Microsoft SharePoint 2013 PL

Architektura i skuteczne rozwiązania

Shannon Bray
Miguel Wood
Patrick Curran

Helion

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.

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.

Spis treści

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`.

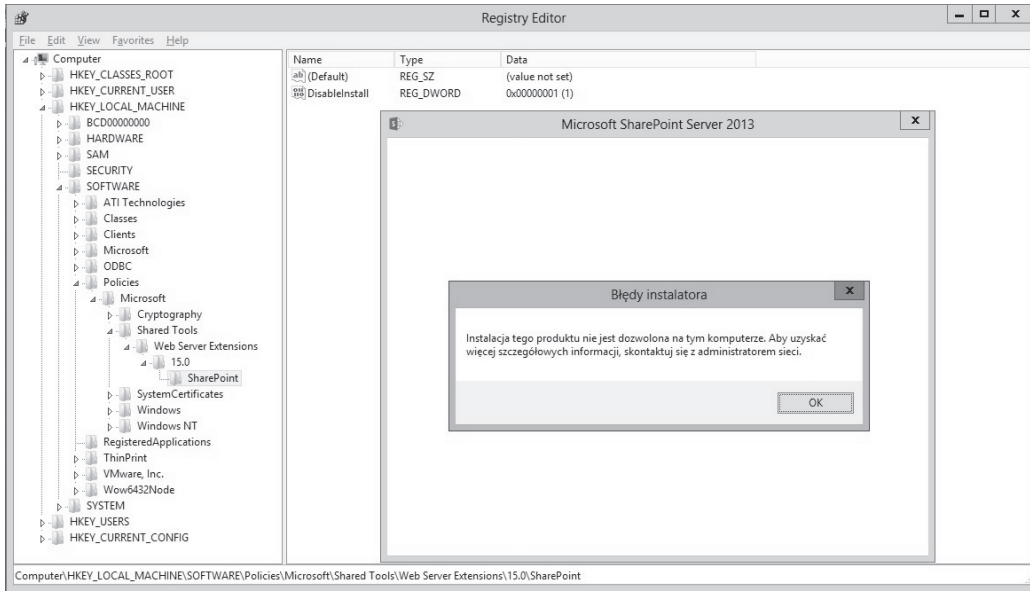
By dodać wartość rejestru do zasady grupy na serwerze z usługą Active Directory, można skorzystać ze skryptu Windows PowerShell (listing 7.1).

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*

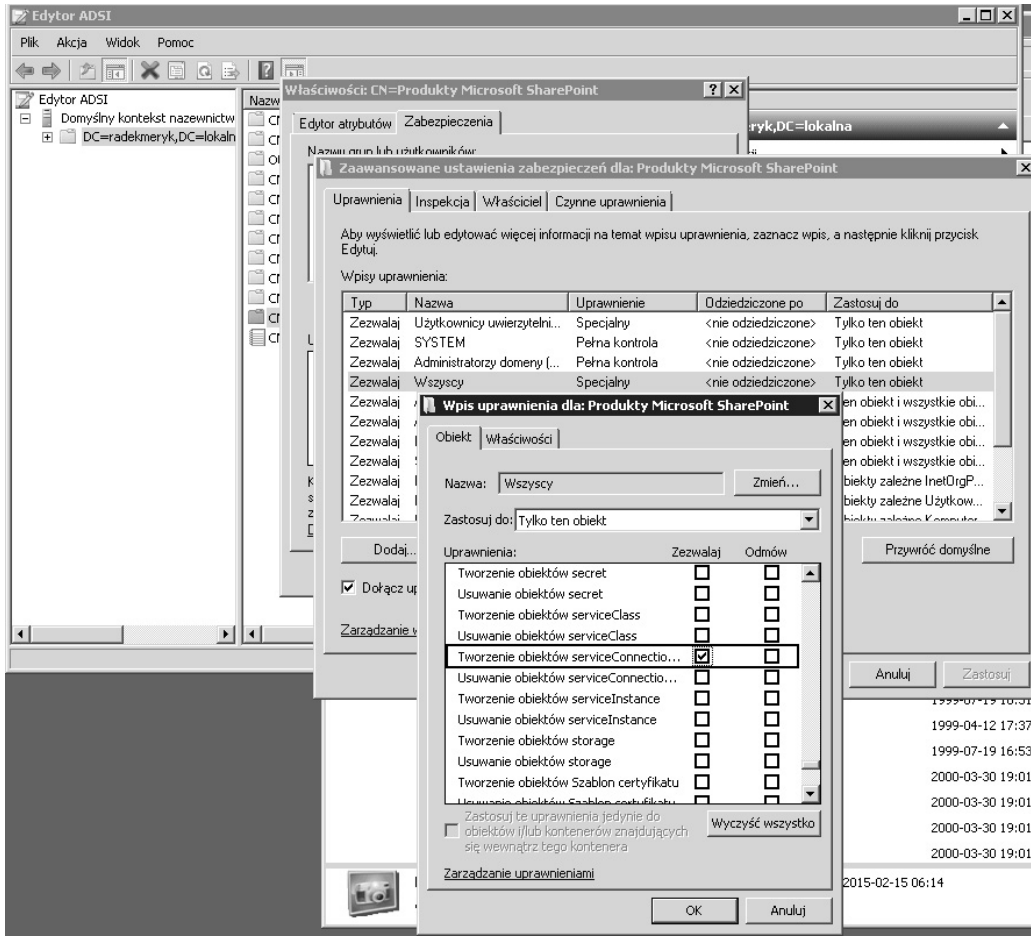
Śledzenie instalacji programu SharePoint

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 instalacje 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 instalacje.
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*.



