

## Co to jest Active Directory?

Active Directory (AD) to usługa katalogowa opracowana przez Microsoft dla systemów Windows. Umożliwia zarządzanie zasobami sieciowymi (użytkownikami, komputerami, serwerami, aplikacjami) oraz centralizację kontroli dostępu. Główne elementy AD to domeny, drzewa domen, lasy, jednostki organizacyjne (OU) i obiekty (np. użytkownicy, grupy, komputery).

### 1. Struktura Active Directory:

- **Domena (Domain):** Logiczna jednostka zarządzania. W domenie wszystkie zasoby są zarządzane centralnie, co oznacza, że użytkownicy i zasoby podlegają politykom (GPO – Group Policy Objects) oraz mogą korzystać z centralnego uwierzytelniania.
- **Las (Forest):** Najwyższy poziom struktury AD, składający się z jednej lub więcej domen. Las jest zbiorem powiązanych domen, które współdzielą wspólny schemat i konfigurację.
- **Jednostka organizacyjna (OU):** Kontener w domenie, służący do grupowania obiektów takich jak użytkownicy, grupy czy komputery. OU pozwala na łatwiejsze zarządzanie uprawnieniami i politykami.
- **Obiekty (Objects):** Podstawowe jednostki, którymi zarządza AD, np. konta użytkowników, komputery, grupy.

### 2. Kontroler domeny (Domain Controller – DC):

Kontroler domeny to serwer, na którym zainstalowana jest usługa Active Directory Domain Services (AD DS). Kontroler domeny zarządza uwierzytelnianiem użytkowników oraz autoryzacją dostępu do zasobów sieciowych. W każdej domenie musi istnieć przynajmniej jeden kontroler domeny, ale zaleca się konfigurację przynajmniej dwóch dla redundancji.

- **Replikacja AD:** AD korzysta z replikacji multimaster, co oznacza, że każdy kontroler domeny przechowuje pełną kopię bazy danych AD i może przyjmować zmiany, które są później replikowane do innych kontrolerów.

### 3. Role FSMO (Flexible Single Master Operation):

Niektóre operacje w AD wymagają centralnego zarządzania i są realizowane przez kontrolery domeny pełniące specjalne role. Wyróżniamy pięć ról FSMO:

- **Schema Master:** Zarządza modyfikacjami schematu AD.
- **Domain Naming Master:** Odpowiada za dodawanie i usuwanie domen w lesie.
- **RID Master:** Przydziela pulę identyfikatorów RID, które są potrzebne do tworzenia obiektów w domenie.
- **PDC Emulator:** Symuluje podstawowego kontrolera domeny (stare PDC) w środowiskach starszych systemów.
- **Infrastructure Master:** Dbą o aktualność odnośników między domenami.

#### 4. Grupy i uprawnienia:

AD umożliwia organizowanie użytkowników i zasobów w **grupy** dla łatwiejszego zarządzania uprawnieniami:

- **Grupy zabezpieczeń (Security Groups):** Używane do przydzielania uprawnień do zasobów.
- **Grupy dystrybucyjne (Distribution Groups):** Używane w celach dystrybucyjnych, np. listy mailingowe.

#### 5. Polityki grupowe (Group Policy Objects – GPO):

Polityki grupowe to zestaw reguł konfiguracji, które mogą być stosowane do użytkowników i komputerów w domenie. Umożliwiają centralne zarządzanie ustawieniami systemów operacyjnych, aplikacji i kont użytkowników. GPO mogą być przypisywane do domen, OU lub lokalnie.

- **Przykłady polityk grupowych:** Konfiguracja haseł, ustawienia zapory sieciowej, instalacja oprogramowania, mapowanie dysków sieciowych.

#### 6. Uwierzytelnianie w Active Directory:

AD wspiera różne mechanizmy uwierzytelniania, z których najczęściej stosowanym jest **Kerberos**. Każdy użytkownik logujący się do domeny uwierzytelnia się na kontrolerze domeny, który potwierdza tożsamość za pomocą systemu biletów (ticketów Kerberos). Dodatkowo AD wspiera **LDAP** (Lightweight Directory Access Protocol) do zapytań o dane katalogowe.

#### 7. Podstawowe operacje administracyjne w AD:

- **Tworzenie użytkowników:** Można to zrobić m.in. za pomocą konsoli Active Directory Users and Computers (ADUC) lub PowerShella.
- **Tworzenie grup i nadawanie uprawnień:** Użytkownicy są przypisywani do grup, którym przydziela się prawa dostępu do zasobów (np. plików, folderów).
- **Dodawanie komputerów do domeny:** Komputery serwerowe i klienckie są dodawane do domeny, co umożliwia im korzystanie z centralnego uwierzytelniania oraz polityk.

#### 8. Narzędzia administracyjne Active Directory

- **Active Directory Users and Computers (ADUC):**  
Umożliwia zarządzanie użytkownikami, komputerami, grupami i OUs.
- **Active Directory Sites and Services:**  
Pozwala zarządzać replikacją AD między różnymi lokalizacjami.
- **Active Directory Domains and Trusts:**  
Umożliwia zarządzanie relacjami zaufania między domenami.
- **Active Directory Schema**  
Umożliwia modyfikację schematu

### Podsumowanie:

W trakcie ćwiczeń praktycznych z Active Directory kursanci będą zarządzać kontrolerem domeny, konfigurować użytkowników, grupy, polityki oraz dodawać serwery do domeny. Celem jest zrozumienie, jak AD centralizuje zarządzanie siecią i pozwala na łatwą administrację użytkownikami oraz zasobami w środowisku serwerowym Windows.

---

Uzupełnienie:

### Rejestracja i uruchomienie przystawki Schema Management:

- Otwórz wiersz polecenia lub PowerShell jako administrator.
- Wpisz polecenie: **regsvr32 schmmgmt.dll**
- Po pomyślnym wykonaniu powinieneś zobaczyć komunikat potwierdzający rejestrację.
- W konsoli MMC (Microsoft Management Console) kliknij File > Add/Remove Snap-in....

Z listy wybierz **Active Directory Schema** i kliknij **Add**, a następnie **OK**.