Temat: Delegowanie i zabezpieczenia obiektów ADDS. Tworzenie profili kont użytkowników ADDS.

Cel Ogólny lekcji: Celem ogólnym lekcji jest zrozumienie koncepcji delegowania i zabezpieczeń obiektów w kontekście usługi katalogowej Active Directory oraz umiejętność tworzenia i konfigurowania profili kont użytkowników w środowisku Active Directory.

Cele szczegółowe:

1. **Delegowanie i Zabezpieczenia Obiektów w Active Directory:**
- Wyjaśnienie, czym jest Active Directory i jego rola w zarządzaniu zasobami sieciowymi.
- Zrozumienie pojęcia delegacji w kontekście zarządzania obiektami w AD.
- Omówienie korzyści z delegowania uprawnień w celu zrównoważonego zarządzania.
- Zrozumienie poziomów, na których można przeprowadzać delegację (drzewo katalogu, domena, jednostka organizacyjna).
- Wyjaśnienie procesu delegacji w AD, obejmującego wybór obiektów, określenie uprawnień i obszaru działania.
- Przykłady typowych uprawnień, które można przekazywać poprzez delegację.
2. **Tworzenie Profili Kont Użytkowników w Active Directory:**
- Przypomnienie podstawowych wiadomości związanych z profilami kont użytkowników z klasy pierwszej.
- Zrozumienie roli profili użytkowników w dostosowaniu środowiska pracy użytkownika na komputerze.
- Wyjaśnienie różnych typów profili użytkowników: lokalne, mobilne, obowiązkowe, tymczasowe.
- Zrozumienie składników profilu użytkownika: gałąź rejestru i zestaw folderów profilu.
- Omówienie korzyści wynikających z korzystania z różnych typów profili użytkowników.
- Zrozumienie procesu tworzenia mobilnych profili użytkowników oraz ich zalet, takich jak automatyczna dostępność zasobów i uproszczona wymiana komputera.
3. **Wdrażanie Profili Użytkowników Mobilnych:**
- Przedstawienie kroków potrzebnych do wdrożenia profili użytkowników mobilnych w środowisku sieciowym.

- Omówienie konieczności stworzenia grupy zabezpieczeń dla użytkowników mobilnych.
- Zrozumienie procesu tworzenia udziału pliku na serwerze dla przechowywania profili użytkowników mobilnych.
- Wyjaśnienie roli obiektu zasad grupy w konfiguracji profili użytkowników mobilnych.
- Omówienie ustawień profili użytkowników mobilnych, włączając na koncie użytkownika w AD DS oraz komputerze w zasadach grupy.

4. Zabezpieczenia i Optymalizacje:

- Wyjaśnienie, dlaczego zabezpieczenia profili użytkowników są ważne w kontekście bezpieczeństwa infrastruktury.
- Omówienie opcji optymalizacji przy pierwszym logowaniu, włączając w to przyspieszenie logowania użytkowników.
- Przedstawienie możliwości usuwania niepotrzebnych aplikacji z obrazu systemu Windows 10 w celu optymalizacji profili użytkowników.

5. Teoretyczne przykłady praktycznego wykorzystania profili użytkowników:

- Wyjaśnienie, jak ustawić domyślny układ pulpitu dla komputerów z Windows 10.
- Omówienie funkcji podstawowego komputera i sposobów jej implementacji.
- Wskazówki dotyczące wdrożenia i monitorowania profili użytkowników mobilnych w praktyce.

Podsumowanie:

Cele ogólne i szczegółowe lekcji mają na celu dostarczenie uczniom wiedzy na temat delegowania i zabezpieczeń obiektów w Active Directory oraz umiejętności tworzenia i konfigurowania

