12.4 Zarządzanie zasadami grup w domenie

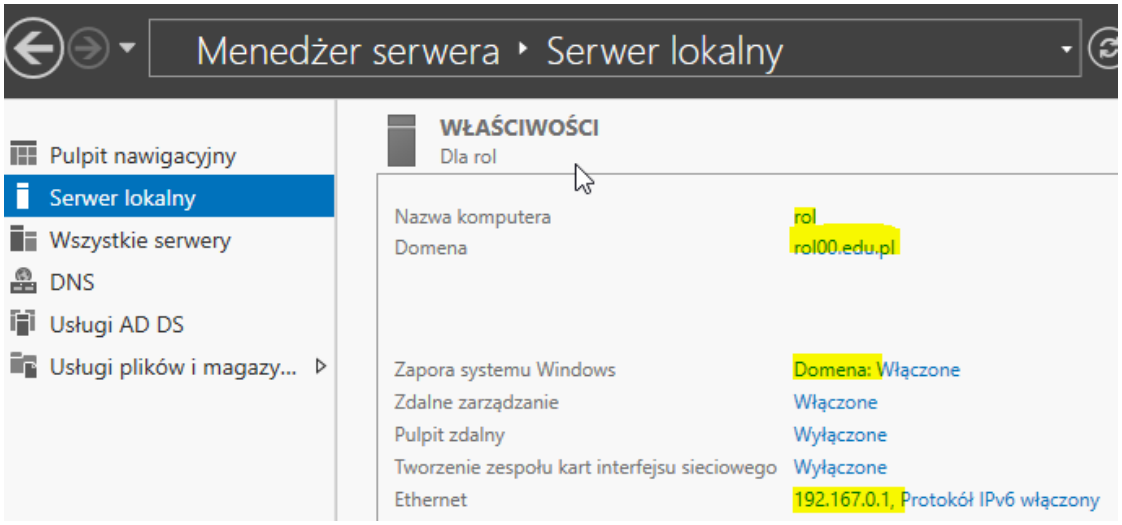
Przed przystąpieniem do ćwiczenia sprawdź i ustaw

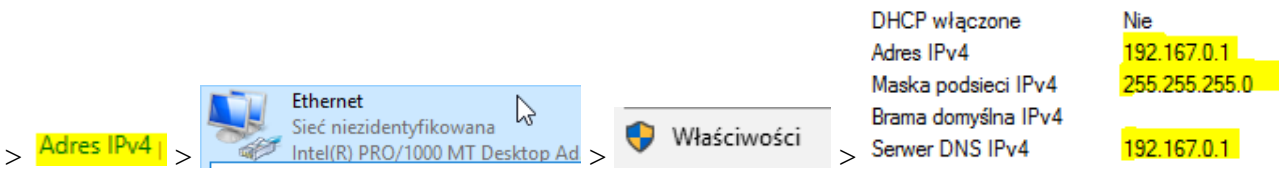
W Menedżer funkcji Hyper-V wybierz nazwa maszynę wirtualna twojej grupy_dc2019

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.

Wynikowy zestaw zasad grup.

Zadanie 1

Korzystanie z narzędzia Group Policy Results Wizard (Kreator wyników zasad grupy)

W tym ćwiczeniu wykorzystamy narzędzie Group Policy Results Wizard (Kreator wyników zasad grupy) do zbadania wynikowego zestawu zasad (RSoP) na komputerze ROL00.

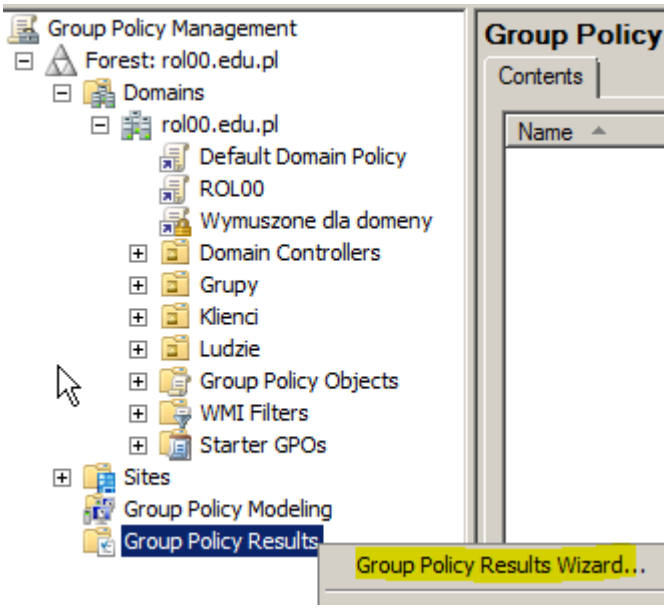
Potwierdzimy, że są stosowane utworzone zasady.

1. Zaloguj się jako Administrator na komputerze serwera.
2. Otwórz wiersz polecenia i wpisać gpupdate.exe /force /boot, aby zainicjować odświeżanie zasad grupy, poczekaj na ponowne uruchomienie procesu. Zanotuj aktualny czas systemowy; znajomość czasu odświeżenia będzie potrzebna w zadaniu 12.4.3 „Przeglądanie zdarzeń dotyczących zasad".

