Spis treści

Wstęp

Egzamin 70-742 koncentruje się na funkcjonalnościach związanych z tożsamością, dostępnych w systemie Windows Server 2016. Obejmuje instalację i konfigurację usług domenowych w usłudze Active Directory (AD DS) oraz zarządzanie i utrzymywanie usług AD DS, włącznie z konfigurowaniem AD DS w złożonym środowisku przedsiębiorstwa. Znaczna część zagadnień egzaminacyjnych dotyczy zarządzania zasadami grupy. Egzamin obejmuje też zagadnienia związane z implementacją usług Active Directory Certificate Services (AD CS), federacji tożsamości oraz rozwiązań dostępu, wraz z usługami Active Directory Federation Services (AD FS), serwerem proxy aplikacji sieci Web oraz z usługami Active Directory Rights Management Services (AD RMS).

Ta książka została opracowana z myślą o administratorach AD DS, którzy potrzebują szkolenia z zakresu technologii związanych z tożsamością i dostępem w systemie Windows Server 2016. Tematyka tej książki obejmuje wdrażanie i konfigurację AD DS w środowisku rozproszonym oraz implementowanie zasad grupy. Ponadto opisuje wdrażanie usług AD FS, AD RMS i AD CS.

Ta książka opisuje wszystkie ważniejsze zagadnienia objęte egzaminem, ale nie zawiera odpowiedzi na wszystkie pytania egzaminacyjne. Tylko zespół egzaminacyjny firmy Microsoft ma dostęp do pytań egzaminacyjnych, a firma Microsoft regularnie dodaje nowe pytania do egzaminu, co uniemożliwia uwzględnienie w książce wszystkich pytań. Powinieneś traktować tę książkę jako uzupełnienie swojego praktycznego doświadczenia i innych materiałów szkoleniowych. Jeśli natkniesz się tu na zagadnienie, którego w pełni nie zrozumiałeś, skorzystaj z łączy dostępnych w sekcjach „Dodatkowe materiały", aby uzyskać więcej informacji i poświęć nieco czasu na przestudiowanie zagadnienia. Wiele przydatnych informacji można znaleźć w witrynach MSDN i TechNet oraz na blogach i forach.

Organizacja tej książki

Ta książka jest zorganizowana według listy „Sprawdzane umiejętności", opublikowanej dla tego egzaminu. Lista ta jest dostępna dla każdego egzaminu i można ją znaleźć w witrynie Microsoft Learning, pod adresem: *https://aka.ms/examlist*. Każdy rozdział w tej książce odpowiada jednemu z głównych zagadnień na liście, a techniczne zadania

w każdym zagadnieniu determinują organizację rozdziału. Jeśli egzamin obejmuje na przykład sześć większych zagadnień, książka będzie zawierać sześć rozdziałów.

Certyfikaty firmy Microsoft

Certyfikaty firmy Microsoft wyróżniają osoby, które wykazały się znajomością szerokich zagadnień oraz doświadczeniem w korzystaniu z bieżących produktów i technologii firmy Microsoft. Egzaminy i odpowiadające im certyfikaty są opracowywane, aby zweryfikować doskonałą znajomość krytycznych kompetencji z zakresu projektowania i rozwijania, lub implementowania i wspierania rozwiązań z wykorzystaniem produktów i technologii firmy Microsoft, zarówno w infrastrukturze lokalnej, jak i w chmurze. Program certyfikacyjny przynosi wiele korzyści osobom indywidualnym, pracodawcom oraz organizacjom.

Dodatkowe informacje Wszystkie certyfikaty firmy Microsoft

Więcej informacji o certyfikatach firmy Microsoft, włącznie z listą wszystkich dostępnych certyfikatów, znajdziesz pod adresem *https://www.microsoft.com/learning*.

Podziękowania

Andrew Warren Gdy zaczynam pisać książkę, przez chwilę siedzę przed ekranem komputera, obserwując migający kursor. W końcu dochodzę do wniosku, że książka nie napisze się sama i zabieram się do pracy. Ale autor jest tylko pierwszym ogniwem tego procesu. Bez mojej redaktorki Triny MacDonald oraz zespołu wydawnictwa Pearson mój kursor nadal by migał na ekranie. Chciałbym także podziękować swojej żonie i córce za to, że dbały, aby w ekspresie do kawy nigdy nie brakowało ziaren.

Darmowe ebooki wydawnictwa Microsoft Press

Darmowe ebooki wydawnictwa Microsoft Press obejmują szeroki zakres tematów, począwszy od przeglądów technicznych do szczegółowych informacji o konkretnych zagadnieniach. Te ebooki są dostępne w formatach PDF, EPUB oraz Mobi dla urządzeń Kindle i można je pobrać ze strony:

https://aka.ms/mspressfree

Zachęcamy do częstego zaglądania i sprawdzania, czy nie pojawiło się coś nowego!

Microsoft Virtual Academy

Poszerz swoją znajomość technologii firmy Microsoft, korzystając z bezpłatnych, prowadzonych przez ekspertów szkoleń online, dostępnych w Microsoft Virtual Academy (MVA). MVA zawiera obszerną bibliotekę wideo, wydarzeń na żywo i innych materiałów, które ułatwią naukę najnowszych technologii oraz przygotowanie do egzaminów certyfikacyjnych. Tutaj znajdziesz potrzebne informacje:

https://www.microsoftvirtualacademy.com

Errata, aktualizacje i wsparcie do książki

Dołożyliśmy wszelkich starań, aby zagwarantować dokładność tej książki i towarzyszących jej materiałów dodatkowych. Aktualizacje do książki są dostępne – w postaci listy nieścisłości i poprawek – na stronie:

https://aka.ms/examref742/errata

W przypadku odkrycia błędu, który nie został jeszcze uwzględniony, można go zgłosić korzystając z tej samej witryny.

Jeśli potrzebne jest dodatkowe wsparcie, napisz e-mail do działu Microsoft Press Book Support, na adres *mspinput@microsoft.com*.

Należy pamiętać, że podane powyżej adresy nie służą do otrzymania wsparcia dla oprogramowania i sprzętu produkowanego przez firmę Microsoft. Pomoc związana z oprogramowaniem lub sprzętem firmy Microsoft jest dostępna na stronie *https://support.microsoft.com*.

Chcemy poznać Twoją opinię

W wydawnictwie Microsoft Press Twoja satysfakcja jest dla nas najważniejsza, a Twoja opinia jest dla nas niezwykle cenna. Napisz nam, co sądzisz o tej książce:

https://aka.ms/tellpress

Wiemy, że jesteś zajęty, dlatego uprościliśmy nasz formularz, który zawiera tylko kilka pytań. Odpowiedzi zostaną przesłane bezpośrednio do redaktorów w wydawnictwie Microsoft Press. (Nie pytamy o żadne dane osobowe.) Z góry dziękujemy za Twój udział w ankiecie!

Pozostańmy w kontakcie

Podtrzymajmy kontakt! Znajdziesz nas na Twitterze: *http://twitter.com/MicrosoftPress*.

Ważne:
Jak używać tej książki podczas przygotowania do egzaminu

Egzaminy certyfikacyjne weryfikują Twoją wiedzę praktyczną i znajomość produktu. Ten podręcznik pomoże ci się przekonać, czy jesteś gotów do przystąpienia do egzaminu, sprawdzając Twoją znajomość zagadnień wchodzących w jego skład. Dzięki niemu możesz określić, które tematy znasz doskonale, a które obszary wymagają dodatkowej pracy. Aby ułatwić odświeżenie umiejętności z określonych dziedzin, dołączyliśmy też wskazówki „Szybki przegląd", kierujące do dodatkowych, zewnętrznych źródeł informacji.

Podręcznik ten nie może zastąpić doświadczenia praktycznego. Książka ta nie ma na celu uczenia nowych umiejętności, ale utrwalenie i uporządkowanie już posiadanej wiedzy.

Zalecamy, aby w trakcie przygotowań do egzaminu korzystać z wielu dostępnych materiałów szkoleniowych. Więcej informacji na temat dostępnych szkoleń można znaleźć pod adresem https://www.microsoft.com/learning. Dla wielu egzaminów dostępne są Microsoft Official Practice Tests – ich spis można znaleźć pod adresem https://aka.ms/practicetests. Dostępne są również darmowe szkolenia online i wykłady na żywo w Microsoft Virtual Academy, pod adresem https://www.microsoftvirtualacademy.com.

Książka ta została uporządkowana według listy mierzonych umiejętności (Skills measured) dla tego egzaminu. Lista taka dla każdego egzaminu jest dostępna w witrynie Microsoft Learning: https://aka.ms/examlist.

Warto odnotować, że niniejsza książka opiera się na publicznie dostępnych informacjach na temat egzaminów oraz doświadczeniach autorów. W celu zachowania pełnej poufności autorzy nie mieli dostępu do treści rzeczywistych egzaminów.

ROZDZIAŁ 1

Instalowanie i konfigurowanie usług domenowych w usłudze Active Directory

Usługi domenowe w usłudze Active Directory (AD DS – Active Directory Domain Services) stanowią sedno rozwiązań związanych z tożsamością i dostępem w systemie Windows Server 2016. To dlatego należy poznać zasady implementacji infrastruktury AD DS, aby skutecznie zaspokoić potrzeby organizacji dotyczące tożsamości.

W tym rozdziale zostaną poruszone zagadnienia związane z instalowaniem i konfigurowaniem kontrolerów domeny, tworzeniem i konfigurowaniem użytkowników, grup, komputerów i jednostek organizacyjnych (OU – organizational unit). Są to umiejętności niezbędne podczas implementacji usług AD DS.

Zagadnienia egzaminacyjne omawiane w tym rozdziale:

Zagadnienie 1.1: Instalowanie i konfiguracja kontrolerów domeny

Kontrolery domeny są hostem roli serwera AD DS w Windows Server 2016. Zapewniają usługi uwierzytelnienia i pokrewne komputerom organizacji oraz innym urządzeniom sieciowym. Zanim będzie można poprawnie zinterpretować scenariusze wdrażania kontrolerów domeny AD DS, trzeba najpierw zrozumieć podstawy dotyczące usługi AD DS, a w szczególności pojęcia lasów, drzew, domen, witryn i jednostek organizacyjnych.

W tym podrozdziale zostaną omówione następujące zagadnienia:

- Podstawy AD DS
- Instalowanie nowego lasu
- Dodawanie lub usuwanie kontrolera domeny
- Instalowanie usługi AD DS w instancji Server Core
- Instalowanie kontrolera domeny za pomocą funkcji Install from Media (Instalowanie z nośnika)
- Instalowanie i konfigurowanie kontrolera domeny tylko do odczytu
- Konfigurowanie serwera wykazu globalnego
- Konfigurowanie klonowania kontrolera domeny
- Aktualizacja kontrolerów domeny
- Transferowanie i przejmowanie ról wzorca operacji
- Rozwiązywanie problemów związanych z rejestracją rekordów DNS SRV

Podstawy AD DS

AD DS opiera się zarówno na komponentach logicznych, jak i fizycznych. Komponent fizyczny jest czymś namacalnym, na przykład kontrolerem domeny, natomiast las AD DS jest niematerialnym komponentem logicznym. AD DS zawiera następujące komponenty logiczne:

- **Las** Las jest kolekcją domen AD DS o wspólnym schemacie, które są połączone dwukierunkową relacją zaufania, utworzoną automatycznie. Większość organizacji implementuje AD DS z jednym lasem. Decyzja o implementacji kilku lasów może wynikać z następujących wymagań:
  - Zapewnienie całkowitej separacji administracyjnej między różnymi oddziałami organizacji.

- Wsparcie różnych typów obiektów i atrybutów w schemacie AD DS, w zależności od istniejących oddziałów organizacji.

- **Domena** Domena jest logiczną jednostką administracyjną, która zawiera użytkowników, grupy, komputery i inne obiekty. Wiele domen może wchodzić w skład jednego lub kilku lasów, w zależności od potrzeb organizacji. Strukturę domeny definiują relacje rodzic-dziecko oraz relacja zaufania.

> ***WSKAZÓWKA EGZAMINACYJNA***
>
> Domena nie zapewnia separacji administracyjnej, ponieważ wszystkie domeny w lesie mają tego samego administratora lasu – uniwersalną grupę zabezpieczeń Enterprise Admins (Administratorzy przedsiębiorstwa). Aby uzyskać całkowitą separację administracyjną, należy zaimplementować kilka lasów AD DS.

