Microsoft®

Dan Holme,
Nelson i Danielle Ruest,
Jason Kellington

Egzamin MCTS 70-640:
Konfigurowanie Active Directory® w Windows Server® 2008 R2 *Training Kit*

Wydanie 2, uzupełnione i rozszerzone

Przekład: Leszek Biolik, Jakub Niedźwiedź

APN Promise
Warszawa 2011

Egzamin MCTS 70-640: Konfigurowanie Active Directory® w Windows Server® 2008 R2 Training Kit

Authorized Polish translation of English edition of
MCTS Self-Paced Training Kit (Exam 70-640): Configuring Windows Server® 2008 Active Directory®, Second Edition, ISBN: 978-0-7356-5193-7

APN PROMISE SA, ul. Kryniczna 2, 03-934 Warszawa
tel. +48 22 35 51 600, fax +48 22 35 51 699
e-mail: mspress@promise.pl

ISBN: 978-83-7541-089-1

Przekład: Leszek Biolik, Jakub Niedźwiedź,
Redakcja: Marek Włodarz
Korekta: Ewa Swędrowska
Skład i łamanie: MAWart Marek Włodarz

Spis treści

Wstęp

Ten zestaw szkoleniowy jest przeznaczony dla specjalistów technologii informatycznych (IT), którzy zamierzają obsługiwać usługi domenowe AD – (Active Directory) w systemie Microsoft Windows Server 2008 R2 i którzy również planują przystąpienie do egzaminu Microsoft Certified Technology Specialist (MCTS) 70-640. Zakładamy, że przed rozpoczęciem korzystania z tego zestawu Czytelnik ma solidną wiedzę podstawową dotyczącą klienckich i serwerowych systemów operacyjnych Microsoft Windows oraz powszechnie stosowanych technologii internetowych. Egzamin MCTS i ta książka zakładają co najmniej roczne doświadczenie w administrowaniu technologiami AD.

Materiał obejmowany przez ten zestaw szkoleniowy i wymagany na egzaminie 70-640 bazuje na doświadczeniu i wiedzy, pomagając w implementowaniu technologii AD w rozproszonych środowiskach, które mogą zawierać złożone usługi sieciowe i składać się z wielu lokacji i kontrolerów domeny. Tematyka niniejszego zestawu szkoleniowego obejmuje zagadnienia potrzebne do zdania egzaminu zgodnie z opisem zamieszczonym na karcie Skills Measured, dostępnej pod adresem: *http://www.microsoft.com/learning/en/us/exam.aspx?ID=70-640&locale=en-us#tab2*. Korzystając z tego zestawu szkoleniowego nauczymy się, jak:

- Wdrażać role Active Directory Domain Services (Usługi domenowe w usłudze Active Directory), Active Directory Lightweight Directory Services (Usługi LDS w usłudze Active Directory), Active Directory Certificate Services (Usługi certyfikatów w usłudze Active Directory), Active Directory Federation Services oraz Active Directory Rights Management Services (Usługi zarządzania prawami dostępu w usłudze Active Directory) w lesie lub domenie.
- Aktualizować istniejące kontrolery domeny, domeny i lasy do systemu Windows Server 2008 R2.
- Efektywnie administrować i automatyzować administrację użytkownikami, grupami i komputerami.
- Zarządzać konfiguracją i zabezpieczeniami domeny przy użyciu zasad grupy, szczegółowych zasad haseł, inspekcji usług katalogowych i narzędzia Security Configuration Wizard (Kreator konfiguracji zabezpieczeń).
- Implementować efektywne rozwiązywanie nazw przy użyciu Domain Name System (DNS) w systemie Windows Server 2008 R2.
- Planować, konfigurować i obsługiwać replikację danych Active Directory wewnątrz i pomiędzy lokacjami.
- Dodawać, usuwać, utrzymywać i tworzyć kopie zapasowe kontrolerów domeny.
- Włączać uwierzytelnianie pomiędzy domenami i lasami.
- Implementować nowe możliwości i funkcjonalność oferowane przez system Windows Server 2008 R2.

Na początku książki zamieszczono spis celów egzaminacyjnych, gdzie można dowiedzieć się, w którym miejscu książki omawiane są poszczególne tematy.

Wymagania systemowe

Ćwiczenia praktyczne są cennym składnikiem tego zestawu szkoleniowego. Umożliwiają nam bezpośrednie wypróbowanie ważnych umiejętności, utrwalają materiał omówiony w lekcjach, a nawet wprowadzają nowe pojęcia. W każdej lekcji podane są wymagania dla danego zestawu ćwiczeń. Chociaż wiele lekcji wymaga tylko jednego komputera skonfigurowanego jako kontroler domeny dla przykładowej domeny o nazwie *contoso.com*, to niektóre lekcje wymagają dodatkowych komputerów działających jako drugi kontroler domeny, jako kontroler domeny w innej domenie w tym samym lesie, jako kontroler domeny w innym lesie albo jako serwer spełniający inne role.

Rozdziały omawiające usługi AD DS (rozdziały 1–13) wymagają co najwyżej trzech maszyn działających jednocześnie. Rozdziały omawiające inne role Active Directory wymagają nawet do siedmiu maszyn działających równocześnie w celu zapewnienia rozbudowanego środowiska dla danej technologii.

Rozdział 1 „Tworzenie domeny usługi Active Directory" zawiera instrukcje instalowania pierwszego kontrolera domeny w domenie *contoso.com*, który będzie wykorzystywany w całym zestawie szkoleniowym. Lekcje, które wymagają dodatkowego komputera, zawierają wskazówki dotyczące konfiguracji tego komputera.

Wymagania sprzętowe

Ćwiczenia można przeprowadzać przy użyciu komputerów fizycznych. Każdy komputer musi spełniać minimalne wymagania sprzętowe dla system Windows Server 2008 R2, zgodnie ze specyfikacją dostępną pod adresem *http://www.microsoft.com/windowsserver2008/en/us/system-requirements.aspx*. System Windows Server 2008 R2 dobrze działa przy 512 MB pamięci w niewielkich środowiskach, takich jak przykładowa domena contoso.com. Jednak przy wykorzystywaniu innych technologii AD, takich jak AD Rights Management Services, AD Certificate Services czy AD Federation Services, komputery powinny być budowane w oparciu o co najmniej 1024 MB pamięci RAM. W przypadku większości rozdziałów wystarczająca będzie wersja systemu Windows Server 2008 R2 Standard, jednak w ostatnich rozdziałach wymagane będzie zastosowanie wersji Enterprise i z tego względu podczas konfigurowania serwerów w rozdziałach 14-17 zalecamy instalowanie wersji Enterprise.

Zaleca się korzystanie z maszyn wirtualnych zamiast komputerów fizycznych do pracy z lekcjami i ćwiczeniami. W ten sposób można ograniczyć czas i koszty konfigurowania komputerów fizycznych. Zaleca się budowanie maszyn wirtualnych przy użyciu oprogramowania Hyper-V, w które wyposażone są systemy Windows Server 2008 i Windows Server 2008 R2 lub innego oprogramowania do wirtualizacji, jak na przykład VMware Workstation czy Oracle VirtualBox. Warto pamiętać, że chociaż opisy w książce odnoszą się do kilku komputerów, jednocześnie nigdy nie będziemy używać więcej niż czterech maszyn. Wymagania sprzętowe i programowe, instrukcje konfigurowania hostów i procedury tworzenia maszyn wirtualnych dla systemu Windows Server 2008 R2 znaleźć można w dokumentacji wybranej platformy wirtualizacji.

Wybierając stosowanie oprogramowania wirtualizacji na komputerze-hoście możemy uruchamiać kilka maszyn wirtualnych. Każdej maszynie wirtualnej należy przydzielić co najmniej 512 MB lub 1024 MB pamięci RAM i każda z maszyn musi spełniać minimalne

wymagania dotyczące procesora i pamięci dyskowej, które odnoszą się do systemu Windows Server 2008 R2. Komputer-host musi mieć wystarczającą ilość pamięci RAM dla wszystkich maszyn wirtualnych jednocześnie uruchomionych na hoście. Jeśli zamierzamy uruchamiać wszystkie maszyny wirtualne na pojedynczym hoście, komputer-host musi mieć co najmniej 4.0 GB pamięci RAM. Na przykład, jedna z najbardziej złożonych konfiguracji używanych w ćwiczeniach zawiera dwa kontrolery domen, gdzie każdy z nich wykorzystuje 512 MB pamięci RAM oraz dwa serwery członkowskie, z których każdy używa 1024 MB pamięci RAM. W takim przypadku na komputerze-hoście z zainstalowaną pamięcią 4 GB dla hosta pozostanie 1 GB pamięci. Warto także pamiętać, że ilekroć uruchamiamy komputer w oparciu o wersję Enterprise systemu Windows Server 2008 R2, maszynie takiej należy przydzielać 1024 MB pamięci RAM.

Jeśli podczas uruchamiania kilku maszyn wirtualnych na jednym hoście fizycznym pojawią się problem dotyczące wydajności, warto rozważyć uruchamianie tych maszyn wirtualnych na dwóch lub większej liczbie hostów fizycznych.

Należy zapewnić, aby wszystkie maszyny wirtualne mogły się komunikować ze sobą przez sieć. Zaleca się, aby to środowisko było zupełnie odłączone od środowiska produkcyjnego. Opis procedur konfiguracji sieci znaleźć można w dokumentacji wybranej platformy wirtualizacji.

Autorzy zalecają zachowanie każdej z tworzonych maszyn wirtualnych aż do zakończenia pracy z tym zestawem szkoleniowym. Po każdym rozdziale należy utworzyć kopię zapasową maszyn wirtualnych używanych w tym rozdziale, aby można było ponownie skorzystać z nich w późniejszych ćwiczeniach.

Na koniec potrzebny będzie komputer fizyczny wyposażony w napęd CD-ROM, by możliwe było odczytanie dołączonego do książki nośnika.

Wymagania programowe

Trzeba mieć egzemplarz systemu Windows Server 2008 R2 wraz z dodatkiem SP1, aby wykonywać ćwiczenia w tym zestawie szkoleniowym.

Wersje ewaluacyjne systemu Windows Server 2008 R2 można pobrać z witryny TechNet Evaluation Center dostępnej pod adresem *http://technet.microsoft.com/evalcenter*. Korzystając z wersji testowej oprogramowania trzeba zwrócić uwagę na datę ważności produktu. Przykładowo, wersja testowa systemu Windows Server 2008 R2 z dodatkiem SP1może być używana przez 60 dni, chociaż można ten okres wydłużyć do 180 dni poprzez trzykrotne zerowanie tego okresu.

Jeśli posiadamy subskrypcję TechNet lub MSDN, możemy pobrać produkty z odpowiedniej witryny. Te wersje nie tracą okresu ważności, dlatego też warto stać się subskrybentem usług TechNet czy MSDN i wykorzystywać zalety oferowanych tam produktów.

Jeśli instalujemy systemy Windows Server 2008 R2 na komputerze fizycznym, potrzebne będzie nam oprogramowanie i sprzęt, które umożliwiają nagranie na dysku DVD pobranego pliku .iso.

W celu skorzystania z dysku CD dołączonego do książki potrzebna będzie przeglądarka internetowa (na przykład Internet Explorer 8) oraz aplikacja wyświetlająca pliki PDF (na przykład program Adobe Acrobat, który można pobrać pod adresem *http://www.adobe.com*).

Korzystanie z obrazu dysku CD

Obraz dysku CD towarzyszącego książce jest dostępny na stronie wydawcy przy opisie książki w zakładce Dodatkowe informacje, pod adresem:

http://www.ksiazki.promise.pl/aspx/produkt.aspx?pid=57992

Na podstawie tego obrazu można wykonać fizyczny dysk CD lub zainstalować go jako napęd wirtualny. Dysk ten zawiera:

- **Testy ćwiczeniowe** Lepsze poznanie omawianych w książce tematów można uzyskać poprzez korzystanie z elektronicznych testów ćwiczeniowych, które dostosowujemy do swoich potrzeb na podstawie pytań do lekcji zamieszczonych w tej książce. Alternatywnie można przygotowywać się do egzaminu certyfikacyjnego 70-640 korzystając z testów tworzonych na bazie 200 realistycznych pytań egzaminacyjnych, co daje możliwość przeprowadzenia wielu próbnych egzaminów w celu zapewnienia sobie odpowiedniego przygotowania do egzaminu.
- **Źródła dodatkowe** Na dysku CD znaleźć można bezpośrednie łącza do dodatkowych źródeł i informacji, do których w książce zamieszczono odniesienia i które są uzupełnieniem opisywanej tematyki.

Jak zainstalować testy ćwiczeniowe

Aby zainstalować na twardym dysku oprogramowanie do testów ćwiczeniowych z dołączonej płyty CD, należy wykonać następujące operacje:

1. Włożyć dołączoną płytę CD do napędu i zaakceptować umowę licencyjną. Pojawi się menu płyty CD.

> **Uwaga Jeśli menu płyty CD się nie pojawi**
>
> Jeśli nie pojawi się menu płyty CD lub umowa licencyjna, to na komputerze może być wyłączona funkcja AutoRun (Autouruchamianie). Należy zajrzeć do pliku Readme.txt na płycie CD-ROM, aby uzyskać alternatywne instrukcje instalacyjne.

2. Należy kliknąć opcję Practice Tests i wykonać instrukcje pojawiające się na ekranie.

Jak korzystać z testów ćwiczeniowych

Aby uruchomić oprogramowanie do testów ćwiczeniowych, należy:

1. Kliknąć opcję Start\All Programs\Microsoft Press Training Kit Exam Prep.
   Pojawi się okno pokazujące wszystkie pakiety przygotowujące do egzaminów z zestawów szkoleniowych Microsoft Press zainstalowanych na komputerze.
2. Podwójnie kliknąć podsumowanie lekcji lub test ćwiczeniowy, z którego chcemy skorzystać.

Uwaga Pytania do lekcji a testy ćwiczeniowe

Należy wybrać opcję (70-640) TS: Configuring Windows Server 2008 Active Directory *lesson review*, aby użyć pytań z działów „Pytania do lekcji" z tej książki. Należy wybrać opcję (70-640) TS: Configuring Windows Server 2008 Active Directory *practice test*, aby skorzystać z puli 200 pytań podobnych do tych, które pojawiają się na egzaminie certyfikacyjnym 70-640.

Opcje pytań do lekcji

Po uruchomieniu opcji pytań do lekcji pojawia się okno dialogowe Custom Mode, w którym można skonfigurować swój test. Można kliknąć OK, aby przyjąć domyślne ustawienia, albo można dostosować liczbę pytań w teście, sposób działania oprogramowania do testów, cele egzaminacyjne, z którymi mają być związane pytania, oraz określić, czy podczas testu ma być mierzony czas. Podczas ponownego przystępowania do testu można wybrać, czy mają pojawiać się ponownie wszystkie pytania, czy tylko pytania pominięte wcześniej lub takie, na które nie udzielono odpowiedzi.

Po kliknięciu OK rozpocznie się test na bazie pytań do lekcji.

- Aby rozwiązać test, należy odpowiadać na pytania i używać przycisków Next oraz Previous do przechodzenia między pytaniami.
- Chcąc po udzieleniu odpowiedzi na dane pytanie sprawdzić poprawne odpowiedzi – razem z wyjaśnieniami do każdej poprawnej odpowiedzi – należy kliknąć Explanation.
- Aby zaczekać do końca testu ze sprawdzeniem swoich wyników, należy odpowiedzieć na wszystkie pytania, a następnie kliknąć Score Test. Pojawi się podsumowanie wybranych celów egzaminacyjnych i procent poprawnych odpowiedzi sumarycznie i w podziale na poszczególne cele. Można wydrukować kopię swojego testu, przejrzeć odpowiedzi lub ponownie przystąpić do testu.

Opcje testów ćwiczeniowych

Po uruchomieniu testu ćwiczeniowego można wybrać jeden z trybów testu: Certification Mode (tryb certyfikacji), Study Mode (tryb nauki) lub Custom Mode (tryb niestandardowy).

- **Certification Mode (tryb certyfikacji)** Bardzo zbliżony do zdawania prawdziwego egzaminu certyfikacyjnego. Test ma określoną liczbę pytań. Mierzony jest czas i nie można zatrzymywać ani wznawiać zegara.
- **Study Mode (tryb nauki)** Tworzy test bez pomiaru czasu, w którym można przeglądać poprawne odpowiedzi i wyjaśnienia do nich po udzieleniu odpowiedzi na każde pytanie.
- **Custom Mode (tryb niestandardowy)** Daje pełną kontrolę nad opcjami testu pozwalając je swobodnie dostosować do własnych potrzeb.

We wszystkich trybach interfejs użytkownika przy rozwiązywaniu testu jest w zasadzie taki sam, ale różne opcje są włączone lub wyłączone, w zależności od trybu. Główne opcje są omówione wcześniej, w części „Opcje pytań do lekcji".

Podczas przeglądania odpowiedzi na dane pytanie testu ćwiczeniowego dostępna jest sekcja „References" wyświetlająca listę odwołań do miejsc w tym zestawie szkoleniowym, w których można znaleźć informacje związane z danym pytaniem, oraz zapewniająca łącza

do innych źródeł informacji. Po kliknięciu opcji Test Results w celu podliczenia wyników całego testu ćwiczeniowego można kliknąć kartę Learning Plan, aby zobaczyć listę odwołań dla każdego celu egzaminacyjnego.

Jak odinstalować testy ćwiczeniowe

Aby odinstalować oprogramowanie do testów ćwiczeniowych dla tego zestawu szkoleniowego, należy użyć opcji Add Or Remove Programs (Dodaj lub usuń programy) w Windows XP albo opcji Programs And Features (Programy i funkcje) w Windows Vista lub Windows 7.

Podziękowania

Nazwiska autorów zamieszczone zostały na okładce książki, ale jesteśmy tylko częścią znacznie większego zespołu. Jeff Koch umożliwił nam aktualizację pierwszego wydania tego zestawu szkoleniowego i zrealizowanie tego projektu. Karen Szall i Rosemary Caperton, z którymi ściśle współpracowaliśmy, były jak zawsze wymarzonym zespołem! A każdy z redaktorów wykonał wspaniałą pracę, dzięki czemu ten zestaw szkoleniowy jest bardziej wartościowy. Kurt Meyer, będący naszym recenzentem technicznym, to osoba wyjątkowo przydatna i rzetelna. Jesteśmy bardzo wdzięczni całemu zespołowi i każdemu, czyj wysiłek pozwolił stać się temu zestawowi szkoleniowemu niezastąpionym źródłem informacji. Mamy nadzieję, że w przyszłości będziemy mogli z każdym z Was ponownie współpracować.

Wsparcie techniczne i kontakt z Czytelnikami

W kolejnych akapitach przedstawiono informacje na temat błędów, wsparcia technicznego i informacji kontaktowych.

Errata

Podjęto wszelkie starania w celu zapewnienia poprawności tej książki i zawartości dołączonej płyty CD. Wszelkie błędy dostrzeżone po opublikowaniu książki zamieszczone są na stronach Microsoft Press w witrynie oreilly.com:

http://go.microsoft.com/FWLink/?LinkiD=219768

Za pośrednictwem tej strony prosimy też o przesyłanie wszelkich błędów, które nie zostały jeszcze znalezione.

Jeśli zachodzi potrzeba uzyskania dodatkowego wsparcia, prosimy skontaktować się poprzez e-mail z działem Microsoft Press Book Support (mspinput@microsotf.com).

Prosimy zwrócić uwagę, że wsparcie dla produktu oprogramowania firmy Microsoft nie jest oferowane za pośrednictwem podanych powyżej adresów.

Pozostańmy w kontakcie

Warto stale rozmawiać! Jesteśmy dostępni na Twitterze pod adresem: *http://twitter.com/MicrosoftPress*

Przygotowanie do egzaminu

Certyfikaty Microsoft stanowią najlepszy sposób potwierdzenia opanowanych umiejętności i posiadanego doświadczenia w zakresie aktualnych produktów i technologii firmy Microsoft. Chociaż nic nie zastąpi doświadczeń zdobywanych poprzez pracę z produktami, przygotowanie poprzez naukę i proponowane ćwiczenia praktyczne ułatwia przygotowanie się do egzaminu. Zalecamy opracowanie planu przygotowywania się do egzaminu poprzez łączenie dostępnych materiałów i kursów. Na przykład, można zestaw szkoleniowy czy inny poradnik wykorzystywać do przygotowywania się „w domu" i brać udział w kursie Microsoft Official Curriculum, by nabyć doświadczeń na sali wykładowej. Wybierz połączenie, które Ci najbardziej odpowiada!

Microsoft®
CERTIFIED
Technology Specialist

Rozdział 1

Tworzenie domeny usługi Active Directory

Usługi Active Directory Domain Services (AD DS – Usługi domenowe w usłudze Active Directory) i powiązane z nimi usługi stanowią podstawę sieci korporacyjnych działających pod kontrolą systemu Microsoft Windows, ponieważ razem działają jako narzędzia do przechowywania informacji na temat tożsamości użytkowników, komputerów i usług; do uwierzytelniania użytkowników lub komputerów; oraz do zapewniania mechanizmu, dzięki któremu użytkownik lub komputer może uzyskać dostęp do zasobów firmowych. W tym rozdziale zaczniemy od zbadania usług Active Directory w systemie Windows Server 2008 R2 przez zainstalowanie roli Active Directory Domain Services i utworzenie kontrolera domeny w nowym lesie Active Directory. Odkryjemy, że system Windows Server 2008 R2 kontynuuje ewolucję usług Active Directory, rozszerzając wiele pojęć i funkcji, które mogą być znane z dotychczasowych doświadczeń w pracy z tymi usługami.

Ważne
Czy przeczytałeś stronę xxiii?

Strona zawiera ważne informacje dotyczące umiejętności potrzebnych do zdania egzaminu.

Ten rozdział skupia się na tworzeniu nowego lasu Active Directory z pojedynczą domeną na pojedynczym kontrolerze domeny. Ćwiczenia praktyczne w tym rozdziale poprowadzą nas przez tworzenie domeny o nazwie *contoso.com*, z której będziemy korzystać we wszystkich innych ćwiczeniach w tym zestawie szkoleniowym. Później, w dalszych rozdziałach poznamy inne scenariusze i implementacje kluczowych składników usług Active Directory zintegrowanych z AD DS.

Umiejętności prezentowane w tym rozdziale:

- Konfigurowanie lasu lub domeny.

Lekcje w tym rozdziale

Przed rozpoczęciem

Do ukończenia lekcji w tym rozdziale potrzebne będą:

- Dwa komputery, na których zainstalujemy system Windows Server 2008 R2. Komputery te mogą być systemami fizycznymi, które spełniają minimalne wymagania sprzętowe dla systemu Windows Server 2008 dostępne pod adresem *http://www.microsoft.com/windowsserver2008/en/us/system-requirements.aspx lub http://technet.microsoft.com/en-us/library/dd379511(WS.10).aspx*. Potrzebne będzie co najmniej 512 MB pamięci RAM, 32 GB wolnego miejsca na dysku twardym i procesor x64 z minimalną prędkością zegara 1,4 GHz. Ewentualnie można skorzystać z maszyn wirtualnych spełniających te same wymagania.
- Wersja ewaluacyjna systemu Windows Server 2008 R2. 180 dniowa wersja testowa systemu Windows Server 2008 R2 z dodatkiem SP1 dostępna jest pod adresem *http://www.microsoft.com/windowsserver2008/en/us/trial-software.aspx*.

Z praktyki

Jason Kellington

System Windows Server 2008 R2 obsługuje jedynie procesory x64 lub Itanium 2; nie są obsługiwane procesory o architekturze x86. Jeśli to wymaganie nie jest spełnione, system Windows Server 2008 R2 nie zainstaluje się. Informacja ta ma największe znaczenie podczas aktualizowania istniejących serwerów do system Windows Server 2008 R2. Istniejący serwer bazujący na procesorze x86 musi zostać zastąpiony sprzętem, który korzysta z procesora x64 lub Itanium 2.

W najbardziej typowych scenariuszach instalacji usług AD DS serwer działa jako kontroler domeny, który utrzymuje kopię bazy danych usług AD DS i replikuje tę bazę danych do innych kontrolerów domen. Kontrolery domeny są najbardziej krytycznym składnikiem infrastruktury usług Active Directory i powinny funkcjonować przy możliwie niewielkiej liczbie zainstalowanych dodatkowych składników, które nie są powiązane z usługami AD. Taka dedykowana konfiguracja zapewnia bardziej stabilną i niezawodną pracę kontrolerów domen, ponieważ ograniczone są w ten sposób możliwości wpływu innych aplikacji czy usług na składniki usług AD DS uruchomionych na kontrolerze domeny.

W wersjach systemu Windows Server wcześniejszych niż system Windows Server 2008, administratorzy serwera musieli wybierać i konfigurować poszczególne składniki serwera, by zapewnić, że nieistotne składniki systemu Windows są wyłączone lub odinstalowane. W systemie Windows Server 2008 kluczowe składniki zostały podzielone na grupy powiązane ze sobą funkcjonalnie, nazywane rolami. Administracja, opierająca się na rolach, pozwala administratorowi po prostu wybrać rolę lub role, które serwer powinien spełniać. Następnie system Windows Server 2008 zainstaluje odpowiednie składniki systemu Windows, które umożliwiają funkcjonowanie tych ról. Administracja oparta na rolach zostanie przybliżona podczas wykonywania ćwiczeń praktycznych zamieszczonych w książce.

Lekcja 1: Instalowanie usług Active Directory Domain Services

Usługi AD DS – Active Directory Domain Services (Usługi domenowe w usłudze Active Directory) zapewniają funkcjonalność zarządzania tożsamością i dostępem (IDA) w sieciach firmowych. W trakcie tej lekcji poznamy usługi AD DS i inne role Active Directory obsługiwane przez system Windows Server 2008. Zbadamy też narzędzie Server Manager (Menedżer serwera), za pomocą którego możemy konfigurować role serwera oraz ulepszonego kreatora instalacji usług Active Directory Domain Services. W tej lekcji przejrzymy też kluczowe pojęcia IDA i Active Directory.

Po ukończeniu tej lekcji Czytelnik będzie umiał:

- Wyjaśnić rolę tożsamości i dostępu w sieci firmowej.
- Zrozumieć relacje pomiędzy usługami Active Directory.
- Zainstalować rolę AD DS – Active Directory Domain Services (Usługi domenowe w usłudze Active Directory) i skonfigurować kontroler domeny systemu Windows Server 2008 R2, korzystając z interfejsu Windows.

Przewidywany czas trwania lekcji: 60 minut

Active Directory, tożsamość i dostęp

Pojęcie infrastruktury IDA (Identity and Access) odnosi się do narzędzi i najważniejszych technologii używanych w celu zintegrowania osób, procesów i technologii danej organizacji. Sprawna infrastruktura IDA zapewnia, że właściwe osoby mają w odpowiednim momencie dostęp do właściwych zasobów.

Jak nadmieniono wcześniej, usługi Active Directory zapewniają funkcjonalność IDA dla sieci firmowych działających pod kontrolą systemów Windows. Usługi AD DS są najistotniejszym składnikiem infrastruktury IDA usług Active Directory. Usługi AD DS gromadzą i przechowują w całym przedsiębiorstwie informacje dotyczące IDA w bazie danych nazwanej magazynem danych usług Active Directory. Magazyn danych zawiera wszystkie informacje (odnoszące się do tych kwestii) dla wszystkich obiektów istniejących wewnątrz infrastruktury Active Directory. Ponadto, usługi AD DS funkcjonują jako koncentrator komunikacji i informacji dla dodatkowych usług Active Directory, które razem tworzą pełną infrastrukturę IDA.

Usługi Active Directory przechowują informacje o użytkownikach, grupach, komputerach i innych tożsamościach. Tożsamość jest w najszerszym sensie reprezentacją jakiejś jednostki, która będzie wykonywać działania w sieci firmowej. Na przykład użytkownik będzie otwierać dokumenty z foldera udostępnianego na serwerze. Dokument będzie zabezpieczany uprawnieniami na liście kontroli dostępu (ACL). Dostęp do dokumentu jest zarządzany przez podsystem zabezpieczeń serwera, który porównuje tożsamość użytkownika z tożsamościami na liście ACL w celu określenia, czy żądanie dostępu do pliku przez użytkownika zostanie przyjęte, czy odrzucone.

Komputery, grupy, usługi i inne obiekty również wykonują działania w sieci i muszą być reprezentowane przez tożsamości. Wśród informacji przechowywanych na temat

tożsamości są właściwości, które w sposób jednoznaczny identyfikują obiekty, takie jak nazwa użytkownika lub identyfikator zabezpieczeń (SID) oraz hasło dla tożsamości. *Magazyn tożsamości* jest więc jednym ze składników infrastruktury IDA. Magazyn danych Active Directory, znany również jako katalog, jest magazynem tożsamości. Sam katalog jest obsługiwany i zarządzany przez kontrolera domeny – serwer pełniący rolę AD DS. Jeśli wewnątrz infrastruktury usług Active Directory istnieje wiele domen, współpracują one ze sobą, utrzymując kopię magazynu danych na każdym kontrolerze domeny. Informacje przechowywane w tym magazynie pozwalają usługom Active Directory wykonywać trzy główne funkcje infrastruktury IDA: uwierzytelnienie, kontrola dostępu i inspekcja.

- **Uwierzytelnianie** Użytkownik, komputer czy inny obiekt musi najpierw poddać weryfikacji swoją tożsamość w infrastrukturze usług Active Directory, zanim przydzielona zostanie mu możliwość funkcjonowania jako część domeny usług Active Directory. Ten proces weryfikacji polega zazwyczaj na wymianie chronionych lub tajnych informacji, takich jak hasło czy certyfikat cyfrowy. Po dostarczeniu tych informacji do usługi Active Directory i poprawnym ich zweryfikowaniu użytkownik może funkcjonować jako członek domeny i wykonywać działania takie, jak żądanie dostępu do plików, przekazywanie zadań do drukarki, uzyskiwanie dostępu i odczytywanie wiadomości e-mail czy wiele innych działań w domenie.

Uwierzytelnianie Kerberos w domenie Active Directory

Do uwierzytelniania tożsamości w domenie Active Directory używany jest protokół o nazwie Kerberos. Gdy użytkownik lub komputer loguje się do domeny, Kerberos uwierzytelnia jego poświadczenia i wydaje pakiet informacji zwany TGT – ticket granting ticket (bilet przydzielający bilet). Zanim użytkownik połączy się z serwerem, aby zażądać dokumentu, żądanie Kerberos zostanie przesłane do kontrolera domeny razem z biletem TGT, który identyfikuje uwierzytelnionego użytkownika. Kontroler domeny wydaje użytkownikowi inny pakiet informacji zwany service ticket (biletem usługowym), który identyfikuje serwerowi uwierzytelnionego użytkownika. Użytkownik przedstawia serwerowi bilet usługowy, który go przyjmuje jako dowód, że użytkownik został uwierzytelniony.

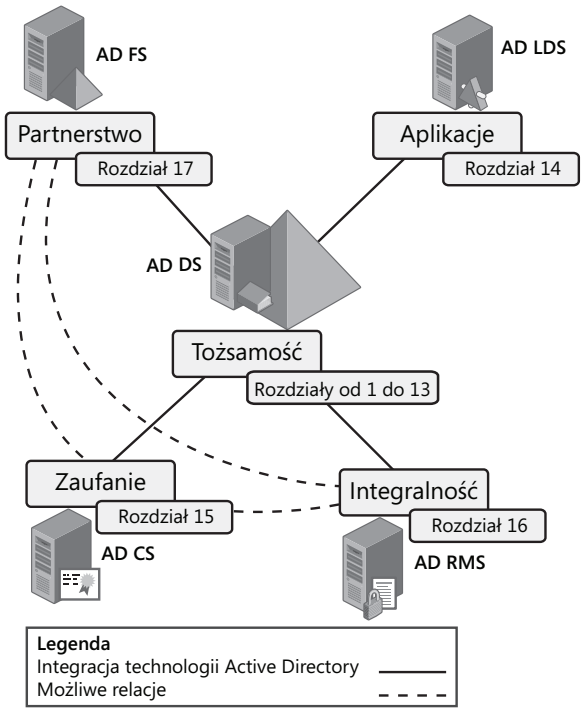
Te transakcje protokołu Kerberos dają w wyniku pojedyncze logowanie w sieci. Po początkowym zalogowaniu użytkownika lub komputera i uzyskaniu biletu TGT użytkownik jest uwierzytelniony w całej domenie i może otrzymywać bilety usługowe identyfikujące użytkownika w dowolnej usłudze. Wszystkie te działania związane z biletami są zarządzane przez klientów Kerberos oraz usługi wbudowane w Windows i są niewidoczne dla użytkownika.

- **Kontrola dostępu** Infrastruktura IDA jest odpowiedzialna za ochronę informacji i zasobów poprzez zapewnienie, że dostęp do zasobów jest przydzielany tylko tożsamościom, które powinny taki dostęp uzyskiwać. Dostęp do informacji poufnych i zasobów musi być zarządzany zgodnie z polityką przedsiębiorstwa. Każdy pojedynczy obiekt (jak komputery, folder, pliki czy drukarki) wewnątrz usługi Active Directory ma przypisaną do siebie listę arbitralnej kontroli dostępu DACL (Discretionary Access Control List). Lista ta zawiera informacje dotyczące tożsamości, którym przydzielony został dostęp do

obiektu, a także informacje, jaki poziom dostępu został im przydzielony. Kiedy użytkownik o tożsamości uwierzytelnionej w domenie próbuje uzyskać dostęp do zasobu, sprawdzana jest lista DACL tego zasobu w celu określenia, czy tożsamość użytkownika umieszczona została na liście. Jeśli tożsamość użytkownika znajduje się na liście, użytkownikowi zezwala się na dostęp do zasobu zgodnie z uprawnieniami dostępu wyspecyfikowanymi w liście DACL dla tego użytkownika.

