Technologia i rozwiązania

Samba 4 Przewodnik administratora

Usługi katalogowe na zawołanie!

Marcelo Leal

Helion

[PACKT] open source* PUBLISHING

Tytuł oryginału: Implementing Samba 4

Tłumaczenie: Robert Górczyński

ISBN: 978-83-246-9820-2

Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: helion@helion.pl
WWW: http://helion.pl (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie/sam4pa
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Pliki z przykładami omawianymi w książce można znaleźć pod adresem:
ftp://ftp.helion.pl/przyklady/sam4pa.zip

Printed in Poland.

Spis treści

ROZDZIAŁ 2

Użycie Samby 4 jako kontrolera domeny usługi Active Directory

W tym rozdziale poznasz podstawowe zadania, które trzeba wykonać, aby poprawnie skonfigurować usługę Active Directory opartą na serwerze Samba 4 jako kontrolerze domeny (ang. *Domain Controller*) dla sieci. Omówione zostaną następujące zagadnienia:

- Minimalne planowanie niezbędne do implementacji usługi Active Directory opartej na serwerze Samba jako kontrolerze domeny (pod uwagę trzeba wziąć domenę, topologię i adresy sieci oraz wymagane usługi). Przedstawione zostaną także podstawowe koncepcje istotne podczas konfiguracji usługi kontrolera domeny.
- Topologia sieci wykorzystywanej w przykładach przedstawionych w książce. Uwzględnione będą podstawowe techniki planowania i lista rzeczy do sprawdzenia, tak aby pokazać czytelnikowi, jak należy się przygotować i jak zebrać wszystkie informacje niezbędne do skonfigurowania Samby 4.
- Wdrożenie serwera Samba 4 i usług niezbędnych do przygotowania prawidłowej konfiguracji Samby za pomocą poleceń wydawanych w powłoce.
- Inne ważne aspekty dowolnego kontrolera domeny usługi Active Directory, między innymi dostępność, wydajność i replikacja. Wymienionymi aspektami zajmiemy się w przykładowym scenariuszu. Wyjaśnione zostaną przyjęte założenia, a także ogólne idee, które trzeba uwzględnić w rzeczywistych wdrożeniach.
- Szczegółowe omówienie użycia Samby 4 jako kontrolera domeny usługi Active Directory. Dowiesz się, jak przeprowadzić podstawową weryfikację konfiguracji oprogramowania Samba 4. To jest bardzo ważne zadanie w celu przygotowania niezawodnego środowiska gwarantującego administratorowi posiadanie w pełni funkcjonalnego, opartego na Sambie 4 kontrolera domeny usługi Active Directory.

Ważne kwestie konieczne do uwzględnienia podczas planowania usługi Active Directory

Podczas planowania funkcji kontrolera domeny usługi Active Directory najważniejszym zadaniem, na którym trzeba się skoncentrować przed przystąpieniem do wykonywania innych czynności, jest określenie topologii usług sieciowych. Jeżeli usługa Active Directory ma być niezawodna, konieczne jest przygotowanie prostej (choć czytelnej) i skalowalnej architektury spełniającej potrzeby i wymagania środowiska.

Kontroler domeny usługi Active Directory może zapewnić miejsce centralne przeznaczone do zarządzania urządzeniami sieciowymi, a tym samym pełną kontrolę nad ogromną liczbą obiektów (na przykład komputerami i użytkownikami). Kluczową kwestią jest maksymalne zmniejszenie kosztu wykonywania zadań administracyjnych, kontroli zasobów i zapewniania bezpieczeństwa (uwierzytelnianie i autoryzacja) w konkretnej sieci. Dlatego też organizacja użytkowników i zasobów w sposób ułatwiający zarządzanie nimi i jednocześnie umożliwiający łatwe skalowanie (na przykład przez ułatwienie zlecania zadań administracyjnych) ma tak istotne znaczenie. Warto pamiętać o jednym: nie ma sensu przygotowywanie kontrolera domeny w sieci, jeśli aplikacje nie będą mogły być z nim zintegrowane. Oznacza to brak możliwości użycia wszystkich funkcji i ułatwień, które może oferować kontroler domeny usług katalogowych. Opracowanie poprawnej architektury dla konkretnego środowiska to skomplikowane i obszerne zadanie, którego omówienie wykracza poza zakres tematyczny książki. Zaprezentowane będą jedynie ogólne informacje, a także przykładowe konfiguracje i topologie; możesz je wykorzystać w przyszłych implementacjach. Podobnie jak w każdej implementacji administrator musi wziąć pod uwagę użytkowników, komputery, jednostki organizacyjne, lasy, domeny i usługi.

Przedstawiona zostanie prosta, choć efektywna architektura dla użytkownika domeny `EALL.COM.BR` wraz ze strukturą ułatwiającą mu zrozumienie ważnych koncepcji. Wspomnianą architekturę czytelnik może wykorzystać jako punkt wyjścia do opracowania bardziej skomplikowanych środowisk. Ogólna rada brzmi: skoncentruj się na konkretnej topologii i wymaganiach, wyodrębnij zasadnicze koncepcje i opracuj podobne struktury, ale przeznaczone dla Twojego środowiska organizacji. Nie kopiuj *wzorcowych projektów architekturalnych* z internetu z założeniem, że w standardowej postaci będą nadawały się do użycia w Twojej sieci. Tego rodzaju projekty zwykle zawierają obsługę wszystkich działów i definicji istniejących w oprogramowaniu. Jeżeli nie potrzebujesz aż tak dużego poziomu skomplikowania, nie używaj projektów znalezionych w internecie. Spotkałem się już z wieloma środowiskami zaprojektowanymi na podstawie ogólnych reguł, które nie zostały przygotowane do użycia w konkretnych sytuacjach. Zamiast tego opracuj proste i skalowane środowiska. Znalezione w internecie **wzorcowe projekty architekturalne** najczęściej tworzą środowisko sieciowe, które jest skomplikowane i naprawdę nieefektywne w najbardziej podstawowych zastosowaniach. To całkowite przeciwieństwo doskonale zaplanowanego kontrolera domeny usługi Active Directory.

Analogią do wspomnianej nieefektywnej architektury może być na przykład struktura katalogów systemu plików. Czasami tworzymy naprawdę skomplikowaną hierarchię katalogów z wieloma podkatalogami. Prowadzi to do powstania wielu poziomów zagnieżdżeń i tak skomplikowanego drzewa katalogów, że ostateczna struktura zniechęca do użycia właściwych plików, zamiast pomagać w zapewnieniu szybkiego i łatwego dostępu do nich.

Możliwość utworzenia wielu katalogów i podkatalogów nie oznacza, że trzeba z niej korzystać dla każdego obiektu lub przygotowywać struktury zawierające setki podkatalogów — to jedynie prowadzi do zwiększenia poziomu skomplikowania. W tego rodzaju sytuacjach warto zastanowić się nad następującymi kwestiami:

- Ile plików trzeba będzie obsługiwać?
- Co chce się osiągnąć — szybkie umieszczanie plików, szybki dostęp do plików, czy też jedno i drugie?
- Czy struktura katalogów będzie bezpośrednio używana przez człowieka, czy przez aplikację?
- Czy istnieje sensowna konwencja nazw dla przechowywanych plików?
- Jeżeli nie, to czy ma się kontrolę nad zmianą nazw plików, aby tym samym zastosować sensowną konwencję nazw?
- Czy konieczne jest zarządzanie różnymi/określonymi użytkownikami i grupami dla poszczególnych katalogów i plików?
- Czy opracowana struktura pomoże w delegacji zadań administracyjnych do pewnych katalogów przeznaczonych dla konkretnych użytkowników i/lub działów?

Być może uważasz, że utworzenie struktury katalogów to proste zadanie. Jednak gdy zaczniesz głębiej się nad tym zastanawiać i analizować wymienione powyżej pytania, wtedy zdasz sobie sprawę, że opracowanie struktury katalogów wcale nie musi zaliczać się do łatwych zadań. Jeśli odpowiedzi na wymienione pytania okażą się nieprawidłowe, proste zadanie utworzenia struktury katalogów może w niedalekiej przyszłości stać się poważnym problemem. Spotkałem się już z wieloma rozwiązaniami, w których problemy związane z wydajnością lub skalowalnością (a nawet zapewnieniem bezpieczeństwa) pojawiały się tylko dlatego, że twórca rozwiązania nie zadał sobie trudu udzielenia odpowiedzi na wymienione pytania.

Podobne pytania związane z projektowaniem rozwiązania pojawiają się podczas planowania usługi Active Directory dla sieci. Odpowiedzi na pytania dotyczące prostych zadań, takich jak np. tworzenie struktury katalogów w systemie plików, mogą pomóc w podjęciu odpowiednich decyzji podczas rozwiązywania różnych problemów architekturalnych. Doskonale zaprojektowane systemy charakteryzują się tymi samymi zasadami i są oparte na tych samych, doskonale znanych cechach charakterystycznych z zakresu skalowalności, wydajności, zapewniania bezpieczeństwa i prostej administracji.

Powróćmy do usługi Active Directory i jej architektury. Ogólnie rzecz biorąc, pod uwagę należy wziąć trzy wymienione podstawowe koncepcje: las (ang. *forest*), domenę i jednostkę organizacyjną. Las to najwyższa warstwa abstrakcji usługi Active Directory. Zapewnia bezpieczeństwo i zawiera jedną lub więcej domen.

Domena to część (partycja) lasu. Może zawierać jedną lub więcej tak zwanych *jednostek organizacyjnych* (ang. *organizational units*). Wspomniane jednostki organizacyjne to encje grupujące różne obiekty (na przykład użytkowników i/lub komputery) w celu łatwej administracji tymi elementami w skalowalny sposób (na przykład ułatwienie zlecania zadań administracyjnych).

Według terminologii używanej w przygotowanej przez Microsoft dokumentacji usługi Active Directory głównym zadaniem lasu jest implementacja kontroli bezpieczeństwa w środowisku usługi Active Directory. Domena zapewnia punkt administracyjny, w którym można kierować replikacją, a tym samym nawiązywaniem zaufanych relacji. Jednostki organizacyjne są punktami administracyjnymi pozwalającymi na zlecanie zadań administracyjnych, a tym samym zapewniają nieocenioną możliwość podziału obowiązków administracyjnych między całą organizację (źródło: *http://technet.microsoft.com/pl-pl/library/cc756901(v=ws.10).aspx*). To jest bardzo ważny aspekt skalowalności, ponieważ pracownicy (a zwłaszcza administratorzy) to ważny i jednocześnie najdroższy zasób w firmie. Opracowując architekturę, trzeba wziąć to pod uwagę już od samego początku prac.