- **Drzewo** Drzewo jest kolekcją domen AD DS, które mają tę samą domenę katalogu głównego i wspólny obszar nazw. Na przykład sales.adatum.com i marketing.adatum.com mają wspólny katalog główny adatum.com; mają też wspólny obszar nazw adatum.com. Las AD DS można zbudować na podstawie jednego lub wielu drzew. Za użyciem wielu drzew przemawia konieczność wsparcia wielu logicznych obszarów nazw w organizacji, na przykład ze względu na fuzje lub przejęcia.
- **Schemat** Schemat AD DS jest kolekcją typów obiektów i ich właściwości, nazywanych też atrybutami, która definiuje, jakie obiekty można utworzyć, przechowywać i zarządzać za pomocą lasu AD DS. Na przykład użytkownik jest typem obiektu logicznego, który ma kilka właściwości, takich jak imię i nazwisko, oddział i hasło. Relacja między obiektami i ich atrybutami jest przechowywana w schemacie, a jego kopia znajduje się we wszystkich kontrolerach domeny w lesie.
- **OU** Jednostka organizacyjna (Organizational Unit) jest kontenerem w domenie, który zawiera użytkowników, grupy, komputery i inne OU. Jednostki organizacyjne upraszczają administrację. Dzięki nim można z łatwością oddelegować prawa administracyjne do kolekcji obiektów. W tym celu należy zgrupować obiekty w jednostce administracyjnej i przydzielić do niej prawa. Można też skorzystać z obiektów zasad grupy (GPO – Group Policy Object). W tym przypadku należy skonfigurować ustawienia użytkownika i komputera, a następnie połączyć ustawienia obiektów GPO z jednostkami organizacyjnymi, upraszczając w ten sposób proces konfiguracji. Jedna jednostka organizacyjna – Domain Controllers (Kontrolery domeny) – jest tworzona domyślnie, podczas instalacji usługi AD DS i tworzenia domeny.
- **Kontener** Kolekcje obiektów można grupować nie tylko w jednostkach organizacyjnych, ale również z kontenerach. Istnieje wiele wbudowanych kontenerów, na przykład: Computers (Komputery), Builtin (Wbudowane) i Managed

Service Accounts (Zarządzane konta usługi). Obiektów GPO nie można łączyć z kontenerami.

- **Lokacja** Lokacja jest logiczną reprezentacją fizycznej lokalizacji w organizacji. Może reprezentować duży obszar fizyczny, taki jak miasto, lub mniejszy, taki jak kolekcja podsieci, zdefiniowana przez granice centrum danych. Dzięki lokacjom AD DS urządzenia podłączone do sieci mogą łatwiej określić swoją lokalizację względem usług, z którymi chcą się połączyć. Na przykład, komputer z systemem Windows 10 podczas uruchamiania próbuje znaleźć sąsiedni kontroler domeny za pomocą ustalonego położenia lokacji, aby wesprzeć logowanie użytkownika. Lokacje umożliwiają też kontrolę replikacji AD DS, poprzez konfigurację harmonogramu i interwałów między replikacjami przychodzącymi.

WSKAZÓWKA EGZAMINACYJNA

Podczas instalacji usługi AD DS i tworzenia pierwszego lasu powstaje domyślna lokacja Default-First-Site-Name. Należą do niej wszystkie kontrolery domeny, dopóki nie utworzysz dodatkowych lokacji i nie przydzielisz do nich kontrolerów domeny. Jeśli zamierzasz utworzyć dodatkowe obiekty lokacji, powinieneś zmienić nazwę domyślnej lokacji.

- **Podsieć** Podsieć jest logiczną reprezentacją fizycznej podsieci w sieci. Definiując podsieci umożliwiasz komputerom w lesie AD DS określenie fizycznej lokalizacji względem usług dostarczanych przez las. Domyślnie nie istnieją żadne podsieci. Po utworzeniu podsieci należy je powiązać z lokacjami. Lokacja może zawierać kilka podsieci.
- **Partycja** AD DS jest fizycznie przechowywana w bazie danych we wszystkich kontrolerach domeny. Ponieważ niektóre części struktury AD DS nie zmieniają się zbyt często, a inne podlegają częstym zmianom, w bazie danych AD DS przechowywanych jest kilka osobnych partycji.

Uwaga Replikacja AD DS

Podczas zmian dokonywanych w AD DS należy też uaktualnić inne instancje zmienionych partycji. Ten proces nosi nazwę replikacji AD DS. Dzieląc bazę danych na kilka elementów, redukujemy obciążenie związane z procesem replikacji.

Dostępne są następujące partycje:

- **Schema (Schemat)** Partycja na poziomie lasu, która rzadko się zmienia. Zawiera schemat lasu AD DS.
- **Configuration (Konfiguracja)** Partycja na poziomie lasu, która rzadko się zmienia i zawiera dane konfiguracji lasu.

- **Domain (Domena)** Partycja na poziomie domeny. Ta partycja zmienia się często, a kopia partycji z możliwością zapisu jest przechowywana we wszystkich kontrolerach domeny. Zawiera rzeczywiste obiekty, na przykład użytkowników i komputery, które istnieją w lesie.

UWAGA Kontrolery domeny tylko do odczytu

Kontrolery domeny tylko do odczytu (RODC – Read Only Domain Controller) zawierają kopię partycji domeny, która jest tylko do odczytu (nie może być modyfikowana na tym kontrolerze domeny).

UWAGA Partycje katalogu aplikacji

Można też utworzyć partycje, przeznaczone na aplikacje z włączoną usługą katalogową, które wdrażasz w swoim lesie. Można na przykład tak skonfigurować system DNS, aby do celów replikacji strefy, zintegrowanej z usługą AD, korzystał z konkretnej partycji aplikacji.

- **Trust relationships (Relacje zaufania)** Relacja zaufania, czasem określana także terminem zaufanie, jest umową dotyczącą bezpieczeństwa, zawieraną między dwiema domenami w lesie AD DS, między dwoma lasami lub między lasem a zewnętrznym obszarem zabezpieczeń. Dzięki tej umowie użytkownik po jednej stronie relacji może uzyskać dostęp do zasobów drugiej strony. W relacji zaufania jedna strona jest uznawana za ufającą, a druga za zaufaną. Encja przechowująca zasoby jest stroną ufającą, a zaufana jest encja zawierająca użytkownika. Łatwiej można to zrozumieć, jeśli zastanowimy się, kto jest osobą zaufaną, a kto osobą ufającą w sytuacji, gdy pożyczamy komuś klucze do swojego samochodu.

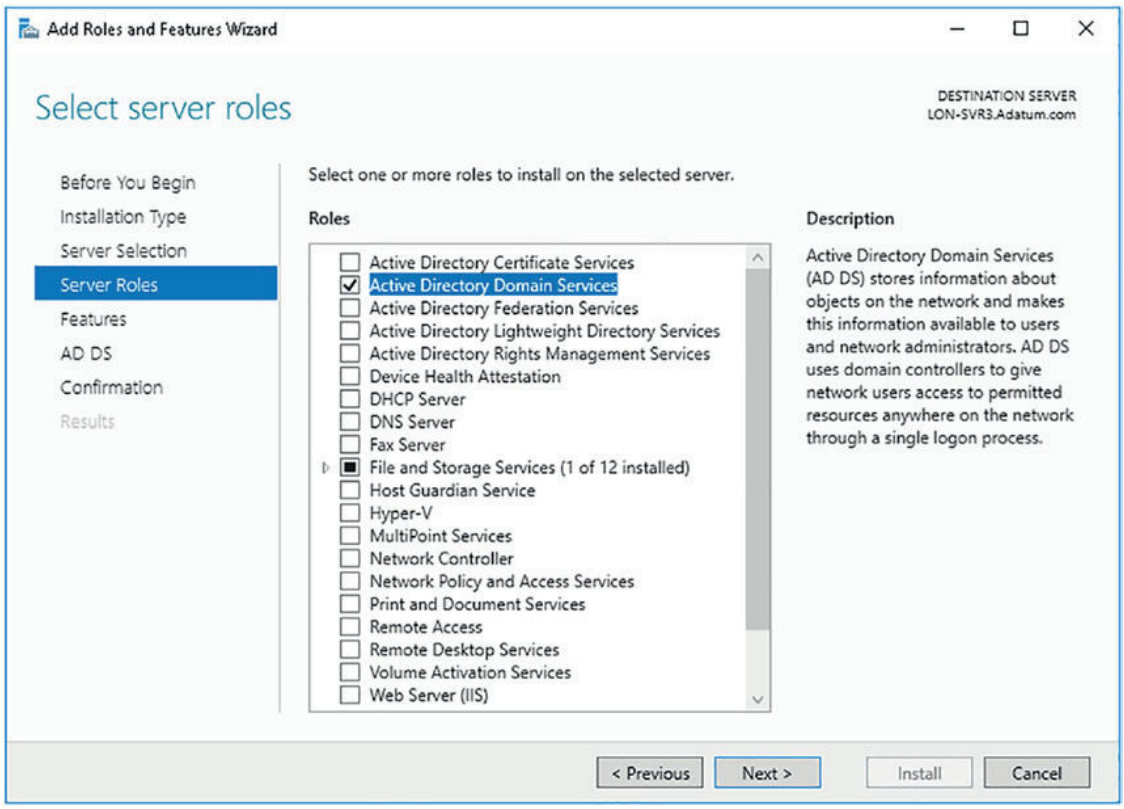
Instalowanie nowego lasu

Aby zainstalować nowy las AD DS, musimy wdrożyć w tym lesie pierwszy kontroler domeny. W tym celu należy wdrożyć rolę serwera AD DS na komputerze z systemem Windows Server 2016, a następnie podwyższyć poziom serwera do kontrolera domeny i dodać nowy las.

Aby utworzyć nowy las, zacznij od instalacji roli AD DS, wykonując następującą procedurę:

1. Zaloguj się na komputerze z systemem Windows Server 2016 jako administrator lokalny.
2. Uruchom konsolę Server Manager (Menedżer serwera), a następnie kliknij Add Roles And Features (Dodaj role i funkcje) w sekcji Dashboard (Pulpit nawigacyjny).

3. Wykonaj kolejne kroki kreatora Add Roles And Features Wizard (Kreator dodawania ról i funkcji), a następnie na karcie Server Roles (Role serwera), widocznej na rysunku 1-1, zaznacz opcję Active Directory Domain Services (Usługi domenowe w usłudze Active Directory), kliknij Add Features (Dodaj funkcje), po czym kliknij Next (Dalej).
4. Wykonaj kolejne kroki kreatora i na końcu kliknij Install (Zainstaluj).
5. Gdy instalacja dobiegnie końca, kliknij Close (Zamknij).



Rysunek 1-1 Instalowanie roli serwera Active Directory Domain Services

WSKAZÓWKA EGZAMINACYJNA

Aby zainstalować potrzebne pliki, można też skorzystać z powłoki Windows PowerShell. W tym celu uruchom następujące polecenie w wierszu poleceń PowerShell z podwyższonym poziomem uprawnień: Install-WindowsFeature AD-Domain-Services.

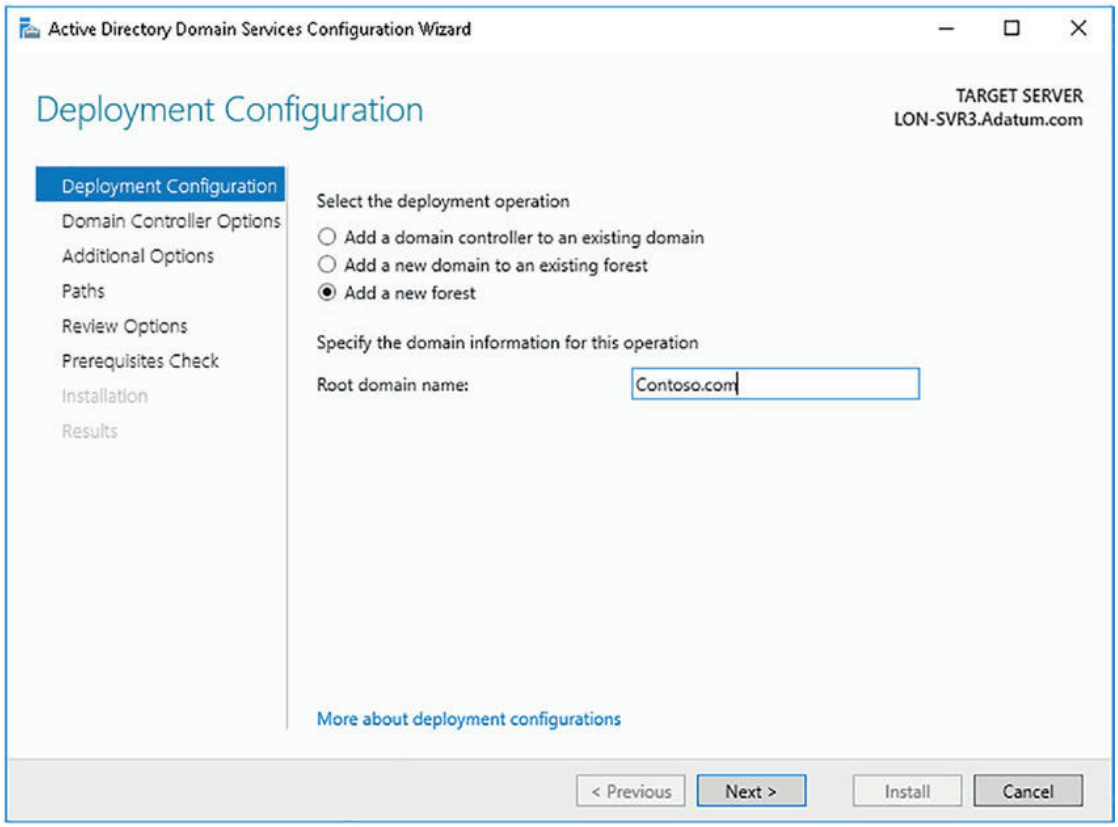
Po zainstalowaniu plików binarnych usługi AD DS należy utworzyć nowy las. W tym celu należy podwyższyć poziom pierwszego kontrolera domeny w lesie. Służy do tego następująca procedura:

1. W konsoli Server Manager kliknij żółtą trójkątną ikonę ostrzeżenia, znajdującą się w sekcji Notifications (Powiadomienia), a następnie kliknij Promote This Server

To A Domain Controller (Podnieś poziom tego serwera do poziomu kontrolera domeny).

