

Microsoft SharePoint 2013 PL

Architektura
i skuteczne
rozwiązania

Tytuł oryginału: Microsoft SharePoint 2013 Designing and Architecting Solutions

Tłumaczenie: Radosław Meryk

ISBN: 978-83-283-0618-9

Authorized translation from the English language edition: MICROSOFT SHAREPOINT 2013 DESIGNING AND ARCHITECTING SOLUTIONS; ISBN 0735671680; by Shannon Bray, and by Miguel Wood, and by Patrick Curran; published by Microsoft Press, a division of Microsoft Corporation, Inc. Copyright © 2013 by Shannon Bray, Miguel Wood, and Patrick Curran.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from Pearson Education, Inc., or Microsoft Press. Polish language edition published by HELION S.A., under license and with the permission of Pearson Education, Inc. Copyright © 2015.

Microsoft and the trademarks listed at:

<http://www.microsoft.com/about/legal/en/us/IntellectualProperty/Trademarks/EN-US.aspx> are trademarks of the Microsoft group of companies.

All other marks are property of their respective owners.

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiegokolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autor oraz Wydawnictwo HELION dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autor oraz Wydawnictwo HELION nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

Wydawnictwo HELION

ul. Kościuszki 1c, 44-100 GLIWICE

tel. 32 231 22 19, 32 230 98 63

e-mail: helion@helion.pl

WWW: <http://helion.pl> (księgarnia internetowa, katalog książek)

Drogi Czytelniku!

Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres

<http://helion.pl/user/opinie/mish13>

Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Pliki z przykładami omawianymi w książce można znaleźć pod adresem:

<ftp://ftp.helion.pl/przyklady/mish13.zip>

Printed in Poland.

- [Kup książkę](#)
- [Poleć książkę](#)
- [Oceń książkę](#)

- [Księgarnia internetowa](#)
- [Lubię to! » Nasza społeczność](#)

Spis treści

Wprowadzenie	11
---------------------------	-----------

CZĘŚĆ I PLANOWANIE WDROŻENIA PROGRAMU MICROSOFT SHAREPOINT 2013

Rozdział 1 Architektura programu Microsoft SharePoint 2013	21
Komponenty farmy SharePoint	21
Hierarchia farmy programu SharePoint	22
Foldery	33
Elementy list	34
System plików programu SharePoint	35
Pliki serwera IIS	35
Główny katalog programu SharePoint	38
Awaryjne zastępowanie funkcji	40
Rozwiązania zainstalowane	41
Bazy danych programu SharePoint	43
Aliasy SQL Server	43
Systemowe bazy danych programu SharePoint	44
Bazy danych aplikacji usługowych programu SharePoint	45
Podsumowanie	47
Rozdział 2 Windows PowerShell i komandlety obsługi programu SharePoint 2013	51
Rola mechanizmu Windows PowerShell	52
Krótka historia mechanizmu Windows PowerShell	52
Podstawowa składnia Windows PowerShell	53
Korzyści ze stosowania mechanizmu Windows PowerShell	53
Usprawnienia wprowadzone w systemie Windows PowerShell 3.0	55
Konfigurowanie uprawnień użytkowników dla Windows PowerShell oraz systemu SharePoint 2013	56
Powłoka zarządzania Windows PowerShell	58
Wybór profilu do wykorzystania w środowisku Windows PowerShell ISE	60
Korzystanie z komandletów Windows PowerShell	61

Komandlety Windows PowerShell specyficzne dla programu SharePoint	65
Zwalnianie pamięci zajmowanej przez obiekty programu SharePoint	67
Podsumowanie	69
Utworzenie przykładowej witryny (zbioru witryn)	69
Zarządzanie topologią usługowej aplikacji wyszukiwania systemu SharePoint 2013	69

Rozdział 3	Zbieranie wymagań	71
	Znaczenie zbierania wymagań	71
	Po co zbierać wymagania?	72
	Kiedy należy zbierać wymagania?	72
	Skuteczne planowanie	73
	Identyfikacja interesariuszy	74
	Cele biznesowe	75
	Rezultaty	76
	Architektura informacyjna	79
	Architektura logiczna	82
	Architektura fizyczna	83
	Wymagania systemowe	84
	Minimalne wymagania sprzętowe i programowe	84
	SharePoint Online i architektury hybrydowe	85
	Podsumowanie	91

CZĘŚĆ II ASPEKTY PROJEKTOWANIA DOTYCZĄCE SYSTEMU MICROSOFT SHAREPOINT 2013

Rozdział 4	Model aplikacji usługowych	99
	Architektura aplikacji usługowych	100
	Kluczowe pojęcia	100
	Składowe aplikacje usługowych	101
	Punkt końcowy aplikacji usługowej korzystający z frameworka WCF	102
	Serwery proxy aplikacji usługowych	102
	Implementacja aplikacji usługowej	103
	Aplikacje usługowe i bazy danych	103
	Zmiany w OWA	104
	Jak to działa?	105
	Zmiany w przepływach pracy	105
	Jak to działa?	107
	Nowe aplikacje usługowe sieci Web dostępne w programie SharePoint 2013	107
	Access Services	108
	Usługa zarządzania aplikacjami	109
	Usługa tłumaczenia maszynowego	109
	Aplikacja usługi zarządzania pracą WMS	110

Zaktualizowane aplikacje usługowe sieci Web dostępne w programie SharePoint 2013	111
Usługi Access 2010	111
Usługa BDC	112
Usługi Excelsa	113
Aplikacja MMS	113
Aplikacja PPS	114
Aplikacja usługi wyszukiwania	115
SSS	118
UPA	118
VGS	119
WAS	120
Aplikacje usługowe, które SharePoint tworzy automatycznie	121
Aplikacja usługi odnajdowania aplikacji i równoważenia obciążenia	121
STS	122
Federacja usług	123
Podsumowanie	124
Tworzenie relacji zaufania pomiędzy farmami	125
Konfiguracja usługi topologii	126
Publikowanie aplikacji usługowej	127
Nawiązanie połączenia z aplikacją usług	128
Ustawienia uprawnień aplikacji usługowej	129
Rozdział 5 Wymagania w zakresie pamięci zewnętrznej dla programu SharePoint	131
Wymagania silnika bazy danych dla systemu SharePoint 2013	132
Przegląd opcji HA	133
Klustry pracy awaryjnej	133
Dublowanie bazy danych	133
Wysyłanie dziennika	133
Egzemplarze klastrów pracy awaryjnej AlwaysOn	134
Grupy dostępności AlwaysOn	134
Wstępna optymalizacja i konfiguracja systemu SQL Server dla programu SharePoint 2013	134
Sortowanie w systemie SQL Server	134
Opcja MDOP w systemie SQL Server	135
Dodatkowe aspekty instalacji systemu SQL Server	136
Przegląd baz danych systemu SharePoint Server 2013 oraz pełnionych przez nie ról	143
Bazy danych w systemie SharePoint Foundation 2013	143
Bazy danych w systemie SharePoint Server 2013	147
Bazy danych zintegrowanych usług raportowania w programie SharePoint 2013	149
Systemowe bazy danych SQL Server 2008 R2 (SP1) i SQL Server 2012	150
Planowanie objętości baz danych systemu SharePoint 2013	150
Pamięć masowa SQL Server a IOPS	150
Funkcje analityki biznesowej systemu SQL Server wewnątrz instalacji SharePoint 2013	152
Funkcjonalność Shredded Storage w programie SharePoint 2013	165

Podsumowanie	166
SQLIO	167
Testowanie wewnętrznych dysków systemu SQL Server	167
Testowanie dysków sieciowych iSCSI	170
Testowanie dysków SQL Server programu SharePoint	172
Testowanie obciążenia dysków SQL Server	172
Dane o wydajności podsystemu dyskowego	172
Rozdział 6 Wymagania w zakresie uwierzytelniania i autoryzacji	175
Analiza opcji AuthN	175
Uwierzytelnianie Windows	176
Uwierzytelnianie anonimowe	186
Uwierzytelnianie bazujące na oświadczeniach	187
Składniki i metody uwierzytelniania w programie SharePoint	199
Strefy uwierzytelniania	199
Mapowania AAM	200
Samoobsługowe tworzenie witryn	200
Nagłówki hosta zbioru witryn	202
Usługi uwierzytelniania (AuthN)	202
Usługa c2WTS	202
Usługa bezpiecznego magazynu	203
Usługi łączności biznesowej	204
Przegląd funkcji autoryzacji AuthZ	205
Zasady aplikacji	205
Kontrolka wyboru osób	208
Udostępnianie	209
Podsumowanie	210
Rozdział 7 Projektowanie bezpieczeństwa platformy	215
Blokowanie, śledzenie instalacji programu Microsoft SharePoint	
i tworzenie raportów na jej temat	216
Blokowanie instalacji programu SharePoint	216
Śledzenie instalacji programu SharePoint	217
Tworzenie raportów na temat instalacji programu SharePoint	219
Szyfrowanie komunikacji	219
Urzędy certyfikacji (CA)	220
Komunikacja pomiędzy klientem a serwerem	221
Komunikacja serwer-serwer	224
Komunikacja pomiędzy serwerami w programie SharePoint	224
SSL i SQL Server	226
IPsec IKEv2	228

Planowanie i konfigurowanie funkcji Microsoft SQL Server Transparent Data Encryption	230
Instalowanie programu SharePoint za pomocą najmniejszych uprawnień	233
Pule aplikacji	234
Konta użytkowników	234
Zarządzane konta programu SharePoint	238
Role i uprawnienia grup	239
Role	239
Uprawnienia grup	240
Podsumowanie	240
Rozdział 8 Aktualizacja środowiska SharePoint 2010	245
Wprowadzenie w tematykę aktualizacji	246
Aktualizacja mechanizmów uwierzytelniania	247
Aktualizacja poprzez dołączenie bazy danych	247
Aktualizacja w miejscu	247
Obsługiwane bazy danych	247
Nieobsługiwane bazy danych	248
Usprawnienia w implementacji aktualizacji	248
Przebieg procesu aktualizacji	253
Przygotowanie uaktualnienia	255
Uporządkowanie baz danych zawartości	255
Porządkowanie środowiska	256
Dokumentowanie środowiska	257
Dokumentowanie bieżących ustawień	257
Dokumentowanie ustawień środowiska	259
Dokumentowanie ustawień usług	259
Zarządzanie personalizacjami	259
Dokumentowanie innych usług	261
Uwierzytelnianie w trybie klasycznym	265
Pakiety językowe	265
Ograniczenie przestojów	266
Testowanie uaktualnienia	268
Uaktualnienie farmy testowej	268
Sprawdzanie poprawności testowego uaktualnienia	269
Wnioski z instalacji	269
Implementacja uaktualnienia	270
Minimalizowanie przestojów	270
Uaktualnienie farmy produkcyjnej	270
Monitorowanie postępów	271
Weryfikacja aktualizacji	272
Weryfikowanie aktualizacji	272
Rozwiązywanie problemów z uaktualnieniem	272

Podsumowanie	272
Scenariusz	272
Bieżąca farma	272
Środowisko testowe	275
Testowanie strategii migracji	276
Budowanie farmy testowej	276
Uaktualnienie aplikacji usługi wyszukiwania	276
Aktualizacja Centrum wyszukiwania	278
Federacja usługi wyszukiwania	279
Aktualizacja pozostałych aplikacji usług	279
Ufaj, ale sprawdzaj	283
Tworzenie aplikacji usług	283
Personalizacje	283
Aktualizacja baz danych zawartości	283
Uaktualnienie zawartości witryn Moja witryna	284
Uaktualnianie witryn	286
Powróćmy do wyszukiwania	288
Na koniec	288

CZĘŚĆ III ZAGADNIENIA NIEZAWODNOŚCI INFRASTRUKTURY

Rozdział 9 Utrzymywanie i monitorowanie programu Microsoft SharePoint	291
Monitorowanie środowiska programu SharePoint	292
Wymagania w zakresie monitorowania w programie SharePoint	293
Monitorowanie kondycji programu SharePoint	297
Konfigurowanie ustawień dostawcy danych użytkownika i kondycji	298
Monitorowanie liczników wydajności	301
Monitorowanie wydajności stron	304
Monitorowanie pamięci trwałej programu SharePoint	306
Dostrajanie i optymalizacja środowiska programu SharePoint	307
Ograniczanie zasobów	307
Optymalizacja SQL	307
Definiowanie i realizacja planu utrzymania bazy danych	311
Dostrajanie wydajności sieci	314
Planowanie i konfigurowanie buforowania	315
Wprowadzenie w tematykę zarządzania żądaniami	322
Rozwiązywanie problemów ze środowiskiem programu SharePoint	325
Rozpoznawanie problemów za pomocą dzienników	326
Podsumowanie	327

Rozdział 10	Planowanie strategii ciągłości działania	333
	Potrzeby w zakresie planowania ciągłości działania	334
	Co należy zabezpieczać?	334
	Stosowanie celów BCM	334
	Funkcje BCM wbudowane w program SharePoint	335
	Wbudowany mechanizm kopii zapasowych i odtwarzania	336
	Kopia zapasowa zbioru witryn	338
	Eksportowanie witryny lub listy	339
	Odtwarzanie danych z niedołączonej bazy danych zawartości	341
	Przywracanie danych z Kosza	342
	Usprawnienia w trybie tylko do odczytu	343
	Unikanie zakłóceń dostępności usług	344
	Implementacja różnych technik zapewniania ciągłości działania	346
	Klastry pracy awaryjnej	346
	Dublowanie bazy danych	349
	Wysyłanie dziennika	352
	Zawsze włączone grupy dostępności	354
	Implementacja sieciowego mechanizmu równoważenia obciążenia	358
	Podsumowanie	360
	Wymagania firmy Contoso	360
	Czynniki kluczowe	361
	Rozwiązanie	362
Rozdział 11	Walidacja architektury	365
	Weryfikacja działania farmy	366
	Microsoft ULS Viewer	366
	Pulpit nawigacyjny	368
	Weryfikacja alokacji portów i żądań WWW	370
	Fiddler	370
	Narzędzia deweloperskie programu Internet Explorer	371
	Weryfikacja działania protokołu Kerberos za pomocą narzędzia Klist	371
	Inspekcja pakietów sieciowych	371
	Microsoft Network Monitor	372
	Microsoft Message Analyzer	372
	Testowanie środowiska	373
	Inspekcja logów IIS	373
	Testowanie wydajności środowiska	377
	Testowanie obciążenia środowiska	383
	Testowanie warunków skrajnych środowiska	400
	Inne możliwości testowania obciążenia	403

Podsumowanie	404
Scenariusz	404
Weryfikacja witryn	406
Weryfikacja protokołu Kerberos	407
Konfiguracja systemu Visual Studio Ultimate 2010	408
Utworzenie testu obciążenia	409
Dokumentacja	413
Na koniec	414
Skorowidz	415

ROZDZIAŁ 7

Projektowanie bezpieczeństwa platformy

W tym rozdziale:

- Blokowanie, śledzenie instalacji programu Microsoft SharePoint i tworzenie raportów na jej temat.
- Komunikacja i szyfrowanie.
- Planowanie i konfigurowanie funkcji Microsoft SQL Server Transparent Data Encryption.
- Instalowanie programu SharePoint za pomocą najmniejszych uprawnień.
- Role i uprawnienia grup.

Instalacje programu Microsoft SharePoint są zarządzane na poziomie farmy. Wraz z rosnącą popularnością produktu administratorzy systemu mogą potrzebować funkcji śledzenia instalacji programu SharePoint lub blokowania możliwości dodawania ich do firmowego intranetu. W tym rozdziale zaprezentujemy sposoby wprowadzania tych funkcji tak, by ułatwić administratorom tworzenie nowych farm.

Po fazie zbierania wymagań bez wątpienia dysponujemy wymaganiami, które są bezpośrednio związane z bezpieczeństwem platformy. W tym rozdziale pokażemy nie tylko sposób zabezpieczenia webowego interfejsu programu SharePoint, ale także komunikacji — od wykonawcy do bazy danych. Ale czy to wystarczy? Zastanówmy się, czym właściwie jest zabezpieczenie platformy.

Oto rozsądna definicja zabezpieczeń platformy: to model, który jest wykorzystywany do ochrony wszystkich aspektów danego systemu. W przypadku programu SharePoint obejmuje to nie tylko funkcje dostępne przez interfejs WWW, ale także dane „w spoczynku”. Do ochrony tych danych można wykorzystać mechanizm Microsoft SQL Server Transparent Data Encryption (TDE). W tym rozdziale dowiesz się, w jaki sposób planować wykorzystanie tej funkcji i jak ją skonfigurować.

Kiedy zapoznasz się ze sposobami śledzenia instalacji i ochrony danych aż do miejsca ich przechowywania w bazie danych, zajmiemy się technikami ograniczania dostępu do różnych części systemu dla wskazanych kont. Zaprezentujemy także kompromisy, jakie należy przyjąć, aby korzystać w środowisku programu SharePoint z jak najmniejszych uprawnień. Następnie zagłębimy się w aplikację *Administracja centralna*. Podczas jej omawiania skoncentrujemy się na różnych kontach wykorzystywanych przez system, ogólnych opcjach zabezpieczeń oraz zasadach informacyjnych.

Bezpieczeństwo w programie SharePoint jest zawsze gorącym tematem. I słusznie. Organizacje umieszczają w systemie istotne dokumenty biznesowe i jest dla nich ważne, by mieć poczucie, że system jest bezpieczny. W kontekście rosnących obaw o bezpieczeństwo oraz regulacji prawnych chroniących prywatność danych bezpieczeństwo platformy jest bez wątpienia jednym z najważniejszych zagadnień dotyczących wdrożeń farm programu SharePoint 2013. W ostatnim podrozdziale tego rozdziału zapoznasz się ze scenariuszem, który pomoże wykorzystać wiele spośród zaprezentowanych koncepcji w taki sposób, aby można było zapewnić interesariuszy o tym, że ich informacje są bezpieczne.

Blokowanie, śledzenie instalacji programu Microsoft SharePoint i tworzenie raportów na jej temat

Zainstalowanie programu SharePoint 2013 na komputerze z klienckim systemem operacyjnym nie jest obsługiwane. Jest to zmiana w porównaniu z wersją 2010. Ponieważ platforma Microsoft SharePoint Foundation była swobodnie dostępna, nie było niczym niezwykłym, że powstawały i rozwijały się „dzikie” farmy programu SharePoint. SharePoint jest instalowany i zarządzany na poziomie farmy. Jedna instalacja programu SharePoint może nie mieć żadnych informacji na temat innych farm, które mogą istnieć w tym samym przedsiębiorstwie. Ponieważ nie ma sposobu, w skali całego przedsiębiorstwa, aby dowiedzieć się, gdzie są tworzone farmy programu SharePoint, mogą być konieczne działania zmierzające do zapobiegania tworzeniu nowych farm lub przynajmniej śledzenia miejsc ich powstawania. W tym podrozdziale nie tylko dowiesz się, jak wykonywać obie te operacje, ale także jak przeglądać miejsca instalacji programu SharePoint, jeśli opcje te zostały już zaimplementowane.

