Ćwiczenie 3: Wdrażanie usługi katalogowej cd..

Scenariusz

Zostałeś zatrudniony w firmie KEJA CORP zajmującej się produkcją morskich jachtów żaglowych. Firma zaimplementowała usługę katalogową Active Directory. Nazwa domeny **AD** to **keja.msft**. Kierownik działu **IT** zlecił Ci następujące zdania do wykonania.

Struktura organizacyjna Firmy

- Firma posiada następujące działy organizacyjne:
  - **HR**
  - **IT**
  - **Sales**
  - **Marketing**
  - **Finance**
  - **Logistics**
- Centrala firmy mieści się w
  - **Opolu (OP)**,
- oddziały firmy mieszczą się w:
  - **Katowicach (KAT)**
  - **Wrocławiu (WR)**
  - **Szczecinie(SZ)**
  - **Gdańsku (GD)**

Zadanie 1

1. **Utwórz brakujące jednostki organizacyjne** zgodnie z już istniejącym schematem oraz zgodnie z działami organizacyjnymi firmy. Szef działu INFORMATYKI podjął decyzję że serwery działające w firmie powinny być podobnie jak desktopy w jednostkach organizacyjnych wskazujących na ich geograficzną lokalizację. Np. jeżeli serwer **SVR1** znajduje się w Opolu to powinien być w jednostce: *OU=OP,OU=Servers,OU=KejaMain,DC=keja,DC=msft*

2. **Konta i grupy użytkowników**.

   Utwórz konta użytkowników, a następnie istniejące konta jak i nowo utworzone umieść we właściwych jednostkach organizacyjnych oraz we właściwych grupach globalnych.

   a. Jesteś pracownikiem działu „IT" i twoje konto powinno zostać umieszczone we właściwej jednostce organizacyjnej i przynależeć do odpowiedniej grupy.

   b. Użytkownicy **I*za, Ania*** są pracownikami działu **Logistics.**

   c. Użytkownicy **Asia**, **Tomasz**, **Agnieszka** są pracownikami działu **Finance**.

   d. Użytkownik **Andrzej** jest pracownikiem **HR**.

   e. Użytkownik **Marzena** jest pracownikiem **Sales**

   f. Użytkownik **Renata** jest pracownikiem **Marketing**

3. **Konta komputerów klienckich** i **serwerów**

   Konta komputerów klienckich i serwerów powinny być umieszczone w odpowiednich jednostkach organizacyjnych zgodnie z ich fizyczną lokalizacją. Sprawdź i ewentualnie skoryguje umieszczenie kont komputerów w odpowiednich **OU**. Jeżeli istnieje konieczność utwórz odpowiednie **OU** oraz odpowiednie **konta komputerów**.

a. Komputer kliencki **CL01** znajduje się w **Centrali** firmy.
b. Komputer kliencki **CL02** znajduje się w oddziale we Wrocławiu.
c. Komputer kliencki **CL03** znajduje się w oddziale we Katowicach.
d. Komputer kliencki **CL04** znajduje się w oddziale we Szczecinie.
e. Komputer kliencki **CL05** znajduje się w oddziale we Gdańsku.
f. Serwer **SVR1**, znajduje się w **Centrali** firmy.
g. Serwer **SVR2** znajduje się w oddziale we Wrocławiu.
h. Serwer **SVR3** znajduje się w oddziale w Katowicach.
i. Serwer **SVR4** znajduje się w oddziale w Szczecinie.
j. Serwer **SVR5** znajduje się w oddziale w Gdańsku.

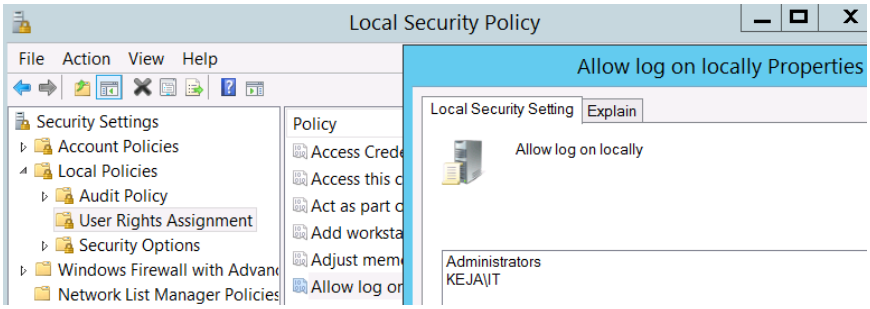
Zadanie 2

Scenariusz

Kontynuujesz pracę jako administrator w firmie „KEJA Corp". Do wykonania masz kilka czynności administracyjnych w domenie.

