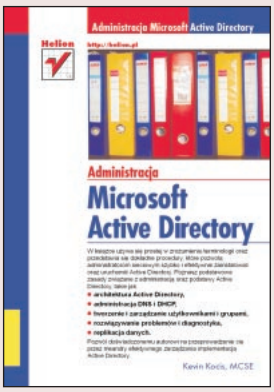
Administracja Microsoft Active Directory



Autor:
Tłumaczenie: Marcin Jędrysiak, Agata Dras
ISBN: 83-7197-474-4
Format: B5, stron: 328

Mimo że Active Directory ma bardzo skomplikowaną strukturę, jego zadaniem jest ułatwianie życia administratorom systemu na poziomie przedsiębiorstwa.
Z perspektywy Microsoftu, Active Directory jest usługą katalogową przeznaczoną dla przedsiębiorstw, opartą na standardach internetowych, dostarczającą użytkownikom informacji i niezbędnych usług. Active Directory jest włączone we wszystkie produkty dla serwerów z serii Windows 2000 i jest implementacją Microsoftu istniejącego modelu (X.500), istniejącego protokołu komunikacji (LDAP) oraz istniejącej technologii lokalizacji (DNS).
Autor, pisząc tą książkę, obrał sobie następujące cele:

- Napisać zrozumiały przewodnik.
- Omówić zadania i zagadnienia związane z administracją.
- Podzielić na poszczególne elementy złożoną strukturę Active Directory.

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

Rozdział 2.

Architektura Active Directory

W tym rozdziale:

- Architektura podsystemowa
- Architektura usługi katalogowej
- Protokoły, interfejsy i usługi dla Active Directory
- Podstawy struktury logicznej
- Podstawy struktury fizycznej

Wiedza o wzajemnym oddziaływaniu składników architektury Active Directory dostarcza podstaw do zrozumienia, jak Active Directory zarządza danymi. Pierwsza część tego rozdziału została poświęcona związkom Active Directory z resztą systemu operacyjnego Windows 2000 Server. Następnie przyjrzymy się strukturze logicznej i fizycznej bazy danych Active Directory, jej składnikom i ich właściwościom.

Architektura podsystemowa

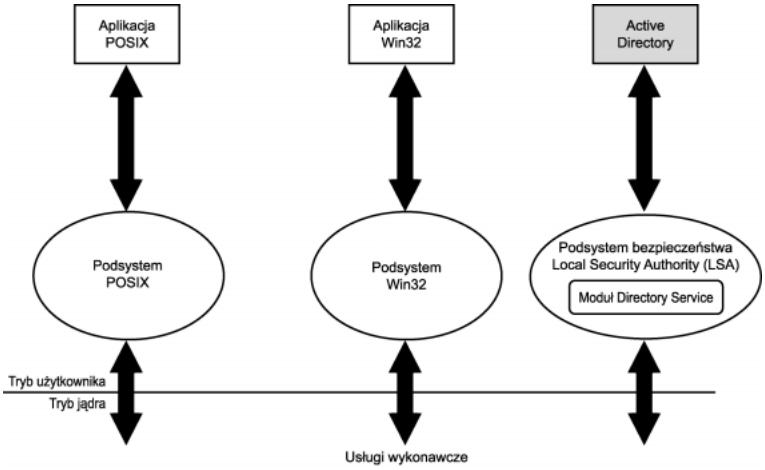
W Windows 2000 istnieją dwa możliwe tryby dostępu do procesora: tryb jądra i tryb użytkownika. Zabezpieczają one aplikacje przed różnicami platform, oddzielając procesy niskopoziomowe, specyficzne dla każdej platformy, od procesów wysokopoziomowych. Zapobiegają również bezpośredniemu dostępowi do kodu systemu i do danych.

Aplikacje i usługi pracują w trybie użytkownika, w którym pobierają usługi systemowe poprzez interfejs programowy aplikacji (API), otrzymujący ograniczony dostęp do danych systemowych. Proces jest przekazywany do trybu jądra, aby wykonywać swoje zadania w środowisku chronionym. Następnie przesyłany jest z powrotem do trybu użytkownika.

Local Security Authority (*LSA*), część podsystemu bezpieczeństwa w trybie użytkownika, jest modułem, w którym działa Active Directory.

Monitor bezpieczeństwa (*security reference monitor*) pracuje w trybie jądra. Narzuca zasady zabezpieczeń podsystemu bezpieczeństwa. Obiekty Active Directory chronione są przez listy kontroli dostępu (*Access Control Lists — ACL*). Lokalizacja Active Directory wewnątrz Windows 2000 jest pokazana na rysunku 2.1.

Rysunek 2.1. *Lokalizacja Active Directory w systemie Windows 2000*



Podstawą sukcesu Windows 2000 jest zintegrowanie Active Directory i usług bezpieczeństwa podsystemu. Wszystkie obiekty katalogowe, do których dostęp można uzyskać, wymagają uwierzytelniania (przeprowadzanego przez podsystem bezpieczeństwa), a następnie sprawdzenia poprawności zezwolenia na dostęp (przeprowadzają je: podsystem bezpieczeństwa oraz monitor wzorcowego bezpieczeństwa). Monitor wzorcowego bezpieczeństwa, który rezyduje w trybie jądra, narzuca kontrolę dostępu do obiektów w Active Directory.

Podsystem bezpieczeństwa

Jak już wcześniej wspomniano, Active Directory jest składnikiem *Local Security Authority*. Składniki podsystemu bezpieczeństwa działają w kontekście procesu *Lsass.exe* i zawierają następujące elementy:

- *Local Security Authority*,
- usługa *Net Logon*,
- usługa *Security Accounts Manager*,
- usługa *LSA Server*,
- *Secure Sockets Layer*,
- protokoły uwierzytelniania *Kerberos V5* i NTLM.

Podsystem bezpieczeństwa monitoruje założenia bezpieczeństwa i w efekcie ma wpływ na cały system operacyjny.

Local Security Authority (LSA)

Local Security Authority (*LSA*) jest modułem chronionym, który utrzymuje bezpieczeństwo lokalne systemu (zwane założeniami bezpieczeństwa lokalnego — *Local Security Policy*).

Generalnie LSA pełni cztery podstawowe funkcje:

- zarządza założeniami bezpieczeństwa lokalnego,
- dostarcza interaktywnych usług logowania użytkownika,
- generuje znaczniki, zawierające informacje o użytkownikach i grupach, dotyczące przywilejów użytkownika w zakresie bezpieczeństwa,
- zarządza zasadami i ustawieniami nadzorowania oraz zapisuje ostrzeżenia do właściwego dziennika systemowego.

Zasady bezpieczeństwa lokalnego identyfikują następujące elementy:

- domeny zaufane w celu uwierzytelnienia procesów uwierzytelniania użytkowników,
- użytkowników posiadających możliwość dostępu do systemu i ich własnych metod (dostępu lokalnego, zdalnego lub poprzez usługę),
- użytkowników, którym nadano przywileje,
- poziom kontroli bezpieczeństwa,
- domyślne ilości przydzielanej pamięci.

LSA zawiera następujące, wymienione niżej, komponenty.

- *Netlogon.dll* — usługa bezpiecznie przekazująca kontrolerowi domen uwierzytelnienia użytkowników i zwracająca identyfikatory bezpieczeństwa domen (*Domain Security Identifiers* — SID) oraz prawa użytkownika. W przypadku kontrolerów domen w systemie Windows NT 4.0 działa ona także jako protokół replikacji.
- *Msv1_0.dll* — protokół uwierzytelniania *NT Lan Manager* (*NTLM*) stosowany wobec klientów, które nie wykorzystują uwierzytelniania przez *Kerberos*.
- *Schannel.dll* — protokół uwierzytelniania *Secure Sockets Layer* (*SSL*), który zapewnia uwierzytelnianie na szyfrowanym kanale.
- *Kerberos.dll* — protokół uwierzytelniający *Kerberos V5* zapewniający uwierzytelnianie Windows 2000.
- *Kdcsvc.dll* — usługa *Kerberos Key Distribution Center* (*KDC*) odpowiedzialna za przyznawanie znaczników klientom.
- *Lsasrv.dll* — usługa serwera LSA narzucająca zasady bezpieczeństwa.

- *Samsrv.dll* — usługa *Security Accounts Manager* (*SAM*) przechowująca lokalne konta bezpieczeństwa, narzucająca lokalnie przechowywane zasady oraz obsługująca API.
- *Ntdsa.dll* — moduł usług katalogowych obsługujący protokół replikacji Windows 2000 i protokół LDAP oraz zarządzający partycjami danych.
- *Secur32.dll* — operator wielokrotnego uwierzytelniania łączący wszystkie aplikacje.

