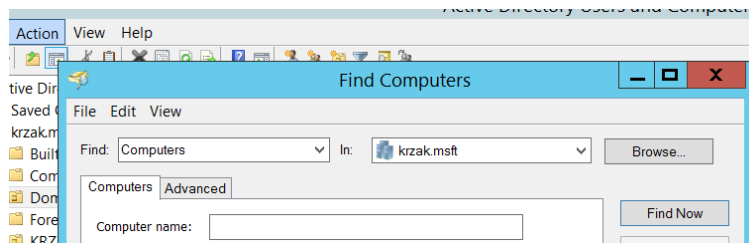


## Ćwiczenie 2 – Obiekty Active Directory (90 minut)

### Zadanie 1

1. Zaloguj się do **DC1** i uruchom **Active Directory Users & Computers**
  - a) Zapoznaj się z 'nawigacją' w Active Directory **Users & Computers**
  - b) sprawdź czy komputer **SVR1** jest członkami domeny **keja.msft** – możesz użyć opcji wyszukiwania (rys. 1).



Rys.1. Wyszukiwanie informacji

2. Uruchom **Narzędzie Active Directory Administrative Center** i wykonaj następujące czynności:
  - a) Zapoznaj się z nawigacją w Active Directory Administrative Center.
  - b) Dodaj konto użytkownika ze swoimi danymi (**imię nazwisko**).
  - c) Dla hipotetycznej osoby Roman Nowak pokazano to na rys. 2. Utworzonego konto w dalszej części niniejszej instrukcji będzie nazywane '**Twoim kontem**'
    - First name: Roman, Last Name: Nowak
    - User UPN logon: **r.nowak** (pierwsza\_litera\_imienia.nazwisko )
    - Hasło nie straci ważności

### Create User: Roman Nowak

Account	Account
Organization	
Member Of	
Password Settings	
Profile	
Policy	
Sign	
	First name: Roman
	Middle initials:
	Last name: Nowak
	Full name: * Roman Nowak
	User UPN logon: r.nowak @ keja.msft
	User SamAccountName l... keja * r.nowak

Rys.2. Tworzenie 'Twojego konta' konta użytkownika

- d) Włącz koszyk AD – **Enable Recycle Bin.**,
  - e) Skasuj konta dwóch użytkowników (np. **renata, ala**)
  - f) Uruchom Active Directory Administrative Center.
  - g) Z kosza AD przywróć usunięte konta

### 3. PowerShell

Uruchom powershell i zapoznaj się z poleceniami

#### Get-ADOrganizationalUnit

Np.

```
Get-ADOrganizationalUnit -Filter * | FT
Get-ADGroup -Filter * | FT
```

## Get-ADUser

Np.

```
Get-ADUser -Filter *  
Get-ADUser -Filter {name -like 'a*'}  
Get-ADUser -Filter * -SearchBase "ou=kejamain,dc=keja,dc=msft"
```

## Zadanie 2

### Scenariusz zadania

Zostałeś zatrudniony jako administrator w firmie „KEJA Corp”. Firma zajmuje się produkcją morskich jachtów. Firma rozwija się bardzo dynamicznie i aktualnie jest w trakcie wdrażania usługi katalogowej Active Directory. Jesteś odpowiedzialny za dział produkcji jachtów żaglowych.

Masz szereg zadań do wykonania

#### 1. Domyślne kontenery (zaloguj się do DC1)

- Domyślną jednostką organizacyjną dla nowo dodawanych kont komputerów powinna być jednostka organizacyjna **New\_Computers** (należy ją utworzyć). Wykorzystaj polecenia **redircmp**.