1. Administrowanie serwerem SVR1

a. Do konsoli serwera SVR1 mogą logować się jedynie członkowie grupy lokalnych administratorów oraz pracownicy działu IT. (SVR1->Server Manager->Tools->Local Security Policy -> rys 1.)



Rys.1.

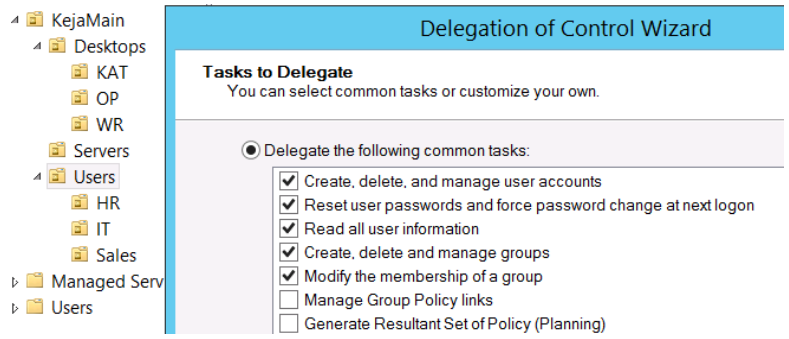
b. Jedynie członkowie grupy lokalnych administratorów oraz pracownicy działu **IT** mogą wyłączać serwer **SVR1**.
c. Pracownicy działu IT powinni mieć prawo do zdalnego i lokalnego administrowania serwerem SVR1. Zezwól grupie IT na zdalne łączenie się przez RDP (Remote desktop)
a. Na serverze SVR1 zainstaluj narzędzia do zdalnej administracji AD i DNS (w dowolny sposób). GUI – Serwer Manager itp. lub PowerShell

np.

```
Install-WindowsFeature -Name RSAT-AD-Tools -IncludeAllSubFeature -ComputerName $komp
Install-WindowsFeature -Name RSAT-DNS-Server -IncludeAllSubFeature -ComputerName $komp
```

Sprawdź czy narzędzia zostały zainstalowane.

2. Delegowanie uprawnień

a. Pracownicy działu **IT** powinni mieć prawa do zarządzania kontami użytkowników firmy w następującym zakresie 

->rys 1.

Rys. 1

b. Użytkownik **adam** powinien mieć prawa do zarządzania kontami użytkowników będących w jednostce organizacyjne **New_Users** w zakresie jak powyżej.

c. Pracownicy działu **IT** powinni mieć możliwość dodawania i usuwania kont komputerów w jednostce organizacyjnej **New_Computers**

d. Pracownicy działu IT powinni mieć możliwość zarządzania domenowym serwerem **DNS**. (Musisz dodać grupę globalną **IT** do grupy **DNSAdmin**)

e. Pracownik **Adam**, został zwolniony z pracy. Wycofaj delegowane dla niego w punkcie **3b** uprawnienia.

3. Testowanie ustawień (SVR1).

a. Zaloguj się jako pracownik działu **IT** na **SVR1** i przetestuj czy możesz wykonać czynności związane z delegowanymi Ci uprawnieniami.

b. Otwórz ActiveDirecory User& Computers i:

- dodaj konto użytkownika **jarek** w jednostce organizacyjnej **HR**
- dodaj konto komputera o nazwie **CL10** w jednostce organizacyjnej **New_Computers**
- skasuj konto użytkownika **adam**

c. Upewnij się , że masz uprawnienia lokalnego administratora, i dodaj lokalne konto o nazwie **roman**

4. Konfiguracja kont użytkowników

a. Pracownicy działu **Marketing** powinni mieć ograniczone czas logowania do domeny. Powinni mieć prawo do logowania się wyłącznie od **czwartku** do **soboty** w godzinach (8.00-18.00).

b. pracownicy działu **Sales** powinni mieć ograniczone prawo logowania do domeny jedynie z komputera **CL04** (mogą logować się jedynie z komputera **CL04**).

