Zbigniew Góra

Active Directory
w systemach wolnego oprogramowania

Serwer Samba 4 jako kontroler domeny

Helion

Opieka redakcyjna: Ewelina Burska
Projekt okładki: Studio Gravite/Olsztyn
Obarek, Pokoński, Pazdrijowski, Zaprucki

Materiały graficzne na okładce zostały wykorzystane za zgodą Shutterstock.

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/acdili
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-246-9815-8

Printed in Poland.

Spis treści

Rozdział 1.

Szczypta teorii i historii

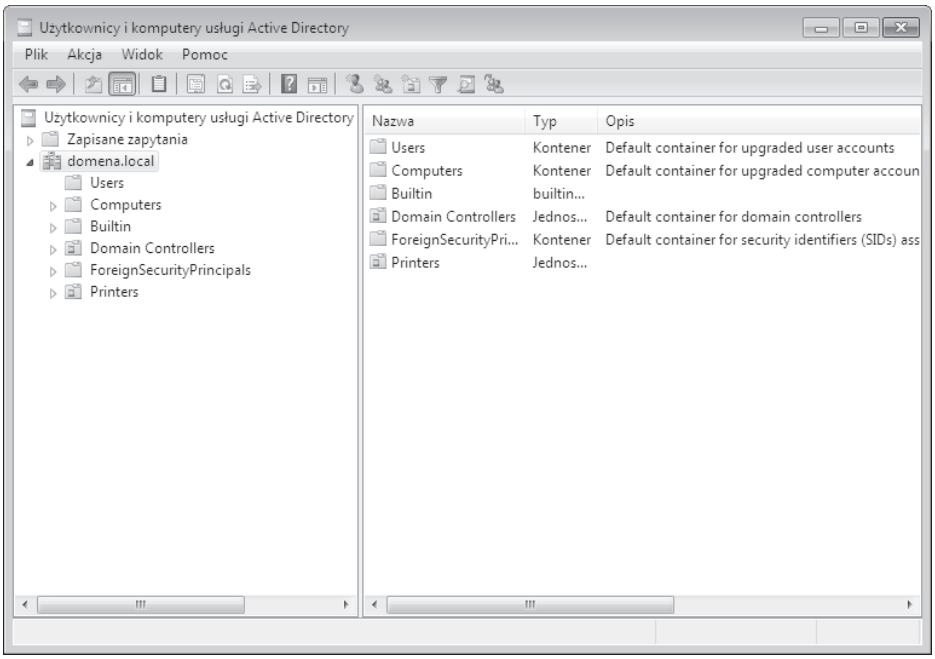
W tym rozdziale omówię pojęcia, które będą się pojawiały w dalszej części książki. Czytelnicy, którzy już pracują w Active Directory i znają serwer plików Samba, mogą ten fragment pominąć. Zachęcam jednak do zapoznania się z opisanymi tutaj tematami. Pozwoli to przybliżyć zagadnienia związane z pracą w grupach roboczych, zaznajomić się z historią omawianych systemów oraz zrozumieć, dlaczego tematyka usługi Active Directory i jej implementacji w systemie Linux ma tak duże znaczenie.

Active Directory w systemie Windows Server

Active Directory jest to usługa katalogowa, czyli hierarchiczna baza danych zawierająca takie elementy jak użytkownicy, sprzęt sieciowy i aplikacje, pozwalająca na centralne zarządzanie relacjami między nimi. Active Directory jest opracowaną przez Microsoft implementacją protokołu LDAP, działającą pierwotnie w środowisku Windows.

Usługa katalogowa Microsoft pojawiła się po raz pierwszy wraz z Windows 2000 Server pod koniec lat 90. XX wieku. Pierwotnie nosiła nazwę NT Directory Service. Windows Server 2003 przyniósł następcę NTDS — Active Directory Domain Services, czyli usługę w kształcie, jaki znamy obecnie. Nie jest to jedyna istniejąca i dostępna usługa katalogowa. Jednak z powodu popularności systemu Windows Active Directory jest obecne w wielu firmach i instytucjach. Podstawowymi narzędziami do zarządzania usługą katalogową Microsoft są przystawki administracyjne. Ich przykładem jest program *Użytkownicy i komputery usługi Active Directory*, zaprezentowany na rysunku 1.1.