RYSUNEK 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 komandletu `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*

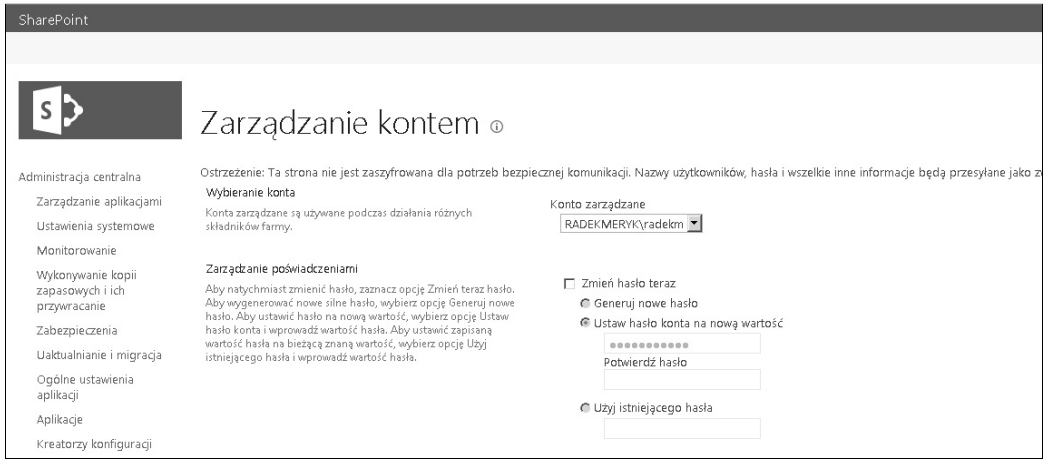
```
$containerPath = 'LDAP://CN=Microsoft SharePoint Products,CN=System,DC=contoso,D
                 C=local'
$entry = New-Object DirectoryServices.DirectoryEntry $containerPath
$searcher = New-Object DirectoryServices.DirectorySearcher
$searcher.SearchRoot = $entry
$searcher.Filter = "(objectClass=serviceConnectionPoint)"
$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 przesyłane w formacie 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.



RYSUNEK 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.

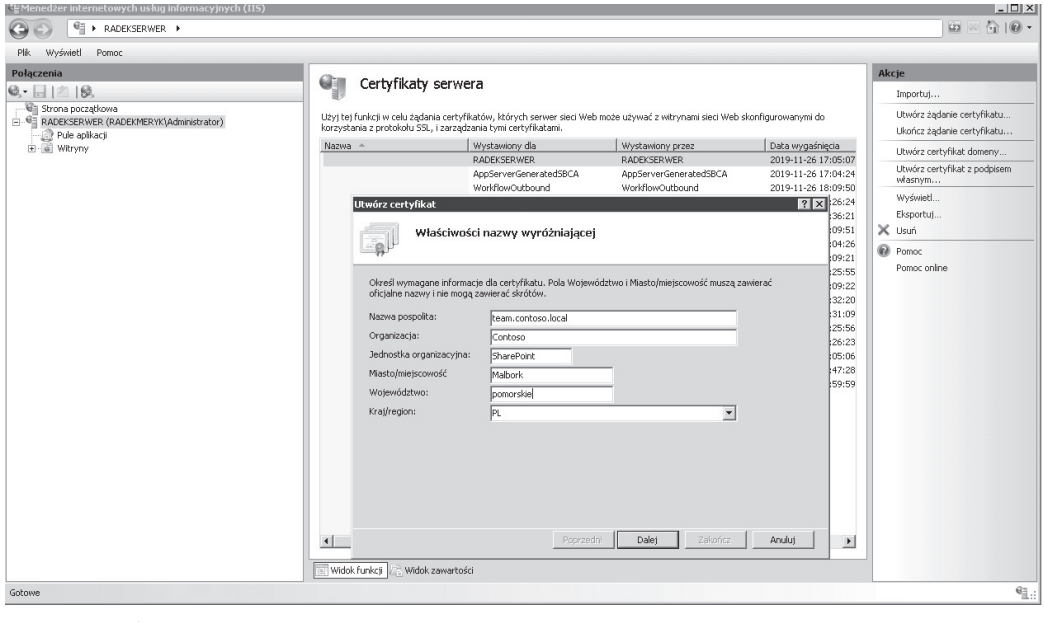
Istnieje kilka rodzajów certyfikatów, o których warto wspomnieć w tym miejscu: standardowe certyfikaty SSL oraz certyfikaty SSL w formie symboli wieloznacznych. Standardowe certyfikaty SSL są ważne dla określonej nazwy