Blokowanie instalacji programu SharePoint

Aby zablokować użytkownikom możliwość instalacji programu SharePoint, można skorzystać z zasady grupy w usłudze Active Directory. By to zrobić, należy zaktualizować następujący klucz na wszystkich serwerach:

```
HKLM\Software\Policies\Microsoft\Shared Tools\Web Server Extensions\15.0\SharePoint\DWORD DisableInstall
```

Aby zablokować instalację, należy ustawić wartość DWORD `DisableInstall=00000001`.

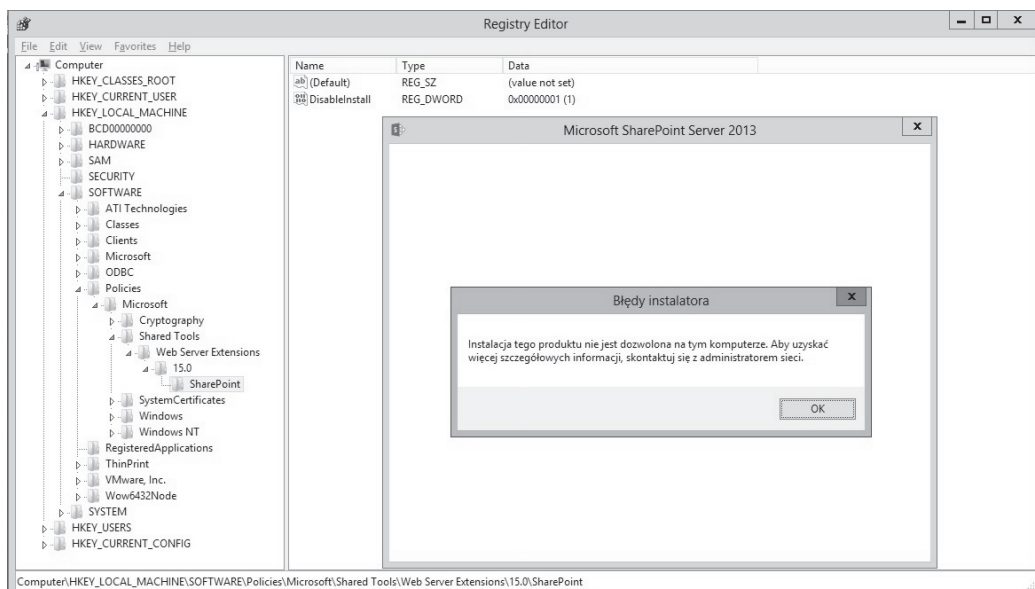
By dodać wartość rejestru do zasady grupy na serwerze z usługą Active Directory, można skorzystać ze skryptu Windows PowerShell (listing 7.1).

LISTING 7.1. Zasady grupy

```
Set-GPRegistryValue -Name "Default Domain Policy" -Key "HKLM\Software\Policies\Microsoft\Shared Tools\Web Server Extensions\15.0\SharePoint" -ValueName "DisableInstall" -Type DWORD -Value 1
```

Po ustawieniu tych wartości w rejestrze przy próbie instalacji wyświetli się komunikat *Błędy instalatora* podobny do pokazanego na rysunku 7.1.

Jeśli wcześniej zdefiniowałeś zasadę grupy w celu zablokowania programu SharePoint 2010 (14.0), musisz stworzyć nową dla wersji 15.0. W procesie instalacji status poprzedniej wersji nie jest sprawdzany. Ponieważ jest to ustawienie *obiektu zasad grupy* (ang. *Group Policy Object* — GPO), możliwe jest obejście procesu poprzez modyfikację rejestru oraz zmianę wartości na zero lub całkowite jej usunięcie. Próba kontrolowania instalacji wyłącznie przez ich blokowanie nie zawsze jest zatem kompletnym rozwiązaniem. Może jednak zatrzymać te osoby, które nie rozumieją, jak działa funkcja.



RYSUNEK 7.1. Instalacja programu SharePoint jest niedozwolona

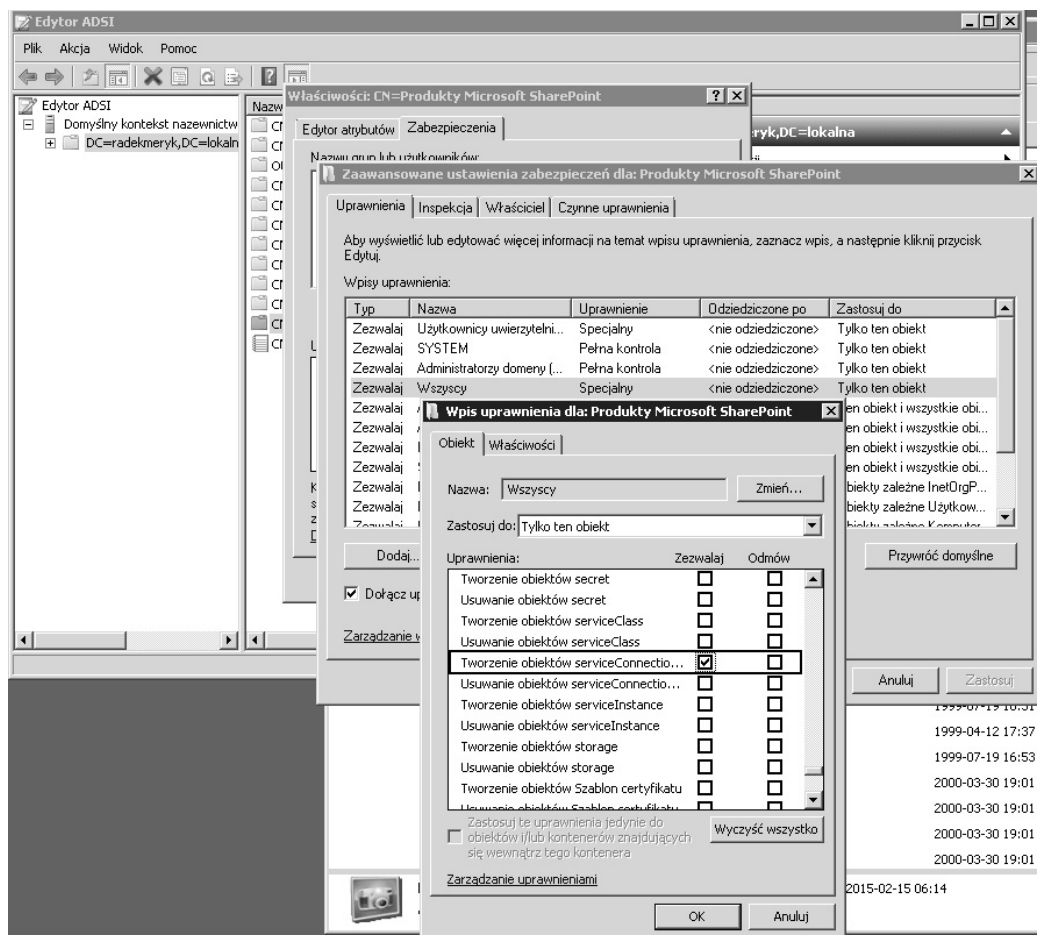
Śledzenie instalacji programu SharePoint

Program SharePoint może działać w połączeniu z punktami połączeń usługi Active Directory (ang. *Active Directory Service Connection Points*), co umożliwia identyfikowanie produktów SharePoint wykorzystywanych w organizacji. Podobnie jak w przypadku blokowania instalacji, śledzenie instalacji także nie zapewnia kompletnego rozwiązania. Po skonfigurowaniu instalacji programu SharePoint, które zostały przeprowadzone za pomocą programu *SharePoint Products Configuration Wizard*, będą miały „wstrzyknięty” znacznik do punktu połączenia usługi, a instalacje wykonane za pomocą Windows PowerShell domyślnie nie będą miały tego znacznika. Tak więc bazowanie na tej funkcji w celu śledzenia wszystkich farm programu SharePoint nie daje wiarygodnych rezultatów. Znaczniki mogą być dodawane za pomocą skryptu Windows PowerShell już po zainstalowaniu albo mogą być dołączane do skryptów instalacyjnych.

Aby stworzyć kontener punktu połączenia usługi do śledzenia instalacji, wykonaj następujące czynności:

1. Na kontrolerze domeny uruchom program Edytor ADSI.
2. W menu *Akcja* kliknij *Połącz z*, aby połączyć się z domeną, w której śledzisz instalację.
3. Rozwiń nazwę domeny, a następnie kliknij *CN=System*.
4. Kliknij prawym przyciskiem myszy w pustym obszarze, następnie kliknij *Nowy*, a potem *Obiekt*.
5. W oknie dialogowym, które się wyświetli, kliknij *Kontener*, a następnie *Dalej*.
6. W oknie wartości wpisz **Produkty Microsoft SharePoint** jako nazwę kontenera, po czym kliknij *Dalej*.
7. Kliknij *Zakończ*.
8. Kliknij prawym przyciskiem myszy kontener *Produkty Microsoft SharePoint*, który przed chwilą utworzyłeś, a następnie *Właściwości*.

9. Na zakładce *Zabezpieczenia* kliknij *Dodaj*.
10. Dodaj do kontenera pozycję *Użytkownicy uwierzytelnieni* lub *Wszyscy* i ustaw dla nich prawa zapisu. Jeśli określona osoba nie ma prawa do zapisu, nadal będzie mogła instalować program SharePoint, ale znacznik nie zostanie utworzony.
11. W grupie, którą przed chwilą wprowadziłeś, kliknij *Zaawansowane*.
12. W oknie *Uprawnienia* wybierz nazwę lub grupę, którą przed chwilą dodałeś, a następnie kliknij *Edytuj*.
13. W oknie dialogowym *Wpis uprawnienia dla: Produkty Microsoft SharePoint* zaznacz pole wyboru *Zezwalaj* przy opcji *Tworzenie obiektów serviceConnectionPoint* (rysunek 7.2), a następnie kliknij *OK*.



RYСУNEK 7.2. *Włączono opcję tworzenia obiektów ServiceConnectionPoint*

Po stworzeniu punktu połączenia usługi i ustawieniu uprawnień wszystkie instalacje wykonane za pomocą programu *SharePoint Product Configuration Wizard* będą automatycznie śledzone. Aby śledzić instalacje wykonane za pomocą skryptów Windows PowerShell, można skorzystać z komendletu `Set-SPFarmConfig` tak, jak pokazano na listingu 7.2.

LISTING 7.2. Wykorzystanie komandletu *Set-SPFarmConfig*

```
Set-SPFarmConfig -ServiceConnectionPointBindingInformation
StringwithBindingInformation
```

Wartość ciągu określonego za pomocą opcji `-ServiceConnectionPointBindingInformation` można zmienić na bardziej opisową, na przykład `Get-SPTopologyServiceApplication | select URI`. Uruchomienie tego komandletu powoduje zwrócenie identyfikatora URI (ang. *Uniform Resource Identifier*) usługi topologii farmy (w tym przypadku `https://contoso-sp1:32844/Topology/topology.svc`). Można również wykorzystać parametr hosta adresu URI. Z tego samego komandletu i tych samych parametrów można skorzystać w celu zaktualizowania ciągu połączenia w dowolnym czasie.

Jeśli masz dostęp do skryptów instalacyjnych Windows PowerShell wewnątrz organizacji, możesz dodać komandlet `Set-SPFarmConfig` na końcu skryptu instalacji farmy. Wprowadzenie wywołania tego komandletu spowoduje śledzenie instalacji korzystających z tych skryptów.

Informacje na temat śledzenia mogą być usunięte dzięki wykorzystaniu parametru `-ServiceConnectionPointDelete` komandletu `Set-SPFarmConfig`.

Tworzenie raportów na temat instalacji programu SharePoint

Po prawidłowym skonfigurowaniu punktów połączeń usługi możemy przeglądać znaczniki utworzone w usłudze Active Directory Domain Services (AD DS) wewnątrz kontenera *Produkty Microsoft SharePoint* albo możemy w tym celu wykorzystać skrypt Windows PowerShell pokazany na listingu 7.3. Użycie tego skryptu spowoduje wyświetlenie wszystkich farm programu SharePoint z ustawionymi znacznikami Active Directory.

LISTING 7.3. Raporty na temat instalacji

```
$containerPath = 'LDAP://CN=Microsoft SharePoint Products,CN=System,DC=contoso,D
C=local'
$entry = New-Object DirectoryServices.DirectoryEntry $containerPath
$searcher = New-Object DirectoryServices.DirectorySearcher
$searcher.SearchRoot = $entry
$searcher.Filter = "(objectClass=serviceConnectionPoint)"
$searcher.FindAll() | % { New-Object PSObject -Property $_.Properties } | select
servicebindinginformation, whencreated, whenchanged
```

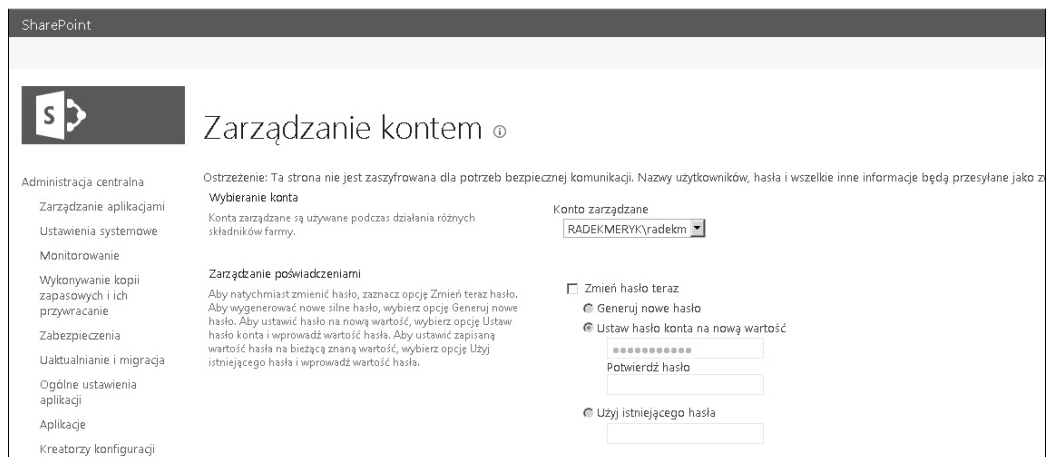
Szyfrowanie komunikacji

Zgodnie z tym, czego dowiedziałeś się w rozdziale 6., „Wymagania w zakresie uwierzytelniania i autoryzacji”, istnieje wiele sytuacji, w których jest wymagane szyfrowanie. Czasami jest ono potrzebne pomiędzy klientem a serwerem, a innym razem pomiędzy różnymi serwerami wchodzącymi w skład farmy programu SharePoint. W programie SharePoint istnieje wiele miejsc, gdzie poświadczenia są przysyłane w formie zwykłego tekstu. W celu ich zaszyfrowania należy skorzystać z zabezpieczeń warstwy transportowej (ang. *Transport Layer Security* — TLS). Najpopularniejszym sposobem implementacji tych zabezpieczeń jest skorzystanie z szyfrowania SSL (ang. *Secure Sockets Layer*). Jeśli dla witryny *Administracja centralna* nie korzystamy z szyfrowanego połączenia, to podczas tworzenia lub modyfikowania informacji dotyczących zarządzanego konta zobaczymy następujący komunikat:

Ostrzeżenie: Ta strona nie jest szyfrowana na potrzeby bezpiecznej komunikacji.

Nazwa użytkownika, hasło oraz inne informacje zostaną wysłane w formie zwykłego tekstu.

Przykład takiego ostrzeżenia pokazano na rysunku 7.3. Witryna *Administracja centralna* jest często pomijana podczas konfigurowania zabezpieczeń, a bez wątpienia jest ona najważniejszą aplikacją sieci Web, o której bezpieczeństwo należałoby zadbać. W wielu organizacjach wykorzystuje się zdalne połączenia do serwera obsługującego aplikację sieci Web w celu wprowadzenia zmian. Należy jednak pamiętać, że do aplikacji *Administracja centralna* można uzyskać dostęp z każdego komputera w domenie — tak samo jak do każdej innej aplikacji sieci Web.



RYСУNEK 7.3. Poniżej tytułu *Zarządzanie kontem* wyświetla się ostrzeżenie dotyczące informacji przesyłanych w formacie zwykłego tekstu

Więcej informacji na temat szyfrowania witryn programu SharePoint przy użyciu protokołu SSL można znaleźć w dalszej części tego rozdziału.

Urzędy certyfikacji (CA)

Zabezpieczenie komunikacji z serwerem wymaga uzyskania certyfikatu z urzędu certyfikacji (ang. *Certification Authority* — CA). W przypadku systemów produkcyjnych, które mają zasięg publiczny (dostęp przez internet), najlepiej skorzystać z publicznego urzędu certyfikacji. To jednak wiąże się z kosztami, dlatego w przypadku wewnętrznych aplikacji sieci Web (działających w sieci intranet) można wykorzystać *UC Domeny* — rolę *Usług certyfikatów w usłudze Active Directory*. To pozwala na stworzenie w razie potrzeby certyfikatów wewnętrznych.

Istnieje kilka rodzajów certyfikatów, o których warto wspomnieć w tym miejscu: standardowe certyfikaty SSL oraz certyfikaty SSL w formie symboli wieloznacznych. Standardowe certyfikaty SSL są ważne dla określonej nazwy domeny lub poddomeny i są bardzo specyficzne. Certyfikaty SSL w formie symboli wieloznacznych mogą być stosowane do wszystkich poddomen i podkatalogów w określonej domenie. Dzięki temu można uzyskać większą elastyczność i często jest to tańsze rozwiązanie w porównaniu z zakupem wielu publicznych standardowych certyfikatów SSL. Aby wygenerować certyfikat SSL w formie symbolu wieloznacznego, należy wykorzystać we wspólnej nazwie przyrostek **.domena.com*. Warto zauważyć, że w wielu organizacjach uważa się, że stosowanie certyfikatów w formie symboli wieloznacznych wprowadza zagrożenie dla bezpieczeństwa, dlatego należy sprawdzić, czy są one dozwolone w danej organizacji. W tym rozdziale wykorzystamy certyfikaty z *UC Domeny* we wszystkich przykładach dotyczących SSL. W podrozdziale „Podsumowanie” na końcu niniejszego rozdziału zademonstrowano procedurę krok po kroku zabezpieczania aplikacji *Administracja centralna*. Trzecią opcją, nieopisaną w tej książce, jest wykorzystanie certyfikatów UCC, które mogą obowiązywać w wielu domenach.

