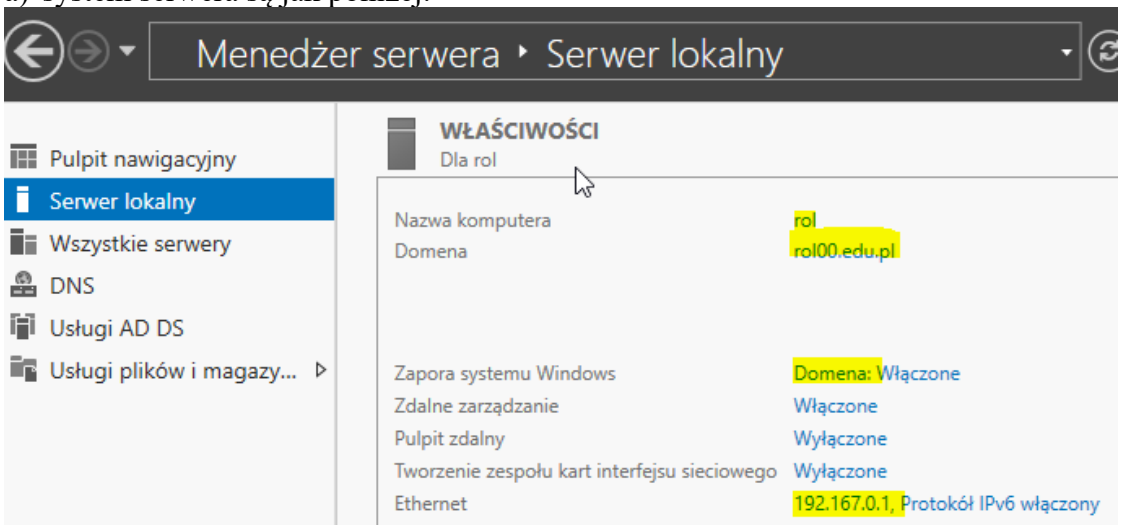
12.5 Zarządzanie zasadami grup w domenie

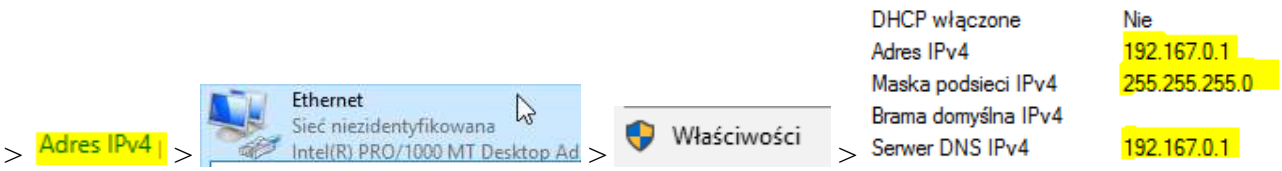
Cel ogólny lekcji: Nauczyć się projektować, wdrażać i analizować zasady grup w domenie Active Directory, z uwzględnieniem struktury organizacyjnej, delegowania uprawnień oraz modelowania wpływu zasad na użytkowników i komputery.

Cele szczegółowe lekcji:

1. Zarządzanie obiektami w domenie za pomocą ADAC, analiza skryptów PowerShell generowanych przez operacje w GUI oraz wykorzystanie Kosza AD do przywracania i trwałego usuwania obiektów.
2. Utworzyć jednostkę organizacyjną i przypisać do niej obiekty komputerowe oraz globalną grupę zabezpieczeń.
3. Skonfigurować obiekt zasad grupy w celu ograniczenia dostępu do edytora rejestru i ustawienia tapety pulpitu.
4. Włączyć przetwarzanie zasad w sprzężeniu zwrotnym w trybie Replace i zrozumieć jego wpływ na użytkownika.
5. Przyłączyć obiekt zasad grupy do jednostki organizacyjnej i zastosować delegowanie uprawnień z odmową stosowania zasad.
6. Przeanalizować konflikt zasad między poziomem domeny a jednostką organizacyjną oraz sposoby jego rozwiązania.
7. Skorzystać z narzędzia Group Policy Modeling Wizard do symulacji działania zasad dla konkretnego użytkownika i komputera.
8. Zrozumieć różnice między trybem Replace a Merge w modelowaniu zasad oraz ich zastosowanie w praktyce.
9. Przeprowadzić aktualizację zasad grupy i ocenić ich skuteczność na podstawie wynikowego zestawu zasad (RSoP).

Przed przystąpieniem do ćwiczenia sprawdź i ustaw:
W Menedżer funkcji Hyper-V wybierz nazwa maszynę wirtualna twojej grupy _dc2019
Upewnij się, że punk kontrolny, zawiera serwer z zainstalowanym kontrolerem domeny.
Uruchom maszynę > Ctrl+Delete > Administrator > zaq1@WSX
a) system serwera są jak poniżej:





Jeśli pracujesz w VirtualBox utwórz migawkę stanu systemu serwera o nazwie DDMM_numer

b) systemu klienta są jak poniżej:

W zeszycie opisz procedury tworzenie zasad grup w domenie.

zgłoszenie Zadanie 1 – ADAC + PowerShell + Kosz AD

Część A – Tworzenie obiektów w ADAC

1. Otwórz Centrum administracyjne usługi Active Directory (ADAC).

Na serwerze otwórz Server Manager > Narzędzia > Centrum administracyjne usługi Active Directory.

Alternatywnie: w Uruchom wpisz dsac.exe.

2. Utwórz w domenie dwie jednostki organizacyjne (OU): Salaszkoleniowa, Salaszkoleniowa2

- W lewym panelu wybierz domenę.
- Włącz funkcje Kosz…> OK
- Kliknij Nowy > Jednostka organizacyjna.
- Nazwy:
  - Salaszkoleniowa > OK
  - Salaszkoleniowa2
- Zaznacz opcję Chroń przed przypadkowym usunięciem.