> ***WSKAZÓWKA EGZAMINACYJNA***
>
> Podwyższenia poziomu można też dokonać za pomocą powłoki Windows PowerShell. W tym celu uruchom cmdlet `Install-ADDSDomainController`. Na przykład polecenie `Install-ADDSDomainController -InstallDns -DomainName adatum.com` pozwala dodać lokalny serwer jako dodatkowy kontroler domeny do domeny Adatum.com i zainstalować rolę serwera DNS.

2. Na karcie Deployment Configuration (Konfiguracja wdrażania) kreatora Active Directory Domain Services Configuration Wizard (Kreator konfiguracji usług domenowych Active Directory), w sekcji Select The Deployment Operation (Wybierz operację wdrażania) kliknij Add A New Forest (Dodaj nowy las), a następnie wpisz nazwę głównego katalogu domeny lasu, jak pokazano na rysunku 1-2. Kliknij Next.



Rysunek 1-2 Dodawanie nowego lasu

3. Na karcie Domain Controller Options (Opcje kontrolera domeny), widocznej na rysunku 1-3, skonfiguruj następujące opcje, po czym kliknij Next:

- **Forest Functional Level (Poziom funkcjonalności lasu)** Poziom funkcjonalności lasu określa, które funkcje na poziomie lasu są dostępne w lesie. Poziom funkcjonalności lasu definiuje też minimalny poziom funkcjonalności domeny w lesie. Jeśli ustawisz ten poziom na Windows Server 2012, wówczas minimalny poziom funkcjonalności domeny również będzie odpowiadał poziomowi Windows Server 2012. Do wyboru mamy następujące opcje:
  - Windows Server 2008
  - Windows Server 2008 R2
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016
- **Domain Functional Level (Poziom funkcjonalności domeny)** Określa funkcje dotyczącej całej domeny, które są dostępne w tej domenie. Do wyboru mamy następujące opcje:
  - Windows Server 2008
  - Windows Server 2008 R2
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016

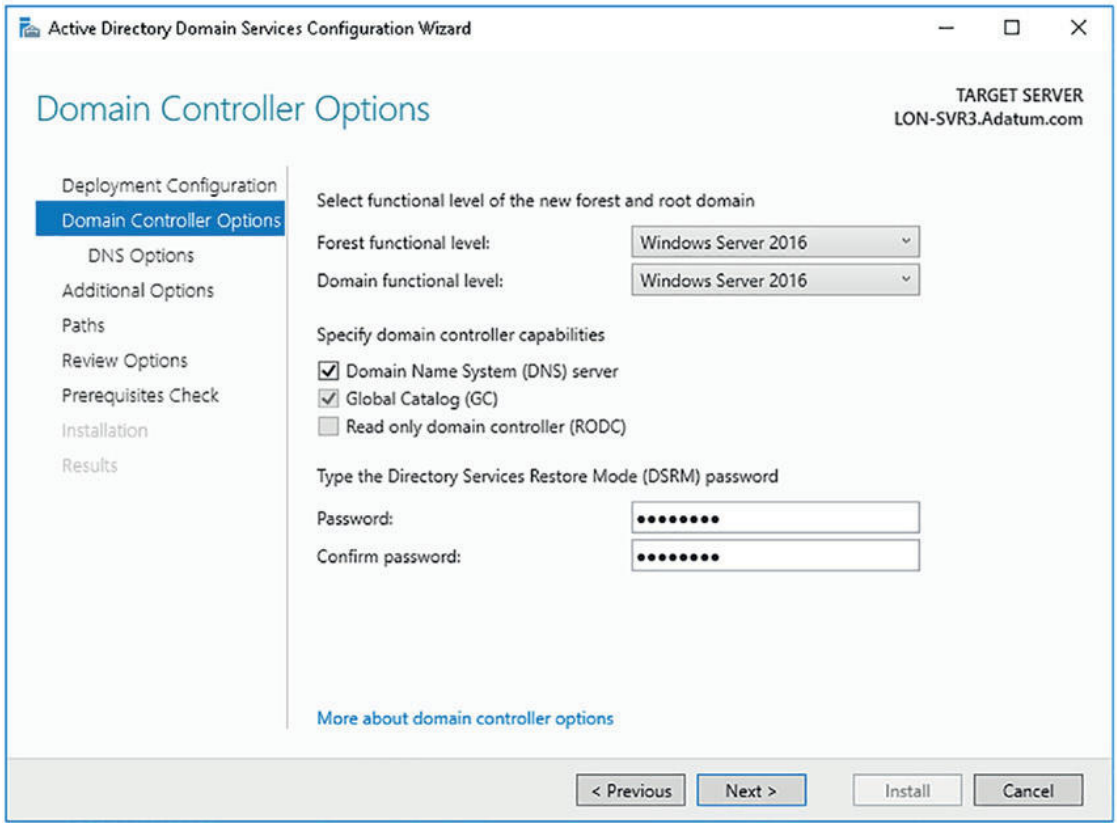
Dodatkowe materiały **Poziomy funkcjonalności w systemie Windows Server 2016**

Więcej szczegółów dotyczących poziomów funkcjonalności domeny i lasu w systemie Windows Server 2016 znajdziemy w witrynie Microsoft TechNet, pod adresem *https://technet.microsoft.com/windows-server-docs/identity/ad-ds/windows-server-2016-functional-levels*.

- **Domain Name System (DNS) Server (Serwer DNS)** DNS służy do rozpoznawania nazw i jest krytyczną składową usługi AD DS. Ta opcja jest domyślnie zaznaczona i nie należy tego zmieniać, chyba że skonfigurowałeś już infrastrukturę DNS.
- **Global Catalog (GC) (Wykaz globalny)** Wykaz globalny zapewnia usługi dotyczące całego lasu. Ta opcja jest domyślnie zaznaczona i nie można tego zmienić. Pierwszy (i jedyny) kontroler domeny musi być serwerem wykazu globalnego. Po dodaniu dodatkowych kontrolerów domeny można powrócić do tego ustawienia.
- **Read Only Domain Controller (RODC) (Kontroler domeny tylko do odczytu)** Opcja ta określa, czy kontroler domeny jest tylko do odczytu. Ta opcja nie jest

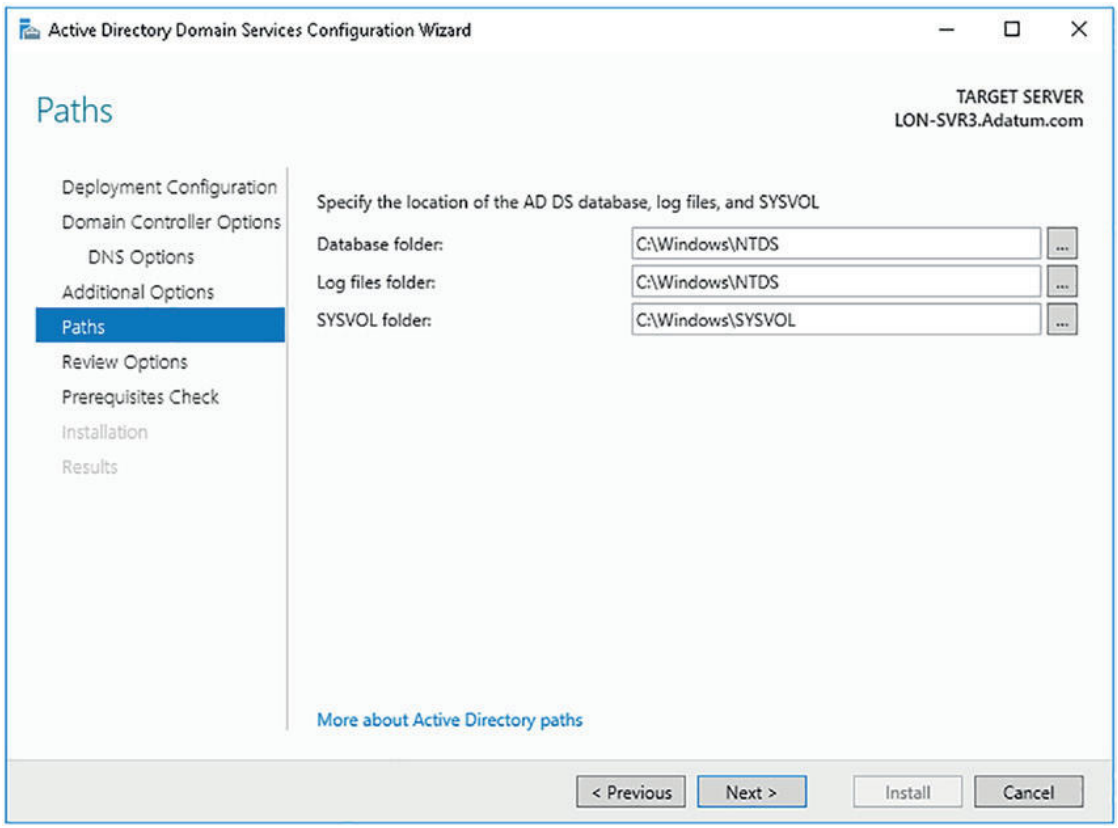
domyślnie zaznaczona i nie jest dostępna dla pierwszego (i obecnie jedynego) kontrolera domeny w lesie.

- **Directory Services Restore Mode (DSRM) Password (Hasło trybu przywracania usług katalogowych)** Opcja ta jest wykorzystywana podczas uruchamiania kontrolera domeny w trybie odzyskiwania.



Rysunek 1-3 Konfigurowanie opcji kontrolera domeny

4. Na karcie Additional Options (Opcje dodatkowe) zdefiniuj nazwę domeny NetBIOS. Protokół NetBIOS, który nie jest już powszechnie używany, jest oparty na niehierarchicznej strukturze nazw. Domyślną nazwą NetBIOS jest pierwsza część nazwy lasu AD DS. Jeśli na przykład las nosi nazwę Contoso.com, domyślną nazwą NetBIOS jest CONTOSO; ogólnie rzecz biorąc nie ma potrzeby jej zmiany. Kliknij Next.
5. Jak widać na rysunku 1-4, zdefiniuj miejsce przechowywania bazy danych AD DS, plików dziennika i zawartości SYSVOL, po czym kliknij Next. Ustawienia domyślne są następujące
   - Database folder (Folder bazy danych): C:\Windows\NTDS
   - Database folder (Folder plików dziennika): C:\Windows\NTDS
   - SYSVOL folder: C:\Windows\SYSVOL



Rysunek 1-4 Konfigurowanie ścieżek AD DS

WSKAZÓWKA EGZAMINACYJNA

Zwykle nie ma sensu zmieniać tych ścieżek. Jednak dzięki rozdzieleniu ścieżek SYSVOL, bazy danych i plików dziennika, można uzyskać nieco lepszą wydajność, o ile serwer ma zainstalowanych wiele fizycznych dysków twardych. W ten sposób możemy rozłożyć obciążenie.

6. Przejrzyj opcje konfiguracji i kliknij Next, aby zweryfikować wymagania wstępne.
7. Gdy pojawi się przycisk Install, kliknij go. Podczas instalacji komputer zostanie ponownie uruchomiony.
8. Zaloguj się na komputerze serwera za pomocą konta administratora domeny.

Dodatkowe materiały **Instalowanie usług domenowych w usłudze Active Directory**

Więcej szczegółów o wdrażaniu AD DS znajdziesz w witrynie Microsoft TechNet pod adresem *https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/deploy/install-active-directory-domain-services--level-100-*.

Dodawanie lub usuwanie kontrolera domeny

Po wdrożeniu pierwszego kontrolera domeny w lesie AD DS można dodać kolejne kontrolery domeny, które zapewnią niezawodność i zwiększą wydajność. Proces wdrażania dodatkowych kontrolerów domeny jest w dużej mierze identyczny jak w przypadku pierwszego kontrolera domeny: należy zainstalować rolę serwera AD DS (za pomocą konsoli Server Manager lub powłoki Windows PowerShell), a następnie podwyższyć poziom kontrolera domeny (również za pomocą konsoli Server Manager lub powłoki Windows PowerShell).

Jednak opcje, jakie można wybrać podczas podwyższania poziomu różnią się w zależności od szczegółów wdrożenia. Na przykład dodawanie nowego kontrolera domeny do istniejącej domeny różni się nieco od dodawania go do nowej domeny.