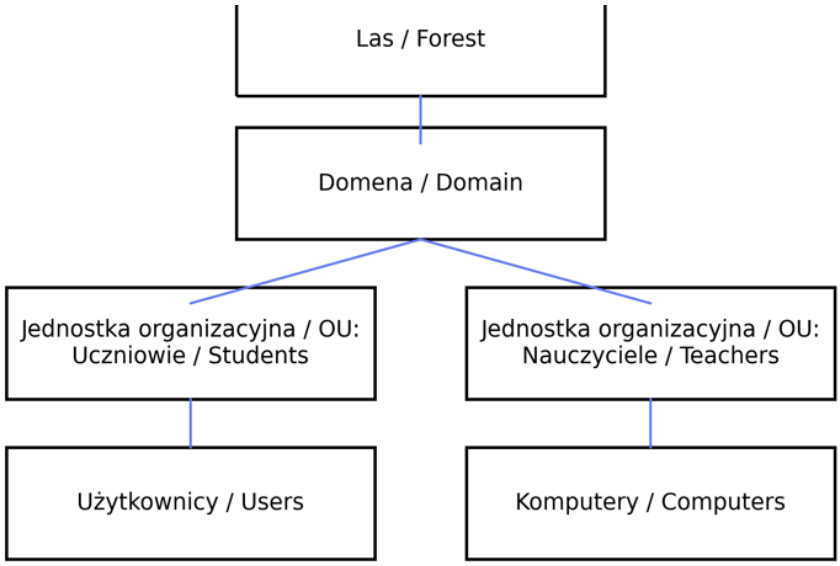
1. Active Directory – podstawy

Active Directory Domain Services (AD DS) to usługa katalogowa Microsoft umożliwiająca zarządzanie użytkownikami, komputerami, grupami i zasobami sieciowymi.

Zapewnia centralizację administracji, wdrażanie zasad bezpieczeństwa oraz delegowanie uprawnień.

2. Delegowanie w Active Directory

Delegowanie oznacza przekazywanie części uprawnień administracyjnych innym użytkownikom lub grupom.



Zwykle wykonuje się je na poziomie jednostek organizacyjnych (OU).

2.1. Po co stosuje się delegowanie?
Rozłożenie obowiązków administracyjnych.

Zwiększenie bezpieczeństwa poprzez nadawanie minimalnych wymaganych uprawnień (zasada least privilege).

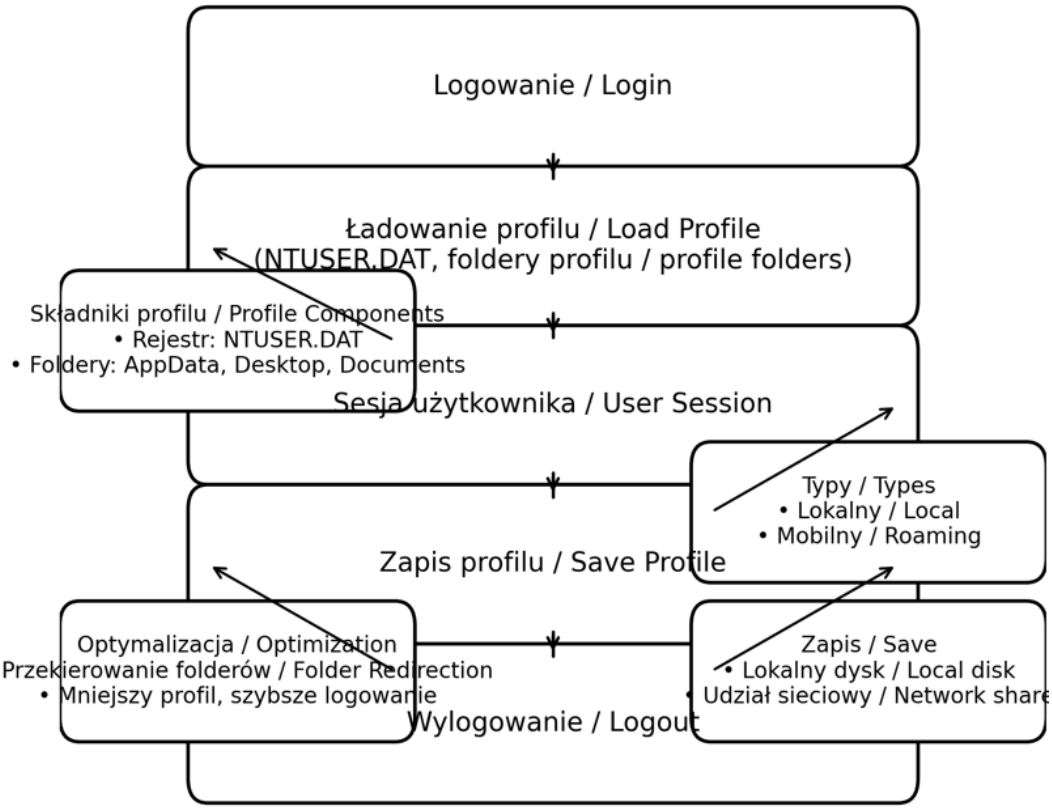
2.2. Jak wykonać delegowanie?
Wybierz OU i uruchom kreator Delegate Control.

Wybierz użytkowników/grupy, którym delegujesz uprawnienia.

Wskaż zakres działań, np. resetowanie haseł lub tworzenie użytkowników.

3. Profile użytkowników – podstawy
Profil użytkownika zawiera ustawienia pulpitu, rejestru i dane użytkownika.

System ładuje profil przy logowaniu i zapisuje go przy wylogowaniu.



