Politechnika Białostocka

Wydział Elektryczny

Katedra Telekomunikacji i Aparatury Elektronicznej

Instrukcja do zajęć laboratoryjnych

Temat ćwiczenia:

Zintegrowane środowisko zarządzania systemem sieciowym z wykorzystaniem usług Active Directory

Numer ćwiczenia: **7**

Laboratorium z przedmiotu:
Zarządzanie sieciami teleinformatycznymi 2

Kod przedmiotu: TS1A611 254

Białystok 2018

Wstęp

W przypadku dużych środowisk sieciowych stosowane są zintegrowane systemy zarządzania pozwalające na scentralizowane administrowanie systemem złożonym z wielu serwerów, stacji roboczych i innych urządzeń sieciowych. Pozwalają one na wykonywanie wielu zadań administracyjnych takich jak instalowanie oprogramowania, poprawek, dodawanie użytkowników, przypisywanie uprawnień użytkownikom, monitorowanie systemu bez konieczności bezpośredniego fizycznego dostępu do zarządzanych stacji.

W systemach rodziny MS Windows dostępny jest system usług katalogowych o nazwie *Active Directory* (AD) zapewniający rozbudowaną funkcjonalność centralnego zarządzania systemem stacji roboczych i serwerów. System AD stanowi przedmiot niniejszego ćwiczenia, które zostało podzielone na dwie części:

– Podstawy usług katalogowych Active Directory w systemie Windows;
– Administrowanie kontami użytkowników w systemie Windows z wykorzystaniem AD.

Część 1 - Podstawy usług katalogowych Active Directory w systemie Windows

1. Wprowadzenie do usługi Active Directory.

Usługa Active Directory jest całkowicie zintegrowana z systemem operacyjnym Windows 2000/2003/2008 Server i oferuje hierarchiczny widok, rozszerzalność, skalowalność oraz rozproszone zabezpieczenia. Usługa umożliwia administratorom, programistom i końcowym użytkownikom uzyskanie dostępu do usługi katalogowej bezproblemowo zintegrowanej ze środowiskiem Internetu i intranetu. Umożliwia ona administratorom i końcowym użytkownikom korzystanie z usługi katalogowej jako źródła informacji, jak również jako usługi administracyjnej.

Usługa Active Directory integruje pochodzącą z Internetu koncepcję przestrzeni nazw z usługą katalogową systemu operacyjnego. Obszar nazw jest strukturalnym zbiorem informacji, w którym nazwy mogą być używane do symbolicznej reprezentacji różnego typu informacji, tak jak nazwa hosta reprezentuje adres IP i w którym ustalone są wyraźne zasady określania, w jaki sposób nazwy mogą być tworzone i używane. Integracja koncepcji nazw z usługą katalogową pozwala na ujednolicenie i zarządzanie wieloma obszarami nazw, które istnieją w heterogenicznych środowiskach sprzętowo-programowych w sieciach korporacyjnych. Usługa Active Directory wykorzystuje protokół LDAP (*Lightweight Directory Access Protocol*) i może działać bez ograniczeń systemowych, integrując wiele obszarów nazw. Może zarządzać katalogami aplikacji, jak również innymi katalogami, opartymi na sieciowych systemach operacyjnych, dostarczając katalog ogólnego użytku mogący zmniejszyć obciążenie administracyjne oraz koszty związane z utrzymywaniem wielu obszarów nazw.

Usługa Active Directory nie jest katalogiem protokołu X.500. Zamiast niego korzysta z LDAP jako protokołu dostępowego i wspiera model informacji protokołu

X.500, bez wymagania, aby systemy obsługiwały pełny protokół X.500. Rezultatem tego jest wysoki poziom współdziałania wspierający rzeczywiste sieci heterogeniczne.

Usługa Active Directory udostępnia jeden punkt administracyjny dla wszystkich ogłaszanych zasobów, takich jak pliki, urządzenia peryferyjne, połączenia hostów, bazy danych, dostęp do sieci Web, użytkownicy, usługi i inne obiekty. Korzysta ona z internetowej usługi DNS (*Domain Name System*) jako usługi lokalizatora oraz organizuje obiekty w domenach w hierarchię jednostek organizacyjnych (*Organizational Unit* - OU) i umożliwia wielu domenom łączenie się w strukturę drzewa. Administracja jest jeszcze bardziej uproszczona, ponieważ nie występują znane z Windows NT4.0 problemy podstawowy/zapasowy kontroler domeny. Zamiast tego usługa Active Directory wykorzystuje tylko kontrolery domeny. Wszystkie kontrolery domeny są równoprawne. Administrator może wprowadzić zmiany w dowolnym kontrolerze domeny, a uaktualnienia zostaną replikowane na wszystkie inne kontrolery domeny.

Usługa Active Directory, jak wszystkie usługi katalogowe jest zasadniczo obszarem nazw. Obszar nazw jest każdą ograniczoną przestrzenią, w której istnieje możliwość przetworzenia nazwy. Przetwarzanie nazw jest procesem tłumaczenia nazw na obiekty lub informację, którą nazwa reprezentuje. Obszar nazw usługi Active Directory opiera się na schemacie nazewniczym DNS, co umożliwia współdziałanie z technologiami internetowymi. Stosując wspólny obszar nazw można ujednolicić i zarządzać wieloma środowiskami sprzętowo-programowymi w sieci. Istnieją dwa typy obszarów nazw: ciągły i nieciągły różniące się sposobem powiązania obiektów nadrzędnego i podrzędnego (np. pliku i katalogu).

Działanie usługi Active Directory wymaga istnienia w domenie, co najmniej jednego (głównego) kontrolera domeny. Konwersje komputera z systemem Windows 2000/2003 z dowolnej wersji serwerowej wymaga uruchomienia odpowiedniego kreatora. Można to uczynić:

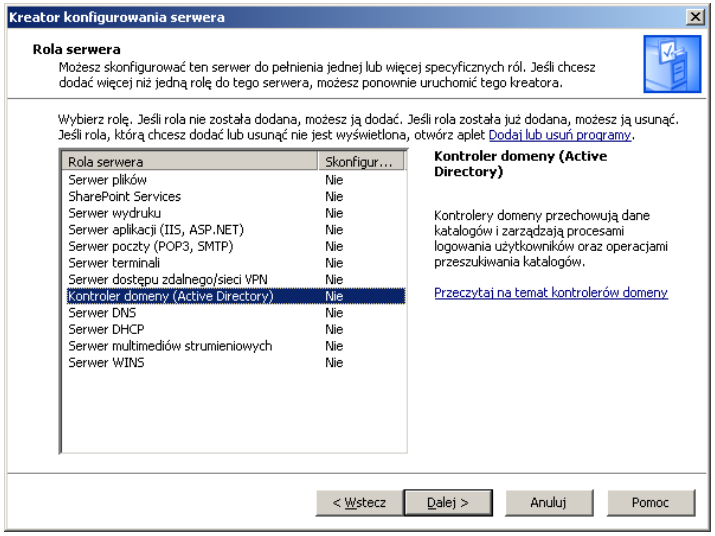
1. Z menu Start wybieramy pozycje *Uruchom* i w okienku wpisujemy ***dcpromo.exe***
2. Z menu *Start* wybieramy *Narzędzia administracyjne -> Zarządzanie tym serwerem*, następnie *Dodaj lub usuń rolę* (rysunek 1), zaznaczamy Kontroler domeny (Active Directory) (rysunek 2) i klikamy przycisk *Dalej*.

Uruchomienie instalatora może również odbyć się z wykorzystaniem Kreatora konfigurowania serwera uruchamianego z menu *Start* i zakładki *Narzędzia administracyjne*.

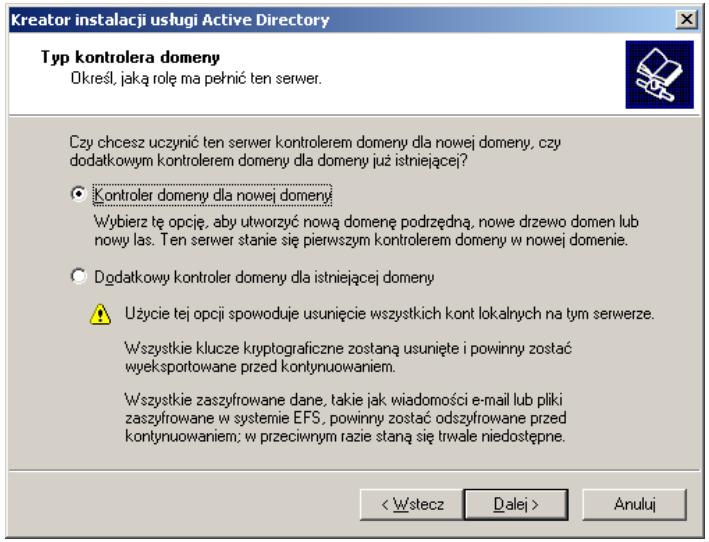
Najłatwiejszym sposobem uruchomienia programu instalatora kontrolera domeny jest wpisanie w okienku *Uruchom* menu *Start* polecenia: ***dcpromo***.

W pierwszym oknie instalatora klikamy przycisk *Dalej*. W kolejnym oknie zostawiamy wybraną opcje *Kontroler domeny dla nowej domeny* (rysunek 3). Klikamy przycisk *Dalej*.

Rys. 1. Widok okna *Zarządzanie tym serwerem*.

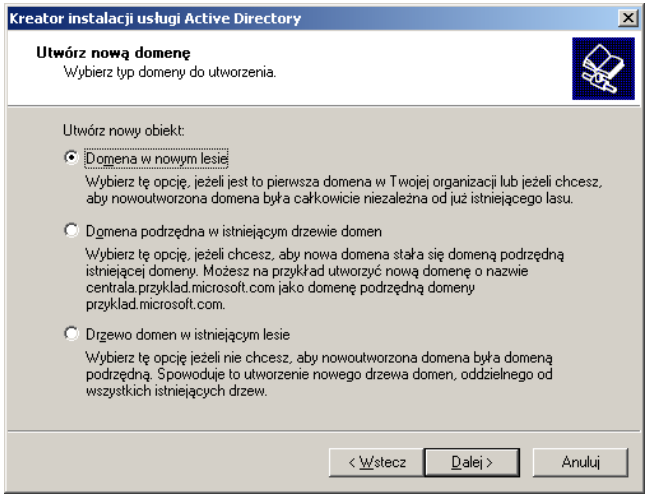


Rys. 2. Uruchomienie instalatora dla kontrolera domeny Windows i usługi Active Directory.