domeny lub poddomeny i są bardzo specyficzne. Certyfikaty SSL w formie symboli wieloznacznych 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.

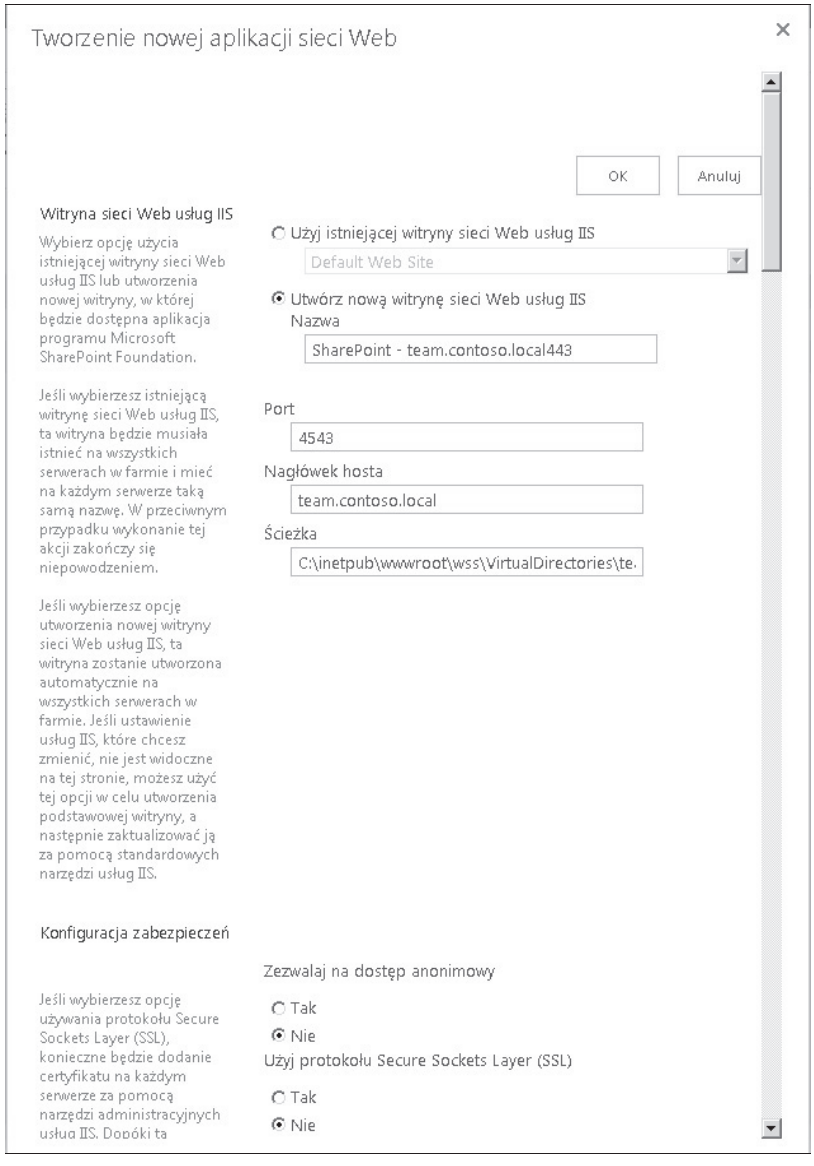
Uruchom *Menedżer internetowych usług informacyjnych*, kliknij węzeł serwera w okienku po lewej stronie, a następnie w środkowym okienku dwukrotnie kliknij *Certyfikaty serwera*. W środkowym okienku wyświetlą się wszystkie certyfikaty, w okienku po prawej stronie natomiast pojawią się nowe akcje. W tym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



RYSUNEK 7.4. *Żądanie certyfikatu z UC Domeny*

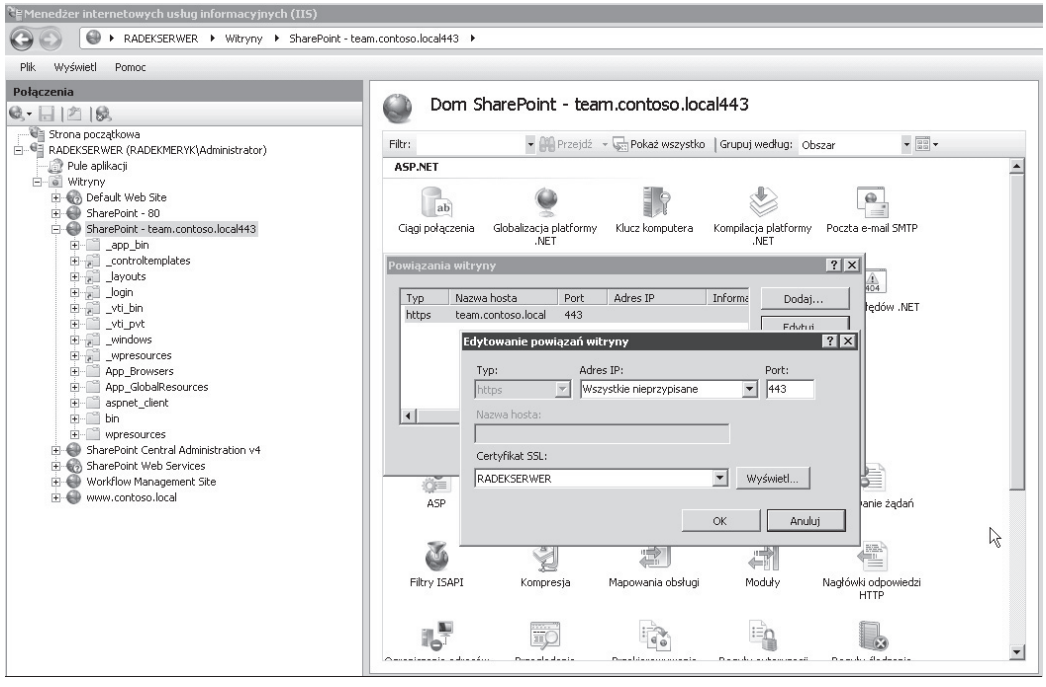
Jeśli proces pozyskiwania certyfikatu zakończy się pomyślnie, będziemy dysponować certyfikatem, którego będzie można użyć w aplikacjach sieci Web programu SharePoint. Niezależnie od tego, czy tworzymy nową aplikację sieci Web programu SharePoint, czy dokonujemy konwersji istniejącej, ogólne czynności 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.



