Windows Server 2008R2

GPO

Mapowanie zasobów za pomocą GPO

Inne zalety GPO

WSTĘP

GPO – co to takiego…?

Zasady grupy (GPO) to potężne narzędzie udostępnione administratorom systemów Windows w celu łatwiejszego zarządzania ustawieniami stacji roboczych.

Wyobraźmy sobie sytuację, w której musimy skonfigurować komputery w taki sposób, aby użytkownicy nie mogli dokonywać zmian konfiguracyjnych, w taki sposób, aby mogli uruchamiać tylko konkretne aplikacje lub też tak, aby mieli dostęp do tylko niezbędnych im do pracy składników systemu.

Jesteśmy w stanie wykonać te czynności konfigurując każdy komputer z osobna, jest to jednak czynność bardzo czasochłonna i niewygodna, a stopień tej „niewygody” wzrasta wraz z liczbą komputerów, którymi zarządzamy.

Można również napisać skrypt, który wykona te zadania i uruchomić go na wszystkich komputerach, ale i to nie jest zbyt wygodne rozwiązanie, a czasem wręcz niemożliwe ponieważ nie wszystkie nasze pomysły możemy w skrypcie zapisać.

Zasady grupy wykorzystują scentralizowany system zarządzania, co oznacza, że konfiguracja tych zasad odbywa się na serwerze i poprzez odpowiednie mechanizmy rozsyłana jest na komputery klienckie.

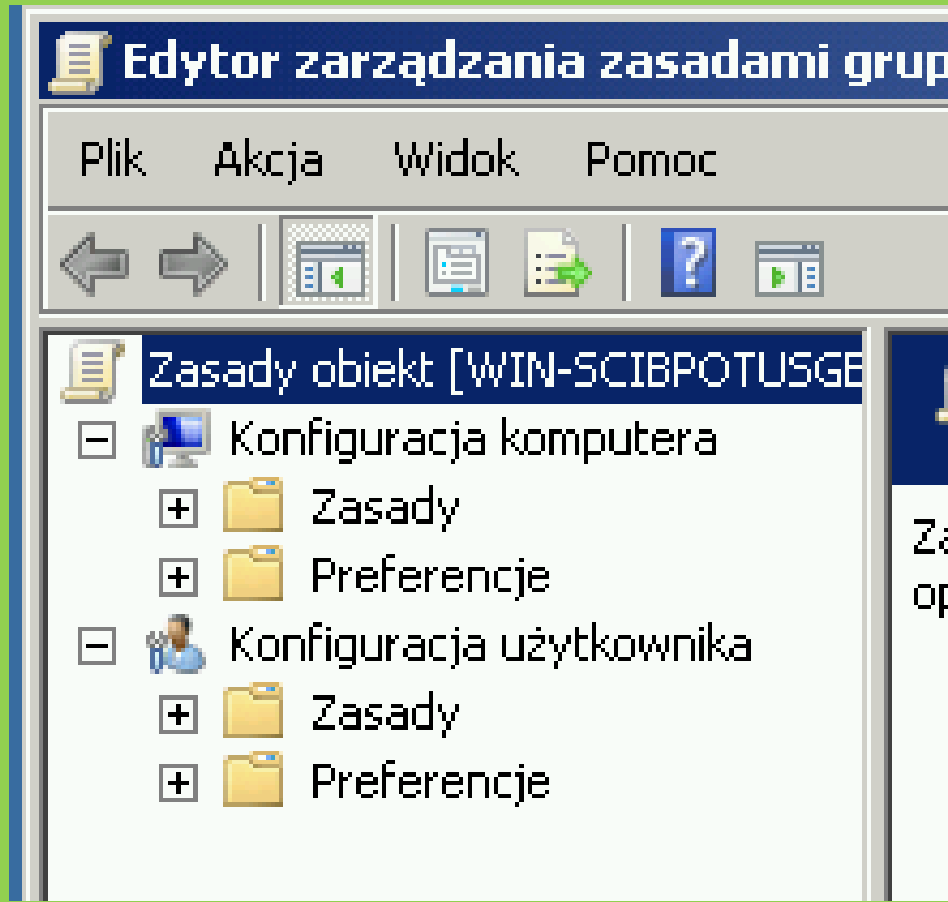
Wszystkie ustawienia przez nas zdefiniowane przechowywane są w obiektach zasad grupy (ang. Group Policy Objects), a do zarządzania tymi obiektami służy konsola zarządzania zasadami grupy (ang. Group Policy Management Console).

GPO z bliska

W pojedynczym obiekcie zasady grupy znajdziemy dwa główne typy ustawień:

-ustawienia komputera (ang. computer configuration) – ustawienia, które stosowane są dla komputerów bez względu na to, który użytkownik jest zalogowany i wprowadzane są podczas uruchamiania systemu operacyjnego (później są odświeżane co 90-120 minut)

-ustawienia użytkownika (ang. user configuration) – ustawienia, które wprowadzane są podczas logowania użytkownika, bez względu na to na jaki komputer się loguje (również są one później odświeżane są co 90-120 minut)

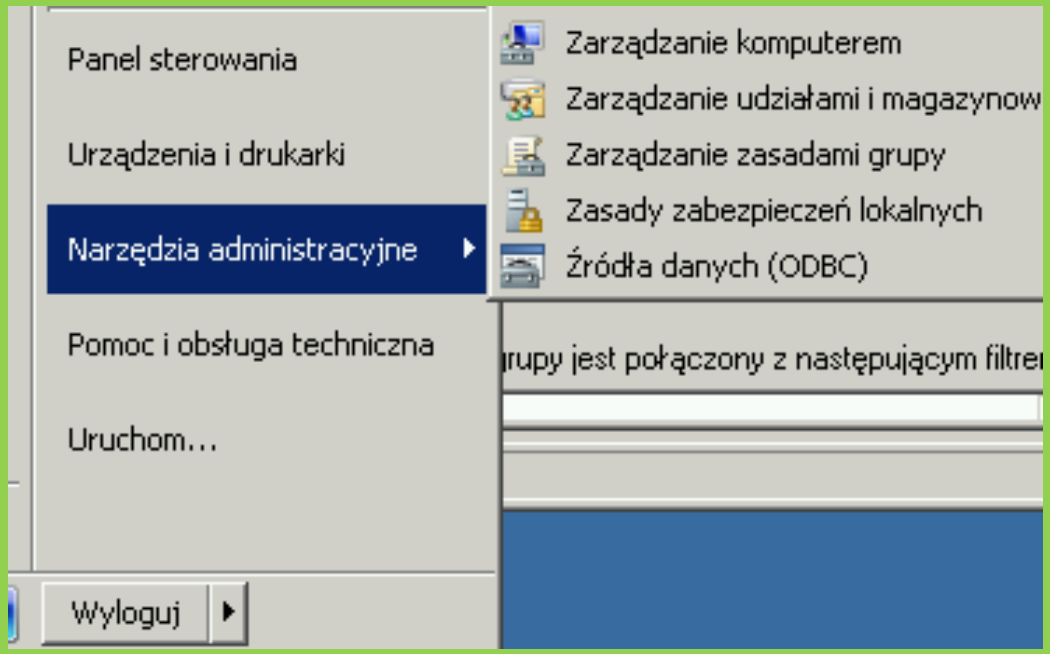


W ramach tych dwóch grup, możemy stosować setki różnych ustawień (np. zabronić dostępu do rejestru, pozwolić na uruchamianie tylko konkretnych aplikacji oraz wiele innych), niektóre z nich są dostępne zarówno dla konfiguracji komputera i użytkownika, inne zaś tylko dla jednej grupy, np. przekierowanie folderu dostępne jest tylko do konfiguracji użytkownika, a np. automatyczna instalacja oprogramowania tylko dla konfiguracji komputera.

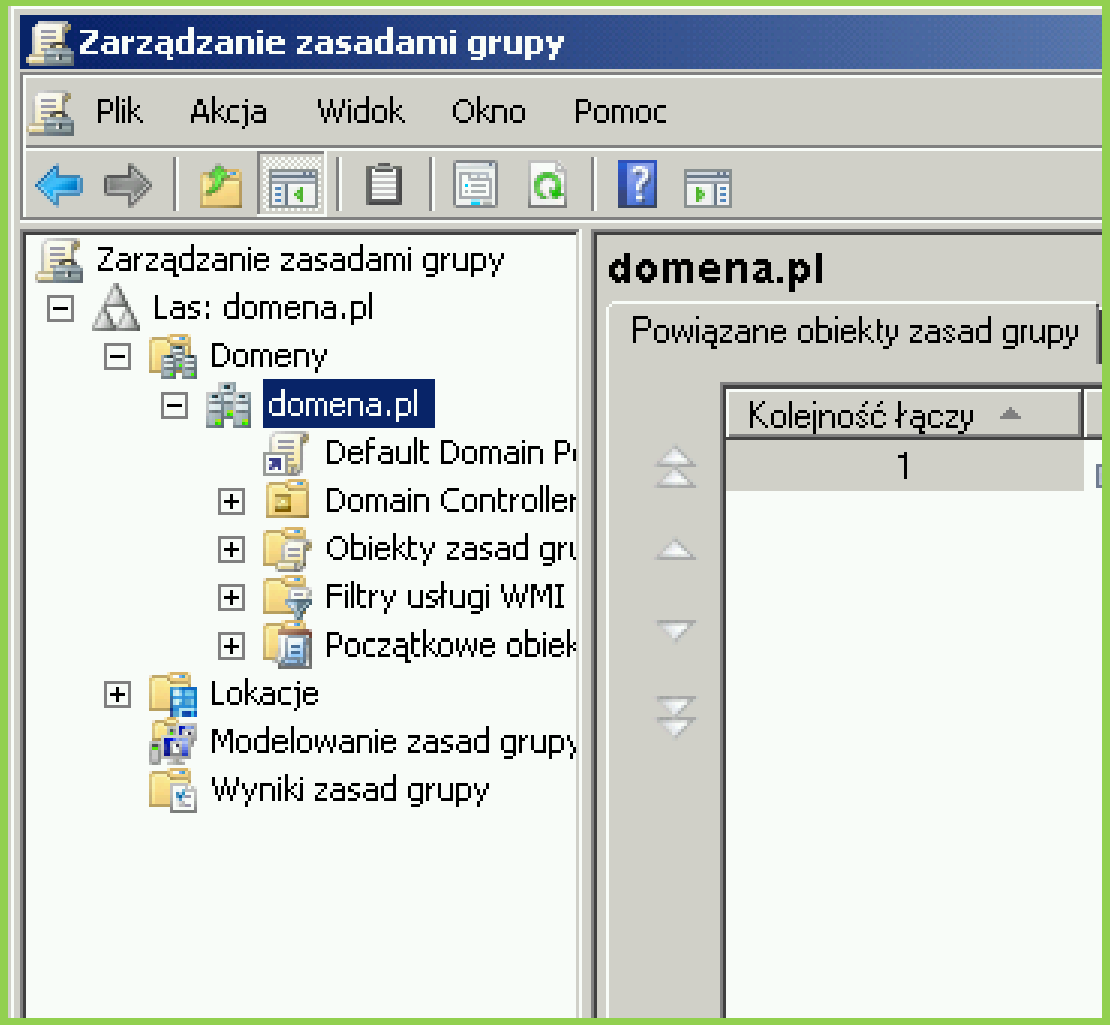
W jaki sposób dostać się do zarządzania GPO w Domenie (AD)

Aby uruchomić konsolę GPO klikamy w :

START →Administrative Tools →Group Policy Management



Następnie rozwijami element FOREST (LAS)



Znajdziemy tutaj elementy, takie jak:

-Default Domain Policy – jest to link do domyślnych zasad przypisanych do całej domeny (zwróćcie uwagę, że znajduje się on bezpośrednio pod nazwą domeny, co oznacza, że jest stosowany właśnie do całej domeny).

-Domain Controllers – jest jednostka organizacyjna, w której możemy umieszczać linki do zasad stosowanych dla kontrolera domeny (czyli naszego serwera), domyślnie znajduję się tutaj link do zasady Default Domain Controllers Policy.

-Group Policy Objects – jest to folder, w którym znajdują się wszystkie zasady, które będziemy tworzyć i stosować, po instalacji serwera znajdują się tam zasady Default Domain Policy oraz Default Domain Controllers Policy.

-WMI Filters – jest to folder, w którym możemy umieszczać filtry WMI, pozwalające określać zakres stosowania zasad na podstawie właściwości komputera, takich jak np. rodzaj zainstalowanego systemu operacyjnego.

-Starter GPOs – jest to folder zawierający zdefiniowane zasady stosowane dla komputerów z systemami Windows XP oraz Windows Vista (domyślnie są one wyłączone, aby je uruchomić klikamy w Starter GPOs i klikami w Create starter GPOs).

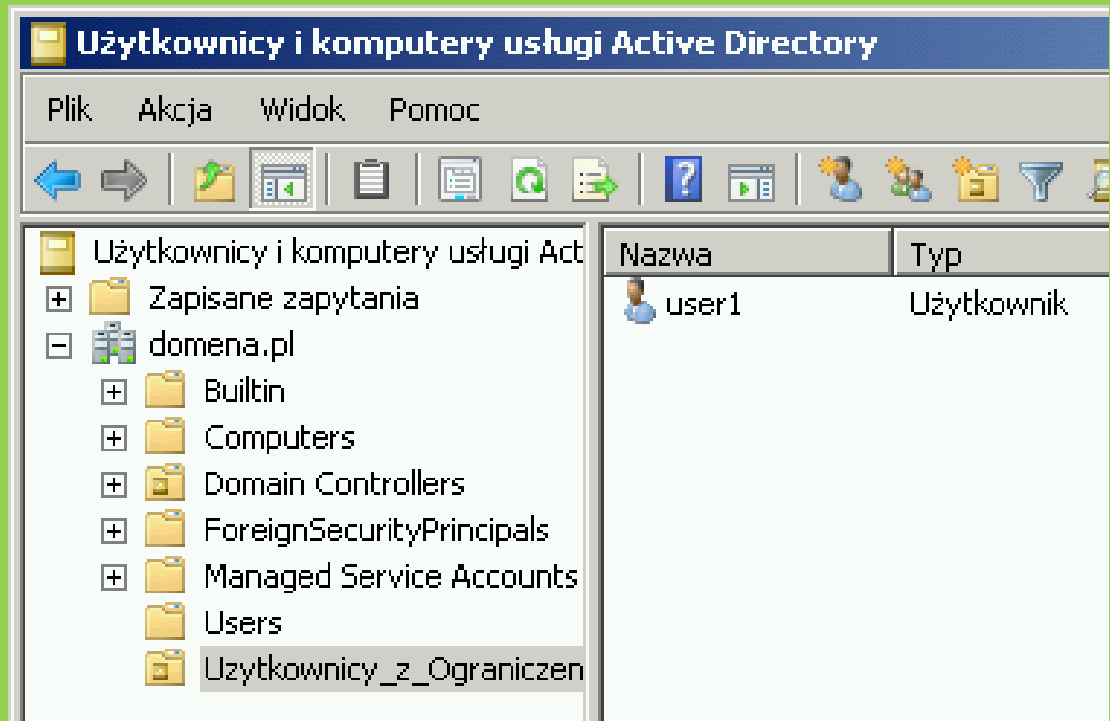
PRZYKŁADY

Przykład 1:

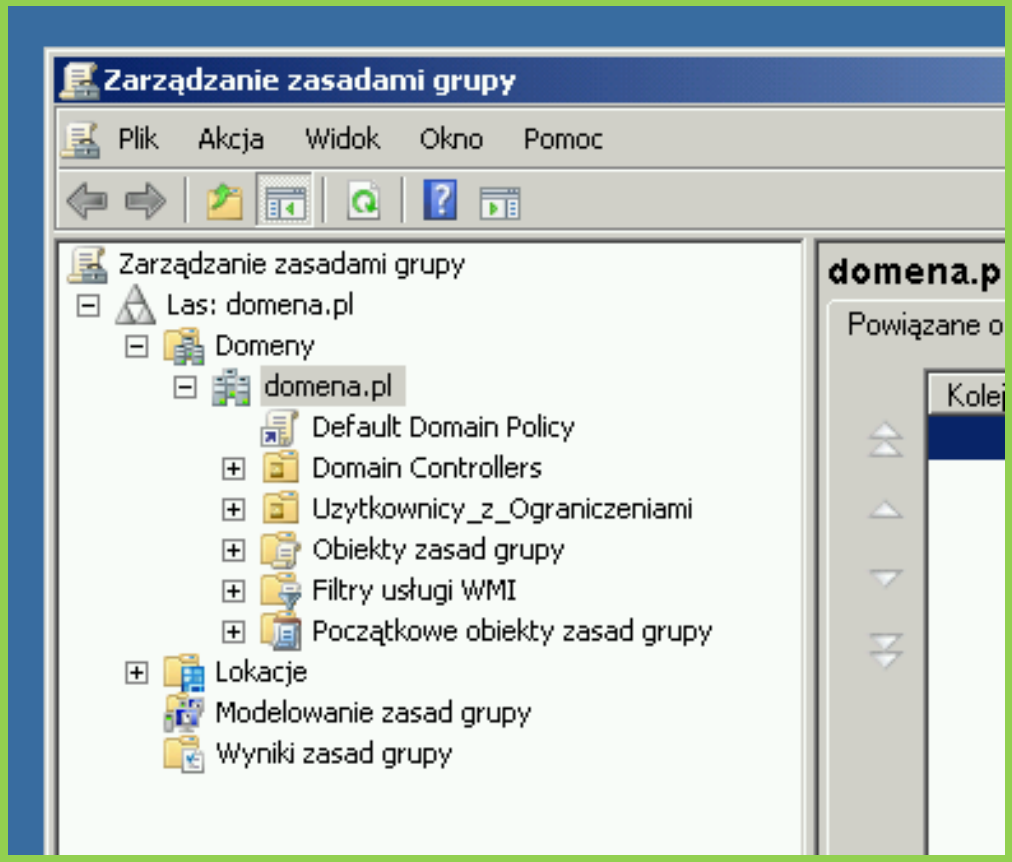
Aby pokazać Wam, w jaki sposób tworzyć i zarządzać zasadami, przygotuję taką, która zabroni konkretnej grupie użytkowników dostępu do panelu sterowania. Zanim to zrobię, utworzę najpierw jednostkę organizacyjną Uzytkownicy_z_Ograniczeniami i dodam do niej użytkownika user1.

