Domena Active Directory w Windows Server 2003

Drzewa
Drzewa — nazywane niekiedy drzewami domen — są kolekcjami domen systemów Windows Server 2000 i Windows Server 2003/2008 tworzącymi ciągły obszar nazw. **Drzewo domeny powstaje w momencie utworzenia domeny podrzędnej. Drzewo domen jest przypisane danej domenie katalogu głównego**.

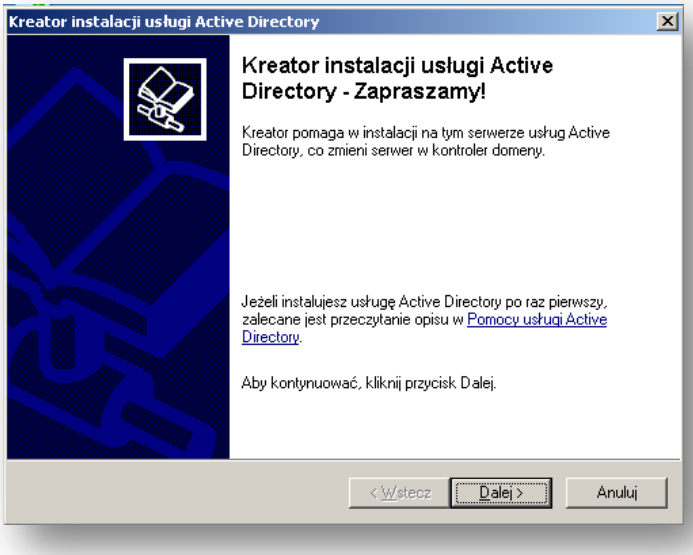
Lasy (Forests)
W niektórych organizacjach może istnieć wiele domen katalogu głównego, na przykład **domena1.com** i **domena2.com**. W takich wypadkach wiele drzew domen tworzy nieciągły obszar nazw nazywany lasem.

Jednostki organizacyjne (OU)
Obiekty trzymane wewnątrz domen mogą być pogrupowane w kontenery zwane Jednostkami organizacyjnymi (ang. Organizational Units - OUs). OU tworzą w domenie hierarchię, ułatwiają zarządzanie i tworzą tzw. pozorną strukturę firmy w rozumieniu geograficznym lub organizacyjnym. OU może zawierać inne OU, tak więc domeny możemy traktować jako kontenery dla OU. Firma Microsoft zaleca stosowanie jak najmniejszych domen w **Active Directory** i stosowanie OU do tworzenia struktur i implementacji zasad (*ang. policies*) oraz administracji. Z reguły to właśnie na poziomie OU stosuje się zasady grup (*ang. group policies*), które same w sobie są obiektami **Active Directory** zwanymi Group Policy Objects (GPOs). Zasady grup mogą być również stosowane na poziomie domen lub miejsc (*ang. Site*).