RYSUNEK 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

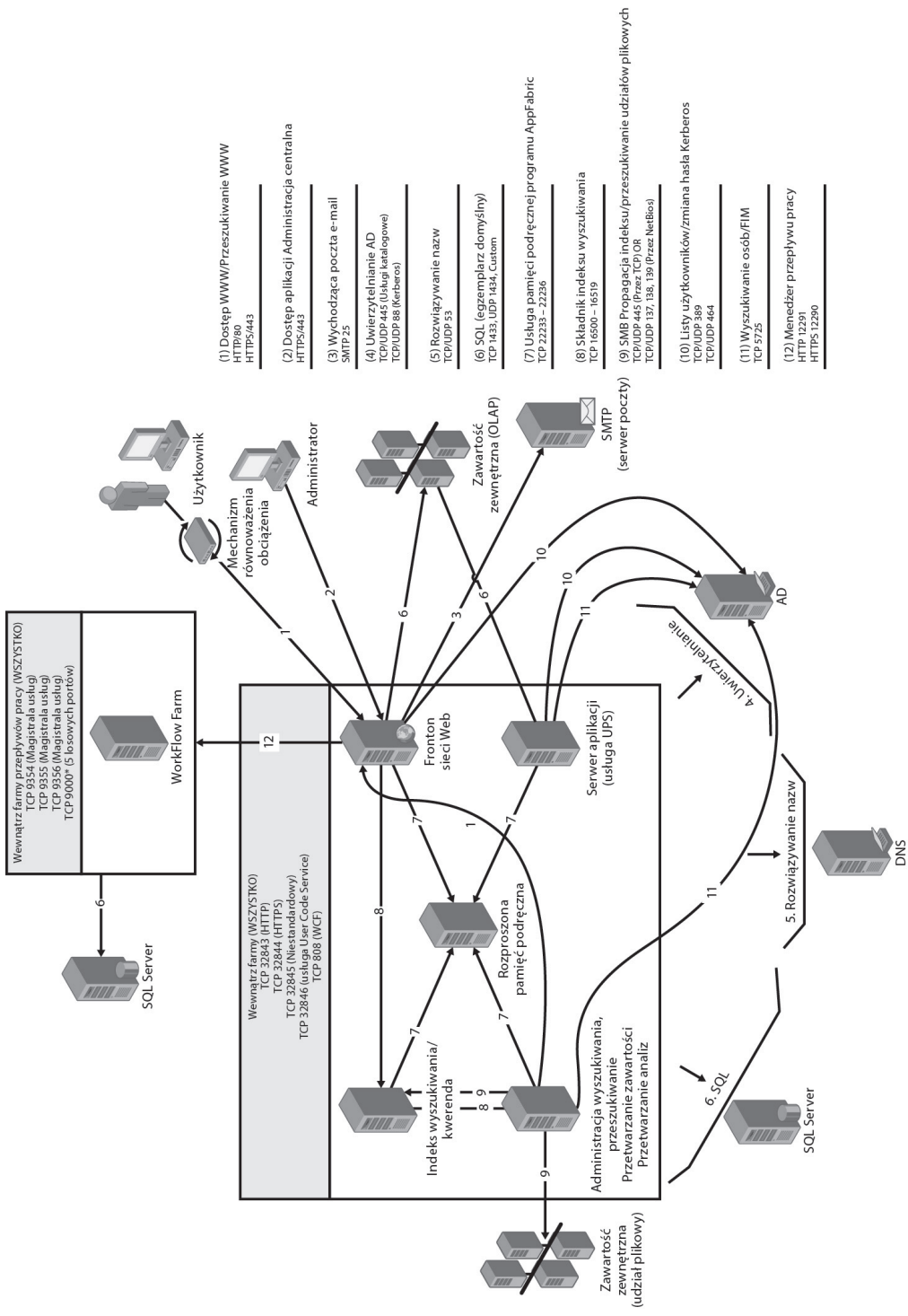
Po omówieniu szyfrowania danych pomiędzy klientami a serwerem SharePoint przetwarzającym żądania witryn sieci Web nadszedł czas, by skupić się na komunikacji między serwerami z systemem SharePoint oraz serwerami z systemem SQL Server. Do zabezpieczenia komunikacji pomiędzy serwerami poprzez zaszyfrowanie 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.

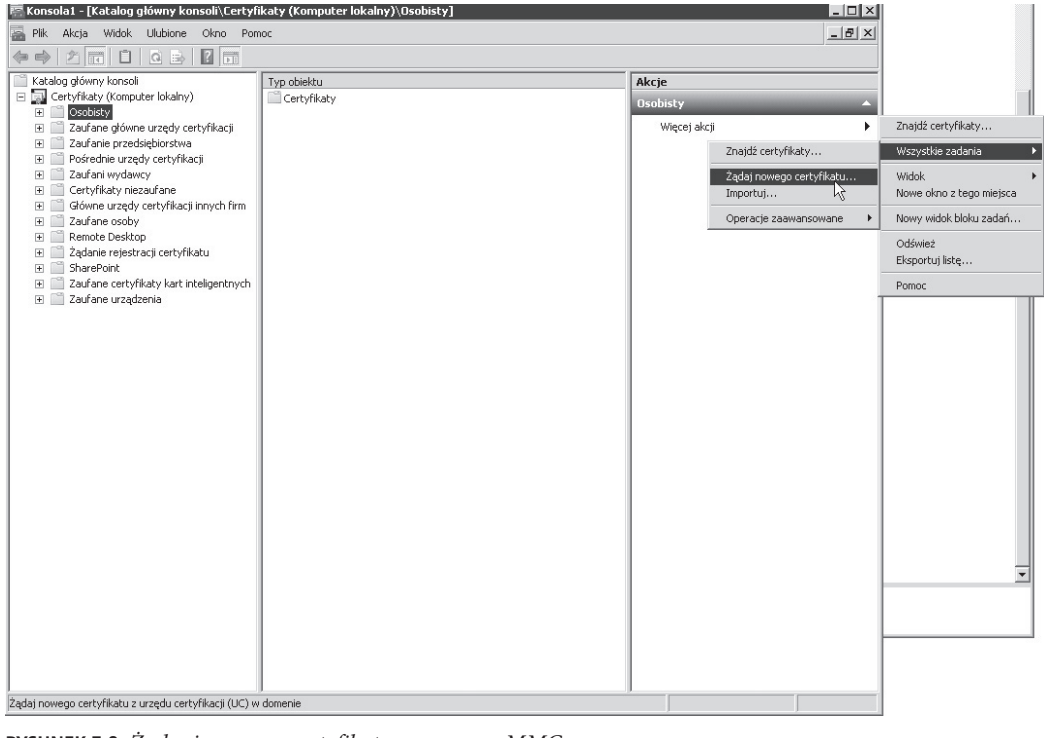
Kiedy cały ruch jest zaszyfrowany za pomocą SSL, zachodzi konieczność wykorzystania następujących dodatkowych procesów:

- 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".

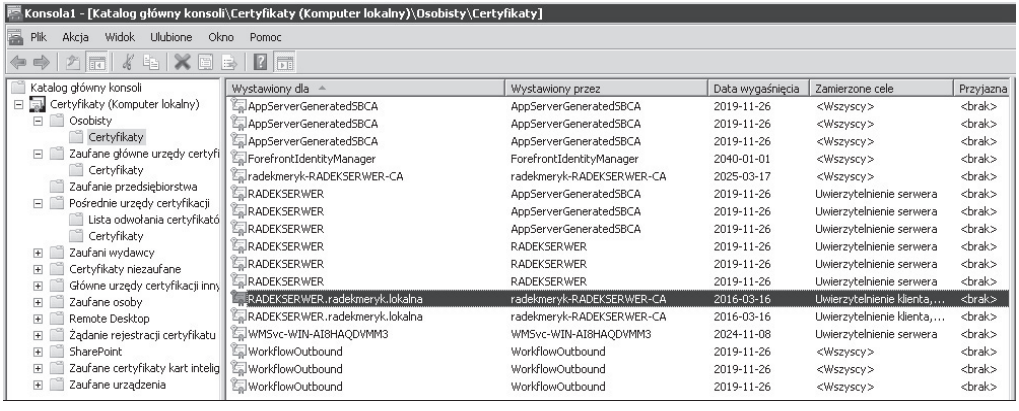
Aby skonfigurować egzemplarz programu SQL Server do korzystania z protokołu SSL, uruchom program *SQL Server Configuration Manager*. By to zrobić, otwórz konsolę MMC (ang. *Microsoft