Usługi katalogowe

Usługi katalogowe występują we wszystkich systemach serwerowych. Tworzą one niejako system bazodanowy, w którym poszczególne informacje gromadzone są w odpowiednie grupy, zwane obiektami. Usługi te pozwalają na gromadzenie następujących danych:
- konta dostępnych użytkowników oraz grupy użytkowników (obiekt użytkownicy)
- dostępne w systemie aplikacje (obiekt aplikacje)
- dostępne w sieci stacje robocze (obiekt urządzenia sieciowe)
- pozostałe informacje, takie jak dostępne zasoby w sieci, grupy zabezpieczeń, informacje o urządzeniach sieciowych: routery, drukarki, serwery NAS; (obiekt pozostałe/inne zasoby sieciowe)

Tego typu usługa pozwala administratorowi z jednego punktu sieciowego (przykładowo serwera) zarządzać wyżej wymienionymi zasobami sieciowymi oraz odpowiednio je katalogować/opisywać.

Wszystkie dane w usługach katalogowych tworzą strukturę drzewa – na szczycie znajduje się serwer usługi katalogowej (korzeń), od którego odchodzą odpowiednie katalogi – obiekty(konary). W każdym katalogu można docelowo utworzyć nowe katalogi (gałęzie) bądź bezpośrednio dodawać informacje – poszczególnych użytkowników, stacje robocze itp. (liście).

I. Podstawowe cechy usług katalogowych:
- informacje w nich zawarte są częściej odczytywane niż zapisywane/dopisywane – przeważnie cała konfiguracja przebiega zaraz po zainstalowaniu usługi, a z czasem dodawane/usuwane są jedynie pojedyncze stacje robocze, konta użytkowników i/lub grupy użytkowników
- schemat ułożenia danych wygląda następująco: klasa obiektu (podane na początku), atrybuty klasy, opcjonalnie przestrzeń nazw oraz same dane
- w klasach pewne atrybuty są obligatoryjne (w zależności od implementacji), a niektóre nieobowiązkowe – przyjmują wtedy wartość pustą
- atrybuty mogą posiadać wiele wartości (niektóre z nich)
- klasy oraz atrybuty są zestandaryzowane – każda implementacja usług katalogowych powinna je posiadać
- każda usługa katalogowa działa w obrębie ustalonej domeny (tzw. jednostki organizacyjnej). Domena to nic innego jak przyjazna nazwa komputera w sieci. Przeważnie nazwą domenową serwera jest np. mojserwer.local bądź mojserwer.nazwafirmy.local itp. Stąd też usługi katalogowe wymagają wręcz by serwer, na którym pracują, posiadał rolę/usługę DNS (Domain Name System).

II. Organizacja usług katalogowych w systemach Windows Server

W Windows 2012 Server usługa katalogowa kryje się pod nazwą Active Directory. Stanowi ona implementację ogólnie używanego protokołu LDAP (Lightweight Directory Access Protocol). Pojedynczy serwer posiadający rolę serwera usługi katalogowej staje się automatycznie pojedynczym drzewem w sieci. Jeżeli sieć jest dużych rozmiarów (hale produkcyjne, hale biurowe itp.) istnieje możliwość ustawienia większej ilości komputerów z aktywowaną rolą Active Directory. Grupa serwerów z aktywną usługą katalogową tworzy las. W lesie istnieje jedno, główne drzewo, pełniące rolę kontrolera całej domeny. W takim przypadku domena zorganizowana jest następująco:
- kontroler domeny – posiada nazwę mojafirma.local
- serwer 1 – posiada nazwę serwer1.mojafirma.local
- serwer 2 – posiada nazwę serwer2.mojafirma.local
- serwer 3 – posiada nazwę serwer3.mojafirma.local

Oczywiście wszystko zależy od wielkości budowanej sieci oraz od potrzeb administracyjnych. Stacje robocze łączone do tak zorganizowanej sieci będą miał odpowiednio adresy:

- do serwera 1: stacja1.serwer1.mojafirma.local, komputerBasi.serwer1.mojafirma.local, laptop.serwer1.mojafirma.local, itp.
- do serwera 2: biuro.serwer2.mojafirma.local, salaobrad.serwer2.mojafirma.local, itp.

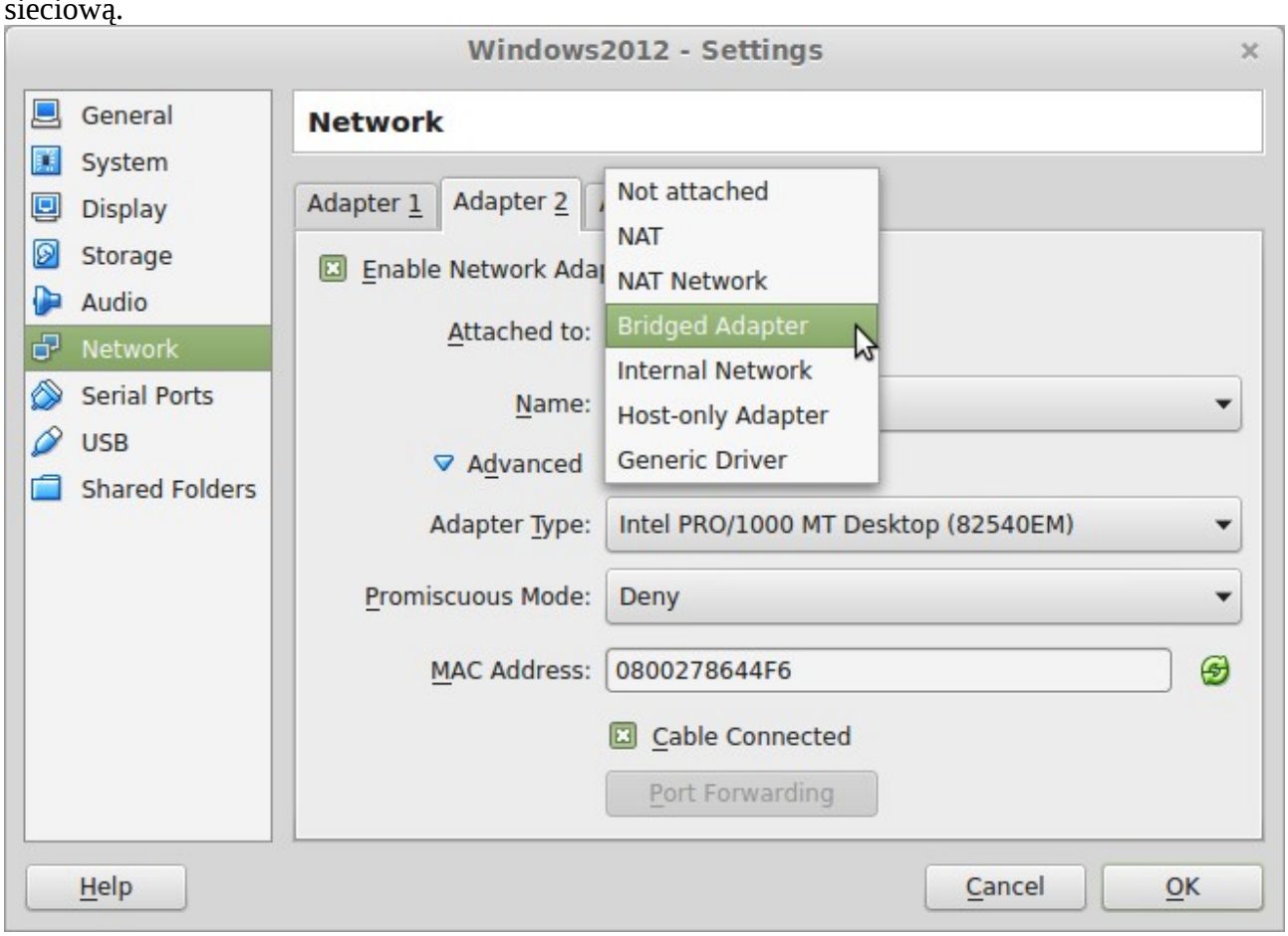
Tyczy się to każdego kolejno podłączanego komputera do utworzonej domeny. Jak łatwo się domyślić pierwszy człon dla docelowego komputera klienckiego to po prostu nazwa komputera, jaka została nadana przez danego użytkownika

WAŻNE: Nazwy komputerów są jak adresy IP czy numery identyfikacyjne – NIE NALEŻY ICH DUBLOWAĆ! W razie problemów z wyegzekwowaniem od użytkowników nadania jednoznacznie brzmiących nazw należy zrobić to samemu, a następnie zablokować takowym osobom możliwość zmiany nazwy (poprzez ograniczenia w rejestrze bądź polityce zabezpieczeń – będą omówione na następnych lekcjach).