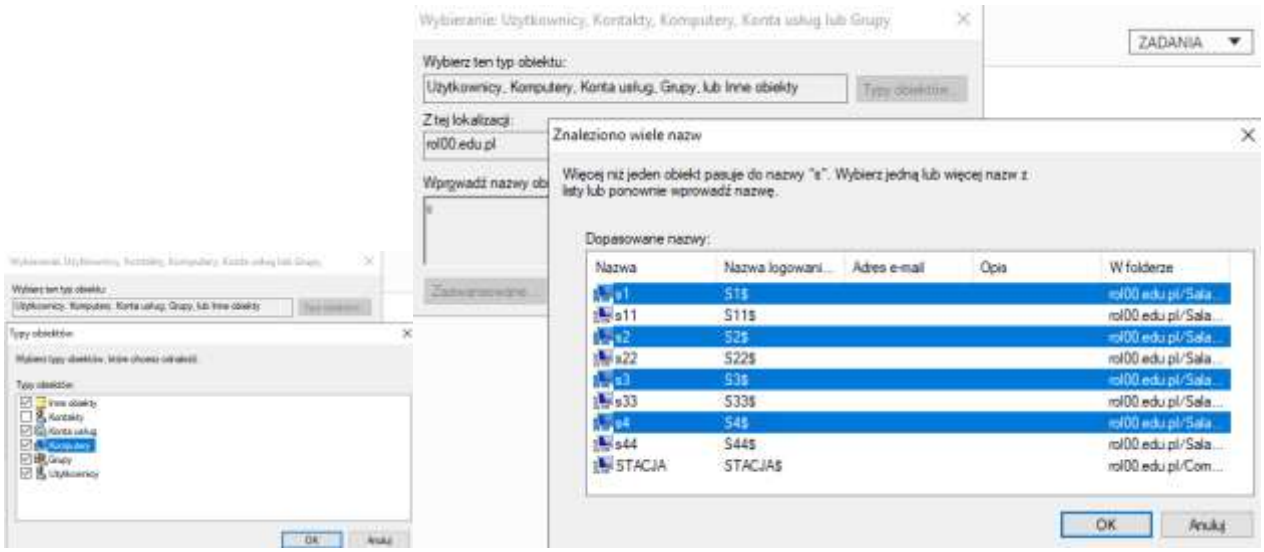
3. W OU **Salaszkoleniowa** dodaj komputery: s1, s2, s3, s4

- W OU Salaszkoleniowa:
  - Kliknij Nowy > Komputer.
  - Nazwy: s1, s2, s3, s4.

4. W OU **Salaszkoleniowa2** dodaj komputery: s11, s22, s33, s44

- W OU Salaszkoleniowa2:
  - Kliknij Nowy > Komputer.
  - Nazwy: s11, s22, s33, s44.

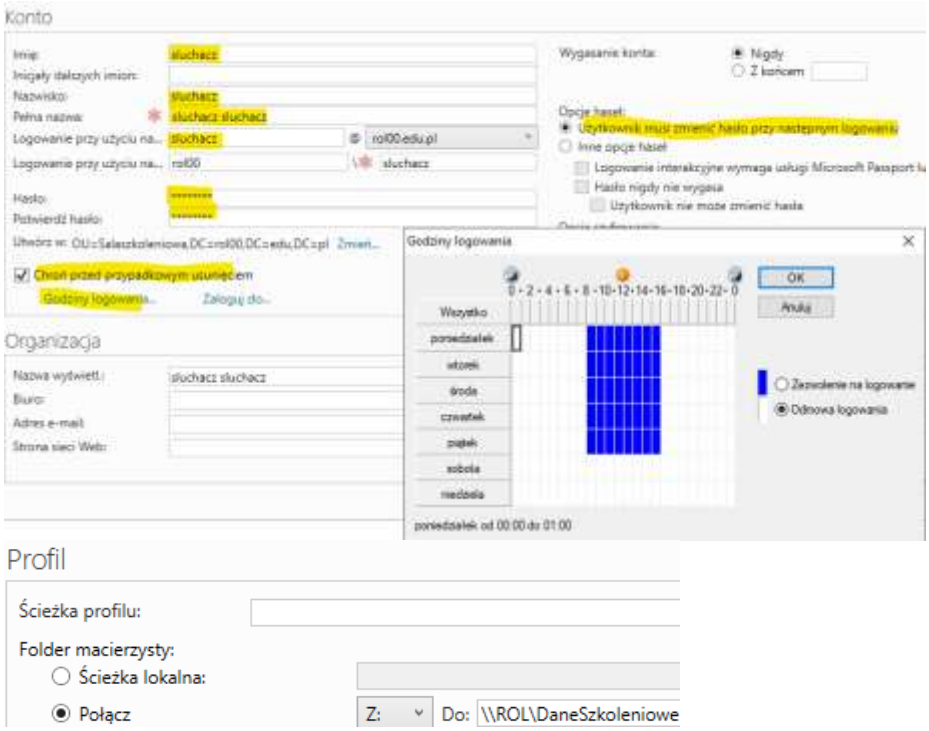
5. Utwórz globalne grupy zabezpieczeń:
   - W OU Salaszkoleniowa: Kompszkolenie i dodaj do niej komputery s1 – s4.
     - Nowy > Grupa.
     - Nazwa: Kompszkolenie.
     - Typ: Zabezpieczeń, Zakres: Globalna.
     - Dodaj komputery s1–s4 jako członków.



   - W OU Salaszkoleniowa2: Kompszkolenie2 i dodaj do niej komputery s11 – s44.
     - Nowy > Grupa.
     - Nazwa: Kompszkolenie2.
     - Typ: Zabezpieczeń, Zakres: Globalna.
     - Dodaj komputery s11–s44.
6. Dodaj konta użytkowników w OU Salaszkoleniowa:
   - Nowy > Użytkownik.
   - sluchacz (będzie używany w dalszych ćwiczeniach)
   - test (konto do usunięcia)

   Ustaw dla nich:
   - Hasło (np. zaq1@WSX)
   - Wymuszenie zmiany hasła przy pierwszym logowaniu: Tak
   - Godziny logowania: 08:00–16:00 poniedziałek - piątek (zakładka Konto > Godziny logowania).
   - Mapowanie dysku sieciowego. Zakładka Profil:

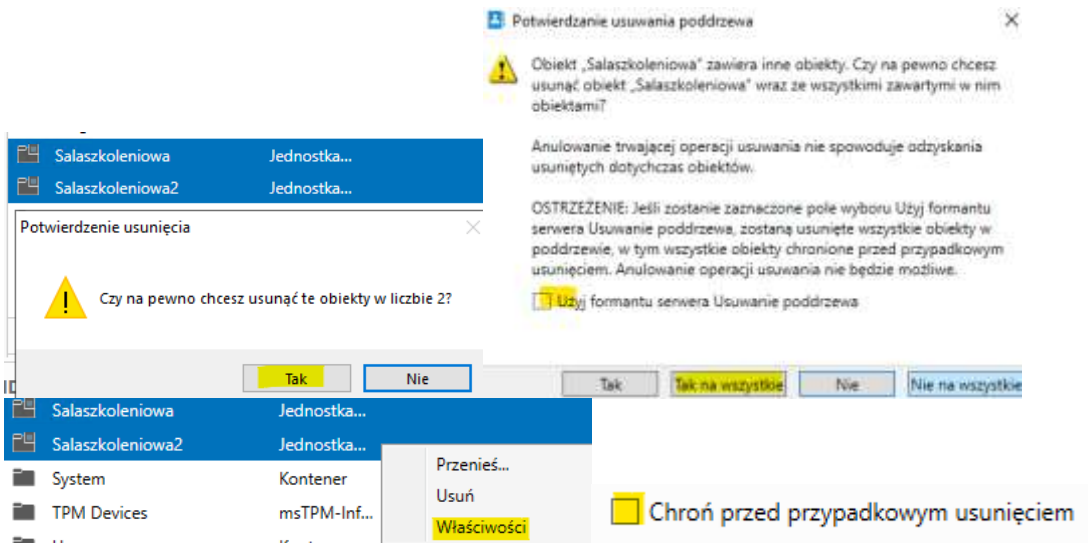
- Folder domowy: Ścieżka UNC > \\ROL\DaneSzkoleniowe.
- Litera dysku: Z:.