W tym celu uruchamiam:

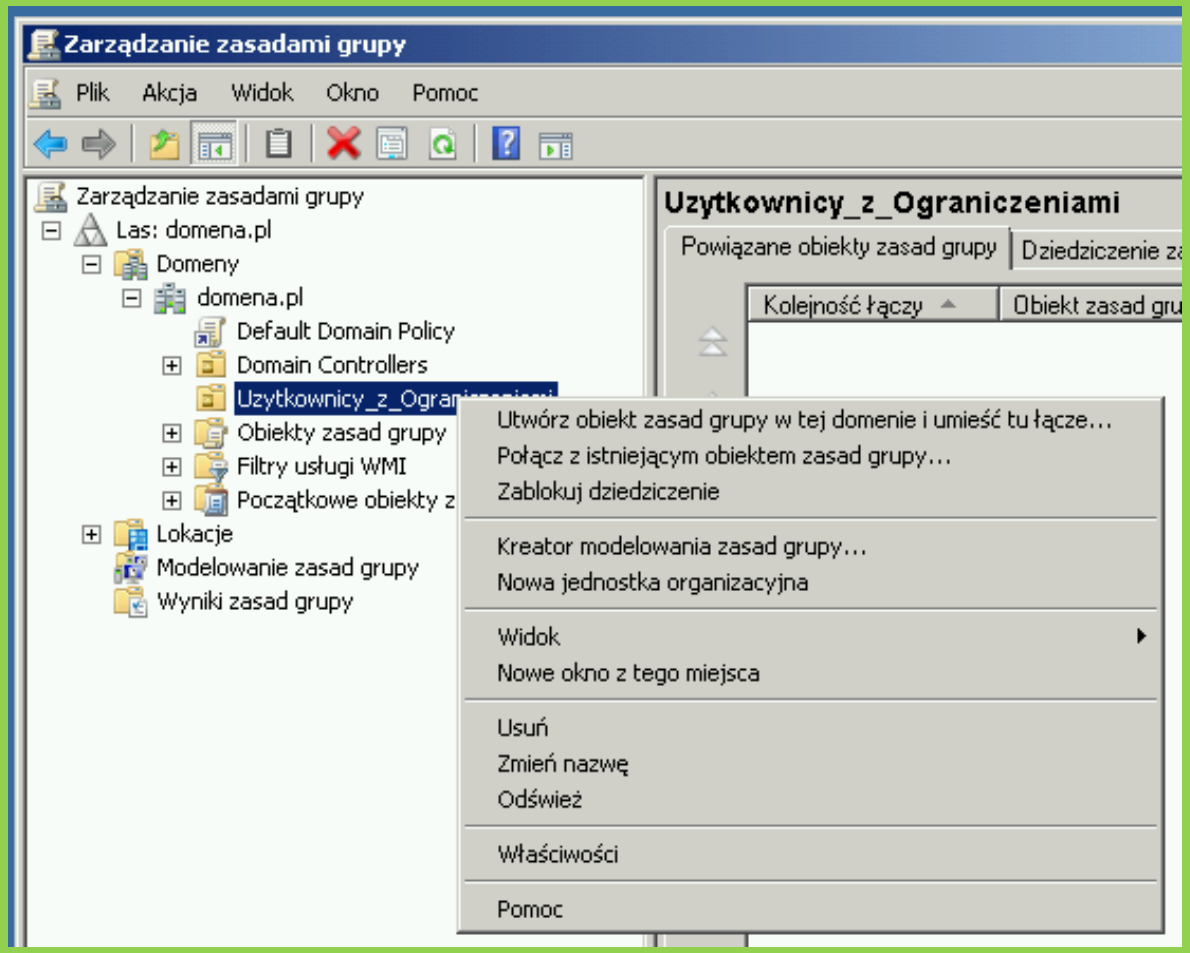
Narzędzia Administracyjne->Uzytkownicy i komputery usługi Active Directory

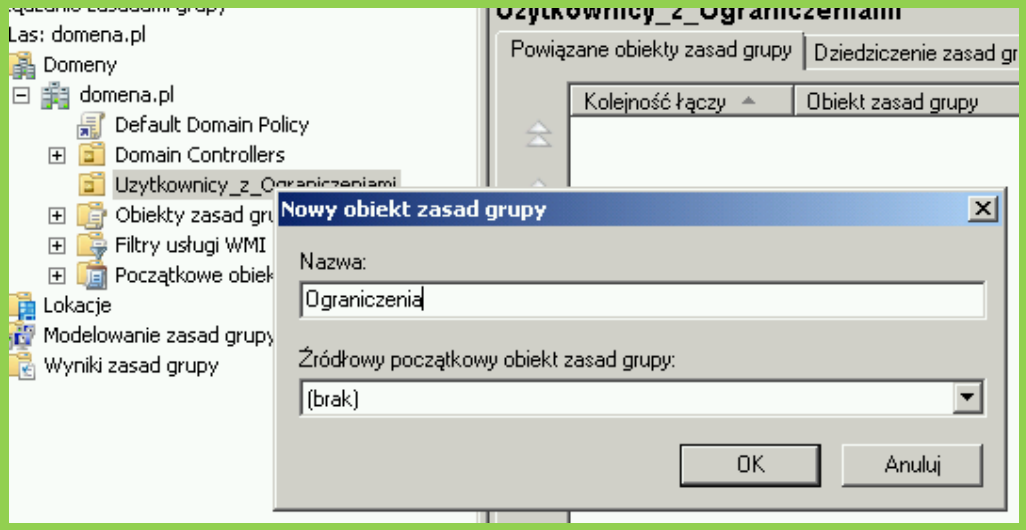


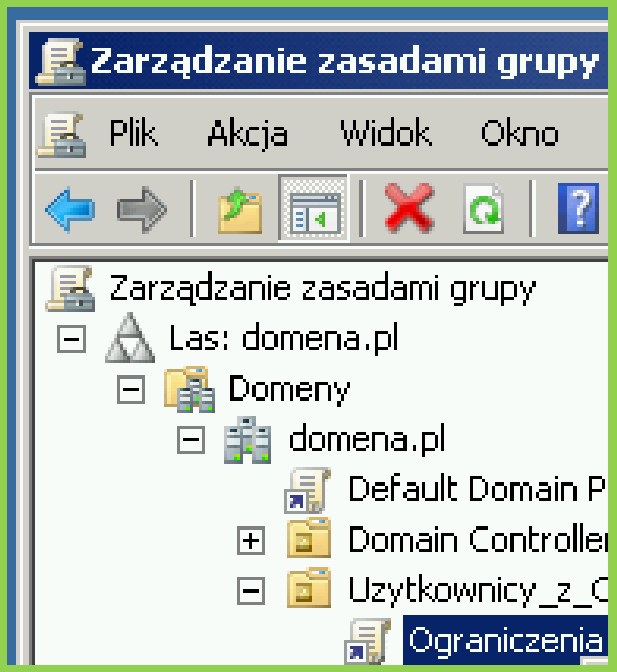
Uruchamiamy ponownie konsolę Group Policy Management, jak widać pojawił się stworzony w AD kontener Użytkownicy_z_Ograniczeniami.



Następnie do kontenera Uzytkownicy_Z_Ograniczeniami dodaję nowy obiekt GPO (o nazwie Ograniczenia)…



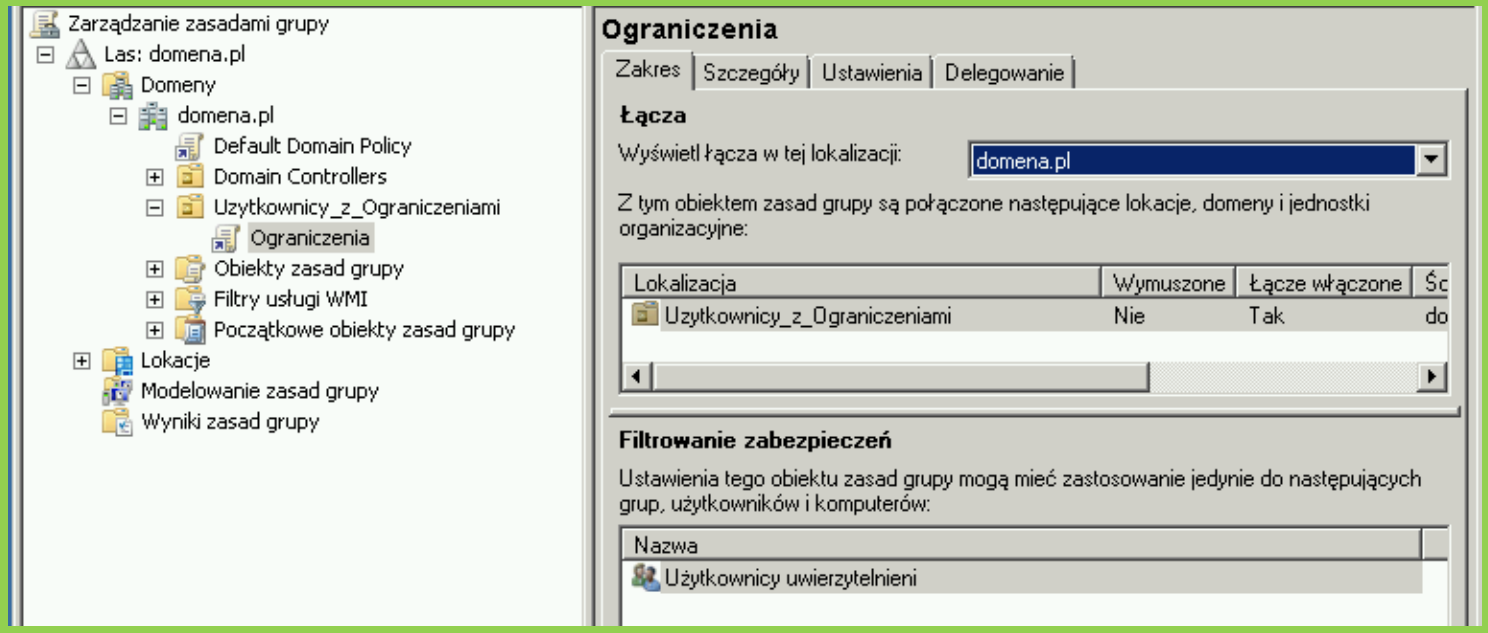




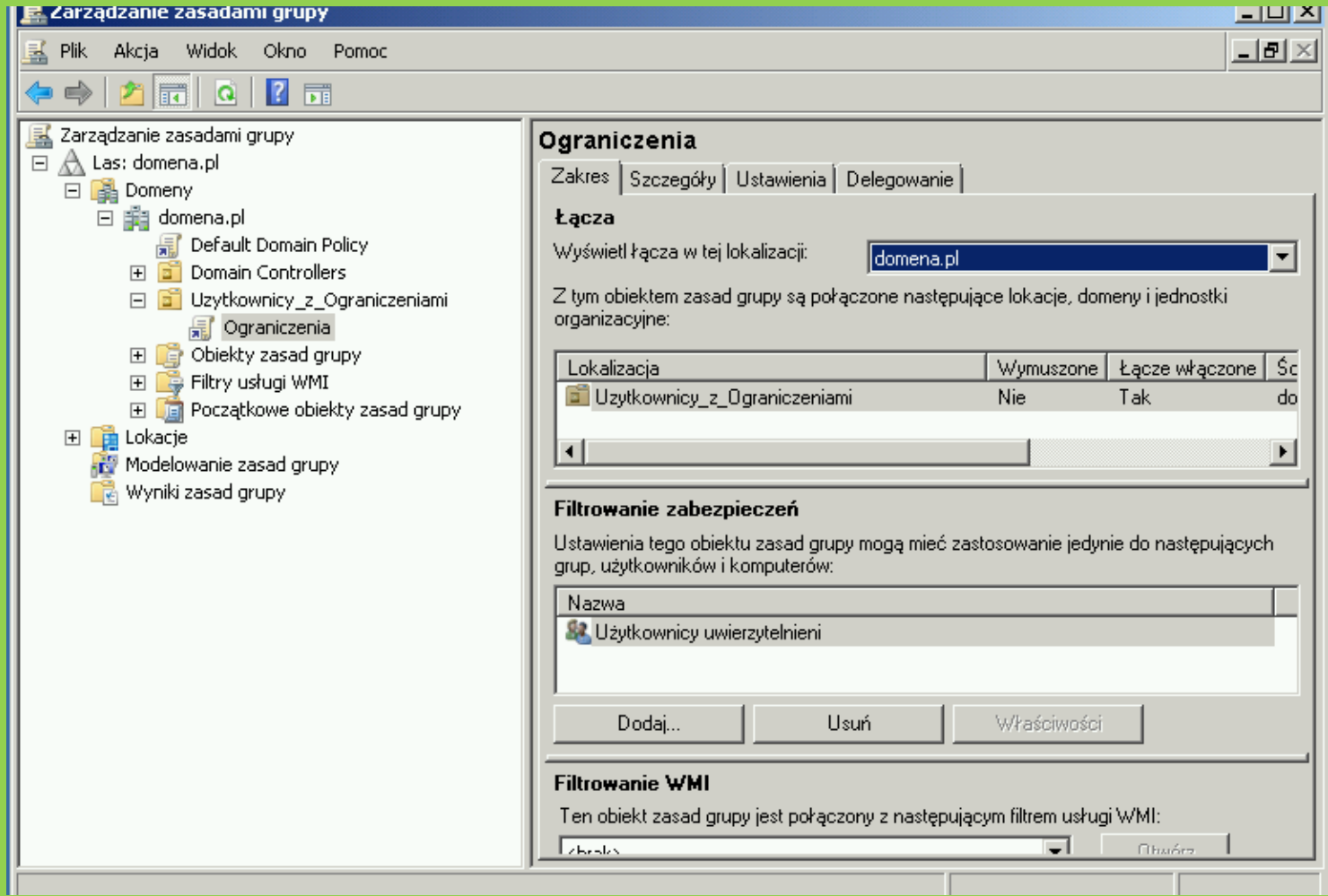
UWAGA: Stworzenie kontenera Uzytkownicy_z_Ograniczeniami nie spowodowało, że domyślnie nasza zasada będzie działać dla użytkowników w nim się znajdujących.

Natomiast stworzenie samego obiektu GPO w odpowiednim miejscu struktury (jednostce organizacyjnej) ogranicza zasięg działania do tej jednostki.

