Laboratorium 05 – Uzupełnienie Teoretyczne

1. Wprowadzenie do Group Policy Object (GPO)

Group Policy Object (GPO) to mechanizm zarządzania i konfiguracji systemów operacyjnych, aplikacji oraz ustawień użytkowników w środowisku Windows. Dzięki GPO administratorzy mogą scentralizować i automatyzować zarządzanie politykami w domenach Active Directory (AD). GPO umożliwia kontrolowanie wielu aspektów systemu, takich jak instalacja oprogramowania, konfiguracja zabezpieczeń, ustawienia sieciowe i zarządzanie sesjami użytkowników.

Podstawowe elementy GPO:

- **Local Group Policy** (polityka lokalna) – polityka dotycząca tylko lokalnego komputera.
- **Domain-based Group Policy** – polityka stosowana w ramach domeny Active Directory.
- **GPOs** mogą być przypisane do:
    - **Site** (witryny),
    - **Domain** (domeny),
    - **Organizational Units (OU)** (jednostki organizacyjne).

Typy ustawień w GPO:

- **Computer Configuration** – ustawienia, które są stosowane do komputerów (niezależnie od użytkownika, który jest zalogowany).
- **User Configuration** – ustawienia, które są stosowane do użytkowników (niezależnie od komputera, na którym są zalogowani).

2. Dziedziczenie GPO

Domyślnie GPO mają charakter dziedziczny. Oznacza to, że polityki przypisane do wyższego poziomu struktury AD (np. domeny) są dziedziczone przez obiekty na niższych poziomach (np. jednostki organizacyjne – OU).

Przykład:

> Jeśli przypiszemy GPO do domeny, to polityka ta będzie automatycznie stosowana do wszystkich obiektów (komputerów i użytkowników) wewnątrz tej domeny, chyba że dziedziczenie zostanie wyłączone lub zmienione.

3. Blokowanie dziedziczenia GPO (Block Inheritance)

Administratorzy mogą zablokować dziedziczenie GPO w jednostkach organizacyjnych (OU) poprzez opcję **Block Inheritance**. Gdy ta opcja jest włączona dla konkretnej OU, wszystkie polityki z wyższego poziomu struktury AD nie będą stosowane do obiektów w tej OU.

Przykład:

> Blokowanie dziedziczenia może być użyteczne, gdy w jednej z jednostek organizacyjnych potrzebne są zupełnie inne polityki niż te, które są przypisane do całej domeny.

4. Force GPO (Wymuszanie polityki)

Aby przeciwdziałać **Block Inheritance**, można użyć opcji **Enforce (Force GPO)**. Ustawiając politykę jako wymuszoną, sprawiamy, że będzie ona stosowana do wszystkich obiektów poniżej, nawet jeśli dziedziczenie zostało zablokowane.

Przykład:

> Możemy wymusić stosowanie polityki zabezpieczeń w całej domenie, aby zapewnić jednolite zasady bezpieczeństwa na wszystkich poziomach organizacyjnych.

Gpupdate:

gpupdate to narzędzie wiersza poleceń w systemach Windows, które umożliwia wymuszenie natychmiastowego odświeżenia zasad grupowych (**Group Policy**), zamiast czekać na domyślny cykl odświeżania (co 90 minut). Przy jego użyciu można zaktualizować zarówno ustawienia komputera, jak i użytkownika.

Przykład użycia:

> ***gpupdate /force***

Polecenie to wymusi natychmiastowe przetwarzanie polityk dla zarówno konfiguracji komputera, jak i użytkownika. Dodatkowe przełączniki, jak np. /logoff, mogą wymusić wylogowanie po aktualizacji polityk, jeśli to wymagane.

Gpresult:

gpresult to narzędzie wiersza poleceń, które pozwala wyświetlić szczegółowe informacje na temat zastosowanych polityk grupowych na danym komputerze i dla zalogowanego użytkownika. Służy do analizy i diagnostyki, jakie zasady GPO zostały zastosowane, które polityki zostały zablokowane i z jakiego źródła pochodzą.

Przykład użycia:

> ***gpresult /r***

Polecenie to wyświetli podsumowanie polityk dla bieżącego użytkownika i komputera, w tym ich źródło oraz czas ostatniego odświeżenia.

Podsumowanie:

- gpupdate służy do **natychmiastowego odświeżenia GPO**.
- gpresult pozwala na **sprawdzenie wyników stosowania polityk GPO**, co jest użyteczne w diagnozowaniu problemów z GPO.

Polityka HASEŁ

Aby ustalić (podstawową) politykę haseł dla całej domeny, należy skonfigurować ją w **GPO połączonym bezpośrednio z poziomem domeny** – najczęściej w **Default Domain Policy**.

Dlaczego w Default Domain Policy?

- Klasyczna (globalna) polityka haseł w Active Directory jest „wyciągana" wyłącznie z GPO przypiętego do obiektu **Domain**. System zawsze będzie używał ustawień haseł (w sekcji **Password Policy**) z GPO mającego najwyższy priorytet na poziomie domeny. Domyślnie jest nim właśnie **Default Domain Policy**.

Uwaga o Fine-Grained Password Policies (FGPP)

- Jeśli pracujemy na Windows Server 2008 i nowszym, istnieje dodatkowa funkcja tzw. *Fine-Grained Password Policies*, która pozwala stosować różne polityki haseł dla różnych grup użytkowników. FGPP konfiguruje się **nie** poprzez GPO, ale przez atrybuty obiektów w AD (np. za pomocą **Active Directory Administrative Center** lub **PowerShell**), tworząc tzw. *Password Settings Objects (PSO)*.

W codziennej praktyce jednak (jeśli chodzi o jedną, główną politykę haseł) zazwyczaj modyfikuje się ustawienia w **Default Domain Policy** w **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Account Policies** → **Password Policy**.

Czy można zdefiniować polityke haseł w innym GPO podłączonym na poziomie domeny

Tak, może to zadziałać – **o ile** spełnione są dwa warunki:

1. **GPO jest podpięte (linked) bezpośrednio do obiektu domeny** (czyli do tego samego miejsca, co „Default Domain Policy"),
2. **Ma wyższy priorytet** (niższy numer link order) niż *Default Domain Policy*.

W takiej sytuacji ustawienia Password Policy z GPO_INIT nadpiszą te z *Default Domain Policy*.