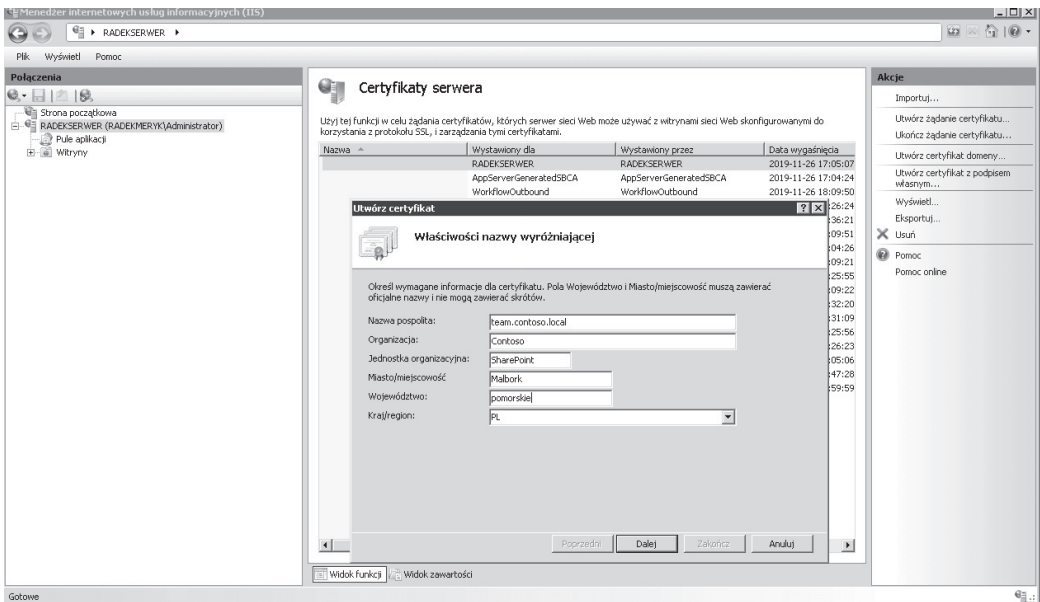


Uwaga. Alternatywnie można skorzystać z certyfikatów z podpisem własnym, ale te nie są zaufane w całej domenie i wymagają importowania certyfikatów. W większości przypadków zastosowanie certyfikatu *UC Domeny* jest lepszą opcją.

Komunikacja pomiędzy klientem a serwerem

Transmisje, które są przekazywane bez szyfrowania, mogą być przechwycone za pomocą takich narzędzi jak WireShark. W celu ochrony środowiska należy rozważyć możliwość użycia protokołu SSL dla wszystkich aplikacji internetowych w farmie. Aby to zrobić, najpierw trzeba uzyskać certyfikat. Może on pochodzić z publicznego urzędu certyfikacji albo z *UC Domeny*. Na potrzeby niniejszego przykładu skorzystamy z aplikacji *team.contoso.local* oraz certyfikatu wygenerowanego przez urząd certyfikacji domeny.

Uruchom *Menedżer internetowych usług informacyjnych*, kliknij węzeł serwera w okienku po lewej stronie, a następnie w środkowym okienku dwukrotnie kliknij *Certyfikaty serwera*. W środkowym okienku wyświetlą się wszystkie certyfikaty, w okienku po prawej stronie natomiast pojawią się nowe akcje. W tym miejscu należy wybrać akcję *Utwórz certyfikat domeny...* i wypełnić formularz certyfikatu w sposób pokazany na rysunku 7.4.



RYСУNEK 7.4. Żądanie certyfikatu z *UC Domeny*

Jeśli proces pozyskiwania certyfikatu zakończy się pomyślnie, będziemy dysponować certyfikatem, którego będzie można użyć w aplikacjach sieci Web programu SharePoint. Niezależnie od tego, czy tworzymy nową aplikację sieci Web programu SharePoint, czy dokonujemy konwersji istniejącej, ogólne czynności są takie same. Jeśli występuje potrzeba przekształcenia istniejącej witryny do korzystania z SSL, łatwiejszą opcją może okazać się ponowne utworzenie aplikacji sieci Web programu SharePoint. To wymaga nie tylko utrzymania bazy danych zawartości, ale również pliku *Web.config* w przypadku jakichkolwiek zmian konfiguracyjnych w istniejącej aplikacji sieci Web. Przy usuwaniu aplikacji sieci Web należy zwrócić uwagę na to, by usunąć aplikację tylko z serwera IIS.

Przy tworzeniu nowej aplikacji sieci Web programu SharePoint, kluczowe wartości to *Port*, *Nagłówek hosta* oraz *Użyj protokołu Secure Sockets Layer (SSL)* (rysunek 7.5). Jeśli witryna *Administracja centralna* nie jest zaszyfrowana, w górnej części formularza wyświetli się ostrzeżenie o tym, że poświadczenia będą przesyłane w formie zwykłego tekstu.

Tworzenie nowej aplikacji sieci Web

OK Anuluj

Witryna sieci Web usług IIS

Wybierz opcję użycia istniejącej witryny sieci Web usług IIS lub utworzenia nowej witryny, w której będzie dostępna aplikacja programu Microsoft SharePoint Foundation.

Jeśli wybierzesz istniejącą witrynę sieci Web usług IIS, ta witryna będzie musiała istnieć na wszystkich serwerach w farmie i mieć na każdym serwerze taką samą nazwę. W przeciwnym przypadku wykonanie tej akcji zakończy się niepowodzeniem.

Jeśli wybierzesz opcję utworzenia nowej witryny sieci Web usług IIS, ta witryna zostanie utworzona automatycznie na wszystkich serwerach w farmie. Jeśli ustawienie usług IIS, które chcesz zmienić, nie jest widoczne na tej stronie, możesz użyć tej opcji w celu utworzenia podstawowej witryny, a następnie zaktualizować ją za pomocą standardowych narzędzi usług IIS.

☐ Użyj istniejącej witryny sieci Web usług IIS
Default Web Site

☒ Utwórz nową witrynę sieci Web usług IIS

Nazwa
SharePoint - team.contoso.local443

Port
4543

Nagłówek hosta
team.contoso.local

Ścieżka
C:\inetpub\wwwroot\wss\VirtualDirectories\te.

Konfiguracja zabezpieczeń

Jeśli wybierzesz opcję używania protokołu Secure Sockets Layer (SSL), konieczne będzie dodanie certyfikatu na każdym serwerze za pomocą narzędzi administracyjnych usługi IIS. Dopóki ta

Zezwalaj na dostęp anonimowy

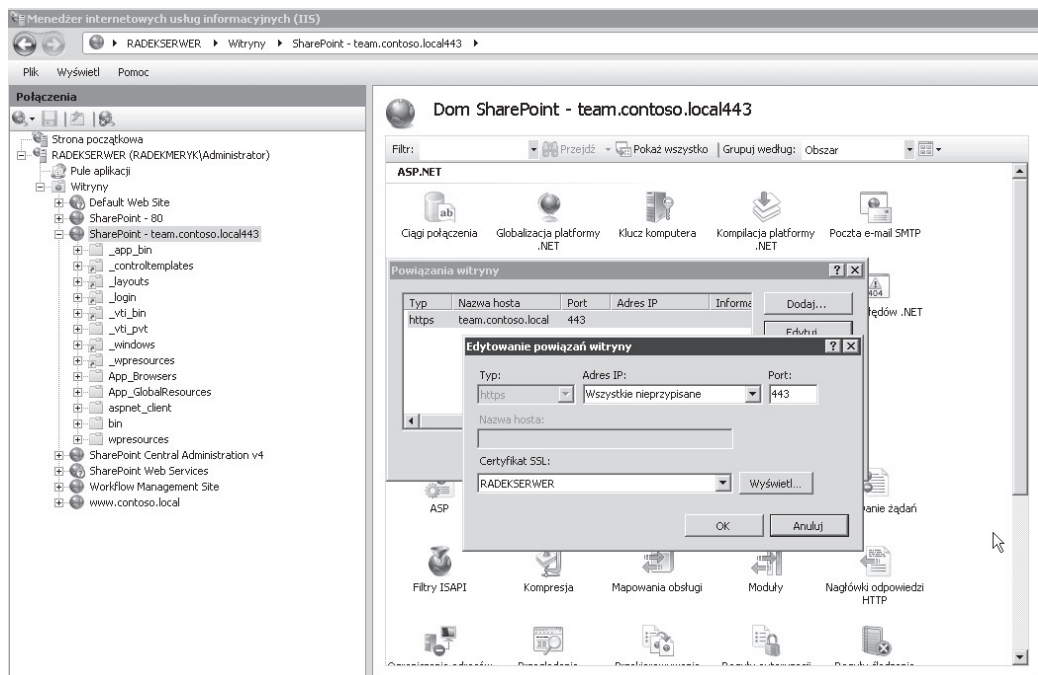
☐ Tak
☒ Nie

Użyj protokołu Secure Sockets Layer (SSL)

☐ Tak
☒ Nie

RYСУNEK 7.5. Formularz *Tworzenie nowej aplikacji sieci Web*

Po stworzeniu nowej aplikacji sieci Web można zauważyć, że jest ona niedostępna. Wynika to stąd, że witryna wymaga certyfikatu przyporządkowanego do powiązania z HTTPS. Okno z żądaniem certyfikatu pokazano na rysunku 7.6.



RYSUNEK 7.6. Okno dialogowe Edytowanie powiązań witryny

Aby można było stworzyć kilka witryn wykorzystujących port 443 z wieloma certyfikatami, należy zaznaczyć pole wyboru *Require Server Name Indication*. Pozwala to na serwowanie wielu bezpiecznych witryn WWW przy użyciu tego samego adresu IP. Ponieważ bez wątpienia będziemy zabezpieczać wszystkie witryny programu SharePoint w połączeniu z witryną *Administracja centralna*, powinniśmy zadbać o to, aby za każdym razem zaznaczyć to pole wyboru.

Po przyporządkowaniu certyfikatu do powiązania IIS witryna powinna działać zgodnie z oczekiwaniami za pośrednictwem protokołu HTTPS. Aby powiązać certyfikat za pomocą Windows PowerShell, można skorzystać ze skryptu zamieszczonego na listingu 7.4.

LISTING 7.4. Skrypt Windows PowerShell do tworzenia powiązań IIS

```
$siteName = "SharePoint - team.contoso.local443"
$certName = "Witryny zespołu"
# Pobranie witryny z wykorzystaniem nazwy i usunięcie istniejącego wiązania
Get-WebBinding -Name $siteName | Remove-WebBinding
# Pobranie certyfikatu z wykorzystaniem nazwy
$cert = get-childitem cert:\LocalMachine\my | where-Object {$_.FriendlyName -like
$certName}
# Aktualizacja powiązania
$cert | New-Item -Path "IIS:\SslBindings\!443!team.contoso.local"
```



Ważne. Informacje na temat powiązań w komputerach czytelników będą się różnić od tych, które podano w przykładach zamieszczonych w tej książce. Aby przeglądać wszystkie certyfikaty i pobierać wartości ich opisowych nazw, należy skorzystać z następującego kodu:

```
#get-childitem cert:\LocalMachine\my | ft issuer, subject, notafter, FriendlyName
```

Komunikacja serwer-serwer

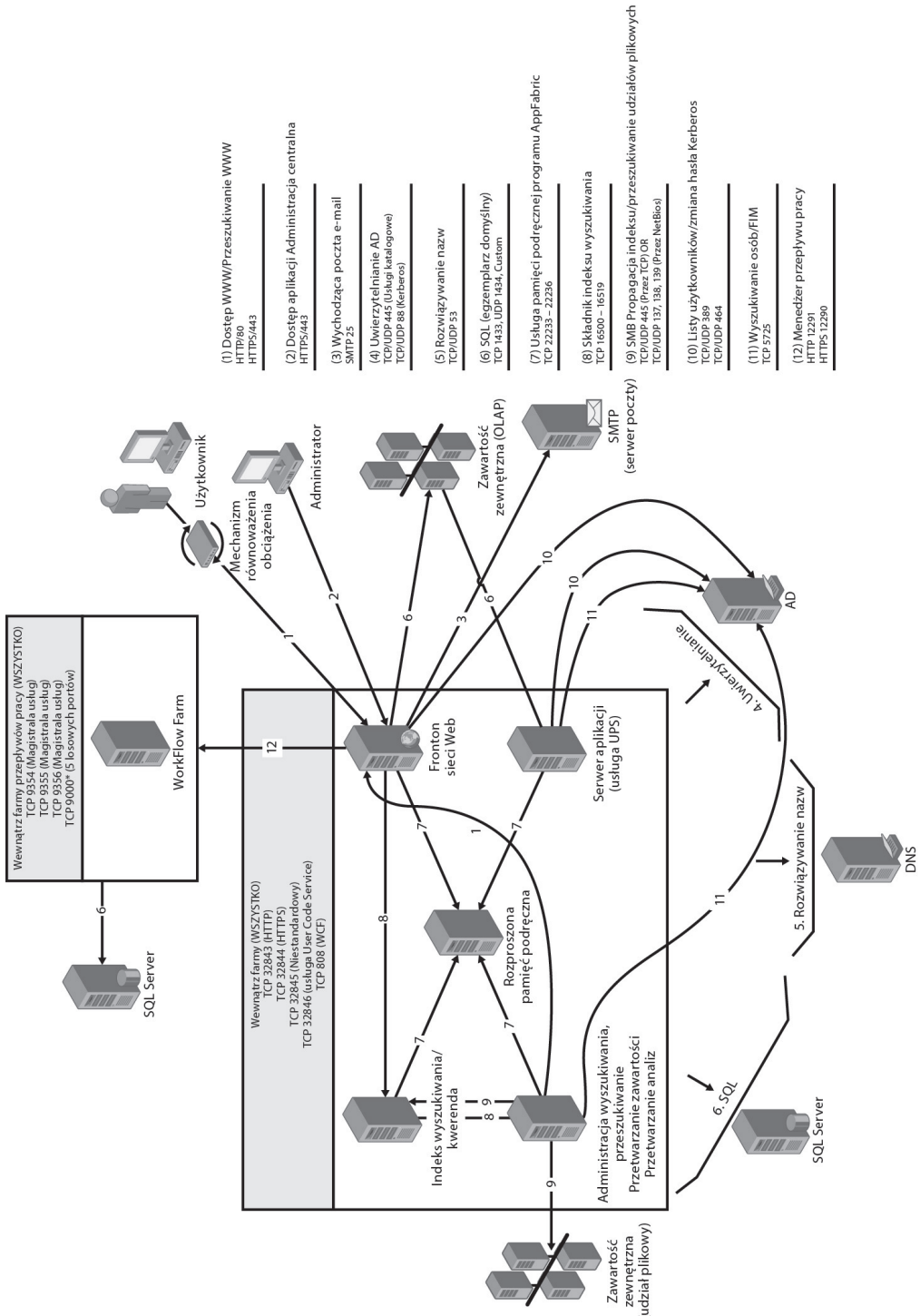
Po omówieniu szyfrowania danych pomiędzy klientami a serwerem SharePoint przetwarzającym żądania witryn sieci Web nadszedł czas, by skupić się na komunikacji między serwerami z systemem SharePoint oraz serwerami z systemem SQL Server. Do zabezpieczenia komunikacji pomiędzy serwerami poprzez zaszyfrowanie ruchu można skorzystać z protokołu SSL i zabezpieczeń protokołu IP (IPsec). Wybór stosowanej metody zależy od wykorzystywanych kanałów komunikacyjnych, które są zabezpieczane, oraz korzyści i kompromisów, które są odpowiednie dla konkretnej organizacji.

Komunikacja pomiędzy serwerami w programie SharePoint

W wielu organizacjach jest stosowana zasada, zgodnie z którą wszystkie nieużywane porty są zamykane. Jeśli zespół zajmujący się wdrażaniem zabezpieczeń nie jest świadomy komunikacji pomiędzy serwerami SharePoint, to prawidłowe działanie systemu SharePoint może być utrudnione. Poniżej zamieszczono listę portów o kluczowym znaczeniu dla komunikacji w programie SharePoint:

- Standardowy ruch WWW zazwyczaj odbywa się za pośrednictwem domyślnych portów TCP 80, TCP 443 (SSL).
- Porty wykorzystywane przez składnik indeksowania wyszukiwania: TCP 16500 – 16519 (wyłącznie wewnątrz farmy).
- Porty wykorzystywane przez usługę pamięci podręcznej programu AppFabric: TCP 22233 – 22236.
- Porty wykorzystywane w komunikacji WCF (ang. *Windows Communication Foundation*): TCP 808.
- Porty wykorzystywane do komunikacji pomiędzy serwerami WWW a aplikacjami usług (domyślny to HTTP):
 - Powiązanie HTTP: TCP 32843.
 - Powiązanie HTTPS: TCP 32844.
 - Powiązanie Net.tcp: TCP 32845 (niestandardowe aplikacje usług).
- Porty wymagane do synchronizacji profili pomiędzy programem SharePoint 2013 a usługą AD DS na serwerze, na którym działa agent FIM (ang. *Forefront Identity Management*):
 - TCP 5725.
 - TCP i UDP 389 (usługa LDAP).
 - TCP i UDP 88 (Kerberos).
 - TCP i UDP 53 (DNS).
 - UDP 464 (zmiana hasła Kerberos).
- Domyślne porty komunikacji programu SQL Server: TCP 1433, UDP 1434. Jeśli na komputerze z systemem SQL Server te porty są zablokowane (co jest zalecane), a bazy danych są zainstalowane na egzemplarzu identyfikowanym przez nazwę, należy skonfigurować alias klienta SQL Server do połączeń z egzemplarzem identyfikowanym przez nazwę.
- Usługa *SharePoint Foundation User Code Service* (dla rozwiązań w formie piaskownicy): TCP 32846. Ten port musi być otwarty dla połączeń wychodzących na wszystkich serwerach WWW. Kiedy ta usługa jest włączona, to ten port musi być otwarty dla połączeń przychodzących na serwerach WWW, na których usługa jest włączona.
- Protokół SMTP (ang. *Simple Mail Transfer Protocol*) do integracji z pocztą elektroniczną: TCP 25.
- Workflow Manager:
 - Powiązanie HTTP: TCP 12291.
 - Powiązanie HTTPS: TCP 12290.

Niedawno Marek Samaj opublikował na swoim blogu artykuł, w którym zamieścił ilustrację komunikacji w farmie programu SharePoint 2013 (rysunek 7.7).



RYSUNEK 7.7. Porty i protokoły w programie SharePoint 2013

SSL i SQL Server

Włączenie szyfrowania SSL zwiększa bezpieczeństwo danych przesyłanych w sieci pomiędzy egzemplarzami systemu SQL Server a innymi aplikacjami. Wydaje się, że o takie zabezpieczenie powinniśmy zadbać w każdej sytuacji. Być może, ale należy pamiętać, że włączenie szyfrowania spowalnia działanie.

