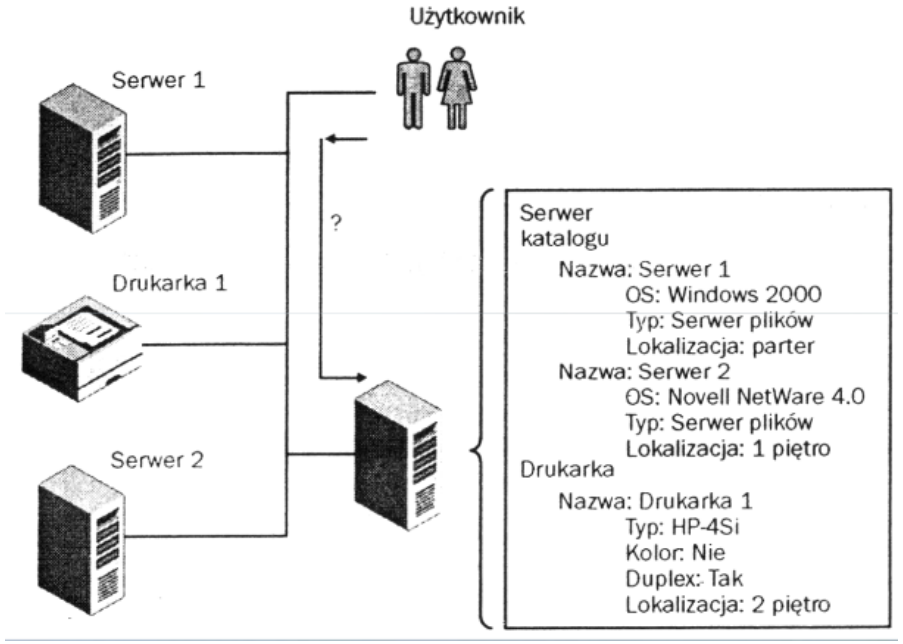
Politechnika Łódzka
Wydział Elektrotechniki Elektroniki Informatyki i Automatyki
Instytut Informatyki Stosowanej

Active Directory

Monitorowanie i zarządzanie serwerami sieciowymi

Katalog i usługa katalogowa

- Katalog -zapisany elektronicznie zbiór informacji dotyczących obiektów np. serwerów plików, drukarek, baz danych i kont użytkowników, które są ze sobą w jakiś sposób powiązane.
- Usługa katalogowa - mechanizm służący do udostępniania informacji użytkownikom.
- Usługa katalogowa daje możliwość uporządkowania i uproszczenia dostępu do zasobów sieciowego systemu komputerowego



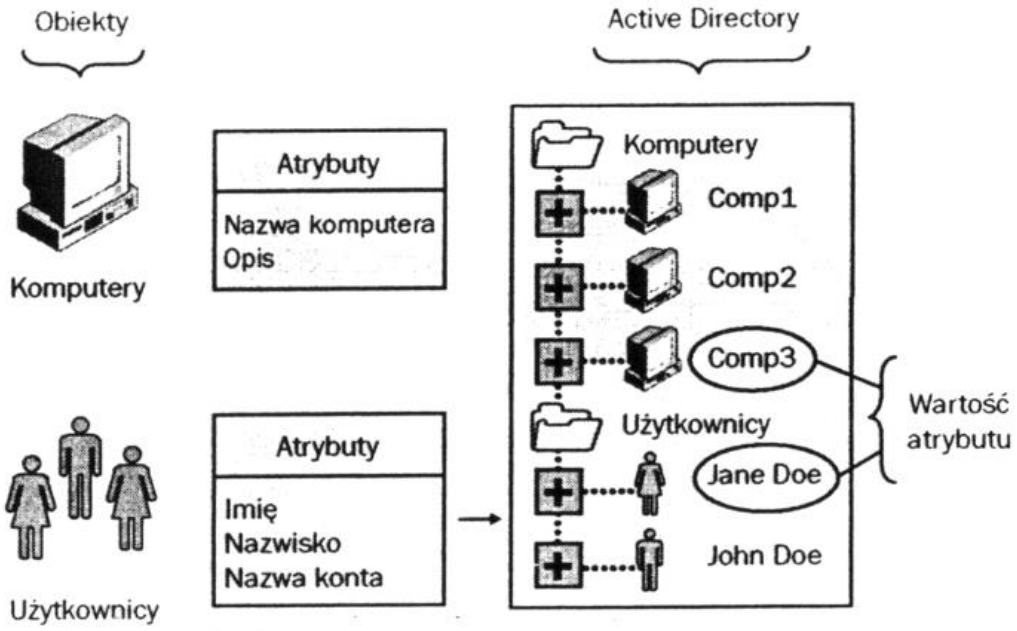
Cechy usługi katalogowej AD

- Scentralizowane przechowywanie danych;
- Skalowalność;
- Rozszerzalność;
- Łatwe zarządzanie;
- Integracja z DNS;
- Zarządzanie konfiguracją klientów;
- Administracja oparta na określonych zasadach;
- Replikacja informacji;
- Elastyczne, bezpieczne uwierzytelnianie i autoryzacja;
- Integracja zabezpieczeń;
- Infrastruktura i aplikacje do obsługi katalogu;
- Współpraca z innymi usługami katalogowymi;
- Podpisywanie i szyfrowanie ruchu LDAP

AD - obiekty

Dane przechowywane w Active Directory, takie jak informacje o użytkownikach, drukarkach, serwerach, bazach danych, grupach, komputerach i zasadach bezpieczeństwa są zorganizowane w postaci obiektów.

- Obiekt jest odrębnym, nazwanym zbiorem atrybutów reprezentującym dany zasób sieciowy.
- Atrybuty obiektu opisują właściwości zasobu np. atrybuty konta użytkownika.
- Kontener jest obiektem, który może zawierać inne obiekty, np. domena.



Schemat Active Directory

- Schemat jest listą definicji określających rodzaje obiektów i typy informacji o tych obiektach.
- Definicje zawarte w schemacie również są przechowywane w postaci obiektów, dlatego można zarządzać nimi podobnie jak innymi obiektami Active Directory.
- Schemat składa się z dwóch typów obiektów:
  - obiektów klasowych (opisujących jakie obiekty mogą zostać utworzone w Active Directory i służących jako szablon dla nowych obiektów Active Directory)
  - Atrybutów obiektów (służących do zdefiniowana cech obiektów klas.
    Wiele klas może zawierać taki sam atrybut np. atrybut Description występuje w wielu klasach, ale ma tylko jedną definicję w schemacie.
- Schematy można rozszerzać.

Komponenty Active Directory

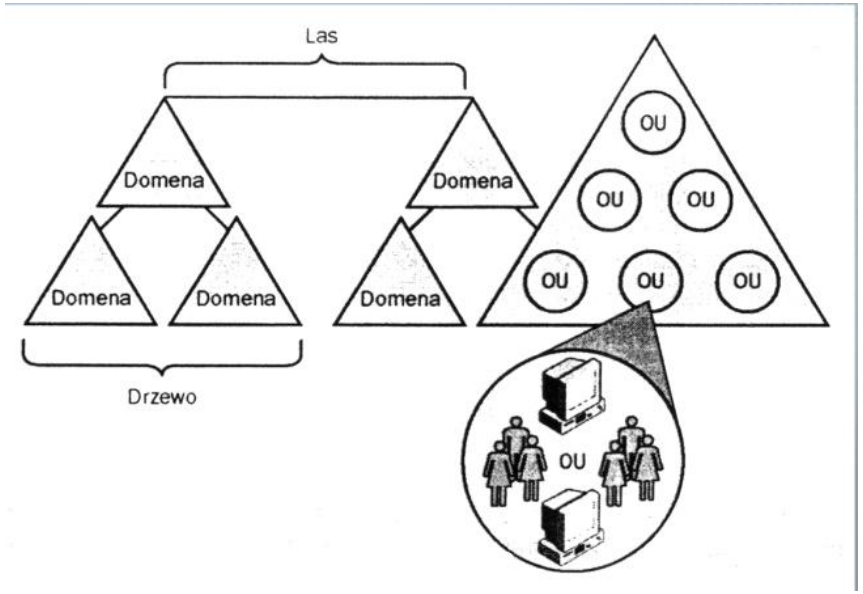
Tworzenie struktury katalogowej spełniającej potrzeby firmy wymaga wykorzystania różnych komponentów Active Directory:

- komponentów reprezentujących struktury logiczne (domeny, jednostki organizacyjne, drzewa, lasy)
- komponentów reprezentujących struktury fizyczne (lokacje, czyli podsieci fizyczne, oraz kontrolery domen).

Struktura logiczna Active Directory jest całkowicie niezależna od struktury fizycznej.

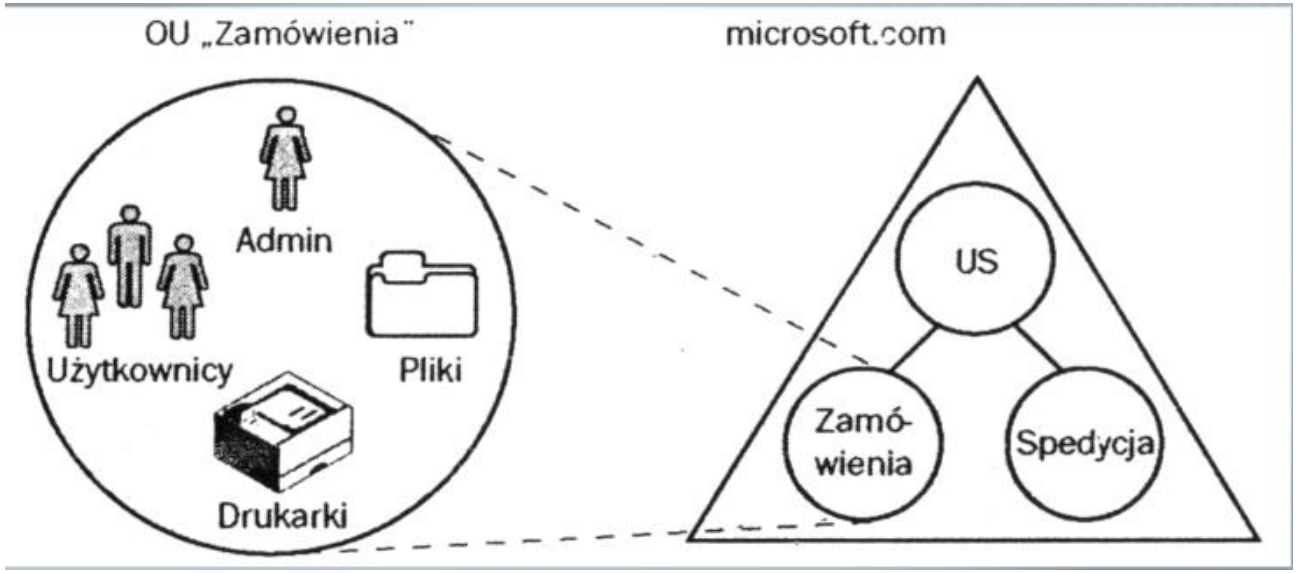
Komponenty Active Directory - Struktura logiczna

- Struktura logiczna Active Directory składa się z domen, jednostek organizacyjnych, drzew i lasów.
- Logiczne pogrupowanie zasobów umożliwia odnalezienie zasobu na podstawie jego nazwy, eliminując konieczność zapamiętania jego fizycznej lokalizacji i dając użytkownikom przejrzysty ogląd struktury sieci.



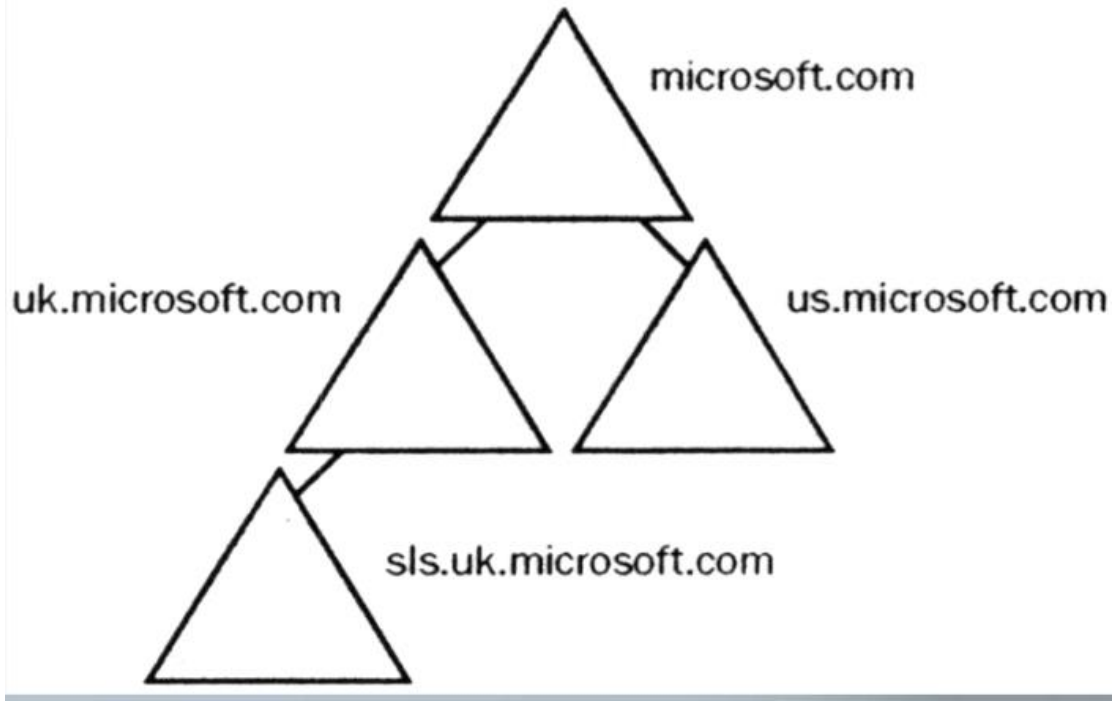
Struktura logiczna AD – jednostki organizacyjne

- Jednostka organizacyjna jest kontenerem służącym do grupowania obiektów należących do jednej domeny i tworzących logiczną grupę dla celów administracyjnych.
- Jednostka organizacyjna może zawierać obiekty, takie jak: konta użytkowników, komputery, drukarki, aplikacje, dzierżawy plikowe oraz inne jednostki organizacyjne należące do tej samej domeny.
- Administrator powinien utworzyć strukturę jednostek organizacyjnych odzwierciedlającą strukturę organizacyjną przedsiębiorstwa.
- Skonfigurowanie uprawnień na wysokim poziomie w celu wykorzystania funkcji dziedziczenia jest skutecznym sposobem ograniczenia ilości pracy administracyjnej.