Architektura usługi katalogowej

Działanie Active Directory opiera się na architekturze warstwowej, w której warstwy reprezentują działania serwerów dostarczające usług katalogowych aplikacjom klientów. Active Directory składa się z trzech warstw usług, wielu interfejsów i protokołów, które, współdziałając ze sobą, dostarczają usług katalogowych. Tymi trzema warstwami są:

- *Directory System Agent* (*DSA*),
- warstwa bazodanowa (*Database Layer*),
- silnik bazy danych (*Extensible Storage Engine — ESE*).

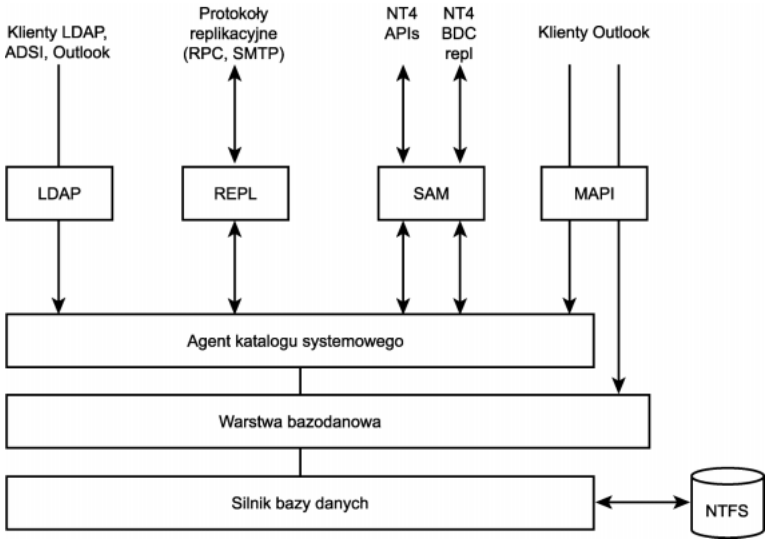
Warstwy te przechowują różne rodzaje informacji wymagane do lokalizowania wpisów w katalogowej bazie danych. W tej architekturze ponad warstwami usług znajdują się protokoły i API (API zlokalizowane są tylko na klientach) umożliwiające komunikację pomiędzy klientami a usługami katalogowymi lub też pomiędzy dwiema usługami katalogowymi w przypadku replikacji.

Na rysunku 2.2 widzimy dwie warstwy usług w Active Directory, ich poszczególne interfejsy i protokoły. Kierunki, w jakie zwrócone są strzałki, pokazują, jak poprzez interfejsy klienty uzyskują dostęp do Active Directory. Klienty LDAP oraz *Messaging API* (*MAPI*) mają dostęp do katalogu za pomocą wywoływania funkcji wskazanych przez jednokierunkowe strzałki do agenta katalogu systemowego. Baza danych SAM funkcjonuje jako osobna biblioteka dołączana dynamicznie (DLL) i może wywoływać jedynie punkty wejścia wysłane przez agenta katalogu systemowego. Wszystkie inne składniki, poza silnikiem bazy danych (*Esent.dll*), znajdują się w *Ntdsa.dll* i są połączone z funkcjami, które miały wywoływać. Ze względu na taki układ pomiędzy bibliotekami wymagane jest istnienie trójkierunkowej interakcji.

Główne składniki usług wymieniamy poniżej.

- *Directory System Agent* (*DSA*) — tworzy hierarchię ze struktury domeny przechowywanej w katalogu oraz dostarcza API który umożliwia wykonywanie wywołań dostępu do katalogu.
- Warstwa bazodanowa — dostarcza abstrakcyjnej warstwy pomiędzy aplikacjami i bazą danych. Przechodzą przez nią wywołania z aplikacji. Nigdy nie wykonuje się wywołań bezpośrednio do bazy danych.

Rysunek 2.2. *Warstwy usług Active Directory i odpowiadające im interfejsy*



- Silnik bazy danych (ESE) — komunikuje się z zapisami w danych katalogowych opartych na atrybucie obiektów zwanym względnie wyróżnioną nazwą.
- Magazyn danych (*Ntds.dit*) — element bazy danych Active Directory. Może być zmieniany tylko przez silnik bazy danych ESE. Plikiem tym można administrować za pomocą *Ntdsutil*, narzędzia wywoływanego z wiersza poleceń (więcej informacji o tym narzędziu znajduje się w dodatku A).

Klienty uzyskujące dostęp do Active Directory stosują jeden z poniższych interfejsów obsługiwanych przez Active Directory.

- LDAP/ADSI — protokół uproszczonego dostępu do katalogów (*Lightweight Directory Access Protocol — LDAP*) oraz interfejsy usługi Active Directory (*Active Directory Service Interfaces — ADSI*).
- MAPI — *Messaging API*, stosowane przez program Microsoft Outlook. Klienty Outlooka łączą się z agentem DSA przez zdalne wywołanie procedury (*Remote Procedure Call — RPC*) operatora interfejsu książki adresowej.
- SAM — emulacja starszej wersji systemu, łączy się z DSA, opierając się na głównej bazie danych użytkowników SAM. Zapasowe kontrolery domen dla trybu mieszanego wykorzystują też interfejs bazy danych SAM do replikacji.
- REPL — agenci DSA w Active Directory, łączą się ze sobą za pomocą własnych interfejsów RPC podczas replikacji katalogowej.
- RPC — zdalne wywołanie procedury (*Remote Procedure Call*) stosowane dla TCP/IP w celu transmisji i synchronizacji informacji w szybkich, niezawodnych sieciach. Działa także jako interfejs zezwalający na zdalne przeprowadzanie operacji systemowych.

Agent katalogu systemowego (DSA)

Agent katalogu systemowego (DSA) jest procesem zachodzącym po stronie serwera, który tworzy egzemplarz usługi katalogowej i dostarcza dostęp do danych katalogowych. Klienty wykorzystują jeden z obsługiwanych interfejsów do uzyskania połączenia z DSA w celu odniesienia się do obiektów Active Directory, zarządzania nimi i ich atrybutami.

Warstwa DSA zapewnia identyfikację obiektów, obsługę replikacji oraz narzucenie odniesień i schematu.

Warstwa bazodanowa

Warstwa bazodanowa zapewnia obiektowy wgląd w informacje o bazie danych Active Directory oraz zapobiega bezpośredniemu dostępowi górnych warstw usługi katalogowej do leżącego poniżej systemu bazodanowego. Warstwa ta jest wewnętrznym interfejsem, przechodzą przez nią wszystkie wywołania i żądania. Nie jest możliwy bezpośredni dostęp do silnika bazy danych.

Silnik bazy danych

Silnik bazy danych (ESE) przechowuje wszystkie dane Active Directory w pliku *ntds.dit* i jest zbudowany na podstawie bazy danych ESE z programu Microsoft Exchange. Wersją tej bazy danych w Windows 2000 jest *Esent.dll*. Według Microsoftu ESE może obsługiwać bazę danych do wielkości 16 TB. Testy wykazały, że jest w stanie utrzymywać do 40 milionów obiektów na domenę.

Active Directory posiada predefiniowany schemat, który określa wszystkie wymagane i możliwe dla danego obiektu atrybuty. ESE rezerwuje obszar tylko dla używanej przestrzeni (wyłącznie atrybuty z wartościami) i rozszerza się w miarę dodawania atrybutów. Gdy pracujesz w sieci, możesz wykonać kopie zapasowe ESE.

Więcej informacji o przechowywaniu danych znajdziesz w podrozdziale „Przechowywanie danych" przy końcu tego rozdziału.

Protokoły, interfejsy i usługi Active Directory

Model danych w Active Directory pochodzi z informacyjnego modelu obiektów i atrybutów (lub własności) X.500. Na przykład atrybuty obiektu użytkownika mogłyby zawierać informacje o nazwie użytkownika, jego numer telefonu oraz adres e-mail. Należy zauważyć, że Active Directory nie jest katalogiem modelu X.500. Nie implementuje protokołów modelu X.500, które to zawierają *Directory Access Protocol* —

DAP, *Directory System Protocol — DSP*, *Directory Information Shadowing Protocol — DISP* oraz *Directory Operational Binding Management Protocol — DOP*. LDAP dostarcza najważniejszych funkcji oferowanych przez DAP i jest zaprojektowane do pracy na TCP/IP, bez dodatkowych kosztów związanych z kapsułkowaniem protokołów modelu OSI poprzez TCP/IP.

Usługa katalogowa X.500

Model informacji w Active Directory pochodzi z modelu informacyjnego X.500. Definiuje rozmaite protokoły komunikacji, których nie implementuje Active Directory. Protokoły te to:

- *DAP — Directory Access Protocol*,
- *DSP — Directory System Protocol*,
- *DISP — Directory Information Shadowing Protocol*,
- *DOP — Directory Operational Binding Management Protocol*.