- **Inspekcja** *Inspekcja* oznacza działania związane z monitorowaniem wewnątrz infrastruktury IDA. Inspekcja pozwala organizacjom monitorować zdarzenia występujące w infrastrukturze IDA, takie jak dostęp do plików i folderów, gdzie i kiedy miało miejsce logowanie użytkownika, zmiany wprowadzane w infrastrukturze IDA oraz główne działania związane z funkcjonowaniem samej usługi Active Directory. Działanie inspekcji jest kontrolowane przez systemowe listy kontroli dostępu SACL (System Access Control List). Podobnie jak w przypadku poprzednio omawianej listy DACL, każdy obiekt wewnątrz infrastruktury IDA posiada przypisaną do siebie listę SACL. Lista SACL zawiera listę tożsamości, których działania dotyczące tego zasobu będą monitorowane, jak również lista ta określa poziom inspekcji, który będzie realizowany dla każdej monitorowanej tożsamości.

Usługi AD DS nie są jedynym składnikiem IDA obsługiwanym przez system Windows Server 2008. Wraz z wydaniem systemu Windows Server 2008 firma Microsoft złączyła ze sobą kilka wcześniej oddzielnych składników w zintegrowaną platformę IDA. Sama usługa Active Directory zawiera teraz pięć technologii, z których każda może być określona słowem kluczowym identyfikującym cel danej technologii, jak pokazano na rysunku 1-1.



Rysunek 1-1 Integracja pięciu technologii Active Directory

Te pięć technologii składa się na pełne rozwiązanie IDA:

- **Active Directory Domain Services – Tożsamość** Usługi AD DS (Usługi domenowe w usłudze Active Directory), jak opisano wcześniej, mają zapewniać centralne repozytorium do zarządzania tożsamościami w organizacji. Usługi AD DS zapewniają usługi uwierzytelniania i autoryzacji w sieci i wspierają zarządzanie obiektami przez zasady grupy. Usługi AD DS zapewniają również usługi zarządzania i udostępniania informacji, umożliwiając użytkownikom znalezienie dowolnego składnika – serwerów plików, drukarek, grup i innych użytkowników – przez przeszukiwanie katalogu. Z tego powodu usługi AD DS są często nazywane usługą katalogową sieciowego systemu operacyjnego. Usługi AD DS są główną technologią Active Directory i powinny być wdrożone w każdej sieci, która działa pod kontrolą systemów operacyjnych Windows Server 2008. Usługi AD DS są omówione w rozdziałach od 1 do 13.

Więcej informacji **Projekt AD DS**

Uaktualnione informacje dotyczące tworzenia projektu i implementacji usług Active Directory Domain Services (Usługi domenowe w usłudze Active Directory) można uzyskać sięgając po poradnik AD DS Design Guide, dostępny pod adresem: *http://technet.microsoft.com/en-us/library/cc754678(WS.10).aspx*.

- **Active Directory Lightweight Directory Services – Aplikacje** Rola AD LDS (Usługi Lightweight Directory Services w usłudze Active Directory), zwana wcześniej jako ADAM – Active Directory Application Mode (Tryb aplikacyjny usług Active Directory), stanowi w gruncie rzeczy autonomiczną wersję Active Directory i zapewnia wsparcie dla aplikacji wykorzystujących usługi katalogowe. Usługi AD LDS są w istocie podzbiorem usług AD DS, ponieważ obie są oparte na tym samym kodzie bazowym. Katalog AD LDS przechowuje i replikuje tylko informacje związane z aplikacjami. Jest powszechnie używany przez aplikacje, które wymagają magazynu katalogowego, ale nie wymagają replikowania informacji na wszystkie kontrolery domen. Usługi AD LDS umożliwiają też wdrażanie niestandardowego schematu wspierania aplikacji bez modyfikowania schematu AD DS. Rola AD LDS jest znacznie uproszczona i obsługuje wiele magazynów danych na pojedynczym systemie, aby każda aplikacja mogła być wdrażana ze swoim własnym katalogiem, schematem, przypisanymi portami protokołów Lightweight Directory Access Protocol (LDAP) i SSL oraz dziennikiem zdarzeń aplikacji. Usługi AD LDS nie są zależne od AD DS, więc mogą być używane w środowisku jednostanowiskowym lub w grupie roboczej. Jednakże w środowiskach domenowych usługi AD LDS mogą korzystać z AD DS do uwierzytelniania podmiotów zabezpieczeń Windows (użytkowników, grup i komputerów). Usługi AD LDS mogą też być używane do zapewniania usług uwierzytelniania w sieciach zewnętrznych, takich jak ekstranety. Korzystanie z usług AD LDS w tej sytuacji stanowi mniejsze ryzyko niż korzystanie z AD DS. Usługi AD LDS zostały omówione w rozdziale 14.
- **Active Directory Certificate Services – Zaufanie** Organizacje mogą wykorzystywać usługi AD CS – Active Directory Certificate Services (Usługi certyfikatów w usłudze Active Directory) do instalowania urzędu certyfikacji w celu wydawania certyfikatów cyfrowych jako część infrastruktury kluczy publicznych (PKI), która wiąże tożsamość osoby, urządzenia lub usługi z odpowiadającym kluczem prywatnym. Certyfikaty mogą być używane do uwierzytelniania użytkowników i komputerów, zapewniania

uwierzytelniania opartego na WWW, obsługi uwierzytelniania przez karty inteligentne i obsługi aplikacji w środowiskach obejmujących sieci bezprzewodowe, wirtualne sieci prywatne (VPN), protokół IPSec, szyfrujący system plików (EFS), podpisy cyfrowe itd. Usługi AD CS zapewniają efektywny i bezpieczny sposób wydawania certyfikatów i zarządzania nimi. Można korzystać z usług AD CS do zapewniania tych usług zewnętrznym społecznościom. W takim przypadku usługi AD CS powinny być połączone z zewnętrznym, uznanym urzędem certyfikacji, który poświadczy przed innymi, że jesteśmy tymi, za kogo się podajemy. Usługi AD CS są zaprojektowane do tworzenia zaufania w świecie niegodnym zaufania; dlatego muszą polegać na sprawdzonych procesach zapewniających, że każda osoba lub komputer, które otrzymają certyfikat, zostaną dokładnie sprawdzone. W sieciach wewnętrznych usługi AD CS mogą integrować się z usługami AD DS, aby automatycznie zaopatrywać użytkowników i komputery w certyfikaty. Usługi AD CS zostały omówione w rozdziale 15.

- **Active Directory Rights Management Services – Integralność** Chociaż serwer działający pod kontrolą systemu Windows może uniemożliwiać lub zezwalać na dostęp do dokumentu w oparciu o jego listy ACL, to niewiele było sposobów kontrolowania, co dzieje się z dokumentem i jego zawartością po otwarciu go przez użytkownika. Usługi AD RMS – Active Directory Rights Management Services (Usługi zarządzania prawami dostępu w usłudze Active Directory) są technologią ochrony informacji, która umożliwia nam implementowanie trwałych szablonów zasad użycia definiujących dozwolone i nieautoryzowane sposoby użycia, czy to w trybie online, offline, po wewnętrznej, czy po zewnętrznej stronie zapory. Na przykład można by skonfigurować szablon, który pozwala użytkownikom na czytanie dokumentu, ale nie na drukowanie lub kopiowanie jego zawartości. Dzięki temu można zapewnić integralność generowanych danych, chronić własność intelektualną i kontrolować, kto i w jaki sposób może korzystać z dokumentów tworzonych przez organizację. Usługi AD RMS wymagają domeny Active Directory z kontrolerami domeny działającymi pod kontrolą systemu Windows 2000 Server z Service Pack 3 (SP3) lub nowszego; serwera IIS; serwera baz danych – takiego jak Microsoft SQL Server 2008; klienta AD RMS, którego można pobrać z witryny Microsoft Download Center i zawartego domyślnie w systemach Windows Vista, Windows 7 i Windows Server 2008; oraz przeglądarki lub aplikacji obsługującej RMS – takiej jak Microsoft Internet Explorer, Microsoft Office, Microsoft Word, Microsoft Outlook lub Microsoft PowerPoint. Usługi AD RMS mogą wykorzystywać usługi AD CS do wbudowywania certyfikatów w dokumenty oraz usługi AD DS do zarządzania prawami dostępu. Usługi AD RMS zostały omówione w rozdziale 16.
- **Active Directory Federation Services – Partnerstwo** Usługi AD FS – Active Directory Federation Services umożliwiają organizacji rozszerzenie IDA na wiele platform obejmujących zarówno środowiska Windows, jak i inne oraz przekazywanie tożsamości i praw dostępu przez granice zabezpieczeń zaufanym partnerom. W środowisku federacyjnym każda organizacja obsługuje i zarządza swoimi własnymi tożsamościami, ale każda organizacja może też bezpiecznie przekazywać i przyjmować tożsamości z innych organizacji. Użytkownicy są uwierzytelniani w jednej sieci, ale mogą korzystać z zasobów w innej – proces ten jest znany jako SSO – single sign-on (rejestracja jednokrotna). Usługi AD FS wspierają partnerstwa, ponieważ pozwalają różnym organizacjom dzielić dostęp do aplikacji ekstranetowych, polegając przy tym na swoich własnych, wewnętrznych strukturach AD DS w celu zapewniania faktycznego procesu uwierzytelniania.

W tym celu usługi AD FS rozszerzają wewnętrzną strukturę AD DS na świat zewnętrzny poprzez typowe porty protokołu Transmission Control Protocol/Internet Protocol (TCP/IP), takie jak 80 (HTTP) i 443 (Secure HTTP, czyli HTTPS). Normalnie umieszczane są w sieci obwodowej. Usługi AD FS mogą wykorzystywać usługi AD CS do tworzenia zaufanych serwerów i usługi AD RMS do zapewniania zewnętrznej ochrony dla własności intelektualnej. Usługi AD FS zostały omówione w rozdziale 17.

Razem role Active Directory zapewniają zintegrowane rozwiązanie IDA. Usługi AD DS lub AD LDS zapewniają podstawowe usługi katalogowe zarówno w implementacjach domenowych, jak i autonomicznych. Usługi AD CS zapewniają zaufane poświadczenia w formie certyfikatów cyfrowych PKI. Usługi AD RMS chronią integralność informacji zawartych w dokumentach. Usługi AD FS wspierają partnerstwa eliminując konieczność tworzenia wielu oddzielnych tożsamości dla pojedynczego podmiotu zabezpieczeń w środowiskach federacyjnych.

Więcej niż tożsamość i dostęp

Usługi Active Directory stanowią jednak więcej niż tylko rozwiązanie IDA. Zapewniają też mechanizmy do wspierania, zarządzania i konfigurowania zasobów w środowiskach sieci rozproszonych.

Jako zbiór reguł, *schemat* definiuje klasy obiektów i atrybuty, które mogą być zawarte w katalogu. To, że w Active Directory występują na przykład obiekty użytkowników zawierające nazwę użytkownika i hasło, jest spowodowane tym, że schemat definiuje klasę obiektu *user*, te dwa atrybuty i powiązania pomiędzy klasą obiektu oraz atrybutami.

Administracja oparta na zasadach ułatwia zarządzanie nawet największymi, najbardziej skomplikowanymi sieciami przez zapewnianie pojedynczego miejsca, w którym konfiguruje się ustawienia, jakie są następnie wdrażane w wielu systemach. Poznamy takie zasady, w tym zasady grupy, zasady inspekcji i szczegółowe zasady haseł w rozdziale 6 „Infrastruktura zasad grupy", rozdziale 7 „Zarządzanie bezpieczeństwem i konfiguracją przedsiębiorstwa za pomocą zasad grupy" i rozdziale 8 „Usprawnienia zabezpieczeń uwierzytelnienia w domenie AD DS".

Usługi replikacji rozprowadzają dane katalogowe po całej sieci. Obejmuje to zarówno sam magazyn danych, jak również dane wymagane do implementacji zasad i konfiguracji, w tym skrypty logowania. W rozdziale 8, rozdziale 11 „Zarządzanie lokacjami i replikacją usługi Active Directory" oraz rozdziale 10 „Administrowanie kontrolerami domen" znajdziemy więcej informacji na temat replikacji Active Directory. Istnieje nawet oddzielna partycja magazynu danych o nazwie *configuration* (konfiguracja), która utrzymuje informacje na temat konfiguracji sieci, topologii i usług.

Kilka składników i technologii umożliwia nam tworzenie zapytań do Active Directory i wyszukiwanie obiektów w magazynie danych. Partycja magazynu danych o nazwie *global catalog* (wykaz globalny) (znana również jako *partial attribute set* – częściowy zbiór atrybutów częściowych) zawiera informacje o każdym obiekcie w katalogu. Jest pewnego rodzaju indeksem, który może służyć do odnajdowania obiektów w katalogu. Interfejsy programistyczne, takie jak Active Directory Services Interface (ADSI) i protokoły, takie jak LDAP mogą być używane do odczytywania i manipulowania magazynem danych.

Magazyn danych Active Directory może też być używany do wspierania aplikacji i usług niepowiązanych bezpośrednio z AD DS. Wewnątrz bazy danych partycje aplikacji mogą

przechowywać dane obsługujące aplikacje, które wymagają replikowanych danych. Usługa DNS (Domain Name System) na serwerze działającym pod kontrolą systemu Windows Server 2008 może przechowywać te informacje w bazie danych zwanej strefą zintegrowaną Active Directory, która jest utrzymywana jako partycja aplikacji w AD DS i replikowana przy użyciu usług replikacji Active Directory.

Uwaga Gdzie znaleźć szczegóły dotyczące Active Directory

Więcej szczegółów dotyczących Active Directory można znaleźć w pomocy zainstalowanej na stronie domowej systemu Windows Server 2008 i Windows Server 2008 R2 dostępnej pod adresem *http://technet.microsoft.com/en-us/windowsserver/bb310558.aspx*.

Składniki infrastruktury Active Directory

Pierwsze 13 rozdziałów tego zestawu szkoleniowego będzie skupiać się na instalacji, konfigurowaniu i zarządzaniu usługami AD DS. Usługi AD DS stanowią podstawę IDA w sieci korporacyjnej. Warto poświęcić kilka chwil na przegląd składników infrastruktury Active Directory.

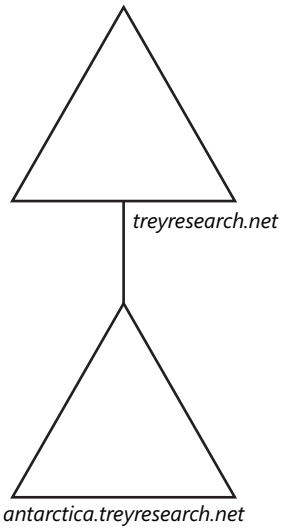
- **Magazyn danych Active Directory** Jak wspomniano wcześniej, usługi AD DS przechowują tożsamości w katalogu – magazynie danych obsługiwanym przez kontrolery domen. Katalog jest pojedynczym plikiem o nazwie Ntds.dit domyślnie znajdującym się w folderze %SystemRoot%\Ntds na kontrolerze domeny. Ta baza danych jest podzielona na kilka partycji, w tym schemat, konfigurację, wykaz globalny i kontekst nazewnictwa domeny, który zawiera dane o obiektach w domenie – na przykład użytkownikach, grupach i komputerach. W zależności od środowiska mogą także występować partycje aplikacji i częściowe zestawy atrybutów PAS (Partial Attribute Set), również nazywane wykazem globalnym.
- **Kontrolery domeny** Kontrolery domeny, skrótowo zwane też DC, są serwerami, które pełnią rolę usług AD DS i utrzymują kopię magazynu danych usługi Active Directory wraz z innymi danymi, które są istotne dla domeny. Jako część tej roli uruchamiają też usługę Kerberos Key Distribution Center (KDC), która zajmuje się uwierzytelnianiem, oraz inne usługi Active Directory. Rozdział 10 opisuje szczegółowo role wykonywane przez kontrolery domeny.
- **Domena** Jeden lub więcej kontrolerów domeny jest wymaganych do utworzenia *domeny* Active Directory. Domena jest jednostką administracyjną, w której udostępniane są pewne możliwości i charakterystyki. Po pierwsze, wszystkie kontrolery domeny replikują partycję domeny z magazynu danych, zawierającą między innymi dane o tożsamościach dla użytkowników, grup i komputerów należących do domeny. Ponieważ wszystkie kontrolery domeny utrzymują ten sam magazyn tożsamości, to dowolny kontroler domeny może uwierzytelniać dowolną tożsamość w domenie. Dodatkowo domena jest zakresem zasad administracyjnych określających na przykład stopień złożoności haseł i zasady blokowania kont. Takie zasady skonfigurowane w jednej domenie wpływają na wszystkie konta w tej domenie i nie wpływają na konta w innych domenach. Zmiany mogą być wprowadzane do obiektów w bazie danych Active Directory przez dowolny kontroler domeny i będą replikowane na wszystkie inne kontrolery domeny. Dlatego w sieciach, gdzie nie można obsłużyć replikacji wszystkich danych

pomiędzy kontrolerami domeny, konieczne może być zaimplementowanie więcej niż jednej domeny w celu zarządzania replikacją podzbiorów tożsamości. Więcej na temat domen dowiemy się w rozdziale 12 „Zarządzanie wieloma domenami i lasami".

- **Las** *Las* jest zbiorem jednej lub więcej domen Active Directory. Pierwsza domena zainstalowana w lesie jest nazywana *domeną główną lasu*. Las zawiera pojedynczą definicję konfiguracji sieci i pojedyncze wystąpienie schematu katalogu. Las jest pojedynczym wystąpieniem katalogu – żadne dane nie są replikowane przez Active Directory poza granice lasu. Dlatego las definiuje granice zabezpieczeń. Rozdział 12 dokładnie zajmie się pojęciem lasu.
- **Drzewo** Przestrzeń nazw DNS dla domen w lesie tworzy drzewa wewnątrz tego lasu. Jeśli domena jest poddomeną innej domeny, to te dwie domeny stanowią drzewo. Na przykład, jeśli las *treyresearch.net* zawiera dwie domeny, *treyresearch.net* i *antarctica.treyresearch.net,* to te domeny stanowią ciągły fragment przestrzeni nazw DNS, więc są pojedynczym drzewem. Jeśli z kolei dwoma domenami są *treyresearch.net* i *proseware.com*, które nie sąsiadują ze sobą w przestrzeni nazw DNS, to uważa się, że las zawiera dwa drzewa. Drzewa wynikają bezpośrednio z nazw DNS wybranych dla domen w danym lesie.

  Rysunek 1-2 ilustruje las Active Directory dla firmy Trey Research, która prowadzi niewielkie działania w stacji naukowej na Antarktydzie. Ponieważ łącza z Antarktydy do głównej siedziby firmy są drogie, powolne i zawodne, to Antarktyda jest skonfigurowana jako osobna domena. Nazwą DNS lasu jest *treyresearch.net*.

  Domena antarktyczna jest domeną podrzędną w przestrzeni nazw DNS: *antarctica.treyresearch.net*, więc jest traktowana jako domena podrzędna w drzewie domen.



Rysunek 1-2 Las usługi Active Directory z dwiema domenami

- **Poziom funkcjonalności** Funkcjonalność dostępna w domenie lub lesie Active Directory zależy od ich *poziomu funkcjonalności*. Poziom funkcjonalności jest ustawieniem usług AD DS, które włącza zaawansowane funkcje AD DS w całej domenie lub w całym lesie. Istnieje sześć poziomów funkcjonalności domeny: macierzysty Windows

2000 (native), mieszany Windows 2000 (mixed), Windows Server 2003, tymczasowy Windows Server 2003 (interim), Windows Server 2008 i Windows Server 2008 R2 oraz pięć poziomów funkcjonalności lasu: Windows Server 2000, Windows Server 2003, tymczasowy Windows Server 2003, Windows Server 2008 i Windows Server 2008 R2. Gdy podniesiony zostanie poziom funkcjonalności domeny lub lasu, to funkcje zapewniane przez daną wersję Windows staną się dostępne dla usług AD DS. Na przykład, gdy poziom funkcjonalności domeny zostanie podniesiony do Windows Server 2008 R2, to dostępna stanie się możliwość włączania kosza usługi AD (Acitive Directory Recycle Bin). Funkcja ta w razie potrzeby pozwala prosto przywracać poprzednio usunięte obiekty. Ważną rzeczą, którą trzeba wiedzieć na temat poziomów funkcjonalności, jest to, że określają wersje Windows dozwolone na kontrolerach domeny. Zanim podniesiemy poziom funkcjonalności domeny do Windows Server 2008, wszystkie kontrolery domeny muszą działać pod kontrolą systemu Windows Server 2008. Rozdział 12 szczegółowo zajmuje się poziomami funkcjonalności domeny i lasu.

- **Jednostki organizacyjne** Active Directory jest hierarchiczną bazą danych. Obiekty w tym magazynie danych mogą być zbierane w kontenerach. Jednym z typów kontenera jest klasa obiektu o nazwie *container*. Można zobaczyć domyślne kontenery, takie jak Users, Computers i Builtin, otwierając przystawkę Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory). Innym typem kontenera jest jednostka organizacyjna (OU). Jednostki organizacyjne stanowią nie tylko kontener dla obiektów, ale również zakres zarządzania obiektami. Dzieje się tak dlatego, ponieważ jednostki organizacyjne mogą mieć połączone ze sobą obiekty zwane obiektami zasad grupy (GPO). Obiekty GPO mogą zawierać ustawienia konfiguracyjne, które następnie będą stosowane automatycznie przez użytkowników i komputery w danej jednostce organizacyjnej. Z rozdziału 2 „Administrowanie usługami AD DS" dowiemy się więcej na temat jednostek organizacyjnych, a w rozdziale 6 zbadamy obiekty zasad grupy.
- **Lokacje** Rozważając topologię sieci rozproszonego przedsiębiorstwa z pewnością trzeba omówić lokacje sieciowe. Lokacje w Active Directory mają jednak bardzo specyficzne znaczenie, ponieważ istnieje określona klasa obiektu o nazwie *site* (lokacja). Lokacja Active Directory jest obiektem, który reprezentuje część przedsiębiorstwa, wewnątrz której istnieje dobra łączność sieciowa. Lokacja tworzy granice replikacji i użycia usług. Kontrolery domeny wewnątrz lokacji replikują zmiany w ciągu sekund. Zmiany są replikowane pomiędzy lokacjami w kontrolowany sposób przy założeniu, że połączenia pomiędzy lokacjami są powolne, drogie lub zawodne w porównaniu z połączeniami wewnątrz lokacji. Dodatkowo klienci będą woleli korzystać z usług rozproszonych zapewnianych przez serwery w swojej własnej lokacji lub w najbliższej lokacji. Na przykład, kiedy użytkownik loguje się do domeny, to klient Windows najpierw próbuje uwierzytelnić go w kontrolerze domeny w jego lokacji. Dopiero jeśli żaden kontroler domeny nie będzie dostępny w danej lokacji, klient spróbuje uwierzytelnić go w kontrolerze domeny w innej lokacji. Rozdział 11 opisuje szczegółowo konfigurację i funkcjonalność lokacji Active Directory.

Każdy z tych składników jest szczegółowo omówiony w dalszej części tego zestawu ćwiczeniowego. W tym momencie, jeśli ktoś jest mniej zaznajomiony z Active Directory, to ważne jest podstawowe zrozumienie terminologii, składników i relacji pomiędzy nimi.

Przygotowanie do utworzenia nowego lasu Windows Server 2008

Zanim zainstalujemy rolę AD DS na serwerze i skonfigurujemy go na działanie jako kontroler domeny, musimy zaplanować swoją infrastrukturę Active Directory. Do informacji potrzebnych w celu utworzenia kontrolera domeny należą:

- Nazwa domeny i nazwa DNS. Domena musi mieć unikalną nazwę DNS, na przykład: *contoso.com*, a także krótką nazwę, na przykład: CONTOSO, zwaną nazwą NetBIOS. NetBIOS jest protokołem sieciowym, który jest używany od pierwszych wersji Microsoft Windows NT i jest nadal wykorzystywany do zachowania kompatybilności ze starszymi aplikacjami.
- Czy domena będzie musiała obsługiwać kontrolery domeny działające pod kontrolą poprzednich wersji Windows? Podczas tworzenia nowego lasu Active Directory będziemy konfigurować poziom funkcjonalności. Jeśli domena będzie zawierać tylko kontrolery domeny Windows Server 2008 R2, to można ustawić zgodny z tym systemem poziom funkcjonalności, aby skorzystać z ulepszonych funkcji wprowadzonych przez tę wersję Windows.
- Szczegóły sposobu implementacji obsługi Active Directory przez DNS. Najlepszą praktyką jest zaimplementowanie usługi DNS dla stref domen Windows, wykorzystując usługę Windows DNS, jak dowiemy się w rozdziale 9 „Integrowanie usługi DNS z usługami domenowymi"; jednakże możliwa jest obsługa domeny Windows na usłudze DNS firmy trzeciej.
- Konfiguracja IP dla kontrolera domeny. Kontrolery domen wymagają statycznych adresów IP i wartości masek podsieci. Dodatkowo kontroler domeny musi być skonfigurowany przy użyciu adresu serwera DNS w celu realizacji rozpoznawania nazw. Jeśli tworzymy nowy las i będziemy uruchamiać usługę Windows DNS na kontrolerze domeny, to możemy skonfigurować adres DNS tak, aby wskazywał na własny adres IP serwera. Po zainstalowaniu usługi DNS serwer może samodzielnie rozwijać nazwy DNS.
- Nazwa użytkownika i hasło konta należącego do grupy Administrators (Administratorzy) serwera. To konto musi mieć hasło – hasło nie może być puste.
- Miejsce, w którym należy zainstalować magazyn danych (w tym *Ntds.dit*) oraz wolumin systemowy (SYSVOL). Domyślnie magazyny te są tworzone w folderze %SystemRoot%, na przykład C:\Windows, odpowiednio w podfolderach NTDS i SYSVOL. Podczas tworzenia kontrolera domeny można przekierować te magazyny na inne napędy.

Więcej informacji Wdrażanie usług AD DS

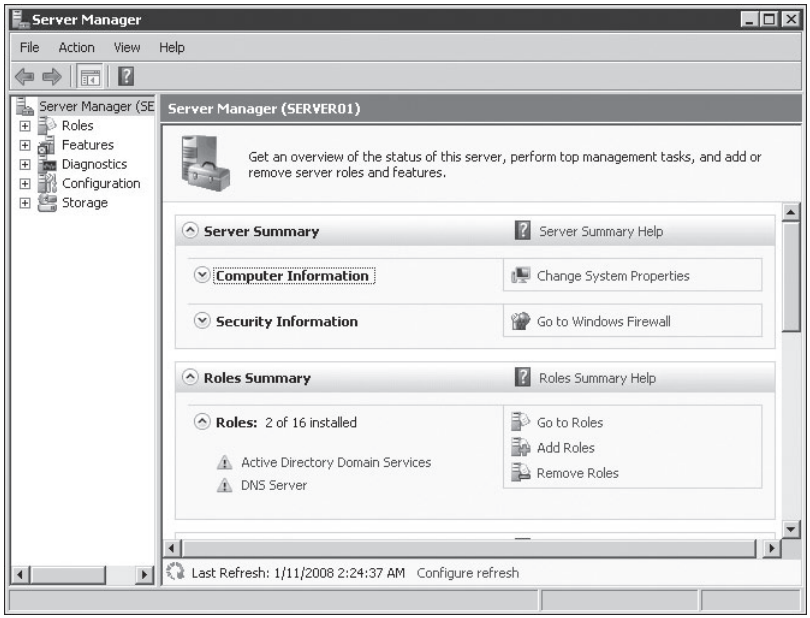
Ta lista obejmuje ustawienia, które będzie trzeba skonfigurować podczas tworzenia kontrolera domeny. Istnieje wiele dodatkowych względów związanych z wdrożeniem usług AD DS w środowisku korporacyjnym. Więcej informacji na ten temat zawiera poradnik AD DS Deployment Guide pod adresem *http://technet.microsoft.com/en-us/library/cc753963(WS.10).aspx*.

Dodawanie roli AD DS przy użyciu interfejsu Windows

Po zebraniu wymaganych informacji wymienionych wcześniej jesteśmy gotowi, aby dodać rolę AD DS. Istnieje kilka sposobów realizacji tego zadania. W tej lekcji dowiemy się, jak utworzyć kontrolera domeny przy użyciu interfejsu Windows. W następnej lekcji dowiemy się, jak to zrobić korzystając z wiersza polecenia.

System Windows Server 2008 obsługuje konfigurację opartą na rolach, instalując tylko te składniki i usługi, które są wymagane przez role odgrywane przez serwer. To zarządzanie serwerem oparte na rolach jest odzwierciedlone w konsoli administracyjnej Server Manager (Menedżer serwera) pokazanej na rysunku 1-3. Server Manager (Menedżer serwera) scala informacje, narzędzia i zasoby potrzebne do obsługi ról serwera.

Role można dodawać do serwera, korzystając z łącza Add Roles (Dodaj role) na głównej stronie okna Server Manager (Menedżer serwera) lub klikając prawym przyciskiem myszy węzeł Roles (Role) w drzewie konsoli i wybierając opcję Add Roles (Dodaj role). Okno Add Roles Wizard (Kreator dodawania ról) przedstawia listę ról dostępnych do zainstalowania i prowadzi nas przez instalację wybranych ról.



Rysunek 1-3 Server Manager (Menedżer serwera)

Tworzenie kontrolera domeny

Po dodaniu roli AD DS pliki wymagane do wykonywania tej roli zostaną zainstalowane na serwerze; jednakże serwer nie działa jeszcze jako kontroler domeny. Należy następnie uruchomić kreatora Active Directory Domain Services Installation Wizard (Kreator instalacji usług domenowych w usłudze Active Directory), który można wywołać korzystając z polecenia *Dcpromo.exe* w celu skonfigurowania, zainicjowania i uruchomienia Active Directory.

Zalecane ćwiczenia

Ćwiczenie 4 „Instalacja nowego lasu Windows Server 2008 R2" na końcu tej lekcji przeprowadzi nas przez konfigurację AD DS za pomocą kreatora Active Directory Domain Services Installation Wizard (Kreator instalacji usług domenowych w usłudze Active Directory).

Pytanie kontrolne

- Chcemy wykorzystać nowy serwer działający pod kontrolą systemu Windows Server 2008 R2 jako kontroler domeny w swojej domenie Active Directory. Jakiego polecenia należy użyć, aby uruchomić konfigurację kontrolera domeny?

Odpowiedź na pytanie kontrolne

- *Dcpromo.exe*

Zadanie Tworzenie lasu Windows Server 2008 R2

W tym zadaniu utworzymy las AD DS dla firmy Contoso, Ltd. Ten las będzie używany w ćwiczeniach w całym niniejszym zestawie szkoleniowym. Zaczniemy od zainstalowania systemu Windows Server 2008 R2 i wykonania zadań konfiguracyjnych po instalacji. Następnie dodamy rolę AD DS i awansujemy serwer do roli kontrolera domeny w lesie *contoso.com* korzystając z kreatora Active Directory Domain Services Installation Wizard (Kreator instalacji usług domenowych w usłudze Active Directory).

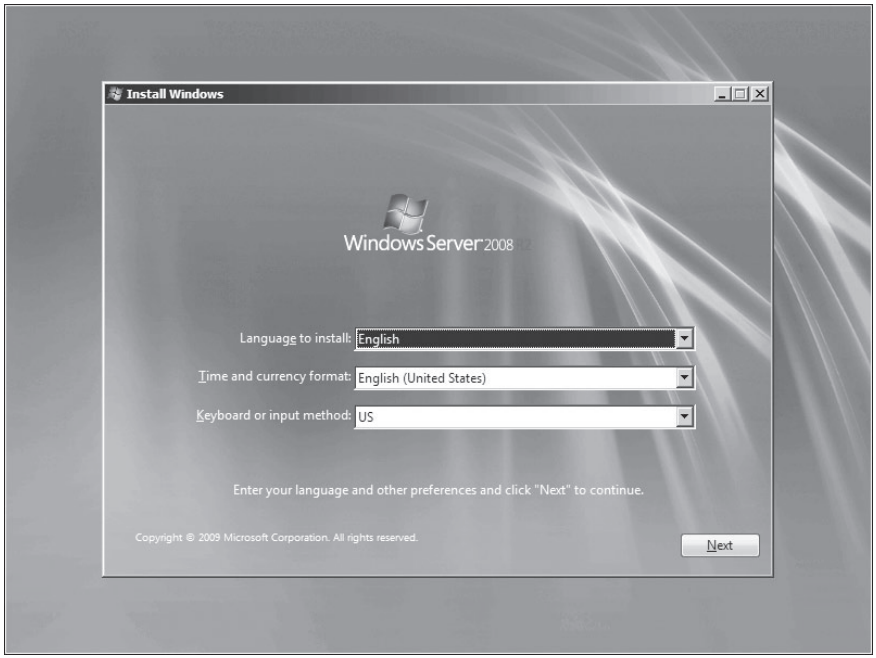
▶ Ćwiczenie 1: Instalacja systemu Windows Server 2008 R2

W tym ćwiczeniu zainstalujemy system Windows Server 2008 R2 na komputerze lub maszynie wirtualnej.