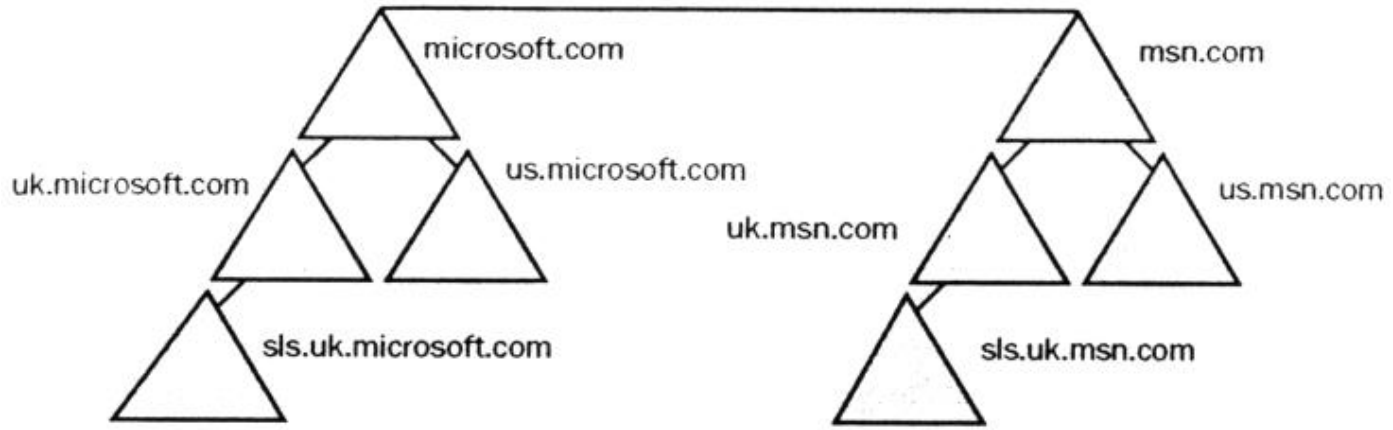
Struktura logiczna AD – drzewa

- Drzewo - hierarchiczna struktura składająca się z jednej lub kilku domen, powstała poprzez utworzenie domen podrzędnych w istniejącej domenie nadrzędnej.
- Domeny należące do tego samego drzewa mają jednolitą przestrzeń nazw i hierarchiczną strukturę nazw. Zgodnie ze standardami DNS, nazwa domeny podrzędnej składa się ze względnej nazwy domeny (prefiksu) oraz nazwy jej domeny nadrzędnej



Struktura logiczna AD – lasy

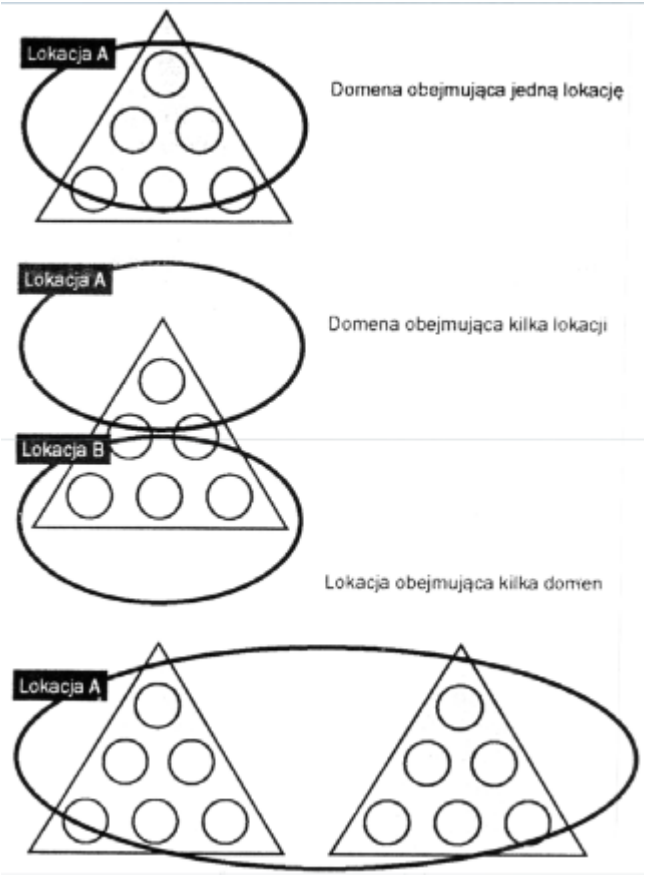
- Las jest grupą lub strukturą hierarchiczną, obejmującą jedno lub kilka odrębnych, całkowicie niezależnych drzew domen.
- Podstawowe cechy lasów:
  - wszystkie domeny w lesie są oparte na wspólnym schemacie;
  - wszystkie domeny w lesie wykorzystują wspólny wykaz globalny;
  - pomiędzy domenami należącymi do tego samego lasu istnieją domniemane dwukierunkowe przechodnie relacje zaufania;
  - poszczególne drzewa mają niezależne struktury nazw, oparte na nazwach domen;
  - domeny w lesie funkcjonują niezależnie od siebie, ale las służy do umożliwienia komunikacji na poziomie całej organizacji.



Struktura fizyczna AD – lokacje

- Komponentami fizycznymi Active Directory są:
  - Lokacje,
  - kontrolery domen.

- Lokacja jest zbiorem jednej lub większej liczby podsieci IP, pomiędzy którymi istnieją połączenia o dużej szybkości i dostępności.
- Zazwyczaj granice lokacji są jednocześnie granicami sieci LAN. Podsieci powinny zostać razem zgrupowane tylko w przypadku, gdy istnieją między nimi szybkie i tanie połączenia sieciowe o wysokim poziomie dostępności.
- Jedna domena może obejmować kilka lokacji, a jedna lokacja może obejmować konta użytkowników i komputery należące do różnych domen



Struktura fizyczna AD – kontrolery domen

- Kontroler domeny to komputer z systemem Windows Server zawierający replikę katalogu domeny (bazy danych domeny lokalnej).
- Domena może zawierać jeden lub kilka kontrolerów domeny.
- Dany kontroler domeny może obsługiwać tylko jedną domenę.
- Kontrolery domen w lokacjach powinny być umieszczone w sposób odzwierciedlający strukturę fizyczną oraz optymalizujący replikację i uwierzytelnianie.

- Funkcje kontrolerów domeny:
  - przechowywanie pełnej kopii wszystkich informacji Active Directory dotyczących danej domeny,
  - zarządzanie zmianami tych informacji,
  - replikacja zmiany do innych kontrolerów należących do tej samej domeny (Active Directory obsługuje replikację w trybie multimaster),
  - wykrywanie konfilktów (kolizji)
  - zarządzanie wszystkimi aspektami interakcji pomiędzy użytkownikami a domeną, takimi jak odnajdowanie obiektów Active Directory i sprawdzenie poprawności prób logowania.

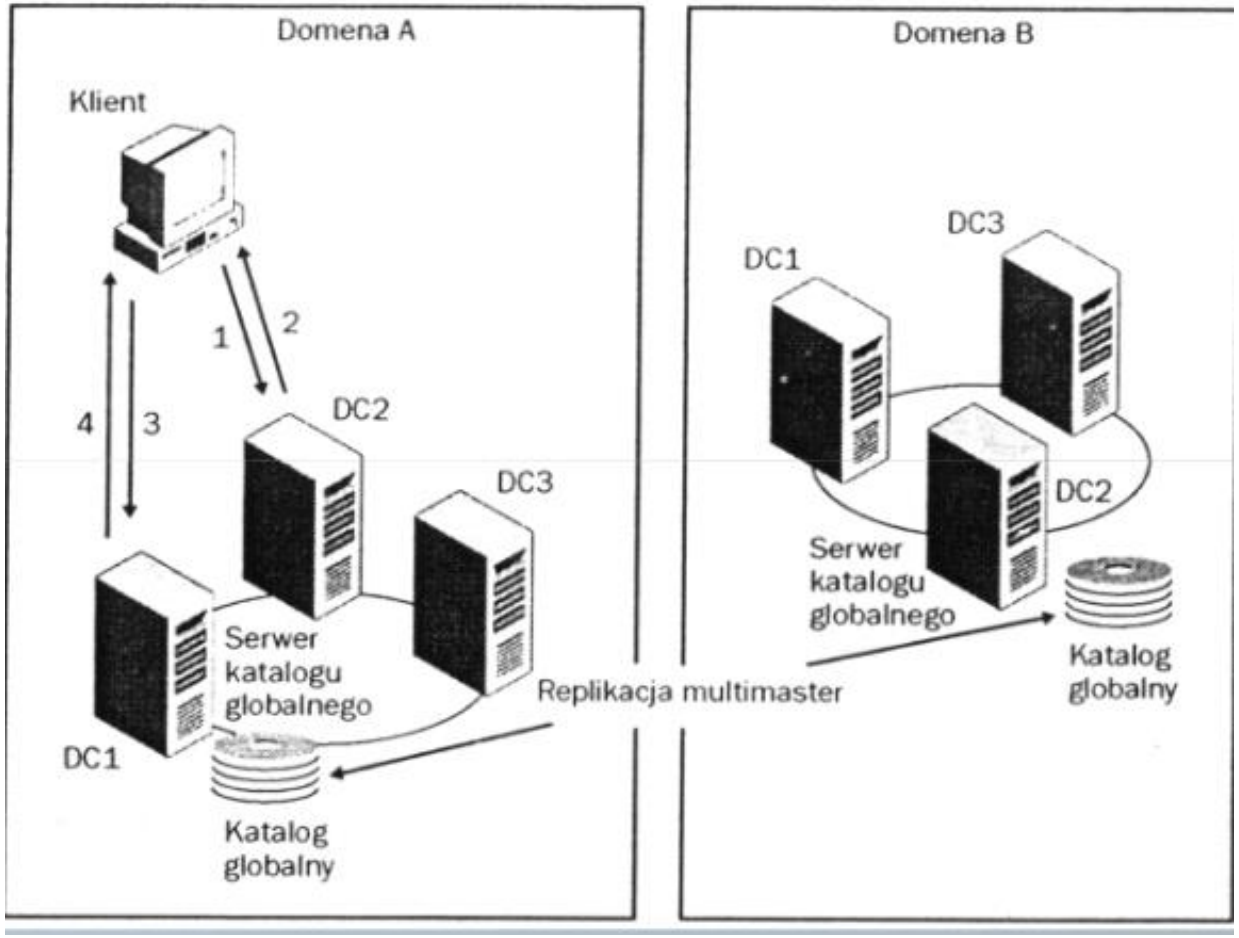
Wykaz globalny

- **Wykaz globalny-** centralne repozytorium informacji o obiektach należących do danego drzewa lub lasu -zawiera wybrane informacje o wszystkich obiektach należących do wszystkich domen, co umożliwia poszukiwanie obiektów w całym przedsiębiorstwie.
- Domyślnie wykaz globalny zostanie utworzony automatycznie na pierwszym kontrolerze domeny w pierwszej domenie lasu.
- Kontroler domeny zawierający kopię wykazu globalnego nazywa się serwerem wykazu globalnego

- Serwerem wykazu globalnego może być każdy kontroler domeny w danym lesie.
- Informacje zawarte w wykazie globalnym są replikowane w trybie multimaster do serwerów wykazu globalnego należących do innych domen.
- Serwer wykazu globalnego przechowuje pełną replikę atrybutów obiektów należących do własnej domeny oraz częściową replikę atrybutów obiektów należących do pozostałych domen lasu.
- Atrybuty replikowane do wykazu globalnego podlegają dziedziczeniu uprawnień zdefiniowanych w domenach źródłowych, co zapewnia odpowiedni poziom zabezpieczenia informacji zawartych w wykazie globalnym.

Proces obsługi zapytań

Zapytanie jest żądaniem wysłanym do wykazu globalnego przez użytkownika w celu pobrania, modyfikacji lub usunięcia danych z Active Directory



Katalog

- Informacje przechowywane w katalogu (w pliku Ntds.dit) są podzielone na cztery kategorie logiczne nazywane partycjami katalogu(lub kontekstem nazwy).
- Partycja katalogu jest jednostką replikacji.
- Katalog składa się z następujących partycji:
  - Schemat- definicje obiektów, jakie mogą zostać utworzone w katalogu, oraz definicje możliwych atrybutów tych obiektów.
  - Konfiguracja-służy do opisania struktury logicznej systemu. Do informacji zawartych w tej partycji należą dane dotyczące struktury domen i topologii replikacji.
  - Domena- informacje o wszystkich obiektach należących do domen.
  - Katalog aplikacji-służy do przechowywania danych dynamicznych należących do określonych aplikacji.

Sposób replikacji informacji

- Active Directory obsługuje dwa rodzaje replikacji:
  - Replikację wewnątrzlokacyjną
  - Replikację międzylokacyjną (pomiędzy lokacjami).

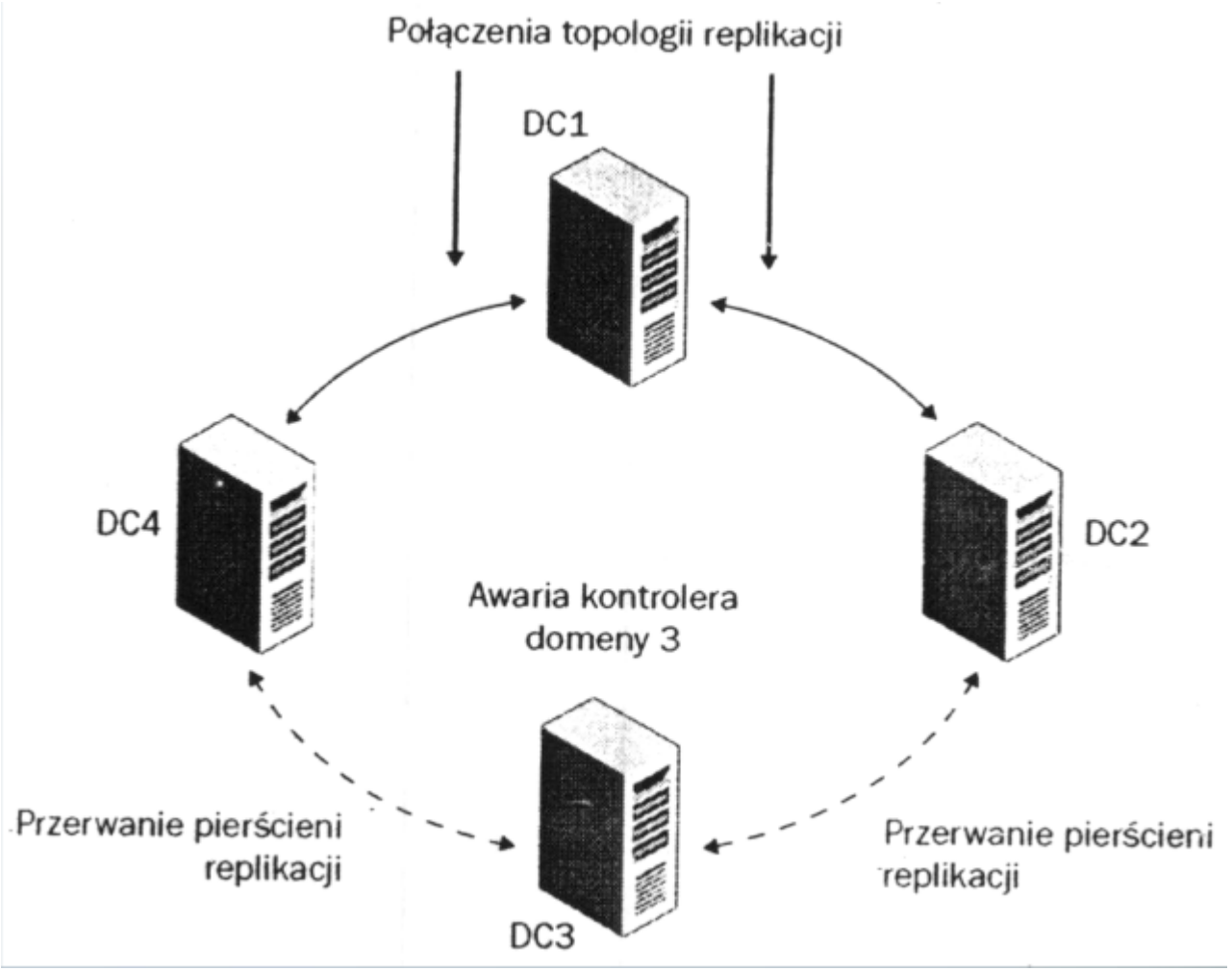
Należy zachować równowagę pomiędzy dostarczaniem najbardziej aktualnych informacji katalogowych a ograniczaniem wykorzystanej szerokości pasma

Replikacja wewnątrzlokacyjna

- W granicach danej lokacji usługa Windows Server nazywana KCC (Knowledge Consistency Checker) automatycznie generuje topologię replikacji opartą na strukturze pierścieniowej, obejmującą kontrolery należące do tej samej domeny.
- KCC działa na każdym kontrolerze domeny.
- Topologia definiuje ścieżkę, po której aktualizacje katalogu są przekazywane do wszystkich kontrolerów domeny znajdujących się w danej lokacji.
- KCC ustala, które serwery są najbardziej odpowiednimi partnerami replikacji na podstawie: cech łączności, historii pomyślnej replikacji oraz dopasowania replik pełnych i częściowych.
- Kontroler domeny może mieć więcej niż jednego partnera replikacji.
- KCC tworzy obiekty połączeń reprezentujące połączenia wykorzystywane do replikacji pomiędzy partnerami

