapasowej	487
Zmiana powiadomień kopii zapasowych	490
Zastosowanie programu NTBackup	490
Zastosowanie rozwiązań innych firm do tworzenia kopii zapasowych	492
Odtwarzanie po awarii za pomocą narzędzi SBS	492
Przywracanie z kopii zapasowej	493
Rozwiązywanie problemów z kopiami zapasowymi	494
Podsumowanie	495
Podsumowanie najlepszych praktyk	495

Rozdział 19. Monitorowanie i raportowanie497

Monitorować czy nie monitorować? Oto jest pytanie	497
Typy raportów i alertów	498
Raport wydajności	498
Raport o użyciu	499
Alerty wydajności	500
Konfigurowanie i wykorzystywanie monitorowania i alertów	501
Uruchamianie Kreatora konfiguracji monitorowania	501
Rozszerzanie monitorowania i alertów	504
Zawartość raportów	504
Kiedy powinniśmy oczekiwać alertu?	507
Modyfikowanie domyślnych raportów i alertów	507
Rozwiązywanie problemów z monitorowaniem i alertami	512
Ponowne instalowanie i konfigurowanie monitorowania i alertów	513
Nieprawidłowe nazwy na raportach	513
Błędy IIS przy próbie dostępu do stron monitorowania w intranecie	514
Podsumowanie	514
Podsumowanie najlepszych praktyk	514

Rozdział 20. Zasady grupy517

Przegląd zasad grupy	517
Elementy zasad grupy	518
Zakres zasad grupy i kolejność stosowania	519

Korzystanie z konsoli Zarządzanie zasadami grupy	521
Nawigacja w konsoli Zarządzanie zasadami grupy	521
Przeglądanie ustawień zasad grupy	523
Korzystanie z narzędzi Group Policy Modeling oraz Group Policy Results	527
Tworzenie raportu modelowania	528
Tworzenie raportu wyników	530
Domyślne obiekty zasad grupy w SBS	532
Zapora systemu Windows programu Small Business Server	532
Zapora połączenia internetowego programu Small Business Server	532
Komputer kliencki programu Small Business Server	532
Zasady Pomocy zdalnej programu Small Business Server	532
Zasady blokady programu Small Business Server	534
Zasady haseł domeny programu Small Business Server	534
Default Domain Policy	536
Zasady inspekcji programu Small Business Server	537
Default Domain Controllers Policy	537
Tworzenie i modyfikacja obiektów zasad grupy w SBS	540
Planowanie obiektów GPO	540
Testowanie obiektu GPO	542
Implementowanie obiektu GPO	545
Rozwiązywanie problemów z zasadami grup	546
Narzędzia testowania zasad grupy	546
Odtwarzanie zasad grupy po awarii	548
Podsumowanie	548
Podsumowanie najlepszych praktyk	549

Rozdział 21. Zarządzanie stacjami roboczymi

poprzez zasady grupy 551

Po co zarządzać stacjami roboczymi?	551
Przekierowanie folderów i pliki trybu offline	552
Konfiguracja przekierowania folderów	554
Konfigurowanie plików w trybie offline	556
Zarządzanie dostępem do stacji roboczych	558
Ograniczenie logowania	558
Ograniczanie użytkowników	559
Inne zastosowania zasad grupy	564
Rozwiązywanie problemów z zasadami grup	565
Tworzenie kopii zapasowych oraz dokumentowanie zmian w zasadach grupy	566
Ogólne wskazówki na temat rozwiązywania problemów	567
Rozwiązywanie problemów z przekierowaniem folderów	569
Podsumowanie	569
Podsumowanie najlepszych praktyk	570

Rozdział 22. Łatki i poprawki zabezpieczeń 571

Budowa poprawki oraz proces powiadamiania	572
Testowanie poprawek i proces analizy ryzyka	574
Firma otwarta	578
Średnio zabezpieczona firma	579
Firma paranoiczna	579

Zasoby poprawek zabezpieczeń i informacji o zagrożeniach	579
Windows Update oraz aktualizacje automatyczne	580
Microsoft Baseline Security Analyzer (MBSA)	583
Witryna pobierania dla SBS	584
Shavlik HFNetChk Pro	585
Implementacja WSUS w SBS	586
Instalowanie WSUS	588
Pierwsza synchronizacja	591
Konfigurowanie zasad grupy dla WSUS na serwerze	594
Proces aprobowania	597
WSUS w systemach OEM	599
Rozwiązywanie problemów z poprawkami	600
Podsumowanie	602
Podsumowanie najlepszych praktyk	603

Część IX Premium Technologies605

Rozdział 23. Podstawy Internet Security and Acceleration Server 2004607

Nowe funkcje w ISA 2004	608
Konsola MMC zarządzania serwerem ISA	608
Sieci ISA	609
Kwarantanna VPN	611
Zaakceptować czy odrzucić?	612
Delegowanie administracji	613
Pojęcia ISA	616
Typy klientów ISA	616
Zarządzanie danymi dzienników	620
Tryb blokady serwera ISA	623
Połączenia klienckie	624
Przyspieszanie internetu	626
Podsumowanie	628
Podsumowanie najlepszych praktyk	629

Rozdział 24. Zaawansowana administracja Internet Security and Acceleration Server 2004631

Zarządzanie serwerem ISA	632
Dostosowanie panelu kontrolnego	632
Potwierdzanie alertów	632
Wykrywanie oszustw DHCP	633
Konfigurowanie punktu dostępu bezprzewodowego	635
Włączanie wykrywania włamań	635
Konfigurowanie automatycznego wykrywania klienta Firewall	638
Modyfikacja ustawień ISA	639
Omówienie filtrów aplikacji i Web	639
Anatomia zasad zapory	639
Tworzenie nowych zasad zapory	642
Konfiguracja witryn do bezpośredniego dostępu	645
Dodawanie portów tunelowania SSL	646

Umożliwianie pobierania z i wysyłania do zewnętrznych serwerów za pomocą FTP	647
Publikowanie serwera Web	649
Rozwiązywanie problemów	651
Podsumowanie	652
Podsumowanie najlepszych praktyk	652

Dodatki 655

Dodatek A Zasoby na temat SBS 657

Zasoby społeczności Microsoft	657
Witryny WWW oraz strumienie RSS	657
Grupy dyskusyjne	658
Dzienniki Web (blogi)	658
Zasoby społeczności Small Business Community	658
Witryny i blogi	658
Listy wysyłkowe	659
Zasoby na temat Exchange	659
Zasoby na temat komputerów Macintosh	660
Witryny WWW oraz strumienie RSS	660
Grupy dyskusyjne	660
Listy wysyłkowe	660
Zasoby na temat programu Outlook	661
Zasoby na temat Outlook Web Access	661
Zasoby na temat ActiveSync/PocketPC	662
Zasoby na temat monitorowania i raportowania w SBS	662
Zasoby na temat zasad grupy	662
Zasoby na temat RRAS, VPN i zapory sieciowej	663
Zasoby na temat serwera terminali	663
Zasoby na temat bezpieczeństwa stacji roboczych	664
Narzędzia antywirusowe	664
Zestaw obsługi zagrożeń	664
Zasoby na temat bezpieczeństwa i aktualizacji	666
Ogólne informacje na temat bezpieczeństwa	666
Zasoby WSUS	666

Skorowidz 667

Rozdział 5.

Integracja usług DNS, DHCP oraz Active Directory

Podstawą każdej instalacji SBS jest solidna infrastruktura Active Directory. Ponieważ usługa Active Directory w znacznej mierze zależy od technologii sieciowych takich jak DNS, udana i pomyślna implementacja SBS powinna mieć prawidłowo skonfigurowaną sieć. Odnosi się to nie tylko do serwera, ale również do stacji roboczych. W rozdziale tym szczegółowo przedstawimy domyślną konfigurację sieci i nakreślimy potencjalne problemy, jakie mogą wynikać podczas zmiany konfiguracji.

Przegląd integracji usług Active Directory oraz DNS

Przy okazji wprowadzenia produktu Windows 2000 Server Microsoft udostępnił nową usługę katalogową, która zastąpiła płaską strukturę katalogową wykorzystywaną w Windows NT. Usługa Active Directory posiada znacznie bardziej skomplikowaną strukturę katalogu i aby działała ona prawidłowo, należy dokładnie znać strukturę sieci. By to osiągnąć, Microsoft związał wiele funkcji usługi Active Directory z DNS i innymi technologiami sieciowymi. Bez prawidłowo działającego i niezawodnego systemu DNS usługa Active Directory jest właściwie bezużyteczna. Z tego powodu nawet w przypadku sieci jednoserwerowej, jak w większości instalacji SBS, bardzo ważna jest podstawowa znajomość DNS oraz sposobu integracji z Active Directory.

Co to jest DNS

DNS to skrót od *Domain Name System* (albo *Domain Name Service* lub *Domain Name Server*, w zależności od źródła), który jest mechanizmem tłumaczącym nazwy komputerów w sieci na ich adresy IP. DNS można porównać do dużej elektronicznej książki telefonicznej, w której komputery z całego świata mogą się wzajemnie wyszukiwać.

Jednak DNS ma służyć bardziej ludziom niż komputerom. Większość ludzi łatwiej zapamiętuje słowa i zdania niż liczby. Ponieważ cała komunikacja komputerów jest realizowana z wykorzystaniem liczb, mechanizm ten jest dla nas szczególnie ważny. Znacznie łatwiej jest zapamiętać *www.microsoft.com* lub *www.google.com* niż 207.46.156.156 lub 64.233.187.99. Dodatkowo żadne z urządzeń nie „zna” nazw i adresów wszystkich urządzeń sieciowych podłączonych do internetu — ale struktura systemu DNS rozwiązuje ten problem.