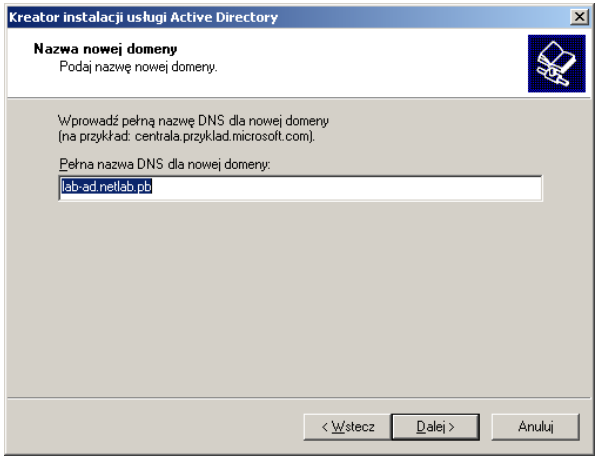
Rys. 3. Na wybranym komputerze instalujemy kontroler nowej domeny.

W kolejnym oknie dialogowym (rysunek 4) wybieramy tworzenie domeny w nowym lesie domen. Na opcje Tworzenie nowego potomka domeny w istniejącym drzewie domen decydujemy się wtedy, gdy w istniejącym już drzewie domen chcemy utworzyć nowa domenę. W naszym przypadku chodzi nam o utworzenie całkowicie nowego, oddzielnego drzewa w nowym, nie istniejącym jeszcze lesie domen. Klikamy przycisk *Dalej*.



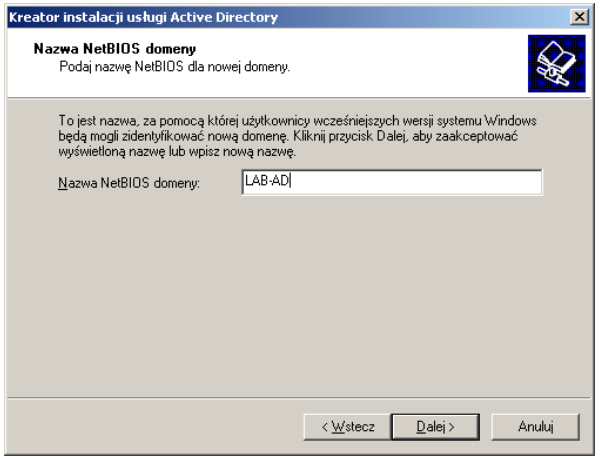
Rys. 4. Tworzymy nowe drzewo domen.

Komputery naszej domeny, w której działa usługa katalogowa powinny być widoczne w sieci globalnej. Stad konieczność nadania jej nazwy (rysunek 5). W okienku dialogowym wpisujemy pełną nazwę domeny (np. **lab-ad.netlab.pb**) i klikamy przycisk *Dalej*.



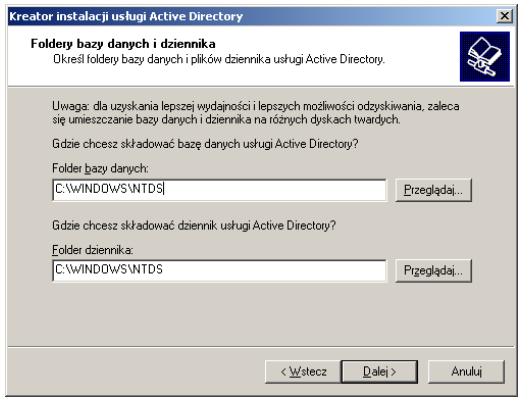
Rys. 5. Propozycja nazwy domeny.

Domena powinna zostać wcześniej zarejestrowana. Powinna zostać również wpisana na najbliższym, uznanym serwerze DNS. W przypadku domeny omawianej w opracowaniu jej pełna nazwa to: **lab-ad.netlab.pb** i została ona zarejestrowana w domenie: **netlab.pb**. Ponieważ usługi katalogowe Windows wykorzystują protokół NetBIOS konieczne jest również podanie nazwy domeny dla potrzeb tego protokołu. Instalator podpowiada nazwę, będącą pierwsza częścią nazwy DNS (rysunek 6). Zatwierdzamy nazwę klikając przycisk *Dalej*.



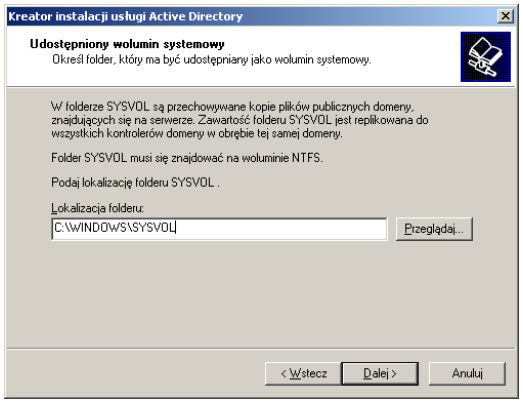
Rys. 6. Nazwa domeny dla protokołu NetBIOS.

W kolejnym oknie kreatora decydujemy o położeniu na dysku serwera pliku bazy danych usługi Active Directory i pliku diagnostyki (dziennika - log). Dla poprawnego działania aplikacji systemowych oraz w celu uniknięcia późniejszych problemów z konfiguracja komponentów usługi katalogowej zaleca się pozostanie przy proponowanych ustawieniach (rysunek 7). Niektórzy zalecają rozdzielenie pliku bazy danych i pliku dziennika na dwa fizyczne dyski. Rozwiązanie to stosujemy w dużych domenach dla zwiększenia wydajności bazy danych usługi.



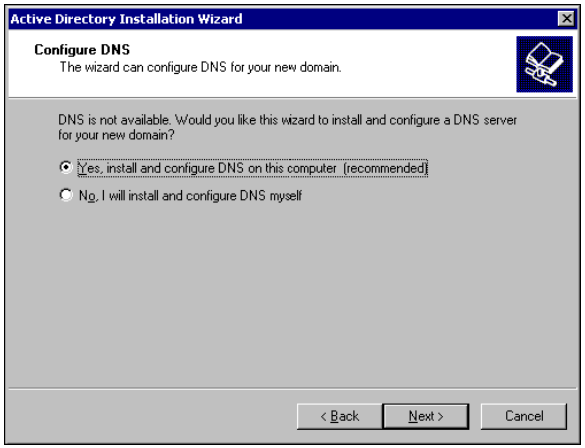
Rys. 7. Katalogi plików bazy danych i diagnostyki (dziennika) usługi Active Directory.

Kolejne okno umożliwia specyfikacje katalogu występującego na kontrolerze domeny, współdzielonego przez wszystkie komputery w domenie (katalogu systemowego – domyślna lokalizacja %systemroot%\Sysvol). Katalog jest wykorzystywany głównie do komunikacji, dla utrzymania spójności danych w bazie Active Directory. Zawiera skrypty i niektóre obiekty zasad grup dla domeny. Jest udostępniony i musi znajdować się na wolumenie partycji sformatowanej w systemie plików NTFS 5.0. Również i tutaj pozostajemy przy proponowanej nazwie i klikamy przycisk *Dalej* (rysunek 8).



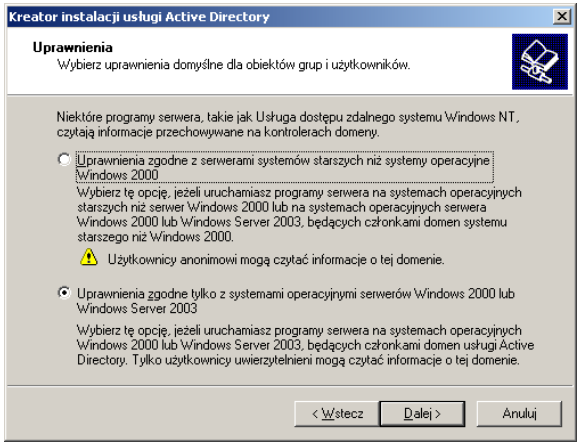
Rys. 8. Specyfikacja folderu systemowego dla potrzeb usługi Active Directory.

Jakiekolwiek braki w konfiguracji DNS objawia się w kolejnym oknie. Jeśli nie mamy połączenia ze światem zewnętrznym lub nasza domena nie została zarejestrowana lub nie mamy poprawnie skonfigurowanej usługi DNS pojawi się okno ostrzeżenia w którym wybieramy opcję zainstalowania serwera DNS na tym komputerze (rysunek 9). Klikamy przycisk *Dalej*.



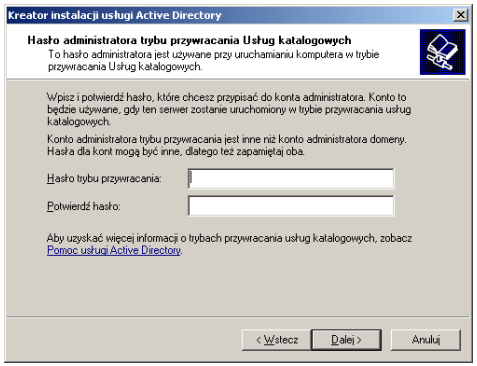
Rys. 9. Automatyczna instalacja i konfiguracja DNS.

Kolejne okno instalatora umożliwia zdecydowanie o sposobie dostępu do zasobów usługi Active Direktory serwera z komputerów domeny. Jest on wymagany przez niektóre aplikacje. Jeśli w domenie mają pracować komputery z systemem starszym od Windows 2000 wybieramy opcję pierwszą. Jeśli nasza domena składa się z komputerów pracujących tylko pod kontrola systemu Windows 2000 lub nowszych wybieramy opcję drugą (rysunek 10).



Rys. 10. Określenie sposobu dostępu do zasobów usługi Active Directory.