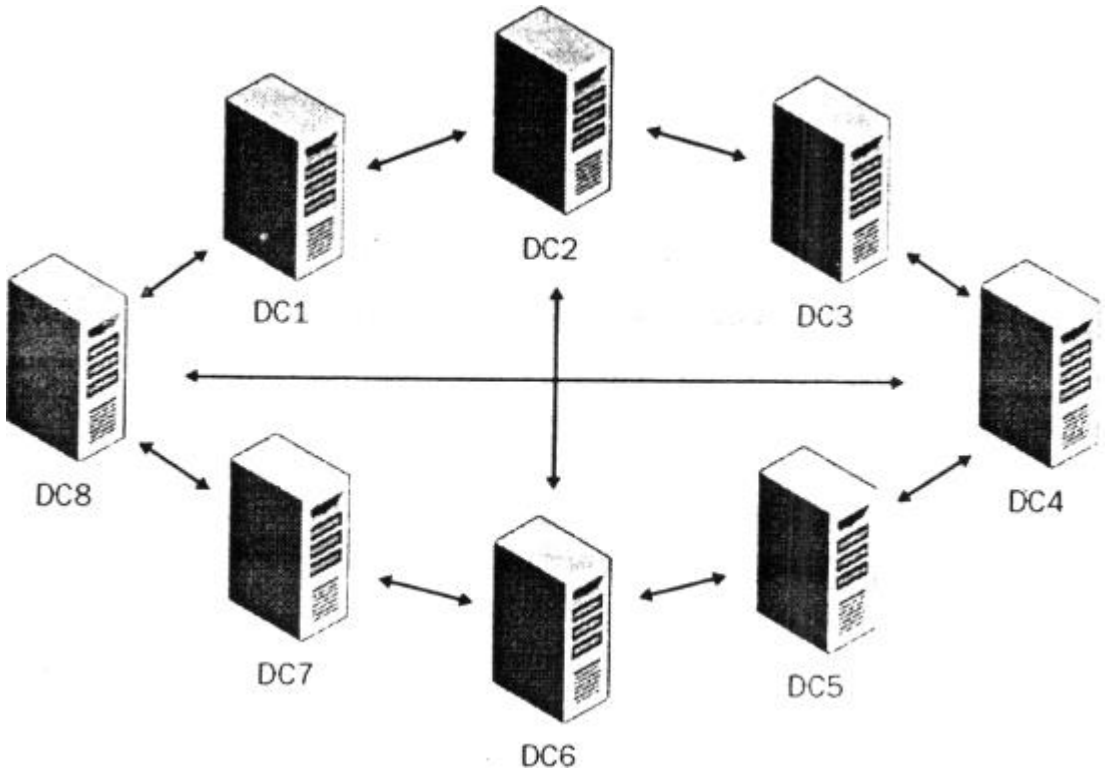
- Występowanie co najmniej dwóch ścieżek replikacji pomiędzy dwoma kontrolerami domeny (dzięki strukturze pierścieniowej).
- Sprawdzanie przez KCC poprawność funkcjonowania topologii replikacji wewnątrzlokacyjnej co 15 minut.
- Rekonfiguracja topologii w przypadkach, kiedy kontroler domeny zostanie dodany lub usunięty z sieci albo z danej lokacji.

Replikacja wewnątrzlokacyjna



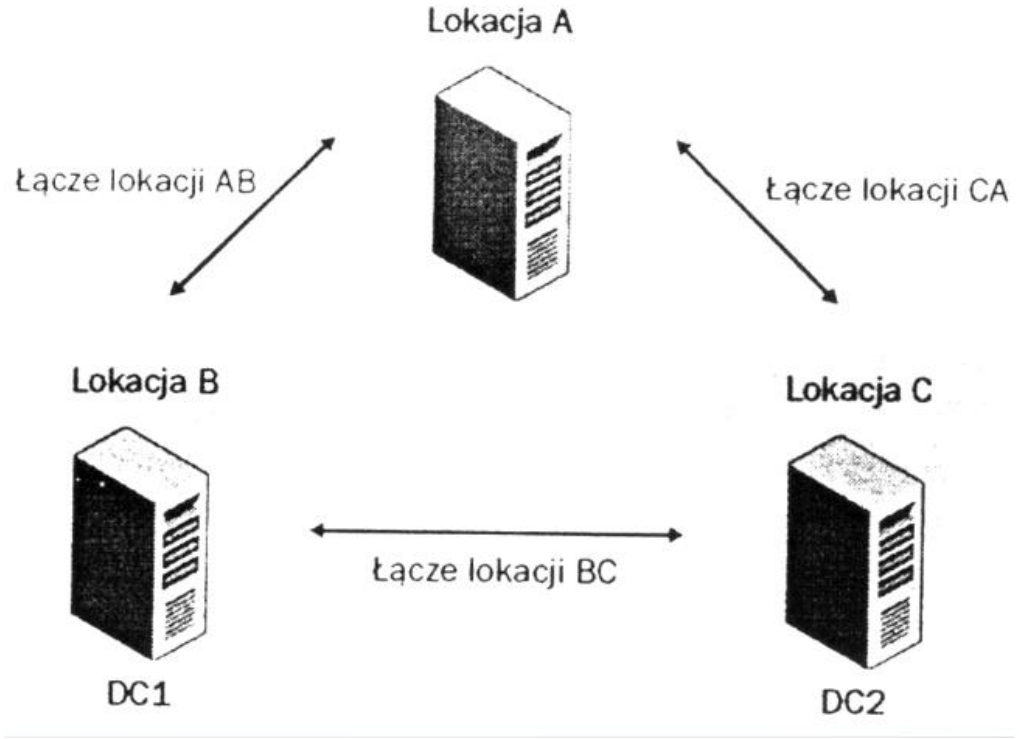
Replikacja wewnątrzlokacyjna

- Gdy lokacja zawiera więcej niż siedem kontrolerów domeny, to KCC tworzy dodatkowe obiekty połączeń pomiędzy komputerami usytuowanymi najdalej od siebie w pierścieniu - ścieżka replikacji pomiędzy dwoma kontrolerami domeny nie może być dłuższa niż trzy przeskoki replikacyjne.
- Połączenia dodatkowe są tworzone w sposób losowy i nie muszą obejmować wszystkich kontrolerów domeny



Replikacja międzylokacyjna

- Aby umożliwić replikację pomiędzy lokacjami, należy ręcznie utworzyć łącza lokacji reprezentujące połączenia sieciowe.
- Każda lokacja zawiera jedną instancję KCC odpowiedzialną za tworzenie wszystkich połączeń pomiędzy lokacjami.
- Active Directory wykorzystuje podane przez administratora informacje o połączeniach sieciowych (protokół transportu, koszty łączy, obciążenia łączy) do utworzenia obiektów połączeń zapewniających efektywną replikację i odporność na błędy.



Active Directory – Administrowanie obiektami

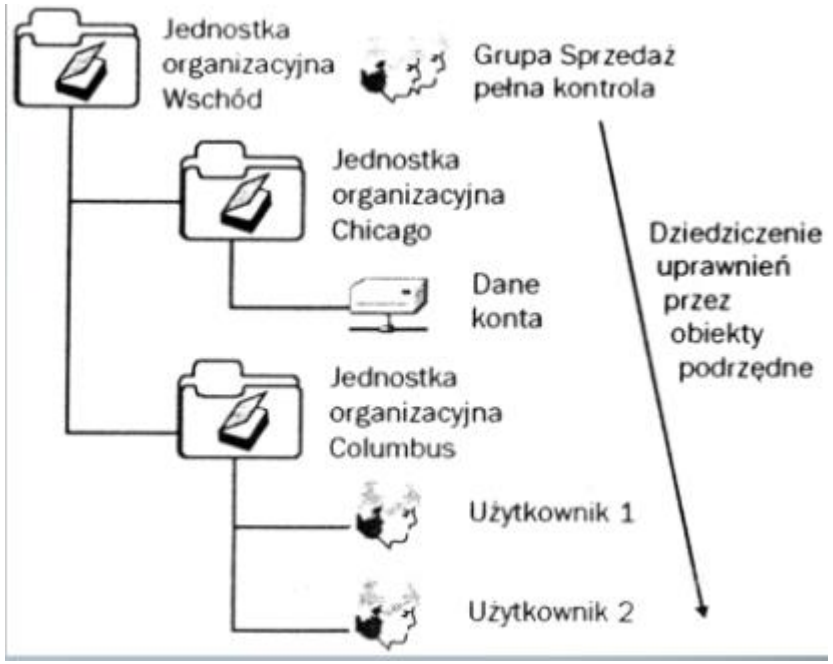
- Obiekt jest nazwanym zbiorem atrybutów reprezentującym określony element (konto, grupę, folder itp.).
- Użytkownicy i programy mogą przesłać zapytania do Active Directory, aby uzyskać informacje o obiektach przechowywanych w katalogu.
- Najczęściej używane typy obiektów:
  - konto użytkownika
  - Kontakt
  - Grupa
  - folder udostępniony
  - Drukarka
  - Komputer
  - kontroler domeny
  - jednostka organizacyjna.

Uprawnienia

- Uprawnienia mogą być ustawione na Allow (Zezwalaj) lub Deny(Odmawiaj).
- Ustawienia Deny (Odmawiaj) mają pierwszeństwo przed innymi uprawnieniami.
- Dostępne ustawienia uprawnień są zależne od typu obiektu (np. uprawnienie do ponownego ustawiania hasła).
- Dla każdego typu obiektu istnieje zbiór uprawnień standardowych oraz zbiór bardziej szczegółowych uprawnień specjalnych.
- Uprawnienia standardowe są uprawnieniami najczęściej konfigurowanymi – znajdują się na zakładce Security w oknie właściwości obiektu (zakładka Security (Zabezpieczenia) jest dostępna tylko wtedy, gdy w menu View (Widok) zaznaczona jest opcja Advanced Features (Opcje zaawansowane)).
- Podmiot zabezpieczeń może być członkiem wielu grup, które mają różne uprawnienia dostępu w stosunku do poszczególnych obiektów.

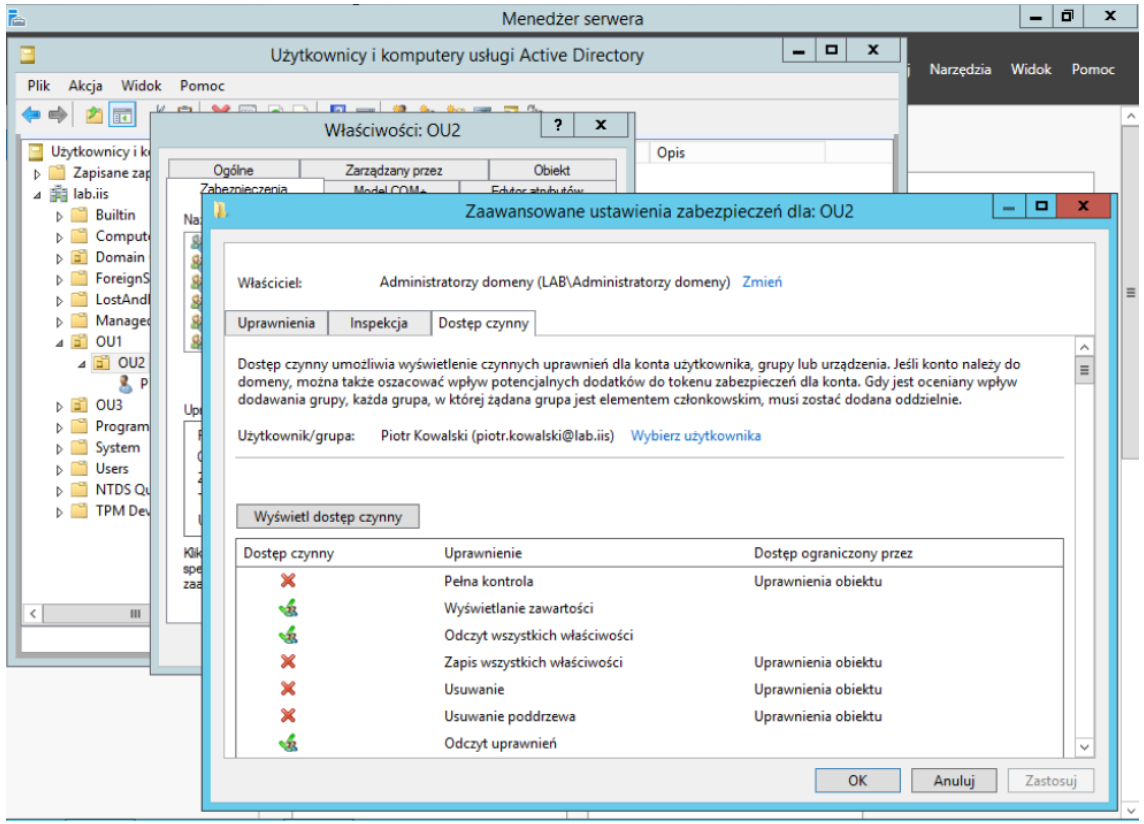
Dziedziczenie uprawnień

Dostęp do danego obiektu jest zależny od dwóch grup uprawnień: uprawnień przypisanych bezpośrednio do obiektu przez jego właściciela
oraz uprawnień dziedziczonych, powiązanych z obiektem nadrzędnym.
Dziedziczenie uprawnień ułatwia proces zarządzania uprawnieniami, pomaga zapewnić zgodność uprawnień powiązanych z obiektami w danym kontenerze oraz minimalizuje liczbę operacji przypisania uprawnień.



Uprawnienia efektywne

- Uprawnienia efektywne obejmują wszystkie uprawnienia, obowiązujące dany podmiot zabezpieczeń w zakresie dostępu do określonego obiektu, w tym uprawnienia wynikające z przynależności do grup oraz uprawnienia dziedziczone.
- Windows Server zawiera funkcję(zakładka Effective Permissions (Dostęp czynny) znajdująca się w zakładce Security właściwości obiektu), która umożliwia wyświetlenie uprawnień efektywnych dla określonego obiektu i podmiotu zabezpieczeń



Zalecenia dotyczące przypisywania uprawnień

- Przypisywanie uprawnień grupom jest skuteczniejsze niż bezpośrednie przydzielanie uprawnień kontom użytkowników.
- Nie należy zbyt często stosować ustawień odmowy uprawnień.
- Uprawnienia powinny być skonfigurowane na dziedziczenie przez obiekty podrzędne.

Przekazywanie prawa własności obiektów

- Sposoby przekazania prawa własności obiektu:
  - obecny właściciel może nadać drugiemu użytkownikowi uprawnienie do przejęcia obiektu na własność, po czym drugi użytkownik powinien przejąć obiekt;
  - administrator może przejąć na własność dowolny plik na komputerze. Administrator nie może jednak przenieść prawa własności (i odpowiedzialności za wykonywane czynności) do innych użytkowników;
  - użytkownik, który ma prawo do przywracania plików i katalogów, może przypisać prawo własności dowolnemu użytkownikowi lub grupie.

Delegowanie kontroli administracyjnej

- Celem delegowania kontroli administracyjnej nad domenami, jednostkami organizacyjnymi i kontenerami jest zapewnienie innym administratorom, grupom lub użytkownikom możliwości zarządzania funkcjami zgodnie z ich potrzebami.
- Kreator delegowania kontroli (Delegation Of Control Wizard) automatyzuje i upraszcza proces konfigurowania uprawnień administracyjnych dla domeny lub jednostki organizacyjnej.
- W wypadku delegowania kontroli administracyjnej do użytkowników należy upewnić się, że użytkownicy przyjmują odpowiedzialność za zarządzanie delegowanymi obiektami i są odpowiednio do tego celu przeszkoleni.

