ITA-107 Systemy operacyjne

Radosław Frąckowiak

Moduł 4

Wersja 1

Wprowadzenie do Active Directory

Spis treści

Informacje o module

Opis modułu

W module tym znajdziesz informacje na temat funkcjonowania usługi **Active Directory** oraz korzyści z jej stosowania. Poznasz budowę logiczna i fizyczną **Active Directory**. Dowiesz się, w jaki sposób zarządzać obiektami jednostek organizacyjnych, przy pomocy różnych narzędzi. Nauczysz się delegować kontrolę administracyjną do wybranej części drzewa katalogu.

Cel modułu

Celem modułu jest zapoznanie z usługą **Active Directory**, oraz narzędziami wykorzystywanymi do zarządzania nią, a także z jednostkami organizacyjnymi wykorzystywanymi do uproszczenia administracji obiektami.

Uzyskane kompetencje

Po zrealizowaniu modułu będziesz:

- wiedział, co to jest usługa katalogowa **Active Directory**, oraz będziesz znał jej budowę logiczna i fizyczną
- potrafił tworzyć jednostki organizacyjne i delegować kontrolę administracyjną
- rozumiał, w jaki sposób usługa **Active Directory** pomaga zarządzać zasobami w sieci

Wymagania wstępne

Ten moduł nie ma żadnego wymagania wstępnego. Możesz od razu rozpocząć pracę z tym modułem

Mapa zależności modułu

Przed przystąpieniem do realizacji tego modułu nie jest wymagane zapoznanie się z materiałem zawartym w innych modułach.

Przygotowanie teoretyczne

Przykładowy problem

W Twojej firmie działa usługa katalogowa **Active Directory**. Wiesz, że przy jej pomocy można znacznie uprościć proces administrowania środowiskiem informatycznym w przedsiębiorstwie. W przyszłości będziesz ją wykorzystywał do zarządzania komputerami i środowiskiem pracy użytkowników. Chcesz przy wykorzystaniu jednostek organizacyjnych stworzyć hierarchię, która będzie odpowiadała strukturze Twojej firmy i ułatwi później zarządzanie stacjami przyłączonymi do domeny. Stworzysz w testowej jednostce organizacyjnej IT Test, jednostkę odpowiadającą Twojemu miastu. W niej trzy jednostki związane z działami w twojej firmie: Produkcja, Logistyka, Ksiegowość. W każdej z nich stworzysz jednostkę Komputery i Użytkownicy. Wykorzystasz do tego różne narzędzia by ocenić, którymi pracuje się najwygodniej. Dla kierownika działu księgowości przypiszesz uprawnienia pozwalające na resetowanie haseł podległych mu użytkowników.

Podstawy teoretyczne

Usługa katalogowa **Active Directory** (ang. **Active Directory Domain Services**) udostępnia rozproszoną bazę danych, która przechowuje i zarządza informacjami o zasobach sieci oraz danymi specyficznymi dla aplikacji potrafiących z tej bazy korzystać. Administratorzy mogą używać **AD DS** do organizowania elementów sieci takich jak użytkownicy, komputery i inne urządzenia w hierarchiczną strukturę. Struktura ta zawiera las, domeny w lesie, a w nich jednostki organizacyjne. Usługi katalogowe umożliwiają użytkownikom pojedyncze logowanie, dzięki czemu autoryzowani użytkownicy mają dostęp do wszystkich zasobów sieciowych.

Funkcje Active Directory

Usługi katalogowe pełnią następujące funkcje:

- Centralna kontrola zasobów sieciowych takich jak serwery, udostępnione pliki i drukarki sprawia, że tylko autoryzowani użytkownicy mają do nich dostęp
- Możliwość centralnej administracji rozproszonymi komputerami, usługami sieciowymi i aplikacjami przy użyciu narzędzi o spójnym interfejsie.
- Bezpieczne przechowywanie wszystkich zasobów, jako obiektów w logicznej, hierarchicznej strukturze.