W kolejnym oknie podajemy oraz weryfikujemy hasło, które może zostać wykorzystane w przypadku odtwarzania zawartości bazy danych usługi AD, np. po awarii systemu (rysunek 11). Pola te można pozostawić puste.



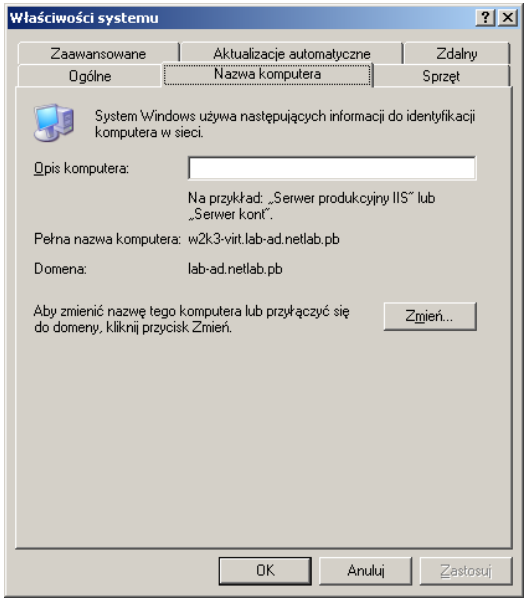
Rys. 11. Hasło administratora domeny.

Na zakończenie pojawia się okno podsumowania wybranych ustawień. Naciskamy przycisk *Dalej* uruchamiając proces instalacji usługi. Na zakończenie pojawia się okno podsumowania wykonanej instalacji. Po kliknięciu przycisku *Zakończ* restartujemy komputer. Serwer kontrolera domeny jest gotowy do pracy.

Czynności do wykonania:

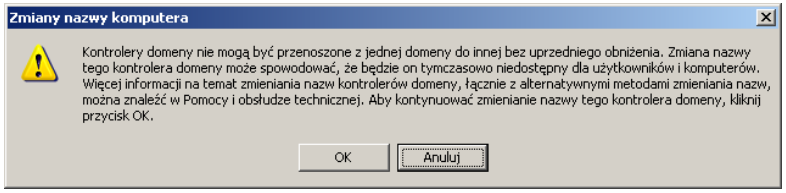
0. **Uruchom system Windows 2003 Server na maszynie wirtualnej skonfigurowanej na jednym z komputerów znajdujących się na stanowisku laboratoryjnym. Zaloguj się do tego serwera jako użytkownik *Administrator*.**
1. **Dla aktywnego interfejsu sieciowego skonfiguruj ustawienia protokołu TCP/IP na adres z sieci 192.168.1.0/24. Nadaj własną nazwę hosta (np. dc, grupy roboczej oraz prefix DNS netlab.pb. Sprawdź czy serwer ten komunikuje się sieciowo z innym komputerem na stanowisku laboratoryjnym. W razie potrzeby dokonaj odpowiednich ustawień sieciowych.**
2. **Dokonaj konwersji skonfigurowanego w poprzednim kroku komputera do kontrolera domeny z usługą Active Direktory (wykonując opisane powyżej kroki).**

Po ponownym uruchomieniu serwera jego identyfikacja sieciowa powinna wyglądać jak na rysunku 12 (z dokładnością do nazwy komputera i domeny).



Rys. 12. Identyfikacja sieciowa serwera domeny.

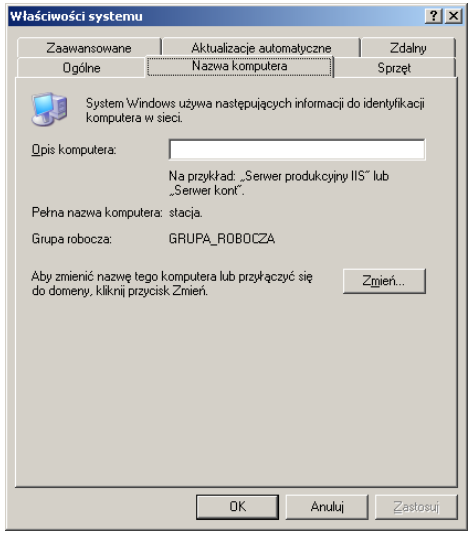
Zmiana nazwy kontrolera domeny (przeniesienie go do innej domeny), jeśli ten został zbudowany z wykorzystaniem systemu Windows2000, jest w ogóle niemożliwa. W przypadku kontrolera z systemu Windows 2003 nazwę kontrolera można zmienić, ale z zachowaniem wskazówek opisanych w oknie przedstawionym na rysunku 13.



Rys. 13. Warunki zmiany nazwy kontrolera domeny.

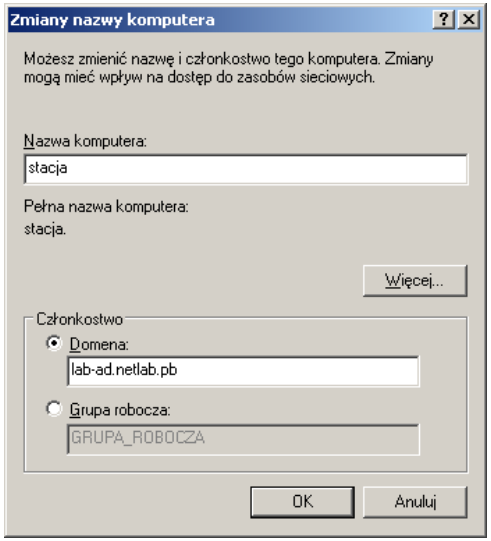
Podłączanie komputera klienckiego do domeny.

Dowolny komputer podłączamy do domeny zmieniając jego identyfikację w środowisku sieciowym. W tym celu klikamy prawym przyciskiem myszy na ikonkę *Mój komputer* i z menu wybieramy pozycje *Właściwości*. Z okienka *Właściwości* wybieramy zakładkę *Nazwa komputera* i klikamy przycisk *Zmień* (rysunek 14).



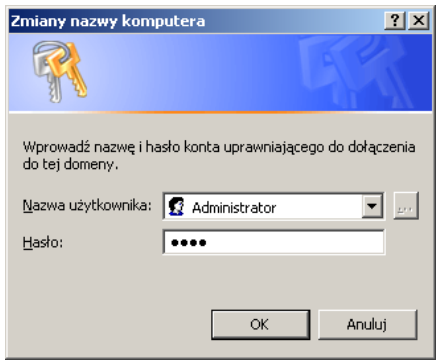
Rys. 14. Identyfikacja sieciowa komputera.

Pojawi się kolejne okienko, w którym nasz komputer będzie widziany jako członek grupy roboczej (rysunek 15). Zaznaczamy opcję *Domena* w ramce *Członkostwo* i w okienku dialogowym wpisujemy nazwę domeny (np. **lab-ad.netlab.pb**).



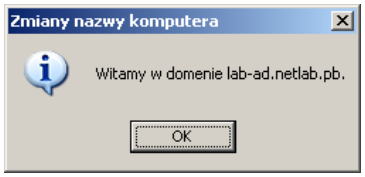
Rys. 15. Zmiana identyfikacji komputera w celu podłączenia go do domeny *lab-ad.netlab.pb*.

Jeśli domena została znaleziona, to pojawi się okienko dialogowe, w którym podajemy nazwę użytkownika (Administrator) i hasło umożliwiające dostęp do zasobów usługi Active Directory. Jest to samo hasło, które zostało podane jako hasło Administratora podczas serwera AD. Klikamy przycisk OK.



Rys. 16. Nazwa użytkownika i hasło umożliwiające podłączenie do domeny.

Po poprawnym podłączeniu do domeny pojawi się okno z komunikatem powitania (Rys. 17).



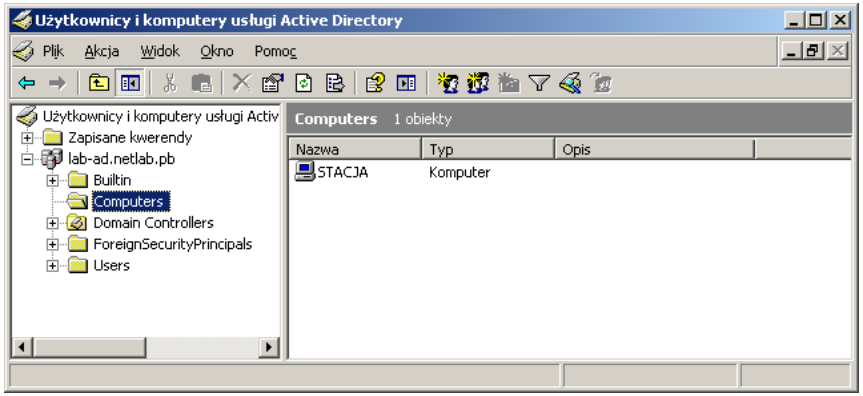
Rys. 17. Poprawne podłączenie komputera do domeny.

Komputer należy przeładować. W tym momencie zmienia się sposób logowania do systemu (następuje rozróżnienie użytkowników lokalnych i domenowych) oraz pojawia się dostęp do zasobów domeny.

Czynności do wykonania:

3. Na komputerze klienckim zmień identyfikacje sieciową, tak aby podłączyć go do domeny o nazwie wykorzystanej podczas konfiguracji serwera. Ustaw statyczny adres IP oraz jako serwer DNS podaj adres serwera DNS obsługującego tę domenę (u nas będzie to ten sam serwer co kontroler domeny). Następnie ustaw wybraną nazwę (np. *stacja)* oraz członkostwo w domenie lab-ad.netlab.pb. Na kontrolerze domeny może być konieczne wyłączenie zapory sieciowej lub skonfigurowanie jej w sposób pozwalający na korzystanie z DNS i innych wymaganych zasobów.

Po przeładowaniu komputerów klienckich możemy sprawdzić ich obecność w domenie. W tym celu na serwerze domeny uruchamiamy z menu Start -> Programy -> Narzędzia Administracyjne ->Użytkownicy i komputery Active Directory. Rozwijając gałąź Komputery (Computers) w lewym fragmencie okna, po prawej stronie powinny pojawić się charakterystyki wszystkich komputerów członkowskich w domenie (rysunek 18).