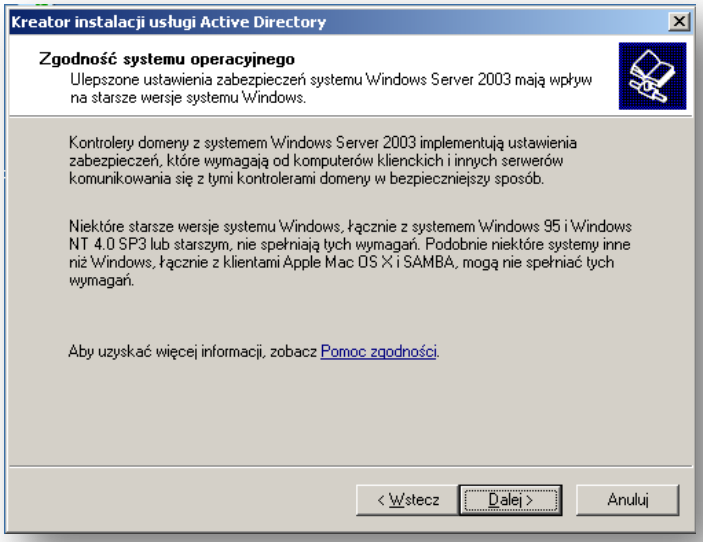
Instalacja kontrolera domeny

Dodanie nowej roli

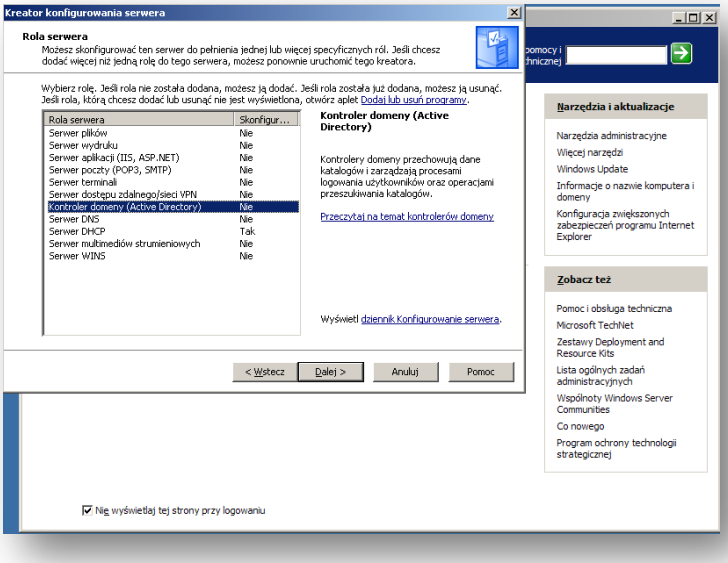
W celu zainstalowania usługi **Active Directory** na komputerze należy uruchomić okno *Zarządzanie tym serwerem*. W oknie tym należy wybrać opcję *Dodaj lub usuń rolę*, która uruchomi kreator konfigurowania serwera (można go także uruchomić poleceniem *dcpromo.exe* z linii poleceń).



Kolejne okno to informacja o możliwych problemach ze zgodnością kontrolera domeny Windows Server 2003 z starszymi wersjami systemów Windows:



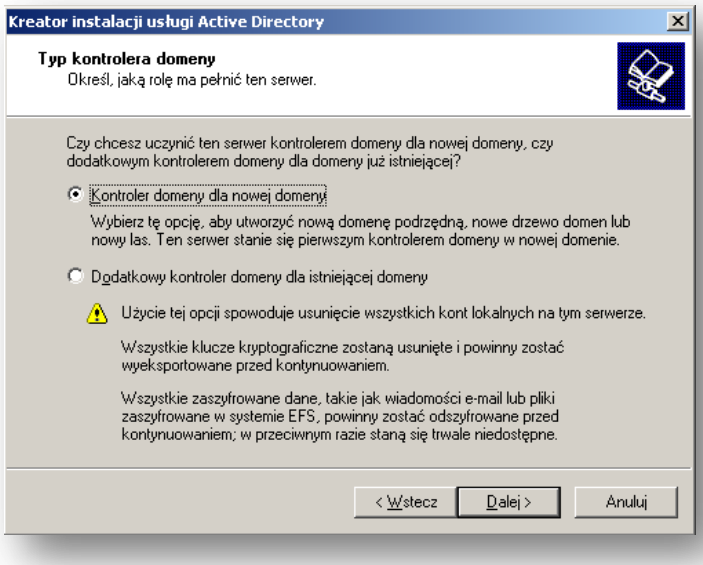
Drugim alternatywnym sposobem wywołania procedury instalacji kontrolera domeny wywołanie panelu Zarządzanie tym serwerem. Tam uruchamiamy kreator Dodaj lub Usuń Rolę. W kreatorze tym należy zaznaczyć rolę jaką ma pełnić nasz serwer – w tym ćwiczeniu wybieramy: *Kontroler domeny (Active Directory)*.



Po wykonaniu pierwszych kroków instalacji usługi Active Directory (obydwoma metodami) uruchomiony zostanie *Kreator instalacji usługi Active Directory*. W kolejnych oknach kreatora należy wybrać rodzaj kontrolera domeny będziemy instalować. Dostępne są dwie opcje:

- Kontroler domeny dla nowej domeny;
- Dodatkowy kontroler domeny dla istniejącej domeny;

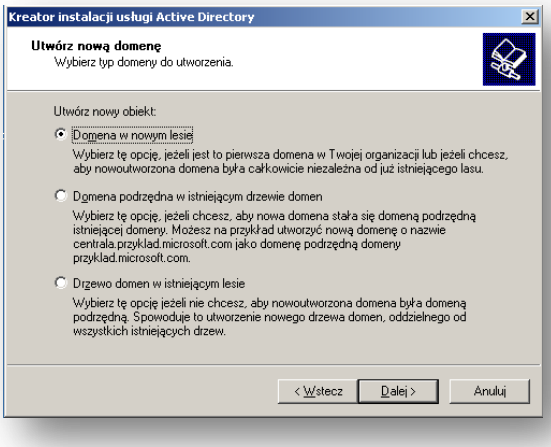
W celu utworzenia nowej domeny należy wybrać pierwsza opcję.



