GPO od środka: tworzenie, łączenie, kolejność i diagnostyka

Poziom: średniozaawansowany

Dotyczy: Group Policy Management Console, moduł PowerShell GroupPolicy, Windows Server 2016+

Czas: ~40 min

GPO wypycha ustawienia z domeny na komputery i konta bez odwiedzania każdego z nich osobno. Tu tworzymy nowe polityki, łączymy je z jednostkami organizacyjnymi i sprawdzamy, dlaczego dana zmiana albo w ogóle nie doszła, albo doszła w złe miejsce. Które GPO w Zielonej wycofujemy do Intune, opisuje osobna strona linkowana niżej.

Skróty użyte na tej stronie (12)

Skrót	Co znaczy
ADML	plik językowy dołączony do szablonu ADMX, z tłumaczeniem nazw i opisów ustawień GPO na dany język
ADMX	format plików szablonów administracyjnych GPO, następca starszego formatu ADM
GPMC	Group Policy Management Console: konsola do zarządzania politykami GPO w domenie
GPO	Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery
GUID	Globally Unique Identifier: unikalny w skali globalnej identyfikator obiektu, tu konkretnego protektora klucza BitLockera
HTML	HyperText Markup Language: format tekstowy stron WWW, tu używany jako format raportu GPO do przeglądania w przeglądarce
LSDOU	Local, Site, Domain, OU: kolejność czterech poziomów, w jakiej Windows stosuje kolejne GPO na komputerze
OU	Organizational Unit: folder w Active Directory grupujący konta i komputery
RSoP	Resultant Set of Policy: wynikowy zestaw ustawień, który faktycznie obowiązuje dany komputer albo konto po zsumowaniu wszystkich stosujących się polityk

Skrót	Co znaczy
USB	Universal Serial Bus: standard portów i urządzeń podłączanych do komputera, tu pendrive'y i inne nośniki wymienne
WMI	Windows Management Instrumentation: interfejs do odczytu stanu Windowsa
WMS	Warehouse Management System: system zarządzania magazynem

Fiszka

◫◫ ZMIENIA SYSTEM

Utworzenie nowego obiektu GPO: New-GPO

```
New-GPO -Name NazwaPolityki -Comment "OpisPolityki"
```

Tworzy w domenie nowy, pusty obiekt GPO, jeszcze nigdzie niepodłączony. Sama polityka bez linku do jednostki organizacyjnej albo domeny nie działa na żadnym komputerze, dopiero kolejny krok decyduje, gdzie zacznie obowiązywać.

Przykład:

```
DisplayName      : Mapowanie dyskow dzialow
DomainName       : ad.zielona.example
Owner            : ZIELONA\Domain Admins
Id               : 4f6a9b12-3c7d-4e21-9a58-1d2e3f4a5b6c
GpoStatus        : AllSettingsEnabled
CreationTime     : 28.09.2026 09:14:02
```

◫◫ **GPO** = Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery

◫◫ ZMIENIA SYSTEM

Powiązanie GPO z jednostką organizacyjną: New-GPLink

```
New-GPLink -Name NazwaPolityki -Target "OU=NazwaOU,DC=ad,DC=zielona,DC=example" -
LinkEnabled Yes
```

Podłącza istniejące GPO do wskazanej jednostki organizacyjnej, domeny albo lokacji, dopiero od tego momentu polityka zaczyna obowiązywać na kontach i komputerach leżących w tym miejscu drzewa katalogu. `-Target` przyjmuje pełny `DistinguishedName` celu, nie samą przyjazną nazwę.

Przykład:

```
DisplayName      GpoId                                Enabled  Enforced  Target
-----------      -----                                -------  --------  ------
Mapowanie...     4f6a9b12-3c7d-4e21-9a58-1d2e3f4a5b6c  True     False
OU=Magazyn,OU=Uzytkownicy,DC=ad,DC=zielona,DC=example
```

GPO = Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery · **OU** = Organizational Unit: folder w Active Directory grupujący konta i komputery · **DC** = Domain Controller: serwer, który trzyma Active Directory i loguje użytkowników

ZMIENIA SYSTEM

Filtrowanie zabezpieczeń: Set-GPPermission

```
Set-GPPermission -Name NazwaPolityki -TargetName NazwaGrupy -TargetType Group -
PermissionLevel GpoApply -Replace
```

Domyślnie prawo `Apply group policy` ma grupa `Authenticated Users`, czyli GPO obejmuje każdego w jednostce, do której je podłączymy. Filtrowanie zabezpieczeń zawęża zasięg do konkretnej grupy bez zakładania osobnej jednostki organizacyjnej tylko na potrzeby jednej polityki.