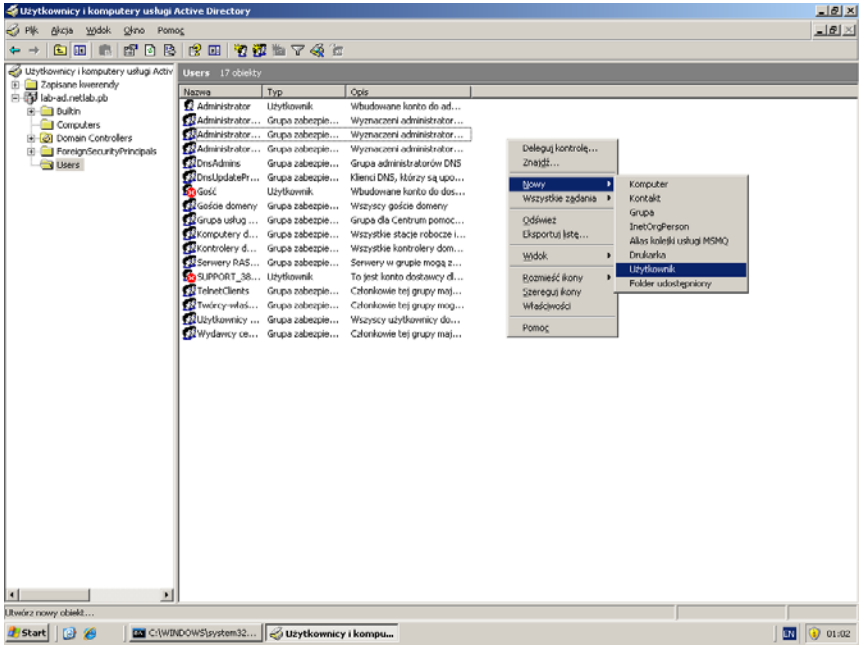


Rys. 18. Komputer(y) w domenie lab-ad.netlab.pb.

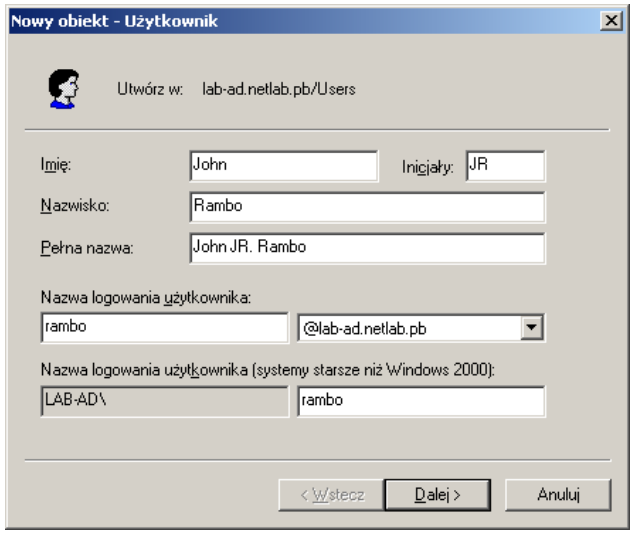
Dodawanie użytkownika domenowego.

Użytkownika domenowego dodajemy na serwerze domeny po podłączeniu się do systemu jako Administrator. Z menu Start wybieramy pozycje Programy -> Narzędzia administracyjne -> Użytkownicy i komputery Active Directory. W lewej części okna aplikacji (rysunek 19) klikamy dwukrotnie lewym przyciskiem myszy na ikonkę naszej domeny. W rozwinięciu pokażą się wszystkie składniki usługi Active Directory. Klikamy lewym przyciskiem myszy na składnik Użytkownicy (Users). W oknie po prawej stronie pojawi się lista użytkowników domenowych. Aby dodać użytkownika klikamy prawym przyciskiem myszy na wolnym polu prawej części okna aplikacji i z menu skrótu wybieramy pozycje Nowy, a następnie Użytkownik (rysunek 19).

W pierwszym oknie opisu użytkownika (rysunek 20) podajemy jego rzeczywiste imię i nazwisko. Założenie użytkownika bez podania imienia i nazwiska jest możliwe, lecz absolutnie nie zalecane. Proponujemy również nazwę w systemie (User logon name). Przykładowy użytkownik będzie mógł się podłączać z każdego komputera postawionego w domenie zast2. Po wypełnieniu wszystkich okienek dialogowych klikamy przycisk Dalej (Next...).

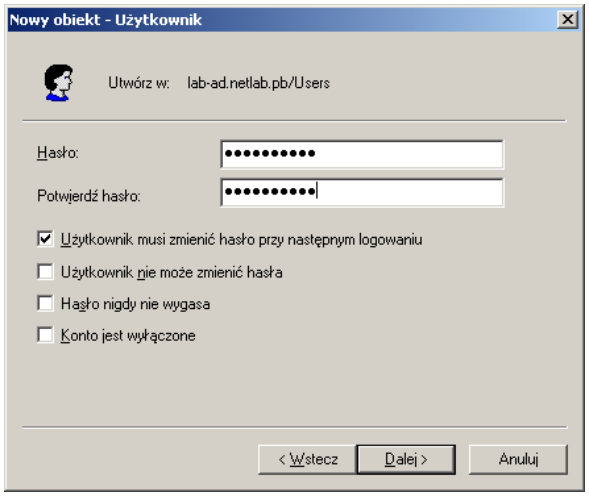


Rys. 19. Dodanie użytkownika domenowego.



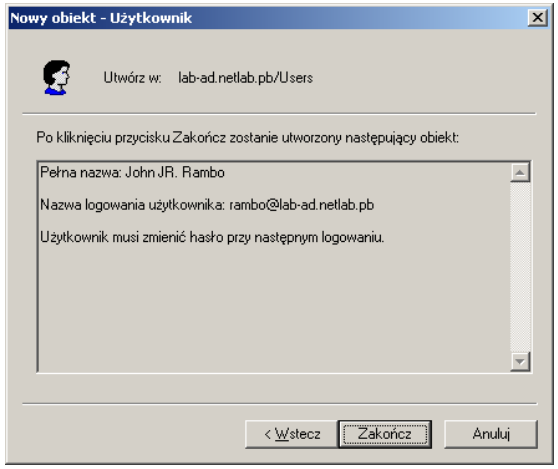
Rys. 20. Podstawowe dane użytkownika.

W kolejnym okienku dialogowym ustalamy pierwsze hasło użytkownika. Nie jest dopuszczalne podanie hasła pustego. Mamy wówczas konto, na które każdy może się zalogować. Hasło powinno składać się z liter dużych i małych (rozróżnialne) i cyfr. Długość 6-8 znaków. Zalecane jest zaznaczenie konieczności zmiany hasła przy kolejnym logowaniu się, jak na rysunku 21 (w celach testowych można pominąć te ograniczenia). Klikamy przycisk *Dalej*.



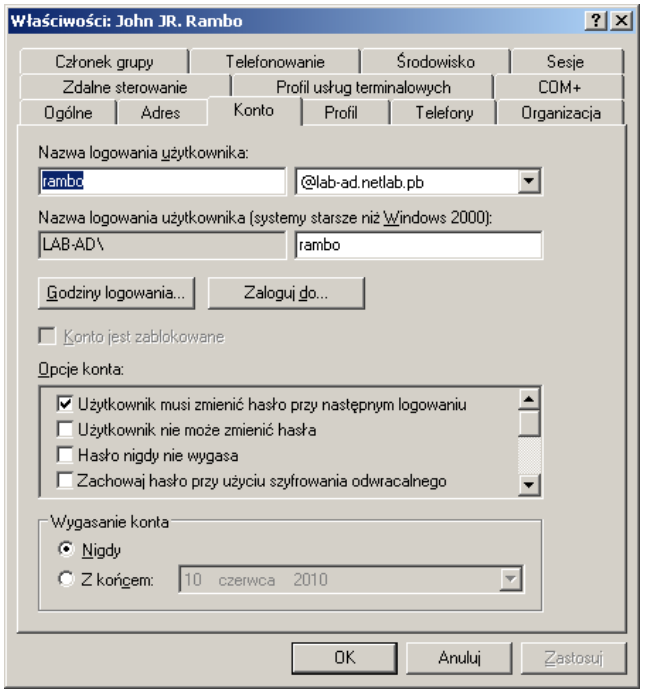
Rys. 21. Ustalenie hasła użytkownika i podstawowych opcji konta i hasła.

Ostatnie okienko zawiera podsumowanie (rysunek 22). Klikamy przycisk *Zakończ*.



Rys. 22. Podsumowanie informacji o nowym użytkowniku w domenie *lab-ad.netlab.pb*.

Od tej pory użytkownik o nazwie w systemie *rambo* może podłączać się korzystając z dowolnego komputera zainstalowanego w domenie *lab-ad.netlab.pb*. Użytkownik ten pojawił się również w okienku aplikacji zarządzania użytkownikami domeny. Jego właściwości są dostępne po dwukrotnym kliknięciu na linie opisu dotyczącą tego użytkownika oknie aplikacji zarządzania użytkownikami domeny. Przykład dostępnych opcji pokazano na rysunku 23.

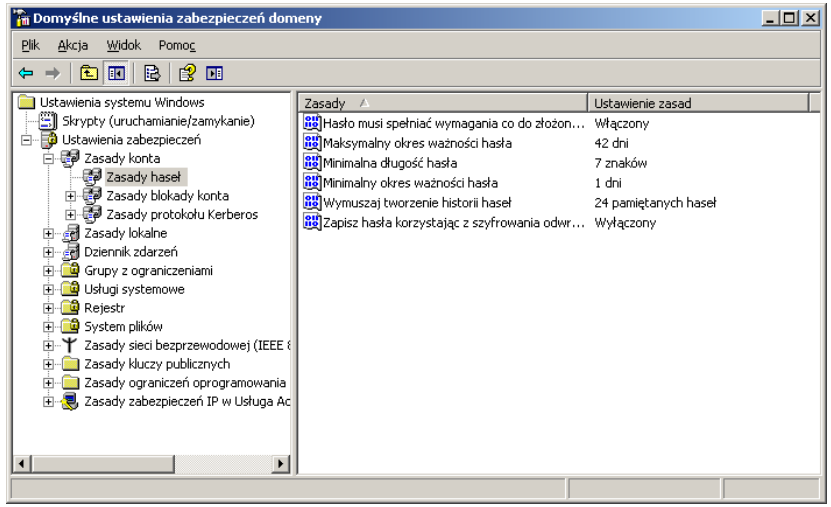


Rys. 23. Właściwości użytkownika w domenie.