Logiczna struktura AD DS

Logiczna struktura **Active Directory** składa się z następujących elementów

- **Obiekt** – najbardziej podstawowy element. Klasa obiektu jest szablonem dla typu obiektu, który można stworzyć w Active Directory. Każda klasa obiektu jest zdefiniowana, jako grupa atrybutów definiujących możliwe wartości, które można przypisać do obiektu. Każdy obiekt posiada unikalną kombinację wartości atrybutów.
- J**ednostka organizacyjna** (**OU**) – obiekt-kontener, umożliwiający organizowanie innych obiektów w sposób ułatwiający wykonywanie czynności administracyjnych. Łączenie obiektów w jednostki organizacyjne powoduje, że łatwiej je wyszukiwać i administrować nimi. Można także delegować kontrolę do zarządzania jednostkami organizacyjnymi. Jednostki organizacyjne można zagnieżdżać w innych jednostkach, co jeszcze bardziej upraszcza administrowanie obiektami.
- **Domena** – podstawowa jednostka funkcjonalna logicznej struktury Active Directory, jest zbiorem administracyjnie zdefiniowanych obiektów które dzielą wspólną bazę katalogu, zasady zabezpieczeń i relacje zaufania z innymi domenami.

Drzewo domen – domeny, które są zgrupowane razem w hierarchiczna strukturę. Kiedy dodajemy następną domenę do drzewa, staje się ona „domeną dzieckiem” (ang. **domain child**). Domena, do której dziecko zostało przyłączone, nazywa się domeną rodzicem (ang. **parent domain**).

Nazwa domeny dziecka jest kombinacją jej nazwy z nazwą domeny rodzica formie nazwy **Domain Name System** (**DNS**) np. corp.nwtraders.msft. Oznacza to, że drzewo posiada wspólną przestrzeń nazw DNS.

- **Las** – kompletna instancja **Active Directory**, korzystająca ze wspólnego schematu, konfiguracji oraz wykazu globalnego. Może się składać z jednej lub kilku domen.

Fizyczna struktura AD DS

W odróżnieniu do logicznej struktury, modelującej administracyjne wymagania, struktura fizyczna **Active Directory** optymalizuje ruch sieciowy, określając, kiedy i gdzie wystąpi ruch związany z replikacją i logowaniem. Elementy struktury sieciowej to:

- **Kontrolery domeny** – komputery z zainstalowanym systemem Microsoft Windows Server 2008 i usługą Active Directory. Każdy z nich przechowuje bazę katalogu i pełni funkcje związane z jej replikacją. Kontroler domeny może obsługiwać tylko jedną domenę. W celu zapewnienia ciągłości działania usług katalogowych, każda domena powinna posiadać więcej niż jeden kontroler domeny.
- **Site** – grupa dobrze połączonych ze sobą komputerów. Po skonfigurowaniu site, kontrolery domeny w znajdujące się w nim, często się ze sobą komunikują redukując opóźnienia związane z replikacją między nimi. Site są tworzone w celu optymalizowania dostępnego pasma pomiędzy kontrolerami znajdującymi się w różnych lokalizacjach.
- **Partycje Active Directory** – baza danych AD jest logicznie podzielona na partycje katalogu. Każda z nich jest jednostką replikacji posiadającą swoją własną topologię replikacji. Wszystkie kontrolery domeny w tym samym lesie maja dwie wspólne partycje katalogu: partycje schematu i konfiguracji. Dodatkowo, wszystkie kontrolery w tej samej domenie współdzielą tą sama partycję domeny.
    - **Partycja domeny** – zawiera replikę wszystkich obiektów w domenie, włączając w to użytkowników, grupy, komputery i jednostki organizacyjne. Partycja domeny jest replikowana tylko pomiędzy kontrolerami domeny znajdującymi się w tej samej domenie.
    - **Partycja konfiguracji** – zawiera topologię lasu. Jest tylko jedna partycja konfiguracji wspólna dla całego lasu. Przechowuje informacje dotyczące istniejących domen i site-ów, rozmieszczenia kontrolerów domen i istniejących połączeń pomiędzy nimi, oraz dostępnych usługach. Partycja konfiguracji jest replikowana pomiędzy wszystkimi kontrolerami w lesie.
    - **Partycja schematu** – zawiera schemat lasu. Replikowana pomiędzy wszystkimi kontrolerach domeny w lesie, przechowuje definicje wszystkich obiektów i atrybutów, które mogą być tworzone w katalogu, oraz zasady ich tworzenia i manipulowania nimi.
    - Opcjonalna **partycja aplikacji** – przechowuje informacje o aplikacjach w Active Directory. Każda aplikacja określa sposób przechowywania, kategoryzowania i użycia wykorzystywanych przez nią informacji. W przeciwieństwie do partycji domeny, partycja aplikacji nie może przechowywać obiektów zabezpieczeń takich jak konta użytkowników. W celu zabezpieczenia się przed niepotrzebną replikacją specyficznych partycji aplikacji, możemy zdefiniować, który z kontrolerów domeny w lesie będzie przechowywał jej kopię. Przykładem może być DNS zintegrowany z Active Directory – korzysta z dwóch partycji aplikacji: **ForestDNSZones** i **DomainDNSZones**.