Przykład:

```
Trustee               TrusteeType  Permission
--------               -----------  ----------
ZIELONA\Magazyn-USB     Group        GpoApply
```

GPO = Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery

KLIKAMY W INTERFEJSIE

Dodanie filtra WMI do polityki: konsola GPMC

```
Group Policy Management → Forest: ad.zielona.example → Domains → ad.zielona.example
→ Group Policy Objects → NazwaPolityki
→ zakładka Scope → sekcja WMI Filtering → wybieramy filtr z listy
```

Filtr WMI dodatkowo zawęża zasięg GPO, tym razem nie po tożsamości konta czy komputera, tylko po jego stanie, na przykład systemie operacyjnym albo modelu sprzętu. Moduł `GroupPolicy` nie ma osobnego polecenia do przypięcia filtra WMI do istniejącej polityki, więc ten jeden krok wykonujemy w konsoli GPMC.

WMI = Windows Management Instrumentation: interfejs do odczytu stanu Windowsa · **GPMC** = Group Policy Management Console: konsola do zarządzania politykami GPO w domenie · **GPO** = Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery

TYLKO ODCZYT

Sprawdzenie dziedziczenia w jednostce: Get-GPInheritance

```
Get-GPInheritance -Target "OU=NazwaOU,DC=ad,DC=zielona,DC=example"
```

Pokazuje, które GPO są podłączone bezpośrednio do wskazanej jednostki, które dochodzą do niej z wyższych poziomów drzewa, i czy dziedziczenie z góry jest zablokowane. Pierwsze polecenie, które uruchamiamy, gdy trzeba ustalić, skąd konkretne ustawienie w ogóle wzięło się na danym komputerze.

Przykład:

```
ContainerName         : Magazyn
ContainerType         : OU
GpoInheritanceBlocked : No
GpoLinks              : {Blokada USB magazyn}
InheritedGpoLinks     : {Default Domain Policy, Mapowanie dyskow dzialow, Blokada USB
magazyn}
```

GPO = Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery · **OU** = Organizational Unit: folder w Active Directory grupujący konta i komputery · **DC** = Domain Controller: serwer, który trzyma Active Directory i loguje użytkowników

TYLKO ODCZYT

Wymuszenie natychmiastowego odświeżenia: gpupdate /force

```
gpupdate /force
```

Uruchamiamy lokalnie na komputerze, na który właśnie podłączyliśmy albo zmieniliśmy GPO, zamiast czekać do najbliższego automatycznego cyklu odświeżania w tle. `/force` dodatkowo każe zastosować wszystkie polityki od nowa, nawet te, które według Windowsa się nie zmieniły.

GPO = Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery · **gpupdate** = group policy update: wymuś odświeżenie GPO

TYLKO ODCZYT

Szybki podgląd zastosowanych polityk: gpresult /r

```
gpresult /r
```

Wypisuje w konsoli na bieżącym komputerze, które GPO faktycznie zostały zastosowane dla komputera i dla zalogowanego użytkownika, a które zostały odfiltrowane i dlaczego. Wygodne do szybkiego sprawdzenia na miejscu, bez generowania osobnego pliku.