Management Console*), wpisując *MMC* w oknie dialogowym *Uruchom*. W menu *Plik* kliknij *Dodaj/usuń przystawkę*. Kliknij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



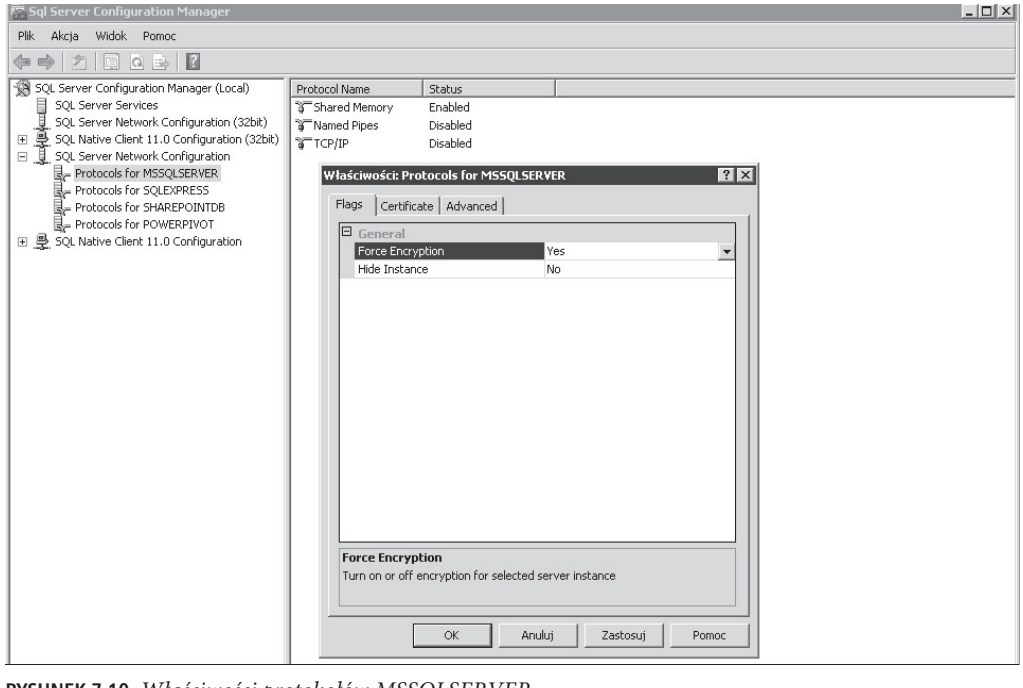
RYSUNEK 7.8. *Żądanie nowego certyfikatu za pomocą MMC*

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).



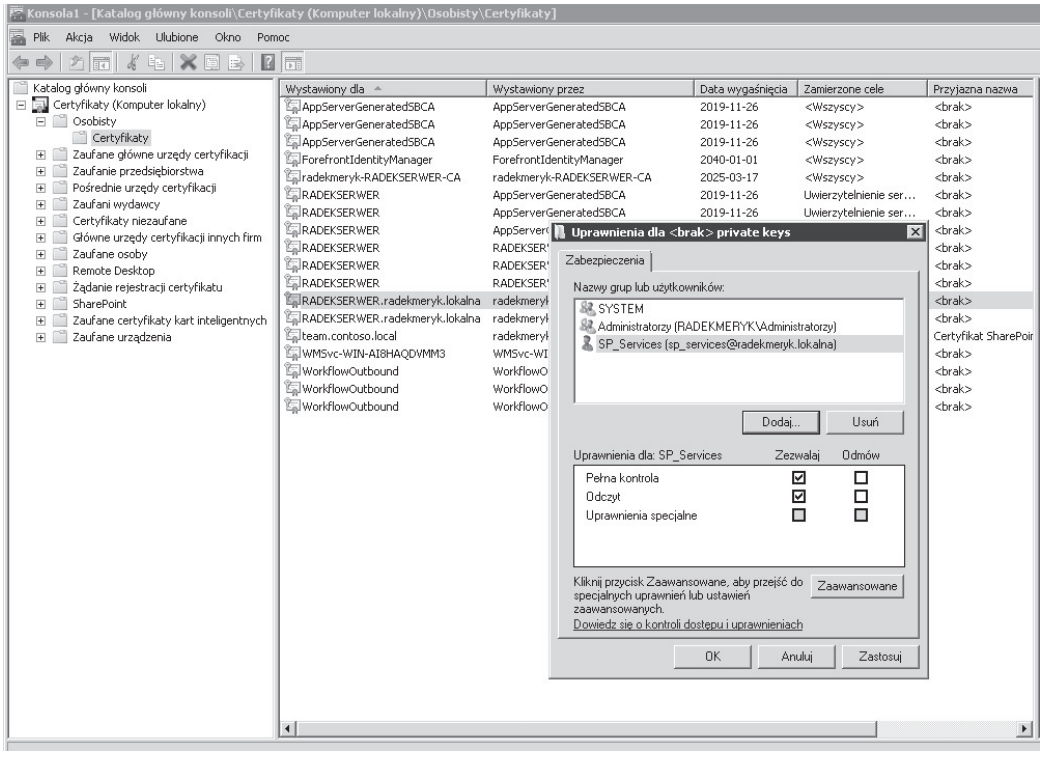
RYSUNEK 7.9. *Przeglądanie certyfikatów osobistych*

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.



RYSUNEK 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.



RYSUNEK 7.11. *Uprawnienia dla certyfikatu*

Następnie należy zrestartować usługę SQL Server. W przypadku niepowodzenia nadania kontu 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 egzemplarzy 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 wznawiania 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.

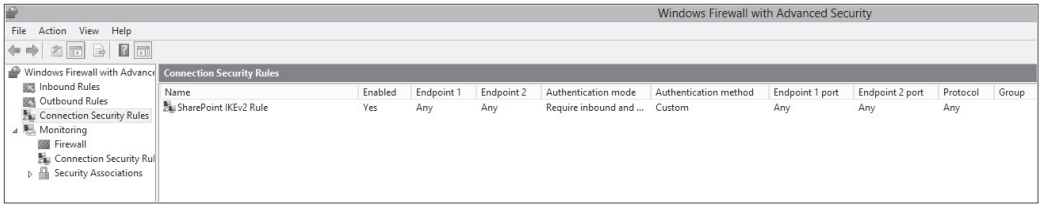
LISTING 7.5. *Zasada zabezpieczeń IKEv2*