Omówiona tutaj przykładowa konfiguracja będzie używała prostego modelu lasu. Wspomniany las to najprostszy model wraz z najmniejszym obciążeniem administracyjnym, a ponadto doskonale pasuje do naszych wymagań. Na pewno spotkasz się z sytuacjami, w których konieczne będzie przygotowanie wielu modeli lasu. W takich przypadkach należy przygotować projekt zawierający wspomniane modele lasu. Jeżeli organizacja nie ma skomplikowanych wymagań (na przykład zupełnie autonomicznych oddziałów), wówczas preferowane jest użycie pojedynczego modelu lasu.

W tworzonej tutaj implementacji domena główna lasu (ang. *forest root domain*) to `MSDCBRZ.EALL.COM.BR`; będziemy pracować tylko z jedną lokacją (domena potomna) o nazwie `POA.MSDCBRZ.EALL.COM.BR`. Istnieje wiele różnych podejść w zakresie przygotowania jednostek organizacyjnych. Wynika to z faktu, że administratorzy mają odmienne punkty widzenia na strukturę, ponieważ poszczególne jednostki organizacyjne mają różne potrzeby.

Rozpoczniemy od 10 jednostek organizacyjnych i zastosujemy model, który praktycznie oddziela stacje robocze, usługi i użytkowników, czyli trzy ważne obiekty wymagające obsługi w dowolnej usłudze katalogowej. Dzięki nim implementacja poszczególnych polityk i administrowanie nimi w przyszłości staną się łatwiejsze.

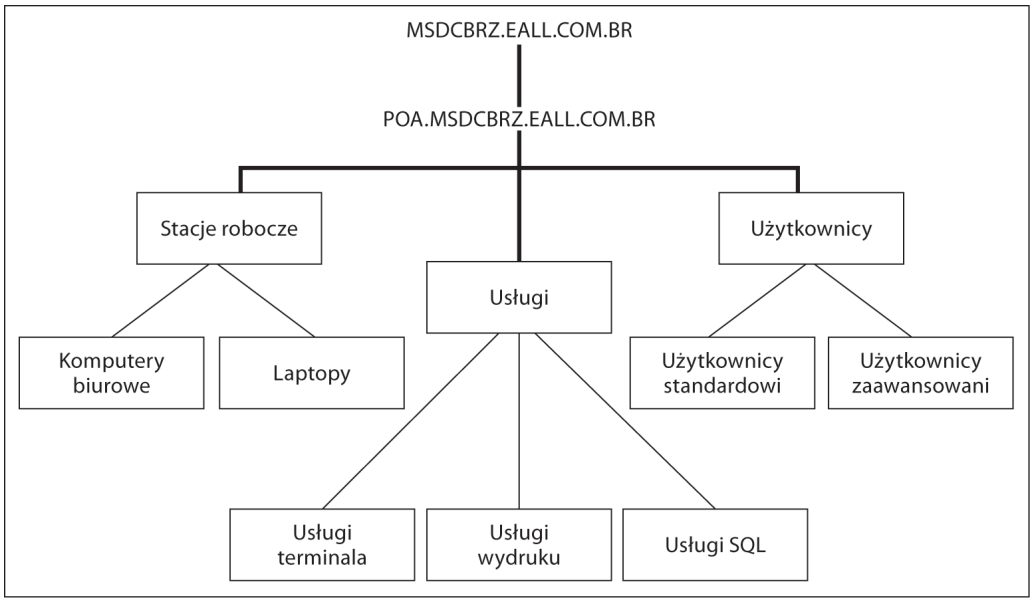
Pobieranie przykładowych fragmentów kodu

Przykładowe fragmenty kodu możesz pobrać dla wszystkich książek kupionych w witrynie *http://www.packtpub.com/*. W tym celu zaloguj się do swojego konta w Packt. Jeżeli książkę kupiłeś gdzie indziej, wówczas przejdź na stronę *http://www.packtpub.com/support* i zarejestruj książkę. Po rejestracji książki otrzymasz wiadomość e-mail wraz z łączem pozwalającym na pobranie plików.

Struktura będzie posiadała trzy jednostki organizacyjne najwyższego poziomu, którymi są stacje robocze, usługi i użytkownicy. Jednostka organizacyjna przeznaczona dla **stacji roboczych** obsługuje różne rodzaje urządzeń, z których będą korzystali użytkownicy. Do wspomnianych urządzeń zaliczamy między innymi komputery biurowe i laptopy. Takie rozdzielenie urządzeń jest bardzo ważne — trzeba identyfikować obsługę używanych przez użytkowników urządzeń mobilnych, ponieważ mają one inne wymagania w zakresie zapewniania bezpieczeństwa. Konfiguracja zależy na przykład od tego, czy użytkownicy przez cały czas korzystają z sieci korporacyjnej i czy używają laptopów poza firmą. Na początek jednostka organizacyjna przeznaczona dla **usług** będzie zapewniała obsługę tylko trzech usług (terminala, wydruku i SQL). Ta liczba na pewno się zwiększy wraz z instalacją kolejnych. Pamiętaj: jeśli usługi sieciowe nie są zintegrowane i nie pozwalają na korzystanie z usług katalogowych, to nie ma zbyt dużego sensu implementowanie usług katalogowych i centralne zarządzanie nimi.

Ostatnia jednostka organizacyjna najwyższego poziomu jest poświęcona **użytkownikom** i składa się z dwóch kolejnych jednostek: dla użytkowników standardowych i zaawansowanych. Jest to podział prosty i jednocześnie wystarczający do administracji siecią.

Na rysunku 2.1 pokazano omówioną strukturę usługi Active Directory.



Rysunek 2.1. Tworzona tutaj struktura usługi Active Directory

Informacje niezbędne do wdrożenia usługi Active Directory

W celu ułatwienia sobie pracy warto wcześniej przygotować wszystkie informacje niezbędne podczas wdrażania usługi Active Directory w sieci. Dobrym rozwiązaniem jest przygotowanie odpowiedniej listy jeszcze przed przystąpieniem do wdrażania usługi. W oparciu o przedstawione wcześniej informacje dokładnie znamy potrzeby, sposób zdefiniowania topologii oraz implementacji sieci. Wspomniane dane pozwalają więc na utworzenie dokumentu zawierającego potrzebne informacje, a sam dokument ułatwi identyfikację punktów, które pominięto w trakcie opracowywania projektu. W tabeli 2.1 wymieniono informacje, które należy zebrać przed rozpoczęciem implementacji usługi Active Directory za pomocą Samby 4. Tabela została przygotowana w taki sposób, aby ułatwić czytelnikowi zrozumienie i odszukanie informacji podczas fazy konfiguracji usługi Active Directory. Gdy będzie się miało wcześniej przygotowane niezbędne informacje, proces konfiguracji usługi stanie się jasny i prosty. Na etapie planowania możesz więc zebrać jak najwięcej informacji. Przedstawiona tabela może być pomocna i służyć w charakterze punktu wyjścia podczas organizacji danych.

Tabela 2.1. Lista rzeczy do zrobienia w zakresie konfiguracji usług katalogowych opartych na Sambie 4

Pytanie lub parametr	Odpowiedź lub wartość
Rola	`Kontroler domeny`
Czy istnieje już infrastruktura DNS?	`( x ) Tak ( ) Nie`
Adres IP usługi Active Directory i interfejs	`192.168.1.1 (eth1)`
Liczba jednostek organizacyjnych	`10`
Lokacje/miejsca fizyczne	`1`
Liczba kontrolerów domeny	`1`
Domena	`POA.MSDCBRZ.EALL.COM.BR`
Konfiguracja DNS	`Przekazywanie (IP: 8.8.8.8)`
Adres IP serwera DHCP	`192.168.1.1`
Adres IP routera domyślnego	`192.168.1.1`
Liczba użytkowników	`50`

Jak wyjaśniono w rozdziale 1., aby zapewnić obsługę pełnych możliwości Samby, usługa Active Directory w Sambie 4 wykorzystuje także inne ważne funkcje. Samba 4 posiada wbudowany serwer DNS, który okazuje się wystarczający dla wielu instalacji. W omawianym tutaj projekcie również z niego skorzystamy. Jednak wymagane jest również użycie **protokołu NTP** (ang. *Network Time Protocol*), ponieważ zegary we wszystkich systemach znajdujących się w sieci muszą być zsynchronizowane. Wspomniana synchronizacja ma jeszcze większą wagę dla uwierzytelniania za pomocą mechanizmu Kerberos. **DHCP** to kolejna niezbędna usługa; zapewnia administratorom sieci łatwy sposób dynamicznej konfiguracji nowych komputerów w sieci

(na przykład przypisanie im adresów IP), a także rejestrację nowych maszyn w serwerze DNS (to ma istotne znaczenie dla usługi Active Directory). Wszystkie usługi wymienione w tabeli 2.1 są już skonfigurowane w systemie Debian, który przygotowaliśmy w rozdziale 1. Konfiguracja usług stanowiła część procedury instalacyjnej serwera Samba 4.

Dostępność, wydajność i replikacja usługi sieciowej

Podczas planowania jakiejkolwiek usługi sieciowej od samego początku konieczne jest uwzględnienie kwestii związanych z jej dostępnością i wydajnością, ponieważ usługa pozbawiona dwóch wymienionych cech charakterystycznych jest po prostu nieużyteczna. To dotyczy również kontrolera domeny usługi Active Directory, która dostarcza podstawowych funkcji całej domenie. Jeżeli usługa okaże się niedostępna, w rezultacie użytkownicy nie będą mogli nawiązać połączenia z siecią, serwery nie będą potrafiły wyszukać komputerów w sieci itd. Tworzona przez nas lista rzeczy do sprawdzenia wymienia ogólne informacje, które pomogą w udzieleniu odpowiedzi na pewne ważne pytania dotyczące dostępności i wydajności. Dlatego też przygotowanie dobrze udokumentowanego planu znacznie ułatwia późniejsze wdrożenie usługi. Wielkość i architektura usługi Active Directory zależą od konkretnego środowiska wdrożeniowego, ale to wykracza poza zakres tematyczny książki. W internecie znajdziesz wiele artykułów przedstawiających różne aspekty projektów charakteryzujących się skalowalnością, wysoką dostępnością i wydajnością. Podczas rozważania kwestii związanych z wydajnością i replikacją trzeba koniecznie zwrócić uwagę na kilka ważnych elementów:

- liczbę użytkowników,
- liczbę domen,
- fizyczne położenie danej lokacji.

Wymienione punkty to jedynie kilka przykładów parametrów, które będą miały ogromny wpływ na obciążenie *serwera usługi Active Directory*. Warto pamiętać, że istnieją również inne ważne parametry. Im więcej informacji uda Ci się zebrać na etapie planowania, tym łatwiej będzie zaplanować zasoby niezbędne do zapewnienia odpowiedniej wydajności w danym środowisku.