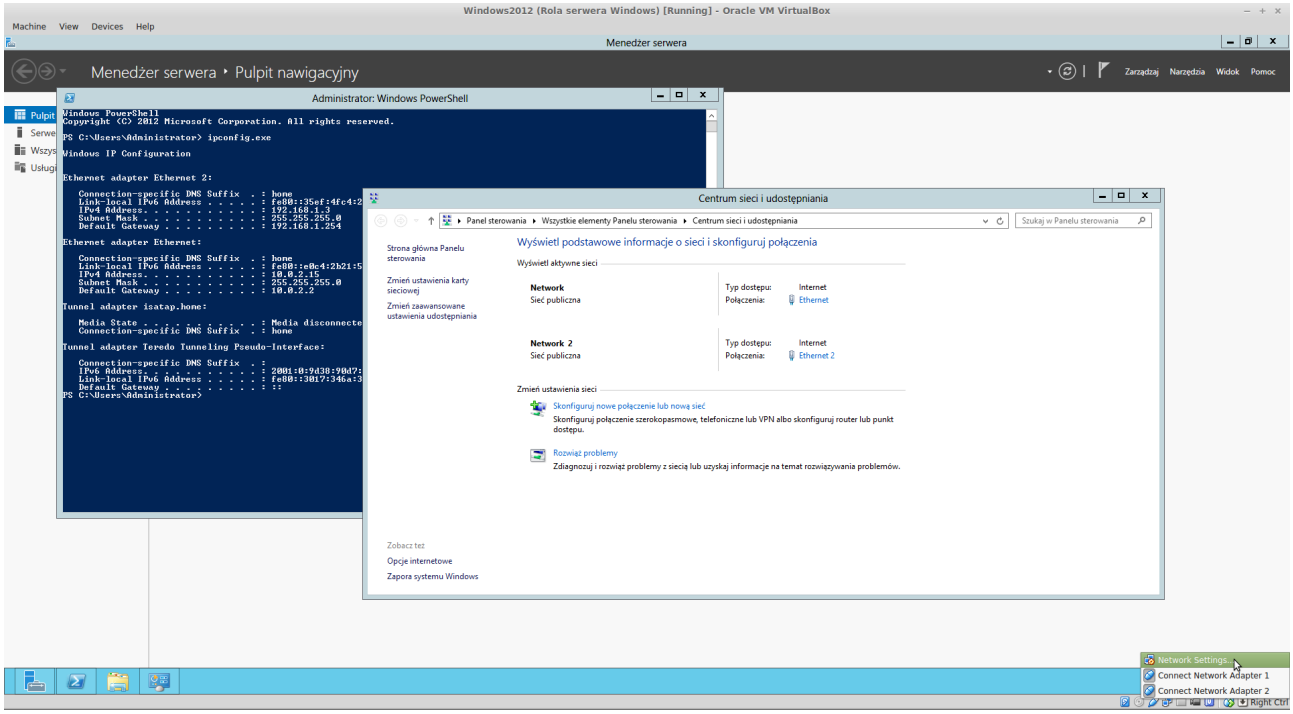
W naszym przypadku będzie rozpatrywać jedynie pojedynczy kontroler domeny, w obrębie którego utworzymy jednego klienta (zostanie doinstalowany kliencki system Windows 8).

III. Instalacja usługi na serwerze.

1. Pierwszym krokiem będzie nadanie odpowiednich właściwości drugiej karcie sieciowej dołączonej do wirtualnej maszyny (utworzona przy okazji tworzenia maszyny wirtualnej).
W tym celu klikamy ustawienia naszej maszyny wirtualnej i przechodzimy do sekcji Network. Nie modyfikujemy pierwszej karty (Adapter 1), tylko przechodzimy do drugiej z nich (Adapter 2). W polu Attached to należy ustawić wartość Bridged Adapter (zmostkowany) i wskazać aktywną kartę sieciową.

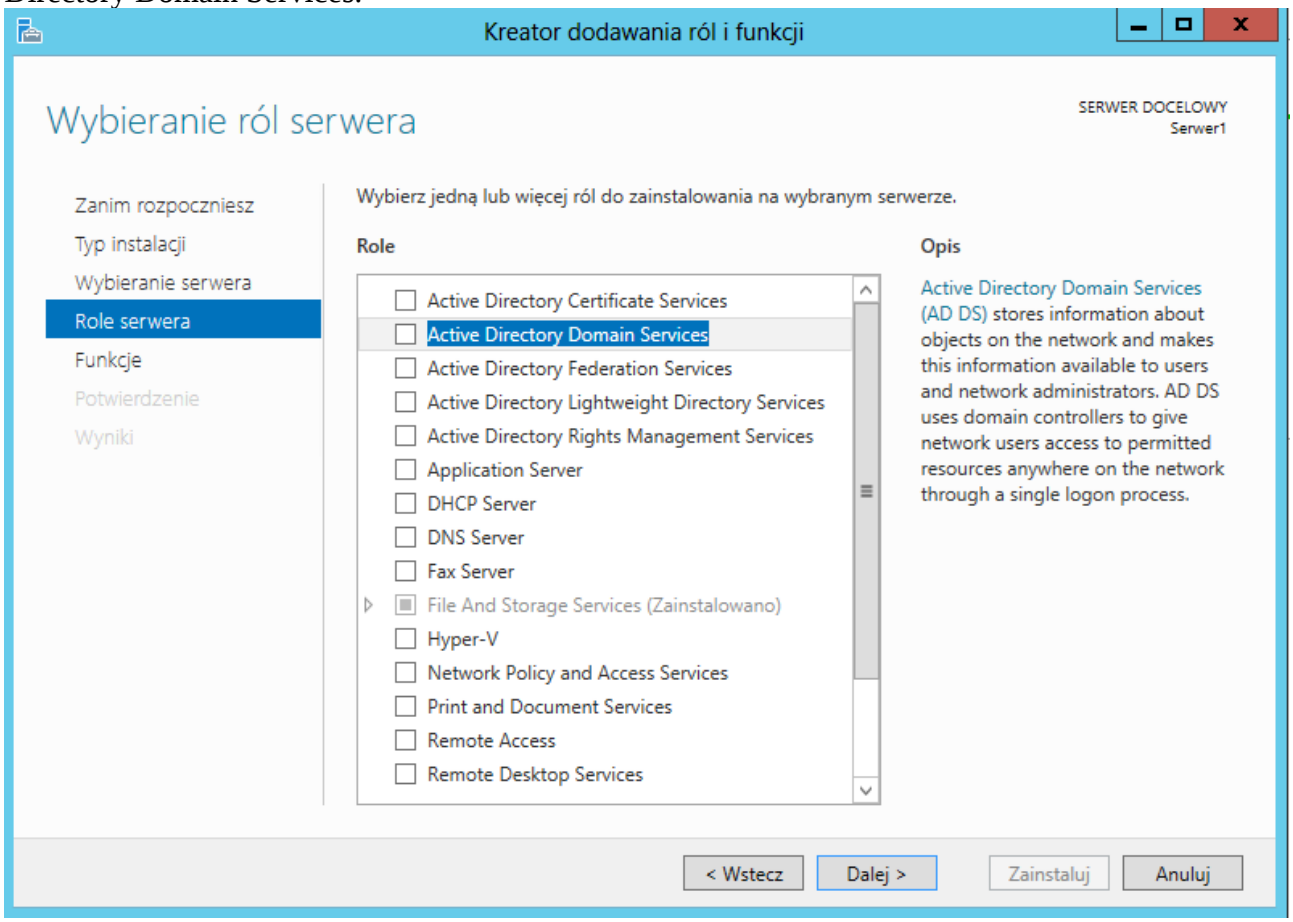


Ustawienia sieci można także zmodyfikować na działającym systemie poprzez kliknięcie prawym przyciskiem myszy na ikonie sieci i wybór ustawień (dolny, prawy róg ekranu):



Niestety rozwiązanie to nie zawsze działa i może się zdarzyć, że trzeba będzie i tak zrestartować system.

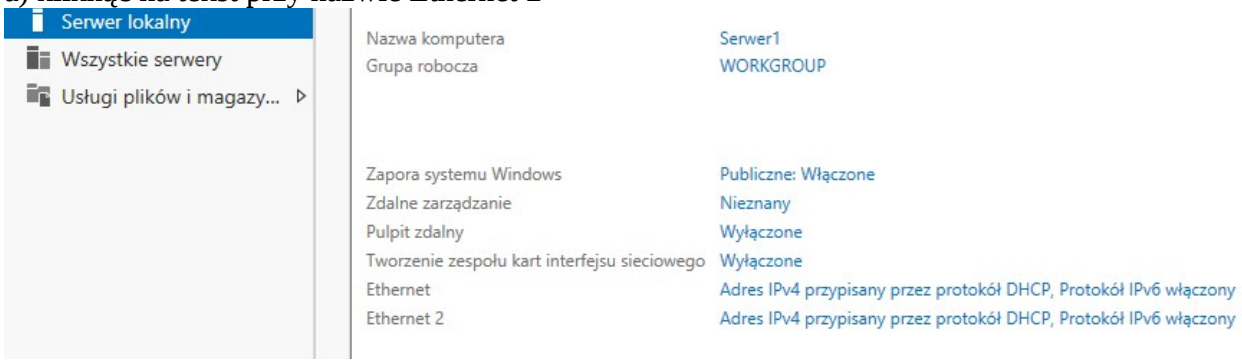
2. Teraz, po uruchomieniu systemu i wybraniu dodawania ról do systemu, wybierzemy rolę Active Directory Domain Services.



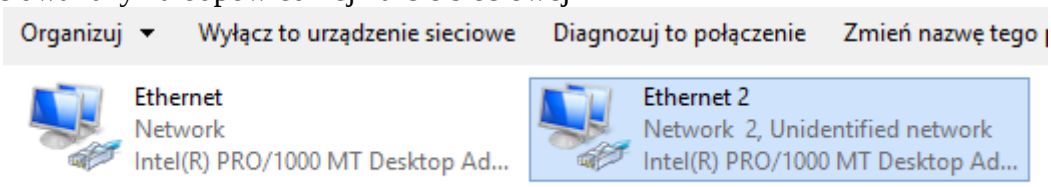
Podobnie jak to miało miejsce na poprzednich zajęciach, system poinformuje nas o konieczności doinstalowania dodatkowych ról/usług systemowych.

WAŻNE: Kreator domyślnie nie dodaje roli DNS. Usługa katalogowa jednak wymaga jej obecności w systemie do prawidłowej pracy – należy ją doinstalować!