W kolejnym etapie musimy określić, jaką rolę będzie pełniła nowa domena. Mamy tutaj do wyboru trzy opcje:

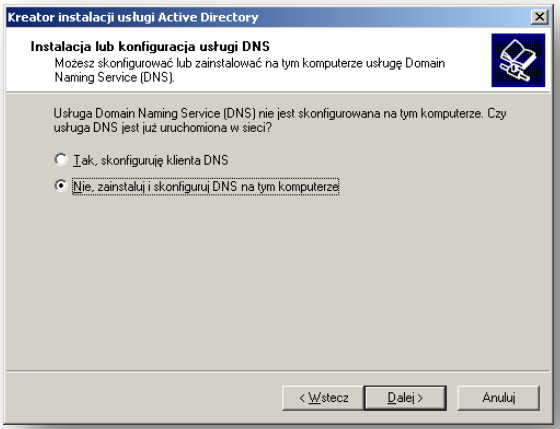
- Domena w nowym lesie - wybierając tę opcję, zakładamy nową domenę niezależną od istniejącego lasu;
- Domena podrzędna w istniejącym drzewie domen - wybierając tę opcję, zakładamy domenę, która będzie domeną podrzędną istniejącej domeny;

- Drzewo domen w istniejącym lesie - tę opcję wybieramy, jeśli nie chcemy, aby nowoutworzona domena była domeną podrzędną. W ten sposób zostanie utworzone nowe drzewo domen, oddzielne od wszystkich istniejących drzew;

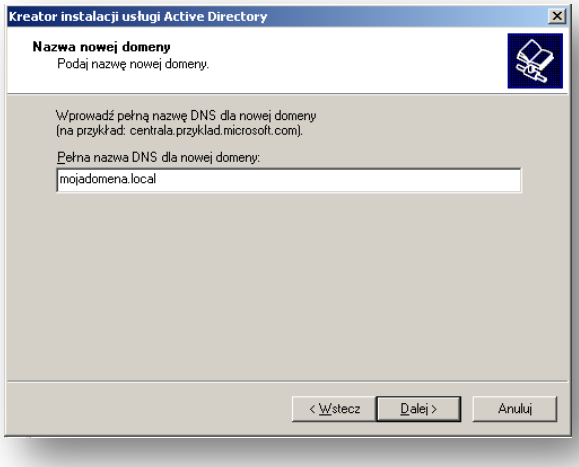


W najprostszym przypadku (np. przy tworzeniu domeny dla małej firmy) wybieramy pierwszą opcję. W przypadku zdecydowania się na jedną z dwóch pozostałych opcji, w kolejnych krokach kreatora należy podać nazwę użytkownika posiadającego uprawnienia administracyjne w domenie oraz miejsce w drzewie, gdzie ma zostać dołączona nowa domena.

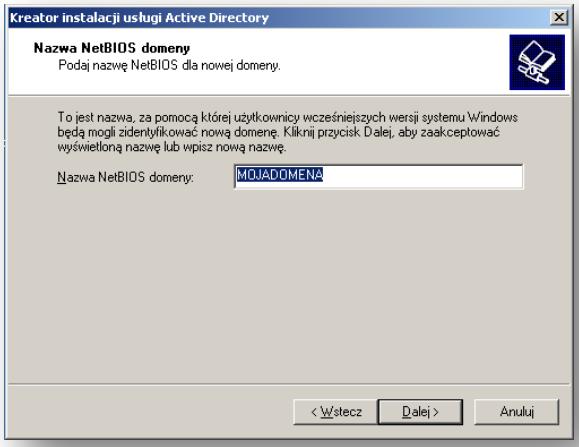
W przypadku systemy domen niezbędna jest albo posiadanie dostępu do funkcjonującego serwera domen DNS (*ang. Domain Names Services*) albo konieczność zainstalowanie takiej usługi w tworzonej domenie. Stąd kolejnym krokiem instalacji jest konfiguracja serwera DNS. Warto tutaj skorzystać z automatycznej konfiguracji usługi DNA dla Active Directory, która uzupełni odpowiednie wpisy i skonfiguruje serwer DNS.