Active Directory nie implementuje tych protokołów ze względu na małe nimi zainteresowanie, które wynika z tego, że protokoły te zależne są od sieci opartych na modelu OSI, alternatywnie dla TCP/IP, który nie został powszechnie zaimplementowany (z powodu niskiej efektywności transportu). LDAP dostarcza najważniejsze funkcje oferowane przez DAP i DSP i jest zaprojektowany do pracy na TCP/IP bez dodatkowych kosztów administracyjnych.

Lightweight Directory Access Protocol (LDAP)

W Active Directory LDAP służy zarówno jako protokół, jak i API. LDAP jest podstawowym protokołem Active Directory, co oznacza, że jest jedynym protokołem komunikacji obsługiwanym przez Active Directory. API dla LDAP zapewnia dostęp do protokołu LDAP. Protokół LDAP wykorzystywany jest przez ADSI.

LDAP jest protokołem komunikacyjnym, co oznacza, że zarządza kapsułkowaniem przeprowadzanym przez klienta i serwer oraz wysyła żądania transmisji.

LDAP był początkowo stosowany z katalogami modelu X.500. LDAPv3 to standard przemysłowy, który może być stosowany z jakąkolwiek usługą katalogową implementującą protokół LDAP. Active Directory obsługuje wersje LDAPv2 oraz LDAPv3.

Wersja LDAPv3 jest kompatybilna ze starszą wersją — LDAPv2. Wymogiem wersji LDAPv3 jest, aby klienty LDAPv2 też mogły się z nią połączyć.

Interfejsy usługi Active Directory — Active Directory Services Interface (ADSI)

Podstawowym i zalecanym API dla Active Directory jest ADSI. Udostępniając obiekty przechowywane w katalogu jako obiekty COM, ADSI dostarcza prostego, zorientowanego obiektowo interfejsu o dużych możliwościach. ADSI składa się z interfejsów programowania obiektów COM. Obiektu katalogowego używamy, stosując metody na jednym lub większej liczbie interfejsów COM. Implementując wymagane interfejsy, operatory ADSI tłumaczą je na wywołania konkretnych usług katalogowych.

ADSI ułatwia programistom i administratorom tworzenie programów za pomocą wysokopoziomowych narzędzi, takich jak Microsoft Visual Basic, Java, C lub Visual C++, bez potrzeby troszczenia się o podstawowe różnice pomiędzy różnymi przestrzeniami nazw.

ADSI umożliwia też budowanie lub kupowanie programów, które dają pojedynczy punkt dostępu do wielu katalogów w sieci, niezależnie od tego, czy są oparte na LDAP, czy na innym protokole. ADSI można zmieniać za pomocą pisanych skryptów, co jest wygodne dla administratorów.

ADSI ukrywa przed użytkownikami szczegóły dotyczące LDAP. Jest to interfejs prostszy w strukturze niż API LDAP.

Replikacja w Active Directory

Replikacja w Active Directory zachodzi poprzez protokoły transmisji replikacji. Active Directory przeprowadza replikację na różne sposoby, w zależności od tego, czy znajduje się wewnątrz lokacji, czy pomiędzy lokacjami (międzylokacyjna). W przypadku replikacji wewnątrz lokacji Active Directory stosuje protokoły transportu RPC ponad IP. W międzylokacyjnej replikacja Active Directory posługuje się wyborem dwóch protokołów replikacji: IP (RPC ponad IP) i *Simple Mail Transfer Protocol* (*SMTP* ponad IP).

RPC ponad IP jest stosowane zawsze, poza jednym wyjątkiem — w wypadku gdy zachodzi ruch związany z replikacją międzylokacyjną pomiędzy różnymi kontrolerami domen w odmiennych domenach i administrator zdecydował się na wybór SMTP.

Więcej informacji o replikacji w Active Directory znajduje się w rozdziale 8. „Zarządzanie lokacjami, replikacją i ruchem w sieci”.

Podstawy struktury logicznej

Zasoby w Active Directory organizuje się w strukturę logiczną, która umożliwia definiowanie i grupowanie zasobów tak, że mogą być lokowane według nazw, a nie lokalizacji fizycznej. W poprzednich wersjach Microsoft Exchange zasoby były tradycyjnie organizowane jako „siedziby” i „serwery” ze względu na wygodę administracji. Zasoby wActive Directory zawierają obiekty, jednostki organizacyjne, domeny, drzewa i lasy.

Hierarchia domen

W Windows 2000 domena definiuje zarówno granicę administracyjną, jak i granicę bezpieczeństwa dla zbioru obiektów, które są istotne dla konkretnej grupy użytkowników w sieci. Przywileje administracyjne nie rozszerzają się od jednej domeny do innych, a założenia bezpieczeństwa domeny odnoszą się tylko do kont bezpieczeństwa wewnątrz niej.

Active Directory składa się z jednej lub więcej domen. Domena jest granicą bezpieczeństwa sieci opartej na Windows NT lub Windows 2000, w której przywileje nadawane w jednej domenie nie przenoszą się na inne. Wszystkie obiekty i jednostki organizacyjne istnieją tylko wewnątrz domeny. Stąd też domena w Windows 2000, podobnie do domeny w Windows NT 4.0, może zawierać komputery, grupy i kontakty.

Do korzyści z organizowania sieci w domeny możemy zaliczyć:

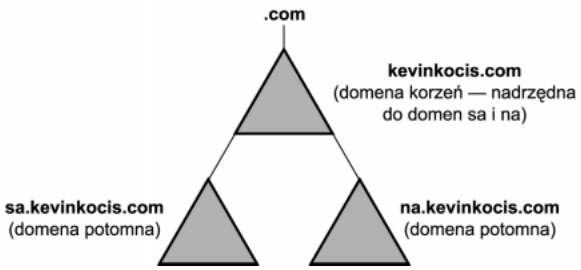
- możliwość ustanowienia zasad bezpieczeństwa (prawa i uprawnienia administracyjne), które nie przechodzą przez granice domen,
- możliwość delegowania uprawnień administracyjnych przez domenę lub jednostkę organizacyjną w celu zmniejszenia liczby administratorów z uprawnieniami na poziomie całej sieci,
- możliwość przechowywania informacji obiektowej wewnątrz specyficznej domeny.

Domeny są jednostkami replikacji, mogą otrzymywać zmiany Active Directory i replikować je do innych kontrolerów domen. Wszystkie kontrolery domen przetrzymują modyfikowalną kopię Active Directory.

Posiadanie kilku domen w sieci nie zawsze jest korzystne. Więcej informacji na ten temat znajduje się w rozdziale 5. „Bezpieczeństwo w Active Directory".

Domeny mogą być organizowane hierarchicznie w związki rodzic-dziecko. Jak wspominaliśmy wcześniej, domena nadrzędna jest domeną bezpośrednio wyższą w hierarchii względem jednej lub więcej podległych bądź potomnych domen.

Rysunek 2.3.
Hierarchia domen w Windows 2000



Ta hierarchiczna struktura różni się od płaskiej struktury domen w poprzednich wersjach NT. Hierarchia domenowa w Windows 2000 umożliwia przeszukiwanie licznych domen w jednym zapytaniu, ponieważ każda z nich zawiera informacje o domenach

nadrzędnych i potomnych. Eliminuje to potrzebę dokładnej znajomości lokalizacji obiektu, jeśli chce się go odnaleźć. W poprzednich wersjach NT, chcąc zlokalizować obiekt, trzeba było znać domenę i serwer, w których znajdował się obiekt. W dużych sieciach było to nieefektywne.

Nazwy domen w Active Directory

Active Directory używa hierarchicznych standardów nazewniczych dla domen i komputerów. Obiekty domenowe i komputerowe istnieją w hierarchii domen DNS i domen Active Directory.

Mimo że te hierarchie domen mają identyczne nazwy, to reprezentują osobne przestrzenie nazw.

Konwencje nazewnicze w systemie DNS

Active Directory stosuje standardy przestrzeni nazw pochodzące z systemu DNS, aby móc obsługiwać mapowanie nazw domen DNS na adresy IP.

Kontrolery domen w Active Directory są identyfikowane ze względu na ich specyficzne usługi, takie jak serwery LDAP, kontrolery domen i serwery przechowujące *katalog globalny*.

Hierarchia DNS jest narzucona przez następujące wymagania:

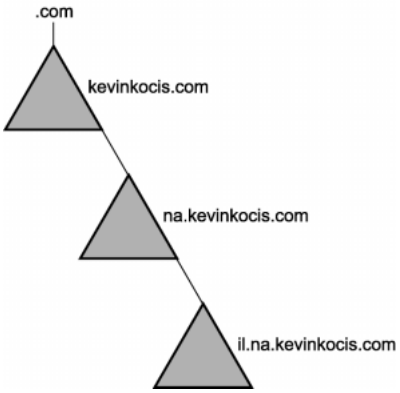
- domena potomna może mieć tylko jedną domenę nadrzędną,
- dwóch potomków tej samej domeny nadrzędnej nie może mieć tej samej nazwy.