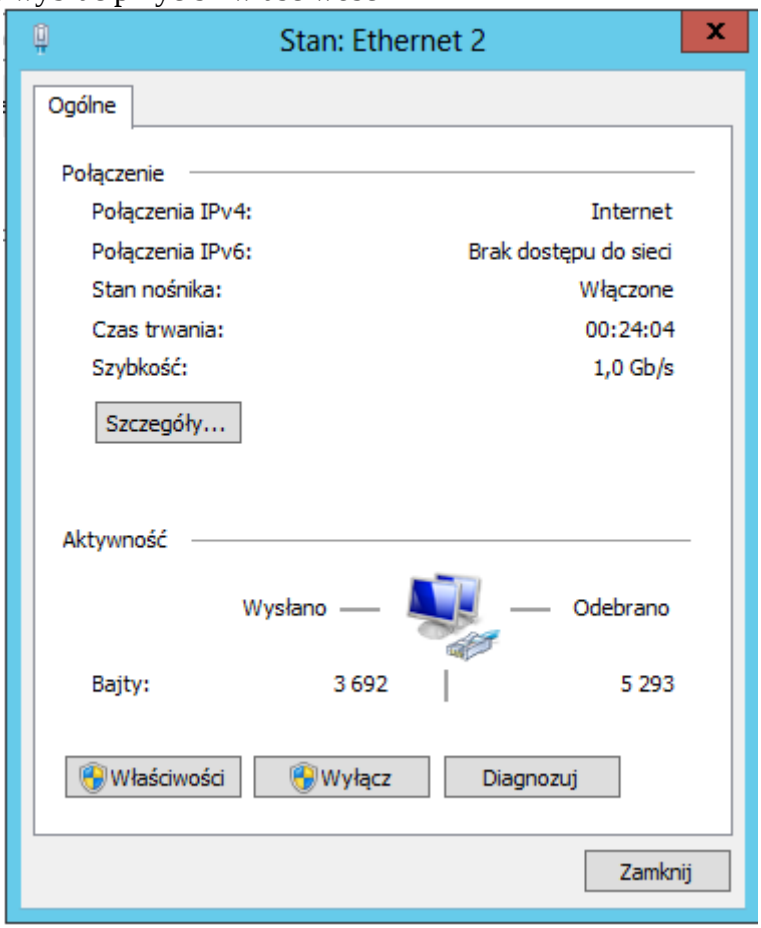
INFORMACJA: Usługa DNS wymaga co najmniej 1 interfejsu sieciowego, który posiada skonfigurowany statycznie adres IP. Aby dokonać zmiany adresu IP na statyczny należy:
a) kliknąć na tekst przy nazwie Ethernet 2



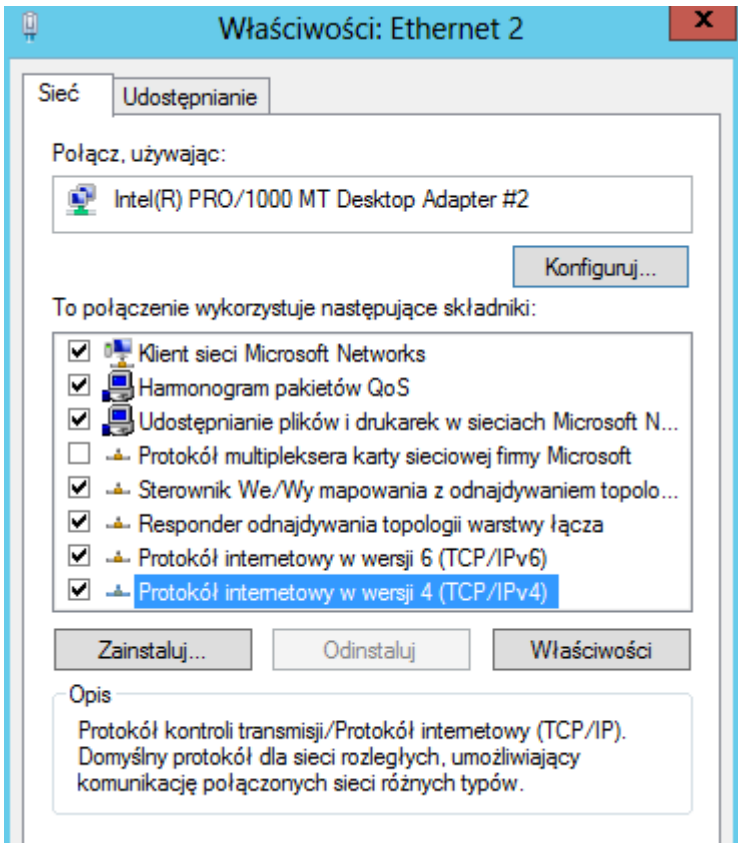
b) kliknąć dwa razy na odpowiedniej karcie sieciowej



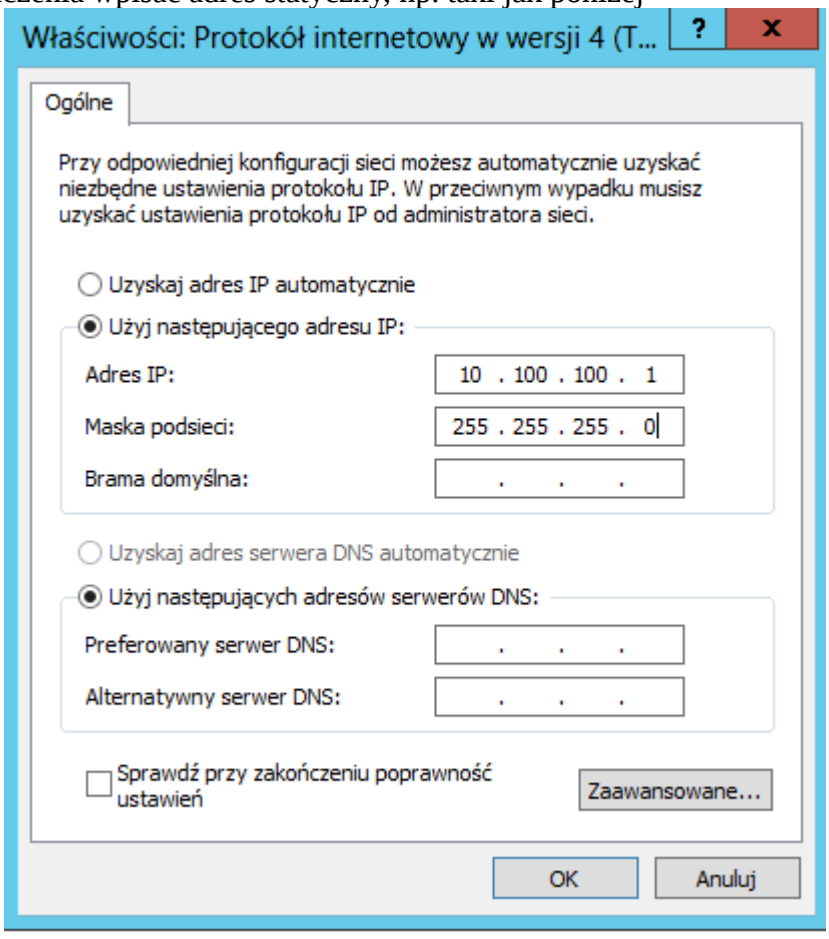
c) w otwartym oknie wybrać przycisk właściwości



d) z okna, które wyskoczyło wybrać protokół TCP/IPv4 (zaznaczony na niebiesko)