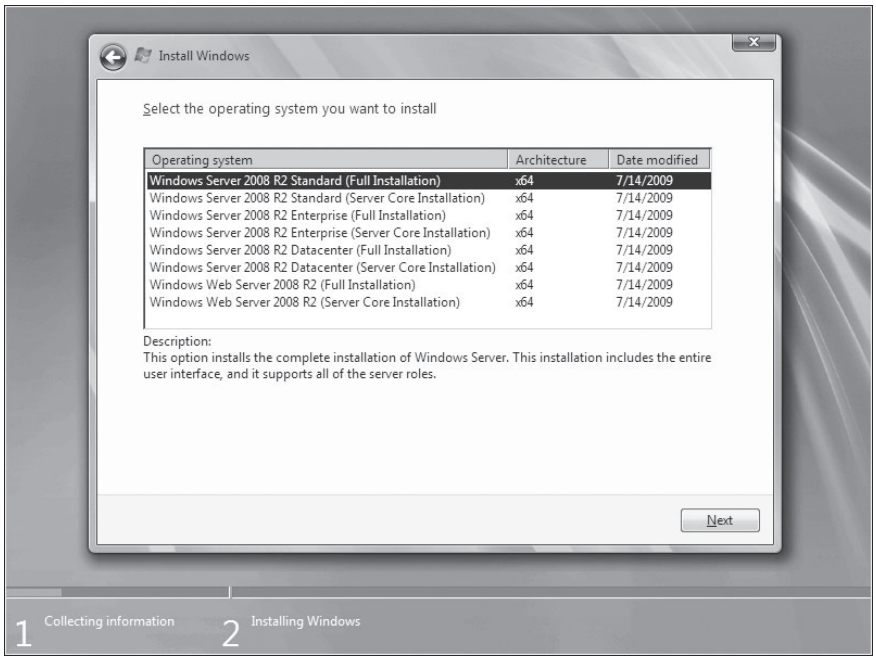
1. Włączyć system i wstawić instalacyjną płytę DVD z systemem Windows Server 2008 R2 do napędu.
   W przypadku korzystania z maszyny wirtualnej można zastosować opcję podłączenia obrazu ISO instalacyjnej płyty DVD. Wskazówek należy szukać w pliku pomocy do oprogramowania maszyn wirtualnych.

   Jeśli dysk twardy jest pusty, system powinien uruchomić się z płyty DVD. Jeśli na dysku twardym są jakieś dane, to może pojawić się zachęta do naciśnięcia klawisza w celu uruchomienia systemu z płyty DVD.

   Jeśli system nie uruchomi się z płyty DVD ani nie zaoferuje menu uruchamiania systemu, należy przejść do ustawień systemu BIOS komputera i skonfigurować kolejność uruchamiania systemu w celu zapewnienia, aby system został uruchomiony z płyty DVD. Pojawi się okno Install Windows (Zainstaluj system Windows) pokazane na rysunku 1-4.
2. Wybrać język, ustawienia regionalne i układ klawiatury odpowiadające danemu systemowi, a następnie kliknąć Next (Dalej).
3. Kliknąć Install Now (Zainstaluj teraz).
   Pojawi się lista wersji możliwych do zainstalowania, jak pokazano na rysunku 1-5.



Rysunek 1-4 Kreator Install Windows (Zainstaluj system Windows)

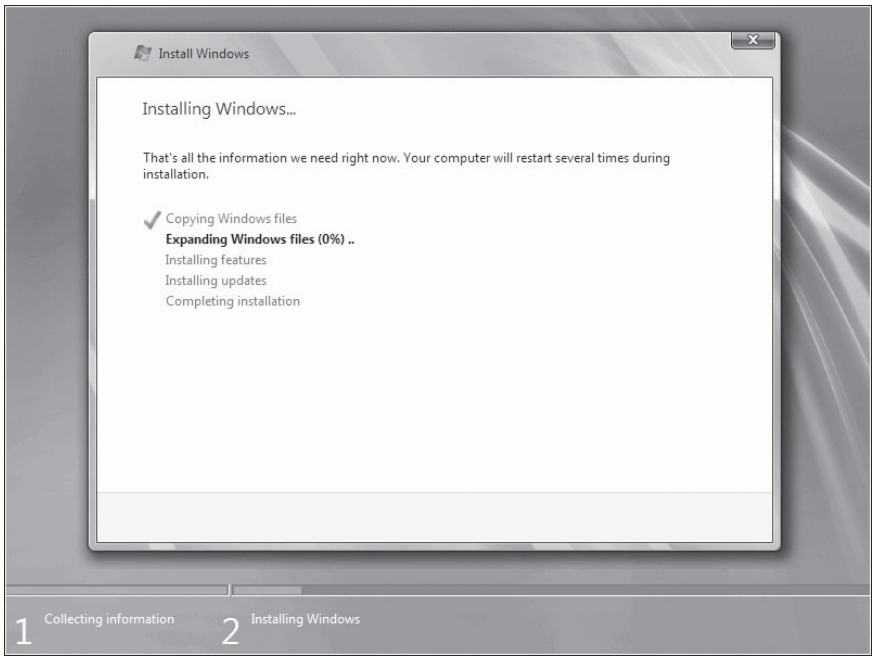


Rysunek 1-5 Strona Select The Operating System You Want To Install (Wybierz system operacyjny, który chcesz zainstalować)

4. Wybrać opcję Windows Server 2008 R2 Standard (Full Installation) i kliknąć Next (Dalej).
5. Zaznaczyć pole wyboru I Accept The License Terms (Akceptuję postanowienia licencyjne) i kliknąć Next (Dalej).
6. Kliknąć opcję Custom (Advanced) (Niestandardowa (Zaawansowana)).
7. Na stronie Where Do You Want to Install Windows (Gdzie chcesz zainstalować system Windows) należy wybrać partycję, na której chcemy zainstalować system Windows Server 2008 R2.

   Jeśli trzeba utworzyć, skasować, rozszerzyć lub sformatować partycje albo jeśli trzeba załadować niestandardowy sterownik pamięci masowej w celu uzyskania dostępu do podsystemu dyskowego, to należy kliknąć Driver Options (Advanced) (Opcje sterownika (Zaawansowane)).
8. Kliknąć Next (Dalej).
   Pojawi się okno dialogowe Installing Windows (Instaluję system Windows) pokazane na rysunku 1-6. Okno to informuje nas o postępach instalacji systemu Windows.

Uwaga Jeśli instalacja przeprowadzana jest na istniejącej wersji systemu Windows, w tym momencie program instalacyjny wyświetli ostrzeżenie, w którym użytkownik musi potwierdzić kontynuację działania.



Rysunek 1-6 Strona Installing Windows (Instaluję system Windows)

Instalacja systemu Windows Server 2008 R2 jest oparta na obrazach. Dlatego instalacja jest znacznie szybsza niż w przypadku poprzednich wersji Windows, mimo że same

systemy operacyjne są znacznie większe niż wcześniejsze wersje. Podczas instalacji komputer będzie ponownie uruchamiany raz lub kilka razy.

Gdy instalacja zostanie zakończona, zostaniemy poinformowani, że trzeba zmienić hasło użytkownika przed zalogowaniem się po raz pierwszy.

9. Kliknąć OK.
10. Wpisać hasło konta Administrator w polach New Password (Nowe hasło) i Confirm Password (Potwierdź hasło) oraz nacisnąć Enter.
    Hasło musi się składać co najmniej z siedmiu znaków i musi zawierać co najmniej trzy spośród czterech typów znaków:
    - ❑ Wielkie litery: A-Z
    - ❑ Małe litery: a-z
    - ❑ Cyfry: 0-9
    - ❑ Znaki niealfanumeryczne: symbole takie jak $, #, @ i !

Uwaga Nie można zapomnieć tego hasła

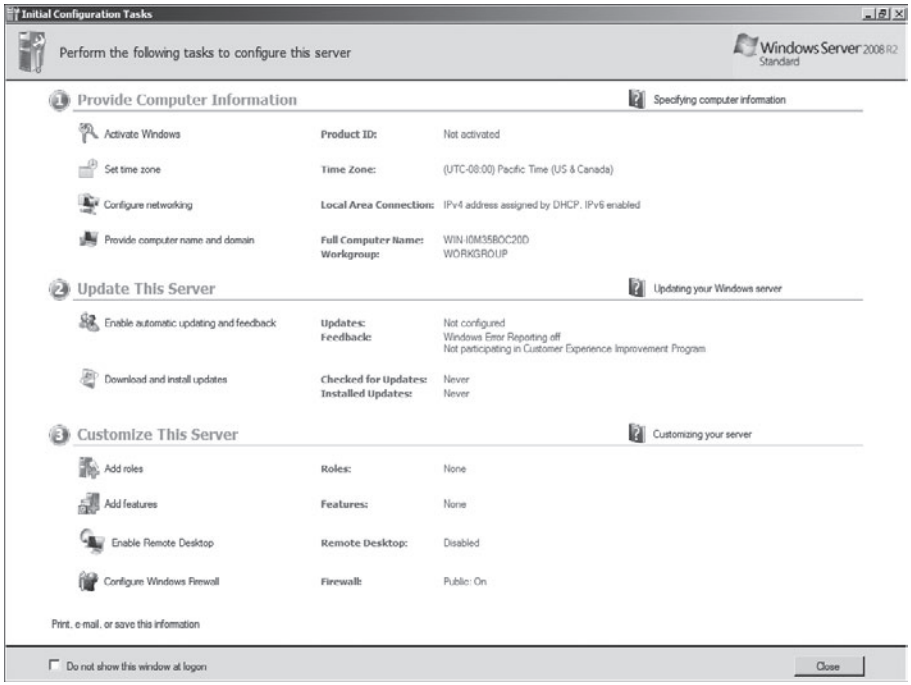
Bez niego nie będziemy w stanie zalogować się na serwerze w celu wykonania pozostałych ćwiczeń w tym zestawie ćwiczeniowym. Ewentualnie możemy wybrać opcję Create A Password Reset Disk (Utwórz dysk resetowania hasła), by uruchomić program tworzenia dysku używanego do odzyskiwania zapomnianego hasła.

11. Kliknąć OK.
    Pojawi się pulpit konta Administrator.

▶ Ćwiczenie 2: Wykonywanie konfiguracji po instalacji

W tym ćwiczeniu wykonamy konfigurację poinstalacyjną serwera w celu przygotowania nazwy i ustawień TCP/IP dla serwera, wymaganych przez ćwiczenia w tym zestawie szkoleniowym.

1. Zaczekać na pojawienie się pulpitu konta Administrator.
   Pojawi się okno Initial Configuration Tasks (Zadania konfiguracji początkowej), jak pokazano na rysunku 1-7. To narzędzie zaprojektowano w celu ułatwienia przeprowadzenia zalecanych po instalacji zadań konfiguracyjnych.
2. W oknie Initial Configuration Tasks (Zadania konfiguracji początkowej) kliknąć polecenie Provide Computer Name And Domain (Wprowadź nazwę komputera i domeny).
3. W oknie System Properties (Właściwości systemu), na karcie Computer Name (Nazwa komputera) kliknąć Change (Zmień).
4. Zmienić tekst w polu Computer Name, wpisując w nim SERVER1, a następnie kliknąć OK.
5. W oknie dialogowym Computer Name/Domain Changes kliknąć OK.
6. W oknie dialogowym System Properties kliknąć przycisk Close (Zamknij).
   Wyświetlony zostanie monit z prośbą o ponowne uruchomienie komputera, by wprowadzone zmiany zostały zastosowane. Nie uruchamiać ponownie komputera, operacja ta wykonana zostanie w dalszej części ćwiczenia.
7. Kliknąć przycisk Restart Later (Uruchom ponownie później).



Rysunek 1-7 Okno Initial Configuration Tasks (Zadania konfiguracji początkowej)

8. Kliknąć łącze Configure Networking (Konfiguruj sieć) w oknie Initial Configuration Tasks (Zadania konfiguracji początkowej).
   Pozostałe ćwiczenia w tym zestawie szkoleniowym utworzą domenę używając adresów IP w zakresie 10.0.0.11–10.0.0.20 z maską podsieci 255.255.255.0. Jeśli te adresy są używane w środowisku produkcyjnym i jeśli serwer jest połączony ze środowiskiem produkcyjnym, to trzeba odpowiednio zmienić adresy IP w tej książce, aby tworzona w tych zadaniach domena *contoso.com* nie wchodziła w konflikt z siecią produkcyjną.
9. Prawym przyciskiem myszy kliknąć Local Area Connection (Połączenie lokalne), a następnie kliknąć opcję Properties (Właściwości).
10. Wybrać opcję Internet Protocol Version 4 (TCP/IPv4) (Protokół internetowy w wersji 4 (TCP/IPv4)) i kliknąć Properties.
    Windows Server 2008 R2 zapewnia też bezpośrednią obsługę protokołu Internet Protocol Version 6 (TCP/IPv6).
11. Kliknąć opcję Use The Following IP Address (Użyj następującego adresu IP). Należy wpisać następującą konfigurację:
    - ❑ IP address (Adres IP): 10.0.0.11
    - ❑ Subnet mask (Maska podsieci): 255.255.255.0
    - ❑ Default gateway (Brama domyślna): 10.0.0.1
    - ❑ Preferred DNS server (Preferowany serwer DNS): 10.0.0.11
12. Kliknąć OK, a następnie kliknąć Close (Zamknij).
13. Zamknąć okno Network Connections (Połączenia sieciowe).

14. Kliknąć Set Time Zone (Ustaw strefę czasową), a następnie określić odpowiednie ustawienia dla danego środowiska.
15. Jeśli serwer ma połączenie z Internetem, to zalecane jest kliknięcie łącza Download And Install Updates (Pobierz i zainstaluj aktualizacje), aby zaktualizować serwer przy użyciu najnowszych aktualizacji zabezpieczeń przygotowanych przez firmę Microsoft. Zwrócić uwagę na łącza Add Roles (Dodaj role) i Add Features (Dodaj funkcje) w oknie Initial Configuration Tasks (Zadania konfiguracji początkowej).
    W następnym ćwiczeniu skorzystamy z aplikacji Server Manager (Menedżer serwera) w celu dodania ról i funkcji do komputera SERVER01. Te łącza są innym sposobem wykonania tych samych zadań.

    Domyślnie okno Initial Configuration Tasks pojawia się, ilekroć logujemy sie do serwera.
16. Zaznaczyć pole wyboru Do Not Show This Window At Logon (Nie pokazuj tego okna przy logowaniu), aby okno to nie pojawiało się przy logowaniu.
    Jeśli trzeba będzie otworzyć w przyszłości okno Initial Configuration Tasks (Zadania konfiguracji początkowej), to można to zrobić uruchamiając polecenie *Oobe.exe*.
17. Kliknąć przycisk Close (Zamknij).
18. W oknie monitu o ponowne uruchomienie kliknąć Yes (Tak).

Uwaga Tworzenie migawki maszyny wirtualnej po ponownym uruchomieniu

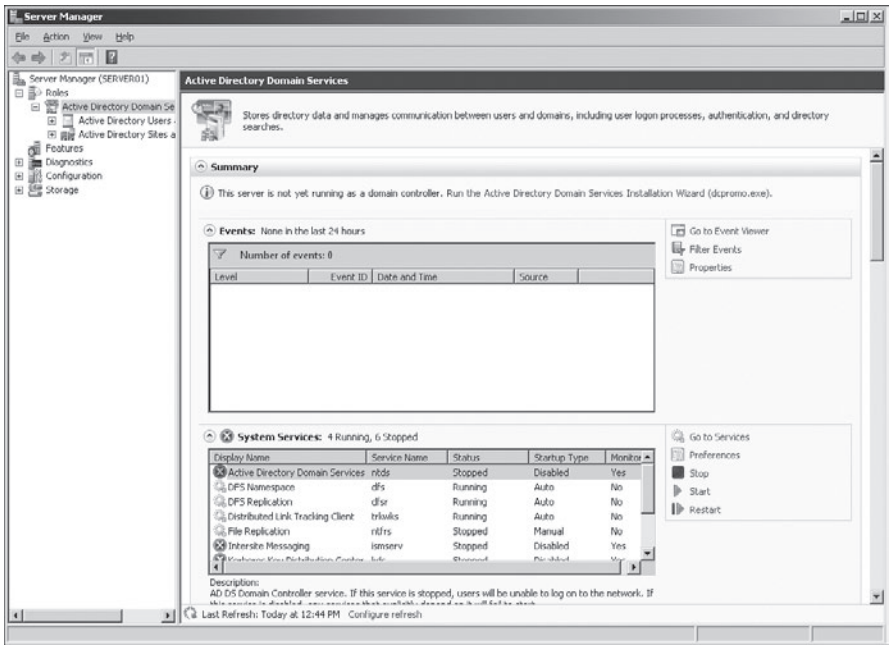
W przypadku korzystania z maszyny wirtualnej do wykonywania tego ćwiczenia i jeśli maszyna wirtualna pozwala na tworzenie migawek zapamiętujących stan maszyny w danym momencie, należy teraz utworzyć taką migawkę. Bazowa instalacja systemu Windows Server 2008 R2 będzie mogła być wykorzystana do wykonywania ćwiczeń w tym rozdziale, co umożliwi nam eksperymentowanie z różnymi metodami dodawania roli AD DS.

▶ Ćwiczenie 3: Instalacja nowego lasu Windows Server 2008 przy użyciu interfejsu Windows

W tym ćwiczeniu dodamy rolę AD DS do serwera, który zainstalowaliśmy i skonfigurowaliśmy w ćwiczeniu 1 „Instalacja systemu Windows Server 2008 R2" i ćwiczeniu 2 „Wykonywanie konfiguracji po instalacji".

1. Zalogować się na serwerze w oparciu o konto Administrator i hasło użyte w ćwiczeniu 1. Jeśli okno Server Manager (Menedżer serwera) nie jest otwarte, to należy je otworzyć z grupy programów Administrative Tools (Narzędzia administracyjne).
2. W sekcji Roles Summary (Podsumowanie ról) na stronie głównej należy kliknąć opcję Add Roles (Dodaj role). Aby wyświetlić sekcję Roles Summary, może zachodzić potrzeba przewinięcia ekranu w dół.
3. Na pierwszej stronie kreatora dodawania ról (Add Roles Wizard) kliknąć przycisk Next (Dalej).
4. Na stronie Select Server Roles (Wybieranie ról serwera) należy zaznaczyć pole wyboru obok opcji Active Directory Domain Services (Usługi domenowe w usłudze Active Directory). Kliknąć Next (Dalej).

5. Aby kontynuować, w oknie monitu dodania wymaganych funkcji usług AD DS kliknąć Add Required Features (Dodaj wymagane funkcje).
6. Na stronie Select Server Role (Wybór ról serwera) kliknąć Next.
7. Na stronie Active Directory Domain Services (Usługi domenowe w usłudze Active Directory) należy kliknąć Next.
8. Na stronie Confirm Installation Selections (Potwierdzanie opcji instalacji) należy kliknąć Install (Zainstaluj).
   Strona Installation Progress (Postęp instalacji) będzie informować o stanie zadań instalacyjnych.
9. Na stronie Installation Results (Wyniki instalacji) należy potwierdzić, że instalacja się powiodła i kliknąć Close (Zamknij).
   W sekcji Roles Summary (Podsumowanie ról) na stronie głównej aplikacji Server Manager (Menedżer serwera) można zauważyć komunikat o błędzie wskazywany przez czerwone kółko z białym znakiem x. Można też zauważyć komunikat w sekcji Active Directory Domain Services (Usługi domenowe w usłudze Active Directory) na tej stronie. Oba te łącza poprowadzą nas do strony roli Active Directory Domain Services (Usługi domenowe w usłudze Active Directory) w oknie Server Manager (Menedżer serwera), pokazanej na rysunku 1-8. Wyświetlany tam komunikat przypomina, że trzeba uruchomić narzędzie *Dcpromo.exe*, co zrobimy w następnym ćwiczeniu.



Rysunek 1-8 Strona roli Active Directory Domain Services (Usługi domenowe w usłudze Active Directory) w oknie Server Manager (Menedżer serwera)

▶ Ćwiczenie 4: Instalacja nowego lasu Windows Server 2008 R2

W tym ćwiczeniu skorzystamy z narzędzia *Dcpromo.exe* – Active Directory Domain Services Installation Wizard (Kreator instalacji usług domenowych w usłudze Active Directory) w celu utworzenia nowego lasu Windows Server 2008 R2.

1. Kliknąć Start, kliknąć Run (Uruchom), wpisać **Dcpromo.exe**, a następnie kliknąć OK.

   Uwaga Dcpromo doda rolę AD DS w razie potrzeby

   W poprzednim ćwiczeniu dodaliśmy rolę AD DS używając programu Server Manager (Menedżer serwera). Jeśli jednak uruchomimy narzędzie *Dcpromo.exe* na serwerze, który nie ma jeszcze zainstalowanej roli AD DS, to *Dcpromo.exe* automatycznie zainstaluje tę rolę.

   Pojawi się okno Active Directory Domain Services Installation Wizard (Kreator instalacji usług domenowych w usłudze Active Directory). W rozdziale 10 poznamy zaawansowane tryby tego kreatora.
2. Kliknąć Next (Dalej).
3. Na stronie Operating System Compatibility (Zgodność systemu operacyjnego) należy przejrzeć ostrzeżenie na temat domyślnych ustawień zabezpieczeń dla kontrolerów domeny Windows Server 2008 R2, a następnie kliknąć Next (Dalej).
4. Na stronie Choose a Deployment Configuration (Wybieranie konfiguracji wdrażania) należy zaznaczyć opcję Create A New Domain In A New Forest (Utwórz nową domenę w nowym lesie) i kliknąć Next (Dalej).
5. Na stronie Name The Forest Root Domain (Nadawanie nazwy domenie głównej lasu) należy wpisać **contoso.com**, a następnie kliknąć Next (Dalej).
   System dokona sprawdzenia, że takie nazwy DNS i NetBIOS nie są jeszcze w użyciu w sieci.
6. Na stronie Set Forest Functional Level (Ustawianie poziomu funkcjonalności lasu) należy wybrać Windows Server 2008 R2, a następnie kliknąć Next (Dalej).
   Każdy z poziomów funkcjonalności jest opisany w polu Details (Szczegóły) na tej stronie. Wybranie poziomu funkcjonalności lasu Windows Server 2008 R2 zapewnia, że wszystkie domeny w tym lesie będą działać na poziomie funkcjonalności domeny Windows Server 2008 R2, co zapewni kilka nowych funkcji oferowanych przez system Windows Server 2008 R2. W rozdziale 12 dowiemy się więcej na temat poziomów funkcjonalności.
   Pojawi się strona Additional Domain Controller Options (Dodatkowe opcje kontrolera domeny). Domyślnie zaznaczona jest opcja DNS Server (Serwer DNS). Kreator Active Directory Domain Services Installation Wizard (Kreator instalacji usług domenowych w usłudze Active Directory) utworzy infrastrukturę DNS podczas instalacji AD DS. Pierwszy kontroler domeny w lesie musi być serwerem wykazu globalnego (GC) i nie może być kontrolerem domeny tylko do odczytu (RODC).
7. Kliknąć Next (Dalej).
   Pojawi się ostrzeżenie informujące, że nie można było utworzyć delegowania dla serwera DNS. W kontekście tego ćwiczenia możemy pominąć ten błąd. Delegacje domen DNS będą omawiane w rozdziale 9. Kliknąć Yes, by kontynuować działanie.

8. Na stronie Location For Database, Log Files, And SYSVOL (Lokalizacja bazy danych, plików dziennika i folderu SYSVOL) należy zaakceptować domyślne lokalizacje dla pliku bazy danych, plików dziennika usługi katalogowej i plików SYSVOL, a następnie kliknąć Next (Dalej).
   Najlepszą praktyką w środowisku produkcyjnym jest przechowywanie tych plików na trzech oddzielnych woluminach, które nie zawierają aplikacji ani innych plików niezwiązanych z usługami AD DS. Takie podejście poprawia wydajność i zwiększa efektywność wykonywania i przywracania kopii zapasowych.
8. Kliknąć odpowiedź Yes, The Computer Will Use A Dynamically Assigned IP Address (Not Recommended) (Tak, na tym komputerze będzie używany dynamicznie przypisywany adres IP (niezalecane)).
   Pojawi się ostrzeżenie informujące, że nie można utworzyć delegowania dla tego serwera DNS. W kontekście tego ćwiczenia można zignorować ten błąd. Delegowanie domen DNS zostanie omówione w rozdziale 9.
9. Na stronie Directory Services Restore Mode Administrator Password (Hasło administratora trybu przywracania Usług katalogowych) należy wpisać silne hasło zarówno w polu Password (Hasło), jak i w polu Confirmed Password (Potwierdź hasło). Kliknąć Next.
   Nie można zapomnieć hasła przypisanego do konta administratora trybu przywracania usług katalogowych.
10. Na stronie Summary (Podsumowanie) należy przejrzeć dokonane wybory.
    Jeśli jakieś ustawienia są nieprawidłowe, należy kliknąć Back (Wstecz), aby dokonać modyfikacji.
13. Kliknąć Next, a następnie Finish (Zakończ).
    Rozpocznie się konfigurowanie usług AD DS. Serwer będzie wymagał ponownego uruchomienia, gdy proces ten się zakończy.

Podsumowanie lekcji

- Usługi Active Directory obejmują zintegrowane rozwiązanie do zarządzania tożsamością i dostępem w sieciach firmowych.
- Usługi AD DS – Active Directory Domain Services (Usługi domenowe w usłudze Active Directory) zapewniają usługi katalogowe i składniki uwierzytelniania infrastruktury IDA. Dodatkowo usługi AD DS ułatwiają zarządzanie nawet dużymi i skomplikowanymi sieciami rozproszonymi.
- Systemy Windows Server 2008 są konfigurowane na bazie ról, które odgrywają. Rolę AD DS można dodać korzystając z aplikacji Server Manager (Menedżer serwera).
- W celu skonfigurowania usług AD DS i utworzenia kontrolera domeny można skorzystać z narzędzia *Dcpromo.exe*.

Pytania do lekcji

Poniższe pytania można wykorzystać do przetestowania swojej wiedzy na temat informacji zawartych w lekcji 1 „Instalowanie usług Active Directory Domain Services”. Pytania są również dostępne na dołączonym do książki dysku CD, jeśli łatwiej jest Czytelnikowi przeglądać je w postaci elektronicznej.

Uwaga Odpowiedzi

Odpowiedzi na te pytania i wyjaśnienia, dlaczego dany wybór odpowiedzi jest poprawny lub niepoprawny, można znaleźć w części „Odpowiedzi" na końcu tej książki.

1. Które z następujących elementów są wymagane do udanego utworzenia kontrolera domeny? (każda prawidłowa odpowiedź stanowi część rozwiązania, należy wybrać wszystkie poprawne odpowiedzi).
   - **A.** Prawidłowa nazwa domeny DNS
   - **B.** Prawidłowa nazwa NetBIOS
   - **C.** Serwer DHCP przypisujący adres IP kontrolerowi domeny
   - **D.** Serwer DNS
2. Firma Trey Research przejęła niedawno firmę Litware, Inc. Z powodu kwestii prawnych związanych z replikacją danych postanowiono skonfigurować domenę potomną w lesie dla użytkowników i komputerów Litware. Las Trey Research obecnie zawiera tylko kontrolery domeny Windows Server 2008 R2. Nowa domena zostanie utworzona poprzez awansowanie kontrolera domeny Windows Server 2008 R2, ale konieczne może być wykorzystanie istniejących systemów Windows Server 2003 jako kontrolerów domeny w domenie Litware. Które poziomy funkcjonalności będą właściwe do skonfigurowania?
   - **A.** Poziom funkcjonalności lasu Windows Server 2008 R2 i poziom funkcjonalności domeny Windows Server 2008 R2 dla domeny Litware
   - **B.** Poziom funkcjonalności lasu Windows Server 2008 R2 i poziom funkcjonalności domeny Windows Server 2003 dla domeny Litware
   - **C.** Poziom funkcjonalności lasu Windows Server 2003 i poziom funkcjonalności domeny Windows Server 2008 R2 dla domeny Litware
   - **D.** Poziom funkcjonalności lasu Windows Server 2003 i poziom funkcjonalności domeny Windows Server 2003 dla domeny Litware

Lekcja 2: Usługi Active Directory Domain Services w instalacji Server Core

Bezpieczeństwo to bardzo istotna kwestia procesu wdrażania serwerów z zainstalowaną rolą AD DS (Active Directory Domain Services) z powodu poufnej natury informacji przechowywanych w katalogu – zwłaszcza haseł i danych osobowych użytkowników. Chociaż konfigurowanie systemu Windows Server 2008 R2 oparte na rolach ogranicza powierzchnię ataku serwera dzięki instalowaniu tylko tych składników i usług, które są wymagane przez jego role, to możliwe jest dalsze ograniczenie obszarów ataku przez zainstalowanie wydania Server Core systemu. Instalacja Server Core jest minimalną instalacją systemu Windows, gdzie zainstalowane zostają jedynie najważniejsze składniki wymagane do działania systemu Windows Server 2008 R2. Większość elementów interfejsu graficznego (GUI) nie jest instalowanych, co ogranicza możliwości złośliwych użytkowników, którzy chcą uzyskać dostęp do serwera przy użyciu znanego im interfejsu Windows Explorer.

Dla większości typowych zadań można zdalnie administrować instalacją Server Core korzystając z narzędzi interfejsu graficznego, takiego jak Server Manager. Jednakże w celu lokalnego zarządzania serwerem i zainstalowanymi jego rolami trzeba korzystać z narzędzi wiersza polecenia. W tej lekcji poznamy opcje instalacji systemu Server Core. Dowiemy się też, jak konfigurować kontroler domeny w wierszu poleceń i jak usunąć kontrolery domeny z domeny.

Po ukończeniu tej lekcji Czytelnik będzie umiał:

- Zidentyfikować zalety i funkcjonalność instalacji Server Core.
- Zainstalować i skonfigurować Server Core.
- Dodawać i usuwać usługi AD DS – Active Directory Domain Services (Usługi domenowe w usługach Active Directory), korzystając z narzędzi wiersza polecenia.

Przewidywany czas trwania lekcji: 60 minut

Zrozumienie działania systemu Server Core

System Windows Server 2008 R2 Server Core, znany lepiej jako Server Core, jest minimalną instalacją systemu Windows, która zajmuje około 3 GB miejsca na dysku i wymaga mniej niż 256 MB pamięci. Instalacja Server Core ogranicza role serwerowe i funkcje, które można dodać, ale może poprawić bezpieczeństwo i łatwość zarządzania serwerem, ograniczając jego powierzchnię ataku. Liczba usług i składników mogących działać jednocześnie jest ograniczona, więc istnieje mniej możliwości dla intruza na zagrożenie serwerowi. Server Core zmniejsza również problemy z zarządzaniem serwerem, ponieważ wymaga mniej aktualizacji i mniej działań związanych z konserwacją systemu.

Server Core może obsługiwać następujące role serwera:

- Active Directory Domain Services (Usługi domenowe w usłudze Active Directory)
- Active Directory Certificate Services (Usługi certyfikatów w usłudze Active Directory)
- Active Directory Lightweight Directory Services (Usługi LDS w usłudze Active Directory)

- BranchCache Hosted Cache (usługi buforowania na serwerze zdalnych treści)
- Dynamic Host Configuration Protocol (DHCP) Server (Serwer DHCP)
- DNS Server (Serwer DNS)
- File Services (Usługi plików)
- Print Server (Usługi drukowania)
- Streaming Media Services (Usługi multimediów strumieniowych)
- Web Server (IIS) (Serwer sieci Web (IIS) – w tym możliwość zainstalowania podzbioru funkcji ASP.NET
- Hyper-V (Windows Server Virtualization)

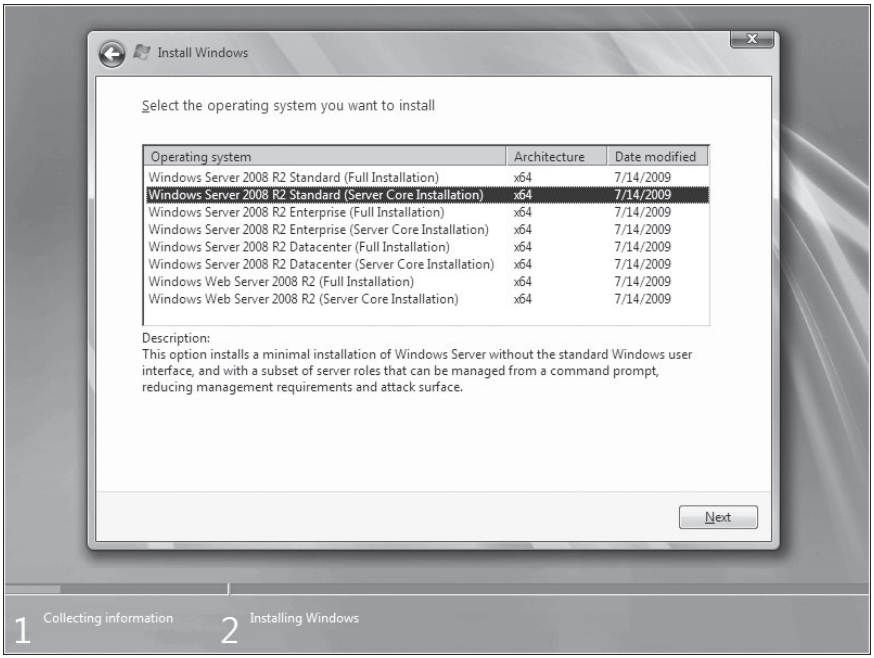
Server Core może również opcjonalnie obsługiwać następujące funkcje:

- Failover Clustering (Klaster pracy awaryjnej)
- Network Load Balancing (Równoważenie obciążenia sieciowego)
- Subsystem for UNIX-based applications (Podsystem aplikacji systemu UNIX)
- Windows Server Backup (Kopia zapasowa serwera)
- Multipath I/O (Wielościeżkowe We/Wy)
- Removable Storage Management (Menedżer magazynu wymiennego)
- Windows Bitlocker Drive Encryption (Szyfrowanie dysków funkcją BitLocker)
- Simple Network Management Protocol (Usługi SNMP)
- Windows Internet Naming Service (Serwer WINS)
- Telnet client (Klient Telnet)
- Quality of Service (QoS)
- Windows-on-Windows 64 (funkcja WoW64 umożliwia uruchamianie aplikacji 32-bitowych w środowisku 64-bitowym)
- Windows PowerShell

Instalowanie Server Core

Server Core można zainstalować korzystając z tych samych kroków, które zostały przedstawione w ćwiczeniu 1 w lekcji 1. Poniżej wymieniono różnice pomiędzy instalacją pełną Windows Server 2008 R2 a instalacją Server Core:

- Trzeba wybrać opcję instalacji Server Core w oknie kreatora instalacji systemu Windows Server 2008 R2 (rysunek 1-9).
- Po zakończeniu instalacji i zalogowaniu się w systemie pojawia się wiersz polecenia zamiast pełnego interfejsu graficznego systemu Windows Server 2008 R2.