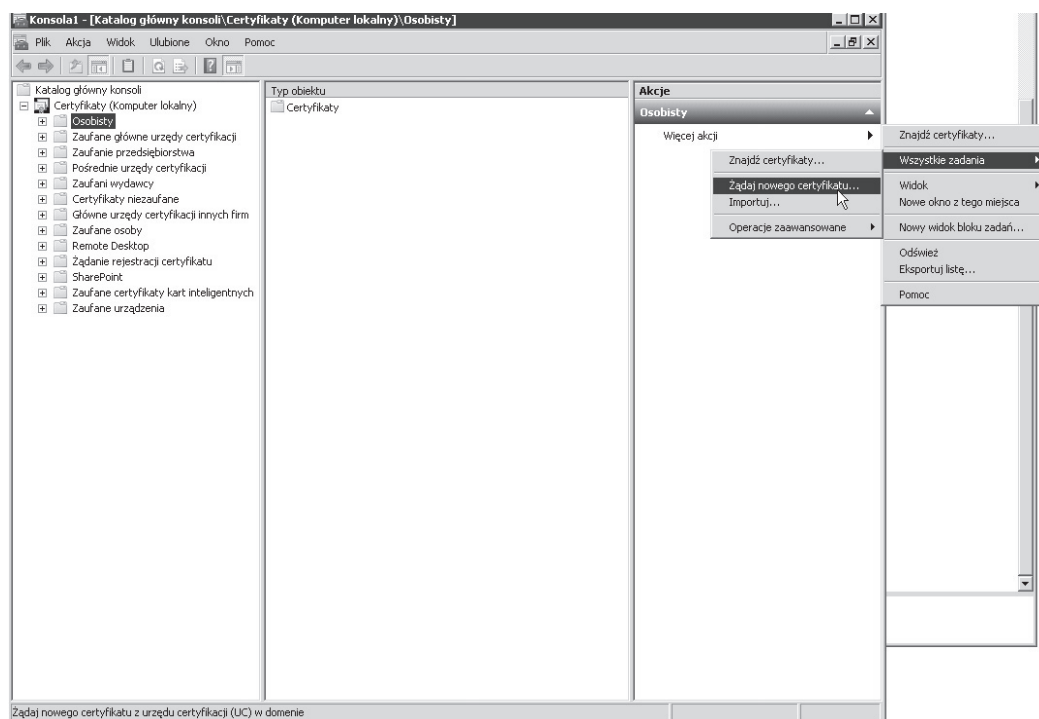
Kiedy cały ruch jest zaszyfrowany za pomocą SSL, zachodzi konieczność wykorzystania następujących dodatkowych procesów:

- W czasie połączenia wymagana jest dodatkowa komunikacja sieciowa w obie strony.
- Pakiety wysyłane z aplikacji muszą być szyfrowane przez klienta i odszyfrowywane przez egzemplarz systemu SQL Server.
- Pakiety wysyłane z egzemplarza SQL Server muszą być szyfrowane przez serwer i odszyfrowywane przez aplikację.

Pomimo to wdrożenie protokołu SSL nie powinno wiązać się ze znaczącym obniżeniem wydajności. Warto jednak przeprowadzić testy obciążenia, aby mieć pewność, że uzyskane metryki są zgodne z oczekiwaniami. Więcej informacji na ten temat można znaleźć w rozdziale 11., „Walidacja architektury”.

Aby skonfigurować egzemplarz programu SQL Server do korzystania z protokołu SSL, uruchom program *SQL Server Configuration Manager*. By to zrobić, otwórz konsolę MMC (ang. *Microsoft Management Console*), wpisując *MMC* w oknie dialogowym *Uruchom*. W menu *Plik* kliknij *Dodaj/usuń przystawkę*. Kliknij *Certyfikaty/Dodaj*. Następnie wybierz *Konto komputera/Komputer lokalny*. Kliknij *Zakończ*.

Po otwarciu przystawki *Certyfikaty* wybierz w lewym okienku folder *Osobisty* i rozwiń strzałkę w prawym oknie, aby wyświetlić *Wszystkie zadania*, tak jak pokazano na rysunku 7.8. Następnie wybierz opcję *Żądaj nowego certyfikatu...*



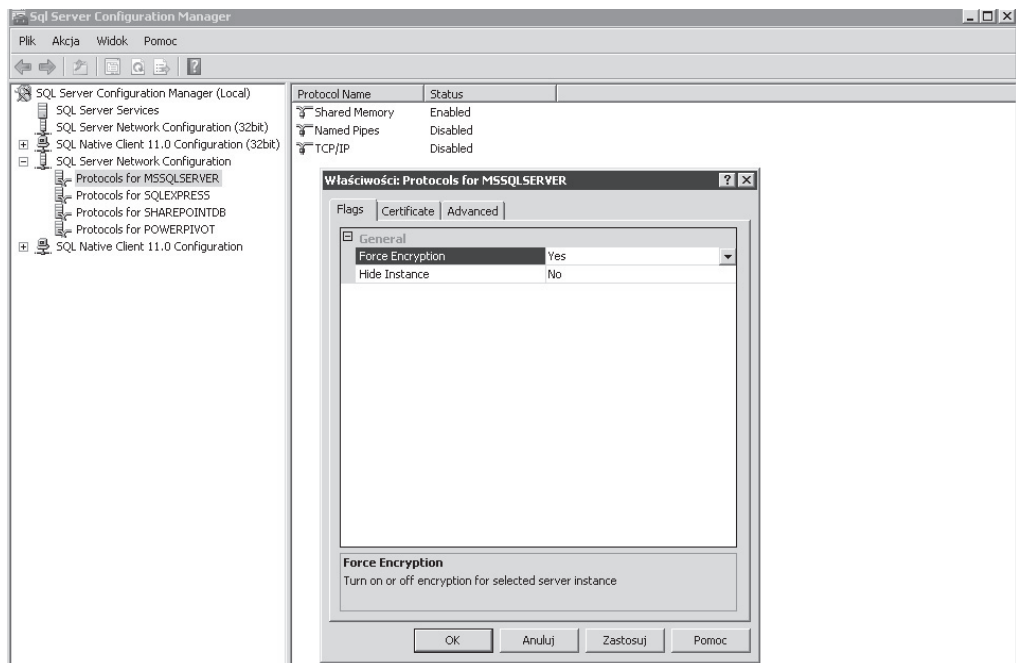
RYСУNEK 7.8. Żądanie nowego certyfikatu za pomocą MMC

W następnym oknie, które wyświetla się w procesie rejestrowania certyfikatów, należy wybrać zasady rejestracji certyfikatów. W tym oknie powinna wyświetlić się wartość domyślna *Zasady rejestracji usługi Active Directory*, można w nim zatem kliknąć *Dalej*. Następnie wyświetli się okno dialogowe, które pozwala żądać różnych certyfikatów. Wybierz *Komputer/Zarejestruj*. Powinien wyświetlić się komunikat z informacją o pomyślnej rejestracji. Po wykonaniu tej procedury można przeglądać *Certyfikaty osobiste*. Na tej liście powinien pojawić się nowo wydany certyfikat (rysunek 7.9).

Katalog główny konsoli	Wystawiony dla	Wystawiony przez	Data wygaśnięcia	Zamierzone cele	Przyjazna
Osobisty	AppServerGeneratedSBCA	AppServerGeneratedSBCA	2019-11-26	<Wszyscy>	<brak>
Certyfikaty	AppServerGeneratedSBCA	AppServerGeneratedSBCA	2019-11-26	<Wszyscy>	<brak>
Zaufane główne urzędy certyfikacji	AppServerGeneratedSBCA	AppServerGeneratedSBCA	2019-11-26	<Wszyscy>	<brak>
Certyfikaty	ForefrontIdentityManager	ForefrontIdentityManager	2040-01-01	<Wszyscy>	<brak>
Zaufanie przedsiębiorstwa	radekmyrk-RADEKSERVER-CA	radekmyrk-RADEKSERVER-CA	2025-03-17	<Wszyscy>	<brak>
Pośrednie urzędy certyfikacji	AppServerGeneratedSBCA	AppServerGeneratedSBCA	2019-11-26	Uwierzytelnienie serwera	<brak>
Lista odwołań certyfikacji	RADEKSERVER	AppServerGeneratedSBCA	2019-11-26	Uwierzytelnienie serwera	<brak>
Certyfikaty	RADEKSERVER	AppServerGeneratedSBCA	2019-11-26	Uwierzytelnienie serwera	<brak>
Zaufani wydawcy	RADEKSERVER	RADEKSERVER	2019-11-26	Uwierzytelnienie serwera	<brak>
Certyfikaty niezaufane	RADEKSERVER	RADEKSERVER	2019-11-26	Uwierzytelnienie serwera	<brak>
Główne urzędy certyfikacji innych	RADEKSERVER	RADEKSERVER	2019-11-26	Uwierzytelnienie serwera	<brak>
Zaufane osoby	RADEKSERVER.radekmyrk.lokalna	radekmyrk-RADEKSERVER-CA	2016-03-16	Uwierzytelnienie klienta...	<brak>
Remote Desktop	RADEKSERVER.radekmyrk.lokalna	radekmyrk-RADEKSERVER-CA	2016-03-16	Uwierzytelnienie klienta...	<brak>
Zadanie rejestracji certyfikatu	WMSvc-WIN-A18HAQDVM3	WMSvc-WIN-A18HAQDVM3	2024-11-08	Uwierzytelnienie serwera	<brak>
SharePoint	WorkflowOutbound	WorkflowOutbound	2019-11-26	<Wszyscy>	<brak>
Zaufane certyfikaty kart inteligentnych	WorkflowOutbound	WorkflowOutbound	2019-11-26	<Wszyscy>	<brak>
Zaufane urządzenia	WorkflowOutbound	WorkflowOutbound	2019-11-26	<Wszyscy>	<brak>

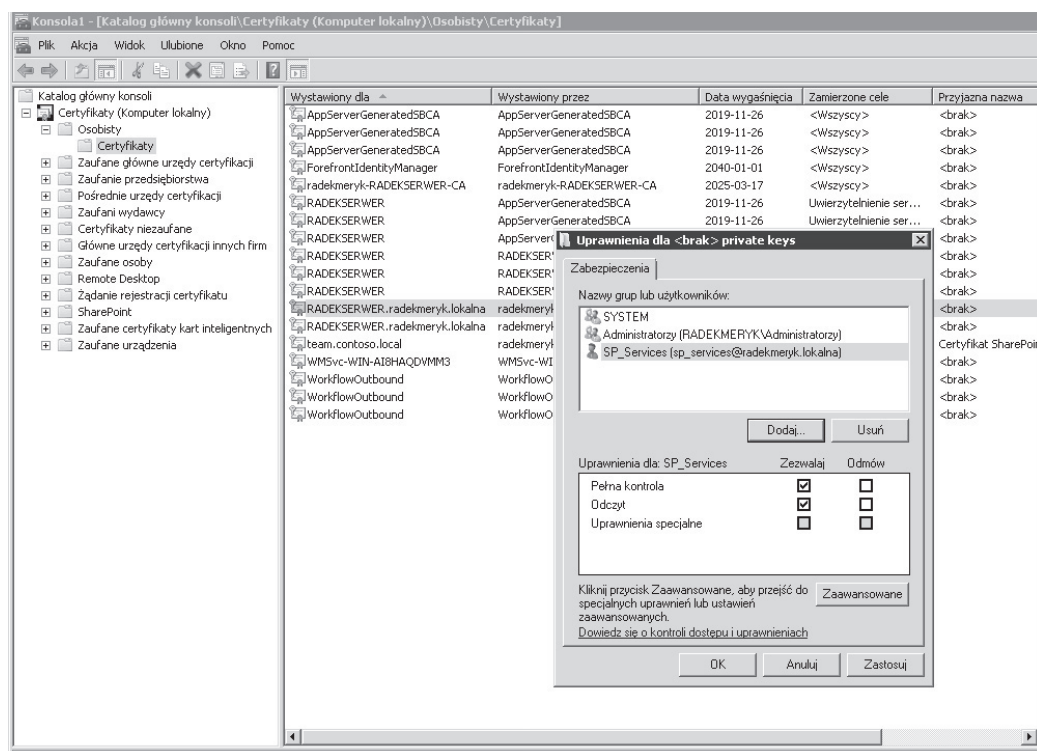
RYСУNEK 7.9. Przeglądanie certyfikatów osobistych

Ponownie uruchom program SQL Server Configuration Manager. W lewym panelu wyświetli się lista usług. Rozwiń węzeł *SQL Server Network Configuration*, a następnie kliknij prawym przyciskiem myszy polecenie *Protocols For MSSQLSERVER* (także w lewym panelu) i *Properties*. Wyświetli się okno właściwości podobne do pokazanego na rysunku 7.10.



RYСУNEK 7.10. Właściwości protokołów MSSQLSERVER

W następnych dwóch krokach zmień wartość właściwości *Force Encryption* na *Yes*, po czym wybierz w zakładce *Certificates* nowo utworzony certyfikat. Dzięki ustawieniu flagi *Force Encryption* na *Yes* cała komunikacja serwer-klient będzie od teraz zaszyfrowana, a dostęp dla klientów, którzy nie mogą obsługiwać szyfrowania, będzie zablokowany. Szyfrowanie jest nadal możliwe, jeśli flaga jest ustawiona na wartość *No*, ale w takim przypadku nie jest obowiązkowe. Za chwilę zajmiemy się konfiguracją po stronie aplikacji. Jednak wcześniej trzeba przypisać odpowiednie uprawnienia do nowo utworzonego certyfikatu. Aby to zrobić, kliknij w prawym panelu powiązane z serwerem menu *Więcej akcji*. Na potrzeby tego przykładu skorzystamy z certyfikatu *RADEKSERWER.radekmeryk.lokalna*. Kliknij menu *Wszystkie zadania*, a następnie polecenie menu *Zarządzaj kluczami prywatnymi*. W dalszej kolejności należy dodać konto usługi wykorzystywane do uruchomienia egzemplarza SQL Server i udzielić temu certyfikatowi uprawnień do odczytu tak, jak pokazano na rysunku 7.11.



RYСУNEK 7.11. Uprawnienia dla certyfikatu

Następnie należy zrestartować usługę SQL Server. W przypadku niepowodzenia nadania konta usługi SQL Server uprawnień odczytu dla certyfikatu restart egzemplarza SQL Server nie powiedzie się. Wystarczy teraz odświeżyć strony w programie SharePoint, a wszystko powinno działać zgodnie z oczekiwaniami.

IPsec IKEv2

Protokół IPsec pozwala zabezpieczyć kanał komunikacji pomiędzy dwoma serwerami. Dzięki jego wykorzystaniu można zablokować możliwość komunikacji pomiędzy wskazanymi komputerami. Protokół IPsec można wykorzystać nie tylko tak jak SSL — do szyfrowania ruchu do egzemplarza programu SQL Server — ale także do szyfrowania komunikacji pomiędzy serwerami programu SharePoint.

IPsec pozwala na ograniczenie komunikacji do specyficznych protokołów oraz portów TCP (UDP). Aby farma programu SharePoint była dobrym kandydatem do wykorzystania protokołu IPsec (by zapewnić wysoką wydajność), wszystkie serwery powinny być umieszczone w jednej fizycznej sieci lokalnej (LAN) i powinny być im przypisane statyczne adresy IP.

Wraz z wydaniem systemu Windows Server 2012 rozszerzono obsługę protokołu Internet Key Exchange w wersji 2 (IKEv2). W tej wersji obsługiwane są połączenia trybu transportu „od końca do końca”, a także możliwość współdziałania z innymi systemami operacyjnymi korzystającymi z protokołu IKEv2 do zabezpieczania komunikacji. Opcje te mogą współistnieć z zasadami wdrażającymi mechanizm AuthIP/IKEv1 oraz uwierzytelnianie certyfikatów. Dla protokołu IKEv2 nie istnieją narzędzia konfiguracji za pośrednictwem interfejsu użytkownika. Protokół można konfigurować wyłącznie za pomocą Windows PowerShell. IKEv2 był dostępny w systemie Windows Server 2008 R2 jako protokół tunelowania wirtualnych sieci prywatnych (VPN) zapewniający możliwość automatycznego wznowiania połączenia VPN.

Pierwszy krok w procesie konfiguracji polega na zdefiniowaniu reguły zabezpieczeń połączenia, która wykorzystuje protokół IKEv2 do komunikacji pomiędzy dwoma komputerami (*Contoso-SP1* i *Contoso-SQL*) podłączonymi do domeny *contoso.local*. Można to zrobić za pomocą kodu z listingu 7.5. Do jego uruchomienia potrzebna jest infrastruktura klucza publicznego (ang. *Public Key Infrastructure* — PKI) wymagana do uwierzytelniania komputera.

LISTING 7.5. Zasada zabezpieczeń IKEv2

```
# Utworzenie grupy zabezpieczeń dla komputerów, których będzie dotyczyła zasada
$pathname = (Get-ADDomain).distinguishedname
New-ADGroup -name "Klient i serwery IPsec" `
-SamAccountName "IPsec SharePoint" -GroupCategory security `
-GroupScope Global -path $pathname

# Dodanie komputerów testowych do grupy zabezpieczeń
$computer = Get-ADComputer -LDAPFilter "(name=Contoso-SP1)"
Add-ADGroupMember -Identity "IPsec SharePoint" -Members $computer
$computer = Get-ADComputer -LDAPFilter "(name=Contoso-SQL)"
Add-ADGroupMember -Identity "IPsec SharePoint" -Members $computer

# Ważne. Aby skorzystać z komandletów zasad grupy na serwerze, który nie jest hostem tej roli,
# należy zainstalować moduł GPO i uruchomić instrukcję import-module GroupPolicy
.

# Utworzenie obiektu GPO i powiązanie go z domeną
$gpo = New-gpo IPsecRequireInRequestOut
$gpo | new-gplink -target "dc=contoso,dc=local" -LinkEnabled Yes

# Ustawienie uprawnień do grupy zabezpieczeń dla obiektu GPO
$gpo | Set-GPPermissions -TargetName "IPsec SharePoint" `
-TargetType Group -PermissionLevel GpoApply -Replace
$gpo | Set-GPPermissions -TargetName "Uwierzytelnieni użytkownicy" `
-TargetType Group -PermissionLevel None -Replace

# Ważne. Te komandlety są nowością wprowadzoną w systemie Windows Server 2012.

# Konfiguracja certyfikatu do uwierzytelniania
$gponame = "contoso.local\IPsecRequireInRequestOut"
$certprop = New-NetIPsecAuthProposal -machine -cert `
-Authority "DC=local, DC=contoso, CN=contoso-dc"
```

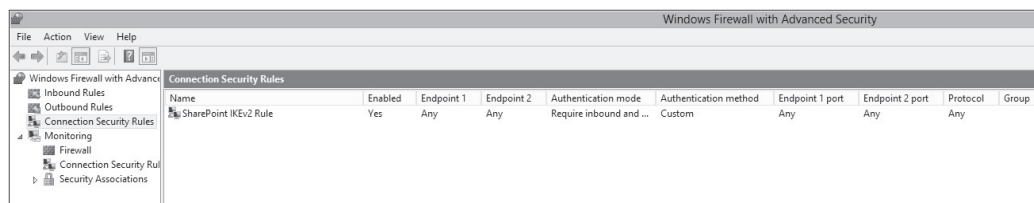
```
$myauth = New-NetIPsecPhase1AuthSet -DisplayName "IKEv2SPPhase1AuthSet" `
-proposal $certprop -PolicyStore GP0:$gponame
```

```
# Utworzenie reguły zabezpieczenia połączenia IKEv2
```

```
New-NetIPsecRule -DisplayName "Reguła IKEv2 SharePoint" `
-RemoteAddress any -Phase1AuthSet $myauth.InstanceID `
-InboundSecurity Require -OutboundSecurity Request `
-KeyModule IKEv2 -PolicyStore GP0:$gponame
```

Skrypt tworzy grupę zabezpieczeń o nazwie IPsecSharePoint i dodaje do niej członków *contoso-sql* i *contoso-sp1*. Następnie tworzy obiekt GPO o nazwie IPsecRequiredInRequestOut i wiąże go z domeną *contoso.local*. Później skrypt ustawia uprawnienia do obiektu GPO tak, by miały zastosowanie tylko do komputerów w grupie IPsecSharePoint, a nie do grupy *Użytkownicy uwierzytelnieni*. Na końcu skrypt tworzy regułę zabezpieczenia połączenia IKEv2 o nazwie *Reguła IKEv2 SharePoint*.