7. Sprawdź w ADAC na dole zakładkę **Historia Środowiska Windows PowerShell**, aby zobaczyć polecenia wygenerowane podczas tworzenia i modyfikacji obiektów (New-ADOrganizationalUnit, New-ADComputer, New-ADGroup, Add-ADGroupMember, New-ADUser, Set-ADUser).

Część B – Usuwanie i Kosz AD

1. Usuń wszystkie obiekty utworzone w części A (OU, komputery, grupy, użytkownicy) > **Usuń**.



> Powtórz usunięcie

2. Sprawdź w Koszu AD (Deleted Objects), czy obiekty są dostępne do przywrócenia.

- W lewym panelu wybierz Kosz AD jest dostępny – w polskim ADAC jest oznaczony jako „Deleted Objects” (kontener w domenie rol00). To właśnie tam trafiają wszystkie usunięte obiekty, jeśli funkcja Kosza jest włączona.
- Zobacz wszystkie usunięte obiekty.

3. Przywróć tylko: Salaszkoleniowa, s1, s2, s3, s4, Kompszkolenie, sluchacz

4. Trwale usuń pozostałe obiekty z Kosza AD (Permanent Delete): Salaszkoleniowa2, s11, s22, s33, s44, Kompszkolenie2, test

- Kliknij Delete (To jest odpowiednik „Permanent Delete” w angielskiej wersji).

5. Sprawdź w ADAC na dole zakładkę **Historia Środowiska Windows PowerShell** skrypty dla operacji usuwania i przywracania (Restore-ADObject, Remove-ADObject).

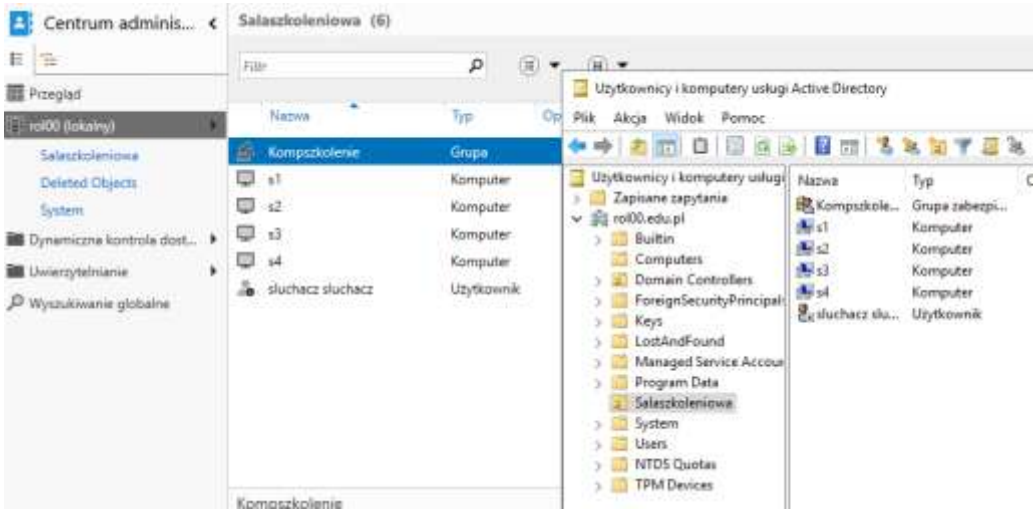
Efekt końcowy

W domenie pozostają tylko: OU: Salaszkoleniowa, Komputery: s1, s2, s3, s4, Grupa: Kompszkolenie, Użytkownik: słuchacz.

Wszystkie dodatkowe obiekty (Salaszkoleniowa2, s11–s44, Kompszkolenie2, test) są trwale usunięte.

Jeśli opcja Usuń (czyli Permanent Delete) jest wyszarzona to zapoznaj się z przyczynami poniżej. Najczęstsze przyczyny Powody, dla których jest nieaktywna w ADAC:

1. Brak uprawnień
   - Musisz być zalogowany jako Enterprise Admin lub Domain Admin.
   - Konto z ograniczonymi uprawnieniami nie może trwale usuwać obiektów.
2. Zaznaczone obiekty są chronione
   - Jeśli obiekty mają włączoną opcję Chroń przed przypadkowym usunięciem, ADAC blokuje trwałe usunięcie.
   - Sprawdź w Właściwościach obiektu > Zakładka „Obiekt” > Odznacz „Chroń przed przypadkowym usunięciem”.
3. Widok ADAC nie odświeżył się
   - Po włączeniu Kosza lub zmianie uprawnień czasem trzeba zamknąć i ponownie otworzyć ADAC.
4. Obiekty są w stanie „soft delete”
   - Jeśli obiekt jest w Koszu, ale ma zależności (np. linki do innych obiektów), ADAC może blokować trwałe usunięcie do czasu ich usunięcia. Zgłoś efekt końcowy:



Zgłoszenie 1

Zadanie 2

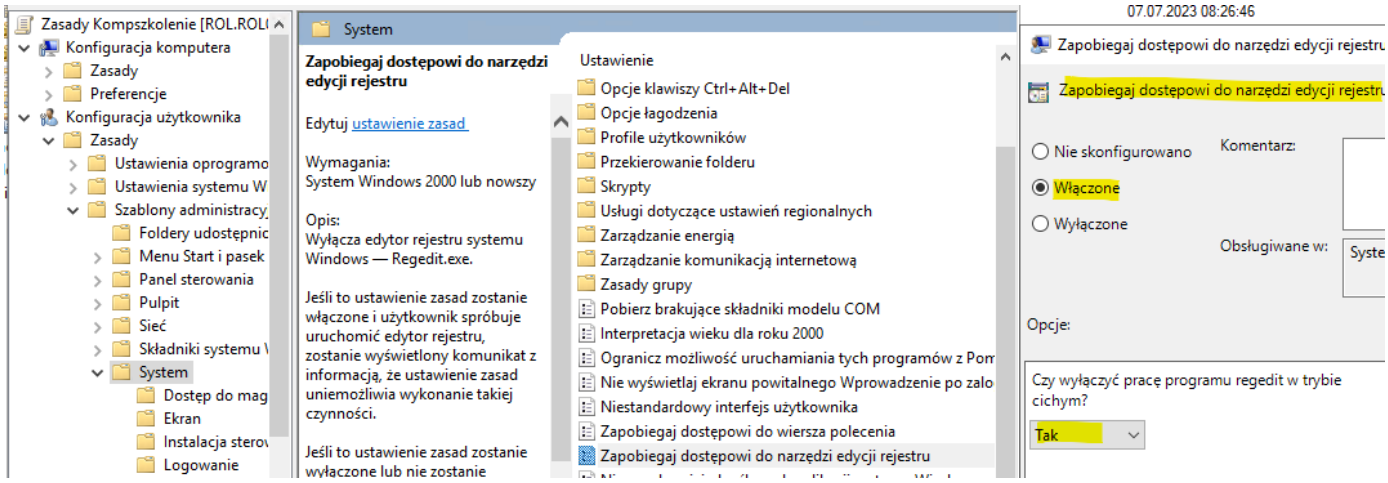
Utwórz obiekt zasad grupy o nazwie Kompszkolenie.