```
# 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 $certprop –PolicyStore GPO:$gponame

# Utworzenie reguły zabezpieczenia połączenia IKEv2
New-NetIPsecRule -DisplayName "Reguła IKEv2 SharePoint" `
-RemoteAddress any -Phase1AuthSet $myauth.InstanceID `
-InboundSecurity Require -OutboundSecurity Request `
-KeyModule IKEv2 -PolicyStore GPO:$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.



RYSUNEK 7.12. *Reguły zabezpieczeń połączeń*

Planowanie i konfigurowanie funkcji Microsoft SQL Server Transparent Data Encryption

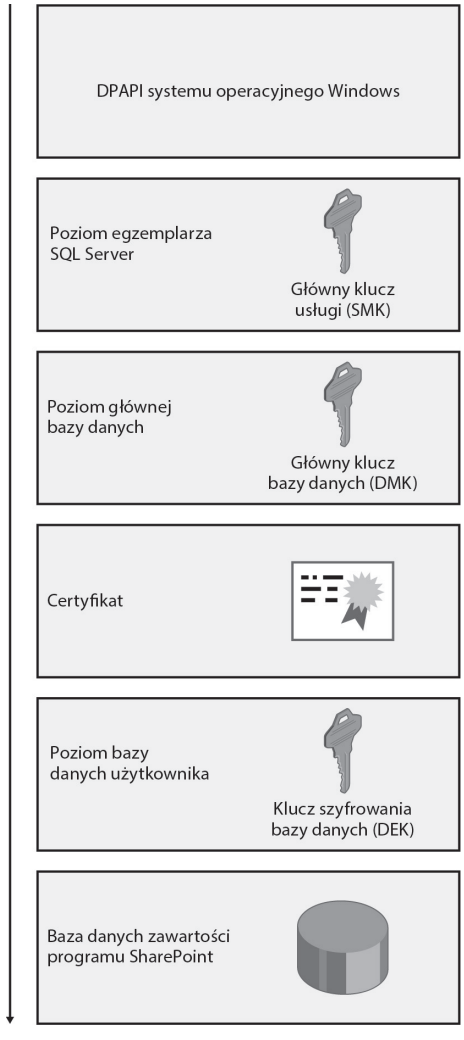
Do tej pory nauczyłeś się sposobów szyfrowania ruchu sieciowego pomiędzy serwerami w farmie oraz pomiędzy klientami korzystającymi z serwerów. Choć mechanizmy te oferują wysoki poziom bezpieczeństwa, dane przechowywane w farmie nadal mogą być wykorzystane w sposób nieodpowiedni lub mogą być skradzione 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.