Przykład:

```
COMPUTER SETTINGS
------------------
    Applied Group Policy Objects
    -----------------------------
        Default Domain Policy
        Blokada USB magazyn

    The following GPOs were not applied because they were filtered out
    -------------------------------------------------------------------
        Mapowanie dyskow dzialow
            Filtering:  Denied (Security)
```

GPO = Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery · **gpresult** = group policy result: które GPO trafiły na komputer

TYLKO ODCZYT

Pełny raport HTML dla jednego komputera: gpresult /h

```
gpresult /h C:\Audyty\raport-komputer.html
```

Zapisuje ten sam wynik co `gpresult /r`, ale jako czytelny plik HTML z podziałem na sekcje, wygodny do wysłania mailem albo dołączenia do zgłoszenia. Przy audycie wielu polityk naraz w całej domenie korzystamy zamiast tego z `Get-GPOReport -All`, opisanego na stronie Skrypty audytowe Active Directory.

HTML = HyperText Markup Language: format tekstowy stron WWW, tu używany jako format raportu GPO do przeglądania w przeglądarce · **gpresult** = group policy result: które GPO trafiły na komputer

TYLKO ODCZYT

Kopia zapasowa wszystkich GPO: Backup-GPO

```
Backup-GPO -All -Path SciezkaKopii
```

Zapisuje kompletną kopię każdego GPO w domenie do wskazanego katalogu, każde jako osobny podfolder nazwany identyfikatorem GUID. Uruchamiamy cyklicznie, najlepiej z harmonogramu zadań, zanim ktoś przez pomyłkę zmieni albo usunie politykę, której nikt świadomie nie planował ruszać.

GPO = Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery · **GUID** = Globally Unique Identifier: unikalny w skali globalnej identyfikator obiektu, tu konkretnego protektora klucza BitLockera

ZMIENIA SYSTEM

Przywrócenie GPO z kopii: Restore-GPO

```
Restore-GPO -Name NazwaPolityki -Path SciezkaKopii
```

Przywraca GPO do stanu zapisanego w kopii, identyfikując je po nazwie zapisanej w folderze kopii, nie po treści ustawień. Jeśli polityka o tej nazwie już istnieje, jej bieżące ustawienia zostają nadpisane zawartością kopii, więc przed przywróceniem warto sprawdzić, z którego dnia pochodzi kopia w `SciezkaKopii`.

GPO = Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery

Z życia wzięte

Z ŻYCIA WZIĘTE

Tomek dostaje zadanie zablokowania portów USB na komputerach w magazynie w Swarzędzu, żeby nikt nie kopiował danych WMS na pendrive. Podłącza nowe GPO wprost do domeny zamiast do jednostki organizacyjnej magazynu, bo z listy jednostek w konsoli szybciej trafić od razu w korzeń drzewa. Po południu dzwoni pani Halina: jej mysz USB w księgowości przestała działać, a razem z nią cała reszta portów USB w biurze.

