Ćwiczenie 5c. Group Policy Object (GPO) cz 3.

W centrali w Opolu pracują pracownicy działu IT, HR i Marketingu. Decyzją kierownika działu IT:

1. Każdy pracownik działu IT ma prawo administrować komputerami klienckimi w Opolu
2. Polityka haseł dla pracowników działu IT jest następująca:
    a. Historia haseł 24
    b. Maksymalny okres ważności hasła 120
    c. Minimalny okres ważności hasła 1
    d. Minimalna długość hasła 12
3. Z komputerów klienckich zlokalizowanych w Opolu: **CL1**, CL2, CL3 korzystają pracownicy działu HR i oni powinni mieć możliwość administrowania przynależącymi im komputerami (np. instalacja oprogramowania).
4. Tworzona jest sala szkoleniowa w której będą zlokalizowane komputery. Utwórz jednostkę OU **Szkolenia**. Na komputerach w Sali szkoleniowej powinny być dla wszystkich uczestników (niezależnie od działu) Identycznen ustawienia 'Użytkownika'. Zrealizuj zadanie. Przenieś komputer CL1 do jednostki organizacyjnej **Szkolenia.**
5. **Punkt_opcjonalny:** Na wszystkich komputerach klienckich w Opolu ma zostać zainstalowane darmowe oprogramowanie **putty**

Uzupełnienie teoretyczne

Loopback Processing Mode to specjalny tryb przetwarzania zasad **Group Policy** (GPO), który pozwala zmodyfikować sposób stosowania polityk **użytkownika** na podstawie lokalizacji **komputera** w Active Directory (AD). Zwykle ustawienia GPO dla użytkownika są stosowane na podstawie jednostki organizacyjnej (OU), w której znajduje się **konto użytkownika**. Dzięki **Loopback Processing**, możemy wymusić, aby ustawienia użytkownika były stosowane na podstawie polityk przypisanych do komputera, na którym ten użytkownik się loguje.

Kiedy stosować Loopback Processing?

Loopback Processing jest przydatny w środowiskach, gdzie komputer pełni specjalną funkcję, np. na komputerach w laboratoriach, klasach lub serwerach terminalowych, gdzie ustawienia użytkownika muszą być narzucone przez komputer, niezależnie od użytkownika.

Przykład: Na komputerach w laboratorium szkolnym lub w kiosku internetowym, gdzie wszyscy użytkownicy mają mieć takie same ograniczenia, niezależnie od tego, kim są, ustawienia GPO dla użytkowników mogą być kontrolowane przez GPO przypisane do komputerów.

Dwa tryby Loopback Processing:

1. **Merge (Scalanie)**:
    - W tym trybie ustawienia użytkownika są **łączone** z ustawieniami komputera.
    - Zasady użytkownika przypisane do konta użytkownika są stosowane normalnie, a następnie **zasady komputera nadpisują lub uzupełniają** te ustawienia.
    - Jeśli istnieją konflikty (tzn. te same ustawienia w obu GPO), ustawienia z polityk komputera mają **priorytet** nad politykami użytkownika.

2. **Replace (Zastąpienie)**:
    - W tym trybie **ignorowane** są wszystkie ustawienia użytkownika, które są przypisane do konta użytkownika.
    - Zamiast tego, stosowane są tylko **zasady użytkownika przypisane do komputera**. Oznacza to, że konfiguracje użytkownika są całkowicie zastępowane przez te przypisane do komputera.

Ścieżka do ustawienia Loopback Processing Mode:

Aby włączyć **Loopback Processing Mode** w GPO, wykonaj następujące kroki:

1. Otwórz **Group Policy Management Console (GPMC)**.
2. Przejdź do odpowiedniej polityki GPO lub utwórz nową, przypisaną do komputerów.
3. Przejdź do:
    - **Computer Configuration** -> **Policies** -> **Administrative Templates** -> **System** -> **Group Policy**.
4. Znajdź i skonfiguruj opcję **Configure user Group Policy loopback processing mode**.
5. Wybierz tryb **Merge** lub **Replace**, w zależności od potrzeby.

Przykłady zastosowania:

- **Tryb Merge**:
    - Firma chce, aby użytkownicy mogli korzystać z własnych ustawień na większości komputerów, ale na niektórych specjalnych komputerach, np. komputerach używanych w strefach publicznych, muszą mieć dodatkowe restrykcje.
    - Ustawienia użytkownika są stosowane normalnie, a dodatkowe ograniczenia (np. blokada dostępu do Panelu sterowania) są nadpisywane na podstawie polityk komputera.
- **Tryb Replace**:
    - Na komputerach w laboratorium komputerowym szkoły, niezależnie od tego, kto się zaloguje, muszą być stosowane te same restrykcyjne ustawienia. Dzięki trybowi **Replace**, polityki użytkownika przypisane do kont są ignorowane, a stosowane są tylko te, które są przypisane do komputera.