Masters Operations

Kiedy zostanie zmodyfikowany któryś z obiektów w domenie, zmiana ta zostanie replikowana pomiędzy wszystkimi kontrolerami w domenie. Niektóre zmiany, np. dotyczące schematu są replikowane pomiędzy wszystkimi domenami w lesie. Taki typ replikacji nazywamy **multimaster replication**. Jeśli w jednym czasie na dwóch kontrolerach w domenie zostanie zmodyfikowany ten sam atrybut tego samego obiektu może występie konflikt replikacji. Aby temu zapobiec używamy

single master replication, mechanizmu polegającego na wyznaczeniu jednego kontrolera domeny odpowiedzialnego za przeprowadzanie pewnych szczególnie wrażliwych modyfikacji w katalogu. Dzięki temu nie ma możliwości by zmiany te nastąpiły w jednym czasie w różnych miejscach w sieci. Active Directory używa **single master replication** do ważnych zmian takich jak dodanie nowej domeny lub zmiany schematu.

Operacje używające **single master replication** są łączone razem w specyficzne role w lesie lub w domenie. Role te są nazywane operations master roles. Dla każdej z nich tylko jeden kontroler domeny, który jest odpowiedzialny za tę rolę może robić zmiany w katalogu i jest nazywany **operations master** dla danej roli. Active Directory przechowuje informacje o kontrolerach domeny, które są odpowiedzialne za specyficzne role.

Active Directory definiuje pięć **operations master roles**, dwie związane z lasem i trzy z domeną.

Role związane z lasem:

- **Schema master** – kontroluje wszystkie zmiany związane ze schematem, zawierającym główną listę klas obiektów i atrybutów, które można użyć do tworzenia wszystkich obiektów AD takich jak użytkownicy, komputery lub drukarki
- **Domain naming master** – kontroluje dodawanie i usuwanie domen w lesie. W czasie tworzenia nowej domeny, tylko kontroler, który przechowuje tę rolę może dokonać odpowiednich wpisów w **AD**. Chroni przed dodaniem domen o takich samych nazwach.

Istnieje tylko jeden schema master i domain namig master w całym lesie

Role związane z domeną:

- **Primary domain controller emulator** (**PDC**) – pracuje jako **Microsoft Windows NT primary domain controller** wspierając kontrolery zapasowe (**BDC**) z systemem Windows NT. Zarządza zmianami haseł dla komputerów z systemem Windows NT, Windows 95 lub Windows 98. Minimalizuje opóźnienia replikacji związane ze zmianą hasła - kiedy klient z systemem Windows 2000 lub późniejszym zmienia hasło na kontrolerze domeny, jest ono natychmiast przesyłane do serwera posiadającego rolę emulatora PDC. Jest źródłem czasu dla wszystkich kontrolerów w domenie.
- **Relative identifier master** (**RID**) - kontroler domeny, który przydziela blok RID-ów dla każdego kontrolera w domenie. Kiedy kontroler w domenie tworzy nowy podmiot zabezpieczeń (np. konto użytkownika, grupę, komputer), przypisuje do obiektu unikalny identyfikator (SID). Składa się on z identyfikatora domeny, który jest taki sam dla każdego obiektu tworzonego w tej domenie i RID-u, który jest unikalny w danej domenie.
- **Infrastructure master** – kiedy obiekt jest przenoszony z jednej domeny do innej, **infrastructure master** uaktualnia obiekt odniesienia znajdujący się w domenie pierwotnej wskazujący na obiekt w nowej domenie. Obiekt odniesienia zawiera globalny unikalny identyfikator (**GUID**), nazwę wyróżniającą i **SID**.

Nazwa wyróżniająca i względna nazwa wyróżniająca

Komputery klienckie używają **Lightweight Directory Access Protocol** (**LDAP**) do przeszukiwania i modyfikowania obiektów w bazie **Active Directory**.