e) dla potrzeb ćwiczenia wpisać adres statyczny, np. taki jak poniżej

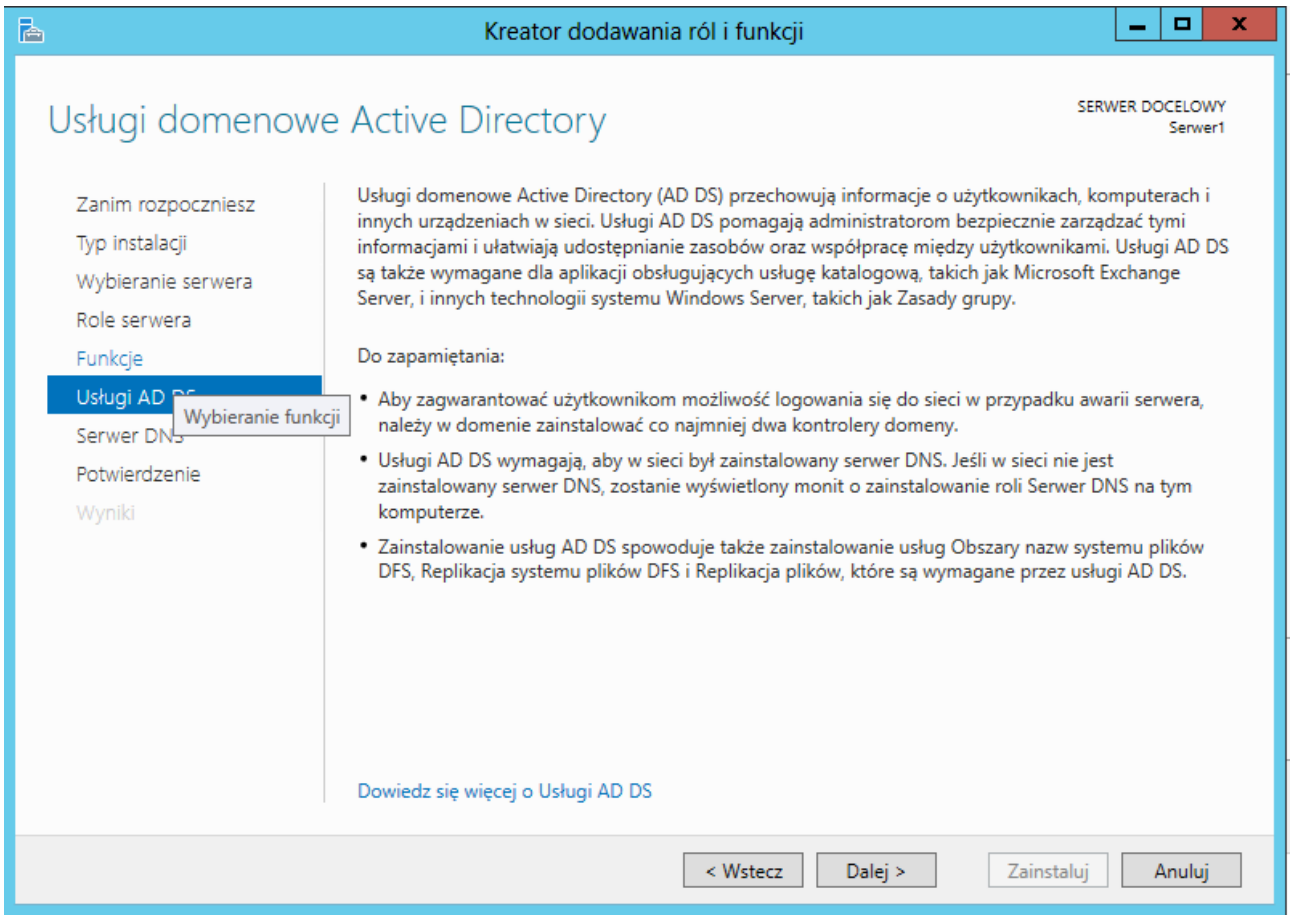


UWAGA! Aby nie spowodować konfliktów w sieci (mogą powstać) proszę dla każdego serwera nadać inne adresy IP, tj. jeżeli jedna osoba przepisze adres ze zrzutu ekranu, to następna wpisuje

adres 10.100.101.1, następna 10.100.102.1 itd.
Adres maski sieci POZOSTAJE BEZ ZMIAN!

---

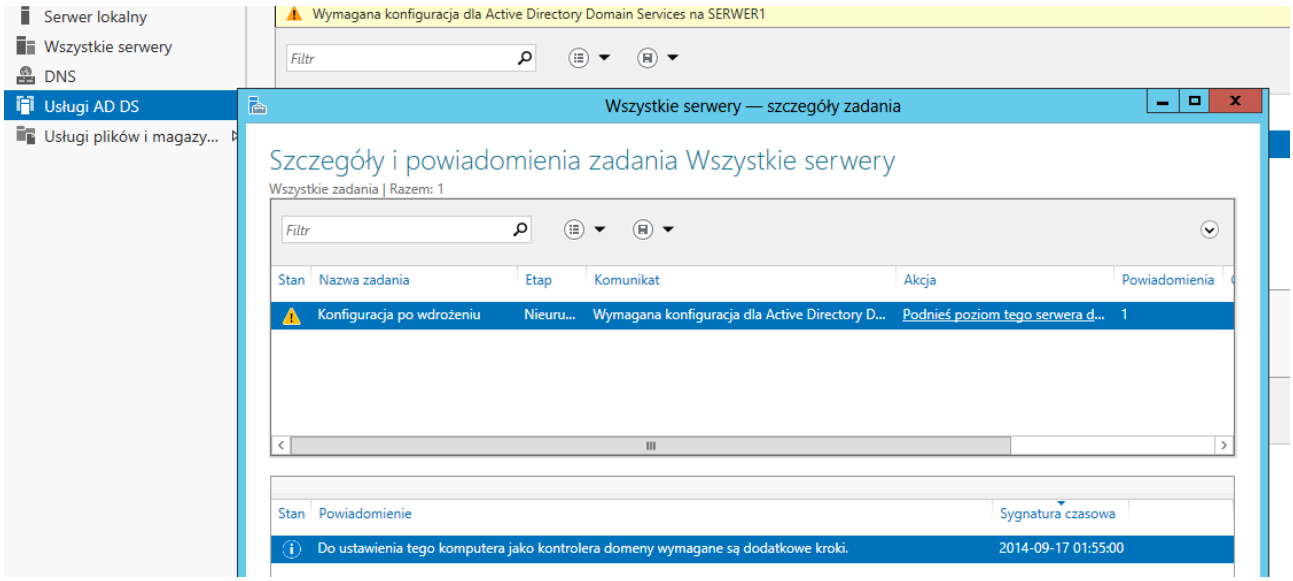
3. Prócz domyślnych narzędzi Active Directory zostanie dodana także usługa Group Policy Management. Usługa ta pozwala na zarządzanie grupami zabezpieczeń dla poszczególnych użytkowników. Dzięki temu osoby logujące się jako zwykli pracownicy nie będą mogli np. zmieniać ustawień systemowych czy zaglądać do rejestru systemu. Z kolei administratorzy będą mogli to jak najbardziej zrobić. Grupy bezpieczeństwa aktywują się same z chwilą, gdy dana osoba loguje się do systemu, który działa w obrębie wskazanej domeny.



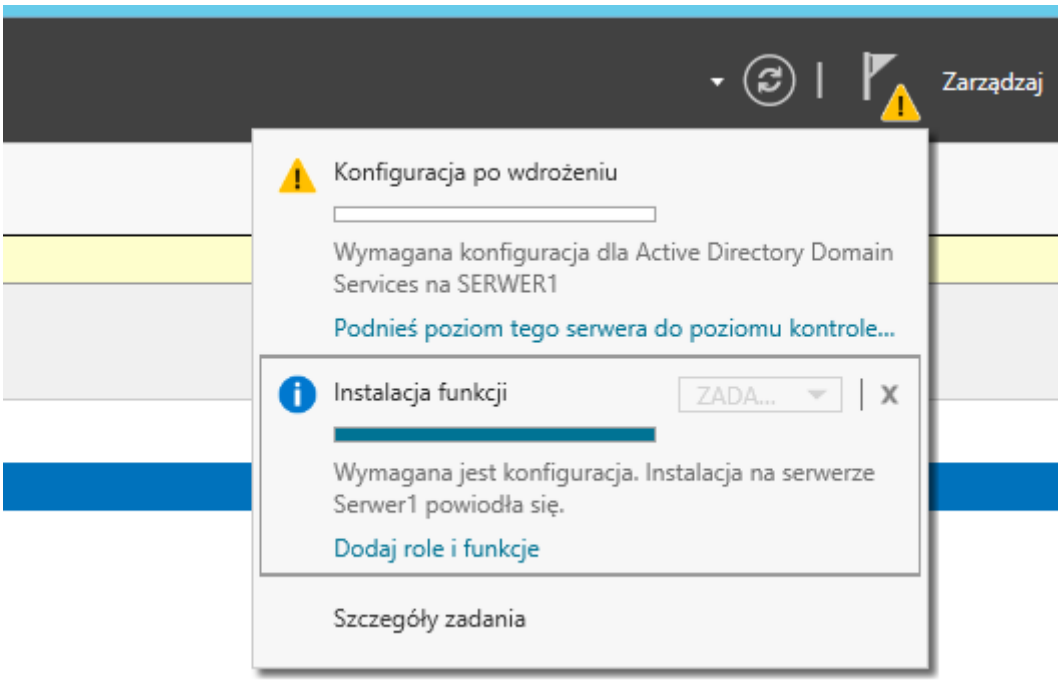
4. W dalszej części instalacji zostaniemy poinformowanie o właściwościach usługi katalogowej, jej wymaganiach (serwer DNS) oraz o konsekwencjach, gdy użytkownicy korzystający z Active Directory zostaną pozbawieni sieci (brak możliwości zalogowania się do sieci na stacji roboczej).

5. Teraz pozostaje już tylko poczekać na koniec instalacji usługi.

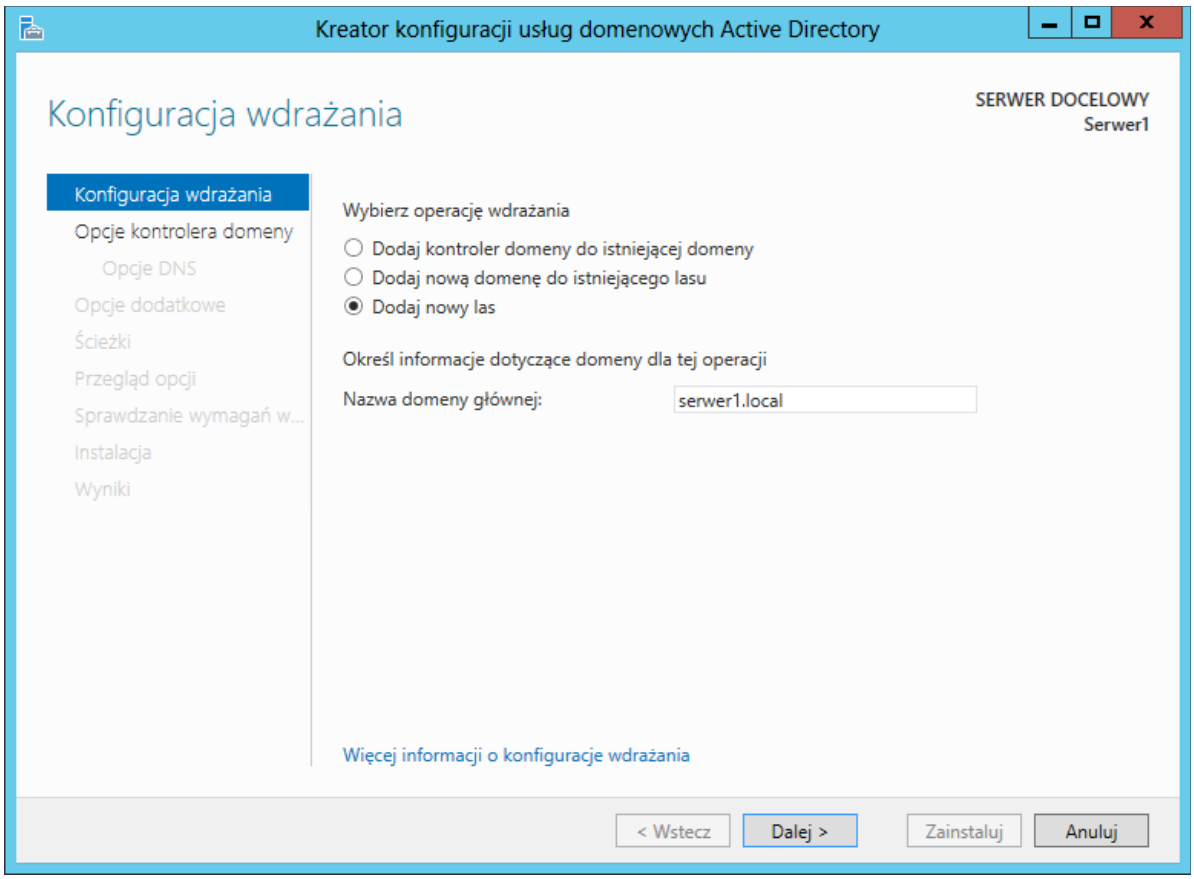
6. Po instalacji, aby serwer Active Directory był gotowy do użycia należy go skonfigurować. Można się tego dowiedzieć po kliknięciu z lewej strony menedżera w Usługi AD DS.