Podsumowanie:

Loopback Processing Mode to funkcja GPO, która pozwala stosować polityki użytkownika na podstawie lokalizacji komputera w AD, a nie użytkownika. Ma dwa tryby:

- **Merge** (łączy ustawienia użytkownika i komputera, komputer ma priorytet w przypadku konfliktu),
- **Replace** (ignoruje ustawienia użytkownika i stosuje tylko ustawienia przypisane do komputera).

Password Settings Object (PSO) to obiekt używany w **Active Directory (AD)**, który pozwala na przypisanie szczegółowych zasad dotyczących haseł i blokowania kont do konkretnych użytkowników lub grup użytkowników. Zasadniczo, PSO umożliwia wdrożenie różnych polityk haseł dla różnych grup użytkowników w tej samej domenie, co daje elastyczność większą niż domyślna polityka haseł przypisana do całej domeny (np. w **Default Domain Policy**).

Jak działa PSO:

1. **PSO** jest stosowany na poziomie konta użytkownika lub grupy zabezpieczeń.
2. Każdy **PSO** może określać:
    - Minimalną i maksymalną długość hasła,
    - Historię haseł (ile poprzednich haseł nie może być używanych),
    - Czas ważności hasła,
    - Wymogi dotyczące złożoności hasła,
    - Polityki blokady konta (np. ile razy można wpisać błędne hasło przed blokadą).

Priorytet PSO – Zasady dla użytkownika są ważniejsze niż dla grupy

1. Indywidualnie przypisany PSO ma wyższy priorytet niż PSO przypisany do grupy:

- Jeśli użytkownik ma przypisane różne PSO, zarówno bezpośrednio, jak i przez grupę, **zasady przypisane bezpośrednio do użytkownika mają wyższy priorytet** niż zasady przypisane do grup, nawet jeśli PSO dla grupy ma niższą wartość **precedence**.
- **Przykład**: Użytkownik **Ewa** ma przypisany PSO bezpośrednio do swojego konta z określonymi zasadami haseł. Ewa jest również członkiem grupy **Finance**, do której przypisano PSO z innymi zasadami. W takim przypadku zasady haseł przypisane bezpośrednio do Ewy mają pierwszeństwo nad tymi, które wynikają z członkostwa w grupie **Finance**.

2. Precedence (priorytet PSO):

- **Precedence** to wartość liczbową przypisaną do każdego PSO, która określa jego priorytet – **im niższa wartość**, tym **wyższy priorytet** PSO.
- W sytuacji, gdy użytkownik ma przypisane wiele PSO (np. przez kilka grup), **PSO o niższej wartości precedence** będzie miał pierwszeństwo.
- **Jednakże**, PSO przypisane bezpośrednio do użytkownika zawsze będzie miało **wyższy priorytet** niż jakiekolwiek PSO przypisane przez grupy, niezależnie od wartości **precedence**.

Przykład zastosowania PSO:

1. **Użytkownik Ewa** ma przypisany PSO bezpośrednio do jej konta, z ustawieniem:
    - **Minimalna długość hasła**: 12 znaków.
    - **Maksymalny czas ważności hasła**: 30 dni.
2. **Grupa Finance**, do której Ewa należy, ma przypisany inny PSO, z ustawieniem:
    - **Minimalna długość hasła**: 8 znaków.

- **Maksymalny czas ważności hasła**: 60 dni.

Wynik:

- **Zasady haseł dla użytkownika Ewa**: Ponieważ PSO jest przypisany bezpośrednio do konta Ewy, to zasady dla jej hasła będą wynikały z tego PSO, nawet jeśli PSO przypisany do grupy Finance ma inną konfigurację. Ewa będzie musiała używać haseł o długości **12 znaków** i zmieniać hasło co **30 dni**, zgodnie z PSO przypisanym do jej konta.

Jak działa precedence:

Jeśli użytkownik nie ma bezpośrednio przypisanego PSO, ale należy do wielu grup, z których każda ma inne PSO:

- System wybierze PSO, które ma **najniższą wartość precedence** (czyli wyższy priorytet).
- Jeśli dwie grupy mają przypisane PSO, to PSO o niższej wartości **precedence** zostanie zastosowane.

Jak przypisać PSO:

1. **Otwórz Active Directory Administrative Center (ADAC)** i przejdź do **Password Settings Container**.
2. Utwórz nowy PSO, konfigurując wymagane zasady.
3. W **Directly applies to**, przypisz PSO do **konkretnego użytkownika** lub do grupy użytkowników.
4. Jeśli przypiszesz PSO do zarówno użytkownika, jak i grupy, pamiętaj, że zasady użytkownika
5. **Sprawdzenie:** Get-ADUserResultantPasswordPolicy -Identity <NazwaUżytkownika> mają pierwszeństwo.

Podsumowanie:

- **PSO przypisany bezpośrednio do użytkownika ma wyższy priorytet** niż PSO przypisany przez grupy, niezależnie od wartości **precedence**.
- Jeśli użytkownik nie ma przypisanego bezpośredniego PSO, system wybierze PSO z grup o **najniższej wartości precedence**.
- **Precedence** określa priorytet PSO w kontekście grup, ale nie ma wpływu, gdy PSO jest przypisany bezpośrednio do użytkownika.