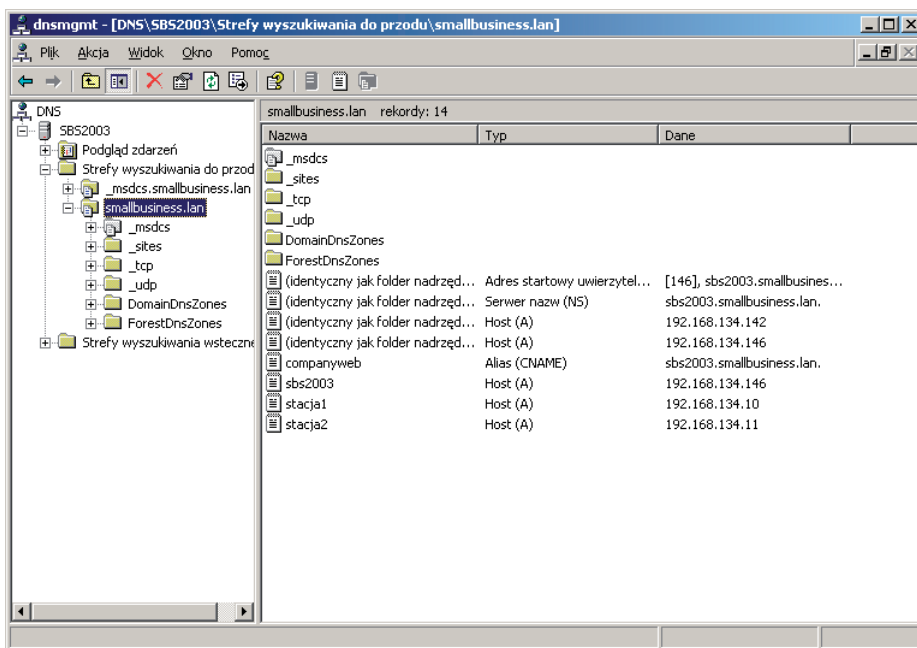
Jak działa DNS

Gdy otworzymy przeglądarkę internetową i wpiszymy w niej *www.google.com*, na ekranie w „magiczny” sposób pojawi się strona domowa wyszukiwarki Google. Jednak zanim się to zdarzy, musi zostać wykonanych wiele operacji. Po pierwsze, komputer przejrzy wewnętrzną pamięć adresów, sprawdzając, czy został już wcześniej odnaleziony adres IP dla *www.google.com*. Jeśli tak będzie, komputer skorzysta z adresu z bufora i spróbuje zrealizować połączenie do serwera korzystającego z tego adresu IP. Jeżeli w lokalnym buforze nie ma tego adresu, do „gry” wchodzi system DNS. Komputer skontaktuje się z serwerem DNS wymienionym we właściwościach połączenia i „zapyta” go o adres *www.google.com*. Serwer DNS sprawdzi w lokalnym buforze, czy adres ten nie był już wcześniej wyszukiwany. Jeżeli tak, wyśle go z powrotem do komputera, a ten będzie mógł skontaktować się z serwerem WWW. Jeżeli serwer DNS nie będzie posiadał tego adresu w swoich danych konfiguracyjnych ani w lokalnej pamięci podręcznej, przekaże pytanie do innego serwera, a cały proces będzie powtarzany aż do momentu znalezienia serwera, który będzie posiadał informacje na temat adresu odpowiadającego szukanej nazwie.

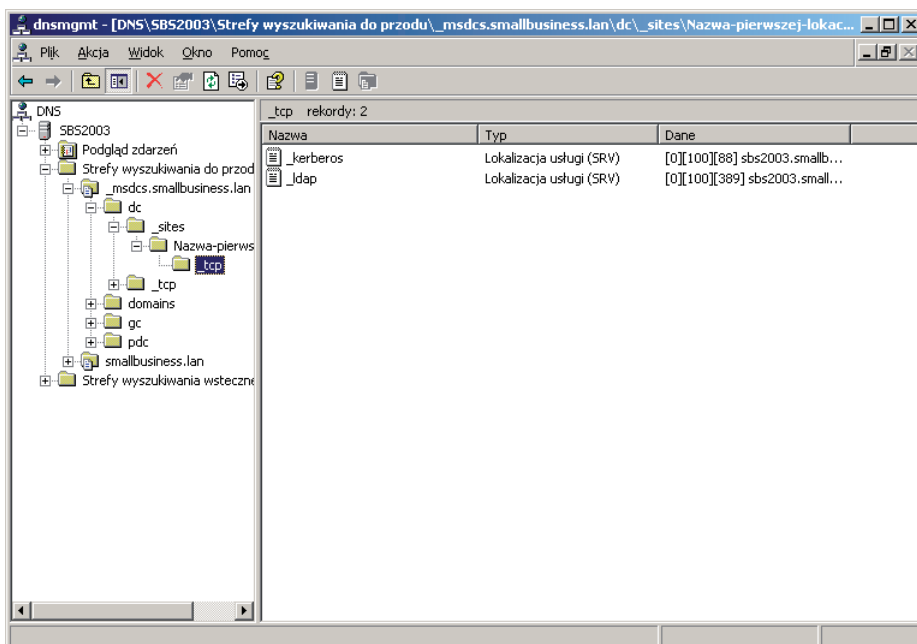
Jak Active Directory korzysta z DNS

Podczas gdy serwer Windows ma uruchomioną usługę DNS i wchodzi w skład struktury Active Directory, serwer DNS przechowuje więcej informacji niż tylko nazwy komputerów i ich adresy. W DNS przechowywana jest duża liczba rekordów usług (SRV), które pozwalają komputerom ze środowiska Active Directory lokalizować komputery udostępniające usługi związane z Active Directory. Do przeglądania i konfiguracji ustawień DNS na serwerze wykorzystywana jest konsola *Zarządzanie systemem DNS*. Aby ją otworzyć, kliknij *Start/Narzędzia administracyjne/DNS* lub w wierszu polecenia wpisz *dnsmgmt.msc* i naciśnij *Enter*. Na rysunku 5.1 pokazany jest wygląd konsoli *Zarządzanie systemem DNS* dla wewnętrznej domeny. Można na nim zauważyć rekordy hostów DNS (nazywane również rekordami A) dla serwera SBS, jak również dla kilku stacji roboczych wchodzących w skład domeny. Dodatkowo widoczne są rekordy niezwiązane z hostami, które pomagają wykonywać podstawowe wyszukiwania nazw hostów z wewnętrznej sieci.

Na rysunku 5.2 przedstawiony jest widok strefy *_msdcs* dla wewnętrznej sieci. Tu właśnie przechowywane są najważniejsze informacje dotyczące sieci na potrzeby usługi Active Directory. Strefa *_msdcs* jest podzielona na cztery obszary: *dc* dla odwołań do kontrolerów domeny; *domains* dla podstawowych informacji o domenie; *gc* dla globalnych odwołań katalogu oraz *pdc* dla odwołań do podstawowych kontrolerów domeny. Choć większość ludzi nigdy nie będzie korzystała interakcyjnie z tych danych, to jednak gdy stacja robocza



Rysunek 5.1. Konsola Zarządzanie systemem DNS zawiera listę przekształceń nazw hostów na adresy IP dla wewnętrznej sieci



Rysunek 5.2. Strefa `_msdcs` zawiera adresy wyszukiwania dla kluczowych komponentów Active Directory

Najlepsze praktyki: Tworzenie aliasów DNS zamiast rekordów hostów

Jak zostało to pokazane na rysunku 5.1, wpis dla nazwy DNS *companyweb* nie jest rekordem hosta (rekordem A), ale rekordem aliasu (CNAME). Gdy w DNS jest wyszukiwany rekord CNAME, zwracana jest inna nazwa DNS, a nie adres IP. Następnie wykonywane jest wyszukiwanie dla nowej nazwy DNS, która, jak w przypadku nazwy *companyweb*, jest przekształcana na adres IP wewnętrznej karty sieciowej serwera.

Jeżeli potrzebujemy utworzyć nowe rekordy DNS wskazujące na istniejący serwer lub stację roboczą, np. tworząc łatwiejszą do zapamiętania nazwę serwera, należy utworzyć rekord CNAME zamiast rekordu hosta. Jeżeli utworzymy ten wpis jako rekord A, a następnie zajdzie potrzeba zmiany adresu IP serwera, będziemy musieli zmienić w DNS wszystkie rekordy związane z rekordem A. Jeżeli utworzymy ten rekord jako CNAME, to przy zmianie adresu IP serwera rekord ten automatycznie pobierze nowy adres serwera, ponieważ zawsze wskazuje on na nazwę DNS serwera, a nie na jego adres IP.

Aby utworzyć nowy rekord CNAME, należy wykonać następujące operacje:

1. Kliknąć prawym przyciskiem myszy strefę przekazywania w przód i wybierać *Nowy alias (CNAME)*.
2. Wpisać nową nazwę hosta w polu *Nazwa aliasu*.
3. Wprowadzić w pełni kwalifikowaną nazwę domenową dla istniejącego komputera w polu *W pełni kwalifikowana nazwa domeny (FQDN) dla hosta docelowego*.
4. Kliknąć *OK*.

będzie próbowała uwierzytelnić się w Active Directory lub przetworzyć logowanie użytkownika w domenę, skorzysta ona z DNS do wyszukania tych usług w celu określenia, gdzie należy się podłączyć do odpowiedniej usługi, np. Kerberos.

Dokładniejsze objaśnienie usług Active Directory, DNS oraz ich integracji ze sobą wykracza poza ramy tej książki. W rzeczywistości na temat samej tylko usługi Active Directory powstało już kilka książek. Dla naszych celów takie podstawowe zrozumienie integracji DNS i Active Directory jest wystarczające, by zapewnić fundament dla obsłużenia większości problemów, jakie mogą pojawić się przy instalacji SBS związanej z DNS oraz AD.

Konfiguracja DNS dla sieci wewnętrznej

Przy wykorzystaniu domyślnych narzędzi konfiguracyjnych serwera i stacji roboczych w środowisku SBS konfiguracja sieci powinna być ustawiona dla każdego komputera w taki sposób, aby prawidłowo działało rozpoznawanie nazw wewnętrznych i zewnętrznych. Czasami jednak wiedza o tym, co powinno się zdarzyć, jest niewystarczająca. Często dopiero wiedza o tym, co faktycznie się dzieje, i porównanie z tym, co dzieć się powinno, pozwala wykryć naturę występujących problemów.

Standardowa konfiguracja serwera DNS

Sieciowa część kreatora *Connect to internet*, nazywanego również CEICW (ang. *Configure Email and Internet Connection Wizard*), pozwala skonfigurować ustawienia dla wewnętrznych i zewnętrznych interfejsów sieciowych. Konfiguracja kart sieciowych zwią-

zana z DNS jest bardzo prosta — oba interfejsy mają ustawiony adres IP wewnętrznej karty sieciowej jako adres serwera DNS. Przedstawiony poniżej wynik działania polecenia `ipconfig /all` pokazuje prawidłową konfigurację sieci dla serwera z dwoma kartami sieciowymi po uruchomieniu kreatora CEICW.

```
C:\Documents and Settings\Administrator>ipconfig /all
```

Windows IP Configuration

```
Host Name . . . . . : sbs
Primary Dns Suffix . . . . . : SmallBizCo.local
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : Yes
WINS Proxy Enabled. . . . . : Yes
DNS Suffix Search List. . . . . : SmallBizCo.local
```

Ethernet adapter Server Local Area Connection:

```
Connection-specific DNS Suffix . : 
Description . . . . . : 3Com 3C920 Integrated Fast Ethernet Controller
➔(3C905C-TX Compatible)
Physical Address. . . . . : 00-08-74-40-5B-61
DHCP Enabled. . . . . : No
IP Address. . . . . : 192.168.16.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 
DNS Servers . . . . . : 192.168.16.2
Primary WINS Server . . . . . : 192.168.16.2
```

Ethernet adapter Network Connection:

```
Connection-specific DNS Suffix . : 
Description . . . . . : Realtek RTL8029(AS) PCI Ethernet Adapter
Physical Address. . . . . : 00-C0-F0-2B-7D-F9
DHCP Enabled. . . . . : No
IP Address. . . . . : 10.10.1.9
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.10.1.1
DNS Servers . . . . . : 192.168.16.2
Primary WINS Server . . . . . : 192.168.16.2
NetBIOS over Tcpip. . . . . : Disabled
```

```
C:\Documents and Settings\Administrator>
```

Jak można zauważyć, zarówno karta wewnętrzna, jak i zewnętrzna mają jako DNS ustawiony adres wewnętrznej karty sieciowej. Dzięki temu wszystkie wyszukiwania w DNS trafiają do usługi DNS uruchomionej na serwerze.