- Nazwa wyróżniająca - **LDAP** używa nazwy reprezentującej obiekt w **AD**, jako serię komponentów powiązanych z logiczną strukturą. Identyfikuje domenę, w której obiekt się znajduje i kompletną ścieżkę, pod którą jest osiągalny. Nazwa wyróżniająca musi być unikalna w całym lesie.
- Względna nazwa wyróżniająca – nazwa unikalnie identyfikująca obiekt w kontenerze, w którym się znajduje. Nie może być dwóch obiektów o takiej samej nazwie w jednym kontenerze.

Np. dla użytkownika Jan Kowalski znajdującego się w jednostce organizacyjnej Logistyka w domenie nwtraders.msft, każdy z elementów logicznej struktury jest reprezentowany przez następującą nazwę wyróżniającą:

```
CN=Jan Kowalski,OU=Logistyka,DC=nwtraders,dc=msft
```

- CN - nazwa ogólna (ang. common name) obiektu w kontenerze
- OU – jednostka organizacyjna (ang. organizational unit) zawierająca obiekt. Jeśli obiekt znajduje się w zagnieżdżonych jednostkach to może być więcej wartości OU.
- DC – komponent domeny (ang. domain komponent) taki jak „com", „edu" czy „msft". Zawsze są przynajmniej dwa komponenty domeny, chyba, że domena jest domena podrzędną.

Narzędzia do zarządzania obiektami Active Directory

Microsoft Windows Server 2008 udostępnia kilka narzędzi, przy pomocy których można tworzyć, modyfikować i usuwać obiekty w AD:

- **Active Directory Users and Computers** – Przystawka do konsoli MMC do zarządzania jednostkami organizacyjnymi, użytkownikami u grupami.
- Narzędzia wiersza poleceń usług katalogowych – Zbiór narzędzi (Dsadd,Dsmod,Dsrm) które w użyciu z parametrami pozwalają tworzyć, modyfikować i usuwać obiekty. Wygodne do użycia w skryptach.
- **Lightweight Directory Access Protocol Data Interchange Format Directory Exchange** (**Ldifde**) – narzędzie wiersza poleceń do zarządzania obiektami. Używa pliku wejściowego zawierającego informacje o obiekcie i akcji, jakiej należy na nim wykonac. Informacje te są przechowywane, jako serie rekordów oddzielonych pustymi liniami.
- **Windows Script Host** – można tworzyć obiekty używając aplikacji Windows lub skryptów Windows korzystając z komponentów udostępnianych przez **Active Directory Service Interface** (**ADSI**).

Jednostki organizacyjne

Szczególnie użytecznymi obiektami w **AD** są jednostki organizacyjne. Są to kontenery, w których mogą się znajdować użytkownicy, grupy, komputery, inne jednostki organizacyjne, a także opublikowane w usłudze **AD** zasoby plikowe i drukarki. Jednostki organizacyjne są najmniejszymi elementami, do których można przypisać zasady grup (**GPO**) lub delegować kontrolę administratorską. Wykorzystując je, można tworzyć kontenery w domenie reprezentujące hierarchiczną, logiczną strukturę organizacji. Zagnieżdżając jednostki organizacyjne w innych można modelować strukturę firmy minimalizując liczbę domen wymaganych w sieci.

Delegowanie kontroli do jednostek organizacyjnych

Delegowanie kontroli administracyjnej do jednostek organizacyjnych umożliwia przypisanie użytkownikom lub grupom uprawnień do zarządzania określonymi obiektami w usłudze Active Directory. Dzięki temu można ograniczyć grupę administratorów posiadających uprawnienia do całej struktury **AD** dając im możliwość zarządzania tylko jej pewną częścią, a także pozwala przydzielić podstawowe zadania administracyjne zwykłym użytkownikom (np. resetowanie haseł). Kontrolę administracyjną można delegować na trzy sposoby:

- Delegowanie uprawnień do zarządzania całym kontenerem, a co za tym idzie wszystkimi znajdującymi się w nim obiektami
- Delegowanie uprawnień do zarządzania (tworzenie, modyfikowanie, usuwanie) obiektami danego typu (użytkownicy, komputery, grupy)
- Delegowanie uprawnień do modyfikowania określonych atrybutów wybranych obiektów, np. zmiana hasła użytkowników

Kontrolę najwygodniej można delegować korzystając z kreatora delegowanie kontroli **Delegation of Control Wizard** dostępnego w konsoli **Active Directory Users and Computers**.