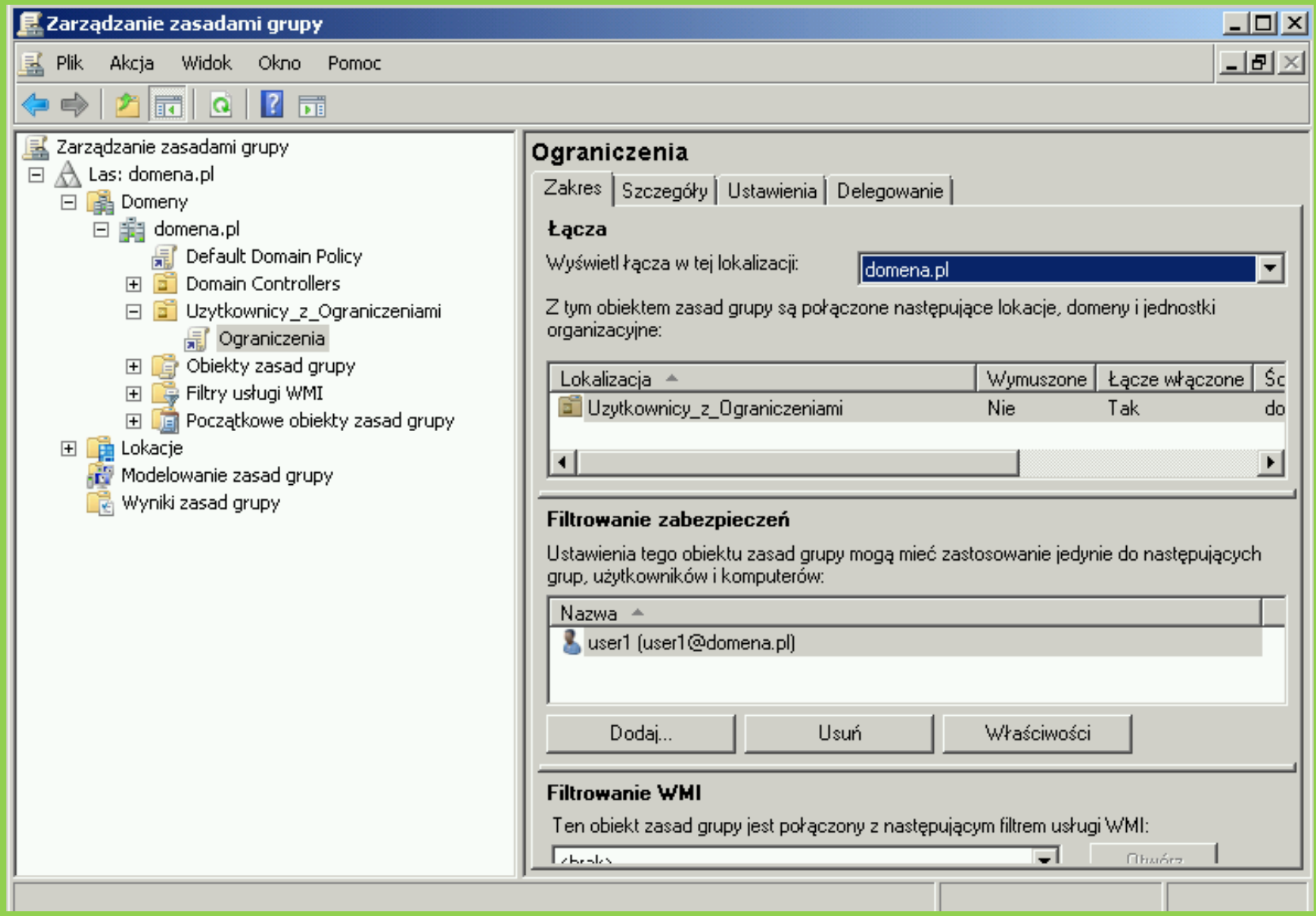
To do jakich użytkowników lub grup dany obiekt GPO będzie miał zastosowanie można kontrolować również za pomocą innego mechanizmu – polega on na kliknięciu obiektu prawym klawiszem myszy i wymedytowaniu opcji FILTROWANIE ZABEZPIECZEŃ widocznej po prawej stronie.



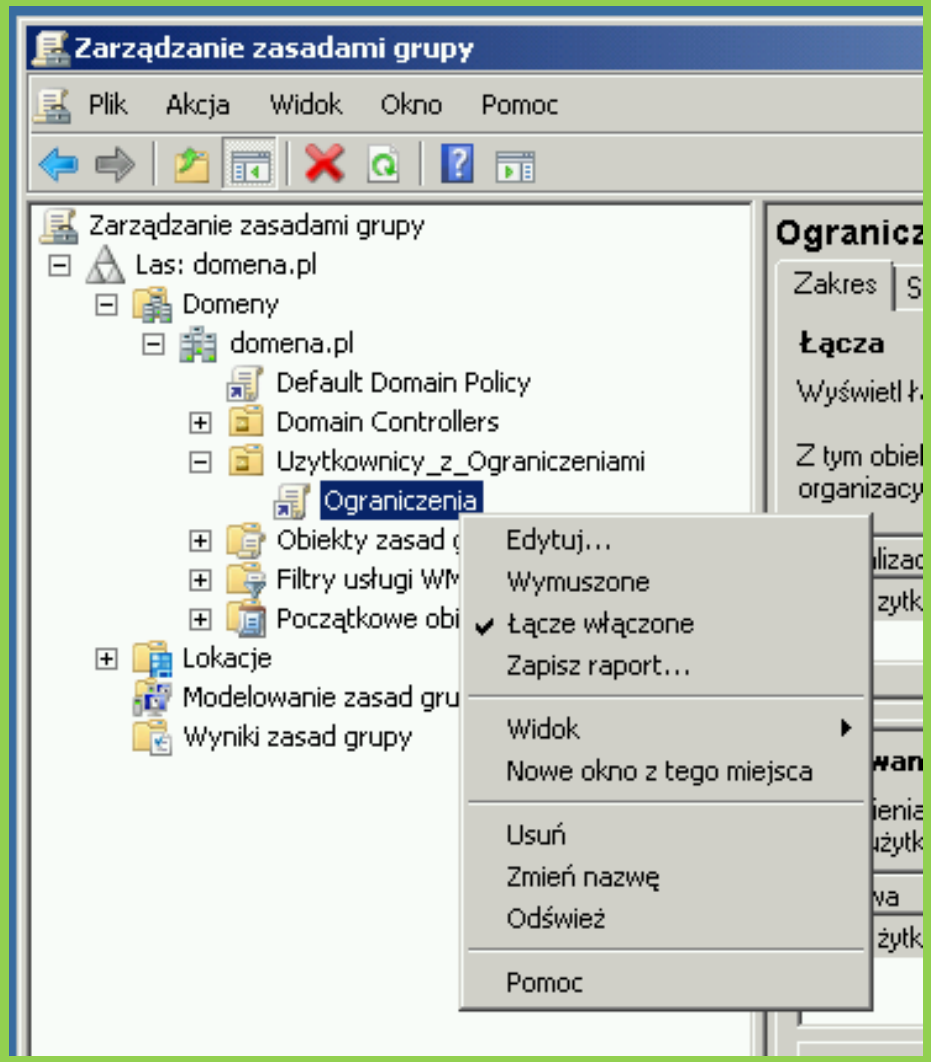
Klikamy w element Użytkownicy uwierzytelnieni i wybieramy Usuń (usuwamy w tym momencie wszystkich użytkowników spod działania zasady, nie chcemy, aby nasza zasada działała dla wszystkich użytkowników lecz dla konkretnych)



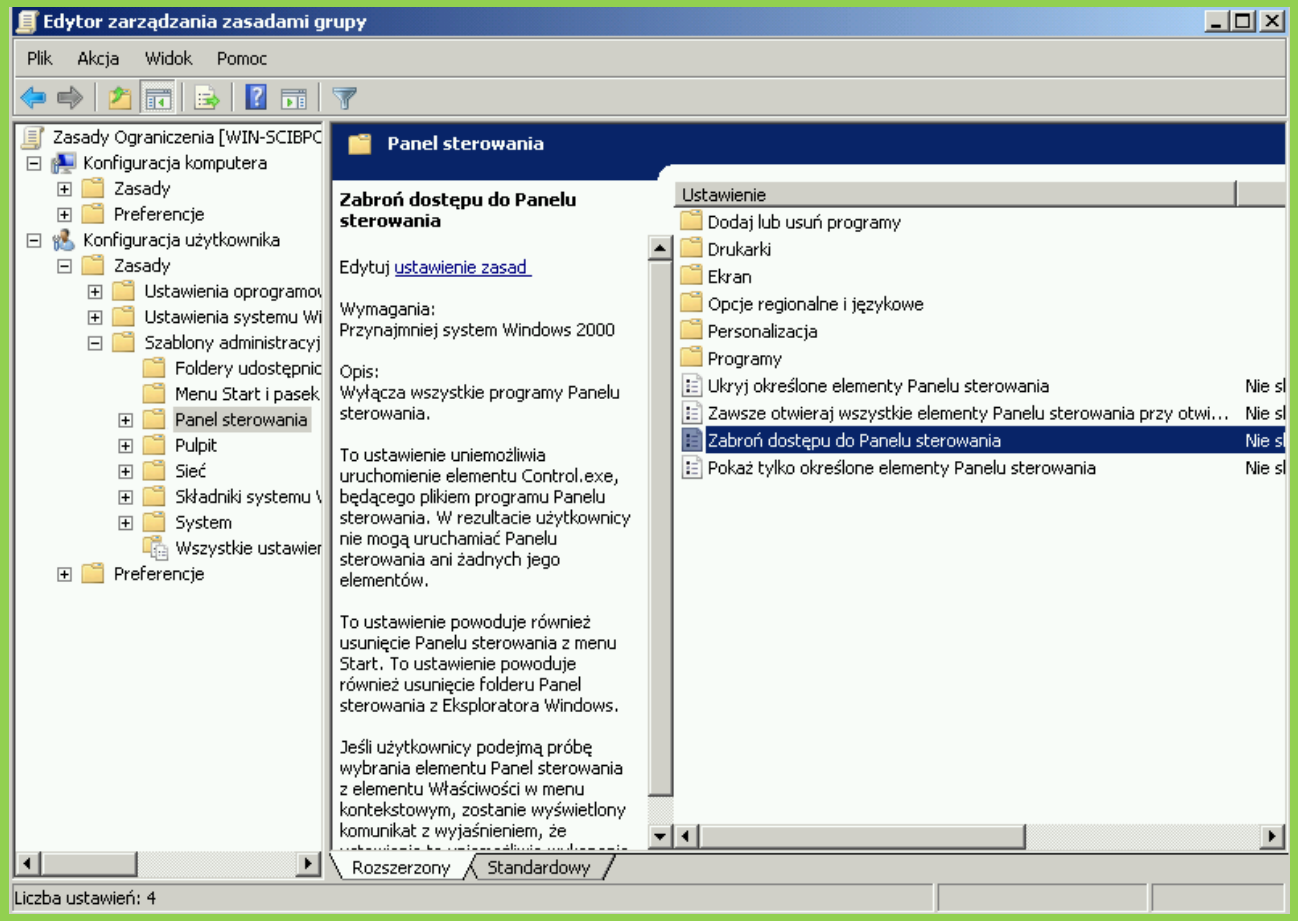
Następnie dodajemy użytkowników, dla których zasada będzie działać…



Dalej zaznaczam utworzony obiekt GPO i wybieram opcję „EDYTUJ”

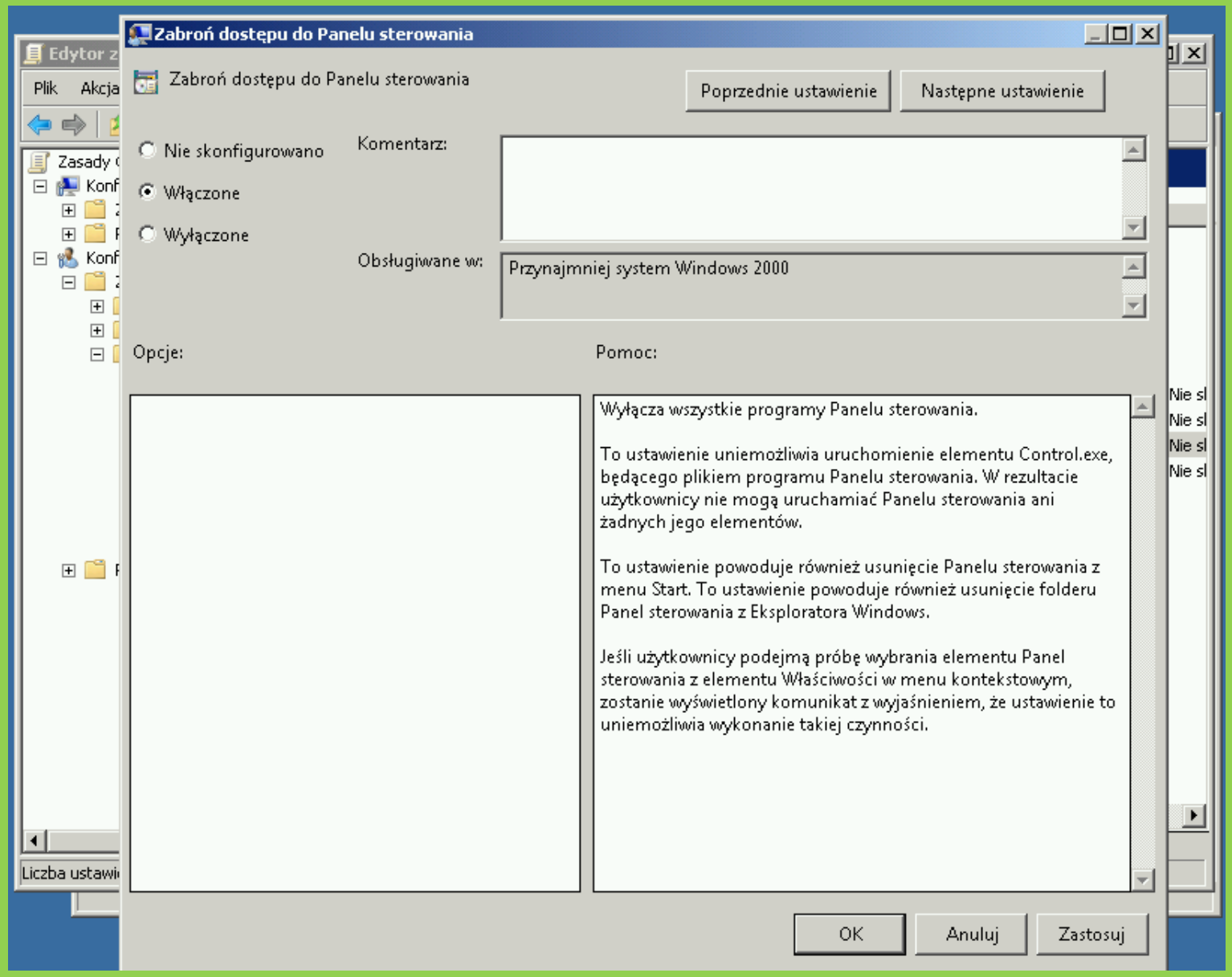


Następnie należy wyedytować odpowiednią zasadę…

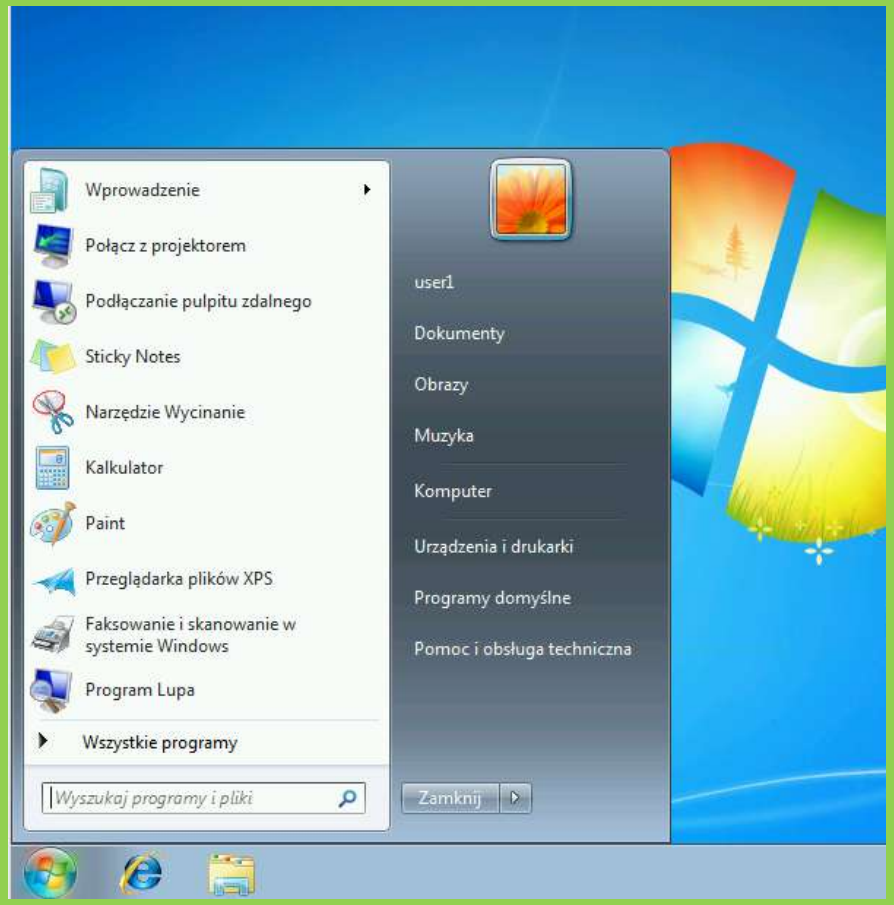


Konfiguracja użytkownika →Zasady → Szablony Administracyjne → Panel sterowania : zabroń dostępu