Dodawanie nowego kontrolera domeny może się odbywać według dwóch podstawowych scenariuszy:

- **Dodawanie nowego kontrolera domeny do istniejącej domeny** Aby wykonać ten proces, musisz się zalogować jako członek docelowej globalnej grupy zabezpieczeń domeny Domain Admins (Administratorzy domeny).
- **Dodawanie nowego kontrolera domeny do nowej domeny** Aby wykonać ten proces, musisz się zalogować jako członek uniwersalnej grupy zabezpieczeń głównego katalogu lasu Enterprise Admins (Administratorzy przedsiębiorstwa). W ten sposób uzyskasz wystarczające uprawnienia, by zmodyfikować partycję konfiguracji AD DS i utworzyć nową domenę, wchodzącą w skład drzewa istniejącej lub nowej domeny.

Często nową domenę dodaje się, aby zdefiniować granice replikacji. Ponieważ większość zmian w bazie danych AD DS dotyczy partycji domeny, to ta partycja generuje większość ruchu podczas replikacji AD DS. Rozdzielając swój las AD DS na wiele domen, można rozdzielić ilość zmian, a tym razem zredukować replikację między lokacjami. Jeśli na przykład firma A. Datum ma wiele komputerów, zarówno w Europie, jak i w Kanadzie, twórcy mogliby utworzyć dwie osobne domeny w głównej domenie lasu Adatum.com: Europe.Adatum.com i Canada.Adatum.com. Zmiany w domenie Europe.Adatum.com nie zostaną zreplikowane w kontrolerach domeny Canada.Adatum.com i odwrotnie.

Dodawanie nowego kontrolera domeny do istniejącej domeny

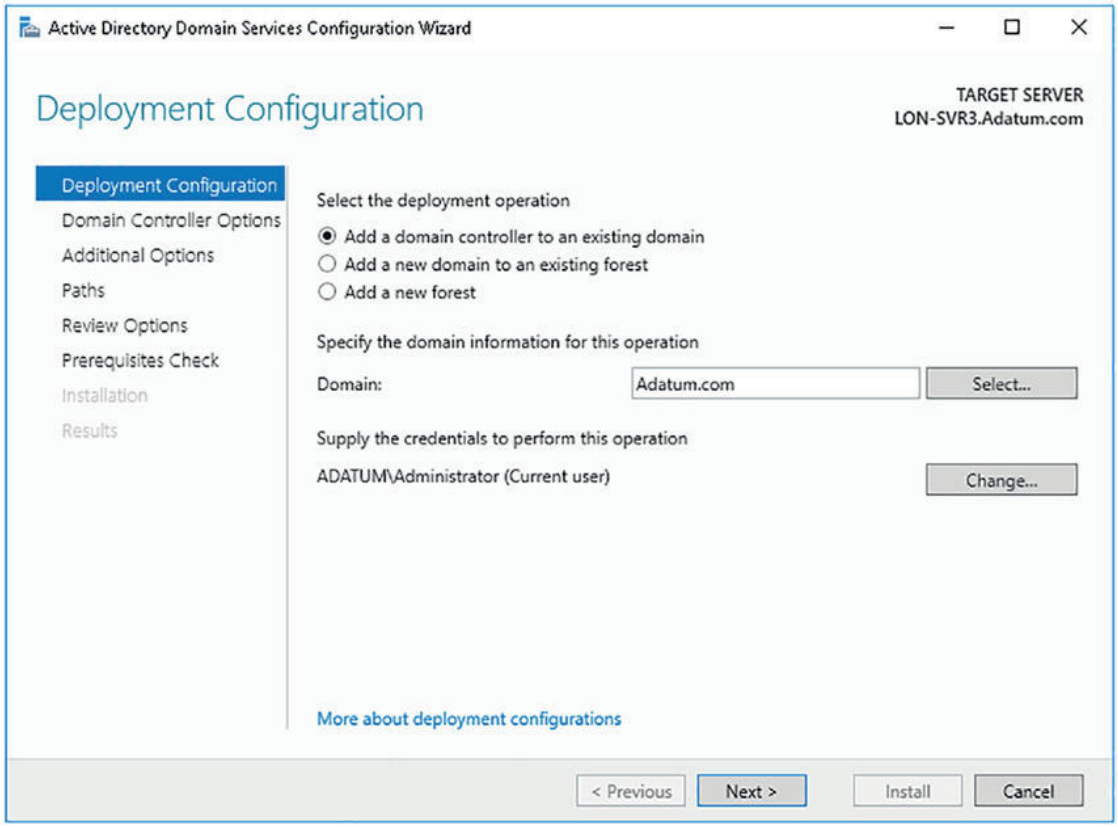
Aby dodać nowy kontroler domeny do istniejącej domeny, zaloguj się jako administrator domeny, po czym wykonaj poniższą procedurę.

1. Dodaj rolę serwera Active Directory Domain Services.
2. W konsoli Server Manager kliknij Notifications, a następnie kliknij Promote This Server To A Domain Controller.

WSKAZÓWKA EGZAMINACYJNA

Jeśli ktoś loguje się jako członek globalnej grupy zabezpieczeń Domain Admins, zakłada się, że komputer serwera, którego poziom ma zostać podniesiony, jest członkiem domeny docelowej. Jeśli nie jest, łatwiej będzie najpierw dodać komputer serwera do domeny docelowej, a następnie dokończyć procedurę. Jeśli zdecydujesz, że nie chcesz dodawać komputera do domeny docelowej, musisz się zalogować jako administrator lokalny i podczas procesu podnoszenia podać dane dostępowe administratora domeny. Wymaga się także, aby komputer podnoszonego serwera mógł rozpoznawać nazwy za pomocą usługi DNS w lesie AD DS.

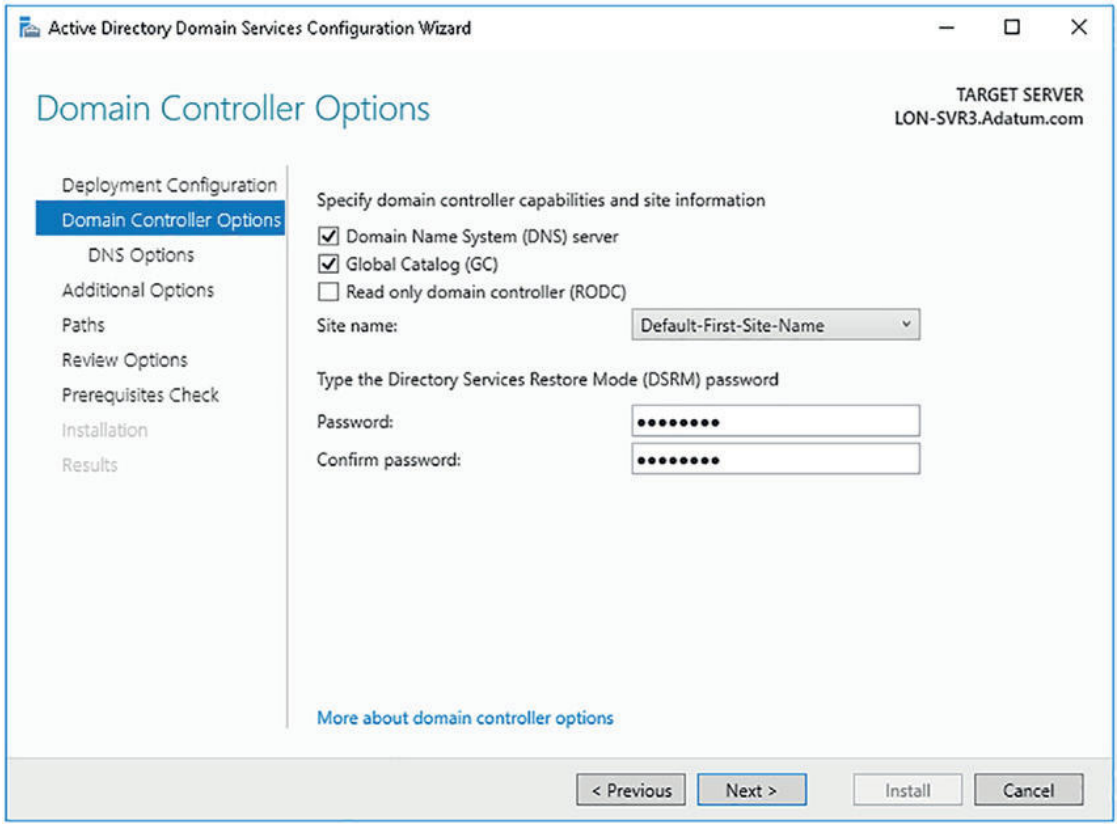
3. W kreatorze Active Directory Domain Services Configuration Wizard, na karcie Deployment Configuration, widocznej na rysunku 1-5, kliknij Add A Domain Controller To An Existing Domain (Dodaj kontroler domeny do istniejącej domeny).



Rysunek 1-5 Wdrażanie dodatkowego kontrolera domeny w istniejącej domenie

4. Podaj nazwę domeny. Domyślna nazwa jest taka sama jak domena, do której należy komputer serwera. Można jednak wybrać inną domenę dostępną w lesie.

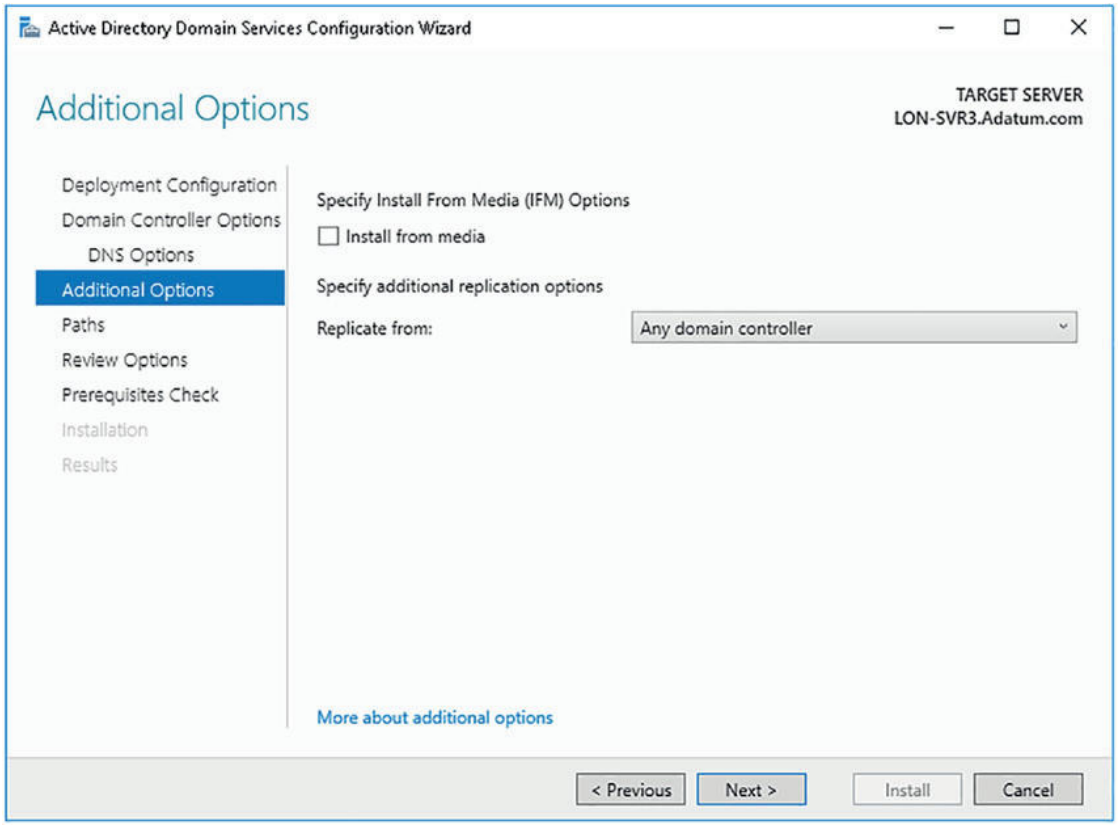
5. Wpisz dane dostępowe konta użytkownika o uprawnieniach, pozwalających na przeprowadzenie procesu podnoszenia poziomu. Domyślnie jest to konto bieżącego użytkownika. Kliknij Next.
6. Na karcie Domain Controller Options skonfiguruj opcje serwera Domain Name System (DNS) (domyślnie włączona), Global Catalog (GC) (domyślnie włączona) i Read Only Domain Controller (RODC) (domyślnie wyłączona). Inaczej niż podczas podnoszenia pierwszego kontrolera domeny w lesie, można włączyć opcję Read Only Domain Controller (RODC), aby ten kontroler domeny był tylko do odczytu.
7. Z listy Site name (Nazwa witryny*), widocznej na rysunku 1-6, wybierz lokację, w której fizycznie znajduje się ten kontroler domeny. Domyślnie jest to Default-First-Site-Name. Dopóki nie utworzysz dodatkowych lokacji AD DS, jest to jedyna dostępna lokacja. Po wdrożeniu można przenieść kontroler domeny do innej lokacji.