Czynności do wykonania:

4. Na komputerze będącym serwerem domeny załóż konta dla dwóch rożnych użytkowników. Sprawdź poprawność operacji logowania próbując podłączyć się z dowolnego komputera jako jeden z nowo założonych użytkowników.

Jednym z aspektów bezpieczeństwa systemu są założenia dotyczące haseł użytkowników. Aplikację Polityk bezpieczeństwa domeny (Domain Security Policy) uruchamiamy z menu Start -> Programy - >Narzędzia Administracyjne -> Zasady zabezpieczeń domeny (rysunek 24).



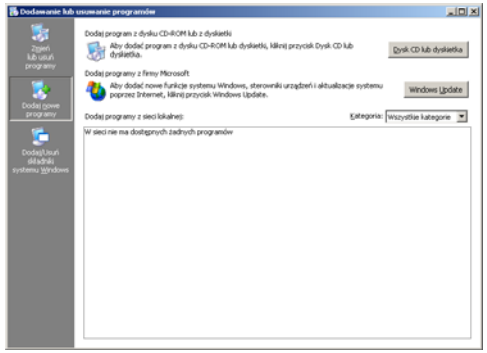
Rys. 24. Założenia polityki bezpieczeństwa w domenie w odniesieniu do haseł użytkowników.

Czynności do wykonania:

5. Sprawdź skuteczność założeń polityki bezpieczeństwa domeny w odniesieniu do haseł użytkowników zmieniając wartości kluczy w prawym oknie aplikacji. Zwróć uwagę na zależności miedzy kluczami.

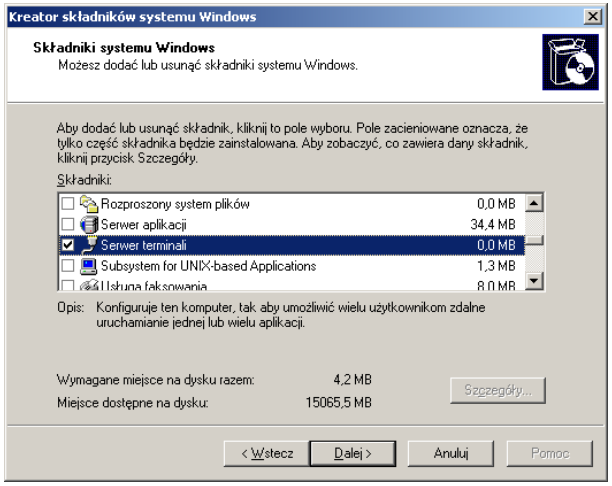
Usługi terminalowe.

Są to usługi typu klient-serwer. Oprogramowanie po stronie serwera jest może być zainstalowane podczas instalacji systemu operacyjnego serwera. Jeżeli opcja ta nie została wybrana, to możliwe jest późniejsze doinstalowanie tego elementu poprzez Start -> Panel sterowania -> Dodaj/Usuń programy -> Dodaj/Usuń składniki systemu Windows (rysunek 25).



Rys. 25. Okienko dialogowe dodawania i usuwania zainstalowanego oprogramowania.

Po wybraniu zakładki Dodaj/Usuń składniki systemu Windows pojawi się okienko z listą komponentów systemu. Zaznaczamy *Serwer terminali*. Wskazane jest uprzednie wyłączenie konfiguracji zwiększonych zabezpieczeń programu Internet Explorer dla użytkowników (jest to także na liście składników systemu Windows). Następnie klikamy przycisk Dalej. Instalacja może wymagać umieszczenia w napędzie płytki CD z instalacją systemu. Po zakończonej instalacji restartujemy system.

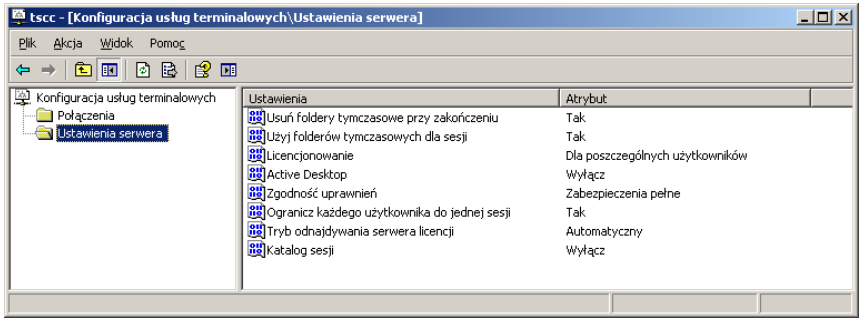


Rys. 26. Instalacja usługi terminalowej.

Czynności do wykonania:

6. Sprawdź, czy w systemie została zainstalowany serwer usług terminalowych. Jeśli nie to zainstaluj go. Wybierz tryb pracy umożliwiający zdalną pracę wszystkim użytkownikom.

Ustawienia Usługi terminalowej znajdują się w aplikacji Konfiguracja usług terminalowych uruchamianej z menu Start -> Programy -> Narzędzia administracyjne ->Konfiguracja usług terminalowych (rysunek 27).



Rys. 27. Ustawienia usługi terminalowej po stronie serwera Windows2003.

Czynności do wykonania:

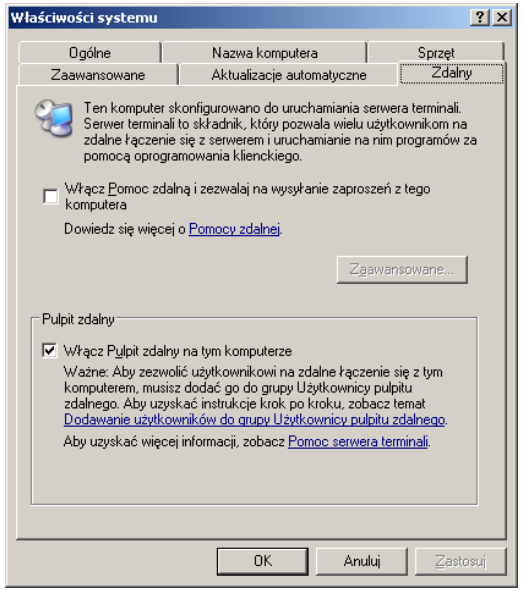
7. Sprawdź, czy ustawienia serwera usługi terminalowej są identyczne jak na rysunku 27. Jeśli występują różnice spróbuj je usunąć.

Oprogramowanie klienta usługi terminalowej

Istnieje tu kilka możliwości. Klient może pracować w systemie Unix. Wówczas z sieci pobieramy kod źródłowy programu **rdesktop**, konfigurujemy go (poleceniem *./configure*), kompilujemy (poleceniem *make*) i program jest gotowy do użycia.

Instalacja klienta w systemie Windows2000 wymaga stworzenia dwóch (lub czterech) dyskietek instalacyjnych. W tym celu uruchamiamy menu Start ->Programy (Programs) -> Narzędzia administracyjne (Administrative Tools)- >Kreator klienta usługi terminalowej (Terminal Services Klient Creator).

W systemie Windows2003 klient usługi terminalowej zostaje zainstalowany podczas instalacji samego systemu. Wystarczy go jedynie uruchomić. Pojawia się jednak konieczność udostępnienia usługi do zdanego wykorzystania oraz zdefiniowania użytkowników, którzy mogą podłączać się do konkretnego hosta, na którym pracuje serwer usługi terminalowej. W tym celu należy wejść do *Właściwości systemu* i wybrać zakładkę *Zdalny* (rysunek 28).



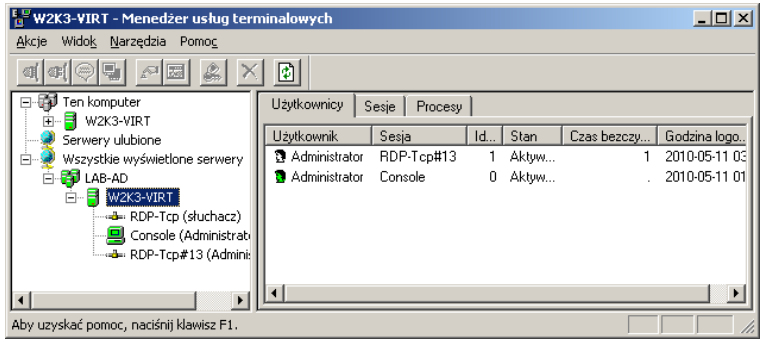
Rys. 28. W zakładce Zdalny (Remote) Właściwości systemu umożliwiamy korzystanie z usługi terminalowej oraz definiujemy uprawnionych użytkowników.

W pierwszym kroku wybieramy opcję *Włącz Pulpit zdalny na tym komputerze* , a następnie definiujemy użytkowników uprawnionych do korzystania z usługi. Po stronie klienta program zdalnego pulpitu można uruchomić wpisując w okienku *Uruchom* **mstsc**.

8. Udostępnij usługę terminalową na kontrolerze domeny. Podłącz się jako użytkownik Administrator do kontrolera domeny z dowolnego serwera korzystając z usługi terminalowej. Sprawdź, czy takie połączenie jest możliwe dla dowolnego użytkownika.

System Windows wyposażony został w narzędzie do monitorowania serwera usług terminalowych. Uruchamiamy menu Start ->Programy (Programs) -> Narzędzia administracyjne (Administrative Tools)- >Zarządca Usługi Terminalowej (Terminal Services Manager) (Rys. 29). Okienko aplikacji podzielone zostało na dwie części. W lewej znajduje się informacja o topologii połączeń, zaś w prawej szczegółowa informacja o wybranym połączeniu. Dostępne jest menu kontekstowe (prawy przycisk myszy) pozwalające zarządzać połączeniem.