Należy włączyć to ograniczenie



Po wszystkim wystarczy pozamykać okna pootwierane po drodze i koniec…



UWAGA:

Jeśli zasady wprowadzamy kiedy już użytkownik jest zalogowany wówczas zaczną one działać dopiero po określonym czasie lub przy następnym zalogowaniu. Możemy również zasady odświeżyć stosując polecenie konsoli Windows na stacji roboczej o składni

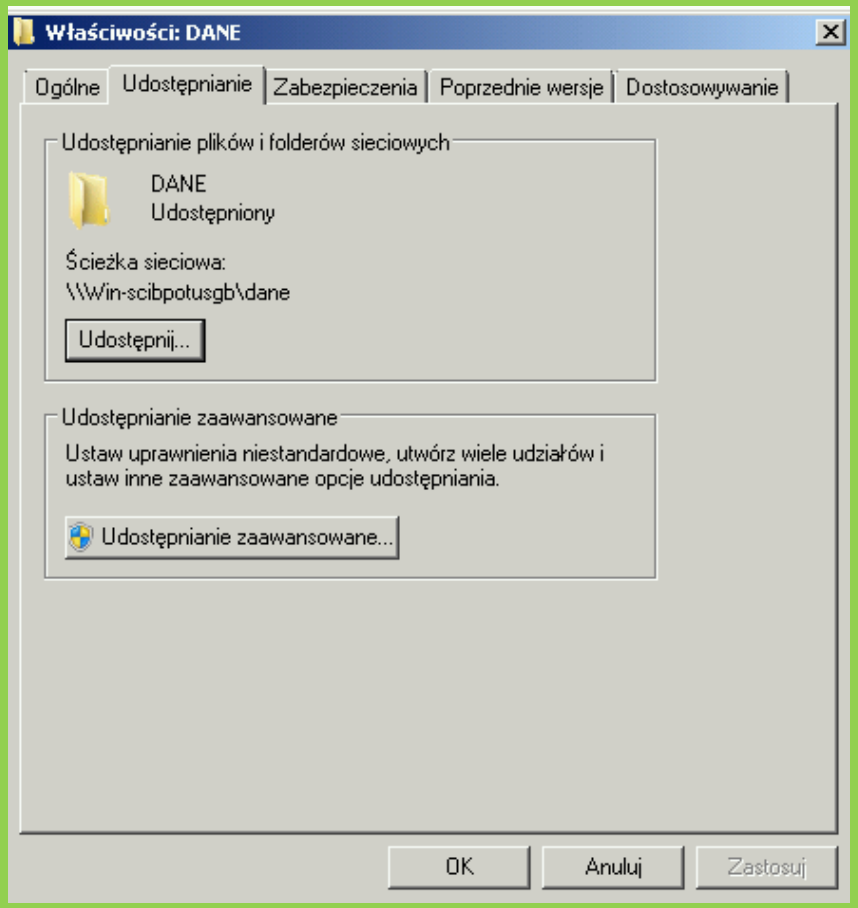
gpupdate /force

, wówczas zasada zacznie działać od razu.

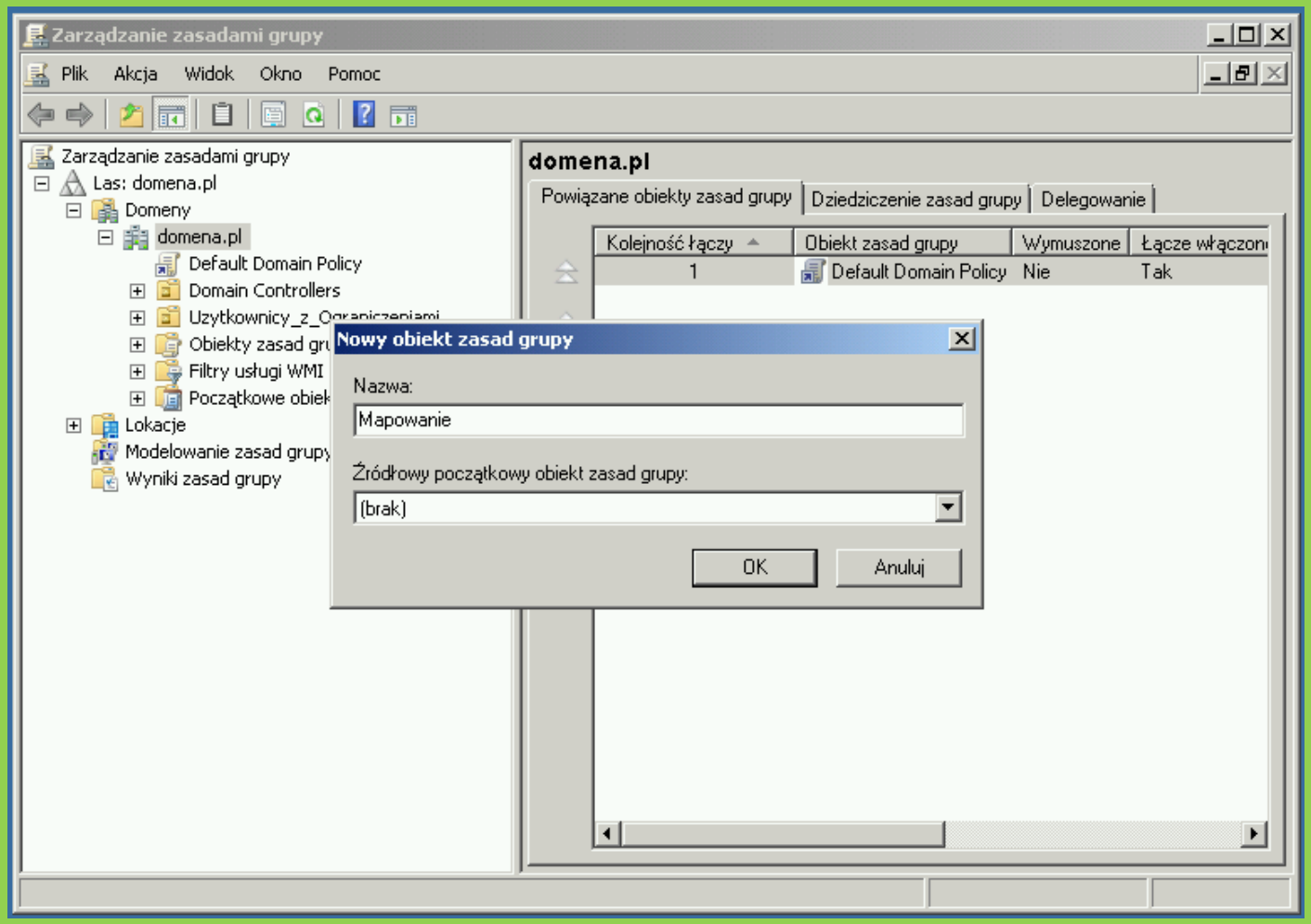
Przykład 2:

Mapowanie udostępnionych zasobów za pomocą GPO.

Na początek należy udostępnić zasób (w tym wypadku będzie to katalog C:\DANE):

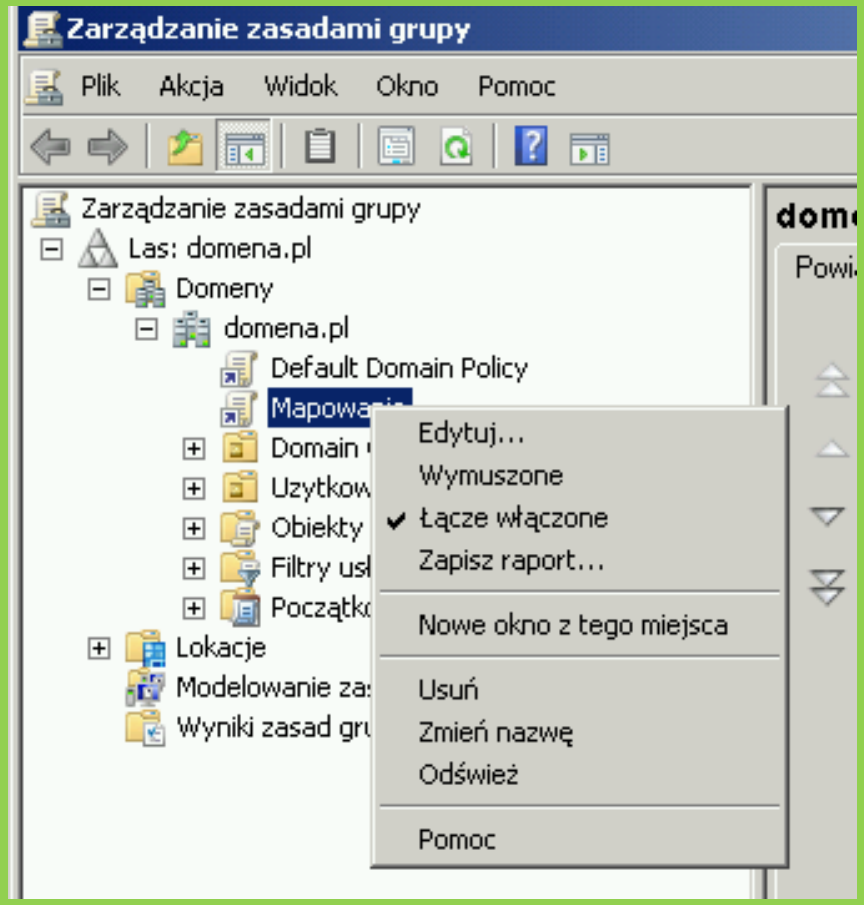


Dalej trzeba stworzyć obiekt GPO

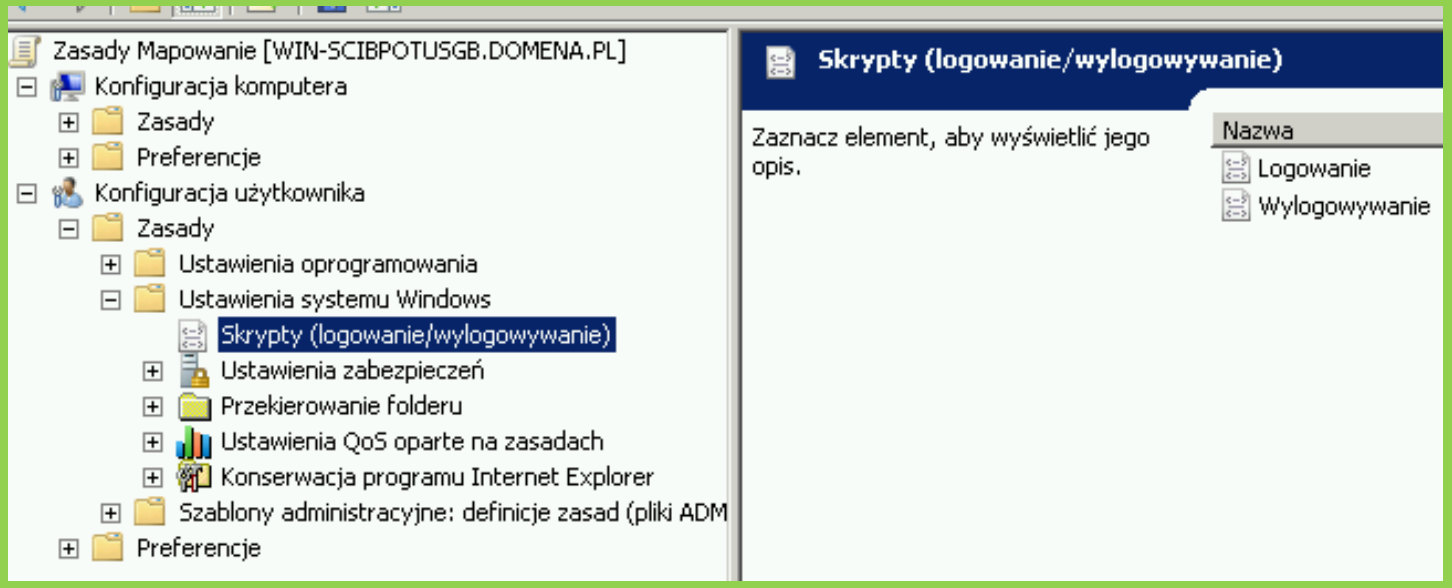


UWAGA: Warto tworząc obiekty GPO nadawać im nazwy które informują o celu/zadaniu jakie pełni dany obiekt (łatwiej dzięki temu nad tym zapanować).

Następnie należy wyedytować obiekt (w tym wypadku nazwany MAPOWANIE)



W ramach obiektu MAPOWANIE będzie trzeba utworzyć odpowiedni skrypt związany z mapowaniem zasobu na kontach użytkowników.

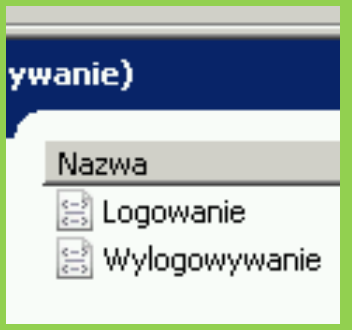


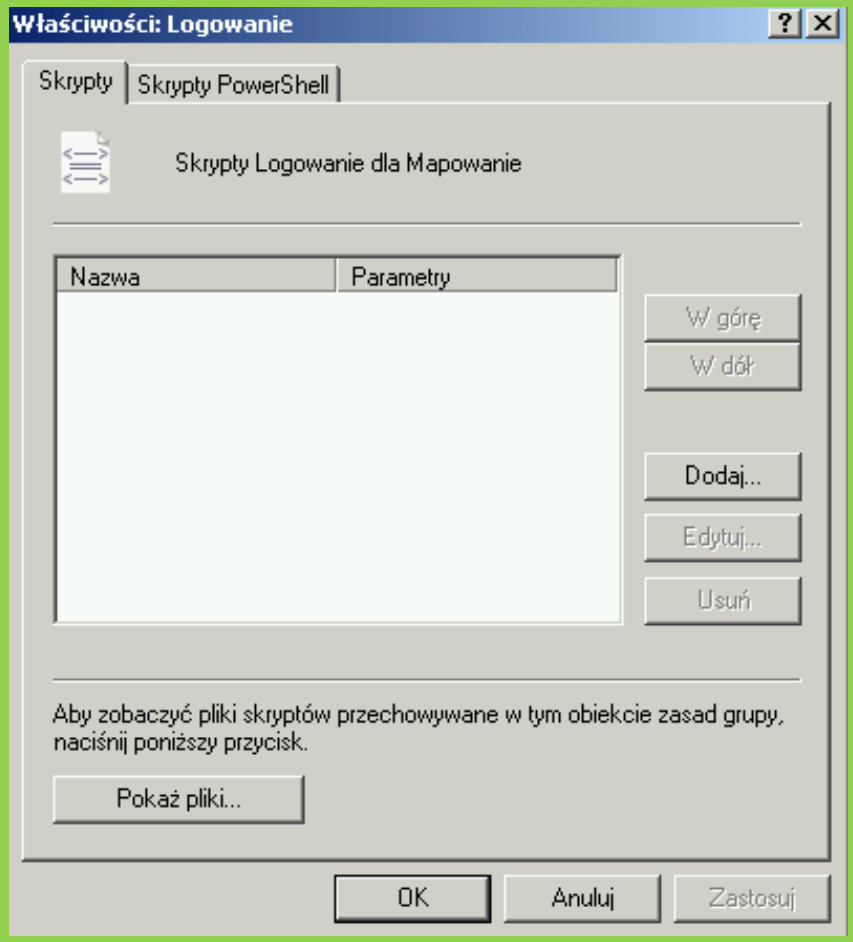
Chcemy by mapowanie działało na wybranych (w naszym wypadku wszystkich) kontach użytkowników. Dlatego rozwijamy:

Konfiguracja użytkownika→Zasady→Ustawienia systemu Windows→Skrypty

Konkretnie będzie to skrypt LOGOWANIA … czyli wykonywany będzie w trakcie logowania się użytkownika.