Aby go uruchomić, należy wybrać z menu kontekstowego otworzonego na wybranej jednostce organizacyjnej polecenie **Delegate Control**. Zostanie uruchomiony **Wizard**, w którym należy wskazać użytkownika lub grupę, dla której wykonujemy akcję, wybrać z listy zadanie, jakie pozwolimy wykonywać i określić, czy będzie to dotyczyło wszystkich obiektów w jednostce czy tylko wybranych. Dodatkowe, specjalne uprawnienia niedostępne w kreatorze należy nadać bezpośrednio na obiekcie.

Podsumowanie

W tym rozdziale przedstawiona została usługa **Active Directory**. Omówiono jej budowę fizyczną i logiczną a także wyjaśniono pojecie master operations. Przedstawiono specyficzne obiekty, jakimi są jednostki organizacyjne oraz omówiono delegowanie kontroli administracyjnej do części struktury **AD**.

Porady praktyczne

- W jednostkach organizacyjnych nie mogą znajdować się obiekty z innych domen
- Chcąc skorzystać z delegowania kontroli administracyjnej należy być członkiem grupy **Account Operators**, **Domain Admins**, lub **Enterprise Admins**.

Uwagi dla studenta

Jesteś przygotowany do realizacji laboratorium jeśli:

- rozumiesz, dlaczego stosuje się usługi katalogowe
- umiesz zarządzać jednostkami organizacyjnymi
- potrafisz delegować kontrolę administracyjną
- wiesz, jaka jest fizyczna i logiczna struktura AD

Pamiętaj o zapoznaniu się z uwagami i poradami zawartymi w tym module. Upewnij się, że rozumiesz omawiane w nich zagadnienia. Jeśli masz trudności ze zrozumieniem tematu zawartego w uwagach, przeczytaj ponownie informacje z tego rozdziału i zajrzyj do notatek z wykładów.

Dodatkowe źródła informacji

1. Rand Morimoto, Michael Noel, Omar Droubi, Ross Mistry, Chris Amaris, *Windows Server 2008 PL. Księga Experta.*, Helion, 2009

   W części 2 zostały omówione zagadnienia związane z usługą Active Directory takie jak projektowanie usługi katalogowej, projektowanie struktury jednostek organizacyjnych i grup, infrastruktura Active Directory

2. Wiliam R.Stanek, *Microsoft Windows Server 2008. Vedemecum administratora*, Microsoft Press, 2008

   Książka wielokrotnie nagradzanego autora wielu podręczników serii „Vedemecum administratora". Wiliam R. Stanek ma za sobą ponad 20 lat owocnych wdrożeń i jest posiadaczem tytułu Microsoft Most Valuable Professional. W przewodniku znajdują się między innymi informacje na temat instalacji Windows Server 2008, wykonywania uaktualnienia i wykonywania dodatkowych zadań administracyjnych podczas instalacji. Informacje dotyczące tego modułu znajdują się w rozdziale drugim.

Laboratorium podstawowe

Problem 1 (czas realizacji 25 min)

Jesteś administratorem w przedsiębiorstwie. Twoja firma rozwija się i przygotowuje się do otworzenia nowego oddziału w kolejnym mieście. Chcesz stworzyć testową strukturę jednostek organizacyjnych dla tej lokalizacji. Wiesz, że będą tam trzy działy. Dwa z nich, IT i Finanse będą kilkuosobowe, natomiast w dziale logistyki będzie pracowało kilkadziesiąt osób. Projektujesz strukturę (Rys. 1) i wdrażasz w swoim środowisku.

Rys. 1 Projekt struktury jednostek organizacyjnych

Zadanie	Tok postępowania
1. Uruchom maszynę wirtualną	• Uruchom maszynę wirtualną **2008 Templ**.
2. Zaloguj się na konto zwykłego użytkownika	• Naciśnij na klawiaturze **Prawy Alt+Delete**. • Naciśnij przycisk **Switch User**. • Naciśnij przycisk **Other User**. • W polu **User Name** wpisz **NazwakomputeraUser**. • W polu **Password** wpisz **P@ssw0rd** i naciśnij Enter.
3. Uruchomienie programu **Active Directory Users and Computers**	• Wybierz **Start** -> **Administrative Tools -> Active Directory Users and Computers**. • Zapoznanie się ze strukturą domeny **nwtraders.msft**.