Główną korzyścią płynącą z wdrożenia usługi katalogowej w sieci jest możliwość centralnego zarządzania użytkownikami, sprzętem sieciowym, aplikacjami i przechowywanymi danymi. Osoby pracujące na co dzień w domenie jako jej cechę na pewno wymienią możliwość logowania się na różnych komputerach za pomocą tej samej nazwy użytkownika



Rysunek 1.1. *Przystawka Użytkownicy i komputery usługi Active Directory — jedno z podstawowych narzędzi administratora*

i hasła. Jest to tzw. **profil wędrujący** lub mobilny (ang. *roaming profile*). Stosując to rozwiązanie, użytkownicy bardzo dużych sieci firmowych rozproszonych po całym świecie mogą logować się na różnych komputerach, w różnych miejscach na Ziemi i mają dostęp do swoich danych i aplikacji.

Taka funkcjonalność została osiągnięta między innymi dzięki protokołowi uwierzytelniania i autoryzacji **Kerberos**. Działa on z wykorzystaniem centrum dystrybucji kluczy (KDC — ang. *Key Distribution Center*). Każdy logujący się użytkownik najpierw musi zostać uwierzytelniony; są tworzone odpowiednie bilety (ang. *tickets*) między użytkownikiem a serwerami i po udanej autoryzacji zostaje przyznany dostęp do zasobów domeny.

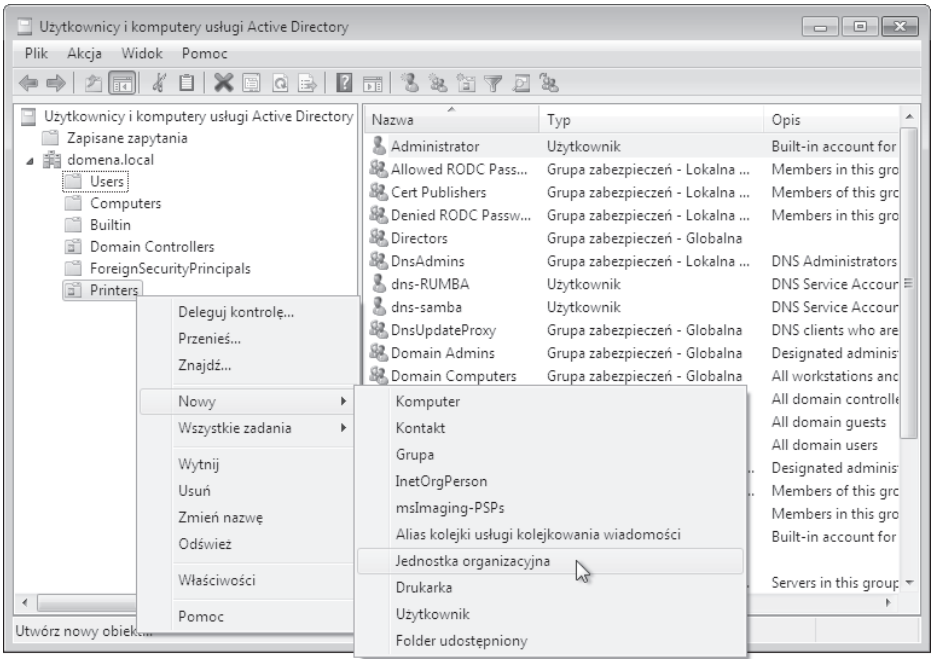
Struktura logiczna Active Directory

Active Directory jest rodzajem bazy danych, która przechowuje pewne informacje, zorganizowane w odpowiedni sposób. Struktura usługi katalogowej Microsoft swoją budową może nieco przypominać drzewo, dlatego jej elementy składowe są nazywane liśćmi, drzewami i lasem.