4. Typy profili użytkowników
Profil lokalny – działa tylko na jednym komputerze.

Profil mobilny – przechowywany na serwerze, synchronizowany na wielu komputerach.

Profil obowiązkowy – użytkownik nie może zapisać zmian, profil posiada plik NTUSER.man.

Profil tymczasowy – ładowany w przypadku błędów, usuwany po wylogowaniu.

Profil superobowiązkowy Profil nie tylko ma zapis NTUSER.man, ale: Ścieżka profilu w AD / GPO kończy się na .man np: \\SERVER\Profiles\Mandatory.man

Kiedy stosować profil superobowiązkowy? Klient NIE może dostać profilu tymczasowego,

5. Elementy profilu użytkownika
Gałąź rejestru (NTUSER.DAT) zawierająca ustawienia użytkownika.

Foldery profilu: Dokumenty, Pulpit, AppData i inne.

6. Wdrożenie profili mobilnych
Komputery muszą należeć do domeny.

Tworzy się udział sieciowy Profiles$ z odpowiednimi uprawnieniami.

W AD DS na koncie użytkownika wskazuje się ścieżkę do profilu, np. \\serwer\Profiles$\%username%.

6A. Profile przez GPO vs klasyczny mechanizm (właściwości konta użytkownika)

W środowisku domenowym istnieją dwa główne sposoby definiowania ścieżki profilu użytkownika:

- Klasyczny mechanizm (AD DS → konto użytkownika → karta "Profile" → "Ścieżka profilu"): wpis przypięty do konkretnego użytkownika; obowiązuje na wszystkich komputerach domeny, na których się zaloguje.
- GPO per-komputer (Computer Configuration → Policies → Administrative Templates → System → User Profiles → "Set roaming profile path for all users logging onto this computer"): wpis ustalany przez zasady dla KOMPUTERA – dotyczy wszystkich użytkowników logujących się na ten komputer.

Profil roamingowy / Roaming profile – profil zapisany na serwerze, dostępny z wielu komputerów.

Priorytet (precedence):

Ustawienie GPO (per-komputer) ma pierwszeństwo przed ścieżką profilu ustawioną na karcie "Profile" konta użytkownika w AD DS (przysłania je na danym komputerze).

Zakres działania:

AD DS (konto) – globalne dla użytkownika (wszędzie, gdzie się zaloguje), chyba że komputer ma GPO nadpisujące.

GPO (per-komputer) – lokalne dla danego komputera/OU komputerów; wygodne w pracowniach, VDI i terminalach.

VDI (Virtual Desktop Infrastructure) – infrastruktura wirtualnych pulpitów, w której uczniowie logują się do zdalnych komputerów w centrum danych. Używane w szkołach, call-center, firmach - zamiast lokalnych systemów.

Terminal – cienki klient pracujący na serwerze przez Remote Desktop Services (RDS), np. w salach komputerowych.

Typowe scenariusze użycia:

Pracownia szkolna: wymuszenie wspólnej lokalizacji profili na stanowiskach sali – GPO per-komputer.

Użytkownik pracujący na wielu salach: ścieżka profilu na koncie użytkownika (AD DS).

Środowiska mieszane: profil na koncie, ale w wybranych pracowniach GPO kieruje profil do innej lokalizacji (A/B test, izolacja).

Uwaga praktyczna:

Wersjonowanie profili (V2…V6) jest niezależne od metody ustawienia ścieżki (AD DS vs GPO).

Stosuj przekierowanie folderów razem z profilami roamingowymi, by zmniejszyć rozmiar profilu i przyspieszyć logowanie.

Folder Redirection (przekierowanie folderów) – mechanizm GPO, który przenosi foldery użytkownika (Documents, Desktop) z profilu roamingowego do serwera, aby przyspieszyć logowanie.

W razie konfliktu sprawdź wynikowe zasady (gpresult /h report.html) oraz atrybut profilePath na koncie użytkownika.

profilePath – pole w koncie użytkownika AD DS określające lokalizację profilu roamingowego (np. \\serwer\Profiles$\%username%).

7. Zabezpieczenia i optymalizacja profili
Możliwe jest przekierowanie folderów użytkownika dla zmniejszenia rozmiaru profilu.

Można ustawić domyślny układ menu Start poprzez GPO.

Niepotrzebne aplikacje można usuwać w celu przyspieszenia logowania.

8. Wersje profili użytkowników
Windows 7/2008 R2 – V2

Windows 8/8.1 – V3/V4

Windows 10 / Server 2016+ – V5/V6

9. Podsumowanie
Uczeń rozumie delegowanie uprawnień, typy profili oraz sposób wdrażania profili mobilnych.

Zna podstawowe zasady zabezpieczeń i optymalizacji środowiska użytkownika.