Możemy teraz sprawdzić konfigurację w lewym panelu przystawki *Zapora systemu Windows z zabezpieczeniami zaawansowanymi*. Kliknij *Reguły zabezpieczeń połączeń* i sprawdź, czy została włączona reguła zabezpieczenia połączeń o tej nazwie (rysunek 7.12). Należy zapamiętać, że skrypt konfiguruje tę regułę poprzez obiekt GPO, więc nie będzie dostępna natychmiast.



Name	Enabled	Endpoint 1	Endpoint 2	Authentication mode	Authentication method	Endpoint 1 port	Endpoint 2 port	Protocol	Group
SharePoint IKEv2 Rule	Yes	Any	Any	Require inbound and ...	Custom	Any	Any	Any	Any

RYСУNEK 7.12. Reguły zabezpieczeń połączeń

Planowanie i konfigurowanie funkcji Microsoft SQL Server Transparent Data Encryption

Do tej pory nauczyłeś się sposobów szyfrowania ruchu sieciowego pomiędzy serwerami w farmie oraz pomiędzy klientami korzystającymi z serwerów. Choć mechanizmy te oferują wysoki poziom bezpieczeństwa, dane przechowywane w farmie nadal mogą być wykorzystane w sposób nieodpowiedni lub mogą być skradzione poprzez przywrócenie kopii bazy danych i dołączenie jej do aplikacji sieci Web programu SharePoint. Jednym ze sposobów zabezpieczenia danych jest zaszyfrowanie ich „w spoczynku” za pomocą mechanizmu TDE (ang. *Transparent Data Encryption*).

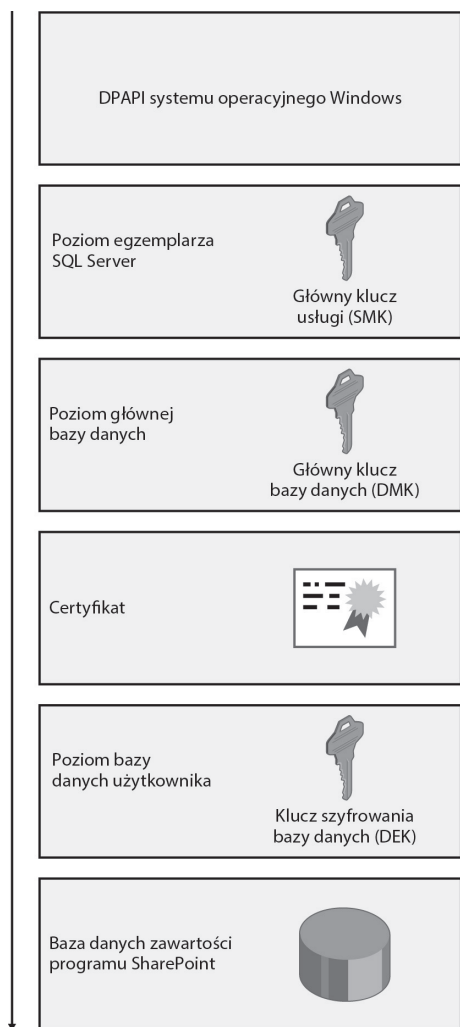


Ważne. Chociaż za pomocą mechanizmu TDE można szyfrować dane „w miejscu”, nadal są one dostępne dla administratorów SQL za pośrednictwem kwerend SQL lub mechanizmu Windows PowerShell.

Mechanizm TDE realizuje szyfrowanie wejścia-wyjścia w czasie rzeczywistym zarówno danych, jak i logów. Do szyfrowania używany jest klucz szyfrujący bazy danych (ang. *Database Encryption Key* — DEK), który jest przechowywany w rekordzie rozruchowym bazy danych, by był dostępny podczas odtwarzania. DEK jest kluczem symetrycznym zabezpieczonym za pomocą magazynu certyfikatów w bazie danych master serwera lub kluczem asymetrycznym zabezpieczonym za pomocą modułu EKM.

Warto zapamiętać, że TDE nie zapewnia szyfrowania w kanałach komunikacyjnych. Do tego służą narzędzia opisane w poprzednim podrozdziale. Szyfrowanie danych jest wykonywane na poziomie strony. Strony są szyfrowane przed zapisem i odszyfrowywane podczas wczytywania do pamięci. Z tego powodu stosowanie mechanizmu TDE nie wpływa na powiększenie rozmiaru bazy danych.

Architektura TDE obejmuje kilka różnych warstw. Interfejs API zabezpieczeń danych na poziomie systemu operacyjnego Windows (ang. *Data Protection API* — DPAPI) jest odpowiedzialny za szyfrowanie klucza głównego usługi (ang. *Service Master Key*). Klucz SMK jest tworzony na poziomie egzemplarza serwera podczas konfigurowania systemu SQL Server. Klucz SMK szyfruje klucz główny bazy danych (ang. *Database Master Key* — DMK) dla głównej bazy danych. Następnie za pomocą klucza głównego głównej bazy danych jest tworzony certyfikat w tej bazie danych. Certyfikat jest wykorzystywany do szyfrowania klucza DEK bazy danych użytkownika. I na koniec cała baza danych użytkownika jest zabezpieczona za pomocą klucza DEK bazy danych użytkownika dzięki wykorzystaniu mechanizmu TDE. Proces ten zilustrowano na rysunku 7.13.



RYСУNEK 7.13. Architektura TDE

Aby korzystać z TDE, wykonaj następujące główne czynności:

1. Stwórz klucz główny.
2. Stwórz lub uzyskaj certyfikat zabezpieczony kluczem głównym.
3. Stwórz klucz DEK i zabezpiecz go za pomocą certyfikatu.
4. Ustaw bazę danych do korzystania z szyfrowania.

Wszystkie te czynności dla bazy danych *Contoso_Content_Team* i z wykorzystaniem hasła *Passw0rd1* wykonuje kwerenda SQL Server zamieszczona na listingu 7.6.

LISTING 7.6. *Kwerenda SQL Server do konfiguracji TDE*

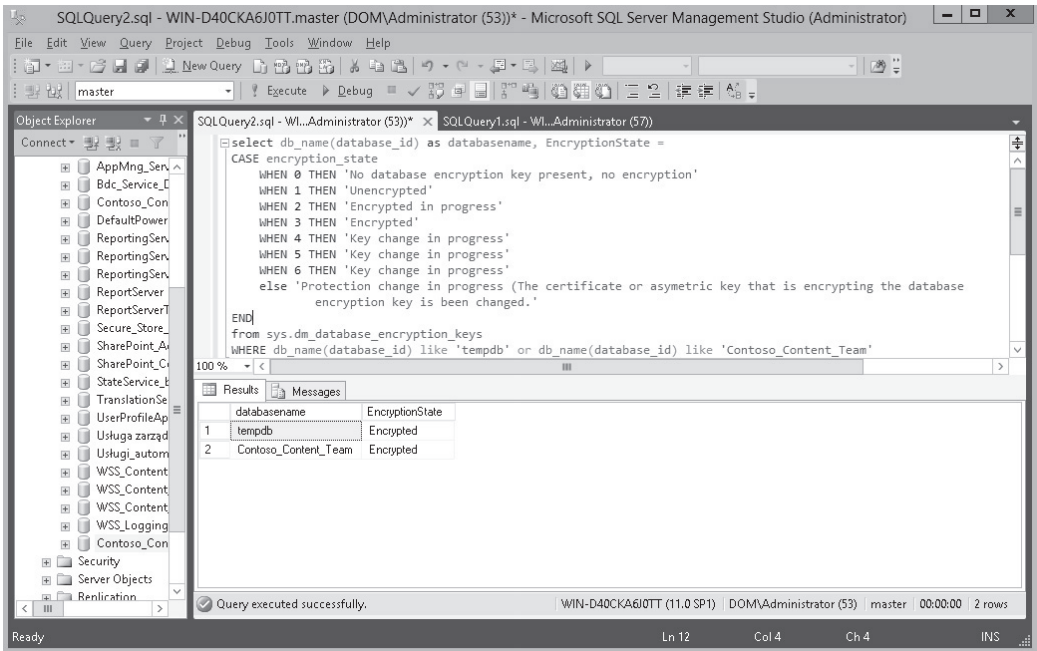
```
USE master;
GO
-- Utworzenie DMK
CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'Passw0rd1';
GO
-- Utworzenie certyfikatu DEK
CREATE CERTIFICATE TDECert WITH SUBJECT = 'Certyfikat TDE SQL Server'
GO
-- Utworzenie kopii zapasowej certyfikatu TDE
BACKUP CERTIFICATE TDECert TO FILE = 'c:\SQLTDECert.bak'
WITH PRIVATE KEY(
    FILE = 'C:\cert_privatekey.bak',
    ENCRYPTION BY PASSWORD = 'Passw0rd1'
)
GO
-- Utworzenie klucza DEK zaszyfrowanego za pomocą certyfikatu serwera
USE Contoso_Content_Team
CREATE DATABASE ENCRYPTION KEY
    WITH
        ALGORITHM = AES_256
        ENCRYPTION BY SERVER CERTIFICATE TDECert
GO
ALTER DATABASE Contoso_Content_Team SET ENCRYPTION ON
GO
```

Procesy wymagane do włączenia TDE mogą zająć trochę czasu. Z tego względu najlepiej je wykonać podczas zadań konserwacji. Aby przejrzeć status szyfrowania, uruchom kwerendę SQL Server (listing 7.7).

LISTING 7.7. *Kwerenda postępu instalacji TDE*

```
select db_name(database_id) as databasename, EncryptionState =
CASE encryption_state
    WHEN 0 THEN 'No database encryption key present, no encryption'
    WHEN 1 THEN 'Unencrypted'
    WHEN 2 THEN 'Encrypted in progress'
    WHEN 3 THEN 'Encrypted'
    WHEN 4 THEN 'Key change in progress'
    WHEN 5 THEN 'Key change in progress'
    WHEN 6 THEN 'Key change in progress'
    else 'Protection change in progress (The certificate or asymmetric key that is
    encrypting the database encryption key is been changed.'
END
from sys.dm_database_encryption_keys
WHERE db_name(database_id) like 'tempdb' or db_name(database_id) like 'Contoso_Content_Team'
```

Po zakończeniu procesu wyniki powinny być podobne do tych, które pokazano na rysunku 7.14.



RYSUNEK 7.14. Kwerenda postępu instalacji TDE

Instalowanie programu SharePoint za pomocą najmniejszych uprawnień

Stosowanie **najmniejszych uprawnień** to praktyka, która nadaje kontu użytkownika lub usługi tylko takie uprawnienia, jakie są potrzebne do realizacji konkretnego zadania i żadnych innych. Czy SharePoint 2013 w pełni obsługuje konfigurację najmniejszych uprawnień, to kwestia sporna. Z pewnością jednak można wykonać czynności zmierzające do ograniczenia uprawnień kont użytkowników i usług wyłącznie do wypełniania przypisanych im ról. Praktyka najmniejszych uprawnień i hartowania serwerów sięga pierwszych dni systemów Novell i Windows NT 4, gdy oprogramowanie było instalowane w imieniu konta systemowego. Ze względu na złożoność działania bieżących produktów programowych składających się z wielu „ruchomych części” umiejętność przyznawania odpowiednich uprawnień dostępu może się zagubić w złożoności oprogramowania. Próba przeprowadzenia analiz zmierzających do udzielenia odpowiedzi na pytanie o to, jak sprawić, by instalacje programu SharePoint pasowały do wzorca najmniejszych uprawnień, może niestety napotkać sprzeczne poglądy i koncepcje. Problem polega na tym, że ze względu na zastosowanie wzorca najmniejszych uprawnień można wprowadzić poważne ograniczenia wsparcia dla produktu. W tym podrozdziale zamieściliśmy ogólne wytyczne dotyczące tego, jakie elementy należy brać pod uwagę. Następnie opisaliśmy to, co jest potrzebne do stworzenia odpowiedniego rozwiązania dla określonej organizacji. Nie wszystkie porady pasują do wszystkich sytuacji, dlatego należy wybrać te, które są najbardziej odpowiednie dla konkretnego środowiska.

Pule aplikacji

Podobnie jak w programie SharePoint 2010, dla nowego produktu istnieje określony limit pul aplikacji, które są dozwolone dla danego serwera WWW. Na tę chwilę ten limit wynosi 10. Maksymalna liczba zależy od możliwości sprzętu i w dużej mierze od ilości pamięci przydzielonej do serwerów WWW. Bardzo aktywna pula aplikacji może zużywać 10 i więcej GB pamięci RAM. Dlaczego zatem pule aplikacji odgrywają rolę w dyskusji dotyczącej najmniejszych uprawnień? Istnieją farmy programu SharePoint, które zostały zbudowane tak, że dla każdej aplikacji usług i każdej aplikacji sieci Web programu SharePoint przypisano odrębne konto. Chociaż początkowo może się wydawać, że w takim projekcie jest przestrzegana zasada najmniejszych uprawnień, to w istocie w tym przypadku jest zużywanych zbyt wiele zasobów. Każde konto, które wykorzystamy do skonfigurowania konta usługi lub puli aplikacji, uszczupla zbiór pul aplikacji obsługiwanych w farmie. Może się zdarzyć, że liczba pul aplikacji przekroczy 10 i farma będzie działała bez zastrzeżeń. Z całą pewnością potrzeba będzie więcej pamięci RAM, niż wynoszą minimalne wymagania. Aby utrzymać liczbę pul aplikacji w ramach przyjaznych limitów, warto zastosować się do zaleceń zamieszczonych w tabeli 7.1. W niektórych organizacjach mogą obowiązywać wymogi bezpieczeństwa, które zmuszają do stosowania innych ustawień, ale zaprezentowane zalecenia powinny się sprawdzić dla większości organizacji i zapewnić lepsze wykorzystanie pamięci RAM na serwerach.

TABELA 7.1. Zalecane pule aplikacji

Pula aplikacji	Konto	Zakres odpowiedzialności
<i>SharePoint Web Services Default</i>	spServices	Host aplikacji usług programu SharePoint.
<i>SharePoint Web Content Default</i>	spContent	Host aplikacji zawartości programu SharePoint.
<i>SharePoint Central Administration v4</i>	spFarm	Host aplikacji sieci Web <i>Administracja centralna</i> .
<i>SecurityTokenServiceApplicationPool</i>	spFarm	Host usługi STS.
<i>SharePoint Secure Store</i>	spSSS	Host usługi bezpiecznego magazynu.
Pula aplikacji korzystająca z identyfikatora GUID w roli nazwy	spFarm	Host usługi topologii.

Aby zapoznać się z najnowszymi limitami dla oprogramowania SharePoint 2013, przeczytaj artykuł Microsoft TechNet znajdujący się pod adresem <http://technet.microsoft.com/en-us/library/cc262787.aspx>.

Konta użytkowników

Projektowanie farmy do spełnienia zasady najmniejszych uprawnień jest realizowane przed instalacją programów SharePoint i SQL Server. Niektóre wybory, które są podejmowane na tym etapie, mogą mieć ogromny wpływ na bezpieczeństwo farmy. W społeczności użytkowników programu SharePoint krąży żart, że aby program SharePoint działał w sposób, w jaki został zaprojektowany, wystarczy użyć konta administratora domeny w roli konta farmy. Niestety istnieją farmy, które zostały zainstalowane w ten sposób, a gdy hasło administratora domeny się zmieniło, wszystko w programie SharePoint przestawało działać. Przywrócenie farmy programu SharePoint do działania wymaga przestudiowania materiału zamieszczonego w tym podrozdziale. Żeby było jasne: nie trzeba tu stosować takich samych nazw kont. Ten wykład nie jest lekcją na temat standardów. To jedynie ogólne wytyczne na temat mapowania ról i odpowiedzialności na obiekty użytkowników usługi Active Directory. Zalecane konta użytkowników z podziałem na role zestawiono w tabeli 7.2.

TABELA 7.2. Zalecane konta użytkowników według ról

Konto	Przeznaczenie	Wymagania
sqlInstall	Konto używane do instalacji systemu SQL Server.	Administrator lokalnego serwera na serwerach z SQL Server podczas procesu instalacji.
sqlService	Konto używane dla: ■ MSSQLSERVER, ■ SQLSERVERAGENT.	Uprawnienia do zewnętrznych zasobów do tworzenia kopii zapasowych i odtwarzania.
spInstall	Konto używane do: ■ wykonywania instalacji, ■ uruchamiania programu <i>SharePoint Product Configuration Wizard</i>.	Administrator lokalnego serwera, na którym jest uruchomiony proces instalacji, podczas tego procesu. Logowanie SQL Server na komputerze z uruchomionym systemem SQL Server. Członek ról SQL: ■ stała rola serwera securityadmin, ■ stała rola serwera dbcreator.
spFarm	Konto używane do: ■ tożsamości puli aplikacji dla witryny sieci Web <i>Administracja centralna</i>, ■ uruchamiania usługi SharePoint Foundation Workflow Timer.	Uprawnienia są udzielane automatycznie kontu farmy serwera. Dla komputerów, na których działa SQL Server, konto jest automatycznie dodawane jako konto logowania SQL Server. Konto jest dodawane do następujących ról: ■ stała rola serwera dbcreator, ■ stała rola serwera securityadmin, ■ stała rola bazy danych db_owner dla wszystkich baz danych programu SharePoint wewnątrz farmy serwera. Tego konta nie należy używać do administrowania farmą! Nigdy nie należy logować się do farmy z wykorzystaniem tego konta.
spAdmin	Konto używane do konfiguracji farmy serwera i zarządzania nią.	Główne konto administracji. Jeśli są potrzebne funkcje administracji za pomocą mechanizmu Windows PowerShell, wymagane jest uprawnienie <code>SharePoint_Shell_Access</code> . Lokalny administrator na serwerach z systemem SharePoint.
spContent	Spełnia rolę tożsamości puli aplikacji dla zawartości sieci Web programu SharePoint.	Automatycznie nadaje potrzebne uprawnienia do baz danych zawartości: <code>spDataAccess</code> .
spServices	Spełnia rolę tożsamości puli aplikacji dla aplikacji usług programu SharePoint.	Automatycznie nadaje potrzebne uprawnienia do baz danych zawartości: <code>spDataAccess</code> .
spC2WTS	Tożsamość, z jaką działa usługa c2WTS.	Prawa lokalnego administratora serwera, na którym działa usługa c2WTS, oraz lokalne zasady zabezpieczeń dla: <i>Działanie jako część systemu operacyjnego</i> , <i>Personifikuj klienta po uwierzytelnieniu</i> , <i>Logowanie w trybie usługi</i> .