4. Stworzenie jednostki organizacyjnej przy pomocy polecenia **Dsadd**	• Wybierz **Start** i w polu **Start Search** wpisz:
	`runas /user:NazwakomputeraAdmin@nwtraders.msft cmd`
	• W oknie **C:\Windows\System32\runas.exe** wpisz hasło **P@ssw0rd**.
	• W oknie wiersza poleceń wpisz:
	`dsadd ou ou=OUNazwakomputera,ou="IT Test",dc=nwtraders,dc=msft`
	• W oknie narzędzia **Active Directory Users and Computers** odśwież widok i sprawdź czy jednostka organizacyjna została stworzona.

5. Stworzenie jednostek organizacyjnych przy pomocy narzędzia **Ldifde**	• Na dysku **Dane (E:)** stwórz folder **Tools**.
	• Otwórz notatnik i wpisz poniższy przykład:
	`dn: ou=IT,ou=OUNazwakomputera,ou="IT Test",DC=nwtraders,DC=msft`
	`changetype: add`
	`objectClass: organizationalUnit`
	
	`dn: ou=Finance,ou=OUNazwakomputera,ou="IT Test",DC=nwtraders,DC=msft`

	changetype: add objectClass: organizationalUnit dn: ou=Logistic,ou=OUNazwakomputera,ou="IT Test",DC=nwtraders,DC=msft changetype: add objectClass: organizationalUnit • Zapisz plik w lokalizacji **E:\Tools** jako **import.ldf**. • W oknie wiersza poleceń wpisz: Ldifde –i –k –f D:\Tooles\import.ldf • W oknie narzędzia **Active Directory Users and Computers** odśwież widok i sprawdź czy jednostki organizacyjne zostały stworzone.
6. Stworzenie jednostek organizacyjnych przy pomocy **Windows Script Host**	• Otwórz notatnik i wpisz poniższy przykład: Set objDom = GetObject("LDAP://ou=Logistic,ou=OUNazwakomputera,ou=It Test,dc=nwtraders,dc=msft") Set objOU = objDom.Create("OrganizationalUnit","ou=Managers") objOU.SetInfo Set objDom = GetObject("LDAP://ou=Logistic,ou=OUNazwakomputera,ou=It Test,dc=nwtraders,dc=msft") Set objOU = objDom.Create("OrganizationalUnit","ou=Personel") objOU.SetInfo • Zapisz plik w lokalizacji **E:\Tools** jako **ouadd.vbs**. • W oknie wiersza poleceń wpisz: wscript C:\ouadd.vbs • W oknie narzędzia **Active Directory Users and Computers** odśwież widok i sprawdź, czy jednostki organizacyjne zostały stworzone. • Wyloguj się.

Problem 2 (czas realizacji 15 min)

Stworzyłeś testową strukturę jednostek organizacyjnych. Okazało się, że są potrzebne pewne modyfikacje, ponieważ struktura twojej firmy zmieniła się. Postanawiasz zmodyfikować testową strukturę tak, by odpowiadała ona Twoim potrzebom. W jednostce *OUNazwakomputera* chcesz wypełnić pole opisu. Dział Finanse nie przeniesie się do tej lokalizacji, dlatego musisz usunąć tą jednostkę organizacyjną. Dział IT zostanie przeniesiony do innej lokalizacji.

W lokalizacji tej posiadasz jednego zaawansowanego użytkownika i chcesz dać mu prawa do wykonywania pewnych czynności administracyjnych. Między innymi chcesz, by mógł resetować hasła użytkownikom, którzy je zapomnieli oraz tworzyć konta komputerów.

Zadanie	**Tok postępowania**
1. Uruchom maszynę wirtualną	• Uruchom maszynę wirtualną **2008 Templ**.

2. Zaloguj się na konto zwykłego użytkownika	• Naciśnij na klawiaturze **Prawy Alt+Delete**. • Naciśnij przycisk **Switch User**. • Naciśnij przycisk **Other User**. • W polu **User Name** wpisz **NazwakomputeraUser**. • W polu **Password** wpisz **P@ssw0rd** i naciśnij Enter.