5. Zdalna Administracja

b. Zdalna Administracja z wykorzystaniem PowerShell

Na **DC1** podłącz się zdalnie do sesji **PowerShell** na **SVR1**

```
Enter-PSSession -ComputerName SVR1
```

Wykonaj następujące polecenia PowerShell np.

```
Get-Process
Start-Process cmd
Get-Process -name c*
Stop-Process -name cmd
Get-WindowsFeature
```

Zakończ zdalną sesje

```
Exit-PSSession
```

Wykonaj polecenia

```
$komp="SVR1.keja.msft"
Invoke-Command -ComputerName $komp -ScriptBlock{Get-Process *}
```

Cele dydaktyczne:

- Umiejętność zdalnej administracji
- Umiejętność zdalnego instalowania
- Umiejętność korzystania z Local Security Policy (User Rights Assignment)
- Umiejętność delegowania uprawnień
- Umiejętność wycofywania uprawnień
- Umiejętność konfigurowania kont użytkowników.

Uzupełnienie teoretyczne

Co to jest delegowanie uprawnień w AD?

Delegowanie uprawnień pozwala na przekazanie zarządzania określonymi obiektami (np. użytkownikami, komputerami, grupami) w ramach jednostki organizacyjnej (OU) lub całej domeny innym osobom, grupom, czy administratorom niższego poziomu.

Przykłady zastosowania:

- Przyznanie liderowi zespołu prawa do resetowania haseł użytkowników w swoim zespole.
- Umożliwienie technikom IT dodawania komputerów do domeny.
- Zarządzanie grupami dystrybucyjnymi przez użytkowników.

Mechanizmy delegowania uprawnień

Delegowanie uprawnień opiera się na listach kontroli dostępu (ACL) i jest zarządzane przez uprawnienia do obiektów w Active Directory.

Typowe uprawnienia:

1. Resetowanie haseł użytkowników.
2. Tworzenie i usuwanie kont użytkowników lub komputerów.
3. Modyfikacja właściwości użytkowników, grup lub komputerów.
4. Zarządzanie członkostwem w grupach.
5. Tworzenie, usuwanie lub modyfikacja obiektów w jednostkach organizacyjnych.

Jak delegować uprawnienia w AD?

3.1. Delegowanie za pomocą Delegation of Control Wizard (GUI)

1. Otwórz Active Directory Users and Computers (ADUC):
    - Uruchom dsa.msc.

2. Przejdź do jednostki organizacyjnej (OU):
    - Znajdź OU, w której chcesz delegować uprawnienia.
3. **Uruchom kreator delegowania:**
    - Kliknij prawym przyciskiem myszy na wybrane OU i wybierz **Delegate Control**.
4. **Dodaj użytkowników lub grupy:**
    - Wybierz użytkowników lub grupy, które mają otrzymać uprawnienia.
5. **Wybierz zadania do delegowania:**
    - Kreator wyświetli listę typowych zadań, takich jak:
        - Resetowanie haseł.
        - Tworzenie/usuwanie kont komputerów.
        - Zarządzanie grupami.
    - Możesz również dostosować zadania, wybierając opcję **Create a custom task to delegate**.
6. **Zakończ delegowanie:**
    - Po zakończeniu kreatora odpowiednie uprawnienia zostaną przypisane do wybranych użytkowników/grup.

Przykładowe scenariusze delegowania

Resetowanie haseł przez helpdesk

- Uprawnienie: Resetowanie haseł i odblokowywanie kont.
- Lokalizacja: Działy (OU).
- Metoda:
    - GUI: Użycie kreatora Delegation of Control Wizard.
    - PowerShell: Dodanie dostępu ResetPassword.

Zarządzanie kontami komputerów

- Uprawnienie: Tworzenie/usuwanie kont komputerów.
- Lokalizacja: OU z komputerami.
- Metoda:
    - GUI: Kreator delegowania z wybraniem opcji zarządzania kontami komputerów.
    - PowerShell: Skonfigurowanie odpowiednich ACE (Access Control Entries).

Zarządzanie delegowaniem

Sprawdzenie istniejących delegacji

1. W GUI:
    - Otwórz właściwości OU i przejdź do zakładki Security > Advanced.
    - Przejrzyj wpisy ACL (Access Control List).

5.2. Usuwanie delegowanych uprawnień

- W GUI:

Usuń wpis ACL z zakładki Security.

- W PowerShell:
    - Usuń odpowiedni wpis ACE.

Zalecenia dotyczące delegowania

1. Używaj grup zamiast użytkowników:
    - Przydzielaj uprawnienia grupom, aby ułatwić zarządzanie.
2. Dokumentuj delegacje:
    - Zapisuj, kto ma jakie uprawnienia i dlaczego.
3. Monitoruj zmiany:
    - Włącz audyt na poziomie domeny, aby śledzić zmiany w uprawnieniach.
4. Regularnie przeglądaj delegacje:
    - Usuwaj delegacje, które nie są już potrzebne.