TABELA 7.2. Zalecane konta użytkowników według ról — ciąg dalszy

Konto	Przeznaczenie	Wymagania
spUPS	Tożsamość wykorzystywana podczas procesu synchronizacji profili użytkowników.	Uprawnienia Active Directory: <i>Replication Directory Changes</i> .
spCrawl	Domyślne konto dostępu do zawartości. Używane do przeszukiwania danych przez usługę wyszukiwania.	Dostęp odczytu do przeszukiwanej zawartości.
spSSS	Spełnia rolę tożsamości puli aplikacji dla usługi bezpiecznego magazynu.	Automatycznie nadaje potrzebne uprawnienia do baz danych zawartości: <i>spDataAccess</i> .
spSuperUser	Konto używane do buforowania.	Konto ma pełny dostęp do aplikacji sieci Web <i>Publikowanie</i> .
spSuperReader	Konto używane do buforowania.	Konto ma dostęp <i>Pełny odczyt</i> do aplikacji sieci Web <i>Publikowanie</i> .
spUnattend	Konto używane do dostępu do zewnętrznych danych.	Dostęp do zewnętrznych danych.

Niektóre z kont wymienionych w tabeli 7.2 mogą być niepotrzebne w części farm. Usługa *Oświadczeń do usługi tokenu systemu Windows* (c2WTS), którą wprowadziliśmy w rozdziale 6., zazwyczaj jest potrzebna tylko w scenariuszach analiz biznesowych. Żadne z kont wyszczególnionych w tabeli nie powinno być odwzorowane na konto *DOMENA\Administrator*. Chociaż to konto może mieć dostęp do programu SharePoint, nie powinny to być wspólne poświadczenia. Poziom dostępu udzielony wybranej osobie przy użyciu tego konta przekracza uprawnienia potrzebne do administracji programem SharePoint. Warto również zauważyć, że w niektórych organizacjach mogą obowiązywać zasady, zgodnie z którymi nie wolno używać ogólnych kont administracji (spAdmin) do celów inspekcji.

Konto instalacji programu SharePoint (spInstall) otrzymuje uprawnienia, które obejmują:

- przynależność do grupy zabezpieczeń Windows *WSS_ADMIN_WPG*,
- przynależność do roli *IIS_WPG*.

Po uruchomieniu kreatorów konfiguracji konto ma następujące uprawnienia do bazy danych:

- *db_owner* dla bazy danych konfiguracji farmy serwerów programu SharePoint,
- *db_owner* dla bazy danych zawartości aplikacji *Administracja centralna* programu SharePoint.

Konto farmy programu SharePoint (spFarm), określane również jako *konto dostępu do bazy danych*, jest używane także jako tożsamość puli aplikacji *Administracja centralna* i spełnia rolę konta przetwarzania usługi czasomierza SharePoint Foundation 2013. Musi to być konto domenowe. Chociaż to konto automatycznie otrzymuje uprawnienia, których potrzebuje, to po uruchomieniu programu SharePoint Configuration Wizard uzyskuje następujące uprawnienia systemowe:

- przynależność do grupy zabezpieczeń systemu Windows *WSS_ADMIN_WPG* dla usługi czasomierza SharePoint Foundation 2013,
- przynależność do usługi *WSS_RESTRICTED_WPG* dla puli aplikacji *Administracja centralna* oraz usługi czasomierza,
- przynależność do grupy *WSS_WPG* dla puli aplikacji *Administracja centralna*.

Po uruchomieniu kreatorów konfiguracji konto ma następujące uprawnienia do bazy danych:

- stała rola serwera dbcreator,
- stała rola serwera securityadmin,
- db_owner dla wszystkich baz danych programu SharePoint z wyjątkiem bazy danych *Farm_Config*, dla której konto otrzymuje uprawnienie SP_DataAccess.

Konto uzyskuje również przynależność do roli WSS_CONTENT_APPLICATION_POOLS dla bazy danych konfiguracji farmy serwera SharePoint oraz przynależność do roli WSS_CONTENT_APPLICATION_POOLS dla bazy danych zawartości *SharePoint_Admin*.

Konto usług programu SharePoint (spServices) to konto puli aplikacji wykorzystywane do określenia tożsamości puli aplikacji. Konto puli aplikacji wymaga zastosowania następujących ustawień konfigurowania uprawnień:

- Automatycznie są konfigurowane poniższe uprawnienia poziomu komputera:
 - konto puli aplikacji należy do grupy WSS_WPG.
- Automatycznie są konfigurowane dla tego konta następujące uprawnienia bazy danych i systemu SQL Server:
 - konta puli aplikacji dla aplikacji sieci Web są przypisywane do roli SP_DATA_ACCESS dla baz danych zawartości;
 - konto jest przypisywane do roli WSS_CONTENT_APPLICATION_POOLS powiązanej z bazą danych konfiguracji farmy;
 - konto jest przypisywane do roli WSS_CONTENT_APPLICATION_POOLS powiązanej z bazą danych zawartości *SharePoint_Admin*.

O ile za pomocą reguły przeszukiwania dla wzorca adresu URL lub wskaźnika URI nie zostanie określona inna metoda uwierzytelniania, to do przeszukiwania zawartości wewnątrz aplikacji usługi wyszukiwania jest wykorzystywane domyślne konto dostępu do zawartości (spCrawl). Konto wymaga następujących ustawień konfigurowania uprawnień:

- Domyślne konto dostępu do zawartości musi być kontem użytkownika domeny posiadającym dostęp odczytu do zewnętrznych lub bezpiecznych źródeł zawartości, które mają być przeszukane przy użyciu tego konta.
- W przypadku witryn serwera SharePoint, które nie należą do farmy serwerów, trzeba jawnie przydzielić do tego konta prawa pełnego odczytu do aplikacji sieci Web będących hostem dla witryn. Najczęściej jest to scenariusz obejmujący wiele farm lub scenariusz federacyjny.
- Konto musi należeć do grupy *Administratorzy farmy*.

Konto usługi nienadzorowanej (spUnattend) jest używane przez kilka usług do podłączenia do zewnętrznych źródeł danych wymagających podania nazwy użytkownika i hasła i bazujących na uwierzytelnianiu w systemach operacyjnych innych niż Windows. Jeśli to konto nie zostanie skonfigurowane, usługi te nie będą podejmowały próby nawiązania połączenia ze źródłami danych tych typów. Chociaż do połączeń ze źródłami danych systemów operacyjnych innych niż Windows są używane poświadczenia konta, to jeśli konto nie jest członkiem domeny, usługi nie mogą uzyskać do nich dostępu. Musi to być konto domenowe. Konto może być wykorzystywane między innymi przez usługę bezpiecznego magazynu albo usługi PerformancePoint lub Microsoft Excel.

Zarządzane konta programu SharePoint

Powinieneś już wiedzieć o tym, w jaki sposób w programie SharePoint działają zarządzane konta. Z tego względu niniejszy podrozdział będzie służyć jako krótkie przypomnienie i wyszczególnienie tych kont, które powinny być kontami zarządzanymi, w zestawieniu z tymi, które nie powinny być zarządzane.

Zarządzane konta programu SharePoint mogą być rejestrowane lub usuwane za pomocą programu *Administracja centralna* albo za pomocą skryptu Windows PowerShell (*-SPManagedAccount). Należy pamiętać, że zarządzanie hasłami w przypadku zarządzanych kont programu SharePoint powinno być realizowane wewnątrz programu SharePoint, a nie za pośrednictwem usług katalogowych Active Directory. Interfejs zarządzania hasłami kont zarządzanych jest dostępny za pośrednictwem okna *Zarządzanie kontem* (rysunek 7.15). Należy pamiętać, że jest to jeszcze jeden obszar w obrębie produktu, w którym poświadczenia są przysyłane jako zwykły tekst, dlatego należy zadbać o to, by aplikacja *Administracja centralna* działała za pomocą protokołu SSL.

Zarządzanie kontem

Administracja centralna

- Zarządzanie aplikacjami
- Ustawienia systemowe
- Monitorowanie
- Wykonywanie kopii zapasowych i ich przywracanie
- Zabezpieczenia
- Uaktualnianie i migracja
- Ogólne ustawienia aplikacji
- Aplikacje
- Kreatorzy konfiguracji

Wybieranie konta

Konta zarządzane są używane podczas działania różnych składników farmy.

Zarządzanie poświadczeniami

Aby natychmiast zmienić hasło, zaznacz opcję **Zmień teraz hasło**. Aby wygenerować nowe silne hasło, wybierz opcję **Generuj nowe hasło**. Aby ustawić hasło na nową wartość, wybierz opcję **Ustaw hasło konta i wprowadź wartość hasła**. Aby ustawić zapisaną wartość hasła na bieżącą znaną wartość, wybierz opcję **Użyj istniejącego hasła i wprowadź wartość hasła**.

Automatyczne zmienianie hasła

Funkcja automatycznego zmieniania hasła umożliwia programowi SharePoint automatyczne generowanie nowych silnych hasel zgodnie z ustawionym harmonogramem. Zaznacz pole wyboru **Włącz automatyczne zmienianie hasła**, aby zezwolić programowi SharePoint na zarządzanie hasłem dla wybranego konta.

Jeśli na podstawie zasad konta dla konta zostanie wykryta data wygaśnięcia i wygaśnięcie nastąpi przed zaplanowaną datą i godziną, hasło zostanie zmienione skonfigurowaną liczbę dni przed datą

Konto zarządzane: RADEKMERYK\radekm

☐ Zmień hasło teraz

☒ Generuj nowe hasło

☒ Ustaw hasło konta na nową wartość

.....

Potwierdź hasło

☒ Użyj istniejącego hasła

☐ Włącz automatyczne zmienianie hasła

Jeśli zostanie wykryta zasada wygasania hasel, zmień hasło

dni przed wymuszeniem zasady wygasania

☒ Uruchom powiadomienie pocztą e-mail

dni przed zmianą hasła

☒ Co tydzień

☐ Co miesiąc

RYСУNEK 7.15. Okno *Zarządzanie kontem*

Okno *Zarządzanie kontem* pozwala na automatyczne bądź ręczne zarządzanie hasłami. Konto farmy programu SharePoint (spFarm) jest dodawane do programu SharePoint jako konto zarządzane automatycznie. Za tworzenie nowych zarządzanych kont, jeśli okażą się potrzebne, jest odpowiedzialny administrator programu. Zazwyczaj takie konta tworzy się dla kont puli aplikacji usług (spServices)

lub zawartości sieci Web (spContent). Domyślne konto dostępu do zawartości (spCrawl) oraz konto usługi synchronizacji profilu użytkownika (spUPS) nie są kontami zarządzanymi. W przypadku zmiany hasła należy samodzielnie wejść do tych obszarów i ręcznie zaktualizować poświadczenia. Wszystkie konta przypisane do usług za pomocą mechanizmu *Konfiguruj konta usług* także powinny być kontami zarządzanymi. Przykładem takiego konta może być konto usługi *Oświadczenia do usługi tokenu systemu Windows* (spC2WTs).

W niektórych organizacjach obowiązują surowe wymagania dotyczące zmiany haseł — na przykład wymaganie zmiany hasła co 90 dni. Takie mechanizmy, jeśli nie zostaną podjęte odpowiednie wysiłki, mogą spowodować wiele problemów w programie SharePoint. Nie będziemy tu dyskutować o tym, czy tego rodzaju zasady powinny być egzekwowane, czy nie. Niektórzy eksperci twierdzą, że automatyczne regularne zmienianie haseł po upływie określonej liczby dni wprowadza większe zagrożenia dla systemu niż ciągłe stosowanie silnych haseł. Jeśli konto zostanie skonfigurowane jako zarządzane, hasło do niego nie musi być znane. Hasła mogą zawierać długie ciągi znaków, które są trudne do zapamiętania. Należy zadbać o to, aby administratorzy zdawali sobie sprawę z tego, że konta zarządzane powinny być modyfikowane w programie SharePoint, a nie w usłudze Active Directory.

Role i uprawnienia grup

Kontom, które wybieramy do obsługi farmy programu SharePoint, są przypisywane różne role i uprawnienia. Chociaż dzieje się to automatycznie, należy zdawać sobie sprawę z tego, jakie ma to znaczenie dla stosowanego modelu bezpieczeństwa. Najpierw zapoznasz się z różnymi rolami bazy danych oraz usprawnieniami wprowadzonymi przez firmę Microsoft po to, by konta miały tylko te uprawnienia, których potrzebują. Niniejszy podrozdział zakończymy opisem uprawnień grup przypisywanych do kont programu SharePoint.

Role

W programie SharePoint 2013 wprowadzono wiele zmian do ról baz danych programu SharePoint. Należą do nich WSS_CONTENT_APPLICATION_POOLS, WSS_SHELL_ACCESS, SP_READ_ONLY oraz SP_DATA_ACCESS.

Rola bazy danych WSS_CONTENT_APPLICATION_POOLS dotyczy konta puli aplikacji dla każdej aplikacji sieci Web, która jest zarejestrowana w farmie programu SharePoint. Rola umożliwia aplikacji sieci Web generowanie kwerend i aktualizowanie mapy witryny oraz określenie dostępu tylko do odczytu do innych elementów w bazie danych konfiguracji. Rola jest przypisywana w procesie konfiguracji. Jest ona stosowana do baz danych SharePoint_Config oraz SharePoint_AdminContent. Członkowie roli mają prawo wykonywania dla zbioru procedur zapisanych w bazie danych. Rola dostarcza również uprawnień wybierania do tabeli *Versions* w bazie danych SharePoint_AdminContent. Można też zauważyć, że z tej roli korzysta baza danych *usługi stanu*.

Przypisanie roli bazy danych WSS_SHELL_ACCESS zastępuje potrzebę dodania konta administratora jako db_owner bazy danych konfiguracji programu SharePoint. Domyślnie do roli WSS_SHELL_ACCESS jest przypisane konto instalacji (spInstall). Dzięki temu konto ma uprawnienia uruchamiania wszystkich procedur składowanych zapisanych w bazie danych. Dodatkowo członkowie tej roli mają uprawnienia odczytu i zapisu do wszystkich tabel bazy danych. Do zarządzania użytkownikami wewnątrz tej roli można skorzystać z komandletów Windows PowerShell (*-SPShellAdmin).

Rola bazy danych SP_READ_ONLY zastępuje potrzebę używania opcji sp_dboption do ustawiania dla bazy danych trybu tylko do odczytu. Opcję tę usunięto z systemu SQL Server 2012. Z roli należy korzystać w przypadku, gdy do danych jest wymagany dostęp tylko do odczytu — na przykład do danych

dotyczących wykorzystania i telemetrii. Rola nadaje swoim członkom uprawnienie SELECT do wszystkich procedur składowanych, funkcji i tabel programu SharePoint oraz uprawnienie EXECUTE do typów definiowanych przez użytkownika w przypadku stosowania schematu dbo.

Rola bazy danych SP_DATA_ACCESS jest domyślną rolą dostępu do bazy danych. Powinna być stosowana w odniesieniu do wszystkich operacji dostępu do bazy danych na poziomie modelu obiektowego. Podczas aktualizacji lub nowych instalacji programu SharePoint do tej roli jest automatycznie dodawane konto puli aplikacji. Rola SP_DATA_ACCESS zastępuje opcję db_owner, chociaż można zauważyć, że własność ta nie została jeszcze wszędzie zaimplementowana. Rola została zaimplementowana między innymi dla baz danych aplikacji, usługi stanu, usługi użycia, a także baz danych konfiguracji i administracji programu SharePoint.

Uprawnienia grup

Podczas procesu instalacji programu SharePoint tworzonych jest wiele grup, które są ważne pod kątem działania produktu. Są to między innymi grupy WSS_ADMIN_WPG, WSS_WPG oraz WSS_RESTRICTED_WPG.

Grupa WSS_ADMIN_WPG ma uprawnienia odczytu i zapisu do lokalnych zasobów. Do tej roli należą konta puli aplikacji *Administracja centralna* oraz usługi czasomierza (spFarm). Grupa ma uprawnienia pełnej kontroli w stosunku do katalogów o kluczowym znaczeniu dla programu SharePoint, w tym do wszystkich podkatalogów katalogu głównego programu SharePoint, katalogu %windir%\System32\drivers\etc\HOSTS oraz lokalizacji IIS folderu Wss. Rolę WSS_ADMIN_WPG należy monitorować za pomocą SCOM. Uruchomienie komandletu Remove-SPShellAdmin powoduje podjęcie próby usunięcia konta, jeśli nie jest ono potrzebne w innym miejscu.

Grupa WSS_WPG ma dostęp odczytu do zasobów lokalnych, a do jej członków należą wszystkie pule aplikacji i konta usług. Grupa nie ma prawa zapisu do lokalizacji dzienników programu SharePoint, ale ma dostęp odczytu do pozostałej części zasadniczej infrastruktury programu SharePoint.

Członkowie grupy WSS_RESTRICTED_WPG mają prawo odczytu zaszyfrowanego wpisu poświadczeń konta administracji farmy. Grupa jest wykorzystywana tylko do szyfrowania i odszyfrowywania haseł, które są przechowywane w bazie danych konfiguracji. Ma pełną kontrolę nad wpisem w rejestrze wykorzystywanym do przechowywania haseł w bazie danych konfiguracji. W przypadku zmodyfikowania klucza konfigurowanie usług i wykonywanie innych funkcji nie powiedzie się.

Podsumowanie

W tym rozdziale zaprezentowano wiele informacji dotyczących bezpieczeństwa platformy. Przedstawiono przykłady blokowania, śledzenia i raportowania instalacji programu SharePoint w przedsiębiorstwie. Następnie omówiliśmy komunikację w programie SharePoint i znaczenie korzystania z protokołu SSL w środowisku programu SharePoint. Ponieważ protokół SSL pozwala na szyfrowanie wyłącznie transmisji, a nie danych „w spoczynku”, pokazaliśmy również sposób wykorzystania mechanizmu TDE systemu SQL Server TDE do szyfrowania danych w bazie danych SQL Server. Na koniec zaprezentowaliśmy konta użytkowników, które są potrzebne do instalowania programu SharePoint zgodnie z zasadą najmniejszych uprawnień, a następnie omówiliśmy uprawnienia ról i grup powiązanych z tymi kontami. Jednym z elementów układanki, którego dotychczas nie analizowaliśmy, jest działanie aplikacji *Administracja centralna* z wykorzystaniem SSL. W wielu miejscach w tym rozdziale wskazywaliśmy obszary programu SharePoint, gdzie poświadczenia są przesyłane w formie zwykłego tekstu. Z pewnością zauważyłeś w programie komunikaty ostrzeżeń wyświetlone na czerwono, podobne do tego, który pokazano na rysunku 7.16.