Rysunek 1-6 Konfigurowanie opcji kontrolera domeny dla dodatkowego kontrolera domeny

* W polskiej wersji interfejsu występuje tu błąd przekładu – chodzi nie o witrynę, ale o lokację (w języku angielskim obydwa pojęcia określane są tym samym terminem „site") (przyp. red. wyd. polskiego).

8. Wpisz hasło Directory Services Restore Mode (DSRM) i kliknij Next.
9. Na karcie Additional Options musisz skonfigurować sposób wypełniania bazy danych AD DS przez ten kontroler domeny. Można skonfigurować wstępne wypełnienie poprzez kontroler domeny online, wybierając Any Domain Controller (Dowolny kontroler domeny), jak na rysunku 1-7, lub podając konkretny kontroler domeny. Inny sposób polega na wybraniu opcji Install From Media (IFM) (Instalowanie z nośnika). Kliknij Next.



Rysunek 1-7 Konfigurowanie dodatkowych opcji kontrolera domeny

10. Jak wcześniej, skonfiguruj opcje w sekcji Paths (Ścieżki), a następnie przejdź przez kolejne kroki kreatora konfiguracji.
11. Gdy pojawi się przycisk Install, kliknij go. Podczas procesu podnoszenia komputer serwera zostanie ponownie uruchomiony.

Gdy proces podnoszenia dobiegnie końca, zaloguj się za pomocą konta administratora domeny.

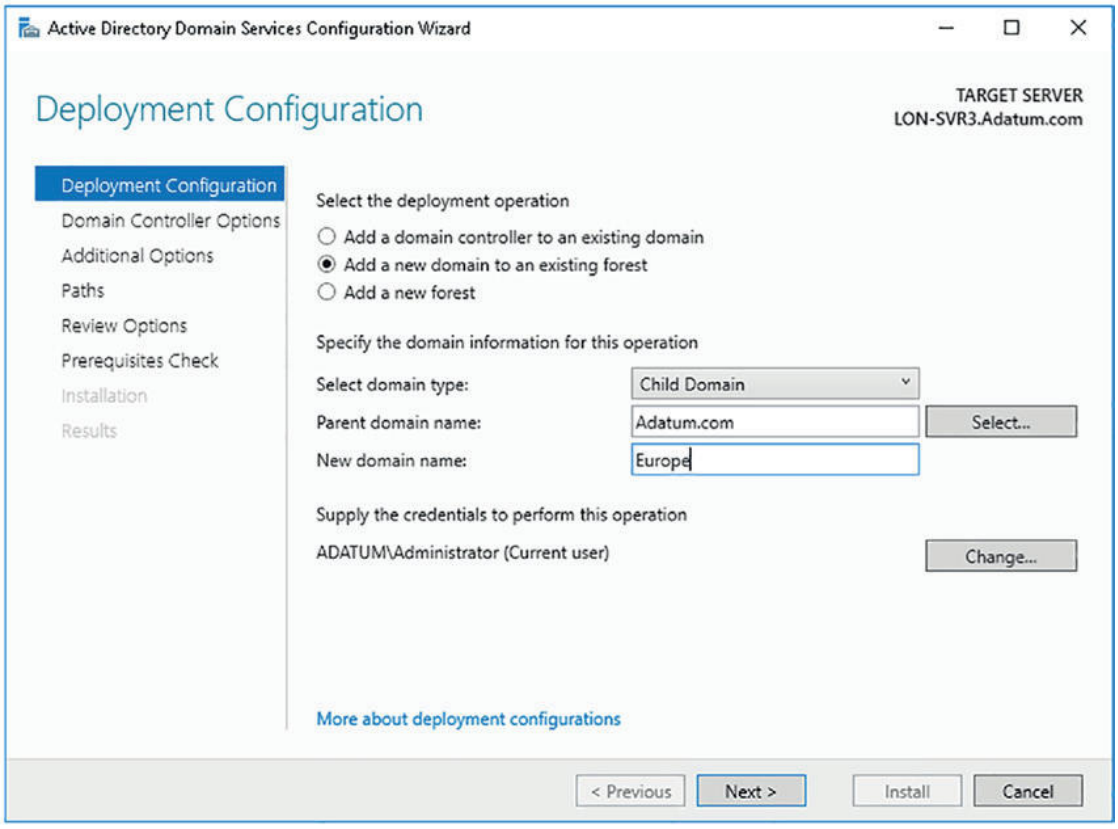
Dodawanie nowego kontrolera domeny do nowej domeny

Aby dodać nowy kontroler domeny do nowej domeny w istniejącym lesie, zaloguj się jako członek uniwersalnej grupy zabezpieczeń lasu Enterprise Admin, a następnie wykonaj poniższą procedurę.

> ***WSKAZÓWKA EGZAMINACYJNA***
>
> Jeśli ktoś loguje się jako członek uniwersalnej grupy zabezpieczeń Enterprise Admins, zakłada się, że komputer serwera, którego poziom ma zostać podniesiony, jest członkiem jednej z domen lasu AD DS. Jeśli nie jest, łatwiej będzie najpierw dodać komputer serwera do głównej domeny lasu, a następnie dokończyć procedurę. Jeśli zdecydujesz się nie dodawać komputera do głównej domeny lasu, musisz się zalogować jako administrator lokalny i podczas procesu podnoszenia podać dane dostępowe administratora przedsiębiorstwa. Ponadto podnoszony komputer serwera powinien móc rozpoznawać nazwy za pomocą usługi DNS w lesie AD DS.

1. Dodaj rolę serwera Active Directory Domain Services.
2. W konsoli Server Manager kliknij Notifications, a następnie kliknij Promote This Server To A Domain Controller.
3. W kreatorze Active Directory Domain Services Configuration Wizard, na karcie Deployment Configuration, widocznej na rysunku 1-8, kliknij Add A New Domain To An Existing Forest (Dodaj nową domenę do istniejącego lasu).
4. Następnie można wybrać sposób dodania nowej domeny. Do wyboru są następujące opcje:
   - **Child Domain (Domena podrzędna)** Po wybraniu tej opcji powstanie subdomena podanej domeny nadrzędnej. Innymi słowy, nowa domena zostanie utworzona w drzewie istniejącej domeny.
   - **Tree Domain (Domena drzewa)** Wybierz tę opcję, jeśli chcesz utworzyć nowe drzewo w tym samym lesie. Nowe drzewo będzie mieć ten sam schemat lasu i tę samą główną domenę lasu, ale można zdefiniować nieciągły obszar nazw. Jest to przydatne, jeśli zamierzasz utworzyć wiele nazw domen DNS w infrastrukturze lasu AD DS, aby zaspokoić potrzeby swojej organizacji, ale nie potrzebujesz lub nie chcesz rozdzielać funkcji administracyjnych, co jest możliwe w przypadku osobnego lasu. Jeśli wybierzesz opcję Tree Domain, musisz zdefiniować domenę lasu, do której zostanie dodane drzewo. Domyślnie jest to las, do którego jesteś zalogowany.
5. Wpisz nazwę nowej domeny. W przypadku domeny podrzędnej nazwa zawiera przedrostek w postaci domeny nadrzędnej. Na przykład dodanie domeny Europe jako domeny potomnej Adatum.com spowoduje utworzenie domeny Europe.

Adatum.com. Jeśli tworzysz nowe drzewo, można wpisać dowolną prawidłową nazwę DNS, która nie zawiera domeny głównej lasu. Kliknij Next.



Rysunek 1-8 Dodawanie nowej domeny podrzędnej do istniejącego lasu

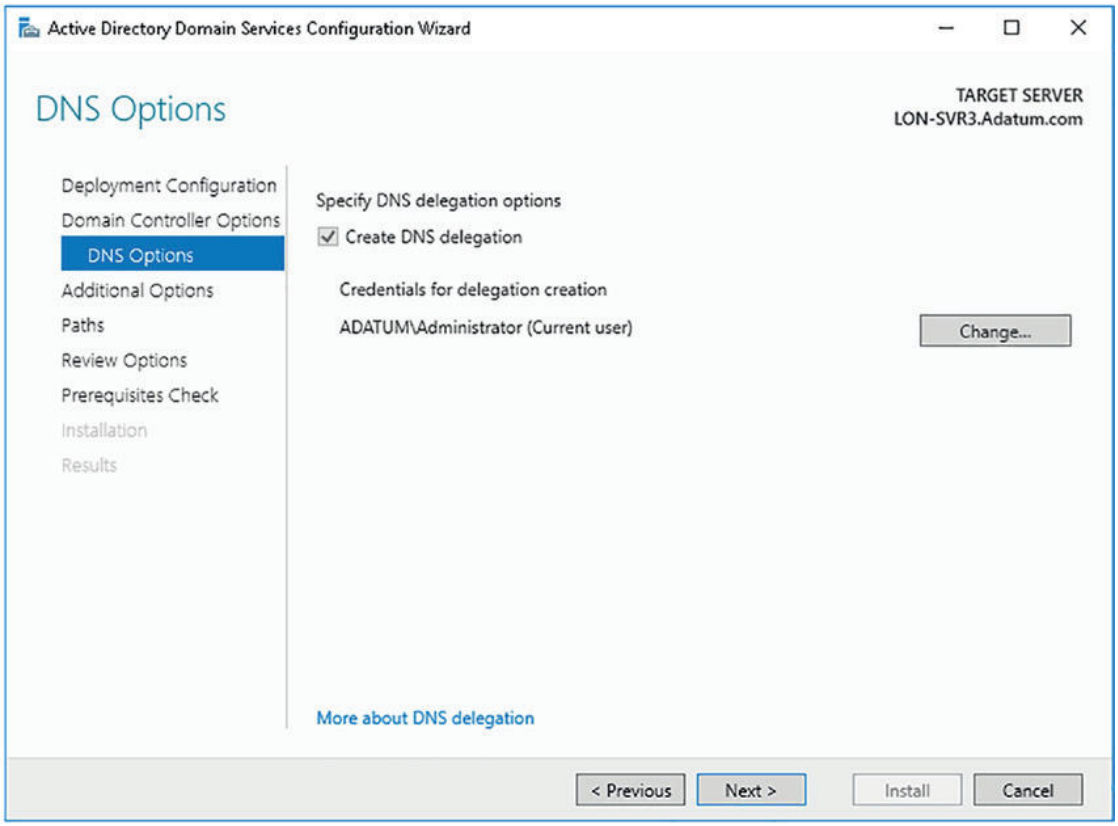
6. Na karcie Domain Controller Options wybierz poziom funkcjonalności domeny i skonfiguruj ustawienia DNS, GC i RODC. Wybierz odpowiednią nazwę lokacji, po czym wpisz hasło DSRM i kliknij Next.
7. Na karcie DNS, widocznej na rysunku 1-9, zaznacz opcję Create DNS Delegation (Utwórz delegowanie DNS). W ten sposób utworzysz delegację DNS dla subdomeny w swoim obszarze nazw DNS. Kliknij Next.

Dodatkowe materiały **Na czym polega delegowanie strefy**

Więcej informacji na temat delegacji DNS w systemie Windows Server znajdziesz w witrynie Microsoft TechNet, pod adresem *https://technet.microsoft.com/library/cc771640(v=ws.11).aspx*.

---

8. Podaj nazwę domeny NetBIOS, a następnie przejdź przez kolejne kroki kreatora. Gdy pojawi się przycisk Install, kliknij go.
9. Podczas procesu podnoszenia kontroler domeny zostanie ponownie uruchomiony. Po zakończeniu procesu zaloguj się jako administrator domeny.