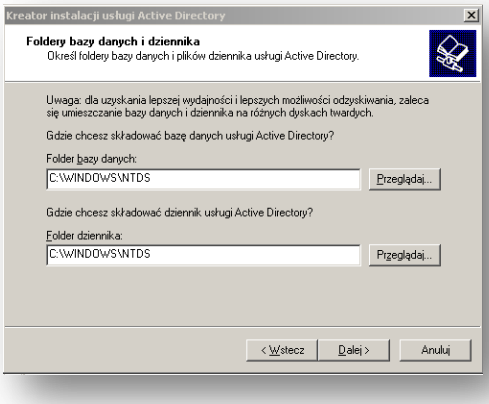
Następnym etapem instalacji kontrolera domeny jest podanie nazwy naszej domeny. W tym miejscu możemy podać albo pełną nazwę domeny w Internecie (np. *firma.com.pl*) albo nazwę lokalną. W przypadku nazwy lokalnej, należy do nazwy domeny dodać przyrostek *local* (np. *mojadomena.local*). Nazwa nie musi składać się tylko z liter, możemy również umieścić w niej kropki i cyfry. Warto również uwzględnić w nazwie domeny jej lokalizację lub zadanie.

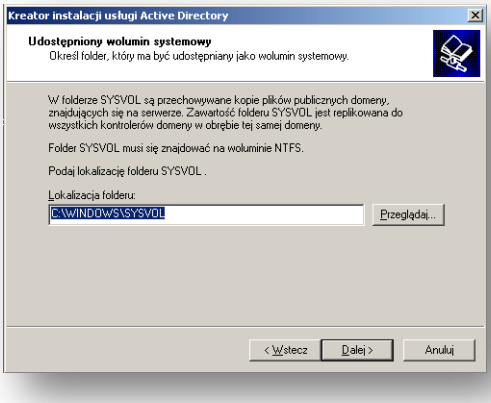


W następnym oknie kreatora należy podać nazwę NetBIOS dla tworzonej domeny, dzięki czemu użytkownicy pracujący nadal na komputerach wyposażonych w starsze wersje systemu Windows (np. Windows 95/98) będą mogli zidentyfikować i komunikować się z tworzoną domeną.

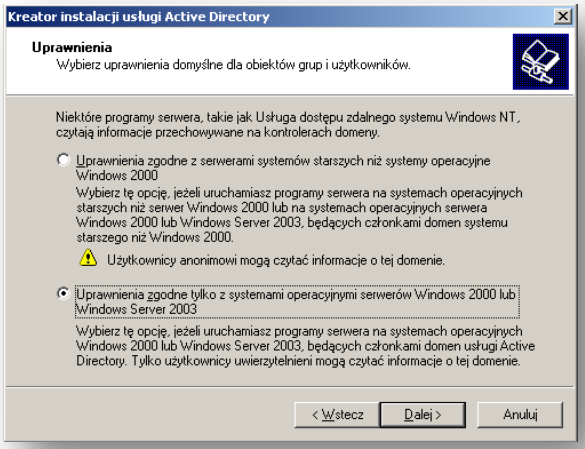


W kolejnych dwóch oknach kreatora należy podać lokalizację dla plików bazy danych i dziennika Active Directory oraz woluminu systemowego. W celu zwiększenia wydajności serwera, zaleca się utworzenie folderu dziennika oraz bazy danych na dwóch różnych dyskach, natomiast folder woluminu musi znajdować się na partycji z systemem plików NTFS. (W naszym ćwiczeniowym przypadku wszystkie foldery pozostaną na jednym dysku).