Standardowa konfiguracja DNS stacji roboczej

Mówiąc ogólnie, stacje robocze w środowisku SBS powinny być skonfigurowane w taki sposób, aby korzystały z DHCP do konfiguracji sieci. W niektórych przypadkach stacje robocze mogą wymagać zastosowania statycznej konfiguracji adresów IP. Poniżej znajduje się wynik działania polecenia `ipconfig /all` dla standardowej konfiguracji stacji roboczej:

```
C:\Documents and Settings\Administrator>ipconfig /all
```

Windows IP Configuration

```
Host Name . . . . . : JONDOUGH01
Primary Dns Suffix . . . . . : SmallBizCo.local
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : SmallBizCo.local
                                   SmallBizCo.local
```

Ethernet adapter Server Area Connection:

```
Connection-specific DNS Suffix . : SmallBizCo.local
Description . . . . . : Intel 21140-Based PCI Fast Ethernet
➡Adapter (Generic)
Physical Address. . . . . : 00-03-FF-81-79-85
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 192.168.16.16
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.16.2
DHCP Server . . . . . : 192.168.16.2
DNS Servers . . . . . : 192.168.16.2
Primary WINS Server . . . . . : 192.168.16.2
Lease Obtained. . . . . :
Lease Expires . . . . . :
```

```
C:\Documents and Settings\Administrator>
```

Przy ręcznej konfiguracji sieci dla stacji roboczej, aby mogła ona prawidłowo komunikować się z serwerem SBS, należy prawidłowo ustawić kilka elementów. Po pierwsze, adres IP oraz maska podsieci muszą odpowiadać zakresowi adresów IP używanych dla wewnętrznej sieci. Po drugie, adres domyślnej bramy musi być adresem wewnętrznej karty sieciowej serwera SBS (w przypadku konfiguracji SBS z dwiema kartami sieciowymi) lub routera (w przypadku konfiguracji SBS z jedną kartą sieciową). Po trzecie, adres serwera DNS musi być adresem wewnętrznej karty serwera SBS. Wynik działania polecenia `ipconfig /all` ze stacji roboczej z prawidłowo skonfigurowaną siecią wygląda tak, jak poniżej:

```
C:\Documents and Settings\Administrator>ipconfig /all
```

Windows IP Configuration

```
Host Name . . . . . : JONDOUGH01
Primary Dns Suffix . . . . . : SmallBizCo.local
Node Type . . . . . : Broadcast
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : SmallBizCo.local
```

Ethernet adapter Network Connection:

```
Connection-specific DNS Suffix . :
Description . . . . . : Intel 21140-Based PCI Fast Ethernet
```

```
▼Adapter (Generic)
Physical Address. . . . . : 00-03-FF-81-79-85
Dhcp Enabled. . . . . : No
IP Address. . . . . : 192.168.16.201
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.16.2
DNS Servers . . . . . : 192.168.16.2
```

C:\Documents and Settings\Administrator>

Stacje robocze powinny być skonfigurowane w taki sposób, aby nie korzystały z żadnych innych serwerów DNS poza serwerem SBS. Jeżeli dla stacji roboczej trzeba ustawić adres zapasowego serwera DNS, adres IP serwera SBS musi być wymieniony jako pierwszy.

Najlepsze praktyki: `ipconfig /all`

Za każdym razem gdy serwer lub stacja robocza mają kłopoty z komunikacją, pierwszym krokiem przy identyfikacji problemu jest wykonanie polecenia `ipconfig /all`. Jeżeli wyślesz opis problemu na listę dyskusyjną SBS lub zadzwonisz pod numer pomocy technicznej Microsoft PSS, najprawdopodobniej niemal od razu zostaniesz poproszony o dostarczenie wyniku działania tego polecenia zarówno na serwerze, jak i na stacji roboczej.

Aby przygotować wynik działania polecenia `ipconfig /all` do wysłania na listę dyskusyjną lub do obsługi technicznej, należy zapisać go do pliku. Najłatwiejszym sposobem wykonania tej operacji jest wpisanie w wierszu polecenia:

```
ipconfig /all > ipconfig.txt
```

Spowoduje to utworzenie w bieżącym katalogu pliku *ipconfig.txt*. Plik ten można otworzyć w Notatniku. Aby szybko go utworzyć i od razu otworzyć, w wierszu poleceń można wpisać:

```
ipconfig /all > ipconfig.txt && ipconfig.txt
```

Polecenie to powoduje utworzenie pliku *ipconfig.txt* w bieżącym katalogu i jego otwarcie w Notatniku.

Konfiguracja DNS do rozpoznawania publicznych adresów internetowych

W jaki sposób usługa DNS może zapewniać rozpoznawanie nazw w publicznym internecie, jeżeli adresy serwera DNS dla obu kart sieciowych wskazują na serwer SBS? Aby skonfigurować jej prawidłowe działanie, musimy ponownie skorzystać z konsoli *Zarządzanie systemem DNS*.

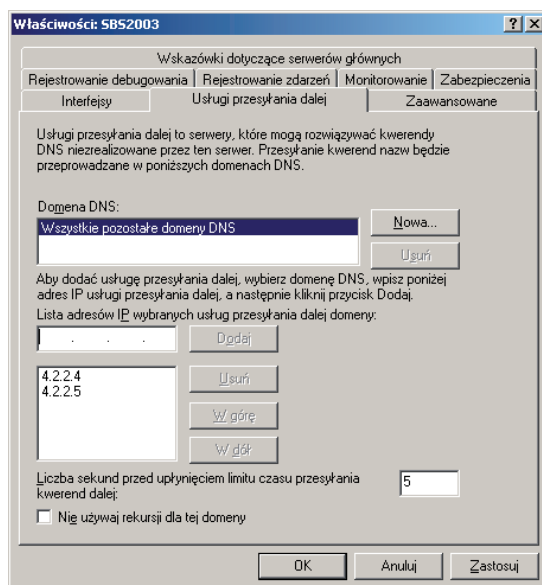
Wykorzystanie usługi przesyłania dalej serwera DNS w konsoli Zarządzanie systemem DNS

Po otwarciu konsoli *Zarządzanie systemem DNS* należy kliknąć prawym przyciskiem myszy nazwę serwera i z menu kontekstowego wybrać *Właściwości*, a następnie kliknąć zakładkę *Usługi przesyłania dalej*. Otwarte zostanie wówczas okno dialogowe pokazane na

rysunku 5.3. Lista domen DNS powinna zawierać jedną pozycję: *Wszystkie pozostałe domeny DNS*. Pole *Lista adresów IP wybranych usług przesyłania dalej domeny* powinno zawierać adresy IP serwerów DNS dostawcy internetu. Konfiguracja ta powinna być ustawiona po uruchomieniu na serwerze kreatora *Połącz z Internetem*.

Rysunek 5.3.

Konsola Zarządzanie serwerem DNS zawiera adresy usług przesyłania dalej



Zgodnie z opisem zawartym we wcześniejszej części tego rozdziału, jeżeli usługa DNS otrzyma żądanie dla adresu, który nie odpowiada jej konfiguracji, na początku szuka go w wewnętrznym buforze DNS. Jeżeli adres nie zostanie znaleziony, serwer DNS kontaktuje się z pierwszym adresem IP wymienionym w części *Usługi przesyłania dalej* i żąda odczytania go z tego serwera. Zalecane jest dodanie drugiego adresu IP serwera DNS, ponieważ będzie on wykorzystywany, jeżeli z jakiegoś powodu nie będzie możliwe skontaktowanie się z pierwszym serwerem.

Wykorzystanie wskazówek dotyczących serwerów głównych w konsoli Zarządzanie systemem DNS

Możliwość wykorzystania serwerów DNS udostępnianych przez dostawcę internetu zmniejsza obciążenie naszego serwera DNS. Gdy serwer DNS nie może znaleźć adresu w lokalnej tabeli lub lokalnym buforze, odpytuje serwer DNS dostawcy i pozwala, aby cała operacja wyszukania adresu została wykonana przez ten serwer.

Jednak usługa serwera DNS nie musi korzystać z zewnętrznych usług przesyłania dalej. Może natomiast skorzystać ze wskazówek dotyczących serwerów głównych i samodzielnie obsłużyć wszystkie operacje wyszukiwania, a nie przekazywać je do usług przesyłania dalej. Jeżeli na zakładce *Usługi przekazywania dalej* konsoli *Zarządzanie systemem DNS* nie zostaną wymienione żadne adresy IP, serwer DNS będzie odpytywał serwery wskazówek głównych wymienione w zakładce *Wskaźniki dotyczące serwerów głównych* okna właściwości. Te wskazówki serwerów głównych zawierają adresy innych serwerów DNS,

które udostępniają informacje o obsługiwanych przez siebie adresach. Gdy zapytanie DNS dotyczące adresu w publicznym internecie dochodzi do serwera DNS w SBS, usługa DNS na początku „odpytuje” główne serwery wskazówek o adres serwera DNS, który pozwoli na odczytanie adresu związanego z nazwą; następnie wysyła do tego serwera zapytanie w celu pobrania faktycznego adresu i odesłania go do klienta.

Najlepsze praktyki: Usługi przesyłania dalej czy wskazówki głównych serwerów

W społeczności SBS najczęściej spotykana jest opinia, że lepiej korzystać z usług przesyłania dalej do zewnętrznych wyszukiwań DNS. Pozwala to odciążyć serwer DNS w SBS od wykonywania wyszukiwań DNS w internecie. Gdy serwer SBS wykonuje zapytanie DNS dla witryny internetowej z wykorzystaniem usług przesyłania dalej, usługa DNS serwera SBS wykonuje tylko jedno wywołanie DNS i czeka na otrzymanie adresu IP od serwera zdefiniowanego w usługach przekazywania dalej.