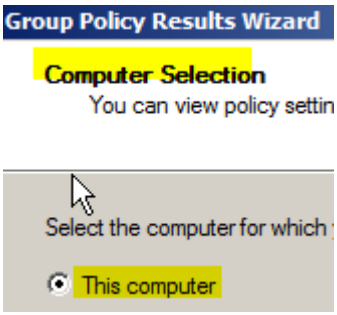
```
C:\Users\Administrator>gpupdate.exe /force /boot
Updating Policy...

User Policy update has completed successfully.
Computer Policy update has completed successfully.
```

13:26

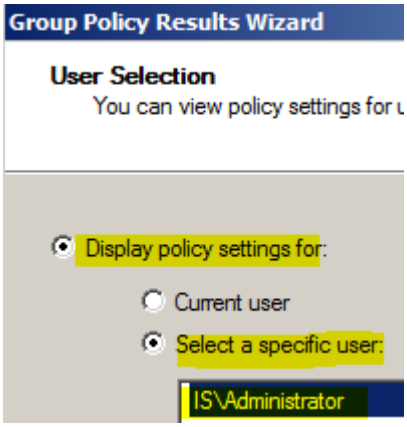
3. Zaloguj się jako Administrator na komputerze serwera i otwórz konsolę Group Policy Management (Zarządzanie zasadami grupy).
4. Rozwiń węzeł lasu.
5. Kliknij prawym przyciskiem myszy węzeł Group Policy Results (Wyniki zasad grupy) i wybierz opcję Group Policy Results Wizard (Kreator wyników zasad grupy).



6. Kliknij Next (Dalej).
7. Na stronie Computer Selection (Wybór komputera) zaznacz opcję This Computer (Ten komputer) i kliknąć Next (Dalej).



8. Na stronie User Selection (Wybór użytkownika) zaznacz opcję Display Policy Settings For (Wyświetl ustawienia zasad dla), zaznacz Select a specific user (Wybierz określonego użytkownika) i zaznaczyć IS\Administrator. Następnie kliknij Next (Dalej).



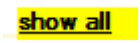
9. Na stronie Summary Of Selections (Podsumowanie wybranych opcji) przejrzyj swoje ustawienia i kliknąć Next (Dalej).

Selection	Settings
User name	IS\Administrator
Display user policy settings	Yes
Computer name	IS\ROL00
Display computer policy settings	Yes

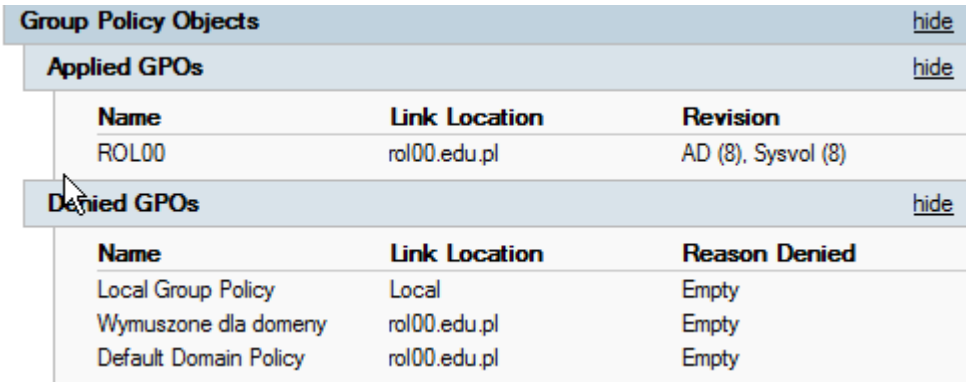
10. Kliknij Finish (Zakończ).

W okienku szczegółów konsoli pojawi się raport wynikowego zestawu zasad (RSoP).

11. Na karcie Summary (Podsumowanie) kliknij łącze Show All (Pokaż wszystkie) u góry raportu.



12. Przejrzyj wyniki podsumowania zasad grupy. Zarówno dla konfiguracji użytkownika, jak i konfiguracji komputera, znajdź godzinę ostatniego odświeżenia zasad Last time Group Policy was processed i listę zastosowanych i odrzuconych obiektów zasad grupy, zidentyfikuj składniki, które zostały użyte do przetworzenia ustawień zasad.



Group Policy Objects hide

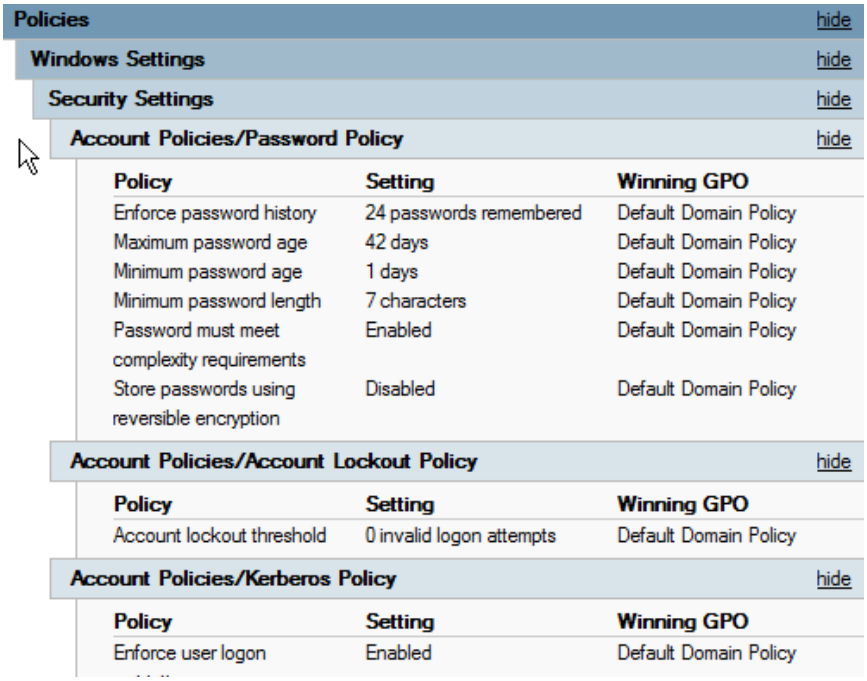
Applied GPOs hide

Name	Link Location	Revision
ROL00	rol00.edu.pl	AD (8), Sysvol (8)

Denied GPOs hide

Name	Link Location	Reason Denied
Local Group Policy	Local	Empty
Wymuszone dla domeny	rol00.edu.pl	Empty
Default Domain Policy	rol00.edu.pl	Empty

13. Kliknij kartę Settings (Ustawienia) i kliknij łącze Show All (Pokaż wszystkie) u góry strony. Należy przejrzeć ustawienia, które zostały zastosowane podczas wprowadzania zasad użytkownika i komputera oraz zidentyfikować obiekt zasad grupy, z których te ustawienia zostały uzyskane.