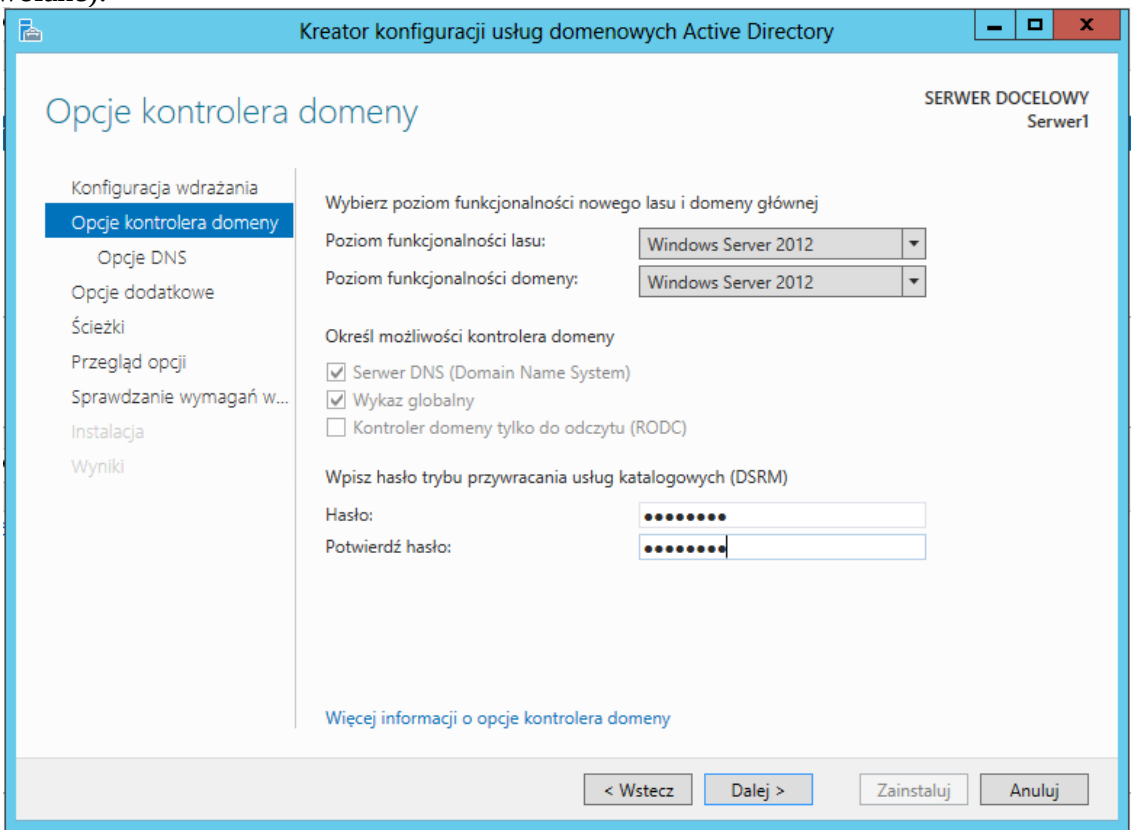
Aby przejść do konfiguracji można wybrać zakładkę zdarzeń i kliknąć „podnieś poziom tego serwera...”



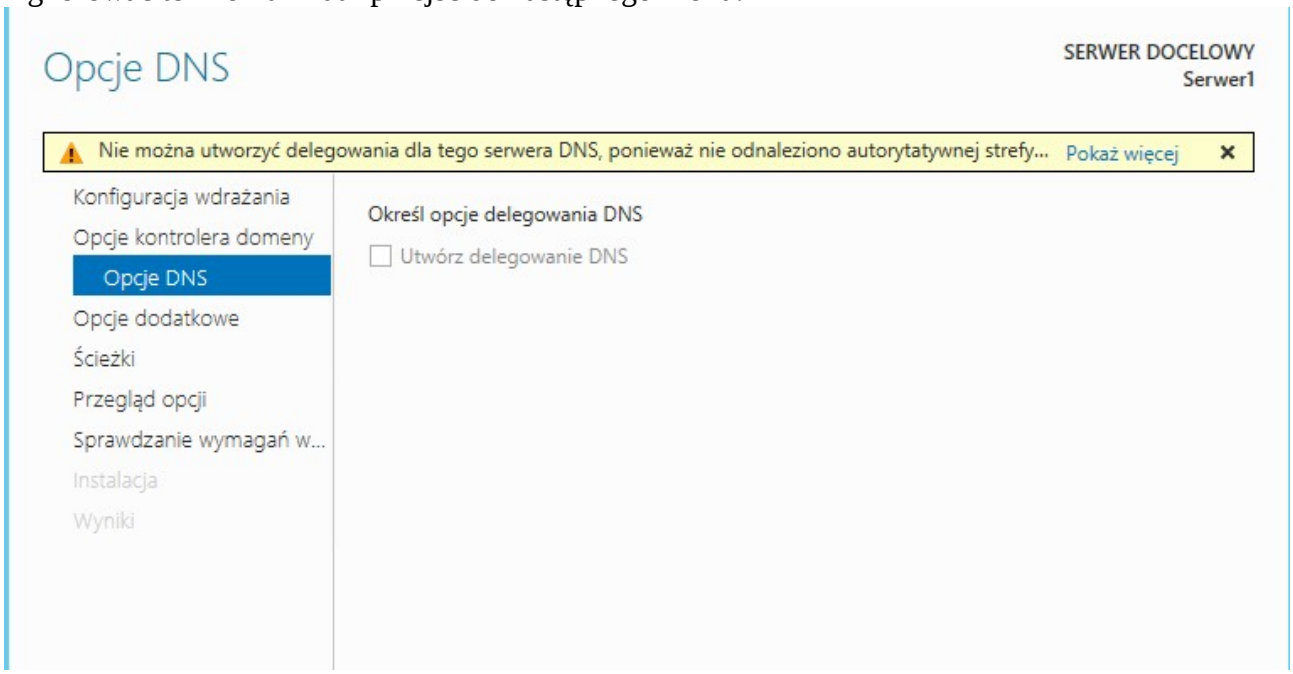
7. Dotychczas nasza sieć nie posiada żadnego kontrolera domeny ani samej domeny. Dlatego należy utworzyć nowy las (Dodaj nowy las) oraz podać nazwę domeny głównej (np. serwer1.local; nazwa może być dowolna)



8. W nastopnym kroku określamy poziom funkcjonalności lasu oraz domeny. Jeżeli w sieci nie będziemy mieć starszych systemów niż Windows 7 spokojnie można wybrać Windows 2012. Jeżeli przewidywalibyśmy starsze wersje systemów Windows to należałoby zmienić funkcjonalność na starszą (np. dla systemu XP wybrać Server 2003). W trym kroku należy także podać hasło odzyskiwania usług katalogowych (w celu zapobieżenia przywrócenia usługi przez osoby niepowołane):

