

Microsoft®

Vademecum administratora

Internet Information Services (IIS) 7.0

William R. Stanek

Vademecum administratora Internet Information Services (IIS) 7.0
Edycja polska Microsoft Press

Tytuł oryginalny: Internet Information Services (IIS) 7.0 Administrator's Pocket Consultant

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

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

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

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

e-mail: mspress@promise.pl

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

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

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

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

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

ISBN: 978-83-7541-014-3

Przekład: Leszek Biolik,
Andrzej Bańkowski, Dorota Grabowska, Dorota Czubaszek

Redakcja: Marek Włodarz

Korekta: Magdalena Kalina-Swoboda

Skład i łamanie: MAWart

*Mojej żonie i dzieciom za miłość, wsparcie i nadzwyczajne umiejętności znoszenia klikania
mojej klawiatury.*

Spis treści

Podziękowania	xiv
Wprowadzenie	xv
Dla kogo przeznaczona jest ta książka?	xv
Struktura książki	xvi
Konwencje stosowane w książce	xvii
Dodatkowe zasoby	xvii
Wsparcie techniczne	xviii
1 Omówienie administracji usług IIS 7.0	1
Użytkowanie IIS 7.0: co należy wiedzieć na początku	1
Omówienie architektury konfiguracji IIS 7.0	4
Schemat konfiguracji IIS 7.0	4
Globalny system konfiguracji IIS 7.0	8
Wymagania sprzętowe IIS 7.0	13
Usługi IIS 7.0 a system Windows	15
Narzędzia i techniki administracji sieci Web	16
Zarządzanie zasobami za pomocą najważniejszych narzędzi administracyjnych	16
Techniki administracji sieci Web	17
2 Instalowanie usług IIS 7.0 w przedsiębiorstwie	23
Protokoły IIS 7.0	23
HTTP i SSL	23
FTP	24
SMTP	25
Role usług IIS 7.0	26
Omówienie funkcji i ról IIS 7.0	33
Usługi ról dla serwerów aplikacji	33
Usługi roli dla stacji systemu Windows i serwerów sieci Web	37
Usługi ról dla serwerów, na których uruchomiono oprogramowanie SharePoint Services	48
Konfigurowanie usług IIS 7.0	48
Instalowanie serwerów aplikacji	48
Instalowanie serwerów sieci Web	51
Instalowanie oprogramowania Windows SharePoint Services	52
Dodawanie lub usuwanie funkcji serwera sieci Web w systemie Windows Vista	55
Zarządzanie zainstalowanymi rolami i usługami ról	56
Przeglądanie skonfigurowanych ról i usług ról	56
Dodawanie lub usuwanie ról serwera	58
Przeglądanie i modyfikowanie usług ról na serwerach	59

3	Administracja głównych funkcji usług IIS 7.0	61
	Korzystanie z usług IIS i adresów URL	61
	Budowa architektury podstawowych funkcji usług IIS.....	64
	Działanie witryny sieci Web	64
	Korzystanie z aplikacji sieci Web i katalogów wirtualnych.....	64
	Kontrolowanie dostępu do serwerów, witryn i aplikacji.....	65
	Budowa architektury usług i przetwarzania.....	66
	Informacje podstawowe o usługach i procesach IIS	66
	Tryb izolacji procesu roboczego IIS	67
	Działanie i używanie aplikacji usług IIS.....	71
	Działanie i używanie aplikacji ASP.NET	72
	Zarządzanie serwerami IIS: najważniejsze kwestie.....	74
	Korzystanie z programu	
	Internet Information Services (IIS) Manager	74
	Włączanie i konfigurowanie administracji zdalnej.....	77
	Uruchamianie, zatrzymywanie	
	i ponowne uruchamianie wszystkich usług internetowych	79
	Zarządzanie poszczególnymi zasobami	
	w programie IIS Manager (Menedżer IIS).....	81
	Ponowne uruchamianie serwerów IIS	82
	Zarządzanie usługami IIS	83
	Uruchamianie, zatrzymywanie i wstrzymywanie usług IIS	84
	Konfigurowanie uruchamiania usług.....	85
	Konfigurowanie odzyskiwania usługi	86
4	Zarządzanie usługami IIS 7.0 w wierszu poleceń	89
	Używanie programu Windows PowerShell.....	89
	Wprowadzenie do programu Windows PowerShell.....	89
	Uruchamianie i używanie Windows PowerShell.....	90
	Uruchamianie i używanie poleceń typu Cmdlets.....	91
	Uruchamianie i używanie innych poleceń	
	i programów narzędziowych.....	93
	Używanie poleceń typu cmdlet.....	93
	Polecenia cmdlet powłoki Windows PowerShell	93
	Używanie parametrów polecenia Cmdlet	95
	Opis błędów poleceń cmdlet	96
	Używanie nazw zastępczych (alias) poleceń cmdlet	96
	Używanie poleceń cmdlet w usługach IIS.....	97
	Używanie narzędzia administracji wiersza poleceń usług IIS	99
	Uruchamianie i korzystanie z narzędzia administracji	
	wiersza poleceń IIS	99
	Korzystanie z narzędzia administracji	
	wiersza poleceń usług IIS	101
	Używanie poleceń IIS	102
	Używanie poleceń zarządzania konfiguracją.....	102
	Używanie poleceń zarządzania modułami.....	103
	Używanie poleceń zarządzania witryną	104
	Używanie poleceń zarządzania pulami aplikacji	105
	Używanie poleceń zarządzania aplikacją.....	106

Używanie poleceń zarządzania katalogiem wirtualnym	106
Używanie poleceń programów narzędziowych.....	107
5 Zarządzanie globalną konfiguracją usług IIS	109
Poziomy konfiguracji i globalna konfiguracja.....	109
Zarządzanie sekcjami konfiguracji.....	115
Opracowywanie sekcji konfiguracji.....	115
Określanie ustawień dla sekcji konfiguracji.....	116
Modyfikowanie ustawień sekcji konfiguracji.....	117
Blokowanie i odblokowanie sekcji konfiguracji	118
Czyszczenie i ponowne ustawianie sekcji konfiguracji	119
Moduły rozszerzeń usług IIS	120
Kontrolowanie modułów macierzystych za pomocą plików konfiguracji	120
Kontrolowanie modułów zarządzanych za pomocą plików konfiguracji	121
Kontrolowanie zarządzanych programów obsługi za pomocą plików konfiguracji	122
Użycie plików konfiguracji i schematu do instalowania niestandardowych modułów rozszerzeń	125
Zarządzanie modułami	126
Przeglądanie zainstalowanych macierzystych i zarządzanych modułów.....	126
Instalowanie modułów macierzystych	128
Włączanie modułów macierzystych.....	129
Włączanie modułów zarządzanych.....	130
Edycja konfiguracji macierzystych i zarządzanych modułów.....	131
Wyłączanie macierzystych i zarządzanych modułów.....	132
Odinstalowanie modułów macierzystych.....	133
Współużytkowanie konfiguracji globalnej.....	134
Korzystanie z udostępnionej konfiguracji.....	134
Eksportowanie i udostępnianie konfiguracji globalnej	134
6 Konfigurowanie witryn i katalogów sieci Web.....	137
Nazewnictwo i identyfikacja witryn sieci Web	137
Adresy IP i rozpoznawanie nazw.....	137
Identyfikatory witryn sieci Web	138
Utrzymywanie wielu witryn na jednym serwerze	139
Sprawdzanie nazw komputera i adresu IP serwerów.....	142
Sprawdzenie konfiguracji witryny	143
Tworzenie witryn sieci Web.....	146
Tworzenie witryny sieci Web: podstawy.....	146
Tworzenie niezabezpieczonej witryny sieci Web	147
Tworzenie zabezpieczonej witryny sieci Web	149
Zarządzanie witrynami sieci Web i ich właściwościami.....	151
Zarządzanie witrynami w programie IIS Manager	151
Konfigurowanie puli aplikacji witryny i katalogu macierzystego	153

Konfigurowanie portów, adresów IP i nazw hostów używanych przez witryny sieci Web	155
Ograniczenia dla połączeń przychodzących i określanie wartości limitów czasu	157
Konfigurowanie parametru HTTP Keep-Alive (urzeczywianie aktywności HTTP).....	160
Konfigurowanie uprawnień dostępu w programie IIS Manager	161
Zarządzanie identyfikatorem numerycznym witryny i stanem AutoStart	162
Usuwanie witryn.....	164
Tworzenie katalogów.....	164
Struktura fizycznych i wirtualnych katalogów	164
Sprawdzanie konfiguracji katalogu wirtualnego	165
Tworzenie katalogów fizycznych.....	167
Tworzenie katalogów wirtualnych.....	167
Zarządzanie katalogami i ich właściwościami.....	169
Włączanie i wyłączanie funkcji przeglądania katalogu	169
Modyfikowanie właściwości katalogu	171
Zmiana nazwy katalogów.....	171
Modyfikowanie ścieżek, metod logowania i innych parametrów katalogów wirtualnych.....	172
Usuwanie katalogów	173
7 Dostosowywanie zawartości serwera sieci Web	175
Zarządzanie zawartością sieci Web	175
Otwieranie i przeglądanie plików.....	176
Modyfikowanie właściwości plików	176
Zmiana nazwy plików.....	176
Usuwanie plików	177
Przekierowanie żądań przeglądarki	177
Przekierowywanie żądań do innych katalogów lub witryn	177
Przekierowanie wszystkich żądań do innej witryny sieci Web.....	178
Przekierowanie żądań do aplikacji	179
Dostosowywanie przekierowania przeglądarki	179
Dostosowywanie zawartości witryny sieci Web i nagłówków HTTP	181
Konfigurowanie dokumentów domyślnych.....	181
Konfigurowanie stopek dokumentów.....	184
Konfigurowanie dołączanych plików.....	184
Wygasanie zawartości i zapobieganie buforowaniu przez przeglądarkę	185
Niestandardowe nagłówki HTTP.....	188
Klasyfikacja zawartości i zasady prywatności	189
Zwiększenie wydajności przy użyciu kompresji.....	190
Konfigurowanie kompresji zawartości dla całego serwera	191

Włączanie lub wyłączanie kompresji zawartości dla witryn i katalogów	194
Dostosowywanie komunikatów o błędach serwera sieci Web	194
Kody stanu i komunikaty o błędach	194
Zarządzanie ustawieniami dotyczącymi niestandardowych błędów	196
Używanie typu MIME i konfigurowanie niestandardowych typów plików	203
Działanie typu MIME	203
Przeglądanie i konfigurowanie typów MIME	205
Dodatkowe wskazówki dotyczące dostosowywania	207
Użycie metody aktualizowania witryn do zarządzania przestojami	207
Używanie stron przeskoku dla reklam	209
Obsługa błędów 404 i zapobieganie „ślepych uliczkom”	209
8 Uruchamianie aplikacji IIS	211
Zarządzanie ustawieniami aplikacji ISAPI i CGI	211
Działanie aplikacji ISAPI	211
Konfigurowanie ograniczeń ISAPI i CGI	212
Konfigurowanie filtrów ISAPI	215
Konfigurowanie ustawień CGI	216
Zarządzanie ustawieniami ASP	217
Kontrolowanie działania ASP	217
Dostosowywanie obsługi żądań ASP	220
Optymalizacja buforowania ASP	222
Dostosowanie wykonywania modelu COM Plus dla ASP	223
Konfigurowanie stanu sesji dla stron ASP	224
Konfigurowanie debugowania i obsługi błędów stron ASP	226
Zarządzanie ustawieniami ASP.NET	228
Konfigurowanie ustawień stanu sesji dla ASP.NET	228
Konfigurowanie ustawień SMTP E-Mail	232
Konfigurowanie par klucz-wartość dla aplikacji ASP.NET	234
Konfigurowanie ustawień dla stron i formantów ASP.NET	235
Podłączenie do źródeł danych	239
Zarządzanie ustawieniami platformy .NET Framework	242
Konfigurowanie dostawców .NET	242
Konfigurowanie poziomów zaufania .NET	245
Konfigurowanie profili .NET	246
Konfigurowanie funkcji .NET Roles	247
Konfigurowanie funkcji .NET Users	248
Konfigurowanie kompilacji .NET	249
Konfigurowanie funkcji .NET Globalization	251
9 Zarządzanie aplikacjami, pulami aplikacji i procesami roboczymi	253
Definiowanie niestandardowych aplikacji	253
Zarządzanie niestandardowymi aplikacjami usług IIS	255
Przeglądanie aplikacji	255
Konfigurowanie ustawień domyślnych dla nowych aplikacji	256

Tworzenie aplikacji	258
Konwertowanie istniejących katalogów do aplikacji	260
Zmiana ustawień aplikacji	260
Konfigurowanie buforowania danych wyjściowych aplikacji	261
Usuwanie aplikacji IIS	265
Zarządzanie platformami ASP.NET i .NET Framework	266
Instalowanie platform ASP.NET i .NET Framework	266
Instalowanie aplikacji ASP.NET	267
Odinstalowanie wersji platformy .NET	268
Pule aplikacji	268
Wyświetlanie pul aplikacji	269
Konfigurowanie ustawień domyślnych nowych pul aplikacji	271
Tworzenie pul aplikacji	277
Zmiana ustawień puli aplikacji	278
Przypisywanie aplikacji do puli aplikacji	279
Konfigurowanie tożsamości puli aplikacji	280
Ręczne uruchamianie, zatrzymywanie i odtwarzanie procesów roboczych	280
Konfigurowanie wielu procesów roboczych dla pul aplikacji	283
Konfigurowanie odtwarzania procesów roboczych	284
Automatyczne odtwarzanie związane z liczbą i czasem przetwarzania żądań	285
Automatyczne odtwarzanie związane z wykorzystaniem pamięci	286
Utrzymywanie dobrej wydajności i stanu aplikacji	287
Konfigurowanie monitorowania CPU	287
Konfigurowanie wykrywania awarii i przywracanie po awarii	289
Zamykanie bezczynnych procesów roboczych	290
Ograniczanie liczby żądań w kolejce	291
Usuwanie pul aplikacji usług IIS	292
10 Zarządzanie zabezpieczeniami serwera sieci Web	293
Zarządzanie zabezpieczeniami systemu Windows	293
Konta użytkowników i grup	294
Podstawowe informacje na temat użytkowników i grup usług IIS	294
Zarządzanie kontami logowania usług IIS	296
Zarządzanie kontem Internet Guest	297
Uprawnienia plików i folderów	298
Stosowanie zasad grupy	302
Zarządzanie zabezpieczeniami usług IIS	307
Konfigurowanie mapowania obsługi aplikacji	307
Ustawianie trybów uwierzytelnienia	311
Ustawianie reguł autoryzacji dla dostępu do aplikacji	315
Konfigurowanie ograniczeń adresów IPv4 i nazw domeny	317
Zarządzanie funkcją delegowania i administracji zdalnej	320

11 Zarządzanie usługami certyfikatów Active Directory i protokołem SSL	325
Działanie protokołu SSL	325
Stosowanie szyfrowania protokołu SSL	325
Używanie certyfikatów SSL	327
Siła szyfrowania SSL	328
Active Directory Certificate Services	329
Działanie Active Directory Certificate Services	329
Instalowanie modułu Active Directory Certificate Services	331
Uzyskiwanie dostępu w przeglądarce do modułu Certificate Services	332
Uruchamianie i zatrzymywanie usług certyfikatów (Certificate Services)	333
Tworzenie kopii zapasowej i przywracanie urzędu certyfikacji	334
Konfigurowanie przetwarzania żądań certyfikatów	336
Zatwierdzanie lub odmowa żądania certyfikatu	337
Ręczne generowanie certyfikatów w przystawce Certification Authority	338
Odwoływanie certyfikatów	338
Przeglądanie i odnawianie certyfikatu głównego CA	339
Tworzenie i instalowanie certyfikatów	340
Tworzenie żądań certyfikatów	340
Przekazywanie żądań certyfikatów do urzędów certyfikacji firm niezależnych	342
Dostarczanie żądań certyfikatów do modułu Certificate Services	344
Przetwarzanie oczekujących żądań i instalowanie certyfikatów witryn	345
Używanie protokołu SSL	346
Konfigurowanie portów protokołu SSL	346
Dodawanie certyfikatu CA do magazynu głównego przeglądarki klienta	346
Sprawdzanie prawidłowości włączenia protokołu SSL	347
Rozwiązywanie problemów SSL	348
Ignorowanie, akceptowanie i wymaganie certyfikatów klienta	348
Wymaganie protokołu SSL dla całej komunikacji	349
12 Dostrajanie wydajności, monitorowanie i śledzenie	351
Monitorowanie wydajności i aktywności usługi IIS	351
Powody monitorowania usług IIS	351
Przygotowanie do monitorowania	352
Wykrywanie i usuwanie błędów usług IIS	353
Analizowanie dzienników dostępu	353
Analizowanie dzienników zdarzeń systemu Windows	354
Analiza dzienników śledzenia	358
Monitorowanie wydajności i niezawodności usług IIS	367
Korzystanie z konsoli niezawodności i wydajności	367
Wybór liczników monitorowania	370

Dostrajanie wydajności serwera sieci Web	372
Monitorowanie i dostrajanie wykorzystania pamięci	372
Monitorowanie i dostrajanie wykorzystania procesora	375
Monitorowanie i dostrajanie dyskowych operacji I/O	376
Monitorowanie i dostrajanie pasma i połączeń sieci	378
Metody zwiększania wydajności usług IIS	380
Usuwanie niepotrzebnych aplikacji i usług	380
Optymalizowanie wykorzystania zawartości	380
Optymalizacja aplikacji ISAPI, ASP i ASP.NET	382
Optymalizacja buforowania, kolejkowania i pul usług IIS	383
13 Śledzenie dostępu użytkownika i rejestrowanie	385
Statystyki śledzenia	385
Format pliku dziennika NCSA	387
Format pliku dziennika Microsoft IIS	391
Rozszerzony format pliku dziennika W3C	392
Rejestrowanie ODBC	395
Scentralizowane rejestrowanie binarne	397
Działanie funkcji rejestrowania	397
Konfigurowanie rejestrowania	399
Konfigurowanie rejestrowania dla serwera i dla witryny	399
Konfigurowanie formatu pliku dziennika NCSA	400
Konfigurowanie formatu pliku dziennika Microsoft IIS	401
Konfigurowanie rozszerzonego formatu pliku dziennika W3C	402
Konfigurowanie rejestrowania ODBC	404
Konfigurowanie scentralizowanego rejestrowania binarnego	408
Wyłączanie rejestrowania	409
14 Tworzenie kopii zapasowych i odtwarzanie usług IIS	411
Tworzenie kopii zapasowych konfiguracji usług IIS	411
Kopie zapasowe konfiguracji usług IIS	411
Zarządzanie historią konfiguracji usług IIS	414
Wyświetlanie kopii zapasowych konfiguracji usługi IIS	415
Tworzenie kopii zapasowych usług IIS	416
Usuwanie kopii zapasowych konfiguracji usługi IIS	416
Przywracanie konfiguracji serwera usług IIS	416
Odbudowa uszkodzonych instalacji usług IIS	417
Tworzenie kopii zapasowych i przywracanie plików serwera	418
Włączanie funkcji Backup (Kopia zapasowa)	419
Program Windows Server Backup	419
Ustawianie podstawowych opcji wydajności	421
Harmonogram kopii zapasowych serwera	421
Tworzenie kopii zapasowych serwera	423
Ochrona serwera przed awariami	425
Odzyskiwanie plików i folderów	427
Dodatek	429
Moduły usług IIS 7.0	430
Moduły macierzyste	430

Wprowadzenie do modułów zarządzanych	434
Opis modułów macierzystych usług IIS 7.0	435
AnonymousAuthenticationModule.....	435
BasicAuthenticationModule.....	437
CertificateMappingAuthenticationModule.....	438
CgiModule.....	439
ConfigurationValidationModule.....	441
CustomErrorModule	441
CustomLoggingModule	444
DefaultDocumentModule.....	445
DigestAuthenticationModule.....	446
DirectoryListingModule.....	447
DynamicCompressionModule.....	448
FailedRequestsTracingModule	452
FastCgiModule	456
FileCacheModule	458
HttpCacheModule	458
HttpLoggingModule.....	461
HttpRedirectionModule.....	464
IISCertificateMappingAuthenticationModule	466
IpRestrictionModule	468
IsapiFilterModule	470
IsapiModule	471
ManagedEngine	473
ProtocolSupportModule	474
RequestFilteringModule.....	475
RequestMonitorModule.....	477
ServerSideIncludeModule.....	477
StaticCompressionModule	478
StaticFileModule.....	479
TokenCacheModule	480
TracingModule.....	480
UriCacheModule	481
UrlAuthorizationModule.....	481
WindowsAuthenticationModule.....	483
Zarządzane moduły usług IIS 7.0	484
AnonymousIdentificationModule.....	484
DefaultAuthenticationModule.....	484
FileAuthorizationModule.....	485
FormsAuthenticationModule	485
OutputCacheModule.....	488
ProfileModule.....	488
RoleManagerModule.....	489
SessionStateModule.....	489
UrlAuthorizationModule.....	490
UrlMappingsModule	490
WindowsAuthenticationModule.....	491
Index	493

Rozdział 1

Omówienie administracji usług IIS 7.0

Na wstępie rozpoczniemy od przekazania złej wiadomości: usługi Internet Information Services (IIS) 7.0 są czymś innym, niż powszechnie się sądzi. Chociaż usługi IIS 7.0 są najnowszą wersją programu Internet Information Services, nie są tym, czym wydają się być. Usługi IIS w dużym stopniu przypominają swoich poprzedników, ale jest to mylące, ponieważ ich wewnętrzna architektura jest zupełnie inna. Zmian jest tak wiele, że w rzeczywistości byłoby lepiej, jeśli firma Microsoft nadałaby nową nazwę dla usług IIS 7.0. Tak więc należy zdawać sobie sprawę, że usługi IIS 7.0 zupełnie różnią się od poprzedników, co umożliwia użytkownikowi rozpoczęcie pracy z nowymi perspektywami i uzasadnionymi oczekiwaniami związanymi z poznaniem całego nowego pakietu metod. Sprawdzone zalety IIS także będą musiały „oduczyć” się stosowania niektórych starych sztuczek – i to nie musi być tylko utrudnienie, to może okazać się największą przeszkodą w opanowaniu usług IIS 7.0.

Program IIS 7.0 udostępnia podstawowe usługi umożliwiające działanie serwerów internetowych, aplikacji sieci Web i programu Microsoft Windows SharePoint Services. W całej książce określenie *administracja sieci Web* lub *administracja sieci Web firmy Microsoft* odnosi się zarówno do administracji IIS, administracji aplikacjami internetowymi, jak i do administracji Windows SharePoint Services. Podczas administrowania usługami Microsoft Web należy skoncentrować się na następujących kwestiach głównych:

- Nowości i zmiany w IIS 7.0
- Sposób używania schematów i globalnej architektury konfiguracji IIS 7.0
- Sposób współpracy IIS 7.0 ze sprzętem
- Sposób współpracy IIS z systemami operacyjnymi Windows
- Dostępne narzędzia administracyjne
- Techniki administracyjne, które można stosować do zarządzania i konserwacji IIS

Użytkowanie IIS 7.0: co należy wiedzieć na początku

Firma Microsoft w usługach IIS 7.0 w pełni zintegrowała platformy Microsoft ASP.NET i Microsoft .NET Framework. Inaczej niż w przypadku IIS 6, usługi IIS 7.0 przenoszą platformy ASP.NET i .NET Framework na następny poziom poprzez zintegrowanie modelu ASP.NET umożliwiającego rozszerzanie działania (runtime extensibility model) z podstawową architekturą serwera, dzięki czemu projektanci stosując technologie ASP.NET i .NET Framework mogą w pełni rozszerzać architekturę serwera. Bardziej ścisła integracja umożliwia w odniesieniu do wszystkich typów zawartości używanie istniejących funkcji ASP.NET, takich jak .NET Roles, Session Management, Output Caching czy Forms Authentication. Usługi IIS 7.0 uogólniły model aktywacji procesu protokołu HTTP (Hypertext Transfer Protocol), wprowadzony w usługach IIS 6.0 wraz z pulami aplikacji i udostępniły ten model dla wszystkich protokołów poprzez niezależną usługę nazywaną Windows Process Activation Service, a projektanci mogą stosować adaptory protokołów WCF (Windows Communication

Foundation), by wykorzystać możliwości tej usługi. Na początku warto również wiedzieć, że usługi IIS 7.0 zawierają składnik zgodności metabazy, który umożliwia działanie istniejących skryptów i aplikacji, ale nie używa metabazy do przechowywania informacji o konfiguracji. Zamiast metabazy usługi IIS 7.0 korzystają z rozproszonego systemu konfiguracji wraz z plikami konfiguracyjnymi specyficznymi dla aplikacji lub dla całego systemu, które opierają się na niestandardowym zestawie plików schematu języka XML (Extensible Markup Language). Te pliki schematów XML oprócz definiowania elementów i atrybutów konfiguracji, definiują wartości tych elementów i atrybutów, co umożliwia dokładną kontrolę sposobów konfigurowania i używania IIS.

Firma Microsoft zbudowała system konfiguracji w oparciu o koncepcję modułów. Moduły są autonomicznymi składnikami, udostępniającymi podstawowe zestawy funkcji serwera IIS. Wraz z usługami IIS 7.0 firma Microsoft dostarcza ponad 40 niezależnych modułów. Moduły te albo są specyficzne dla usługi IIS 7.0 i korzystają z bibliotek Win32 DLL, albo są modułami zarządzanymi przez IIS 7.0, które używają bibliotek .NET Framework Class Library zawartych w zestawie. Ponieważ wszystkie funkcje serwera zawarte są w modułach, dostępne funkcje można łatwo modyfikować poprzez dodawanie, usuwanie lub zastępowanie modułów serwera. Ponadto, optymalizując zainstalowane moduły w oparciu o sposób stosowania serwera IIS, można zwiększyć bezpieczeństwo poprzez zmniejszenie możliwości przeprowadzania ataków i można zwiększyć wydajność poprzez zmniejszenie zasobów wymaganych do uruchomienia podstawowych usług.