Policies hide

Windows Settings hide

Security Settings hide

Account Policies/Password Policy hide

Policy	Setting	Winning GPO
Enforce password history	24 passwords remembered	Default Domain Policy
Maximum password age	42 days	Default Domain Policy
Minimum password age	1 days	Default Domain Policy
Minimum password length	7 characters	Default Domain Policy
Password must meet complexity requirements	Enabled	Default Domain Policy
Store passwords using reversible encryption	Disabled	Default Domain Policy

Account Policies/Account Lockout Policy hide

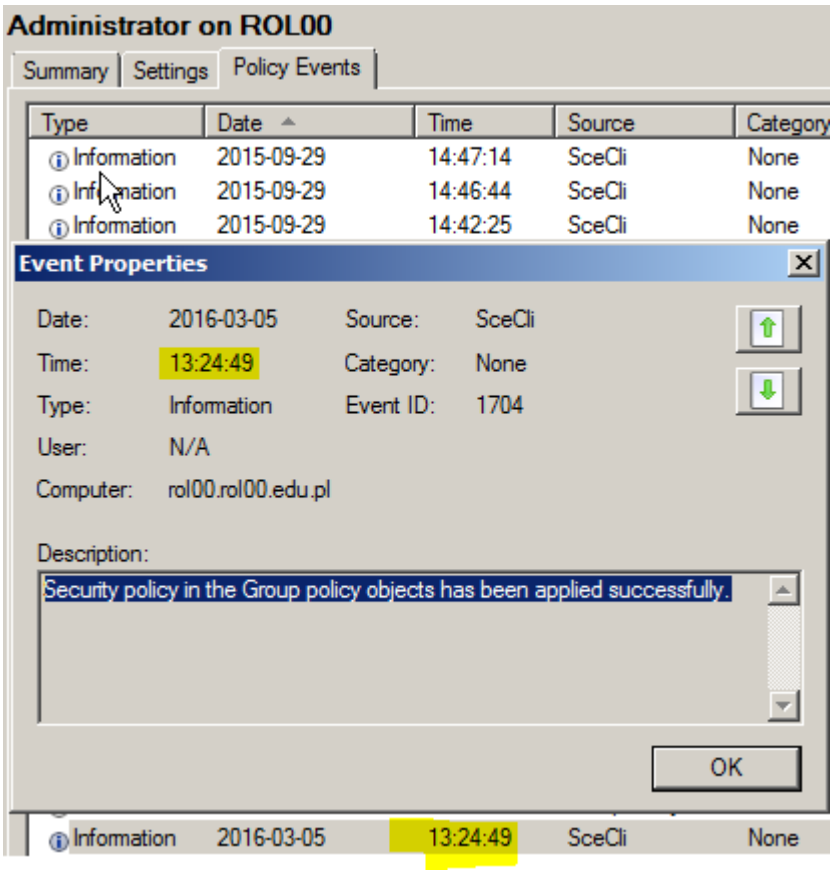
Policy	Setting	Winning GPO
Account lockout threshold	0 invalid logon attempts	Default Domain Policy

Account Policies/Kerberos Policy hide

Policy	Setting	Winning GPO
Enforce user logon	Enabled	Default Domain Policy

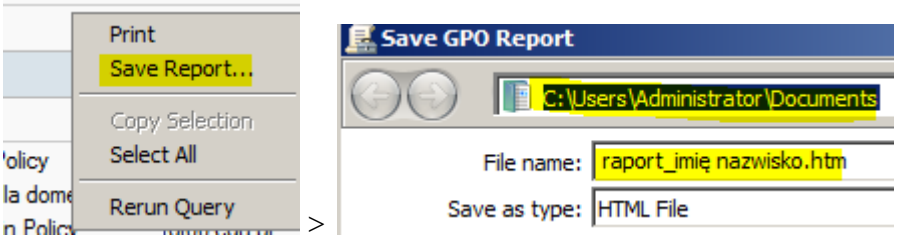
itd.

14. Kliknij kartę Policy Events (Zdarzenia dotyczące zasad) i zlokalizować zdarzenie, które odnotowuje odświeżenie zasad, które wymusiliśmy poleceniem Gpupdate.exe w kroku 2.

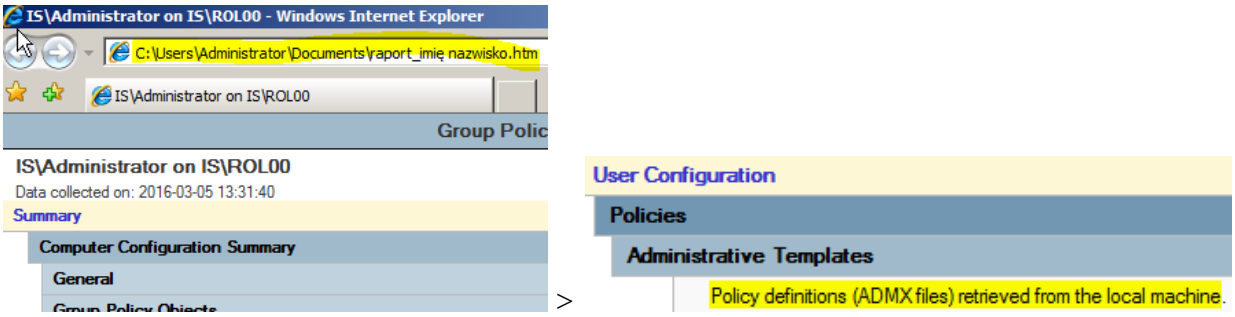


sprawdź zapisaną godzinę.