Active Directory – Administrowanie kontami użytkowników i grupami

- Konto użytkownika jest zbiorem wszystkich informacji, służących do zdefiniowania danego użytkownika w systemie.
- Informacje wchodzące w skład konta:
  - nazwa użytkownika i hasło;
  - lista grup, do których dane konto należy;
  - Prawa lub uprawnienia posiadane przez użytkownika w stosunku do innych obiektów AD.
- Konto może być wykorzystane przez użytkownika do:
  - logowania na danym komputerze,
  - logowania w domenie.
- Proces uwierzytelniania służy do potwierdzenia tożsamości użytkownika, próbującego zalogować się w domenie lub uzyskać dostęp do zasobów sieciowych.
- Uwierzytelnianie Windows Server umożliwia pojedyncze logowanie - po zalogowaniu się na jednym komputerze klienckim użytkownik może uzyskać dostęp do zasobów przechowywanych na dowolnym komputerze w domenie.

Rodzaje kont użytkowników

- Windows Server obsługuje trzy rodzaje kont użytkowników:
  - lokalne - logowanie na danym komputerze - dostęp do lokalnych zasobów;
  - domenowe - logowanie do domeny - dostęp do zasobów sieciowych;
  - wbudowane – tworzone automatycznie dla celów administracyjnych lub dostępu do zasobów sieciowych.

Konta lokalne

- Lokalne konto użytkownika:
  - Umożliwia użytkownikowi logowanie tylko komputerze, na którym konto zostało utworzone,
  - daje dostęp tylko do zasobów przechowywanych na tym komputerze,
  - jest przechowywane w lokalnej bazie danych zabezpieczeń danego komputera,
  - informacje o nim nie są replikowane do kontrolerów domen.
- Nie należy tworzyć lokalnych kont użytkowników na komputerach, z których konieczny jest dostęp do zasobów domenowych - nie są rozpoznawane w domenie.

Konta domenowe

- Konta domenowe:
  - używane do logowania się w domenie oraz do uzyskania dostępu do zasobów przechowywanych w dowolnym punkcie w sieci – na podstawie nazwy użytkownika i hasła podanego podczas logowania, Windows Server uwierzytelnia użytkownika oraz tworzy (na czas trwania sesji logowania) token dostępu zawierający informacje o użytkowniku wraz z ustawieniami zabezpieczeń;
  - są tworzone w kontenerze lub jednostce organizacyjnej w kopii bazy danych Active Directory (katalogu), przechowywanej na kontrolerze domeny;
  - replikacja do wszystkich kontrolerów domeny należących do jego domeny;
  - użytkownik może zostać uwierzytelniony przez dowolny kontroler domeny należący do drzewa domen.

Konta wbudowane

- Najczęściej używane są wbudowane konta Administrator oraz Gość.
- Konto Administrator:
  - służy do zarządzania konfiguracją komputera i domeny,
  - hasło konta Administrator należy określić podczas instalacji Active Directory,
  - ze względu na szerokie uprawnienia konta Administrator należy zapobiec jego wykorzystaniu przez osoby nieupoważnione:
  - należy nadać kontu Administrator nową nazwę niekojarzącą się z zadaniami administracyjnymi (wmic useraccount where name= ’Administrator’ call rename name= ’Gucio’)
  - należy zastosować silne hasło,
  - nie należy ujawniać hasła administratora zbyt wielu osobom,
  - administrator powinien utworzyć dla siebie osobne konto użytkownika służące do wykonywania pracy nie administracyjnej.

Konto Gość

- Służy do udostępnienia zasobów użytkownikom, nie posiadającym konta w danej domenie,
- domyślnie nie wymaga podania hasła (hasło może być puste) i jest wyłączone,
- można je włączyć tylko w przypadku, gdy sieć nie wymaga wysokiego poziomu zabezpieczenia,
- jeśli ma zostać włączone, to należy zastosować hasło oraz przypisać mu nazwę nieskojarzoną z kontem gościa,
- nie można go usunąć.

Hasła kont

- Każde konto użytkownika powinno mieć silne hasło.
- Ważne jest zapoznanie użytkowników z metodami tworzenia silnych haseł oraz z przyczynami, dla których takie hasła powinny być stosowane.
- Hasło może zawierać do 127 znaków, natomiast w sieci zawierającej komputery oparte na Microsoft Windows 95, 98 i Me nie należy stosować haseł zawierających więcej niż 14 znaków.
- Silne hasło charakteryzuje się tym, że:
  - zawiera co najmniej 7 znaków,
  - nie zawiera nazwy użytkownika, imienia, nazwiska ani nazwy firmy,
  - nie zawiera żadnego pełnego wyrazu znajdującego się w słownikach,
  - nie jest podobne do poprzednio używanych haseł,
  - zawiera znaki z każdej z grup: duże litery, małe litery, cyfry, inne symbole.

Profile użytkowników

- Profil użytkownika jest zbiorem folderów i danych, służącym do przechowywania bieżącego środowiska pulpitu
- ustawień aplikacji i danych osobistych, należących do określonego użytkownika.

- Profil użytkownika zawiera m.in. następujące elementy:
  - Obrazy, Ulubione, Moje miejsca sieciowe, Zawartość pulpitu,
  - Kolory ekranu i czcionki, Dane aplikacji, Ustawienia drukarek,
  - Panel sterowania,
  - Ustawienia akcesoriów,
  - Ustawienia programów opartych na Windows.

- Zazwyczaj Windows Server przechowuje lokalne profile
- użytkowników w folderze X:\Documents and Settings.

Rodzaje profili użytkowników

- W Windows Server występują następujące rodzaje profili użytkowników:
  - lokalne;
  - mobilne;
  - obowiązkowe;
  - tymczasowe.

Grupy - wprowadzenie

- Grupa jest zbiorem kont użytkowników służącym do uproszczenia administracji.

- Przypisanie praw i uprawnień do grupy eliminuje konieczność skonfigurowania uprawnień dla każdego konta użytkownika.
- Użytkownicy mogą należeć do kilku grup.
- Grupy mogą zawierać nie tylko konta użytkowników, lecz także komputery, kontakty i inne grupy.

- Utworzenie grup mieszczących inne grupy umożliwia ich konsolidację w celu zmniejszenia liczby operacji nadania
- uprawnień.

Rodzaje grup

- Usługa katalogowa AD obsługuje dwa rodzaje grup:
  - **grupy zabezpieczeń**
    - służą do przypisania uprawnień dostępu do zasobów;
    - mogą być wykorzystane także do innych celów, takich jak np. pobranie informacji o użytkownikach w celu ich wykorzystania w aplikacji WWW - grupa zabezpieczeń oferuje wszystkie możliwości grupy dystrybucyjnej.
  - **grupy dystrybucyjne**
    - Są wykorzystywane przez aplikacje do funkcji nie związanych z zabezpieczeniami, na przykład do przesyłania wiadomości e-mail do określonej grupy użytkowników;
    - nie mogą być używane do przypisywania uprawnień;
    - Mogą być wykorzystane tylko przez programy współpracujące z Active Directory, takie jak np. Microsoft Exchange Server.

Zakresy grup

- Podczas tworzenia grupy należy określić jej **rodzaj** oraz **zakres**.
- Od zakresu grupy zależy sposób, w jaki może być ona używana do przypisania uprawnień.
- W zależności od jej zakresu grupa może być grupą:
  - lokalną (członkowie tylko z komputera lokalnego, mają dostęp do zasobów komputera lokalnego)
  - globalną (członkowie tylko z domeny lokalnej, mają dostęp do zasobów dowolnej domeny)
  - domenową lokalną (członkowie z dowolnej domeny, mają dostęp tylko do zasobów domeny lokalnej)
  - uniwersalną (członkowie z dowolnej domeny, mają dostęp do zasobów dowolnej domeny). Używane są najczęściej do przypisywania uprawnień do powiązanych zasobów należących do różnych domen,

Active Directory – Zasady grupy

- Zasady grupy są zbiorami ustawień konfiguracyjnych mających zastosowanie do użytkowników lub komputerów, które mogą zostać powiązane z poszczególnymi komputerami, lokacjami, domenami i jednostkami organizacyjnymi w celu sterowania zachowaniem użytkowników.
- Aby wprowadzić określoną konfigurację dla danej grupy użytkowników, należy utworzyć **Obiekty Zasad Grupy** (**GPO**), które są zbiorami ustawień zasad grupy.
- Każdy komputer Windows Server ma jeden lokalny obiekt zasad grupy i może podlegać także ustawieniom zawartym w dowolnej liczbie obiektów nielokalnych (opartych na AD).
- Nielokalny obiekt zasad grupy zastępuje ustawienia lokalne.
- Zgodnie z regułami dziedziczenia obowiązującymi w Active Directory, nielokalne obiekty zasad grupy są stosowane hierarchicznie, od największej grupy (lokacji) po najmniejszą (jednostkę organizacyjną), oraz kumulatywnie.

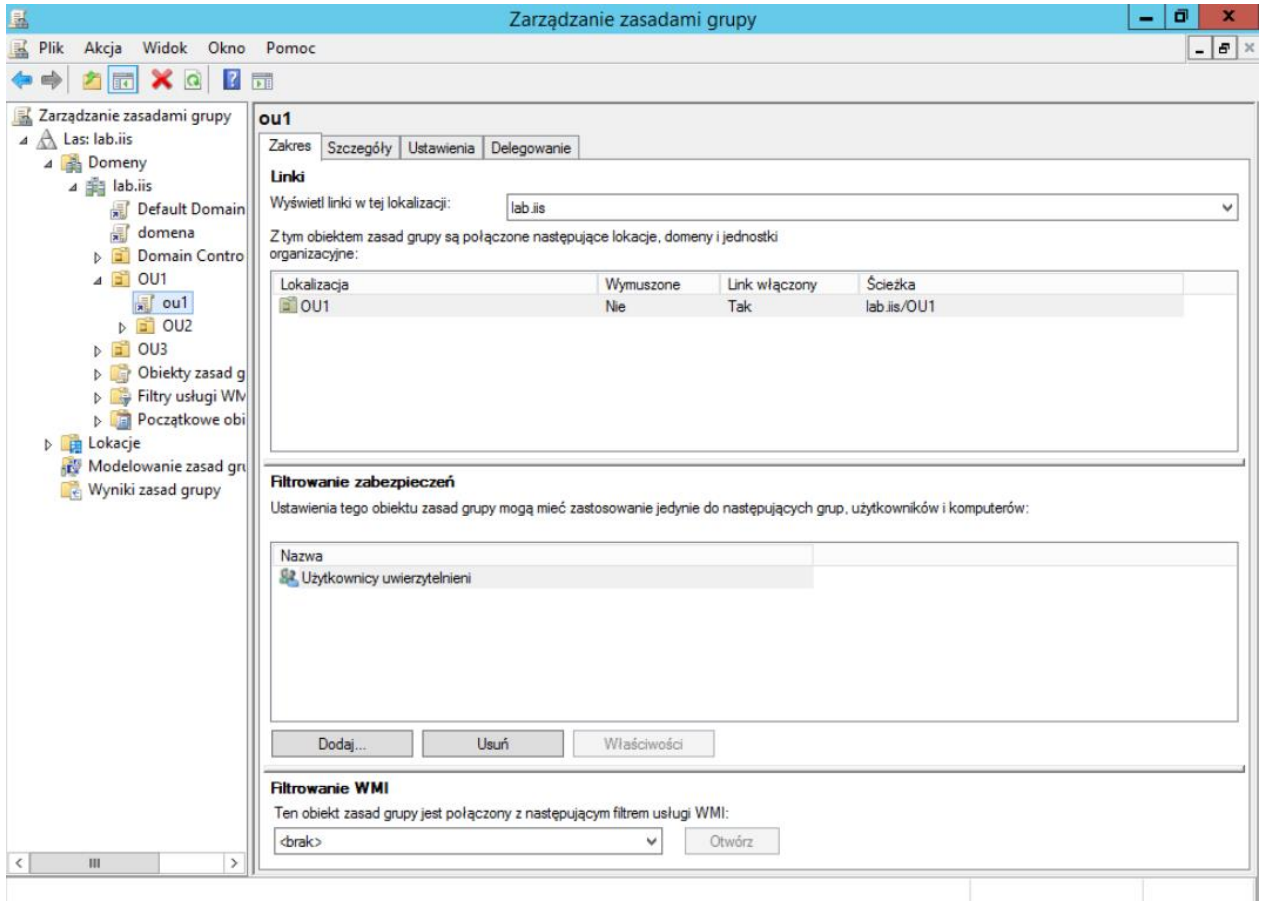
Zasady grupy

Kolejność stosowania zasad grupy:

1. Lokalny obiekt zasad grupy - każdy serwer oparty na Windows Server zawiera dokładnie jeden lokalnie przechowywany obiekt zasad grupy.
2. Obiekty powiązane z lokacjami
3. Obiekty powiązane z domenami
4. Obiekty powiązane z jednostkami organizacyjnymi

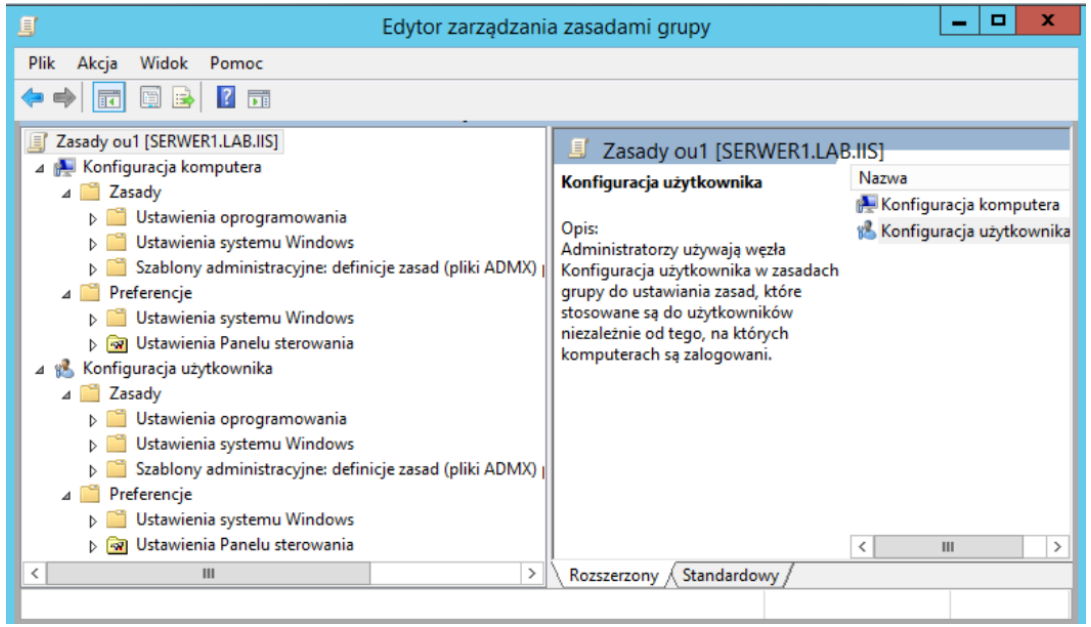
Edycja GPO

Do edycji GPO służy konsola Zarządzanie zasadami grupy, którą można uruchomić z menu Narzędzia Menedżera Serwera.



Edycja GPO

- Ustawienia zasad grupy znajdują się w **Obiektach Zasad Grupy** (**GPO**) i służą do zdefiniowania środowiska pulpitowego użytkowników.
- Ustawienia zasad grupy zawarte w danym GPO można przeglądać za pomocą Edytora GPO.
- Istnieją dwa rodzaje ustawień zasad grupy:
  - ustawienia konfiguracji komputera
  - ustawienia konfiguracji użytkownika.
- Uwaga: Ustawienia zasad grupy mają pierwszeństwo przed ustawieniami profili użytkowników.