W tym obiekcie zasad grupy włącz ustawienie, które uniemożliwia dostęp do narzędzi edycyjnych rejestru i skonfigurowanie standardowej tapety pulpitu. Oba te ustawienia są w ustawieniach konfiguracji użytkownika w węźle Administrative Templates (Szablony administracyjne).

Wskazówki: Konfiguracja ustawień w GPO

1. Kliknij prawym przyciskiem na GPO Kompszkolenie > Edytuj.
2. W edytorze przejdź do: Konfiguracja użytkownika > Szablony administracyjne > System

o Znajdź ustawienie: Zapobiegaj dostępowi do narzędzi edycyjnych rejestru (Prevent access to registry editing tools) > Włącz.



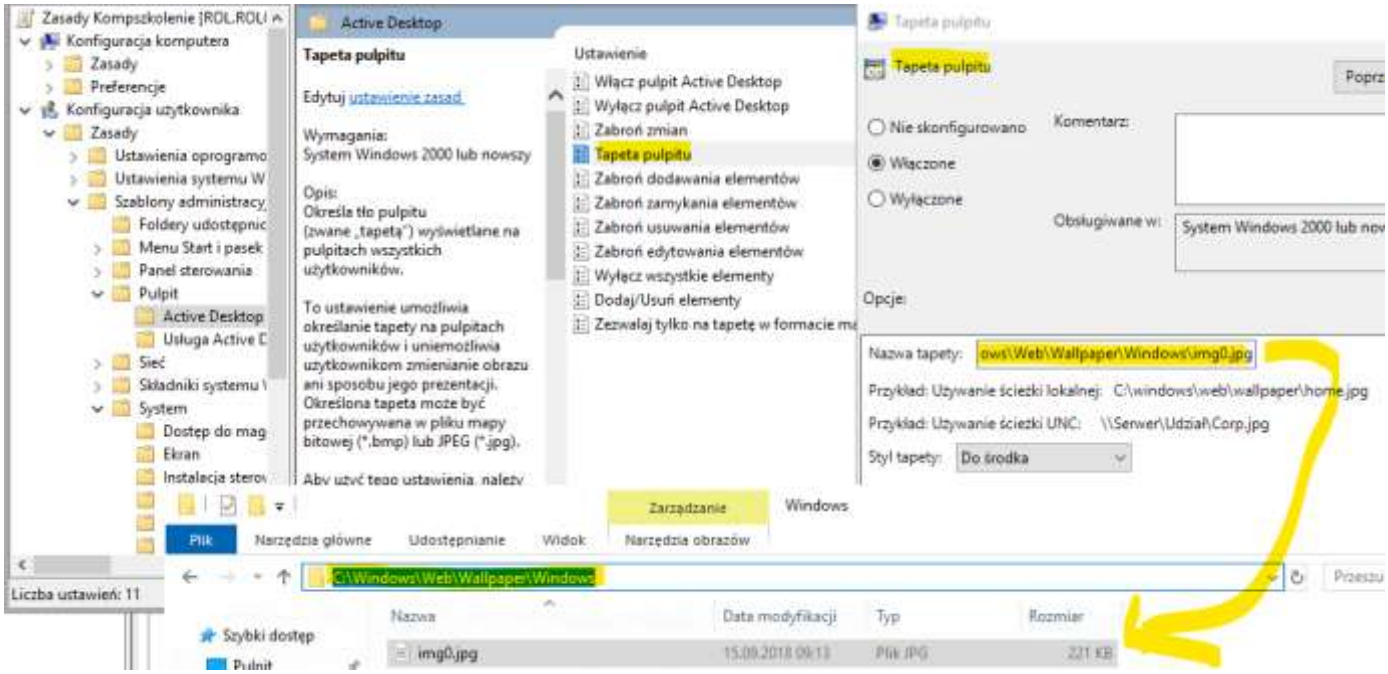
Następnie przejdź do:

Konfiguracja użytkownika > Szablony administracyjne > Pulpit > Pulpit

- Znajdź ustawienie: Tapeta pulpitu (Desktop Wallpaper)

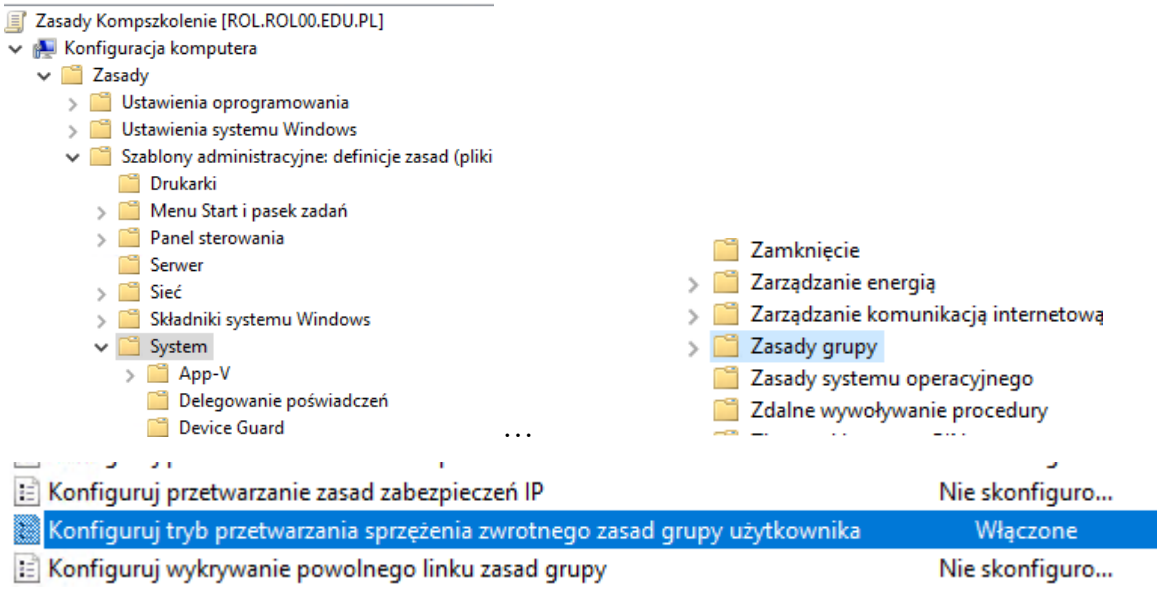
  Włącz.