15. Kliknij kartę Summary (Podsumowanie), kliknąć stronę prawym przyciskiem myszy i wybierz Save Report (Zapisz raport). Zapisać raport jako plik HTML w swoim folderze Documents (Dokumenty) pod nazwą raport_imię nazwisko.



16. Otwórz zapisany raport wynikowego zestawu zasad (RSOP) z foldera Documents (Dokumenty). Odszukaj zaznaczony element.



Zadanie 2

Korzystanie z polecenia GpresuIt.exe

W tym ćwiczeniu wykonamy analizę wynikowego zestawu zasad (RSoP) z wiersza polecenia. korzystając z polecenia Gpresult.exe.

1. Otwórz wiersz polecenia.

2. Wpisać gpresult /r i nacisnąć Enter.

```
        Local Group Policy
            Filtering:  Not Applied (Empty)

    The user is a part of the following security groups
    ---------------------------------------------------
        Domain Users
        Everyone
        BUILTIN\Administrators
        BUILTIN\Users
        BUILTIN\Pre-Windows 2000 Compatible Access
        NT AUTHORITY\INTERACTIVE
        NT AUTHORITY\Authenticated Users
        This Organization
        LOCAL
        Group Policy Creator Owners
        Domain Admins
        Schema Admins
        Enterprise Admins
        Denied RODC Password Replication Group
        High Mandatory Level

C:\Users\Administrator>gpresult /r
```

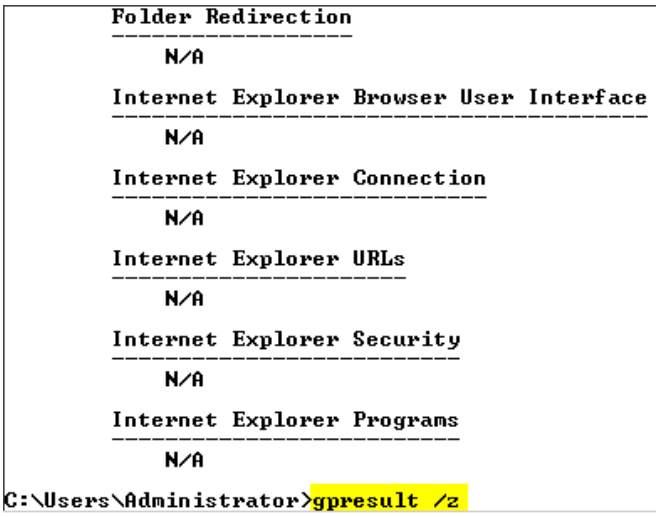
Wyświetlone zostaną wyniki podsumowania RSoP. Ta informacja jest bardzo podobna do karty Summary (Podsumowanie) raportu wynikowego zestawu zasad (RSOP) wygenerowanego przez narzędzie Group Policy Results Wizard (Kreator wyników zasad grupy).

3. Wpisz gpresult /v i nacisnąć Enter.

```
        Folder Redirection
        ------------------
            N/A

        Internet Explorer Browser User Interface
        ----------------------------------------
            N/A

        Internet Explorer Connection
        ----------------------------
            N/A

        Internet Explorer URLs
        ----------------------
            N/A

        Internet Explorer Security
        --------------------------
            N/A

        Internet Explorer Programs
        --------------------------
            N/A

C:\Users\Administrator>gpresult /v
```

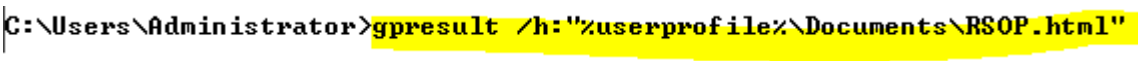
Wygenerowany zostanie bardziej szczegółowy raport wynikowego zestawu zasad (RSOP).
Należy zwrócić uwagę, że wiele ustawień zasad grupy wprowadzonych przez klienta jest wymienionych w tym raporcie.

4. Wpisać gpresult /z i nacisnąć Enter.



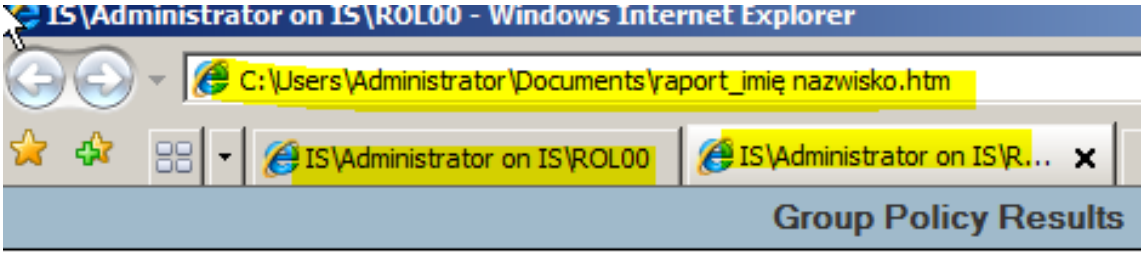
Wygenerowany zostanie najbardziej szczegółowy raport wynikowego zestawu zasad (RSoP).

5. Wpisz gpresult /h:"%userprofile%\Documents\RSOP.html" i naciśnij Enter.



Raport wynikowego zestawu zasad (RSOP) zostanie zapisany jako plik HTML w folderze Documents (Dokumenty).

6. Otwórz zapisany raport wynikowego zestawu zasad (RSoP) z foldera Documents (Dokumenty). Należy porównać ten raport, zawarte w nim informacje i formatowanie z raportem wynikowego zestawu zasad (RSoP) zapisanym w poprzednim zadaniu.



