

Laboratorium 02-03 – 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).

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:
 - Usuвай delegacje, które nie są już potrzebne.