**Ćwiczenie 3 - Dodawanie obiektów w domenie**

**Cel:**

W ramach tematu wykonasz podstawowe czynności administracyjne z zakresu zarządzania domeną w zakresie dodawania, usuwania oraz modyfikowania obiektów dla przyszłego zarządzania dostępem do zasobów.

**Wstęp teoretyczny:**

W domenie przechowywane są obiekty administracyjne pozwalające organizować i zarządzać dostępem do zasobów jak: foldery, pliki, drukarki, aplikacje czy ustawienia systemowe. W tym zakresie kluczowe obiekty to:

* Jednostki organizacyjne – pozwalające grupować konta użytkowników czy grupy. Pełnią rolę analogiczną do folderów, gdzie nikt nie przechowuje wszystkich plików w tym samym folderze dla chociażby łatwości wyszukiwania. Ponadto jednostki organizacyjne pozwalają zbiorczo wykonywać czynności administracyjne, np. usunąć dostęp do panelu sterowania dla wszystkich komputerów, które znajdują się w jednostce o nazwie Sopot.
* Konta użytkowników – są wymagane dla dostępu do zasobów w domenie typu aplikacje czy foldery. Użytkownik nie ma możliwości skorzystania z żadnego z komputerów, jeśli nie posiada konta domenowego.
* Konta komputerów – są wymagane dla dostępu do zasobów w domenie. Nawet jeśli użytkownik posiada konto domenowe, to dostęp do zasobów jest możliwy wyłącznie z komputera, który posiada konto domenowe, czyt. został dołączony do domeny.
* Grupy – pozwalają na zbiorcze przypisanie uprawnień. Jeśli do 100 folderów 100 użytkowników wymagałoby dostępu, konieczne jest wykonanie 10000 operacji (na każdym folderze 100 dodań użytkowników). Dzięki zdefiniowaniu grupy liczba operacji spada do 200 - 100 operacji dodania kont użytkowników do grupy plus 100 operacji przypisania grupy do folderów (zaledwie jedna operacja per folder). Istnieje szereg predefiniowanych grup systemowych, jak np. administrators.

**Zadanie 1**: Utwórz jednostkę organizacyjną o nazwie Polska, a w niej dwie jednostki organizacyjne o nazwach Gdansk i Gdynia.

**Sposób wykonania**:

* Dodanie jednostki organizacyjnej – konsola Active Directory Users and Computers -> na nazwie domeny/jednostki organizacyjnej operacja New i jako typ obiektu Organizational Unit -> podanie nazwy jednostki

**Szczegółowy tutorial:**

1. Przejdź do menadżera serwera – ikona Server Manager w lewym dolnym rogu pulpitu.
2. Po lewej stronie zaznacz usługę AD DS i następnie po wyborze w centralnej części serwera (kontroler) kliknij prawym przyciskiem myszki na nazwie serwera i wybierz operację Active Directory Users and Computers.
Alternatywnie możesz wybrać tą samą operację z menu Tools w prawym górnym rogu.
3. Otworzy się konsola zarządzania użytkownikami i komputerami. W tym oknie kliknij prawym klawiszem myszki, na wcześniej utworzoną domenę (zsl.pl) i z menu kontekstowego wybierz New a następnie Organizational Unit.
4. Wprowadź nazwę jednostki organizacyjnej (Polska) i zatwierdź OK.
Jednostka została utworzona
5. Zaznacz wcześniej utworzoną jednostkę organizacyjną (Polska) i z menu kontekstowego wybierz New a następnie Organizational Unit. Podaj jako nazwę Gdansk. Analogicznie dodaj jednostkę Gdynia.

**Zadanie 2**: Utwórz w jednostce organizacyjnej Gdansk konto użytkownika o loginie menedzerTwojeInicjały (np. menedzerMP), który nie musi zmieniać hasła przy następnym logowaniu oraz o niewygasającym haśle. Jako hasło podaj P@$$w0rd, a jako imię i nazwisko swoje dane. We właściwościach konta ustaw adres użytkownika jako: Sopot, Pomorskie. Następnie zresetuj hasło konta na zaq1@WSX i zablokuj konto. Na podstawie konta menedzerTwojeInicjały utwórz kolejne w tej samej jednostce organizacyjnej o nazwie pracownikTwojeInicjały oraz analitykTwojeInicjały.

Utwórz w jednostce organizacyjnej Gdynia konto użytkownika o loginie janKowalski, które nie musi zmieniać hasła przy następnym logowaniu oraz o niewygasającym haśle. Jako hasło podaj zaq1@WSX. Utwórz w jednostce organizacyjnej Gdynia konto użytkownika o loginie andrzejNowak, z domyślnymi wartościami – jakie to są? Jako hasło podaj 12345678, czy hasło zostało zaakceptowane? Jeśli nie jako hasło podaj zaq1@WSX.