Niektóre małe firmy zauważyły, że ich dostawcy internetu nie zapewniają niezawodnych serwerów DNS. Przez skonfigurowanie serwera SBS w taki sposób, aby korzystał ze wskazówek serwerów głównych, usługa DNS w SBS wykonuje wyszukiwanie samodzielnie, przez co wyszukanie adresu IP może wymagać wykonania kilku zapytań. Jednak wskazówki głównych serwerów są znacznie bardziej niezawodne niż serwery DNS dostawców internetu.

Jako generalną zasadę należy przyjąć, że serwer SBS powinien mieć skonfigurowane usługi przesyłania dalej DNS. Jednak w przypadkach gdy serwery DNS dostawcy internetu nie są wystarczająco niezawodne, jako akceptowalną alternatywę można przyjąć skonfigurowanie wskazówek głównych serwerów.

Niedawno pojawiły się raporty zabezpieczeń informujące o ataku *DNS poisoning* oraz problemach, jakie mogą wystąpić przy wykorzystaniu przekazywania dalej. Przedstawiając zagadnienie w skrócie, atak *DNS poisoning* (zatrutowanie DNS) polega na zastępowaniu adresu IP w rekordzie DNS innym, fałszywym adresem. W efekcie komunikacja z określoną witryną jest przekierowana do innej lokalizacji, zazwyczaj w niewłaściwych celach. Poza zapewnieniem, że dostawca internetu korzysta z „załatanych” i aktualnych serwerów DNS, jedynym rozwiązaniem jest wyłączenie usług przesyłania dalej i wykorzystywanie wskazówek serwerów głównych. Na razie społeczność SBS nadal zaleca korzystanie z usług przesyłania dalej, ale zauważa zagrożenie atakiem zatrutowania DNS i przyjmuje korzystanie ze wskazówek głównych serwerów jako akceptowalną alternatywę.

Konfiguracja DHCP dla sieci wewnętrznej

Każdy, kto kiedykolwiek pracował w dużym środowisku sieciowym, powinien znać i doceniać wartość DHCP (ang. *Dynamic Host Configuration Protocol*) przy dynamicznym przydzielaniu adresów IP i innych ustawień sieciowych. Choć zalety zastosowania DHCP w małej sieci mogą nie być widoczne natychmiast, technologia ta jest niemal wymagana w świecie SBS. W tym podrozdziale przedstawiony zostanie przegląd DHCP oraz sposób jego zastosowania w SBS 2003.

Co to jest DHCP

Protokół DHCP, zdefiniowany w RFC 1541 (www.ietf.org/rfc/rfc1541.txt) oraz RFC 2131 (www.ietf.org/rfc/rfc2131.txt), jest sposobem pobierania danych dotyczących ustawień sieci przez komputery do niej dołączone. W pierwszych latach stosowania sieci TCP/IP każda stacja robocza i serwer miały przydzielony statyczny adres IP i gdy zmieniał się schemat adresowania IP, musiały one mieć ręcznie zmienianą konfigurację. Dodatkowo

komputery przenośne podłączane do sieci w różnych miejscach musiały mieć zmienianą konfigurację przy każdej zmianie lokalizacji.

Aby zautomatyzować przydzielanie danych IP klientom sieci, został opracowany protokół BOOTP, który dopasowywał adres MAC karty sieciowej do adresu IP. Podczas inicjalizacji karty sieciowej stacja robocza wysyła pakiet broadcast zawierający jej adres MAC, który jest kierowany do serwera BOOTP. Serwer BOOTP odbiera żądanie, szuka w wewnętrznej bazie danych odebranego adresu MAC i zwraca klientowi dane konfiguracyjne, dzięki czemu klient może kontynuować podłączanie się do sieci.

Wykorzystanie BOOTP wymagało jednak znacznego nakładu pracy na jego utrzymanie, ponieważ za każdym razem, gdy została dodana nowa stacja robocza, jej dane musiały być dodawane do bazy danych BOOTP. To samo dotyczyło przypadków, w których została wymieniona karta sieciowa komputera.

Protokół DHCP został opracowany na podstawie BOOTP, ale nie zawiera ograniczeń swojego „poprzednika”. Adresy MAC stacji roboczych nie muszą być zapisywane w bazie danych serwera DHCP, co znacznie ogranicza zakres obowiązków administratora.

DHCP zapewnia więcej funkcji niż tylko dostarczanie adresu IP stacjom roboczym w sieci. Za jego pomocą można w nich skonfigurować wiele ustawień sieciowych. W tabeli 5.1 wymienione zostały ustawienia, jakie mogą być przekazywane do stacji roboczej z serwera DHCP firmy Microsoft.

Tabela 5.1. *Niektóre ustawienia sieciowe konfigurowane za pomocą serwera DHCP firmy Microsoft*

Ustawienie	Opis
Router	Ustawienie bramy domyślnej.
Serwer czasu	Ustawienie adresu serwera czasu.
Serwery DNS	Ustawienie adresów serwerów DNS.
Nazwa hosta	Ustawia nazwę hosta dla bieżącego klienta.
Nazwa domeny DNS	Ustawia domyślną nazwę domeny DNS dla klienta.
Nazwa domeny NIS	Ustawia domyślną nazwę domeny Network Information Service.
Serwery NIS	Ustawienie adresów serwerów NIS.
Serwery NTP	Ustawia adresy serwerów Network Time Protocol.
Serwery WINS/NBNS	Ustawia adresy serwerów WINS oraz NBNS.
Serwery SMTP	Ustawia adresy dostępnych serwerów Simple Mail Transport Protocol.
Serwery POP3	Ustawia adresy dostępnych serwerów Post Office Protocol.
Serwery NNTP	Ustawia adresy dostępnych serwerów Network News Transport Protocol.

Protokół DHCP może być również wykorzystywany do przydzielania stacjom roboczym tych samych adresów IP za każdym żądaniem. Jest to funkcja podobna do BOOTP, ponieważ rezerwacja adresów jest realizowana poprzez połączenie adresu MAC karty sieciowej stacji roboczej z adresem IP. W efekcie stacja robocza otrzymuje „statyczny” adres IP w sieci. Jest to przydatne w przypadku drukarek sieciowych i innych urządzeń, które muszą posiadać stałe adresy, a jednocześnie uwalnia nas od konieczności ręcznego konfigurowania tych urządzeń.

Domyślne ustawienia DHCP w SBS

Początkowa konfiguracja serwera SBS tworzy we wszystkich instalacjach specyficzną konfigurację DHCP. W tabeli 5.2 wymienione są elementy DHCP konfigurowane przez program instalacyjny SBS oraz ich domyślne wartości.

Tabela 5.2. Domyślne ustawienia DHCP konfigurowane przez program instalacyjny SBS

Obszar zawartości	Konfiguracja	Domyślne ustawienie
Właściwości zakresu	Nazwa zakresu	Zakres SBS
Właściwości zakresu	Czas trwania dzierżawy	8 dni
Pula adresów	Zakres adresów	192.168.x.1 – 192.168.x.254
Pula adresów	Adresy wykluczone	192.168.x.1 – 192.168.x.9
Opcje zakresu	Router	Wewnętrzny adres IP SBS
Opcje zakresu	Serwer DNS	Wewnętrzny adres IP SBS
Opcje zakresu	Nazwa domeny DNS	Nazwa wewnętrznej domeny
Opcje zakresu	Serwery WINS/NBNS	Wewnętrzny adres IP SBS
Opcje zakresu	Typ węzła WINS/NBT	0x8

Zgodnie z najlepszymi praktykami konfiguracji sieci, serwer DHCP przydziela klientom prawidłowe adresy IP, przekazuje stacjom roboczym adresy IP dla serwerów DNS oraz WINS, a także prawidłową nazwę wewnętrznej domeny. Zakres DHCP ma wyłączone pierwsze 10 adresów na potrzeby komputerów, które wymagają stosowania statycznych adresów IP takich jak wewnętrzna karta sieciowa serwera.

Oprócz tego, że ustawienia te wykorzystuje się w czasie instalacji, służą one również kreatorowi *Change IP Address Wizard*. Uruchomienie tego kreatora jest najprostszym sposobem na przebudowanie uszkodzonej konfiguracji DHCP na serwerze.

Najlepsze praktyki: Niech SBS udostępnia usługi DHCP

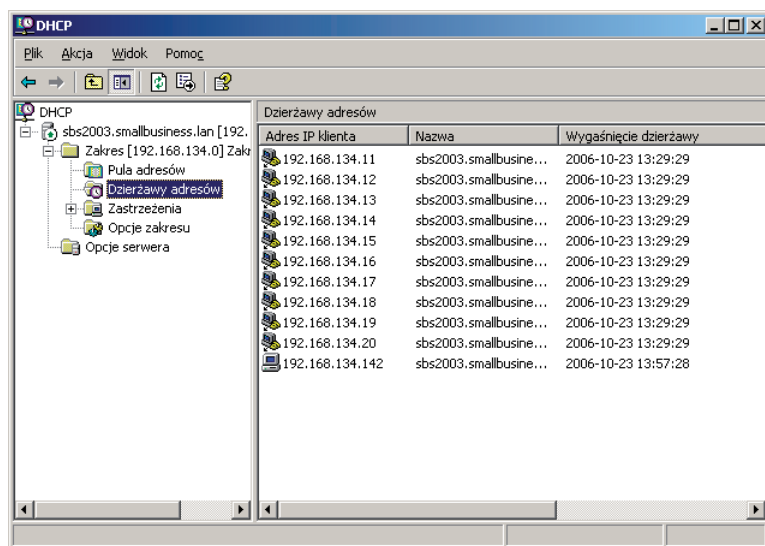
Gdy wiele urządzeń w sieci może udostępniać usługę DHCP dla stacji roboczych, w takim przypadku właśnie serwer SBS powinien być wykorzystywany do zapewnienia usług DHCP. Usługa DHCP w SBS ma wstępnie skonfigurowane ustawienia potrzebne stacjom roboczym do tego, aby podłączyć się do sieci SBS. Nawet jeżeli serwer DHCP innej firmy może udostępniać wszystkie te ustawienia (niektóre nie obsługują wszystkich ustawień DHCP), to przy zmianie konfiguracji sieci SBS aktualizuje potrzebne ustawienia DHCP, natomiast produkty innych firm wymagają ręcznej zmiany konfiguracji.

Modyfikowanie ustawień DHCP

Dla większości środowisk domyślne ustawienia DHCP skonfigurowane przez kreatory SBS są wystarczające do obsłużenia stacji roboczych. Czasami mogą się jednak zdarzyć sytuacje, w których specyficzne wymagania sieciowe wymuszają wprowadzenie w nich zmian. Domyślne ustawienia DHCP powinny być zmieniane tylko w takich właśnie przypadkach.