9. Uruchom zarządcę serwera usług terminalowych. Określ, ilu użytkowników korzysta z usługi w systemie. Korzystając z menu kontekstowego spróbuj przerwać dowolną sesję.



Rys. 29. Okienko zarządcy serwera usług terminalowych.

Kończenie pracy klienta usługi terminalowej przebiega podobnie jak odłączanie się od systemu z wykorzystaniem konsoli. Pojawia się jednak dodatkowa możliwość nazwana rozłączeniem (Disconnect). Wybranie jej spowoduje, że uruchomione w sesji aplikacje na serwerze nie zostaną zakończone, a po ponownym podłączeniu się do serwera z wykorzystaniem usługi terminalowej zastaniemy pulpit w stanie, w jakim pozostawiliśmy go w momencie odłączania się od systemu.

Literatura

1. S. Reimer, M. Mulcare: Active Directory dla Microsoft Windows Server 2003. Przewodnik techniczny. APN Promise, Warszawa, 2005.
2. S. Gotojuch, E. Nowacka: Microsoft Windows Server 2003: projektowanie i organizacja Active Directory oraz usług zabezpieczeń. APN Promise, Warszawa, 2005.
3. J. Spealman, K. Hudson, M. Kraft, A. Steven: Planowanie, wdrażanie I obsługa infrastruktury Active Direktory Windows Server 2003. Training Kit 70-294. Wydanie II. APN Promise, Warszawa, 2007.

Część 2 - Administrowanie kontami użytkowników w systemie Windows z wykorzystaniem AD

Konto użytkownika daje użytkownikowi możliwość podłączenia się do domeny w celu uzyskania dostępu do zasobów sieciowych lub zalogowania się do komputera w celu uzyskania dostępu do jego zasobów lokalnych. System Windows 2003 obsługuje dwa typy kont użytkownika: lokalne i domenowe. Korzystając z konta użytkownika domeny użytkownik może się zalogować do domeny i korzystać z jej zasobów (dyski, drukarki) zgodnie z uzyskanymi uprawnieniami. Konto lokalne pozwala na wykorzystywanie jedynie zasobów lokalnych zgodnie z lokalnymi zasadami zabezpieczeń.

Profil użytkownika jest zbiorem folderów i danych przechowujących informację o aktualnych ustawieniach systemu, pulpitu i aplikacji jak również dane prywatne. Zawiera on również informację o wszystkich połączeniach sieciowych, które są ustanawiane w momencie logowania się użytkownika do komputera, ustawienia menu Start oraz mapowania dysków serwerów. Profile użytkownika zapewniają stałą konfigurację środowiska pulpitu, jakie było podczas ostatniej sesji z komputerem. Profil użytkownika jest tworzony podczas jego pierwszego podłączania się do systemu i przechowywany w tym systemie.

Podstawowe zasady działania profili użytkownika w Windows 2003 są następujące:

- Podczas podłączania się do komputera pracującego pod kontrolą systemu Windows 2003 użytkownik ustala indywidualne ustawienia środowiska, pulpitu i połączeń całkowicie niezależne od pozostałych użytkowników.
- Przy pierwszym podłączaniu się do komputera klienta, system kopiuje lokalny profil (zawartość katalogu Default User) do katalogu *%systemdrive%\Documents and Settings\<nazwa_logowania_użytkownika>* (*nazwa_logowania_użytkownika* oznacza nazwę konta użytkownika w systemie.
- Jeżeli komputer, do którego logują się użytkownicy, został uaktualniony z Windows 95 lub Windows 98 z włączonymi profilami lub Windows NT do Windows 2000 Professional folder profili w *%systemroot%\profiles* i nie jest tworzony w folderze *Documents and Settings*.
- Folder profilu umożliwia przechowywanie wielu informacji konfiguracyjnych (np. **Moje dokumenty**)
- Najprostszym sposobem modyfikowania profilu użytkownika jest zmiana ustawień osobistych, które są automatycznie uaktualniane przez kopiowanie profilu podczas odłączania użytkownika od systemu.

Mobilne profile użytkowników (***Roaming User Profile*** **– RUP**) zostały wprowadzone dla wsparcia użytkowników wykorzystujących wiele komputerów w domenie. Profil Mobilny jest ustawiony na serwerze sieci, dzięki czemu może być dostępny na każdym komputerze domeny do którego użytkownik się zaloguje. Podczas logowania się system Windows 2003 kopiuje mobilny profil z serwera. Dzięki temu użytkownik otrzymuje zawsze swoje indywidualne ustawienia, niezależnie od tego na którym komputerze domeny się zalogował. Przeciwieństwo stanowi **profil lokalny**, który obowiązuje jedynie na jednym komputerze. W trakcie

procesu podłączania, system Windows 2003 stosuje ustawienia zapisane w profilu mobilnym na bieżącym komputerze. Przy pierwszym logowaniu się do tego komputera z serwera kopiowane są wszystkie pliki konfiguracyjne profilu oraz związane z nimi dokumenty. Podczas kolejnych logowań, system porównuje pliki profilu użytkownika przechowywane lokalnie z zawartością profilu mobilnego i kopiuje jedynie te pliki, które zostały zmienione lub nowo stworzone w profilu mobilnym (co prowadzi do skrócenia czasu logowania). Podczas odłączania się od systemu, system kopiuje jedynie zmiany wprowadzone w ustawieniach profilu, które staną się obowiązujące podczas kolejnego podłączania się użytkownika na dowolnym komputerze domeny.

Możliwe jest również dostosowywanie i przydzielanie wstępnie skonfigurowanych mobilnych profili użytkownika, przydzielonych do kont wszystkich użytkowników, jak również zapisywanie profili użytkowników jako **tylko do odczytu**. Dostosowany mobilny profil użytkownika można utworzyć konfigurując środowisko dla określonego użytkownika, a następnie kopiując dostosowany profil do lokalizacji mobilnego profilu danego użytkownika.

Profil obowiązkowy jest mobilnym profilem tylko do odczytu. W momencie odłączania się od systemu użytkownik nie zapisuje w nim żadnych zmian (dokonanych w trakcie sesji). Przy następnym logowaniu profil jest taki sam jak przy logowaniu poprzednim.

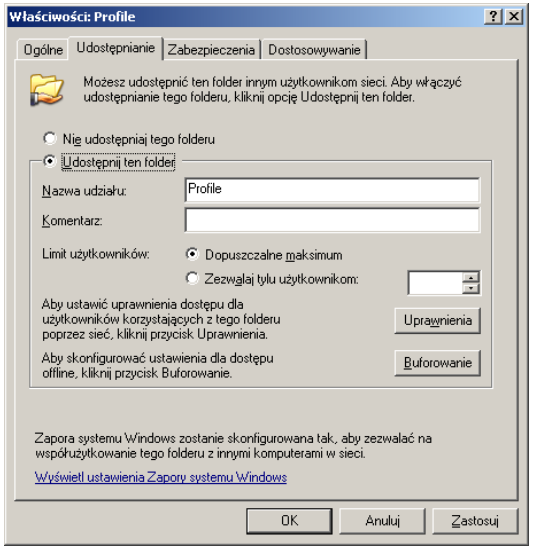
Plik ukryty o nazwie **Ntuser.dat** zawiera sekcję ustawień systemowych odnoszącą się do indywidualnego konta użytkownika i zawierającą ustawienia jego środowiska. Jest to plik, który po zmianie nazwy na **Ntuser.man** staje się plikiem tylko do odczytu.

0a. Podłącz się do dowolnego komputera jako użytkownik Administrator. Zgodnie z instrukcjami zawartymi w części 1 przekonwertuj go do kontrolera domeny. Załóż użytkowników domenowych o nazwach test1 oraz test2.

0b. Podłącz się jako użytkownik Administrator do pozostałych na stanowisku komputerów i uczyń je komputerami członkowskimi domeny. Na dowolnym komputerze członkowskim sprawdź, czy zdefiniowani w poprzednim kroku użytkownicy test1 i test2 mogą podłączać się do komputera jako użytkownicy domenowi.

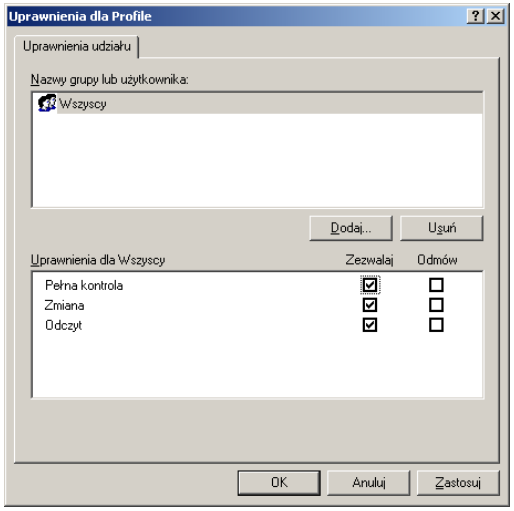
1. Podłącz się do kontrolera domeny jako użytkownik Administrator.

Profile użytkowników zazwyczaj przechowuje się w udostępnionym folderze na serwerze członkowskim (nie kontrolerze domeny). Jest to wynik dążenia do zrównoważenia obciążenia serwerów domeny. W naszym przypadku, ze względu na brak w domenie serwerów członkowskich profile przechowywać będziemy na kontrolerze domeny. W tym celu na dysku C: kontrolera domeny tworzymy folder **Profile**, udostępniamy go zmieniając prawa dostępu na pełną kontrolę dla wszystkich użytkowników (Rys. 2.1).