Zaloguj się na utworzone konto menedzerTwojeInicjały na komputerze klienta. Czy jest to możliwe? Usuń blokadę konta, czy teraz jest to możliwe? Wyloguj się i zaloguj na konto andrzejNowak, co musiałeś w tym celu zrobić?

**Sposób wykonania**:

* Zarządzanie kontami - konsola Active Directory Users and Computers
* Dodanie konta użytkownika - na nazwie domeny/jednostki organizacyjnej/kontenera operacja New -> typ obiektu User
* Konieczność zmiany hasła przy pierwszym logowaniu – zaznaczenie opcji User must change password at next logon
* Brak wygasania hasła – zaznaczenie opcji User cannot change password
* Resetowanie, blokowanie konta, tworzenie na podstawie konta kolejnych - odpowiednie operacje są dostępne pod prawym przyciskiem myszki dla zaznaczonego konta

**Szczegółowy tutorial:**

1. Uruchom obie maszyny wirtualne jeśli nie są one uruchomione.
2. W maszynie serwera w konsoli Active Directory Users and Computers (ADUAC) zaznacz jednostkę organizacyjną Gdansk i poprzez prawy przycisk myszki wybierz New -> User.
3. Podaj dane konta: imię i nazwisko oraz menedzerTwojeInicjały.
4. Kliknij na przycisk Next i podaj hasło (P@$$w0rd).
5. Odznacz opcję User must change… - w ten sposób użytkownik nie będzie musiał zmieniać hasła przy pierwszym logowaniu.
6. Zaznacz opcję Password never expires – w ten sposób użytkownik nie będzie musiał co pewien czas zmieniać hasła (domyślnie co 42 dni).
7. Kliknij na Next, a potem Finish.

Dodałeś konto użytkownika.

1. Zaznacz konto i wybierz operację Properties. Przejrzyj zawartość poszczególnych zakładek. Na zakładce Address ustaw dane: Sopot, Pomorskie.
2. Zaznacz konto menedzerTwojeInicjały i wybierz operację poprzez prawy przycisk myszy Reset password. Ustaw nowe hasło jako zaq1@WSX.
3. Zaznacz konto i wybierz operację Disable account.
4. Analogicznie dodaj pozostałe 4 konta. Możesz zastosować do tego celu operacje Copy na koncie. Jakie elementy są kopiowane, a jakie nie?
5. Przejdź do maszyny wirtualnej klienta i zaloguj się (Jeśli to konieczne uprzednio wyloguj się) na konto menedzerTwojeInicjały z ustawionym hasłem (zaq1@WSX). Jaki jest efekt?
6. W wirtualce serwera w konsoli ADUAC zaznacz konto menedzerTwojeInicjały i wybierz operację Enable account. Ponownie spróbuj zalogować się na konto menedzerTwojeInicjały. Czy teraz jest to możliwe?
7. Wyloguj się i zaloguj na konto andrzejNowak. Wykonaj stosowne wymagane czynności podania nowego hasła.

**Zadanie 3**: W konsoli ADUAC sprawdź zawartość kontenerów Computers i Domain Controlers. Czy nazwy kont, które się tam znajdują coś Ci mówią?

Utwórz konto komputera o nazwie SerwerWWW w jednostce organizacyjnej Gdansk. Ustaw dla konta możliwość dodania komputera przez menedzerTwojeInicjały. Zdefiniuj lokalizację jako Polska/Gdansk. Dodaj analogicznie do jednostki organizacyjnej Gdynia komputer o nazwie SerwerWydruku.

Jak uważasz, jest cel dodania w ten sposób konta, skoro tworzy się ono automatycznie w trakcie dołączania komputera do domeny?

**Sposób wykonania**:

* Zarządzanie kontami komputerów - konsola Active Directory Users and Computers
* Dodanie konta komputera - na nazwie domeny/jednostki organizacyjnej/kontenera operacja New -> typ obiektu Computer - dla bezpieczeństwa można zdefiniować GUID dodawanego komputera

**Szczegółowy tutorial**:

1. W maszynie wirtualnej serwera w konsoli ADUAC na jednostce organizacyjnej Gdansk wykonaj operację New -> Computer podając jako nazwę SerwerWWW.
2. Kliknij na przycisk Change.
3. Wpisz w pole tekstowe wprowadź menedzer i kliknij na przycisk Check names. Nazwa konta zostanie ustalona na podstawie wprowadzonego tekstu.
4. Zatwierdź dane. Konto zostało dodane, ale jako kto?
5. Dodaj pozostałe konto komputera zgodnie z treścią zadania.