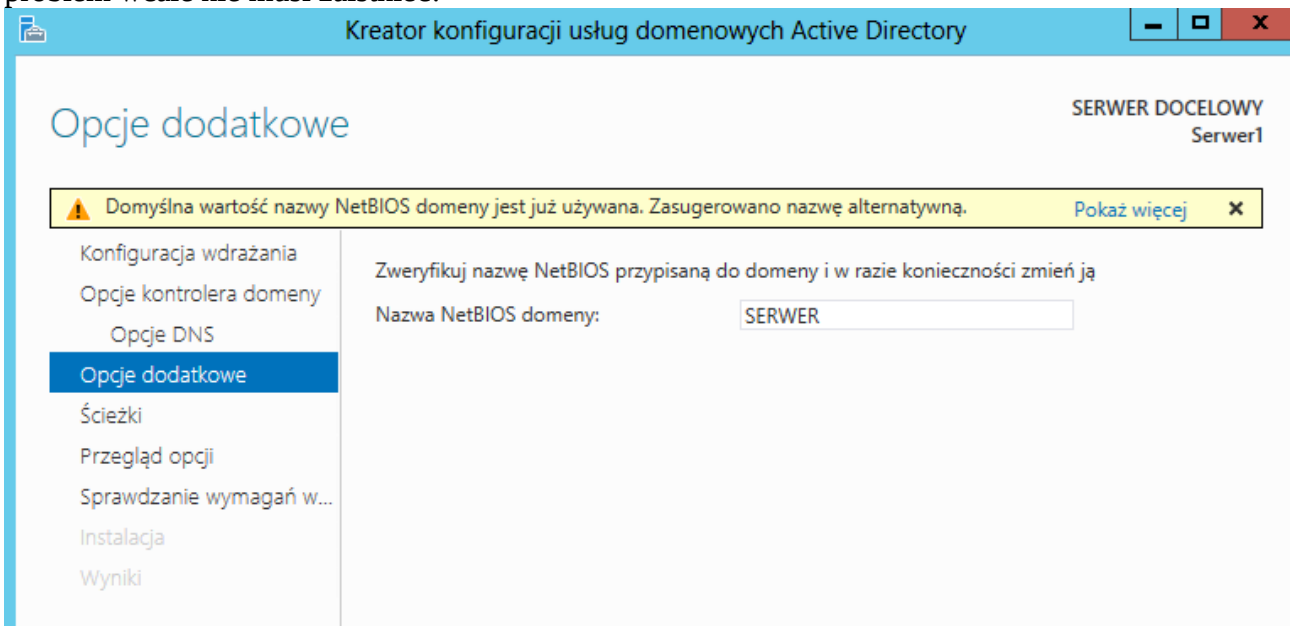


9. Przy opcjach DNS pojawi się komunikat, że nie mamy poprawnie skonfigurowanego serwera DNS. Spowoduje to brak możliwość przeglądania brzostów sieciowych w domenie oraz przeglądanie sieci lokalnej poza domeną. Ponieważ zależy nam jedynie, by usługa DNS obsługiwana naszą domenę (dostępem do sieci zajmuje się osobne urządzenie - router) możemy zignorować ten komunikat i przejść do następnego kroku.



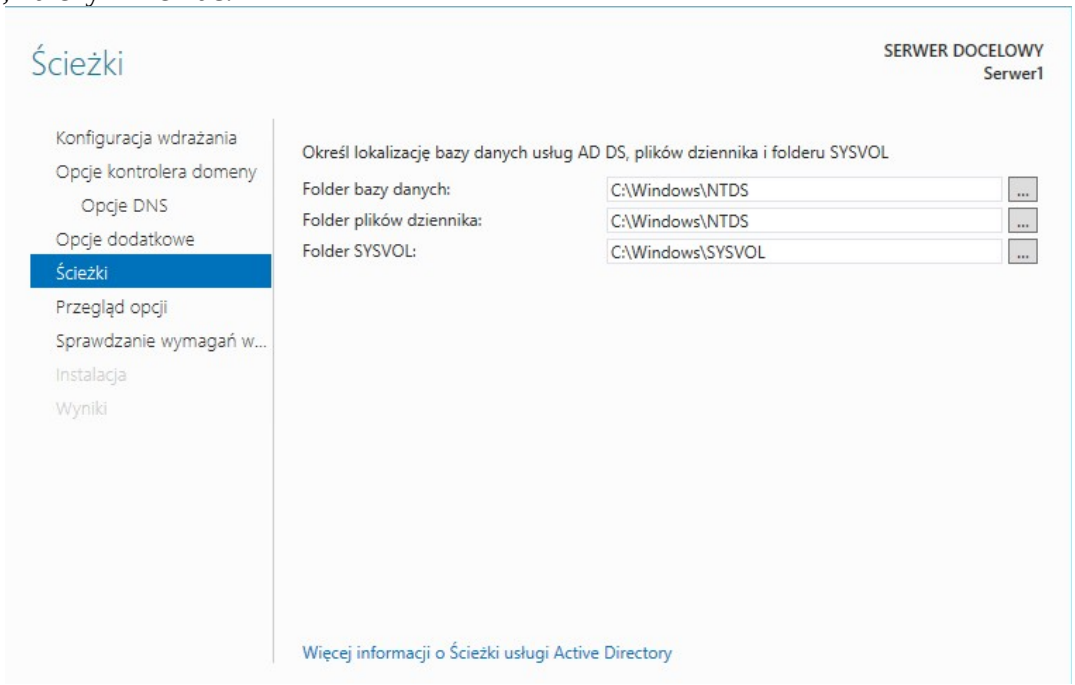
10. Konfigurator będzie prosił o podanie nazwy NetBIOS, pod jaką będzie widziany serwer w domenie. Ponieważ nazwa komputera oraz nazwa DNS domeny to SERWER1, usługa automatycznie doda do nazwy 0 tworząc nazwę „SERWER10”. Nazwa została zamieniona po prostu na SERWER

INFORMACJA: Nazwy są dowolne. Każdy może mieć inne nazwy przez co opisany powyżej problem wcale nie musi zaistnieć!

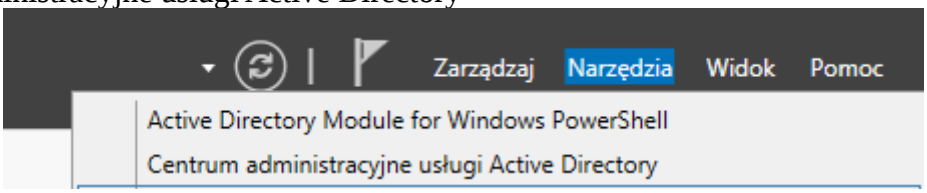


11. W tym kroku należy podać katalogi, w których będą przechowywane bazy danych Active Directory. System domyślnie proponuje dysk C. W dobrym tonie jest zmiana domyślnych katalogów i przeniesienie ich na inny dysk (na wypadek awarii systemu, by nie zostały usunięte np. wraz z systemem przy reinstalacji). Ponieważ jednak korzystamy z jednego dysku wirtualnego to możemy zachować domyślnie ścieżki

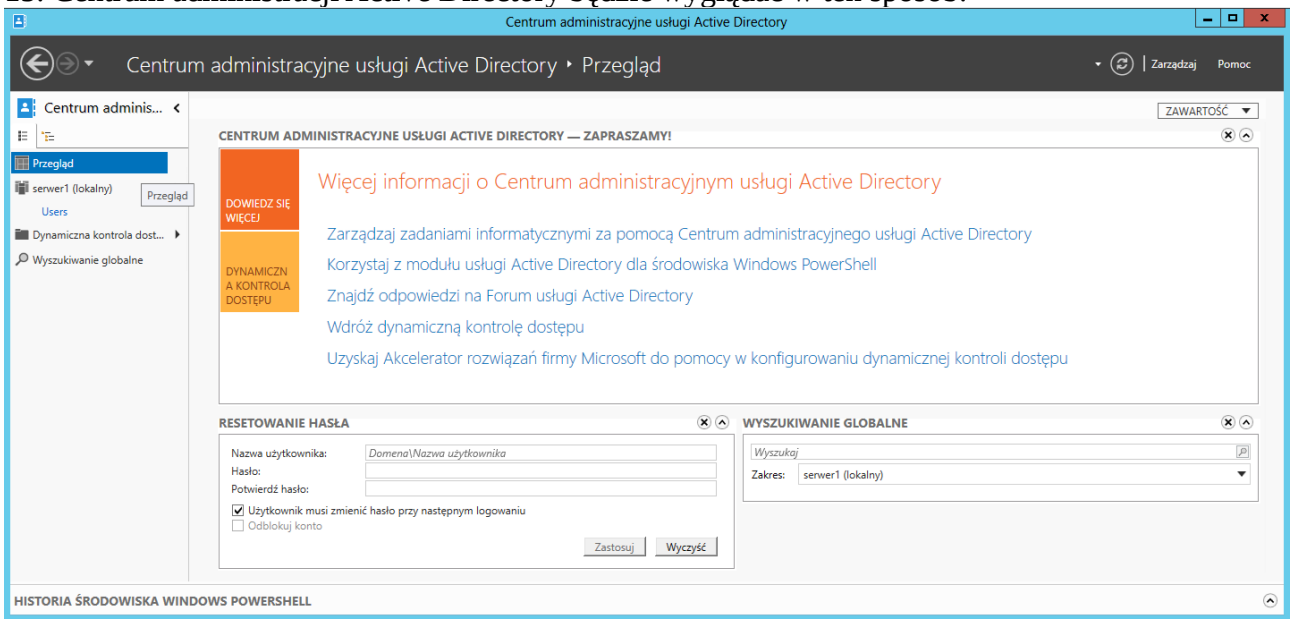
UWAGA: Niekiedy przechowywanie baz danych Active Directory uważane jest za poważne naruszenie bezpieczeństwa folderu systemowego. Każdy komputer kliencki ma bowiem dostęp do tych katalogów (musi mieć). Tak więc przy profesjonalnej konfiguracji ścieżki te, nawet w obrębie dysku C, należy zmieniać.