Jak to działa

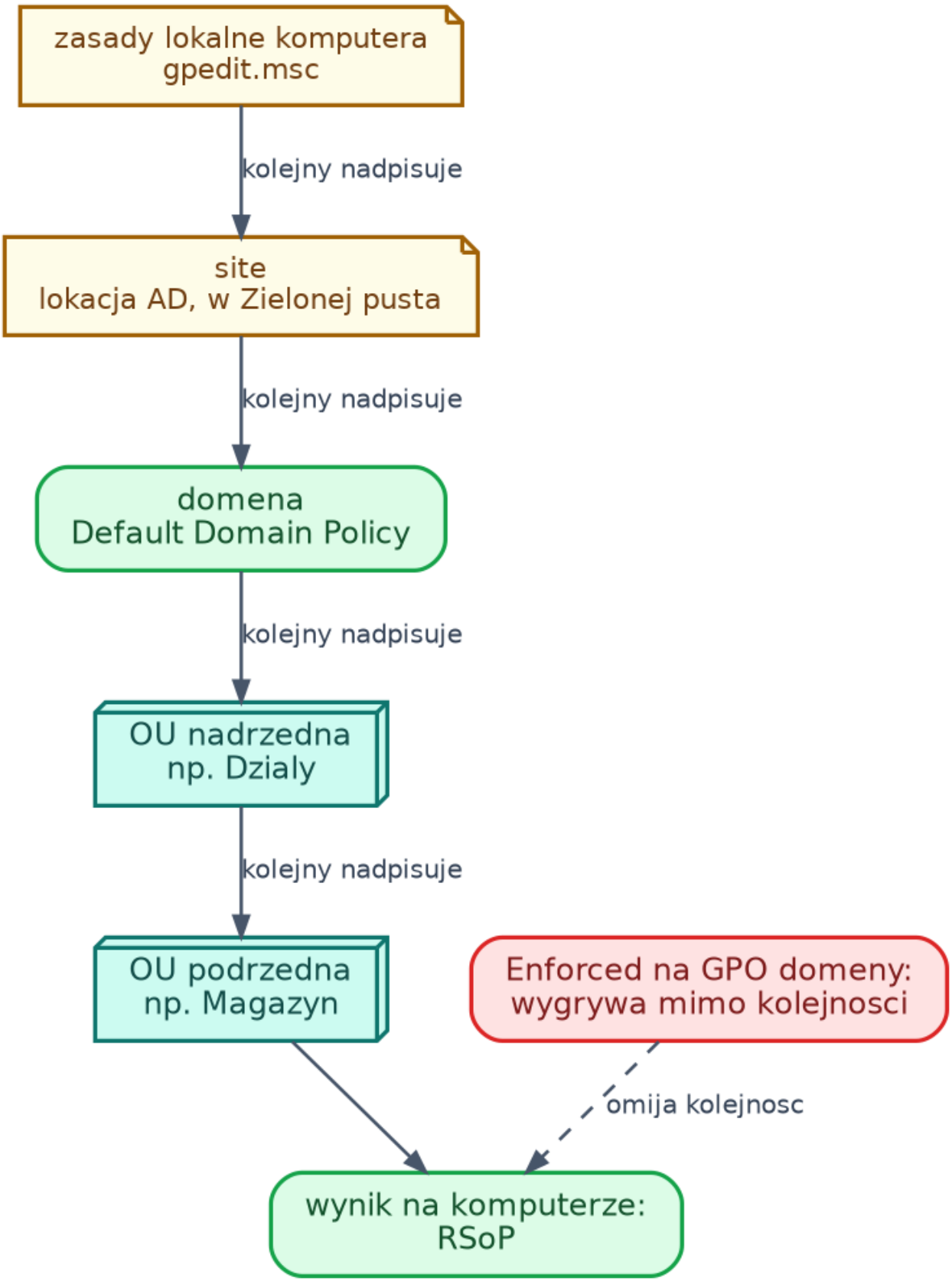
Rozwiń: jak to działa pod spodem

Pojęcie: konfiguracja komputera kontra konfiguracja użytkownika. Każde GPO ma dwie osobne gałęzie ustawień. Konfiguracja komputera stosuje się przy starcie systemu, niezależnie od tego, kto się później zaloguje, konfiguracja użytkownika przy logowaniu, niezależnie od tego, na jakim komputerze dana osoba akurat pracuje.

Pojęcie: zasady kontra preferencje. Zasady (Policies) są wymuszone: użytkownik widzi zablokowaną opcję albo w ogóle jej nie widzi. Preferencje (Preferences) ustawiają tylko wartość domyślną, którą użytkownik może później samodzielnie zmienić, GPO tylko nie pilnuje, żeby została zmieniona z powrotem.

Pojęcie: kolejność LSDOU. Skrót od czterech poziomów, na których GPO może być podłączone: Local (zasady lokalne komputera), Site (lokacja Active Directory), Domain (cała domena) i OU (jednostka organizacyjna, licząc od najwyższej do tej, w której faktycznie stoi obiekt). Ustawienia z każdego kolejnego poziomu nadpisują to samo ustawienie z poziomu wcześniejszego.