Rysunek 1-9 Strona wyboru systemów operacyjnych w oknie kreatora Install Windows (Instaluję system Windows)

Wykonywanie zadań konfiguracji początkowej

W pełnej instalacji Windows Server 2008 R2 pojawia się okno Initial Configuration Tasks (Zadania konfiguracji początkowej) prowadzące nas przez konfigurację serwera po instalacji. Server Core nie zapewnia graficznego interfejsu użytkownika, trzeba więc wykonywać te zadania korzystając z narzędzi wiersza polecenia. Tabela 1-1 wymienia typowe zadania konfiguracyjne i polecenia, z których można skorzystać. Aby dowiedzieć się więcej na temat dowolnego z tych poleceń, należy otworzyć wiersz polecenia i wpisać nazwę polecenia z przełącznikiem **/?**.

Tabela 1-1 Polecenia konfiguracyjne Server Core

Zadanie	Polecenie
Zmiana hasła administratora	*Net user administrator ** (* wyświetla monit o dotychczasowe hasło)
Ustawienie konfiguracji statycznej dla protokołu IPv4	*Netsh interface ipv4*
Aktywacja serwera Windows	*Cscript c:\windows\system32\slmgr.vbs –ato*
Dołączenie komputera do domeny	*Netdom*
Wyświetlanie zainstalowanych ról, składników i funkcji	*Oclist.exe*
Włączanie Pulpitu zdalnego	*Cscript c:\windows\system32\scregedit.wsf /AR 0*

Tabela 1-1 Polecenia konfiguracyjne Server Core

Zadanie	Polecenie
Instalowanie składników opcjonalnych (role, usługi ról lub funkcje)	*Ocsetup.exe* <pakiet lub funkcja> Należy zwrócić uwagę, że w nazwach pakietów lub funkcji istotne są różnice między wielkimi i małymi literami. Listę prawidłowych nazw pakietów i funkcji można wyświetlić za pomocą polecenia Ocsetup /?.
Awansowanie kontrolera domeny	*Dcpromo.exe*
Konfigurowanie DNS	*Dnscmd.exe*
Konfigurowanie DFS	*Dfscmd.exe*

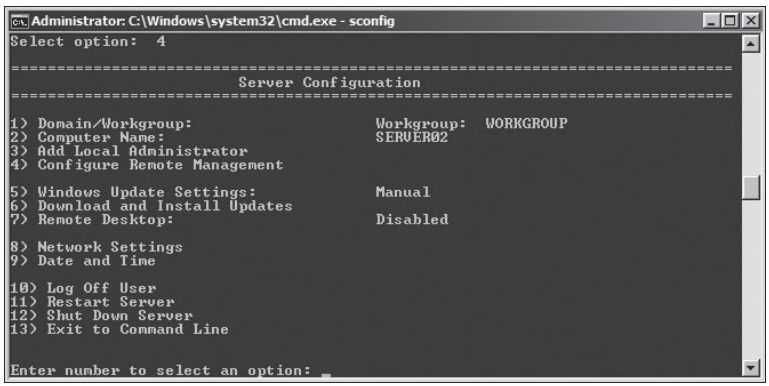
Polecenie *Ocsetup.exe* jest używane do dodawania do serwera obsługiwanych ról i funkcji systemu Server Core. Wyjątkiem od tej reguły jest rola AD DS. Nie należy używać *Ocsetup.exe* w celu dodawania lub usuwania usług AD DS. Zamiast tego należy korzystać z *Dcpromo.exe*.

Konfiguracja serwera

W celu wykonywania podstawowych zadań administracyjnych system Windows Server 2008 R2 wyposażony jest w oparte o menu narzędzie wiersza poleceń nazwane Server Configuration (Konfiguracja serwera), co ilustruje rysunek 1-10. Narzędzie Server Configuration udostępnia prosty zestaw poleceń administracyjnych, które możemy uruchamiać wprowadzając odpowiednie numery wyświetlane w menu i przypisane do wykonywania standardowych funkcji w wierszu poleceń, dzięki czemu nie trzeba ręcznie wpisywać składni tych poleceń. Chociaż narzędzie Server Configuration oszczędza czas w przypadku prostych zadań administracyjnych, bardziej złożone zadania, takie jak konfigurowanie usług AD DS, nadal trzeba będzie wykonywać w wierszu poleceń.

Uwaga Uruchamianie narzędzia Server Configuration

W celu uruchomienia narzędzia Server Configuration w instalacji Server Core systemu Windows Server 2008 R2 należy w wierszu poleceń wpisać sconfig.exe i nacisnąć Enter.



Rysunek 1-10 Okno narzędzia Server Configuration

Dodawanie usług AD DS do instalacji Server Core

Ponieważ w Server Core nie ma narzędzia Active Directory Domain Services Installation Wizard (Kreator instalacji usług domenowych w usłudze Active Directory), to trzeba użyć wiersza polecenia do uruchomienia *Dcpromo.exe* z parametrami konfigurującymi usługi AD DS. Aby poznać parametry polecenia *Dcpromo.exe*, należy otworzyć wiersz polecenia i wpisać **dcpromo.exe /?**. Każdy scenariusz konfiguracji ma dodatkowe informacje na temat jego użycia. Na przykład należy wpisać **dcpromo.exe /?:Promotion**, aby uzyskać szczegółowe instrukcje dotyczące awansowania kontrolera domeny.

Więcej informacji Parametry instalacji nienadzorowanej

Listę parametrów instalacji nienadzorowanej dla usług AD DS można znaleźć pod adresem *http://technet.microsoft.com/en-us/library/cc732086(WS.10).aspx*.

Usuwanie kontrolerów domeny

Czasem może pojawić się powód, aby wyłączyć kontroler domeny w celu przeprowadzenia działań porządkowych lub aby całkiem go usunąć. Ważne jest, aby poprawnie usunąć kontrolera domeny, tak aby informacje o tym kontrolerze domeny zostały wyczyszczone w Active Directory.

Aby usunąć kontrolera domeny, należy skorzystać z polecenia *Dcpromo.exe*. Jeśli uruchomimy to polecenie na kontrolerze domeny korzystając z interfejsu Windows, to okno Active Directory Domain Services Installation Wizard (Kreator instalacji usług domenowych w usłudze Active Directory) przeprowadzi nas przez ten proces. Jeśli chcemy użyć wiersza polecenia lub jeśli usuwamy usługi AD DS z instalacji Server Core, to należy wpisać **dcpromo.exe /?:Demotion** w celu uzyskania informacji na temat parametrów związanych z operacją wyłączania kontrolera domeny.

Przy degradowaniu kontrolera domeny trzeba podać hasło, które będzie przypisane do lokalnego konta administratora na serwerze po degradacji kontrolera domeny.

Zadanie Instalowanie kontrolera domeny w systemie Server Core

W tym ćwiczeniu dodamy kontroler domeny do lasu *contoso.com*, który utworzyliśmy w ćwiczeniach z lekcji 1. Aby zwiększyć bezpieczeństwo i ograniczyć koszty zarządzania nowym kontrolerem domeny, awansujemy serwer działający pod kontrolą Server Core na kontrolera domeny. Przed wykonaniem tych ćwiczeń trzeba mieć ukończone ćwiczenia z lekcji 1.

▶ Ćwiczenie 1: Instalacja Server Core

W tym ćwiczeniu zainstalujemy Server Core na komputerze lub maszynie wirtualnej.

1. Wstawić instalacyjną płytę DVD z systemem Windows Server 2008 R2 do napędu. Korzystając z maszyny wirtualnej można zastosować opcję podłączenia obrazu ISO instalacyjnej płyty DVD. Wskazówek należy szukać w pliku pomocy do oprogramowania maszyn wirtualnych.

2. Uruchomić system.
   Jeśli dysk twardy jest pusty, system powinien uruchomić się z płyty DVD. Jeśli na dysku twardym są jakieś dane, to może pojawić się monit o naciśnięcie klawisza w celu uruchomienia systemu z płyty DVD.

   Jeśli system nie uruchomi się z płyty DVD, ani nie zaoferuje menu uruchamiania systemu, należy przejść do ustawień systemu BIOS komputera i skonfigurować kolejność uruchamiania systemu w celu zapewnienia, że system zostanie uruchomiony z płyty DVD.
3. Wybrać język, ustawienia regionalne i układ klawiatury odpowiadające danemu systemowi, a następnie kliknąć Next (Dalej).
4. Kliknąć Install Now (Zainstaluj teraz).
5. Wybrać opcję Windows Server 2008 R2 Standard (Server Core Installation) i kliknąć Next (Dalej).
6. Zaznaczyć pole wyboru I Accept The License Terms (Akceptuję postanowienia licencyjne) i kliknąć Next (Dalej).
7. Kliknąć opcję Custom (Advanced) (Niestandardowa (Zaawansowana)).
8. Na stronie Where Do You Want to Install Windows (Gdzie chcesz zainstalować system Windows) należy wybrać dysk, na którym chcemy zainstalować system Windows Server 2008 R2.
   Jeśli trzeba utworzyć, skasować, rozszerzyć lub sformatować partycje, albo jeśli trzeba załadować niestandardowy sterownik pamięci masowej w celu uzyskania dostępu do podsystemu dyskowego, należy kliknąć Driver Options (Advanced) (Opcje sterownika (Zaawansowane)).
9. Kliknąć Next (Dalej).
10. Po zakończeniu instalacji pojawi się monit dotyczący zmiany hasła Administratora. Kliknąć OK.
11. Wpisać hasło konta Administrator w polach New Password (Nowe hasło) i Confirm Password (Potwierdź hasło) oraz nacisnąć Enter.
    Hasło musi się składać co najmniej z siedmiu znaków i musi zawierać co najmniej trzy spośród czterech typów znaków:
    - ❑ Wielkie litery: A-Z
    - ❑ Małe litery: a-z
    - ❑ Cyfry: 0-9
    - ❑ Znaki niealfanumeryczne: symbole takie jak $, #, @ i !

    Uwaga Nie można zapomnieć tego hasła

    Bez niego nie będziemy w stanie zalogować się na serwerze w celu wykonania pozostałych ćwiczeń w tym zestawie ćwiczeniowym.
12. Kliknąć OK.
    Pojawi się wiersz polecenia dla konta Administrator.

▶ Ćwiczenie 2: Przeprowadzanie konfiguracji Server Core po instalacji

W tym ćwiczeniu wykonamy konfigurację poinstalacyjną serwera w celu przygotowania nazwy i ustawień TCP/IP dla serwera, wymaganych przez pozostałe ćwiczenia w tej lekcji.

Uwaga Podczas przeprowadzania tych ćwiczeń system SERVER01 musi być uruchomiony – w czasie ćwiczeń system SERVER02 będzie uzyskiwał dostęp do bazy danych AD DS systemu SERVER01.

1. Zmienić nazwę serwera wpisując **netdom renamecomputer %computername% /newname: SERVER02.** Zostaniemy poproszeni o naciśnięcie **Y** w celu potwierdzenia tej operacji.
   Inna metoda skonfigurowania nazwy komputera polega na wpisaniu w wierszu poleceń **sconfig** i użycia menu narzędzia Server Configuration. W obu przypadkach po zmianie nazwy konieczne będzie ponowne uruchomienie komputera. Na tym etapie nie należy ponownie uruchamiać komputera – operacja ta zostanie wykonana pod koniec ćwiczenia.
2. Ustawić adres IPv4 serwera, wpisując kolejno każde z następujących poleceń:

```
netsh interface ipv4 set address name="Local Area Connection"
source=static address=10.0.0.12 mask=255.255.255.0 gateway=10.0.0.1 1

netsh interface ipv4 set dns name="Local Area Connection"
source=static address=10.0.0.11 primary
```

3. Potwierdzić wprowadzoną konfigurację IP, używając polecenia **ipconfig /all**.
4. Ponownie uruchomić komputer, wpisując **shutdown –r –t 0**.
5. Zalogować się jako Administrator.
6. Przyłączyć się do domeny za pomocą polecenia **netdom join %computername% /domain: contoso.com**.
7. Ponownie uruchomić komputer, wpisując **shutdown –r –t 0**, a następnie ponownie zalogować się jako Administrator.
8. Wyświetlić zainstalowane role serwera, wpisując **oclist**.
   Należy zwrócić uwagę na identyfikator pakietu dla roli serwera DNS: DNS-Server-Core-Role.
9. Wpisać **ocsetup** i nacisnąć Enter.
   Niespodzianka! Jest jakiś graficzny interfejs użytkownika w Server Core.
10. Kliknąć OK, aby zamknąć okno.
11. Wpisać **ocsetup DNS-Server-Core-Role**.
    W identyfikatorach pakietów rozróżniane są wielkie i małe litery.
12. Wpisać **oclist** i upewnić się, że rola serwera DNS jest zainstalowana.

▶ Ćwiczenie 3: Tworzenie kontrolera domeny w systemie Server Core

W tym ćwiczeniu dodamy rolę AD DS do instalacji Server Core, korzystając z polecenia *Dcpromo.exe*.

1. Wpisać **dcpromo.exe /?** i nacisnąć Enter, aby przejrzeć wyświetlone informacje na temat użycia tego polecenia.
2. Wpisać **dcpromo.exe /?:Promotion** i nacisnąć Enter.
   Należy przejrzeć wyświetlone informacje na temat użycia tego polecenia.
3. Wpisać następujące polecenie, aby dodać i skonfigurować rolę AD DS:

   ```
   dcpromo /unattend /replicaOrNewDomain:replica
   /replicaDomainDNSName:contoso.com /ConfirmGC:Yes
   /UserName:CONTOSO\Adminsitrator /Password:* /safeModeAdminPassword:P@ssword
   ```

   gdzie * to hasło użyte w ćwiczeniu 1.
4. Po wyświetleniu monitu o wprowadzenie poświadczeń sieciowych należy wpisać hasło konta administratora w domenie *contoso.com* i kliknąć OK.
   Rola AD DS zostanie zainstalowana i skonfigurowana, a serwer zostanie ponownie uruchomiony.

▶ Ćwiczenie 4: Usuwanie kontrolera domeny

W tym ćwiczeniu usuniemy usługi AD DS z instalacji Server Core.

1. Zalogować się w instalacji Server Core jako Administrator.
2. Wpisać **dcpromo /unattend /AdministratorPassword:*hasło***, gdzie *hasło* jest silnym hasłem, które stanie się hasłem lokalnego administratora serwera po usunięciu usług AD DS. Nacisnąć Enter.

Podsumowanie lekcji

- Instalacja Windows Server 2008 R2 Server Core, znana lepiej jako Server Core, jest minimalną instalacją systemu Windows, która obsługuje podzbiór ról i funkcji serwera.
- Server Core może poprawić bezpieczeństwo i sposób zarządzania serwerami Windows.
- Polecenie *Ocsetup.exe* służy do dodawania i usuwania ról Server Core z wyjątkiem roli AD DS, która jest dodawana przy użyciu *Dcpromo.exe*.
- Można w pełni konfigurować automatyczną operację awansu lub degradacji kontrolera domeny, korzystając z polecenia *Dcpromo.exe /unattend* z parametrami odpowiednimi dla tej operacji.

Pytania do lekcji

Poniższe pytania można wykorzystać do przetestowania swojej wiedzy na temat informacji zawartych w lekcji 2 „Usługi Active Directory Domain Services w instalacji Server Core".

Uwaga Odpowiedzi

Odpowiedzi na te pytania i wyjaśnienia, dlaczego dany wybór odpowiedzi jest poprawny lub niepoprawny, można znaleźć w części „Odpowiedzi" na końcu tej książki.

1. Jesteśmy zalogowani jako Administrator na komputerze SERVER02, jednym z czterech kontrolerów domeny *contoso.com* działającym pod kontrolą Server Core. Chcemy zdegradować tego kontrolera domeny. Które z poniższych informacji będą wymagane?
   - **A.** Hasło lokalnego administratora
   - **B.** Poświadczenia dla użytkownika z grupy Domain Admins (Administratorzy domeny)
   - **C.** Poświadczenia dla użytkownika z grupy Domain Controllers (Kontrolery domeny)
   - **D.** Adres serwera DNS
2. SERVER02 działa pod kontrolą Server Core. Jest już skonfigurowana na nim rola AD DS. Chcemy dodać rolę AD CS – Active Directory Certificate Services (Usługi certyfikatów w usłudze Active Directory) do serwera. Co trzeba zrobić?
   - **A.** Zainstalować rolę Active Directory Certificate Services (Usługi certyfikatów w usłudze Active Directory)
   - **B.** Zainstalować rolę Active Directory Federation Services (AD FS)
   - **C.** Zainstalować rolę AD RMS (Usługi zarządzania prawami dostępu w usłudze Active Directory)
   - **D.** Przeinstalować serwer jako Windows Server 2008 R2 (Full Installation)

Przegląd rozdziału

Aby dalej ćwiczyć i utrwalać umiejętności poznane w tym rozdziale, można wykonać następujące zadania:

- Przejrzeć podsumowanie rozdziału.
- Przejrzeć listę kluczowych terminów wprowadzonych w tym rozdziale.
- Wykonać przykładowy scenariusz. Ten scenariusz przedstawia rzeczywistą sytuację związaną z tematami tego rozdziału i wymaga stworzenia rozwiązań.
- Przystąpić do testu ćwiczeniowego.

Podsumowanie rozdziału

- Usługi Active Directory pełnią funkcje zarządzające tożsamością i dostępem służące do obsługi sieci organizacji.
- Kontroler domeny utrzymuje magazyn danych Active Directory oraz powiązane z nim usługi. Kontrolery domeny są tworzone przez dodanie roli AD DS, a następnie skonfigurowanie usług AD DS przy użyciu *Dcpromo.exe*
- Server Core umożliwia zredukowanie kosztów zarządzania i zwiększenie bezpieczeństwa kontrolerów domeny.

Kluczowe terminy

Można wykorzystać te terminy kluczowe, aby lepiej zrozumieć pojęcia omówione w tym rozdziale.

- **uwierzytelnianie**
- **domena**
- **las**
- **domena główna lasu**
- **poziom funkcjonalności**
- **wykaz globalny (lub częściowy zbiór atrybutów)**
- **magazyn tożsamości**
- **Kerberos**
- **schemat**
- **lokacja**

Scenariusz przykładowy

W poniższym scenariuszu przykładowym zastosujemy to, czego dowiedzieliśmy się o instalacji Server Core i powiązanych usługach Active Directory Domain Services. Odpowiedzi na te pytania można znaleźć w sekcji „Odpowiedzi" na końcu tej książki.

Scenariusz przykładowy: Tworzenie lasu Active Directory

Zostaliśmy poproszeni o utworzenie nowego lasu Active Directory dla nowego projektu badawczego w Trey Research. Z powodu wrażliwej natury projektu trzeba zapewnić, żeby katalog był jak najlepiej zabezpieczony. Rozważamy opcję wykorzystania instalacji Server Core na dwóch serwerach, które będą działać jako kontrolery domeny.

1. Czy można utworzyć las Active Directory korzystając tylko z serwerów Server Core?
2. Jakiego polecenia trzeba użyć do skonfigurowania statycznych adresów IP na tych serwerach?
3. Jakiego polecenia musimy użyć, aby dodać rolę serwera DNS?
4. Jakiego polecenia użyjemy, aby dodać rolę Active Directory Domain Services (Usługi domenowe w usłudze Active Directory)?

Test ćwiczeniowy

Testy ćwiczeniowe na płycie CD dołączonej do tej książki oferują wiele opcji. Na przykład można sprawdzić swoją wiedzę tylko pod kątem jednego celu egzaminacyjnego lub sprawdzić swoją wiedzę z całej zawartości egzaminu certyfikacyjnego 70-640. Można skonfigurować test tak, aby w sposób zbliżony symulował doświadczenie zdawania prawdziwego egzaminu certyfikacyjnego lub też można skonfigurować go w trybie nauki, tak aby można było po odpowiedzi na każde pytanie oglądać prawidłowe odpowiedzi i wyjaśnienia do nich.

Więcej informacji Testy ćwiczeniowe

Szczegóły dotyczące dostępnych opcji testów ćwiczeniowych można znaleźć w dziale „Jak korzystać z testów ćwiczeniowych" we wstępie do tej książki.

Rozdział 2

Administrowanie usługami AD DS

Większość administratorów styka się po raz pierwszy z usługami AD DS – Active Directory Domain Services (Usługi domenowe w usłudze Active Directory) otwierając narzędzie Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) i tworząc obiekty użytkowników, komputerów lub grup w jednostkach organizacyjnych (OU) domeny. Niestety wielu administratorów nie poświęca czasu, by podnosić swoje umiejętności związane z wykorzystywaniem narzędzi administracyjnych usług Active Directory. Niezależnie, czy jesteś administratorem o niewielkim doświadczeniu czy weteranem z wieloletnią praktyką, twoje działania muszą być bezpieczne i efektywne. W tym rozdziale przedstawimy sekrety efektywnej administracji, z którymi często można się zapoznać dopiero po miesiącach czy latach doświadczeń.

Teraz, po utworzeniu domeny w rozdziale 1 „Tworzenie domeny usługi Active Directory", możemy zająć się narzędziami, wskazówkami i najlepszymi rozwiązaniami, dotyczącymi tworzenia i zarządzania użytkowników, komputerów, grup i jednostek organizacyjnych w domenie usług AD DS. W późniejszych rozdziałach szczegółowo zbadamy każdą z tych klas obiektów.

W tym rozdziale przyjrzymy się też dwóm ważnym problemom wysokiego poziomu występującym w przedsiębiorstwie: jak wyszukiwać obiekty w katalogu i jak zapewnić, aby usługi Active Directory były bezpieczne, umożliwiając przy tym pracownikom wykonywanie zadań wymaganych przez ich role.

Umiejętności prezentowane w tym rozdziale:

- Utrzymywanie kont Active Directory

Lekcje w tym rozdziale

Przed rozpoczęciem

Do ukończenia lekcji w tym rozdziale trzeba mieć zainstalowany system Windows Server 2008 R2 na fizycznym komputerze lub maszynie wirtualnej. Maszyna powinna mieć nazwę SERVER01 i powinna być kontrolerem domeny *contoso.com*. Szczegóły tej konfiguracji przedstawiono w rozdziale 1.

Z praktyki

Dan Holme

Wszyscy z pewnością znają narzędzia administracyjne, takie jak przystawka Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory) i mają podstawowe umiejętności wymagane do tworzenia jednostek organizacyjnych, użytkowników, komputerów i grup. W tym rozdziale przejrzymy te narzędzia i umiejętności, abyśmy mogli wypełnić wszelkie luki w swojej wiedzy. Przede wszystkim jednak ten rozdział wprowadzi sposoby na podniesienie własnej produktywności i efektywności jako administratora. Często odkrywam, że wielu administratorów nadal korzysta z domyślnych konsol i dlatego musi otwierać wiele narzędzi do wykonywania swojej pracy, zamiast utworzyć pojedynczą, niestandardową konsolę MMC – Microsoft Management Console (Konsola zarządzania firmy Microsoft), która będzie zawierała wszystkie potrzebne przystawki. Spotykam też administratorów zagłębiających się w swoją strukturę jednostek organizacyjnych w celu wyszukiwania i zarządzania obiektami, zamiast wykorzystania możliwości zapisanych kwerend do wirtualizacji widoku swoich domen. Choć ten rozdział obejmuje tylko jeden cel egzaminacyjny „Utrzymywanie kont Active Directory", to wskazówki tutaj podane są jednymi z najcenniejszych w tej książce, ponieważ pozwolą na efektywniejszą i bezpieczniejszą codzienną pracę w rzeczywistych warunkach korporacyjnych.

Lekcja 1: Praca z przystawkami usług Active Directory

Narzędzia administracyjne usług Active Directory, czyli przystawki, zapewniają funkcjonalność wymaganą do obsługi usług katalogowych. W tej lekcji poznamy i zlokalizujemy najważniejsze przystawki Active Directory. Dowiemy się też, jak efektywnie z nimi pracować, korzystać z alternatywnych poświadczeń i jak budować niestandardowe konsole, które można dystrybuować wśród administratorów w danej organizacji.

Po ukończeniu tej lekcji czytelnik będzie umiał:

- Wykonywać podstawowe zadania administracyjne przy użyciu przystawki Active Directory Users And Computers (Użytkownicy i komputery usług Active Directory).
- Rozpoznać przystawki narzędzia Server Manager i macierzyste konsole używane do administrowania usług AD DS.
- Korzystać z konsoli zarządzania MMC (Microsoft Management Console).
- Zainstalować oprogramowanie RSAT – Remote Server Administration Tools (Narzędzia administracji zdalnej serwera).
- Uruchamiać narzędzia administracyjne z alternatywnymi poświadczeniami, korzystając z opcji Run As Administrator (Uruchom jako administrator).
- Tworzyć, zarządzać i rozprowadzać niestandardową konsolę MMC.

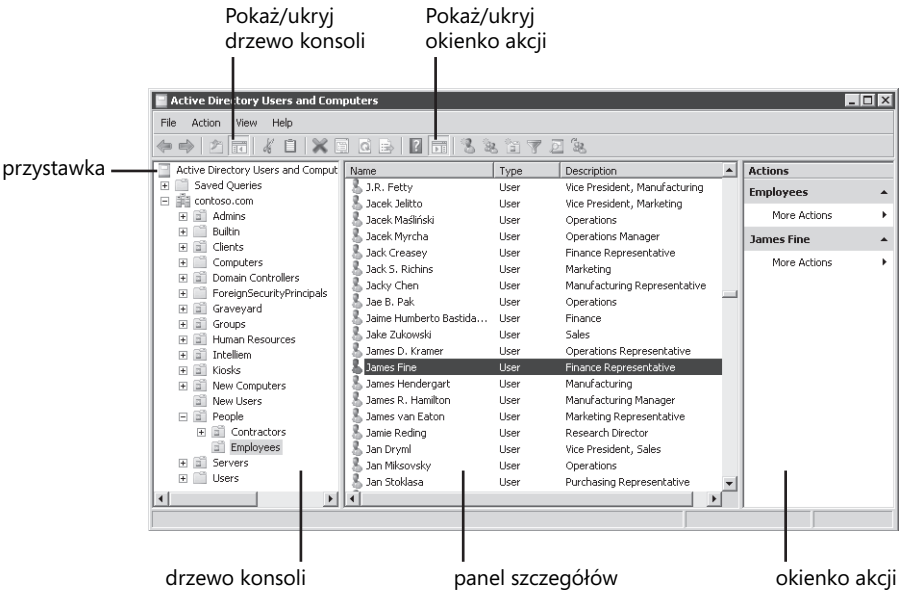
Przewidywany czas trwania lekcji: 35 minut

Zrozumienie narzędzia Microsoft Management Console

Narzędzia administracyjne Windows wykorzystują wspólną konstrukcję zwaną MMC – Microsoft Management Console (Konsola zarządzania firmy Microsoft). Konsola MMC wyświetla narzędzia (nazywane przystawkami) w konfigurowalnym oknie z lewym okienkiem wyświetlającym drzewo konsoli (podobne do drzewa folderów Eksploratora Windows) i środkowym okienkiem wyświetlającym szczegóły. Okienko Actions (Akcje) z prawej strony wyświetla polecenia zwane przez konsolę MMC akcjami. Rysunek 2-1 pokazuje główne składniki konsoli MMC:

- **Drzewo konsoli** Okienko z lewej strony, w którym wyświetlane jest drzewo konsoli; nazywane również okienkiem zakresu.
- **Przycisk paska narzędzi Show/Hide Console Tree (Pokaż/Ukryj drzewo konsoli)** Włączenie lub wyłączenie wyświetlania okienka drzewa konsoli.
- **Przystawki** Narzędzia udostępniające funkcje administracyjne.
- **Okienko szczegółów** W oknie tym wyświetlane są informacje szczegółowe dotyczące wybranych obiektów (zakresu) w trzewie konsoli.
- **Okienko Action (Akcje)** Wyświetlane są tutaj polecenia, które możemy wykonywać dla zakresu wybranego w drzewie konsoli lub dla elementów wybranych w okienku szczegółów.

- **Menu Action** Menu to również wyświetla polecenia, które możemy wykonywać dla wybranego zakresu lub elementu.
- **Menu kontekstowe (nie pokazane)** Menu to wyświetlone zostaje po kliknięciu prawym przyciskiem myszy elementu zakresu lub okienka szczegółów; jest to trzecie miejsce, w którym można wykonywać działania.
- **Przycisk paska narzędzi Show/Hide Action Panel (Pokaż/Ukryj okienko akcji)** Włączenie lub wyłączenie wyświetlania okienka Akcja.
  Aby określać widzialność lewego i prawego okienka, należy skorzystać z przycisków.



Rysunek 2-1 Konsola MMC i przystawka

Konsolę MMC można traktować jako pas z narzędziami, do którego można doczepiać więcej narzędzi (przystawek). Przystawki nie mogą być uruchamiane bezpośrednio; mogą funkcjonować tylko w kontekście konsoli MMC. Większość narzędzi w folderze Administrative Tools (Narzędzia administracyjne) składa się z pojedynczej konsoli z pojedynczą przystawką. Do narzędzi tych należą Event Viewer (Podgląd zdarzeń), Services (Usługi) i Task Scheduler (Harmonogram zadań). Inne narzędzia, takie jak Computer Management (Zarządzanie komputerem), są konsolami, które zawierają wiele przystawek, w tym takie, które istnieją też jako samodzielne konsole. Na przykład konsola Computer Management (Zarządzanie komputerem) zawiera przystawki Event Viewer (Podgląd zdarzeń), Services (Usługi) i Task Scheduler (Harmonogram zadań).

Administrując systemem Windows za pomocą przystawek będziemy wykonywać polecenia zwane *akcjami* przez konsolę MMC, które można znaleźć w menu Action (Akcja) konsoli, w menu kontekstowym pojawiającym się po kliknięciu prawym przyciskiem myszy i w okienku Actions (Akcje) z prawej strony konsoli. Większość doświadczonych administratorów uważa menu kontekstowe za najbardziej wydajny sposób wykonywania działań w przystawce MMC. Jeśli korzysta się wyłącznie z menu kontekstowego, to można

wyłączyć okienko Actions (Akcje), aby mieć większy obszar do wyświetlania informacji w okienku szczegółów.

Istnieją dwa typy konsol MMC: wstępnie skonfigurowane i niestandardowe. Wstępnie skonfigurowane konsole są instalowane automatycznie, gdy dodajemy rolę lub funkcję do obsługiwania administracji tą rolą lub funkcją. Działają w trybie użytkownika, więc nie można ich modyfikować ani zapisywać. Użytkownik może jednak tworzyć niestandardowe konsole, aby zebrać dokładnie te narzędzia i funkcjonalności, które są mu potrzebne. W kolejnych częściach tej lekcji przyjrzymy się zarówno wstępnie skonfigurowanym, jak i niestandardowym konsolom.

Narzędzia administracyjne Active Directory

Większość działań administracyjnych w Active Directory jest wykonywanych za pomocą następujących przystawek i konsol:

- **Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory)** Zarządzanie najpowszechniejszymi codziennymi zasobami, w tym użytkownikami, grupami, komputerami, drukarkami i folderami udostępnionymi. Jest to chyba najczęściej używana przystawka przez administratora Active Directory.
- **Active Directory Sites and Services (Lokacje i usługi Active Directory)** Zarządzanie replikacją, topologią sieci i powiązanymi usługami. Będziemy intensywnie korzystać z tej przystawki w rozdziale 11 „Zarządzanie lokacjami i replikacją usługi Active Directory”.
- **Active Directory Domains and Trusts (Domeny i relacje zaufania usługi Active Directory)** Konfigurowanie i utrzymywanie relacji zaufania oraz poziomów funkcjonalności domeny i lasu. To narzędzie będzie omówione w rozdziale 12 „Zarządzanie wieloma domenami i lasami”.
- **Active Directory Schema (Schemat usługi Active Directory)** Badanie i modyfikowanie definicji atrybutów i klas obiektów Active Directory. Schemat jest planem Active Directory. Jest rzadko przeglądany i jeszcze rzadziej zmieniany. Dlatego przystawka Active Directory Schema (Schemat usługi Active Directory) nie jest domyślnie instalowana.

Konsole i przystawki Active Directory są instalowane, gdy dodajemy rolę AD DS do serwera. Dwa często używane narzędzia administracyjne Active Directory są dodawane do aplikacji Server Manager (Menedżer serwera), gdy instalujemy rolę AD DS: przystawka Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory) oraz przystawka Active Directory Sites and Services (Lokacje i usługi Active Directory). Jednakże do administrowania Active Directory z systemu, który nie jest kontrolerem domeny, trzeba zamontować funkcję RSAT, która może być zainstalowana z węzła Features (Funkcje) aplikacji Server Manager (Menedżer serwera) w systemie Windows Server 2008. Może być ona pobierana z firmy Microsoft i instalowana na klientach działających pod kontrolą Windows Vista Service Pack 1.