Najbardziej podstawowym składnikiem usługi Active Directory jest tzw. liść. Może nim być na przykład konto użytkownika, komputera lub grupa użytkowników. Elementem grupującym liście jest kontener będący najczęściej jednostką organizacyjną (OU, ang. *Organizational Unit*). Kontenery i liście są składowymi domen. W domenie można tworzyć

hierarchiczne struktury jednostek administracyjnych (jedne pod drugimi). Kontener grupujący liście nie jest jednostką organizacyjną, kiedy nie można w nim tworzyć kolejnych jednostek.

Rysunek 1.2 przedstawia podstawowe elementy struktury logicznej Active Directory.

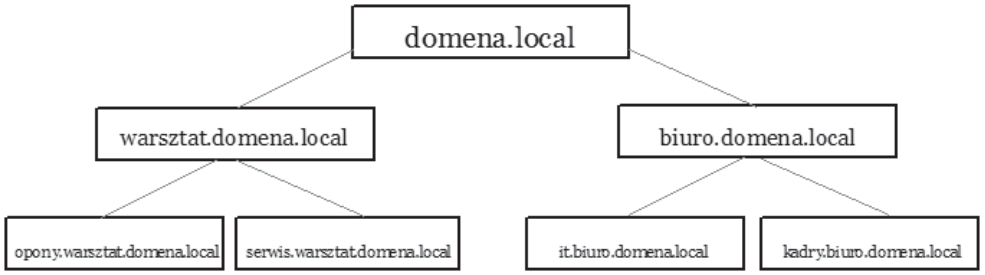


Rysunek 1.2. *Przystawka Użytkownicy i komputery usługi Active Directory z wyszczególnionymi elementami*

W okienku po lewej stronie znajduje się lista rozwijana, na której szczycie umieszczona jest domena o nazwie *domena.local*. Jej składowymi są foldery będące kontenerami i jednostkami organizacyjnymi. Katalog *Users* jest kontenerem niebędącym jednostką administracyjną. Zawiera on liście, czyli konta i grupy użytkowników, ale nie można w nim tworzyć jednostek podrzędnych. Przykładem liścia jest profil użytkownika *Administrator*.

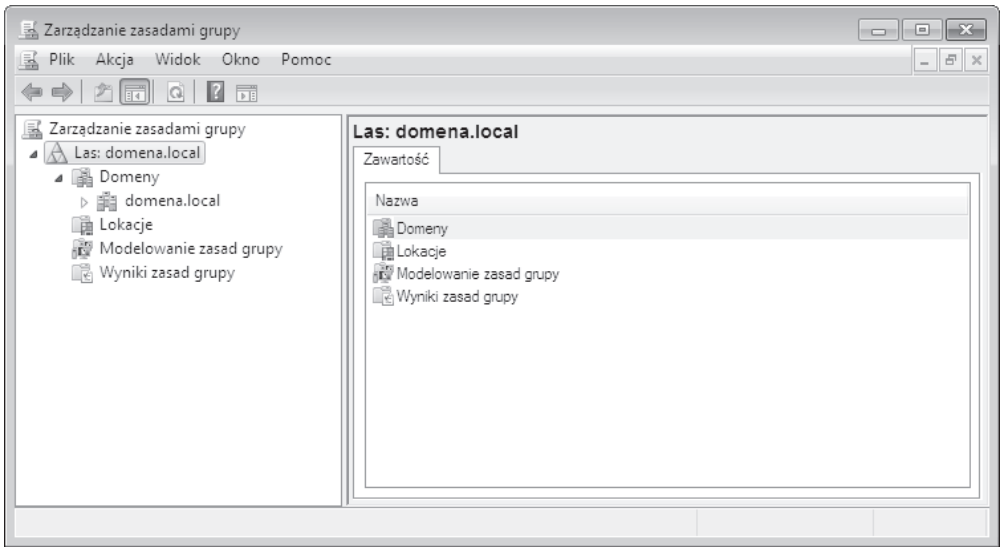
Jednostką administracyjną jest natomiast folder *Printers*. Jak pokazuje rysunek, można w nim tworzyć kolejne jednostki oraz liście w postaci kont komputerów, grup, użytkowników, drukarek i innych.