Zadanie 3

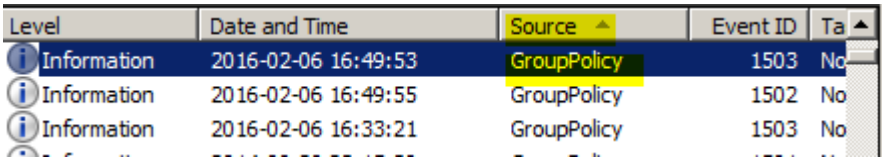
Przeglądanie zdarzeń dotyczących zasad

Gdy klient wykonuje odświeżanie zasad, składniki zasad grupy dokonują wpisów w dziennikach zdarzeń systemu Windows. W tym ćwiczeniu wyszukasz i zbadasz zdarzenia związane z zasadami grupy.

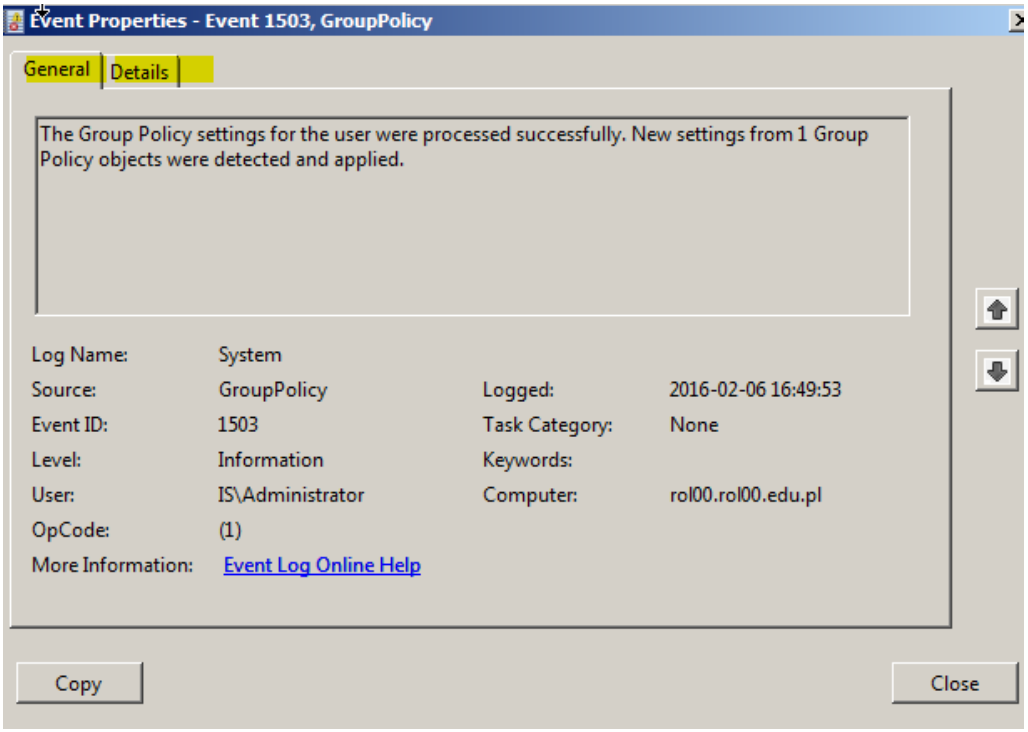
1. Otwórz konsolę Event Viewer (Podgląd zdarzeń) z foldera Administrative Tools (Narzędzia administracyjne).

2. Rozwiń folder Windows Logs\System (Dzienniki systemu Windows\System)

3. Znajdź elementy mające wartość GroupPolicy W kolumnie Source (Źródło). Można kliknąć łącze Filter Current Log (Filtruj bieżący dziennik) w okienku Actions (Akcje), a następnie wybrać GroupPolicy z listy rozwijanej Event Sources (Źródła zdarzeń).



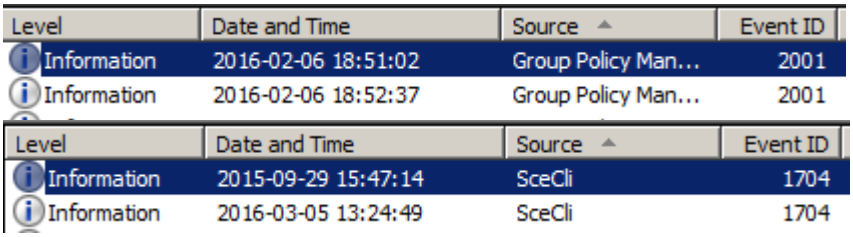
4. Przejrzyj informacje skojarzone ze zdarzeniami GroupPolicy.



5. Kliknij węzeł Application (Aplikacja) w drzewie konsoli pod węzłem Windows Logs (Dzienniki systemu Windows).

6. Posortuj dziennik Application (Aplikacja) według kolumny Source (Źródło).

7. Przejrzyj wpisy dziennika według źródła i zidentyfikować zdarzenia dotyczące zasad grupy, które zostały wprowadzone w tym dzienniku. Które zdarzenia są związane z wprowadzaniem zasad grupy, a które są związane z działaniami, które wykonywaliśmy zarządzając zasadami grupy?