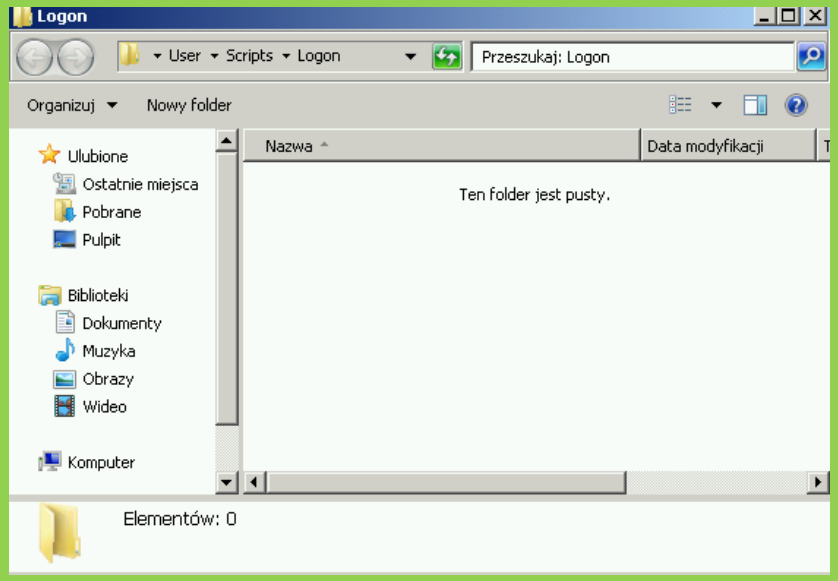
Podwójne kliknięcie na pozycji LOGOWANIE powoduje otwarcie odpowiedniego okna do konfiguracji:





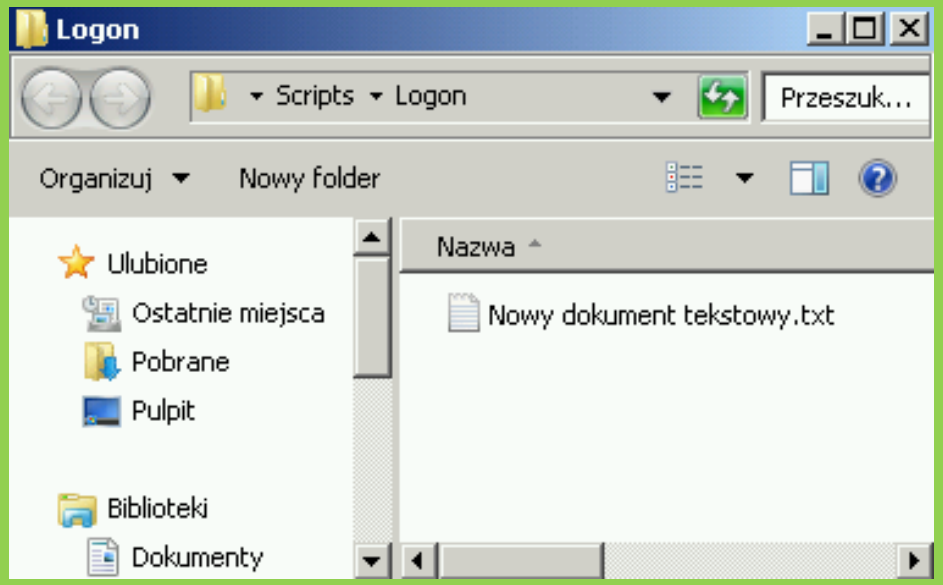
W zakładce Srypty należy kliknąć na przycisk *Pokaż pliki…*

Dzięki temu otworzy się okno z katalogiem, w którym należy utworzyć odpowiedni skrypt (plik BAT, COM… etc).

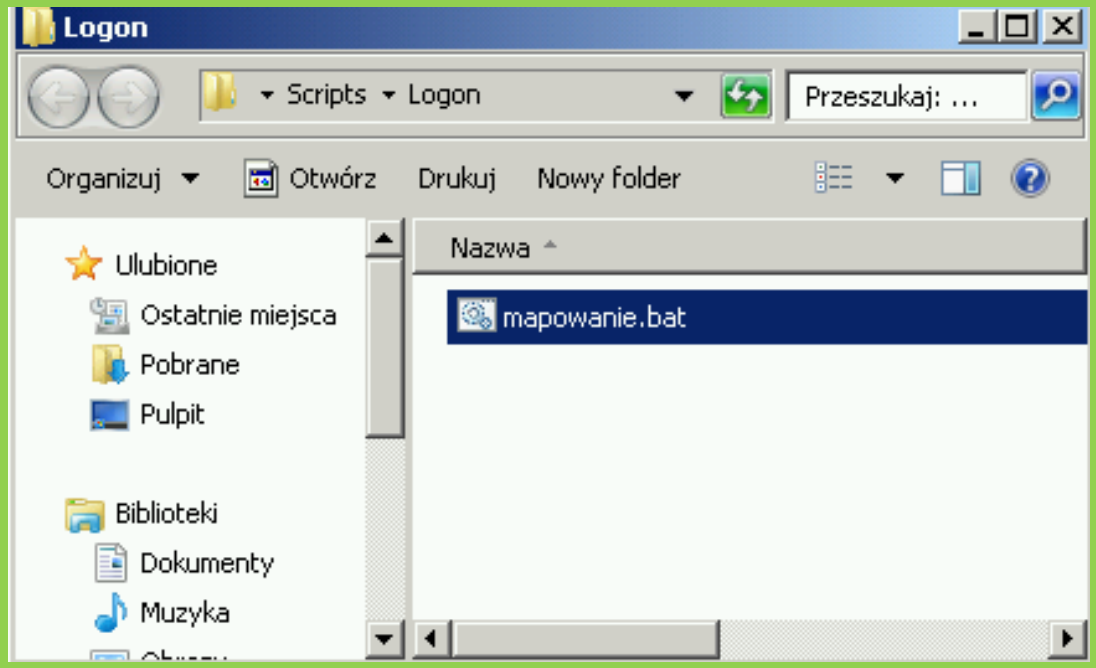


UWAGA: nie powinno się zmieniać lokalizacji pliku ze skryptem (może to spowodować, że nie będzie on działał)

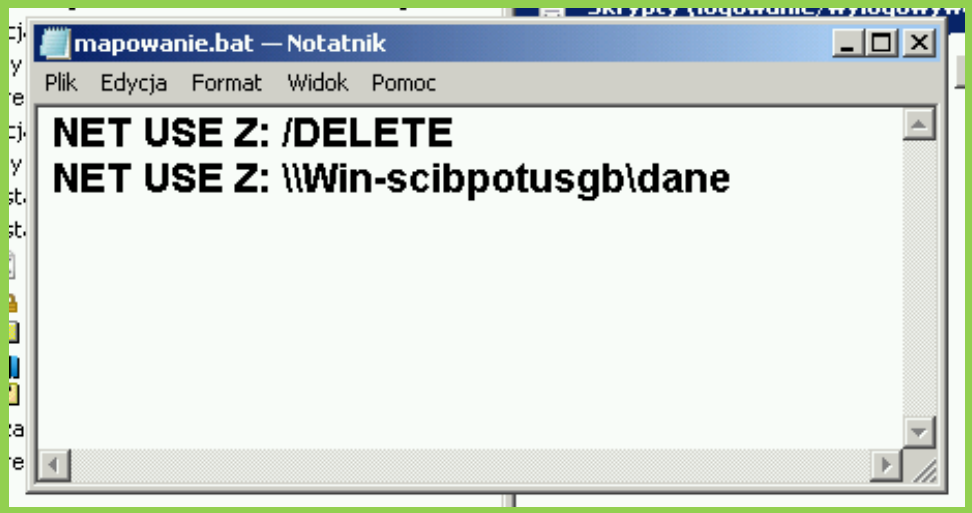
Należy w katalogu utworzyć zwykły plik tekstowy, a następnie zmienić jego nazwę i rozszerzenie na np. *.BAT.



→

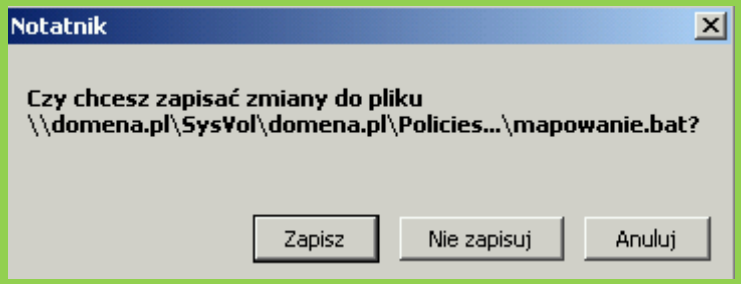


Dalej trzeba wymedytować plik (skrypt mapowania) w taki sposób by działał prawidłowo – edycji dokonuje się za pomocą NOTATNIKA.

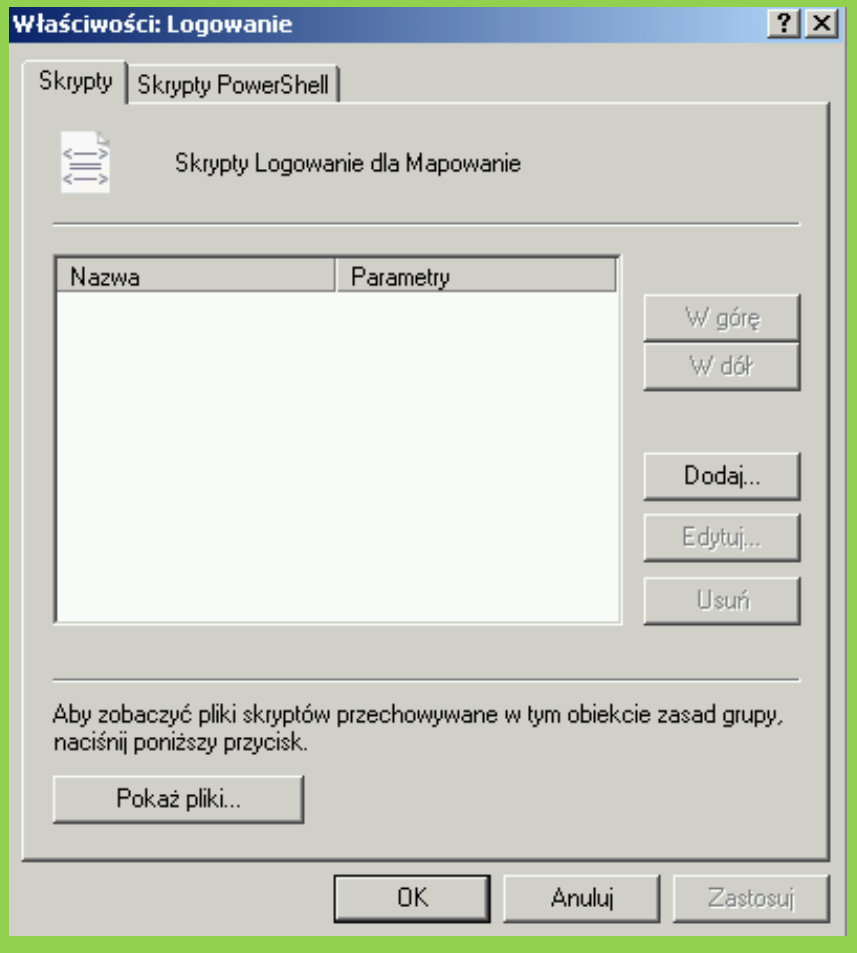


Należy w pliku wpisać powyższa wartość odpowiednio ją dostosowując – wyjaśnienie co oznaczają poszczególne opcje później…

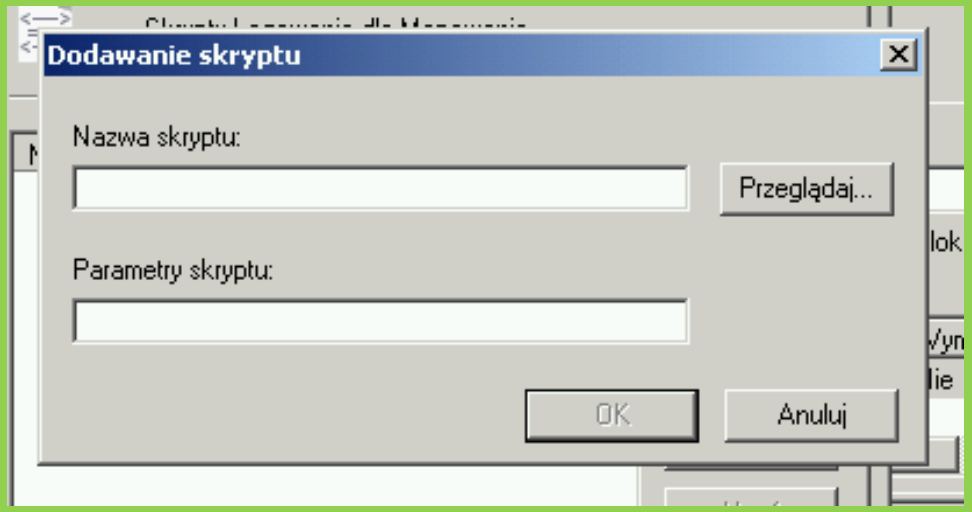
Mając już wyedytowany odpowiednio plik ze skryptem zapisujemy zmiany w nim i zamykamy okno z folderem w którym się znajduje.