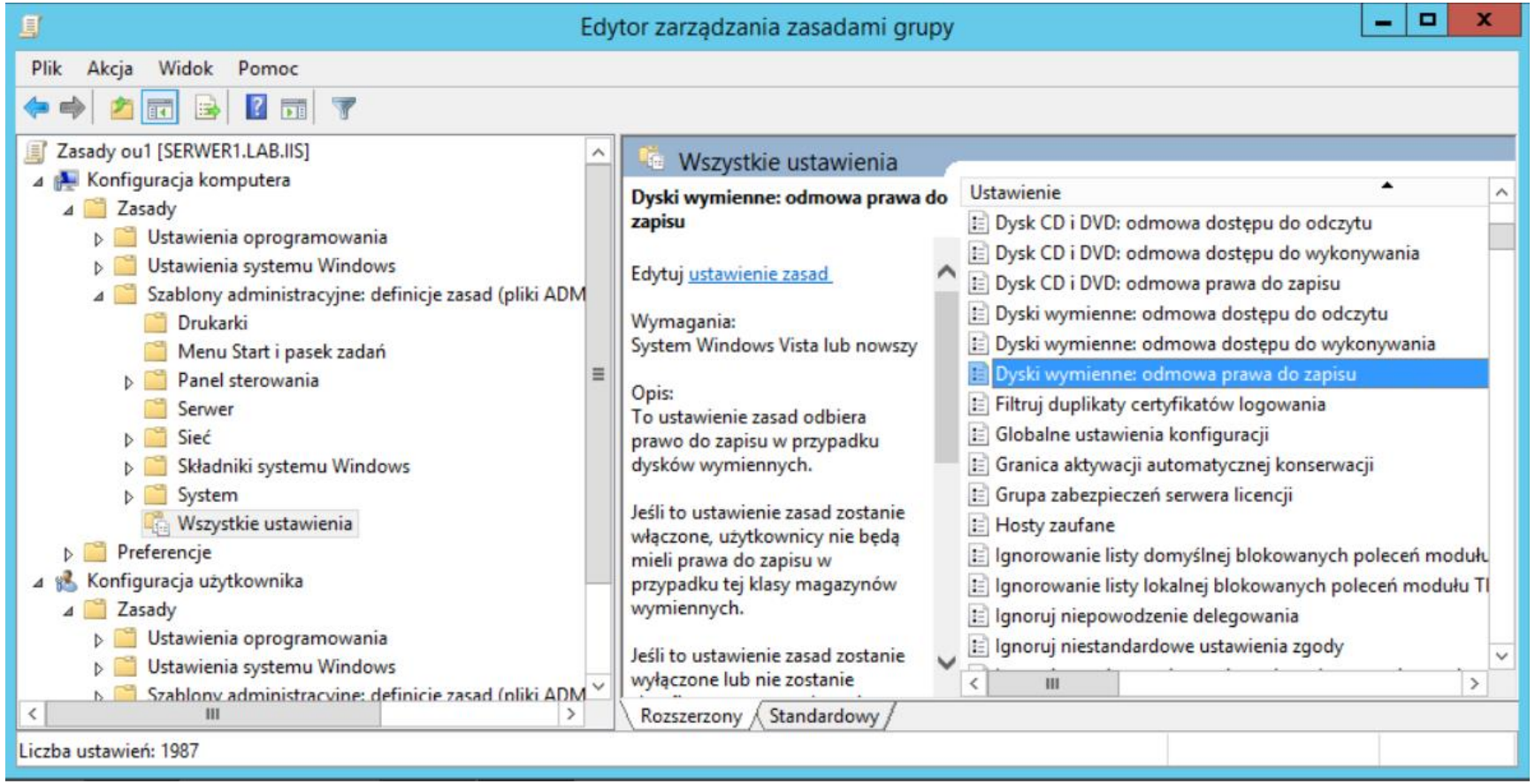


Węzeł ustawień oprogramowania

- Domyślnie pod tym węzłem znajduje się tylko rozszerzenie **Software Installation** (**Instalacja Oprogramowania**).
- Rozszerzenie to umożliwia określenie metod instalacji i utrzymywania oprogramowania dla organizacji;
- Producenci oprogramowania mogą tutaj dodać własne ustawienia.
- Umożliwia zarządzanie aplikacją w ramach GPO powiązanego z określoną lokacją, domeną lub jednostką organizacyjną Active Directory.
- Zarządzanie aplikacją może polegać na jej przypisaniu (komputery i użytkownicy podlegający danemu GPO będą posiadać tę aplikację) lub publikacji (użytkownicy podlegający GPO mają możliwość posiadania tej aplikacji - nie można publikować aplikacji komputerom).

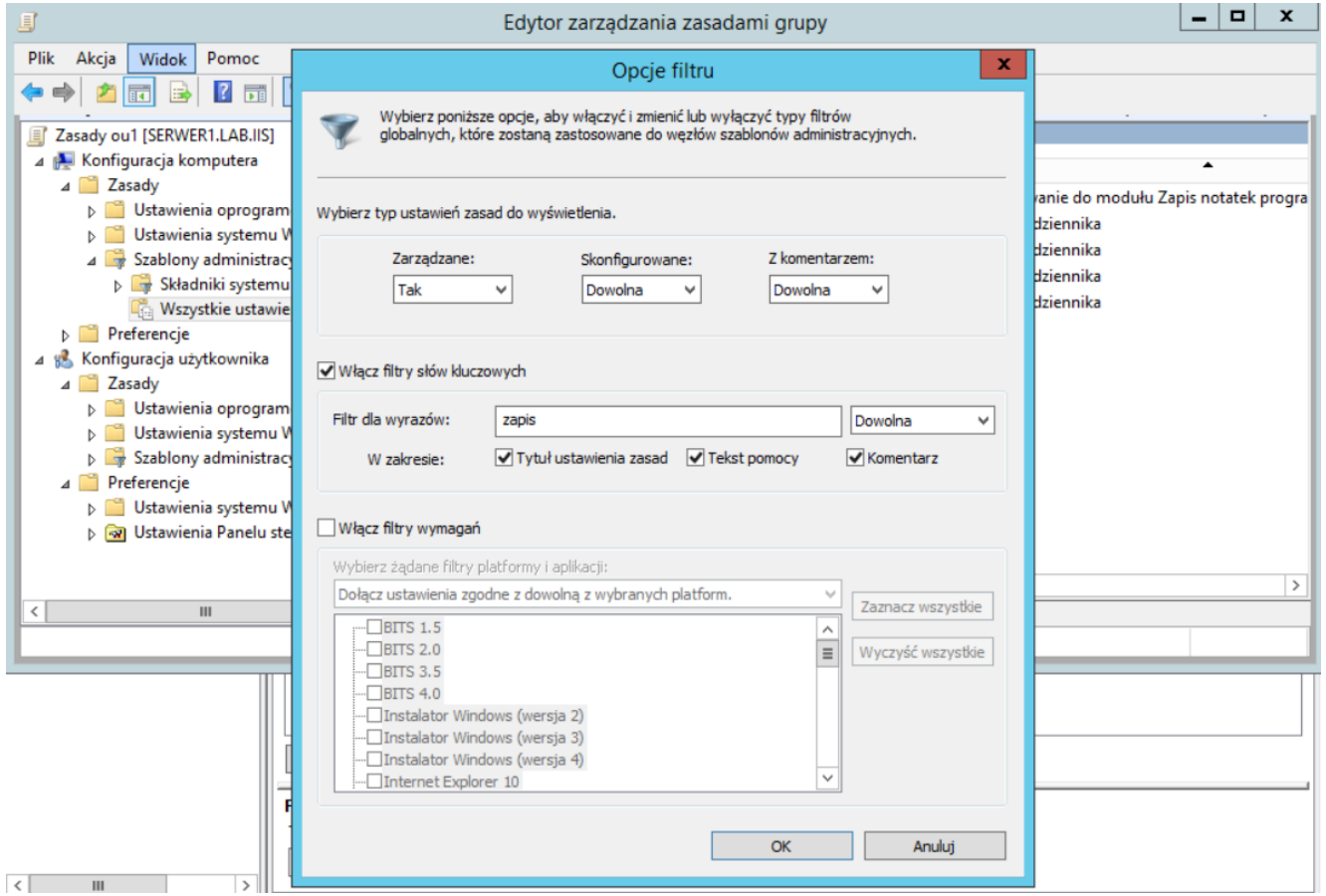
Węzeł szablonów administracyjnych

Istnieje blisko 2000 ustawień, które można wykorzystać do skonfigurowania środowiska użytkownika.



Węzeł szablonów administracyjnych

Ponieważ węzeł szablonów administracyjnych zawiera dużą ilość ustawień, to Windows Server oferuje funkcję umożliwiającą filtrowanie ich widoku - określenie, które ustawienia mają być wyświetlane w Edytorze obiektów zasad grupy.



Szablony administracyjne

- Szablon administracyjny jest plikiem tekstowym o rozszerzeniu .adm służącym do generowania interfejsu użytkownika, odpowiadającego ustawieniom **Zasad Grupy** konfigurowanym w edytorze.
- Istnieją trzy rodzaje szablonów administracyjnych:
  - Szablony domyślne - szablony administracyjne dostarczone razem z Windows Sewer (system.adm, inetres.adm, wmplayer.adm, conf.adm, wuau.adm).
  - Szablony dostarczone przez producentów – szablony dostarczone razem z aplikacjami przeznaczonymi dla Windows Server.
  - Szablony niestandardowe - szablony tworzone przy użyciu języka adm służące do dalszego sterowania ustawieniami komputerów lub użytkowników.
- Zazwyczaj szablony niestandardowe są tworzone przez projektantów aplikacji.
- *Informacje o języku adm i tworzeniu własnych szablonów administracyjnych można znaleźć pod hasłem „adm Language Reference” w witrynie pomocy technicznej firmy Microsoft pod adresem http://technet.microsoft.com/default.aspx*

Dziedziczenie zasad grupy

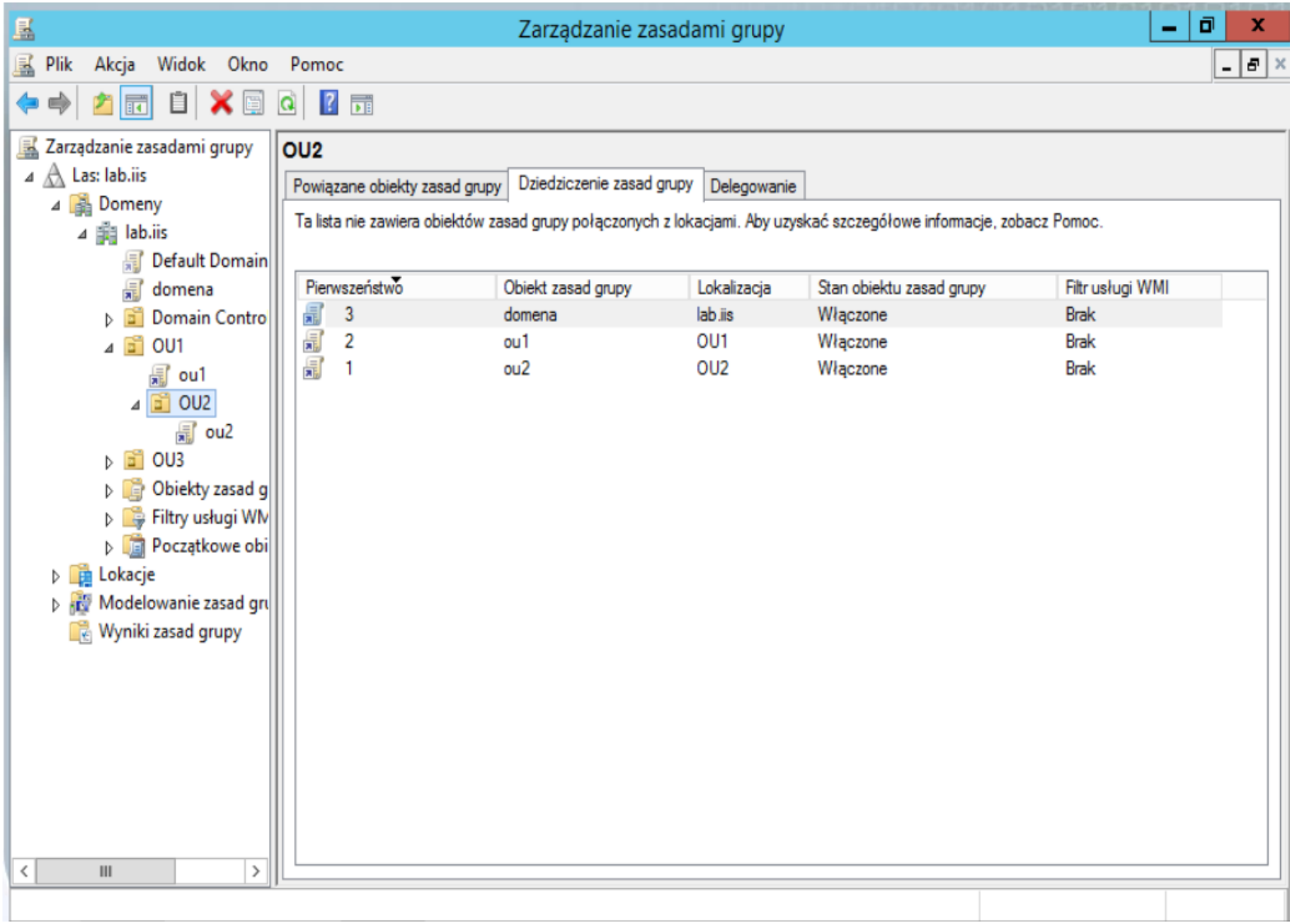
Zasady:

- Jeśli dane ustawienie zasad jest skonfigurowane (włączone lub wyłączone) na poziomie nadrzędnej jednostki organizacyjnej, a nie zostało skonfigurowane na poziomie podrzędnej jednostki organizacyjnej, to podrzędna jednostka organizacyjna dziedziczy ustawienie skonfigurowane na poziomie nadrzędnym.
- Jeśli dane ustawienie zasad jest skonfigurowane (włączone lub wyłączone) na poziomie nadrzędnej jednostki organizacyjnej oraz jest skonfigurowane na poziomie podrzędnej jednostki organizacyjnej, to w wypadku konfliktu ustawienie skonfigurowane dla podrzędnej jednostki organizacyjnej zastępuje ustawienie dziedziczone
- Ustawienia nieskonfigurowane na poziomie nadrzędnej jednostki organizacyjnej nie są dziedziczone przez podrzędne jednostki organizacyjne