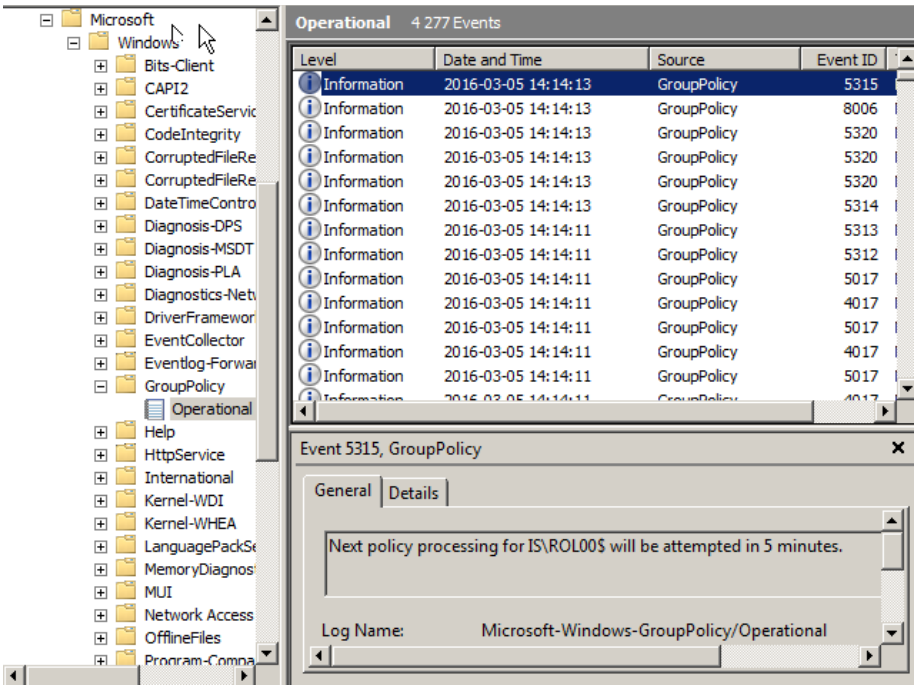


Level	Date and Time	Source	Event ID
Information	2016-02-06 18:51:02	Group Policy Man...	2001
Information	2016-02-06 18:52:37	Group Policy Man...	2001

Level	Date and Time	Source	Event ID
Information	2015-09-29 15:47:14	SceCli	1704
Information	2016-03-05 13:24:49	SceCli	1704

8. W drzewie konsoli rozwiń węzeł Applications And Services Logs\Microsoft\Windows \GroupPolicy\Operational (Dzienniki aplikacji i usług\Microsoft\Windows \GroupPolicy\ Operational).

9. Odszukaj pierwsze zdarzenie związane z odświeżaniem zasad grupy, które wywołaliśmy w zadaniu 1 „Korzystanie z narzędzia Group Policy Results Wizard (Kreator wyników zasad grupy)“ poleceniem Gpupdate.exe. Należy przejrzeć to zdarzenie i zdarzenia następujące po nim.



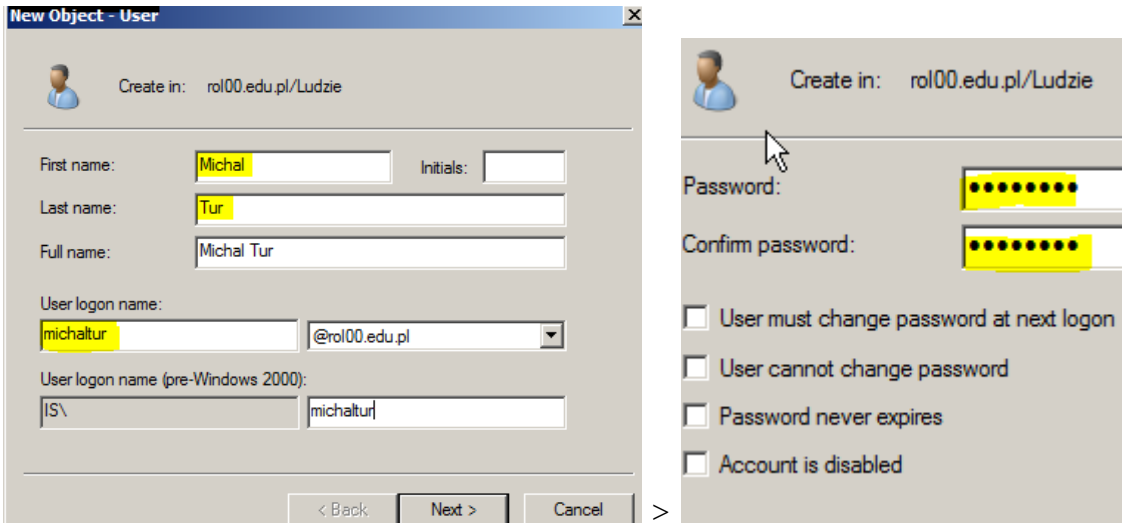
Zadanie 4

Wykonywanie modelowania zasad grupy

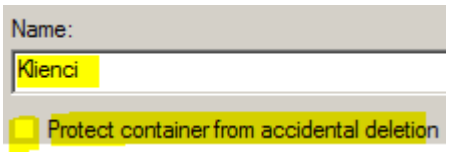
W tym ćwiczeniu skorzystamy z modelowania zasad grupy do oceny potencjalnego wpływu naszych ustawień zasad na użytkowników, którzy logują się na laptopach sprzedawców.

1. Otwórz przystawkę Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory).

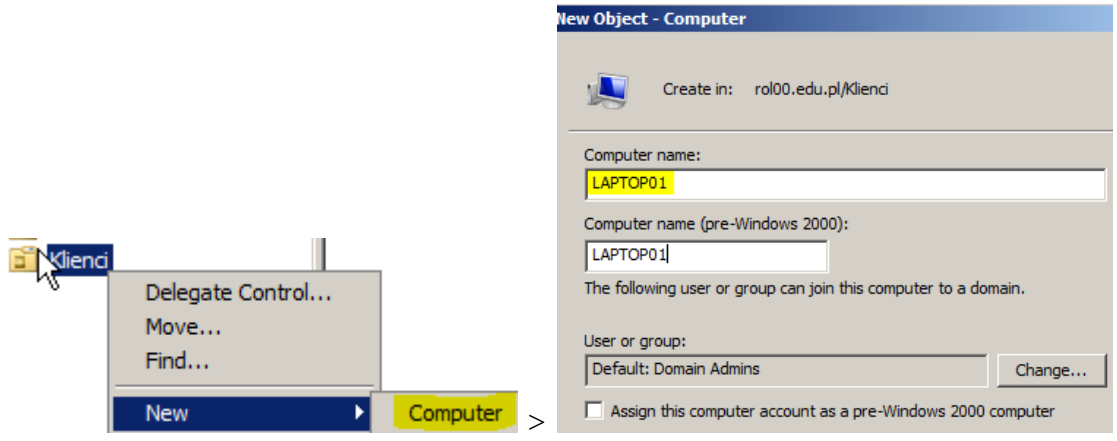
2. Utwórz konto użytkownika Michal Tur w jednostce organizacyjnej Ludzie.