W Active Directory pod kontrolą systemu Windows Server może pracować wiele domen. Mogą też istnieć domeny podrzędne. Domena nadrzędna wraz ze swoimi subdomenami tworzy tzw. drzewo. Przykład drzewa domen przedstawiono na diagramie na rysunku 1.3.



Rysunek 1.3. *Przykładowe drzewo domen*

W Active Directory może istnieć wiele drzew oraz pojedynczych domen. Każdą domeną i subdomeną zarządza oddzielny serwer, czyli kontroler. Domeny i drzewa są składowymi największego obiektu w usłudze katalogowej, czyli lasu. Las jest tworzony automatycznie wraz z pierwszą domeną i przyjmuje jej nazwę. Listę domen w lesie można zobaczyć, korzystając z narzędzia *Zarządzanie zasadami grupy*, co zostało pokazane na rysunku 1.4.



Rysunek 1.4. *Przystawka Zarządzanie zasadami grupy z zaznaczonym lasem i rozwiniętą listą domen*

Active Directory a DNS

System **DNS** (ang. *Domain Name System* — system nazw domenowych) jest wykorzystywany przez Active Directory do identyfikowania obiektów takich jak domeny i komputery. Podobnie jak usługa katalogowa, system nazw ma budowę hierarchiczną. DNS obejmuje całą sieć Internet i grupuje domeny w topologii drzewa. Dzięki systemowi nazw możliwe jest uszeregowanie komputerów i serwerów w domenach. Hierarchiczna budowa pozwala natomiast na poprawną identyfikację urządzeń fizycznych w logicznej strukturze. Do zadań systemu DNS należy także rozpoznawanie nazw domenowych,

na przykład *samba.domena.local*, i kojarzenie ich z adresami IP odpowiednich komputerów. Dzięki temu między urządzeniami możliwa jest poprawna komunikacja na poziomie sieci.

Domena a grupa robocza

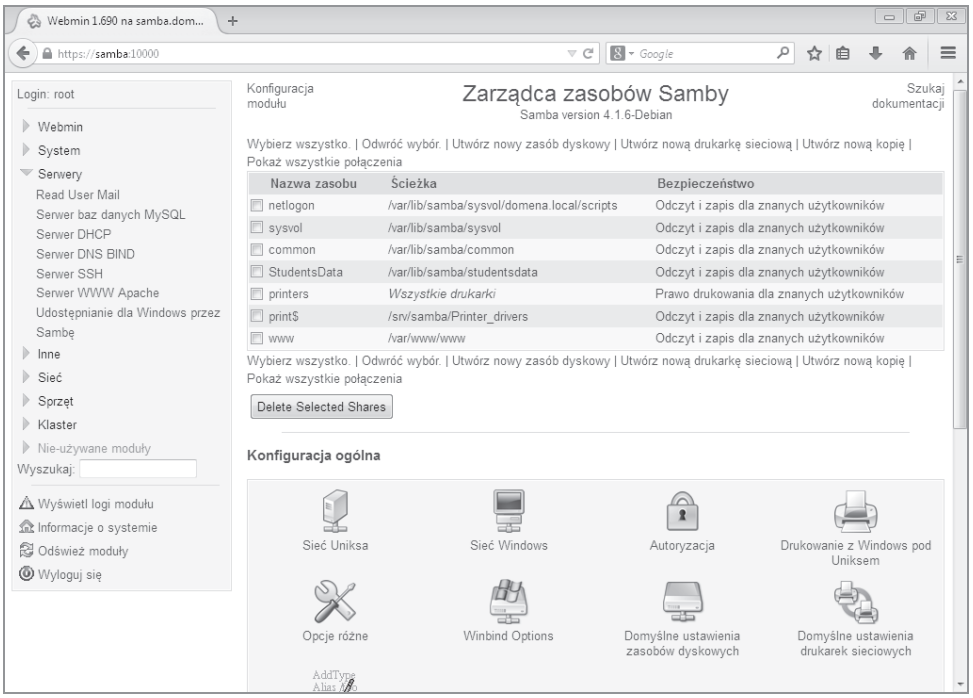
Użytkownikom systemu Windows (ale nie tylko tego) pracującym w sieci nie jest obce pojęcie grupy roboczej. Rozwiązanie to stosuje się w małych środowiskach, w których brak centralnego zarządzania nie stanowi problemu. Grupa robocza pozwala na komunikację komputerów w sieci i wymianę plików. Nie występują tutaj profile wędrujące. Zwykle jeden użytkownik jest przypisany do jednego komputera. Maszyny działające pod kontrolą systemu Windows 7 są domyślnie dodawane do grupy roboczej o nazwie `WORKGROUP`.