RYСУNEK 7.16. Komunikat ostrzeżenia o przesyłaniu haseł jako zwykłego tekstu

Żałujemy, że otrzymaliśmy polecenie zapewnienia szyfrowania całej komunikacji aplikacji *Administracja centralna*. Ponieważ farma już została zbudowana, nasze zadanie polega na dokonaniu konwersji wcześniej stworzonej witryny sieci Web, tak by korzystała z protokołu SSL. Niezależnie od tego, czy konwertujemy istniejącą aplikację, czy też tworzymy nową, ogólnie rzecz biorąc, procedura jest taka sama. Aby zrealizować zadanie, wykonaj następujące czynności:

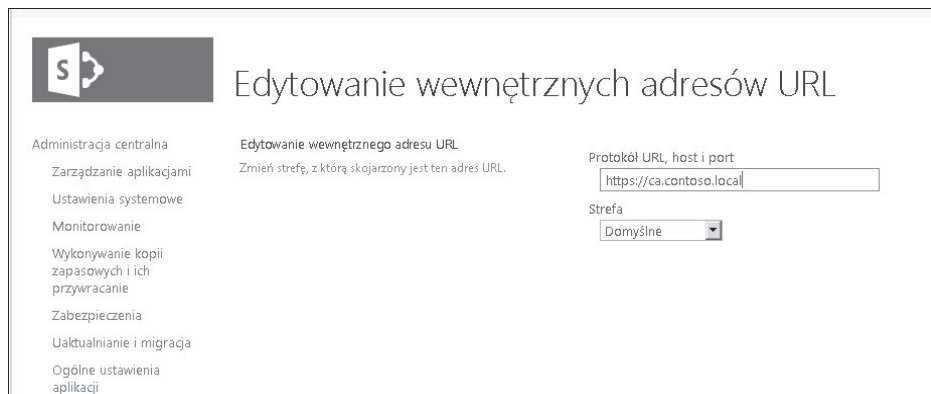
1. Sprawdź, czy istnieje wpis w usłudze DNS dla nazwy *ca.contoso.local*.
2. Stwórz certyfikat SSL dla adresu URL (*ca.contoso.local*).
3. Skonfiguruj *Mapowania dostępu alternatywnego* (ang. *Alternate Access Mappings* — AAM) dla aplikacji *Administracja centralna*.
4. Zmień powiązany port.
5. Skonfiguruj powiązania IIS.

Pierwszy krok polega na stworzeniu wpisu DNS dla adresu URL, który chcemy wykorzystać. Aplikacja *Administracja centralna* jest zainstalowana na serwerze z dużym numerem portu. Będziemy adresowali ją za pomocą wspólnej nazwy. Na potrzeby tego przykładu będzie to nazwa *ca.contoso.local*.

Następny krok polega na stworzeniu certyfikatu SSL. Jak wspomniano wcześniej w tym rozdziale, najlepszym sposobem na dostarczenie organizacji certyfikatu SSL do wykorzystania w sieci intranet przedsiębiorstwa jest wykorzystanie urzędu certyfikacji domeny (*UC Domeny*) — rysunek 7.17.

RYСУNEK 7.17. Okno dialogowe Utwórz certyfikat

Po stworzeniu certyfikatu należy zmodyfikować powiązane mapowania AAM z nazwy serwera na wspólną nazwę w sposób pokazany na rysunku 7.18.



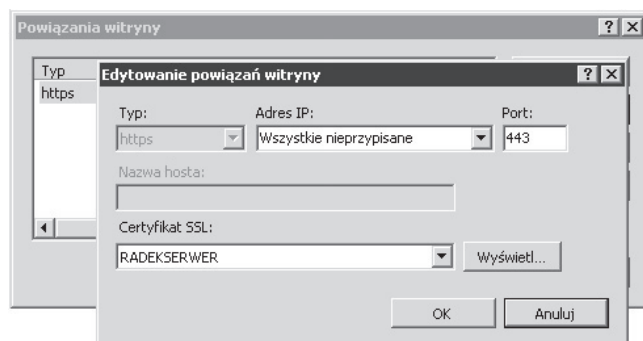
RYСУNEK 7.18. Strona *Edytowanie wewnętrznych adresów URL*

Następna czynność polega na zmianie portu przypisanego do aplikacji *Administracja centralna*. Gdyby to była nowa farma, moglibyśmy zamiast portu o dużym numerze użyć portu 443. Ponieważ jednak w tym ćwiczeniu przeprowadzamy konwersję istniejącej witryny, skorzystamy z komendletu `Set-SPCentralAdministration` i ustawimy port na 443 tak, jak pokazano na listingu 7.8.

LISTING 7.8. Zmiana portu

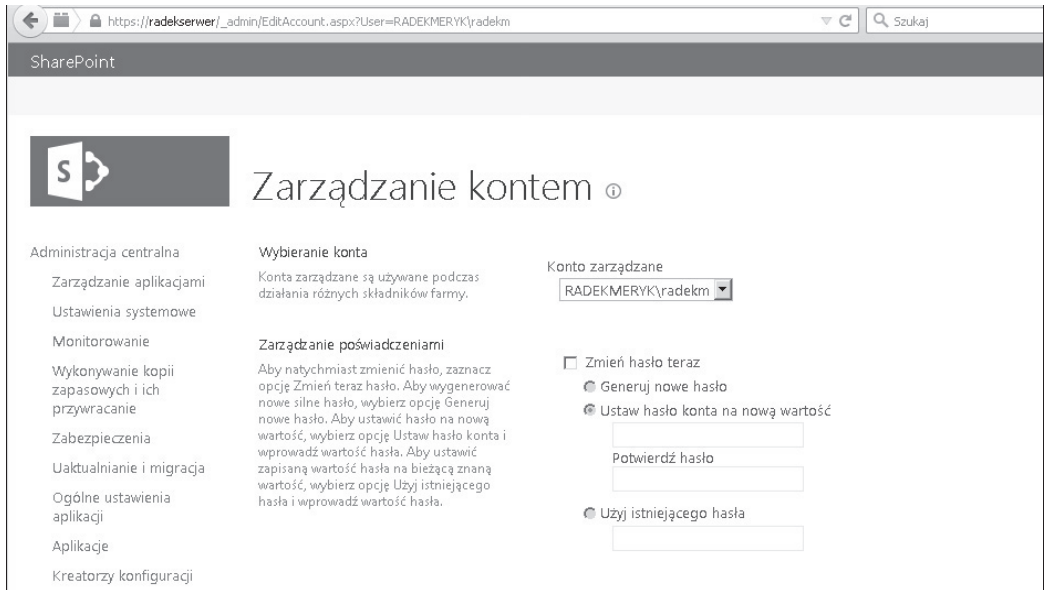
```
Set-SPCentralAdministration -Port 443
```

Wspólna nazwa używana do utworzenia certyfikatu będzie wykorzystana do powiązania IIS. Powiązania można ustawić za pomocą interfejsu użytkownika albo za pośrednictwem skryptu Windows PowerShell. Na potrzeby niniejszego przykładu skorzystamy z interfejsu użytkownika (rysunek 7.19).



RYСУNEK 7.19. Okno dialogowe *Edytowanie powiązań witryny*

Po skonfigurowaniu powiązań witryny możemy przeglądać aplikację *Administracja centralna* za pośrednictwem SSL. Po przejściu do ekranów, w których wcześniej wyświetlały się ostrzeżenia o przesyłaniu haseł w formacie zwykłego tekstu, można zauważyć, że ostrzeżenia już się nie wyświetlają (rysunek 7.20).



RYСУNEK 7.20. Strona Zarządzanie kontem bez ostrzeżenia o przesyłaniu haseł jako zwykłego tekstu

Skorowidz

A

AAM, Alternate Access Mappings, 27, 241
ACS, Access Control Service, 194
ACS, Azure Access Control, 90
agent FIM, 224
aktualizacja
 aplikacji usług, 279
 baz danych zawartości, 283
 Centrum wyszukiwania, 278
 mechanizmów uwierzytelniania, 247
 odroczonego zbiorów witryn, 248
 pokazowych zbiorów witryn, 249
 poprzez dołączenie bazy danych, 247
 równoległa witryn, 266
 środowiska, 245
 w miejscu, 247
aliasy
 SQL, 138
 SQL Server, 43
AlwaysOn, 134
analiza
 biznesowa, 94
 opcji AuthN, 175
analizator
 kondycji bazy danych, 311
 kondycji programu, 293
API, 28

aplikacja, 33
 Administracja centralna, 144, 220
 usługi
 automatycznego tłumaczenia, 47
 automatyzacji Worda, 46
 bezpiecznego magazynu, 46, 281
 Excel Services, 156
 łączności danych biznesowych, 46, 281
 odnajdowania aplikacji, 121
 PerformancePoint, 281
 profilu użytkowników, 282
 programu PerformancePoint, 46
 SQL Server PowerPivot, 46
 SQL Server Reporting Services, 162, 163
 stanu, 46
 tłumaczenia maszynowego, 109
 ustawień subskrypcji, 46
 wyszukiwania, 115
 zarządzania aplikacjami, 109
 zarządzania pracą, 110
 zarządzanych metadanych, 281
 zbierania danych, 46
usługowa, 100
 Access 2010, 111
 Access Services, 108
 BDC, 112MMS, 113

 Excela, 113
 PPS, 114
 SSS, 118
 STS, 122
 UPA, 118
 VGS, 119
 WAS, 120
aplikacje
 docelowe, 203
 sieci Web, 23, 47
usługowe
 implementacja, 103
 nawiązanie połączenia, 128
 publikowanie, 127
 punkt końcowy, 102
 równoważenia obciążenia, 121
 serwery proxy, 102
 ustawienia uprawnień, 129
w chmurze, 195
Web pakietu Microsoft Office, 262
architektura
 aplikacji usługowych, 100
 fizyczna, 83
 hybrydowa, 85
 informacyjna, 79, 92
 logiczna, 82
 metadanych, 81
 programu, 21
 SAML, 190
 TDE, 231
 witryny, 80
 wyszukiwania, 87

ASP.NET, 303
 automatyczne tworzenie
 statystyk, 138
 autoryzacja, 175
 autoryzacja AuthZ, 205
 awaria, 55
 awaryjne zastępowanie funkcji, 40

B

baza danych, 27, 43, 103
 administracji wyszukiwania,
 145
 alertowania serwera raportów,
 149
 aplikacji usługi wyszukiwania,
 145
 aplikacji usługowych, 45
 automatyzacji Worda, 147
 bezpiecznego magazynu, 146
 konfiguracji, 143
 łączności danych
 biznesowych, 145
 łączy, 146
 PowerPivot, 148
 profilu, 147
 przeszukiwania, 145
 raportowania analiz, 145
 SharePoint_Config, 44
 SharePoint_Content_Admin,
 44
 serwera raportów, 149
 synchronizacji, 147
 usług PerformancePoint
 Services, 148
 usługi stanu, 148
 usługi tłumaczenia
 maszynowego, 148
 ustawień subskrypcji, 146
 WSS_Content, 44
 zarządzania aplikacjami, 144
 zarządzanych metadanych, 148
 zawartości, 144
 zintegrowanych usług
 raportowania, 149

bazy danych
 nieobsługiwane, 248
 obsługiwane, 247
 SQL Server, 150
 systemowe, 44
 BCS, Business Connectivity
 Services, 24
 bezpieczeństwo, 93
 bezpieczeństwo platformy, 215
 BI, Business Intelligence, 114
 BIA, Business Impact Analysis,
 333
 biblioteki, 32, 34
 blokowanie instalacji, 216
 błędy spójności, 311
 brak większości, 348
 budowanie, 12
 budowanie farmy testowej, 276
 buforowanie, 315

C

c2WTS, 184
 CA, Certification Authority, 220
 całkowita liczba użytkowników,
 385
 cele
 BCM, 334
 biznesowe, 75
 certyfikat
 osobisty, 227
 SSL, 89
 ciągłość działania, 333, 346
 CLI, Command Line Interfaces, 53
 CSOM, Client-Side Object
 Model, 90
 cykl utrzymania, 291
 czas
 ładowania strony, 382
 myślenia, 392
 czerwona strefa, 386

D

dane LOB, 112
 DDL, Data Definition Language,
 135
 DEK, Database Encryption Key,
 230
 delegowanie, 183
 DNS, Domain Name System, 24,
 180
 dodatek
 Commands, 62
 LPS, 375
 Reporting Services, 162
 spPowerPivot.msi, 152
 dodawanie zestawów liczników,
 411
 dokumentacja, 55, 79, 413
 dokumentowanie
 innych usług, 261
 środowiska, 257
 ustawień bieżących, 257
 ustawień środowiska, 259
 ustawień usług, 259
 dostawca
 danych użytkownika, 299
 SSP, 99
 dostrajanie, 307
 konfiguracji, 55
 wydajności indeksu, 312
 wydajności sieci, 314
 DPAPI, Data Protection API, 231
 DR, Disaster Recovery, 333
 dublowanie bazy danych, 132,
 349, 356
 dwukierunkowe wyszukiwanie
 federacyjne, 88
 dysk, 302
 dysk iSCSI, 173
 dystrybucja obciążenia, 395
 dziennik zdarzeń systemu
 Windows, 328
 dzienniki, 326

E

edytowanie
 adresów URL, 242
 powiązań witryny, 242
 egzemplarz
 maszynowy usługi, 100
 klastrów pracy awaryjnej,
 132, 134
 eksportowanie
 konfiguracji wyszukiwania, 31
 witryny, 339
 elementy list, 34
 emisja pojedyncza, 359
 etapy aktualizacji, 253

F

farma, 273, 274
 menedżera żądań, 323
 SharePoint, 22
 SharePoint Server 2013, 404
 usług współdzielonych, 255
 FBA, Forms-Based
 Authentication, 25, 189
 federacja
 usług, 123
 usługi wyszukiwania, 279
 Fiddler, 370
 FIM, Forefront Identity Manager,
 118, 224
 folder, 33
 _app_bin, 36
 _vti_pvt, 36
 ADMIN, 39
 ADMISAPI, 38
 App_Browsers, 36
 App_GlobalResources, 37
 Bin, 37
 BIN, 38
 Client, 38
 CONFIG, 38
 CONTROLTEMPLATES, 39
 DocumentTemplates, 39
 FEATURES, 39

HCCab, 38
 Help, 38
 IMAGES, 39
 ISAPI, 38
 LAYOUTS, 39
 LCIDSts, 39
 LOGS, 38
 Policy, 38
 Resources, 38
 SiteTemplates, 39
 SQL, 40
 TEMPLATE, 39
 THEMES, 40
 UserCode, 40
 WebClients, 40
 WebServices, 40
 WorkflowActivities, 40
 wpresources, 37

formularz Tworzenie nowej
 aplikacji, 222
 fragmentacja indeksu, 312
 funkcja
 Feature Fallback, 40, 249
 Rejestrowanie serwera IIS, 374
 funkcje
 analityki biznesowej, 152
 autoryzacji AuthZ, 205
 BCM, 335
 wyszukiwania, 30
 funkcjonalność Shredded
 Storage, 165

G

geoklaster, 347
 główny katalog, 38
 graficzny interfejs użytkownika,
 GUI, 52
 grupy
 dostępności, 132, 134, 354
 serwerów proxy usługi, 100

H

hierarchia farmy, 22
 hybrydowa architektura BCS, 88

I

identyfikacja
 interesariuszy, 74
 procesów biznesowych, 93
 identyfikator aplikacji, 204
 IIS, Internet Information
 Services, 175
 implementacja
 aplikacji usługowej, 103
 uaktualnienia, 270
 importowanie konfiguracji
 wyszukiwania, 31
 informacje dotyczące ładowania
 strony, 369
 infrastruktura, 289
 infrastruktura klucza
 publicznego, 229
 inspekcja
 logów IIS, 373
 pakietów sieciowych, 371
 instalacja
 SQL Server, 136, 138
 TDE, 232
 instrukcja DBCC CheckDB, 311
 interesariusze, 74
 interfejs
 programowania aplikacji,
 API, 28
 wiersza poleceń, CLI, 53
 IOPS, 150

J

jednostka LUN, 141

K

karty sieciowe, 303, 314
 Kerberos, 180
 klastry pracy awaryjnej, 132,
 346, 348
 klasy dostępności, 335
 klucz
 DEK, 231, 232
 MIISKMU, 264
 SMK, 231

kodowanie oświadczeń, 196, 197
 kody wyników, 381
 komandlet, 51, 65
 Backup-SPSite, 339
 Connect-SPOService, 58
 Export-SPWeb, 340
 Get-Help -Examples, 64
 Get-SPClaimTypeEncoding, 198
 Import-SPWeb, 341
 Mount-SPContentDatabase, 185
 New-PSSession, 56
 New-SPTTrustedSecurity
 ➔TokenIssuer, 196
 New-SPUsageApplication, 298
 PowerShell, 65
 Restore-SPSite, 339
 Set-ExecutionPolicy, 57
 Set-SPFarmConfig, 219
 Set-SPUsageApplication, 298
 Set-SPUsageService, 299
 Start-SPAssignment -Global,
 68
 Stop-SPAssignment -Global,
 68
 kompaktowanie plików danych,
 313
 komponenty
 analitiky biznesowej, 152
 farmy, 21
 serwerowe, 345
 kompresja plików, 143
 komunikacja, 221
 serwer-serwer, 224
 konfigurowanie
 aliasów klienta, 138, 140
 buforowania, 315
 dodatku LPS, 375
 menedżera żądań, 324
 opcji MDOP, 137
 programu Fiddler, 370
 programu PowerPivot, 158
 protokołu Kerberos, 180
 przeglądarki ULS Viewer, 367
 serwera, 181
 systemu SQL Server, 134

systemu Visual Studio
 Ultimate, 387
 systemu Visual Studio
 Ultimate 2010, 408
 uprawnień użytkowników, 56
 usługi topologii, 126
 ustawień dostawcy danych,
 298
 ustawień modelu danych, 156
 zabezpieczeń, 25
 konsola MMC, 226
 konsument usługi, 100
 konta użytkowników, 234, 236
 kontrola wprowadzanych zmian,
 55
 kontrolka wyboru osób, 208
 konwersja
 aplikacji trybu klasycznego, 185
 Worda, 46
 kopia zapasowa zbioru witryn, 338
 kopie zapasowe, 336
 kreator Test Mix Model, 394
 kworum, 347

L

liczniki wydajności, 302
 lista, 32
 błędów, 329
 profilu, 61
 relacji zaufania, 126
 sprzętu, 405
 logi IIS, 373
 LUN, Logical Unit Number, 141

M

mapowania
 AAM, 200
 dostępu alternatywnego, 27
 zestawu liczników, 411
 mechanizm
 federacji usług, 99
 kopii zapasowych, 336
 OAuth, 106
 potoku, 54

równoważenia obciążenia, 358
 TDE, 230
 Windows PowerShell, 52
 menedżer żądań, 323
 metadane, 77
 metadane JSON, 196
 metoda Dispose(), 68
 metody uwierzytelniania, 199
 metryki sukcesu, 73
 Microsoft
 Log Parser, 375
 Message Analyzer, 372
 Network Monitor, 372
 SharePoint 2013, 97
 SQL Server Reporting
 Services, 294
 ULS Viewer, 366
 migracja, 276
 minimalizowanie przestoju, 270
 MMS, Managed Metadata
 Service, 113
 model
 aplikacji, 42
 aplikacji usługowych, 99
 OAuth, 212
 moduły programu, 47
 modyfikowanie
 konta, 183
 usługi użytkownika i kondycji,
 299
 monitor wydajności, 308
 monitorowanie
 kondycji programu, 297
 liczników wydajności, 301
 pamięci masowej, 142
 pamięci trwałej, 306
 postępów, 271
 środowiska programu, 292
 wydajności, 142
 wydajności stron, 304
 możliwości odkrywania, 54
 MSODS, 90
 multiemisja, 359