Ponieważ domeny Active Directory stosują nazwy DNS, oba te standardy odnoszą się do domen Active Directory.

W konwencji nazw sytemu DNS kropka (.) oddziela każdą część nazwy DNS, tak samo jak nazwę domeny w hierarchicznej strukturze drzewiastej Active Directory.

Przykładowo: w DNS nazwie *il.na.kevinkocis.com* wszystkie wyrażenia *il*, *na*, *kevinkocis* oraz *com* odnoszą się do domeny DNS. Jak przedstawiono na rysunku 2.4, w Active Directory nazwa domeny *il.na.kevinkocis.com* reprezentuje hierarchię, w której *kevinkocis.com* jest domeną nadrzędną (najwyższą w hierarchii), *.na* jest domeną potomną *kevinkocis.com*, a *.il* jest domeną potomną *na.kevnikocis.com*.

Domena *.com* znajduje się na zewnątrz Active Directory, pomimo że wydaje się częścią nazwy domeny. Domeny, takie jak *.com*, *.org* i *.edu*, są domenami najwyższego poziomu, stosowanymi w Internecie do klasyfikowania organizacji według ich typów.



Rysunek 2.4. *Hierarchia w Active Directory wraz z nazwami DNS*

Hierarchia domen jest tworzona jako rezultat ciągłego schematu przestrzeni nazw, w którym każdy podległy poziom odnosi się do poprzedniego poziomu.

Ponieważ każda domena Windows 2000 posiada nazwę DNS (*kevinkocis.com*) i każdy komputer oparty na Windows 2000 posiada także nazwę DNS (*dc1.kevinkocis.com*), to domeny i komputery są reprezentowane zarówno jako obiekty w Active Directory, jak i węzły w systemie DNS.

Warto jednak zauważyć, że obiekt konta domeny komputera jest w innej przestrzeni nazw niż zapis węzła DNS, który reprezentuje ten sam komputer w przestrzeni DNS.

Struktura drzew i lasów

Liczne domeny mogą zostać połączone w struktury zwane drzewami i lasami domenowymi. Domeny w Active Directory są tworzone w odwróconej strukturze drzewa (podobnie jak w systemie DNS), gdzie korzeń znajduje się na szczycie. Hierarchie w Active Directory są połączone dwukierunkowymi, przechodnimi relacjami zaufania.

Liczba relacji zaufania wymaganych do połączenia domen wynosi n–1, przy czym n oznacza liczbę wszystkich domen.

Jeśli domeny w tej samej sieci wymagają różnych przestrzeni nazw, należy utworzyć osobne drzewo dla każdej przestrzeni nazw. Nieciągłe, połączone relacjami zaufania, drzewa tworzą las. Pojedyncze drzewo bez związków z innymi drzewami jest lasem składającym się z jednego drzewa.

Związki w strukturze Windows 2000 dla całego lasu są przechowywane w Active Directory jako obiekty kont relacji zaufania w kontenerze systemowym wewnątrz specjalnej partycji domeny katalogowej. Informacje o połączeniach wybranej domeny z domeną nadrzędną są dodawane do danych konfiguracyjnych, replikowanych do każdego drzewa w lesie. W ten sposób każdy kontroler domen w lesie zna strukturę drzew całego lasu, włącznie ze znajomością połączeń pomiędzy drzewami.

Drzewa

Drzewo jest hierarchicznym pogrupowaniem jednej lub więcej domen posiadających wspólną strukturę nazw. Końcówki drzewa są zwykle obiektami. Węzły w drzewie (punkty, w których drzewo się rozgałęzia) są kontenerami, zawierającymi grupę obiektów lub inne kontenery. Drzewo pokazuje, jak połączone są obiekty albo jak wygląda ścieżka od jednego z nich do drugiego (rysunek 2.3).

Standardowe nazwy DNS są wykorzystywane do reprezentowania struktury drzew (na przykład *na.kevinkocis.com*). Pierwsza domena w drzewie zwana jest domeną-korzeniem (w tym przypadku, *kevinkocis*). Dodatkowe domeny w tym samym drzewie zwane są domenami potomnymi. *Na.kevinkocis.com* jest domeną potomną dla *kevinkocis.com*.

Active Directory uważane jest za przestrzeń nazw, a wszystkie domeny posiadające wspólną domenę-korzeń tworzą ciągłą przestrzeń nazw.

Drzewa domen w Windows 2000 rozciągają się w Active Directory przedsiębiorstwa. Wszystkie domeny danego przedsiębiorstwa muszą należeć do drzewa domenowego tego przedsiębiorstwa. Te przedsiębiorstwa, które muszą obsługiwać nieciągłe nazwy DNS dla swych domen, są zmuszone do utworzenia lasu.

Lasy

Las może składać się z jednego lub więcej drzew nietworzących ciągłej przestrzeni nazw. Lasy pozwalają organizacjom na grupowanie oddziałów, które funkcjonują niezależnie, ale i tak muszą się komunikować. Lasy posiadają domeny-korzenie, czyli pierwsze domeny w lesie, które są niezbędne do ustalania relacji zaufania pomiędzy drzewami domen. Las funkcjonuje jako zestaw wzajemnie powiązanych obiektów oraz relacji zaufania. Domeny w drzewach i lasach również współdzielą wspólny schemat i informacje o konfiguracji. Stąd też organizacja w programie Exchange może rozciągać się na cały las, ale nie na kilka lasów.

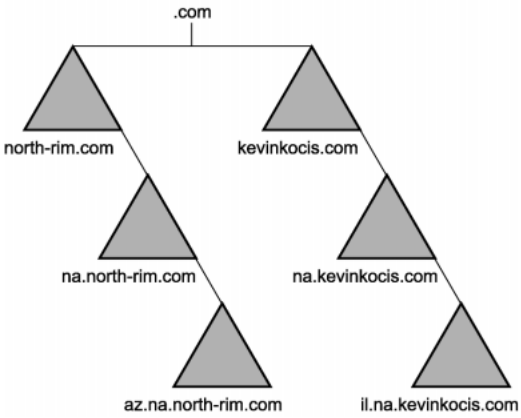
Lasy będą ewoluować głównie ze spółek i fuzji przedsiębiorstw. Będzie to zależało od bieżącej struktury katalogowej każdej firmy.

Większą liczbę lasów i relacji zaufania można utworzyć pomiędzy konkretnymi domenami w różnych lasach. Umożliwia to zapewnienie dostępu do zasobów i kont, znajdujących się na zewnątrz konkretnego lasu. Jednak w przypadku programu Exchange infrastruktura nie może rozciągać się na więcej niż jeden las.

Związki zaufania tworzone pomiędzy domenami w różnych lasach są domyślnie jednokierunkowe i nieprzechodnie.

Rysunek 2.5 przedstawia związki w lesie. Lasy są na szczycie hierarchii składającej się z drzew zawierających domeny. Domeny składają się z innych domen lub jednostek organizacyjnych.

Rysunek 2.5.
Struktura lasu w Active Directory



Nazwa wyróżniająca (Distinguished Name — DN)

Nazwa wyróżniająca jest unikalna i identyfikuje pojedynczy obiekt w sieci. LDAP nazywa osobno każdy obiekt w sieci dzięki liście oddzielonych przecinkami wartości. Pełna ścieżka dostępu do obiektu jest identyfikowana za pomocą nazwy DN.

W Active Directory nie mogą istnieć dwie identyczne nazwy wyróżniające. Jeśli takie nazwy pojawią się w tej samej grupie (na przykład dwóch użytkowników nazywających się Chris Smith, pracujących w dziale zarządzania w tej samej lokacji), może być konieczna zmiana konwencji nazewniczej.

Nazwa wyróżniająca zawiera informacje dla klienta LDAP niezbędne do pobrania danych o obiekcie z katalogu.