Zanim GPO dotrze do konkretnego komputera, przechodzi przez cztery poziomy, jeden po drugim, w stałej kolejności.


zasady lokalne komputera
gpedit.msc
kolejny nadpisuje
site
lokacja AD, w Zielonej pusta
kolejny nadpisuje
domena
Default Domain Policy
kolejny nadpisuje
OU nadrzedna
np. Dzialy
kolejny nadpisuje
OU podrzedna
np. Magazyn
Enforced na GPO domeny:
wygrywa mimo kolejnosci
omija kolejnosc
wynik na komputerze:
RSoP

Kolejnosc LSDOU: lokalny, site, domena, OU nadrzedna, OU podrzedna, kazdy kolejny nadpisuje wczesniejszy, Enforced omija te kolejnosc (kliknięcie otwiera pełny rozmiar)

Wynik tego całego przejścia to RSoP, czyli wynikowy zestaw ustawień faktycznie zastosowanych na komputerze po zsumowaniu i nadpisaniu kolejnych poziomów. Enforced na dowolnym poziomie wyżej w drzewie wygrywa z tym samym ustawieniem niżej, nawet jeśli niższy poziom normalnie miałby pierwszeństwo według LSDOU, i nawet jeśli po drodze stoi Block Inheritance.

Pojęcie: Enforced i Block Inheritance. Enforced na linku GPO sprawia, że jego ustawienia zawsze wygrywają z tymi samymi ustawieniami niżej w drzewie, niezależnie od zwykłej kolejności LSDOU. Block Inheritance na jednostce organizacyjnej odcina napływ polityk z wyższych poziomów, ale nie działa na te z ustawionym Enforced, bo Enforced ma pierwszeństwo przed blokadą.

Pojęcie: filtrowanie zabezpieczeń i filtrowanie WMI. Oba zawężają zasięg GPO poniżej poziomu jednostki organizacyjnej, do której jest podłączone, ale po różnych kryteriach. Filtrowanie zabezpieczeń (`Set-GPPermission`) patrzy na tożsamość konta albo komputera, filtrowanie WMI patrzy na jego stan, na przykład system operacyjny albo obecność konkretnej usługi.

Pojęcie: loopback processing. Tryb, w którym na danym komputerze konfiguracja użytkownika z GPO podłączonych do tego komputera zastępuje albo łączy się z konfiguracją użytkownika z GPO podłączonych do konta, które się na nim loguje. Przydatny tam, gdzie liczy się to, na jakim komputerze ktoś pracuje, a nie kim jest, na przykład na `rds01`, żeby każdy handlowiec dostawał tam ten sam, ujednolicony pulpit, niezależnie od własnych ustawień z komputera biurowego.

Pojęcie: Central Store dla szablonów ADMX. Wspólny folder w `SYSVOL`, z którego wszystkie kontrolery domeny i konsole GPMC czytają te same szablony administracyjne (pliki ADMX i językowe ADML), zamiast każdy z lokalnej kopii na swoim dysku. Bez Central Store nowsza wersja szablonu skopiowana tylko na jeden kontroler powoduje, że różne osoby edytujące GPO widzą różny zestaw dostępnych ustawień.

Przykładowe GPO w Zielonej

Polityka	Co robi	Gdzie podłączona	Kluczowe ustawienie

Mapowanie dysków działów	podłącza litery dysków do folderów przestrzeni nazw DFS `\\ad.zielona.example\pliki\NazwaUdzialu` (cele leżą na `fs01`, strona fs01 od środka: maszyna na hvclu01, wolumeny, udziały działów i przestrzeń nazw DFS), osobno dla każdego działu	OU Uzytkownicy i jej jednostki podrzędne	Preferencje, mapowanie dysków po grupie działu
Blokada USB w magazynie	wyłącza magazyny wymienne USB na komputerach obsługujących WMS	OU Magazyn	Konfiguracja komputera, Removable Storage Access
Tapeta i wygaszacz z blokadą	ustawia firmową tapetę i wygaszacz ekranu z wymuszonym hasłem po powrocie	domena, dotyczy wszystkich	Konfiguracja użytkownika, Personalization