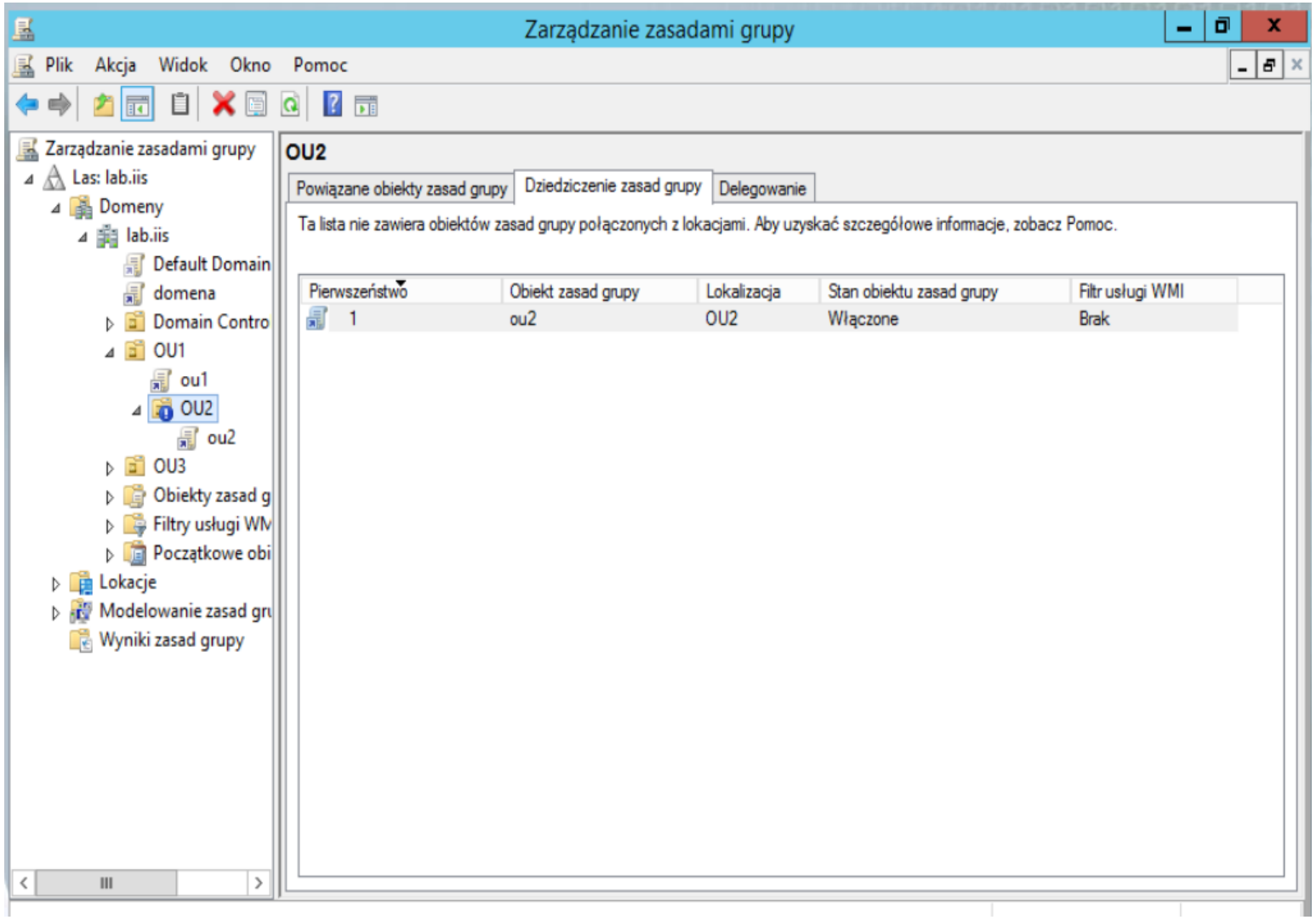
Wyjątki od reguł stosowania zasad

- Członkowie **Grup Roboczych** - Komputer należący do grupy roboczej przetwarza tylko lokalny GPO.
- Wymuszanie łącza obiektu zasad grupy - GPO powiązany z lokacją, domeną lub jednostką organizacyjną (ale nie GPO lokalny) może być ustawiony na Enforced (Wymuszony) – ustawienia zawarte w tym GPO nie będą zastępowane przez ustawienia później stosowanych zasad.
- Blokowanie dziedziczenia zasad - każda lokacja, domena lub jednostka organizacyjna może zostać skonfigurowana na Block Inheritance (Zablokuj dziedziczenie) – nieuwzględnienie wszystkich ustawień zasad grupy, pochodzących z kontenerów nadrzędnych.
- Ustawienia Enforced (Wymuszaj) i Block Inheritance (Blokuj dziedziczenie) mogą zakłócić funkcjonowanie innych GPO, a więc powinny być stosowane tylko w razie konieczności

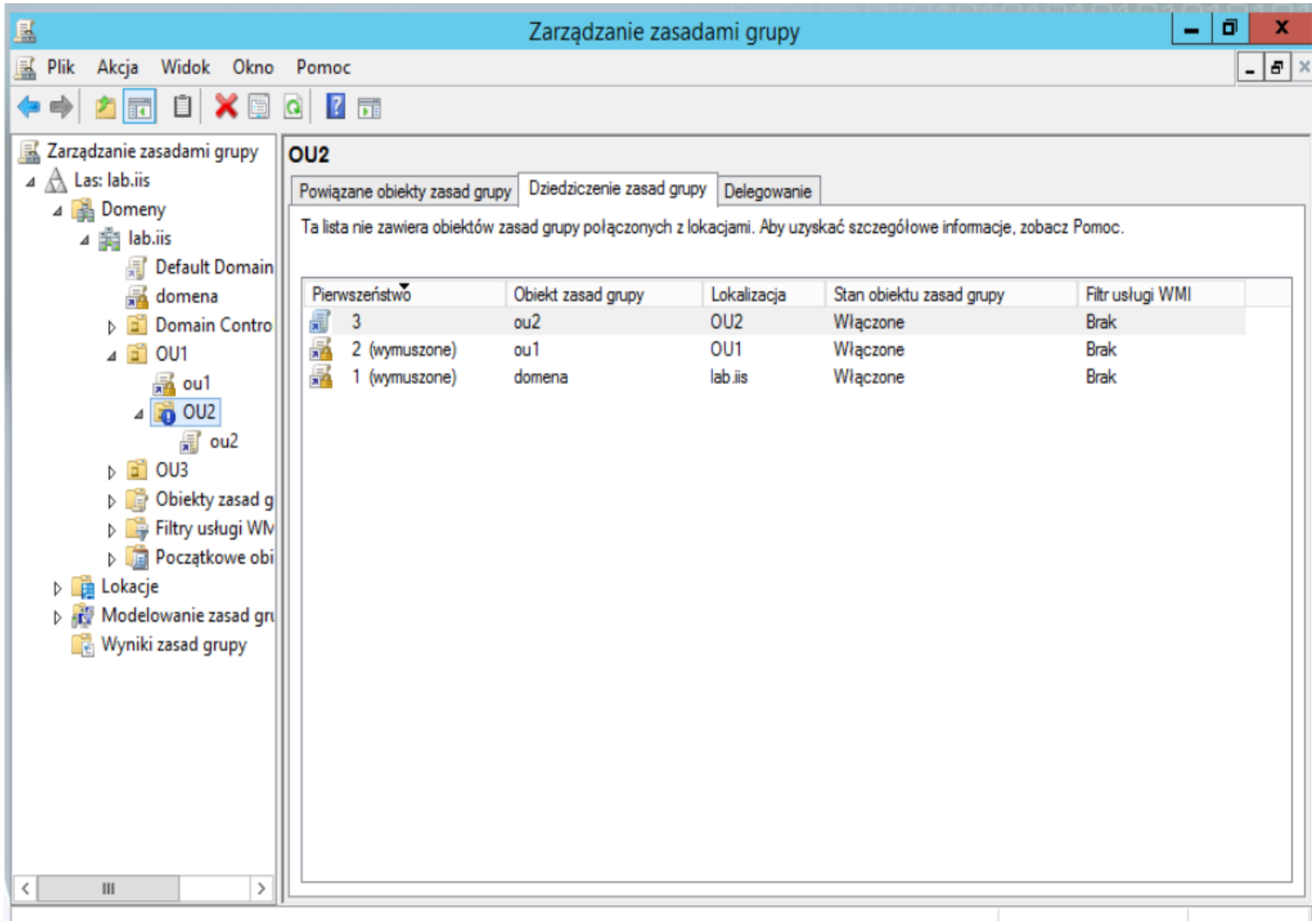
Dziedziczenie GPO - przykład



Wyłączenie dziedziczenia



Wymuszenie stosowania zasad



Delegowanie kontroli nad obiektami zasad grupy

- Niektóre zadania związane z obiektami zasad grupy (edycja GPO, tworzenie GPO, zarządzanie łączami GPO) mogą podlegać delegowaniu.
- Aby delegować prawo edycji GPO, należy dla określonych użytkowników i grup ustawić uprawnienia odczytu i zapisu na Allow (Zezwalaj).
- Aby delegować prawo tworzenia GPO, należy przypisać użytkowników do grupy Group Policy Creator Owners (Twórcy właściciele zasad grupy) oraz delegować kontrolę nad łączami GPO.

Active Directory – Zarządzanie

- Głównymi narzędziami służącymi do obsługi Active Directory są konsole:
  - Domeny i relacje zaufania Active Directory,
  - Lokacje i usługi Active Directory,
  - Użytkownicy i komputery Active Directory,
- Schemat Active Directory (dostępna na komputerach skonfigurowanych jako kontrolery domen, wymagająca ręcznej instalacji).
- Oprócz konsol, do administrowania AD używa się narzędzi przeznaczonych dla Active Directory, należących do zestawu Narzędzia obsługi systemu Windows.

Narzędzia AD do obsługi systemu Windows

- **Adsiedit.msc** (Edit ADSI - edycja ADSI):
  - dodawanie, przenoszenie i usuwanie z katalogu obiektów (w tym partycji schematu i konfiguracji),
  - wyświetlanie, modyfikacja i usuwanie atrybutów obiektów.
- **Dcdiag.exe** (Domain Controller Diagnostic – narzędzie diagnostyczne kontrolera domeny):
  - analizowanie stanu kontrolerów domen lesie lub w w przedsiębiorstwie i zwracanie informacji o ewentualnych problemach.
- **Dfscmd.exe** (Distributed File System Command Tool – narzędzie z poleceniami dla rozproszonego systemu plików):
  - zarządzanie rozproszonym systemem plików z linii polecenia.

Narzędzia AD do obsługi systemu Windows

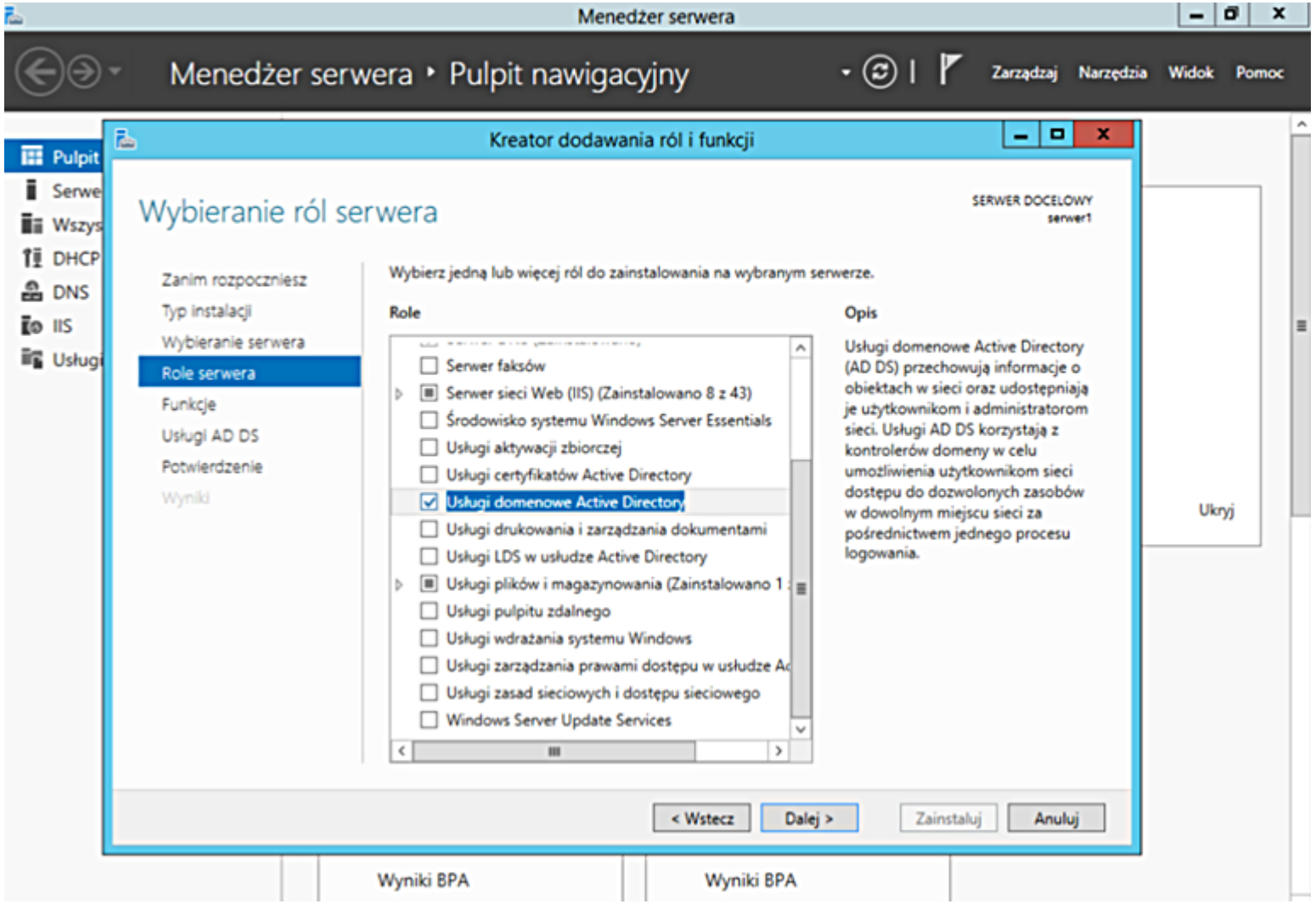
- **Dfsutil.exe** (Distributed File System Utility – narzędzia dla rozproszonego systemu plików):
  - zarządzanie wszystkimi aspektami rozproszonego systemu plików,
  - sprawdzenie zgodności konfiguracji serwerów DFS,
  - wyświetlenie topologii DFS.
- **Ldp.exe** (LDP Tool - narzędzie LDP):
  - wykonywanie w Active Directory operacji LDAP (łączenie, wiązanie, wyszukiwanie, modyfikowanie, dodawanie, usuwanie itd).

Narzędzia AD do obsługi systemu Windows

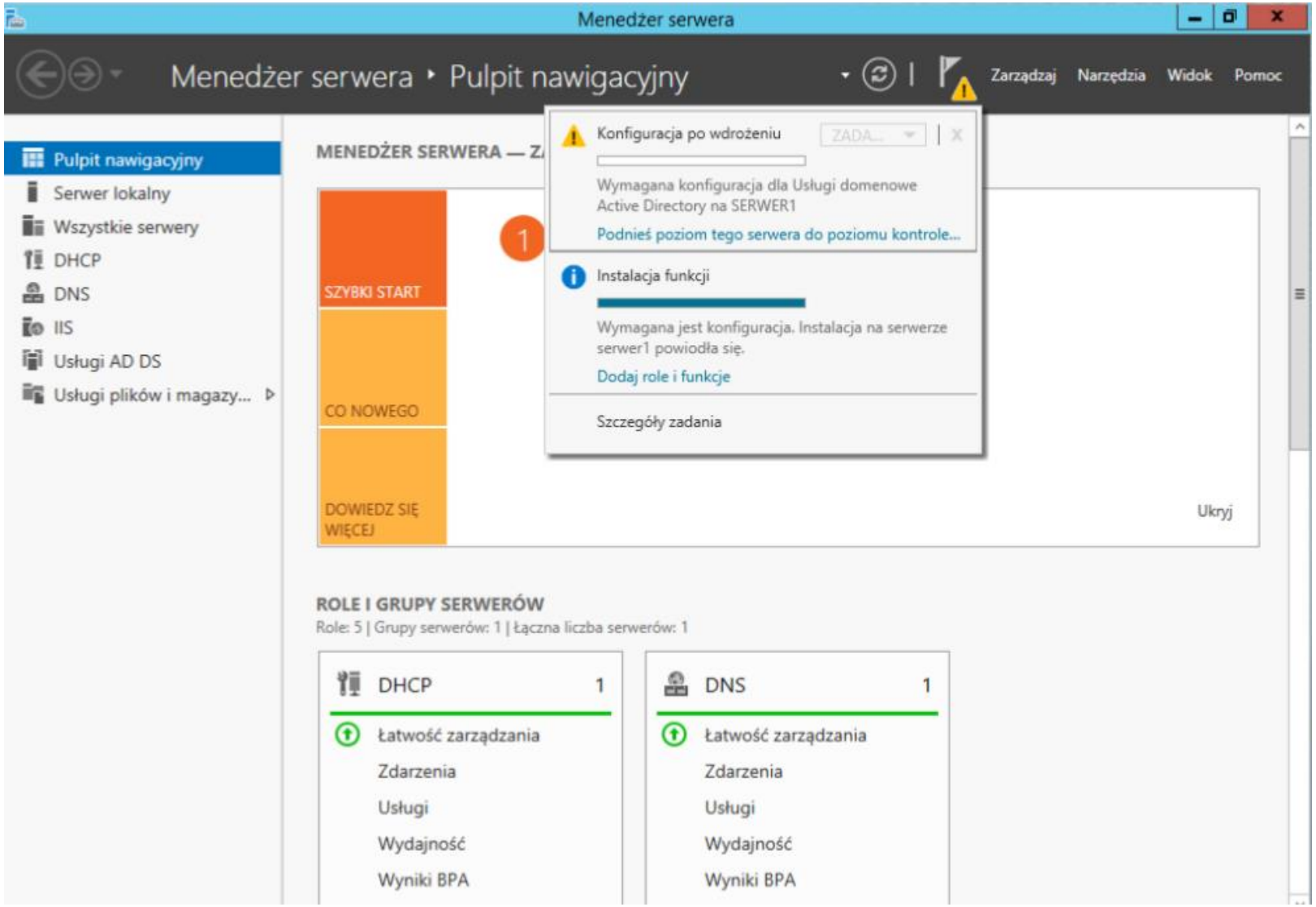
- **Netdom.exe** (Windows Domain Manager - menedżer domeny):
  - zarządzanie domenami Windows Server i relacjami zaufania z wiersza polecenia.
- **Nlest.exe**:
  - dostarczanie listy głównych kontrolerów domen
  - zamykanie komputera zdalnego
  - wyświetlanie informacji o relacjach zaufania i replikacji.
- **Repadmin.exe** (Replication diagnostyczne replikacji):
  - diagnostyka problemów kontrolerami domen.