Odnajdowanie narzędzi administracyjnych Active Directory

Konsole i przystawki Active Directory są instalowane, gdy dodajemy rolę AD DS do serwera. Dwa często używane narzędzia administracyjne Active Directory są dodawane do aplikacji Server Manager (Menedżer serwera), gdy instalujemy rolę AD DS: przystawka Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory) oraz przystawka Active Directory Sites and Services (Lokacje i usługi Active Directory).

Jednakże do administrowania Active Directory z systemu, który nie jest kontrolerem domeny, trzeba zainstalować funkcję RSAT, co możemy zrobić w węźle Features (Funkcje) aplikacji Server Manager (Menedżer serwera) w systemie Windows Server 2008 lub Windows Server 2008 R2.

Narzędzia RSAT możemy także zainstalować w klienckich systemach Windows – Windows Vista Service Pack 1 (lub nowsze) i Windows 7. W tym celu po prostu pobieramy pliki instalacyjne RSAT udostępnione pod adresem *http://www.microsoft.com/downloads* i postępujemy zgodnie z instrukcjami programu instalacyjnego. Po zainstalowaniu musimy również narzędzia te włączyć, jeśli mają być widoczne. W tym celu posługujemy się poleceniem Turn Windows Features On Or Off (Włącz lub wyłącz funkcje system Windows), które znajduje się w Panelu sterowania w aplikacji Programs And Features (Programy i funkcje).

Po zainstalowaniu i włączeniu wszystkie konsole administracyjne usług Active Directory możemy znaleźć w folderze Administrative Tools (Narzędzia administracyjne), który znajduje się w Panelu sterowania. W przypadku widoku klasycznego Panelu sterowania folder Narzędzia administracyjne jest widoczny bezpośrednio, natomiast w przypadku widoku strony głównej Panelu sterowania narzędzia administracyjne znajdują się w grupie System And Maintenance (System i konserwacja).

Przystawka Active Directory Schema przed dodaniem do konsoli musi być zarejestrowana. Procedura rejestrowania przystawki zamieszczona jest w dalszej części tej lekcji.

Dodawanie narzędzi administracyjnych do menu Start

Domyślnie narzędzia administracyjne nie są dodawane do menu Start dla klientów systemów Windows Vista lub Windows 7. Można ułatwić sobie dostęp do narzędzi administracyjnych, dodając je do menu Start.

1. Kliknąć prawym przyciskiem myszy przycisk Start i wybrać Properties (Właściwości).
2. Kliknąć Customize (Dostosuj).
3. W przypadku korzystania z domyślnego menu Start należy przewinąć zawartość okna w dół do opcji System Administrative Tools (Systemowe narzędzia administracyjne) i zaznaczyć Display On The All Programs Menu And The Start Menu (Wyświetl w menu Wszystkie programy i w menu Start) lub Display On The All Programs Menu (Wyświetl w menu Wszystkie programy). W przypadku korzystania z klasycznego menu Start należy zaznaczyć Display Administrative Tools (Wyświetl polecenie Narzędzia administracyjne).
4. Dwa razy należy kliknąć OK.

Tworzenie niestandardowej konsoli z przystawkami Active Directory

Łatwiej jest administrować systemem Windows, gdy potrzebne narzędzia są w jednym miejscu i można je dostosować, tak aby spełniały nasze potrzeby. Można to osiągnąć tworząc niestandardową administracyjną konsolę MMC, która (kontynuując naszą metaforę z pasem na narzędzia) będzie pasem na narzędzia skrojonym dla nas na miarę. W przypadku tworzenia niestandardowej konsoli MMC można:

- Dodać wiele przystawek, dzięki czemu nie trzeba przełączać się między różnymi konsolami, aby wykonywać swoje zadania i wystarczy uruchamiać tylko jedną konsolę.
- Zapisać konsolę, aby regularnie z niej korzystać.
- Przekazać konsolę innym administratorom.
- Scentralizować konsole w udostępnianym miejscu w celu udostępniania zunifikowanych, niestandardowych narzędzi administracyjnych.

Aby utworzyć niestandardową konsolę MMC:

1. Kliknąć przycisk Start. Następnie w polu Start Search (Rozpocznij wyszukiwanie) wpisać **mmc.exe** i nacisnąć Enter.
2. W menu File (Plik) kliknąć polecenie *Add/Remove Snap-in* (Dodaj/Usuń przystawkę).

Okno dialogowe *Add/Remove Snap-in* (Dodaj/Usuń przystawkę) umożliwia nam dodawanie, usuwanie, zmienianie kolejności i zarządzanie przystawkami konsoli.

Po zainstalowaniu narzędzia RSAT zainstalowane są wszystkie cztery przystawki zarządzania usługami Active Directory, jednakże przystawka Active Directory Schema do momentu jej zarejestrowania nie jest pokazywana w oknie dialogowym Add/Remove Snap-in.

Aby zarejestrować przystawkę Active Directory Schema:

1. Otworzyć okno wiersza poleceń przy użyciu opcji Run As Administrator (Uruchom jako administrator).
2. Wpisać **regsvr32.exe schmmgmt.dll** i nacisnąć Enter.

Zalecane ćwiczenia

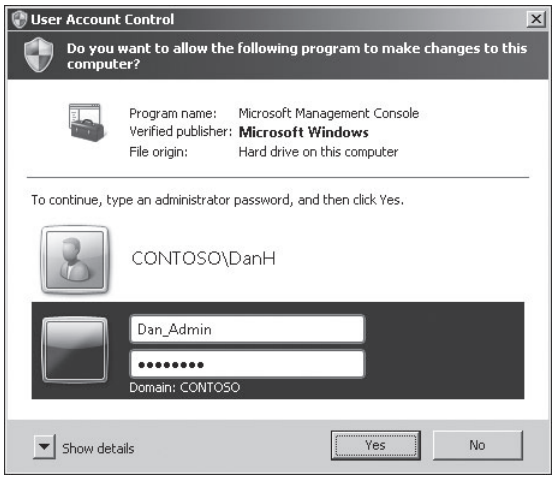
W ćwiczeniu 1 „Tworzenie niestandardowej konsoli MMC", ćwiczeniu 2 „Dodawanie przystawki do konsoli MMC" i ćwiczeniu 3 „Zarządzanie przystawkami konsoli MMC" w zestawie ćwiczeń na końcu tej lekcji będą przedstawione umiejętności związane z tworzeniem niestandardowej konsoli MMC z wieloma przystawkami.

Uruchamianie narzędzi administracyjnych z alternatywnymi poświadczeniami

Wielu administratorów loguje się na swoich komputerach, korzystając ze swoich kont administracyjnych. Taka praktyka jest niebezpieczna, ponieważ konto administracyjne ma więcej uprawnień i dostęp do szerszego zakresu sieci niż konto standardowego użytkownika. Dlatego szkodliwe oprogramowanie uruchomione z poświadczeniami administracyjnymi

może spowodować znaczne szkody. Aby uniknąć tego problemu, nie należy logować się jako administrator. Zamiast tego należy logować się jako standardowy użytkownik i korzystać z funkcji Run As Administrator (Uruchom jako administrator) do uruchamiania narzędzi administracyjnych w kontekście zabezpieczeń konta administracyjnego:

1. Kliknąć skrót do aplikacji, apletu Panelu sterowania lub konsoli MMC, którą chcemy uruchomić, a następnie wybrać opcję Run As Administrator (Uruchom jako administrator). Jeśli to polecenie się nie pojawi, należy spróbować przytrzymać wciśnięty klawisz Shift i ponownie kliknąć prawym przyciskiem myszy.
   Pojawi się okno dialogowe User Account Control (Kontrola konta użytkownika).
2. Kliknąć opcję Use Another Account (Użyj innego konta).
3. Wpisać nazwę użytkownika i hasło dla konta administracyjnego (rysunek 2-2).



Rysunek 2-2 Okno dialogowe User Account Control (Kontrola konta użytkownika) monitujące o poświadczenia administracyjne

3. Kliknąć OK.

Wskazówka Zmniejszenie liczby czynności potrzebnych do uruchamiania narzędzi przy poświadczeniach administracyjnych

Jeśli jakaś aplikacja będzie często uruchamiana w kontekście administratora, należy utworzyć nowy skrót wstępnie skonfigurowany z opcją Run As Administrator (Uruchom jako administrator). Należy utworzyć skrót i otworzyć okno dialogowe Properties (Właściwości) dla tego skrótu. Kliknąć przycisk Advanced (Zaawansowane) i zaznaczyć opcję Run As Administrator (Uruchom jako administrator). Po uruchomieniu tego skrótu pojawiać się będzie okno dialogowe User Account Control (Kontrola konta użytkownika).

W systemach Windows 7 i Windows Server 2008 R2 istnieje inna metoda uruchamiania narzędzi administracyjnych. Należy nacisnąć i przytrzymać klawisz Shift i kliknąć prawym przyciskiem myszy skrót do narzędzia administracyjnego w menu Start, a następnie kliknąć polecenie Run As Different User (Uruchom jako inny użytkownik).

Zapisywanie i rozprowadzanie konsoli niestandardowej

Jeśli planujemy dystrybucję konsoli, zaleca się zapisanie tej konsoli w trybie użytkownika. Aby zmienić tryb konsoli, należy wybrać Options (Opcje) z menu File (Plik). Domyślnie nowe konsole są zapisywane w trybie autorskim, który umożliwia dodawanie i usuwanie przystawek, przeglądanie wszystkich fragmentów drzewa konsoli i zapisywanie ustawień niestandardowych. Tryb użytkownika z kolei ogranicza funkcjonalność konsoli, tak aby nie można jej było modyfikować. Istnieją trzy typy trybów użytkownika opisane w tabeli 2-1. Tryb użytkownika – pełny dostęp: jest zwykle wybierany dla konsoli udostępnianej biegłym administratorom wykonującym różnorodne zadania wymagające szerokiego użycia przystawek konsoli. Tryb użytkownika – ograniczony dostęp (wiele okien lub jedno okno): jest trybem zablokowanym i dlatego jest wybierany dla konsoli udostępnianej administratorom z węższym zakresem zadań do wykonania.

Tabela 2-1 Tryby konsoli MMC

Tryb	Stosować, gdy
Tryb autorski	Chcemy kontynuować dostosowywanie konsoli.
Tryb użytkownika – pełny dostęp	Chcemy, aby użytkownicy konsoli byli w stanie korzystać ze wszystkich przystawek i nawigować pomiędzy nimi. Użytkownicy nie będą w stanie dodawać lub usuwać przystawek ani zmieniać właściwości przystawek albo konsoli.
Tryb użytkownika – ograniczony dostęp, wiele okien	Chcemy, aby użytkownicy wykorzystywali i nawigowali tylko do tych przystawek, które zostały uwidocznione w drzewie konsoli i chcemy wstępnie skonfigurować wiele okien, które skupiają się na określonych przystawkach. Użytkownicy nie będą w stanie otwierać nowych okien.
Tryb użytkownika – ograniczony dostęp, jedno okno	Chcemy, aby użytkownicy wykorzystywali i nawigowali tylko do tych przystawek, które zostały uwidocznione w drzewie konsoli w pojedynczym oknie.

Gdy konsola nie jest już zapisana w trybie autorskim, to pierwotny autor może dokonywać zmian w tej konsoli, klikając prawym przyciskiem myszy zapisaną konsolę i wybierając opcję Author (Autor).

Zalecane ćwiczenia

Ćwiczenie 4 „Przygotowywanie konsoli do dystrybucji wśród użytkowników" w zestawie ćwiczeń na końcu tej lekcji przeprowadzi nas przez proces zapisywania konsoli w trybie użytkownika tak, aby można ją było zablokować przed przekazaniem innym administratorom.

Konsole są zapisywane w plikach z rozszerzeniem .msc. Domyślną lokalizacją, w której zapisywane są konsole, jest folder Administrative Tools (Narzędzia administracyjne), ale nie ten folder w Panelu sterowania. Są one natomiast zapisywane w folderze menu Start w profilu danego użytkownika: *%userprofile%*\AppData\Roaming\Microsoft\Windows\StartMenu.

Ta lokalizacja stanowi pewien problem, ponieważ jest zabezpieczona uprawnieniami pozwalającymi tylko kontu tego użytkownika na dostęp do tej konsoli. Najlepszą praktyką

jest logowanie się do komputera na koncie, które nie jest uprzywilejowane, a następnie uruchamianie narzędzi administracyjnych, takich jak konsola niestandardowa z poświadczeniami alternatywnymi, które mają wystarczające uprawnienia do wykonywania zadań administracyjnych. Ponieważ w grę będą wchodzić dwa konta, to zapisanie konsoli w podfolderze menu Start w profilu użytkownika jednego konta będzie oznaczało dla drugiego konta co najmniej konieczność dodatkowej nawigacji, a w najgorszym przypadku błędy odmowy dostępu.

Należy zapisywać swoje konsole w miejscu, które może być dostępne zarówno dla posiadanych poświadczeń zwykłego użytkownika, jak i administratora. Zaleca się zapisywanie konsol w udostępnionym folderze w sieci, tak aby można było mieć dostęp do swoich narzędzi będąc zalogowanym na innych komputerach. Opcjonalnie może być udostępniony folder przez innych administratorów do tworzenia scentralizowanego magazynu niestandardowych konsol. Można też zapisywać konsole na urządzeniu przenośnym, takim jak napęd USB, lub nawet można przesyłać konsolę jako załącznik poczty elektronicznej.

Ważne jest, aby pamiętać, że konsole są w zasadzie zbiorami instrukcji, które są interpretowane przez program *mmc.exe* – instrukcji określających, które przystawki mają zostać dodane i które komputery mają być zarządzane przez te przystawki. Konsole nie zawierają właściwych przystawek. Dlatego konsola nie będzie działała poprawnie, jeśli dana przystawka nie będzie zainstalowana, więc należy upewnić się, że odpowiednie przystawki są zainstalowane w systemach, w których konsola będzie używana.

Pytanie kontrolne

- Jaka jest różnica pomiędzy konsolą zapisaną w trybie użytkownika i w trybie autorskim?

Odpowiedź na pytanie kontrolne

- Tryb autorski umożliwia użytkownikowi dodawanie i usuwanie przystawek oraz gruntowne dostosowywanie konsoli. Tryb użytkownika uniemożliwia użytkownikom dokonywanie zmian w konsoli.

Zadanie Tworzenie i zarządzanie niestandardową konsolą MMC

W tym zadaniu utworzymy niestandardową konsolę MMC. Będziemy dodawać, usuwać i zmieniać kolejność przystawek. Następnie przygotujemy konsolę do dystrybucji wśród innych administratorów.

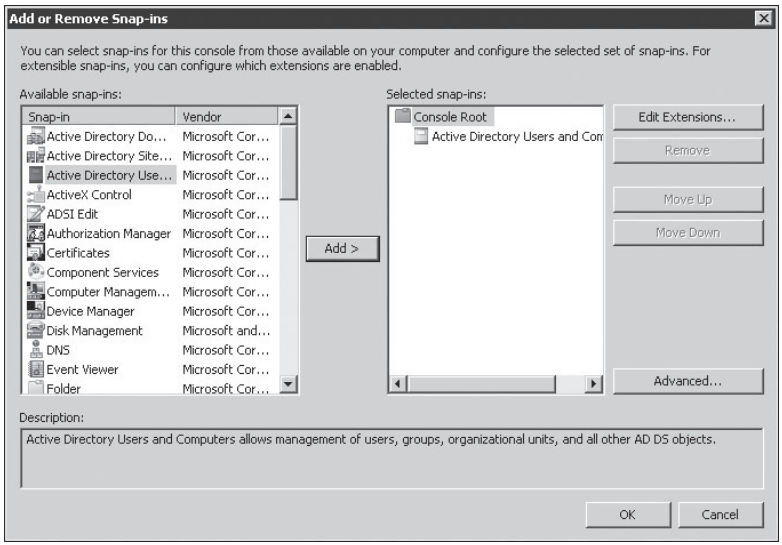
▶ Ćwiczenie 1: Tworzenie niestandardowej konsoli MMC

W tym ćwiczeniu utworzymy niestandardową konsolę MMC z przystawkami Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory), Active Directory Schema (Schemat usługi Active Directory) oraz Computer Management (Zarządzanie komputerem). Narzędzia te są przydatne do administrowania Active Directory i kontrolerami domeny.

1. Zalogować się jako Administrator na komputerze SERVER01.
2. Kliknąć przycisk Start i w polu Start Search wpisać **mmc.exe**, po czym nacisnąć Enter.

Pojawi się pusta konsola MMC. Domyślnie nowe okno konsoli nie jest zmaksymalizowane w oknie MMC. Należy je zmaksymalizować, aby skorzystać z pełnego rozmiaru aplikacji.

3. Z menu File (Plik) wybrać opcję Add/Remove Snap-in (Dodaj/Usuń przystawkę). Pojawi się okno dialogowe Add Or Remove Snap-ins (Dodawanie lub usuwanie przystawek) pokazane na rysunku 2-3.



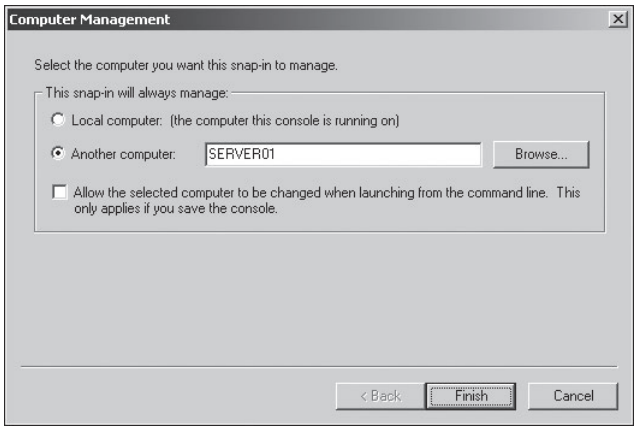
Rysunek 2-3 Okno dialogowe Add Or Remove Snap-ins (Dodawanie lub usuwanie przystawek)

Jeśli żądane przystawki nie są wymienione, należy upewnić się, że zainstalowano RSAT – Remote Server Administration Tools (Narzędzia administracji zdalnej serwera).

4. W oknie dialogowym Add Or Remove Snap-ins (Dodawanie lub usuwanie przystawek) zaznaczyć opcję Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) na liście Available Snap-ins (Dostępne przystawki).
5. Kliknąć przycisk Add (Dodaj), aby dodać tę przystawkę do listy Selected Snap-ins (Wybrane przystawki).

   Należy zwrócić uwagę, że przystawki Active Directory Schema (Schemat usługi Active Directory) nie ma na liście dostępnych przystawek do dodania. Przystawka Active Directory Schema (Schemat usługi Active Directory) jest instalowana z rolą Active Directory Domain Services (Usługi domenowe w usłudze Active Directory), ale nie jest rejestrowana, więc się nie pojawia na liście.
6. Kliknąć OK, aby zamknąć okno dialogowe Add Or Remove Snap-ins (Dodawanie lub usuwanie przystawek).
7. Kliknąć przycisk Start. W polu Start Search (Rozpocznij wyszukiwanie) wpisać **cmd.exe**.
8. W wierszu polecenia wpisać polecenie **regsvr32.exe schmmgmt.dll**.
   To polecenie rejestruje dynamicznie dołączaną bibliotekę (DLL) dla przystawki Active Directory Schema (Schemat usługi Active Directory). Trzeba to zrobić w systemie tylko raz, zanim będzie można dodać przystawkę do konsoli.

9. Pojawi się komunikat wskazujący, że rejestracja się powiodła. Kliknąć OK.
10. Wrócić do naszej niestandardowej konsoli MMC i powtórzyć kroki 2-6, aby dodać przystawkę Active Directory Schema (Schemat usługi Active Directory).
11. Z menu File (Plik) wybrać opcję Add/Remove Snap-in (Dodaj/Usuń przystawkę).
12. W oknie dialogowym Add Or Remove Snap-ins (Dodawanie lub usuwanie przystawek) zaznaczyć opcję Computer Management (Zarządzanie komputerem) na liście Available Snap-ins (Dostępne przystawki).
13. Kliknąć przycisk Add (Dodaj), aby dodać tę przystawkę do listy Selected Snap-ins (Wybrane przystawki).
    Jeśli przystawka obsługuje administrację zdalną, pojawi się monit o wybranie komputera, którym chcemy zarządzać, jak pokazano na rysunku 2-4.
    - ❑ Aby zarządzać tym komputerem, na którym uruchomiona jest konsola, należy zaznaczyć opcję Local Computer (Komputer lokalny). Nie odnosi się to wyłącznie do komputera, na którym konsola jest tworzona. Jeśli konsola zostanie uruchomiona na innym komputerze, to będzie ona zarządzała tym właśnie komputerem.
    - ❑ Aby określić pojedynczy komputer, którym przystawka powinna zarządzać, należy zaznaczyć opcję Another Computer (Inny komputer). Następnie wpisać nazwę komputera lub kliknąć Browse (Przeglądaj), aby wybrać ten komputer.



Rysunek 2-4 Wybieranie komputera, który ma być zarządzany przez przystawkę.

14. Wybrać opcję Another Computer (Inny komputer) i wpisać **SERVER01** jako nazwę komputera.
15. Kliknąć Finish (Zakończ).
16. Kliknąć OK, aby zamknąć okno dialogowe Add Or Remove Snap-ins (Dodawanie lub usuwanie przystawek).
17. Wybrać Save (Zapisz) z menu File (Plik) i zapisać konsolę na pulpicie pod nazwą **MojaKonsola.msc**.
18. Zamknąć konsolę.

▶ Ćwiczenie 2: Dodawanie przystawki do konsoli MMC

W tym ćwiczeniu dodamy przystawkę Event Viewer (Podgląd zdarzeń) do konsoli utworzonej w ćwiczeniu 1. Przystawka Event Viewer (Podgląd zdarzeń) jest przydatna do monitorowania działań na kontrolerach domeny.

1. Otworzyć konsolę MojaKonsola.msc.
   Jeśli w ćwiczeniu 1 konsola nie została zapisana na pulpicie, a zamiast tego została zapisana w domyślnej lokalizacji, to można ją znaleźć w folderze Start\All Programs\Administrative Tools (Start\Wszystkie programy\Narzędzia administracyjne).
2. Z menu File (Plik) wybrać opcję Add/Remove Snap-in (Dodaj/Usuń przystawkę).
3. W oknie dialogowym Add Or Remove Snap-ins (Dodawanie lub usuwanie przystawek) należy zaznaczyć opcję Event Viewer (Podgląd zdarzeń) na liście Available Snap-ins (Dostępne przystawki).
4. Kliknąć przycisk Add (Dodaj), aby dodać tę przystawkę do listy Selected Snap-ins (Wybrane przystawki).
   Pojawi się monit o wybranie komputera do zarządzania.
5. Wybrać opcję Another Computer (Inny komputer) i wpisać **SERVER01** jako nazwę komputera.
6. Kliknąć OK.
7. Kliknąć OK, aby zamknąć okno dialogowe Add Or Remove Snap-ins (Dodawanie lub usuwanie przystawek).
8. Zapisać i zamknąć konsolę.

▶ Ćwiczenie 3: Zarządzanie przystawkami konsoli MMC

W tym ćwiczeniu zmienimy kolejność przystawek i usuniemy przystawkę. Poznamy też rozszerzenia przystawek.

1. Otworzyć konsolę MojaKonsola.msc.
2. Z menu File (Plik) wybrać opcję Add/Remove Snap-in (Dodaj/Usuń przystawkę).
3. Na liście Selected snap-ins (Wybrane przystawki) należy zaznaczyć Event Viewer (Podgląd zdarzeń).
4. Kliknąć przycisk Move Up (Przenieś w górę).
5. Zaznaczyć Active Directory Schema (Schemat usługi Active Directory).
6. Kliknąć przycisk Remove (Usuń).
7. Na liście Selected snap-ins (Wybrane przystawki) należy zaznaczyć Computer Management (Zarządzanie komputerem).
8. Kliknąć Edit Extensions (Edytuj rozszerzenia).
   Rozszerzenia są przystawkami, które istnieją wewnątrz innej przystawki, zapewniając dodatkową funkcjonalność. Przystawka Computer Management (Zarządzanie komputerem) ma wiele znajomych przystawek jako swoje rozszerzenia, a każdą z nich można włączyć lub wyłączyć.
9. Zaznaczyć opcję Enable Only Selected Extensions (Włącz tylko wybrane rozszerzenia).

10. Wyłączyć Event Viewer (Podgląd zdarzeń). Dodaliśmy już Event Viewer (Podgląd zdarzeń) jako samodzielną przystawkę do naszej konsoli.
11. Kliknąć OK, aby zamknąć okno dialogowe Extensions For Computer Management (Rozszerzenia zarządzania komputerem).
12. Kliknąć OK, aby zamknąć okno dialogowe Add Or Remove Snap-ins (Dodawanie lub usuwanie przystawek).
13. Zapisać i zamknąć konsolę.

▶ Ćwiczenie 4: Przygotowywanie konsoli do dystrybucji wśród użytkowników

W tym ćwiczeniu zapiszemy swoją konsolę w trybie użytkownika, aby użytkownicy nie mogli dodawać, usuwać ani modyfikować przystawek. Należy mieć na uwadze, że użytkownicy konsoli MMC zwykle sami są administratorami.

1. Otworzyć konsolę MojaKonsola.msc.
2. Z menu File (Plik) wybrać Options (Opcje).
3. Z listy rozwijanej Console Mode (Tryb konsoli) wybrać opcję User Mode – Full Access (Tryb użytkownika – pełny dostęp).
4. Kliknąć OK.
5. Zapisać i zamknąć konsolę.
6. Otworzyć konsolę podwójnie ją klikając.
7. Kliknąć menu File (Plik). Trzeba zwrócić uwagę, że brakuje polecenia *Add/Remove Snap-in* (Dodaj/Usuń przystawkę).
8. Zamknąć konsolę.
9. Kliknąć konsolę prawym przyciskiem myszy i kliknąć Author (Autor).
10. Kliknąć menu File (Plik). W trybie autorskim pojawia się polecenie *Add/Remove Snap-in* (Dodaj/Usuń przystawkę).
11. Zamknąć konsolę.

Podsumowanie lekcji

- Narzędzia administracyjne Windows są przystawkami, które można dodawać do konsoli MMC. Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory). Inne przystawki zarządzające Active Directory są również dodawane do konsoli Server Manager (Menedżer serwera) i są zawarte we wstępnie skonfigurowanych konsolach w folderze Administrative Tools (Narzędzia administracyjne).
- Administratorzy nie powinni logować się na swoich komputerach przy użyciu poświadczeń administracyjnych. Zamiast tego powinni używać konta standardowego użytkownika do logowania się i uruchamiać narzędzia administracyjne korzystając z polecenia *Run As Administrator* (Uruchom jako administrator).
- Warto utworzyć sobie niestandardową konsolę MMC zawierającą wszystkie przystawki potrzebne do wykonywania swojej pracy. Taka konsola może być zapisywana w miejscu, w którym również inni administratorzy mogą mieć do niej dostęp i uruchamiać ją z poświadczeniami administracyjnymi. Idealnie powinno być to jedyne narzędzie

potrzebne do uruchamiania z poświadczeniami administratora, jeśli będzie w pełni dostosowane do naszych potrzeb.

- Zaleca się zapisywanie konsoli w trybie użytkownika, tak aby nie można było wprowadzać zmian do konsoli i jej przystawek.
- Konsole wymagają, aby odpowiednie narzędzia administracyjne były zainstalowane. W przeciwnym razie przystawki konsoli nie będą funkcjonować poprawnie.

Pytanie do lekcji

Poniższe pytanie można wykorzystać do przetestowania swojej wiedzy na temat informacji zawartych w lekcji 1 „Praca z przystawkami usług Active Directory".

Uwaga Odpowiedź

Odpowiedź na to pytanie i wyjaśnienia, dlaczego dany wybór odpowiedzi jest poprawny lub niepoprawny, można znaleźć w części „Odpowiedzi" na końcu tej książki.

1. Pracujemy w dziale wsparcia w firmie Contoso, Ltd. Administratorzy domeny udostępnili niestandardową konsolę z przystawką Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory). Po otwarciu tej konsoli i próbie zresetowania hasła użytkownika pojawiają się błędy odmowy dostępu. Na pewno mamy uprawnienia do resetowania haseł użytkowników. Jakie jest najlepsze rozwiązanie?
   A. Zamknąć niestandardową konsolę i otworzyć narzędzie Server Manager (Menedżer serwera). Skorzystać z przystawki Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory) w konsoli Server Manager (Menedżer serwera).
   B. Zamknąć niestandardową konsolę i otworzyć wiersz polecenia. Wpisać **dsa.msc.**
   C. Zamknąć niestandardową konsolę, a następnie kliknąć konsolę prawym przyciskiem myszy i wybrać opcję Run As Administrator (Uruchom jako administrator). Wpisać poświadczenia dla swojego dodatkowego konta administracyjnego.
   D. Zamknąć niestandardową konsolę, a następnie kliknąć konsolę prawym przyciskiem myszy i otworzyć wiersz polecenia. Użyć polecenia *DSMOD USER* z przełącznikiem *–p*, aby zmienić hasło użytkownika.

Lekcja 2: Tworzenie obiektów w Active Directory

Active Directory jest usługą katalogową, a rolą usługi katalogowej jest utrzymywanie informacji o zasobach przedsiębiorstwa obejmujących użytkowników, grupy i komputery. Zasoby są podzielone na jednostki organizacyjne (OU), aby ułatwić zarządzanie i dostępność obiektów – to znaczy mogą one ułatwiać odnajdowanie obiektów. W tej lekcji dowiemy się, jak tworzyć jednostki organizacyjne, użytkowników, grupy i komputery. Poznamy też ważne umiejętności pomagające lokalizować i znajdować potrzebne obiekty.

Doświadczeni użytkownicy Active Directory będą w stanie szybko przejrzeć kilka pierwszych fragmentów tej lekcji, ale warto zwrócić szczególną uwagę na ostatnie części, zaczynając od nagłówka „Odnajdowanie obiektów w usługach Active Directory", ponieważ pomogą one w lepszym wykorzystaniu narzędzi Active Directory.

Ważne będzie ukończenie ćwiczeń praktycznych na końcu tej lekcji, ponieważ utworzymy w nich kilka obiektów, które będą wykorzystywane w przyszłych ćwiczeniach.

Po ukończeniu tej lekcji Czytelnik będzie umiał:

- Tworzyć użytkowników, grupy, komputery i jednostki organizacyjne.
- Wyłączać zabezpieczenie przed usunięciem jednostki organizacyjnej.
- Dostosowywać i wykorzystywać widoki i funkcje przystawki Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory) do efektywnej pracy z obiektami w katalogu.
- Tworzyć zapisane kwerendy generujące oparte na regułach widoki obiektów w katalogu.

Przewidywany czas trwania lekcji: 45 minut

Tworzenie jednostki organizacyjnej

Jednostki organizacyjne (OU) są pojemnikami administracyjnymi wewnątrz Active Directory, które są używane do zbierania obiektów mających wspólne wymagania związane z administrowaniem, konfigurowaniem lub pokazywaniem. Co to dokładnie oznacza, wyjaśni się w miarę dowiadywania się więcej na temat projektowania i zarządzania jednostkami organizacyjnymi. Na razie wystarczy zrozumieć, że jednostki organizacyjne zapewniają hierarchię administracyjną podobną do hierarchii folderów na twardym dysku: jednostki organizacyjne tworzą *kolekcje* obiektów, którymi można wspólnie *administrować*. Termin *administrowanie* został tu podkreślony, ponieważ jednostki organizacyjne nie są używane do przypisywania uprawnień do zasobów – do tego służą grupy. Użytkownicy są umieszczani w grupach, którym nadawane są uprawnienia do zasobów. Jednostki organizacyjne są pojemnikami administracyjnymi, wewnątrz których administratorzy mogą zarządzać użytkownikami i grupami.

Aby utworzyć jednostkę organizacyjną, należy:

1. Otworzyć przystawkę Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory).

2. Kliknąć prawym przyciskiem myszy węzeł domeny albo węzeł jednostki organizacyjnej, do której chcemy dodać nową jednostkę organizacyjną, wybrać New (Nowy), a następnie wybrać opcję Organizational Unit (Jednostka organizacyjna).
3. Wpisać nazwę jednostki organizacyjnej.
   Nazwa powinna zachowywać konwencje nazewnicze używane w danej organizacji.
4. Zaznaczyć opcję Protect Container From Accidental Deletion (Chroń kontener przed przypadkowym usunięciem).
   Później dowiemy się więcej na temat tej opcji.
5. Kliknąć OK.
   Jednostki organizacyjne mają inne właściwości, których skonfigurowanie może być przydatne. Te właściwości mogą zostać ustawione po utworzeniu obiektu.
6. Kliknąć prawym przyciskiem myszy jednostkę organizacyjną i wybrać Properties (Właściwości).

   Przy definiowaniu właściwości jednostki należy stosować się do konwencji nazewniczych oraz innych standardów i procesów obowiązujących w danej organizacji.

   Można użyć pola *Description* (Opis) do wyjaśnienia znaczenia danej jednostki organizacyjnej.

   Jeśli jednostka organizacyjna reprezentuje fizyczną lokalizację, taką jak biuro, to właściwości adresowe jednostki organizacyjnej mogą być przydatne.

   Karta Managed By (Zarządzany przez) może służyć do łączenia danej jednostki organizacyjnej z użytkownikiem lub grupą, które za nią odpowiadają. W tym celu należy kliknąć przycisk Change (Zmień) pod polem Name (Nazwa). Więcej na temat okna dialogowego Select Users, Contacts, Or Groups (Wybieranie: Użytkownicy, Kontakty lub Grupy) dowiemy się w dalszej części tej lekcji. Pozostałe informacje kontaktowe na karcie Managed By (Zarządzany przez) są wypełniane na podstawie konta określonego w polu Name (Nazwa). Karta Managed By (Zarządzany przez) jest używana jedynie do informacji kontaktowych – podany użytkownik lub grupa nie zyskują żadnych uprawnień ani dostępu do jednostki organizacyjnej.
7. Kliknąć OK.