Ustawienia DHCP można zmienić za pomocą konsoli DHCP, którą uruchamia się poprzez wybranie *Start/Narzędzia administracyjne/DHCP* lub wpisanie `dhcpcmgmt.msc` w wierszu poleceń albo po wybraniu *Start/Uruchom*. W konsoli tej można również przeglądać bieżące dzierżawy DHCP, co zostało pokazane na rysunku 5.4.

Rysunek 5.4.
Konsola DHCP
z bieżącymi
dzierżawami
adresów IP



Tworzenie dodatkowych zastrzeżeń adresów

Jedną z często spotykanych modyfikacji domyślnych ustawień DHCP jest rozszerzenie zakresu zastrzeżonych adresów. Można to zrobić, jeżeli w sieci lokalnej potrzeba więcej niż dziesięciu adresów statycznych. Aby zrealizować to zadanie, można albo utworzyć dodatkowy zakres zastrzeżenia, albo usunąć już istniejący i utworzyć nowy.



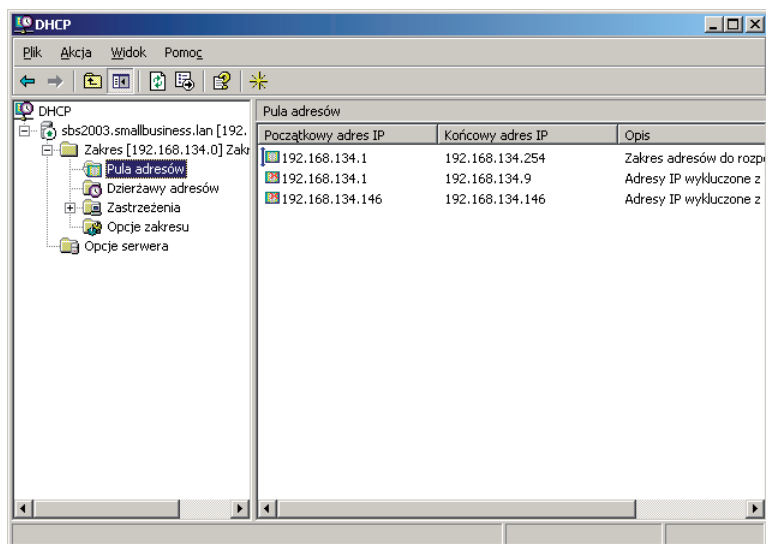
Modyfikując zakres zastrzeżeń adresów DHCP, należy pamiętać, aby zastrzec również adres wewnętrznej karty sieciowej SBS.

Aby dodać kolejny zakres zastrzeżenia do puli adresów DHCP, należy:

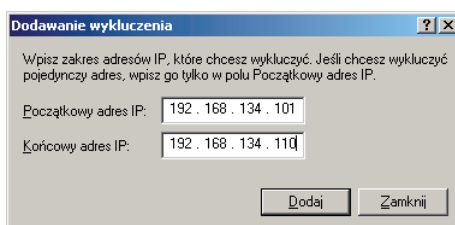
1. Otworzyć konsolę DHCP.
2. Rozwinąć ikonę serwera.
3. Rozwinąć folder *Zakres*.
4. Kliknąć folder *Zakres*, aby wyświetlić istniejące zakresy adresów i zastrzeżeń (patrz rysunek 5.5).
5. Kliknąć prawym przyciskiem myszy *Pula adresów* i wybrać z menu *Nowy zakres wykluczenia*.
6. Wprowadzić początkowy i końcowy adres IP z zakresu przeznaczonego do wykluczenia (patrz rysunek 5.6).
7. Kliknąć *Dodaj*, a następnie *Zamknij*.

Rysunek 5.5.

Zdefiniowane w puli adresów DHCP zakresy adresów i zastrzeżeń

**Rysunek 5.6.**

Określanie początkowego i końcowego adresu IP do wykluczenia z zakresu DHCP



Wszystkie nowe żądania przetwarzane przez serwer nie będą otrzymywały adresów IP we właśnie dodanym wykluczonym zakresie. Wszystkie dzierżawy adresów, które istniały jeszcze przed utworzeniem nowego zakresu, nie będą modyfikowane aż do momentu, gdy stacja robocza będzie próbowała odnowić dzierżawę dla danego adresu.

Tworzenie zastrzeżeń adresów DHCP

Inną często spotykaną modyfikacją domyślnych ustawień DHCP jest dodawanie zastrzeżeń adresów DHCP dla określonego urządzenia. Może być to zrealizowane, gdy urządzenie sieciowe pobiera swoją konfigurację z DHCP, ale musi mieć ono ten sam adres IP przy każdym połączeniu do sieci. Aby zarezerwować adres dla określonego urządzenia, będziemy potrzebować adresu MAC jego karty sieciowej. Żeby dodać nowe zastrzeżenie do konfiguracji DHCP, należy wykonać następujące operacje:

1. Otworzyć konsolę DHCP.
2. Rozwinąć ikonę serwera.
3. Rozwinąć folder *Zakres*.
4. Kliknąć folder *Zastrzeżenia*, aby wyświetlić wszystkie istniejące zastrzeżenia.
5. Kliknąć prawym przyciskiem myszy *Zastrzeżenia* i wybrać z menu *Nowe zastrzeżenie*.

6. Do pól *Nazwa zastrzeżenia*, *Adres IP*, *Adres MAC* oraz *Opis* wpisać odpowiednie dane (patrz rysunek 5.7).

Rysunek 5.7.

Ustawienia nowego zastrzeżenia wprowadzone w konsoli zarządzania DHCP

7. Zaznaczyć przycisk opcji *Tylko DHCP*. Jeżeli w sieci jest wykorzystywany protokół BOOTP, należy wybrać przycisk *Oba* lub *Tylko BOOTP*.

8. Kliknąć *Dodaj*, a następnie *Zamknij*.

Przy następnym żądaniu nowego adresu DHCP przez to urządzenie lub przy odnowieniu dzierżawy DHCP zostanie przydzielony adres podany przy definiowaniu zastrzeżenia.

Wyszukiwanie adresu MAC

W przypadku stacji roboczych Windows adres MAC można odczytać poprzez uruchomienie `ipconfig /all` w wierszu poleceń. Jeżeli urządzenie jest dołączone do sieci i wiemy, że adres IP został odczytany z DHCP, można uruchomić polecenie `arp -a` i odczytać jego adres MAC. Wynik działania tego polecenia będzie podobny do następującego:

```
C:\> arp a
Interfejs: 192.168.16.2 --- 0x10003
Adres internetowy    Adres fizyczny    Typ
192.168.16.20       00-03-ff-8f-79-85    dynamicznie
```

Rozwiązywanie problemów z usługami DNS, DHCP oraz Active Directory

Z powodu wzajemnej zależności usług Active Directory oraz DNS może wydawać się początkowo, iż wiele z problemów z DNS dotyczy Active Directory. W pozostałej części rozdziału przedstawimy kilka często spotykanych problemów oraz sposoby ich rozwiązywania.

Rozwiązywanie problemów z wewnętrznym wyszukiwaniem w DNS

Większość często spotykanych problemów z wewnętrzną siecią występuje, gdy serwer lub stacja robocza nie mają prawidłowo skonfigurowanego serwera DNS. Przedstawione poniżej dwa przykłady opisują dany problem oraz przyczynę jego wystąpienia.

Serwer zawiesza się przy stosowaniu ustawień sieciowych

Jeżeli serwer SBS uruchamia się bardzo długo, a dokładniej — wiesza się na dwadzieścia minut lub dłużej w czasie przygotowywania połączeń sieciowych, to niemal zawsze jest to spowodowane tym, że w danych karty sieciowej skonfigurowany jest zewnętrzny serwer DNS. Wynik działania polecenia `ipconfig /all` na serwerze z podobnym problemem może wyglądać następująco:

```
C:\Documents and Settings\Administrator>ipconfig /all
```

Windows IP Configuration

```
Host Name . . . . . : sbs
Primary Dns Suffix . . . . . : SmallBizCo.local
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : Yes
WINS Proxy Enabled. . . . . : Yes
DNS Suffix Search List. . . . . : SmallBizCo.local
```

Ethernet adapter Server Local Area Connection:

```
Connection-specific DNS Suffix . : 
Description . . . . . : 3Com 3C920 Integrated Fast Ethernet Controller
(3C905C-TX Compatible)
Physical Address. . . . . : 00-08-74-40-5B-61
DHCP Enabled. . . . . : No
IP Address. . . . . : 192.168.16.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 
DNS Servers . . . . . : 192.168.16.2
Primary WINS Server . . . . . : 192.168.16.2
```

Ethernet adapter Network Connection:

```
Connection-specific DNS Suffix . : 
Description . . . . . : Realtek RTL8029(AS) PCI Ethernet Adapter
Physical Address. . . . . : 00-C0-F0-2B-7D-F9
DHCP Enabled. . . . . : No
IP Address. . . . . : 10.10.1.9
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.10.1.1
DNS Servers . . . . . : 4.2.2.4
                        4.2.2.3
Primary WINS Server . . . . . : 192.168.16.2
NetBIOS over Tcpip. . . . . : Disabled
```

W takim przypadku, gdy w czasie uruchamiania serwer wchodzi w fazę *Przygotowanie połączeń sieciowych*, próbuje zarejestrować wszystkie dane z Active Directory na serwerze (lub serwerach) DNS skonfigurowanym dla karty sieciowej. Najczęściej serwer DNS udostępniany przez dostawcę internetu nie akceptuje rejestracji DNS i na pewno nie rozpoznaje nieroutowalnych przyrostków DNS. Gdy więc dochodzi do próby rejestrowania danych DNS na zdalnym serwerze, nie będzie on odpowiadał i w końcu zostanie przekroczony czas oczekiwania. Niestety, procedury rozruchowe usługi Active Directory są „wytrwale” i wykonują wiele takich prób, aż w końcu je przerywają. Proces ten może trwać dwadzieścia minut lub dłużej, w zależności od liczby zewnętrznych serwerów DNS skonfigurowanych dla każdej karty.

Dzieje się tak również, gdy adres wewnętrznej karty sieciowej jest skonfigurowany jako adres serwera DNS dla obu kart, ale jedna z kart ma skonfigurowany zewnętrzny serwer DNS. Proces rejestracji Active Directory w DNS udaje się dla wewnętrznego serwera DNS, a próbuje rejestrować dane usługi Active Directory we wszystkich serwerach DNS wymienionych w konfiguracji kart. Jedynym sposobem na uniknięcie tej sytuacji jest skonfigurowanie adresu wewnętrznej karty sieciowej jako **jedynego** adresu serwera DNS — dla każdej z kart sieciowych w serwerze.