- Podaj ścieżkę do pliku tapety, np.:
  C:\Windows\Web\Wallpaper\Windows\img0.jpg
- Ustaw tryb: Do środka.



Aby pomóc sobie w znalezieniu tych ustawień można przefiltrować ustawienia korzystając ze słów kluczowych.

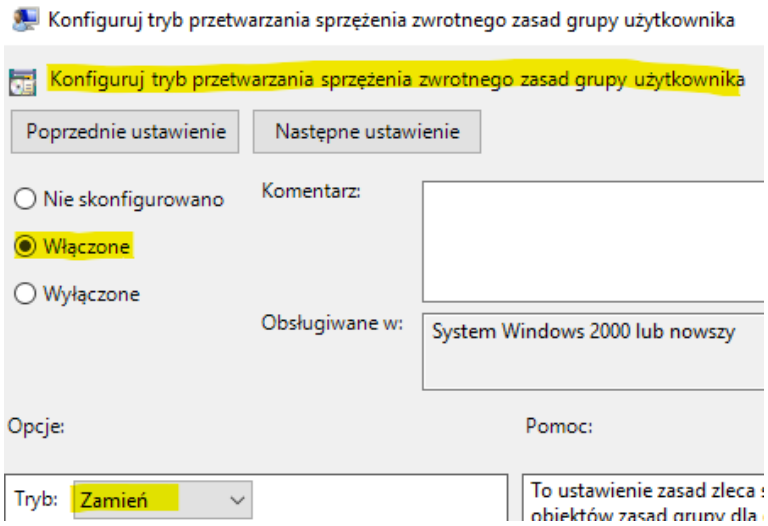
W węźle Computer Configuration (Konfiguracja komputera) znajdź ustawienie szablonów administracyjnych, które umożliwia przetwarzanie zasad w sprzężeniu zwrotnym. Włącz to ustawienie i wybierz implementację przetwarzania w sprzężeniu zwrotnym w trybie Replace (Zamień). Wskazówki: Konfiguruj tryb przetwarzania sprzężenia zwrotnego zasad grupy użytkownika.



Jak ustawić:

1. Kliknij dwukrotnie Konfiguruj tryb przetwarzania sprzężenia zwrotnego zasad grupy użytkownika.
2. Zaznacz Włączone.
3. W polu Tryb wybierz:

   Zamień
4. Kliknij OK i zamknij edytor.

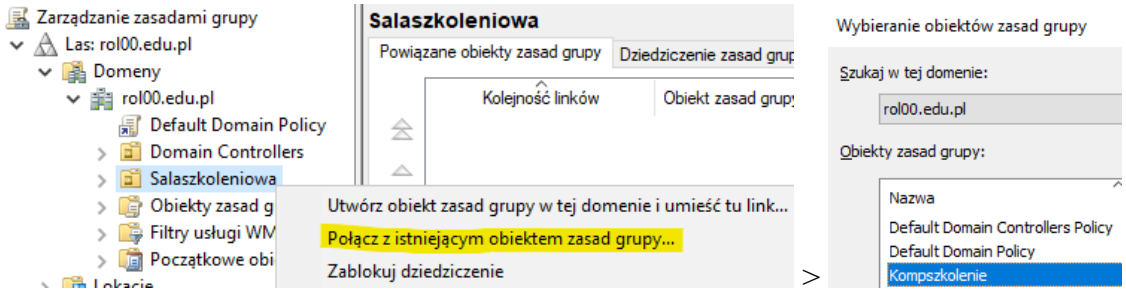


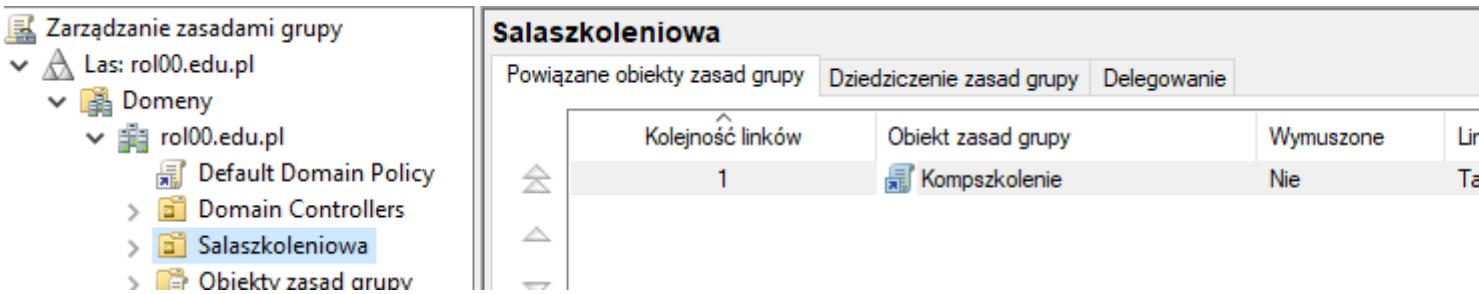
zgłoszenie 2

Zadanie 3

Przyłączyć obiekt zasad grupy Kompszkolenie do jednostki organizacyjnej Salaszkoleniowa.