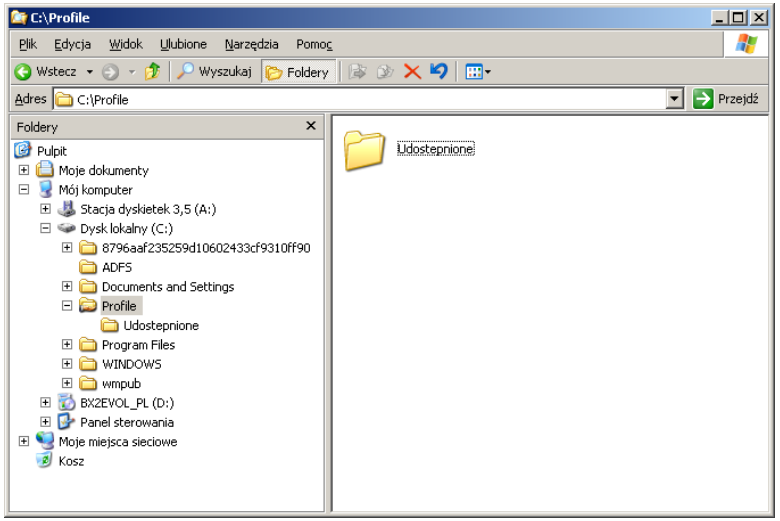
Rys. 2.1. Udostępnienie folderu **Profile** jako zasobu sieciowego pod nazwą **Profile**.

Klikamy przycisk *Uprawnienia* i ustalamy prawa dostępu na „Pełną kontrolę" dla grupy „Wszyscy" jak na rysunku 2.2. Te prawa dostępu są sprawdzane jako pierwsze przy każdym odwołaniu się do zasobu sieciowego i jeśli nie zostaną ustawione, to prawa szczegółowe nie będą sprawdzane – od razu pojawi się komunikat o braku możliwości tworzenia i modyfikowania plików w tym katalogu.



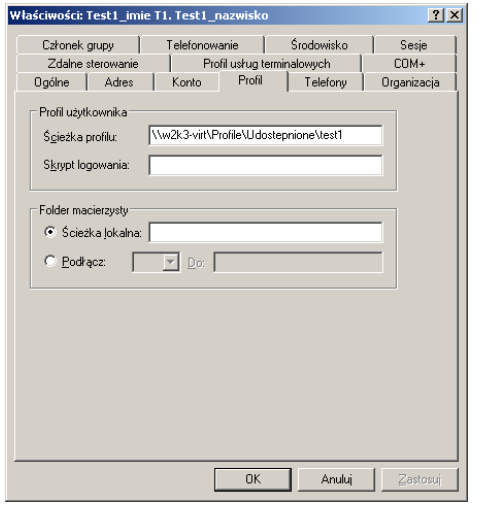
Rys. 2.2. Ustawienie praw dostępu do zasobu sieciowego, na którym przechowywane będą profile migrujące użytkowników.

Następnie tworzymy w nim podkatalog **Udostepnione** dla profili użytkowników (Rys. 2.3).



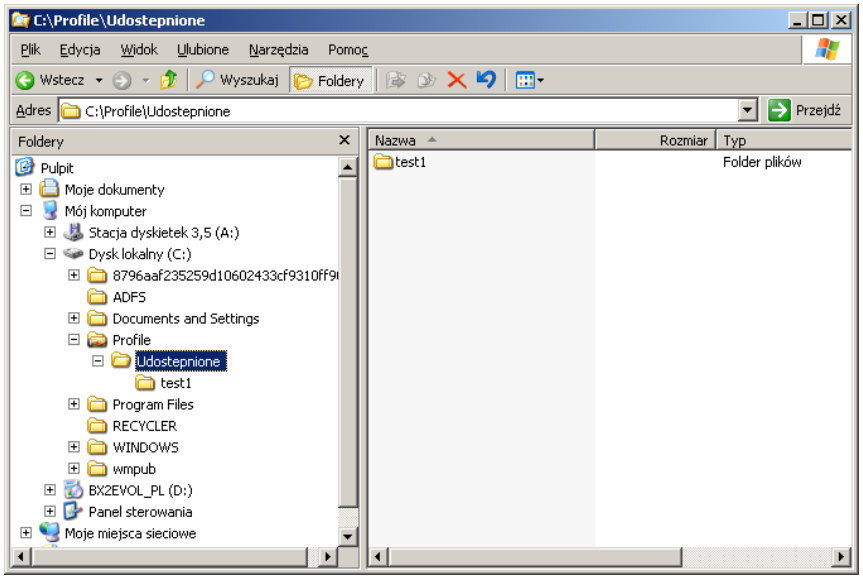
Rys. 2.3. Podkatalog udostępniony w folderze Profile dysku C: serwera. W nim pojawią się profile użytkowników.

Profile użytkownika mogą być tworzone na dwa sposoby. Pierwszy polega na podaniu w charakterystyce użytkownika ścieżki dostępu do zasobu (*\\komputer\udzial*) na którym przygotowane zostało miejsce na profile użytkowników (Rys. 2.4).



Rys. 2.4. Zakładka profile we właściwościach użytkownika.

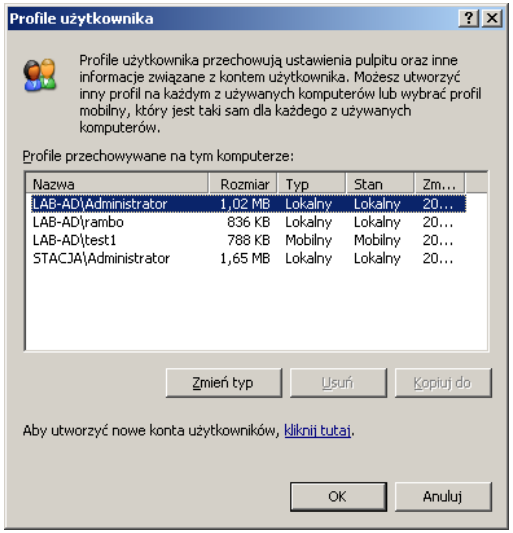
Po zatwierdzeniu klawiszem Ok., użytkownik **test1** otrzymuje możliwość przechowywania swojego profilu na serwerze o nazwie **w2k3-virt** w katalogu **Profile\Udostepnione\test1**. Będzie on wykorzystywany na wszystkich komputerach domeny. Po pierwszym podłączeniu w katalogu przechowującym profil przykładowego użytkownika będzie wyglądał jak na Rys. 2.5.



Rys. 2.5. Zawartość folderu przechowującego profil użytkownika.

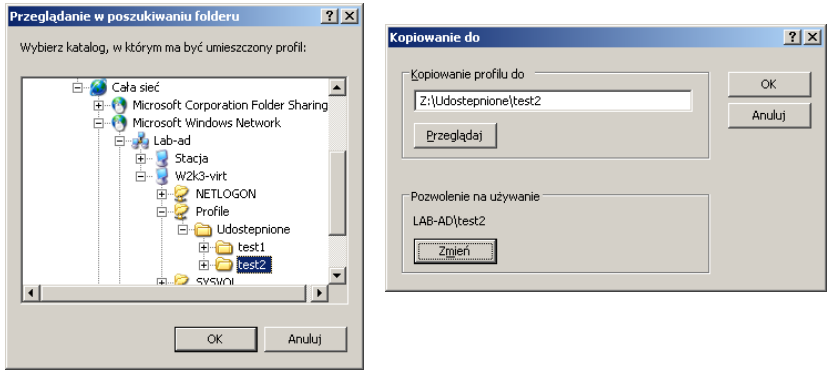
2. Na serwerze domeny uzupełnij charakterystykę użytkownika test1 podając ścieżkę dostępu do odpowiedniego folderu w przygotowanym folderze profile. Podłącz się do dowolnego komputera członkowskiego (nie będącego kontrolerem domeny) jako użytkownik test1. Dokonaj zmiany tapety oraz palety kolorów. Umieść na pulpicie ikonkę skrótu do programu notatnika oraz linii komend (cmd). Odłącz się od systemu. Sprawdź, czy po ponownym podłączeniu wygląd pulpitu jest taki sam. Odłącz się od systemu.

Drugi sposób polega na skopiowaniu profilu „wzorcowego" do katalogu profilu innego użytkownika. W tym przypadku w folderze przeznaczonym dla przechowywania profili należy stworzyć podkatalog o nazwie jak nazwa użytkownika (np. **test2**)i uzupełnić pole *ścieżka profilu* w zakładce *Profile* okienka *właściwości użytkownika*. Następnie podłączamy się do dowolnego komputera domeny jako użytkownik Administrator. Dokonujemy mapowania udostępnionego zasobu Profile na dysk Z. Prawym przyciskiem myszy klikamy na ikonkę *Mój komputer* i z zakładki *Zaawansowane* okienka *Właściwości systemu* wybieramy *Ustawienia* w grupie *Profile użytkownika* (Rys. 2.6).



Rys. 2.6 Zakładka *Profile użytkownika* z *Właściwości systemu/Zaawansowane*.

Wskazujemy profil wzorcowy (np. test1) i wybieramy przycisk *Kopiuj do*, a następnie wskazujemy poprzez Otoczenie sieciowe katalog przygotowany na serwerze dla przechowywania profilu użytkownika **test2** (Rys. 2.7).



Rys. 2.7. Wskazanie folderu do przechowywania profilu użytkownika.

Zaznaczamy utworzony katalog i klikamy przycisk Ok. Przed skopiowaniem profilu ustalamy pozwolenie na jego używanie przez użytkownika **test2**. Profil zostaje skopiowany do wskazanego katalogu i udostępniony użytkownikowi o takiej nazwie w systemie jak folder.

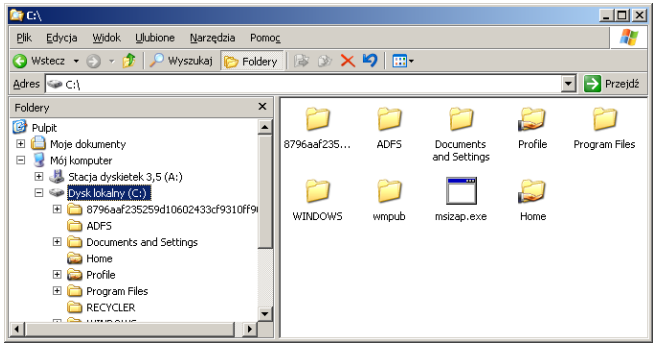
3. Utwórz na pulpicie użytkownika test1 kilka skrótów (np. do notatnika i innych programów). Podłącz się do dowolnego komputera w domenie (nie do kontrolera domeny) jako użytkownik Administrator. Zapisz do katalogu z profilem użytkownika test2 profil użytkownika test1. Odłącz się od systemu. Podłącz się jako użytkownik test2 i sprawdź, czy jego środowisko jest identyczne ze środowiskiem użytkownika test1 (ikony skrótów na pulpicie i inne ustawienia).