RYSUNEK 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*

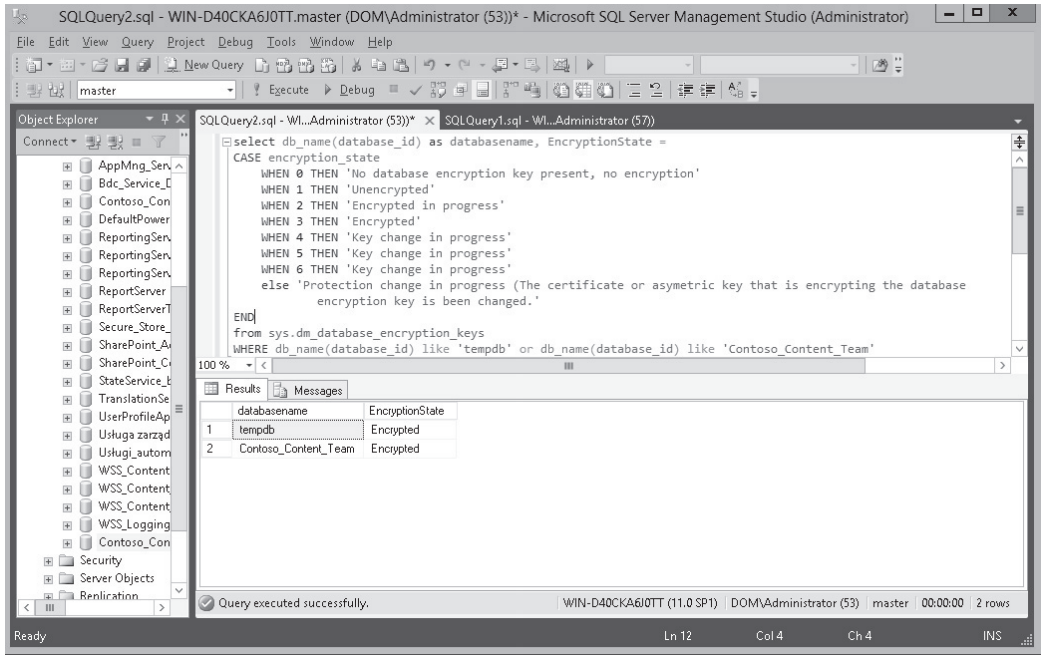
```
USE master;
GO
-- Utworzenie DMK
CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'Passw0rd1';
GO
-- Utworzenie certyfikatu DEK
CREATE CERTIFICATE TDECert WITH SUBJECT = 'Certyfikat TDE SQL Server'
GO
-- Utworzenie kopii zapasowej certyfikatu TDE
BACKUP CERTIFICATE TDECert TO FILE = 'c:\SQLTDECert.bak'
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 asymetric 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
SharePoint Web Services Default	`spServices`	Host aplikacji usług programu SharePoint.
SharePoint Web Content Default	`spContent`	Host aplikacji zawartości programu SharePoint.
SharePoint Central Administration v4	`spFarm`	Host aplikacji sieci Web *Administracja centralna*.
SecurityTokenServiceApplicationPool	`spFarm`	Host usługi STS.
SharePoint Secure Store	`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 *SharePoint Product Configuration Wizard*.	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 *Administracja centralna*, ■ 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 `SharePoint_Shell_Access`. 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: `spDataAccess`.
`spServices`	Spełnia rolę tożsamości puli aplikacji dla aplikacji usług programu SharePoint.	Automatycznie nadaje potrzebne uprawnienia do baz danych zawartości: `spDataAccess`.
`spC2WTs`	Tożsamość, z jaką działa usługa c2WTS.	Prawa lokalnego administratora serwera, na którym działa usługa c2WTS, oraz lokalne zasady zabezpieczeń dla: *Działanie jako część systemu operacyjnego*, *Personifikuj klienta po uwierzytelnieniu*, *Logowanie w trybie usługi*.

TABELA 7.2. *Zalecane konta użytkowników według ról — ciąg dalszy*

Konto	Przeznaczenie	Wymagania
`spUPS`	Tożsamość wykorzystywana podczas procesu synchronizacji profili użytkowników.	Uprawnienia Active Directory: *Replication Directory Changes*.
`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: `spDataAccess`.
`spSuperUser`	Konto używane do buforowania.	Konto ma pełny dostęp do aplikacji sieci Web *Publikowanie*.
`spSuperReader`	Konto używane do buforowania.	Konto ma dostęp *Pełny odczyt* do aplikacji sieci Web *Publikowanie*.
`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:

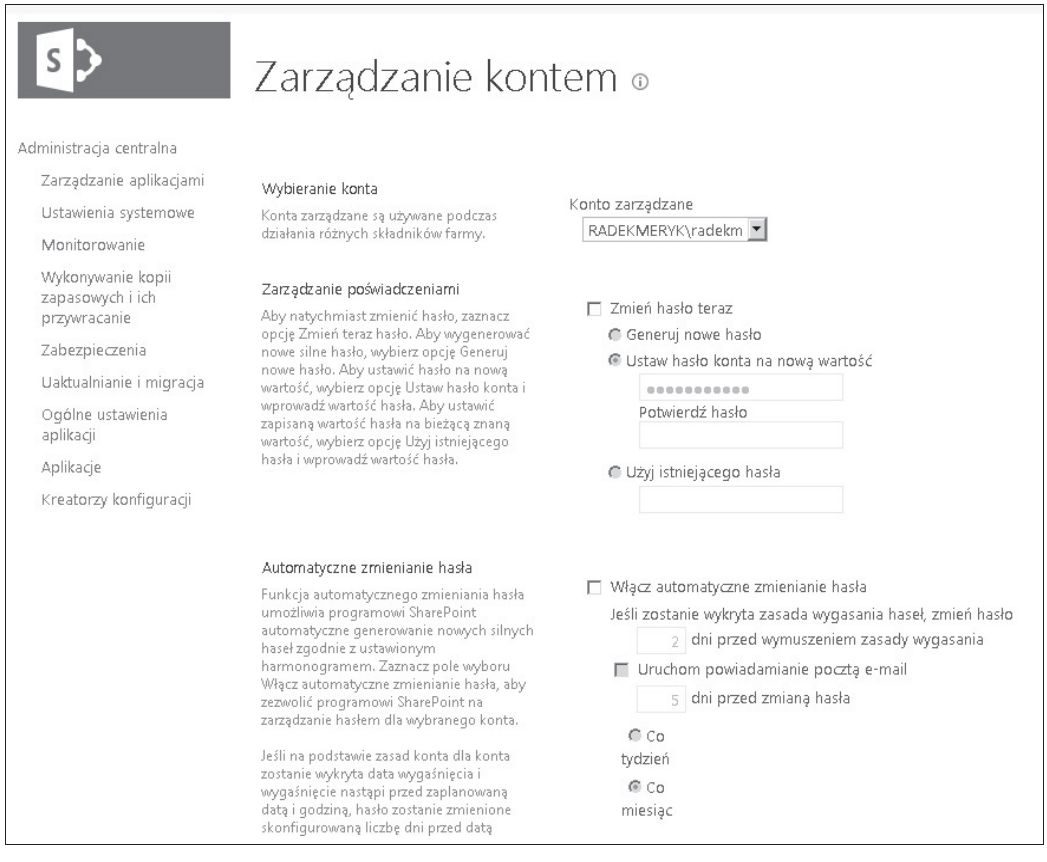
- Domyślne konto dostępu do zawartości musi być kontem użytkownika domeny posiadającym dostęp odczytu do zewnętrznych lub bezpiecznych źródeł zawartości, które mają być przeszukane przy użyciu tego konta.