Wskazówki:





zgłoszenie Zadanie 3a - Konflikt zasad (w zeszycie zapisz odpowiedzi na pytania):

Odpowiedzi na pytania dotyczące konfliktu zasad w Active Directory:

a. Co się stanie, jeśli zasada z OU „Salaszkoleniowa” koliduje z zasadą z poziomu domeny?
Jeżeli w Active Directory występuje konflikt ustawień pomiędzy zasadą GPO przypisaną do domeny a zasadą przypisaną do jednostki organizacyjnej (OU), to obie zasady są przetwarzane, ale w przypadku sprzecznych ustawień zostanie zastosowana ta, która ma wyższy priorytet w kolejności przetwarzania GPO.
b. Która zasada ma pierwszeństwo?
Kolejność przetwarzania zasad GPO jest następująca (od najniższego do najwyższego priorytetu):
1. Local Group Policy (zasady lokalne na komputerze)
2. Site (jeśli jest skonfigurowane)
3. Domain (zasady przypisane do domeny)
4. Organizational Unit (OU) – od najwyższego poziomu OU do najniższego (najbardziej szczegółowego)

> Największe pierwszeństwo ma zasada przypisana do najniższego poziomu OU, czyli w tym przypadku zasada z OU „Salaszkoleniowa” nadpisze ustawienia z poziomu domeny, jeśli dotyczą tych samych parametrów.
c. Jak można rozwiązać taki konflikt?
Możliwe sposoby:
- Zmiana kolejności linkowania GPO – w konsoli Group Policy Management można ustawić priorytet (Link Order).
- Wykorzystanie opcji „Enforce” – wymusza stosowanie danej zasady nawet w przypadku zasad z niższych poziomów.
- Blokowanie dziedziczenia (Block Inheritance) – na poziomie OU można zablokować dziedziczenie zasad z wyższych poziomów.
- Filtrowanie za pomocą Security Filtering lub WMI Filtering – aby zasada dotyczyła tylko określonych komputerów lub użytkowników.
- Projektowanie zasad tak, aby nie były sprzeczne – np. rozdzielenie ustawień na różne GPO.

zgłoszenie 3

Zadanie 4

Utworzyłeś w zadaniu poprzednim **12.3**, obiekt zasad grupy ROL00, skonfigurowałeś go na implementację ustawień zasad dla wygaszacza ekranu, jeśli nie masz już tego obiektu zasad grupy, wykonaj to zadanie.
Wskazówki:
Sprawdz czy moduł GroupPolicy jest zainstalowany?
Uruchom PowerShell jako Administrator i wykonaj
sprawdzenie dostępność modułu

```
Get-Module -ListAvailable GroupPolicy
```

(opcjonalnie) Załaduj moduł do bieżącej sesji

```
Import-Module GroupPolicy
```

Sprawdź, jakie cmdlety są w module

```
Get-Command -Module GroupPolicy
```

Windows Server (2016/2019/2022)

Moduł GroupPolicy instaluje się razem z Group Policy Management (GPMC).

Instalacja przez PowerShell:

Uruchom jako Administrator

```
Install-WindowsFeature GPMC
```

Po instalacji (czasem wymagany restart)

```
Import-Module GroupPolicy
```

Get-Module -ListAvailable GroupPolicy

Uwaga: na serwerze będącym kontrolerem domeny GPMC często jest już dostępne. Jeśli nie — polecenie powyżej doinstaluje konsolę oraz moduł.

W Windows Server (z zainstalowanym modułem **GroupPolicy**) możesz skonfigurować ustawienia GPO dla wygaszacza ekranu za pomocą cmdletów:

```
# Nazwa GPO
$GPOName = "ROL00"
# Utwórz GPO, jeśli nie istnieje
if (-not (Get-GPO -Name $GPOName -ErrorAction SilentlyContinue)) {
    New-GPO -Name $GPOName
}
# Ścieżka do ustawień wygaszacza ekranu (User Configuration)
$ScreenSaverPath = "User Configuration\Policies\Administrative Templates\Control Panel\Personalization"
# Włącz wygaszacz ekranu
Set-GPRegistryValue -Name $GPOName -Key "HKCU\Software\Policies\Microsoft\Windows\Control Panel\Desktop" -ValueName "ScreenSaveActive" -Type String -Value "1"
# Ustaw czas bezczynności (np. 600 sekund = 10 minut)
Set-GPRegistryValue -Name $GPOName -Key "HKCU\Software\Policies\Microsoft\Windows\Control Panel\Desktop" -ValueName "ScreenSaveTimeOut" -Type String -Value "600"
```

```
# Włącz blokadę po wygaszaczu
Set-GPRegistryValue -Name $GPOName -Key
"HKCU\Software\Policies\Microsoft\Windows\Control Panel\Desktop" -ValueName
"ScreenSaverIsSecure" -Type String -Value "1"
# Opcjonalnie ustaw konkretny wygaszacz (np. scrnsave.scr)
Set-GPRegistryValue -Name $GPOName -Key
"HKCU\Software\Policies\Microsoft\Windows\Control Panel\Desktop" -ValueName
"SCRNSAVE.EXE" -Type String -Value "C:\Windows\System32\scrnsave.scr"
```

Set-GPRegistryValue ustawia wartości w rejestrze w ramach GPO.

Klucz HKCU\Software\Policies\Microsoft\Windows\Control Panel\Desktop odpowiada za ustawienia wygaszacza ekranu.

Po skonfigurowaniu GPO należy połączyć je z OU „Salaszkoleniowa”:

```
New-GPLink -Name $GPOName -Target
"OU=Salaszkoleniowa,DC=rol00,DC=edu,DC=pl"
```

Wymuś przetworzenie zasad

```
# jako Administrator
gpupdate /force
# tylko część użytkownika (bo ustawienia wygaszacza są w HKCU)
gpupdate /target:user /force
```

Korzystając z karty Delegation (Delegowanie) obiektu zasad grupy dodaj ustawienie odmawiające grupie Kompszkolenie uprawnienie Apply Group Policy (Stosowanie zasad grup). Wskazówki:

Procedura w konsoli Group Policy Management:

1. Otwórz GPMC (Group Policy Management Console):

Start > Server Manager > Tools > Group Policy Management\ lub w „Uruchom” wpisz: gpmc.msc

2. W drzewie domeny znajdź obiekt zasad grupy **ROL00** (lub inny, który chcesz edytować).
3. Kliknij ROL00 > przejdź do zakładki Delegation (Delegowanie).
4. Kliknij Advanced (Zaawansowane) > otworzy się okno Security.
5. Kliknij Add (Dodaj):
   - Wprowadź nazwę grupy: Kompszkolenie.
   - Kliknij OK.
6. W tabeli uprawnień znajdź Apply Group Policy:
   - Zaznacz Deny (Odmów) dla tej pozycji.
   - Upewnij się, że Read pozostaje zaznaczone (bez Read GPO nie będzie widoczne, ale Deny Apply blokuje jego zastosowanie).