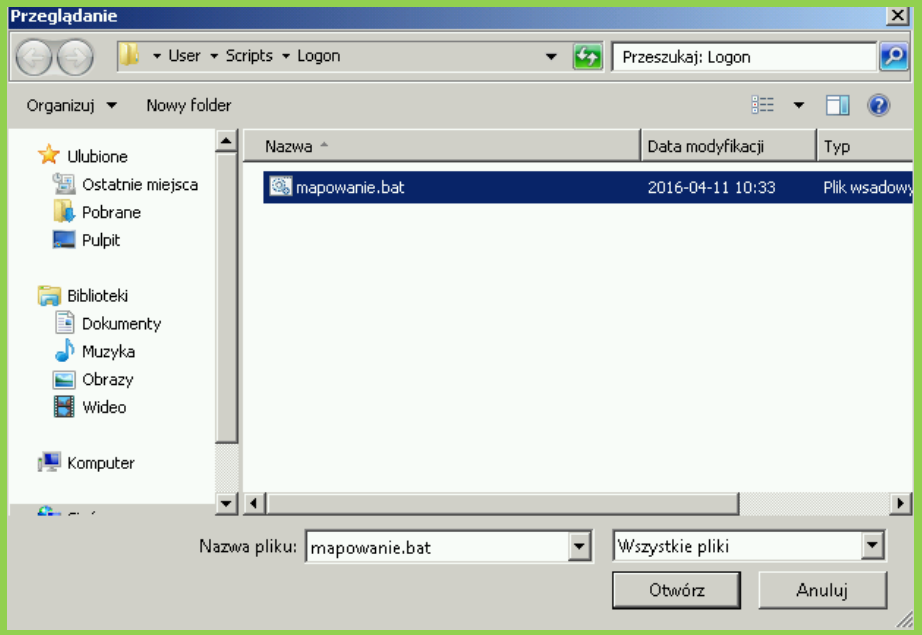


Dalej trzeba w zakładce *Skrypty* okna *LOGOWANIE* kliknąć na guzik **Dodaj...**



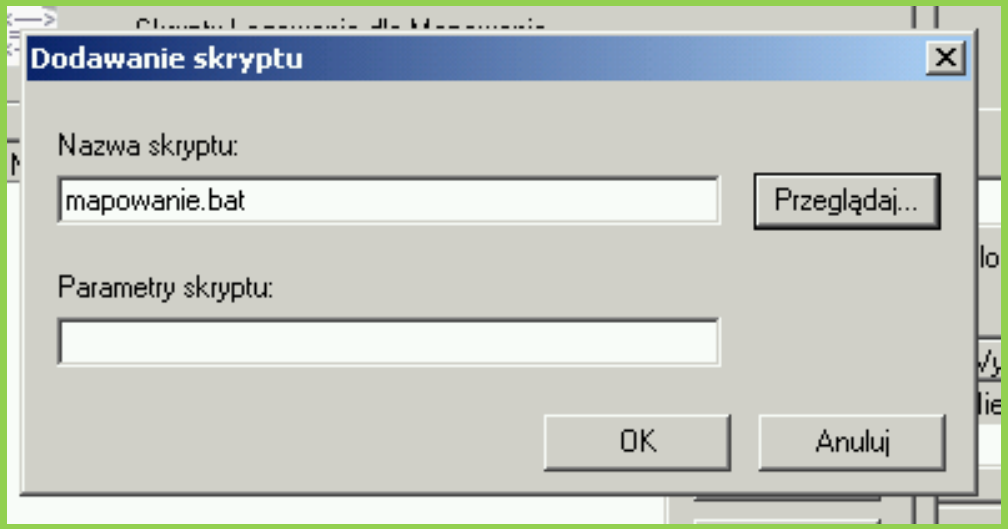
Pojawi się okno w którym trzeba wskazać skrypt, który ma być uruchamiany w trakcie logowania użytkowników:

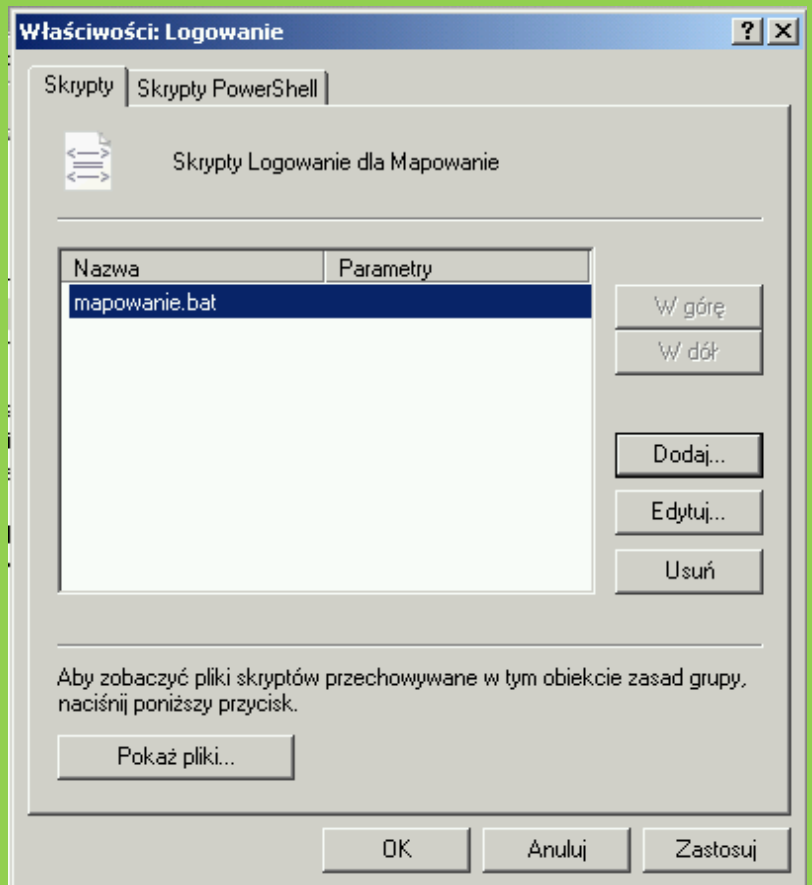




Najlepiej kliknąć na Przeglądaj… i wskazać plik, którym przed chwilą był utworzony i zmodyfikowany. Dalej trzeba zatwierdzić wybór pliku poprzez kliknięcie Otwórz.

Mając już wskazany odpowiedni plik należy zatwierdzić go do dodania na listę skryptów uruchamianych w trakcie logowania (przycisk OK.).





Plik powinien być już widoczny na liście skryptów LOGOWANIA.

Teraz wystarczy kliknąć OK. i pozamykać pootwierane okna… Zasada powinna już obowiązywać. Należy jedynie pamiętać, że zmiany dotyczące zasad użytkownika odświeżają się w momencie ponownego logowania (lub co pewien okres czasu).

Jeśli chcemy mieć pewność, że zasada zadziała od razu można użyć polecenia GPUPDATE /FORCE

Wyjaśnienie działania pliku mapowanie.BAT:

NET USE ← polecenie, które umożliwia m.in. mapowanie zasobów z sieci lokalnej oraz zwalnianie już zmapowanych zasobów

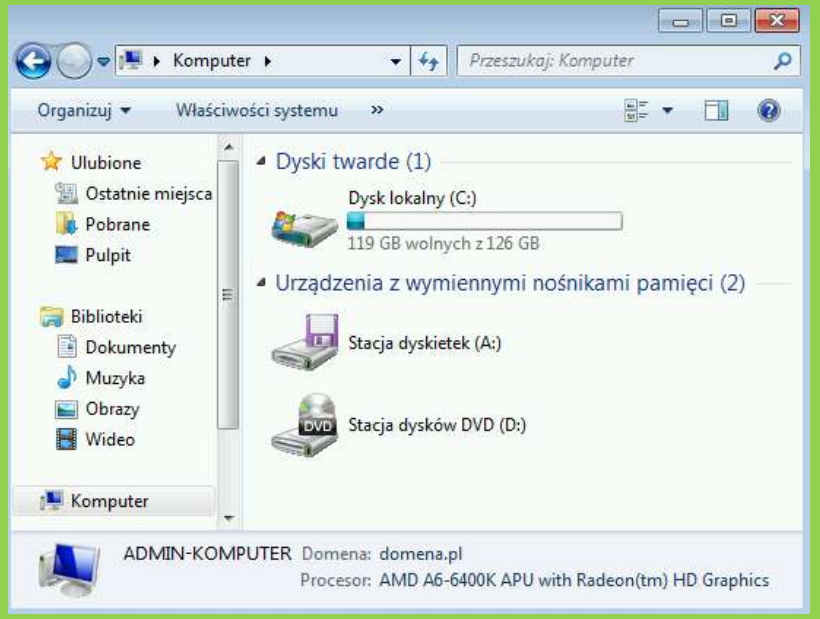
NET USE Z: /DELETE ← zwalnia zasób (jeśli był) a tym samym zwalnia literę Z: w Moim komputerze. Polecenie o tyle istotne, gdyż nigdy mapując nie ma pewności, że dana litera nie została już zajęta wcześniej.

NET USE Z: \\nazwa-serwera\nazwa -zasobu ← mapowanie zasobu o określonej nazwie udostępnionego na określonym serwerze o określonej nazwie (nazwę można zastąpić numerem IP serwera). Zasób będzie zmapowany w Moim komputerze na konkretną wskazaną literę – w tym wypadku Z:

Litera, na którą dokonuje się mapowania musi być wolna!!!

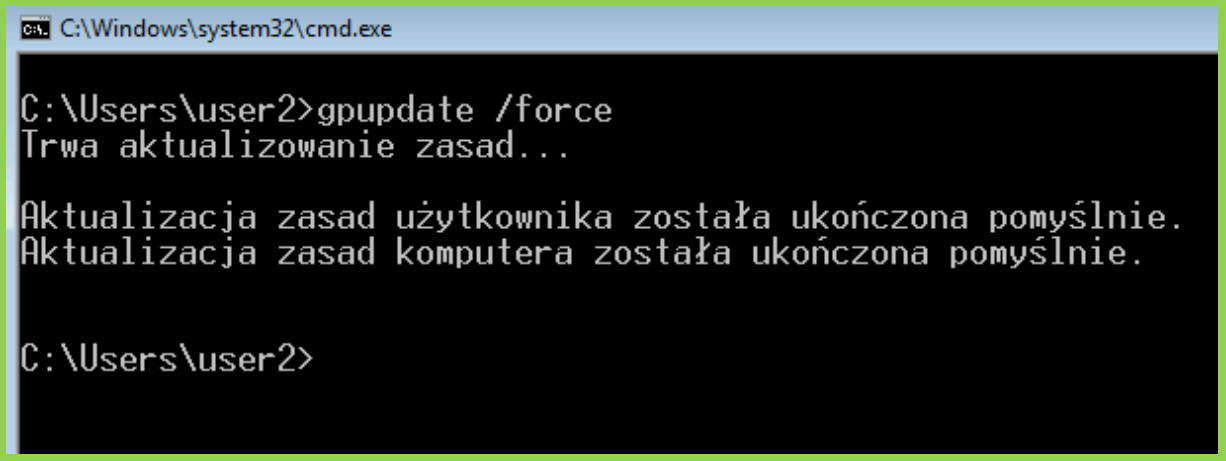
Efekt:

→



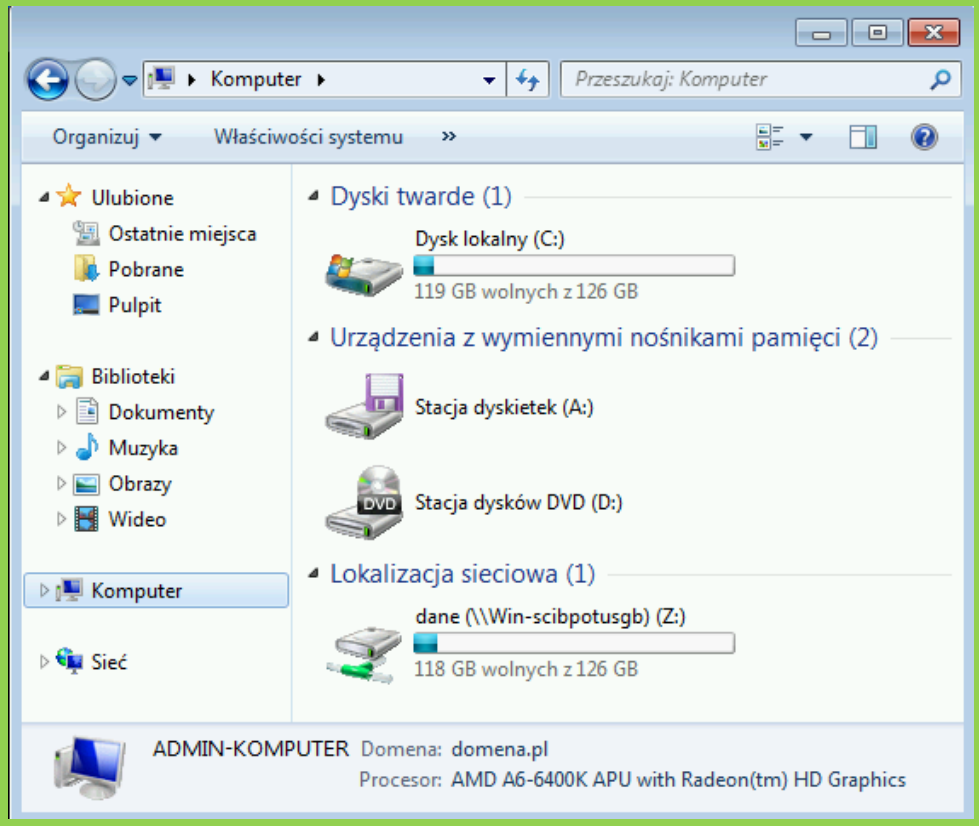
BRAK EFEKTU…?

Rozwiązanie : GPUPDATE /FORCE



→

Ponowne logowanie i →



PODSUMOWANIE

Mechanizm GPO to bardzo rozbudowany w możliwości oraz bardzo wygodny sposób na zarządzaniem środowiskiem klienckim w sieciach lokalnych firm etc.

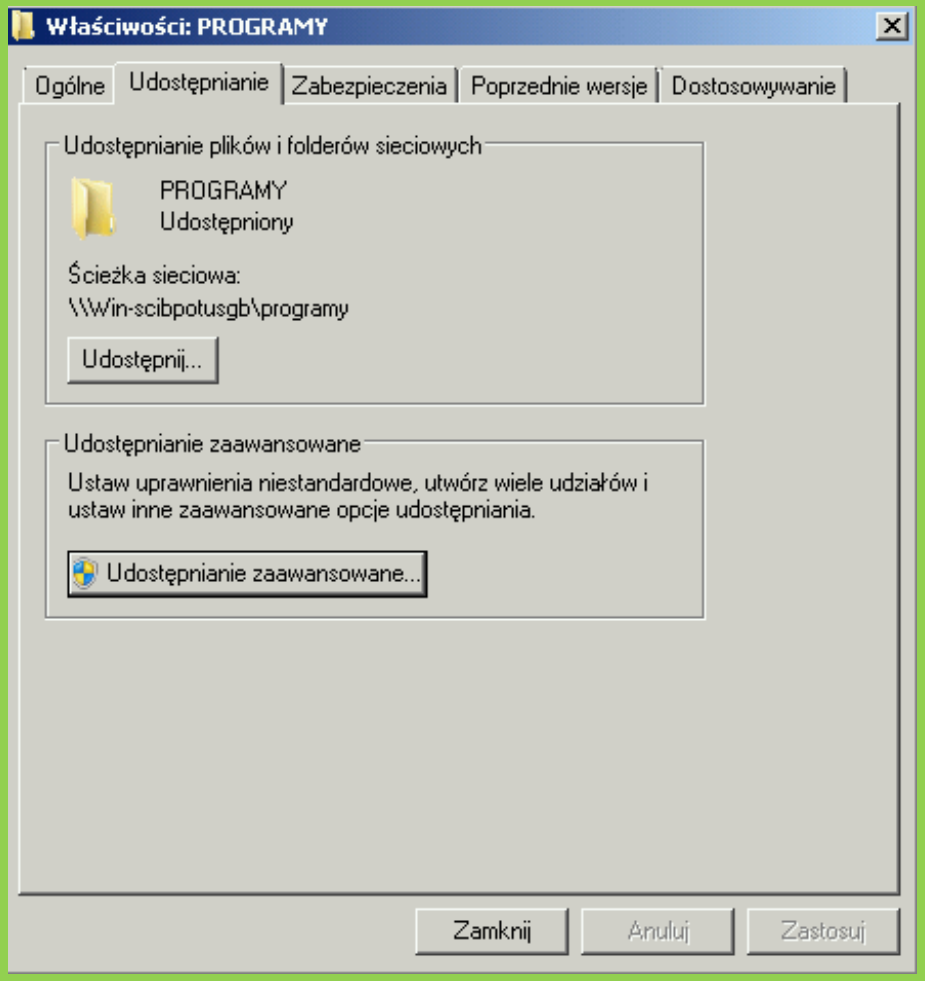
W sposób scentralizowany można łatwo i szybko zmieniać przywileje lub uprawnienia użytkowników.