Uwaga Ponieważ moduły i sposób ich używania są bardzo ważną częścią usług IIS 7.0, tematy te zostały dokładniej omówione w dalszej części książki. W rozdziale 2 „Instalowanie usług IIS 7.0 w przedsiębiorstwie” omówione zostały wszystkie dostępne moduły. W rozdziale 5 „Zarządzanie globalną konfiguracją IIS” zamieszczono szczegółowy opis instalacji i zarządzania modułami. Natomiast w dodatku „Pełny wykaz modułów i schematów usług IIS 7.0” znaleźć można kompletny poradnik korzystania z modułów i schematów.

Usługi IIS 7.0 są bardziej bezpieczne niż usługi IIS 6, ponieważ w odniesieniu do żądań wbudowana w nie została obsługa autoryzacji filtrowania i reguł bazujących na URL (Uniform Resource Locator). Istnieje możliwość skonfigurowania filtrowania żądań tak, aby podejrzone żądania były odrzucane poprzez przeglądanie adresów URL wysyłanych do serwera i filtrowaniu niepożądanych żądań. Użytkownik może skonfigurować reguły autoryzacji URL tak, aby wymagane było logowanie oraz może odmówić bądź zezwolić na dostęp do określonych adresów URL w odniesieniu do nazw użytkowników, ról platformy .NET i metod żądania HTTP. W celu ułatwianiem administracji problemów serwerów i aplikacji internetowych, usługi IIS 7.0 wyposażone zostały w nowe funkcje diagnostyczne, przeglądania żądań w czasie rzeczywistym i tworzenia raportów o błędach. Funkcje te pozwalają na:

- Przeglądanie bieżącego stanu działania serwera.
- Śledzenia niepomysłnych żądań przez podstawową architekturę serwera.
- Uzyskanie szczegółowych informacji o błędach w celu wskazania przyczyn problemów.

Usługi IIS 7.0 mają wiele innych nowych i rozszerzonych funkcji, a niektóre z nich są tak samo ważne, jak nowy zestaw narzędzi administracyjnych, wliczając w to nowe narzędzia graficzne, narzędzia wiersza poleceń i narzędzia tworzenia skryptów. Nowe graficzne narzędzia administracyjne korzystają z interfejsu podobnego do przeglądarki, dodają funkcje związane z delegowaniem administracji, związane z administracją zdalną poprzez protokół HTTPS (Secure HTTP) i z możliwościami rozszerzania poprzez niestandardowe składniki interfejsu użytkownika. Nowe narzędzia administracji bazujące na wierszu poleceń umożliwiają

wykonywanie większości zadań konfiguracyjnych za pomocą pojedynczego wiersza tekstu polecenia. Przy użyciu ASP.NET można zarządzać konfiguracją IIS poprzez platformę .NET Framework stosując interfejs programowy (API) Microsoft.Web.Administrators, natomiast skrypty można wykorzystywać do zarządzania konfiguracją usług IIS poprzez oprogramowanie dostawcy WMI (Windows Management Instrumentation) usług IIS 7.0.

Ze względu na ogrom zmian dotychczasowa wiedza na temat usług IIS nie ma większego znaczenia lub jest przestarzała. Ale na końcu tunelu widać światło – przypomina to pociąg przejeżdżający obok – który jednak jest w naszym zasięgu. Zmiany usług IIS 7.0 są warte czasu i wysiłku poświęconego na zapoznanie się z nową architekturą i nowymi technikami wymaganymi do zarządzania serwerami sieci Web. Z czasem wzrastać będzie nasza zależność od oprogramowania ASP.NET i .NET Framework, a im więcej poznamy informacji o sercu architektury .NET – IIS 7.0 – tym lepiej będziemy przygotowani teraz i w przyszłości.

W przypadku usług IIS 7.0 najważniejsze składniki będące częścią poprzednich wersji IIS nie są już dostępne lub działają w inny sposób, niż poprzednio. Ponieważ usługi IIS 7.0 nie korzystają z metabazy, aplikacje zaprojektowane dla usług IIS 6 nie będą działały przy użyciu IIS 7.0 bez przedsięwzięcia specjalnych działań. W celu uruchomienia aplikacji IIS 6 należy zainstalować funkcje obsługujące kompatybilność i metabazę. Aby zarządzać aplikacjami i funkcjami usług IIS 6, trzeba zainstalować moduł IIS 6 Manager, narzędzia tworzenia skryptów IIS 6 i zgodności IIS 6 WMI. Ponadto do usług IIS 7.0 nie zostały dołączone usługi protokołów POP3 (Post Office Protocol wersja 3) lub SMTP (Simple Mail Transfer Protocol). Korzystając z usług IIS 7.0 można wysłać wiadomości e-mail z aplikacji internetowej przy użyciu składnika SMTP E-mail zawartego w ASP.NET.

Program IIS Manager jest graficznym interfejsem użytkownika (GUI) dla zarządzania lokalnymi i zdalnymi instalacjami IIS 7.0. Aby skorzystać z programu IIS Manager do zdalnego zarządzania serwerem IIS należy zainstalować i uruchomić usługę WMSVC (Web Management Service) na serwerze IIS, który ma być zarządzany zdalnie. Usługa WMSVC jest również wymagana, jeśli administratorzy witryny lub aplikacji IIS chcą zarządzać funkcjami, których kontrola została im przekazana.

Usługa WMSVC stanowi podstawę dla umożliwienia działania w sieci Web (HWC, Hostable Web Core), a dla administracji zdalnej działa jak autonomiczny serwer internetowy. Po zainstalowaniu i uruchomieniu usługi WMSVC na serwerze IIS, rozpoczyna się nasłuchiwanie na porcie 8172 wszystkich nieprzypisanych adresów IP dla czterech wymienionych poniżej typów żądań:

- **Żądania logowania** Program IIS Manager wysyła żądania logowania do usługi WMSVC w celu zainicjowania połączenia. W środowisku HWC żądania logowania są obsługiwane przez Login.axd. W tym przypadku typem uwierzytelnienia jest NT LAN Manager (NTLM) lub Basic, w zależności od tego, co zostało wybrane podczas wprowadzania powiadzczeń w oknie dialogowym połączenia.
- **Żądania pobrania kodu** Jeśli proces logowania przebiegł pomyślnie, usługa WMSVC zwraca listę modułów interfejsu użytkownika (UI) dla połączenia. Każda strona programu IIS Manager dotyczy określonego modułu UI. Jeśli występuje moduł, którego nie zawiera program IIS Manager, nastąpi żądanie pobrania kodu binarnego modułu. Żądania pobrania kodu są obsługiwane przez Download.axd.
- **Żądania dotyczące zarządzania usługą (Management Service Requests)** Po nawiązaniu połączenia interakcja użytkownika z programem IIS Manager wywołuje żądania związane z zarządzaniem usługą. Żądania te nakazują usługom modułu w usłudze WMSVC odczytywanie bądź zapisywanie danych konfiguracyjnych, danych o stanie

działania i dostawcach na serwerze. Żądania dotyczące zarządzania usługą są obsługiwane przez Service.axd.

- **Żądania polecenia Ping (Ping Requests)** Żądania Ping są wykonywane wewnątrz usługi WMSVC w odniesieniu do usług HWC. Żądania Ping są wykonywane przez Ping.axd w celu sprawdzenia, czy usługi HWC w dalszym ciągu mogą odpowiadać.

Usługa WMSVC (Web Management Service) przechowuje w rejestrze okrojony zestaw wartości konfiguracyjnych. Każdorazowe uruchomienie usługi powoduje odświeżenie plików konfiguracyjnych sieci Web w następującym katalogu: %SystemRoot%\ServiceProfiles\LocalService\AppData\Local\Temp\WMSvc. Dla wszystkich połączeń, w celu zwiększenia bezpieczeństwa usługa WMSVC żąda używania protokołu SSL (HTTPS). Dzięki temu dane przekazywane pomiędzy zdalnym klientem IIS Manager a usługą WMSVC są bezpieczne. Ponadto usługa WMSVC uruchamiana jest jako usługa lokalna (Local Service) przy ograniczonych uprawnieniach i zablokowanej konfiguracji. Takie podejście zapewnia, że podczas uruchamiania usługi HWC ładowany jest jedynie minimalny zestaw wymaganych modułów. Dodatkowe informacje na ten temat znaleźć można w rozdziale 3 „Główne zadania administracyjne usług IIS 7.0”.

Uwaga Wyrażenie %SystemRoot% odnosi się do zmiennej środowiskowej SystemRoot. W systemie operacyjnym Windows jest wiele zmiennych środowiskowych, które są używane jako odniesienie do wartości specyficznych dla systemu bądź użytkownika. W niniejszej książce w odniesieniach do zmiennych środowiskowych używana jest składnia: %Nazwa_zmiennej%.

Omówienie architektury konfiguracji IIS 7.0

Usługi IIS 7.0 są używane do publikowania informacji w sieciach typu intranet, extranet i w Internecie. Ponieważ dzisiejsze witryny sieci Web korzystają z odpowiednich mechanizmów, takich jak filtry ISAPI, ASP, ASP.NET, CGI czy .NET Framework, usługi IIS łączą wszystkie te funkcje tworząc kompletne rozwiązanie. Na początku w odniesieniu do IIS 7.0 trzeba zapoznać się, w jaki sposób usługi IIS 7.0 korzystają ze schematu konfiguracyjnego i swojego globalnego systemu konfiguracji. W rozdziale 2 czytelnik zostanie zapoznany z dostępnymi funkcjami konfiguracji i związanymi z nimi modułami.

Schemat konfiguracji IIS 7.0

Inaczej niż w przypadku usług IIS 6, gdzie większość informacji konfiguracyjnych przechowywanych jest w plikach matabazy, usługi IIS 7.0 mają zuniifikowany system konfiguracyjny dla przechowywania ustawień serwera, witryny i aplikacji. Ustawienia te mogą być zarządzane za pomocą dołączonego zestawu kodu, skryptów interfejsu API i narzędzi zarządzania. Ustawienia te mogą być także zarządzane poprzez bezpośrednią edycję samych plików konfiguracyjnych. Bezpośrednia edycja plików konfiguracyjnych jest możliwa dzięki temu, że pliki używają języka XML i są otwartymi plikami tekstowymi bazującymi na wstępnie zdefiniowanym zestawie plików schematów XML.

Uwaga Usługi IIS 7.0 zawsze pobierają wzorcowy stan konfiguracji z plików konfiguracyjnych, co stanowi zasadniczą różnicę w odniesieniu do usług IIS 6, gdzie stan wzorcowy był pobierany z konfiguracyjnej bazy danych przechowywanej w pamięci, która była okresowo zapisywana na dysku.

Używanie schematów XML do określenia ustawień konfiguracji zapewnia, że odpowiednie pliki konfiguracji mają prawidłową strukturę plików XML i są łatwe do zmodyfikowania i utrzymywania. Z tego względu, że wartości konfiguracyjne są przechowywane w postaci prostych do zrozumienia ciągów tekstowych i wartości, łatwo jest nimi operować i ich używać. Poprzez analizę samego schematu można określić dokładny zestaw dopuszczalnych wartości dla każdej opcji konfiguracji. Usługi współużytkują ten sam schemat, co konfiguracja ASP.NET, dzięki czemu tak samo prosto jest zarządzać ustawieniami konfiguracji i je konserwować dla aplikacji ASP.NET.

Na serwerze IIS pliki schematów przechowywane są w katalogu `%SystemRoot%\System32\Inetsrv\Config\Schema`. Poniżej wymienione zostały cztery standardowe pliki schematów:

- **IIS_schema.xml** Plik ten udostępnia schemat konfiguracji IIS.
- **ASPNET_schema.xml** Plik ten udostępnia schemat konfiguracji ASP.NET.
- **FX_schema.xml** Plik ten udostępnia schemat konfiguracji .NET Framework (zapewnia funkcje, których nie oferuje schemat ASP.NET).
- **rscaxext.xml** Plik ten udostępnia schemat konfiguracji dla funkcjonalności Runtime Status oraz Control API (RSCA), dostarczając właściwości dynamicznych w celu uzyskania szczegółowych danych dotyczących działania.

Usługi IIS automatycznie odczytują pliki schematu podczas uruchamiania puli aplikacji. Plik schematu IIS jest wzorcowym plikiem schematu. Wewnątrz pliku schematu IIS znajdują się sekcje dotyczące konfiguracji każdej głównej funkcji IIS, od funkcji tworzenia puli aplikacji po śledzenie niepomyślnych żądań. Plik schematu ASP.NET zbudowany jest na schemacie wzorca i stanowi jego rozszerzenie o sekcje konfiguracji specyficzne dla ASP.NET. W pliku schematu ASP.NET znaleźć można sekcje konfiguracji dotyczące różnych ustawień od identyfikacji anonimowej po bufor wyjściowy. Plik schematu FX zbudowany jest w oparciu o plik schematu ASP.NET i stanowi jego rozszerzenie. W pliku tym znaleźć można ustawienia konfiguracji dla ustawień aplikacji, ciągów połączeń, serializacji czasu i innych. Chociaż sekcje konfiguracji są również grupowane w celu łatwiejszego zarządzania, dla grup sekcji nie są określone definicje schematu. Jeśli zachodzi potrzeba rozszerzenia funkcji konfiguracji i opcji dostępnych w usługach IIS, można tego dokonać poprzez rozszerzenie schematu XML. Schemat może być rozszerzany zgodnie z poniższą procedurą ogólną:

1. Określić w pliku schematu XML potrzebne właściwości konfiguracji i kontenery sekcji.
2. Umieścić plik schematu w katalogu `%SystemRoot%\System32\Inetsrv\Config\Schema`.
3. Umieścić odniesienie do nowej sekcji w globalnym pliku konfiguracji IIS 7.0.

Poniżej zaprezentowana została ogólna składnia pliku schematu:

```
<!--
```

```
Tekst tej sekcji jest komentarzem. Standardową praktyką jest wprowadzanie informacji szczegółowych w komentarzach na początku pliku schematu.
```

```
-->
```

```

<configSchema>
  <sectionSchema name="configSection1">
  </sectionSchema>
  <sectionSchema name="configSection2">
  </sectionSchema>
  <sectionSchema name="configSection3">
  </sectionSchema>
</configSchema>

```

Administrator czy projektant nie musi koniecznie posiadać umiejętności czytania i interpretowania schematów XML, aby z powodzeniem wykonać swoje zadanie. Ponieważ jednak przydatne jest posiadanie podstawowej wiedzy w tym zakresie, umożliwiającej zrozumienie schematów, w książce zamieszczony został opis najważniejszych kwestii. Wewnątrz plików schematów ustawienia konfiguracyjne są grupowane w zestawy odpowiednich funkcji zwanych *sekcjami schematu*. Schemat sekcji konfiguracji jest zdefiniowany w elemencie XML <sectionSchema>. Na przykład funkcje odnoszące się do nasłuchu HTTP w usługach IIS zostały zdefiniowane za pomocą sekcji schematu nazwanej system.applicationHost/listenerAdapters. W pliku IIS_schema.xml sekcja ta ma następującą postać:

```

<sectionSchema name="system.applicationHost/listenerAdapters">
  <collection addElement="add" >
    <attribute name="name" type="string" required="true" isUniqueKey="true"
  />
    <attribute name="identity" type="string" />
    <attribute name="protocolManagerDll" type="string" />
    <attribute name="protocolManagerDllInitFunction" type="string" />
  </collection>
</sectionSchema>

```

Ta definicja schematu oznacza, że element system.applicationHost/listenerAdapters może zawierać zbiór elementów dodatkowych o następujących atrybutach:

- **name** Unikatowy ciąg, który jest wymaganą częścią elementu dodatkowego.
- **identity** Ciąg identyfikacyjny, który jest opcjonalną częścią elementu dodatkowego.
- **protocolManagerDll** Ciąg identyfikujący bibliotekę DLL menedżera protokołu.
- **protocolManagerDllInitFunction** Ciąg identyfikujący funkcje inicjujące bibliotekę DLL menedżera protokołu.

Atrybut elementu jest albo opcjonalny, albo wymagany. Jeśli definicja atrybutu stanowi required="true", jak w przypadku atrybut *name*, atrybut jest wymagany i musi być dostarczony, jeśli powiązany z nim element jest używany. W przeciwnym razie atrybut traktowany jest jako opcjonalny i nie musi być wprowadzany podczas używania powiązanego elementu. Oprócz tego, że atrybuty mogą być wymagane, można także wymuszać stosowanie innych warunków:

- **isUniqueKey** Jeśli warunek ustawiony jest jako *true*, odnośna wartość musi być unikatowa.
- **encrypted** Jeśli warunek ustawiony jest jako *true*, oczekuje się, że odnośna wartość zostanie zaszyfrowana.

W przypadku niektórych atrybutów można zauważyć wartości domyślne, a także listę akceptowanych wartości ciągu i ich odpowiednich wartości wewnętrznych. W poniższym przykładzie, atrybut `identityType` ma wartość domyślną `NetworkService` oraz listę innych możliwych wartości:

```
<attribute name="identityType" type="enum" defaultValue="NetworkService">
  <enum name="LocalSystem" value="0"/>
  <enum name="LocalService" value="1"/>
  <enum name="NetworkService" value="2"/>
  <enum name="SpecificUser" value="3"/>
</attribute>
```

W celu ułatwienia operowania wartościami wprowadzane są ich zrozumiałe nazwy. Rzeczywista wartość używana przez IIS jest dostarczana w odnośnej definicji wartości. Przykładowo, jeśli zmienna `identityType` określona została jako `LocalService`, rzeczywista wartość konfiguracji używana wewnętrznie przez IIS wynosi 2.

Standardowa reguła określa, że nie można używać wymienionych wartości w połączeniu z innymi. Z tego względu atrybut `identityType` może przyjmować tylko jedną możliwą wartość. W przeciwieństwie do tego, atrybuty mogą mieć flagi, których można używać łącznie w postaci kombinacji wartości. W poniższym przykładzie atrybut `logEventOnRecycle` używa flag i ma domyślny zestaw flag, które są stosowane łącznie:

```
<attribute name="logEventOnRecycle" type="flags" defaultValue="Time,
Memory, PrivateMemory">
  <flag name="Time" value="1"/>
  <flag name="Requests" value="2"/>
  <flag name="Schedule" value="4"/>
  <flag name="Memory" value="8"/>
  <flag name="IsapiUnhealthy" value="16"/>
  <flag name="OnDemand" value="32"/>
  <flag name="ConfigChange" value="64"/>
  <flag name="PrivateMemory" value="128"/>
</attribute>
```

Jak już było nadmienione, zrozumiałe nazwy ułatwiają operowanie wartościami. Rzeczywista wartość używana przez usługi IIS jest sumą połączonych wartości flag. W przypadku ustawienia „Time, Requests, Schedule” atrybut `logEventOnRecycle` przyjmuje wartość 7 ($1+2+4=7$).

Wartości atrybutów mogą także być sprawdzane. Usługi IIS przeprowadzają sprawdzenie wartości atrybutów podczas analizy XML i podczas wywoływania odnośnych API. W tabeli 1-1 wymienione zostały walidacje spotykane w schematach.

Tabela 1-1 Podsumowanie typów walidacji atrybutów w schemacie XML IIS

Typ walidacji	Parametr walidacji	Walidacja nie powiodła się, jeśli...
<code>validationType=„applicationPoolName”</code>	<code>validationParameter=””</code>	Sprawdzana wartość zawiera te znaki: <code> <&A”</code>
<code>validationType=„integerRange”</code>	<code>validationParameter=„<minimum>, <maximum>[,exclude]”</code>	Sprawdzana wartość jest poza zakresem [inside], wartości całkowite.

Ciąg dalszy na stronie następnej

Ciąg dalszy ze strony poprzedniej

Tabela 1-1 Podsumowanie typów walidacji atrybutów w schemacie XML IIS

Typ walidacji	Parametr walidacji	Walidacja nie powiodła się, jeśli...
validationType= „nonEmptyString”	validationParameter=””	Sprawdzana wartość ma wartość ciągu, która nie jest określona.
validationType= „siteName”	validationParameter=””	Sprawdzana wartość zawiera te znaki: \.?
validationType= „timeSpanRange”	validationParameter= „<minimum>, <maximum>, <granularity> [,exclude]”	Sprawdzana wartość jest poza zakresem [inside], w sekundach.
validationType= „requireTrimmedString”	validationParameter=””	Sprawdzana wartość zawiera znaki niewidoczne na początku lub na końcu wartości.

Globalny system konfiguracji IIS 7.0

Usługi IIS używają globalnego systemu konfiguracji, który początkowo może wydawać się trudny do zrozumienia, jednak w miarę jego używania staje się coraz bardziej przejrzysty. Ponieważ próby ułatwienia przejścia przez ten temat nie mają sensu, lepiej wskoczyć od razu na głęboką wodę. Następnym kilku stronom warto poświęcić trochę czasu, ponieważ przeprowadzają przez najtrudniejsze fragmenty i umożliwiają poznanie dokładnie tego, co należy wiedzieć.

Ustawienia konfiguracji IIS przechowywane są w plikach konfiguracji, które razem określają konfigurację działania usług IIS i powiązanych z nimi składników. Jednym ze sposobów myślenia o pliku konfiguracji jest traktowanie go jako kontenera stosowanych ustawień i ich wartości. Do serwera i aplikacji na nim uruchomionych stosować można wiele plików konfiguracyjnych. Ogólnie mówiąc, pliki konfiguracyjne zarządzane są na poziomie katalogu głównego platformy .NET Framework, katalogu głównego serwera i różnych poziomów katalogów zawartości serwera sieci Web. Katalogi zawartości serwera sieci Web obejmują katalog główny samego serwera, katalogi główne konfigurowanych witryn sieci Web i podkatalogi wewnątrz witryn Web. Poziomy katalog głównego i różne poziomy katalogów zawartości serwera sieci Web mogą być przedstawiane jako kontenery stosowanych ustawień i ich wartości. Jeśli czytelnik zna trochę programowanie obiektowe, może spodziewać się stosowania koncepcji dotyczących zależności nadrzędny-podrzędny i dziedziczenia – i będzie miał rację.

Poprzez dziedziczenie ustawienie zastosowane na poziomie nadrzędnym staje się ustawieniem domyślnym dla innych poziomów hierarchii konfiguracji. W skrócie oznacza to, że ustawienie zastosowane na poziomie nadrzędnym jest domyślnie przenoszone w dół do poziomu podrzędnego. Przykładowo, jeśli stosowane jest ustawienie na poziomie katalogu głównego serwera, ustawienie to jest dziedziczone przez wszystkie witryny Web na serwerze oraz przez wszystkie katalogi zawartości wewnątrz tych witryn. Kolejność dziedziczenia jest następująca:

Katalog główny .NET Framework → katalog główny serwera → katalog główny witryny Web → katalogi najwyższych poziomów → podkatalogi

Oznacza to, że ustawienia bieżącego katalogu głównego .NET Framework są przekazywane w dół do IIS, ustawienia dla IIS są przekazywane w dół do witryny sieci Web, a ustawienia witryn Web są przekazywane w dół do katalogów i podkatalogów zawartości. Jak można było oczekiwać, dziedziczenie może być zastępowane. W tym celu należy specyficznie przypisać ustawienie dla poziomu podrzędnego, które unieważnia ustawienie określone dla poziomu nadrzędnego. Tak długo jak zastępowanie jest dopuszczone (to znaczy zastępowanie nie jest blokowane), ustawienie poziomu podrzędnego będzie odpowiednio stosowane. Więcej informacji na temat zastępowania i blokowania ustawień znaleźć można w rozdziale 5.

Podczas używania plików konfiguracyjnych warto pamiętać o następujących kwestiach:

- Usługi IIS określają katalog główny .NET Framework w zależności od aktualnie działającej wersji ASP.NET i .NET Framework. Domyślne pliki konfiguracji dla katalogu głównego .NET Framework to `Machine.config` i `Web.config`, które są przechowywane w katalogu `%SystemRoot%\Microsoft.net\Framework\Version\Config\Machine.config`. Plik `Machine.config` dodatkowo definiuje globalne ustawienia domyślne dla ustawień platformy .NET Framework (oprócz niektórych ustawień ASP.NET). Plik `Web.config` definiuje pozostałe ustawienia domyślne dla ASP.NET. Więcej informacji na temat konfigurowania .NET Framework i ASP.NET znaleźć można w rozdziale 8 „Uruchamianie aplikacji IIS” i w rozdziale 9 „Zarządzanie aplikacjami, pulami aplikacji i procesami roboczymi”.
- `ApplicationHost.config` to domyślny plik konfiguracji katalogu głównego serwera, który przechowywany jest w katalogu `%SystemRoot%\System32\Inetsrv\Config`. Plik ten kontroluje globalną konfigurację usługi IIS. W rozdziale 5 zamieszczono więcej informacji na temat konfigurowania serwerów IIS.
- Domyślnym plikiem konfiguracji katalogu głównego witryny sieci Web jest plik `Web.config`. Plik ten przechowywany jest w katalogu głównym witryny Web, do której jest stosowany i kontroluje zachowanie witryny Web. W rozdziałach 8 i 9 znaleźć można więcej informacji na temat konfigurowania aplikacji IIS.
- Plik `Web.config` jest domyślnym plikiem konfiguracji dla katalogów zawartości wysokiego poziomu lub dla podkatalogów zawartości. Plik ten jest przechowywany w katalogu zawartości, do którego jest stosowany i kontroluje działanie tego poziomu hierarchii zawartości oraz poziomów znajdujących się poniżej. W rozdziale 6 znaleźć można dodatkowe informacje na temat konfigurowania katalogów zawartości.