Kreator konfiguracji sieci nie może znaleźć użytkowników i komputerów

Inny częsty błąd występuje przy próbie dołączenia stacji roboczej do domeny SBS z wykorzystaniem kreatora konfiguracji sieci. Po uruchomieniu kreatora z przeglądarki WWW generowany jest błąd: „Nie można znaleźć listy użytkowników i komputerów na serwerze. Upewnij się, że karty sieciowe SBS są prawidłowo skonfigurowane”. Pojawia się on dlatego, że stacja robocza klienta nie jest prawidłowo skonfigurowana, a nie dlatego, że problem tkwi w konfiguracji serwera, jak sugeruje komunikat. Microsoft przedstawił wyjaśnienie tego błędu w artykule KB nr 837369 (<http://support.microsoft.com/?id=837369>). Zostało tam wskazane, iż problem wynika ze skonfigurowania na stacji roboczej adresu serwera DNS, który nie jest wewnętrznym adresem IP serwera. I tym razem problem można rozwiązać poprzez zmodyfikowanie ustawień sieci na stacji roboczej, tak aby jedynym serwerem DNS był serwer SBS.

Użycie programu nslookup do wyszukiwania wewnętrznych nazw DNS

Czasami można spotkać się z sytuacją, gdy rozpoznawanie nazw w wewnętrznym serwerze DNS działa nieprawidłowo, ale nie można znaleźć oczywistego powodu. Zwykle użytkownicy raportują, że po otwarciu przeglądarki nie ładuje się witryna Companyweb i generowany jest błąd *Nie można wyświetlić strony*. Zdarza się, że nagle nie można otworzyć udziału z innego serwera lub stacji roboczej znajdującej się w sieci lokalnej. Jeżeli problem dotyczy jednego komputera lub niewielkiej grupy komputerów, mało prawdopodobne jest, aby był związany z serwerem SBS, więc próba jego zlokalizowania powinna się zacząć od stacji roboczej.

Najlepszym narzędziem do lokalizowania problemów klientów z DNS jest program *nslookup*. Jest on instalowany domyślnie w każdym systemie Windows 2000, Windows XP oraz Windows 2003. Podczas szukania przyczyny problemów będziemy korzystać z programu *nslookup* w trybie interaktywnym, który jest uruchamiany po wpisaniu w wierszu poleceń *nslookup*. W trybie interaktywnym wyświetlany jest znak zachęty *>*, po którym można wprowadzać kolejne polecenia. Aby zakończyć działanie programu, po znaku zachęty należy wpisać polecenie *exit*.

Aby natomiast sprawdzić wyszukiwanie w DNS dla lokalnego systemu, po znaku zachęty programu *nslookup* trzeba wpisać nazwę bieżącego komputera. Jeżeli zostanie już ona wprowadzona (w poniższym przykładzie to *jimdough01*), powinny wyświetlić się wyniki podobne do zamieszczonych poniżej.

```
C:\>nslookup
Default Server: sbs.smallbizco.local
Address: 192.168.16.2

> jimdough01
Server: sbs.smallbizco.local
Address: 192.168.16.2

Name: jimdough01.SmallBizCo.local
Address: 192.168.16.25
```

Gdy *nslookup* przechodzi na tryb interaktywny, wyświetla nazwę i adres IP domyślnego serwera DNS wykorzystywanego przez klienta. W poprzednim przykładzie stacja robocza ma skonfigurowany jako DNS lokalny serwer SBS, co jest prawidłowym ustawieniem. Jeżeli zostanie wyświetlony inny serwer, od razu widać, że domyślny serwer DNS dla stacji jest nieprawidłowo ustawiony, co najprawdopodobniej powoduje problem. W tym przykładzie stacja robocza jest w stanie wyszukać nazwę *jimdough01* i uzyskać adres IP tego komputera.



Jeżeli nie są prawidłowo skonfigurowane strefy przeszukiwania wstecznego, na początku programu *nslookup* wyświetla następujący komunikat:

```
*** Can't find server name for address 192.168.16.2: Non-existent domain
Default Server: Unknown
Address: 192.168.16.2
```

Jeżeli zobaczymy taką odpowiedź, nie będą jednak występowały problemy z wyszukiwaniem w serwerze DNS. Ten problem można rozwiązać poprzez utworzenie strefy przeszukiwania wstecznego dla wewnętrznej sieci i dodanie rekordu wskaźnika (PTR) dla serwera SBS w tej strefie.

Gdy program *nslookup* wyszukuje nazwę systemu, który nie znajduje się w tabeli DNS na serwerze SBS, generuje odpowiedź podobną do przedstawionej poniżej. W takim przypadku należy przejrzeć wpisy w strefie przekazywania do przodu dla domeny *smallbizco.local* i sprawdzić, czy znajduje się tam pozycja dla *companyweb*. W poniższym przykładzie nie ma odpowiedniego wpisu:

```
> companyweb
Server: sbs.smallbizco.local
Address: 192.168.16.2

*** sbs.smallbizco.local can't find companyweb: Non-existent domain
```

W kolejnym przykładzie program *nslookup* odczytuje z serwera DNS adres dla *companyweb*:

```
> companyweb
Server: sbs.smallbizco.local
Address: 192.168.16.2

Name: companyweb.SmallBizCo.local
Address: 192.168.16.8
```

Jednak zwracany adres nie jest taki sam jak adres serwera SBS. W takim przypadku wiemy już, że brak możliwości załadowania witryny *companyweb* do przeglądarki internetowej na stacji roboczej jest spowodowany tym, iż rekord DNS wskazuje na niewłaściwy adres.

Jak widać na tych kilku przykładach, program *nslookup* może dostarczyć dosyć dużo danych na temat sieci lokalnej, korzystając tylko z kilku poleceń. W następnym punkcie nieco dokładniej przedstawimy użycie programu *nslookup* do rozwiązywania problemów z serwerem DNS w zewnętrznej sieci.

Gdy adres <http://Companyweb> jest przekształcany na www.companyweb.com

Wiele nowoczesnych przeglądarek posiada wewnętrzne procedury pozwalające na odszukanie witryn po wprowadzeniu w pasku adresu tylko jednego słowa. Na początku przeglądarka szuka nazwy *companyweb* w lokalnej domenie. Jeżeli witryna ta nie zostanie znaleziona, przeglądarka zaczyna „zgadywać”, jaką witrynę mamy na myśli, zaczynając od *.com*, poprzez *.net*, *.org* itd. Jeżeli więc w przeglądarce użyjemy adresu <http://companyweb> i w lokalnej domenie nie będzie ona mogła znaleźć komputera o nazwie *companyweb*, spróbuje załadować www.companyweb.com.

Ostatnio działanie takie zostało zauważone w firmie z dużą liczbą użytkowników komputerów Macintosh. Po zainstalowaniu serwera SBS i dołączeniu wszystkich komputerów PC do domeny za pomocą kreatora konfiguracji sieci domyślna strona komputera została ustawiona na <http://companyweb>. Aby zachować spójność na wszystkich platformach, pracownik IT w firmie ustawił domyślną stronę domową na komputerach Macintosh również na <http://companyweb>. Niestety, po otwarciu przeglądarki na komputerze Mac wykonywana była próba otwarcia witryny <http://www.companyweb.com>.

Pracownik IT wykorzystał program *nslookup* dla stacji roboczych Macintosh do zlokalizowania problemów z DNS i pomimo tego że interfejs był nieco inny niż na komputerach PC, był w stanie stwierdzić, że Mac nie korzysta z serwera SBS jako podstawowego serwera DNS. Po pewnym czasie zauważył, że komputery Macintosh nie pobierały adresu IP z serwera DHCP, jak wcześniej myślał. Po wprowadzeniu odpowiedniej zmiany strona zaczęła otwierać się tak, jak tego oczekiwano. (Więcej informacji na temat problemów z połączeniem z SBS w komputerach Macintosh znajduje się w rozdziale 17., „Integracja komputerów Macintosh ze środowiskiem Small Business Server 2003”).

Niektóre nowe przeglądarki nie korzystają z tej metody i nie „zgadują”, co użytkownik miał na myśli, wprowadzając dane słowo. Zamiast tego, gdy dana nazwa nie zostanie znaleziona w lokalnej domenie, przeglądarka przesyła to słowo do wyszukiwarki lub od razu otwierana jest strona znajdująca się na pierwszym miejscu w wynikach wyszukiwania. Aby sprawdzić, jak to działa, możemy w przeglądarce Firefox wpisać <http://companyweb>, gdy serwerem DNS dla stacji roboczej jest serwer publiczny. Strona, jaka się wówczas pokazuje, jest artykułem w Microsoft KB dotyczącym przywracania witryny *Companyweb* po usunięciu komponentu Intranet z SBS.

Rozwiązywanie problemów z zewnętrznym wyszukiwaniem w DNS

Administratorzy systemów szybko dowiadują się o problemach z połączeniem internetowym w firmie. Użytkownicy zwykle bardzo szybko reagują, jeśli nie mogą otworzyć określonej witryny; często dzwonią po pomoc, twierdząc, że „internet jest wyłączony!”, zamiast powiedzieć: „Mam problemy z otwarciem tej witryny, choć pozostałe działają bez problemów”. Zatem pierwszym krokiem przy rozwiązywaniu problemów z DNS dla internetu jest zadanie kilku pytań pomagających określić zasięg problemu.

Określone witryny mają przejściowe problemy z połączeniem

Przejściowe problemy są często bardzo trudne do zdiagnozowania, ponieważ nie zawsze występują lub objawiają się nie zawsze w taki sam sposób. Gdy użytkownik narzeka, że niektóre witryny czasami działają, a czasami nie, a problem jest związany z określonym podzbiorem witryn i pozostałe działają bez zarzutu, na początek należy sprawdzić, czy źródłem problemów nie jest EDNS.

EDNS, czyli *Extended DNS*, to rozszerzony proces odpytywania DNS, który jest domyślnie implementowany w Windows Server 2003. Specyfikacja EDNS pozwala na stosowanie większej liczby odpowiedzi DNS w porównaniu do standardowego DNS i ta większa liczba odpowiedzi może powodować niektóre problemy związane z konfiguracją.

Aby wyłączyć EDNS na serwerze i wyczyścić pamięć podręczną DNS, należy wpisać w wierszu polecenia:

```
dnscmd /Config /EnableEdnsProbes 0  
ipconfig /flushdns
```

Pierwsze polecenie informuje serwer, że powinien wysyłać standardowe zapytania DNS zamiast zapytań rozszerzonych. Drugie natomiast powoduje wyczyszczenie lokalnej pamięci podręcznej na serwerze SBS i wymusza nowe wyszukiwanie w przypadku wszystkich żądań DNS. Ta zmiana powinna rozwiązać przejściowe problemy przy połączeniach do określonych witryn.