**Zadanie 4**: Wyszukaj konto komputera o nazwie klient. Następnie wyszukaj konta użytkowników – menedżerów z Sopotu.

[Opcjonalne] Co należałoby zrobić, aby mieć zapisane zapytanie na stałe jako kwerendę?

**Sposób wykonania**:

* Zarządzanie obiektami - konsola Active Directory Users and Computers
* Wyszukanie obiektu - na nazwie domeny/jednostki organizacyjnej/kontenera operacja Find

-> podanie parametrów wyszukiwania.

**Szczegółowy tutorial:**

1. W konsoli Active Directory Users and Computers, kliknij prawym przyciskiem myszy na nazwie domeny (zsl.pl) wybierz polecenie Find.
2. W oknie wyszukiwania z pola Find wybierz Computers.
3. W polu Computer name wpisz klient i kliknij na przycisk Find now.
4. Przeanalizuj wyniki, dwukrotnie kliknij na wynik wyszukiwania i przejrzyj właściwości komputera.
5. W polu Find wybierz pozycję Users, Contacts, and Groups.
6. Na karcie Advanced kliknij przycisk Field, rozwiń pozycję User i wybierz atrybut City.
7. Upewnij się, czy w polu Condition wybrany jest warunek Starts with.
8. W polu Value wpisz Sopot i kliknij przycisk Add.
9. Analogicznie dodaj warunek dla Logon name dla wyszukania menedżerów.
10. Kliknij na przycisk Find now.

[Opcjonalne] Aby kwerenda była zapisana na stałe należy ją zdefiniować w konsoli ADUAC w sekcji Saved Queries. Zdefiniuj stosowną kwerendę dla wyszukania menedżerów z Sopotu.

**Zadanie 5**: Sprawdź jakie są wbudowane grupy domenowe i lokalne.

**Sposób wykonania:**

* Grupy domenowe – konsola Active Directory Users and Computers \ sekcje Builtin oraz Users
* Grupy lokalne – konsola Computer Management \ sekcja Users and Local Groups

Szczegółowy tutorial:

1. Uruchom obie maszyny wirtualne, jeśli nie są one uruchomione.
2. W maszynie serwera w konsoli Active Directory Users and Computers zobacz zawartość kontenerów Builtin oraz Users . Grupy oznaczone są ikonami 2 osób – są to grupy domenowe, a więc istniejące na poziomie całej domeny. Oznacza, to że jeśli ktoś jest członkiem takiej grupy to ma uprawnienia jej przypisane na każdym komputerze należącym do grupy - np. jeśli należy do grupy Domain administrators, to ma uprawnienia administratora na każdym komputerze. Przeczytaj tekst w kolumnie Description.
3. Będąc w maszynie wirtualnej serwera naciśnij klawisz Windows + Q.
4. Wpisz Computer management (nie musisz wchodzić do żadnego pola) i naciśnij Enter.
5. Wejdź do folderu Local Users and Computers. Czy jest on dostępny? Jeśli nie, dlaczego?
6. W systemie klienta kliknij na przycisk Start -> Mój komputer -> prawy przycisk myszki i operacja Zarządzaj.
7. Rozwiń folder Użytkownicy i grupy lokalne -> Grupy.
8. Zapoznaj się ze zdefiniowanymi grupami.

**Zadanie 6**: Utwórz grupy globalne o nazwie menedzerowieGdansk oraz analitycyGdansk i pracownicyGdansk w jednostce organizacyjnej Gdansk. Utwórz grupę globalną o nazwie menedzerowieGdynia, analitycyGdynia, pracownicyGdynia w jednostce organizacyjnej Gdynia.

W jednostce organizacyjnej Polska utwórz grupę o nazwie pracownicyPolska.

Dodaj stosowne konta użytkowników do jednostek organizacyjnych: menedzerowieGdansk, analitycyGdansk, menedzerowieGdynia (janKowalski), analitycyGdynia (andrzejNowak). Zagnieźdź grupy (ustaw do których grup należą), tak aby odzwierciedlało to strukturę organizacyjną firmy (stanowisko, lokalizacja jako miasto, lokalizacja jako kraj).

Gdzie i na jakich zakładkach sprawdza się:

* do której grupy należy konto użytkownika?
* jacy użytkownicy i konta należą do grupy?