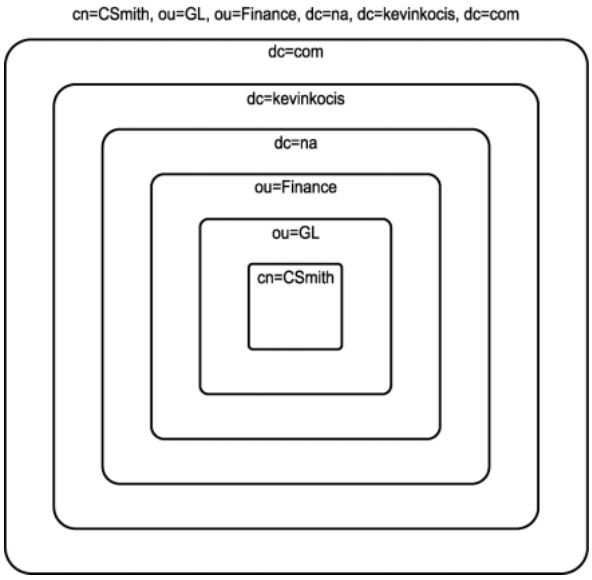
Na przykład użytkownik nazywający się Chris Smith pracuje w wydziale finansów wymyślonej przez nas firmy. Jego konto użytkownika jest tworzone w jednostce organizacyjnej, która przechowuje konta pracowników wydziału finansowego, pracujących z księgą główną (GL). Identyfikator użytkownika dla Chrisa Smitha to `Csmith` (on sam pracuje w północnoamerykańskim oddziale tej firmy). Domeną-korzeniem firmy jest *kevinkocis.com*, a domeną lokalną jest *na.kevinkocis.com*. DN dla tego konta wyglądałby następująco:

```
cn=Csmith,ou=GL,ou=Finance,dc=na,dc=kevinkocis,dc=com
```

Rysunek 2.6 przedstawia warstwy wyznaczające nazwę wyróżniającą.

Należy zauważyć, że każda część DN jest powiązana z klasą obiektu schematem nazw zaadaptowanym z protokołu LDAP. Istnieją trzy ważne zasady przy używaniu atrybutów klas, wymieniamy je poniżej.

- Atrybut *DC* jest przyznawany składnikom systemu DNS.
- Atrybut *OU* jest przyznawany jednostkom organizacyjnym.
- Atrybut *CN* jest przyznawany wszystkim innym atrybutom.



Rysunek 2.6. *Nazwa wyróżniająca dla obiektu użytkownika Chris Smith*

Nazwę wyróżniającą czyta się, rozpoczynając od nazwy najbardziej szczegółowej i kończąc na najbardziej ogólnej, czyli od lewej do prawej. W przypadku nazw wyróżniających w LDAP rozpoczynają się one od lewej i kończą po prawej nazwą korzenia.

Moduły z MMC nie wyświetlają skrótów LDAP domenowego składnika atrybutów nazw (`dc=`), jednostki organizacyjnej (`ou=`) ani wspólnej nazwy (`cn=`). Te skróty pokazywane są tylko w celu zilustrowania sposobu, w jaki LDAP rozpoznaje części nazwy wyróżniającej. Większość narzędzi w Active Directory umożliwia zobaczenie nazw obiektów w formie kanonicznej (ponieważ nazwy wyróżniające są trudne do zapamiętania), co opiszemy w dalszej części tego rozdziału.

Każda część nazwy wyróżniającej jest wyrażana w formie `typ_atrybutu=wartość` (na przykład `cn=Csmith`).

Względna nazwa wyróżniająca

Względna nazwa wyróżniająca obiektu (*Relative Distinguished Name — RDN*) jest częścią nazwy odróżniającej ten obiekt od innych w jego hierarchii nazw. Sama nazwa obiektu (atrybut *CN*), występująca oddzielnie od ścieżki obiektu, jest zdefiniowana przez RDN.

Na rysunku 2.6 w poprzednim podrozdziale RDN obiektu jest `Csmith`. Dozwolona maksymalna długość RDN wynosi 255 znaków, ale schemat narzuca bardziej wyspecyfikowane ograniczenia. Przykładowo typ atrybutowy *cn*, często stosowany do określania RDN, jest ograniczony do 64 znaków.

RDN w Active Directory są unikatowe wewnątrz konkretnego kontenera nadrzędnego. Active Directory nie zezwala na istnienie dwóch identycznych RDN w tym samym kontenerze nadrzędnym, ale mogą one istnieć w różnych hierarchiach.

Dwa obiekty mogą mieć identyczne RDN, ale wciąż pozostawać unikatowe, ponieważ wewnątrz własnych kontenerów nadrzędnych ich DN nie są takie same. Patrząc kategoriami LDAP, obiekt `cn=Csmith,dc=na,dc=kevinkocis,dc=com` jest identyfikowany jako inny niż `cn=Csmith,dc=kevinkocis,dc=com`.

RDN każdego obiektu jest przechowywana w bazie danych Active Directory i zawiera referencję do jego obiektu nadrzędnego.

Atrybuty nazywania

Active Directory korzysta ze standardów nazewniczych atrybutów zaproponowanych w serii dokumentów *Request For Comments* (*RFC*) *2253*, ale nie implementuje wszystkich standardów. Na przykład Active Directory nie stosuje pewnej nomenklatury, co zaraz zostanie opisane.

W Active Directory typ atrybutowy, stosowany do opisywania RDN obiektu (w tym przypadku, `cn=`), został zdefiniowany jako atrybut nazywania. Przykładowo w klasie *User* atrybut *cn* (*Common Name*) jest atrybutem nazywania. Z tego powodu RDN dla użytkownika *Csmith* jest wyrażana jako `cn=Csmith`.

Atrybuty nazywania przedstawione w tabeli 2.1 są stosowane w Active Directory, jak zostało to opisane w RFC 2253.

Tabela 2.1. *Atrybuty nazywania w Active Directory (domyślne)*

Klasa obiektu	Nazwa wyświetlana	Nazwa atrybutu nazywania LDAP
User	Nazwa wspólna (*Common-Name*)	*cn*
Organizational Unit	Nazwa jednostki organizacyjnej (*Organizational-Unit-Name*)	*ou*
Domain	Składnik domenowy (*Domain-Component*)	*dc*

Inne atrybuty nazywania opisane w RFC 2253 (`o=organizacja` i `c=kraj/region`) nie zostały zaimplementowane do Active Directory, pomimo faktu, że są rozpoznawane przez LDAP.

Atrybutów nazywania (takich jak DN i RDN) używa się tylko przy programowaniu pod LDAP, użytkowaniu ADSI czy innych języków skryptowych lub języków programowania.

Tożsamość i unikalność obiektów

Każdy obiekt w Active Directory posiada unikatową tożsamość, nawet jeśli został on przeniesiony lub usunięty. Tożsamość obiektu jest zdefiniowana poprzez globalnie unikalny identyfikator (*Globally Unique Identifier — GUID*), 128-bitowy numer przyznawany przez systemowego agenta katalogowego (DSA) w czasie tworzenia obiektu. GUID jest stale przechowywany w atrybucie *objectGUID* obecnym w każdym obiekcie. Atrybut *objectGUID* jest zabezpieczony i nie może być zmieniany ani usuwany.

Zwykle nazwę GUID czyta się jako „głid".

Formaty nazw w Active Directory

Active Directory obsługuje wiele formatów nazw obiektów. Formaty te zależą od sposobu, w jaki obiekt został utworzony. Active Directory wyświetla nazwy w formacie kanonicznym, co przedstawia poniższa lista. Wymienione tu formaty są obsługiwane przez Active Directory i oparte na nazwach wyróżniających protokołu LDAP.

- LDAP *Distinguished Name* — wersje LDAPv2 i LDAPv3 rozpoznają standardowe konwencje nazw, w których `cn` oznacza nazwę wspólną, `ou` — jednostkę organizacyjną, `o` — organizację, `c` — kraj/region. Active Directory implementuje składnik domenowy (`dc`) zamiast oznaczającego organizację i nie obsługuje `c` oznaczającego kraj/region. Przykładowo:

  ```
  Cn=csmith,ou=gl,ou=finance,dc=na,dc=kevinkocis,dc=com
  ```

- LDAP *Uniform Resource Locator* (*URL*) — Active Directory wspomaga dostęp LDAP dla każdego klienta obsługującego LDAP. URL w protokole LDAP nazywa serwer posiadający usługi Active Directory i DN obiektu. Przykładowo:

  ```
  LDAP://server1.na.kevinkocis.com/cn=smith,ou=gl,ou=finance,dc=na,dc=kevinkocis,
    dc=com
  ```

- *Active Directory Canonical Name* — w interfejsach użytkowników w Windows 2000 nazwy obiektów są domyślnie wyświetlane według nazw kanonicznych (potocznych), przy wykorzystaniu nazw domen DNS (oddzielonych kropkami). Odpowiednia nazwa kanoniczna dla poprzedniego przykładu wyglądałaby następująco:

  ```
  na.kevinkocis.com/finance/gl/csmith
  ```

Jeśli nazwa jednostki organizacyjnej posiada znak (/), na przykład nazwa OU to *finance/gl*, system wymaga specjalnego znaku sterującego w formie ukośnika (\). Robi się to dla rozróżnienia pomiędzy znakiem (/) oddzielającym nazwę kanoniczną i znakiem (/) będącym też częścią nazwy jednostki organizacyjnej.