7. Kliknij OK, zamknij okno.
8. Odśwież zasady na stacjach:

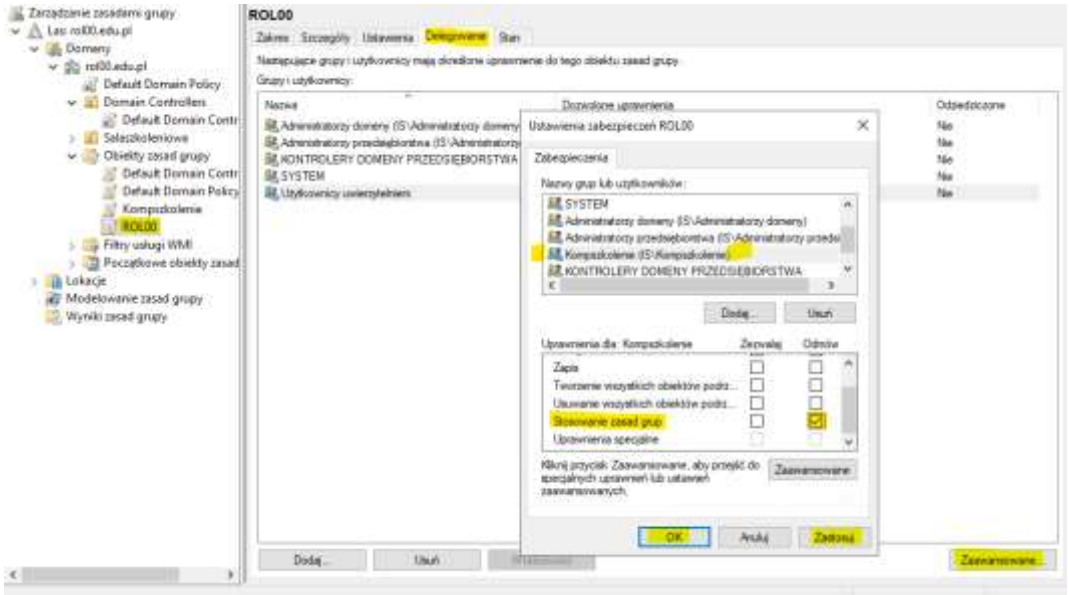
gpupdate /force

Efekt:

- Komputery lub użytkownicy należący do grupy Kompszkolenie nie będą objęci zasadami z GPO ROL00, nawet jeśli GPO jest linkowane do ich OU.
- Deny ma najwyższy priorytet – nie można go nadpisać innymi ustawieniami.

Wskazówki dodatkowe:

- Security Filtering i Delegation działają razem:
- Jeśli chcesz, aby GPO stosowało się tylko do wybranych grup, użyj Security Filtering (np. usuń „Authenticated Users" i dodaj właściwą grupę).
- Jeśli chcesz zablokować stosowanie dla konkretnej grupy, użyj Deny Apply Group Policy w Delegation.
- Sprawdzenie efektu:
  - Na stacji zalogowanej użytkownikiem z grupy Kompszkolenie uruchom: gpresult /r W sekcji Denied GPOs powinna pojawić się nazwa GPO ROL00 z powodem „Access Denied".



Odśwież zasady grupy poleceniem: gpupdate /force /boot oznacza:

- gpupdate – wymusza natychmiastowe odświeżenie zasad grupy (Group Policy) na komputerze.
- /force – wymusza ponowne zastosowanie wszystkich ustawień zasad, nawet jeśli nie uległy zmianie.
- /boot – powoduje restart komputera po zakończeniu aktualizacji, ale tylko wtedy, gdy jest to wymagane do zastosowania ustawień (np. ustawienia węzła Computer Configuration, które wymagają restartu).

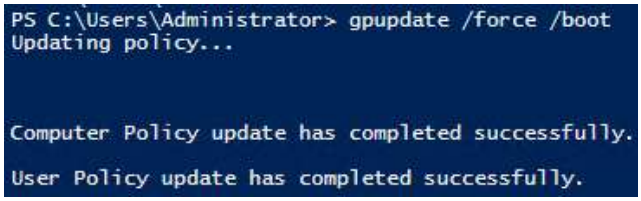
Dlaczego to jest potrzebne?

Niektóre ustawienia GPO (np. w Computer Configuration, sterowniki, polityki zabezpieczeń) nie mogą być w pełni zastosowane bez restartu systemu.

Dodanie /boot automatyzuje ten proces – po odświeżeniu zasad komputer uruchomi się ponownie, aby wszystkie zmiany weszły w życie.

Kiedy używać /boot?

- Gdy wiesz, że GPO zawiera ustawienia wymagające restartu (np. zmiany w usługach, sterownikach, politykach systemowych).
- W środowisku testowym, aby mieć pewność, że wszystkie zasady są aktywne po jednym cyklu.



zgłoszenie 4

Zadanie 4a - Analiza delegowania (w zeszycie zapisz odpowiedzi na pytania):

a. Jakie konsekwencje ma odebranie uprawnienia Apply Group Policy grupie Kompszkolenie?

Jeśli w zakładce Delegation ustawisz Deny dla uprawnienia Apply Group Policy dla grupy Kompszkolenie, to:

- Członkowie tej grupy nie będą objęci zasadami z tego GPO, nawet jeśli GPO jest linkowane do ich OU.
- Odmowa (Deny) ma najwyższy priorytet – nie można jej nadpisać innymi ustawieniami ani Security Filtering.

b. Czy użytkownicy z tej grupy nadal będą objęci zasadami?

Nie, użytkownicy (lub komputery) należący do grupy Kompszkolenie nie będą stosować ustawień z tego GPO.\ Zasada zostanie całkowicie pominięta dla nich, nawet jeśli spełniają inne kryteria (OU, Security Filtering).

c. W jakich sytuacjach warto stosować delegowanie z odmową?

- Wykluczenie wyjątków: gdy chcesz, aby GPO obowiązywało w całej OU, ale pewna grupa (np. komputery do testów, administratorzy) była wyłączona.
- Scenariusze szkoleniowe: np. w pracowni, gdzie część komputerów ma inne ustawienia niż reszta.
- Bezpieczeństwo: gdy chcesz zablokować stosowanie polityki dla grupy z podwyższonymi uprawnieniami (np. Domain Admins), aby nie ograniczać ich funkcji.
- Testowanie: gdy chcesz tymczasowo wyłączyć GPO dla określonej grupy bez zmiany linków i struktury OU.

Jak sprawdzić efekt? Na komputerze należącym do grupy Kompszkolenie: gpresult /r

W sekcji Denied GPOs zobaczysz nazwę GPO z powodem „Access Denied”.

zgłoszenie 4a

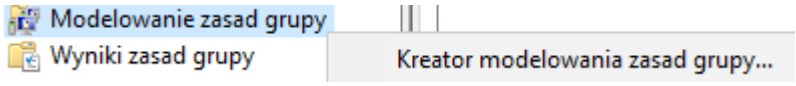
Zadanie 5

Skorzystaj z narzędzia Group Policy Modeling Wizard (Kreator modelowania zasad grupy) do oceny wynikowego zestawu zasad (RSoP) dla utworzonego użytkownika sluchacz w rol00.edu.pl/Salaszkoleniowa logującego się na komputerze s4 w rol00.edu.pl/Salaszkoleniowa.