Linux w grupie roboczej

W grupach roboczych wcześniej czy później zachodzi potrzeba centralnego gromadzenia danych, czyli skonfigurowania serwera plików. Jeśli wszystkie komputery mają zainstalowany system Windows, to wystarczy jeden z nich wyposażyć w odpowiednio pojemne dyski twarde. Sytuacja trochę się komplikuje, gdy użytkownicy korzystają z urządzeń na różnych platformach systemowych w ramach tej samej grupy. Wówczas może zachodzić problem komunikacji między nimi. Z pomocą przychodzi Linux z serwerem Samba.

Pewnie w niejednej sieci działa jeszcze serwer skonfigurowany kilka lub kilkanaście lat temu na bazie tego oprogramowania. Na początku pierwszej dekady XXI wieku w czasopismach komputerowych można było znaleźć poradniki instalacji domowej LAN z linuksowym serwerem plików i drukarek. Sambą, jak również innymi składnikami systemu operacyjnego serwera można było (i można nadal) zarządzać przez przeglądarkę internetową, korzystając z narzędzia Webmin. Rysunek 1.5 pokazuje interfejs tego oprogramowania z listą zasobów serwera Samba 4 w systemie Debian.

Jednak w sytuacji gdy Samba 4 pracuje jako kontroler domeny Active Directory, do jego obsługi stosuje się przede wszystkim narzędzia administracji zdalnej serwera w systemie Windows.



Rysunek 1.5. *Interfejs narzędzia Webmin z listą zasobów Samby*

Historia Samby

Samba powstała w 1991 roku. Jej twórcą jest Andrew Tridgell, który napisał program serwera plików dla protokołu SMB[1]. Jak mówi strona główna *samba.org*: „Samba jest Otwartym/Wolnym Oprogramowaniem, które zapewnia bezproblemową wymianę plików oraz serwisy drukowania dla klientów protokołów SMB i CIFS". Samba, w przeciwieństwie do innych implementacji SMB/CIFS, jest łatwo dostępna, a także pozwala na komunikację pomiędzy serwerami opartymi na systemach Linux/Unix a klientami Windows.

Na stronie *http://www.samba.org/samba/history/* można zapoznać się z uwagami do wydań Samby od wersji 1.9.17 do najnowszej. Administratorom na pewno jest znana Samba w wersji 3. Na niej i na jej poprzedniczkach działa jeszcze wiele linuksowych serwerów. Zgodnie z założeniem Samba jako serwer Linux/Unix pozwala na współpracę zarówno z klientami tych systemów, jak i systemu Windows. Trzeba też wspomnieć, że już dzięki wcześniejszym wersjom Samby komputery użytkowników systemu Linux można podłączyć do Active Directory. Jednak do wersji 3 włącznie nie mogą one pełnić funkcji kontrolera domeny.

[1] Zainteresowanych szczegółowymi informacjami na temat historii Samby i protokołu SMB zachęcam do zapoznania się z książką Richarda Sharpe'a, Tima Pottera, Jima Morrisa, *Samba dla każdego*, Helion, Gliwice 2002.

Dokładnie 11 grudnia 2012 roku, po kilku latach prac, została wydana pierwsza stabilna wersja oprogramowania Samba 4.0. Wersje rozwojowe, niestabilne można było pobierać wiele miesięcy wcześniej. Samba w wersji czwartej oprócz dotychczas oferowanych usług daje możliwość skonfigurowania kontrolera i zarządzania domeną Active Directory w systemie Linux. Coś, co do niedawna można było tylko drogo kupić od firmy Microsoft, stało się wolne i darmowe.