Active Directory – Wdrażanie

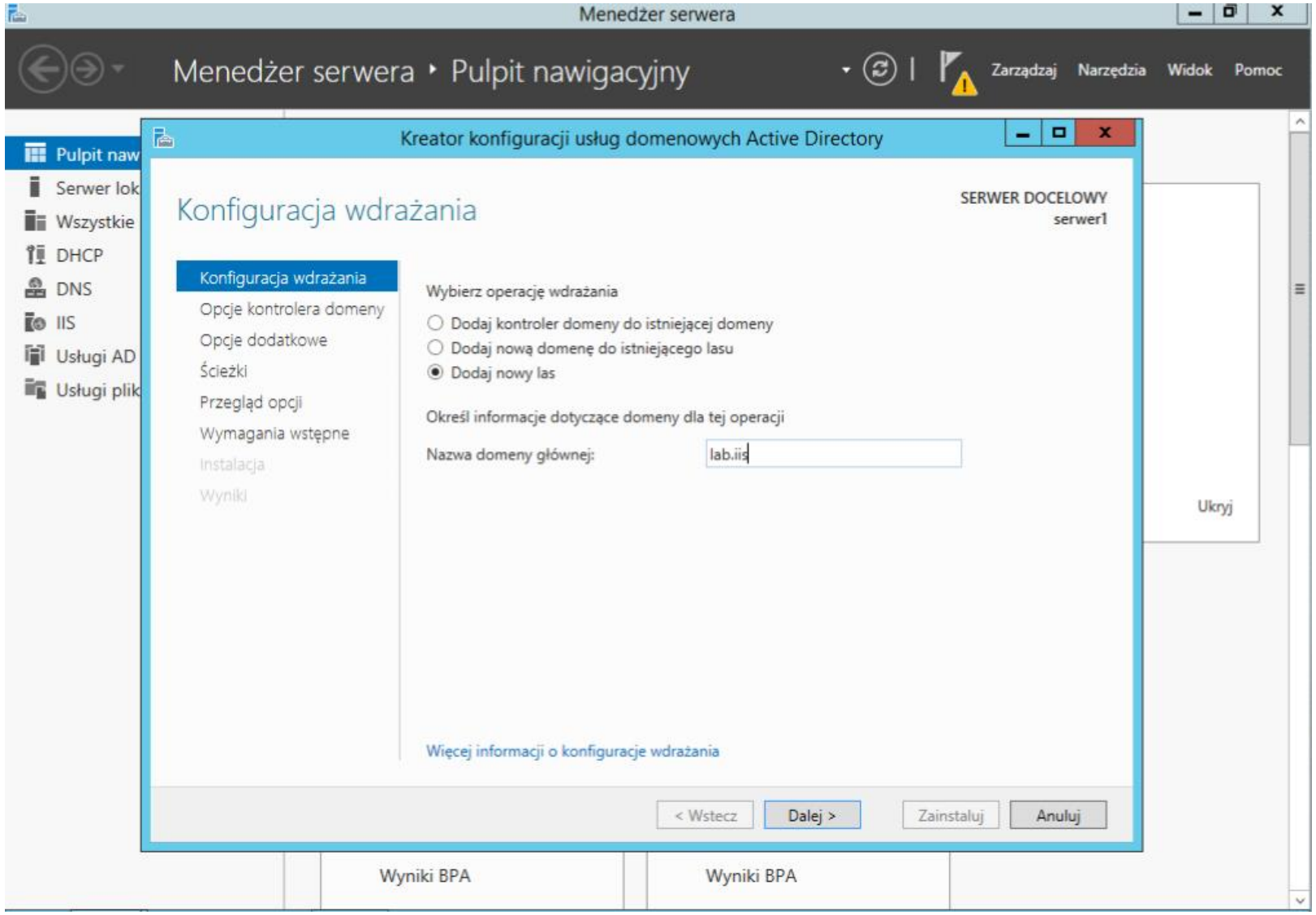
Instalacja usługi Active Directory



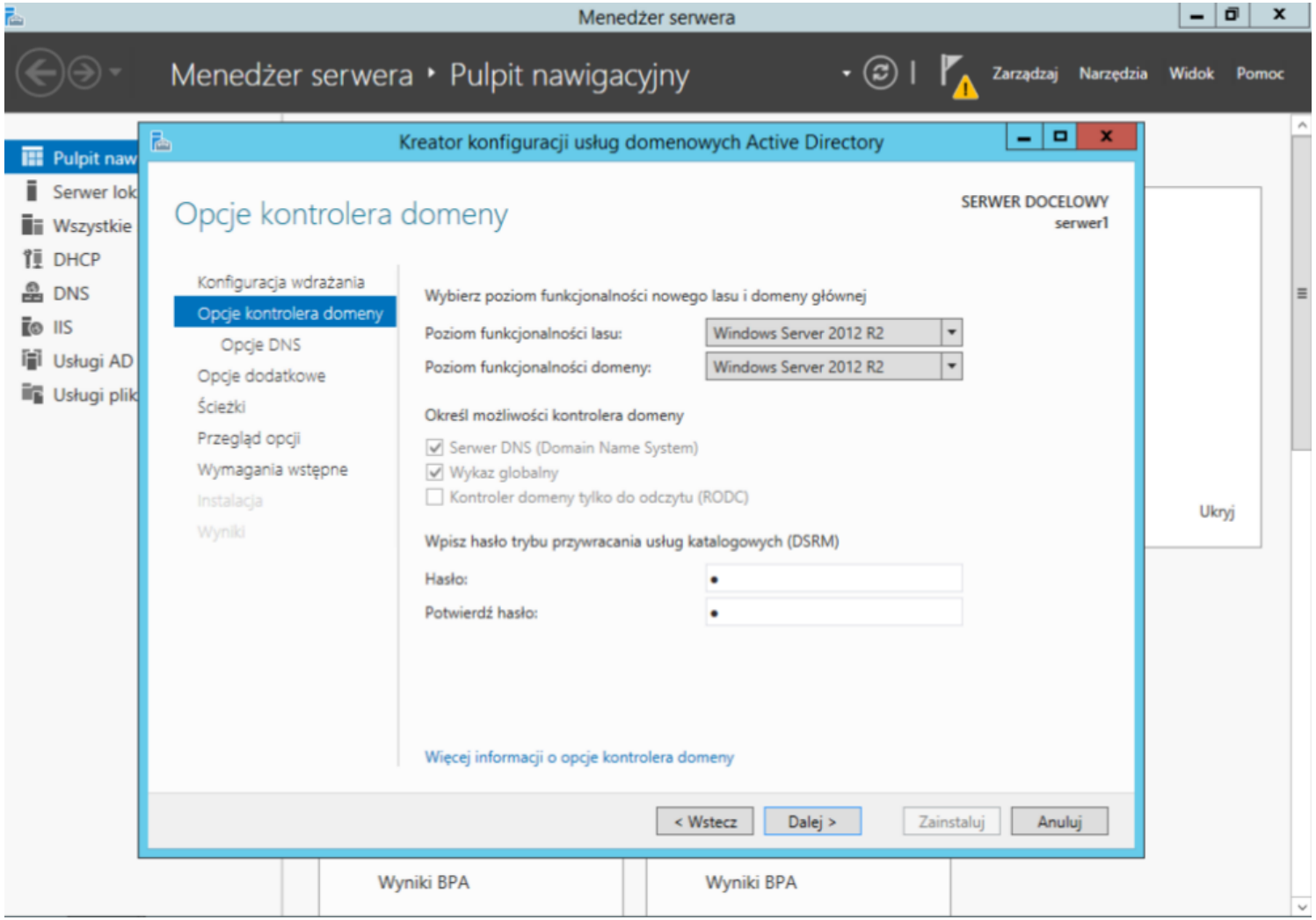
Uruchomienie konfiguracji AD



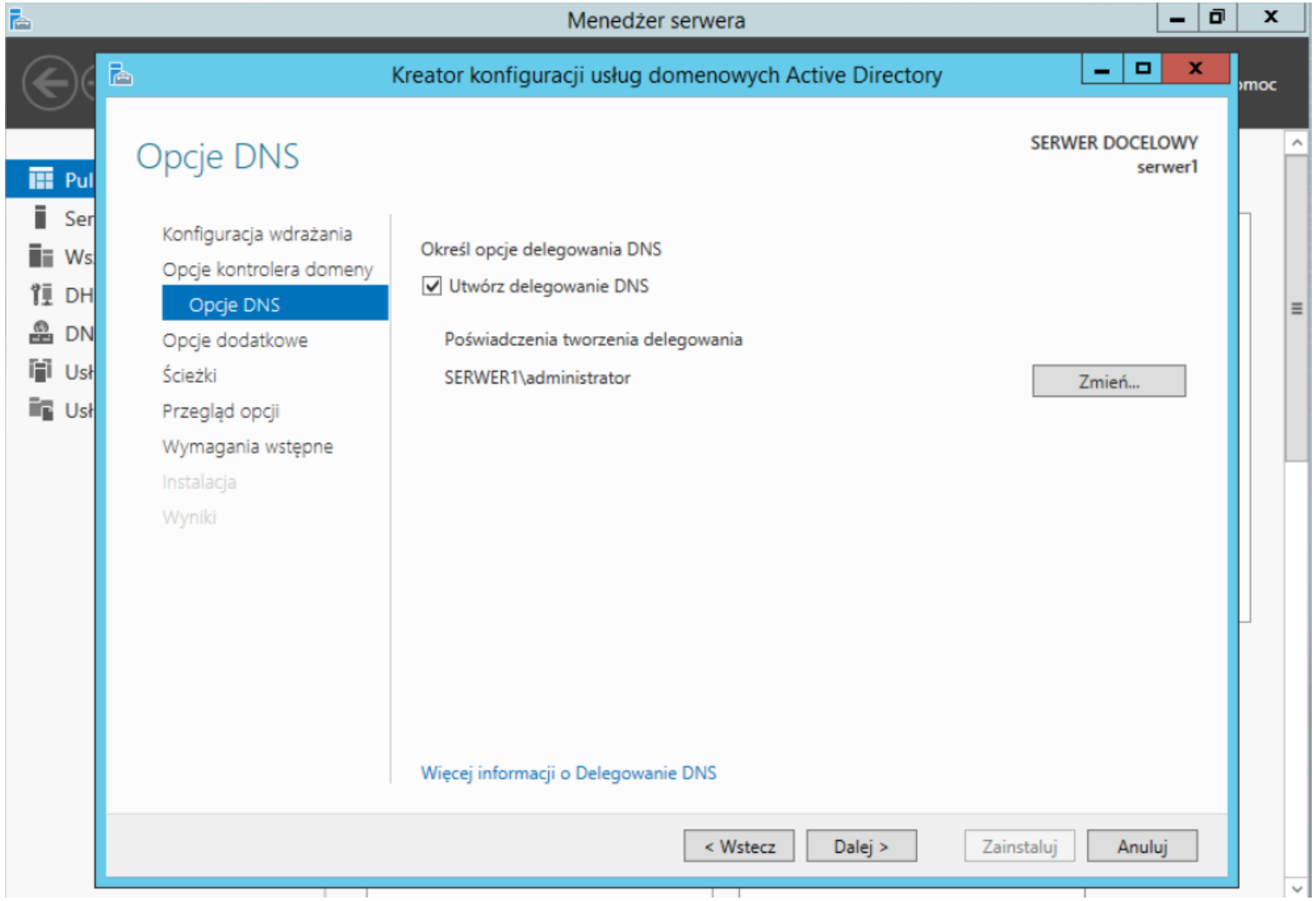
Wybór lokalizacji domeny



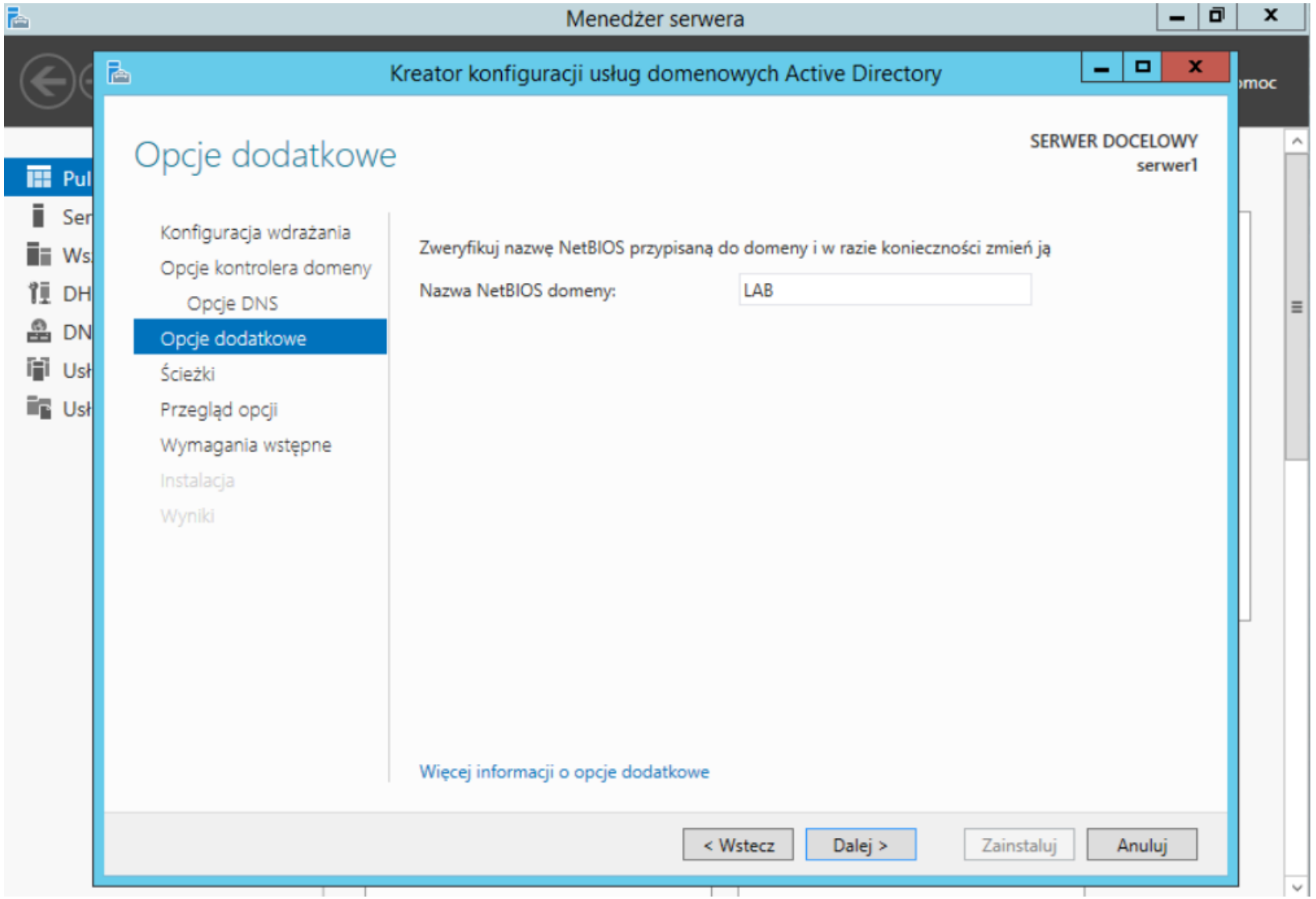
Wybór poziomu funkcjonalności domeny oraz hasła przywracania