Okresowa utrata połączenia z wszystkimi zewnętrznymi witrynami

Innym problemem z połączeniem internetowym jest okresowa utrata połączenia z wszystkimi zewnętrznymi witrynami. Jeżeli fizyczne połączenie z internetem jest dobre, tzn. można dostać się do serwera SBS z internetu lub odwołać się do witryn za pomocą adresu IP, to następnym krokiem jest przyjrzenie się serwerowi DNS w SBS. Również w tym przypadku pomocny okazuje się program *nslookup*.

Poniżej przedstawiona jest przykładowa sesja programu *nslookup*, w której próbujemy określić, czy problem leży po stronie serwera DNS w SBS:

```
C:\>nslookup  
Default Server: sbs.smallbizco.local  
Address: 192.168.16.2
```

```
> www.google.com
Server: sbs.smallbizco.local
Address: 192.168.16.2

DNS request timed out.
    timeout was 2 seconds.
*** Request to sbs.smallbizco.local timed-out
> www.sams.com
Server: sbs.smallbizco.local
Address: 192.168.16.2

DNS request timed out.
    timeout was 2 seconds.
*** Request to sbs.smallbizco.local timed-out
> companyweb
Server: sbs.smallbizco.local
Address: 192.168.16.2

Name: sbs.Smallbizco.local
Address: 192.168.16.2
Aliases: companyweb.Smallbizco.local
```

Po uruchomieniu programu *nslookup* nie powiodło się wykonanie dwóch zapytań dotyczących popularnych witryn. Błąd **** Request to sbs.smallbizco.local timed-out* wydaje się wskazywać na problem z usługą DNS w serwerze SBS. Jednak trzecie zapytanie dotyczące lokalnej nazwy Companyweb zwraca poprawne wyniki, co wskazuje, iż serwer działa prawidłowo. Następnym krokiem jest użycie programu *nslookup* do bezpośredniego wysłania zapytania do serwera lub serwerów wymienionych w sekcji *Usługi przesyłania dalej* w konsoli DNS. Poniżej znajduje się przykładowy zapis takich działań:

```
> server 65.97.168.254
DNS request timed out.
    timeout was 2 seconds.
Default Server: [65.97.168.254]
Address: 65.97.168.254

> www.google.com
Server: [65.97.168.254]
Address: 65.97.168.254

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to [65.97.168.254] timed-out
```

Pierwsze z wymienionych poleceń pozwala zmienić serwer DNS wykorzystywany przez program *nslookup*. W tym przykładzie zobaczymy błąd przekroczenia czasu oczekiwania przy zmianie serwera DNS. Choć taka odpowiedź nie jest niczym niezwykłym, powinien być to sygnał wskazujący na problemy ze zdalnym serwerem DNS. Drugie polecenie to próba wyszukania adresu dobrze znanej witryny. W tym przypadku dwa razy otrzymaliśmy błąd przekroczenia czasu połączenia. Jest to wystarczające potwierdzenie tego, że problem leży po stronie zdalnego serwera DNS.

Jedną z metod, która może być wykorzystana do potwierdzenia problemów z serwerami DNS wymienionymi w sekcji *Usługi przesyłania dalej*, jest wysłanie zapytań do różnych

serwerów DNS. Gdy dostawca internetu zapewnia serwery DNS dla połączeń sieciowych, zwykle dostarcza adresy dwóch serwerów, dzięki czemu jeśli pierwszy będzie niedostępny, drugi posłuży jako serwer zapasowy. Nie wszyscy dostawcy internetu umieszczają jednak swoje serwery w różnych segmentach sieci, dzięki czemu w przypadku awarii jednego segmentu niedostępny stałby się tylko jeden z serwerów — więc w przypadku problemów z połączeniem nie będą dostępne oba serwery. Z tego powodu wielu konsultantów utrzymuje listę alternatywnych serwerów DNS dostępnych do wykorzystania i testowania. Mogą to być serwery DNS dostawców, z usług których korzystali oni wcześniej, lub dobrze znane, publiczne serwery.

Następnym krokiem w procesie rozwiązywania problemów jest testowanie tłumaczenia adresów przez zapasowy serwer zapewniający przez dostawcę internetu. Aby sprawdzić, czy zapasowy serwer działa prawidłowo, można wykonać te same operacje, które zostały przedstawione w poprzednim przykładzie. Jeżeli również ten test zawiedzie, należy spróbować użyć serwerów DNS o adresach 4.2.2.1 oraz 4.2.2.2 (dwóch publicznych serwerów DNS). Serwery te zwykle odpowiadają na żądania wyszukiwania, chyba że problemy z routowaniem uniemożliwiają klientowi kontakt z nimi. Ponieważ odpowiadają one na wywołania ping, polecenie `ping 4.2.2.1` lub `ping 4.2.2.2` pozwala sprawdzić, czy serwery te są osiągalne. Jeżeli odpowiadają one na zapytania DNS, to znaczy, że problemy z wyszukiwaniem występują w serwerach wymienionych jako serwery przekazywania dalej.

Jak wspomnieliśmy we wcześniejszej części rozdziału, serwery DNS w SBS nie muszą mieć ustawionych usług przekazywania dalej. Jeżeli w usługach tych nie zostały wpisane żadne adresy, przy wyszukiwaniu wykorzystywane będą główne serwery wskazówek. Może to stanowić jeszcze jeden test, który może być wykorzystywany do sprawdzenia, czy problem leży po stronie usług przekazywania dalej. Jeżeli po usunięciu usług przekazywania dalej serwer DNS w SBS prawidłowo zaczyna proces wyszukiwania, problem tkwi w usługach przesyłania dalej.

Aby rozwiązać problem nieprawidłowych odpowiedzi na zapytania DNS, należy usunąć usługi przesyłania dalej z konsoli DNS i skorzystać z głównych serwerów wskazówek lub też skonfigurować alternatywne serwery przekazywania dalej. Zmiany te dają natychmiastowy efekt, dzięki czemu nie trzeba restartować usług DNS, ale niezbędne może się okazać wywołanie polecenia `ipconfig /flushdns`, co spowoduje wyczyszczenie nieprawidłowych wyników wyszukiwania DNS z lokalnej pamięci podręcznej.

Rozwiązywanie problemów z DHCP

W systemie SBS od czasu do czasu pojawiają się dwa problemy związane z DHCP. Pierwszym jest nieoczekiwane zatrzymanie usługi DHCP powiązane z wygenerowaniem komunikatu o błędzie w dzienniku zdarzeń. Występuje on niemal zawsze, gdy w wewnętrznej sieci SBS włączony zostanie drugi serwer SBS. Serwer DHCP w SBS wykrywa drugi serwer DHCP i wyłącza się, aby uniknąć konfliktów. Niestety, pozwala to na przejęcie przez wrogi serwer DHCP kontroli nad żądaniami DHCP i przekazywanie klientom nieprawidłowych danych konfiguracyjnych. Problem ten często ujawnia się w sieci, ponieważ nowy serwer DNS nie zapewnia odpowiedniej konfiguracji stacji roboczych. Jednak po dalszym dochodzeniu staje się jasne, że usługa DHCP na serwerze SBS jest wyłączona i nie obsługuje wysyłania konfiguracji.

W przypadku wykrycia innego serwera DHCP w sieci lokalnej serwer SBS zapisuje w dzienniku zdarzeń *System* dwa błędy. Pierwszym z nich jest błąd 1053 pochodzący z *DhcpServer*. Jego opis jest następujący:

Usługa DHCP/BINL, działająca na tym komputerze z systemem Windows Server 2003 for Small Business Server, napotkała w sieci inny serwer o adresie IP [adres IP], należący do domeny:.

Drugim jest błąd 1054, pochodzący również z *DhcpServer*, z opisem:

Usługa DHCP/BINL na tym komputerze zostanie zamknięta. W celu sprawdzenia przyczyn przejrzyj poprzednie komunikaty w dzienniku zdarzeń.

Uwaga

W konfiguracji z dwiema kartami sieciowymi serwer SBS nie będzie informował o aktywnym serwerze DHCP w zewnętrznej sieci. W niektórych przypadkach serwer może być tak skonfigurowany, aby pobierał zewnętrzny adres IP z serwera DHCP. Problemy występują tylko wtedy, gdy zostanie wykryty inny serwer DHCP w wewnętrznej sieci.

Drugą częstą przyczyną błędów jest zmiana adresu IP wewnętrznej sieci bez zastosowania kreatora *Zmień adres IP serwera*. Jeżeli adres IP wewnętrznej karty sieciowej zostanie zmieniony bezpośrednio na karcie sieciowej, nie jest automatycznie aktualizowany zakres DHCP. W takim przypadku po uruchomieniu stacji roboczej nie otrzymuje ona adresu z serwera DHCP i korzysta z adresu Automatic Private IP Address (APIPA), z zakresu 169.254.x.x. Jeśli tak się zdarzy, stacja robocza nie będzie w stanie komunikować się w sieci. Uruchomienie na niej polecenia `ipconfig /all` i porównanie wyniku z wynikiem działania tego samego polecenia uruchomionego na serwerze pozwala wykryć, że stacja robocza oraz serwer są w różnych podsieciach lub że stacja robocza posiada nieprawidłowy adres IP serwera SBS. Sytuacja taka występuje również, gdy adres IP serwera został zmieniony w opisany wcześniej sposób, a stacja robocza od tego czasu nie odnawiała dzierżawy DHCP. Również w takim przypadku zakresy adresów IP na serwerze i w stacji roboczej są inne.

Aby rozwiązać ten problem, można ręcznie zmienić ustawienia serwera DHCP, choć łatwiej jest uruchomić kreator *Zmień adres IP serwera*, który automatycznie przebuduje zakres DHCP. Jednak w czasie pracy tego kreatora nowy zakres SBS będzie miał standardowe ustawienia SBS. Jeżeli więc wcześniej do zakresu były wprowadzane zmiany, zostaną one utracone.

Rozwiązywanie problemów Active Directory związanych z DNS

Problemy z usługą Active Directory często sprowadzają się do błędów konfiguracyjnych DNS lub błędów usługi. O niektórych z nich wspominaliśmy we wcześniejszej części rozdziału (np. ustawienia karty sieciowej wskazujące na zewnętrzny serwer DNS), jednak, jak się okazuje, część z problemów wskazujących na Active Directory wynika z usługi DNS. W ostatnich punktach tego rozdziału przedstawimy kilka sposobów na szybkie rozwiązanie problemów z DNS, które mogą powodować błędy w usłudze Active Directory.