Częste błędy

Objaw	Przyczyna	Co robimy
Zmiana w GPO nie jest widoczna na komputerze mimo poprawnego linku	GPO nie zdążyło się jeszcze odświeżyć, domyślny cykl w tle trwa do 90 minut	uruchamiamy `gpupdate /force` na komputerze i sprawdzamy wynik przez `gpresult /r`
Polityka działa na całej domenie zamiast tylko na jednej jednostce	`New-GPLink` podłączył GPO do korzenia domeny zamiast do konkretnej OU	usuwamy zły link i tworzymy nowy, z poprawną wartością `-Target`
`Set-GPPermission -Replace` odbiera dostęp wszystkim, GPO przestaje działać dla kogokolwiek	domyślne uprawnienie `GpoApply` dla `Authenticated Users` zostało usunięte bez dodania właściwej grupy zamiennej	dodajemy grupę docelową z `GpoApply` , `-Replace` ma sens tylko wtedy, gdy wiemy dokładnie, kto ma zostać
`Get-GPInheritance` pokazuje `GpoInheritanceBlocked : Yes`, a polityka z wyższego poziomu i tak działa	GPO wyżej w drzewie ma ustawione Enforced, które ignoruje Block Inheritance niżej	sprawdzamy w GPMC kolumnę Enforced przy linkach wyżej, Enforced zawsze wygrywa z blokadą dziedziczenia
`Restore-GPO` zwraca błąd, że nie znajduje kopii	`-Path` wskazuje inny folder niż użyty w `Backup-GPO`, albo kopia dotyczy GPO o innej nazwie	sprawdzamy zawartość folderu kopii, poszczególne kopie rozpoznajemy po podfolderach z GUID, nie po nazwie widocznej na pierwszy rzut oka

Ćwiczenia

1. Dlaczego GPO blokujące USB, podłączone przez pomyłkę do domeny zamiast do OU Magazyn, zablokowało też mysz pani Haliny w księgowości, skoro obie jednostki są zupełnie różne?

Odpowiedź

Zgodnie z kolejnością LSDOU link na poziomie domeny obejmuje wszystkie jednostki organizacyjne leżące niżej w drzewie, w tym księgowość, chyba że po drodze ktoś zablokuje dziedziczenie albo inna polityka niżej nadpisze to samo ustawienie. Podłączenie do domeny zamiast do konkretnej OU rozciąga zasięg polityki na całą firmę, nie tylko na zamierzony dział.

1. Dwie polityki, jedna mapująca dyski działów a druga blokująca USB, są podłączone do tej samej jednostki Magazyn, każda z innym numerem kolejności widocznym w `Get-GPInheritance`. Która wygra przy konflikcie tego samego ustawienia?

Odpowiedź

Niższy numer kolejności linku oznacza wyższy priorytet i to ta polityka wygrywa przy konflikcie tego samego ustawienia, o ile żadna z nich nie ma ustawionego Enforced wyżej w drzewie. Kolejność linków w obrębie jednej jednostki organizacyjnej liczy się osobno od kolejności LSDOU między poziomami Local, Site, Domain i OU.

1. Dlaczego audyt wszystkich GPO w Zielonej, opisany na stronie o migracji do Intune, korzysta z `Get-GPOReport -All` zamiast z `gpresult /h` uruchamianego na każdym komputerze po kolei?

Odpowiedź

`gpresult /h` pokazuje, które GPO zostały zastosowane na jednym, konkretnym komputerze, więc do audytu całej domeny trzeba by je uruchomić na każdym komputerze z osobna. `Get-GPOReport -All` eksportuje od razu treść wszystkich polityk istniejących w domenie do jednego raportu, gotowego do przeczytania i przedyskutowania z zespołem, bez względu na to, gdzie akurat są zastosowane. Pełny opis tej metody i planu migracji fala po fali stoi na stronie Intune obok domeny: audyt GPO i plan migracji, tu zajmujemy się tworzeniem i diagnostyką GPO, nie ich audytem.

Powiązane: Intune obok domeny: audyt GPO i plan migracji · Skrypty audytowe Active Directory · DHCP: adresy dla biura i magazynu z przełączaniem awaryjnym · Zasady haseł i blokady konta: polityka domeny i PSO

Źródła: New-GPO · New-GPLink · Set-GPPermission · Get-GPInheritance · Backup-GPO · Backup, restore, migrate, and copy Group Policy Objects · `Get-Help Restore-GPO` · `Get-Help gpresult`

Revision #30
Created 2026-09-28 09:24:33 UTC by Tomasz Konieczny
Updated 2026-10-26 14:26:28 UTC by Tomasz Konieczny