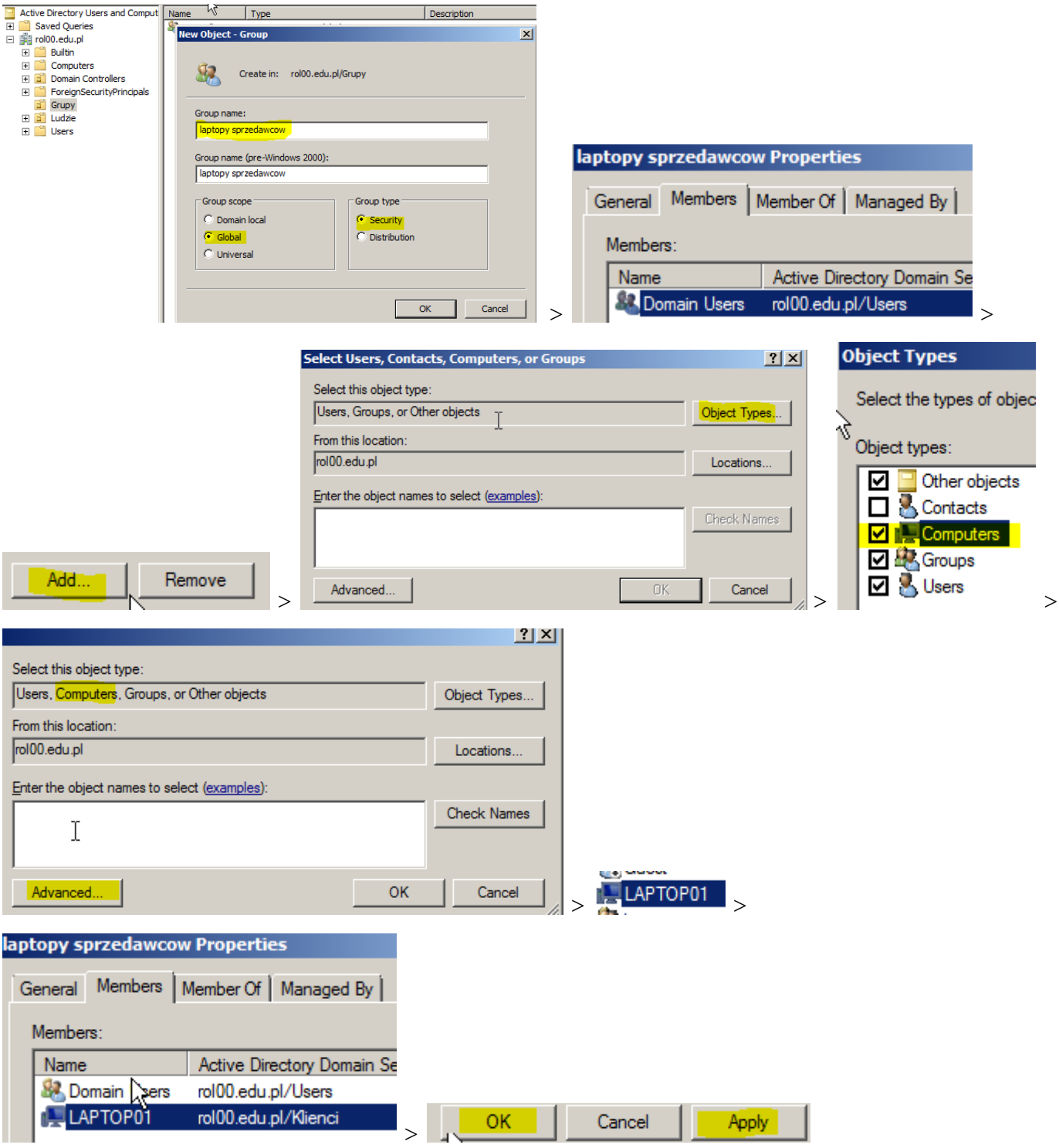
3. Utwórz w domenie jednostkę organizacyjną o nazwie Klienci.



4. Utwórz w jednostce organizacyjnej Klienci konto komputera o nazwie LAPTOP01.



5. Dodać LAPTOP01 i grupę Domain Users (Użytkownicy domeny) do grupy Laptopy sprzedawców.



Jest słabo udokumentowanym faktem, że podczas łączenia przetwarzania w sprzężeniu zwrotnym z filtrowaniem grup zabezpieczeń stosowanie ustawień użytkownika podczas odświeżania zasad wykorzystuje poświadczenia komputera do określenia, które obiekty zasad grupy mają być zastosowane jako cześć przetwarzania w sprzężeniu zwrotnym. ale zalogowany użytkownik musi również mieć uprawnienie Apply Group Policy (Stosowanie zasad grup).

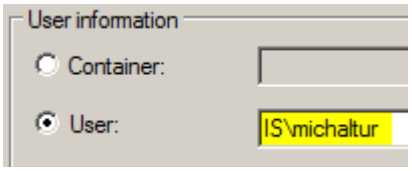
6. W konsoli Group Policy Management (Zarządzanie zasadami grupy) rozwinąć węzeł lasu.

7. Kliknąć prawym przyciskiem myszy węzeł Group Policy Modeling (Modelowanie zasad grupy) i wybrać opcję Group Policy Modeling Wizard (Kreator modelowania zasad Group).

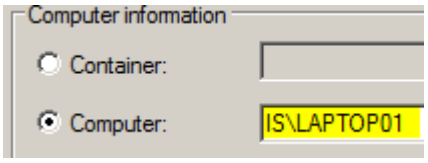
8. Kliknąć Next (Dalej).