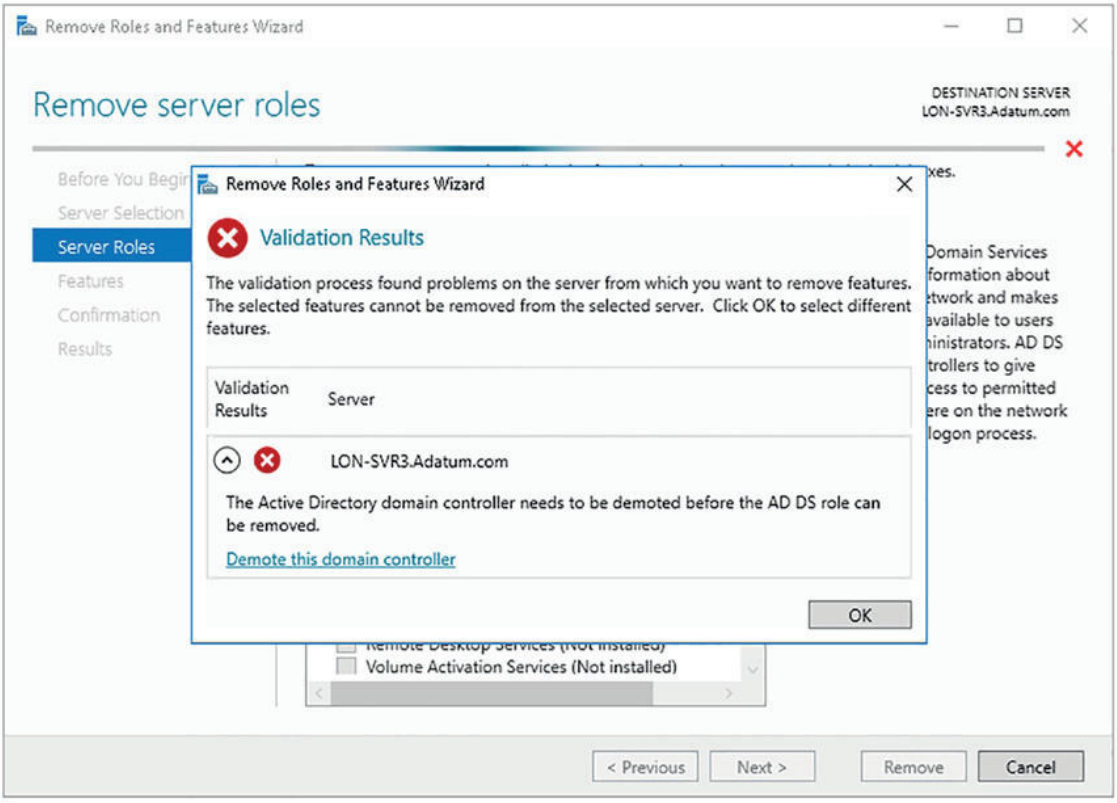
Rysunek 1-9 Dodawanie nowej domeny potomnej do istniejącego lasu

Usuwanie kontrolerów domeny

Od czasu do czasu należy wycofać z użytku i usunąć kontroler domeny. Jest to dość łatwy proces, który można wykonać za pomocą konsoli Server Manager.

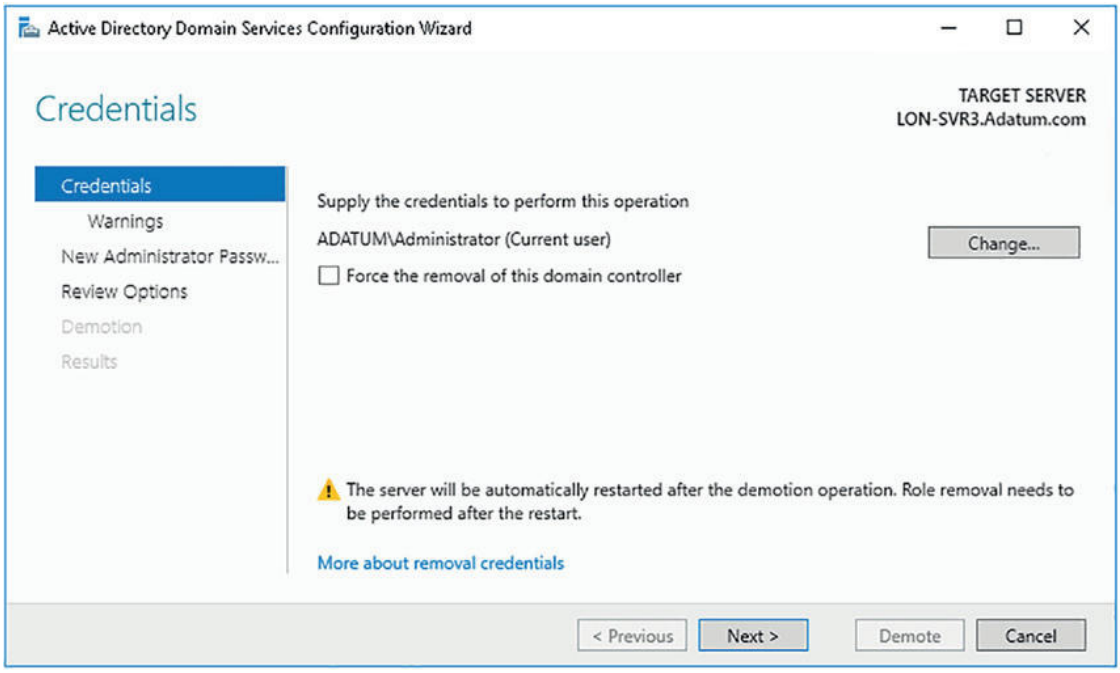
1. Zaloguj się za pomocą konta o wystarczających uprawnieniach. Aby usunąć kontroler domeny z domeny, zaloguj się jako administrator domeny. Aby usunąć całą domenę, zaloguj się jako członek uniwersalnej grupy zabezpieczeń Enterprise Admins.
2. Otwórz Server Manager i kliknij Remove Roles And Features (Usuń role i funkcje) w menu Manage (Zarządzaj).
3. W kreatorze Remove Roles And Features Wizard (Kreator usuwania ról i funkcji), na karcie Before You Begin (Zanim rozpoczniesz) kliknij Next.
4. Wybierz odpowiedni serwer na karcie Select Destination Server (Wybieranie serwera docelowego), a następnie kliknij Next.
5. Na karcie Remove Server Roles (Usuwanie ról serwera) usuń zaznaczenie opcji Active Directory Domain Services (Usługi domenowe w usłudze Active Directory), kliknij Remove Features (Usuń funkcje), a następnie kliknij Next.

6. W oknie dialogowym Validation Results (Wyniki sprawdzania poprawności), widocznym na rysunku 1-10, kliknij Demote This Domain Controller (Obniż poziom tego kontrolera domeny).

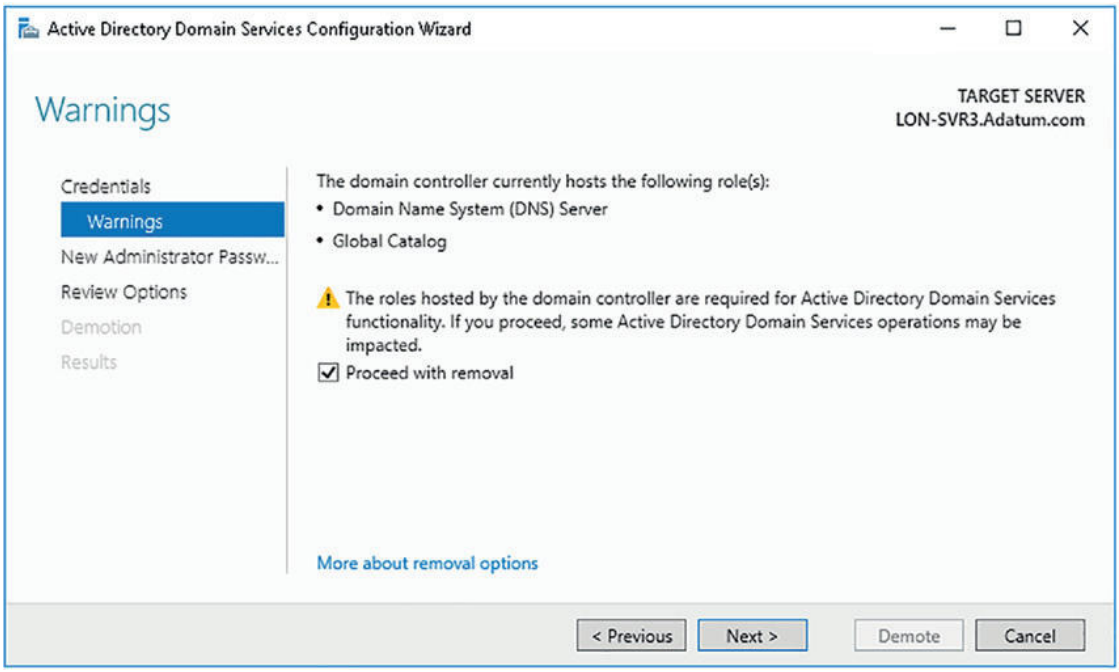


Rysunek 1-10 Usuwanie AD DS

7. Na ekranie zostanie wyświetlony kreator Active Directory Domain Services Configuration Wizard, widoczny na rysunku 1-11. Jeśli to konieczne, na karcie Credentials (Poświadczenia) podaj dane dostępowe użytkownika, który ma wystarczające uprawnienia do przeprowadzenia usunięcia. Nie zaznaczaj opcji Force The Removal Of This Domain Controller (Wymuś usunięcie tego kontrolera domeny), chyba że kontroler domeny uległ awarii i nie można się z nim połączyć. Kliknij Next.
8. Na karcie Warnings (Ostrzeżenia), widocznej na rysunku 1-12, zostaniesz poproszony o potwierdzenie usunięcia DNS i ról GC. Zaznacz opcję Proceed With Removal (Kontynuuj usuwanie) i kliknij Next.
9. W oknie New Administrator Password (Hasło nowego administratora) wpisz i potwierdź hasło lokalnego administratora, po czym kliknij Next.
10. Zweryfikuj swoją konfigurację i kliknij Demote (Obniż).
11. Poziom serwera zostanie obniżony, po czym serwer zostanie ponownie uruchomiony. Zaloguj się za pomocą konta lokalnego administratora.



Rysunek 1-11 Obniżanie poziomu kontrolera domeny



Rysunek 1-12 Usuwanie komponentów opcjonalnych

Teraz można zweryfikować powodzenie obniżenia poziomu i usunięcia roli. W kontrolerze domeny:

1. Otwórz konsolę Active Directory Users And Computers. Zweryfikuj, że kontroler domeny o obniżonym poziomie nie znajduje się już na liście kontrolerów domeny jednostki organizacyjnej.

2. Kliknij kontener Computers. Powinieneś ujrzeć komputer serwera o obniżonym poziomie.
3. Otwórz konsolę Active Directory Sites And Services (Lokacje i usługi Active Directory). Rozwiń katalog Sites, rozwiń Default-First-Site-Name, a następnie w sekcji Servers (Serwery) usuń obiekt reprezentujący serwer o obniżonym poziomie.

WSKAZÓWKA EGZAMINACYJNA

Jeśli serwer, który ma zostać wycofany z użytku, jest ostatnim kontrolerem domeny w domenie, musisz najpierw usunąć wszystkie pozostałe komputery z domeny, na przykład przenosząc je do innych domen w swoim lesie. Procedura wygląda wówczas tak jak opisano powyżej.

Poziom można też obniżyć za pomocą powłoki Windows PowerShell. W tym celu uruchom następujące dwa cmdlety w wierszu poleceń powłoki Windows PowerShell:

```
Uninstall-addsdomaincontroller

Uninstall-windowsfeature AD-Domain_Services
```

Dodatkowe materiały Obniżanie poziomu kontrolerów domeny

Więcej informacji na temat obniżania poziomu kontrolerów domeny znajdziesz w witrynie Microsoft TechNet, pod adresem *https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/deploy/demoting-domain-controllers-and-domains--level-200-*.

Instalowanie usługi AD DS w instancji Server Core

Rolę serwera AD DS można wdrożyć w instancji Server Core. Rolę tę można zainstalować zdalnie za pomocą konsoli Server Manager lub cmdletu `Install-WindowsFeature AD-Domain-Services` powłoki Windows PowerShell.

Po zainstalowaniu niezbędnych plików można uruchomić kreator Active Directory Domain Services Configuration Wizard za pomocą konsoli Server Manager, aby zdalnie skonfigurować instalację Server Core lub skorzystać z cmdletu `Install-ADDSDomainController` powłoki Windows PowerShell, aby ukończyć proces podnoszenia. Innymi słowy, proces instalowania AD DS w instancji Server Core systemu Windows Server 2016 jest taki sam jak na serwerze ze środowiskiem pulpitu.

WSKAZÓWKA EGZAMINACYJNA

Roli serwera AD DS nie można wdrożyć na serwerze Nano Server. Dlatego serwer Nano Server nie może służyć jako kontroler domeny.

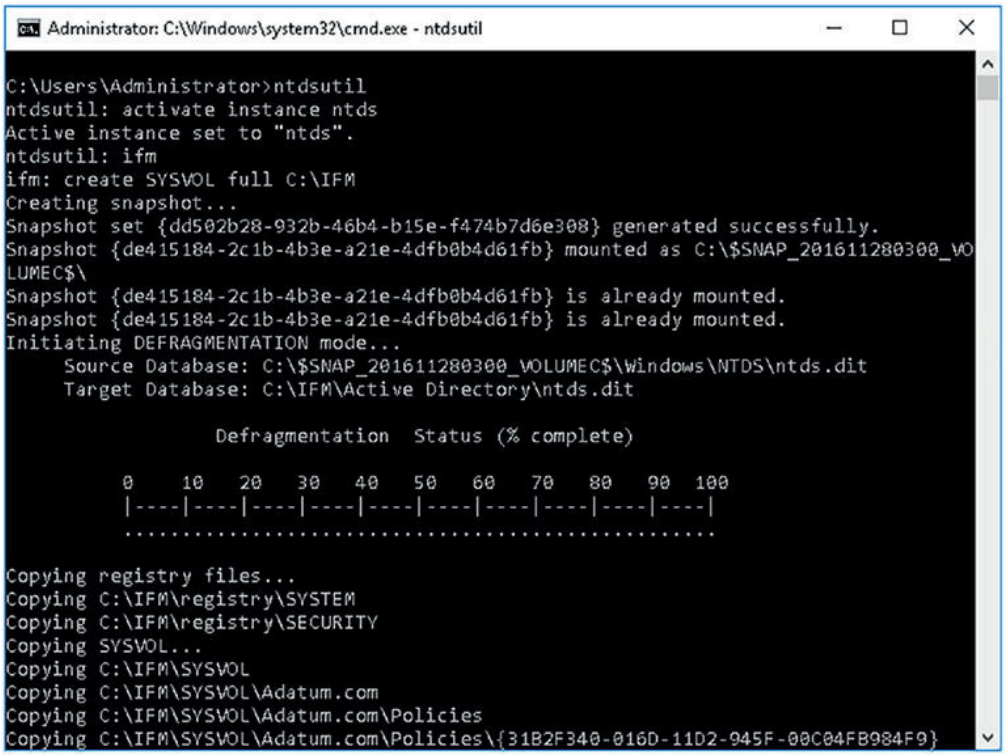
Instalowanie kontrolera domeny za pomocą funkcji Install from Media

Podczas wdrażania kontrolera domeny zawartość bazy danych AD DS jest replikowana do nowego kontrolera domeny. Ta replikacja obejmuje schemat, konfigurację partycji w całym lesie, a także odpowiednią partycję domeny. Po tej wstępnej synchronizacji replikacja między kontrolerami domeny odbywa się w zwykły sposób.