Inne przykłady – dla ciekawskich

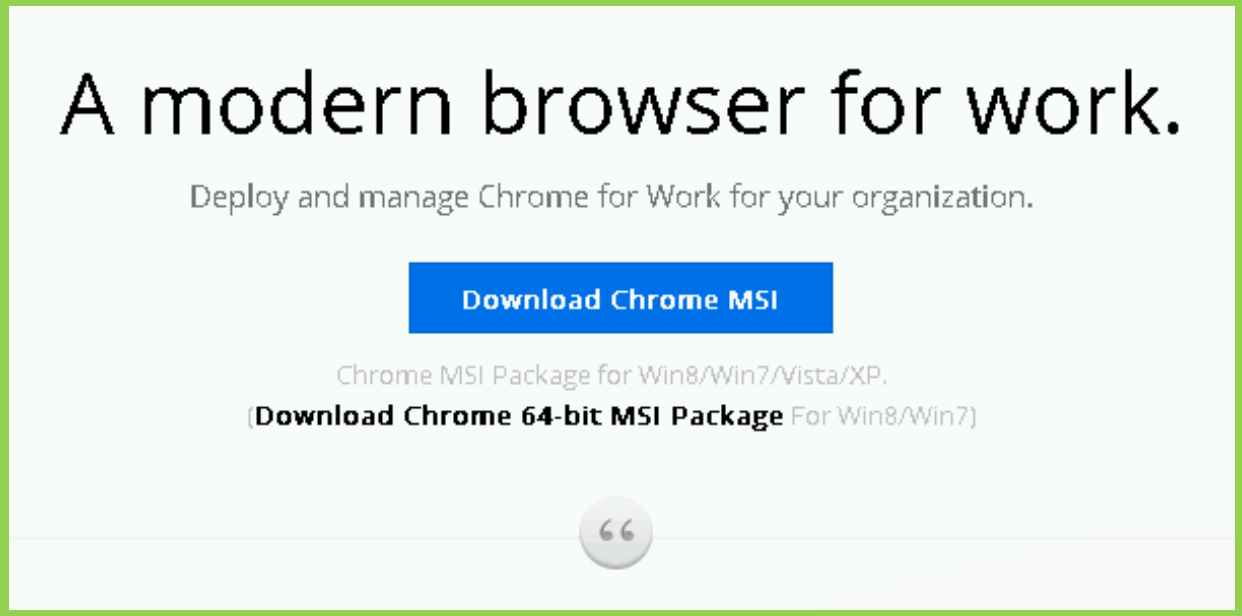
Przykład 3 – zdalne instalowanie oprogramowania na stacjach klienckich

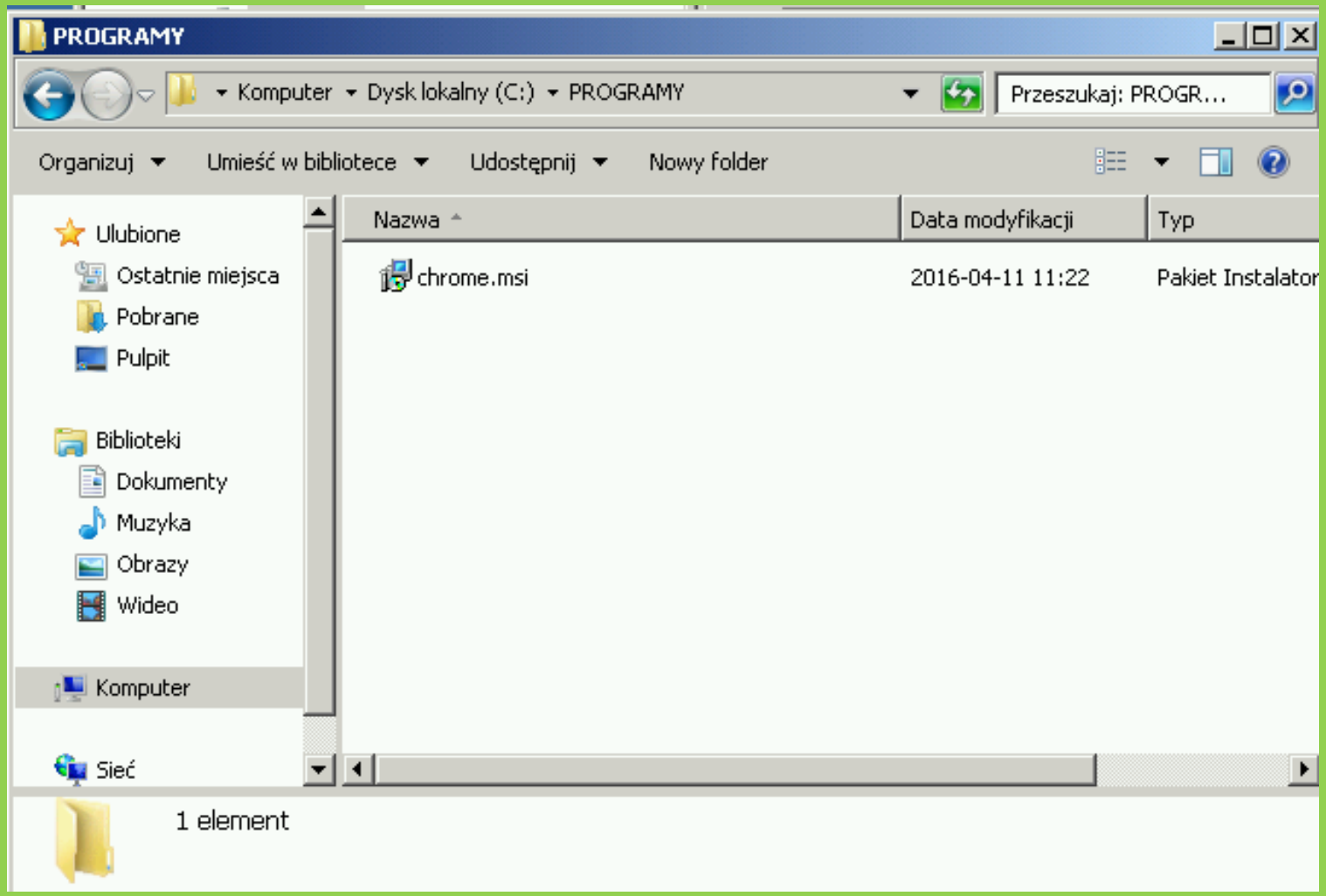
Wprowadzenie: do tego celu stosuje się mechanizm GPO oraz specjalne pakiety instalacyjne oprogramowania (.MSI). Pakiety MSI to nic innego jak ‘paczka’ z instalacją programu, która instaluje dany program nie pytając użytkownika o nic – krótko mówiąc taki pakiet instalacyjny nie wymaga żadnej interakcji użytkownika w trakcie instalacji, co jest niezbędne jeśli instalacja odbywa się w sposób zautomatyzowany i zdalnie.

Krok 1 polegał będzie na tym, że trzeba będzie przygotować oraz udostępnić do odczyty dla wszystkich użytkowników na serwerze katalog, w którym będą znajdowały się paczki MSI. Jest to o tyle istotne, że w czasie instalacji zdalnej pakiet fizycznie będzie zlokalizowany na serwerze w udostępnionym katalogu.

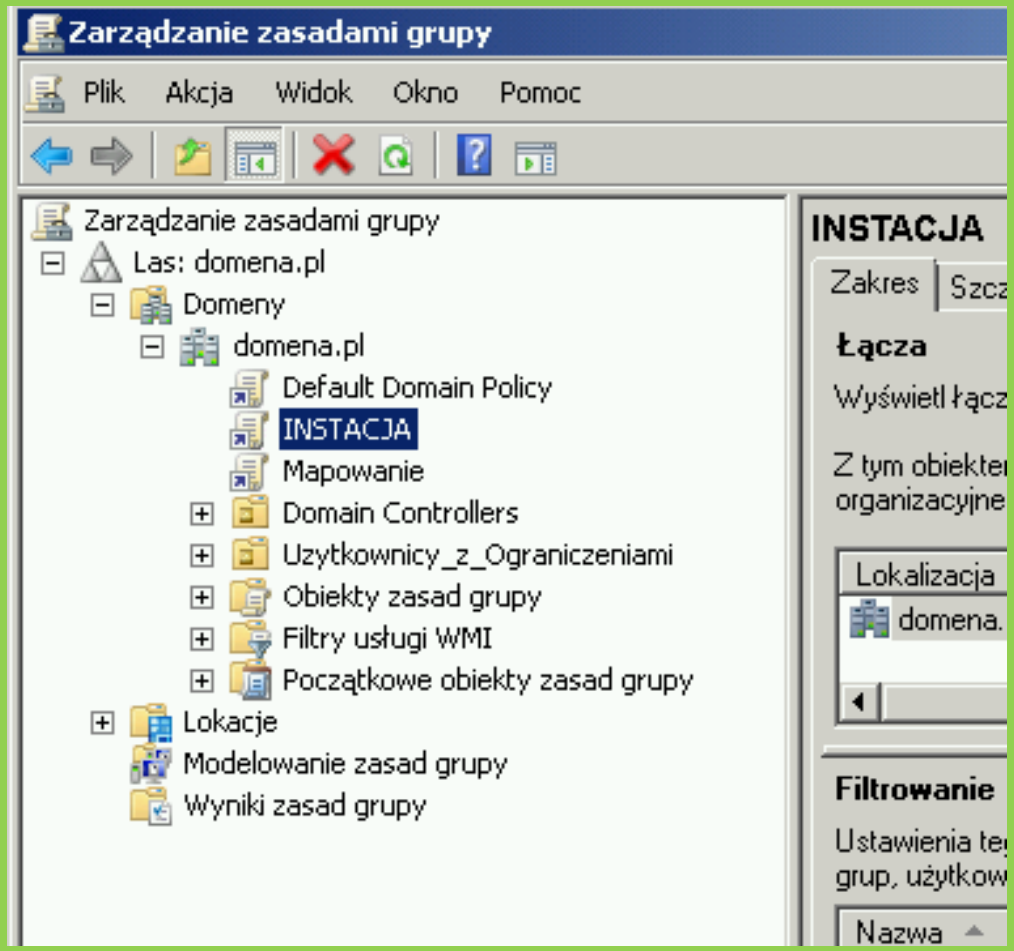


Krok 2 – umieszczenie we w/w katalogu paczki MSI z instalacją programu (np. Google Chrome)




PROGRAMY
Komputer
Dysk lokalny (C:)
PROGRAMY
Przeszukaj: PROGR...
Organizuj
Umieść w bibliotece
Udostępnij
Nowy folder
Ulubione
Ostatnie miejsca
Pobrane
Pulpit
Biblioteki
Dokumenty
Muzyka
Obrazy
Wideo
Komputer
Sieć
Nazwa
Data modyfikacji
Typ
chrome.msi
2016-04-11 11:22
Pakiet Instalator
1 element

Następnie trzeba będzie utworzyć nowy obiekt GPO – jeśli chcemy by obejmował on swym zasięgiem wszystkie komputery można go umieścić na początku hierarchii…



Można też utworzyć sobie w domenie jednostkę organizacyjną (np. o nazwie INSTALACJA_PROGRAM) i umieszczać tam komputery z domeny, na którym ma się dokonać instalacja programów. Wówczas obiekt GPO odpowiedzialny za instalację należy umieścić w tym kontenerze…

W ten sposób można też tworzyć wiele różnych grup dystrybucyjnych oprogramowanie.

Dla potrzeb poglądowych ja skorzystam z pierwszej wersji – instalacja będzie dotyczyć wszystkich komputerów w domenie…

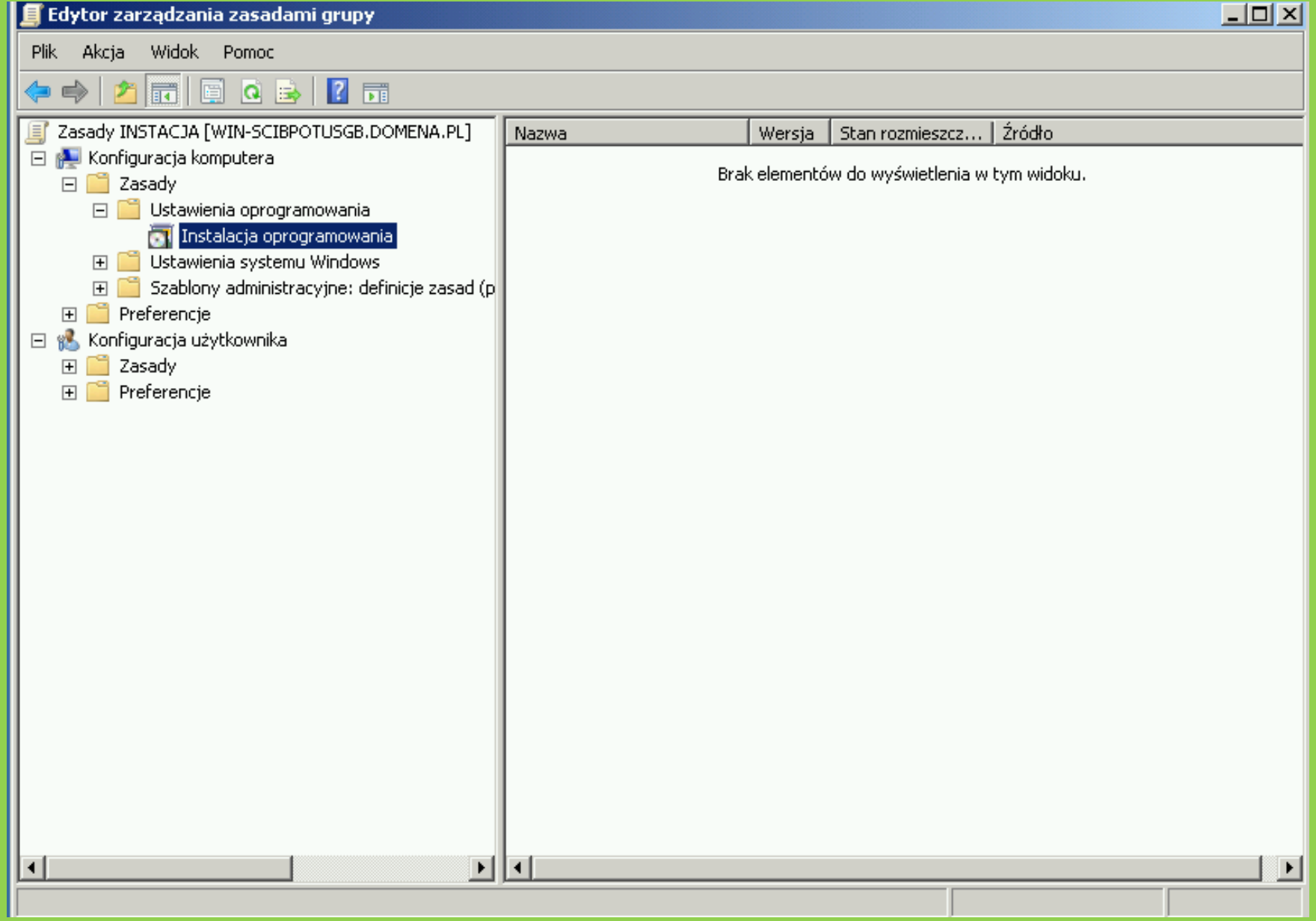
UWAGA: Jeśli komputer znajduje się na liście dystrybucji oprogramowania, a dany program został już w nim zainstalowany, to instalacja nie będzie ponawiana.

To dość ważne!!!

Kolejny krok to edycja obiektu GPO (w moim wypadku o nazwie INSTALACJA).