N

nagłówki hosta zbioru witryn, 202
 naprawa klastra pamięci, 317
 narzędzia
 deweloperskie, 371
 IE Dev Tools, 371, 378
 Windows PowerShell, 55
 narzędzie
 Microsoft TechNet Script Center, 67
 Klist, 371
 LPS, 376
 NETBIOS, 196
 NLB, Network Load Balancer, 376
 NTLM, 177, 180

O

obiekt
 BLOB, 166, 261
 ServiceConnectionPoint, 218
 SPRequest, 68
 SPSite, 68
 SPTrustedIdentityTokenIssuer, 192
 SPWeb, 68
 obiektowość, 54
 odkrywanie, 11
 odtwarzanie, 336, 338
 danych z niedołączonej bazy danych, 341
 odwzorowanie celów na funkcje, 76
 Office 365 Enterprise, 89
 ograniczanie
 aktualizacji zbiorów witryn, 251
 przestojów, 266
 zasobów, 307
 okno
 Edytowanie powiązań witryny, 223, 242
 Server Properties, 310
 Utwórz certyfikat, 241
 Zarządzanie kontem, 238

określanie
 możliwości farmy, 386
 priorytetów celów, 75
 opcja
 AuthN, 175
 Avg. Page Time, 399
 Avg. Response Time, 399
 MDOP, 135
 opcje
 czasu uruchamiania testów, 398
 HA, 133
 programu ULS Viewer, 368
 środowiska testowego, 384
 testowania obciążenia, 396
 zbioru liczników, 397
 operacje CRUD, 112
 optymalizacja, 307
 SQL, 307
 SQL Server, 134
 OWA, Office Web Apps, 99, 104, 107, 262

P

pakiet
 Office, 94
 OWA, 99
 pakiety językowe, 265
 PAMIĘĆ, 302
 pamięć masowa SQL Server, 150
 pamięć podręczna, 316
 BLOB, 321
 obiektów, 319
 stron wyjściowych, 318
 pamięć zewnętrzna, 131
 pasek stanu, 252
 personalizacje, 259, 283
 piaskownica, 42
 PKI, Public Key Infrastructure, 229
 plan zarządzania, 79
 planowanie
 architektury informacji, 92
 buforowania, 315
 ciągłości działania, 334
 objętości baz danych, 150
 strategii ciągłości działania, 333
 strategii zarządzania, 92
 testów, 377
 wdrożenia, 19
 plik
 global.asax, 37
 Microsoft.SharePoint.
 ↳ PowerShell.dll, 65
 stronicowania, 303
 web.config, 36, 37
 pliki
 dzienników, 142
 serwera IIS, 35
 wewnątrz aplikacji, 36
 WSP, 260
 pływające ramki, 31
 podgląd zdarzeń, 294
 pojedyncze
 logowanie, 86, 87
 powinowactwo, 193
 polecenie
 Add-SPShellAdmin, 56
 Get-Command, 63, 66
 setspn, 182
 porównanie testów obciążenia, 414
 port, 224, 225
 porządkowanie
 baz danych zawartości, 255
 środowiska, 256
 poświadczenie NTLM, 177
 potok CSOM, 90
 powiadomienia, 252
 powiadomienia e-mailem, 252
 PPS, PerformancePoint Service, 114
 problemy
 z uaktualnieniem, 272
 ze środowiskiem, 325
 procedury
 codzienne, 294
 comiesięczne, 296
 wykonywane co tydzień, 296
 proces, 303
 aktualizacji, 253
 W3WP, 184

procesor, 302
 program
 Edytor ADSI, 217
 FBA Configuration Manager, 189
 Fiddler, 370
 Internet Explorer, 371
 PerformancePoint, 46
 Power View, 165
 PowerPivot, 158
 SQLIO, 167
 ULS Log Viewer, 328
 ULS Viewer, 367
 VRTA, 378–380
 Project Server 2013, 46
 projektowanie
 bezpieczeństwa platformy, 215
 protokół, 225
 IKEv2, 229
 IPsec, 228
 Kerberos, 179
 MSSQLSERVER, 227
 OData, 113
 SMTP, 224
 SSL, 25, 221
 przegląd aktualizacji, 254
 przeglądarka ULS Viewer, 367
 przełączniki, 315
 przepływ pracy, 105, 107
 przeznaczenie serwerów, 405
 przydziały, 42
 przygotowanie uaktualnienia, 255
 przyporządkowanie dysków, 141
 przywracanie danych z Kosza, 342
 pula aplikacji, 26, 234
 pulpit nawigacyjny, 368
 punkty zasobów, 42

R

RAID, 142
 raport, 216, 293, 413
 raporty na temat instalacji, 219
 redukcja fragmentacji indeksu, 312

reguły
 analizatora, 311, 312
 kwerend wyszukiwania, 31
 rejestrowanie, 253
 relacja zaufania, 126
 serwer-serwer, 87
 dwukierunkowa, 88
 jednokierunkowa, 86
 pomiędzy farmami, 125
 rezerwa
 aktywna, 350
 dynamiczna, 350
 rezultaty, 76
 RM, Request Management, 48
 role, 239
 routery, 315
 rozmiar bazy danych zawartości, 151
 rozpoznawanie problemów, 326
 rozszerzalność programu, 41
 rozwiązania
 na poziomie farmy, 41
 w formie piaskownicy, 42
 równoważenie obciążenia, 358
 RPO, 334
 RPS, Requests Per Second, 385
 RTO, 334

S

S2S, 195
 samoobsługowe tworzenie
 witryn, 29, 200
 scenariusze
 użycia, 76
 użytkowników, 410
 schemat wyszukiwania, 30
 serwer
 APP, 161
 Contoso.com, 194
 IIS, 23, 35, 175
 PowerPivot, 157
 proxy aplikacji usługowej, 100
 WAWS, 105, 106
 serwery wirtualne, 315

SharePoint Developer
 Dashboard, 294
 SharePoint Online, 85
 sieciowy mechanizm
 równoważenia obciążenia, 358
 sieć wysokiej dostępności, 362
 silnik bazy danych, 132
 składnia Windows PowerShell, 53
 składowe aplikacje usługowych, 101
 skorowidz komandletów, 67
 skrypty, 54
 skuteczne planowanie, 73
 SMTP, Simple Mail Transfer Protocol, 224
 sortowanie, 134, 136
 SPFWA, 322
 SPN, Service Principal Names, 25, 180, 184
 spójność, 54
 sprawdzanie
 baz danych, 311
 kondycji zbioru witryn, 249
 poprawności testowego uaktualnienia, 269
 SQL Client Configuration Utility, 139
 SQL Server, 134, 136
 aliasy klienta, 138
 AlwaysOn, 134
 funkcje analityki biznesowej, 152
 instalacja, 136
 klastry pracy awaryjnej, 133
 konfiguracja, 134
 konfigurowanie aliasów klienta, 140
 monitorowanie pamięci masowej, 142
 monitorowanie wydajności, 142
 opcja MDOP, 135
 opcje HA, 133
 optymalizacja, 134
 SSL, 226
 testowanie dysków, 167, 172
 tworzenie statystyk, 138

SQL Server Transparent Data Encryption, 230

SSL, Secure Sockets Layer, 23, 89, 226

SSO, Single Sign-On, 118

SSP, SharePoint Service Providers, 99

SSSC, Self-Service Site Creation, 200

standardy testów obciążenia, 385

statystyki, 138

stosowanie

- celów BCM, 334
- najmniejszych uprawnień, 233
- Windows PowerShell, 53

strategia

- wdrożenia, 91
- zarządzania, 92

strefy uwierzytelniania, 199

struktura witryny, 78

STS, Security Token Service, 100, 122

synchronizacja

- danych, 357
- katalogów, 86–88

System Center 2012 Operations Manager, 294

system plików, 35

szczytowy procent jednoczesnych użytkowników, 385

szyfrowanie komunikacji, 219

Ś

ścieżki profili, 61

śledzenie instalacji, 217

środowisko

- interaktywne i skryptowe, 54
- ISE, 60
- testowe, 275

T

taksonomia, 77

TDE, Transparent Data Encryption, 230

technologia HADRON, 355, 363

testowanie

- dysków, 167
- dysków sieciowych iSCSI, 170
- dysków SQL Server, 172
- negatywne, 400
- obciążenia, 391, 395, 403, 409
- obciążenia dysków, 172
- obciążenia środowiska, 383
- strategii migracji, 276
- środowiska, 373
- uaktualnienia, 268
- warunków skrajnych, 400
- wydajności, 389, 408
- wydajności sieci Web, 389
- wydajności środowiska, 377

tłumaczenie maszynowe, 109

token, 190

topologia serwerów, 211

tryb

- asynchroniczny, 350
- klasyczny, 184
- oświadczeń, 184, 185
- synchroniczny, 350
- tylko do odczytu, 266
- wysokiego bezpieczeństwa, 351
- wysokiej dostępności, 351
- wysokiej wydajności, 351

tworzenie

- aplikacji usług, 283
- certyfikatu, 241
- nowej aplikacji, 222
- obiektów
 - ServiceConnectionPoint, 218
- planów konserwacji, 313
- planu testów, 377
- powiązań IIS, 223
- raportów, 216, 219, 413
- relacji zaufania, 125
- testu obciążenia, 391, 409
- testu warunków skrajnych, 401
- testu wydajności, 389, 408

typy

- wyników, 30
- zawartości, 78

U

uaktualnianie

- witryn, 286
- aplikacji usługi wyszukiwania, 276
- farmy produkcyjnej, 270
- farmy testowej, 268
- usług, 254
- zawartości witryn, 284

udostępnianie, 209

układ

- farmy, 273, 274
- serwerów farmy, 275

ULS, Unified Logging Service, 253

ULS, Unified Logging System, 365

unikanie zakłóceń dostępności usług, 344

UPA, User Profile Application, 195

UPA, User Profile Service Application, 118

UPN, User Principal Name, 195

uprawnienia, 56

- dla certyfikatu, 228
- grup, 240

UPS, User Profile Service, 262

uruchamianie skryptu, 164

urzędy certyfikacji, CA, 220

usługa, 100

- Access 2010, 111
- ACS, 194, 196
- Active Directory, 217, 365
- AD DS, 89, 187
- AD FS, 89
- automatyzacji Worda, 120
- BCS Runtime, 90
- BDC, 112
- bezpiecznego magazynu, 90, 118, 203
- c2WTS, 202
- FIM, 118
- formularzy InfoPath, 261
- IP-STS, 191, 192
- łączności biznesowej, 24

OData, 90
 profili użytkowników, 45, 262
 RM, 49
 rozproszonej pamięci
 podręcznej, 316
 Secure Token, 122
 SSS, 118
 tłumaczenia maszynowego, 109
 topologii, 126
 uwierzytelniania, 202
 użytkowania i kondycji, 299
 VGS, 119
 Windows Azure Access
 Control, 90
 wyszukiwania, 45, 115, 276, 279
 zarządzania aplikacjami, 109
 zarządzanych metadanych, 46
 usługi
 Access 2013, 149
 Excel Services, 156
 Excela, 113, 262
 łączności biznesowej, 86, 204
 SQL Server Reporting
 Services, 162
 usprawnienia
 w trybie tylko do odczytu, 343
 Windows PowerShell, 55
 ustalenie standardów testów
 obciążenia, 385
 ustawianie poziomu zgodności, 277
 ustawienia wyszukiwania, 30
 utrzymanie bazy danych, 311
 uwierzytelnianie, 175, 314
 anonimowe, 186
 aplikacji, 193
 bazujące na oświadczeniach,
 187
 bazujące na tokenach, 190
 Kerberos, 25
 Negocjowane, 179, 183
 NTLM, 25, 178
 OAuth, 193
 oparte na formularzach, 189
 podstawowe, 25, 176
 przekazywane, 204

S2S, 123, 195
 SAML, 190, 191
 Szyfrowane, 177
 typu Zaufany dostawca
 tożsamości, 25
 w trybie klasycznym, 265
 Windows, 176

V

VGS, Visio Graphics Service, 119
 Visual Studio Team System 2008
 Team Suite, 403
 Visual Studio Ultimate 2010,
 403, 408
 Visual Studio Ultimate 2012, 387

W

walidacja
 architektury, 365
 ustawień, 159
 WAS, Word Automation Service,
 120
 WAWS, Windows Azure
 Workflow Server, 105
 wbudowane polecenia, 52
 wdrożenie, 19
 wdrożenie programu, 91
 weryfikacja
 aktualizacji, 272
 alokacji portów, 370
 działania farmy, 366
 działania protokołu Kerberos,
 371
 protokołu Kerberos, 407
 witryn, 406
 wielofirmowość, 30
 większość węzłów, 347
 i dysków, 347
 i udziałów plikowych, 347
 Windows Management
 Instrumentation, 294
 Windows PowerShell, 51
 dodatek Commands, 62
 historia, 52
 komandlety, 61, 65
 konfigurowanie uprawnień, 56
 korzyści, 53
 powłoka zarządzania, 58
 profile, 60
 składnia, 53
 usprawnienia, 55
 Windows PowerShell ISE, 60
 Windows Server 2008 R2, 59
 Windows Server 2012, 60
 witryny, 32
 WMS, Work Management
 Service, 110
 wnioski z instalacji, 269
 współdzielenie, 11
 wydajność
 podsystemu dyskowego, 172
 środowiska, 377
 wykaz serwera raportów, 149
 wykres żądania i ładowania
 strony, 381
 wymagania
 analizy biznesowej, 94
 architektury hybrydowej, 89
 bezpieczeństwa, 93
 dotyczące niezawodności, 95
 dotyczące wydajności, 95
 funkcjonalne, 77
 niefunkcjonalne, 77
 programowe, 84
 silnika bazy danych, 132
 sprzętowe, 84
 systemowe, 84
 wyniki testu obciążenia, 412
 wysyłanie dziennika, 132, 133, 352
 wyszukiwanie, 115, 279, 288
 federacyjne, 86, 87
 komandletów, 66

Z

zabezpieczenia, 33
 zadania czasomierza, 293
 zakłócenia dostępności usług, 344
 zalanie przełącznika, 359

- zapewnianie ciągłości działania, 346
 - zarządzane konta, 238
 - zarządzanie, 12
 - aplikacjami, 109
 - danymi, 142
 - personalizacjami, 259
 - pracą WMS, 110
 - samoobsługowym tworzeniem witryn, 201
 - Windows PowerShell, 58
 - żądaniem, 322
 - zasada
 - wykonywania, 57
 - zabezpieczeń IKEv2, 229
 - zasady
 - aplikacji, 205
 - uprawnień, 206, 207
 - zaufany dostawca tożsamości, 25
 - zbieranie
 - danych dotyczących użycia i kondycji, 300
 - wymagań, 71
 - zbiór witryn, 27
 - bazujący na nagłówkach hosta, 24
 - bazujący na ścieżkach, 24
 - zdalny magazyn obiektów BLOB, 261
 - zestaw liczników, 411
 - zielona strefa, 385
 - zmiana
 - konfiguracji przydziału pamięci, 317
 - portu, 242
 - poziomu zgodności, 280
- Ż**
- źródła wyników wyszukiwania, 31
- Ż**
- żądanie certyfikatu, 221, 226

PROGRAM PARTNERSKI

GRUPY WYDAWNICZEJ HELION



1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ

Zmień swoją stronę WWW
w działający bankomat!

Dowiedz się więcej i dołącz już dzisiaj!

<http://program-partnerski.helion.pl>

GRUPA WYDAWNICZA



Helion SA

Zapanuj nad chaosem informacyjnym!

SharePoint to platforma pozwalająca zapanować nad ogromem informacji przetwarzanych w firmach i korporacjach. Rozwijana od lat przez firmę Microsoft, zdobyła ogromną popularność i jest wykorzystywana w najbardziej wymagających warunkach. Jej poprawne wdrożenie pozwala uzyskać błyskawiczny i atrakcyjny wizualnie dostęp do danych. Jeżeli chcesz w pełni wykorzystać potencjał platformy SharePoint 2013, to masz przed sobą idealną książkę!

Dzięki tej lekturze poznasz dostępne komponenty i architekturę SharePointa oraz zaplanujesz wdrożenie Twojej instalacji. Na kolejnych stronach książki znajdziesz informacje na temat zbierania wymagań od użytkowników oraz ich opracowania. Potem przejdziesz do zapoznania się z dostępnymi bazami danych oraz funkcjami, jakie pełnią one w strukturze platformy SharePoint, a także ze sposobami autoryzacji i z technikami aktualizacji. Ponieważ platforma SharePoint ma kluczowe znaczenie dla funkcjonowania przedsiębiorstwa, należy zagwarantować jej wysoką dostępność. Jak to zrobić? Jak przygotować infrastrukturę? Odpowiedź na te pytania również znajdziesz w książce! Jest ona obowiązkową lekturą dla każdej osoby stojącej przed wyzwaniem, jakim jest skuteczne wdrożenie Microsoft SharePoint 2013 w przedsiębiorstwie!

Dzięki tej książce:

- poznasz możliwości platformy SharePoint
- zbierzesz od użytkowników wymagania związane z platformą
- zaznajomisz się z dostępnymi elementami platformy oraz ich rolą
- wybierzesz odpowiedni sposób autoryzacji
- zbudujesz niezawodną platformę do współdzielenia informacji

Helion

34786 numer katalogowy

księgarnia internetowa

<http://helion.pl>

zamówienia telefoniczne



0 801 339900



0 601 339900

Sprawdź najnowsze promocje:
• <http://helion.pl/promocje>
Książki najchętniej czytane:
• <http://helion.pl/bestsellery>
Zamów informacje o nowościach:
• <http://helion.pl/nowosci>

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel.: 32 230 98 63
e-mail: helion@helion.pl
<http://helion.pl>

ISBN 978-83-283-0618-9



9 788328 306189

Informatyka w najlepszym wydaniu

cena: 79,00 zł

Shannon Bray — wierzy w potęgę platformy SharePoint i stara się przekonać do niej inne osoby. Jest związany z tą platformą od 2006 roku. Posiada certyfikaty: MCM, MCT, MCS, MCSE, MCDBA, MCITP, MCPD, MCSM. Wielokrotnie był prelegentem na konferencjach Microsoft. Jest głównym architektem w firmie Planet Technologies.

Miguel Wood — jest dyrektorem w firmie Planet Technologies, a wcześniej był prezesem i dyrektorem generalnym TekFocus — dostawcy specjalistycznych szkoleń związanych z produktami Microsoftu. Może pochwalić się certyfikatami: MCM, MCT, MCITP, MCPD, MCSE, MCS, MCDBA, MCSM. Ma ogromne doświadczenie specjalistyczne i biznesowe, doceniane przez klientów różnej wielkości. Jest weteranem oddziałów desantowych armii USA.

Patrick Curran — jest dyrektorem Federal Group w firmie Planet Technologies. Aktywnie używa platformy SharePoint od 2003 roku. W obszarze jego zainteresowań znajdują się: tworzenie aplikacji, administrowanie oraz rozwiązywanie problemów i migracja danych. Współpracuje z klientami z całego świata. Posiada certyfikaty: MCT, MCTS, MCP, MCITP, MCPD, MCSA.



sięgnij po WIĘCEJ



KOD KORZYŚCI