12. W tym kroku wyświetli nam się podsumowanie konfiguracji; klikamy dalej.
13. W ostatnim kroku przed instalacją następuje sprawdzenie wymagań instalacyjnych domeny. Ponieważ spełniamy je (ostrzeżenia ignorujemy – nie są w tej chwili ważne), możemy zainstalować usługę. Po instalacji serwer sam dokona ponownego rozruchu.
14. Teraz należy skonfigurować usługę Active Directory. W tym celu należy wybrać narzędzie Centrum Administracyjne usługi Active Directory



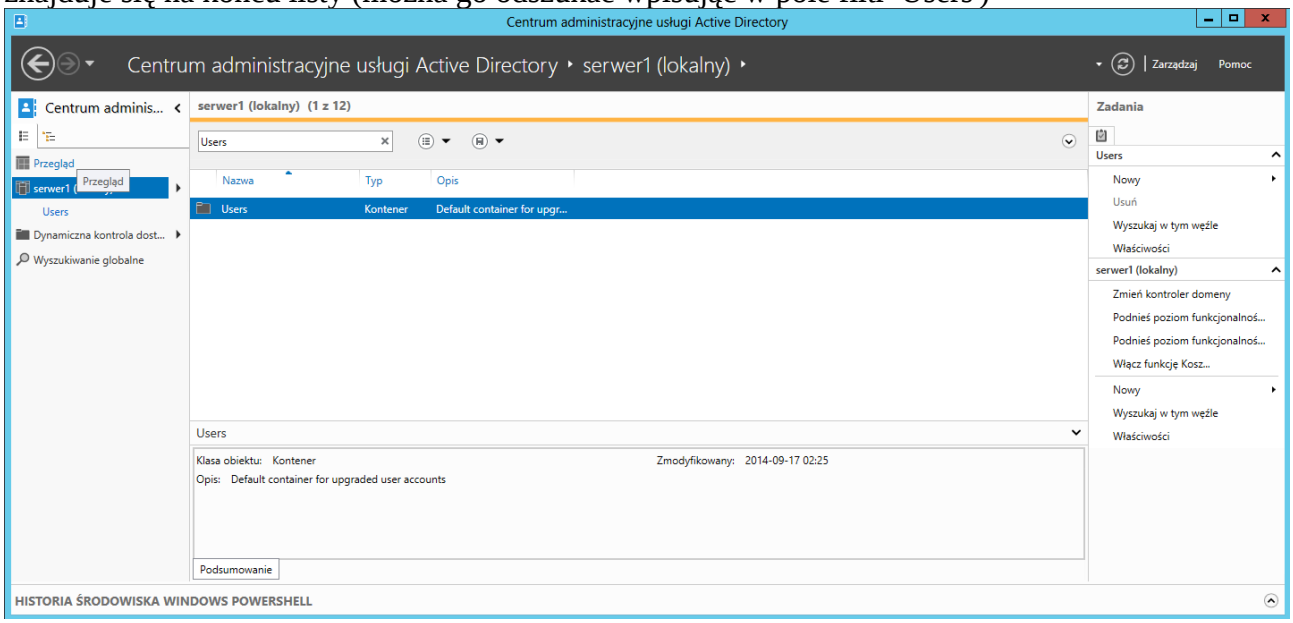
15. Centrum administracji Active Directory będzie wyglądać w ten sposób:



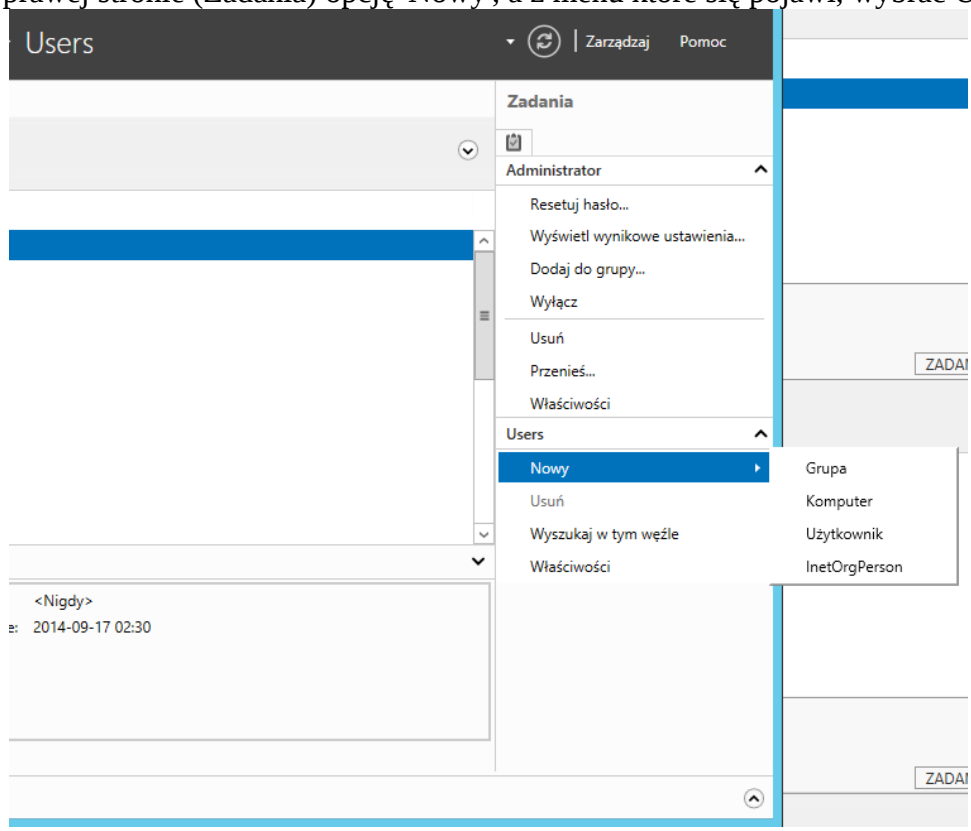
Prezentowany ekran pozwala na resetowanie hasła wskazanemu użytkownikowi oraz na znalezieniu

informacji w usłudze katalogowej (AD). Resetu hasła dokonuje się poprzez podanie nazwy domeny oraz nazwie użytkownika, który zgubił/zapomniał swojego hasła.
Przykładowo w domenie z przykładu reset wyglądałby następująco:
serwer1\User

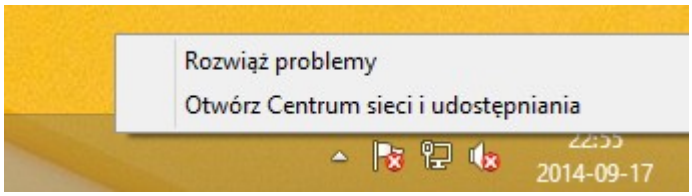
16. Bardziej interesuje nas dodanie nowego użytkownika. W tym celu wybieramy nazwę naszego serwera z listy po lewej stronie (serwer1). Wyświetlą się wszystkie dostępne katalogi (kontenery oraz jednostki organizacyjne) – stąd nazwa usługa katalogowa. Interesujący nas kontener Users znajduje się na końcu listy (można go odszukać wpisując w pole filtr 'Users')



17. W tej chwili dostępni są tylko 3 użytkownicy (można sprawdzić segregując wszystkie dostępne „liście” kolumną typ). Dodajmy nowego użytkownika, który będzie mógł logować się na swojej stacji roboczej z poświadczeniami zdobytymi z domeny. Aby tego dokonać należy kliknąć z zakładki po prawej stronie (Zadania) opcję 'Nowy', a z menu które się pojawi, wybrać Użytkownik.



18. Tworzenie konta jest dosyć intuicyjne. Wymaga wprowadzenia nazwy logowania użytkownika (Logowanie przy użyciu UPN użytkownika). Pole niżej (logowanie przy użyciu SAM użytkownika uzupełni się automatycznie). Wszystkie pozostałe pola są polami ponadobowiązkowymi i nie trzeba ich wypełniać (aczkolwiek stanowią one niejako kartę użytkownika). Wszelkie dane można edytować później, edytując profil danego użytkownika. Proszę zauważyć, iż profil zezwala na założenie konta bez hasła. Dodatkowo zostało zaznaczone pole „Hasło nigdy nie wygasa" oraz „Użytkownik nie może zmienić hasła". W normalnych warunkach nie jest to dobre rozwiązanie – hasło powinno być zmieniane minimum co 30 dni oraz to użytkownik powinien je zmieniać (powinna być zaznaczona opcja Użytkownik musi zmienić hasło przy następnym logowaniu). Konto można także ochronić przez usunięciem (usunięcie będzie wymagać dodatkowych potwierdzeń), ustalić czas logowania (dni i godziny), a także komputery, do których dany użytkownik będzie miał dostęp (domyślnie może zalogować się na dowolnym komputerze należącym do domeny).
19. Mając już użytkownika możemy przystąpić do podłączenia do naszej sieci stacji roboczej. Na potrzeby eksperymentu będzie to system Windows 8.1 również zainstalowany na maszynie wirtualnej. Należy pamiętać, iż system ten także musi znajdować się w tej samej adresacji IP. Dlatego pierwszym krokiem będzie zmiana adresu IP na adres z zakresu naszego serwera Windows 2012. W Windows 8.1 zmiana adresów przebiega w ten sam sposób co w Windows 2012. Na pulpicie klikamy prawym przyciskiem myszy na ikonę sieci, po czym na Otwórz Centrum sieci i udostępniania