9. Na stronie Domain Controller Selection (Wybór kontrolera domeny) kliknąć Next (Dalej).

10. Na stronie User And Computer Selection (Wybór użytkownika i komputera) w sekcji User Information (Informacje o użytkowniku) kliknąć opcję User (Użytkownik) kliknąć Browse (Przeglądaj), a następnie wybrać użytkownika Michal Tur.

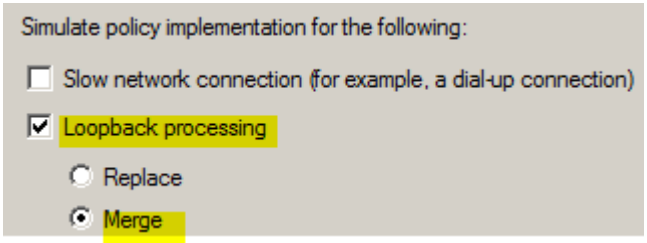


11. W sekcji Computer Information (Informacje o komputerze) kliknąć opcję Computer (Komputer), kliknij Browse (Przeglądaj), i wybierz LAPTOP01 jako komputer.



12. Kliknij Next (Dalej).

13. Na stronie Advanced Simulation Options (Zaawansowane opcje symulacji) zaznaczyć pole wyboru Loopback Processing (Przetwarzanie sprzężenia zwrotnego) i zaznaczyć opcję Merge (Scal).



Chociaż obiekt zasad grupy Konfiguracja laptopów sprzedawców określa przetwarzanie w sprzężeniu zwrotnym. to musimy poinstruować narzędzie Group Policy Modeling Wizard (Kreator modelowania zasad grupy), żeby w swojej symulacji rozważyło zastosowanie przetwarzania w sprzężeniu zwrotnym.

14. Kliknąć Next (Dalej).

15. Na stronie Alternate Active Directory Paths (Alternatywne ścieżki usługi Active Directory) kliknąć Next (Dalej).

16. Na stronie User Security Groups (Grupy zabezpieczeń użytkowników) kliknąć Next (Dalej).

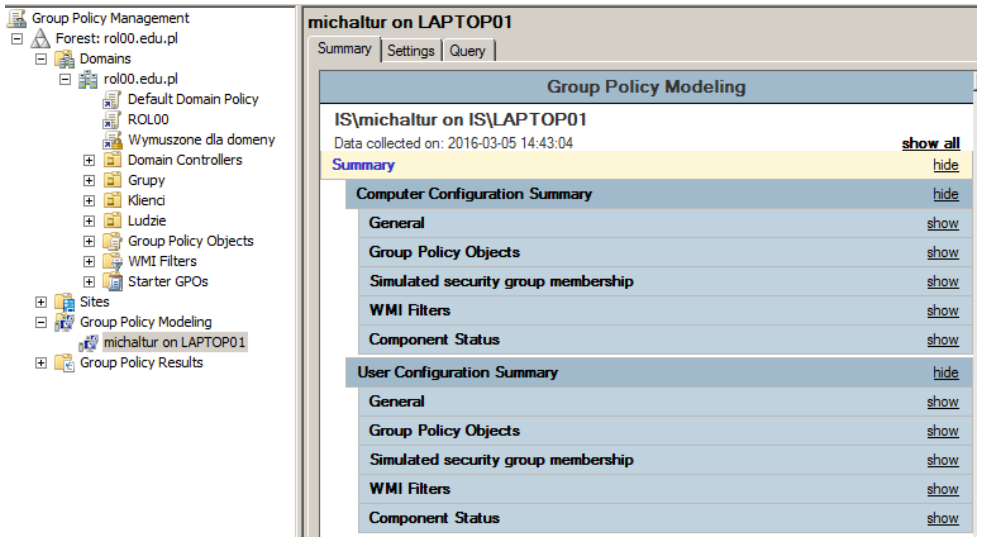
17. Na stronie Computer Security Groups (Grupy zabezpieczeń komputera) kliknąć Next (Dalej).

18. Na stronie WMI Filters For Users (Filtry WMI dla użytkowników) kliknąć Next (Dalej).

19. Na stronie WMI Filters For Computers (Filtry WMI dla komputerów) kliknąć Next (Dalej).

20. Przejrzeć swoje ustawienia na stronie Summary Of Selections (Podsumowanie wybranych opcji). Kliknąć Next (Dalej), a następnie kliknąć Finish (Zakończ).

Selection	Settings
User name	IS\michaltur
Computer name	IS\LAPTOP01
Slow network simulation	No
Loopback mode	Merge
Site name	(None)
User Location	(Not specified)
Computer location	(Not specified)
User security groups	(Not specified)
Computer security groups	(Not specified)
Processing the simulation on this domain controller:	
rol00.rol00.edu.pl	



W zeszycie zapisz: Podsumowanie:

Raporty wynikowego zestawu zasad (RSoP) mogą być generowane w interfejsie Windows za pomocą narzędzia Group Policy Results Wizard (Kreator wyników zasad grupy), który jest składnikiem konsoli Group Policy Management (Zarządzanie zasadami grupy).

Raporty wynikowego zestawu zasad (RSOP) przedstawiają faktyczne wyniki przetwarzania zasad przy ostatnim odświeżaniu zasad.

Raporty wynikowego zestawu zasad (RSoP) mogą być generowane z wiersza polecenia przy użyciu narzędzia Gpresult.exe. Opcja /scope może być używana do generowania raportu zawierającego tylko ustawienia użytkownika lub komputera. Przełącznik Is może służyć do uruchamiania Gpresult.exe dla systemu zdalnego.

Narzędzie Group Policy Modeling Wizard (Kreator modelowania zasad grupy) umożliwia nam symulowanie stosowania zasad grupy do oceny możliwego wpływu zmian w naszej infrastrukturze zasad grupy lub przenoszenia użytkowników i komputerów pomiędzy jednostkami organizacyjnymi i grupami.

Składniki zasad grupy tworzą wpisy w dziennikach zdarzeń systemu Windows.