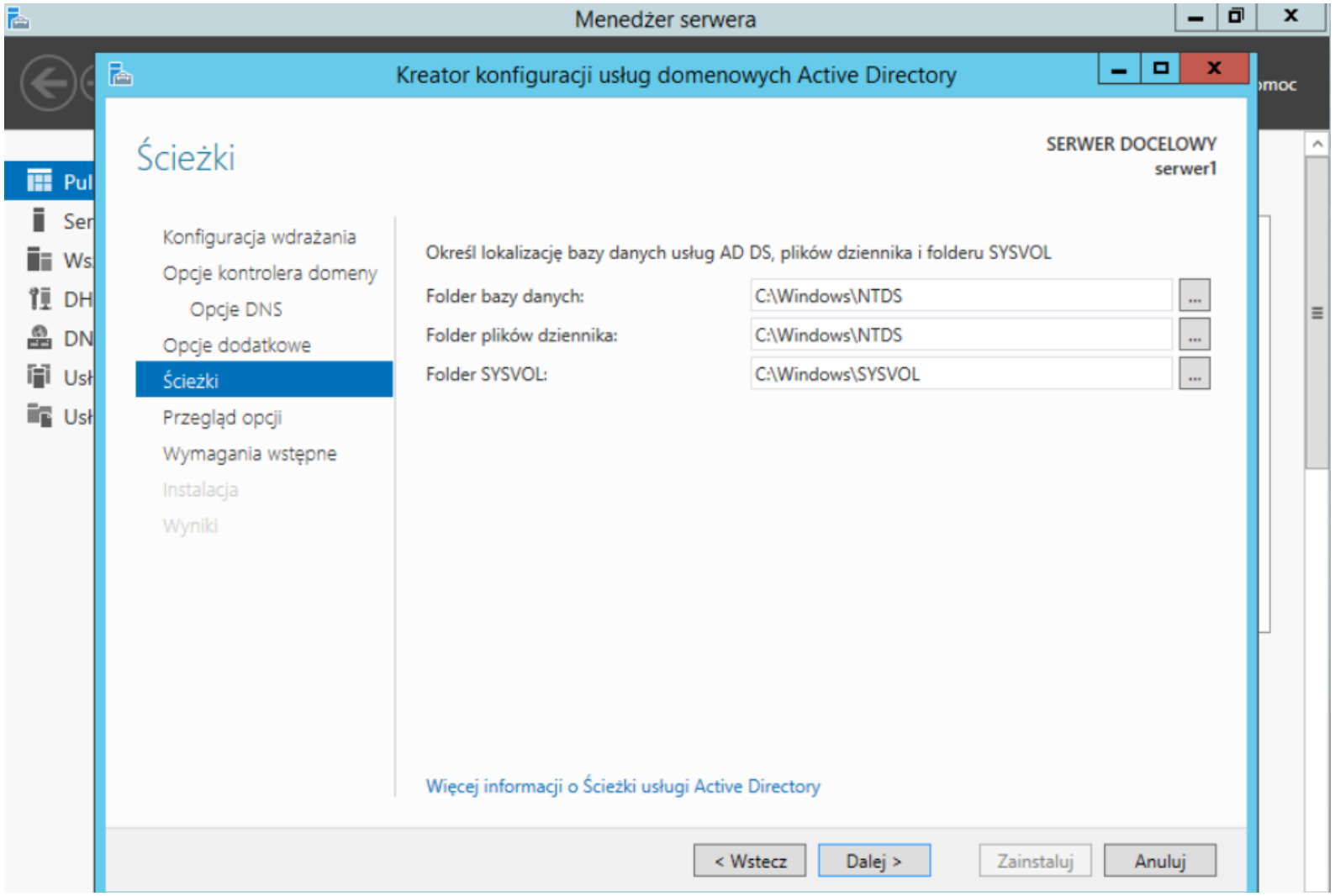
Delegowanie DNS



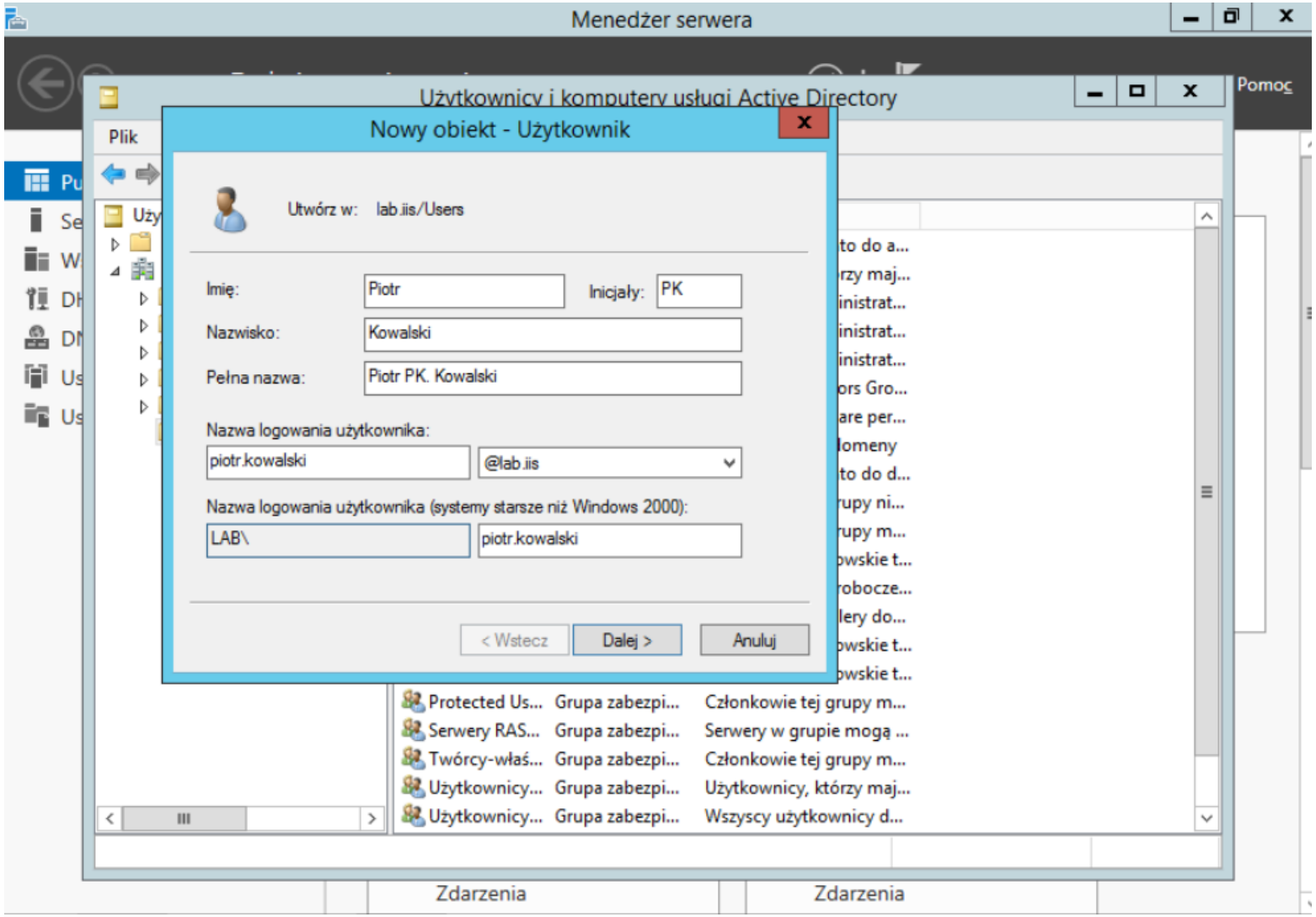
Wybór nazwy NetBIOS domeny



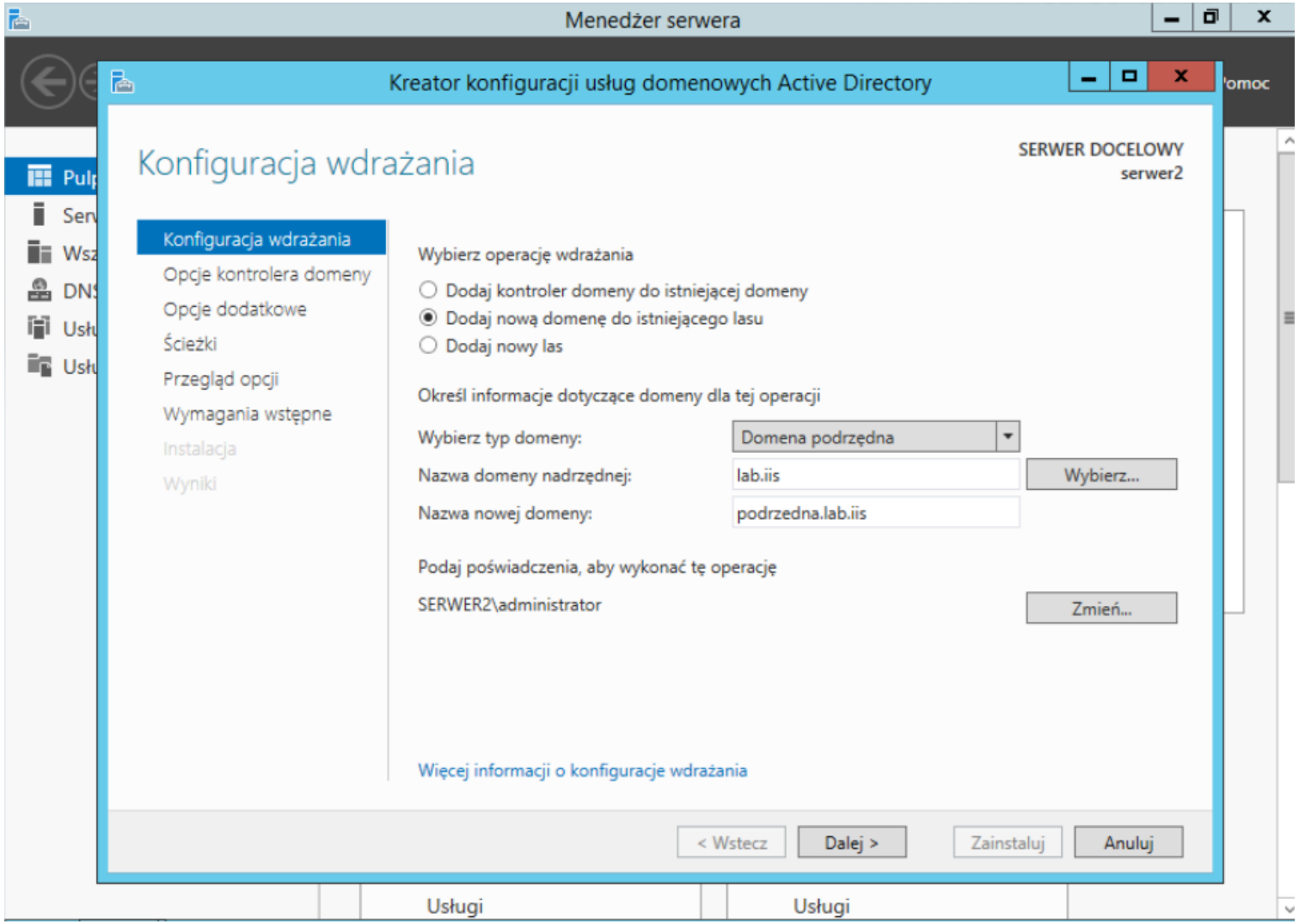
Wybór lokalizacji plików bazy danych AD



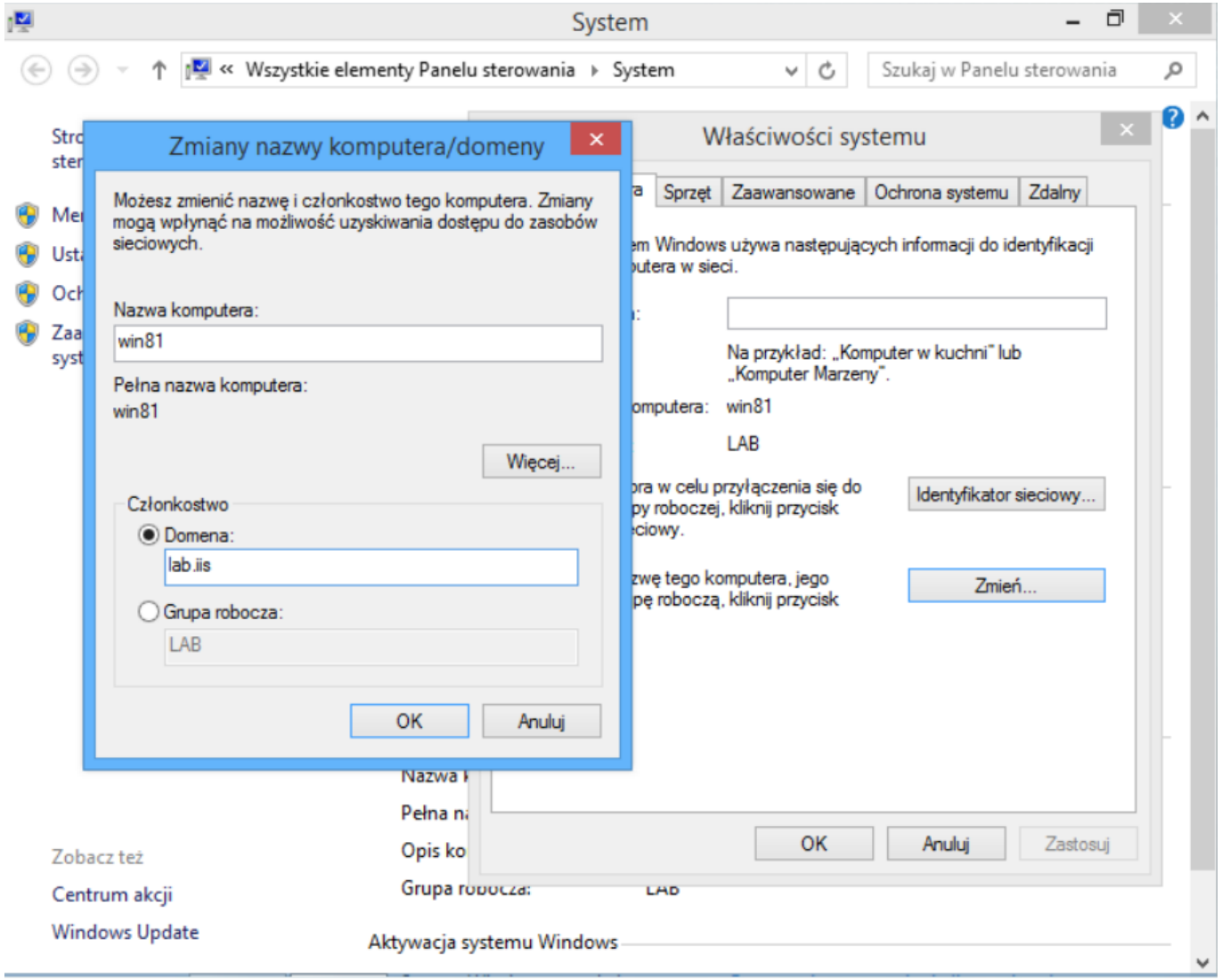
Dodanie użytkownika



Instalacja kontrolera domeny podrzędnej



Dodawanie komputera do domeny



Logowanie do domeny