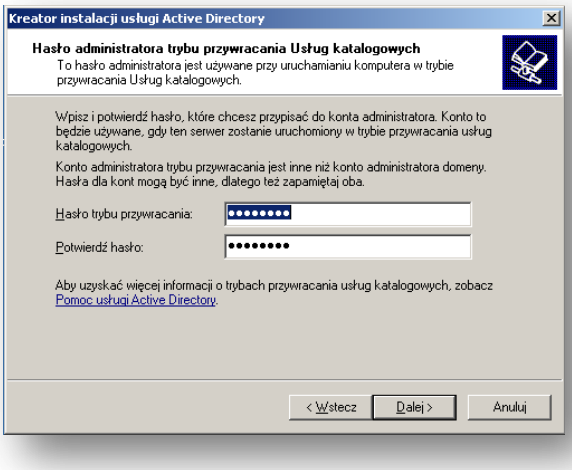




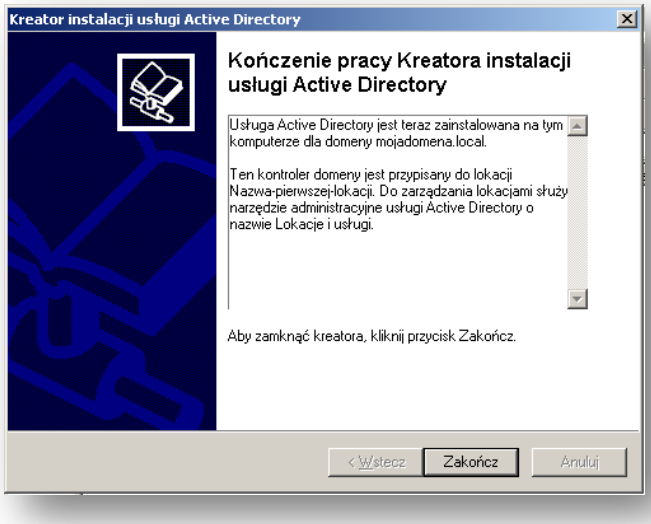
W kolejnym kroku należy podać w jakim trybie autoryzacji będzie pracował serwer. Ponieważ w obrębie laboratorium nie występują starsze systemy zalecaną opcją jest *Uprawnienia zgodne tylko z systemami operacyjnymi serwerów Windows 2000 lub Windows Server 2003:*



W ostatnim etapie instalacji usługi Active Directory należy zdefiniować hasło do *Trybu odzyskiwania*.



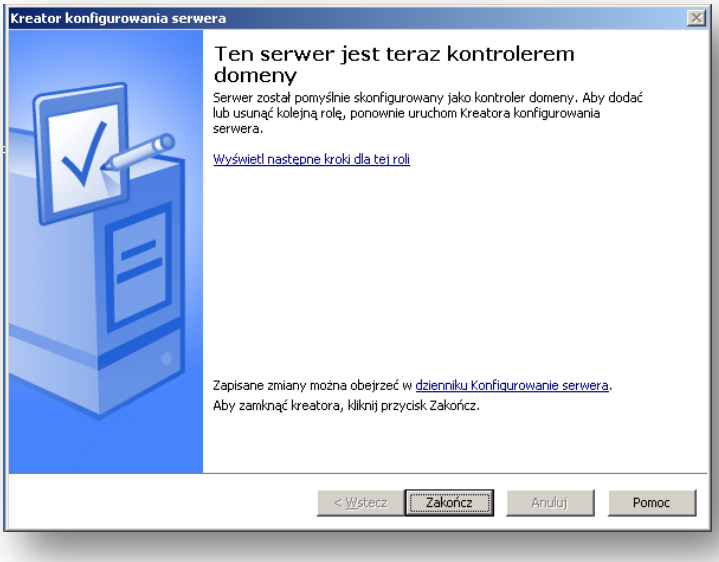
Należy przy tym pamiętać, że hasło to nie dotyczy konta *Administrator* dla naszej domeny, natomiast może być przydatne, gdybyśmy mieli problemy z zalogowaniem do naszej domeny. Hasło należy wpisać dwukrotnie i kliknąć przycisk *Dalej* dwukrotnie. W tym momencie zaczyna się właściwa instalacja usługi. Może to zająć kilka minut. Może zaistnieć potrzeba podłączenia dysku instalacyjnego Windows Server 2003 (należy zamontować go w opcjach maszyny wirtualnej). Po zakończeniu instalacji na ekranie pojawi się stosowny komunikat:



Uruchom ponownie komputer.

Pierwsze logowanie do domeny

Po ponownym uruchomieniu komputera warto zwrócić uwagę, że zmianie uległo okno *Logowania do systemu* (naciśnij przycisk Opcje w celu wyświetlenia pełnego okna). Pojawiła się w nim opcja *Zaloguj do*. Po zalogowaniu się na konto *Administrator* (podajemy hasło lokalne) na ekranie powinien pojawić się komunikat informujący, że nasz komputer stał się kontrolerem domeny.