*Np. redircmp "ou=New-Comp,OU=KejaMain,DC=Keja,DC=msft"*

- Domyślną jednostką organizacyjną dla nowych użytkowników powinna być jednostka organizacyjna **New\_Users** umieszczona się w jednostce **KejaMain**. (należy ją utworzyć) Wykorzystaj polecenia **redirusr**

*Np. redirusr "ou=New-Users,OU=KejaMain,DC=Keja,DC=msft"*

- Sprawdź czy ustawienia zostały zmienione, w tym celu uruchom okienko PowerShell i wykonaj komendę

```
Get-AdDomain
```

- Jedynie osoby wskazane w sposób jawny mogą dodawać konta komputerów do domeny. (wykorzystaj **Adsiedit**, zweryfikuj efekt swoich działań)

- Przetestuj działanie:

Np. `New-ADUser janusz`

Np. `New-ADComputer svr111`

Twoim kolejnym zadaniem jest utworzenie wskazanych obiektów w AD

#### 2. Jednostki Organizacyjne.

`OU=KejaSail,DC=keja,DC=msft`

`OU=Users,OU=KejaSail,DC=keja,DC=msft`

`OU=Desktops,OU=KejaSail,DC=keja,DC=msft`

`OU=WR,OU=Desktops,OU=KejaSail,DC=keja,DC=msft`

`OU=KAT,OU=Desktops,OU=KejaSail,DC=keja,DC=msft`

`OU=IT,OU=Users,OU=KejaSail,DC=keja,DC=msft`

`OU=HR,OU=Users,OU=KejaSail,DC=keja,DC=msft`

`OU=Sales,OU=Users,OU=KejaSail,DC=keja,DC=msft`

`OU=Marketing,OU=Users,OU=KejaSail,DC=keja,DC=msft`

Gdzie np. wpis:

OU=KejaSail,DC=keja,DC=msft

Znaczy że w domenie keja.msft ma powstać jednostka organizacyjna KejaSail

A wpis:

OU=KAT,OU=Desktops,OU=KejaSail,DC=keja,DC=msft

Znaczy jednostka organizacyjna KAT znajduje się w jednostce Desktops a to kolejno w KejaSail

### 3. Grupy globalne.

CN=Sail\_IT,OU=IT,OU=Users,OU=KejaSail,DC=keja,DC=msft

CN= Sail\_HR,OU=HR,OU=Users,OU=KejaSail,DC=keja,DC=msft

CN= Sail\_Sales,OU=Sales,OU=Users,OU=KejaSail,DC=keja,DC=msft

CN= Sail\_Marketing,OU=Marketing,OU=Users,OU=KejaSail,DC=keja,DC=msft

Gdzie np. wpis:

CN= Sail\_IT,OU=IT,OU=Users,OU=KejaSail,DC=keja,DC=msft

Znaczy że w jednostce organizacyjnej IT ma powstać grupa Sail\_IT

### 4. Konta użytkowników

CN=marcin,OU=IT,OU=Users,OU=KejaSail,DC=keja,DC=msft

CN=alicja,OU=IT,OU=Users,OU=KejaSail,DC=keja,DC=msft

CN=aleksandra,OU=HR,OU=Users,OU=KejaSail,DC=keja,DC=msft

CN=maja,OU=HR,OU=Users,OU=KejaSail,DC=keja,DC=msft

CN=artur,OU= Sales,OU=Users,OU=KejaSail,DC=keja,DC=msft

CN=mariusz,OU=Sales,OU=Users,OU=KejaSail,DC=keja,DC=msft

CN=robert,OU=Marketing,OU=Users,OU=KejaSail,DC=keja,DC=msft

CN=zygmunt,OU=Marketing,OU=Users,OU=KejaSail,DC=keja,DC=msft

Gdzie np. wpis:

CN=marcin,OU=IT,OU=Users,OU=KejaSail,DC=keja,DC=msft

Znaczy że konto użytkownika marcin ma być w jednostce organizacyjnej IT

Uwagi:

- Ustaw hasło **Pa55w.rd** dla wszystkich kont ( hasło nie ulega przedawnieniu )
- Konta powinny być aktywne