Dobrym przykładem innego rodzaju informacji, które można umieścić na wspomnianej wcześniej liście rzeczy do sprawdzenia, jest rysunek 2.1 pokazujący schemat tworzonej usługi Active Directory. Usługi, które mają być oferowane w domenie oraz współpracują z usługą Active Directory, będą generowały obciążenie (zapytania DNS, obsługa uwierzytelniania itd.). Dlatego też stanowią czynniki wydajności konieczne do uwzględnienia na etapie planowania. W omawianym tutaj przykładzie mamy zaledwie kilku użytkowników i niewiele usług, więc serwer z pewnością poradzi sobie z obsługą obciążenia. Ponieważ istnieje tylko jedno miejsce (lokacja) i jedna domena, nie ma obaw związanych z wydajnością podczas replikacji bazy danych usługi Active Directory. Kiedy analizujemy dostępność, nie istnieje coś takiego jak małe środowisko i nie można sobie pozwolić na brak redundancji (zapewnienie wysokiej dostępności) naszych usług. W rozdziale 4. przeczytasz, jak zapewnić redundancję w tworzonym środowisku oraz jak zapewnić wysoką dostępność usługi Active Directory.

Konfiguracja Samby 4 jako kontrolera domeny usług katalogowych

Jedną z ważniejszych zmian konfiguracyjnych, dzięki której znacznie ułatwimy sobie pracę, jest dodanie ścieżki dostępu do katalogu, w którym zainstalowano Sambę 4, do zmiennej `PATH` w pliku *.bash_profile*. W ten sposób podczas pracy z narzędziami Samby 4 nie trzeba będzie podawać pełnej (bezwzględnej) ścieżki dostępu. W powłoce wydaj przedstawione poniżej polecenie:

```
leal@debian7:~$ sudo echo 'export PATH=/usr/local/samba/bin:\
➥/usr/local/samba/sbin:$PATH' >> /root/.bash_profile && echo OK
```

Dane wyjściowe powyższego polecenia powinny zawierać komunikat `OK`. To będzie sygnał świadczący o udanej modyfikacji pliku *.bash_profile*, polegającej na dodaniu katalogu zawierającego Sambę 4 do listy katalogów sprawdzanych po wydaniu polecenia w powłoce.

Po spełnieniu wszystkich wymagań stawianych przez środowisko Samby 4 oraz po sprawdzeniu zainstalowanego oprogramowania konfiguracja Samby 4 do działania w charakterze usługi Active Directory jest prostym zadaniem. W tym celu wystarczy wydać poniższe polecenie:

```
leal@debian7:~$ sudo samba-tool domain provision --realm=POA.MSDCBRZ.EALL.COM.BR --
➥domain=POA --adminpass='w1ndow$$!' --server-role='domain controller'
```

Polecenie `samba-tool` może być uruchomione w trybie interaktywnym przez użycie argumentów `domain provision`. Następnie trzeba będzie udzielać odpowiedzi na poszczególne pytania (na przykład `domain`, `adminpass` itd.). Jednym z celów książki jest zaprezentowanie czytelnikom jak największej liczby zautomatyzowanych procedur i prostych skryptów. Narzędzie `samba-tool` zostało wywołane bezpośrednio wraz z wszystkimi poleceniami i argumentami. W ten sposób konfiguracja serwera Samba 4 jest przeprowadzana bez konieczności prowadzenia dalszej interakcji.

> Jeżeli chcesz ponownie wykonać przedstawione polecenie `samba-tool`, konieczne będzie wcześniejsze usunięcie pliku konfiguracyjnego *smb.conf*. W przeciwnym razie wystąpi błąd i działanie polecenia zostanie przerwane. Wymieniony plik konfiguracyjny możesz usunąć za pomocą polecenia `sudo rm /usr/local/samba/etc/smb.conf`.

Przyjrzymy się teraz poleceniu `samba-tool` i wyjaśnimy użyte argumenty. Dzięki temu będziesz doskonale rozumiał sposób działania poszczególnych opcji, co pozwoli na ich dostosowanie do własnych potrzeb. W wydanym poleceniu użyto następujących argumentów:

- `samba-tool` — to podstawowe narzędzie administracyjne Samby.
- `domain provision` — to argument, w którym `domain` stanowi podpolecenie narzędzia `samba-tool` odpowiedzialne za zadania zarządzania domeną, natomiast `provision` oznacza podpolecenie faktycznie konfigurujące domenę. To podstawowa część wydanego polecenia `samba-tool` i zapewnia możliwość konfiguracji domeny.

- `--realm` — to wartość realm.
- `--domain` — to nazwa domeny.
- `--adminpass` — to hasło administracyjne. (Jeżeli nie zostanie zdefiniowane, Samba wygeneruje losowe hasło). Zdefiniowanie hasła to ważny etap podczas konfiguracji Samby 4, ponieważ w usłudze Active Directory istnieje ściśle określona polityka dotycząca haseł (tzw. **Microsoft Windows Password Policies**). W przypadku podania niewystarczająco silnego hasła otrzymasz komunikat błędu i polecenie trzeba będzie wykonać ponownie. Hasło użyte w przykładzie jest proste i choć uwzględniono w nim zasady wspomnianej polityki, to jednak *nie* jest przeznaczone do użycia w środowiskach produkcyjnych.

Argument `--server-role` wskazuje na konieczność użycia silnego hasła dla instalacji. Ponieważ przeprowadzamy konfigurację kontrolera domeny usługi Active Directory, wartością omawianego argumentu jest `domain controller`. Jednak dostępne są także inne opcje, między innymi `dc`, `member server`, `member` i `standalone`. W przypadku pominięcia argumentu domyślnie użyta zostanie opcja `server-role`.

> Listę wszystkich dostępnych opcji możesz wyświetlić, po prostu wydając polecenie `samba-tool` bez żadnych argumentów. Ewentualnie zajrzyj na stronę podręcznika systemowego `man` dla omawianego narzędzia (`man samba-tool`).

Po wydaniu wcześniej przedstawionego polecenia przeznaczonego do konfiguracji serwera Samba 4 jako usługi Active Directory sprawdź dane wyjściowe i upewnij się, że wykonanie polecenia przebiegło zgodnie z oczekiwaniami. Poniżej przedstawiono przykładowe dane wyjściowe otrzymane po wydaniu omawianego polecenia:

```
Looking up IPv4 addresses
More than one IPv4 address found. Using 192.168.1.1
Looking up IPv6 addresses
No IPv6 address will be assigned
Setting up share.ldb
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
Adding DomainDN: DC=poa,DC=msdcbrz,DC=eall,DC=com,DC=br
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
```

```
Modifying display specifiers
Adding users container
Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=poa,DC=msdcbrz,DC=eall,\
C=com,DC=br
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
A Kerberos configuration suitable for Samba 4 has been generated
 at /usr/local/samba/private/krb5.conf
Once the above files are installed, your Samba 4 server will be
 ready to use
Server Role:      active directory domain controller
Hostname:         debian7
NetBIOS Domain:   POA
DNS Domain:       poa.msdcbrz.eall.com.br
DOMAIN SID:       S-1-5-21-1069074877-2280341390-3609431641
```

Wyświetlone dane wyjściowe zawierają pewne informacje o poszczególnych krokach konfiguracji serwera Samba 4. Na podstawie tych komunikatów możemy dowiedzieć się o ustawieniu określonych zasobów, o utworzeniu pewnych kontenerów domyślnych i użytkowników, o grupach oraz konfiguracji DNS.

Ostatnie wiersze zawierają pewne użyteczne informacje: nazwę domeny i jej wartość SID. W tych wierszach znajdują się również ważne informacje dotyczące pliku konfiguracyjnego Kerberos, który został wygenerowany automatycznie. Te informacje będą potrzebne do zakończenia konfiguracji serwera Samba 4. Plik konfiguracyjny Kerberos trzeba umieścić w odpowiednim katalogu, co następuje po wydaniu polecenia:

```
lеal@debian7:~$ su – root
Password:
root@debian7:~# cp -pRf /usr/local/samba/private/krb5.conf /etc/ && echo OK
OK
root@debian7:~# exit
lеal@debian7:~$
```

Jeżeli dane wyjściowe zawierają komunikat `OK`, oznacza to, że plik konfiguracyjny Kerberos został skopiowany do odpowiedniego katalogu. Teraz trzeba przeprowadzić edycję pliku *smb.conf* i skonfigurować serwer DNS, którego serwer Samba będzie używał do przekazywania wszystkich zapytań DNS spoza strefy autorytatywnej. W omawianym przykładzie wykorzystujemy serwery DNS udostępniane przez Google, ale w rzeczywistym wdrożeniu powinieneś podać

adres własnego serwera DNS. Przed edycją pliku *smb.conf* spójrz na jego zawartość, ponieważ przekazywanie adresów IP mogło zostać skonfigurowane automatycznie przez `samba-tool` i nie będziesz musiał wprowadzać żadnych zmian.

Jeżeli trzeba wprowadzić zmiany, poniższy skrypt zajmie się tym automatycznie:

```
leal@debian7:~$ sudo cp -pRf /usr/local/samba/etc/smb.conf
  /usr/local/samba/etc/smb.conf-bkp && sed -e 's/dns forwarder =.*$/dns
  forwarder = 8.8.8.8/g' /usr/local/samba/etc/smb.conf >
  /usr/local/samba/etc/smb.conf-new && mv
  /usr/local/samba/etc/smb.conf-new /usr/local/samba/etc/smb.conf && echo OK
OK
leal@debian7:~$
```

Jeżeli dane wyjściowe zawierają komunikat `OK`, oznacza to, że edycja pliku *smb.conf* zakończyła się powodzeniem i jesteśmy gotowi do uruchomienia serwera Samba 4. W przypadku wystąpienia błędu nie należy wprowadzać żadnych zmian w oryginalnym pliku konfiguracyjnym Samby. Jeśli jednak wprowadzono zmiany i nastąpiło wygenerowanie błędu, oznacza to, że operacja edycji pliku zakończyła się niepowodzeniem. Trzeba wówczas przywrócić oryginalny plik konfiguracyjny Samby z kopii zapasowej utworzonej na początku skryptu. Dlatego też warto zachować plik *smb.conf.bkp* wraz z oryginalną konfiguracją Samby — tak na wszelki wypadek.