**Sposób wykonania**:

* Zarządzamie grupami - konsola Active Directory Users and Computers
* Dodanie grupy - na nazwie domeny/jednostki organizacyjnej/kontenera operacja New -> typ obiektu Group
* Dodawanie członków do grupy – zakładki Members i Member of

**Szczegółowy tutorial**:

1. W maszynie wirtualnej serwera w konsoli ADUAC w jednostce organizacyjnej Gdansk wykonaj operację New -> Group podając jako nazwę grupy menedzerowieGdansk i wskazując jako typ grupy (Group scope) Global.
Czym się różnią poszczególne typu i zakresy grupy? Jeśli nie jesteś wskazać różnic przeczytaj artykuły:

[http://technet.microsoft.com/pl-pl/library/cc755692(v=ws.10).aspx](http://technet.microsoft.com/pl-pl/library/cc755692%28v%3Dws.10%29.aspx)

[http://technet.microsoft.com/pl-pl/library/cc781446(v=ws.10).aspx](http://technet.microsoft.com/pl-pl/library/cc781446%28v%3Dws.10%29.aspx)

1. Zatwierdź OK.
2. Dodaj analogicznie pozostałe grupy: analitycyGdansk, pracownicyGdansk w jednostce organizacyjnej Gdansk; menedzerowieGdynia, analitycyGdynia, pracownicyGdynia w jednostce organizacyjnej Gdynia; pracownicyPolska w jednostce organizacyjnej Polska.
3. Wejdź we właściwości grupy menedzerowieGdansk dwukrotnie klikając na niej.
4. Na zakładce Members, służącej ustalaniu członków grupy (analogicznie jak studentów, którzy należą do grupy dziekańskiej) kliknij na przycisk Add.
5. Aby wskazać konto, które należy do grupy konieczne jest podanie początku nazwy i kliknięcie na przycisk Check Names lub kliknięcie na przycisk Advanced -> następnie przycisk Find now. Wykonaj tą drugą wersję. Zaznacz konto menedżera z Gdańska - powinno to być konto o Twoim imieniu i nazwisku. Zauważ, że możliwe jest zaznaczenie kilku kont na raz.
6. Kliknij na OK -> OK.

Zdefiniowałeś członków grupy menedzerowieGdansk.

1. Analogicznie dodaj odpowiednie konta do grup: analitycyGdansk, menedzerowieGdynia (janKowalski), analitycyGdynia (andrzejNowak).
2. Wejdź we właściwości jednostki organizacyjnej pracownicyGdansk dwukrotnie klikając na niej.
3. Na zakładce Members, służącej ustalaniu członków grupy kliknij na przycisk Add.
4. Kliknij na przycisk Advanced -> następnie przycisk Find now.
5. Zaznacz grupy menedzerowieGdansk i analitycyGdansk.
6. Kliknij na OK -> OK.

Zdefiniowałeś członków grupy pracownicyGdansk jako 2 podgrupy: menedzerowieGdansk i analitycyGdansk. W związku, z tym konta użytkowników należące do grup menedzerowieGdansk i analitycyGdansk, pośrednio należą również do grupy pracowników.

1. Wykonaj analogiczne czynności zagnieżdżania grup dla pozostałych grup zgodnie z treścią zadania. Efekt powinien być zgodny z poniższym. 
2. Wejdź we właściwości konta menedzerTwojeInicjały. To do jakich grup należy to konto zawarte jest na zakładce Member Of.
3. Wejdź we właściwości grupy **menedzerowieGdansk**. To do jakich grup należy grupa zawarte jest na zakładce **Member Of.** To jakie konta należą do grupy zawarte jest na zakładce **Members**.

**Zadanie 7**: Wszystkimi czynnościami administracyjnymi nie może zajmować się administrator, który ponadto za każdym razem kiedy zgłosi się do niego użytkownik twierdzący, że jest menedżerem musi to każdorazowo weryfikować u kierownika działu (może pracownik podaje nieprawdziwe dane bo np. chce uzyskać dostęp do folderu z danymi o wynagrodzeniach). W związku z tym przydziel menedżera do grupy menedzerowieGdansk jako konto użytkownika menedzerTwojeInicjały. Sprawdź czy użytkownik menedzerTwojeInicjały może dodać do grupy menedzerowieGdansk użytkownika o nazwie andrzejNowak.

**Sposób wykonania**:

* Zarządzanie grupami - konsola Active Directory Users and Computers
* Określenie menadżera grupy – właściwości grupy, zakładka Managed By. Jeśli menadżer ma mieć prawo modyfikowania członkostwa w grupie należy zaznaczyć pole Manager can update membership list.