## 5. Przynależność do grup

marcin, alicja należą do grupy **Sail\_IT**

aleksandra, maja należą do grupy **Sail\_HR**

artur, mariusz należą do grupy **Sail\_Sales**

robert, zygmunt należą do grupy **Sail\_Marketing**

## 6. Usuwanie OU

- Usuń jednostkę organizacyjną 'Saila\_HR' – korzystając z AD users& Computers
- Usuń jednostkę organizacyjną 'Sail\_Sales' – korzystając z ActiveDirectory Administrative Center
- Usuń jednostkę organizacyjną 'Sail\_Marketing' – korzystając z PowerShell

### Pomocne komendy

- New-ADOrganizationalUnit
- New-ADUser
- New-ADGroup
- Add-ADGroupMember

Np.

```
New-ADOrganizationalUnit -name "test1" -Path "ou=kejamain,dc=keja,dc=msft"
```

```
New-ADGroup -name "TESTGR" -Path "ou=kejamain,dc=keja,dc=msft" `
-GroupCategory Security -GroupScope Global
```

```
Add-ADGroupMember -Identity TESTGR -Members Maciej
```

### Dodanie użytkownika

```
New-ADUser -name "maciej1" -Path` "ou=kejamain,dc=keja,dc=msft"
-PasswordNeverExpires:$true
```

```
Set-ADAccountPassword -Identity maciej
-NewPassword (ConvertTo-SecureString "Pa55w.rd" -AsPlainText -Force)
```

```
Set-ADUser maciej -Enabled:$true
```

### **LUB**

```
[securestring]$pass = ConvertTo-SecureString "Pa55wd" -AsPlainText -Force
```

```
New-ADUser sebastian -AccountPassword $pass -Enabled:$true
-PasswordNeverExpires:$true
```

```
Set-ADAccountPassword -Identity maciej -NewPassword $secStringPassword
```

```
$pass=[securestring]$secStringPassword = ConvertTo-SecureString "Pa55wd"
-AsPlainText -Force
```

## Uzupełnienie teoretyczne

### **ms-DS-MachineAccountQuota**

to atrybut na poziomie domeny, który definiuje, ilu komputerom użytkownik bez uprawnień administracyjnych może utworzyć konto komputerowe w domenie.

- **Domyślna wartość** tego klucza to **10**, co oznacza, że standardowy użytkownik może dodać do 10 komputerów do domeny.

### **Sprawdzenie wartości za pomocą PowerShell:**

Aby sprawdzić bieżącą wartość **ms-DS-MachineAccountQuota**, możesz użyć następującego polecenia

*Get-ADObject (Get-ADDomain).DistinguishedName -Property ms-DS-MachineAccountQuota*

**redircmp** i **redirusr** to narzędzia w Active Directory, które pozwalają administratorom zmieniać domyślne lokalizacje (OU) dla nowo tworzonych kont komputerów i użytkowników. Domyślnie, nowe konta komputerów trafiają do kontenera **CN=Computers**, a nowe konta użytkowników do **CN=Users**. Te narzędzia pozwalają przekierować te obiekty do wybranych jednostek organizacyjnych (OU), co ułatwia zarządzanie i stosowanie polityk grupowych (GPO).

### **Przykład zastosowania:**

- **redircmp**: Używane do przekierowania nowych kont komputerów do innej OU.

*redircmp "OU=NewComputers,DC=domain,DC=com"*

- **redirusr**: Używane do przekierowania nowych kont użytkowników do innej OU.

*redirusr "OU=NewUsers,DC=domain,DC=com"*

**redircmp** i **redirusr** ma sens w środowiskach Active Directory, zwłaszcza gdy organizacja stosuje **polityki grupowe (GPO)** lub chce lepiej zorganizować zasoby AD. Umożliwiają one:

1. **Lepszą organizację**: Obiekty trafiają bezpośrednio do odpowiednich OU, co ułatwia ich zarządzanie.
2. **Automatyczne przypisanie polityk GPO**: Używanie odpowiednich OU sprawia, że nowo utworzone konta są automatycznie objęte politykami, co eliminuje konieczność ręcznego przenoszenia obiektów.