Błędy DNS 4004 i 4015

Jeżeli w dzienniku zdarzeń zostaną zauważone błędy DNS 4004 lub DNS 4015, pierwszym miejscem, w którym należy sprawdzić konfigurację DNS dla Active Directory, jest konsola zarządzania DNS. Należy porównać zawartość pola *Strefa wyszukiwania do przodu* z tym, które zostało przedstawione na rysunku 5.1 we wcześniejszej części rozdziału. Główna strefa wyszukiwania musi zawierać co najmniej cztery następujące rekordy:

(identyczny jak folder nadrzędny)	Adres startowy uwierzytelnienia (SOA)
(identyczny jak folder nadrzędny)	Serwer nazw (NS)
(identyczny jak folder nadrzędny)	Host (A)
<i>Nazwa serwera</i>	Host (A)

Pierwsze dwa rekordy zawierają w polu danych wewnętrzną nazwę serwera (FQDN), natomiast ostatnie dwa adres IP; przykład jest pokazany na rysunku 5.1. Jeżeli brakuje jednego z tych rekordów lub zawierają one nieprawidłowe dane, poprawka może zostać wprowadzona bezpośrednio w konsoli DNS — należy dodać brakujący rekord lub poprawić nieprawidłowe dane.

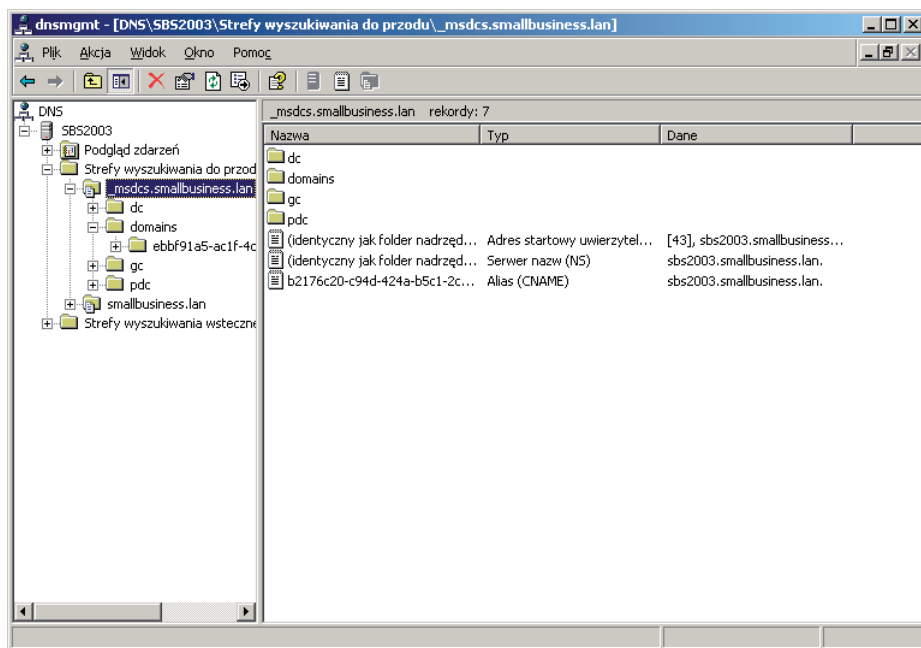
Netlogon

Na rysunku 5.8 pokazano część *Strefy wyszukiwania do przodu* dla Active Directory w konsoli zarządzania DNS. Podobnie jak w przypadku omówionej wcześniej *Strefy wyszukiwania do przodu* dla wewnętrznej domeny, aby usługa Active Directory działała prawidłowo, muszą zostać dla niej skonfigurowane niektóre kluczowe elementy. Na rysunku 5.8 przedstawione są rekordy SOA (Adres startowy uwierzytelnienia) oraz NS (Serwer nazw) dla strefy *_msdcs*, podobnie jak dla domeny wewnętrznej, a oba te rekordy zawierają nazwę FQDN serwera SBS. Strefa *_msdcs* zawiera również rekord aliasu, który wskazuje na nazwę FQDN dla serwera SBS. W strefie *domains* znajduje się też strefa GUID domeny.

Ponieważ usługa DNS korzysta z bazy danych do zapisywania tych informacji, może pojawić się również problem uszkodzenia bazy danych — tak samo jak w przypadku innych systemów. Jednym z sygnałów uszkodzenia bazy danych jest brak rekordu CNAME dla strefy wyszukiwania *_msdcs*. Na szczęście odtwarzanie bazy danych nie jest trudne.

Usługa Netlogon to komponent łączący usługę DNS z Active Directory. Obsługuje ona rekordy DNS dla Active Directory w dwóch plikach zlokalizowanych w katalogu *config* znajdującym się w *system32*. Pliki te to *netlogon.dns* oraz *netlogon.dnb*. Jeżeli nie są one dostępne w momencie uruchomienia procesu Netlogon, zostaną utworzone automatycznie i będą zawierać właściwe informacje DNS dla Active Directory. Jeżeli natomiast są dostępne, ale mają nieprawidłową zawartość, usługa Netlogon zostanie uruchomiona, jednak może działać w nieprawidłowy sposób.

Bazy danych Netlogon można naprawić za pomocą jednego polecenia. Na początek należy zmienić katalog bieżący na *C:\Windows\system32\config*, a następnie wprowadzić następujące polecenie:



Rysunek 5.8. Strefa wyszukiwania do przodu *_msdcs* zawierająca rekordy dla serwera i domen

```
net stop netlogon && del netlogon.* && net start netlogon
```

Powoduje ono zatrzymanie usługi Netlogon, skasowanie plików *netlogon.dnb* oraz *netlogon.dns* z folderu *config* oraz ponowne uruchomienie procesu Netlogon. Jeżeli zajrzymy do folderu *config* po uruchomieniu tego polecenia, zobaczymy, że pliki *netlogon.dns* oraz *netlogon.dnb* zostały odtworzone. Jeśli brakowało rekordu CNAME dla serwera, to po odświeżeniu konsoli DNS można zauważyć, że został on przywrócony. Proces ten odtwarza również strefę *domains* znajdującą się w strefie *_msdcs*.



Jeżeli pliki *netlogon.dns* oraz *netlogon.dnb* nie zostaną odtworzone w folderze *config*, a w dzienniku zdarzeń pojawi się ostrzeżenie (Netlogon 5781), należy sprawdzić, czy ustawienia serwera DNS dla wszystkich kart sieciowych wskazują na wewnętrzny adres IP serwera SBS. Jeżeli wskazują one na dowolne inne miejsce, nie nastąpi prawidłowe utworzenie rekordów w DNS.

netdiag oraz dcdiag

Inny zestaw narzędzi przydatnych przy diagnozowaniu problemów z siecią oraz usługą Active Directory jest dostępny w pakiecie Support Tools. Pakiet ten nie jest instalowany domyślnie, więc aby użyć programów *netdiag* i *dcdiag*, trzeba go zainstalować.

Wyniki działania programów *netdiag* oraz *dcdiag* zajmują kilka stron, aby więc można było wygodnie je przeszukiwać, warto skierować je do pliku. Poniższe polecenia pozwalają na uruchomienie programów *netdiag* oraz *dcdiag* z dokładnym raportowaniem, przekierowanie wyników do pliku oraz otwarcie pliku z wynikami w programie Notatnik.

```
netdiag /v > netdiag.txt && netdiag.txt  
dcdiag /v > dcdiag.txt && dcdiag.txt
```

Po otwarciu pliku z wynikami w Notatniku należy wyszukać w nim słów „fail” oraz „fatal”, co pozwoli szybko zidentyfikować problemy odnalezione przez program diagnostyczny. Jeżeli znajdziemy informacje o problemach, możemy, używając Google’a, dotrzeć do opisu błędów i szybko zlokalizować ich źródło, o ile nie okażą się one oczywiste na podstawie informacji zawartych w pliku.

Uruchomienie `netdiag /fix` pozwala również na przywrócenie plików bazy danych Netlogon. Działanie tego programu jest takie samo jak opisane wcześniej zatrzymanie usługi Netlogon, skasowanie plików bazy danych oraz ponowne uruchomienie usługi.

Najlepsze praktyki: Instalacja pakietu Support Tools

Oprócz wspomnianych wcześniej *netdiag* i *dcdiag* pakiet Support Tools zawiera wiele przydatnych narzędzi diagnostycznych. Plik instalatora pakietu Support Tools, *SUPTOOLS.MSI*, znajduje się na dysku nr 2 instalacji SBS, w folderze `\SUPPORT\TOOLS`. Kliknij dwukrotnie plik instalatora i zaakceptuj wszystkie domyślne ustawienia procesu instalacji, co spowoduje zainstalowanie pakietu w folderze `C:\Program Files\Support Tools` na serwerze SBS.

Warto poświęcić nieco czasu na zapoznanie się z postacią wyników działania programów *netdiag* oraz *dcdiag*. Po pewnym czasie będziesz wiedział, co powinno się znajdować w wynikach, a co nie, oraz jak szybko identyfikować problemy z konfiguracją serwera.

Podsumowanie

W tym rozdziale przedstawione zostały wzajemne relacje pomiędzy usługami DNS, DHCP oraz Active Directory w środowisku SBS. Ponieważ usługi DNS oraz Active Directory są ze sobą tak powiązane, aby możliwa była praca w lokalnej domenie, jak również korzystanie z internetu, ustawienia sieciowe we wszystkich systemach sieci SBS muszą być prawidłowo skonfigurowane. Jeżeli serwer SBS jest prawidłowo skonfigurowany, usługa DHC przekazuje stacjom roboczym niezbędne informacje. Do lokalizacji problemów z wyszukiwaniem DNS w sieci lokalnej i internecie można użyć programu *nslookup*. Usługa Netlogon łączy Active Directory z DNS, a usunięcie baz danych przy restarcie usług pozwala w łatwy sposób usunąć błędy w bazie danych Netlogon. Polecenia *netdiag* oraz *dcdiag* są przydatne przy diagnozowaniu problemów z siecią oraz Active Directory.

Podsumowanie najlepszych praktyk

- ♦ Rekordy DNS — tworząc dodatkowe rekordy dla istniejących komputerów, należy stworzyć je jako rekordy CNAME (aliasy DNS), a nie rekordy A (hosty DNS).
- ♦ `ipconfig /all` — polecenie to jest dobrym punktem wyjścia przy diagnozowaniu problemów z połączeniem w przypadku stacji roboczej lub serwera.

- ♦ Usługi przesyłania dalej w DNS — tam, gdzie to możliwe, należy korzystać z usług przesyłania dalej.
- ♦ Serwery DNS — jeżeli mamy do wyboru serwer SBS lub inne urządzenie służące jako serwer DHCP, należy uruchomić usługę DHCP na serwerze SBS.
- ♦ Pakiet Support Tools — możliwie szybko po zainstalowaniu nowego systemu należy zainstalować również pakiet Support Tools z dysku instalacyjnego nr 2.