**Szczegółowy tutorial**:

1. W maszynie wirtualnej serwera przeloguj się na konto menedzerTwojeInicjały.
2. Pojawi się komunikat The sign in … is not allowed. Wynika to z tego, że bezpośrednio na kontrolerze mogą zalogować się wyłącznie członkowie grup administracyjnych. W związku z tym zmienisz odpowiednie ustawienia w polisach bezpieczeństwa.
3. Zaloguj się ponownie jako admnistrator.
4. W ServerManager wybierz w menu Tools konsole Group Policy Management
5. W drzewie polis znajdź polisę Default Domain Controler Policy, która jest zlokalizowana zgodnie z rys. poniżej. 
	1. Dla polisy wybierz operację Edit. 
6. Znajdź uprawnienie Allow log on localy, zgodnie z rys. poniżej. 

UPRAWNIENIE LOGOWANIA LOKALNEGO WSKAZUJE KTO MA PRAWO LOGOWAĆ SIĘ DO DOMENY BEZPOŚREDNIO Z KONTROLERÓW DOMENY.

1. Wybierz operację Properties -> przycisk Add user or group -> przycisk Browse -> przycisk Advanced -> przycisk Find now.
2. Wskaż Authenticated Users. Oznacza to, że każdy użytkownik, który posiada konto może się logować do domeny bezpośrednio korzystając z komputera, który jest kontrolerem domeny.
3. Kliknij na OK -> OK.
4. Zamknij konsolę.
5. Ustawienia są wdrażane co kilkadziesiąt minut. Wymuś ich wdrożenie wchodząc do konsoli Command Prompt (Windows + D -> cmd -> enter) i wprowadzając polecenie gpupdate / force.
6. W maszynie wirtualnej serwera przeloguj się na konto menedzerTwojeInicjały. Teraz powinno to być możliwe.
7. W konsoli ADUAC w jednostce organizacyjnej Gdansk wejdź we właściwości grupy organizacyjnej menedzerowieGdansk dwukrotnie klikając na niej.
8. Na zakładce Members, służącej ustalaniu członków grupy kliknij na przycisk Add.
9. Aby wskazać konto, które należy do grupy konieczne jest podanie początku nazwy i kliknięcie na przycisk Check Names lub kliknięcie na przycisk Advanced -> następnie przycisk Find now. Wykonaj tą drugą wersję. Zaznacz konto analitykTwojeInicjały.
10. Kliknij na OK -> OK. Czy udało się dodać konto użytkownika do grupy?
11. W maszynie wirtualnej serwera przeloguj się na konto administratora.
12. W konsoli ADUAC w jednostce organizacyjnej Gdansk wejdź we właściwości grupy organizacyjnej menedzerowieGdansk dwukrotnie klikając na niej.
13. Na zakładce Managed by, kliknij na przycisk Change.
14. Aby wskazać konto, które należy do grupy konieczne jest podanie początku nazwy i kliknięcie na przycisk Check Names kliknięcie na przycisk Advanced -> następnie przycisk Find now. Wykonaj tą drugą wersję. Zaznacz konto menedżera dla Gdańska (menedzerTwojeInicjały)
15. Kliknij na **OK -> OK**.
16. Zaznacz pole **Manager can update membership list**.
Zdefiniowałeś menedżera grupy. Co by powodowały ustawienia jeśli nie zaznaczyłbyś tego pola? Jeśli tego nie wiesz sprawdź to po zakończeniu zadania empirycznie.
17. W maszynie wirtualnej serwera przeloguj się na konto menedzerTwojeInicjały.
18. W konsoli ADUAC w jednostce organizacyjnej Gdansk wejdź we właściwości grupy organizacyjnej menedzerowieGdansk dwukrotnie klikając na niej.
19. Na zakładce Members, służącej ustalaniu członków grupy (analogicznie jak studentów, którzy należą do grupy dziekańskiej) kliknij na przycisk Add.
20. Aby wskazać konto, które należy do grupy konieczne jest podanie początku nazwy i kliknięcie na przycisk Check Names lub kliknięcie na przycisk Advanced -> następnie przycisk Find now. Wykonaj tą drugą wersję. Zaznacz konto analitykTwojeInicjały.
21. Kliknij na OK -> OK.
Czy udało się dodać konto użytkownika do grupy?

[Opcjonalne] **Zadanie 8**: Otwórz konsolę Active Directory Administrative Center i za jej pomocą dodaj jednostkę organizacyjną o nazwie Temp, a w niej dowolne konto: użytkownika, grupy, komputera. Zresetuj hasło dla konta użytkownika. Czy ta konsola jest wygodniejsza od ADUAC?

**Sposób wykonania**:

* Wykonywanie najczęstszych czynności - konsola Active Directory Administrative Center