W dużych i rozbudowanych środowiskach, gdzie porządek i automatyzacja są kluczowe, stosowanie tych narzędzi jest zalecane.

### **Obiekty w Active Directory (AD)**

to podstawowe elementy, którymi zarządza AD. Każdy obiekt reprezentuje zasób w sieci, taki jak użytkownik, komputer, serwer, drukarka czy grupa. Obiekty są przechowywane w bazie danych AD i organizowane w strukturze hierarchicznej.

1. **Konta użytkowników**: Umożliwiają użytkownikom logowanie się do domeny i korzystanie z zasobów sieciowych. Każde konto użytkownika zawiera atrybuty takie jak imię, nazwisko, hasło i członkostwo w grupach.

2. **Konta komputerów:** Reprezentują komputery podłączone do domeny. Konta te są niezbędne do uwierzytelniania komputerów i stosowania polityk grupowych.
3. **Grupy:** Obiekty, które umożliwiają zarządzanie uprawnieniami i dostępem. Mogą być używane do przydzielania uprawnień do zasobów (np. plików, folderów) większej liczbie użytkowników lub komputerów.
4. **Jednostki organizacyjne (OU):** Logiczne kontenery, które organizują obiekty w AD. Umożliwiają delegowanie uprawnień administracyjnych i stosowanie polityk grupowych (GPO) dla wybranych grup obiektów.
5. **Obiekty polityk grupowych (GPO):** Zbiory reguł konfiguracji systemu, które mogą być stosowane do użytkowników i komputerów w domenie w celu zarządzania środowiskiem systemowym i bezpieczeństwem.

Obiekty AD są kluczowe dla centralnego zarządzania siecią i kontrolowania dostępu do zasobów w domenie.

Konta użytkowników w Active Directory (AD) są kluczowe dla uwierzytelniania i zarządzania dostępem do zasobów w domenie. Każde konto użytkownika reprezentuje indywidualnego użytkownika i posiada zestaw właściwości, które określają jego tożsamość oraz uprawnienia.

#### Najważniejsze właściwości konta użytkownika:

1. **sAMAccountName (Security Account Manager Name):** Krótsza nazwa logowania (do 20 znaków), która musi być **unikalna** w obrębie domeny. Używana przy logowaniu w starszych systemach (np. Windows NT).
2. **UserPrincipalName (UPN):** Pełna nazwa logowania, w formacie przypominającym adres e-mail (np. user@domain.com). Jest unikalna w całej lesie AD i wykorzystywana w nowszych systemach Windows oraz aplikacjach zgodnych z AD.
3. **DistinguishedName (DN):** Unikalny identyfikator konta w hierarchii Active Directory. Zawiera pełną ścieżkę do obiektu, np. CN=JanKowalski,OU=Users,DC=domain,DC=com.
4. **ObjectGUID:** Globalnie unikalny identyfikator (GUID) przypisywany każdemu obiektowi w AD, w tym kontom użytkowników. **ObjectGUID** jest zawsze unikalny w całej strukturze AD i nigdy się nie zmienia.
5. **CN (Common Name):** Nazwa obiektu, która identyfikuje konto w strukturze AD. **CN** musi być unikalne w obrębie jednostki organizacyjnej (OU), w której znajduje się konto.
6. **Hasło:** Każde konto użytkownika musi mieć przypisane hasło, które spełnia zasady polityki haseł w domenie (np. minimalna długość, złożoność).
7. **Członkostwo w grupach:** Określa, do jakich grup bezpieczeństwa i dystrybucji należy użytkownik, co wpływa na jego uprawnienia i dostęp do zasobów w domenie.

#### unikalne:

- **sAMAccountName:** Musi być unikalny w obrębie domeny.
- **UserPrincipalName (UPN):** Musi być unikalny w całym lesie AD.
- **ObjectGUID:** Globalnie unikalny w całej strukturze AD.
- **DistinguishedName (DN):** Musi być unikalny w obrębie struktury AD.