W niektórych przypadkach zachodzi potrzeba umieszczania pliku `config` w innym pliku konfiguracyjnym (`config`). W tym celu można posłużyć się atrybutem `configSource` i odnieść się do pliku `config` zawierającego ustawienia, które mają być użyte. Aktualnie plik `config`, do którego następuje odniesienie, musi znajdować się w tym samym katalogu, co pierwotny plik `config`. Warto zwrócić uwagę, że takie działanie można zmienić tak, aby używane pliki `config` mogły znajdować się w innych katalogach. Działanie takie ilustruje poniższy przykład zaczerpnięty z pliku `ApplicationHost.config`:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- applicationHost.config -->
<configuration>
  <system.webServer>
    <httpErrors    <error statusCode="401"
prefixLanguageFilePath="%SystemDrive%\
inetpub\custerr" path="401.htm" />    <error statusCode="403"
```

```

prefixLanguageFilePath="%SystemDrive%\
inetpub\custerr" path="403.htm" /> <error statusCode="404"
prefixLanguageFilePath="%SystemDrive%\
inetpub\custerr" path="404.htm" /> <error statusCode="405"
prefixLanguageFilePath="%SystemDrive%\
inetpub\custerr" path="405.htm" /> <error statusCode="406"
prefixLanguageFilePath="%SystemDrive%\
inetpub\custerr" path="406.htm" /> <error statusCode="412"
prefixLanguageFilePath="%SystemDrive%\
inetpub\custerr" path="412.htm" /> <error statusCode="500"
prefixLanguageFilePath="%SystemDrive%\
inetpub\custerr" path="500.htm" /> <error statusCode="501"
prefixLanguageFilePath="%SystemDrive%\
inetpub\custerr" path="501.htm" /> <error statusCode="502"
prefixLanguageFilePath="%SystemDrive%\
inetpub\custerr" path="502.htm" />
</httpErrors>
</system.webServer>
</configuration>

```

W tym przykładzie elementy dotyczące błędów określają, w jaki sposób powinny być obsługiwane pewne typy kodów statusu błędów HTTP. Jeśli zachodzi potrzeba dostosowania obsługi błędów serwera, można rozszerzyć lub zmodyfikować wartości domyślne w oddzielnym pliku config zamieszczonym w pliku ApplicationHost.config. W tym celu należy zmodyfikować plik ApplicationHost.config tak, aby wskazać dodatkowy plik config, jak w poniższym przykładzie:

```

<?xml version="1.0" encoding="UTF-8"?>
<!-- applicationHost.config -->
<configuration>
  <system.webServer>
    <httpErrors configSource=errorMode.config />
  </configuration>

```

Następnie należy utworzyć plik errorMode.config i zapisać go w tym samym katalogu, co plik ApplicationHost.config. Poniżej zaprezentowany został przykładowy plik errorMode.config:

```

<?xml version="1.0" encoding="UTF-8"?>
<!-- errorMode.config -->

<configuration>
  <system.webServer>
    <httpErrors> <error statusCode="401"
prefixLanguageFilePath="%SystemDrive%\inetpub\
custerr" path="401.htm" /> <error statusCode="403"
prefixLanguageFilePath="%SystemDrive%\inetpub\
custerr" path="403.htm" /> <error statusCode="404"
prefixLanguageFilePath="%SystemDrive%\inetpub\
custerr" path="404.htm" /> <error statusCode="405"
prefixLanguageFilePath="%SystemDrive%\inetpub\
custerr" path="405.htm" /> <error statusCode="406"

```

```

prefixLanguageFilePath="%SystemDrive%\inetpub\
custerr" path="406.htm" /> <error statusCode="412"
prefixLanguageFilePath="%SystemDrive%\inetpub\
custerr" path="412.htm" /> <error statusCode="500"
prefixLanguageFilePath="%SystemDrive%\inetpub\
custerr" path="500.htm" /> <error statusCode="501"
prefixLanguageFilePath="%SystemDrive%\inetpub\
custerr" path="501.htm" /> <error statusCode="502"
prefixLanguageFilePath="%SystemDrive%\inetpub\
custerr" path="502.htm" />
</httpErrors>
</system.webServer>
</configuration>

```

Jeśli przeprowadzane zostały takie lub innego rodzaju modyfikacje plików konfiguracji, nie trzeba pamiętać o ponownym uruchamianiu IIS lub usług powiązanych z IIS. Usługi IIS automatycznie uwzględniają zmiany i zaczynają je stosować. W tych przykładach można zauważyć, że opracowywana była sekcja `system.webServer` pliku konfiguracyjnego. Podobnie, jak w przypadku plików definicji schematu, wszystkie ustawienia są zdefiniowane wewnątrz określonych sekcji konfiguracyjnych. Chociaż sekcje nie mogą być zagnieżdżane, sekcja może istnieć wewnątrz grupy sekcji, a ta grupa sekcji może być z kolei zawarta w nadrzędnej grupie sekcji. Grupa sekcji jest po prostu kontenerem logicznie powiązanych sekcji.

W pliku `ApplicationHost.config` grupy sekcji i poszczególne sekcje są definiowane w elemencie `configSections`. Element `configSections` kontroluje rejestrację sekcji. Każda sekcja należy do jednej grupy sekcji. Domyślnie plik `ApplicationHost.config` zawiera następujące grupy sekcji:

- **system.applicationHost** Grupa definiuje następujące sekcje: `applicationPools`, `configHistory`, `customMetadata`, `listenerAdapters`, `log`, `sites` i `webLimits`.
- **system.webServer** Grupa definiuje następujące sekcje: `asp`, `caching`, `cgi`, `defaultDocument`, `directoryBrowse`, `globalModules`, `handlers`, `httpCompression`, `httpErrors`, `httpLogging`, `httpProtocol`, `httpRedirect`, `httpTracing`, `isapiFilters`, `modules`, `odbcLogging`, `serverRuntime`, `serverSideInclude`, `staticContent`, `urlCompression`, i `validation`. Zawiera podgrupy dotyczące bezpieczeństwa (`security`) i śledzenia (`tracing`).
- **system.webServer.security** Podgrupa `system.webServer`, która definiuje następujące sekcje: `access`, `applicationDependencies`, `authorization`, `ipSecurity`, `isapiCgiRestriction` i `requestFiltering`. Zawiera podgrupę uwierzytelnienia.
- **system.webServer.security.authentication** Podgrupa `system.webServer.security`, która definiuje następujące sekcje: `anonymousAuthentication`, `basicAuthentication`, `clientCertificateMappingAuthentication`, `digestAuthentication`, `iisClientCertificateMappingAuthentication` i `windowsAuthentication`.
- **system.webServer.security.tracing** Podgrupa `system.webServer.security`, która definiuje sekcje `traceFailedRequests` i `traceProviderDefinitions`.

W pliku `ApplicationHost.config` grupy sekcji i poszczególne sekcje są zdefiniowane w następujący sposób:

```

<configSections>
<sectionGroup name="system.applicationHost">
<section name="applicationPools" allowDefinition="AppHostOnly"

```

```

overrideModeDefault="Deny" />
  <section name="configHistory" allowDefinition="AppHostOnly"
overrideModeDefault="Deny" />
  <section name="customMetadata" allowDefinition="AppHostOnly"
overrideModeDefault="Deny" />
  <section name="listenerAdapters" allowDefinition="AppHostOnly"
overrideModeDefault="Deny" />
  <section name="log" allowDefinition="AppHostOnly"
overrideModeDefault="Deny" />
  <section name="sites" allowDefinition="AppHostOnly"
overrideModeDefault="Deny" />
  <section name="webLimits" allowDefinition="AppHostOnly"
overrideModeDefault="Deny" />
</sectionGroup>
<sectionGroup name="system.webServer">
...
</sectionGroup>
</configSections>

```

W pliku Machine.config można znaleźć także definicje grup sekcji i poszczególnych sekcji. Są one podobne do używanych w pliku ApplicationHost.config, ale są stosowane do konfigurowania platformy .NET Framework i niektórych ustawień ASP.NET. Podczas pracy z plikami config trzeba pamiętać, że sekcja jest podstawową jednostką instalacji, blokowania, wyszukiwania i przechowywania ustawień konfiguracji. Każda sekcja ma atrybut nazwy oraz opcjonalne atrybuty allowDefinition i overrideModeDefault. Atrybut nazwy określa unikatową nazwę sekcji. Atrybut allowDefinition określa poziom, na którym sekcja może być zdefiniowana:

- **Everywhere** Sekcja może być definiowana w dowolnym pliku konfiguracyjnym zawierającym katalogi mapowane do katalogów wirtualnych, które nie są katalogami głównymi aplikacji i ich podkatalogami.
- **MachineOnly** Sekcja może być definiowana tylko w pliku ApplicationHost.config lub Machine.config. Ponieważ jest to ustawienie domyślne, sekcja, która nie ma atrybutu allowDefinition, automatycznie używa tego ustawienia.
- **MachineToWebRoot** Sekcja może być definiowana tylko w pliku konfiguracyjnym Machine.config bądź Web.config katalogu głównego .NET Framework lub w pliku ApplicationHost.config.
- **MachineToApplication** Sekcja może być definiowana jedynie w pliku konfiguracyjnym Machine.config bądź Web.config katalogu głównego .NET Framework, w pliku ApplicationHost.config lub w plikach Web.config katalogów głównych aplikacji.
- **AppHostOnly** Sekcja może być definiowana tylko w plikach Web.config katalogów głównych aplikacji.

Atrybut OverrideModeDefault definiuje domyślny stan zablokowania sekcji. Zasadniczo oznacza to, że kontroluje on, czy sekcja jest zablokowana do poziomu, na którym jest zdefiniowana lub czy może być zastępowana przez niższe poziomy hierarchii konfiguracji. Jeśli ten atrybut nie jest ustawiony, wartość domyślna wynosi Allow (Zezwalaj). W przypadku wartości Allow pliki konfiguracji niższego poziomu mogą zastępować ustawienia odnośnej sekcji. W przypadku wartości Deny (Odmawiaj), pliki konfiguracji niższego poziomu nie

mogą zastępować ustawień odnośnej sekcji. Zgodnie z opisem zamieszczonym w rozdziale 5, znaczniki lokalizacji używane są zazwyczaj do blokowania lub odblokowywania sekcji dla określonych witryn sieci Web lub aplikacji.

Ponieważ kompletne ustawienia konfiguracji serwera oraz powiązanych z nim witryn i aplikacji są przechowywane w plikach konfiguracji, można w prosty sposób utworzyć kopię zapasową lub powielić konfigurację serwera. Utworzenie kopii zapasowej serwera jest prostą operacją i polega na utworzeniu kopii plików konfiguracyjnych. Podobnie powielenie konfiguracji serwera na innym serwerze sprowadza się do skopiowania źródłowych plików konfiguracji do prawidłowej lokalizacji na innym serwerze.

Wymagania sprzętowe IIS 7.0

Zanim rozpocznie się instalowanie usług IIS 7.0, należy starannie zaplanować architekturę serwera. Częścią tego planowania jest dokładna ocena wstępnych wymagań i sprzętu, który ma być używany. Usługi nie są już tylko prostym rozwiązaniem utrzymywania witryn sieci Web, tak jak było to do tej pory. Usługi te obecnie udostępniają podstawową infrastrukturę utrzymywania serwerów i aplikacji sieci Web oraz oprogramowania Windows SharePoint Services.

Poradniki doboru sprzętu dla serwerów internetowych różnią się znacznie od tych, które pomagają wybrać inne typy serwerów. Dostawca usług utrzymywania sieci Web może obsługiwać wiele witryn na tym samym komputerze oraz może także oferować usługę określającą poziom dostępności i wymaganą wydajność. Z drugiej strony obciążona witryna e-commerce może składać się z dedykowanego serwera Web lub nawet wielu serwerów równoważących obciążenie. Tak więc serwery internetowe są używane w różnorodnych warunkach i mogą być współużytkowanymi lub dedykowanymi serwerami. Poniżej wymienione zostały niektóre porady ułatwiające dobór sprzętu serwera:

- **Pamięć** Wielkość wymaganej pamięci RAM (Random Access Memory) zależy od wielu czynników, wliczając w to wymagania dla innych usług, rozmiar plików zawartości, do których najczęściej uzyskiwany jest dostęp czy wymagania dla pamięci RAM wnoszone przez aplikacje Web. W przypadku większości instalacji zaleca się używanie co najmniej 1 GB pamięci RAM. Serwery o dużych woluminach powinny mieć od 2 do 4 GB pamięci RAM. Większa ilość pamięci RAM pozwala na buforowanie większej liczby plików, co zmniejsza liczbę żądań skierowanych do dysku. Dla wszystkich instalacji IIS rozmiar pliku stronicowania systemu operacyjnego powinien co najmniej mieć wielkość równą pamięci RAM na serwerze.

Uwaga Nie należy zapominać, że dodanie pamięci fizycznej powoduje również zwiększenie wirtualnego stronicowania. Uwzględniając to należy upewnić się, że plik Pagefile.sys znajduje się na odpowiednim dysku – który ma odpowiednią przestrzeń dyskową do przechowywania zwiększonego pliku stronicowania i który zapewni optymalną wydajność operacji wejścia/wyjścia (I/O).

Dodatkowe źródła Szczegółowe informacje na temat zarządzania pamięcią i optymalizowania wydajności znaleźć można w rozdziale 12 „Dostosowywanie wydajności, monitorowanie i śledzenie”.

- **CPU** CPU przetwarza instrukcje odebrane przez komputer. Częstotliwość zegara CPU i wielkość magistrali danych określa prędkość przekazywania informacji pomiędzy CPU, RAM magistralami systemu. Statyczna zawartość, taka jak HTML czy obrazy, wprowadza niewielkie obciążenie dla procesora i standardowo zalecana konfiguracja powinna być wystarczająca.

Szybszy zegar procesora i zwiększenie liczby procesorów zwiększa skalowalność wydajności serwera Web, w szczególności dla witryn, które są zależne od dynamicznej zawartości. 32-bitowa wersja systemu Windows uruchomiona może być na procesorze Intel x86 lub kompatybilnym sprzęcie. 64-bitowe wersje systemów Windows uruchamiane są na procesorach rodziny x64 firmy AMD i Intel, wliczając w to AMD64 czy Intel Extended Memory 64 Technology (Intel EM64T). Usługi IIS zapewniają dobrą wydajność na procesorach Intel Xeon, AMD Opteron czy AMD Athlon. Każdy z tych procesorów zapewnia dobry punkt startowy dla typowego serwera IIS. Znaczące zwiększenie wydajności można uzyskać stosując dużą pamięć podręczną procesora (cache). Warto przyglądać się dostępnym opcjom pamięci podręcznej L1, L2 i L3 – większy bufor może znacznie poprawić ogólną wydajność systemu.

- **SMP** Usługi IIS obsługują symetryczną wieloprocesorowość (SMP) i dla zwiększenia wydajności można używać dodatkowych procesorów. Pojedynczy procesor powinien być wystarczający, jeśli w systemie działają jedynie usługi IIS i nie jest obsługiwana zawartość dynamiczna lub szyfrowanie. Jeśli jednak usługi IIS są uruchamiane wraz z innymi usługami, jak Microsoft SQL Server czy Microsoft Exchange Server, w systemie należy stosować kilka procesorów.
- **Dyski** Wielkość potrzebnego magazynu danych zależy od rozmiarów plików zawartości i liczby obsługiwanych witryn. W systemie musi być wystarczająco dużo przestrzeni dyskowej do przechowywania wszystkich danych, obszarów roboczych, plików systemowych i pamięci wirtualnej. Przepustowość systemu I/O dysków jest tak samo ważna, jak pojemność. Chociaż system I/O dysku rzadko jest wąskim gardłem w przypadku witryn sieci Web publicznego Internetu, to mówiąc ogólnie, szerokość pasma ogranicza przepustowość. Dla witryn o dużej szerokości pasma powinno się rozważyć stosowanie sprzętowych macierzy RAID (Redundant Array of Independent Disks) przy użyciu miedzianych lub światłowodowych kanałów w oparciu o urządzenia SCSI (Small Computer System Interface).
- **Ochrona danych** Należy zapobiegać nieoczekiwanym awariom dysków przy użyciu macierzy RAID, chyba że rozwiązanie dopuszcza wielogodzinne przerwy w pracy. Sprzętowe instalacje macierzy RAID są zawsze rozwiązaniami lepszymi, niż implementacje programowe. Macierz RAID 0 (dyski rozłożone bez parzystości) zapewnia optymalną wydajność odczytu/zapisu, jeśli jednak jeden z dysków ulega awarii, usługi IIS przestaną działać, aż nastąpi wymiana dysku i przywrócenie zawartości z kopii zapasowej. Z tego względu nie jest to zalecane rozwiązanie. Macierz RAID 1 (dyski lustrzane) tworzy drugą kopię danych na oddzielnym dysku fizycznym, co umożliwia serwerowi wykonywanie operacji, jeśli dysk ulega awarii, a także, kiedy kontroler RAID odbudowuje wymieniony po awarii dysk. Macierz RAID 5 (dyski rozłożone z parzystością) umożliwia dobrą ochronę danych w przypadku awarii pojedynczego dysku, ale charakteryzuje się nie najlepszą wydajnością operacji zapisu. Warto pamiętać, że jeśli w systemie są skonfigurowane nadmiarowe serwery dla równoważenia obciążenia, macierz RAID nie musi być potrzebna. W przypadku równoważenia obciążenia dodatkowe serwery zapewniają potrzebną odporność na uszkodzenia.
- **UPS** Niespodziewane zaniki zasilania i przepięcia mogą być przyczyną poważnych uszkodzeń sprzętu. Aby temu zapobiec, należy stosować zasilacze UPS (Uninterruptible Power Supply). Prawidłowo skonfigurowany system UPS umożliwia automatyczne wyłączenie systemu operacyjnego serwera, w przypadku braku zasilania, i co ważne dla utrzymania integralności systemu, nastąpi prawidłowe zatrzymanie serwerów, których kontrolery pamięci podręcznej dla zapisu nie mają zainstalowanej baterii dla podtrzymania kopii zapasowej. Profesjonalni dostawcy usług hostingowych oferują często systemy UPS, które zapewniają ciągłe podtrzymanie zasilania, nawet przy długotrwałych przerwach.

Jeśli podczas doboru sprzętu uwzględnione są powyższe porady, najprawdopodobniej sprzęt nie będzie przyczyną nieprawidłowego działania usług IIS.

Usługi IIS 7.0 a system Windows

Usługi IIS 7.0 są dostępne dla systemów Windows zarówno w wersji serwerowej, jak i dla stacji roboczej. W systemie Windows Vista usługi IIS 7.0 udostępniają administratorom i projektantom sieci Web kompletną platformę budowania i testowania dynamicznych witryn i aplikacji sieci Web. Usługi IIS 7.0 uruchomione w systemie Windows Vista umożliwiają także aktywację procesu, zarządzanie procesem i udostępniają potrzebną infrastrukturę HTTP tworzenia aplikacji bazujących na WCF.

Zgodnie ze szczegółowym opisem zamieszczonym w rozdziale 2, sposób działania usług IIS 7.0 w systemie Windows Vista zależy od używanej wersji systemu Windows Vista. W przypadku wersji Windows Vista Starter i Home Basic usługi IIS 7.0 nie mogą być używane do utrzymywania witryn i aplikacji sieci Web lub oprogramowania Windows SharePoint Services. Dla tych wersji dostępny jest ograniczony zestaw funkcji usług IIS, takich jak składniki Windows Activation Service, które są używane do włączenia aplikacji bazujących na WCF. Użytkownicy, którzy instalują aplikacje WCF nie muszą instalować tych składników. Potrzebne składniki instalowane są automatycznie przez WCF. W przypadku tych wersji jednocześnie wykonywanie żądania ograniczone jest dla usług IIS do trzech, co oznacza, że aplikacja lub grupa uruchomionych aplikacji, poprzez zainstalowane składniki usług IIS, może wykonywać maksymalnie trzy jednocześnie żądania dotyczące zawartości sieci Web.

W przypadku wersji Windows Vista Home Premium dostępnych jest większość funkcji usług IIS 7.0 wymaganych do projektowania witryny sieci Web. Dostępne funkcje powinny umożliwiać administratorom i programistom (zajmujący się tematem hobbistycznie lub dorywczo) tworzenie i testowanie dynamicznych witryn i aplikacji sieci Web. Nie są jednak dostępne różne zaawansowane funkcje, jak zaawansowane uwierzytelnienie składników, zaawansowane logowanie składników czy składniki serwera FTP. Podobnie jak dla wersji Starter i Home Basic, w przypadku wersji Vista Home Premium ograniczenie wykonywania jednoczesnych żądań wynosi trzy, co oznacza, że uruchomione aplikacje poprzez zainstalowane składniki usług IIS mogą wykonywać jednocześnie trzy żądania dotyczące zawartości sieci Web.

Dla wersji Windows Vista Business, Enterprise i Ultimate dostępne są wszystkie funkcje usług IIS 7.0. Oznacza to, że administratorzy i projektanci (zajmujący się tematem zawodowo) dysponują wszystkim, co potrzebne jest do projektowania, tworzenia i testowania witryn i aplikacji sieci Web. Dla tych wersji systemu Windows Vista ograniczenie liczby wykonywanych jednoczesnych żądań wynosi 10, co oznacza, że użytkownik lub uruchomione aplikacje za pośrednictwem składników IIS mogą wykonać do 10 jednoczesnych żądań dotyczących zawartości sieci Web.

W przypadku serwerowych wersji systemu Windows usługi IIS mogą być używane do utrzymywania serwerów sieci Web, aplikacji internetowych i oprogramowania Windows SharePoint Services. Dla wszystkich wersji systemu Windows Server 2008 dostępne są wszystkie funkcje usług IIS 7.0. W systemach operacyjnych Windows Server usługi IIS 7.0 nie mają ograniczenia liczby wykonywanych żądań, co oznacza, że za pośrednictwem usług IIS 7.0 wykonywana może być nieograniczona liczba jednoczesnych żądań.

Narzędzia i techniki administracji sieci Web

Dla administratorów sieci Web opracowanych zostało wiele sposobów zarządzania siecią Web i serwerami aplikacji. Najważniejsze narzędzia i techniki administracyjne omówione zostały w kolejnych rozdziałach.

Zarządzanie zasobami za pomocą najważniejszych narzędzi administracyjnych

Do zarządzania zasobami sieci Web udostępnionych zostało wiele narzędzi. W tabeli 1-2 wymienione zostały najważniejsze z tych narzędzi. Większość narzędzi dostępnych jest w menu Start/Programy/Narzędzia administracyjne. Wszystkie narzędzia wymienione w tabeli mogą służyć do zarządzania zasobami lokalnymi lub zdalnymi. Przykładowo, jeśli połączymy się z nowym komputerem w programie IIS Manager, możliwe będzie zdalne zarządzanie wszystkimi jego witrynami i usługami.

Tabela 1-2 Przegląd głównych narzędzi administracyjnych

Narzędzie administracyjne	Zastosowanie
Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory)	Zarządzanie kontami użytkowników, grup i komputerów domeny.
Computer Management (Zarządzanie komputerem)	Zarządzanie usługami, magazynami i aplikacjami. Węzeł Services And Applications (Usługi i aplikacje) umożliwia szybki dostęp do katalogów usługi indeksowania (Indexing Service) oraz witryn i serwerów IIS.
Data Sources (ODBC) [Źródła danych]	Konfigurowanie i zarządzanie źródłami danych ODBC (Open Database Connectivity) i sterownikami. Źródła danych łączą fronton sieci Web z wewnętrzną bazą danych.
DNS	Publiczne witryny internetowe muszą mieć w pełni kwalifikowane nazwy domen (FQDN), aby były poprawnie rozpoznawane w przeglądarkach. Przystawka administracyjna Domain Name System (DNS) jest używana do zarządzania konfiguracją serwerów DNS systemu Windows.
Event Viewer (Podgląd zdarzeń)	Przeglądanie i zarządzanie dziennikami zdarzeń i systemowymi. Śledzenie zdarzeń systemowych pozwala uzyskać informacje, kiedy występują problemy.
Internet Information Services (IIS) 6.0 Manager [Menedżer internetowych usług informacyjnych (IIS) 6.0]	Zarządzanie zasobami serwerów i aplikacji sieci Web, które zostały zaprojektowane dla usług IIS 6. Narzędzie to dołączone zostało jedynie dla zapewnienia kompatybilności z poprzednimi rozwiązaniami.

Tabela 1-2 Przegląd głównych narzędzi administracyjnych

Narzędzie administracyjne	Zastosowanie
Internet Information Services (IIS) Manager [Menedżer internetowych usług informacyjnych]	Zarządzanie zasobami serwerów i aplikacji sieci Web, które zostały zaprojektowane dla usług IIS 7.0.
Web Management Service (WMSVC)	Umożliwienie używania narzędzia IIS Manager do zarządzania zasobami serwerów i aplikacji sieci Web na serwerach zdalnych.
Reliability and Performance Monitor (monitor niezawodności i wydajności)	Śledzenie niezawodności i wydajności systemu w celu wskazania występujących w tym zakresie problemów.
Services (usługi)	Przeglądanie informacji o usługach, uruchamianie i zatrzymywanie usług systemowych oraz konfigurowanie logowania i automatycznego przywracania usług.

Podczas dodawania usług do serwera narzędzia potrzebne do ich zarządzania są instalowane automatycznie. Jeśli zachodzi potrzeba zdalnego zarządzania tymi serwerami, narzędzia te mogą nie być zainstalowane na stacji roboczej i w takim przypadku należy je wcześniej zainstalować.

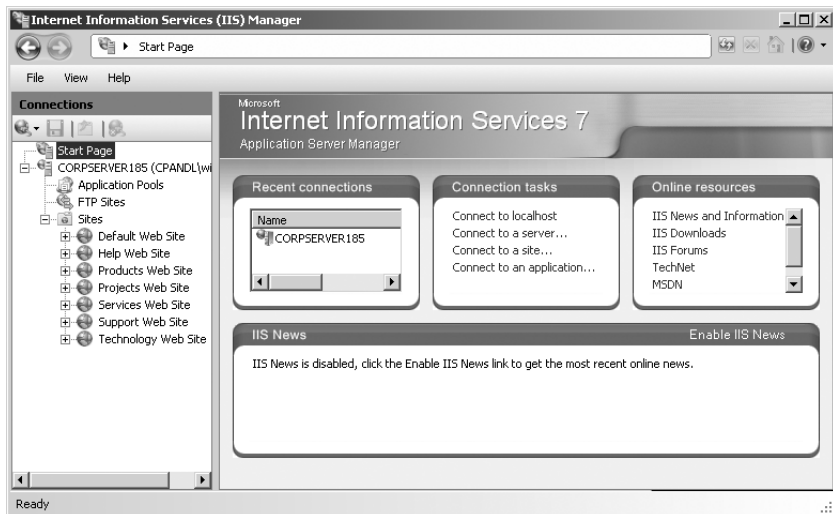
Techniki administracji sieci Web

Administratorzy sieci Web dysponują wieloma możliwościami w zakresie zarządzania usługami IIS. Najważniejsze narzędzia administracyjne to:

- IIS Manager (InetMgr.exe)
- Obiekty IIS Administration udostępniane są poprzez dostawcę IIS 7.0 WMI
- Narzędzie administracyjne wiersza poleceń IIS (AppCmd.exe)

Narzędzie IIS Manager udostępnia standardowy interfejs administracji dla usług IIS. W celu uruchomienia programu IIS Manager należy kliknąć menu Start/Wszystkie programy/ Narzędzia administracyjne, a następnie opcję Internet Information Services (IIS) Manager [Menedżer internetowych usług informacyjnych (IIS)]. Po uruchomieniu narzędzie IIS Manager wyświetla stronę startową pokazaną na rysunku 1-1 i automatycznie łączy się z lokalną instalacją IIS, jeśli ta jest dostępna. Na stronie startowej umieszczone są następujące opcje:

- **Connect to localhost (Połącz z localhost)** Opcja umożliwia połączenie z instalacją IIS na komputerze lokalnym
- **Connect to a server (Połącz z serwerem)** Opcja umożliwia połączenie z serwerem zdalnym
- **Connect to a site (Połącz z witryną)** Opcja umożliwia połączenie z określoną witryną sieci Web na wyznaczonym serwerze Web
- **Connect to an application (Połącz z aplikacją)** Opcja umożliwia połączenie z określoną aplikacją sieci Web na wyznaczonym serwerze i witrynie



Rysunek 1-1 Za pomocą programu IIS Manager można uzyskać dostęp do serwerów, witryn i aplikacji.

Jak było poprzednio nadmienione, dostęp zdalny do serwera IIS jest kontrolowany przez usługę WMSVC. Po zainstalowaniu i uruchomieniu usługi WMSVC na serwerze IIS, usługa ta nasłuchuje na porcie 8172 wszystkie nieprzypisane adresy IP i umożliwia nawiązywanie połączeń zdalnych autoryzowanych kont użytkownika. Z serwerem zdalnym można połączyć się stosując poniższą procedurę:

1. W drzewie konsoli programu Internet Information Services (IIS) Manager kliknąć węzeł Start Page (Strona startowa), a następnie kliknąć opcję Connect To A Server (Połącz z serwerem). Uruchomiony zostanie kreator Connect To A Server.
2. W polu tekstowym Server Name (Nazwa serwera) wpisać lub wybrać nazwę serwera. W przypadku serwera internetowego wpisać nazwę FQDN serwera, jak na przykład `www.adatum.com`. W przypadku serwera sieci lokalnej wpisać nazwę komputera, jak na przykład `WEBSVR87`. Port 80 jest domyślnym portem połączeń. W razie potrzeby można wprowadzić numer portu, z którym ma nastąpić połączenie. Przykładowo, jeśli zachodzi potrzeba połączenia z serwerem na porcie 8080, należy po nazwie serwera wpisać `:8080`, na przykład `WEBSVR87:8080`.
3. Po wpisaniu nazwy serwera (i opcjonalnie numeru portu) kliknąć przycisk Next (Dalej). Program IIS Manager będzie próbował zalogować się na serwerze przy użyciu bieżących poświadczeń użytkownika. Jeśli próba nawiązania połączenia nie powiedzie się, użytkownik powinien na stronie Provide Credentials (Wprowadź poświadczenia) wprowadzić odpowiednie poświadczenia, zanim kliknie przycisk Next. Kliknąć przycisk Finish (Zakończ), aby zakończyć nawiązywanie połączenia.

Wskazówka Jeśli w programie IIS Manager wyświetlony zostanie komunikat o błędzie połączenia informujący, że serwer zdalny nie akceptuje połączeń, należy zalogować się lokalnie lub poprzez pulpit zdalny. Po zalogowaniu należy sprawdzić, czy prawidłowo uruchomiona została usługa zarządzania Management Service. Dodatkowe informacje na ten temat znaleźć można w rozdziale 3 w podrozdziale „Włączanie i konfigurowanie administracji zdalnej”.

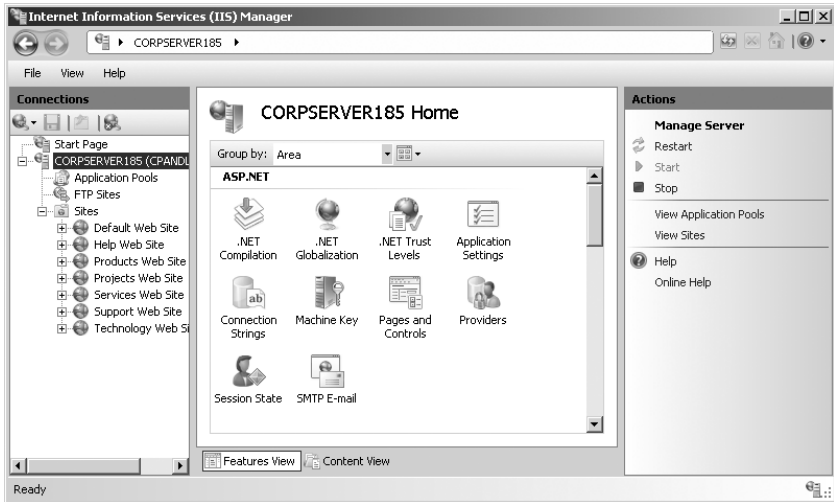
Z określoną witryną sieci Web na wyznaczonym serwerze można połączyć się stosując poniższą procedurę:

1. W drzewie konsoli programu Internet Information Services (IIS) Manager kliknąć węzeł Start Page, a następnie kliknąć opcję Connect To A Site (Połącz z witryną). Uruchomiony zostanie kreator Connect To A Site Wizard.
2. W polu Server Name (Nazwa serwera) wpisać lub wybrać nazwę serwera, jak na przykład TESTSVR22. W polu Site Name (Nazwa witryny) wpisać lub wybrać nazwę witryny sieci Web, z którą ma być nawiązane połączenie (na przykład Default Web Site).
3. Kliknąć przycisk Next. Program IIS Manager będzie próbował zalogować się na serwerze przy użyciu bieżących poświadczeń użytkownika. Jeśli próba nawiązania połączenia nie powiedzie się, użytkownik powinien na stronie Provide Credentials (Wprowadź poświadczenia) wprowadzić odpowiednie poświadczenia, zanim kliknie przycisk Next. Kliknąć przycisk Finish, aby zakończyć nawiązywanie połączenia.

Z określoną aplikacją na wyznaczonym serwerze i witrynie można połączyć się stosując poniższą procedurę:

1. W drzewie konsoli programu Internet Information Services (IIS) Manager kliknąć węzeł Start Page, a następnie kliknąć opcję Connect To An Application (Połącz z aplikacją). Uruchomiony zostanie kreator Connect To An Application Wizard.
2. W polu Server Name (Nazwa serwera) wpisać lub wybrać nazwę serwera, jak na przykład TESTSVR22. W polu Site Name (Nazwa witryny) wpisać lub wybrać nazwę witryny sieci Web, z którą ma być nawiązane połączenie (na przykład Default Web Site).
3. W polu Application Name (Nazwa aplikacji) wpisać lub wybrać relatywną ścieżkę do aplikacji sieci Web, z którą ma nastąpić połączenie (na przykład /MyApplication lub /Apps/Myapp).
4. Kliknąć przycisk Next. Program IIS Manager będzie próbował zalogować się na serwerze przy użyciu bieżących poświadczeń użytkownika. Jeśli próba nawiązania połączenia nie powiedzie się, użytkownik powinien na stronie Provide Credentials (Wprowadź poświadczenia) wprowadzić odpowiednie poświadczenia, zanim kliknie przycisk Next. Kliknąć przycisk Finish, aby zakończyć nawiązywanie połączenia.

Zgodnie z rysunkiem 1-2, dla usług IIS 7.0 program IIS Manager został zupełnie na nowo zaprojektowany. Poprzednio narzędzie było przystawką konsoli MMC (Microsoft Management Console), a teraz IIS Manager jest autonomiczną aplikacją o interfejsie podobnym do przeglądarki. Po połączeniu z serwerem, witryną lub aplikacją, program IIS Manager automatycznie łączy z tymi instalacjami podczas uruchamiania. Działanie takie można zmienić odłączając się od serwera zdalnego w programie IIS Manager. Dodatkowe informacje na temat używania programu IIS Manager znaleźć można w rozdziale 3.



Rysunek 1-2 Dla usług IIS 7.0 całkowicie został zmieniony interfejs programu IIS Manager.

W usługach IIS 7.0 wprowadzono koncepcję delegowania administracji. Za pomocą *delegowanej administracji* administrator może bezpiecznie przekazywać kontrolę administracyjną. Delegowana administracja umożliwia zarządzanie przez innych użytkowników różnymi poziomami hierarchii konfiguracji, takimi jak administratorzy witryn czy projektanci aplikacji. W przypadku standardowej konfiguracji domyślny stan delegowania zezwala na zapis większości ustawień konfiguracji tylko administratorom komputerów i ustawienia te trzeba zmieniać bezpośrednio, aby zezwolić na zapis innym użytkownikom. Więcej informacji na temat bezpieczeństwa i delegowania w usługach IIS zamieszczono w rozdziale 10 „Zarządzanie zabezpieczeniami serwera sieci Web”.

Program IIS Manager i inne narzędzia graficzne udostępniają wszystkie funkcje potrzebne do pracy z usługami IIS 7.0. W dalszym ciągu zdarzają się momenty, że zachodzi potrzeba używania wiersza poleceń, w szczególności, jeśli trzeba zautomatyzować instalację lub wykonać zadania administracyjne. Aby pomóc w korzystaniu z wiersza poleceń, dla usług IIS 7.0 opracowano narzędzie administracyjne wiersza poleceń (AppCmd.exe). Program AppCmd.exe przechowywany jest w katalogu `%SystemRoot%\System32\Inetsrv`. Domyślnie katalog ten nie znajduje się na ścieżce poleceń. Z tego względu należy albo dodać ten katalog do ścieżki domyślnej, albo zmieniać ten katalog każdorazowo, kiedy zachodzi potrzeba użycia tego narzędzia. Chwilowe dodanie tego katalogu do ścieżki domyślnej można wykonać za pomocą poniższego polecenia przy podniesionych uprawnieniach dla wiersza poleceń:

```
path %PATH%;%SystemRoot%\System32\inetsrv
```

Następnie można dodać ten katalog na stałe do ścieżki domyślnej wpisując następujące polecenie (przy podniesionych uprawnieniach dla wiersza poleceń):

```
setx PATH %PATH%;%SystemRoot%\System32\inetsrv
```

Uwaga Polecenie Path używane jest do chwilowej aktualizacji ścieżki poleceń dla bieżącego okna. Polecenie SETX PATH używane jest do trwałego zaktualizowania ścieżki poleceń również dla okien wiersza poleceń używanych w przyszłości.

W tabeli 1-3 zamieszczono podsumowanie podstawowego zestawu obiektów administracji dla narzędzia administracyjnego wiersza poleceń usług IIS.

Tabela 1-3 Obiekty administracji narzędzia administracji wiersza poleceń dla usług IIS

Typ obiektu	Opis	Polecenia powiązane
APP	Umożliwia tworzenie i zarządzanie ustawieniami aplikacji Web przy użyciu poleceń powiązanych: list, set, add oraz delete	list, set, add oraz delete
APPPPOOL	Umożliwia tworzenie i zarządzanie pulami aplikacji przy użyciu poleceń powiązanych: list, set, add, delete, start, stop oraz recycle	list, set, add, delete, start, stop oraz recycle
BACKUP	Umożliwia tworzenie i zarządzanie kopiami zapasowymi konfiguracji serwera przy użyciu poleceń powiązanych: list, add, delete oraz restore	list, add, delete oraz restore
CONFIG	Umożliwia zarządzanie ogólnymi ustawieniami konfiguracji przy użyciu poleceń powiązanych: list, set, search, lock, unlock, clear, reset oraz migrate	list, set, search, lock, unlock, clear, reset oraz migrate
MODULE	Umożliwia zarządzanie modułami IIS przy użyciu poleceń powiązanych: list, set, add, delete, install oraz uninstall	list, set, add, delete, install oraz uninstall
REQUEST	Umożliwia utworzenie listy bieżących żądań HTTP przy użyciu polecenia powiązanego list	List
SITE	Umożliwia tworzenie i zarządzanie witrynami wirtualnymi przy użyciu poleceń powiązanych: list, set, add, delete, start oraz stop	list, set, add, delete, start oraz stop
TRACE	Umożliwia zarządzanie śledzenia niepomysłnych żądań przy użyciu poleceń powiązanych: list, configure oraz inspect	list, configure oraz inspect
VDIR	Umożliwia tworzenie i zarządzanie wirtualnymi ustawieniami katalogu przy użyciu poleceń powiązanych: list, set, add oraz delete	list, set, add oraz delete
WP	Umożliwia utworzenie listy uruchomionych procesów roboczych przy użyciu polecenia powiązanego list	list

Podstawy działania przy użyciu narzędzia administracyjnego wiersza poleceń są proste. Większość obiektów administracji obsługuje poniżej wymienione polecenia podstawowe:

- **ADD** Tworzenie nowego obiektu o właściwościach wyspecyfikowanych przez użytkownika.
- **DELETE** Usunięcie określonego obiektu.
- **LIST** Wyświetlenie listy powiązanych obiektów. Opcjonalnie można wyspecyfikować obiekt unikatowy lub wpisać jeden bądź kilka parametrów, które mają być zgodne z właściwościami obiektu.
- **SET** Ustawienie parametrów wyspecyfikowanego obiektu. Niektóre obiekty obsługują inne polecenia, wliczając w to:
- **RECYCLE** Wyspecyfikowany obiekt zostaje usunięty, a następnie ponownie utworzony
- **START** Wyspecyfikowany obiekt zostaje uruchomiony, jeśli był zatrzymany
- **STOP** Wyspecyfikowany obiekt zostaje zatrzymany, jeśli jest uruchomiony lub aktywny

W celu wpisania polecenia należy posługiwać się następującą składnią ogólną:

```
appcmd Command <Object-type>
```

gdzie *Command* to działanie, które należy wykonać, takie jak list, add czy delete, a *Object-type* to obiekt, dla którego ma być wykonane działanie, takie jak app, site, or vdir. Przykładowo, jeśli zachodzi potrzeba wyświetlenia skonfigurowanych witryn na serwerze, należy wpisać poniższe polecenie (przy podniesionych uprawnieniach dla wiersza poleceń):

```
appcmd list site
```

Ponieważ narzędzie administracyjne wiersza poleceń usługi IIS akceptuje również formy liczby mnogiej nazw obiektów, takie jak apps, sites czy vdirs, można również posłużyć się następującym poleceniem:

```
appcmd list sites
```

W obu przypadkach jako wynik otrzymywana jest lista wszystkich skonfigurowanych witryn na serwerze wraz z ich powiązanymi właściwościami, jak na przykład:

```
SITE "Default Web Site" (id:1,bindings:http/*:80:,state:Started)
```

W rozdziale 4 „Zarządzanie usługami IIS 7.0 w wierszu poleceń” zamieszczono szczegółowe omówienie użycia tego narzędzia administracyjnego. Ponadto przykłady użycia tego narzędzia spotkać można w całej książce.

Rozdział 2

Instalowanie usług IIS 7.0 w przedsiębiorstwie

Przed zainstalowaniem produktu Internet Information Services (IIS) 7.0, należy starannie zaplanować typ komputera i architekturę administracji. Częścią planowania jest dokładne określenie używanych protokołów i pełnionych ról przez IIS oraz zmodyfikowanie sprzętu serwera i infrastruktury tak, aby spełniane były wymagania tych ról w odniesieniu do danego komputera. Powodzenie stosowania usług IIS 7.0 będzie istotnie zależne od zrozumienia sposobu, w jaki można używać oprogramowania i od możliwości zainstalowania oprogramowania w taki sposób, aby role te były obsługiwane.

Protokoły IIS 7.0

TCP/IP jest zestawem protokołów składających się z protokołu TCP (Transmission Control Protocol) i IP (Internet Protocol). Protokół TCP/IP jest wymagany dla komunikacji między sieciami oraz dla dostępu do sieci Internet. Protokół TCP funkcjonuje w warstwie transportu i jest protokołem połączeniowym zaprojektowanym do zapewnienia niezawodnej komunikacji pomiędzy dwoma końcowymi punktami. Protokół IP natomiast działa w warstwie sieci i jest protokołem międzysieciowym używanym w sieciach do routowania pakietów danych. W usługach IIS 7.0 używane są protokoły, które zbudowane są na protokołach TCP/IP:

- Hypertext Transfer Protocol (HTTP)
- Secure Sockets Layer (SSL)
- File Transfer Protocol (FTP)
- Simple Mail Transfer Protocol (SMTP)

HTTP i SSL

Protokół HTTP jest protokołem warstwy aplikacji, który umożliwia publikowanie statycznej i dynamicznej zawartości na serwerze przeglądanej w aplikacjach klienckich, takich jak Microsoft Windows Internet Explorer. Publikowanie dokumentów w sieci Web jest prostą operacją, polegającą na udostępnieniu dokumentu w odpowiednim katalogu na serwerze HTTP i przypisaniu mu odpowiednich uprawnień tak, aby aplikacja kliencka HTTP mogła uzyskać dostęp do tego dokumentu. Sesja protokołu HTTP działa w następujący sposób:

1. Aplikacja kliencka HTTP używa TCP do nawiązania połączenia z serwerem HTTP. Port domyślny, powszechnie używany do połączeń HTTP to port 80 protokołu TCP. Można również skonfigurować serwery, by używane były inne porty. Przykładowo port TCP 8080 jest popularną alternatywą dla portu 80 dla witryn, które mają mieć ograniczony dostęp.
2. Po nawiązaniu połączenia z serwerem, aplikacja kliencka HTTP żąda na serwerze strony sieci Web lub innego zasobu. W aplikacji klienckiej użytkownicy określają strony lub zasoby, do których chcą uzyskać dostęp, przy użyciu adresu sieci Web, nazywanego inaczej adresem URL (Uniform Resource Locator).

3. Serwer odpowiada na żądanie poprzez przesłanie klientowi żadanego zasobu i innych powiązanych plików, takich jak obrazy, które zostały wstawione do żadanego zasobu. Jeśli na serwerze włączona została funkcja HTTP Keep-Alive, połączenie protokołu TCP pomiędzy klientem a serwerem pozostaje otwarte, aby przyspieszyć proces przekazywania kolejnych żądań klienta. W przeciwnym razie połączenie TCP zostaje zamknięte, a podczas kolejnego żądania klient musi nawiązywać nowe połączenie.

Tak w skrócie przedstawia się istota działania HTTP. Protokół zaprojektowany został, by obsługiwać procesy dynamiczne i jest podstawą tworzenia sieci WWW (World Wide Web).

W przypadku protokołu HTTP można konfigurować dostęp do dokumentów tak, aby każdy mógł go uzyskać lub aby dokumenty były dostępne tylko dla autoryzowanych osób. Aby każdy mógł uzyskać dostęp do dokumentu, zabezpieczenia dokumentu należy tak skonfigurować, by klienci używali uwierzytelnienia typu Anonymous (anonimowo). W przypadku uwierzytelnienia typu Anonymous serwer HTTP loguje automatycznie użytkownika za pomocą konta guest (gość), takiego jak IUSR. W celu żądania autoryzacji przy uzyskiwaniu dostępu do dokumentu, należy skonfigurować zabezpieczenia dokumentu tak, aby uwierzytelnienie wymagane było przy użyciu jednego z dostępnych mechanizmów uwierzytelnienia, jak na przykład uwierzytelnienie typu Basic (podstawowe), przy którym użytkownik musi wprowadzić nazwę użytkownika i hasło.

W celu włączenia transferów protokołu HTTPS (Hypertext Transfer Protocol Secure) można używać protokołu SSL (Secure Sockets Layer). SSL jest protokołem internetowym używanym do szyfrowania informacji związanych z uwierzytelnieniem i danych przekazywanych pomiędzy klientami HTTP a serwerami HTTP. W przypadku SSL klienci HTTP łączą się ze stronami sieci Web przy użyciu adresów URL, które rozpoczynają się wyrażeniem *https://*. Prefiks *https* informuje, że klient HTTP próbuje nawiązać połączenie przy użyciu protokołu SSL. Port domyślny używany przy bezpiecznych połączeniach to port 443 protokołu TCP, a nie port 80. W rozdziale 10 „Zarządzanie zabezpieczeniami serwera sieci Web” znaleźć można dodatkowe informacje na temat protokołu SSL.

FTP

FTP jest protokołem warstwy aplikacji, który umożliwia aplikacjom klienckim pobieranie z serwerów zdalnych i wysyłanie plików do tych serwerów. Protokół FTP był wcześniej opracowany, niż protokół HTTP, a jego użycie można porównać do HTTP. W przypadku protokołu FTP można publikować pliki tak, aby klient mógł je pobierać, poprzez udostępnienie plików w odpowiednich katalogach na serwerze FTP i przypisanie plikom odpowiednich uprawnień tak, aby aplikacja kliencka FTP mogła uzyskać dostęp do dokumentu. W celu przesłania pliku na serwer FTP należy klienckiej aplikacji FTP przypisać uprawnienia do logowania się na serwerze i uzyskania dostępu do katalogu używanego do zapisywania plików.

Sesja protokołu FTP działa w następujący sposób:

1. Kliencka aplikacja FTP używa protokołu TCP do nawiązania połączenia z serwerem FTP. Port domyślny, powszechnie używany dla tych połączeń to port 21 protokołu TCP. Serwery FTP nasłuchują na tym porcie żądań połączeń przesłanych przez klientów. Po nawiązaniu połączenia pomiędzy klientem a serwerem, serwer przypisuje klientowi przypadkowy numer portu TCP z zakresu numerów powyżej 1023. To początkowe połączenie TCP (port 21 dla serwera i przypadkowy numer portu dla klienta) jest następnie używane do transmisji informacji sterujących protokołu FTP, takich jak polecenia wysłane od klienta do serwera i kody odpowiedzi przesłane przez serwer do klienta.

2. Następnie klient wysyła polecenie FTP do serwera na porcie 21 protokołu TCP. Standardowe polecenia FTP to GET służące do pobierania pliku, CD służące do zmiany katalogu, PUT służące do przekazywania plików na serwer i BIN służące do przełączenia w tryb binarny.
3. Kiedy klient rozpoczyna transfer danych z serwerem, serwer otwiera drugi port połączenia TCP, który będzie służył do przesyłu danych. Połączenie to korzysta z portu 20 protokołu TCP na serwerze i na kliencie z przypadkowo przypisanego portu powyżej 1023. Po zakończeniu przesyłania danych drugie połączenie przechodzi w stan oczekiwania, dopóki klient nie zainicjuje innego transferu danych lub przekroczony zostanie limit czasu otwartego połączenia.

Tak w skrócie przedstawia się zasada działania protokołu FTP. Jak widać obsługa protokołu FTP jest trochę bardziej skomplikowana, niż HTTP, ale w sumie jest dość prosta.

W praktyce Protokoły FTP i HTTP odróżniają się od siebie zasadniczo sposobem przekazywania plików. Protokół FTP transferuje pliki jako standardowy tekst lub w postaci binarnej. Protokół HTTP umożliwia przekazywanie do klienta formatu pliku, a taka funkcja pozwala klientowi na określenie, w jaki sposób obsługiwać plik. Jeśli klient potrafi bezpośrednio obsługiwać format pliku, będzie od razu wyświetlał zawartość pliku. Jeśli klient ma skonfigurowane pomocnicze aplikacje, jak na przykład przeglądarkę dokumentów PDF, klient może wywołać tę aplikację pomocniczą i za jej pomocą wyświetlić plik w oknie klienta. Składnikiem, który umożliwia klientom i serwerom HTTP określenie formatu plików, jest moduł obsługi protokołu MIME (Multipurpose Internet Mail Extensions). Za pomocą protokołu MIME serwer HTTP identyfikuje każdy plik na podstawie odpowiedniego typu MIME. Na przykład dokument HTML ma typ protokołu MIME określony jako text/html, a obraz GIF ma typ protokołu MIME określony jako image/gif.

Dla protokołu FTP można zezwolić na anonimowe przesyłanie plików, a także można skonfigurować ograniczenia przy pobieraniu czy przekazywaniu plików. Aby każdy mógł uzyskać dostęp do pliku, należy tak skonfigurować zabezpieczenia katalogu, by używane było uwierzytelnienie typu Anonymous. W przypadku uwierzytelnienia Anonymous, w celu pobrania bądź przekazania pliku, serwer FTP automatycznie loguje użytkownika przy użyciu konta gość. Jeśli ma być wymagana autoryzacja logowania i dostępu do katalogu, należy skonfigurować zabezpieczenia katalogu tak, aby wymagane było uwierzytelnienie przy użyciu jednej z dostępnych metod uwierzytelniania, takiej jak uwierzytelnienie typu Basic (podstawowe), przy którym użytkownik musi wprowadzić nazwę użytkownika i hasło, zanim będzie mógł zalogować się i pobrać bądź przekazać plik.

SMTP

SMTP jest protokołem warstwy aplikacji, który umożliwia aplikacjom klienckim przesyłanie wiadomości e-mail do serwera i umożliwia serwerom przesyłanie wiadomości e-mail do innych serwerów. Powiązany protokołem potrzebnym do pobierania wiadomości z serwera jest protokół POP3 (Post Office Protocol wersja 3). W przypadku usług IIS 6 zaimplementowana została pełna obsługa protokołów SMTP (Simple Mail Transfer Protocol) i POP3. Usługi IIS 7.0 nie zawierają obsługi tych protokołów.

W przypadku usług IIS 7.0 aplikacja sieci Web może przesyłać wiadomości e-mail w imieniu użytkownika za pomocą składnika SMTP E-mail platformy Microsoft ASP.NET. Sesja protokołu SMTP zainicjowana przez aplikację sieci Web działa w następujący sposób:

1. Aplikacja Web generuje wiadomość e-mail w konsekwencji odpowiednich działań użytkownika.
2. Składnik System.Net.Mail API (składnik ASP.NET) dostarcza wiadomość e-mail do działającego serwera SMTP lub przechowuje ją na dysku, aby dostarczyć ją później.
3. Podczas przesyłania poczty do serwera SMTP, serwer IIS używa portu 25 protokołu TCP w celu nawiązania połączenia. Protokół SMTP może być uruchomiony na komputerze lokalnym lub na innym komputerze.

Tak zasadniczo przedstawia się sposób używania SMTP przez aplikacje sieci Web. Firma Microsoft nie dostarcza innych funkcji związanych z pocztą e-mail, jako części usług IIS. Jednakże oddzielny składnik SMTP Server dołączony został jako funkcja opcjonalna, którą można instalować na komputerze działającym pod kontrolą systemu operacyjnego Windows Server.

Role usług IIS 7.0

Usługi IIS mogą być instalowane na platformach serwera lub stacji roboczej. Na stacji roboczej usługi IIS 7.0 mogą być używane do projektowania, tworzenia i testowania dynamicznych witryn i aplikacji sieci Web. W przypadku platformy serwera usługi IIS 7.0 mogą pełnić kilka innych ról:

- **Serwer aplikacji** Serwery aplikacji utrzymują aplikacje rozproszone zbudowane przy użyciu platform ASP.NET, Enterprise Services Network Support i Microsoft .NET Framework 3.0. Serwery aplikacji można instalować zarówno z obsługą, jak i bez obsługi Web Server (IIS). Jeśli serwer aplikacji instalowany jest bez obsługi Web Server (IIS), usługi aplikacji konfigurowane są poprzez podstawowe funkcje API serwera aplikacji i poprzez dodawanie bądź usuwanie usług ról. Ponieważ w serwerze brak składników konfiguracji i administracji usług IIS, nie będą dostępne najczęściej używane funkcje IIS i nie będzie można konfigurować serwera przy użyciu modułów usług IIS 7.0 czy zarządzać nim za pomocą narzędzi administracyjnych IIS 7.0. W celu uniknięcia tych ograniczeń należy instalować serwer aplikacji razem z obsługą Web Server (IIS), dzięki czemu będzie możliwe używanie funkcji IIS do lepszego zarządzania instalacją serwera aplikacji.
- **Serwer sieci Web** Serwery sieci Web używają usług wbudowanych w IIS 7.0 do utrzymywania witryn i aplikacji sieci Web. Witryny utrzymywane na serwerze sieci Web mogą mieć statyczne i dynamiczne zawartości. Aplikacje sieci Web utrzymywane na serwerze Web mogą być budowane przy użyciu platform ASP.NET i .NET Framework 3.0. Po zainstalowaniu serwera sieci Web można zarządzać jego konfiguracją za pomocą modułów i narzędzi administracyjnych usług IIS 7.0.
- **Serwer Microsoft Windows SharePoint Services** Na komputerach, na których uruchomiono oprogramowanie Windows SharePoint Services, usługi te umożliwiają współpracę zespołów poprzez łączenie osób i informacji. Serwer SharePoint Services jest zasadniczo serwerem sieci Web z uruchomioną pełną instalacją usług IIS i wykorzystuje zarządzane aplikacje, które udostępniają potrzebne funkcje dotyczące współpracy. Po zainstalowaniu oprogramowania SharePoint Services można zarządzać serwerem przy użyciu modułów i narzędzi administracyjnych usług IIS 7.0, a także za pomocą kilku narzędzi

specyficznych dla programu SharePoint, takich jak SharePoint Central Administration czy SharePoint Products and Technologies Configuration Wizard.

W tabeli 2-1 przedstawiono 75 funkcji konfiguracyjnych dostępnych dla trzech ról serwera podzielonych na 14 kategorii ogólnych. Każdy wpis dotyczący poszczególnej funkcji konfiguracyjnej ma jedną z następujących wartości:

- **Available (dostępna)** Wskazuje funkcję dostępną do wybrania podczas instalacji. Dostępne funkcje można dodawać w celu zoptymalizowania konfiguracji serwera.
- **Default (domyślna)** Wskazuje funkcję, która jest domyślnie wybrana do zainstalowania. Chociaż podczas instalowania istnieje możliwość usunięcia zaznaczenia funkcji domyślnych, w większości przypadków nie należy tego robić, ponieważ może to wpłynąć na wydajność serwera lub jego niezbędne funkcje podstawowe.
- **Included (dołączona)** Wskazuje dołączoną, ale nie wymienioną funkcję, która jest częścią rdzenia serwera IIS. W przypadku serwerów aplikacji, funkcje te są dołączane jedynie, jeśli wybrana została do zainstalowania obsługa Web Server (IIS). W przypadku Web Server i SharePoint Services Server funkcje te są dołączane automatycznie.
- **Not Installed (niezainstalowana)** Wskazuje niedostępną funkcję, która nie została zainstalowana jako część standardowej instalacji. W przypadku serwerów Web Server i SharePoint Services można te funkcje skonfigurować po instalacji poprzez włączenie odpowiednich modułów. W przypadku serwerów aplikacji funkcje te są konfigurowane po instalacji tylko, jeśli do zainstalowania wybrana została obsługa Web Server (IIS) lub zmodyfikowane są usługi ról skojarzone z zainstalowaną rolą serwera sieci Web.
- **Required (wymagana)** Wskazuje funkcję, która jest wymagana, aby zainstalować rolę serwera. Podczas działania program instalacyjny wybiera wymagane funkcje automatycznie.
- **N/A** Wskazuje funkcję, która nie jest dostępna lub która nie ma zastosowania w odniesieniu do danej roli serwera.
- **Web Common (wspólna dla sieci Web)** Wskazuje funkcję zainstalowaną domyślnie jako część wspólnych funkcji Web Server (IIS) serwera aplikacji.
- **WPASS Required (wymagana dla WPASS)** Wskazuje funkcję serwera aplikacji wymaganą dla obsługi WPASS (Windows Process Activation Service Support).

Tabela 2-1 Funkcje konfiguracyjne dla aplikacji i serwerów Web oraz komputerów z uruchomionym oprogramowaniem SharePoint Services

Funkcja	Serwer aplikacji	Serwer Web	Usługi SharePoint
.NET Framework 3.0			
.NET Framework 3.0	Wymagana	Dostępna	Wymagana
Obsługa serwera aplikacji			
Application Server Foundation	Domyślna	N/A	N/A
COM+ Network Access (dostęp do sieci COM+)	Dostępna	N/A	N/A

ciąg dalszy na stronie następnej

*Ciąg dalszy ze strony poprzedniej***Tabela 2-1** Funkcje konfiguracyjne dla aplikacji i serwerów Web oraz komputerów z uruchomionym oprogramowaniem SharePoint Services

Funkcja	Serwer aplikacji	Serwer Web	Usługi SharePoint
TCP Port Sharing (udostępnianie portów TCP)	Wymagana dla WPASS	N/A	N/A
Web Server (IIS) Support (obsługa serwera Web)	Dostępna	N/A	N/A
Funkcje projektowania aplikacji			
.NET Extensibility	Web Common; wymagana dla WPASS	Dostępna	Wymagana
ASP	Dostępna	Dostępna	Dostępna
ASP.NET	Web Common	Dostępna	Wymagana
CGI	Dostępna	Dostępna	Dostępna
ISAPI Extensions (rozszerzenia ISAPI)	Web Common	Dostępna	Wymagana
ISAPI Filters (filtry ISAPI)	Web Common	Dostępna	Wymagana
Server-Side Includes	Dostępna	Dostępna	Dostępna
Wspólne funkcje HTTP			
Default Document (dokument domyślny)	Web Common	Domyślna	Wymagana
Directory Browsing (przeoglądanie katalogów)	Web Common	Domyślna	Wymagana
HTTP Errors (błędy HTTP)	Web Common	Domyślna	Wymagana
HTTP Redirection (przeadresowanie HTTP)	Web Common	Dostępna	Dostępna
Static Content (zawartość statyczna)	Web Common	Domyślna	Wymagana
Obsługa transakcji rozproszonych			
Incoming Remote Transaction Support (obsługa przychodzących transakcji zdalnych)	Dostępna	N/A	N/A
Outgoing Remote Transaction Support (obsługa wychodzących transakcji zdalnych)	Dostępna	N/A	N/A
WS-Atomic Transaction Support (obsługa transakcji WSAT)	Dostępna	N/A	N/A

Tabela 2-1 Funkcje konfiguracyjne dla aplikacji i serwerów Web oraz komputerów z uruchomionym oprogramowaniem SharePoint Services

Funkcja	Serwer aplikacji	Serwer Web	Usługi SharePoint
Funkcje rozszerzone			
File Cache (bufor pliku)	Niezainstalowana	Niezainstalowana	Niezainstalowana
Managed Engine (mechanizm zarządzany)	Niezainstalowana	Niezainstalowana	Niezainstalowana
Token Cache (bufor tokenu)	Niezainstalowana	Niezainstalowana	Niezainstalowana
HTTP Trace (śląd HTTP)	Niezainstalowana	Niezainstalowana	Niezainstalowana
URI Cache (bufor URI)	Niezainstalowana	Niezainstalowana	Niezainstalowana
Usługa publikowania FTP			
FTP Management Console (konsola zarządzania FTP)	Niezainstalowana	Dostępna	Niezainstalowana
FTP Server (serwer FTP)	Niezainstalowana	Dostępna	Niezainstalowana
Funkcje dotyczące stanu i diagnostyki			
Custom Logging (rejestrwanie niestandardowe)	Niezainstalowana	Dostępna	Niezainstalowana
HTTP Logging (rejestrwanie HTTP)	Web Common	Domyślna	Wymagana
Logging Tools (narzędzia rejestrowania)	Web Common	Dostępna	Wymagana
ODBC Logging (rejestrwanie ODBC)	Niezainstalowana	Dostępna	Niezainstalowana
Request Monitor (monitor żądań)	Web Common	Domyślna	Wymagana
Tracing (śledzenie)	Web Common	Dostępna	Wymagana
Rdzeń serwera IIS			
Anonymous Authentication (uwierzytelnienie anonimowe)	Dołączona	Dołączona	Dołączona
Configuration Validation (walidacja konfiguracji)	Dołączona	Dołączona	Dołączona
HTTP Cache (bufor HTTP)	Dołączona	Dołączona	Dołączona
Protocol Support (obsługa protokołu)	Dołączona	Dołączona	Dołączona

Ciąg dalszy na stronie następczej

Ciąg dalszy ze strony poprzedniej

Tabela 2-1 Funkcje konfiguracyjne dla aplikacji i serwerów Web oraz komputerów z uruchomionym oprogramowaniem SharePoint Services

Funkcja	Serwer aplikacji	Serwer Web	Usługi SharePoint
Funkcje dotyczące wydajności			
Dynamic Content Compression (kompresja zawartości dynamicznej)	Web Common	Dostępna	Wymagana
Static Content Compression (kompresja zawartości statycznej)	Web Common	Domyślna	Wymagana
Funkcje dotyczące bezpieczeństwa			
Basic Authentication (uwierzytelnienie podstawowe)	Web Common	Dostępna	Wymagana
Client Certificate Mapping Authentication (uwierzytelnienie mapowania certyfikatu klienta)	Web Common	Dostępna	Dostępna
Digest Authentication (uwierzytelnienie szyfrowane)	Web Common	Dostępna	Wymagana
IIS Client Certificate Mapping Authentication	Web Common	Dostępna	Dostępna
IP and Domain Restrictions (ograniczenia IP i domeny)	Web Common	Dostępna	Dostępna
Request Filtering (filtrowanie żądania)	Web Common; Wymagana dla WPASS	Domyślna	Dostępna
URL Authorization (autoryzacja URL)	Web Common	Dostępna	Dostępna
Windows Authentication (uwierzytelnienie systemu Windows)	Web Common	Dostępna	Wymagana
Narzędzia zarządzania siecią Web			
IIS Management Console (konsola zarządzania IIS)	Domyślna	Domyślna	Wymagana
IIS Management Scripts and Tools (narzędzia i skrypty zarządzania IIS)	Web Common	Dostępna	Nie zainstalowana

Tabela 2-1 Funkcje konfiguracyjne dla aplikacji i serwerów Web oraz komputerów z uruchomionym oprogramowaniem SharePoint Services

Funkcja	Serwer aplikacji	Serwer Web	Usługi SharePoint
IIS Management Service (usługa zarządzania IIS)	Web Common	Dostępna	Niezainstalowana
IIS 6 Management Compatibility (zgodność zarządzania IIS 6)	Niezainstalowana	Dostępna	Wymagana
IIS Metabase Compatibility (zgodność metabazy IIS)	Niezainstalowana	Dostępna	Wymagana
IIS 6 WMI Compatibility (zgodność WMI IIS 6)	Niezainstalowana	Dostępna	Niezainstalowana
IIS 6 Scripting Tools (narzędzia tworzenia skryptów IIS 6)	Niezainstalowana	Dostępna	Niezainstalowana
IIS 6 Management Console (konsola zarządzania IIS 6)	Niezainstalowana	Dostępna	Niezainstalowana
Windows Activation Service			
.NET Environment (środowisko .NET)	Wymagana	Dostępna	Wymagana
Configuration APIs (interfejsy API konfiguracji)	Wymagana	Wymagana	Wymagana
Process Model (model procesu)	Wymagana	Wymagana	Wymagana
Obsługa WPASS (Windows Process Activation Service Support)			
HTTP Activation (aktywacja HTTP)	Wymagana dla WPASS	N/A	N/A
MSMQ Activation (aktywacja MSMQ)	Wymagana dla WPASS	N/A	N/A
Named Pipes Activation (aktywacja potoków nazwanych)	Dostępna	N/A	N/A
TCP Activation (aktywacja TCP)	Dostępna	N/A	N/A

Ciąg dalszy na stronie następczej

Ciąg dalszy ze strony poprzedniej

Tabela 2-1 Funkcje konfiguracyjne dla aplikacji i serwerów Web oraz komputerów z uruchomionym oprogramowaniem SharePoint Services

Funkcja	Serwer aplikacji	Serwer Web	Usługi SharePoint
Windows Process Activation Service Support (dodatkowe)			
Message Queuing Server (serwer kolejki wiadomości)	Wymagana dla WPASS	N/A	N/A
Non-HTTP Activation (aktywacje inne niż HTTP)	Wymagana dla WPASS	N/A	N/A
Windows SharePoint Services Support			
SharePoint Applications (aplikacje SharePoint)	N/A	N/A	Domyślna
SharePoint Management Tools (narzędzia zarządzania SharePoint)	N/A	N/A	Domyślna

Podczas konfigurowania serwerów aplikacji, serwerów sieci Web i oprogramowania SharePoint Services istotne jest zrozumienie, z czego dokładnie składa się platforma .NET Framework 3.0. Platforma Microsoft .NET Framework 3.0 jest modelem programowania zarządzanego kodu dla systemu Windows i łączy w sobie możliwości platformy .NET Framework 2.0 i czterech nowych technologii:

- **Windows CardSpace (WCS)** Zestaw technologii .NET dotyczących zarządzania tożsamością cyfrową. Windows CardSpace obsługuje dowolny system tożsamości cyfrowej i udostępnia użytkownikom spójną kontrolę swoich tożsamości cyfrowych. Tożsamość cyfrowa może być czymś tak prostym jak adres e-mail i hasło używane do zalogowania się w witrynie sieci Web lub może zawierać pełne informacje kontaktowe i logowania dotyczące użytkownika. Aplikacje klienckie wyświetlają każdą tożsamość cyfrową jako kartę informacyjną. Każda karta zawiera informacje na temat poszczególnej tożsamości cyfrowej, wliczając w to, jakich informacji kontaktowych potrzebuje dostawca, aby pobrać token zabezpieczeń tożsamości. Wybierając kartę i wysyłając ją do dostawcy, takiego jak Amazon czy Yahoo!, użytkownicy mogą potwierdzać swoją tożsamość i logować się do usług oferowanych przez witrynę.
- **Windows Communication Foundation (WCF)** Zestaw technologii .NET tworzenia i uruchamiania połączonych systemów. WCF obsługuje duży zestaw funkcji systemów rozproszonych w celu zapewnienia bezpiecznego, niezawodnego i transakcyjnego systemu przekazywania wiadomości wraz z umożliwieniem współdziałania. Serwery ustanawiają komunikację rozproszoną poprzez punkty końcowe usług (ang. service endpoints). Punkty końcowe usług mają adres, powiązanie określające sposób komunikowania się punktu końcowego i opis kontraktu, który określa, co przekazuje punkt końcowy.
- **Windows Presentation Foundation (WPF)** Zestaw technologii .NET budowania aplikacji o atrakcyjnych i sprawnych interfejsach użytkownika. WPF wspiera ścisłą integrację interfejsów użytkownika aplikacji, dokumentów i zawartości multimedialnych,