Samba 4 jako kontroler Active Directory

Dzięki oprogramowaniu Samba 4 można skonfigurować główny kontroler domeny Active Directory oraz kontrolery dodatkowe do istniejących już domen zbudowanych zarówno w systemie Windows Server, jak i z wykorzystaniem Samby. Za pomocą narzędzi administracji serwerem z poziomu dowolnego systemu Windows można zarządzać domeną Active Directory. Te funkcje nie byłyby dostępne, gdyż Microsoft bardzo długo i skutecznie strzegł swojego oprogramowania usług katalogowych. Dopiero pomoc Komisji Europejskiej sprawiła, że producent Windows udostępnił informacje, które pozwoliły na stworzenie wolnego oprogramowania serwerowego.

W momencie pisania tej książki (sierpień 2014) najnowszym wydaniem Samby jest wersja 4.1.11. W uwagach do wydań można przeczytać, że Samba 4.1.x to kolejna wersja pakietu, obejmująca wszystkie technologie wersji stabilnych, zarówno 3, jak i 4. Dodatkowo usługi znane z wersji 3 będą rozwijane tak, aby współpraca z protokołami Active Directory była jeszcze wydajniejsza. Znakiem rozpoznawczym projektu Samba jest logo zaprezentowane na rysunku 1.6.

Rysunek 1.6.
Logo Samby

Skorowidz

E

F

G

H

I

J

K

L

M

N

O

P

R

S

Ś

T

U

V

W

Y

Z

Podstawą działania każdej sieci komputerowej jest hierarchiczna struktura, której wewnętrzna logika decyduje o miejscu i roli elementów składowych oraz o relacjach między nimi. Tę strukturę zapewnia usługa katalogowa Active Directory, pozwalająca uporządkować wszystkie obiekty w sieci firmowej i wygodnie nimi zarządzać. Ponieważ jest to rozwiązanie kosztowne, warto postawić na równie funkcjonalną darmową alternatywę — serwer Samba 4. Świetnie sprawdzi się w roli kontrolera domeny Active Directory w systemach wolnego oprogramowania. Jeśli chcesz zaoszczędzić, a przy okazji poszerzyć swoją wiedzę, to książka dla Ciebie!

Ten poradnik zawiera praktyczne i konkretne wskazówki dotyczące konfiguracji kontrolera domeny w systemie Linux oraz dopasowania usług do oczekiwań administratora i użytkowników. Dowiesz się stąd, co to jest Samba 4 i jak przygotować środowisko testowe dla Twojej sieci. Posłużysz się jasnymi instrukcjami instalacyjnymi i konfiguracyjnymi, by uruchomić Active Directory. Znajdziesz tu także opisy podłączania do tego środowiska komputerów klienckich działających w różnych systemach operacyjnych. Administratorze sieci, sprawdź, jak bardzo ta książka może ułatwić Ci życie!

- Podstawy działania Active Directory
- Przygotowanie laboratorium testowego
- Linux jako kontroler domeny Active Directory
- Serwer pełniący role punktu dostępowego i serwera DHCP
- Podłączanie komputerów klienckich do domeny
- Zarządzanie Active Directory i serwerem Samba 4 poprzez konsolę Linux
- Samba 4 jako serwer drukarek
- Serwer czasu NTP
- Samba 4 jako dodatkowy kontroler istniejącej domeny
- Replikacja SysVol na linuksowych kontrolerach Samba 4
- Instalacja serwera Apache i konfiguracja foldera stron użytkowników domeny

Active Directory, Linux i Samba 4
— filary Twojej sieci!

Helion
25529 numer katalogowy
księgarnia internetowa
http://helion.pl
zamówienia telefoniczne
0 801 339900
0 601 339900

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

ISBN 978-83-246-9815-8
9 788324 698158

Informatyka w najlepszym wydaniu
cena: 44,90 zł