**Prestage konta komputera** (ang. **pre-staging computer account**) to proces ręcznego tworzenia konta komputera w Active Directory (AD) przed faktycznym dołączeniem komputera do domeny. Jest to technika stosowana głównie w sytuacjach, gdzie konieczna jest większa kontrola nad procesem dołączania komputerów do domeny, szczególnie w środowiskach o podwyższonym poziomie bezpieczeństwa.

#### **Korzyści z pre-stagingu konta komputera:**

1. **Zwiększona kontrola:** Administratorzy mogą z góry utworzyć konto komputera w odpowiedniej jednostce organizacyjnej (OU), zapewniając, że komputer będzie zarządzany zgodnie z politykami przypisanymi do tej OU.
2. **Bezpieczeństwo:** Pre-stage umożliwia ograniczenie, kto może dołączyć komputer do domeny. Komputer może zostać dołączony do domeny tylko, jeśli jego konto zostało wcześniej utworzone przez administratora, co zapobiega nieautoryzowanemu dołączaniu urządzeń.
3. **Automatyczne przypisywanie polityk:** Dzięki pre-stagingowi komputer jest od razu przypisany do odpowiedniej OU, co oznacza, że po dołączeniu do domeny natychmiast zaczynają na niego działać polityki grupowe (GPO) przypisane do tej jednostki organizacyjnej.

#### **Jak działa proces pre-staging konta komputera:**

1. **Ręczne tworzenie konta komputera:** Administrator w narzędziu **Active Directory Users and Computers** ręcznie tworzy konto komputera w odpowiedniej jednostce organizacyjnej (OU), gdzie komputer będzie zarządzany. Tworzone są podstawowe atrybuty konta, takie jak nazwa komputera, ale bez połączenia z fizycznym urządzeniem.
2. **Dołączenie komputera do domeny:** Kiedy fizyczny komputer jest dołączany do domeny, proces weryfikuje, czy istnieje już zarejestrowane konto komputera w AD. Jeśli takie konto istnieje (przez pre-staging), system skojarzy nowy komputer z tym kontem.
3. **Przypisywanie uprawnień:** Administratorzy mogą również przypisać prawa do dołączenia komputera do domeny wybranym użytkownikom lub grupom. Jeśli użytkownik próbuje dodać komputer do domeny, ale nie ma przypisanych praw, proces zostanie zablokowany.

#### **Scenariusze, w których pre-staging jest przydatny:**

- **Środowiska o wysokim poziomie bezpieczeństwa:** W firmach z restrykcyjnymi zasadami bezpieczeństwa, gdzie nie każdy użytkownik może dodawać komputery do domeny.
- **Przygotowanie maszyn przed masowym wdrożeniem:** W środowiskach, gdzie przed masowym wdrożeniem komputerów, administratorzy chcą upewnić się, że wszystkie komputery trafią do odpowiednich jednostek organizacyjnych (OU) i będą objęte odpowiednimi politykami grupowymi.
- **Ograniczenie nieautoryzowanego dodawania komputerów do domeny:** Pre-stage ogranicza możliwość, aby standardowy użytkownik przypadkowo (lub celowo) dodał nieznany komputer do domeny, co mogłoby zagrozić bezpieczeństwu sieci.

#### **Podsumowanie:**

**Prestage konta komputera** to praktyka stosowana przez administratorów Active Directory w celu zwiększenia kontroli nad procesem dołączania komputerów do domeny. Dzięki pre-stagingowi możliwe jest przypisanie komputerów do odpowiednich jednostek organizacyjnych z góry oraz kontrola, kto ma uprawnienia do dołączania komputerów do domeny, co poprawia bezpieczeństwo i organizację infrastruktury sieciowej.

**Cele dydaktyczne, które powinieneś osiągnąć po wykonaniu ćwiczenia:**

- Umiejętność korzystania z Active Directory Users & Computers.
- Umiejętność odnalezienia i wykorzystania odpowiednich poleceń PowerShell
- Dodawania użytkowników, grup globalnych , jednostek organizacyjnych