dzięki czemu projektanci mogą tworzyć zunifikowany interfejs dla wszystkich typów dokumentów i multimediów. Oznacza to, że aplikacja może używać tego samego interfejsu do wyświetlania formularzy, kontrolki, dokumentów o ustalonych formatach, dokumentów ekranowych, obrazów 2D i 3D, wideo i audio.

- **Windows Workflow Foundation (WF)** Zestaw technologii .NET budowania w systemach Windows aplikacji zarządzania procesami pracy (*ang. workflow*). WF udostępnia mechanizm reguł, który pozwala na modelowanie jednostek logiki aplikacji wewnątrz ogólnego procesu biznesowego. Oznacza to, że projektanci mogą używać WF do modelowania i implementowania potrzebnej logiki programowania od początku do końca procesu biznesowego.

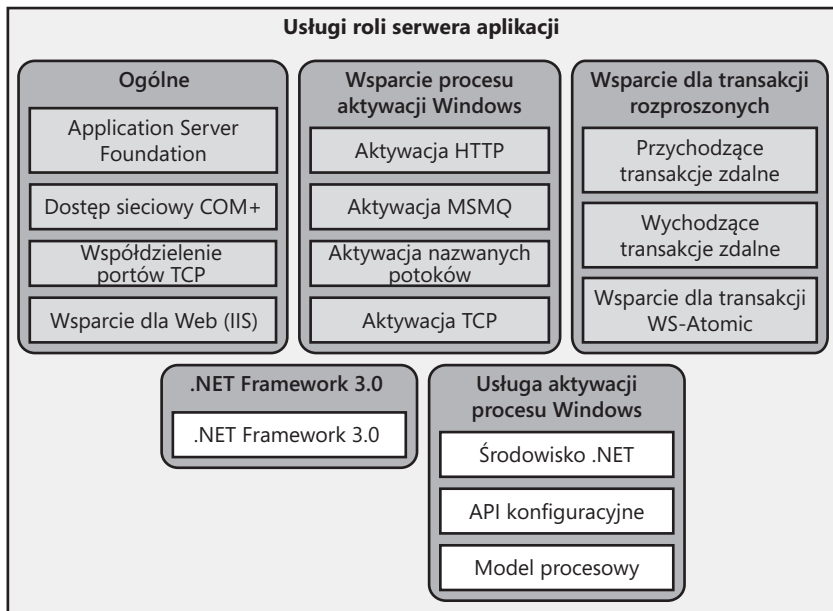
W celu obsługi aplikacji napisanych dla usług IIS 6 można zainstalować IIS 7.0 wraz z modulem zgodności z IIS 6. W przypadku istniejącej instalacji serwera IIS 6 można również zainstalować narzędzia IIS 6 Management Compatibility, które umożliwiają administrację zdalną tych instalacji serwerowych. Usługi IIS 7.0 można także instalować do umożliwienia administracji zdalnej. Zarówno platforma stacji, jak i serwera może być używana do administracji zdalnej innych serwerów IIS, a także witryn i aplikacji skonfigurowanych na tych serwerach. Aby umożliwić administrację zdalną serwera IIS, należy włączyć usługę WMSVC (Web Management Service) na serwerze, który ma być zarządzany zdalnie, a następnie zainstalować narzędzia zarządzania sieci Web na komputerze, który ma być używany do administracji zdalnej.

Omówienie funkcji i ról IIS 7.0

Jak już nadmieniono poprzednio, usługi IIS 7.0 można uruchomić na komputerze systemu Windows Server 2008, by obsługiwać trzy określone role: serwer aplikacji, serwer sieci Web i serwer Windows SharePoint Services. Usługi IIS 7.0 uruchomione na stacji systemu Windows można używać do projektowania, tworzenia i testowania witryn i aplikacji. Składniki używane do obsługi tych ról nazywane są usługami lub funkcjami ról, w zależności od tego, który interfejs użytkownika jest używany. W kolejnych podrozdziałach omówione zostały wszystkie role serwera i powiązane z nimi usługi ról.

Usługi ról dla serwerów aplikacji

Serwery aplikacji uruchamiane w systemach Windows Server 2008 używane są do utrzymywania aplikacji rozproszonych zbudowanych przy użyciu platform ASP.NET, Enterprise Services i WCF. Na rysunku 2-1 zaprezentowano przegląd usług powiązanych z serwerami aplikacji.



Rysunek 2-1 Usługi ról serwerów aplikacji.

Po zainstalowaniu serwera aplikacji, jako standardowy rdzeń funkcjonalny dołączane są jedynie usługi Application Server Core i Enterprise Services Network Access. Oprócz standardowego zestawu funkcji podstawowych należy zainstalować składniki platformy .NET Framework 3.0 i usługi Windows Activation Service. Inne składniki są opcjonalne i powinny być instalowane w oparciu o określone wymagania utrzymywanych aplikacji rozproszonych.

Serwery aplikacji mogą używać następujących usług ról ogólnego przeznaczenia:

- **Application Server Foundation** Usługa udostępnia podstawowe funkcje serwera aplikacji za pomocą następujących technologii platformy .NET Framework 3.0: Windows CardSpace, WCF, WPF oraz WF. Technologie te pozwalają na dostarczanie aplikacji o zarządzanym kodzie, które modelują procesy biznesowe.
- **COM+ Network Access (dostęp sieciowy COM+)** Usługa umożliwia serwerom aplikacji wywoływanie zdalnej aplikacji poprzez sieć. Wywoływane aplikacje muszą być tworzone za pomocą składnika Enterprise Services i muszą obsługiwać składniki COM+.
- **TCP Port Sparring (współużytkowanie portu TCP)** Usługa umożliwia wielu aplikacjom współużytkowanie jednego portu TCP. Przy użyciu tej funkcji wiele aplikacji sieci Web może współistnieć na tym samym serwerze w oddzielnych, izolowanych procesach, chociaż współużytkują infrastrukturę sieci wymaganą do wysyłania i odbierania danych przez porty TCP.
- **Web Server (IIS) Suport [obsługa serwera Web]** Usługa umożliwia serwerowi aplikacji utrzymywanie witryn sieci Web o dynamicznej i statycznej zawartości. Witryny Web obsługują standardowe rozszerzenia serwera IIS i umożliwiają tworzenie stron sieci Web

zawierających dynamiczne zawartości. Dzięki temu serwer aplikacji może utrzymywać wewnętrzne i zewnętrzne witryny sieci Web lub udostępniać projektantom środowisko tworzenia aplikacji sieci Web. W tabeli 2-2 zamieszczona została pełna lista funkcji usług IIS zainstalowanych domyślnie po wybraniu tej funkcji.

Windows Process Activation Service obsługuje rozproszone aplikacje internetowe, które używają do transferu informacji różnych protokołów. Stosować można następujące składniki powiązane:

- **.NET Environment (środowisko .NET)** Instaluje składnik .NET Environment używany do aktywacji zarządzanego kodu.
- **Configuration APIs (interfejsy API konfiguracji)** Instaluje interfejsy API kodu zarządzanego, co umożliwia konfigurowanie modelu procesu.
- **Process Model (model procesu)** Instaluje model procesu do projektowania i uruchamiania aplikacji.

Usługa Windows Process Activation Service Support umożliwia serwerowi zdalne wywołanie aplikacji w sieci przy użyciu protokołów, takich jak HTTP, Microsoft Message Queuing (MSMQ), potoki nazwane i TCP. Dzięki temu aplikacje mogą być dynamicznie uruchamiane bądź zatrzymywane odpowiednio do przychodzących żądań, co zwiększa wydajność i możliwości zarządzania. W celu określenia, których protokołów może używać serwer aplikacji w usłudze Windows Process Activation, można posłużyć się następującymi powiązaniem usługami ról:

- **HTTP Activation (aktywacja HTTP)** Usługa wspiera aktywację procesu poprzez HTTP. Jest to standardowa metoda aktywacji używana przez większość aplikacji sieci Web. Aplikacje obsługujące metodę HTTP Activation mogą być dynamicznie uruchamiane i zatrzymywane w odpowiedzi na żądania przychodzące poprzez HTTP. W przypadku HTTP, aplikacja i komputery, z którymi się ona komunikuje muszą być w trybie online, aby przekazywać informacje tam i z powrotem bez konieczności generowania żądań kolejkowania.
- **Message Queuing Activation (aktywacja kolejkowania wiadomości)** Usługa wspiera aktywację procesu przy użyciu funkcji Microsoft Message Queue (MSMQ). Ta metoda aktywacji jest używana, jeśli na serwerze aplikacji uruchomione są rozproszone aplikacje przekazywania wiadomości. Aplikacje obsługujące metodę MSMQ Activation i kolejkowanie wiadomości mogą być dynamicznie uruchamiane i zatrzymywane w odpowiedzi na żądania przychodzące poprzez MSMQ. W przypadku kolejkowania wiadomości, aplikacje źródłowe wysyłają wiadomości do kolejek, gdzie są tymczasowo przechowywane, aż pobierze je aplikacja docelowa. Ta technika kolejkowania pozwala aplikacjom na komunikowanie się poprzez różnego typu sieci i z komputerami, które mogą być w trybie offline.
- **Named Pipes Activation (aktywacja potoków nazwanych)** Usługa wspiera aktywację procesu za pomocą funkcji potoków nazwanych. Aplikacje, które obsługują metodę Named Pipes Activation mogą być dynamicznie uruchamiane i zatrzymywane w odpowiedzi na żądania przychodzące poprzez potoki nazwane. Ta metoda aktywacji jest używana, kiedy aplikacje sieci Web komunikują się ze starszymi wersjami systemów operacyjnych Windows. Potok nazwany jest częścią pamięci używaną przez jeden proces do przekazywania informacji innemu procesowi, tak że dane wyjściowe jednego procesu

są danymi wejściowymi dla innego procesu. Potoki nazwane mają standardowe adresy sieci, jak na przykład `\\Pipe\SqlQuery`, do których proces może się odnosić na komputerze lokalnym lub zdalnym. Protokół Named Pipes jest używany głównie dla lokalnych lub zdalnych połączeń przez aplikacje napisane dla systemów Microsoft Windows NT, Windows 98 i wcześniejszych wersji.

- **TCP Activation (aktywacja TCP)** Usługa wspiera aktywację procesu poprzez TCP. Aplikacje, które obsługują metodę TCP Activation mogą być dynamicznie uruchamiane i zatrzymywane w odpowiedzi na żądania przychodzące poprzez TCP. W przypadku TCP, aplikacja i komputery, z którymi się ona komunikuje, muszą być w trybie online, aby przekazywać informacje tam i z powrotem bez konieczności generowania żądań kolejkowania.

Podczas używania usługi Windows Process Activation Support mogą być wymagane następujące dodatkowe usługi ról:

- **Non-HTTP Activation (aktywacja nie-HTTP)** Usługa zapewnia aktywację inną niż przez HTTP, przy użyciu jednego z następujących protokołów: MSMQ, potoki nazwane i TCP. W usługach IIS funkcja ta instalowana jest jako składnik WCF Activation.
- **Message Queuing Server (serwer kolejkowania wiadomości)** Usługa udostępnia potrzebne funkcje serwera dla kolejkowania wiadomości.

Wskazówka Każda z funkcji Windows Process Activation Support ma powiązany ze sobą zestaw wymaganych usług roli. W przypadku metody HTTP Activation wymagane są wszystkie funkcje wymienione w tabeli 2-1 jako Web Common. W przypadku metody Message Queuing Activation wymagane są funkcje Message Queuing Server i Non-HTTP Activation. Dla metod TCP Activation i Named Pipes Activation wymagana jest funkcja Non-HTTP Activation.

Kiedy aplikacje komunikują się między sobą, mogą przeprowadzać różnego rodzaju transakcje, takie jak kwerendy pobierania danych przechowywanych w bazie danych czy przesyłanie danych w celu aktualizacji bazy danych. Jeśli serwer aplikacji utrzymuje bazę danych lub musi przesłać zapytanie do pojedynczej bazy danych w celu wykonania transakcji, transakcje takie są zasadniczo proste. Zagadnienia szybko komplikują się, kiedy wykorzystywanych jest wiele baz danych utrzymywanych na wielu komputerach. Transakcja, która wywołuje wiele baz danych przechowywanych na wielu komputerach jest nazywana *transakcją rozproszoną*. W przypadku transakcji rozproszonych, potrzebna jest metoda gwarantująca, że wszystkie pobrania bądź aktualizacje danych są przeprowadzone odpowiednio i w takim momencie kluczową rolę zaczyna odgrywać obsługa funkcji Distributed Transactions (transakcje rozproszone). Funkcja Distributed Transactions udostępnia usługi, które ułatwiają prawidłowe przeprowadzenie transakcji rozproszonych.

W celu włączenia obsługi funkcji Distributed Transactions na serwerze aplikacji można użyć następujących powiązanych usług roli:

- **Incoming Remote Transactions (zdalne transakcje przychodzące)** Usługa wspiera transakcje rozproszone w celu ułatwienia prawidłowego wykonania przychodzących transakcji zdalnych
- **Outgoing Remote Transactions (zdalne transakcje wychodzące)** Usługa wspiera transakcje rozproszone w celu ułatwienia prawidłowego wykonania wychodzących transakcji zdalnych

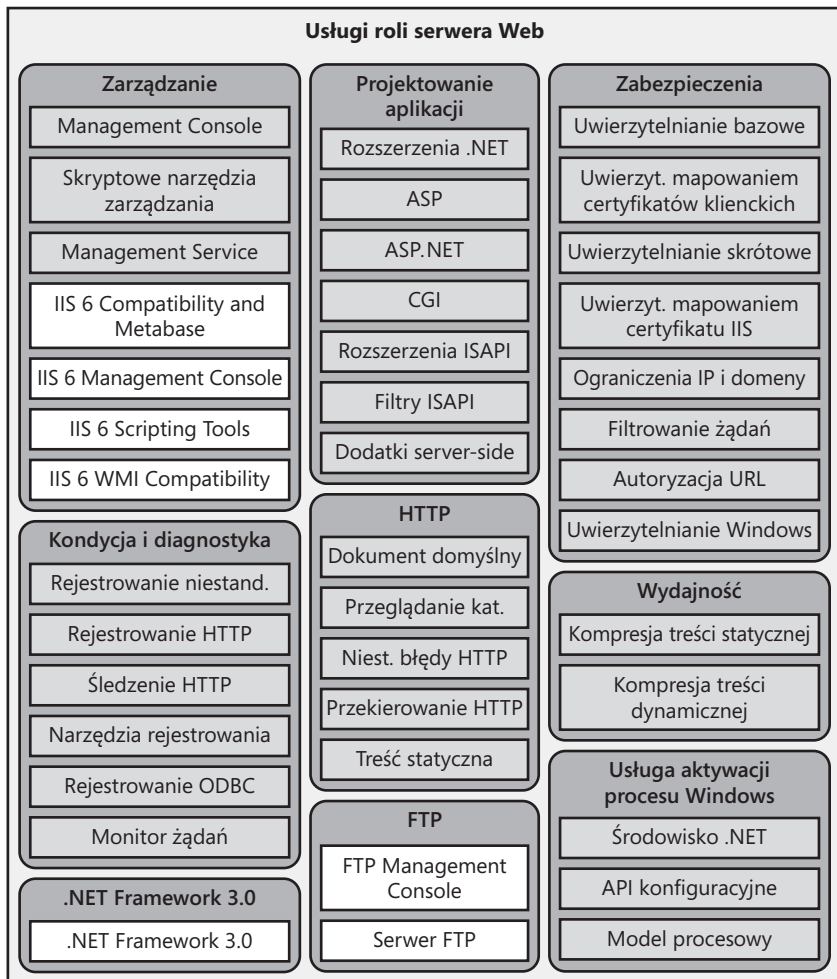
- **WS-Atomic Transactions (transakcje WS_Atomic)** Usługa wspiera transakcje rozproszone dla aplikacji, które używają dwufazowych transakcji przekazu przy wymianach opartych na protokole SOAP (Simple Object Access Protocol). Wymiany bazujące na protokole SOAP zawierają polecenia tekstowe formatowane za pomocą języka XML. Jeśli planowane jest użycie protokołu SOAP dla dwufazowych transakcji przekazu, trzeba również określić i skonfigurować punkty końcowe HTTP.

W praktyce Usługa roli WS-Atomic Transactions podczas komunikowania się z klientami korzysta z protokołu SSL do szyfrowania ruchu sieci. W celu używania SSL, w usługach IIS w witrynie WS-AT należy zainstalować certyfikat uwierzytelnienia serwera odpowiedni dla szyfrowania SSL. Jeśli certyfikat uzyskiwany jest z urzędu certyfikacji (CA), można go zaimportować jako część procesu instalacji. W przypadku małych czy testowych środowisk, podczas instalowania istnieje również opcja utworzenia certyfikatu typu self-signed (z podpisem własnym). Wadą tego typu certyfikatu jest konieczność ręcznego instalowania certyfikatu w systemach klienckich.

Podczas planowania instalacji niewątpliwą zaletą jest instalowanie serwera aplikacji razem z obsługą usługi Web Server. Jeśli instalacja serwera aplikacji wspiera usługę Web Server, można konfigurować usługi aplikacji przy użyciu interfejsów API udostępnianych przez platformy ASP.NET i .NET Framework. Ponieważ serwer obejmuje konfigurację składników konfiguracji i administracji usług IIS, będą dostępne wszystkie wspólne funkcje usług IIS i będzie możliwa konfiguracja serwera przy użyciu modułów i narzędzi administracyjnych usług IIS 7.0.

Usługi roli dla stacji systemu Windows i serwerów sieci Web

Serwery sieci Web uruchomione na stacji systemu Windows Vista lub w systemie Windows Server 2008 mogą utrzymywać witryny i aplikacje sieci Web. Na rysunku 2-2 przedstawiono przegląd powiązanych usług ról dla serwerów sieci Web.



Rysunek 2-2 Usługi ról dla serwerów sieci Web.

Zgodnie z podsumowaniem zamieszczonym w tabeli 2-1, jeśli instalowany jest serwer sieci Web, automatycznie instalowanych jest szereg funkcji konfiguracyjnych, jako część rdzenia serwera, a inne funkcje są instalowane domyślnie (jeśli ma to zastosowanie dla używanej wersji systemu operacyjnego). Funkcje te reprezentują główne składniki wewnętrzne oprócz zalecanego minimum i wymaganych składników potrzebnych do zarządzania serwerem sieci Web i publikowania witryn Web. Dla większości instalacji usług IIS 7.0 będą instalowane dodatkowe funkcje w oparciu o specyficzne wymagania witryn i aplikacji sieci Web utrzymywanych na serwerze.

Zgodnie z omówieniem zamieszczonym w rozdziale 1 „Omówienie administracji usług IIS 7.0”, wersje systemów Windows Server i Windows Vista wyposażone są w różne zestawy

obsługiwanych funkcji. W tabeli 2-2, w odniesieniu do poszczególnych wersji systemu Windows, zaprezentowano porównanie funkcji, a także przedstawiono ograniczenia liczby żądań. Ponieważ wersje systemu Windows Server nie mają limitów liczby żądań, mogą być używane w rzeczywistych instalacjach produkcyjnych. Ze względu na ograniczenia liczby żądań, systemy Windows Vista najlepiej nadają się dla indywidualnych administratorów lub projektantów oraz do używania w środowiskach testowych i projektowych.

Tabela 2-2 Porównanie funkcji w odniesieniu do wersji systemów Windows

Funkcja	Windows Server 2008	Windows Vista Business & Ultimate	Windows Vista Home Premium	Windows Vista Home Basic
Rdzeń serwera IIS				
Anonymous Authentication (uwierzytelnienie anonimowe)	Dołączona	Dołączona	Dołączona	N/A
Configuration Validation (walidacja konfiguracji)	Dołączona	Dołączona	Dołączona	N/A
HTTP Cache (bufor HTTP)	Dołączona	Dołączona	Dołączona	N/A
Protocol Support (obsługa protokołów)	Dołączona	Dołączona	Dołączona	N/A
Wspólne funkcje HTTP				
Default Document (dokument domyślny)	Domyślna	Domyślna	Domyślna	N/A
Directory Browsing (przeglądanie katalogów)	Domyślna	Domyślna	Domyślna	N/A
HTTP Errors (błędy HTTP)	Domyślna	Domyślna	Domyślna	Domyślna
HTTP Redirection (przeadresowanie HTTP)	Dostępna	Dostępna	Dostępna	Dostępna
Static Content (zawartość statyczna)	Domyślna	Domyślna	Domyślna	N/A
Funkcje projektowe aplikacji				
.NET Extensibility	Dostępna	Dostępna	Dostępna	Dostępna
ASP	Dostępna	Dostępna	Dostępna	N/A
ASP.NET	Dostępna	Dostępna	Dostępna	N/A
CGI	Dostępna	Dostępna	Dostępna	N/A
ISAPI Extensions (rozszerzenia ISAPI)	Dostępna	Dostępna	Dostępna	N/A

ciąg dalszy na stronie następczej

Ciąg dalszy ze strony poprzedniej

Tabela 2-2 Porównanie funkcji w odniesieniu do wersji systemów Windows

Funkcja	Windows Server 2008	Windows Vista Business & Ultimate	Windows Vista Home Premium	Windows Vista Home Basic
ISAPI Filters (filtry ISAPI)	Dostępna	Dostępna	Dostępna	N/A
Server-Side Includes	Dostępna	Dostępna	Dostępna	N/A
Funkcje dotyczące stanu i diagnostyki				
Custom Logging (rejestrowanie niestandardowe)	Dostępna	Dostępna	Dostępna	N/A
HTTP Logging (rejestrowanie HTTP)	Domyślna	Domyślna	Domyślna	Domyślna
Logging Tools (narzędzia rejestrowania)	Dostępna	Dostępna	Dostępna	Dostępna
ODBC Logging (rejestrowanie ODBC)	Dostępna	Dostępna	N/A	N/A
Request Monitor (monitor żądań)	Domyślna	Domyślna	Domyślna	Domyślna
Tracing (śledzenie)	Dostępna	Dostępna	Dostępna	Dostępna
Funkcje dotyczące bezpieczeństwa				
Basic Authentication (uwierzytelnienie podstawowe)	Dostępna	Dostępna	Dostępna	N/A
Client Certificate Mapping Authentication (uwierzytelnienie mapowania certyfikatu klienta)	Dostępna	Dostępna	N/A	N/A
Digest Authentication (uwierzytelnienie szyfrowane)	Dostępna	Dostępna	N/A	N/A
IIS Client Certificate Mapping Authentication (uwierzytelnienie mapowania certyfikatu klienta)	Dostępna	Dostępna	N/A	N/A
IP and Domain Restrictions (ograniczenia IP i domeny)	Dostępna	Dostępna	Dostępna	Dostępna
Request Filtering (filtrowanie żądań)	Domyślna	Dostępna	Dostępna	Dostępna

Tabela 2-2 Porównanie funkcji w odniesieniu do wersji systemów Windows

Funkcja	Windows Server 2008	Windows Vista Business & Ultimate	Windows Vista Home Premium	Windows Vista Home Basic
URL Authorization (uwierzytelnienie autoryzacji)	Dostępna	Dostępna	Dostępna	Dostępna
Windows Authentication (uwierzytelnienie systemu Windows)	Dostępna	Dostępna	N/A	N/A
Funkcje dotyczące wydajności				
Static Content Compression (kompresja zawartości statycznej)	Domyślna	Domyślna	Domyślna	N/A
Dynamic Content Compression (kompresja zawartości dynamicznej)	Dostępna	Dostępna	Dostępna	Dostępna
Narzędzia zarządzania siecią Web				
IIS Management Console (konsola zarządzania IIS)	Domyślna	Domyślna	Domyślna	N/A
IIS Management Scripts and Tools (skrypty i narzędzia zarządzania IIS)	Dostępna	Dostępna	Dostępna	Dostępna
IIS Management Service (usługa zarządzania IIS)	Dostępna	Dostępna	Dostępna	N/A
IIS 6 Management Compatibility (zgodność zarządzania IIS 6)	Dostępna	Dostępna	Dostępna	Dostępna
IIS Metabase compatibility (zgodność metabazy IIS)	Dostępna	Dostępna	Dostępna	Dostępna
IIS 6 WMI Compatibility (zgodność usługi WMI IIS 6)	Dostępna	Dostępna	Dostępna	N/A
IIS 6 Scripting Tools (narzędzia tworzenia skryptów IIS 6)	Dostępna	Dostępna	Dostępna	N/A
IIS 6 Management Console (konsola zarządzania IIS 6)	Dostępna	Dostępna	Dostępna	N/A

Ciąg dalszy na stronie następnej

Ciąg dalszy ze strony poprzedniej

Tabela 2-2 Porównanie funkcji w odniesieniu do wersji systemów Windows

Funkcja	Windows Server 2008	Windows Vista Business & Ultimate	Windows Vista Home Premium	Windows Vista Home Basic
Usługi publikowania FTP				
FTP Management Console (konsola zarządzania FTP)	Dostępna	Dostępna	N/A	N/A
FTP Server (serwer FTP)	Dostępna	Dostępna	N/A	N/A
Windows Activation Service				
.NET Environment	Dostępna	Dostępna	Dostępna	Dostępna
Configuration APIs (konfiguracja interfejsów API)	Domyślna	Dostępna	Dostępna	Dostępna
Process Model (model procesu)	Domyślna	Domyślna	Domyślna	Domyślna
Ograniczenia				
Limit liczby wykonywanych żądań	Brak ograniczenia	10	3	3

Na podstawie informacji prezentowanych w tabeli 2-2 można zauważyć, że dla serwerów sieci Web dostępnych jest wiele różnych funkcji. Omówione zostaną wszystkie funkcje, które nie były opisane poprzednio w rozdziale, a także w całej książce można znaleźć szczegółowe informacje na ich temat w odpowiednich rozdziałach. W dodatku „Pełny wykaz modułów i schematów usług IIS 7.0” zamieszczony został szczegółowy opis funkcji wraz z powiązanymi modułami konfiguracyjnymi.

Usługa IIS Server Core udostępnia podstawowe funkcje dla IIS. Funkcje tych można używać w następujący sposób:

- **Anonymous Authentication (uwierzytelnienie anonimowe)** Funkcja umożliwia anonimowy dostęp do serwera. W przypadku anonimowego dostępu każdy użytkownik może uzyskać dostęp do zawartości bez konieczności przedstawienia poświadczeń. Każdy serwer musi mieć skonfigurowany co najmniej jeden mechanizm uwierzytelnienia, a ten jest mechanizmem domyślnym.
- **Configuration Validation (walidacja konfiguracji)** Usługa sprawdza konfigurację serwera i jego aplikacji. Jeśli ktokolwiek nieprawidłowo skonfiguruje serwer lub aplikację, usługi IIS 7.0 wygenerują komunikat o błędzie, który ułatwia wykrycie i diagnozę problemu.
- **HTTP Cache (bufor HTTP)** Funkcja zwiększa wydajność poprzez zwracanie przetworzonej kopii żądanej strony sieci Web z bufora, co zmniejsza obciążenie serwera i skraca czas odpowiedzi. Usługi IIS 7.0 wspierają szereg poziomów buforowania, włączając w to buforowanie danych wyjściowych w trybie użytkownika i trybie jądra. Jeśli włączone zostanie buforowanie w trybie jądra, buforowane odpowiedzi obsługiwane są przez

jądro, a nie przez tryb użytkownika usług IIS, co daje usługom IIS dodatkowy wzrost wydajności i zwiększenie liczby żądań, które mogą być przetworzone przez IIS.

- **Protocol Support (obsługa protokołów)** Funkcja obsługuje protokoły najczęściej używane przez serwery sieci Web, jak podtrzymanie aktywnego połączenia HTTP (keep-alives), niestandardowe nagłówki i nagłówki przekierowania. Mechanizm *HTTP keep-alives* pozwala klientom na utrzymywanie otwartych połączeń z serwerami, co przyspiesza proces żądania po ustanowieniu połączenia z serwerem. Nagłówki niestandardowe i przekierowania *umożliwiają* optymalizowanie działania usług IIS, by obsługiwane były funkcje specyfikacji HTTP 1.1.

Funkcje Common HTTP instalują wspólne usługi wymagane do obsługi zawartości sieci Web. Funkcje te mogą być używane w następujący sposób:

- **Default Dokument (dokument domyślny)** Funkcja obsługuje wyświetlanie dokumentów domyślnych. Po włączeniu tej funkcji i wprowadzeniu przez użytkownika żądania zakończonego znakiem '/', jak na przykład <http://www.adatum.com/>, usługi IIS mogą przekierować żądanie do dokumentu domyślnego serwera sieci Web lub do katalogu. Dla zapewnienia najlepszej wydajności używany dokument domyślny powinien być wymieniany jako pierwszy, a lista dokumentów domyślnych powinna być ograniczona tylko do niezbędnych dokumentów.
- **Directory Browning (przeglądanie katalogu)** Funkcja obsługuje przeglądanie katalogów. Jeśli włączona została funkcja dokumentu domyślnego, ale taki bieżący dokument nie został znaleziony, usługi mogą użyć tej funkcji do wygenerowania listy zawartości określonego katalogu. Jeśli nie są włączone funkcje dokumentu domyślnego lub przeglądania katalogu, a klient żąda adresu URL na poziomie katalogu, usługi IIS zwrócą pustą odpowiedź.
- **HTTP Errors (błędy HTTP)** Funkcja obsługuje niestandardowe błędy i szczegółowe powiadomienia o błędach. Po włączeniu tej funkcji i wystąpieniu błędu na serwerze, serwer może zwrócić niestandardową stronę o błędzie do wszystkich klientów niezależnie od lokalizacji, szczegółowy komunikat o błędzie do wszystkich klientów niezależnie od lokalizacji lub szczegółowe informacje o błędzie do klientów lokalnych i niestandardową stronę o błędzie do klientów zdalnych. Usługi IIS wyświetlają niestandardową stronę o błędzie w oparciu o typ błędu http, jaki miał miejsce.
- **HTTP Redirection (przekierowanie HTTP)** Funkcja obsługuje przekierowanie żądań HTTP w celu przekierowania użytkowników ze starej do nowej witryny. Dla domyślnej konfiguracji przekierowania wszystkie żądania dotyczące plików w starej lokalizacji zostają automatycznie mapowane do plików w nowej lokalizacji wyspecyfikowanej przez użytkownika. Działanie to można zmieniać w różny sposób.
- **Static Content (zawartość statyczna)** Funkcja obsługuje statyczną zawartość sieci Web, taką jak dokumenty HTML, obrazy GIF lub JPEG. Zestaw konfiguracyjny `staticContent/mimeMap` w pliku `applicationHost.config` określa listę obsługiwanych rozszerzeń.

Uwaga Każda z tych wspólnych funkcji ma powiązany macierzysty moduł usługi IIS 7.0, który jest instalowany i aktywowany przez program instalacyjny po zaznaczeniu danej funkcji. Dokładne mapowanie funkcji wspólnych do odpowiadających im modułów macierzystych opisane jest w dodatku. Więcej informacji na temat działania tych funkcji znaleźć można w rozdziale 5 „Zarządzanie globalną konfiguracją IIS”.

Funkcje Application Development instalują mechanizmy wymagane do projektowania i utrzymywania aplikacji Web. Funkcje te mogą być używane w następujący sposób:

- **.NET Extensibility** Funkcja umożliwia serwerowi sieci Web utrzymywanie aplikacji platformy .NET Framework i udostępnia potrzebną funkcjonalność dla integracji usług IIS z platformami ASP.NET i .NET Framework. Podczas konfigurowania sposobu używania zarządzanych modułów należy również włączyć funkcję Managed Engine. Funkcja *Managed Engine* jest składnikiem serwera, który rzeczywiście wykonuje integrację funkcji.