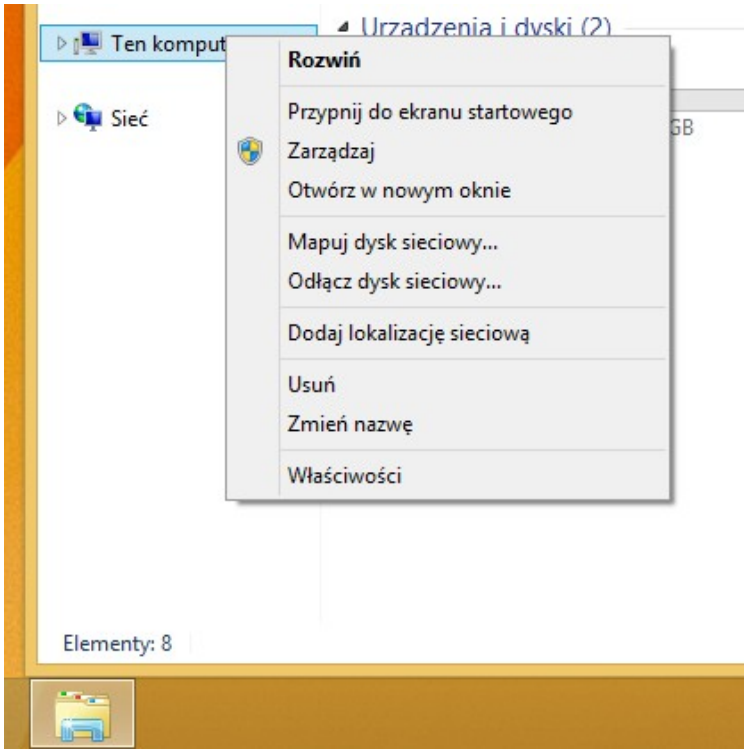
Następnie wybieramy naszą kartę Ethernet, jej właściwości, a na końcu właściwości składnika Protokół internetowy w wersji 4 (TCP/IPv4)
należy dokonać następujących ustawień:
Adres IP: 10.100.100.2 (bądź 10.100.101.2 , 10.100.102.2, 10.100.103.2, 10.100.104.2, 10.100.105.2 - w zależności jaki adres IP ustawiliśmy na serwerze)
Maska: 255.255.255.0
Brama: musi to być adres IP naszego serwera
DNS: musi to być adres IP naszego serwera

Gdy system zaakceptuje ustawienia poleceniem ping należy sprawdzić czy istnieje możliwości komunikacji pomiędzy konfigurowanymi systemami poleceniem ping (w konsoli należy wpisać

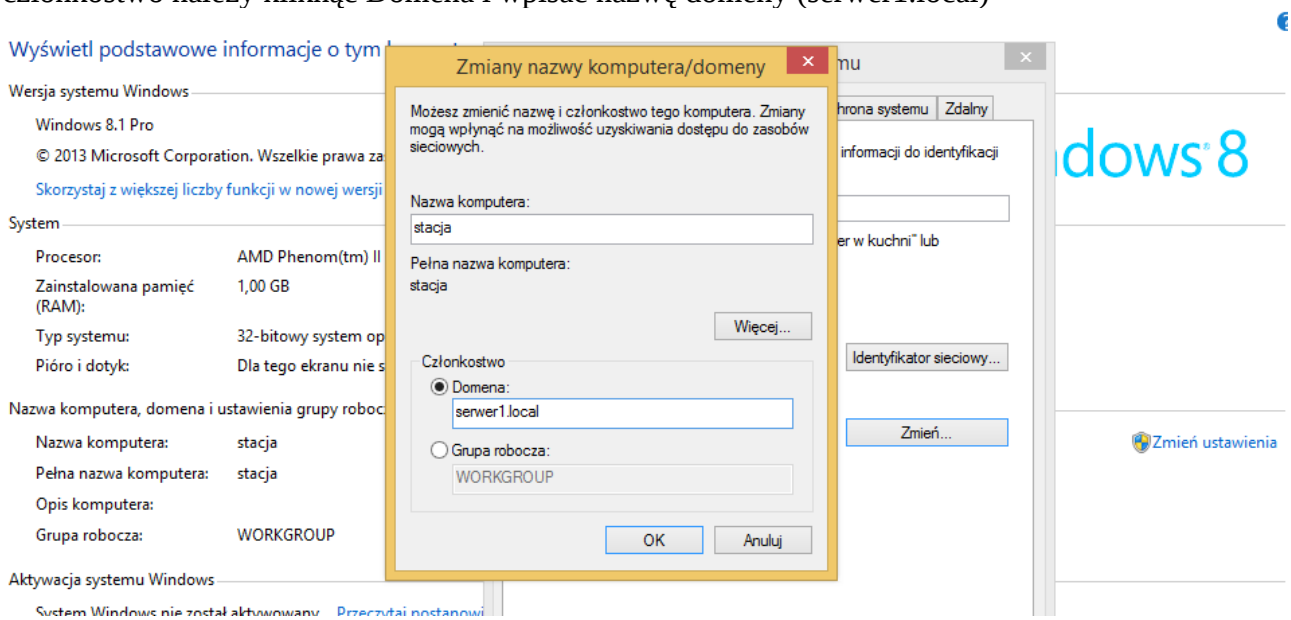
ping 10.100.100.1

(chodzi o adres IP serwera – należy zmienić na właściwy)
Jeżeli dostaniemy odpowiedź to znaczy iż sieć została skonfigurowana prawidłowo.

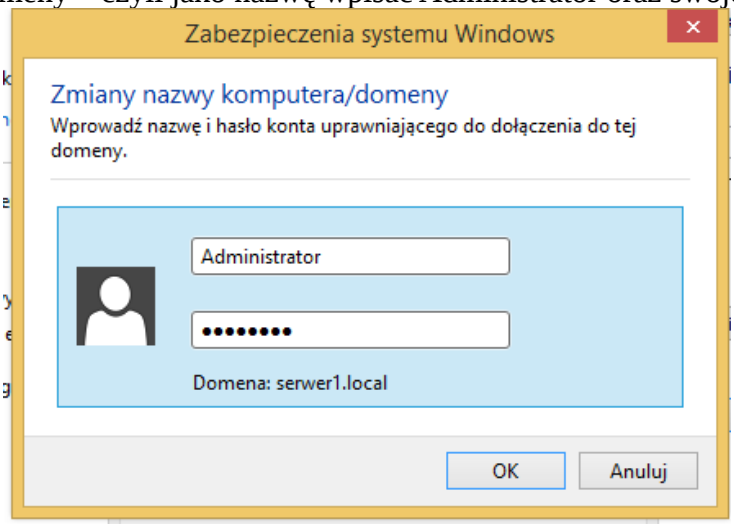
20. Kolejnym etapem jest podłączenie stacji roboczej do domeny. W tym celu najlepiej jest otworzyć na Windows 8 Eksplorator Windows, kliknąć prawym przyciskiem myszy na Ten komputer i wybrać Właściwości



21. W nowo otwartym oknie należy wybrać w polu Nazwa komputera, domena i ustawienia grupy roboczej przycisk Zmień ustawienia. W nowym oknie należy kliknąć przycisk Zmień. W sekcji członkostwo należy kliknąć Domena i wpisać nazwę domeny (serwer1.local)

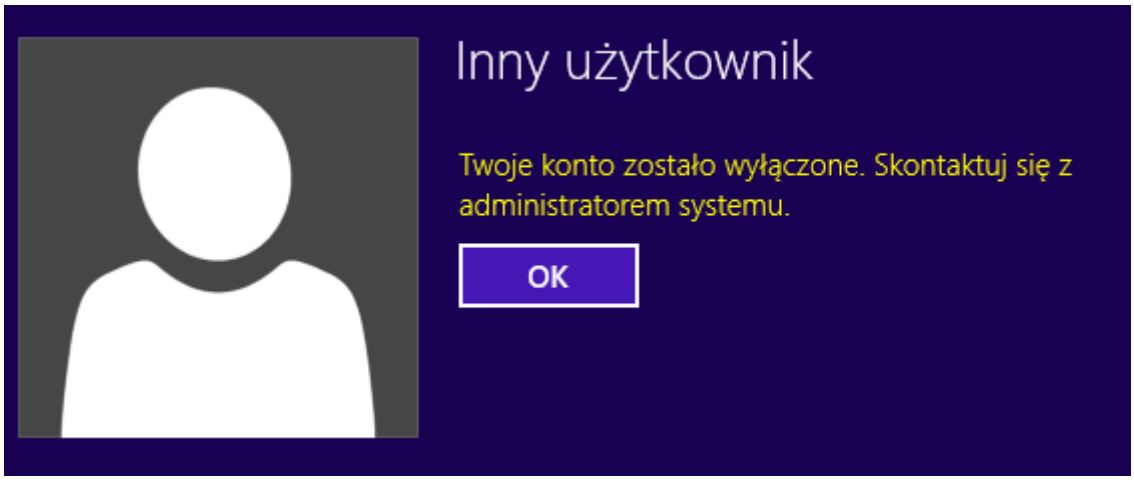


22. System zapyta nas o nazwę i hasło użytkownika domeny. Najlepiej jest się zautomatyzować jako administrator domeny – czyli jako nazwę wpisać Administrator oraz swoje hasło.



Po weryfikacji system wyświetli komunikat o dołączeniu komputera do domeny oraz o wymogu restartu. Po wykonaniu restartu będzie można zalogować się do systemu jako użytkownik user1.

UWAGA! Przy logowaniu do naszego konta może zdarzyć się, iż otrzymamy następujący komunikat:



Oznacza to, że utworzone przez nas konto NIE ZOSTAŁO WŁĄCZONE. Aby włączyć konto należy uruchomić narzędzie AD, wybrać konto utworzonego użytkownika i wybrać opcję włącz

Przy włączeniu system może poinformować nas, że nie można włączyć konta ze względu na brak hasła (nie ustawione). Wystarczy wybrać opcję Resetuj hasło... i przypisać użytkownikowi jakiekolwiek hasło. Od tego momentu będzie możliwe włączenie użytkownika.

Zadania:
1. Proszę utworzyć dodatkowe dwa konta użytkowników w systemie Active Directory.
2. Proszę wyłączyć wirtualne maszyny z Windows 8 z domeny. Następnie proszę podłączyć je pod domenę utworzoną przez inną osobę. Czy operacja powiodła się?
3. Proszę znaleźć sposób na zalogowanie się poprzez konto lokalne na maszynie, która została podłączona do domeny (odpowiedzi proszę szukać w sieci internet).