Teraz można uruchomić serwer Samba 4, aby działał w tle. Serwer powinien być jednowątkowy, aby umożliwiać identyfikację wszelkich błędów lub ostrzeżeń powodowanych przez oprogramowanie w kolejnych wykonywanych przez nas krokach. Przeprowadzimy więc serię testów i operacji weryfikacji, aby upewnić się, że przygotowana tutaj konfiguracja jest gotowa do użycia w środowisku produkcyjnym. W oknie terminala wydaj polecenie:

```
leal@debian7:~$ sudo /usr/local/samba/sbin/samba -i -M single
Password:
```

Jeżeli zainstalowane oprogramowanie Samba 4 i konfiguracja nie zawierają żadnych błędów i nie powodują problemów, powinieneś otrzymać następujące dane wyjściowe:

```
samba version 4.0.5 started.
Copyright Andrew Tridgell and the Samba Team 1992-2012
samba: using 'single' process model
Attempting to autogenerate TLS self-signed keys for https for  hostname 'DEBIAN7.
↪poa.msdcbrz.eall.com.br'
TLS self-signed keys generated OK
```

Powinieneś zauważyć, że proces Samby został powiązany z powłoką, a nie rozwidlony. Wyświetlony komunikat wskazuje na użycie opcji `single` jako modelu procesu, co się zgadza, ponieważ demona uruchomiliśmy wraz z opcją `-M single`. W ten sposób ułatwimy sobie pracę podczas debugowania i wyszukiwania komunikatów ewentualnych błędów — mamy tylko jeden proces przeznaczony do obsługi Active Directory. Nie występuje więc ryzyko przeoczenia komunikatu z powodu analizy niewłaściwego procesu.

Weryfikacja konfiguracji Samby 4

Po zainstalowaniu i skonfigurowaniu serwera Samba 4 przeprowadzimy podstawową weryfikację, aby upewnić się, że przygotowane środowisko można zastosować w produkcji. Testy będą związane z zapytaniami DNS, uwierzytelnianiem Kerberos, a także pewnymi podstawowymi możliwościami w zakresie obsługi żądań i udzielania odpowiedzi przez nasz nowy serwer.

Jak wspomniano w rozdziale 1. i jak to będzie powtarzane w całej książce, zawsze warto opracować zautomatyzowaną procedurę testową przeznaczoną do weryfikacji środowiska. Gorąco zachęcam więc do rozpoczęcia tworzenia skryptów przeprowadzających testy konfiguracji Samby 4 dla przyszłych instalacji, uaktualnień i obsługi bazy danych. Opracowanie zestawu testów i procedur weryfikacyjnych ma kluczowe znaczenie podczas wprowadzania jakichkolwiek zmian w środowisku. Może również pomóc w wychwytywaniu problemów przed wdrożeniem instalacji w środowisku produkcyjnym, a także pozwoli na wycofanie modyfikacji i powrót do fazy planowania.

Rozpoczniemy od testów DNS, ponieważ prawidłowe działanie serwera DNS ma istotne znaczenie dla poprawnego działania usługi Active Directory (patrz odwołanie [13] w dodatku A). Jeżeli wystąpią jakiekolwiek problemy z konfiguracją, będziesz miał możliwość ich wcześniejszego rozwiązania. Usługa Active Directory używa rekordu **SRV** do zlokalizowania kontrolerów domeny, ponieważ wspomniany rekord jest stosowany do identyfikacji serwerów oferujących określone usługi. Dla kontrolera domeny Active Directory konieczne jest utworzenie dwóch rekordów SVR: `_kerberos` i `_ldap`. Konieczne jest upewnienie się, że system posiada wymienione rekordy, co pozwoli klientom na komunikację z serwerem i wykrywanie usług dostępnych w sieci. W nowej powłoce wykonaj następujące polecenia:

```
leal@debian7:~$ host -t SRV _kerberos._udp.poa.msdcbrz.eall.com.br
_kerberos._udp.poa.msdcbrz.eall.com.br has SRV record 0 100 88 debian7. poa.
↪msdcbrz.eall.com.br.
leal@debian7:~$ host -t SRV _ldap._tcp.poa.msdcbrz.eall.com.br
_ldap._tcp.poa.msdcbrz.eall.com.br has SRV record 0 100 389 debian7.poa.
↪msdcbrz.eall.com.br.
leal@debian7:~$ host -t A poa.msdcbrz.eall.com.br
poa.msdcbrz.eall.com.br has address 192.168.1.1
```

W Twoim środowisku po wydaniu powyższych poleceń powinieneś otrzymać podobne dane wyjściowe. W przypadku wystąpienia błędu wskazującego na nieznalezienie rekordów konieczne jest przejrzenie procesu konfiguracji i upewnienie się o prawidłowym wykonaniu poszczególnych kroków. Jak można się przekonać na podstawie danych wyjściowych poleceń, rekordy SVR dla `_ldap` i `_kerberos` zostały skonfigurowane prawidłowo.

Inna ważna kwestia dotycząca konfiguracji DNS to zdefiniowanie przekazywania — aby w ten sposób zapewnić sobie możliwość ustalania nazw, dla których nasza usługa Active Directory nie jest autorytatywna. Konfigurację można przetestować, wykorzystując pewne doskonale znane witryny internetowe. Oto niezbędne kroki:

1. Wykonanie następującego polecenia w powłoce:

```
leal@debian7:~$ host www.amazon.com
```

Wygenerowane dane wyjściowe powinny być podobne do poniższych:

```
www.amazon.com has address 72.21.215.232
```

2. Teraz można podjąć próbę określenia rekordu MX dla domeny `amazon.com`. W tym celu z poziomu powłoki należy wydać polecenie:

```
leal@debian7:~$ host -t mx amazon.com
```

Dane wyjściowe powinny być podobne do następujących:

```
amazon.com mail is handled by 5 amazon-smtp.amazon.com.
amazon.com mail is handled by 10 smtp-fw-4101.amazon.com.
amazon.com mail is handled by 10 smtp-fw-9101.amazon.com.
amazon.com mail is handled by 10 smtp-fw-31001.amazon.com.
amazon.com mail is handled by 10 smtp-fw-33001.amazon.com.
amazon.com mail is handled by 15 smtp-fw-2101.amazon.com.
```

Dzięki przeprowadzonym testom można potwierdzić, że serwer DNS wbudowany w usługę Active Directory działa prawidłowo, poprawie określa nazwy DNS dla naszej domeny (`poa.msdcbrz.eall.com.br`) i przekazuje żądania dla innych domen. Zweryfikowaliśmy także rekordy SVR `_kerberos` i `_ldap` i możemy przystąpić do przetestowania mechanizmu uwierzytelniania Kerberos.

3. W celu przetestowania mechanizmu uwierzytelniania Kerberos można wykorzystać polecenie `kinit`. Wymienione narzędzie potrafi pobrać i buforować bilet dostępu Kerberos (patrz strona podręcznika wyświetlana po wydaniu polecenia `man kinit`). Najprostsza forma wywołania `kinit` i przetestowania konfiguracji Samby 4 to wykonanie poniższego polecenia:

```
leal@debian7:~$ kinit administrator@POA.MSDCBRZ.EALL.COM.BR
```

4. Powinieneś otrzymać następujące dane wyjściowe:

```
Password for administrator@POA.MSDCBRZ.EALL.COM.BR:
```

5. Musisz w tym momencie podać hasło administratora i nacisnąć klawisz *Enter*. Wyświetlone dane wyjściowe będą miały postać komunikatu ostrzeżenia:

```
Warning: Your password will expire in 41 days on Sat Jul 13 19:22:46 2013
```

6. Teraz można użyć polecenia `klist` w celu potwierdzenia rzeczywistego otrzymania biletu oraz prawidłowego działania mechanizmu uwierzytelniania Kerberos:

```
leal@debian7:~$ klist
```

7. Dane wyjściowe polecenia `klist` powinny być podobne do przedstawionych poniżej:

```
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: administrator@POA.MSDCBRZ.EALL.COM.BR

Valid starting     Expires            Service principal
06/02/13 02:09:59  06/02/13 12:09:59  krbtgt/POA.MSDCBRZ.EALL.COM.BR
   @POA.MSDCBRZ.EALL.COM.BR
      renew until 06/03/13 02:09:54
```

Jeżeli otrzymasz dane wyjściowe podobne do przedstawionych, oznacza to, że mechanizm uwierzytelniania Kerberos działa prawidłowo.

Kolejna operacja weryfikacji jest związana z serwerem `ldap` w kontrolerze domeny usługi Active Directory zbudowanej w oparciu o Sambę 4. Do wykonywania zapytań względem usługi Active Directory i potwierdzenia jej prawidłowego działania można wykorzystać narzędzie `ldapsearch`. Pierwsze zapytanie będzie miało postać następującego polecenia:

```
leal@debian7:~$ ldapsearch -x -h localhost -s base -D  cn=administrator,
↪cn=Users,dc=poa,dc=msdcbrz,dc=eall,dc=com,dc=br -W
```