- W przypadku witryn serwera SharePoint, które nie należą do farmy serwerów, trzeba jawnie przydzielić 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 zapamiętać, 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 zapamiętać, że jest to jeszcze jeden obszar w obrębie produktu, w którym poświadczenia są przesyłane jako zwykły tekst, dlatego należy zadbać o to, by aplikacja *Administracja centralna* działała za pomocą protokołu SSL.



RYSUNEK 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 ciąg 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`.

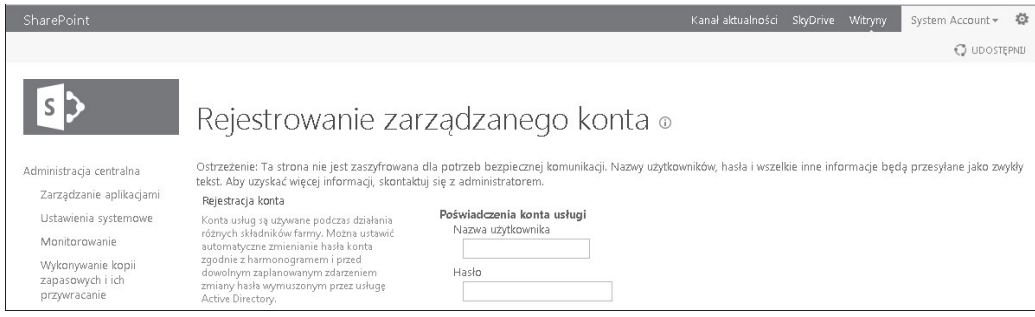
Grupa `WSS_ADMIN_WPG` ma uprawnienia odczytu i zapisu do lokalnych zasobów. Do tej roli należą konta puli aplikacji *Administracja centralna* oraz usługi czasomierza (`spFarm`). Grupa ma uprawnienia pełnej kontroli w stosunku do katalogów o kluczowym znaczeniu dla programu SharePoint, w tym do wszystkich 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.



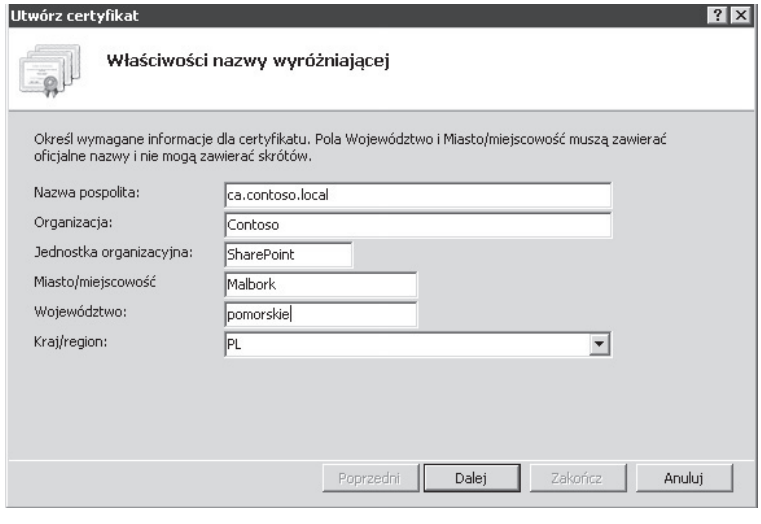
RYSUNEK 7.16. *Komunikat ostrzeżenia o przesyłaniu haseł jako zwykłego tekstu*

Załóżmy, 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.

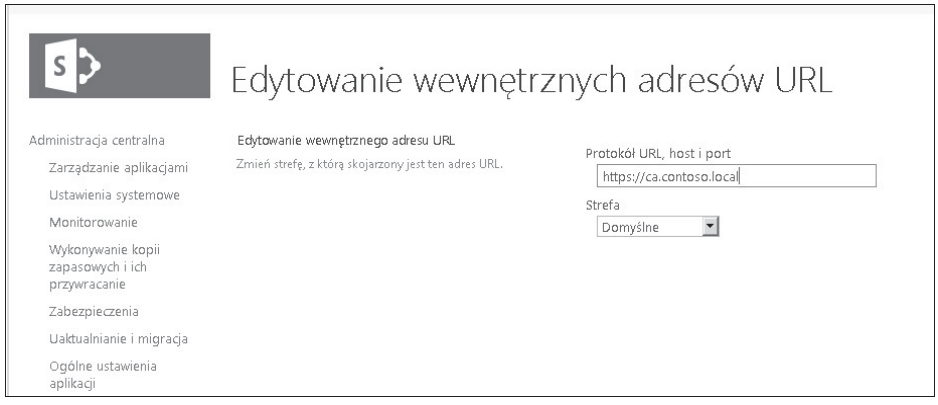
Pierwszy krok polega na stworzeniu wpisu DNS dla adresu URL, który chcemy wykorzystać. Aplikacja *Administracja centralna* jest zainstalowana na serwerze z dużym numerem portu. Będziemy adresowali ją za pomocą wspólnej nazwy. Na potrzeby tego przykładu będzie to nazwa *ca.contoso.local*.

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.



RYSUNEK 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.



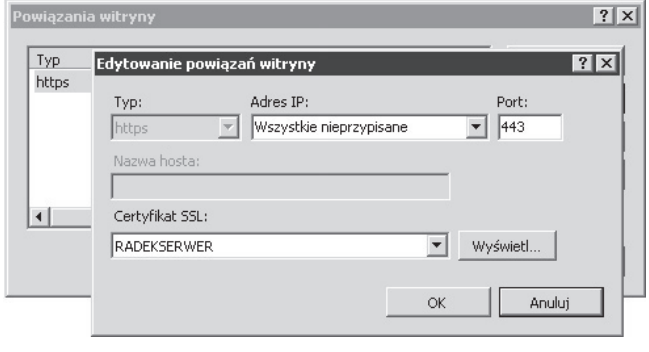
RYSUNEK 7.18. *Strona Edytowanie wewnętrznych adresów URL*

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 komandletu `Set-SPCentralAdministration` i ustawimy port na 443 tak, jak pokazano na listingu 7.8.

LISTING 7.8. *Zmiana portu*

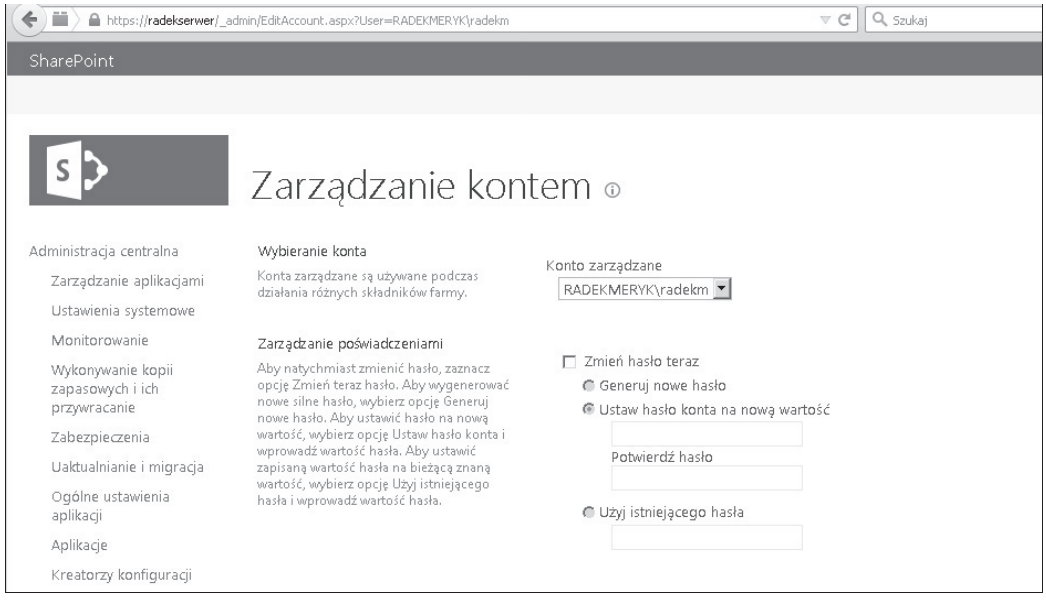
```
Set-SPCentralAdministration -Port 443
```

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).



RYSUNEK 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).



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

Skorowidz

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

Ś

T

U

V

W

Z

Ź

Ż

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

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, MCSD, 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, MCSD, 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.

Microsoft

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

Informatyka w najlepszym wydaniu

cena: 79,00 zł