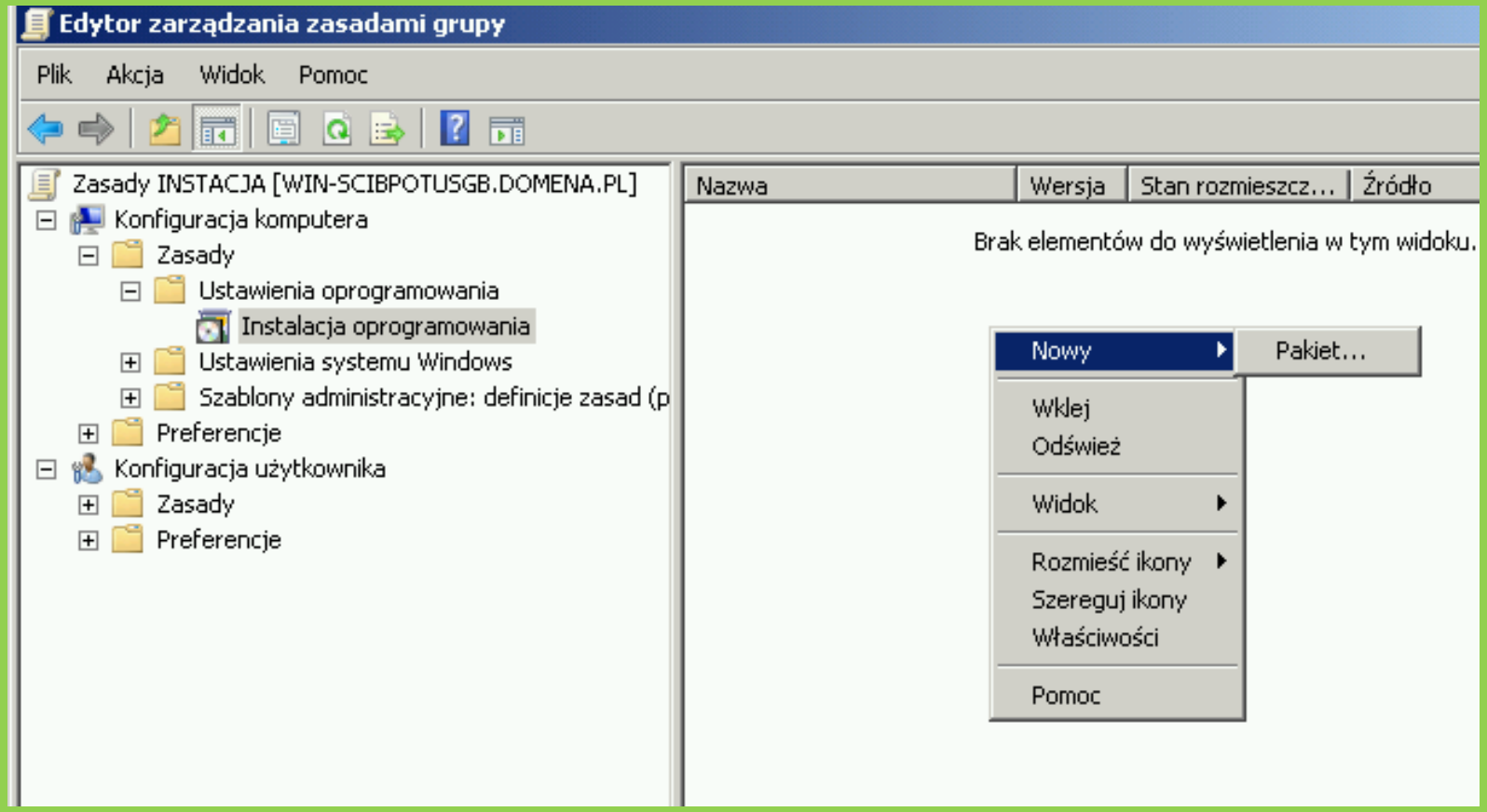
Instalacje programów można dokonać zarówno w przypadku Konfiguracji komputera jak i Konfiguracji użytkownika.

Efekt końcowy będzie ten sam – jednak instalacja wynikająca z Konfiguracji komputera będzie dokonywała się w czasie uruchomienia komputera i wydaje się lepszym rozwiązaniem…

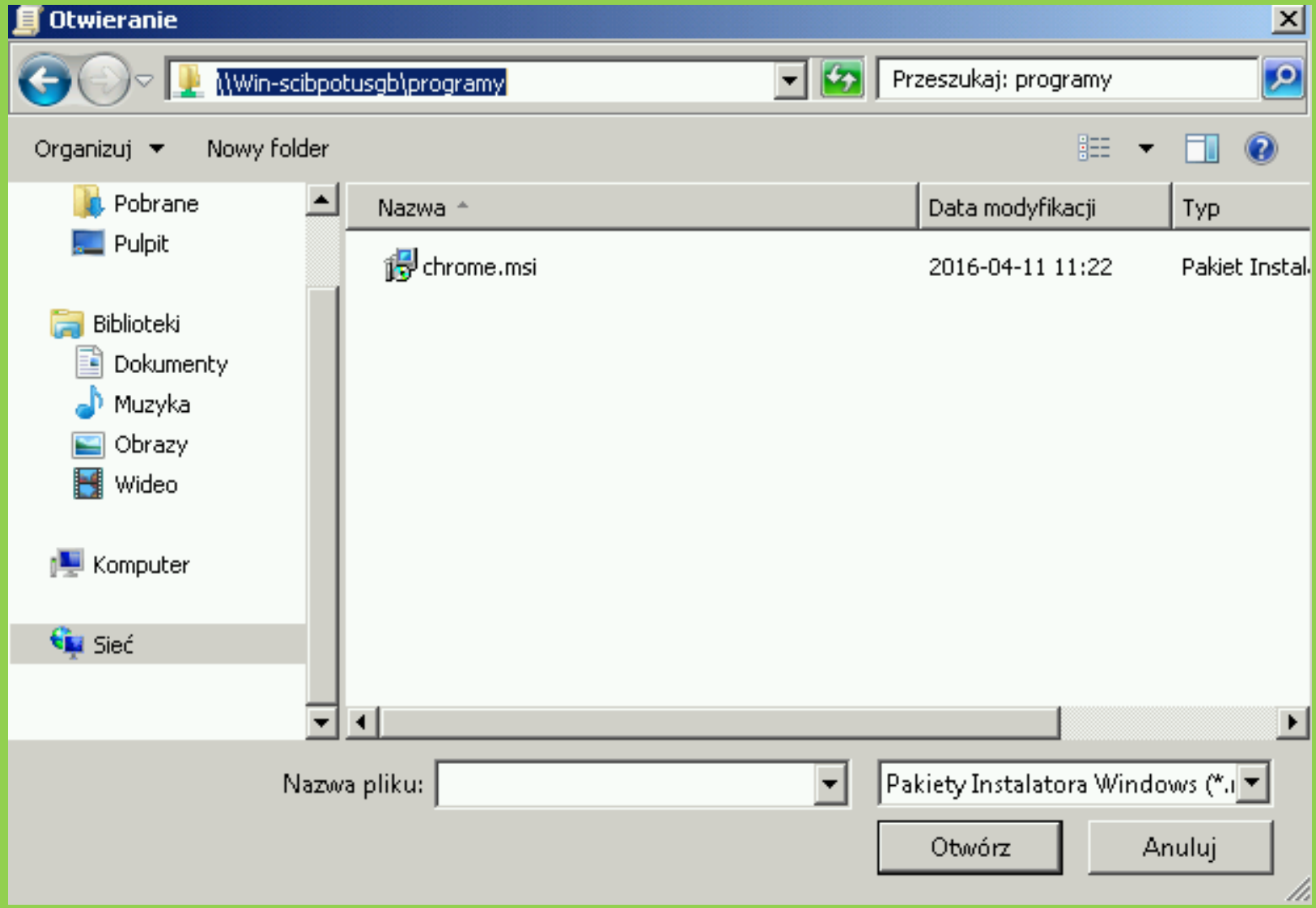


Konfiguracja komputera →Zasady→Ustawienia Oprogramowania→Instalacja Oprogramowania

Kolejny krok to dodanie pakietu do instalacji:

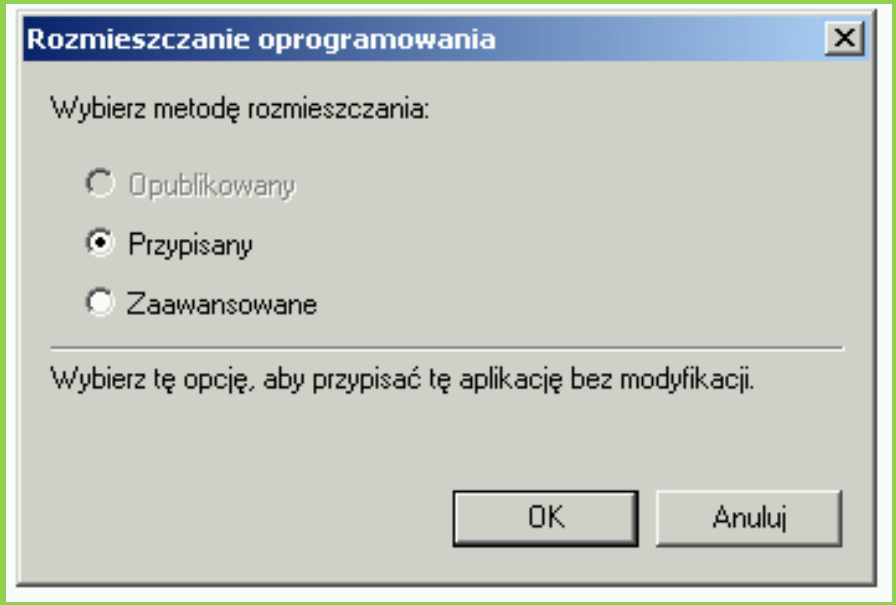


Należy wskazać konkretny pakiet (pamiętać należy, że powinna to być ścieżka sieciowa):

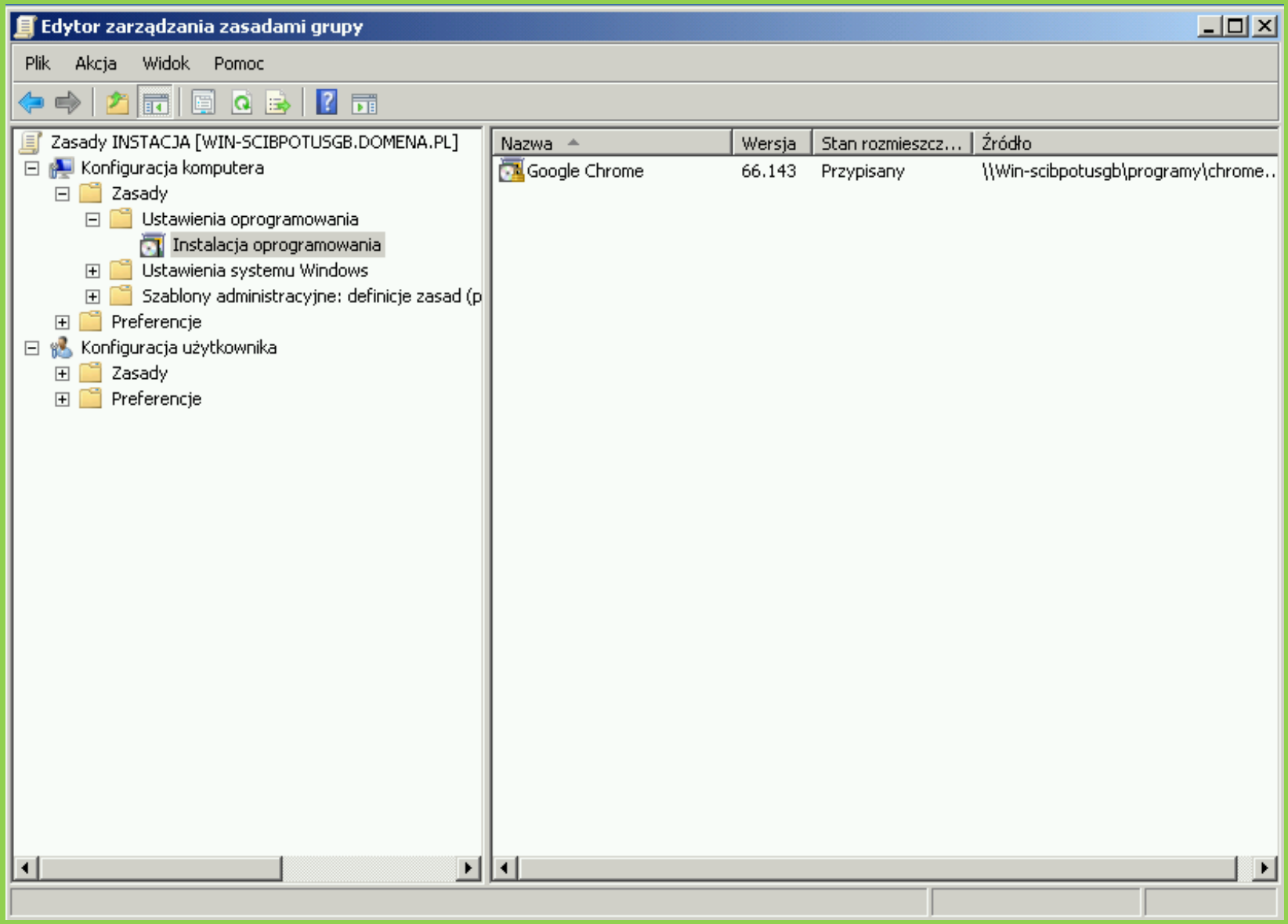


Dalej trzeba wybrać metodę Rozmieszczania oprogramowania.

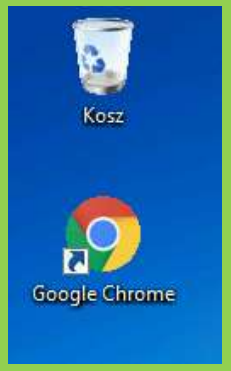
(Dla zainteresowanych odsyłam do poczytania – a w tym wypadku wybieram domyślnie Przypisany)



Na liście oprogramowania powinien być już nowo dodany pakiet

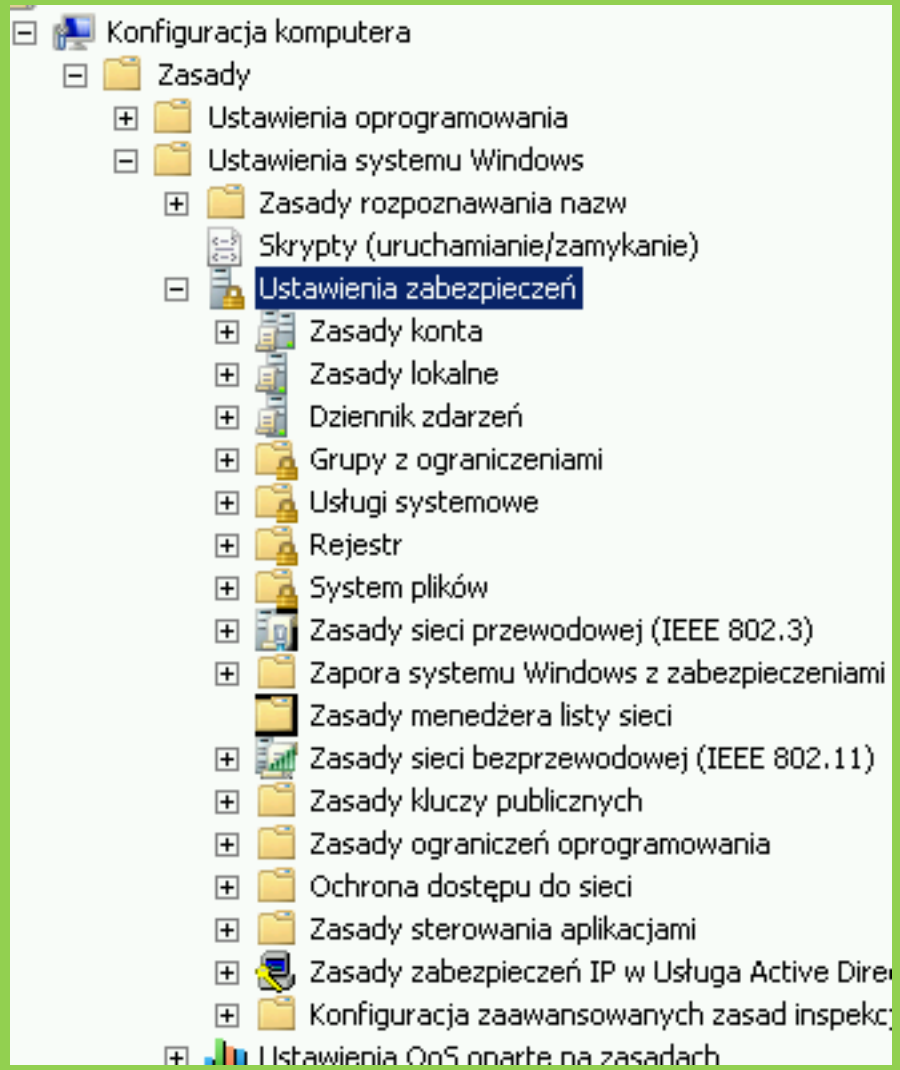


I w zasadzie to wszystko – po tym jak zasady grupy zostaną zaktualizowane na komputerach klienckich przy kolejnym uruchomieniu ich powinna ruszyć automatyczna instalacja Google Chrome:



Uwaga: sam proces uruchamiania (ekran z napisem CZEKAJ…) może trwać nieco dłużej – to wynik tego, że w tym czasie następuje instalacja programów…

Inne ciekawe możliwości GPO:



-Zasady konta (wymogi dot. hasła itp.)

-Zasady lokalne (m.in. zasady inspekcji systemu)

-i wiele innych…

Dla osób zainteresowanych – Google

The End