Nazwa kanoniczna pojawiająca się we właściwościach *Active Directory Users and Computers* (Użytkownicy i komputery usługi Active Directory) wyświetla znak sterujący, występujący zaraz po znaku *forward slash* (/) w nazwie jednostki organizacyjnej. Na przykład, jeśli nazwą jednostki organizacyjnej jest *Fiance/GL*, a nazwa domeny to *Kevinkocis.com*, nazwa kanoniczna wyświetlana jest jako *Kevinkocis.com/Finance\/GL*.

Mapowanie nazw wyróżniających dla DNS-do-LDAP

Ponieważ nazwy domen w systemie DNS tworzą kopie lustrzane nazw domen z Active Directory, może powstać zamieszanie z powodu obecnej przestrzeni nazw. Nazwy w Active Directory mają inny format, wymagany przez LDAP do identyfikowania obiektów katalogowych. Dlatego nazwy domen w systemie DNS są mapowane do nazw domen DNS i *vice versa*.

Active Directory korzysta z algorytmu do automatycznego przyznawania DN protokołu LDAP dla każdej nazwy domeny w systemie DNS. Algorytm ten dostarcza etykiety typu atrybutowego składnika domenowego każdej etykiecie w nazwie domenowej DNS. Na przykład domena DNS *na.kevinkocis.com* jest tłumaczona na DN protokołu LDAP w formie `dc=na,dc=kevinkocis,dc=com`.

Nazwy logowania użytkowników

Użytkownik uzyskujący dostęp do domeny i jej zasobów musi otrzymać nazwę logowania użytkownika. Konta użytkowników należą do kategorii *security principals* (są więc obiektami, do których zabezpieczenia nadawane są w formie uwierzytelniania i autoryzacji) i są uwierzytelniane w momencie zalogowania się do domeny lub komputera lokalnego. Są autoryzowane, kiedy otrzymują dostęp do zasobów.

Konta użytkowników należące do kategorii *security principals* posiadają dwa rodzaje nazw logowania:

- nazwa konta SAM,
- główna nazwa użytkownika (*User Principal Name — UPN*).

Nazwa konta SAM wymagana jest dla kompatybilności z poprzednimi domenami Windows NT. Nazwy kont SAM, w porównaniu do hierarchicznych nazw DNS, są nazwami płaskimi.

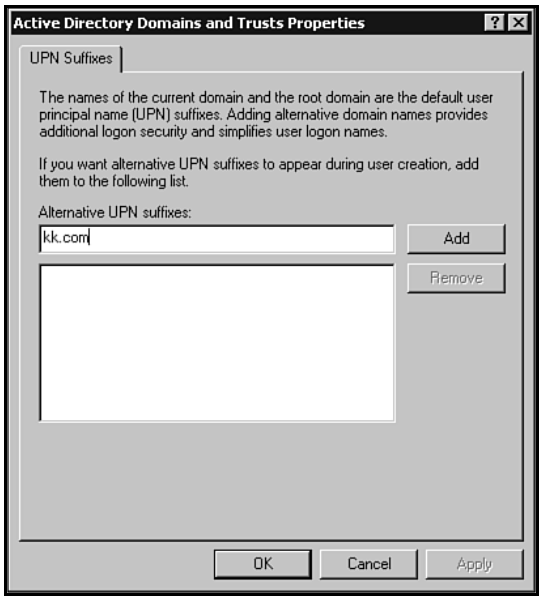
Główna nazwa użytkownika (UPN) jest nazwą „przyjazną", krótszą i łatwiejszą do zapamiętania niż DN. Składa się ze skróconej nazwy, która zwykle reprezentuje użytkownika, oraz DNS nazwy domeny, w której rezyduje obiekt użytkownik. Na przykład użytkownik Chris Smith, posiadający konto użytkownika w domenie *kevinkocis.com*, może mieć UPN *Csmith@kevinkocis.com*. Ponieważ UPN nie zależy od DN użytkownika, można przenosić obiekt użytkownika oraz nadawać mu inną nazwę bez zmiany nazwy logowania użytkownika.

UPN jest atrybutem (*UserPrincipalName*) obiektu *security principal*. Jeśli atrybut nie ma wartości, domyślną UPN jest *<nazwaużytkownika>@<nazwadomenyDNS>*.

Jeśli nie chcemy stosować domyślnej nazwy domeny (na przykład bardzo długiej nazwy DNS), można tworzyć i przyznawać dodatkowe sufiksy głównej nazwy użytkownika (*User Principal Name Suffix)*. Dlatego Chris Smith, zamiast nazwy *csmith@na.kevinkocis.com*, może używać nazwy *csmith@kk.com* (zilustrowano to na rysunku 2.7). Więcej informacji na temat tworzenia dodatkowych sufiksów do nazw UPN znajduje się w rozdziale 4. „Zarządzanie użytkownikami, grupami i komputerami".

Podstawy struktury fizycznej sieci

Active Directory rozdziela strukturę logiczną hierarchii domen od fizycznej struktury sieci. Dzięki logicznemu grupowaniu zasobów można je umiejscawiać za pomocą



Rysunek 2.7. *Dodawanie sufiksów do nazw UPN w oknie Active Directory Domains and Trusts Properties (Właściwości domen i relacje zaufania w Active Directory)*

nazw, a nie fizycznej lokalizacji. Ponieważ zasoby grupowane są logicznie, fizyczna struktura sieci jest przezroczysta dla użytkowników.

Fizyczna struktura Active Directory opiera się na lokacjach, które są kombinacjami jednej lub więcej podsieci opartych na protokole IP i połączonych szybkimi łączami.

Microsoft za szybkie łącze uważa takie, w którym przepustowość wynosi 10 milionów lub więcej bitów na sekundę. Z punktu widzenia administratorów łącze T1 można uznać za szybkie, jeśli nie jest zapchane. Administrator będzie też musiał zadecydować, czy należy tworzyć dodatkowe lokacje do kontrolowania ruchu w sieci.

Active Directory stosuje replikację w celu zapewnienia, że całość zmian w kontrolerach domen została zaktualizowana we wszystkich innych kontrolerach w danej domenie. Active Directory generuje wewnątrz lokacji topologię pierścienia służącą do replikacji pomiędzy kontrolerami w domenie. Zapewnia to przynajmniej dwie ścieżki replikacji od jednego do drugiego kontrolera domen. Replikacja może mieć miejsce nawet wtedy, gdy kontroler domeny uległ awarii lub nie jest podłączony do sieci. Jeśli doda się lub usunie kontroler domeny z sieci lub lokacji, Active Directory automatycznie rekonfiguruje topologię, aby odzwierciedlić zmianę.

Więcej informacji znajduje się w rozdziale 8. „Zarządzanie lokacjami, replikacją i ruchem w sieci".

Składniki katalogów

Active Directory posiada różnorodne obiekty pogrupowane za pomocą kontenerów (w formie jednostek organizacyjnych — OU). Katalog jest ponadto podzielony na partycje zwane katalogowymi lub *Naming Contexts*.

Obiekty

Obiekt jest w Active Directory podstawowym elementem, oddzielnym zestawem atrybutów i reprezentuje na przykład użytkownika, drukarkę, komputer lub aplikację. Atrybuty są cechami charakterystycznymi każdego obiektu zdefiniowanego w katalogu. Atrybuty obiektów zawierają informacje o lokalizacji i cechach danego obiektu. Każdy użytkownik jest również uznawany za obiekt. W Microsoft Exchange do atrybutów użytkownika wliczaliśmy: jego imię (np. Chris), nazwisko (Smith), adres e-mail (*csmith@kevinkocis.com*) i możliwość odbierania przez niego poczty elektronicznej, jej rodzajów i miejsca, gdzie mógł ją otrzymywać. Obiekty są przypisanymi zezwoleniami na dostęp i mogą być gromadzone oraz organizowane w elementy zwane kontenerami.

Nazwy obiektów

Wszystkie obiekty w Active Directory stosują się do konwencji nazewniczych, których w Active Directory jest wiele. Mimo że DNS jest efektywnym narzędziem do tłumaczenia nazw internetowych, nie przechowuje szczegółowości wymaganej dla nazewnictwa w Active Directory. LDAP jest bardziej adekwatnym narzędziem, ponieważ potrafi jednoznacznie identyfikować obiekty w Active Directory.

Kontenery

Kontenerem w drzewie katalogowym może być każdy element, do którego dodane są obiekty. Oczywistym przykładem kontenera jest folder. W każdym razie MMC można używać przy dodawaniu narzędzia do elementów innych niż foldery, które następnie również stają się kontenerami.

Podstawowym kontenerem w Active Directory jest jednostka organizacyjna.