- **ASP** Funkcja umożliwia serwerowi sieci Web utrzymywanie klasycznych aplikacji ASP (Active Server Pages). Strony sieci Web, które korzystają z ASP, są traktowane jako strony dynamiczne, ponieważ usługi IIS generują je w momencie żądania. Aby korzystać z funkcji ASP, należy również używać funkcji ISAPI Extensions.
- **ASP.NET** Funkcja umożliwia serwerowi sieci Web utrzymywanie aplikacji ASP.NET. Strony sieci Web, które używają ASP.NET, są traktowane jako strony dynamiczne, ponieważ usługi IIS generują je w momencie żądania. Aby korzystać z funkcji ASP.NET, należy również używać funkcji .NET Extensibility, ISAPI Extensions i ISAPI Filters.
- **CGI** Funkcja umożliwia serwerowi sieci Web utrzymywanie plików wykonywalnych CGI (Common Gateway Interface). Interfejs CGI opisuje, w jaki sposób plik wykonywalny określony w adresie sieci Web, nazywany również *gateway scripts* (*skrypty bramy*), przekazuje informacje do serwerów sieci Web. Zgodnie z ustawieniami domyślnymi, usługi IIS obsługują wszystkie pliki z rozszerzeniem `exe` jako skrypty CGI.
- **ISAPI Extensions (rozszerzenia ISAPI)** Funkcja ISAPI Extensions umożliwia obsługę żądań klientów. W rdzeniu serwer IIS szereg składników jest zależnych od programów obsługi bazujących na funkcjach ISAPI Extensions, wliczając w to składniki ASP i ASP.NET. Domyślnie IIS obsługują wszystkie pliki o rozszerzeniu `dll`, jako ISAPI Extensions.
- **ISAPI Filters (filtry ISAPI)** Funkcja ISAPI Filters umożliwia modyfikowanie działania serwera sieci Web. Usługi IIS używają funkcji ISAPI Filters w celu udostępniania dodatkowej funkcjonalności. Jeśli w początkowej instalacji zaznaczony został składnik ASP.NET, program instalacyjny konfiguruje filtr ASP.NET tak, aby funkcjonalność ta została udostępniona. W pliku `applicationHost.config` każda wersja ASP.NET zainstalowana na serwerze sieci Web musi mieć definicje filtra, który identyfikuje wersję i ścieżkę do odnośnego filtra.
- **SSI (Server-Side Includes)** Funkcja SSI umożliwia serwerowi sieci Web analizę plików zawierających mechanizm SSI (Server-Side Includes). SSI jest technologią, która pozwala usługom IIS wstawiać dane do dokumentu, kiedy żąda tego klient. Po włączeniu tej funkcji pliki o rozszerzeniach `stm`, `shtm` i `shtml` są analizowane, by sprawdzić, czy zawierają wstawienia, które powinny być zastąpione rzeczywistymi wartościami. Jeśli funkcja ta jest wyłączona, usługi IIS obsługują pliki `stm`, `shtm` i `shtml` jako zawartość statyczną, co powoduje, że w odpowiedzi będzie zwracane rzeczywiste polecenie dołączenia.

Funkcje związane ze stanem i diagnostyką pozwalają na monitorowanie serwerów, witryn i aplikacji oraz na diagnozę występujących problemów. Funkcji tych można używać w następujący sposób:

- **Custom Logging (rejestrowanie niestandardowe)** Funkcja umożliwia obsługę niestandardowego rejestrowania. Najczęściej rejestrowanie niestandardowe korzysta

z interfejsu ILogPlugin modelu COM (Component Object Model). Zamiast używania tej funkcji, firma Microsoft zaleca tworzenie zarządzanego modułu i subskrypcję powiadomienia RQ_LOG_REQUEST.

- **HTTP Logging (rejestrowanie HTTP)** Funkcja umożliwia rejestrowanie aktywności witryny sieci Web. Usługi IIS 7.0 można skonfigurować tak, by używany był jeden plik dziennika dla jednego serwera lub dla jednej witryny. Rejestrowanie w odniesieniu do jednego serwera powinno być używane, jeśli zachodzi potrzeba, żeby wszystkie witryny uruchomione na serwerze zapisywały dane dziennika w jednym pliku. Rejestrowanie w odniesieniu do witryny jest używane, jeśli zachodzi potrzeba śledzenia dostępu oddzielnie dla każdej witryny na serwerze.
- **Logging Tools (narzędzia rejestrowania)** Funkcja umożliwia zarządzanie dziennikami aktywności serwera i automatyzację często wykonywanych zadań rejestrowania przy użyciu skryptów.
- **ODBC Logging (rejestrowanie ODBC)** Funkcja umożliwia obsługę rejestrowania aktywności witryny sieci Web w odniesieniu do baz danych zgodnych z ODBC. W usługach IIS 7.0 rejestrowanie ODBC jest zaimplementowane jako typ rejestrowania niestandardowego.
- **Request Monitor (monitor żądań)** Funkcja umożliwia przeglądanie informacji szczegółowych dotyczących aktualnie wykonywanych żądań, stanu działania witryny sieci Web, aktualnie wykonywanych domen aplikacji i innych.
- **Tracing (śledzenie)** Funkcja obsługuje śledzenie niepomysłnie zakończonych żądań. Innym typem śledzenia, który może być włączony po skonfigurowaniu, jest funkcja śledzenia HTTP, pozwalająca poprzez rdzeń serwera IIS śledzić zdarzenia i ostrzeżenia związane ze swoimi źródłami.

Funkcje dotyczące bezpieczeństwa umożliwiają kontrolę dostępu do serwera i jego zawartości. Funkcje używane są następujący sposób:

- **Basic Authentication (uwierzytelnienie podstawowe)** W celu uzyskania dostępu do zawartości, funkcja wymaga od użytkownika podania prawidłowej nazwy użytkownika i hasła. Wszystkie przeglądarki obsługują ten mechanizm uwierzytelniania, ale hasła przekazywane są w bez szyfrowania, co umożliwia ujawnienie hasła podczas transmisji. Jeśli funkcja Basic Authentication ma być wymagana dla witryny lub katalogu, dla tej witryny lub katalogu należy wyłączyć funkcję Anonymous Authentication.
- **Client Certificate Mapping Authentication (uwierzytelnienie mapowania certyfikatu klienta)** W celu przeprowadzenia uwierzytelnienia funkcja mapuje certyfikaty klientkie do kont usługi Active Directory. Jeśli mapowanie certyfikatów zostało włączone, funkcja ta wykonuje potrzebne mapowanie certyfikatu do usługi Active Directory dla uwierzytelnienia klientów autoryzowanych.
- **Digest Authentication (uwierzytelnienie szyfrowane)** Funkcja używa kontrolera domeny systemu Windows do uwierzytelnienia żądań użytkownika dotyczących zawartości. Funkcja Digest Authentication może być używana poprzez zapory i usługi proxy.
- **IIS Client Certificate Mapping Authentication** W celu uwierzytelnienia funkcja mapuje certyfikaty klienta SSL do kont systemu Windows. W przypadku tej metody

uwierzytelniania poświadczenia użytkownika i reguły mapowania są przechowywane w magazynie konfiguracji usług IIS.

- **IP and Domain Restrictions (ograniczenia IP i domen)** Funkcja pozwala na przydzielanie lub odmowę dostępu do serwera poprzez adres IP, identyfikator sieci lub domenę. Przydzielenie dostępu pozwala komputerowi na wykonywanie żądań dotyczących zasobów, ale niekoniecznie zezwala na pracę z tymi zasobami. Jeśli wymagane jest uwierzytelnienie, użytkownicy będą musieli uwierzytelnić się sami. Odmowa dostępu do zasobów uniemożliwia komputerowi dostęp do tych zasobów, co oznacza, że użytkownicy nie uzyskują dostępu do zasobów, nawet jeśli mogą sami się uwierzytelnić.
- **Request Filtering (filtrowanie żądań)** Funkcja pozwala na odrzucanie podejrzanych żądań poprzez skanowanie adresów URL wysłanych przez serwer i odfiltrowanie niepożądanych żądań. Domyślnie usługi IIS blokują żądania rozszerzenia plików, które mogłyby być niewłaściwie użyte, a także blokują przeglądanie krytycznych segmentów kodu.
- **URL Authorization (autoryzacja URL)** Funkcja obsługuje autoryzację w oparciu o reguły konfiguracji. Metoda ta pozwala żądać logowania i zezwalać bądź odmawiać dostępu do określonych adresów URL w oparciu o nazwy użytkowników, role .NET i metody żądania HTTP.
- **Windows Authentication (uwierzytelnienie systemu Windows)** Funkcja obsługuje uwierzytelnienie systemu Windows przy użyciu protokołów NTLM, Kerberos lub obu. Funkcja Windows Authentication będzie używana głównie w sieciach wewnętrznych.

W celu zapewnienia zwiększonej wydajności usługi IIS obsługują zarówno statyczną, jak i dynamiczną kompresję. W przypadku kompresji statycznej usługi IIS wykonują w pamięci kompresję statycznej zawartości podczas pierwszego żądania, a następnie zapisują skompresowane wyniki na dysku, by mogły być pobrane podczas następnego użycia. W przypadku zawartości dynamicznych usługi IIS wykonują w pamięci kompresję każdorazowo, kiedy klient żąda zawartości dynamicznej. Usługi muszą każdorazowo kompresować zawartość dynamiczną, ponieważ dane te są zmienne.

Podczas prób poprawy wydajności serwera i jego możliwości współdziałania należy pamiętać o poniżej wymienionych funkcjach rozszerzonych:

- **File Cache (bufor plików)** Funkcja buforuje uchwyt plików dla plików otwartych przez mechanizm serwera i powiązane z serwerem moduły. Jeśli usługi IIS nie buforują uchwytów plików, IIS musi otwierać pliki dla każdego żądania, co może powodować zmniejszenie wydajności.
- **Managed Engine (mechanizm zarządzany)** Funkcja umożliwia integrację usług IIS z mechanizmem działania platformy ASP.NET. Jeśli funkcja ta nie zostanie skonfigurowana, również wyłączona jest integracja z ASP.NET i żadne moduły zarządzane lub programy obsługi ASP.NET nie będą wywoływane, kiedy aplikacje puli działają w trybie Integrated.
- **Token Cache (bufor tokenu)** Funkcja buforuje tokeny zabezpieczeń systemu Windows dla schematów uwierzytelnienia bazujących na hasłach, takich jak Anonymous Authentication, Basic Authentication czy Digest Authentication (uwierzytelnienie anonimowe, podstawowe, szyfrowane). Jeśli usługi IIS buforują token zabezpieczeń użytkownika, mogą go używać przy kolejnych żądaniach generowanych przez tego użytkownika. Jeśli funkcja ta jest wyłączona lub usunięta, użytkownik musi logować się przy każdym

żądaniu, co powoduje wielokrotne wywoływanie procedury logowania użytkownika i może istotnie zmniejszyć ogólną wydajność.

- **HTTP Trace (śledzenie HTTP)** Funkcja obsługuje śledzenie żądania ilekroć klient żąda jednego ze śledzonych adresów URL. Sposób, w jaki usługi IIS śledzą poszczególne pliki jest określony regułami śledzenia utworzonymi przez administratora.
- **URI Cache (bufor URI)** Funkcja buforuje stany serwera specyficzne dla identyfikatorów URI (Uniform Resource Identifier), takie jak informacje szczegółowe o konfiguracji. Jeśli funkcja ta jest włączona, serwer będzie odczytywał informacje o konfiguracji jedynie przy pierwszym żądaniu dla danego URI. Dla kolejnych żądań serwer będzie korzystał z buforowanych informacji, jeśli konfiguracja nie uległa zmianie. Narzędzia zarządzania siecią Web używane do administracji można podzielić na kategorie ogólne: narzędzia wymagane do zarządzania usługami IIS 7.0 i narzędzia wymagane do zapewnienia zgodności z usługami IIS 6. Powiązane funkcje instalacji używane są w następujący sposób:
- **IIS Management Console (konsola zarządzania IIS)** Funkcja instaluje program Internet Information Services (IIS) Manager – główne narzędzie zarządzania przy korzystaniu z usług IIS 7.0.
- **IIS Management Scripts and Tools (narzędzia i skrypty zarządzania IIS)** Funkcja instaluje narzędzie administracji wiersza poleceń i powiązane z nim funkcje zarządzania z wiersza poleceń serwerami sieci Web.
- **IIS Management Service (usługi zarządzania IIS)** Funkcja instaluje usługę WMSVC (Web Management Service), która stanowi podstawę dla umożliwienia działania w sieci Web (HWC, Hostable Web Core), a dla administracji zdalnej działa jak autonomiczny serwer internetowy.
- **IIS Metabase Compatibility (zgodność metabazy IIS)** Funkcja zapewnia zgodność z serwerami, na których uruchomione są witryny sieci Web usług IIS 6 dzięki zainstalowaniu składnika, który tłumaczy zmiany w metabazie IIS 6 dla magazynu konfiguracji usług IIS 7.0.
- **IIS 6 WMI Compatibility (zgodność WMI IIS 6)** Usługa zapewnia potrzebną funkcjonalność dla serwerów skryptowych, na których uruchomione są witryny sieci Web usług IIS 6 dzięki zainstalowaniu interfejsów tworzenia skryptów usługi WMI (Windows Management Instrumentation).
- **IIS 6 Scripting Tools (narzędzia tworzenia skryptów IIS 6)** Usługa zapewnia potrzebną funkcjonalność dla serwerów skryptowych, na których uruchomione są witryny sieci Web usług IIS 6 dzięki zainstalowaniu składnika IIS 6 Scripting Tools.
- **IIS 6 Management Console (konsola zarządzania IIS 6)** Funkcja instaluje program Internet Information Services (IIS) 6.0 Manager, który jest wymagany do zdalnego zarządzania serwerami, na których uruchomione są witryny usługi IIS 6 i do zarządzania serwerami FTP dla usług IIS 6.

Usługi ról dla serwerów, na których uruchomiono oprogramowanie SharePoint Services

Oprogramowanie Windows SharePoint Services umożliwia współpracę zespołów poprzez łączenie osób i informacji. Serwer SharePoint Services jest zasadniczo serwerem sieci Web z uruchomioną pełną instalacją usług IIS i wykorzystuje zarządzane aplikacje, które udostępniają potrzebne funkcje dotyczące współpracy. Po zainstalowaniu oprogramowania SharePoint Services można zarządzać serwerem przy użyciu modułów i narzędzi administracyjnych usług IIS 7.0, a także za pomocą kilku narzędzi specyficznych dla programu SharePoint, takich jak SharePoint Central Administration czy SharePoint Products And Technologies Configuration Wizard. Po zainstalowaniu oba narzędzia zarządzania są dostępne w menu Administrative Tools (Narzędzia administracyjne).

W witrynie SharePoint można utrzymywać listy i biblioteki. *Lista* jest zbiorem informacji witryny, która jest współużytkowana przez zespół, wliczając w to ogłoszenia, kontakty, tablice dyskusyjne, zadania i kalendarze zespołów. *Biblioteka* jest miejscem w witrynie, gdzie można tworzyć, przechowywać i zarządzać plikami używanymi przez zespół. Oprócz list i bibliotek witryny SharePoint mogą utrzymywać strony sieci, a strony sieci Web mogą używać zawartości statycznej, dynamicznej lub obu tych typów.

Podczas planowania instalacji serwerów, na których uruchomione będzie oprogramowanie SharePoint Services, należy rozważyć kilka dodatkowych kwestii, a w tym dodatkowe zabezpieczenia i wymagania łączności, które mogą być potrzebne dla współpracujących zespołów. Należy uważnie chronić dostęp do serwera SharePoint Services, a także zapewnić, aby członkowie zespołów z lokalizacji zdalnych mogli uzyskać odpowiedni dostęp do serwera i potencjalnie ważnych informacji, które współużytkują.

Podczas planowania, oprócz zasobów używanych przez połączenia użytkowników, należy uwzględnić dodatkowe obciążenia wnoszone przez aplikacje SharePoint uruchomione na serwerze. Oprogramowanie Windows SharePoint Services ma szereg standardowych aplikacji, które uruchamiane są na serwerze SharePoint Services i aplikacje te pochłaniają dodatkowe fizyczne zasoby serwera. Każde połączenie użytkownika wnosi dodatkowe obciążenie na serwerze, odpowiednie do żądań i modyfikacji wykonywanych przez użytkowników.

Konfigurowanie usług IIS 7.0

Sposób konfigurowania usług IIS 7.0 zależy od roli i używanego systemu operacyjnego. Zgodnie z poprzednio zamieszczonym opisem, usługi IIS 7.0 mogą być konfigurowane tak, by obsługiwały jedną z trzech ról serwera: serwer aplikacji, serwer sieci Web i serwer z uruchomionym oprogramowaniem SharePoint Services. Usługi IIS 7.0 mogą być również konfigurowane jako część instalacji stacji. Poniżej omówiona została instalacja IIS 7.0 każdej z tych sytuacji.

Instalowanie serwerów aplikacji

Serwer aplikacji można zainstalować z obsługą serwera sieci Web lub bez tej obsługi, postępując się następującą procedurą:

1. Uruchomić program Server Manager (Menedżer serwera) klikając ikonę Server Manager na pasku narzędzi Quick Launch (Szybkie uruchamianie) lub klikając kolejno menu Start, Administrative Tools, Server Manager.

2. W programie Server Manager, w oknie z lewej strony zaznaczyć węzeł Roles (Role), a następnie w ramce Roles Summary (Podsumowanie ról) kliknąć odnośnik Add Roles (Dodaj rolę). Uruchomiony zostanie program Add Roles Wizard (Kreator dodawania ról). Jeśli kreator wyświetli stronę Before You Begin, należy przeczytać informacje na stronie powitalnej, a następnie kliknąć przycisk Next. Strona powitalna nie będzie wyświetlana przy kolejnym uruchomieniu kreatora, jeśli przed kliknięciem przycisku Next zaznaczone zostanie pole wyboru Do Not Show Me This Page Again.
3. Na stronie Select Server Roles (Wybór ról serwera) wybrać rolę serwera aplikacji. Następnie wyświetlone zostanie okno dialogowe Add Features Required For Application Server (Dodawanie funkcji wymaganych dla serwera aplikacji). W tym oknie dialogowym wymienione są funkcje wymagane do zainstalowania serwera aplikacji. Kliknąć przycisk Add Required Features (dodaj wymagane funkcje), aby zamknąć okno dialogowe i dodać do instalacji serwera aplikacji składniki platformy .NET Framework 3.0 oraz usługi Windows Process Activation Service.
4. W przypadku instalacji serwera aplikacji razem z obsługą Web Server, można wybrać domyślny zestaw wspólnych funkcji sieci Web lub skonfigurować tylko te funkcje, które będą używane. Jeśli poprzednio składniki Web Server (IIS) nie były zainstalowane, aby je zainstalować, należy zaznaczyć opcję Web Server (IIS), a następnie dwukrotnie kliknąć przycisk Next. W przeciwnym razie należy dwukrotnie kliknąć przycisk Next, aby kontynuować.
5. Wyświetlona zostaje strona Select Role Services (Wybierania usług ról). Jeśli poprzednio nie był zainstalowany, zaznaczyć składnik Web Server (IIS) Support, aby zainstalować serwer aplikacji razem z obsługą serwera sieci Web w standardowej konfiguracji domyślnej. Wyświetlone zostanie okno dialogowe, w którym wymienione są dodatkowe role wymagane. Po przejrzaniu wymaganych ról kliknąć przycisk Add Required Role Services (Dodaj wymagane usługi ról), aby zamknąć okno dialogowe.

Uwaga Wymagane role są takie same, jak role wymienione w tabeli 2-1 i opisane jako Web Common. Zaleca się wybranie składnika Web Server (IIS) Support, jeśli na serwerze aplikacji będą utrzymywane witryny lub usługi sieci Web. Dzięki temu zapewnione jest, że program instalacyjny domyślnie wybierze wymagane funkcje wspólne (Web Common), a to będzie później przydatne w procesie instalacji.
6. Zaznaczyć odpowiednie usługi ról, które mają być zainstalowane, a następnie kliknąć przycisk Next. Jeśli usługa roli zaznaczona została razem z dodatkowymi funkcjami wymaganymi, wyświetlone zostanie okno dialogowe, w którym wymienione są dodatkowe role wymagane. Po przejrzaniu wymaganych ról kliknąć przycisk Add Required Role Services, aby zamknąć okno dialogowe.
7. Jeśli zaznaczona zostanie funkcja WS-Atomic Transactions, następną wyświetloną stroną będzie Choose A Certificate For SSL Encryption (Wybieranie certyfikatu dla szyfrowania SSL). Dostępne są następujące opcje:
 - **Choose An Existing Certificate For SSL Encryption (Wybierz istniejący certyfikat dla szyfrowania SSL)** Opcja ta jest wybierana, jeśli certyfikat uzyskany został poprzednio z urzędu certyfikacji (CA) i ma być zainstalowany do korzystania z witryny WS-AT, którą program instalacyjny będzie konfigurował na serwerze. Jeśli dostępne są certyfikaty poprzednio zaimportowane przy użyciu przystawki Certyfikaty lub programu Import Certificate Wizard, wyświetlona zostanie lista dostępnych

certyfikatów, na której należy wskazać, który z nich będzie używany. W przeciwnym razie kliknąć przycisk Import, aby uruchomić program Certificate Import Wizard, a następnie postępować zgodnie z instrukcjami, aby zaimportować certyfikat.

- ❑ **Create A Self-Signed Certificate For SSL Encryption (Utwórz certyfikat z podpisem własnym dla szyfrowania SSL)** Opcję tę należy wybrać, jeśli używane są transakcje WS-Atomic przy ograniczonej liczbie klientów lub dla celów testowych bądź projektowych, a certyfikat z podpisem własnym ma być utworzony i następnie automatycznie zainstalowany do korzystania z witryny WS-AT, którą program instalacyjny będzie konfigurował na serwerze. Ten sam certyfikat trzeba będzie ręcznie zainstalować na wszystkich systemach klienckich, które mogą uwierzytelniać się na serwerze.
- ❑ **Choose A Certificate For SSL Encryption Later (Wybierz później certyfikat dla szyfrowania SSL)** Opcja ta jest zaznaczana, jeśli w danym momencie nie jest dostępny certyfikat uzyskiwany z CA, ale ma być uzyskany później. Jeśli opcja ta została wybrana, usługi IIS wyłączają protokół SSL dla witryny WS-AT do momentu, aż certyfikat nie zostanie zaimportowany (opis znaleźć można w rozdziale 10).

8. Jeśli na stronie Select Server Roles zaznaczona została opcja Web Server (IIS), co opisano w punkcie 5, kliknąć dwa razy przycisk Next, aby dla serwera sieci Web wyświetlić stronę Select Role Services. Następnie można zaznaczyć, które funkcje serwera sieci Web mają być zainstalowane. W większości przypadków, wybierane będą dodatkowe funkcje, a te zaznaczone nie będą usuwane. Podczas zaznaczania lub usuwania zaznaczenia usług ról warto uwzględnić poniższe uwagi, zanim kliknięty zostanie przycisk Next:

- ❑ Jeśli usługa roli zaznaczona została razem z dodatkowymi funkcjami wymaganymi, wyświetlone zostanie okno dialogowe, w którym wymienione są dodatkowe role wymagane. Po przejrzaniu ról wymaganych należy kliknąć przycisk Add Required Role Services, aby zaakceptować dodatki i zamknąć okno dialogowe. Jeśli kliknięty zostanie przycisk Cancel, program instalacyjny usunie zaznaczenie poprzednio wybranych funkcji.
- ❑ Jeśli zachodzi potrzeba usunięcia usługi roli, która jest wymagana na podstawie poprzednio dokonanego wyboru, wyświetlone zostaje ostrzeżenie na temat usług zależnych, które program instalacyjny musi również usunąć. W większości przypadków należy kliknąć przycisk Cancel, aby zachować poprzedni wybór. Jeśli kliknięty zostanie przycisk Remove Dependent Role Services (Usuń zależne usługi ról), program instalacyjny usunie zaznaczone poprzednio usługi zależne, które mogłyby powodować, że serwer sieci Web nie będzie funkcjonował zgodnie z oczekiwaniami.

9. Kliknąć przycisk Next. Na stronie Confirm Installation Selections (Potwierdzenie wybranych opcji instalacji) kliknąć odnośnik Print, E-mail, Or Save This Information (Wydrukuj, wyślij e-mail lub zapisz te informacje), aby wygenerować raport dotyczący instalacji i wyświetlić go w programie Windows Internet Explorer. Można następnie posłużyć się standardowymi funkcjami programu Windows Internet Explorer, aby raport ten wydrukować bądź zapisać. Po przejrzaniu opcji instalacji i w razie potrzeby ich zapisaniu, kliknąć przycisk Install, aby rozpocząć proces instalacji.

10. Po zakończeniu instalacji serwera aplikacji wraz z wybranymi funkcjami wyświetlona zostaje strona Installation Results (Wyniki instalacji). Przejrzeć informacje szczegółowe na temat przebiegu instalacji, aby upewnić się, że wszystkie jej fazy zakończyły się prawidłowo. Jeśli jakkolwiek fragment instalacji zakończył się niepowodzeniem, za-

notować przyczynę, a następnie posłużyć się następującymi metodami rozwiązywania problemów:

- a. Kliknąć łącze Print, E-mail, Or Save The Installation Report, aby utworzyć lub aktualizować raport dotyczący instalacji i wyświetlić go w programie Windows Internet Explorer.
- b. Przewinąć w dół raport instalacji w oknie przeglądarki, a następnie kliknąć Full Log (For Troubleshooting Only) [Pełny dziennik], aby wyświetlić dziennik programu Server Manager w Notatniku.
- c. W notatniku nacisnąć Ctrl+F, wpisać bieżącą datę w odpowiednim formacie (zgodnym z ustawieniami regionalnymi), jak na przykład 2007-08-30, a następnie kliknąć przycisk Find Next (Znajdź następny). W ten sposób w programie Notatnik znaleziony zostanie pierwszy wpis dotyczący instalacji, który odpowiada wprowadzonej dacie.
- d. Przejrzeć wpisy programu Server Manager dotyczące problemów występujących podczas instalacji i wprowadzić odpowiednie korekty.

Instalowanie serwerów sieci Web

Serwery sieci Web instalowane są zgodnie z następującą procedurą:

1. Uruchomić program Server Manager klikając ikonę Server Manager na pasku narzędzi Quick Launch lub klikając kolejno menu Start, Administrative Tools (Narzędzia administracyjne), Server Manager.