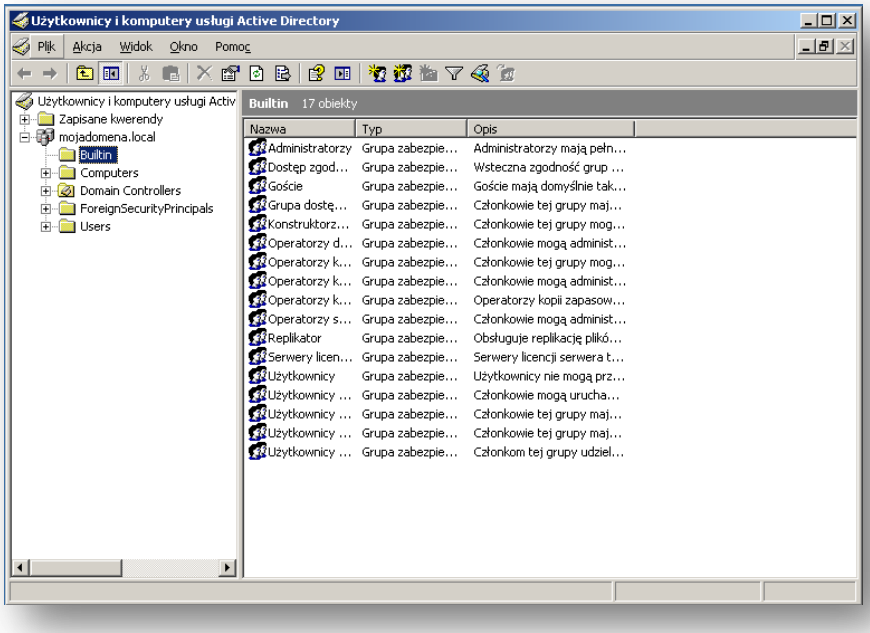


Zadanie: Skonfiguruj kontroler domeny na maszynie wirtualnej Windows Server 2003. Nazwę domeny wybierz według własnego uznania.

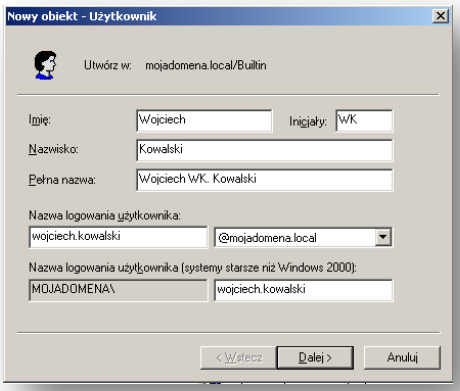
Konta domenowe

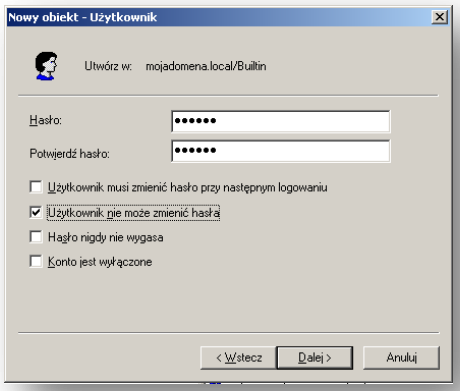
Tworzenie kont użytkowników domeny

Po zainstalowaniu w sieci kontrolera domeny możemy się do niego zalogować jako Administrator. Po zalogowaniu się możemy pozakładać konta dla użytkowników, którzy będą mogli logować się w naszej domenie. W celu dodania nowego użytkownika należy przejść do konsoli *Użytkownicy i komputery usługi Active Directory* (patrz Rysunek poniżej), która znajduje się w Narzędziach Administracyjnych (lub bezpośrednio z panelu Zarządzania tym serwerem) Następnie w istniejącej strukturze folderów przechodzimy do folderu *Users*.



W obszarze roboczym klikamy prawym przyciskiem myszy i wybieramy opcje *New User*. Tworzenie nowego użytkownika składa się z dwóch elementów. W pierwszym podajemy informacje o nowym użytkowniku (np. imię, nazwisko, nazwę konta, itp), natomiast w drugim podajemy hasło oraz wybieramy odpowiednie opcje odnoszące się do hasła (np. czy użytkownik będzie mógł zmienić hasło samodzielnie) oraz logowania (Rys. 8).