Jednostki organizacyjne

Jednostka organizacyjna to kontener używany do przechowywania obiektów. Jest najmniejszym zasięgiem lub jednostką, do której można przydzielić lub oddelegować uprawnienia administracyjne. Jednostek organizacyjnych używamy do tworzenia w domenie kontenerów reprezentujących hierarchiczne, logiczne lub wydziałowe (biznesowe) struktury wewnątrz danej organizacji.

Wiele domen z Windows NT 4.0 przechodzących do Active Directory w Windows 2000 może być przekonwertowanych do postaci jednostek organizacyjnych w ich nowym modelu domenowym i otrzymać delegowane uprawnienia.

Jednostki organizacyjne mogą zawierać inne jednostki organizacyjne, co oznacza, że można tworzyć hierarchię kontenerów, które, jeśli jest to konieczne, mogą być rozszerzane w celu modelowania hierarchii wewnątrz domeny. Jednostki organizacyjne są również w katalogu najmniejszymi jednostkami, do których stosują się założenia grupowe.

Trzema głównymi przyczynami stosowania jednostek organizacyjnych są:

- konta organizacyjne,
- delegowanie uprawnień,
- stosowanie zasad grupowych.

Jednostka organizacyjna nie może zawierać obiektów z innych domen.

Partycje katalogowe

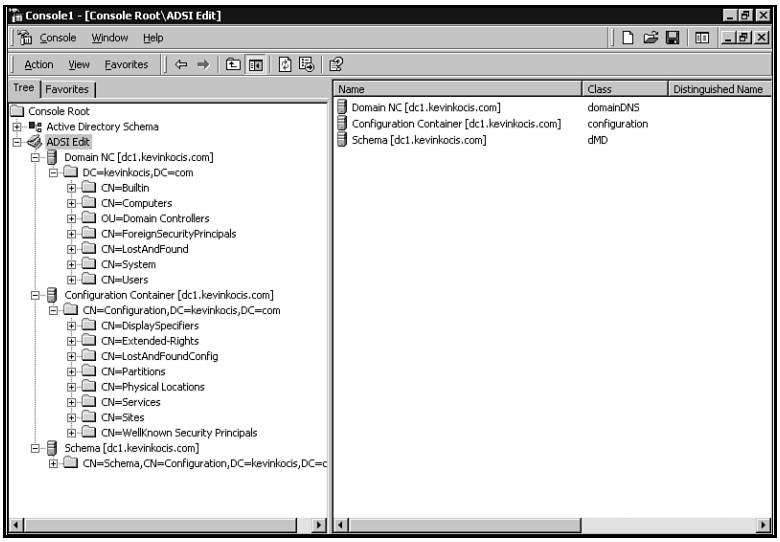
W Active Directory las jest partycjonowany na domeny. Kontrolery wewnątrz tej samej domeny współdzielą ze sobą informacje. Kontrolery z różnych domen współdzielą ze sobą konfigurację, schemat i informacje o *katalogu globalnym* (*GC*), ale nie współdzielą danych o domenach. Partycja katalogowa (*Naming Context — NC*) umożliwia dystrybucję archiwów. Wspomaga to skalowalność bazy danych w Active Directory do milionów obiektów.

Każda partycja katalogowa zawiera podkatalog obiektów w drzewie. Kopie tej partycji mogą być przechowywane pomiędzy kontrolerami domen, które są uaktualniane poprzez replikację.

Informacje o każdym kontrolerze domeny, przechowywane w Active Directory (niezależnie od tego, czy jest to serwer GC, czy nie), są partycjonowane na trzy kategorie: dane domeny, schematu i konfiguracji. Partycje katalogowe są jednostkami replikacji. Trzy, niżej opisane, partycje przechowywane są na każdym kontrolerze domeny.

- Partycja konfiguracji — zawiera informacje o topologii lokacji i replikacji oraz o partycji usług i katalogu. Dane te są wspólne dla wszystkich domen w drzewie lub lesie. Dane konfiguracyjne są replikowane do wszystkich kontrolerów domen w lesie.
- Partycja schematu — zawiera wszystkie typy obiektów (i ich atrybuty), które mogą zostać utworzone w Active Directory. Dane te są wspólne dla wszystkich domen w drzewie czy lesie. Przechowywane są w niej definicje klas i atrybutów dla wszystkich istniejących oraz możliwych obiektów. Partycja schematu jest replikowana do wszystkich kontrolerów domen w lesie.
- Partycja domeny NC — zawiera wszystkie obiekty z katalogu dla tej domeny. Aktualizacje tego kontenera są replikowane do kontrolerów wewnątrz domeny i do serwerów GC, jeśli aktualizacja jest utworzona dla atrybutu skonfigurowanego dla replikacji w GC. Podgląd partycji domenowych został przedstawiony na rysunku 2.8.

Rysunek 2.8. *Partycje domenowe — widok w edytorze ADSI Edit*



Korzystanie z edytora ADSI

Aby skorzystać z edytora ADSI (*ADSI Edit*), trzeba zainstalować zestaw narzędzi *Support Tools*, znajdujący się w folderze *Support\Tools* na dysku CD z systemem Windows 2000 Serwer. Aby rozpocząć instalację, musisz kliknąć dwukrotnie ikonę *Setup* w tym folderze.

Aby oglądać lub zmieniać wartości atrybutów za pomocą *ADSI Edit*, wykonaj poniższe kroki.

1. Wejdź kolejno do menu: *Start*, *Programs*, *Windows 2000 Support Tools*, *Tools*, *ADSI Edit*.
2. Jeśli partycja katalogowa, której atrybuty chcesz zmienić, nie jest wyświetlana, kliknij prawym przyciskiem myszy na ikonę *ADSI Edit* a później opcję *Connect to*.
3. Jeśli bieżący komputer nie jest kontrolerem domeny, na którym chcesz zmienić atrybuty, w menu *Computer* kliknij opcję *Select* albo wpisz kontroler domeny i wybierz go lub wejdź do nazwy komputera.
4. Aby wybrać partycję katalogową w menu *Connection Point*, kliknij *Naming Context*.
5. Na liście *Naming Context* kliknij partycję katalogową i *OK*.

W okienku *Name* wyświetlona zostaje nazwa wybranej partycji katalogowej. Można ją zmienić na taką, która lepiej identyfikuje dane połączenie.

6. Wybierz obiekt, którego wartości atrybutów chcesz zobaczyć lub zmienić.
7. W okienku dialogowym *Properties*, w opcji *Select Which Properties to View* kliknij jedną z alternatyw: *Optional* (Opcjonalnie), *Mandatory* (Obowiązkowo) lub *Both* (Obie).

8. W okienku *Select a Property to View* kliknij własność, którą chcesz podejrzeć.
9. Aby zmienić wartość własności, wpisz nową w okienku *Edit Attribute*.
10. Kliknij *Set*, a następnie *OK*.

Jeśli kontroler domeny jest serwerem GC, posiada również czwartą kategorię informacji — częściową replikę partycji katalogu danych domenowych.

Częściowa replika partycji katalogu danych domenowych dla wszystkich domen

Serwer katalogu globalnego przechowuje i replikuje częściową replikę partycji katalogu danych domenowych dla wszystkich innych domen w lesie. Częściowa replika zawiera podzestaw własności dla wszystkich obiektów we wszystkich domenach w lesie i jest przeznaczona tylko do odczytu. Replika kompletna jest przeznaczona i do zapisu, i do odczytu.

Każda domena jest mapowana do innej partycji katalogowej, więc obiekty należące do dwóch różnych domen mogą być utrzymywane i replikowane niezależnie. Informacje nieistotne dla całego lasu są replikowane osobno.

Nie da się zmienić nazwy obiektu korzenia, co oznacza, że nie można zmienić kontenera domeny, schematu ani konfiguracji.

Konfigurowanie partycji katalogowych

Kreator instalacji Active Directory kopiuje plik bazy danych katalogu (*Ntds.dit*) z jego położenia w katalogu *%SystemRoot%\System32* do innego, który został wyspecyfikowany przez administratora, po czym kreator konfiguruje lokalny serwer do przechowywania usługi katalogowej. Proces ten zawiera tworzenie partycji katalogowych i domyślnych założeń bezpieczeństwa domeny.

Poniższe partycje katalogowe są tworzone jako partycje domyślne na pierwszym kontrolerze w lesie i uaktualniane przez replikację na każdym kontrolerze tworzonym w lesie.