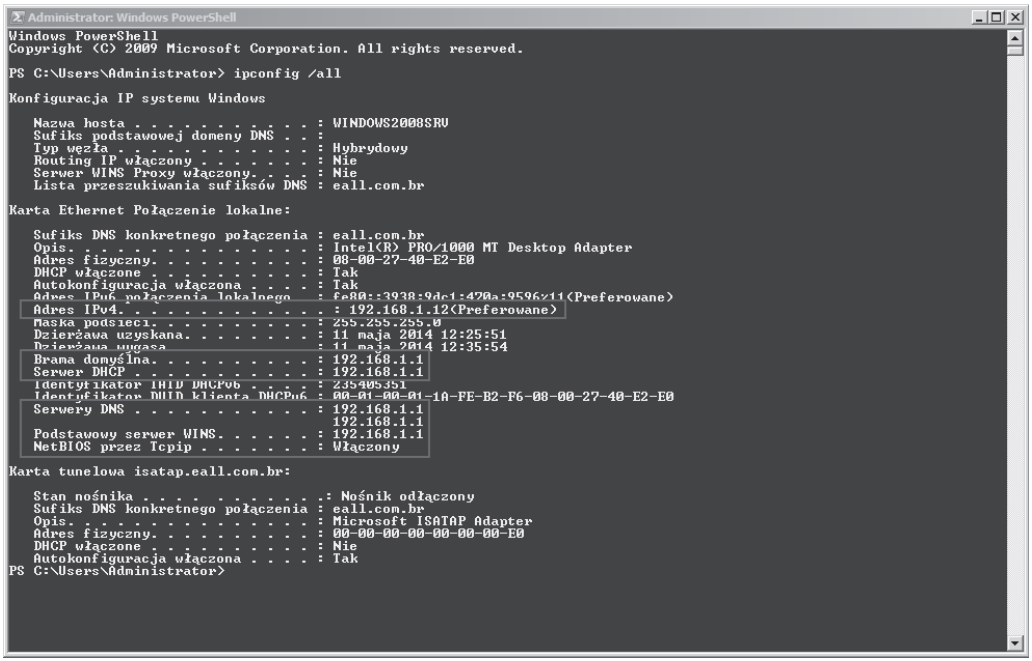
Zostaniesz poproszony o podanie hasła administracyjnego LDAP, a następnie na ekranie będą wyświetlone obszerne dane wyjściowe. W celu zachowania zwięzłości poniżej przedstawiono jedynie kilka ostatnich wierszy danych wyjściowych:

```
namingContexts: DC=DomainDnsZones,DC=poa,DC=msdcbrz,DC=eall,DC=com,DC=br
namingContexts: DC=ForestDnsZones,DC=poa,DC=msdcbrz,DC=eall,DC=com,DC=br
supportedSASLMechanisms: GSS-SPNEGO
supportedSASLMechanisms: GSSAPI
supportedSASLMechanisms: NTLM
highestCommittedUSN: 3723
domainFunctionality: 2
forestFunctionality: 2
domainControllerFunctionality: 4
isGlobalCatalogReady: TRUE

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

Jeżeli po wydaniu polecenia `ldapsearch` otrzymałeś dane wyjściowe podobne do przedstawionych, oznacza to, że `ldap` w usłudze Active Directory działa prawidłowo.

Ostatni i najważniejszy krok to rzeczywiste przetestowanie komputera działającego pod kontrolą systemu operacyjnego Microsoft Windows i próba jego dodania do naszej nowej domeny. W omawianym przykładzie wykorzystamy system operacyjny Windows Server 2008 R2. Po dołączeniu komputera do domeny użyjemy go do utworzenia jednostek organizacyjnych w kontrolerze domeny usługi Active Directory.

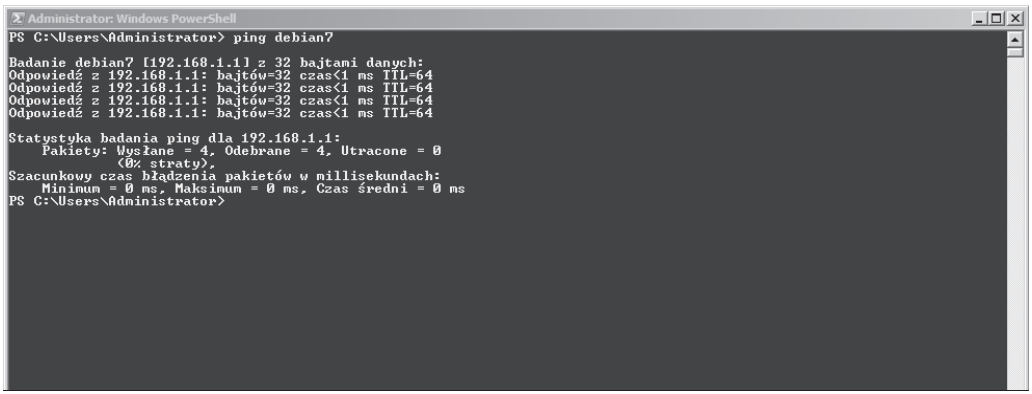
Po zainstalowaniu Microsoft Windows Server 2008 R2 można sprawdzić, czy system pobiera adres IP z przygotowanego serwera DHCP. W tym celu wykonaj szybki test (na przykład za pomocą polecenia `ping`), aby upewnić się, że konfiguracja sieci działa zgodnie z oczekiwaniami. Za pomocą wiersza poleceń PowerShell możesz wydać polecenie `ipconfig /all` (patrz rysunek 2.2) i sprawdzić konfigurację sieci (spójrz na przykład na wiersze `Adres IPv4`, `Serwery DNS`, `Brama domyślna` itd.).



Rysunek 2.2. Sprawdzenie konfiguracji sieci w wierszu poleceń PowerShell

Na rysunku 2.2 widać, że system Windows Server 2008 pobrał adres IP (`192.168.1.12`). Dane w wierszach `Serwer DHCP`, `Adres IPv4`, `Podstawowy serwer WINS`, `Serwery DNS` i `Brama domyślna` pochodzą z przygotowanego przez nas wcześniej kontrolera domeny usługi Active Directory (jego adres IP to `192.168.1.1`).

Aby upewnić się, że system jest w stanie uzyskać dostęp do usługi Active Directory (serwer Samba 4), warto przeprowadzić test za pomocą polecenia `ping`, jak pokazano na rysunku 2.3.



Rysunek 2.3. Sprawdzenie dostępności serwera Samba 4 za pomocą polecenia ping

Jak możesz zobaczyć na wcześniejszych rysunkach, nie wystąpiły żadne problemy z nawiązaniem połączenia z serwerem usługi Active Directory (system Debian 7). Przeprowadzony test pozwolił na weryfikację konfiguracji serwera DNS — sprawdziliśmy możliwość uzyskania przez Windows Server 2008 dostępu do przygotowanego wcześniej serwera DNS (system Debian 7) i przekonaliśmy się, czy nazwy komputerów są prawidłowo określane.

Zanim będziemy kontynuować procedurę i faktycznie przyłączymy się do domeny `POA.MSDCBRZ.EALL.COM.BR`, możemy przeprowadzić ostatni test, aby się upewnić o prawidłowym działaniu zegara w systemie Windows Server. W tym celu można po prostu spojrzeć na zegar wyświetlany w prawym dolnym rogu ekranu (na pasku zadań) lub też wydać polecenie `date` w wierszu poleceń PowerShell. Jeżeli zegar serwera nie wskazuje prawidłowej daty lub godziny, trzeba to poprawić przed przejściem do kolejnego kroku. Aby zmienić godzinę, po prostu dwukrotnie kliknij zegar na pasku zadań, a następnie kliknij przycisk *Zmień ustawienia daty i godziny…* (patrz rysunek 2.4).

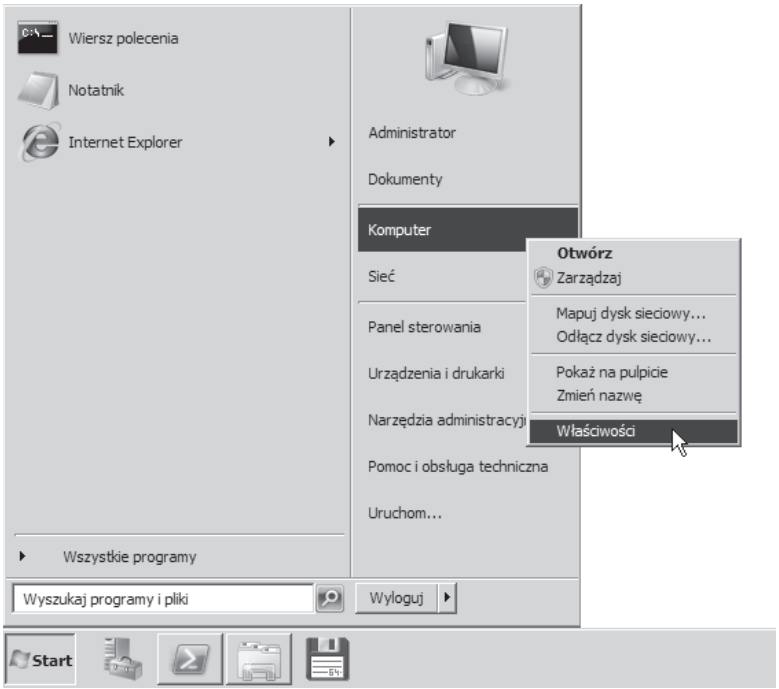
Rysunek 2.4. Zmiana ustawień daty i godziny

W ten sposób przeprowadziliśmy wstępne operacje weryfikacji mające na celu upewnienie się o prawidłowej konfiguracji usługi Active Directory i serwera Windows Server 2008, a także o możliwości komunikacji między nimi. Kontynuujemy więc procedurę i przystępujemy do przyłączenia systemu Windows Server 2008 do domeny usługi Active Directory.

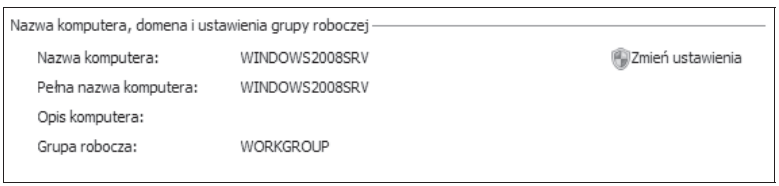
Procedura dołączenia komputera do domeny jest w Windows Server 2008 bardzo prosta i szybka. Kliknij przycisk *Start*, a następnie prawym przyciskiem myszy opcję *Komputer*. Z wyświetlonego menu kontekstowego wybierz opcję *Właściwości*.

Wybór odpowiedniej opcji pokazano na rysunku 2.5.

Na ekranie zostanie wyświetlone okno *Panel sterowania/System i zabezpieczenia/System* zawierające informacje o systemie. Mniej więcej pośrodku okna są wyświetlone informacje takie jak nazwa komputera, domena i grupa robocza (patrz rysunek 2.6). Obok wymienionych informacji znajduje się przycisk *Zmień ustawienia*, który należy kliknąć.



Rysunek 2.5. Wyświetlenie właściwości komputera

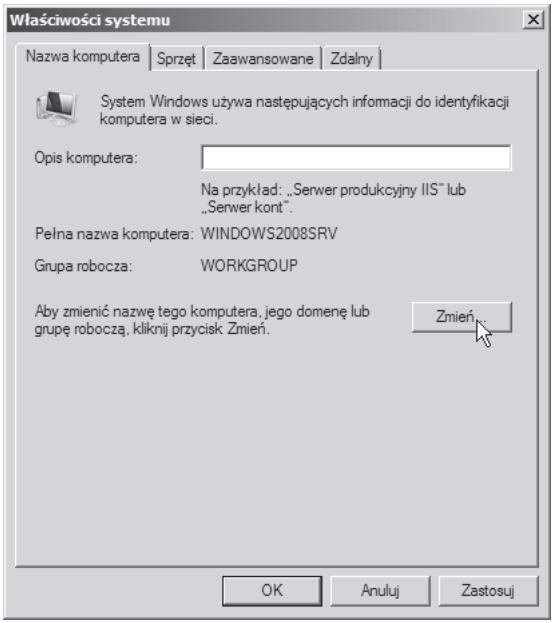


Rysunek 2.6. Wyświetlone informacje o nazwie komputera, domenie i grupie roboczej

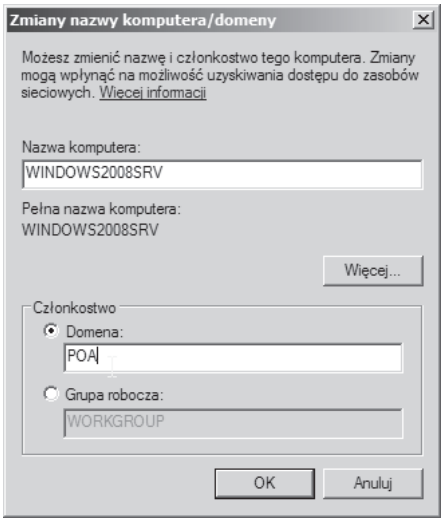
Na ekranie zostanie wyświetlone okno dialogowe zawierające przycisk *Zmień…* obok opisu *Aby zmienić nazwę tego komputera, jego domenę lub grupę roboczą, kliknij przycisk Zmień* (patrz rysunek 2.7). Kliknij wskazany przycisk.

Po kliknięciu przycisku *Zmień…* na ekranie zostanie wyświetlone okno dialogowe pozwalające na przyłączenie się do domeny. Jako nazwę domeny podaj `POA`. Na rysunku 2.8 pokazano wygląd wspomnianego okna dialogowego po wprowadzeniu wymaganej zmiany.