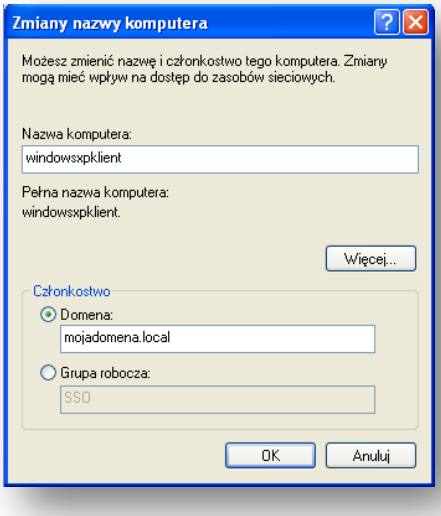


Dodanie komputera do domeny

Aby zbudować sieć opartą o domenę Windows Server 2003 należy dodać stacje robocze do domeny. Dodanie komputerów z systemem Windows XP Professional lub Windows 2000

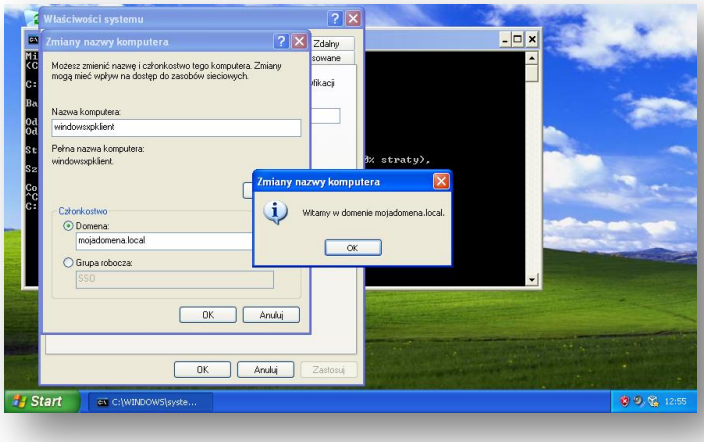
przebiega w sposób pokazany poniżej. Dodanie komputerów z systemem Windows 9x lub Windows Millenium jest możliwie jedynie po wyborze trybu zgodności ze starszymi systemami, podczas instalacji kontrolera domeny. Komputery wyposażone w system Windows XP Home Edition nie będą mogły zostać przyłączone do domeny.

W celu dodania komputera klienta do domeny trzeba zalogować się na tym komputerze jako użytkownik z prawami Administratora. Następnie należy upewnić się poprzez polecenie *ping* co do prawidłowego funkcjonowania połączenia sieciowego pomiędzy klientem a serwerem. Następnie kliknąć prawy klawiszem myszy na ikonie *Mój komputer* i wybrać polecenie *Właściwości* (lub w *Panelu sterowania* wybrać polecenie *System*). W kolejnym kroku należy wybrać zakładkę *Nazwa komputera* i nacisnąć przycisk *Zmień*.



W wyświetlonym oknie w obszarze *Członkostwo* zaznaczamy opcję *Domena* i podajemy nazwę naszej (stworzonej wcześniej) domeny do której chcemy się przyłączyć – **proszę pamiętać o wcześniejszym uzupełnieniu protokołu TCP/IP poprzez wskazanie adresu IP Windows Server 2003 jako bramy domyślnej i lokalnego serwera DNS**.

Następnie pojawi się okno logowania do domeny w którym wprowadzamy jako użytkownika: **Administrator** a hasło: **P@$$word**. Powinniśmy w rezultacie uzyskać okno przywitania w naszej domenie:



W celu zakończenia dołączania komputera do domeny należy ponownie uruchomić komputer. Następnie możemy zalogować się do domeny jako **Administrator**, upewniając się, że w oknie *Logowanie do systemu* wybrana jest odpowiednia domena. Oczywiście w trakcie powyższych operacji serwer, który skonfigurowany został jako kontroler musi być uruchomiony.

Dodanie do domeny komputera z systemem operacyjnym UNIX (np. Linux Ubuntu)

Aby dodać komputer z zainstalowanym systemem Linux Ubuntu do domeny Active Directory należy w najprostszym przypadku zainstalować oprogramowanie umożliwiające logowanie do tej domeny. Popularnym rozwiązaniem jest zainstalowanie programu Likewise:

administrator@SSOUbuntuMaster:~$ sudo aptitude install likewise-open-gui

Po zainstalowaniu tego pakietu uruchamiamy program:

administrator@SSOUbuntuMaster:~$ sudo domainjoin-gui

Pojawi się okno logowania, którym wprowadzamy nazwę domeny np. mojadomena.local oraz podajemy hasło dla użytkownika Administrator: np*. P@$$word*

Po poprawnym zalogowaniu się do domeny Active Directory, komputer z systemem Linux pojawi się na liście komputerów domenowych.

