

# Group Policy Object (GPO)

## 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.

## 5. Loopback Processing Mode

Tryb przetwarzania **Loopback** to opcja konfiguracji GPO, która umożliwia zastosowanie ustawień dla użytkowników w zależności od komputera, na którym są zalogowani, a nie od ich konta użytkownika.

Loopback może być skonfigurowany w dwóch trybach:

- **Replace** – ustawienia użytkownika z GPO są całkowicie zastępowane ustawieniami GPO przypisanymi do komputera.
- **Merge** – ustawienia użytkownika są łączone z ustawieniami komputera. Jeśli są konflikty, ustawienia komputera mają priorytet.

### Przykład zastosowania:

Loopback jest przydatny w środowiskach takich jak komputery w laboratoriach szkolnych lub na serwerach terminalowych, gdzie niektóre ustawienia użytkownika mogą być ignorowane na rzecz bardziej restrykcyjnych ustawień komputera.

## 6. Polityki inicjowania (Startup/Shutdown Scripts)

GPO umożliwia administratorom konfigurowanie skryptów, które są uruchamiane podczas różnych wydarzeń, takich jak:

- **Startup** – skrypty uruchamiane podczas startu systemu.
- **Shutdown** – skrypty uruchamiane podczas wyłączania systemu.
- **Logon** – skrypty uruchamiane podczas logowania użytkownika.
- **Logoff** – skrypty uruchamiane podczas wylogowywania użytkownika.

### Przykład:

Skrypty **Startup** mogą być użyte do automatycznego montowania zasobów sieciowych lub uruchamiania serwisów przed zalogowaniem użytkownika.

## 7. Filtry WMI

**Windows Management Instrumentation (WMI) Filtering** to zaawansowane narzędzie, które pozwala na precyzyjne kontrolowanie stosowania polityk na podstawie określonych warunków. WMI umożliwia dynamiczne filtrowanie GPO w zależności od różnych kryteriów, takich jak wersja systemu operacyjnego, model komputera lub status sieci.

### Przykład:

Jeśli chcemy, aby konkretna polityka była stosowana tylko na komputerach z systemem Windows 10, możemy zastosować filtr WMI z odpowiednim zapytaniem.

**Więcej o WMI w dalszej części dokumentu**

## 8. Delegacja GPO

Delegacja umożliwia przypisywanie praw do zarządzania GPO określonym użytkownikom lub grupom. Dzięki temu administratorzy mogą kontrolować, kto ma prawo edytować, linkować lub stosować GPO, bez nadawania im pełnych uprawnień administracyjnych.

**Delegacja obejmuje:**

- **Linkowanie GPO** – kto może przypisać GPO do określonych obiektów w domenie.
- **Modyfikacja GPO** – kto może edytować zawartość polityk.

## 9. Stosowanie GPO – Order of Precedence (Kolejność przetwarzania)

Polityki są stosowane zgodnie z następującą kolejnością:

1. **Local Group Policy** – polityka lokalna komputera.
2. **Site** – polityki przypisane do witryny AD.
3. **Domain** – polityki przypisane do domeny.
4. **Organizational Unit (OU)** – polityki przypisane do jednostki organizacyjnej. W przypadku podjednostek w strukturze OU, polityki są stosowane od góry (najbliższej domeny) w dół (najbliższej jednostki organizacyjnej).

Polityki ustawione na niższych poziomach (np. w OU) mają wyższy priorytet niż te przypisane do wyższych poziomów (np. domeny), chyba że są wymuszone (Enforced).

## 10. Backup i restore GPO

Administratorzy mogą tworzyć kopie zapasowe GPO oraz przywracać je w razie potrzeby. Narzędzia takie jak Group Policy Management Console (GPMC) pozwalają na:

- **Backup GPO** – tworzenie kopii zapasowej polityki.
- **Restore GPO** – przywracanie polityki z kopii zapasowej.
- **Import GPO** – importowanie ustawień polityki z innej domeny lub środowiska.

**Przykład zastosowania:**

Tworzenie regularnych kopii zapasowych polityk GPO umożliwia szybkie odzyskanie ustawień po błędnej modyfikacji lub usunięciu GPO.

## 11. Narzędzia do zarządzania GPO

### Group Policy Management Console (GPMC)

GPMC to główne narzędzie do zarządzania politykami GPO. Dzięki niemu można:

- Tworzyć i modyfikować GPO,
- Zarządzać delegacjami,
- Stosować kopie zapasowe,
- Monitorować wynik stosowania polityk.

### **Group Policy Results (gpresult)**

gpresult to narzędzie wiersza poleceń, które pozwala sprawdzić, jakie polityki są stosowane na danym komputerze i użytkowniku.

Przykład użycia:

```
cmd
```

```
gpresult /r
```

Ten polecenie wyświetli wyniki polityk zastosowanych dla bieżącego użytkownika i komputera.

### **Group Policy Modeling**

Symulacja, która umożliwia administratorom przetestowanie, jakie polityki zostaną zastosowane w określonym scenariuszu przed ich wdrożeniem.

---

### **Podsumowanie**

GPO to potężne narzędzie administracyjne, które pozwala na scentralizowane zarządzanie konfiguracją systemów w domenie. Zrozumienie dziedziczenia, blokowania, Loopback Processing, skryptów inicjujących, filtrów WMI oraz kolejności przetwarzania GPO jest kluczowe dla efektywnego wdrożenia i utrzymania polityk w dużych środowiskach IT.