Narzędzia administracyjne Windows Server 2008 dodają nową opcję: Protect Container From Accidental Deletion (Chroń kontener przed przypadkowym usunięciem). Ta opcja dodaje przełącznik zabezpieczający do jednostki organizacyjnej, aby nie można jej było przypadkiem usunąć. Do jednostki organizacyjnej dodawane są dwa uprawnienia: Everyone::Deny::Delete (Wszyscy::Odmów::Usuwanie) i Everyone::Deny::Delete Subtree (Wszyscy::Odmów::Usuwanie poddrzewa). Żaden użytkownik, nawet administrator, nie będzie w stanie przypadkowo usunąć jednostki organizacyjnej i jej zawartości. Zaleca się włączanie tej ochrony dla wszystkich nowych jednostek organizacyjnych.

Chcąc usunąć jednostkę organizacyjną trzeba najpierw wyłączyć ten przełącznik zabezpieczający. Aby usunąć chronioną jednostkę organizacyjną, należy:

1. W przystawce Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) kliknąć menu View (Widok) i wybrać opcję Advanced Features (Opcje zaawansowane).
2. Kliknąć prawym przyciskiem myszy jednostkę organizacyjną i wybrać Properties (Właściwości).

3. Kliknąć kartę Object (Obiekt).
   Jeśli nie widać karty Object (Obiekt), to znaczy, że nie włączono funkcji Advanced Features (Opcje zaawansowane) w kroku 1.
4. Wyczyścić pole wyboru o nazwie Protect Object From Accidental Deletion (Chroń obiekt przed przypadkowym usunięciem).
5. Kliknąć OK.
6. Kliknąć prawym przyciskiem myszy jednostkę organizacyjną i wybrać Delete (Usuń).
7. Pojawi się monit o potwierdzenie chęci usunięcia jednostki organizacyjnej. Kliknąć Yes (Tak).
8. Jeśli jednostka organizacyjna zawiera jakieś inne obiekty, to zostaniemy poproszeni w oknie dialogowym Confirm Subtree Deletion (Potwierdź usuwanie poddrzewa) o potwierdzenie chęci usunięcia jednostki organizacyjnej i wszystkich zawartych w niej obiektów. Kliknąć Yes (Tak).

Pytanie kontrolne

- Użytkownik próbuje usunąć jednostkę organizacyjną i otrzymuje błąd o braku wystarczających uprawnień. Jest zalogowany jako członek grupy Domain Admins (Administratorzy domeny), więc z pewnością powinien mieć uprawnienia do usunięcia jednostki organizacyjnej. Co się dzieje i co trzeba zmienić, aby usunąć jednostkę organizacyjną?

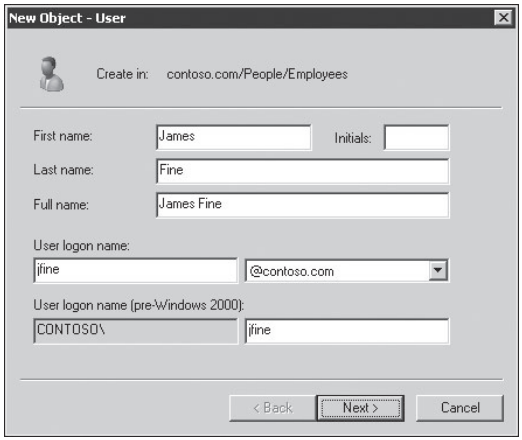
Odpowiedź na pytanie kontrolne

- Jednostka organizacyjna jest chroniona przed przypadkowym usunięciem. Trzeba wyłączyć opcję chroniącą obiekt przed przypadkowym usunięciem. Opcja ta znajduje się na karcie Object (Obiekt) okna dialogowego Properties (Właściwości) dla jednostki organizacyjnej i jest dostępna tylko wtedy, gdy włączona jest funkcja Advanced Features (Opcje zaawansowane).

Tworzenie obiektu użytkownika

Aby utworzyć nowego użytkownika w Active Directory, należy wykonać następujące kroki. Należy stosować konwencje nazewnicze i procesy ustanowione w swojej organizacji.

1. Otworzyć przystawkę Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory).
2. W drzewie konsoli należy rozwinąć węzeł reprezentujący domenę (na przykład *contoso.com*) i przejść do jednostki organizacyjnej lub kontenera (na przykład Users), w którym chcemy utworzyć konto użytkownika.
3. Kliknąć prawym przyciskiem myszy jednostkę organizacyjną lub kontener, wybrać New (Nowy), a następnie wybrać User (Użytkownik).
   Pojawi się okno dialogowe New Object – User (Nowy obiekt – Użytkownik), jak pokazano na rysunku 2-5.
4. W polu First Name (Imię) wpisać imię użytkownika.



Rysunek 2-5 Okno dialogowe New Object – User (Nowy obiekt – Użytkownik)

5. W polu Initials (Inicjały) wpisać inicjał drugiego imienia użytkownika.
   Należy zwrócić uwagę, że ta właściwość jest przeznaczona na inicjały drugiego imienia użytkownika, a nie na inicjały imienia i nazwiska użytkownika.
6. W polu Last Name (Nazwisko) wpisać nazwisko użytkownika.
7. Pole *Full Name* (Pełna nazwa) jest wypełniane automatycznie. Można je zmodyfikować, jeśli to konieczne.

   Pole *Full Name* (Pełna nazwa) jest używane do tworzenia kilku atrybutów obiektu użytkownika, a zwłaszcza jego nazwy pospolitej (CN). Nazwa pospolita (CN) użytkownika jest nazwą wyświetlaną w okienku szczegółów przystawki. Musi być ona unikalna w danym kontenerze lub jednostce organizacyjnej. Dlatego jeśli tworzymy obiekt użytkownika dla osoby o takim samym imieniu/nazwisku jak istniejący użytkownik w tej samej jednostce organizacyjnej lub kontenerze, to musimy wprowadzić unikalną nazwę w polu *Full Name* (Pełna nazwa).
8. W polu User Logon Name (Nazwa logowania użytkownika) wpisać nazwę, której użytkownik będzie używać do logowania, a z listy rozwijanej wybrać sufiks głównej nazwy użytkownika (UPN), który będzie dołączany do nazwy logowania użytkownika za symbolem @.

   Nazwy użytkowników w Active Directory mogą zawierać pewne znaki specjalne (w tym kropki, myślniki i apostrofy), co umożliwia nam tworzenie zgodnych z rzeczywistością nazw użytkowników, takich jak O'Hara i Smith-Bates. Jednakże pewne aplikacje mogą mieć inne ograniczenia, więc zaleca się używanie tylko standardowych liter i cyfr, dopóki nie przetestuje się dokładnie aplikacji używanych w przedsiębiorstwie pod kątem zgodności ze znakami specjalnymi w nazwach logowania.

   Lista dostępnych sufiksów UPN może być zarządzana przy użyciu przystawki Active Directory Domains And Trusts (Domeny i relacje zaufania usługi Active Directory). W tym celu należy kliknąć prawym przyciskiem myszy główny węzeł przystawki Active Directory Domains And Trusts (Domeny i relacje zaufania usługi Active Directory), wybrać Properties (Właściwości), a następnie skorzystać z karty UPN Suffixes (Sufiksy głównych nazw użytkowników), aby dodawać lub usuwać sufiksy. Nazwa DNS domeny Active Directory zawsze będzie dostępna jako sufiks i nie może zostać usunięta.

9. W polu User logon name (Pre-Windows 2000) (Nazwa logowania użytkownika (systemy starsze niż Windows 2000)) przystawki Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) należy wprowadzić nazwę logowania w systemach starszych niż Windows 2000.

   W rozdziale 3 „Administracja kontami użytkowników" dowiemy się więcej na temat tych dwóch różnych nazw logowania.
10. Kliknąć Next (Dalej).
11. Wpisać hasło początkowe dla użytkownika w polach Password (Hasło) i Confirm Password (Potwierdź hasło).
12. Zaznaczyć opcję User Must Change Password At Next Logon (Użytkownik musi zmienić hasło przy następnym logowaniu).

    Zaleca się zawsze zaznaczać tę opcję, tak aby użytkownik mógł utworzyć nowe hasło nieznane personelowi informatycznemu. Właściwi pracownicy wsparcia technicznego będą mogli zawsze zresetować hasło użytkownika w przyszłości, jeśli trzeba będzie zalogować się na konto tego użytkownika lub uzyskać dostęp do jego zasobów. Jednakże w codziennych warunkach tylko użytkownicy powinni znać swoje hasła.
13. Kliknąć Next (Dalej).
14. Przejrzeć podsumowanie i kliknąć Finish (Zakończ).
    Interfejs okna New Object – User (Nowy obiekt – Użytkownik) umożliwia skonfigurowanie ograniczonej liczby właściwości związanych z kontem, takich jak ustawienia nazwy i hasła. Jednakże obiekt użytkownika w Active Directory obsługuje dziesiątki dodatkowych właściwości. Mogą być one konfigurowane po utworzeniu obiektu.
15. Kliknąć prawym przyciskiem myszy utworzony obiekt i wybrać Properties (Właściwości).
16. Skonfigurować właściwości użytkownika.
    Należy stosować się do konwencji nazewniczych oraz innych standardów obowiązujących w danej organizacji.

    Więcej na temat wielu właściwości użytkowników dowiemy się w rozdziale 3 i w rozdziale 8 „Usprawnienia zabezpieczeń uwierzytelnienia w domenie AD DS".
17. Kliknąć OK.

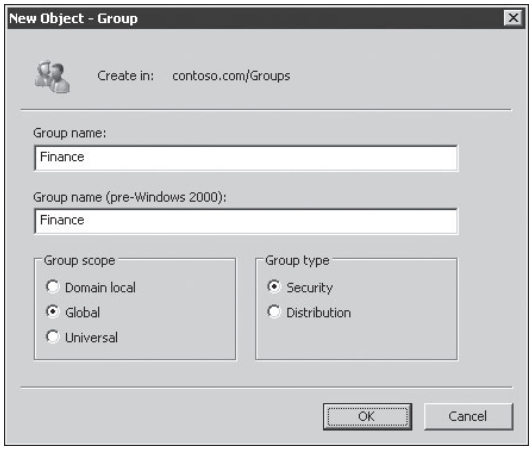
Tworzenie obiektu grupy

Grupy stanowią ważną klasę obiektów, ponieważ służą do zbierania razem użytkowników, komputerów i innych grup w celu zarządzania nimi z jednego miejsca. Najpowszechniejszym zastosowaniem grupy jest nadawanie uprawnień do udostępnionego foldera. Na przykład, jeśli grupa otrzymała prawo dostępu do odczytu do foldera, to każdy z członków tej grupy będzie w stanie odczytywać zawartość tego foldera. Nie trzeba nadawać dostępu do odczytu bezpośrednio każdemu członkowi z osobna; można zarządzać dostępem do foldera po prostu dodając i usuwając członków grupy.

Aby utworzyć grupę:

1. Otworzyć przystawkę Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory).
2. W drzewie konsoli należy rozwinąć węzeł reprezentujący domenę (na przykład *contoso.com*) i przejść do jednostki organizacyjnej lub kontenera (na przykład Users), w którym chcemy utworzyć grupę.

3. Kliknąć prawym przyciskiem myszy jednostkę organizacyjną lub kontener, wybrać New (Nowy), a następnie wybrać Group (Grupa).
   Pojawi się okno dialogowe New Object – Group (Nowy obiekt – Grupa), jak pokazano na rysunku 2-6.



Rysunek 2-6 Okno dialogowe New Object – Group (Nowy obiekt – Grupa)

4. Wpisać nazwę nowej grupy w polu Group Name (Nazwa grupy).
   Większość organizacji stosuje konwencje nazewnicze, które określają, jak mają być tworzone nazwy grup. Należy stosować się do wskazówek swojej organizacji. Domyślnie wpisana nazwa jest też wprowadzana jako nazwa nowej grupy dla systemów starszych niż Windows 2000. Jest wysoce zalecane, aby obie te nazwy były takie same.
5. Nie należy zmieniać nazwy w polu Group Name (Pre-Windows 2000) (Nazwa grupy (systemy starsze niż Windows 2000)).
6. Wybrać typ grupy.
   - ❑ Grupie typu Security (Zabezpieczenia) można nadawać uprawnienia do zasobów. Można ją też skonfigurować jako listę dystrybucyjną poczty elektronicznej.
   - ❑ Grupa typu Distribution (Dystrybucja) jest grupą związaną z pocztą elektroniczną, której nie można nadawać uprawnień do zasobów i dlatego może być ona używana tylko jako lista dystrybucyjna poczty elektronicznej, która nie ma wymagań związanych z dostępem do zasobów.
7. Wybrać zakres grupy.
   - ❑ Grupa o zakresie Global (Globalny) jest używana do identyfikowania użytkowników w oparciu o kryteria, takie jak stanowisko, lokalizacja itd.
   - ❑ Grupa o zakresie Domain Local (Lokalny w domenie) jest używana do zbierania razem użytkowników i grup mających podobne potrzeby w zakresie dostępu do zasobów, na przykład wszystkich użytkowników, którzy mogą modyfikować raport dotyczący jakiegoś projektu.
   - ❑ Grupa o zakresie Universal (Uniwersalny) jest używana do zbierania razem użytkowników i grup z wielu domen.

   Zakres grupy będzie omówiony bardziej szczegółowo w rozdziale 4 „Zarządzanie grupami”.

Należy zwrócić uwagę, że jeśli domena, w której tworzymy obiekt grupy, jest na mieszanym lub przejściowym poziomie funkcjonalności domeny, to można wybrać tylko zakresy Domain Local (Lokalny w domenie) lub Global (Globalny) dla grup zabezpieczeń. Poziomy funkcjonalności domeny będą omówione w rozdziale 12.

8. Kliknąć OK.
   Obiekty grupy mają wiele właściwości, które można konfigurować. Mogą być one określane po utworzeniu obiektu.
9. Kliknąć grupę prawym przyciskiem myszy i wybrać Properties (Właściwości).
10. Skonfigurować właściwości grupy.
    Należy stosować się do konwencji nazewniczych oraz innych standardów obowiązujących w danej organizacji.

    Karty Members (Członkowie) i Member Of (Członek grupy) w oknie właściwości grupy określają, kto należy do tej grupy i do jakich grup ta grupa sama należy. Członkostwo w grupach zostanie omówione w rozdziale 4.

    Pole *Description* (Opis) dla grupy, jako że jest łatwo widoczne w okienku szczegółów przystawki Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory), jest dobrym miejscem na wpisanie podsumowania celu danej grupy i informacji kontaktowych do osób odpowiedzialnych za decydowanie, kto jest, a kto nie jest członkiem tej grupy.

    Pole *Notes* (Uwagi) dla grupy może być używane w celu podawania dodatkowych szczegółów na temat grupy.

    Karta Managed By (Zarządzany przez) może służyć do łączenia danej grupy z użytkownikiem lub grupą, które za nią odpowiadają. Kliknąć przycisk Change (Zmień) pod polem Name (Nazwa). Aby wyszukać grupę, trzeba najpierw kliknąć przycisk Object Types (Typy obiektów) i zaznaczyć opcję Groups (Grupy). Okno dialogowe Select User, Contact, Or Group (Wybieranie: Użytkownik, Kontakt lub Grupa) będzie omawiane w dalszej części tej lekcji.

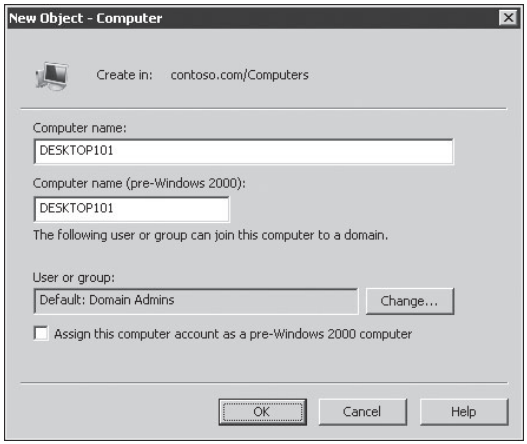
    Pozostałe informacje kontaktowe na karcie Managed By (Zarządzany przez) są wypełniane na podstawie konta określonego w polu Name (Nazwa). Karta Managed By (Zarządzany przez) jest zwykle używana do informacji kontaktowych, tak żeby w przypadku gdy użytkownik chce dołączyć do tej grupy, można było określić, z kim w firmie należy się skontaktować, aby uzyskać akceptację dla nowego członka grupy. Jednakże, jeśli zaznaczona zostanie opcja Manager Can Update Membership List (Menedżer może aktualizować listę członkostwa), to konto podane w polu Name (Nazwa) będzie miało uprawnienia do dodawania i usuwania członków tej grupy. Jest to jedna z metod delegowania nadzoru administracyjnego nad grupą. Inne opcje delegowania zostaną omówione w lekcji 3.
11. Kliknąć OK.

Tworzenie obiektu komputera

Komputery są reprezentowane przez konta i obiekty w Active Directory tak jak użytkownicy. Właściwie w tle komputer loguje się do domeny tak samo jak użytkownik. Komputer ma nazwę użytkownika – będącą nazwą komputera z dołączonym znakiem dolara, na przykład DESKTOP101$ – oraz hasło, które jest ustanawiane, gdy komputer jest dołączany

do domeny i później automatycznie zmieniane co trzydzieści dni. Aby utworzyć obiekt komputera w Active Directory:

1. Otworzyć przystawkę Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory).
2. W drzewie konsoli rozwinąć węzeł reprezentujący domenę (na przykład *contoso.com*) i przejść do jednostki organizacyjnej lub kontenera (na przykład Users), w którym chcemy utworzyć komputer.
3. Kliknąć prawym przyciskiem myszy jednostkę organizacyjną lub kontener, wybrać New (Nowy), a następnie wybrać Computer (Komputer). Pojawi się okno dialogowe New Object – Computer (Nowy obiekt – Komputer), jak pokazano na rysunku 2-7.



Rysunek 2-7 Okno dialogowe New Object – Computer (Nowy obiekt – Komputer)

4. W polu Computer Name (Nazwa komputera) wpisać nazwę komputera.
   Wpisana nazwa zostanie też automatycznie wstawiona do pola Computer Name (Pre-Windows 2000) (Nazwa komputera (systemy starsze niż Windows 2000)).
5. Nie należy zmieniać nazwy w polu Computer Name (Pre-Windows 2000) (Nazwa komputera (systemy starsze niż Windows 2000)).
6. Konto określone w polu *User Or Group* (Użytkownik lub grupa) będzie w stanie dołączać komputer do domeny. Domyślną wartością jest grupa Domain Admins (Administratorzy domeny). Kliknąć Change (Zmień), aby wybrać inną grupę lub użytkownika.

   Zasadniczo należy wybrać grupę reprezentującą zespół wdrożeniowy, zespół wsparcia lub helpdesk. Można też wybrać użytkownika, do którego przypisany jest dany komputer. Sprawami związanymi z dołączaniem komputera do domeny zajmiemy się w rozdziale 5 „Konfigurowanie kont komputerów".
7. Nie należy zaznaczać pola wyboru Assign This Computer Account As A Pre-Windows 2000 Computer (Przypisz to konto komputera jako komputer z systemem starszym niż Windows 2000), o ile to konto nie jest przeznaczone dla komputera działającego pod kontrolą systemu Microsoft Windows NT 4.0.
8. Kliknąć OK.
   Obiekty komputerów mają wiele właściwości, które można konfigurować. Mogą być one określane po utworzeniu obiektu.

9. Kliknąć prawym przyciskiem myszy komputer i wybrać Properties (Właściwości).
10. Wprowadzić właściwości komputera.
    Należy stosować się do konwencji nazewniczych oraz innych standardów obowiązujących w danej organizacji.

    Pole *Description* (Opis) dla komputera może być używane do wskazywania, do kogo komputer jest przypisany, jaka jest jego rola (na przykład komputer z sali szkoleniowej) lub może zawierać inne informacje opisowe. Ponieważ ta właściwość jest widoczna w okienku szczegółów przystawki Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory), jest to dobre miejsce na przechowywanie informacji na temat komputera, które mogą okazać się najbardziej przydatne.

    Istnieje kilka właściwości opisujących komputer, w tym DNS Name (Nazwa DNS), DC Type (Typ kontrolera domeny), Site (Lokacja) oraz właściwości opisujące system operacyjny, takie jak Name (Nazwa), Version (Wersja) i Service Pack (Dodatek Service Pack). Te właściwości zostaną wypełnione automatycznie, gdy komputer zostanie dołączony do domeny.

    Karta Managed By (Zarządzany przez) może służyć do łączenia danego komputera z użytkownikiem lub grupą, które za niego odpowiadają. Kliknąć przycisk Change (Zmień) pod polem Name (Nazwa). Okno dialogowe Select Users, Contacts, Or Groups (Wybieranie: Użytkownicy, Kontakty lub Grupy) będzie omawiane w dalszej części tej lekcji. Pozostałe informacje kontaktowe na karcie Managed By (Zarządzany przez) są wypełniane na podstawie konta określonego w polu Name (Nazwa). Karta Managed By (Zarządzany przez) jest zwykle używana do określania informacji kontaktowych. Niektóre organizacje wykorzystują tę zakładkę do wskazywania na zespół (grupę) wsparcia odpowiedzialny za dany komputer. Inni mogą wykorzystywać te informacje do śledzenia użytkownika, do którego dany komputer jest przypisany.
11. Kliknąć OK.

Odnajdowanie obiektów w usłudze Active Directory

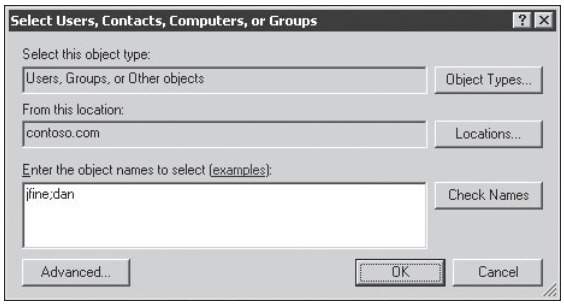
Dowiedzieliśmy się, jak tworzyć obiekty w usłudze Active Directory, ale wyszukiwanie określonego obiektu, który zamierzamy zmodyfikować, staje się trudniejsze, jeśli zwiększa się liczba obiektów usługi Active Directory. Obiekty w usługach Active Directory będziemy musieli wyszukiwać przy wielu okazjach:

- **Nadawanie uprawnień** Podczas konfigurowania uprawnień dla pliku lub foldera trzeba zaznaczyć grupę (lub użytkownika), do których należy przypisać uprawnienia.
- **Dodawanie członków do grup** Członkostwo grupy może składać się z użytkowników, komputerów, grup lub dowolnej kombinacji tych trzech obiektów. Gdy dodajemy obiekt jako członka grupy, trzeba zaznaczyć ten obiekt.
- **Tworzenie łączy** Właściwości połączone są właściwościami jednego obiektu, które odwołują się do innego obiektu. Członkostwo w grupie jest w istocie właściwością połączoną. Inne właściwości połączone, takie jak atrybut *Managed By* omawiany wcześniej, również są łączami. Podczas określania nazwy dla właściwości *Managed By* (Zarządzany przez) trzeba wybrać odpowiedniego użytkownika lub grupę.
- **Wyszukiwanie obiektu** Można szukać dowolnego obiektu w domenie Active Directory.

Istnieje wiele innych sytuacji, które wiążą się z przeszukiwaniem Active Directory i w tym celu używanych jest kilka interfejsów użytkownika. W tej części poznamy niektóre techniki pracy z każdym z nich.

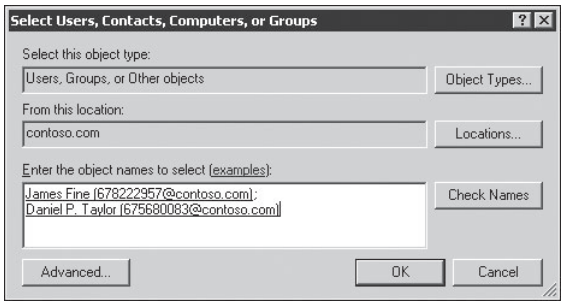
Korzystanie z okna dialogowego Select Users, Contacts, Computers, Or Groups

Gdy dodajemy członka do grupy, przypisujemy uprawnienie albo tworzymy właściwość połączoną, to pojawia się okno dialogowe Select Users, Contacts, Computers, Or Groups (Wybieranie: Użytkownicy, Kontakty, Komputery lub Grupy) pokazane na rysunku 2-8. To okno dialogowe będzie nazywane *oknem dialogowym Select* (Wybieranie) w tym zestawie szkoleniowym. Chcąc zobaczyć przykład, należy otworzyć właściwości obiektu grupy, kliknąć kartę Members (Członkowie), a następnie kliknąć przycisk Add (Dodaj).



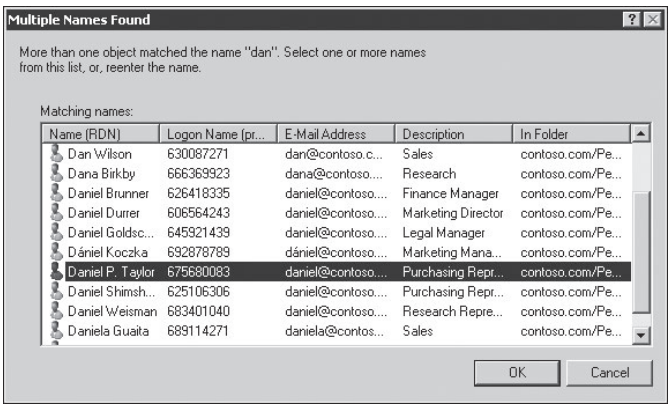
Rysunek 2-8 Okno dialogowe Select Users, Contacts, Computers, Or Groups (Wybieranie: Użytkownicy, Kontakty, Komputery lub Grupy)

Jeśli znamy nazwy potrzebnych obiektów, to możemy je wpisać bezpośrednio w polu tekstowym Enter The Object Names To Select (Wprowadź nazwy obiektów do wybrania). Można wpisać kilka nazw oddzielając je średnikami, jak pokazano na rysunku 2-8. Gdy klikniemy OK, system Windows zablokuje każdy z elementów na liście i przekonwertuje go na łącze do obiektu, a następnie zamknie okno dialogowe. Przycisk Check Names (Sprawdź nazwy) również konwertuje każdą nazwę na łącze, ale pozostawia okno dialogowe otwarte, jak pokazano na rysunku 2-9



Rysunek 2-9 Nazwy przetworzone na łącza za pomocą przycisku Check Names (Sprawdź nazwy)

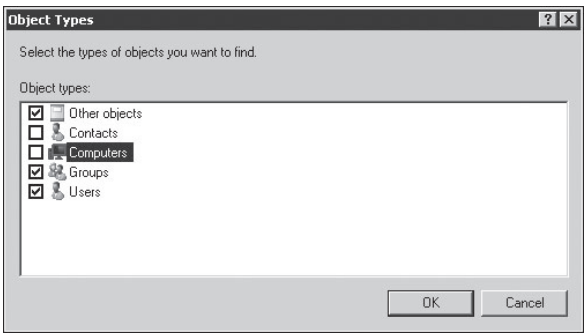
Nie trzeba wpisywać pełnych nazw; wystarczy podać część nazwy. Na przykład rysunek 2-8 pokazuje nazwy jfine i dan. Gdy klikniemy OK lub Check Names (Sprawdź nazwy), system Windows spróbuje przekonwertować częściowe nazwy na prawidłowe obiekty. Jeśli istnieje tylko jeden pasujący obiekt, jak na przykład nazwa logowania jfine, to nazwa zostanie przetworzona, jak pokazano na rysunku 2-9. Jeśli jest wiele pasujących obiektów, jak w przypadku imienia Dan, to pojawi się okno Multiple Names Found (Znaleziono wiele nazw), pokazane na rysunku 2-10. Należy zaznaczyć właściwą nazwę (nazwy) i kliknąć OK. Zaznaczona nazwa pojawi się w oknie, jak pokazano na rysunku 2-9.



Rysunek 2-10 Okno dialogowe Multiple Names Found (Znaleziono wiele nazw)

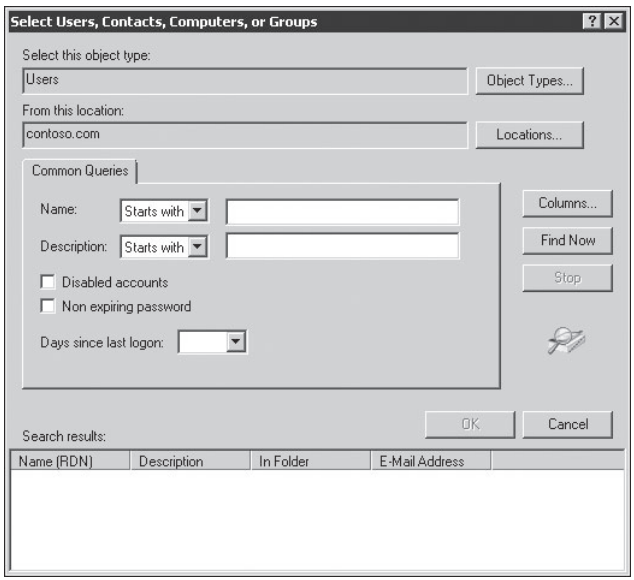
Domyślnie okno dialogowe Select (Wybieranie) przeszukuje całą domenę. Jeśli dostajemy zbyt wiele wyników i chcemy zawęzić zakres wyszukiwania albo jeśli potrzebujemy przeszukać inną domenę lub lokalnych użytkowników i grupy w komputerze będącym członkiem domeny, należy kliknąć Locations (Lokalizacje).

Dodatkowo okno dialogowe Select (Wybieranie), pomimo pełnej nazwy Select Users, Contacts, Computers, Or Groups (Wybieranie: Użytkownicy, Kontakty, Komputery lub Grupy), rzadko służy do wyszukiwania wszystkich czterech typów obiektów. Kiedy na przykład dodajemy członków do grupy, to komputery nie są domyślnie wyszukiwane. Jeśli podamy nazwę komputera, to nie zostanie ona prawidłowo rozpoznana. Należy kliknąć przycisk Object Types (Typy obiektów) i skorzystać z okna dialogowego Object Types (Typy obiektów) pokazanego na rysunku 2-11, aby zaznaczyć odpowiednie typy, a następnie kliknąć OK.



Rysunek 2-11 Okno dialogowe Object Types (Typy obiektów)

Jeśli mamy trudności ze znalezieniem żądanych obiektów, to należy kliknąć przycisk Advanced (Zaawansowane) w oknie dialogowym Select (Wybieranie). Widok zaawansowany, pokazany na rysunku 2-12, umożliwia nam przeszukiwanie zarówno pól nazw, jak i opisu, a także kont wyłączonych, niewygasających haseł i nieużywanych kont, na które nikt się nie zalogował przez określony czas. Niektóre pola na karcie Common Queries (Zwykłe kwerendy) mogą być wyłączone, w zależności od typu wyszukiwanego obiektu. Kliknąć przycisk Object Types (Typy obiektów), aby określić dokładnie typ żądanego obiektu.



Rysunek 2-12 Widok zaawansowany okna dialogowego Select (Wybieranie)

Kontrolowanie widoku obiektów w przystawce Active Directory Users and Computers

Okienko szczegółów przystawki Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory) może być dostosowywane, aby pomóc użytkownikowi efektywnie pracować z obiektami w katalogu. Należy skorzystać z polecenia *Add/Remove Columns* (Dodaj/Usuń kolumny) w menu View (Widok), aby dodać kolumny do okienka szczegółów. Nie każdy atrybut może być wyświetlany jako kolumna, ale na pewno można znaleźć kolumny, których wyświetlanie będzie przydatne, takie jak User Logon Name (Nazwa logowania użytkownika). Można też wyłączyć kolumny, które są niepotrzebne. Jeśli jednostka organizacyjna zawiera tylko jeden typ obiektów (na przykład użytkowników lub komputery), to kolumna Type (Typ) może nie być przydatna.

Gdy kolumna jest widoczna, można zmieniać kolejność kolumn przeciągając nagłówki kolumn w lewo lub w prawo. Można też sortować widok wyświetlany w okienku szczegółów klikając nagłówek kolumny: pierwsze kliknięcie spowoduje posortowanie w kolejności rosnącej, a drugie w kolejności malejącej, podobnie jak w Eksploratorze Windows. Często stosowaną zmianą jest dodanie kolumny Last Name (Nazwisko) do widoku użytkowników, aby można go było sortować według nazwiska. Zwykle jest łatwiej odnajdować

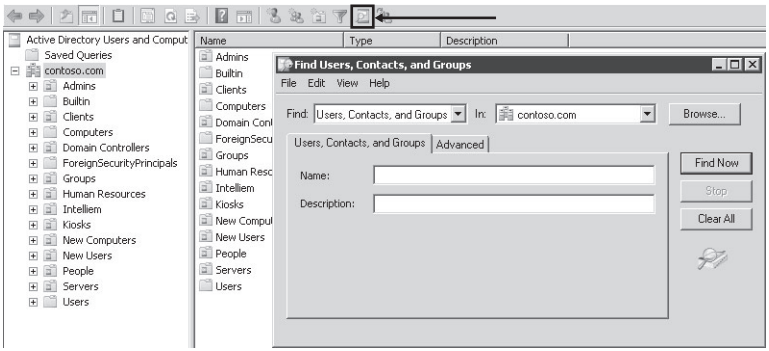
użytkowników według nazwiska, niż według kolumny Name (Nazwa), która odpowiada atrybutowi CN, zwykle zawierającemu imię/nazwisko.