Tworzenie folderów macierzystych

Folder macierzysty jest dodatkowym folderem, który może być dostarczany użytkownikom do przechowywania własnych plików lub jako domyślny folder do zapisywania dokumentów. Folder ten może zostać zdefiniowany na lokalnym komputerze lub na serwerze i udostępniony poprzez sieć. Nie jest on częścią profilu więc nie wpływa na obciążenie sieci podczas logowania. Umieszczenie folderów osobistych na serwerze pozwala na 1. szybki dostęp użytkownikom do ich informacji z dowolnego komputera sieci, 2. scentralizowanie wykonywania kopii zapasowych i administracji, 3. ewentualny dostęp do folderów osobistych z wykorzystaniem komputerów pracujących pod kontrolą praktycznie dowolnego systemu operacyjnego rodziny Windows.

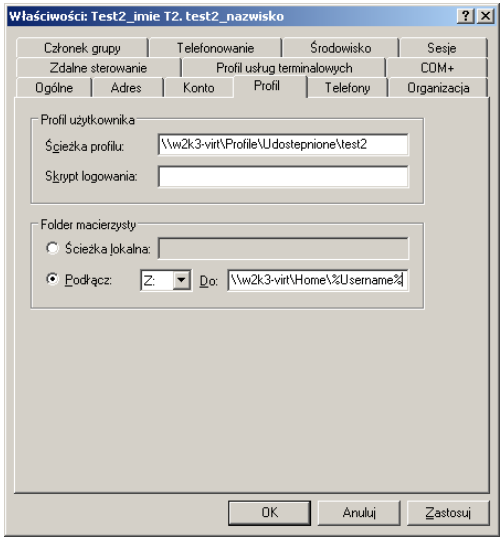
Istotnym jest, aby foldery macierzyste umieszczać w wolumenie systemu plików NTFS. Umożliwi to zastosowanie uprawnień NTFS do zabezpieczenia plików użytkowników oraz wprowadzenie systemu *quota* do kontroli ilości zajmowanego miejsca.

Podobnie jak w przypadku profili należy na serwerze przygotować odpowiedni folder i udostępnić go. Przez analogię do innych systemów folder ten może nazywać się **Home** (Rys. 2.8).



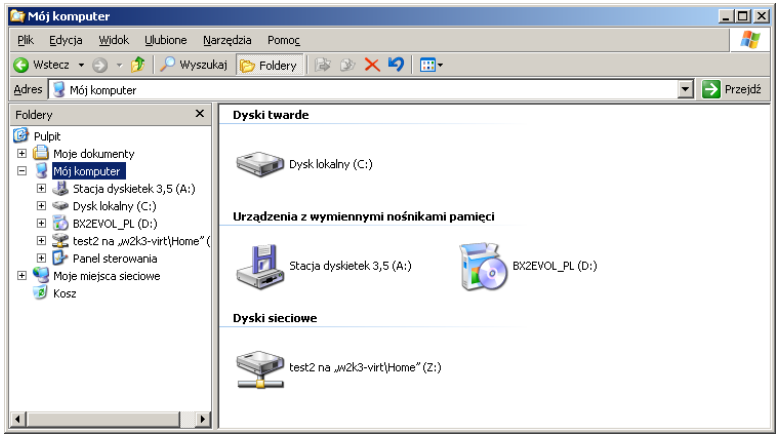
Rys. 2.8. Foldery profili i katalogów osobistych powinny znajdować się „koło" siebie – ułatwia to administrację.

Kolejnym krokiem jest uzupełnienie charakterystyki użytkownika w znanej zakładce Profile okienka *Właściwości użytkownika* (Rys. 2.9). W sekcji *Folder macierzysty* zaznaczamy przycisk *Podłącz*, z rozwijanej listy wybieramy literę dla dysku i wpisujemy ścieżkę dostępu do utworzonego folderu osobistego.



Rys. 2.9. Katalog osobisty dla użytkownika test2 będzie widoczny na komputerach domeny jako dysk Z.

Po podłączeniu się do dowolnego komputera domeny, użytkownik test2 będzie widział katalog osobisty jako dysk Z (Rys. 2.10).

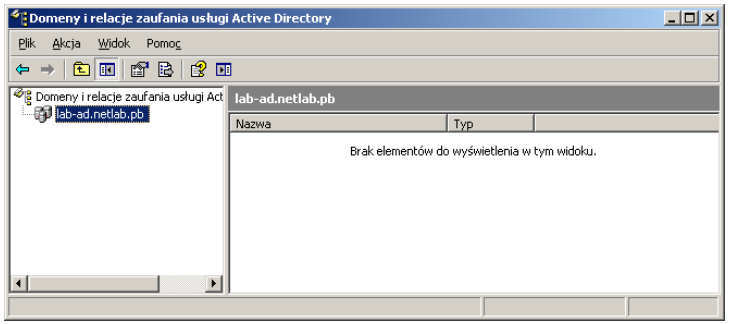


Rys. 2.10 Po podłączeniu się do komputera użytkownik widzi swój folder osobisty.

4. Będąc podłączonym do kontrolera domeny jako użytkownik Administrator, utwórz na dysku C folder Home i udostępnij go. Uzupełnij charakterystykę użytkownika test1 podając ścieżkę dostępu do folderu osobistego. Podłącz się do dowolnego innego komputera domeny jako użytkownik test1 i sprawdź, czy posiada on dostęp do folderu osobistego.

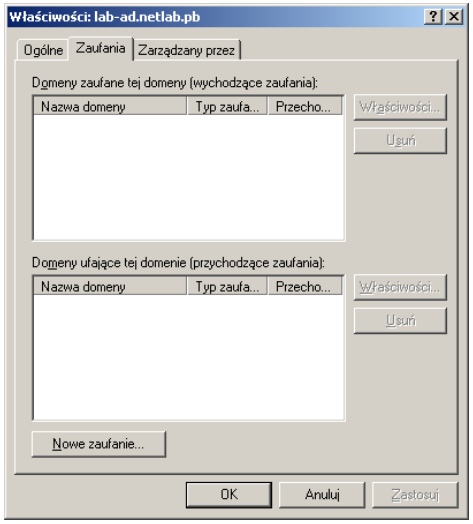
Zaufanie między domenami

Relacja zaufania między domenami pozwalają na udostępnianie zasobów jednej domeny użytkownikom zdefiniowanym w innej domenie. Relacje zaufania są w systemie Windows 2003 jednokierunkowe, co oznacza, że jeśli ufamy innej domenie to nie oznacza to że ona ufa nam. Tak więc każda relacja zaufania musi zostać zdefiniowana indywidualnie. W tym celu sięgamy do Menu Start -> Programy -> Narzędzia Administracyjne -> Domeny i zaufanie usługi Active Directory. Zaznaczamy interesującą nas domenę i klikamy prawym przyciskiem myszy. Pojawi się menu wyskakujące (Rys. 2.11).



Rys. 2.11 Przystawka Domeny i zaufanie usługi Active Directory.

Z menu wybieramy pozycję *Właściwości* (Rys. 2.12), a z okna zakładkę *Zaufania*.



Rys. 2.12 Zakładka *Zaufania* z właściwości domeny.

Okno dzieli się na dwie części. W górnej podajemy nazwy domen, którym ufamy. Użytkownicy z tych domen będą mogli korzystać z zasobów naszej domeny. W okienku dolnym nazwy tych domen, które zaufały naszej domenie i udostępniły nam swoje zasoby. Przy podawaniu nazw domen posługujemy się nazwami krótkimi (NetBIOS), a jeśli zaufanie ma dotyczyć lasów domen wymagane jest podanie pełnej nazwy DNS.

Utworzenia relacji zaufania możemy dokonać przy pomocy odpowiedniego kreatora, który uruchamiamy po naciśnięciu przycisku New Trust (Nowa relacja zaufania). Oprócz podania nazwy domeny, wymagane jest również podanie hasła. Zaufanie należy zdefiniować po obu stronach relacji – po jednej domenę której ufamy po drugiej domenę która udzieliła nam zaufania. W obu przypadkach należy podać dokładnie to samo hasło zabezpieczające relację. Uwaga: przed tworzeniem relacji zaufania zaleca się sprawdzenie poprawności skonfigurowania DNS poprzez np. wykonanie z linii komend komendy ping z podaniem pełnego adresu symbolicznego kontrolera domeny, z którą chcemy nawiązać relację zaufania. Istotny jest również wybór rodzaju relacji zaufania zależnie od trybu pracy domeny, z którą relacja jest tworzona.

5. Utwórz jednokierunkową relację zaufania między dwoma domenami. Sprawdź, czy faktycznie możliwe jest korzystanie z zasobów domeny przez użytkowników innej domeny, której udzielono zaufania.

Sprawozdanie

W sprawozdaniu należy przedstawić wykonaną konfigurację oraz zamieścić opis przeprowadzonych prób mających na celu potwierdzenie zgodności działania utworzonego systemu z wstępnymi założeniami.

Wymagania BHP

Zgodnie z podanymi na pierwszych zajęciach i potwierdzonymi przez studentów zasadami obowiązującymi w pomieszczeniu, w którym odbywają się ćwiczenia. Stosowny regulamin BHP jest też wywieszony w pomieszczeniu laboratorium.

Literatura

1. S. Reimer, M. Mulcare: Active Directory dla Microsoft Windows Server 2003. Przewodnik techniczny. APN Promise, Warszawa, 2005.
2. S. Gotojuch, E. Nowacka: Microsoft Windows Server 2003: projektowanie i organizacja Active Directory oraz usług zabezpieczeń. APN Promise, 2005.
3. J. Spealman, K. Hudson, M. Kraft, A. Steven: Planowanie, wdrażanie I obsługa infrastruktury Active Direktory Windows Server 2003. Training Kit 70-294. Wydanie II. APN Promise, Warszawa, 2007.
4. Dokumentacja techniczna *Microsoft* do systemu Windows Server 2003 (dostępna w laboratorium na CD-ROM oraz w witrynie http://www.microsoft.com/poland/windowsserver2003)