2. W programie Server Manager, w oknie z lewej strony zaznaczyć węzeł Roles, a następnie w ramce Roles Summary (Podsumowanie ról) kliknąć odnośnik Add Roles (Dodaj role). Uruchomiony zostanie program Add Roles Wizard. Jeśli kreator wyświetli stronę Before You Begin, należy przeczytać informacje na stronie powitalnej, a następnie kliknąć przycisk Next. Strona powitalna nie będzie wyświetlana przy kolejnym uruchomieniu kreatora, jeśli przed kliknięciem przycisku Next zaznaczone zostanie pole wyboru Do Not Show Me This Page Again.
3. Na stronie Select Server Roles wybrać opcję Web Server (IIS). Następnie wyświetlone zostanie okno dialogowe Add Features Required For Web Server (Dodawanie funkcji wymaganych dla serwera Web). W tym oknie wymienione są funkcje wymagane do zainstalowania serwera sieci Web. Kliknąć przycisk Add Required Features (Dodaj wymagane funkcje), aby zamknąć okno dialogowe i dodać do instalacji serwera Web składniki Windows Activation Service. Dwa razy kliknąć przycisk Next, aby kontynuować procedurę.
4. Na stronie Select Role Services program instalacyjny określa podstawowy zestaw domyślnych funkcji standardowych. Podczas zaznaczania lub usuwania zaznaczenia usług ról warto uwzględnić poniższe uwagi, zanim kliknięty zostanie przycisk Next:
 - Jeśli usługa roli zaznaczona została razem z dodatkowymi funkcjami wymaganymi, wyświetlone zostanie okno dialogowe, w którym wymienione są dodatkowe role wymagane. Po przejrzaniu ról wymaganych należy kliknąć przycisk Add Required Role Services, aby zaakceptować dodatki i zamknąć okno dialogowe. Jeśli kliknięty

zostanie przycisk Cancel, program instalacyjny usunie zaznaczenie poprzednio wybranych funkcji.

- Jeśli zachodzi potrzeba usunięcia usługi roli, która jest wymagana na podstawie poprzednio dokonanego wyboru, wyświetlone zostaje ostrzeżenie na temat usług zależnych, które program instalacyjny musi również usuwać. W większości przypadków należy kliknąć przycisk Cancel, aby zachować poprzedni wybór. Jeśli kliknięty zostanie przycisk Remove Dependent Role Services (Usuń zależne usługi ról), program instalacyjny usunie zaznaczone poprzednio usługi zależne, które mogłyby powodować, że serwer sieci Web nie będzie funkcjonował zgodnie z oczekiwaniami.
5. Kliknąć przycisk Next. Na stronie Confirm Installation Selections (Potwierdzenie wybranych opcji instalacji) kliknąć odnośnik Print, E-mail, Or Save This Information, aby wygenerować raport dotyczący instalacji i wyświetlić go w programie Windows Internet Explorer. Można następnie posłużyć się standardowymi funkcjami programu Windows Internet Explorer, aby raport ten wydrukować bądź zapisać. Po przejrzaniu opcji instalacji i w razie potrzeby ich zapisaniu, kliknąć przycisk Install, aby rozpocząć proces instalacji.
 6. Po zakończeniu instalacji serwera aplikacji wraz z wybranymi funkcjami wyświetlona zostaje strona Installation Results (Wyniki instalacji). Przejrzeć informacje szczegółowe na temat przebiegu instalacji, aby upewnić się, że wszystkie jej fazy zakończyły się prawidłowo. Jeśli jakikolwiek fragment instalacji zakończył się niepowodzeniem, zanotować przyczynę, a następnie posłużyć się następującymi metodami rozwiązywania problemów:
 - a. Kliknąć łącze Print, E-mail, Or Save The Installation Report, aby utworzyć lub aktualizować raport dotyczący instalacji i wyświetlić go w programie Windows Internet Explorer.
 - b. Przewinąć w dół raport instalacji w oknie przeglądarki, a następnie kliknąć odnośnik Full Log (For Troubleshooting Only), aby wyświetlić dziennik programu Server Manager w Notatniku.
 - c. W notatniku nacisnąć Ctrl+F, wpisać bieżącą datę w odpowiednim formacie (zgodnym z ustawieniami regionalnymi), jak na przykład 2007-08-30, a następnie kliknąć przycisk Find Next. W ten sposób w programie Notatnik znaleziony zostanie pierwszy wpis dotyczący instalacji, który odpowiada wprowadzonej dacie.
 - d. Przejrzeć wpisy programu Server Manager dotyczące problemów występujących podczas instalacji i wprowadzić odpowiednie korekty.

Instalowanie oprogramowania Windows SharePoint Services

Usługi Windows SharePoint stosują dwie istotnie różne konfiguracje: niezależna konfiguracja serwera i zależna konfiguracja równoważenia obciążenia. W przypadku niezależnej konfiguracji serwera oprogramowanie Windows SharePoint Services instalowane jest na pojedynczym serwerze, który ma swoją własną bazę danych do przechowywania informacji o aplikacji i użytkownika. Dla zależnej konfiguracji równoważenia obciążenia usługi SharePoint instalowane są na komputerze jako część farmy sieci Web, gdzie wszystkie serwery współużytkują bazę danych Microsoft SQL Server 2000 lub SQL Server 2005. Chociaż

oba typy instalacji konfigurowane są przy użyciu podobnego początkowo procesu, jeśli zachodzi potrzeba podłączenia się do bazy danych SQL Server i wykorzystywania równoważenia obciążeń, należy konfigurować serwer, jako część farmy sieci Web.

Uwaga Oprogramowanie Windows SharePoint Services 2008 jest uzupełnieniem systemu operacyjnego Windows Server 2008. Ponieważ oprogramowanie Windows SharePoint Services 2008 nie jest dołączane do systemu Windows Server 2008, musi być instalowane oddzielnie. Po pobraniu pakietów instalacyjnych z firmy Microsoft i ich uruchomieniu, można skonfigurować tę rolę przy użyciu programu Server Manager, co zostało opisane w tym podrozdziale. Ponieważ jednak usługi SharePoint są dodatkiem, mogą różnić się strony kreatora i powiązane opcje instalacyjne.

Oprogramowanie Windows SharePoint Services może być instalowane na komputerze zgodnie z poniższą procedurą:

1. Uruchomić program Server Manager klikając ikonę Server Manager na pasku narzędzi Quick Launch lub klikając kolejno menu Start, Administrative Tools, Server Manager.
2. W programie Server Manager, w oknie z lewej strony zaznaczyć węzeł Roles, a następnie w ramce Roles Summary (Podsumowanie ról) kliknąć odnośnik Add Roles (Dodaj rolę). Uruchomiony zostanie program Add Roles Wizard. Jeśli kreator wyświetli stronę Before You Begin, należy przeczytać informacje na stronie powitalnej, a następnie kliknąć przycisk Next. Strona powitalna nie będzie wyświetlana przy kolejnym uruchomieniu kreatora, jeśli przed kliknięciem przycisku Next zaznaczone zostanie pole wyboru Do Not Show Me This Page Again.
3. Na stronie Select Server Roles zaznaczyć opcję Windows SharePoint Services. Wyświetlone zostanie okno dialogowe Add Role Services And Features Required For Windows SharePoint Services (Dodawanie usług ról i funkcji wymaganych dla Windows SharePoint Services). Zgodnie informacjami zamieszczonymi w tabeli 2-1, w tym oknie dialogowym wymienione są funkcje wymaganego zainstalowania usług SharePoint. Kliknąć przycisk Add Required Features, aby zamknąć okno dialogowe i dodać składniki Web Server (IIS), Windows Activation Service oraz .NET Framework 3.0 do instalacji usług SharePoint. Kliknąć przycisk Next.
4. Przeczytać wprowadzenie do oprogramowania Windows SharePoint Services. W razie potrzeby kliknąć odnośnik umożliwiający dokładniejsze zapoznanie się z funkcjami oferowanymi przez program Windows SharePoint Services. Kliknąć przycisk Next, aby kontynuować.
5. Na stronie Select Configuration Type (Wybieranie typu konfiguracji) wskazać typ instalacji. Jeśli instalowane będzie rozwiązanie oparte na pojedynczym serwerze, zaznaczyć opcję Install Only On This Server (Instaluj tylko na tym serwerze), a następnie kliknąć przycisk Next. Jeśli natomiast serwer będzie instalowany, jako część farmy sieci Web, należy zaznaczyć opcję Install As Part Of A Server Farm (Instaluj, jako część farmy serwerów), a następnie kliknąć przycisk Next.
6. Choć w poszczególnych witrynach usług SharePoint można używać różnych języków, witryna administracji programu Windows SharePoint Services może korzystać tylko z języka wybranego podczas instalowania i nie jest możliwa późniejsza zmiana tego języka. Na stronie Select The Language For The Administration Site (Wybieranie języka witryny administracyjnej) z listy rozwijanej wybrać odpowiedni język witryny administracyjnej, jak na przykład English czy German, a następnie kliknąć przycisk Next.

7. Jeśli instalowana jest konfiguracja pojedynczego serwera dla usług Windows SharePoint, na stronie Specify E-mail Settings (Określenie ustawień e-mail), skonfigurować ustawienia dotyczące domyślnej poczty e-mail, która będzie używana przez usługi SharePoint do wysyłania powiadomień do administratorów. Należy skonfigurować następujące opcje:
- Outbound SMTP Server (Serwer poczty wychodzącej SMTP)** Określenie w pełni kwalifikowanej nazwy domeny serwera e-mail, który będzie wysyłał powiadomienia do administratorów, jak na przykład mail.adatum.com.
 - From E-mail Address (Adres e-mail pola Od)** Określenie dla wiadomości powiadomienia adresu e-mail, który jest wyświetlany w polu From (Od), jak na przykład wss-admin@adatum.com.
 - Reply-To E-mail Address (Adres e-mail odpowiedzi)** Określenie dla wiadomości powiadomienia adresu e-mail, na który kierowana jest odpowiedź, jak na przykład wss-incoming@adatum.com.
8. Jeśli poprzednio nie był zainstalowany składnik Web Server (IIS), kliknąć dwa razy przycisk Next, aby wyświetlić stronę Select Role Services dla funkcji serwera sieci Web. Następnie można wybrać do zainstalowania funkcję serwera sieci Web. W większości przypadków wybierane są dodatkowe funkcje. Podczas zaznaczania lub usuwania zaznaczenia usług ról warto uwzględnić poniższe uwagi, zanim kliknięty zostanie przycisk Next:
- Jeśli usługa roli zaznaczona została razem z dodatkowymi funkcjami wymaganymi, wyświetlone zostanie okno dialogowe, w którym wymienione są dodatkowe role wymagane. Po przejrzaniu ról wymaganych należy kliknąć przycisk Add Required Role Services, aby zaakceptować dodatki i zamknąć okno dialogowe. Jeśli kliknięty zostanie przycisk Cancel, program instalacyjny usunie zaznaczenie poprzednio wybranych funkcji.
 - Jeśli zachodzi potrzeba usunięcia usługi roli, która jest wymagana na podstawie poprzednio dokonanego wyboru, wyświetlone zostaje ostrzeżenie na temat usług zależnych, które program instalacyjny musi również usunąć. W większości przypadków należy kliknąć przycisk Cancel, aby zachować poprzedni wybór. Jeśli kliknięty zostanie przycisk Remove Dependent Role Services, program instalacyjny usunie zaznaczone poprzednio usługi zależne, które mogłyby powodować, że serwer sieci Web nie będzie funkcjonował zgodnie z oczekiwania.
9. Na stronie Confirm Installation Selections kliknąć odnośnik Print, E-mail, Or Save This Information, aby wygenerować raport dotyczący instalacji i wyświetlić go w programie Windows Internet Explorer. Można następnie posłużyć się standardowymi funkcjami programu Windows Internet Explorer, aby raport ten wydrukować bądź zapisać. Po przejrzaniu opcji instalacji i w razie potrzeby ich zapisaniu, kliknąć przycisk Install, aby rozpocząć proces instalacji.
10. Jeśli serwer konfigurowany jest jako część farmy sieci Web, należy skonfigurować połączenie do współużytkowanej bazy danych SQL Server i wykonać inne wstępne zadania instalacyjne za pomocą narzędzia Windows SharePoint Services Central Administration.
11. Po zakończeniu instalacji serwera aplikacji wraz z wybranymi funkcjami wyświetlona zostaje strona Installation Results. Przejrzeć informacje szczegółowe na temat przebiegu instalacji, aby upewnić się, że wszystkie jej fazy zakończyły się prawidłowo. Jeśli jakikolwiek fragment instalacji zakończył się niepowodzeniem, zanotować przyczynę, a następnie posłużyć się następującymi metodami rozwiązywania problemów:

- a. Kliknąć łącze Print, E-mail, Or Save The Installation Report, aby utworzyć lub aktualizować raport dotyczący instalacji i wyświetlić go w programie Windows Internet Explorer.
- b. Przewinąć w dół raport instalacji w oknie przeglądarki, a następnie kliknąć Full Log (For Troubleshooting Only), aby wyświetlić dziennik programu Server Manager w Notatniku.
- c. W notatniku nacisnąć Ctrl+F, wpisać bieżącą datę w odpowiednim formacie (zgodnym z ustawieniami regionalnymi), jak na przykład 2007-08-30, a następnie kliknąć przycisk Find Next (Znajdź następny). W ten sposób w programie Notatnik znaleziony zostanie pierwszy wpis dotyczący instalacji, który odpowiada wprowadzonej dacie.
- d. Przejrzeć wpisy programu Server Manager dotyczące problemów występujących podczas instalacji i wprowadzić odpowiednie korekty.

Dodawanie lub usuwanie funkcji serwera sieci Web w systemie Windows Vista

We wcześniejszych wersjach systemów Windows do dodawania lub usuwania składników systemu operacyjnego był używany moduł Add/Remove Windows Components (Dodaj/Usuń składniki systemu Windows), który znajdował się w aplikacji Add or Remove Programs (Dodaj lub usuń programy). W systemie Windows Vista składniki systemu operacyjnego są konfigurowane jako funkcje systemu Windows, które można włączać lub wyłączać, a nie dodawać lub usuwać.

Funkcje serwera sieci Web można skonfigurować na komputerze systemu Windows Vista stosując się do następującej procedury:

1. Kliknąć menu Start, a następnie Panel sterowania.
2. W Panelu sterowania kliknąć aplikację Programy.
3. W grupie Programs And Features (Programy i funkcje) kliknąć Turn Windows Features On Or Off (Włącz lub wyłącz funkcje systemu Windows). Wyświetlone zostanie okno dialogowe Windows Features (Funkcje systemu Windows).
4. Funkcje systemu Windows dla serwerów sieci Web znajdują się w następujących węzłach:
 - Internet Information Services/FTP Publishing Service (Internetowe usługi informacyjne/Usługa FTP)** Znajdują się tu programy FTP Management Console (Konsola zarządzania usługą FTP) i FTP Server
 - Internet Information Services/Web Management Tools (IIS/Narzędzia zarządzania siecią Web)** Znajdują się tu składniki IIS 6 Management i IIS 7.0 Management (Zarządzanie usługami IIS 6 i IIS 7)
 - Internet Information Services/World Wide Web Services (IIS/Usługi WWW)** Znajdują się tu funkcje Application Development (Funkcje tworzenia aplikacji), Common HTTP (Wspólne funkcje HTTP), Health and Diagnostics (Stan i diagnostyka), Performance (Funkcje wydajnościowe) i Security (Zabezpieczenia)
 - Microsoft .NET Framework 3.0** Znajdują się tu składniki XPS View, HTTP Activation i Non-HTTP Activation dla WCF

- ❑ **Microsoft Message Queue (MSMQ) Server (Serwer usługi MSMQ)** Znajdują się tu podstawowe składniki serwera MSMQ, a oprócz tego składniki obsługi i integracji kolejkowania wiadomości
- ❑ **Windows Process Activation Service (Usługa aktywacji procesów systemu Windows)** Znajdują się tu składniki .NET Environment (Środowisko .NET), Configuration APIs (Konfiguracyjne interfejsy API) i Process Model (Schemat procesów)

W celu włączenia funkcji należy zaznaczyć odpowiednie pola wyboru, a wyłączenie funkcji polega na usunięciu zaznaczenia odpowiedniego pola wyboru. Po zaznaczeniu funkcji system Windows Vista automatycznie wybiera wszystkie powiązane funkcje wymagane bez generowania komunikatów.

5. Po kliknięciu przycisku OK system Windows Vista rekonfiguruje składniki zgodnie z wprowadzonymi zmianami. Być może potrzebny będzie oryginalny nośnik instalacyjny.

Zarządzanie zainstalowanymi rolami i usługami ról

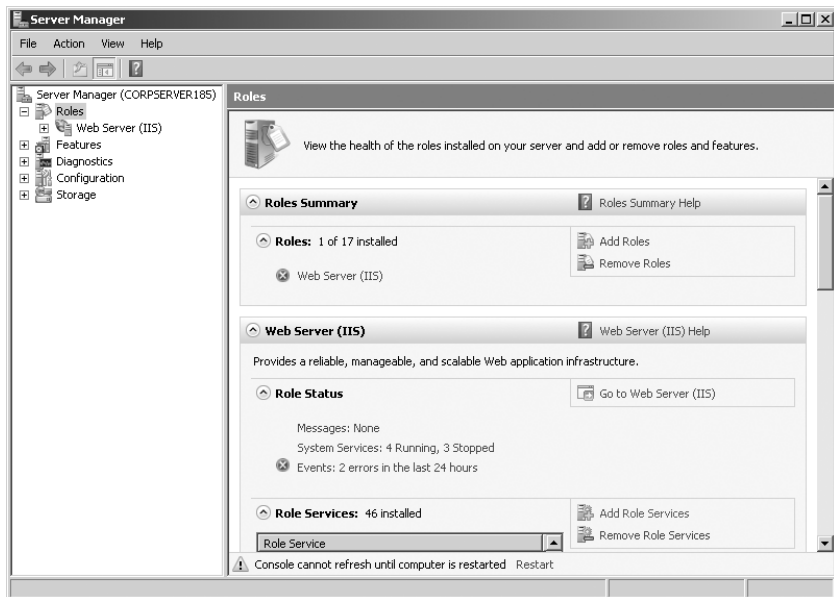
W przypadku wykorzystywania serwerów aplikacji, sieci Web i serwerów usług SharePoint podstawowym narzędziem używanym do zarządzania rolami i usługami ról jest program Server Manager (Menedżer serwera). Program ten używany jest do dodawania lub usuwania ról bądź usług ról, a także do przeglądania informacji szczegółowych o konfiguracji i stanie ról i usług ról.

Przeglądanie skonfigurowanych ról i usług ról

W systemie Windows Server program Server Manager wyświetla zainstalowane role po zaznaczeniu węzła Roles (Role), znajdującego się w oknie z lewej strony. Zgodnie z rysunkiem 2-3 w głównym widoku węzła Roles wyświetlana jest sekcja Roles Summary (Podsumowanie ról), w której wyświetlona jest liczba ról i nazwy zainstalowanych ról. Jeśli dla danej roli serwera wystąpiło zdarzenie związane z błędnym działaniem, w programie Server Manager wyświetlana jest ikona ostrzeżenia (z lewej strony nazwy roli).

W oknie Roles nazwa roli jest jednocześnie odnośnikiem, kliknięcie którego powoduje wyświetlenie informacji szczegółowych o wybranej roli. Informacje te obejmują następujące dane:

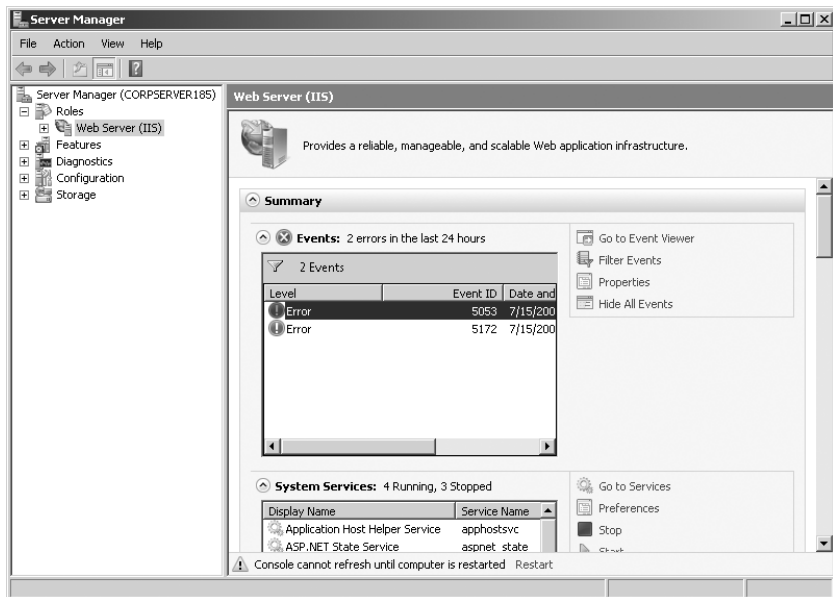
- Informacje podsumowania dotyczące stanu powiązanych usług systemowych. Jeśli ma to zastosowanie, w programie Server Manager wyświetlana jest liczba powiązanych usług, które są zatrzymane bądź uruchomione, jak na przykład „System Services: 3 Running, 2 Stopped” (Usługi systemowe: 3 uruchomione, 2 zatrzymane).
- Informacje podsumowania dotyczące zdarzeń, które zostały wygenerowane w ostatnich 24 godzinach przez powiązane usługi i składniki, wliczając w to informacje szczegółowe na temat, czy błędy miały miejsce, jak na przykład „Events: 1 error(s), 6 warning(s), 2 informational in the last 24 hours” (Zdarzenia: 1 błąd, 6 ostrzeżeń, 2 informacje w ciągu ostatnich 24 godzin).
- Informacje podsumowania na temat zainstalowanych usług ról, wliczając w to liczbę zainstalowanych usług ról oraz stan (zainstalowana, niezainstalowana) w odniesieniu do usług ról, których można używać razem z daną rolą.



Rysunek 2-3 Przegląd informacji o stanie zainstalowanych ról.

Wskazówka Domyślnie program Server Manager odświeża informacje szczegółowe co godzinę. Informacje te mogą być odświeżone ręcznie poprzez kliknięcie przycisku Refresh (Odśwież), znajdującym się w menu Action. Jeśli zachodzi potrzeba skonfigurowania innego domyślnego interwału odświeżania, należy kliknąć polecenie Configure Refresh (Konfiguruj odświeżanie), znajdujące się na dole okna Summary, posłużyć się dostępnymi opcjami do zdefiniowania nowego okresu odświeżania, a następnie kliknąć przycisk OK.

W głównym oknie programu Server Manager, jeśli w sekcji Roles Summary zostanie kliknięta rola lub odnośnik Go To Manage Roles (Przejdź do zarządzanej roli), w programie Server Manager wyświetlone zostają rozszerzone informacje podsumowania dotyczące zdarzeń i usług związanych z powiązaną rolą. Zgodnie z rysunkiem 2-4 w programie Server Manager wyświetlone są wszystkie zdarzenia mające miejsce w ostatnich 24 godzinach. Po kliknięciu zdarzenia, a następnie kliknięciu przycisku View Event Properties (Wyświetl właściwości zdarzenia), można uzyskać informacje szczegółowe na temat zdarzenia. Ponadto program Server Manager udostępnia szczegółowe informacje w odniesieniu do usług systemu używanych przez rolę. Usługą można zarządzać klikając daną usługę, a następnie klikając odpowiednie odnośniki Stop, Start lub Restart. W wielu przypadkach, jeśli usługa nie jest uruchomiona, a administrator sądzi, że powinna być, może kliknąć polecenie Restart, aby rozwiązać kwestię poprzez zatrzymanie, a następnie uruchomienie usługi.



Rysunek 2-4 Przeglądanie ostatnich zdarzeń i zarządzanie usługami systemowymi.

Dodawanie lub usuwanie ról serwera

Po zaznaczeniu węzła Roles w programie Server Manager w sekcji Roles Summary wyświetlone są informacje szczegółowe o zainstalowanych rolach. W sekcji Roles Summary umieszczone zostały opcje pozwalające na dodawanie bądź usuwanie ról. Rolę można dodać zgodnie z opisem zamieszczonym we wcześniejszym podrozdziale „Konfigurowanie usług IIS 7.0”. W zależności od typu serwera można usuwać różne role:

- Na serwerze aplikacji można usuwać rolę serwera aplikacji, serwera sieci Web lub obie.
- Na serwerze sieci Web można usuwać rolę serwera sieci Web.
- Na komputerze z uruchomionymi usługami SharePoint można usuwać rolę Windows SharePoint Services lub obie role: Windows SharePoint Services i serwer sieci Web.

Rolę serwera można usuwać postępując zgodnie z następującą procedurą:

1. Uruchomić program Server Manager klikając ikonę Server Manager na pasku narzędzi Quick Launch lub klikając kolejno menu Start, Administrative Tools, Server Manager.
2. W programie Server Manager, w oknie z lewej strony zaznaczyć węzeł Roles, a następnie w ramce Roles Summary kliknąć odnośnik Remove Roles (Usuń rolę). Uruchomiony zostanie program Remove Roles Wizard (Kreator usuwania ról). Jeśli kreator wyświetli stronę Before You Begin, należy przeczytać informacje na stronie powitalnej, a następnie kliknąć przycisk Next. Strona powitalna nie będzie wyświetlana przy kolejnym uru-

chomieniu kreatora, jeśli przed kliknięciem przycisku Next zaznaczone zostanie pole wyboru Do Not Show Me This Page Again.

3. Na stronie Remove Server Roles usunąć zaznaczenie pola wyboru odnoszącego się do roli, która ma być usunięta, a następnie kliknąć przycisk Next. Jeśli następuje próba usunięcia roli, od której zależy inna rola, wyświetlone zostanie ostrzeżenie informujące, że rola nie może być usunięta, chyba że usunięta zostanie również inna rola. Jeśli kliknięty zostanie przycisk Remove Dependent Role Services (Usuń zależne usługi ról), program instalacyjny usunie obie role.
4. Na stronie Confirm Removal Selections przejrzeć powiązane usługi ról, które będą usunięte przez program instalacyjny w oparciu o poprzednio dokonane wybory, a następnie kliknąć przycisk Remove.
5. Po zakończeniu modyfikowania konfiguracji przez program instalacyjny wyświetlona zostaje strona Removal Results (Wyniki usuwania). Przejrzeć informacje szczegółowe na temat modyfikacji, aby upewnić się, że wszystkie fazy procesu usuwania zakończyły się prawidłowo. Jeśli jakikolwiek fragment procesu zakończył się niepowodzeniem, należy zanotować przyczynę, a następnie posłużyć się poprzednio opisanymi metodami rozwiązywania problemów.

Przeglądanie i modyfikowanie usług ról na serwerach

W programie Server Manager można przeglądać usługi ról skonfigurowane dla roli poprzez zaznaczenie węzła Roles w oknie z lewej strony, a następnie przewinąć w dół do sekcji Role Services (Usługi ról), by znaleźć rolę, która ma być opracowywana. W sekcji informacji szczegółowych znajduje się lista usług ról, które można instalować, niezależnie od ich stanu bieżącego (Zainstalowana/Niezainstalowana). Usługi ról serwerów aplikacji i serwerów sieci Web mogą być zarządzane za pomocą funkcji Add Role Services i Remove Role Services udostępnianych dla wpisu dotyczącego powiązanej roli. Rola Windows SharePoint Services nie ma jednak indywidualnych usług ról, którymi w ten sposób można zarządzać. W przypadku serwera z uruchomionymi usługami SharePoint można modyfikować rolę serwera sieci Web lub jedynie usunąć rolę Windows SharePoint Services.

Dodawanie usług ról wiąże się z wykonaniem następującej procedury:

1. Uruchomić program Server Manager klikając ikonę Server Manager na pasku narzędzi Quick Launch lub klikając kolejno menu Start, Administrative Tools, Server Manager.
2. W programie Server Manager zaznaczyć węzeł Roles w oknie z lewej strony, a następnie przewinąć w dół, aż pojawi się sekcja Roles Services dla roli, która ma być zarządzana. W sekcji Roles Services dla tej roli kliknąć przycisk Add Role Services (Dodaj usługę roli). Uruchomiony zostaje program Add Role Services Wizard (Kreator dodawania usług roli).
3. Na stronie Select Role Services (Wybieranie usług roli), aktualnie wybrane role są niedostępne, tak że nie można ich zaznaczać. W celu dodania roli należy ją zaznaczyć na liście Role Services. Po zakończeniu wybierania ról, które mają być dodane, kliknąć przycisk Next, a następnie przycisk Install.

Usługi ról mogą być usuwane zgodnie z następującą procedurą:

1. Uruchomić program Server Manager klikając ikonę Server Manager na pasku narzędzi Quick Launch lub klikając kolejno menu Start, Administrative Tools, Server Manager.

2. W programie Server Manager, w oknie z lewej strony zaznaczyć węzeł Roles, a następnie przewinąć w dół, aż pojawi się sekcja Roles Services dla roli, która ma być zarządzana. W sekcji Roles Services dla tej roli kliknąć przycisk Remove Role Services (Usuń usługi roli). Uruchomiony zostaje program Remove Role Services Wizard (Kreator usuwania usług roli).
3. Na stronie Select Role Services aktualnie wybrane role są zaznaczone. W celu usunięcia roli należy usunąć zaznaczenie odpowiednich pól wyboru. Po zakończeniu zaznaczania ról, które mają być usunięte, kliknąć przycisk Next, a następnie przycisk Remove.