3. Modyfikacja jednostki organizacyjnej OUNazwakomputera	• Wybierz **Start** i w polu **Start Search** wpisz:
	`runas /user:NazwakomputeraAdmin@nwtraders.msft cmd`
	• W oknie **C:\Windows\System32\runas.exe** wpisz hasło **P@ssw0rd**.
	• W oknie wiersza poleceń wpisz:
	`Dsmod ou ou=OUNazwakomputera,ou="IT Test",dc=nwtraders,dc=msft –desc "Nowy oddzial - testy"`
	• Wybierz **Start** -> **Administrative Tools** -> **Active Directory Users and Computers**.
	• W oknie narzędzia **Active Directory Users and Computers** odśwież widok i sprawdź czy jednostka organizacyjna **OUNazwakomputera** została zmodyfikowana.

4. Usunięcie jednostki organizacyjnej przy pomocy polecenia Dsrm	• W oknie wiersza poleceń wpisz: `Dsrm ou=Finance,ou=OUNazwakomputera,ou="IT Test", dc=nwtraders,dc=msft` • Na pytanie, czy na pewno chcesz usunąć obiekt, odpowiedz twierdząco wybierając **Y**. • W oknie narzędzia Active **Directory Users and Computers** odśwież widok i sprawdź czy jednostka organizacyjna **Finance** została usunięta.
5. Przenoszenie jednostki	• Wybierz menu **Start** -> **Administrative Tools** i naciśnij prawy przycisk na **Active Directory Users and Computers**. • Z menu kontekstowego wybierz **Run as Administrator**. • W oknie **User Account Control** w polu **User name** wpisz **NazwakomputeraAdmin**, w polu **Password** wpisz **P@ssw0rd i** naciśnij **OK**. • W oknie narzędzia **Active Directory Users and Computers** znajdź obiekt **ou=IT,ou=OUNazwakomputera,ou=”IT Test”,dc=nwtraders,dc=msft**. • Naciśnij na nim prawy przycisk myszy i z menu kontekstowego wybierz **Move**. • W oknie **Move** rozwiń **nwtraders** -> **Locations**, zaznacz jednostkę organizacyjną odpowiadającą nazwie Twojego komputera i naciśnij **OK**. • W oknie narzędzia Active **Directory Users and Computers** odśwież widok i sprawdź czy jednostka organizacyjna **IT** została przeniesiona.
6. Delegowanie kontroli do jednostki - zarządzanie hasłami użytkowników	• W konsoli **Active Directory Users and Computers** znajdź obiekt **ou=Personel,ou=Logistic,ou=OUNazwakomputera,ou="IT Test",dc=nwtraders,dc=msft**, kliknij na nim prawy przycisk myszy i wybierz **Delegate Control**. • W oknie **Welcome to the Delegation of Control Wizard** wybierz **Next**. • W oknie **Users and Groups** naciśnij przycisk **Add**. • W oknie **Select Users, Computers, or Groups** wpisz **NazwakomputeraUser**, a następnie wybierz **OK**. • Naciśnij przycisk **Next**. • W oknie **Task to Delegate** wybierz:

	– **Reset user passwords and force password change at next logon** – **Read all user information** • Wybierz **Next**, a następnie **Finish**.
7. Delegowanie kontroli do jednostki – zarządzanie kontami komputerów	• W konsoli **Active Directory Users and Computers** znajdź obiekt **ou=Logistic,ou=OUNazwakomputera,ou="IT Test",dc=nwtraders,dc=msft**, kliknij na nim prawy przycisk myszy i wybierz **Delegate Control**. • W oknie **Welcome to the Delegation of Control Wizard** wybierz **Next**. • W oknie **Users and Groups** naciśnij przycisk **Add**. • W oknie **Select Users, Computers, or Groups** wpisz **NazwakomputeraUser**, a następnie wybierz **OK**. • Naciśnij przycisk **Next**. • W oknie **Task to Delegate** zaznacz **Create a custom task to delegate** i naciśnij **Next**. • W oknie **Active Directory Object Type** zaznacz **Only the following object in the folder**, na liście zaznacz **Computer object**. • Pod listą zaznacz: – **Create selected object in the folder** – **Delete selected object in the folder** • Wybierz **Next**. • W oknie **Permission** na liscie zaznacz **Read, Write**. • Wybierz **Next**, a następnie **Finish**. • Wyloguj się

Laboratorium rozszerzone