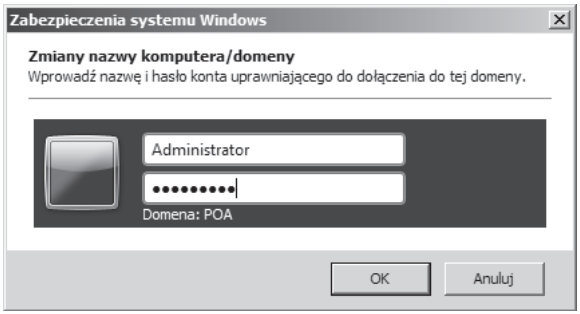
Po podaniu nazwy domeny należy kliknąć przycisk *OK* i podać dane uwierzytelniające w nowo wyświetlonym oknie dialogowym (patrz rysunek 2.9).



Rysunek 2.7. Okno dialogowe wyświetlające właściwości systemu

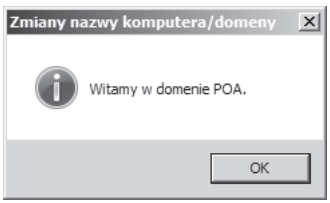


Rysunek 2.8. Wskazanie nazwy domeny, do której zostanie przyłączony komputer



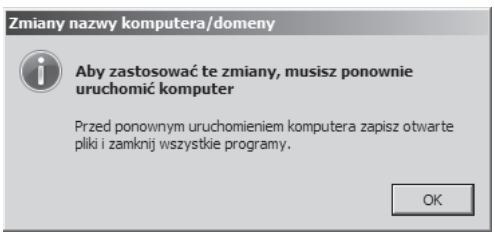
Rysunek 2.9. Okno dialogowe pozwalające na podanie danych uwierzytelniających

Jeżeli zostaną podane prawidłowe dane uwierzytelniające i wszystko przebiegnie bez problemów, po kilku sekundach powinno być wyświetlone kolejne okno dialogowe, tym razem zawierające komunikat *Witamy w domenie POA*, jak pokazano na rysunku 2.10.



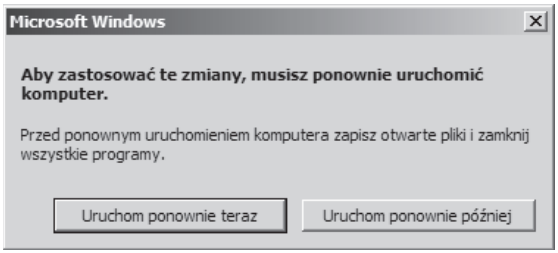
Rysunek 2.10. Komunikat powitalny po przyłączeniu komputera do domeny

Po kliknięciu przycisku *OK* wyświetlone zostanie kolejne okno dialogowe. Zawiera ono komunikat informujący o konieczności ponownego uruchomienia komputera, aby wprowadzone zmiany odniosły skutek (patrz rysunek 2.11). Przed ponownym uruchomieniem systemu upewnij się o zapisaniu wszystkich otwartych plików.



Rysunek 2.11. Komunikat informujący o konieczności ponownego uruchomienia komputera

Teraz można bezpiecznie nacisnąć przycisk *OK*. System Windows Server 2008 zostanie ponownie uruchomiony po naciśnięciu przycisku *Uruchom ponownie teraz* pokazanego na rysunku 2.12.



Rysunek 2.12. Przyciski, których kliknięcie spowoduje ponowne uruchomienie systemu

Po ponownym uruchomieniu komputera trzeba koniecznie zwrócić baczną uwagę na ekran logowania. Jeżeli tego nie zrobisz, może Ci się wydawać, że masz dostępne te same opcje co wcześniej. Domyślnie następuje zalogowanie na ostatnio używanym koncie użytkownika (**Administrator** w systemie lokalnym). W przeciwieństwie do innych wersji systemu Microsoft Windows oferujących wygodną możliwość wyboru domeny, do której zaloguje się użytkownik, tutaj trzeba ręcznie podać nazwę domeny i użytkownika w postaci **DOMENA\Użytkownik**.

Na rysunku 2.13 pokazano przykład logowania użytkownika do domeny POA, do której przed chwilą został dołączony komputer (pamiętaj o konieczności podania hasła administratora domeny POA).

Rysunek 2.13. Zalogowanie się do domeny POA

Po naciśnięciu klawisza *Enter* powinno nastąpić zalogowanie do nowej domeny. W ten sposób w pełni skonfigurowałeś system operacyjny Microsoft Windows Server 2008 R2 do użycia domeny POA usługi Active Directory oferowanej przez Sambę 4. To jest ostatni test i ostatnia procedura weryfikacji poprawności działania konfiguracji, a kontroler domeny jest gotowy do umieszczenia w środowisku produkcyjnym.

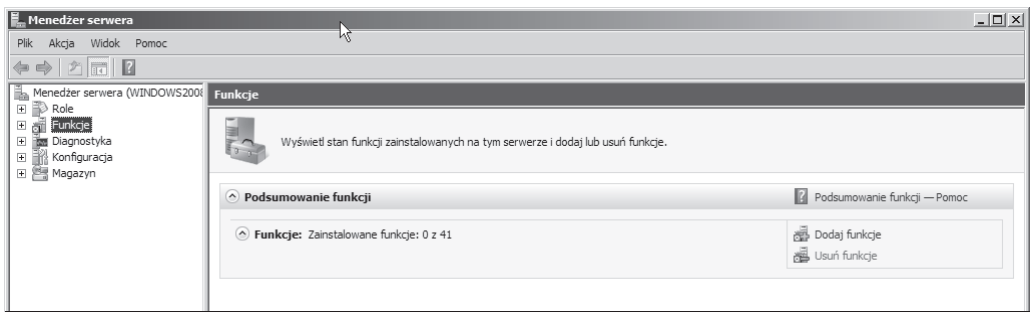
Ponieważ komputer został przetestowany i zintegrowany z domeną, wykorzystamy go do utworzenia struktury organizacyjnej w usłudze Active Directory. W omawianym przykładzie wspomniana struktura będzie się składała z 10 jednostek organizacyjnych, po których utworzeniu komputer będzie można umieścić w środowisku produkcyjnym. To jest bardzo ważna procedura i mamy pewne konfiguracje domyślne możliwe do użycia w celu przetestowania komputera podczas jego przygotowywania do umieszczenia w środowisku docelowym. Wiele wprowadzanych zmian nie będzie tutaj szczegółowo omawianych. Przedstawioną procedurę zalecam stosować w trakcie konfiguracji każdej usługi Active Directory. Wszystkie wprowadzane zmiany mają za zadanie skonfigurowanie środowiska w sposób najbardziej odpowiedni do wymagań.

Aby z poziomu systemu Microsoft Windows Server 2008 R2 zdalnie zarządzać kontrolerem domeny usługi Active Directory opartej na Sambie 4, nie trzeba instalować oprogramowania dodatkowego ani pobierać czegokolwiek więcej, jak ma to miejsce w innych wersjach Microsoft Windows. Należy jednak skonfigurować (to znaczy włączyć) pewne funkcje w narzędziu *Menedżer serwera*, które domyślnie nie są włączone.

> Istnieje możliwość zarządzania serwerem Samba 4 za pomocą innej wersji systemu Microsoft Windows, na przykład Microsoft Windows 2003, Microsoft Windows XP i Microsoft Windows 7.

Uruchom narzędzie *Menedżer serwera*. W tym celu kliknij menu *Start*, następnie *Uruchom…*, wpisz `ServerManager.msc` w wyświetlonym oknie dialogowym i naciśnij *Enter*. Trzeba koniecznie pamiętać o podaniu rozszerzenia (`.msc`). Jeżeli je pominiesz, wtedy zostanie uruchomiony Eksplorator Windows wyświetlający zawartość katalogu *Windows/System32/ServerManager*. Alternatywną metodą uruchomienia Menedżera serwera jest kliknięcie jego ikony znajdującej się na pasku zadań lub wybór odpowiedniej opcji z menu *Start*.

Po wyświetleniu okna *Menedżera serwera* w lewym panelu kliknij opcję *Funkcje*, natomiast w prawym przycisk *Dodaj funkcje*. Na rysunku 2.14 pokazano okno Menedżera serwera wraz z wybraną opcją *Funkcje* w lewym panelu oraz przyciskiem *Dodaj funkcje* w prawym panelu.

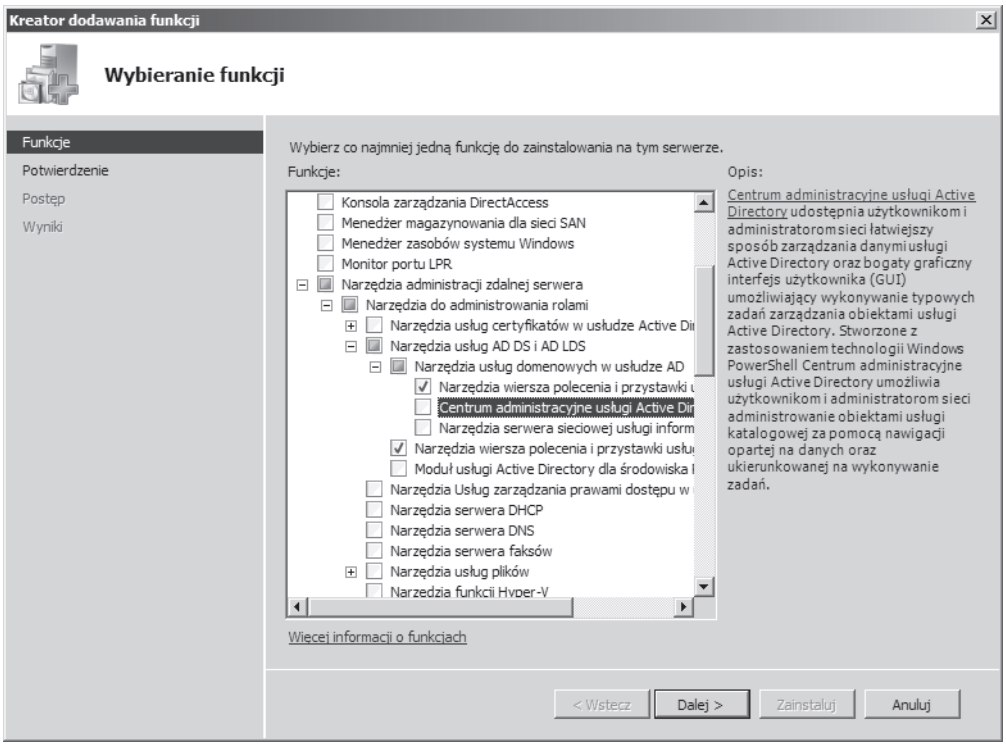


Rysunek 2.14. Okno Menedżera serwera po wybraniu opcji Funkcje

Istnieje wiele funkcji, które można włączyć za pomocą **Kreatora dodawania funkcji**. Znaczna część z nich (na przykład Centrum administracyjne usługi Active Directory) wymaga instalacji Microsoft .NET Framework. Na tym etapie dodamy jedynie dwie funkcje:

```
Narzędzia wiersza polecenia i przystawki usług AD DS
Narzędzia wiersza polecenia i przystawki usług LDS w usłudze AD
```

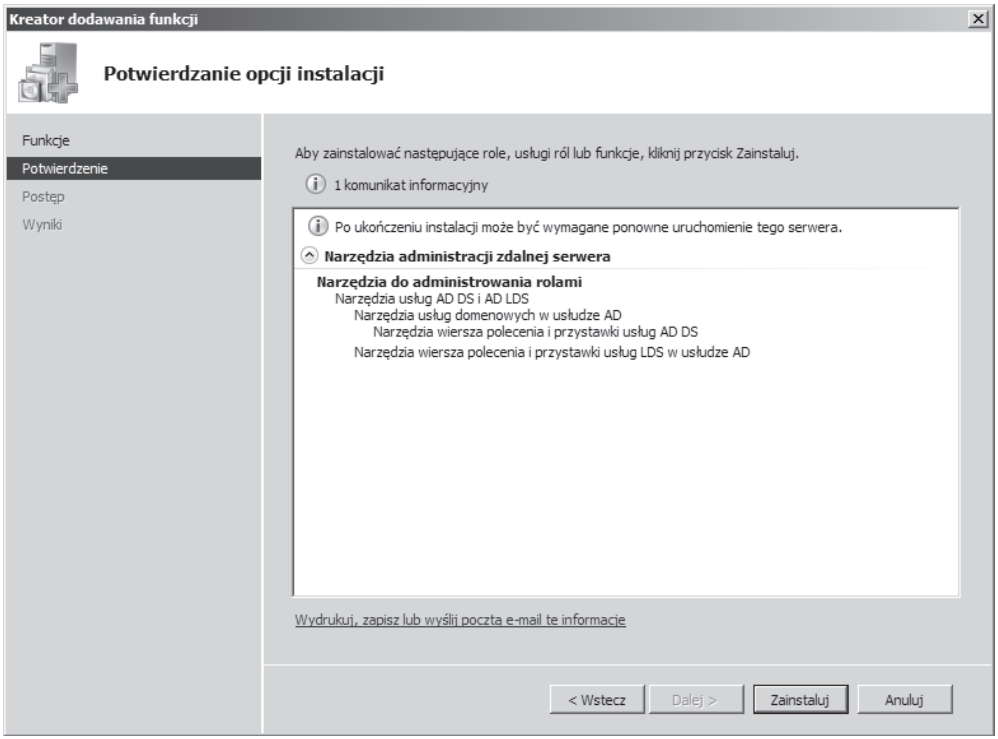
Dodanie wymienionych funkcji będzie wystarczające do uruchomienia narzędzia `dsa.msc`, co pozwoli na rozpoczęcie tworzenia jednostek organizacyjnych. Na rysunku 2.15 pokazano wspomnianego wcześniej **Kreatora dodawania funkcji**.



Rysunek 2.15. Kreator dodawania funkcji

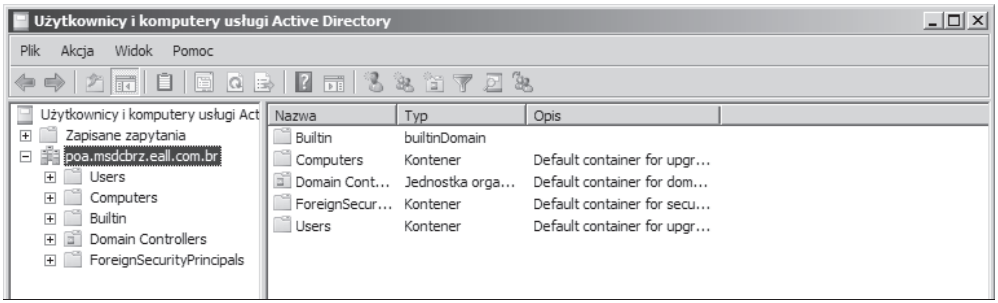
Naciśnij przycisk *Dalej*, a następnie w wyświetlonym oknie dialogowym upewnij się o wybraniu odpowiednich opcji. Jeżeli zaznaczyłeś prawidłowe opcje, naciśnij przycisk *Zainstaluj* (patrz rysunek 2.16).

Jeżeli w systemie nie jest włączona opcja automatycznej aktualizacji systemu Windows Server, na ekranie zostanie wyświetlony odpowiedni komunikat ostrzeżenia wraz z zaleceniem włączenia wspomnianej opcji. Po prostu upewnij się, że proces instalacji został zakończony bezbłędnie i narzędzia AD, DS i LDS zainstalowano bez problemów. W takim przypadku możesz przejść do kolejnego kroku. Kliknij przycisk *Zamknij*, a następnie zakończ działanie *Menedżera serwera*.



Rysunek 2.16. Potwierdzenie wyboru funkcji do instalacji

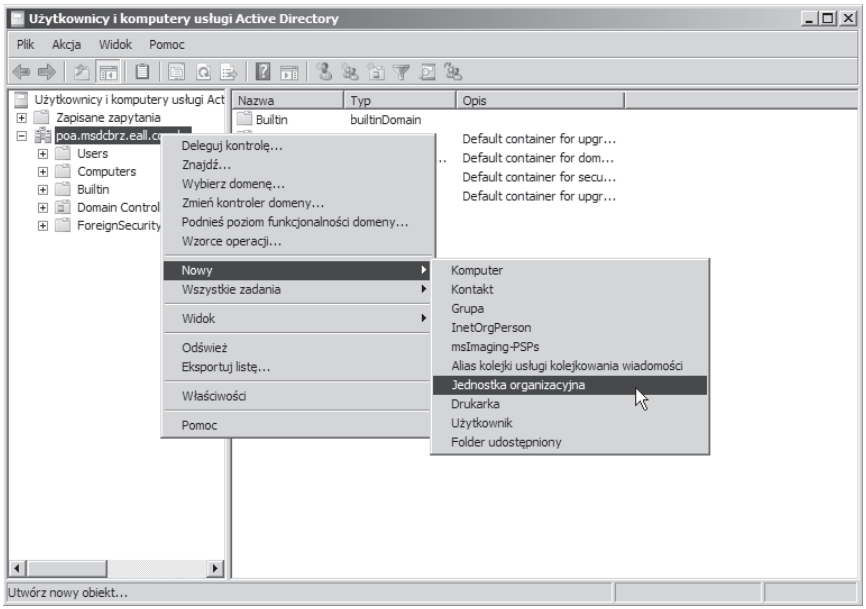
Teraz przejdź do menu *Start*, wybierz opcję *Uruchom…* i wydaj polecenie `dsa.msc`. Na ekranie zostanie wyświetlone okno pokazane na rysunku 2.17.



Rysunek 2.17. Narzędzie Użytkownicy i komputery usługi Active Directory

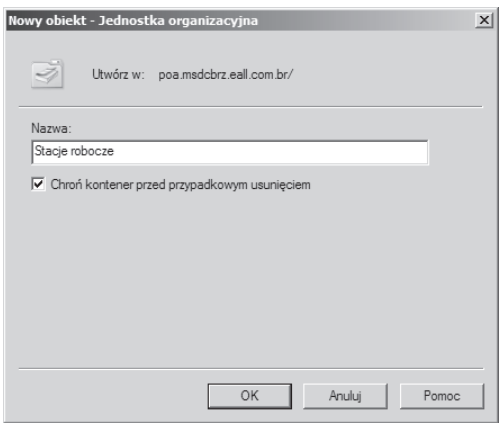
W uruchomionym narzędziu, w lewym panelu, wybrano naszą domenę usługi Active Directory (`poa.msdcbrz.eall.com.br`), natomiast w prawym można zobaczyć domyślne obiekty, które zostały utworzone podczas konfiguracji kontrolera domeny opartego na Sambie 4.

Dzięki uruchomionemu narzędziu można tworzyć jednostki organizacyjne, a tym samym strukturę przeznaczoną do przechowywania planowanych obiektów. Na rysunku 2.18 pokazano tworzenie najwyższego poziomu jednostki organizacyjnej o nazwie `Stacje robocze`. (Na rysunku, pod oknem dialogowym, widać wybraną domenę. Oznacza to, że nowe jednostki organizacyjne będą umieszczane we wskazanej domenie).



Rysunek 2.18. Tworzenie nowej jednostki organizacyjnej

Na ekranie zostanie wyświetlone okno dialogowe przeznaczone do podania nazwy jednostki organizacyjnej (patrz rysunek 2.19). Podaj nazwę tworzonej jednostki organizacyjnej, a następnie kliknij przycisk *OK*.

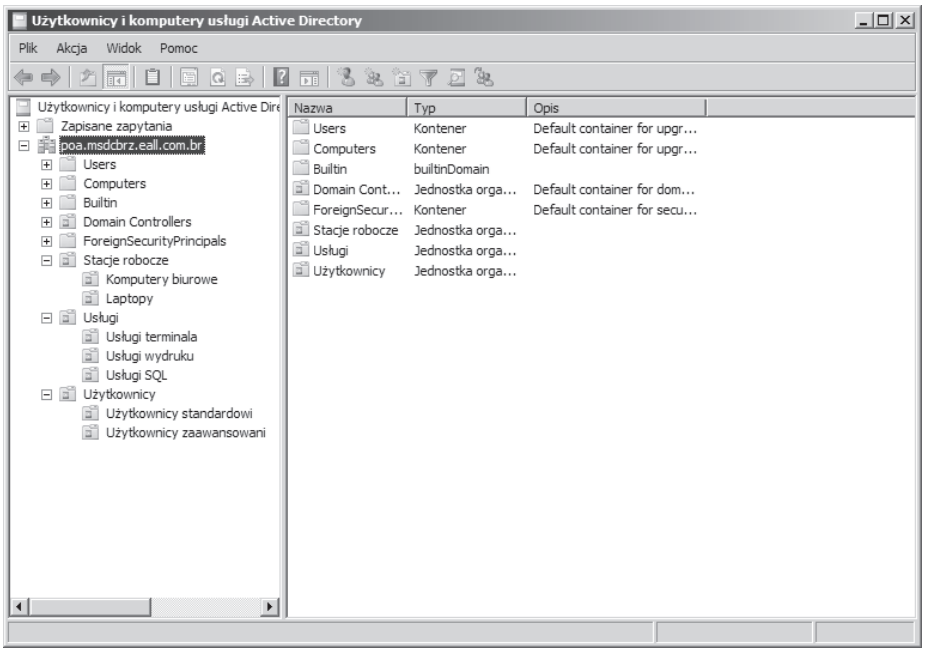


Rysunek 2.19. Podanie nazwy nowej jednostki organizacyjnej

Teraz tę samą procedurę trzeba powtórzyć w celu utworzenia pozostałych jednostek organizacyjnych, które zostały zaplanowane dla naszej usługi Active Directory. Poniżej wymieniono pozostałe 9 jednostek organizacyjnych:

- komputery biurowe,
- laptopy,
- usługi,
- usługi terminala,
- usługi wydruku,
- usługi SQL,
- użytkownicy,
- użytkownicy standardowi,
- użytkownicy zaawansowani.

Po utworzeniu wszystkich zaplanowanych jednostek organizacyjnych struktura naszej usługi Active Directory będzie przedstawiała się, jak pokazano na rysunku 2.20.



Rysunek 2.20. Usługa Active Directory wraz z utworzonymi wszystkimi zaplanowanymi jednostkami organizacyjnymi

Po zakończeniu operacji tworzenia struktury usługi Active Directory można zamknąć narzędzie `dsa.msc` i wylogować się z systemu Windows Server 2008 R2. Teraz powracamy do serwera Samba 4, w którym utworzymy 50 kont użytkowników (47 **standardowych** i 3 **zaawansowanych**). W materiałach dołączonych do książki znajduje się wiele skryptów, między innymi narzędzie

przeznaczone do utworzenia wszystkich naszych kont użytkowników we właściwych jednostkach organizacyjnych i wraz z odpowiednimi atrybutami. Wszyscy użytkownicy (**użytkownicy standardowi**) będą na początku mieli takie samo hasło. Każdy z nich po pierwszym zalogowaniu będzie musiał zdefiniować własne hasło. W celu utworzenia kont użytkowników przejdź do powłoki, a następnie wydaj następujące polecenie:

```
lealdebian7:~$ cd ~/workspace/implementing_samba4/ && ./createusers.sh -h
```

Spowoduje ono wygenerowanie poniższych danych wyjściowych:

```
+------------------------------------------------------------+
| Simple script to create users on the AD/DC (Samba 4 Server) |
|                                        Implementing Samba 4 |
|                                                             |
|                              Copyright(c) 2013 Marcelo Leal |
+------------------------------------------------------------+
Usage:

"-h" for this help message
"-c" creates users (silently).
"-v" creates users (verbosely),

Dalsze polecenie służące do rzeczywistego tworzenia kont użytkowników.
```

Aby utworzyć konta użytkowników, skrypt korzysta z pliku o nazwie *users.txt*, który powinien znajdować się w katalogu roboczym.

```
Error Codes:   (0)OK,
         (1)Wrong Options,
         (2)At least one user creation error,
         (3) Could not open users.txt file.
```

W pierwszej kolejności utwórz konta użytkowników standardowych na podstawie danych znajdujących się w pliku *users.txt*. Omawiany tutaj skrypt powoduje utworzenie kont użytkowników jedynie w jednostce organizacyjnej `Użytkownicy/Użytkownicy standardowi`.

Plik *users.txt* jest bardzo prosty i zawiera po prostu imię oraz nazwisko użytkownika tworzonego konta. Wszystkie argumenty (na przykład nazwa użytkownika i inicjały) są obsługiwane za pomocą skryptu *createusers.sh*. Poniżej przedstawiono fragment pliku *users.txt*:

```
Vincent Vega
Jules Winnfield
Bruce Coolidge
Mia Wallace
Marsellus Wallace
Jimmie Dimmick
Phil Marvin
```

Kolejnym krokiem jest wydanie następującego polecenia w powłoce serwera Samba 4:

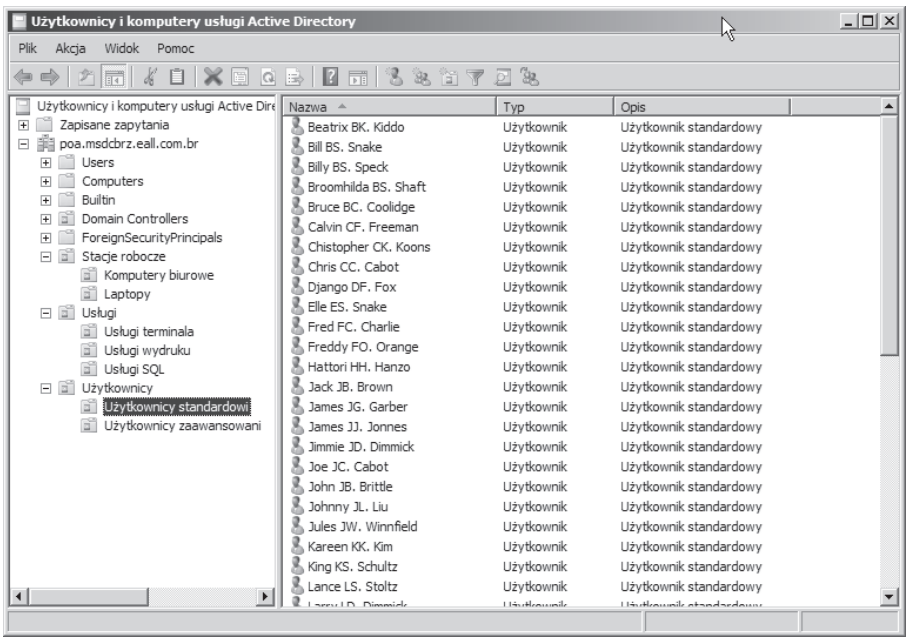
```
lealdebian7:~$ sudo ./createusers.sh -c
```

Dane wyjściowe zawierają po jednym wierszu dla każdego utworzonego konta użytkownika wraz z informacją, czy operacja tworzenia konta użytkownika zakończyła się powodzeniem, czy wystąpił jakiś błąd. Poniższe wiersze to fragment danych wyjściowych wygenerowanych na skutek operacji tworzenia kont użytkowników na podstawie pliku *users.txt*:

```
User: jajonnes created  OK.
User: zojarratt created  OK.
User: sahill created  OK.
User: qumichael created  OK.
User: rojohnson created  OK.
User: jabrown created  OK.
User: legecko created  OK.
-------------------------
Total Users Created..: 47
Total Creation Errors: 0
Total Users Processed: 47
-------------------------
```

Na końcu danych wyjściowych znajduje się podsumowanie: utworzono 47 kont użytkowników, w trakcie operacji nie wystąpił żaden błąd. Tak więc wszystkie konta użytkowników zostały utworzone bez problemów, powinny znajdować się w jednostce organizacyjnej `Użytkownicy standardowi`.

Teraz możemy ponownie spojrzeć na strukturę usługi Active Directory i w interfejsie graficznym (patrz rysunek 2.21) przekonać się, że wszystkie konta użytkowników faktycznie zostały utworzone.



Rysunek 2.21. Lista użytkowników standardowych

Podsumowanie

W tym rozdziale dość dokładnie przedstawiono konfigurację serwera Samba 4 działającego w charakterze kontrolera domeny usługi Active Directory. Omówiono fazy początkowe: planowanie topologii sieci, opracowanie struktury usługi Active Directory, a także przygotowanie listy rzeczy do sprawdzenia, co pomaga w organizowaniu informacji.

W dalszej części rozdziału przeprowadzono serię testów i operacji weryfikacji ważnych komponentów serwera usługi Active Directory. W ten sposób zetknąłeś się z podsystemem dostarczającym podstawowych funkcji związanych z usługą Active Directory w Sambie 4. Ostatni test polegał na przyłączeniu serwera testowego (działającego po kontrolą systemu operacyjnego Microsoft Windows Server 2008 R2) do naszej domeny POA. Dowiedziałeś się również, jak zarządzać serwerem Samba 4 z poziomu Windows Server 2008 za pomocą funkcji, które trzeba włączyć w zainstalowanym systemie Windows Server.

Wykorzystując komputer testowy, sprawdziliśmy działanie procedury tworzenia jednostek organizacyjnych w usłudze Active Directory i utworzyliśmy zaplanowaną wcześniej strukturę. Podczas tej operacji pomocne okazały się pewne skrypty, dzięki którym w łatwy sposób utworzyliśmy 47 kont użytkowników standardowych.

W następnym rozdziale poznasz narzędzia przeznaczone do zarządzania serwerem Samba 4 i podstawy zarządzania polityką grup. Poruszone zostaną również zagadnienia związane z uwierzytelnianiem i autoryzacją, a także inne ważne funkcje systemu GNU/Linux.

Skorowidz

Samba 4 Przewodnik administratora

Usługa Active Directory jest implementacją protokołu LDAP i została wprowadzona na rynek wraz z premierą systemu Windows 2000. Stanowi kluczowy element organizacji usług w firmach. Pozwala przechowywać informacje o komputerach, użytkownikach i innych urządzeniach w ramach organizacji. Jednym z kluczowych zadań Active Directory jest uwierzytelnianie elementów podłączonych do domeny. Jeżeli chcesz wdrożyć w Twojej firmie usługę Active Directory, możesz wykorzystać płatne rozwiązania giganta z Redmond lub pokusić się o użycie darmowej alternatywy.

Samba doskonale sprawdza się w roli kontrolera domeny. W trakcie lektury tej książki zdobędziesz dogłębną wiedzę na temat jej stosowania. Na samym początku przeczytasz o tym, jak zainstalować serwer Samba 4 oraz nim zarządzać. Z kolejnych rozdziałów dowiesz się, jak zastąpić istniejący kontroler domeny współpracujący z systemem Windows przez system z Sambą 4. Ponadto w tej wspaniałej książce znajdziesz szczegółowe informacje na temat aktualizacji Samby, rozbudowy schematu Active Directory oraz implementacji rozproszonego serwera plików o wysokiej dostępności. To obowiązkowa lektura dla administratorów i pasjonatów, chcących wdrożyć usługę Active Directory z użyciem darmowych rozwiązań.

Dzięki tej książce:

- poznasz możliwości usługi Active Directory
- wdrożysz tę usługę z wykorzystaniem Samby
- zastąpisz kontroler domeny współpracujący z systemem Windows
- uruchomisz serwer plików i wydruków

Poznaj potencjał serwera Samba!

helion.pl księgarnia internetowa

Nr katalogowy: 24861

Księgarnia internetowa: http://helion.pl

Zamówienia telefoniczne: 0 801 339900 0 601 339900

[PACKT] open source PUBLISHING

Helion

Sprawdź najnowsze promocje: http://helion.pl/promocje
Książki najchętniej czytane: http://helion.pl/bestsellery
Zamów informacje o nowościach: http://helion.pl/nowosci

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel.: 32 230 98 63
e-mail: helion@helion.pl
http://helion.pl

Informatyka w najlepszym wydaniu

sięgnij po WIĘCEJ

KOD KORZYŚCI

ISBN 978-83-246-9820-2

Cena: 44,00 zł