Wskazówki:

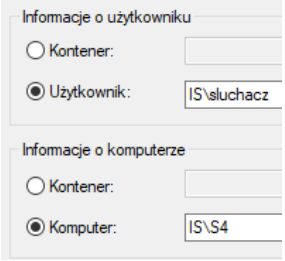
Polska wersja językowa Windows Server 2019 jest w pełni obsługiwana przez narzędzie **Group Policy** Management Console (GPMC) i kreator Group Policy Modeling Wizard, ale nazwy opcji są przetłumaczone. Oto jak wygląda procedura w polskim interfejsie:

1. Uruchom konsolę Zarządzanie zasadami grupy:
   - Start > Menedżer serwera > Narzędzia > Zarządzanie zasadami grupy.
2. W lewym panelu wybierz Modelowanie zasad grupy > kliknij Uruchom kreatora modelowania zasad grupy.



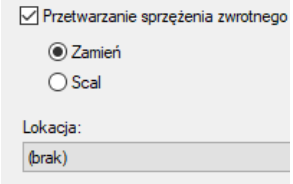
3. Wybierz kontroler domeny:
   - Wybierz np. rol00.edu.pl > Dalej.
4. Wybierz użytkownika i komputer:
   - Użytkownik: sluchacz (OU: Salaszkoleniowa).
   - Komputer: s4 (OU: Salaszkoleniowa).

   Kliknij Dalej.



5. Opcje dodatkowe:
   - Zaznacz Przetwarzanie zasad w sprzężeniu zwrotnym.
   - Wybierz tryb: Zamień (Replace).

   Kliknij Dalej.



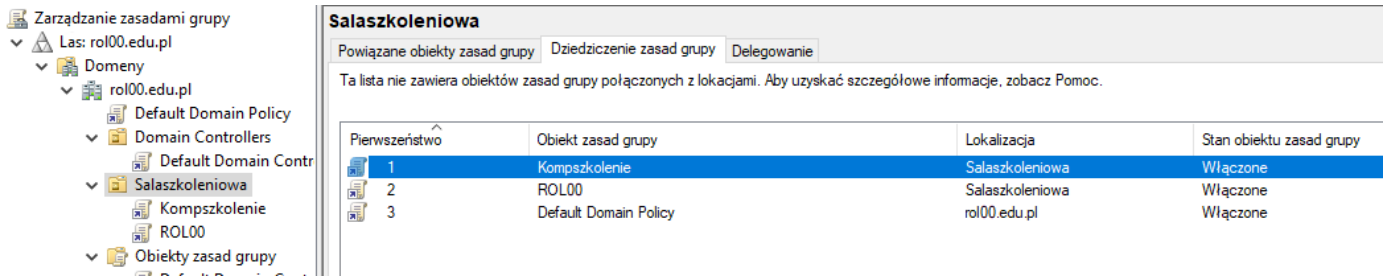
6. Lokalizacja (Site): pozostaw domyślnie lub wybierz odpowiednią.
   - Kliknij Dalej.

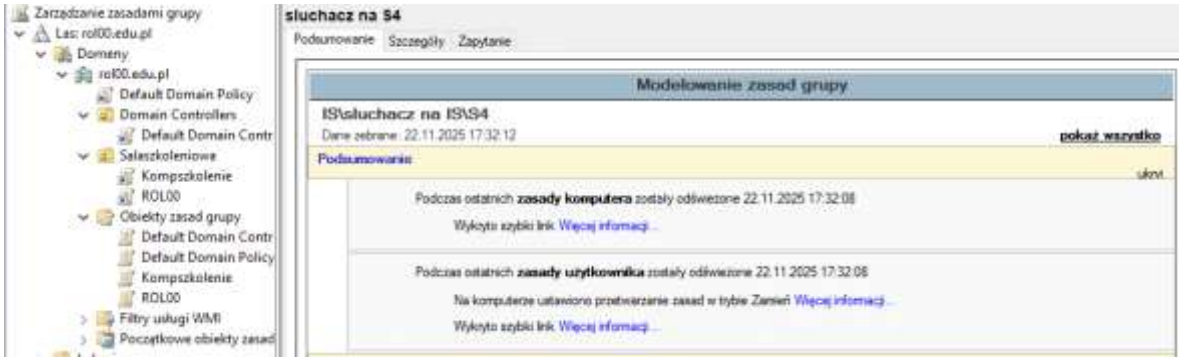
7. Filtry WMI: pozostaw domyślnie.
   - Kliknij Dalej.
8. Podsumowanie > Dalej > Zakończ.

Raport RSoP (Wynikowy zestaw zasad):

- Sprawdź w raporcie:
  - Zastosowane obiekty zasad grupy (Applied GPOs).
  - Odmówione obiekty zasad grupy (Denied GPOs) – np. jeśli ustawiłeś Deny dla grupy Kompszkolenie.
  - Ustawienia wygaszacza ekranu (ROL00) i tapety (Kompszkolenie).

Oczekiwane efekty:





zgłoszenie 5

Zadanie 5a (w zeszycie zapisz odpowiedzi na pytania):

a. Jakie różnice występują między trybem Replace a Merge?

- Replace (Zamień):
  - Ustawienia użytkownika są całkowicie zastępowane przez ustawienia z GPO przypisanych do OU komputera.
  - Ignorowane są wszystkie GPO z OU użytkownika.
- Merge (Scal):
  - Ustawienia użytkownika są łączone z ustawieniami z OU komputera.
  - Jeśli wystąpi konflikt, priorytet mają ustawienia z OU komputera.

b. W jakich przypadkach należy stosować tryb Replace?

- Gdy chcesz, aby komputer decydował o pełnym zestawie ustawień użytkownika, np. w pracowniach szkoleniowych, kioskach, terminalach.
- W środowiskach, gdzie profil użytkownika nie ma znaczenia, a konfiguracja ma być jednolita dla wszystkich logujących się na danym komputerze.

c. Czy przetwarzanie w sprzężeniu zwrotnym może wpłynąć na użytkownika, który nie należy do jednostki organizacyjnej komputera?

Tak:

- Jeśli włączysz Loopback Processing na komputerze, to użytkownik otrzyma ustawienia z OU komputera, niezależnie od tego, w jakiej OU znajduje się jego konto.
- W trybie Replace ignorowane są jego własne GPO z OU użytkownika.

- W trybie Merge jego własne GPO są brane pod uwagę, ale priorytet mają ustawienia z OU komputera.

Zgłoszenie 5a

Przywróć pierwszy punkt kontrolny

Podsumowanie:
Po wykonaniu wszystkich czynności z powyższej instrukcji przeczytaj ponownie z zrozumieniem cel ogólny i cele szczegółowe, które znajdują się na pierwszej stronie instrukcji. Jeżeli one zostały niezrealizowane to powtarzaj wykonie tej instrukcji w szkole lub/i w domu do momentu zrealizowania.