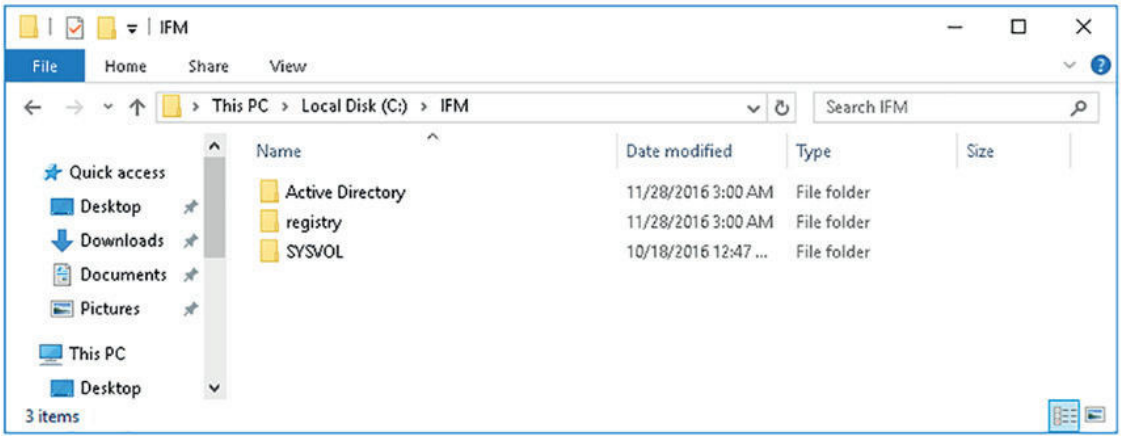
W pewnych sytuacjach początkowa synchronizacja może stanowić wyzwanie, na przykład podczas wdrażania kontrolera domeny w lokacji, która jest połączona z infrastrukturą sieciową organizacji za pomocą łącza o niskiej przepustowości. W tej sytuacji początkowa synchronizacja może trwać bardzo długo lub może wykorzystać nadmierną część dostępnej przepustowości.

Aby temu zaradzić, można się zdecydować na wdrożenie kontrolera domeny i przeprowadzenie wstępnej synchronizacji AD DS za pomocą lokalnej kopii lub migawki bazy danych AD DS; ta procedura nosi nazwę Install from Media (IFM) (Instalowanie z nośnika). Ten proces składa się z następujących kroków.

1. W eksploratorze plików w istniejącym kontrolerze domeny utwórz nowy folder, na przykład C:\IFM, w którym zostanie zapisana migawka AD DS.
2. Otwórz wiersz poleceń z podwyższonym poziomem uprawnień i wykonaj polecenie `ntdsutil.exe`.
3. W wierszu poleceń ntdsutil: wpisz **Activate instance ntds**, a następnie naciśnij Enter.
4. W wierszu poleceń ntdsutil: wpisz **ifm**, a następnie naciśnij Enter.
5. W wierszu poleceń ifm:, widocznym na rysunku 1-13, wpisz **create SYSVOL full C:\IFM**, a następnie naciśnij Enter.
6. W wierszu poleceń ifm: wpisz **quit**, a następnie naciśnij Enter.
7. W wierszu poleceń ntdsutil: wpisz **quit**, a następnie naciśnij Enter.
8. Zamknij wiersz poleceń.
9. Za pomocą eksploratora plików skopiuj zawartość foldera C:\IFM, widoczną na rysunku 1-14, do magazynu wymiennego, na przykład do nośnika USB.



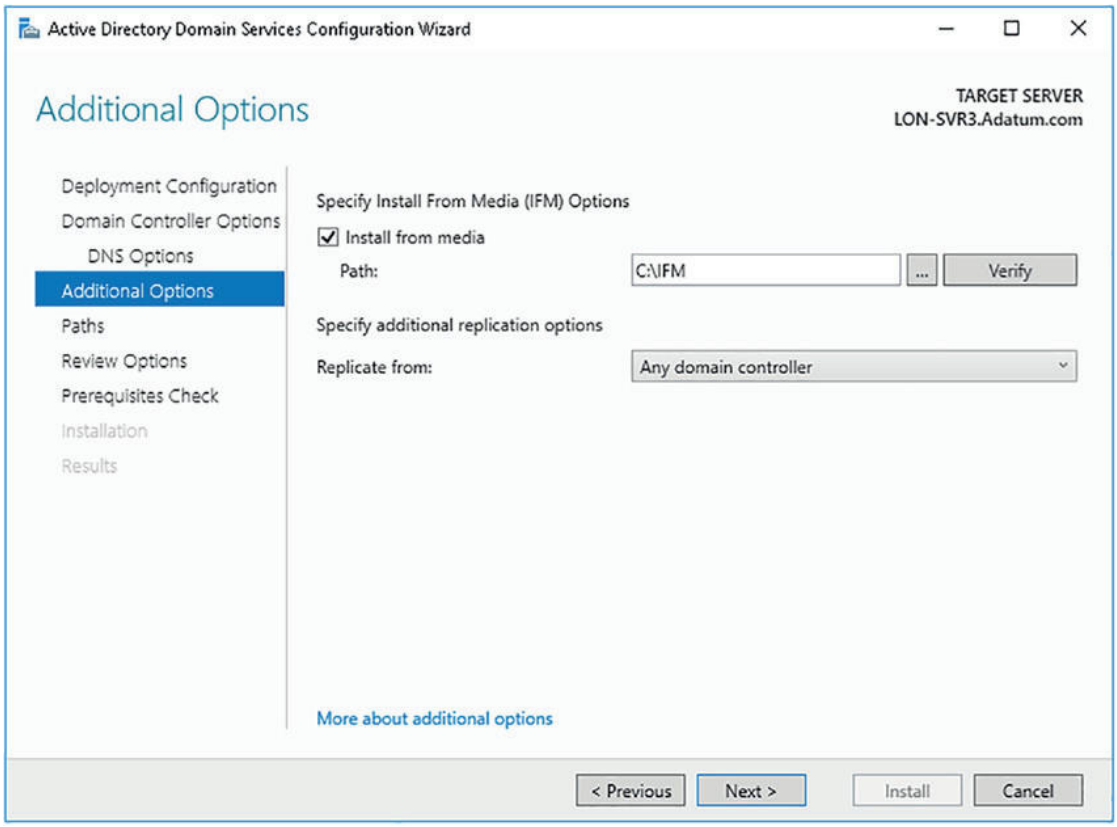
Rysunek 1-13 Tworzenie migawki NTDS w celu wdrożenia IFM



Rysunek 1-14 Foldery przeznaczone do przechowywania migawki AD DS

10. Na komputerze, który chcesz podnieść do poziomu kontrolera domeny, zainstaluj w zwykły sposób rolę serwera Active Directory Domain Services, korzystając z konsoli Server Manager lub powłoki Windows PowerShell.
11. Podłącz nośnik pamięci zawierający migawkę AD DS lub skopiuj pliki migawki, aby były dostępne na docelowym komputerze, a następnie uruchom kreator Active Directory Domain Services Configuration Wizard za pomocą konsoli Server Manager i przejdź przez kolejne kroki kreatora.

12. Na karcie Additional Options, widocznej na rysunku 1-15, zaznacz opcję Install From Media. W polu Path wpisz ścieżkę do lokalnej kopii migawki AD DS, kliknij Verify (Weryfikuj), a następnie kliknij Next.



Rysunek 1-15 Wybór opcji Install From Media

13. Przejdź przez kolejne kroki kreatora, sprawdź konfigurację i gdy przycisk Install będzie dostępny, kliknij go. Podczas procesu podnoszenia serwer zostanie uruchomiony ponownie.
14. Zaloguj się jako administrator domeny.

Kontroler domeny zostanie zreplikowany w zwykły sposób, wraz z innymi kontrolerami domeny w lesie. Jeśli chcesz, można zdefiniować lokację AD DS, do której należy kontroler domeny, a następnie skonfigurować dla niej harmonogram replikacji. Te procedury są omówione w rozdziale 2, „Zarządzanie i utrzymywanie usługi AD DS", w zagadnieniu 2.3: *Konfiguracja usługi Active Directory w złożonym środowisku przedsiębiorstwa*.

WSKAZÓWKA EGZAMINACYJNA

Wdrożenie można też wykonać za pomocą powłoki Windows PowerShell, korzystając z polecenia `Install-ADDSDomaincontroller -InstallationMediaPath x:\ifm`, służącego do podniesienia poziomu serwera.

Instalowanie i konfigurowanie kontrolera domeny tylko do odczytu

RODC jest kontrolerem domeny, zawierającym kopię AD DS tylko do odczytu. Kontrolery RODC umożliwiają wdrażanie kontrolerów domeny w biurach, w których nie można zagwarantować fizycznych zabezpieczeń. Biuro oddziału może na przykład wymagać obecności lokalnego kontrolera domeny, ale jednocześnie może nie dysponować zabezpieczonym pomieszczeniem na komputery, w którym można go umieścić.

Chociaż kontrolery RODC zapewniają kilka korzyści administracyjnych, to zanim je wdrożymy, powinniśmy uwzględnić następujące czynniki:

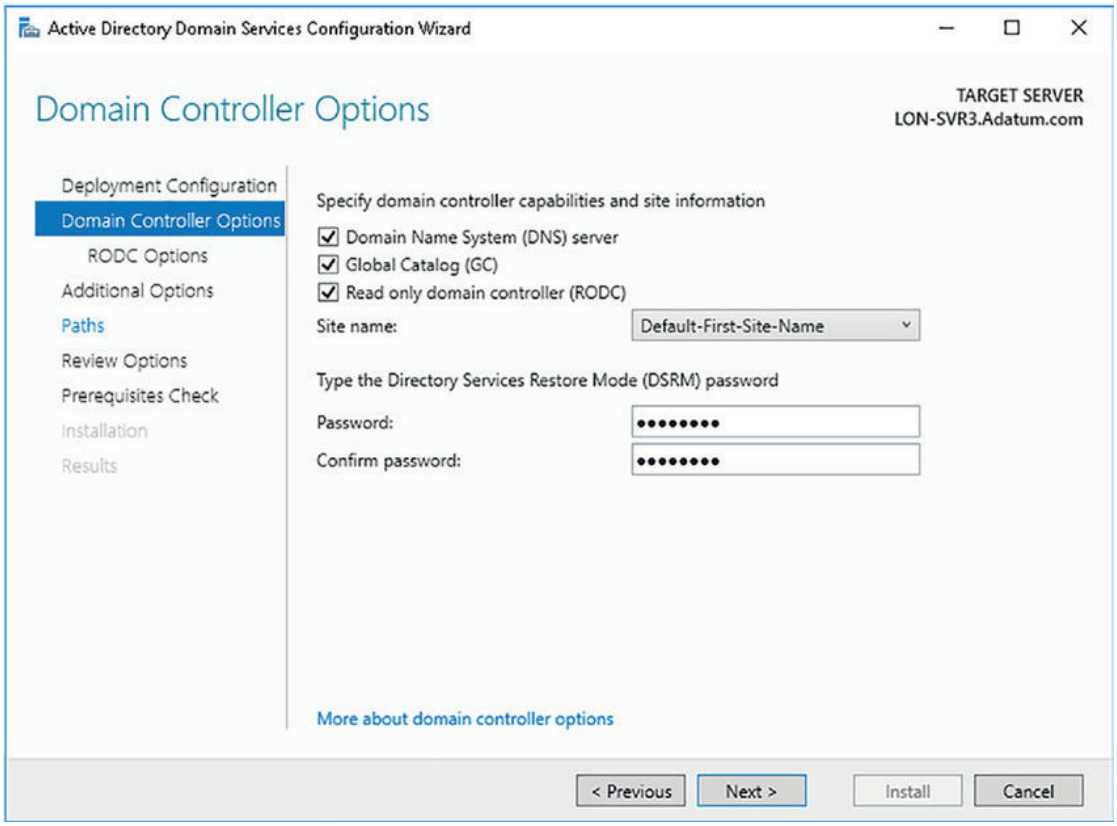
- W danej witrynie i domenie należy wdrożyć tylko jeden kontroler RODC. Jeśli wdrożymy w jednej witrynie kilka kontrolerów RODC, zapisywanie w pamięci podręcznej może się okazać niespójne, prowadząc do potencjalnych problemów z zalogowaniem się użytkownika i komputera.
- Wraz z rolą RODC można zainstalować rolę serwera DNS. Lokalni klienci mogą korzystać z zainstalowanej roli DNS tak samo jak z dowolnej innej instancji DNS w obrębie organizacji, z jednym wyjątkiem: aktualizacji dynamicznych. Ponieważ informacja o strefie DNS jest tylko do odczytu, klienci nie mogą dokonywać aktualizacji dynamicznych w instancji kontrolera RODC strefy DNS. W tej sytuacji RODC udostępnia klientom nazwę kontrolera domeny z możliwością zapisu, którego klient może użyć do uaktualnienia swoich rekordów.
- RODC nie może wykonywać następujących funkcji AD DS:
  - **Role wzorca operacji** Role wzorca operacji muszą mieć możliwość zapisu bazy danych AD DS. W rezultacie, RODC nie może przechowywać żadnej z pięciu ról wzorca operacji. Role wzorca operacji są omówione w dalszej części tego zagadnienia.
  - **Serwery czołowe replikacji AD DS** Ponieważ serwery czołowe są odpowiedzialne za replikację AD DS, muszą wspierać zarówno przychodzącą, jak i wychodzącą replikację AD DS. Kontrolery RODC wspierają tylko replikację przychodzącą, stąd nie mogą służyć jako serwery czołowe replikacji AD DS.
- Kontrolery RODC nie mogą:
  - **Uwierzytelniać w obrębie relacji zaufania, gdy połączenie WAN jest niedostępne** Jeśli biuro oddziału hostuje użytkowników z kilku domen lasu AD DS, użytkownicy i komputery z domeny, której RODC nie jest członkiem, nie mogą dokonać uwierzytelnienia, gdy połączenie WAN nie jest dostępne. Wynika to z tego, że RODC zapisuje w pamięci podręcznej dane dostępowe tylko dla kont domeny, których jest członkiem.
  - **Wspierać aplikacji, które wymagają stałej interakcji z AD DS** Niektóre aplikacje, takie jak Microsoft Exchange Server, wymagają interakcji AD DS. RODC