W celu dodania kolumny Last Name (Nazwisko) do okienka informacji szczegółowych:

1. W menu View (Widok) kliknąć polecenie Add/Remove Columns (Dodaj/Usuń kolumny).
2. Na liście Available Columns (Dostępne kolumny) kliknąć pozycję Last Name (Nazwisko).
3. Kliknąć Add (Dodaj).
4. Na liście Displayed Columns (Kolumny wyświetlane) kliknąć pozycję Last Name i dwukrotnie kliknąć przycisk Move Up (Przenieś w górę).
5. Na liście Displayed Columns kliknąć pozycję Type (Typ) i kliknąć przycisk Remove (Usuń).
6. Kliknąć OK.
7. W oknie szczegółów kliknąć nagłówek kolumny Last Name, by posortować pozycje w kolejności alfabetycznej według nazwisk.

Korzystanie z poleceń *Find*

Systemy Windows zapewniają też narzędzie do odpytywania Active Directory zwane przez wielu administratorów oknem Find (Znajdowanie). Jednym ze sposobów uruchomienia okna Find (Znajdowanie) jest kliknięcie przycisku Find Objects In Active Directory Domain Services (Znajdź obiekty w usługach domenowych w usłudze Active Directory) na pasku narzędzi przystawki Active Directory Users And Computers. Ten przycisk i wywoływane przez niego okno są pokazane na rysunku 2-13.



Rysunek 2-13 Okno Find (Znajdowanie)

Należy skorzystać z listy rozwijanej Find (Znajdź), aby określić typy obiektów, których ma dotyczyć zapytanie, ewentualnie można wybrać opcję Common Queries (Zwykłe kwerendy) lub Custom Search (Wyszukiwanie niestandardowe). Lista rozwijana In (W) określa zakres wyszukiwania.

Zaleca się, o ile to możliwe, zawężanie zakresu wyszukiwania w celu uniknięcia wpływu dużej operacji wyszukiwania w całej domenie na wydajność serwera. Listy Find (Znajdź) oraz In (W) wspólnie definiują zakres wyszukiwania.

Następnie należy skonfigurować kryteria wyszukiwania. Często używane pola są dostępne jako kryteria w oparciu o typ wykonywanej kwerendy. Po wyspecyfikowaniu

zakresu wyszukiwania i kryteriów kliknąć Find Now (Znajdź teraz). Na liście wyników możemy kliknąć prawym przyciskiem myszy dowolny element i wybrać polecenia administracyjne, takie jak Move (Przenieś), Delete (Usuń) czy Properties (Właściwości).

Jeśli wybierzemy Custom Search (Wyszukiwanie niestandardowe), a następnie klikniemy kartę Advanced (Zaawansowane), to możemy tworzyć rozbudowane kwerendy LDAP. Na przykład kwerenda **OU=*main*** wyszukuje jednostkę organizacyjną o nazwie zawierającej słowo *main*. Bez użycia wyszukiwania niestandardowego można korzystać z wyszukiwania opartego jedynie na tekście występującym *na początku* nazwy; wyszukiwanie niestandardowe ze znakami wieloznacznymi umożliwia budowanie bardziej zaawansowanych kwerend.

Okno Find (Znajdowanie) pojawia się też w innych miejscach systemu Windows, na przykład w oknie kreatora Add Printer (Dodaj drukarkę) podczas wyszukiwania drukarki sieciowej. Folder Network (Sieć) również ma przycisk Search Active Directory (Wyszukaj w usłudze Active Directory). Można dodać niestandardowy skrót, na przykład do menu Start lub pulpitu, aby wyszukiwanie było jeszcze bardziej dostępne. Docelową lokalizacją skrótu powinno być *rundll32 dsquery,OpenQueryWindow*.

Określenie, gdzie znajduje się dany obiekt

Czasami zachodzi potrzeba wyszukania obiektu przy użyciu polecenia Find (Znajdź), ponieważ nie wiemy, gdzie obiekt się znajduje.

Aby określić lokalizację obiektu, należy:

1. W menu View (Widok) kliknąć opcję Advanced Features (Opcje zaawansowane).
2. Kliknąć przycisk paska narzędzi Find Objects In Active Directory Domain Services (Znajdź obiekty w usługach AD DS), a następnie wykonać wyszukiwanie obiektu.
3. Kliknąć obiekt prawym przyciskiem myszy, kliknąć polecenie Properties (Właściwości), a następnie kliknąć zakładkę Object (Obiekt).
4. Nazwa kanoniczna obiektu (Canonical Name Of Object) wskazuje ścieżkę do obiektu, rozpoczynając ją od domeny.

Inna metoda, którą możemy stosować w oknie dialogowym Find (Znajdź), polega na wyświetleniu kolumny Published At (Opublikowane w):

1. W oknie dialogowym Find (Znajdź) kliknąć menu View, a następnie Choose Columns (Wybierz kolumny).
2. Na liście Columns Available (Dostępne kolumny) kliknąć pozycję Published At, a następnie kliknąć przycisk Add (Dodaj).
3. Kliknąć OK.

Korzystanie z zapisanych kwerend

System Windows Server 2003 wprowadził węzeł Saved Queries (Zapisane kwerendy) do przystawki Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory). Ta funkcja umożliwia nam tworzenie widoków domeny sterowanych regułami, wyświetlających obiekty z jednej lub kilku jednostek organizacyjnych.

Aby utworzyć zapisaną kwerendę:

1. Otworzyć przystawkę Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory).

   Węzeł Saved Queries (Zapisane kwerendy) nie jest dostępny w przystawce Active Directory Users And Computers, która jest częścią konsoli Server Manager. Trzeba skorzystać z samodzielnej konsoli Active Directory Users And Computers lub konsoli niestandardowej zawierającej tę przystawkę.
2. Kliknąć prawym przyciskiem myszy węzeł Saved Queries (Zapisane kwerendy), wybrać New (Nowy), a następnie wybrać Query (Kwerenda).
3. Wpisać nazwę kwerendy.
4. Opcjonalnie wpisać opis kwerendy.
5. Kliknąć Browse (Przeglądaj), aby wybrać katalog główny kwerendy.
   Wyszukiwanie będzie ograniczone do wybranej domeny lub jednostki organizacyjnej. Zaleca się ograniczać wyszukiwanie tak bardzo, jak to możliwe, aby poprawić wydajność wyszukiwania.
6. Kliknąć Define Query (Definiuj kwerendę), aby zdefiniować swoją kwerendę.
7. W oknie dialogowym Find wybrać typ obiektów, które chcemy wyszukiwać.
   Karty w tym oknie dialogowym i pola do wprowadzania danych na każdej karcie zmieniają się, zapewniając opcje odpowiednie dla wybranej kwerendy.
8. Skonfigurować kryteria kwerendy.
9. Kliknąć OK.

Po utworzeniu kwerendy zostanie ona zapisana wewnątrz danej instancji przystawki Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory), jeśli więc korzystaliśmy z konsoli Active Directory Users And Computers (*dsa.msc*), to nasza kwerenda będzie dostępna przy następnym otwarciu tej konsoli. Jeśli utworzymy zapisaną kwerendę w konsoli niestandardowej, to będzie ona dostępna w tej konsoli niestandardowej. Aby przenieść zapisane kwerendy do innych konsol lub użytkowników, można wyeksportować zapisaną kwerendę jako plik XML, a następnie zaimportować ją do docelowej przystawki.

Widok w okienku szczegółów zapisanej kwerendy można dostosować, jak opisano to wcześniej, przez wyświetlanie określonych kolumn i sortowanie. Bardzo ważną korzyścią z zapisanych kwerend jest to, że dostosowany widok jest przypisywany do każdej zapamiętanej kwerendy. Gdy dodajemy kolumnę Last Name (Nazwisko) do „normalnego" widoku jednostki organizacyjnej, to kolumna Last Name (Nazwisko) jest faktycznie dodawana do widoku *każdej* jednostki organizacyjnej, więc pusta kolumna Last Name (Nazwisko) będzie widoczna nawet dla jednostek organizacyjnych z komputerami i grupami. W przypadku zapisanych kwerend można dodać kolumnę Last Name (Nazwisko) do kwerendy dla obiektów użytkowników, a inne kolumny dla innych zapisanych kwerend.

Zapisane kwerendy są dobrym sposobem wirtualizacji widoku katalogu i monitorowania problemów, takich jak wyłączone lub zablokowane konta. Warto poświęcić swój czas na naukę tworzenia i zarządzania zapisanymi kwerendami.

Więcej informacji Zapisane kwerendy

Następująca witryna jest wielce zalecanym źródłem informacji i przykładów związanych z zapisanymi kwerendami: *http://www.petri.co.il/saved_queries_in_windows_2003_dsa.htm*.

Zrozumienie nazw DN, RDN i CN

Nazwa wyróżniająca (DN) stanowi swego rodzaju ścieżkę do obiektu w Active Directory. Każdy obiekt w Active Directory ma zupełnie unikalną nazwę DN. Nasz użytkownik, James Fine, ma nazwę DN postaci CN=James Fine,OU=User Accounts,DC=contoso,DC=com.

Widać, co się dzieje: nazwa DN jest ścieżką rozpoczynającą się od danego obiektu i idącą w górę do domeny górnego poziomu w przestrzeni nazw DNS *contoso.com*. Jak wspominano wcześniej, CN oznacza nazwę pospolitą, a przy tworzeniu użytkownika pole Full Name (Pełna nazwa) jest używane do tworzenia nazwy CN obiektu użytkownika. OU oznacza jednostkę organizacyjną, a DC oznacza składnik domeny.

Część nazwy DN poprzedzająca pierwsze wystąpienie OU lub kontenera to *relative distinguished name* (względna nazwa wyróżniająca) lub RDN. W przypadku użytkownika James Fine nazwą RDN obiektu jest CN=James Fine. Nie każda nazwa RDN obiektu jest jego nazwą CN. Nazwą DN jednostki organizacyjnej User Accounts jest OU=User Accounts,DC=contoso,DC=com. Nazwą RDN jednostki organizacyjnej User Accounts jest więc OU=User Accounts.

Ponieważ nazwa DN obiektu musi być unikalna w całej usłudze katalogowej, to nazwa RDN obiektu musi być unikalna w danym kontenerze. Dlatego, jeśli zatrudnimy drugiego pracownika nazywającego się James Fine, a obydwa obiekty użytkowników będą musiały znaleźć się w tej samej jednostce organizacyjnej, to trzeba będzie nadać temu użytkownikowi inną nazwę CN. Stosowana jest ta sama logika, co w przypadku plików zapisanych w folderach: nie można mieć dwóch plików o identycznych nazwach w jednym folderze.

Będziemy regularnie spotykać nazwy DN podczas pracy z Active Directory, tak samo jak regularnie spotykamy ścieżki do plików podczas pracy z plikami i folderami. Bardzo ważne jest, aby mieć możliwość ich odczytywania i interpretowania.

Odnajdowanie obiektów przy użyciu *Dsquery*

System Windows zapewnia narzędzia wiersza polecenia, które spełniają podobne funkcje do narzędzi usług katalogowych z interfejsem użytkownika, takich jak przystawka Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory). Wiele z tych poleceń zaczyna się od liter DS, więc są często nazywane *poleceniami DS*. *Dsquery* może wyszukiwać obiekty w Active Directory.

Polecenie *Dsquery,* podobnie jak inne polecenia DS, jest dobrze udokumentowane. Aby poznać jego składnię i sposoby użycia, należy wpisać **dsquery /?**.

Większość poleceń DS wykorzystuje się określając klasę obiektów, nad którymi dane polecenie ma pracować. Na przykład trzeba wpisać **dsquery user**, aby szukać użytkowników, z kolei polecenia *Dsquery computer*, *Dsquery group* i *Dsquery ou* będą szukać odpowiednio komputerów, grup i jednostek organizacyjnych.

Jeśli stosujemy samo polecenie DSQuery objectType (typ obiektu), polecenie zwróci nazwy wyróżniające wszystkich obiektów w domenie zgodnych z wyspecyfikowanym typem obiektu. Aby polecenie działało sprawnie, DSQuery ogranicza liczbę wyników do

100. Możemy używać przełącznika *-limit* do określania, ile wyników ma być zwracanych. Przełącznik *-limit 0* spowoduje wyświetlenie wszystkich obiektów.

Po określeniu typu obiektu można zastosować przełączniki wskazujące kryteria kwerendy. Na przykład każdy obiekt można znaleźć na podstawie jego nazwy za pomocą przełącznika *-name*. Większość obiektów można wyszukiwać na podstawie opisu (*-desc*). Podmioty zabezpieczeń mogą być wyszukiwane na podstawie swojej nazwy logowania w systemach starszych niż Windows 2000 (*-samid*). Aby dowiedzieć się, które właściwości mogą być używane do wyszukiwania, wystarczy wpisać **dsquery *typobiektu* /?**. Na przykład możemy wpisać **dsquery user /?**.

Jeśli na przykład chcemy znaleźć użytkownika Tony Krijnen, powinniśmy wprowadzić następujące polecenie: **dsquery user -name "Tony Krijnen"**. Po przełączniku właściwości, *name* w tym przypadku, można wprowadzić kryteria, w których nie są rozróżniane wielkie i małe litery i które mogą zawierać znaki wieloznaczne, takie jak gwiazdka reprezentująca dowolną liczbę znaków. Poniższe polecenie wyszukuje wszystkich użytkowników, których nazwa rozpoczyna się od Jam:

```
dsquery user -name "Jam*"
```

Polecenie *Dsquery* zwraca pasujące obiekty domyślnie w postaci ich nazw wyróżniających (DN), jak widać na rysunku 2-14.

```
c:\>dsquery user -name jam*
"CN=James D. Kramer,OU=Employees,OU=People,DC=contoso,DC=com"
"CN=James Fine,OU=People,DC=contoso,DC=com"
"CN=James Hendergart,OU=Employees,OU=People,DC=contoso,DC=com"
"CN=James R. Hamilton,OU=Employees,OU=People,DC=contoso,DC=com"
"CN=James van Eaton,OU=Employees,OU=People,DC=contoso,DC=com"
"CN=Jamie Reding,OU=Employees,OU=People,DC=contoso,DC=com"
```

Rysunek 2-14 Polecenie *Dsquery*

Jeśli chcemy przeglądać wyniki w innej postaci niż nazwy DN, to należy dodać przełącznik *-o* do polecenia *Dsquery*. Można na przykład dodać przełącznik *-o samid*, aby zwracać wyniki w postaci nazw logowania w systemach starszych niż Windows 2000 lub przełącznik *-o upn*, aby zwracać listę wyników w postaci nazw logowania użytkowników (UPN).

Na koniec możemy ograniczać zakres wyszukiwania realizowany przez polecenie DSQuery poprzez dodanie nazwy DN jednostki organizacyjnej lub kontenera po elemencie objectType. Na przykład poniższe polecenie wyszukuje użytkowników, których nazwy rozpoczynają się od Dan, ale tylko w jednostce organizacyjnej Admins:

```
dsquery user "ou=Admins,dc=contoso,dc=com" -name "Dan*"
```

Domyślnie wyszukiwanie obejmuje wszystkie podrzędne jednostki organizacyjne dla wyspecyfikowanego kontenera. Parametr *-base* może być używany do dalszego zawężania wyszukiwania – na przykład do przeszukania jedynie wyspecyfikowanej jednostki organizacyjnej bez jej pod-jednostek.

Zadanie Tworzenie i odnajdowanie obiektów w Active Directory

W tym zadaniu utworzymy, a następnie wyszukamy obiekty w Active Directory. Utworzymy jednostki organizacyjne, użytkowników, grupy i komputery. Następnie utworzymy zapisaną kwerendę i dostosujemy widok tej zapisanej kwerendy. Obiekty, które utworzymy w tym zadaniu, będą używane w innych ćwiczeniach w tym zestawie ćwiczeniowym.

▶ Ćwiczenie 1: Tworzenie jednostek organizacyjnych

Domyślne kontenery Users i Computers są udostępniane w celu ułatwiania instalacji i migracji do domeny Active Directory. Zaleca się utworzenie jednostek organizacyjnych odzwierciedlających model administracyjny i stosowanie tych jednostek organizacyjnych do tworzenia i zarządzania obiektami w usłudze katalogowej. W tym ćwiczeniu utworzymy jednostki organizacyjne dla domeny przykładowej *contoso.com*. Te jednostki organizacyjne będą używane w dalszych zadaniach i ćwiczeniach w tym zestawie ćwiczeniowym.

1. Zalogować się jako Administrator na komputerze SERVER01.
2. Otworzyć przystawkę Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory).
3. Rozwinąć węzeł domeny.
4. Kliknąć prawym przyciskiem myszy węzeł domeny, wybrać New (Nowy), a następnie wybrać Organizational Unit (Jednostka organizacyjna).
5. Wpisać nazwę jednostki organizacyjnej: User Accounts.
6. Zaznaczyć opcję Protect Container From Accidental Deletion (Chroń kontener przed przypadkowym usunięciem).
7. Kliknąć OK.
8. Kliknąć prawym przyciskiem myszy tę jednostkę organizacyjną i wybrać Properties (Właściwości).
9. W polu *Description* (Opis) wpisać **Tożsamości użytkowników nie będących administratorami**.
10. Kliknąć OK.
11. Powtórzyć kroki 2-10, aby utworzyć następujące jednostki organizacyjne:

Nazwa OU	Opis OU
Clients	Komputery klienckie
Groups	Grupy nie-administracyjne
Admins	Tożsamości i grupy administracyjne
Servers	Serwery

▶ Ćwiczenie 2: Tworzenie użytkowników

Gdy już utworzyliśmy jednostki organizacyjne w domenie *contoso.com*, jesteśmy gotowi do wypełnienia usługi katalogowej obiektami. W tym ćwiczeniu utworzymy kilku użytkowników w dwóch spośród jednostek organizacyjnych utworzonych w ćwiczeniu 1 „Tworzenie jednostek organizacyjnych”. Te obiekty użytkowników będą używane w dalszych zadaniach i ćwiczeniach w tym zestawie ćwiczeniowym. Dla każdego użytkownika tworzymy złożone, bezpieczne hasło. Hasła trzeba zapamiętać, ponieważ w oparciu o te konta użytkowników będziemy logować się do systemu w trakcie przeprowadzania innych ćwiczeń.

1. Zalogować się jako administrator na komputerze SERVER01 i otworzyć przystawkę Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory).

2. W drzewie konsoli rozwinąć węzeł domeny *contoso.com* i zaznaczyć jednostkę organizacyjną User Accounts.
3. Kliknąć prawym przyciskiem myszy jednostkę organizacyjną User Accounts, wybrać New (Nowy), a następnie wybrać User (Użytkownik).
   Pojawi się okno dialogowe New Object – User (Nowy obiekt – Użytkownik).
4. W polu First Name (Imię) wpisać imię użytkownika: **Dan**.
5. W polu Last Name (Nazwisko) wpisać nazwisko użytkownika: **Holme**.
6. W polu User Logon Name (Nazwa logowania użytkownika) wpisać nazwę logowania tego użytkownika: **dholme**.
7. W polu tekstowym User Logon Name (Pre-Windows 2000) (Nazwa logowania użytkownika (systemy starsze niż Windows 2000)) wpisać nazwę logowania w starszych systemach: **dholme.**
8. Kliknąć Next (Dalej).
9. Wpisać hasło początkowe dla użytkownika w polach Password (Hasło) i Confirm Password (Potwierdź hasło).
   Domyślne zasady haseł dla domeny Active Directory wymagają siedmiu lub więcej znaków. Ponadto hasło musi zawierać trzy z czterech typów znaków: wielkie litery (A-Z), małe litery (a-z), cyfry (0-9) i znaki niealfanumeryczne (na przykład, ! @ # $ %). Hasło nie może zawierać fragmentu nazwy użytkownika lub nazwy logowania.

   Należy zapamiętać hasło przypisane do tego użytkownika – będziemy logować się na koncie tego użytkownika w innych ćwiczeniach i zadaniach w tym zestawie szkoleniowym.

   Wiele zasobów szkoleniowych stosuje ogólne hasło, takie jak P@ssword. Można zastosować tego typu hasło w ćwiczeniach w tym zestawie szkoleniowym; jednakże zaleca się, aby tworzyć unikalne hasła nawet podczas ćwiczeń, żeby stosować najlepsze praktyki także w środowisku laboratoryjnym.
10. Zaznaczyć opcję User Must Change Password At Next Logon (Użytkownik musi zmienić hasło przy następnym logowaniu).
11. Kliknąć Next (Dalej).
12. Przejrzeć podsumowanie i kliknąć Finish (Zakończ).
13. Kliknąć prawym przyciskiem myszy utworzony obiekt i wybrać Properties (Właściwości).
14. Zbadać atrybuty, które można skonfigurować w oknie dialogowym Properties (Właściwości). Nie należy teraz zmieniać żadnych właściwości użytkownika.
15. Kliknąć OK.
16. Powtórzyć kroki 3-12 i utworzyć następujących użytkowników w jednostce organizacyjnej User Accounts.
    - James Fine
      - First name (Imię): James
      - Last name (Nazwisko): Fine
      - Full name (Pełna nazwa): James Fine
      - User logon name (Nazwa logowania użytkownika): jfine

- Barbara Mayer
  - First name (Imię): Barbara
  - Last name (Nazwisko): Mayer
  - Full name (Pełna nazwa): Barbara Mayer
  - User logon name (Nazwa logowania użytkownika): bmayer
  - Pre-Windows 2000 logon name (Nazwa logowania użytkownika (systemy starsze niż Windows 2000)): bmayer
- Barbara Moreland
  - First name (Imię): Barbara
  - Last name (Nazwisko): Moreland
  - Full name (Pełna nazwa): Barbara Moreland
  - User logon name (Nazwa logowania użytkownika): bmoreland
  - Pre-Windows 2000 logon name (Nazwa logowania użytkownika (systemy starsze niż Windows 2000)): bmoreland

17. Powtórzyć kroki 3-12 i utworzyć konto użytkownika dla siebie w jednostce organizacyjnej User Accounts. Jako nazwy logowania użytkownika należy użyć inicjału imienia połączonego z nazwiskiem, na przykład dholme dla imienia i nazwiska Dan Holme. Należy utworzyć złożone, bezpieczne hasło.
18. Powtórzyć kroki 3-12 i utworzyć konto administracyjne dla siebie w jednostce organizacyjnej Admins. To konto otrzyma uprawnienia administracyjne. Należy utworzyć obiekt użytkownika w jednostce organizacyjnej Admins, a nie w jednostce organizacyjnej User Accounts. Jako nazwy logowania użytkownika należy użyć inicjału imienia połączonego z nazwiskiem i przyrostkiem _admin, na przykład dholme_admin dla imienia i nazwiska Dan Holme Należy utworzyć złożone, bezpieczne hasło.

▶ Ćwiczenie 3: Tworzenie kont komputerów

Konta komputerów powinny być utworzone przed dołączaniem maszyn do domeny. W tym ćwiczeniu utworzymy kilka komputerów w dwóch jednostkach organizacyjnych utworzonych w ćwiczeniu 1. Te obiekty komputerów będą używane w dalszych zadaniach i ćwiczeniach w tym zestawie ćwiczeniowym.

1. Zalogować się jako administrator na komputerze SERVER01 i otworzyć przystawkę Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory).
2. W drzewie konsoli rozwinąć węzeł domeny *contoso.com* i zaznaczyć jednostkę organizacyjną Servers.
3. Kliknąć prawym przyciskiem myszy jednostkę organizacyjną Servers, wybrać New (Nowy), a następnie wybrać Computer (Komputer).
   Pojawi się okno dialogowe New Object – Computer (Nowy obiekt – Komputer).
4. W polu Computer Name (Nazwa komputera) wpisać nazwę komputera: **FILESERVER01**. Wpisana nazwa zostanie też automatycznie wstawiona do pola Computer Name (Pre-Windows 2000) (Nazwa komputera (systemy starsze niż Windows 2000)).

5. Nie należy zmieniać nazwy w polu Computer Name (Pre-Windows 2000) (Nazwa komputera (systemy starsze niż Windows 2000)).
6. Zwrócić uwagę na konto określone w polu tekstowym User Or Group (Użytkownik lub grupa). Nie należy teraz zmieniać tej wartości.
7. Nie należy zaznaczać pola wyboru Assign This Computer Account As A Pre-Windows 2000 Computer (Przypisz to konto komputera jako komputer z systemem starszym niż Windows 2000).
8. Kliknąć OK.
9. Kliknąć prawym przyciskiem myszy komputer i wybrać Properties (Właściwości).
10. Zbadać właściwości, które są dostępne dla komputera. Nie należy teraz zmieniać żadnych atrybutów.
11. Kliknąć OK.
12. Powtórzyć kroki 3-8, aby utworzyć obiekty komputerów dla następujących komputerów:
    - ❑ SHAREPOINT02
    - ❑ EXCHANGE03
13. Powtórzyć kroki 3-8 i utworzyć następujące komputery w jednostce organizacyjnej Clients, zamiast w jednostce organizacyjnej Servers.
    - ❑ DESKTOP101
    - ❑ DESKTOP102
    - ❑ LAPTOP103

▶ Ćwiczenie 4: Tworzenie grup

Najlepszą praktyką jest zarządzanie obiektami w grupach zamiast zarządzania każdym obiektem indywidualnie. W tym ćwiczeniu utworzymy kilka grup w dwóch jednostkach organizacyjnych utworzonych w ćwiczeniu 1. Te grupy będą używane w dalszych zadaniach i ćwiczeniach w tym zestawie ćwiczeniowym.

1. Zalogować się jako administrator na komputerze SERVER01 i otworzyć przystawkę Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory).
2. W drzewie konsoli należy rozwinąć węzeł domeny *contoso.com* i zaznaczyć jednostkę organizacyjną Groups.
3. Kliknąć prawym przyciskiem myszy jednostkę organizacyjną Groups, wybrać New (Nowy), a następnie wybrać Group (Grupa).
   Pojawi się okno dialogowe New Object – Group (Nowy obiekt – Grupa).
4. Wpisać nazwę nowej grupy w polu Group Name (Nazwa grupy): **Finanse.**
5. Nie należy zmieniać nazwy w polu Group Name (Pre-Windows 2000) (Nazwa grupy (systemy starsze niż Windows 2000)).
6. Na liście Group Type (Typ grupy) należy zaznaczyć opcję: Security (Zabezpieczenia).
7. Na liście Group Scope (Zakres grupy) należy zaznaczyć opcję: Global (Globalny).
8. Kliknąć OK.
   Obiekty grupy mają wiele właściwości, które można konfigurować. Mogą być one określane po utworzeniu obiektu.

9. Kliknąć grupę prawym przyciskiem myszy i wybrać Properties (Właściwości).
10. Zbadać właściwości dostępne dla grupy. Nie należy teraz zmieniać żadnych atrybutów.
11. Kliknąć OK.
12. Powtórzyć kroki 3-8, aby utworzyć następujące globalne grupy zabezpieczeń w jednostce organizacyjnej Groups:
    - ❑ Finance Managers
    - ❑ Sales
    - ❑ APP_Office 2007
13. Powtórzyć kroki 3-8, aby utworzyć następujące globalne grupy zabezpieczeń w jednostce organizacyjnej Admins, zamiast w jednostce organizacyjnej Groups:
    - ❑ Help Desk
    - ❑ Windows Administrators

▶ Ćwiczenie 5: Dodawanie użytkowników i komputerów do grup

Po utworzeniu grup można dodać obiekty jako członków grup. W tym ćwiczeniu dodamy użytkowników i komputery do grup. W trakcie przeprowadzania tej operacji nabierzemy doświadczenia w pracy z oknem dialogowym Select (Wybieranie), które jest używane w kilku procedurach do wynajdowania obiektów w Active Directory.

1. Zalogować się jako administrator na komputerze SERVER01 i otworzyć przystawkę Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory).
2. Otworzyć właściwości swojego konta administracyjnego w jednostce organizacyjnej Admins.
3. Kliknąć kartę Member Of (Członek grupy).
4. Kliknąć przycisk Add (Dodaj).
5. W oknie dialogowym Select Groups (Wybieranie: Grupy) wpisać nazwę **Domain Admins** (Administratorzy domeny).
6. Kliknąć OK.
7. Kliknąć ponownie OK, aby zamknąć właściwości konta.
8. Otworzyć właściwości grupy Help Desk w jednostce organizacyjnej Admins.
9. Kliknąć kartę Members (Członkowie).
10. Kliknąć przycisk Add (Dodaj).
11. W oknie dialogowym Select (Wybieranie) wpisać **Barb**.
12. Kliknąć Check Names (Sprawdź nazwy).
    Pojawi się okno Multiple Names Found (Znaleziono wiele nazw).
13. Zaznaczyć nazwę Barbara Mayer i kliknąć OK.
14. Kliknąć OK, aby zamknąć okno dialogowe Select (Wybieranie).
15. Kliknąć ponownie OK, aby zamknąć właściwości grupy.
16. Otworzyć właściwości grupy APP_Office 2007 w jednostce organizacyjnej Groups.

17. Kliknąć kartę Members (Członkowie).
18. Kliknąć przycisk Add (Dodaj).
19. W oknie dialogowym Select (Wybieranie) wpisać DESKTOP101.
20. Kliknąć Check Names (Sprawdź nazwy).
    Pojawi się okno dialogowe Name Not Found (Nie znaleziono nazwy) wskazujące, że nie udało się ustalić podanego obiektu.
21. Kliknąć Cancel (Anuluj), aby zamknąć okno Name Not Found (Nie znaleziono nazwy).
22. W oknie Select (Wybieranie) kliknąć Object Types (Typy obiektów).
23. Zaznaczyć Computers (Komputery) jako typ obiektu i kliknąć OK.
24. Kliknąć Check Names (Sprawdź nazwy). Tym razem nazwa zostanie ustalona, ponieważ okno Select (Wybieranie) będzie uwzględniać komputery przy rozstrzyganiu nazw.
25. Kliknąć OK.

► Ćwiczenie 6: Odnajdowanie obiektów w Active Directory

Gdy trzeba znaleźć obiekt w usłudze katalogowej domeny, czasami efektywniej jest skorzystać z funkcjonalności wyszukiwania, niż ręcznie przechodzić przez strukturę jednostek organizacyjnych w poszukiwaniu obiektu. W tym ćwiczeniu skorzystamy z trzech interfejsów do odnajdowania obiektów w Active Directory.

1. Zalogować się na komputerze SERVER01 i otworzyć przystawkę Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory).
   Należy otworzyć konsolę Active Directory Users And Computers lub niestandardową konsolę, która zawiera tę przystawkę. Nie należy otwierać narzędzia Server Manager (Menedżer serwera), ponieważ przystawka Active Directory Users And Computers w narzędziu Server Manager nie obsługuje kwerend zapisanych (Saved Queries).
2. Kliknąć przycisk Find Objects In Active Directory Domain Services (Znajdź obiekty w usługach domenowych w usłudze Active Directory).
3. Upewnić się, że na liście rozwijanej In (W) wybrana jest opcja *contoso.com* (nazwa domeny).
4. W polu Name (Nazwa) wpisać **Barb**.
5. Kliknąć Find Now (Znajdź teraz).
6. Dwóch użytkowników o imieniu Barbara powinno pojawić się w wynikach wyszukiwania.
7. Zamknąć okno Find (Znajdowanie).
8. W przystawce Active Directory Users And Computers kliknąć prawym przyciskiem myszy węzeł Saved Queries (Zapisane kwerendy), wskazać polecenie New (Nowa), a następnie kliknąć Query (Kwerenda).
9. W polu Name (Nazwa) wpisać Wszyscy użytkownicy.
10. W polu Description (Opis) wpisać Użytkownicy całej domeny.
11. Kliknąć przycisk Define Query (Definiuj kwerendę).
12. Na karcie Users (Użytkownicy) w polu Name (Nazwa) wybrać Has A Value (Ma wartość).
13. Dwa razy kliknąć OK, aby zamknąć okna dialogowe.

Pojawią się wyniki zapisanej kwerendy. Warto zauważyć, że pokazani będą użytkownicy zarówno z jednostki organizacyjnej User Accounts, z jednostki organizacyjnej Admins, jak również konta z wbudowanego kontenera Users.

14. Z menu wybrać View, a następnie kliknąć Add/Remove Columns (Dodaj/Usuń kolumny).
15. Na liście Available Columns (Dostępne kolumny) zaznaczyć Last Name (Nazwisko) i kliknąć przycisk Add (Dodaj).
16. Na liście Displayed columns (Kolumny wyświetlane) zaznaczyć Type (Typ) i kliknąć przycisk Remove (Usuń).
17. Kliknąć OK.
18. Przeciągnąć nagłówek kolumny Last Name (Nazwisko) tak, aby znalazł się pomiędzy kolumnami Name (Nazwa) a Description (Opis).
19. Kliknąć nagłówek kolumny Last Name (Nazwisko), aby posortować użytkowników w kolejności alfabetycznej według nazwiska.

Podsumowanie lekcji

- Jednostki organizacyjne (OU) są pojemnikami administracyjnymi, które gromadzą obiekty mające wspólne wymagania związane z administrowaniem, konfigurowaniem lub prezentowaniem. Zapewniają sposób na łatwy dostęp i zarządzanie zbiorem użytkowników, grup, komputerów lub innych obiektów. Jednostce organizacyjnej nie można nadawać uprawnień do zasobu, takiego jak folder udostępniany.
- Podczas tworzenia obiektu, takiego jak użytkownik, komputer lub grupa można konfigurować tylko ograniczoną liczbę jego właściwości. Po utworzeniu obiektu można otworzyć jego właściwości i konfigurować atrybuty, które nie były widoczne podczas tworzenia.
- Właściwości obiektu, takie jak Description (Opis), Managed By (Zarządzany przez) i Notes (Uwagi) mogą służyć do dokumentowania ważnych informacji na temat obiektu.
- Domyślnie jednostki organizacyjne są tworzone z ochroną uniemożliwiającą przypadkowe usunięcie danej jednostki organizacyjnej. Aby wyłączyć tę ochronę, trzeba włączyć opcję Advanced Features (Opcje zaawansowane) z menu View (Widok). Następnie we właściwościach jednostki organizacyjnej należy kliknąć kartę Object (Obiekt), aby wyłączyć ochronę.