Uwaga: Proszę pamiętać o poprawnym skonfigurowaniu i nterfejsu sieciowego dla sieci wewnętrznej VirtualBox, dodaniu naszego lokalnego serwera DNS oraz zmodyfikowaniu jednej z linii pliku nsswitch.conf:

*hosts: files **dns** mdns4_minimal [NOTFOUND=return] mdns4*
znacznik dns MUSI BYĆ na 2 pozycji listy typów hostów

Aby wypisać komputer z systemem Linux z domeny wydajemy polecenie:

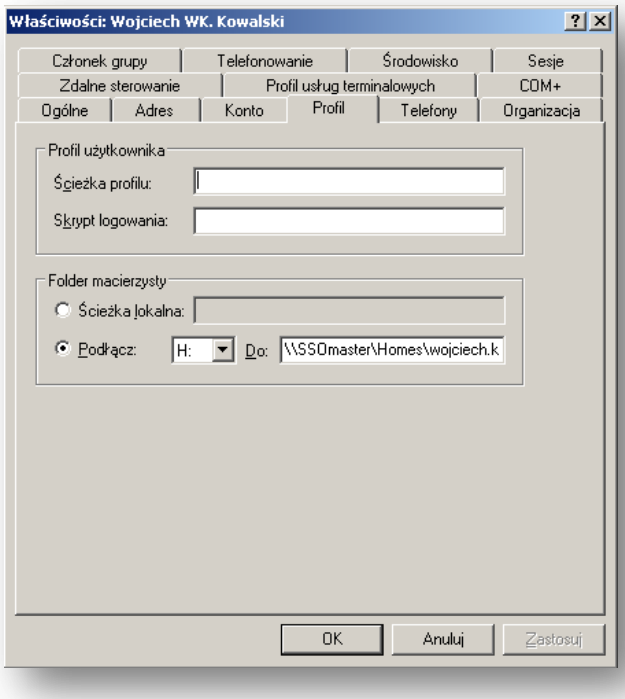
administrator@SSOUbuntuMaster:~$ sudo domainjoin-cli leave
Leaving AD Domain: MOJADOMENA.LOCAL
SUCCESS

Przypisywanie folderów macierzystych dla użytkowników

Jedną z wielu zalet jakie udostępnia nam domena Windows jest scentralizowanie zasobów sieci. Zaletę domen widać szczególnie w sieci wyposażonej w dużą liczbę stacji roboczych. Użytkownik posiadający konto domenowe, będzie mógł zalogować się na nie z każdej stacji roboczej w sieci, o ile należy ona do domeny. Dodatkowo możemy udostępnić użytkownikowi jego pliki. W tym celu zakładamy dla każdego nowego użytkownika tzw. folder macierzysty znajdujący się na serwerze, który będzie jego prywatnym folderem w sieci. Aby utworzyć dla użytkowników ich foldery macierzyste oraz scentralizować zarządzenie takimi folderami na serwerze warto utworzyć na serwerze folder główny np.

homes i w tym folderze umieszczać foldery macierzyste dla każdego użytkownika, który posiada konto domenowe.

Aby to zrobić należy uruchomić konsolę *Active Directory Users and Computers* i wybierać użytkownika, któremu chcemy przypisać folder macierzysty. Następnie na zakładce *Profil* (*Profile*) w polu *Folder macierzysty -> Podłącz* wprowadzamy odpowiednią literę dysku, jaki będzie mapowany na komputerze lokalnym oraz podajemy pełną ścieżkę do folderu według konwencji *nazwa_serwera**path**%username%*. Przykładowo dla użytkownika *wojciech.kowalski* posiadającego konto domenowe na serwerze *SSOmaster*, założyliśmy w folderze *homes* folder *wojciech.kowalski*. Aby przypisać temu użytkownikowi folder macierzysty należy w polu *Folder macierzysty* wybrać dysk H: i wpisać ścieżkę *SSOmaster**Homes**%username%*.



Zadania

1. Dodaj czterech różnych użytkowników domeny (np.: user1, user2, user3, user4);
2. Utwórz na serwerze folder katalogów domowych *homes* oraz foldery dla wszystkich stworzonych użytkowników; Zainstaluj **samodzielnie** serwer plików z panelu Zarządzaj tym serwerem (ustaw limity udziałów dyskowych według własnego uznania); Udostępnij foldery macierzyste w sieci nadając użytkownikom prawa pełnej kontroli do ich katalogów;
3. Dodaj komputer klienta Windows XP do domeny i sprawdź czy istnieje możliwość zalogowania z tego komputera na konta użytkowników domenowych.
4. Dodaj komputer klienta Ubuntu do domeny.