nie może wspierać wymaganej interaktywności, dlatego w tych lokalizacjach, które także hostują serwery Exchange Server, należy wdrożyć kontrolery domeny z możliwością zapisu.

Wdrażanie kontrolera RODC

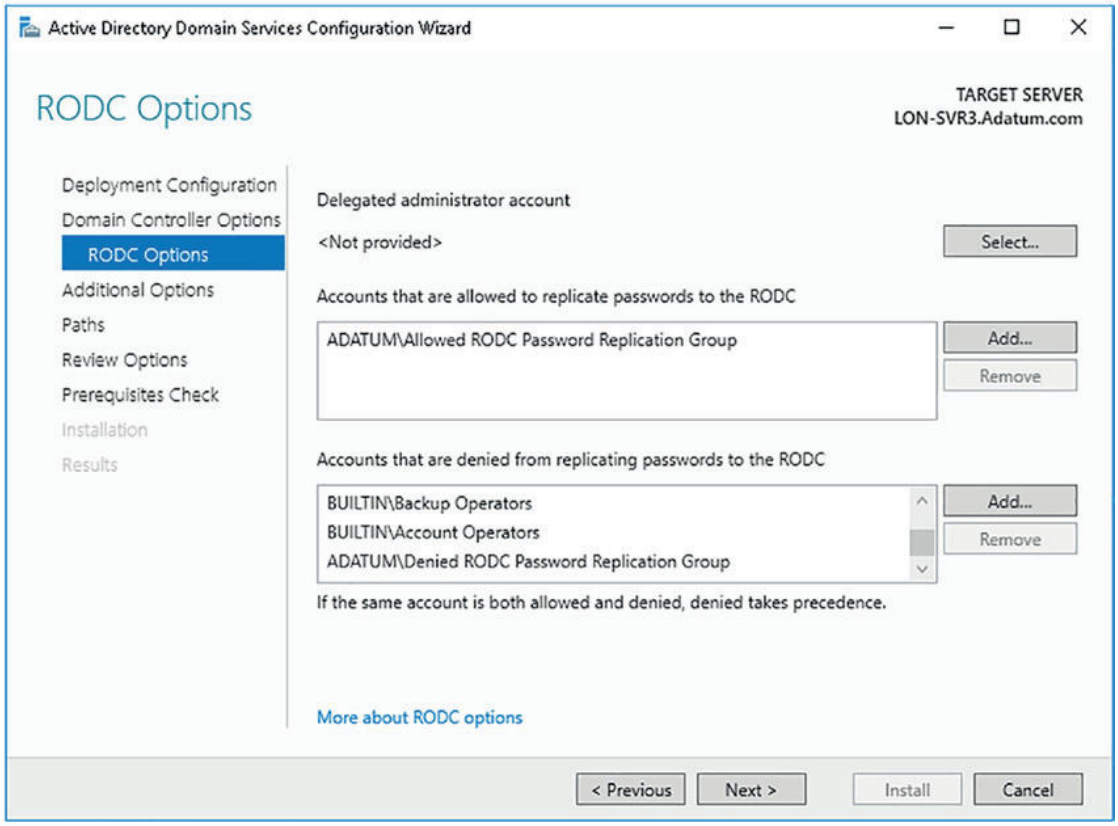
Przed wdrożeniem kontrolera RODC trzeba zagwarantować, że w organizacji istnieje co najmniej jeden zapisywalny kontroler domeny. Kontrolery RODC wdraża się zasadniczo tak samo jak inne kontrolery domeny:

1. Zainstaluj rolę serwera Active Directory Domain Services na komputerze serwera, który chcesz wdrożyć jako RODC.
2. Uruchom kreator Active Directory Domain Services Configuration Wizard, a następnie przejdź przez kolejne kroki.
3. Na karcie Domain Controller Options, widocznej na rysunku 1-16, zaznacz pole Read Only Domain Controller (RODC), a następnie skonfiguruj inne potrzebne opcje, po czym kliknij Next.



Rysunek 1-16 Instalowanie kontrolera RODC

4. Na karcie RODC Options (Opcje kontrolera RODC), widocznej na rysunku 1-17, skonfiguruj następujące opcje, po czym kliknij Next.



Rysunek 1-17 Konfiguracja opcji RODC

- **Delegated Administrator Account (Delegowane konto administratora)** Delegowany administrator lub administratorzy mogą prowadzić lokalną administrację kontrolera RODC bez posiadania równoważnych praw i uprawnień administratora domeny. Zwykle delegowany administrator RODC może wykonać następujące zadania:
  - Instalowanie i zarządzanie urządzeniami i nośnikami, dyskami twardymi i aktualizacjami
  - Zarządzanie usługą AD DS
  - Zarządzanie rolami i funkcjami serwera
  - Wyświetlanie dziennika zdarzeń
  - Zarządzanie udostępnionymi folderami, aplikacjami i usługami
- **Accounts That Are Allowed To Replicate Passwords To The RODC (Konta, które mogą replikować hasła do kontrolera RODC)** Domyślnie, kontroler RODC nie przechowuje wrażliwych informacji dotyczących hasła. Gdy użytkownik się zaloguje, RODC przekazuje żądanie logowania do kontrolera domeny z możliwością zapisu, znajdującego się gdzieś w organizacji.

Można jednak ulepszyć używalność, konfigurując zapisywanie kont konkretnego użytkownika i komputera w pamięci podręcznej przez kontroler RODC, co umożliwi lokalne uwierzytelnianie. W tym celu należy zdefiniować zasadę replikacji hasła RODC. Ogólnie rzecz biorąc, do zasad replikacji można dodać jedynie użytkowników i komputery znajdujące się w tej samej lokacji, w której znajduje się kontroler RODC.

WSKAZÓWKA EGZAMINACYJNA

Kontrolery RODC przechowują jedynie podzbiór poświadczeń użytkownika i komputera. W rezultacie, jeśli RODC zostanie skradziony, naruszenie bezpieczeństwa zostanie ograniczone tylko do tych kont, które zostały zapisane w pamięci podręcznej. Dzięki temu można zredukować ryzyko naruszeń i problemów administracyjnych, ponieważ w tej sytuacji należy zresetować hasła tylko tych kont.

Domyślnie, jak przedstawiono na rysunku 1-17, opcja Allowed RODC Password Replication Group (Grupa z replikacją haseł na kontrolerach RODC) jest włączona. Po wdrożeniu RODC można dodać do tej grupy użytkowników i komputery.

WSKAZÓWKA EGZAMINACYJNA

Istnieje też grupa Denied RODC Password Replication Group (Grupa bez replikacji haseł na kontrolerach RODC). Poświadczeń jej członków nie można nigdy zapisać na kontrolerze RODC. Domyślnie ta grupa zawiera konta Domain Admins, Enterprise Admins i Group Policy Creator Owners.

- **Accounts That Are Denied From Replicating Passwords To The RODC (Konta, które nie mogą replikować haseł do kontrolera RODC)** Domyślnie zaznaczona jest opcja Denied RODC Password Replication Group. Po wdrożeniu RODC można dodać do tej grupy użytkowników i komputery. Zabroniona jest też replikacja haseł następujących grup lokalnych: Administrators, Server Operators (Operatorzy serwerów), Backup Operators (Operatorzy kopii zapasowych) i Account Operators (Operatorzy kont).

WSKAZÓWKA EGZAMINACYJNA

Grupy Allowed RODC Password Replication Group i Denied RODC Password Replication Group umożliwiają konfigurację zasad replikacji haseł na wszystkich kontrolerach RODC. Jednakże, jeśli istnieje wiele biur oddziałów – a tym samym wiele kontrolerów RODC – bezpieczniej jest skonfigurować oddzielną grupę dla każdego kontrolera RODC na potrzeby dozwolonej replikacji haseł. W tej sytuacji usuń grupę Allowed RODC Password Replication Group i dodaj grupę, którą utworzyłeś ręcznie, a następnie dodaj wymaganych pracowników tego oddziału.

5. Przejdź przez kolejne kroki kreatora, sprawdź wybrane opcje, a gdy przycisk Install będzie dostępny, kliknij go. Podczas procesu podnoszenia poziomu serwer zostanie ponownie uruchomiony.

WSKAZÓWKA EGZAMINACYJNA

RODC można zainstalować za pomocą polecenia Install-ADDSDomainController –ReadOnlyReplica w powłoce Windows PowerShell.

Po wdrożeniu kontrolera RODC można zdefiniować członkostwa w grupach Allowed RODC Password Replication Group i Denied RODC Password Replication Group, aby skonfigurować zasady replikacji haseł do kontrolera RODC.

Konfigurowanie serwera wykazu globalnego

W lesie z pojedynczą domeną AD DS każdy kontroler domeny zawiera kopię wszystkich obiektów w lesie. Natomiast w przypadku lasów zawierających wiele domen jest inaczej. Chociaż wszystkie kontrolery domeny zawierają kopię partycji schematu i konfiguracji, to zawierają one tylko partycję domeny lokalnej. Stąd, jeśli aplikacja odpytuje kontroler domeny znajdujący się w domenie lokalnej o atrybuty obiektu znajdującego się w innej domenie, lokalny kontroler domeny nie może zwrócić odpowiedzi.

W tej sytuacji przydaje się wykaz globalny. Wykaz globalny jest częściową kopią tylko do odczytu wszystkich obiektów w lesie i hostuje podzbiór wszystkich atrybutów schematu konta AD DS. Wszystkie kontrolery domeny, które są skonfigurowane jako serwery wykazu globalnego, przechowują lokalnie kopię tej informacji. Dzięki temu można zwrócić odpowiedź na zapytanie o atrybuty obiektów, które znajdują się w innych domenach lasu – bez konieczności odpytywania kontrolera domeny w innej domenie.

WSKAZÓWKA EGZAMINACYJNA

W lesie zawierającym jedną domenę skonfiguruj wszystkie kontrolery domeny jako serwery wykazu globalnego. W lesie z wieloma domenami, o ile wszystkie kontrolery domeny nie są serwerami wykazu globalnego, nie można konfigurować wzorca infrastruktury jako serwera wykazu globalnego.

Kontroler domeny można skonfigurować jako serwer wykazu globalnego podczas jego wdrażania. W tym celu, w kreatorze Active Directory Domain Services Configuration Wizard, na karcie Domain Controller Options, widocznej na rysunku 1-16, należy zaznaczyć opcję Global Catalog (GC).

Natomiast po instalacji można skorzystać z narzędzia Active Directory Sites And Services (Lokacje i usługi Active Directory):