Pytania do lekcji

Poniższe pytania można wykorzystać do przetestowania swojej wiedzy na temat informacji zawartych w lekcji 2 „Tworzenie obiektów w Active Directory”.

Uwaga Odpowiedzi

Odpowiedzi na te pytania i wyjaśnienia, dlaczego dany wybór odpowiedzi jest poprawny lub niepoprawny, można znaleźć w części „Odpowiedzi” na końcu tej książki.

1. Otworzyliśmy wiersz polecenia korzystając z opcji Run As Administrator (Uruchom jako administrator) i używając poświadczeń należących do grupy Domain Admins (Administratorzy domeny). Korzystamy z polecenia *Dsrm*, aby usunąć jednostkę

organizacyjną, która została przypadkowo utworzona przez Jamesa, członka grupy Administrators. Otrzymujemy odpowiedź: Dsrm Failed: Access Is Denied (dsrm niepowodzenie: Odmowa dostępu). Jaka jest przyczyna tego błędu?

A. Trzeba uruchomić wiersz polecenia jako członek grupy Administrators (Administratorzy), żeby wykonywać działania na Active Directory.

B. Tylko członkowie grupy Administrators (Administratorzy) mogą usuwać jednostki organizacyjne.

C. Tylko właściciel jednostki organizacyjnej może usunąć jednostkę organizacyjną.

D. Jednostka organizacyjna jest chroniona przed usunięciem.

Lekcja 3: Delegowanie i zabezpieczenia obiektów Active Directory

W poprzednich lekcjach tego rozdziału dowiedzieliśmy się, jak tworzyć użytkowników, grupy, komputery i jednostki organizacyjne oraz jak uzyskiwać dostęp do właściwości tych obiektów. Możliwość wykonywania tych działań była zależna od członkostwa w grupie administratorów domeny. Nie chcielibyśmy, aby każdy użytkownik zespołu helpdesk był członkiem grupy administratorów domeny tylko po to, aby resetować hasła i odblokowywać konta użytkowników. Należy natomiast umożliwić zespołowi helpdesk i wszystkim rolom w organizacji wykonywanie zadań, które są wymagane przez daną rolę i nic ponadto. W tej lekcji dowiemy się, jak delegować określone zadania administracyjne w Active Directory, co można osiągnąć zmieniając listy kontroli dostępu (ACL) dla obiektów Active Directory.

Po ukończeniu tej lekcji Czytelnik będzie umiał:

- Opisać cel biznesowy delegowania.
- Przypisać uprawnienia do obiektów Active Directory korzystając z interfejsów użytkownika edytora zabezpieczeń oraz narzędzia Delegation of Control Wizard (Kreator delegowania kontroli).
- Przeglądać i raportować uprawnienia do obiektów Active Directory korzystając z interfejsu użytkownika narzędzi wiersza polecenia.
- Oceniać czynne uprawnienia dla użytkownika lub grupy.
- Przywracać domyślne ustawienia uprawnień dla obiektu.
- Opisać relację pomiędzy delegowaniem a projektem jednostek organizacyjnych.

Przewidywany czas trwania lekcji: 35 minut

Zrozumienie delegowania

W większości organizacji istnieje więcej niż jeden administrator, a wraz ze wzrostem organizacji zadania administracyjne są często przekazywane różnym administratorom lub organizacjom wspierającym. Na przykład w wielu organizacjach helpdesk jest w stanie resetować hasła użytkowników i odblokowywać zablokowane konta użytkowników. Ta możliwość helpdesku jest oddelegowanym zadaniem administracyjnym.

Helpdesk zwykle nie może tworzyć nowych kont użytkowników, ale może dokonywać określonych zmian w istniejących kontach użytkowników. Delegowane zadanie jest specyficzne lub szczegółowe.

Wracając do przykładu, w większości organizacji możliwość resetowania haseł przez pracowników helpdesku dotyczy zwykłych kont użytkowników, a nie kont używanych do administracji czy kont usług. Można więc powiedzieć, że zakres delegowania obejmuje konta standardowych użytkowników.

Wszystkie obiekty Active Directory, takie jak użytkownicy, komputery i grupy utworzone w poprzedniej lekcji mogą być zabezpieczone przy użyciu listy uprawnień, co pozwoli nadać członkom helpdesku uprawnienia do resetowania haseł użytkowników. Uprawnienia do obiektu są nazywane ACE – *access control entries* (wpisami kontroli dostępu) i są przypisywane do użytkowników, grup lub komputerów (zwanych *podmiotami zabezpieczeń*). Wpisy ACE są zapisywane na arbitralnej liście kontroli dostępu (DACL) dla danego obiektu. Lista DACL jest częścią listy kontroli dostępu (ACL) dla obiektu, która zawiera też systemową listę kontroli dostępu (SACL) Może to brzmieć znajomo dla kogoś, kto zajmował się uprawnieniami do plików i folderów – terminy i pojęcia są identyczne.

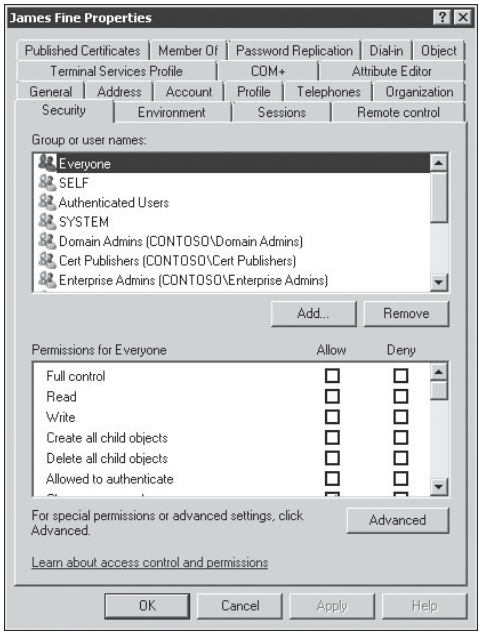
Delegowanie kontroli administracyjnej, zwane też delegowaniem kontroli lub po prostu delegowaniem, oznacza przypisywanie uprawnień, które zarządzają dostępem do obiektów i właściwości w Active Directory. Tak jak można nadać grupie możliwość zmieniania plików w folderze, tak można nadać grupie możliwość resetowania haseł dla obiektów użytkowników.

Przeglądanie listy ACL dla obiektu Active Directory

Na najniższym poziomie jest lista ACL dla obiektu pojedynczego użytkownika w Active Directory. Aby przejrzeć listę ACL dla obiektu należy:

1. Otworzyć przystawkę Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory).
2. Kliknąć menu View (Widok) i zaznaczyć Advanced Features (Opcje zaawansowane).
3. Kliknąć prawym przyciskiem myszy dany obiekt i wybrać Properties (Właściwości).
4. Kliknąć kartę Security (Zabezpieczenia).
   Jeśli funkcja Advanced Features (Opcje zaawansowane) nie jest włączona, to karta Security (Zabezpieczenia) nie będzie widoczna w oknie dialogowym Properties (Właściwości) dla obiektu.

   Karta Security (Zabezpieczenia) okna dialogowego Properties (Właściwości) dla obiektu jest pokazana na rysunku 2-15.
5. Kliknąć przycisk Advanced (Zaawansowane).
   Karta Security (Zabezpieczenia) pokazuje ogólny przegląd podmiotów zabezpieczeń, którym nadano uprawnienia do obiektu, ale w przypadku list ACL dla Active Directory karta Security (Zabezpieczenia) rzadko jest wystarczająco szczegółowa, aby zapewnić informacje potrzebne do interpretowania lub zarządzania listą ACL. Należy zawsze klikać przycisk Advanced (Zaawansowane), aby otwierać okno dialogowe Advanced Security Settings (Zaawansowane ustawienia zabezpieczeń).



Rysunek 2-15 Karta Security (Zabezpieczenia) okna dialogowego Properties dla obiektu Active Directory

Pojawi się okno dialogowe Advanced Security Settings (Zaawansowane ustawienia zabezpieczeń) dla danego obiektu, pokazane na rysunku 2-16. Karta Permissions (Uprawnienia) okna dialogowego Advanced Security Settings (Zaawansowane ustawienia zabezpieczeń) pokazuje listę DACL danego obiektu. Na rysunku 2-16 można zobaczyć, że wpisy ACE są podsumowywane w pojedynczym wierszu na liście Permission entries (Wpisy uprawnienia). W tym oknie dialogowym nie widać pojedynczych wpisów ACE na liście DACL. Na przykład uprawnienie zaznaczone na rysunku 2-16 faktycznie składa się z dwóch wpisów ACE.

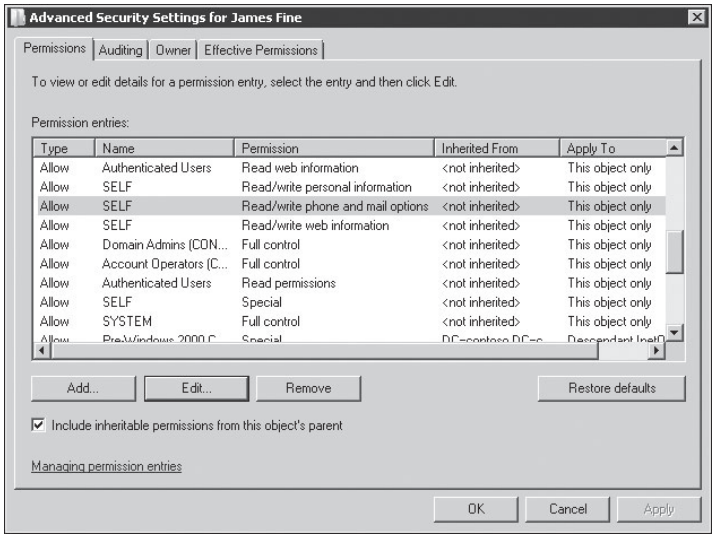
6. Aby zobaczyć poszczególne wpisy ACE dla wpisu uprawnienia, należy zaznaczyć dany wpis i kliknąć Edit (Edytuj). Pojawi się okno dialogowe Permission Entry (Wpis uprawnienia) pokazujące szczegółowo poszczególne wpisy ACE składające się na dany wpis, jak pokazano na rysunku 2-17.

Pytanie kontrolne

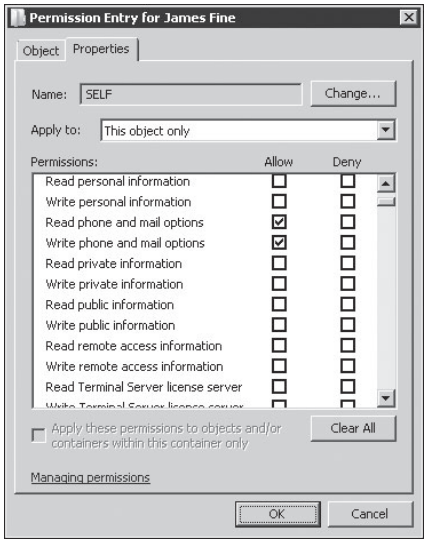
- Chcemy przejrzeć uprawnienia przypisane do jednostki organizacyjnej. Otwieramy okno dialogowe Properties (Właściwości) dla jednostki organizacyjnej, ale nie widać w nim karty Security (Zabezpieczenia). Co trzeba zrobić?

Odpowiedź na pytanie kontrolne

- W przystawce Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) należy kliknąć menu View (Widok) i zaznaczyć opcję Advanced Features (Opcje zaawansowane).



Rysunek 2-16 Okno dialogowe Advanced Security Settings (Zaawansowane ustawienia zabezpieczeń) dla obiektu Active Directory



Rysunek 2-17 Okno dialogowe Permission Entry (Wpis uprawnienia)

Prawa dostępu do obiektów i właściwości, prawa kontroli dostępu

Lista DACL dla obiektu umożliwia przypisywanie uprawnień dla określonych właściwości obiektu. Jak mogliśmy zobaczyć na rysunku 2-17, można zezwolić (lub odmówić) na zmienianie opcji telefonicznych i poczty elektronicznej. Nie jest to w istocie jedna właściwość; jest to zbiór, który obejmuje kilka konkretnych właściwości. Zbiory właściwości ułatwiają zarządzanie uprawnieniami do często używanych kolekcji właściwości. Można

nawet przejść na dokładniejszy poziom i zezwolić lub odmówić uprawnień do zmieniania tylko numeru telefonu komórkowego lub tylko adresu domowego.

Można też przypisywać uprawnienia do zarządzania prawami dostępu dla działań takich, jak zmienianie lub resetowanie hasła. Różnica pomiędzy tymi dwoma prawami kontroli dostępu jest ważna do zrozumienia. Jeśli mamy prawo do *zmieniania* hasła, to musimy znać i podać aktualne hasło przed dokonaniem zmiany. Jeśli mamy prawo do *zresetowania* hasła, to nie musimy znać poprzedniego hasła.

Na koniec można przypisywać uprawnienia do obiektów. Na przykład możliwość zmieniania uprawnień dla obiektu jest kontrolowana przez wpis ACE Allow::Modify Permissions (Zezwalaj::Modyfikacja uprawnień). Uprawnienia dla obiektu określają też, czy jesteśmy w stanie tworzyć obiekty potomne. Na przykład można nadać zespołowi wsparcia technicznego uprawnienia do tworzenia obiektów komputerów w jednostce organizacyjnej dla biurkowych i przenośnych komputerów klienckich. Wpis ACE Allow::Create Computer Objects (Zezwalaj::Tworzenie obiektów Komputer) zostałby przypisany zespołowi wsparcia technicznego dla tej jednostki organizacyjnej.

Typem i zakresem uprawnień można zarządzać korzystając z dwóch kart: Object (Obiekt) i Properties (Właściwości) oraz list rozwijanych Apply To (Zastosuj do) na każdej z tych kart.

Przypisywanie uprawnienia przy użyciu okna dialogowego Advanced Security Settings

Wyobraźmy sobie scenariusz, w którym chcemy pozwolić zespołowi helpdesk zmieniać hasło dla konta użytkownika James Fine. W tej części najpierw nauczymy się, jak to zrobić w najbardziej skomplikowany sposób: przypisując wpis ACE do listy DACL dla obiektu użytkownika. Później dowiemy się, jak przeprowadzić delegowanie korzystając z narzędzia Delegation Of Control Wizard (Kreator delegowania kontroli) dla całej jednostki organizacyjnej użytkowników i zobaczymy, dlaczego ta druga metoda jest zalecana.

1. Otworzyć przystawkę Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory).
2. Kliknąć menu View (Widok) i zaznaczyć Advanced Features (Opcje zaawansowane).
3. Kliknąć prawym przyciskiem myszy dany obiekt i wybrać Properties (Właściwości).
4. Kliknąć kartę Security (Zabezpieczenia).
5. Kliknąć przycisk Advanced (Zaawansowane).
6. Kliknąć przycisk Add (Dodaj).
   Jeśli włączona jest funkcja User Account Control (Kontrola konta użytkownika), to konieczne może być kliknięcie przycisku Edit (Edytuj) i być może wpisanie poświadczeń administracyjnych, zanim pojawi się przycisk Add (Dodaj).
7. W oknie dialogowym Select (Wybieranie) zaznaczyć podmiot zabezpieczeń, do którego będą przypisywane uprawnienia.
   Ważną, najlepszą praktyką jest przypisywanie uprawnień grupom, a nie pojedynczym użytkownikom. W naszym przykładzie wybralibyśmy grupę Help Desk.
8. Kliknąć OK.
   Pojawi się okno dialogowe Permission Entry (Wpis uprawnienia).

9. Skonfigurować uprawnienia, które chcemy przypisać.
   W naszym przykładzie na karcie Object (Obiekt) przewinąć listę Permissions (Uprawnienia) i zaznaczyć Allow::Reset Password (Zezwalaj::Resetowanie hasła).
10. Klikać OK, aby zamknąć wszystkie okna dialogowe.

Zrozumienie i zarządzanie uprawnieniami z dziedziczeniem

Można sobie wyobrazić, że przypisywanie grupie Help Desk uprawnień do resetowania haseł dla każdego, pojedynczego obiektu użytkownika byłoby bardzo czasochłonne. Na szczęście nie trzeba tego robić, a w istocie jest okropną praktyką przypisywanie uprawnień pojedynczym obiektom w Active Directory. Zamiast tego należy przypisywać uprawnienia do jednostek organizacyjnych. Uprawnienia przypisane jednostce organizacyjnej będą dziedziczone przez wszystkie obiekty w tej jednostce organizacyjnej. W ten sposób, jeśli nadamy pracownikom helpdesku uprawnienia do resetowania haseł dla obiektów użytkowników i przyłączymy te uprawnienia do jednostki organizacyjnej zawierającej użytkowników, to wszystkie obiekty użytkowników wewnątrz tej jednostki organizacyjnej odziedziczą te uprawnienia. Za jednym zamachem oddelegujemy to zadanie administracyjne.

Dziedziczenie jest łatwym do zrozumienia pojęciem. Obiekty potomne dziedziczą uprawnienia nadrzędnego kontenera lub jednostki organizacyjnej. Ten kontener lub jednostka organizacyjna dziedziczą z kolei swoje uprawnienia ze swojego nadrzędnego kontenera, jednostki organizacyjnej albo z samej domeny w przypadku kontenera lub jednostki organizacyjnej pierwszego poziomu. Powodem, dla którego obiekty potomne dziedziczą uprawnienia po swoich obiektach nadrzędnych, jest to, że domyślnie każdy nowy obiekt jest tworzony z włączoną opcją Include Inheritable Permissions From This Object's Parent (Dołącz uprawnienia dziedziczne z tego obiektu nadrzędnego). Można zobaczyć tę opcję na rysunku 2-16.

Należy jednak zwrócić uwagę, że, jak wskazuje ta opcja, tylko właściwości *dziedziczne* będą dziedziczone przez obiekt potomny. Jednakże nie każde uprawnienie jest dziedziczne. Na przykład uprawnienie do resetowania haseł przypisane do jednostki organizacyjnej nie będzie dziedziczone przez obiekty grup, ponieważ obiekty grup nie mają atrybutu hasła. Tak więc dziedziczenie ograniczone jest do określonych klas obiektów: hasła mają zastosowanie do obiektów użytkowników, a nie grup. Dodatkowo można użyć pola Apply To (Zastosuj do) w oknie dialogowym Permission Entry (Wpis uprawnienia), aby określić zakres dziedziczenia uprawnienia. Te rozważania mogą stać się bardzo skomplikowane. Trzeba wiedzieć, że domyślnie nowe obiekty dziedziczą właściwości dziedziczne po swoich obiektach nadrzędnych – zwykle po jednostce organizacyjnej lub kontenerze.

Co, jeśli odziedziczone uprawnienie nie jest właściwe? Można zrobić trzy rzeczy, aby zmodyfikować uprawnienia, które dziedziczy obiekt potomny.

Po pierwsze, można wyłączyć dziedziczenie wyłączając opcję Include Inheritable Permissions From This Object's Parent (Dołącz uprawnienia dziedziczne z tego obiektu nadrzędnego) w oknie dialogowym Advanced Security Settings (Zaawansowane ustawienia zabezpieczeń). W takim przypadku obiekt nie będzie już dziedziczył żadnych ustawień po swoim obiekcie nadrzędnym – wszystkie uprawnienia będą jawnie zdefiniowane dla obiektu potomnego. Zwykle nie jest to dobrą praktyką, ponieważ tworzy wyjątek od reguły ustanowionej przez uprawnienia kontenerów nadrzędnych.

Drugą opcją jest zezwolenie na dziedziczenie, a przy tym uchylenie odziedziczonego uprawnienia przez jawne uprawnienie konkretnie przypisane do obiektu potomnego. Jawne uprawnienia zawsze uchylają uprawnienia dziedziczone po obiektach nadrzędnych. Ma to ważne konsekwencje: Jawne uprawnienie, które *zezwala* na dostęp, uchyli w istocie odziedziczone uprawnienie, które *odmawia* tego samego dostępu. Może to się wydawać nieintuicyjne, ale w istocie takie nie jest: reguła jest definiowana przez obiekt nadrzędny (odmów), ale dla obiektu podrzędnego skonfigurowano wyjątek (zezwalaj).

Po trzecie, możemy zmienić zakres dziedziczenia dla samego uprawnienia nadrzędnego poprzez zmianę opcji na liście rozwijanej Apply To (Zastosuj do) w oknie dialogowym Permission Entry (Wpis uprawnień). W większości przypadków jest to najlepsza metoda. W rezultacie to, co robimy, jest bardziej dokładnym definiowaniem zasady zabezpieczeń w postaci listy ACL w jej źródle, a nie próbą zastępowania jej na niższych poziomach drzewa.

Wskazówka egzaminacyjna

Należy uważać na scenariusze, w których dostęp lub delegowanie nie działa w oczekiwany sposób, ponieważ dziedziczenie zostało naruszone – obiekt potomny nie dziedziczy już uprawnień po obiekcie nadrzędnym – albo ponieważ obiekt potomny ma jawne uprawnienie uchylające uprawnienie odziedziczone po obiekcie nadrzędnym.

Delegowanie zadań administracyjnych przy użyciu narzędzia Delegation Of Control Wizard

Widząc złożoność list DACL można stwierdzić, że zarządzanie uprawnieniami za pomocą okna dialogowego Permission Entry (Wpis uprawnienia) nie jest prostym zadaniem. Na szczęście najlepszą praktyką nie jest zarządzanie uprawnieniami przy użyciu interfejsów zabezpieczeń, ale raczej przez zastosowanie narzędzia Delegation of Control Wizard (Kreator delegowania kontroli). Następująca procedura przedstawia szczegółowo użycie tego kreatora.

1. Otworzyć przystawkę Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory).
2. Kliknąć prawym przyciskiem myszy węzeł (domeny lub jednostki organizacyjnej), dla którego chcemy delegować zadania administracyjne lub kontrolę, i wybrać opcję Delegate Control (Deleguj kontrolę).
   W tym przykładzie wybralibyśmy jednostkę organizacyjną, która zawiera użytkowników. Wyświetlone zostanie okno Delegation of Control Wizard (Kreator delegowania kontroli), które poprowadzi nas przez wymagane kroki.
3. Kliknąć Next (Dalej).
   Najpierw wybierzemy grupę administracyjną, której przydzielimy uprawnienia.
4. Na stronie Users or Groups (Użytkownicy lub grupy) należy kliknąć przycisk Add (Dodaj).
5. Korzystając z okna dialogowego Select (Wybieranie) wybrać grupę i kliknąć OK.
6. Kliknąć Next (Dalej).
   Następnie określimy konkretne zadania, które chcemy przypisać do tej grupy.

7. Na stronie Tasks To Delegate (Zadania do oddelegowania) należy zaznaczyć zadanie. W tym przykładzie zaznaczylibyśmy Reset User Passwords and Force Password Change at Next Logon (Resetowanie haseł użytkowników i wymuszanie zmiany hasła przy następnym logowaniu).
8. Kliknąć Next (Dalej).
9. Przejrzeć podsumowanie wykonanych zadań i kliknąć Finish (Zakończ). Narzędzie Delegation of Control Wizard (Kreator delegowania kontroli) zastosuje wpisy ACE, które są wymagane do umożliwienia wybranej grupie wykonywania danego zadania.

Raportowanie i przeglądanie uprawnień

Istnieje kilka innych sposobów przeglądania i raportowania uprawnień, gdy trzeba ustalić, kto co może zrobić. Widzieliśmy już, że można przeglądać uprawnienia na liście DACL korzystając z okien dialogowych Advanced Security Settings (Zaawansowane ustawienia zabezpieczeń) i Permission Entry (Wpis uprawnienia).

Dostępne jest też narzędzie wiersza polecenia DSACLs (*Dsacls.exe)*, które generuje raporty dotyczące obiektów usługi katalogowej. Jeśli wpiszemy to polecenie podając nazwę wyróżniającą obiektu, to zobaczymy raport na temat uprawnień obiektu. Na przykład poniższe polecenie utworzy raport z uprawnieniami powiązanymi z jednostką organizacyjną User Accounts:

```
dsacls.exe "ou=User Accounts,dc=contoso,dc=com"
```

Narzędzie *Dsacls* może być też używane do ustawiania uprawnień – do delegowania. Wpisać **dsacls.exe /?**, aby uzyskać pomoc dotyczącą składni i użycia polecenia *Dsacls*.

Usuwanie lub resetowanie uprawnień dla obiektu

Jak usunąć lub zresetować uprawnienia, które zostały oddelegowane? Niestety, nie ma polecenia wycofania delegowania. Trzeba wykonać jedną z następujących operacji:

- Otworzyć okna dialogowe Advanced Security Settings (Zaawansowane ustawienia zabezpieczeń) i Permission Entry (Wpis uprawnienia), aby usunąć uprawnienia.
- Jeśli chcemy zresetować uprawnienia dla obiektu z powrotem do wartości domyślnych, otworzyć okno dialogowe Advanced Security Settings (Zaawansowane ustawienia zabezpieczeń) i kliknąć Restore Defaults (Przywróć domyślne). Ustawienia domyślne są definiowane przez schemat Active Directory dla danej klasy obiektów. Po przywróceniu wartości domyślnych można przekonfigurować jawne uprawnienia, które chcemy dodać do listy DACL.
- Polecenie *Dsacls* udostępnia także przełącznik */s* do resetowania uprawnień do wartości domyślnych zdefiniowanych przez schemat oraz przełącznik */t*, który dokonuje tej zmiany w całym drzewie – dla danego obiektu i wszystkich jego obiektów potomnych. Na przykład, aby zresetować uprawnienia dla jednostki organizacyjnej User Accounts i wszystkich jej potomnych jednostek organizacyjnych i obiektów, należałoby wpisać:

  ```
  dsacls "ou=User Accounts,dc=contoso,dc=com" /resetDefaultDACL
  ```

Zrozumienie czynnych uprawnień

Czynne uprawnienia są wynikowymi uprawnieniami dla danego podmiotu zabezpieczeń, takiego jak użytkownik lub grupa, opartymi na skumulowanym wpływie wszystkich odziedziczonych i jawnych wpisów ACE. Na przykład nasza możliwość resetowania hasła użytkownika może wynikać z naszego członkostwa w grupie, której udzielono uprawnienia Reset Password (Resetowanie hasła) dla jednostki organizacyjnej o kilka poziomów powyżej danego obiektu użytkownika. Odziedziczone uprawnienie przypisane do grupy, do której należymy, spowodowało czynne uprawnienie Allow::Reset Password (Zezwalaj::Resetowanie hasła). Czynne uprawnienia mogą być skomplikowane, jeśli weźmie się pod uwagę uprawnienia zezwalające i odmawiające, jawne i odziedziczone wpisy ACE oraz fakt, że można należeć do wielu grup, z których każda może mieć przypisane różne uprawnienia.

Uprawnienia, czy to przypisane do naszego konta użytkownika, czy do grupy, do której należymy, są równoważne. Ostatecznie wpis ACE ma zastosowanie względem użytkownika. Najlepszą praktyką jest zarządzanie uprawnieniami przez przypisywanie ich do grup, ale możliwe jest też przypisywanie wpisów ACE pojedynczym użytkownikom lub komputerom. Sam fakt przypisania uprawnienia bezpośrednio użytkownikowi nie oznacza, że to uprawnienie jest bardziej lub mniej ważne niż uprawnienie przypisane do grupy, do której należy użytkownik.

Uprawnienia, które zezwalają na dostęp, kumulują się. Jeśli użytkownik należy do kilku grup, a tym grupom nadano uprawnienia, które zezwalają na różne działania, to użytkownik będzie w stanie wykonywać wszystkie zadania przypisane do tych wszystkich grup, jak również zadania przypisane bezpośrednio do konta użytkownika.

Uprawnienia, które odmawiają dostępu, uchylają odpowiadające im uprawnienia zezwalające na dostęp. Jeśli użytkownik należy do jednej grupy, której nadano uprawnienia do resetowania haseł, i innej grupy, której odmówiono uprawnienia do resetowania haseł, to ta odmowa uprawnienia uniemożliwi użytkownikowi resetowanie haseł.

Uwaga Oszczędne stosowanie uprawnień odmawiających dostępu

Zwykle nie jest konieczne przypisywanie uprawnień odmawiających dostępu. Jeśli po prostu nie przypiszemy uprawnienia zezwalającego na dostęp, to użytkownicy nie będą mogli wykonywać danego zadania. Przed przypisaniem uprawnienia odmawiającego dostępu należy sprawdzić, czy nie można by osiągnąć tego celu przez usunięcie uprawnienia zezwalającego na dostęp. Należy korzystać z uprawnień odmawiających dostępu rzadko i w sposób przemyślany.

Każde uprawnienie jest bardzo szczegółowe. Mimo że użytkownik może nie mieć możliwości resetowania haseł, to nadal może mieć poprzez inne uprawnienia zezwalające na dostęp możliwość zmieniania nazwy logowania użytkownika lub adresu poczty elektronicznej.

Wcześniej w tej lekcji dowiedzieliśmy się też, że obiekty potomne dziedziczą domyślnie uprawnienia dziedziczne po obiektach nadrzędnych, a uprawnienia jawne mogą anulować uprawnienia dziedziczne. Oznacza to, że jawne uprawnienie zezwalające na dostęp w istocie uchyli odziedziczone uprawnienie odmawiające dostępu.

Niestety, skomplikowana interakcja pomiędzy uprawnieniami użytkownika, grupy, jawnymi, odziedziczonymi, zezwalającymi i odmawiającymi dostępu może znacznie utrudnić ustalenie faktycznych uprawnień. Istnieje karta Effective Permissions (Czynne uprawnienia) w oknie dialogowym Advanced Security Settings (Zaawansowane ustawienia zabezpieczeń)

dla obiektu Active Directory, ale ta zakładka jest praktycznie bezużyteczna; nie przedstawia wystarczającej liczby uprawnień, aby zapewniać wymaganą szczegółowość informacji. Można skorzystać z uprawnień raportowanych przez polecenie *Dsacls* lub kartę Permissions (Uprawnienia) okna dialogowego Advanced Security Settings (Zaawansowane ustawienia zabezpieczeń), aby szacować czynne uprawnienia, ale będzie to ręczna praca.

Więcej informacji Kontrola dostępu oparta na rolach

Najlepszym sposobem zarządzania delegowaniem w Active Directory jest zastosowanie kontroli dostępu opartej na rolach. Chociaż to podejście nie jest obejmowane przez egzamin certyfikacyjny, to jest warte zrozumienia w celu zaimplementowania delegowania w praktyce. Więcej informacji można znaleźć w książce *Windows Administration Resource Kit: Productivity Solutions for IT Professionals,* Dan Holme (Microsoft Press, 2008)*.

Projektowanie struktury jednostek organizacyjnych do obsługi delegowania

Jednostki organizacyjne są, jak już wiemy, kontenerami administracyjnymi. Zawierają obiekty, które mają podobne wymagania ze względu na administrowanie, konfigurowanie i widoczność. Rozumiemy teraz pierwsze z tych wymagań: administrowanie. Obiekty, które będą administrowane w ten sam sposób i przez tych samych administratorów, powinny być zawarte w pojedynczej jednostce organizacyjnej. Umieszczając użytkowników w pojedynczej jednostce organizacyjnej o nazwie „User Accounts" można delegować uprawnienia helpdesku do zmiany haseł wszystkich użytkowników, przypisując jedno uprawnienie do jednej jednostki organizacyjnej. Wszelkie inne uprawnienia wpływające na to, co administrator może robić z obiektem użytkownika, będą przypisywane na poziomie jednostki organizacyjnej User Accounts. Na przykład można by pozwolić menedżerom zasobów ludzkich na wyłączanie kont użytkowników w przypadku zwalniania pracowników. To uprawnienie byłoby znowu oddelegowane na poziomie jednostki organizacyjnej User Accounts.

Trzeba pamiętać, że administratorzy powinni logować się w systemach z poświadczeniami użytkownika i uruchamiać narzędzia administracyjne z poświadczeniami drugiego konta, które ma odpowiednie uprawnienia do wykonywania zadań administracyjnych. Te dodatkowe konta są kontami administracyjnymi dla całego przedsiębiorstwa. W przypadku zespołu helpdesku nie jest odpowiednie umożliwianie resetowania haseł z użyciem takich uprzywilejowanych kont i prawdopodobnie nie chcemy, aby menedżerowie zasobów ludzkich mogli wyłączać konta administracyjne. Dlatego konta administracyjne są administrowane inaczej niż konta użytkowników nie będących administratorami. Dlatego właśnie utworzyliśmy osobną jednostkę organizacyjną Admins dla obiektów użytkowników administracyjnych. Uprawnienia dla tej jednostki organizacyjnej będą delegowane inaczej niż w przypadku jednostki organizacyjnej User Accounts.

W podobny sposób można by oddelegować zespołowi wsparcia technicznego możliwość dodawania obiektów komputerów do jednostki organizacyjnej Komputery klienckie, która zawiera stacjonarne i przenośne komputery klienckie, ale nie do jednostki organizacyjnej

* Wydanie polskie: Zestaw narzędzi do administracji Windows: Efektywne rozwiązania dla specjalistów IT Resource Kit, ISBN 978-83-7541-026-6, APN Promise, Warszawa 2008 (przyp. red.).