- Partycja schematu jest tworzona jako `cn=schema,cn=konfiguracja, dc=domenakorzenialasu`. Plik *schema.ini* jest używany do tworzenia domyślnych obiektów katalogowych i wyświetlania specyfikatorów oraz do implementowania domyślnego bezpieczeństwa w bazie danych katalogu.
- Partycja konfiguracji tworzona jest jako `cn=konfiguracja, dc=domenakorzenialasu`.
- Partycja domeny jest tworzona jako `dc=nazwadomeny` i zawiera założenia bezpieczeństwa dla domeny.
- Podczas tworzenia nowej domeny kreator tworzy nową partycję katalogową, zawierającą domyślne obiekty domeny.

- Podczas tworzenia dodatkowego kontrolera domeny w istniejącej domenie obiekty są uaktualniane poprzez replikację. Kreator nie tworzy domyślnych obiektów partycji domenowych.
- Podczas uaktualniania podstawowego kontrolera domen spod Windows NT 4.0 kreator tworzy założenia bezpieczeństwa domen oraz założenia lokalnego bezpieczeństwa. Przenosi również członkostwa LSA i istniejące konta.

Partycja konfiguracji

Katalogowa partycja konfiguracji jest tworzona wraz z pierwszą domeną w Windows 2000. W przyszłości partycja konfiguracji będzie replikowana do nowego kontrolera domen przy tworzeniu domen potomnych, nowych domen-korzeni lub wtedy, gdy dodatkowy kontroler zostanie dodany do domeny.

Następujące obiekty są kontenerami potomnymi wewnątrz kontenera konfiguracji (*Configuration Container*):

- *DisplaySpecifiers*,
- *Extended-Rights*,
- *LostAndFoundConfig*,
- *Partitions*,
- *Physical Locations*,
- *Sites*,
- *Services*,
- *Well-Known Security Principals*.

Pomimo że inne informacje mogą być przechowywane w kontenerze *Configuration Container*, zalecamy, żeby do tych danych odnosiły się następujące kryteria. Wymieniamy je poniżej.

- Informacje są zdefiniowane jako globalne zainteresowanie (na przykład domyślna konfiguracja i informacja o założeniach dla wszystkich instancji danej usługi w sieci).
- Informacje są szeroko dostępne, tak że odwoływanie się do informacji przechowywanych w innej domenie nie jest wystarczające.
- Ulotność informacji jest niska.
- Objętość informacji jest mała.

Informacje globalne powinny być przechowywane w jednym lub dwóch miejscach: w potomku kontenera *Services* lub w potomku obiektu lokacji.

Zarządzanie danymi konfiguracyjnymi

Różnymi częściami kontenera *Configuration Container* można zarządzać za pomocą narzędzi do administrowania załączonych do Windows 2000. Po wejściu kolejno do menu *Start*, *Programs*, *Administrative Tools* mamy dostęp do następujących narzędzi (można do nich dotrzeć również poprzez przystawki w MMC).

- *Active Directory Sites and Services* (Lokacje i usługi Active Directory).

Kontener usług (*Services*) w *Active Directory Sites and Services* (Lokacje i usługi Active Directory) jest domyślnie ukryty. Aby go odsłonić, trzeba kliknąć prawym przyciskiem myszy opcję *Active Directory Sites and Services*, wskazać *View* (Widok), a następnie *Show Services Node* (Pokaż węzeł usług).

- *Active Directory Domains and Trusts* (Domeny i relacje zaufania usługi Active Directory).
- *Active Directory Schema* (Schemat usługi Active Directory).

Przystawka schematu wymaga osobnej instalacji. Szczegóły na temat instalacji kontenera schematu znajdują się w rozdziale 9. „Zarządzanie aktualizacjami przy użyciu Flexible Single-Master Operations”.

Katalogowa partycja schematu

Schema Active Directory składa się z zestawu klas obiektów, atrybutów i składni. Schemat wyznacza zasady spójności dotyczące tworzenia i modyfikowania obiektów. Pomimo że Active Directory posiada domyślny zestaw klas i atrybutów, którego nie da się zmodyfikować, można rozszerzyć schemat przez dodawanie nowych atrybutów i klas z kwalifikowanego kontrolera domen (wzorzec schematu FSMO). Zmiany te muszą być wykonane w kontrolerze domen pełniącym rolę wzorca schematu w lesie.

Więcej informacji na temat aktywowania modyfikacji i rozszerzania schematu znajduje się w rozdziale 7. „Zarządzanie i modyfikowanie schematu Active Directory”. Natomiast swoją wiedzę o FSMO poszerzysz, czytając rozdział 9.

Do oglądania obiektów i właściwości partycji schematu można też używać narzędzia *ADSI Edit*. Przy otwieraniu *ADSI Edit* domyślnie wyświetlany jest kontener *Schema*. Aby obejrzeć atrybuty i klasy należy go rozszerzyć.

Katalogowe partycje domenowe

Przy tworzeniu nowych domen powstaje domenowa partycja katalogowa.

Obiekt korzeń w każdej partycji domenowej jest obiektem kontenerem nazywanym dla domeny DNS. Kontenery potomne kontenera domeny można oglądać za pomocą konsoli *Active Directory Users and Computers* (Użytkownicy i komputery usługi Active Directory).

Kontener domeny posiada następujące kontenery potomne:

- *Builtin*,
- *Computers*,
- *Deleted Objects*,
- *Domain Controllers*,
- *ForeignSecurityPrincipals*,
- *Infrastructure*,
- *LostAndFound*,
- *System*,
- *Users*.

Domyślnie tylko niektóre kontenery pojawiają się w oknie *Active Directory Users and Computers*. Aby oglądać wszystkie kontenery, kliknij menu *View* i wybierz *Advanced Features*.

Inaczej niż w przypadku katalogowych partycji konfiguracji i schematu pełna kopia partycji domeny jest replikowana tylko pomiędzy kontrolerami domen wewnątrz tej samej domeny, a nie do innych domen w lesie. Częściowa kopia obiektów domenowych (zawierająca wszystkie obiekty, ale ograniczony zestaw atrybutów, które zostały skonfigurowane tak, aby replikować się w katalogu globalnym) jest replikowana do wszystkich kontrolerów domen, które są skonfigurowane jako serwery GC.

Do zarządzania zawartością partycji domenowej można używać modułu *Active Directory Users and Computers* (Użytkownicy i komputery usługi Active Directory). Do zarządzania właściwościami niewyświetlanymi w *Active Directory Users and Computers* można używać *ADSI Edit*. Przy otwieraniu *ADSI Edit* jako domyślna wyświetlana jest partycja domenowa dla domeny, w której jesteś zalogowany.

Składniki kontenera System

Kontener *System* (mieszczący się w partycji domenowej) przechowuje informacje operacyjne dla każdej domeny, takie jak: lokalne bezpieczeństwo, śledzenie połączeń plikowych, spotkania sieciowe, obiekty reprezentujące inne zaufane domeny oraz składniki dla punktów połączeń RPC i Winsock.

Kontener *System* posiada następujące kontenery potomne:

- *AdminSDHolder*,
- *Default Domain Policy*,
- *Dfs-Configuration*,
- *File Replication Service*,
- *FileLinks*,

- *IP Security*,
- *Meetings*,
- *Microsoft DNS*,
- *Policies*,

Zaleca się, aby nie zmieniać ani nie modyfikować kontenera *Policies*. W zamian za to, posługując się przystawką *Group Policy* w MMC, należy wyznaczać konfigurację bezpośrednich powiązań dla konkretnego obiektu w *Group Policy*.

- *RpcServices*,
- *RAS and IAS Servers Access Check*,
- *WinsockServices.*

Podczas instalacji Windows 2000 Server domyślny plik bazodanowy (*Ntds.dit*) umieszczany jest w katalogu *%SystemRoot%\System32*. W tej lokalizacji plik nie funkcjonuje jako katalogowa baza danych. Istnieje jako kopia dystrybucyjna, dzięki której nie trzeba używać dysku CD do instalacji Active Directory.

Ntds.dit zawiera domyślną kopię schematu i partycje konfiguracji oraz domyślną partycję domenową. Podczas instalacji Active Directory domyślne kopie partycji schematu i konfiguracji (wraz z partycją domeny, jeśli kontroler domeny jest w niej kontrolerem dodatkowym) są synchronizowane z istniejącymi kontrolerami z tej domeny. Po ukończeniu procesu instalacji Active Directory jest w pełni zsynchronizowane i otwarte dla aktualizacji na nowym serwerze.

Podczas instalowania Active Directory możesz zatrzymać proces replikacji, klikając przycisk *Finish Replication Later* (Zakończ replikację później), kiedy się pojawi. Replikacja będzie kontynuowana po ponownym uruchomieniu komputera. Kontroler domeny nie ujawnia się, dopóki replikacja nie zakończy się w pełni.

Jeśli baza danych do replikacji jest mała, przycisk *Finish Replication* (Zakończ replikacje) nie pojawi się wcale albo tylko na krótko.

Kontrolery domen

Active Directory musi rezydować na kontrolerze domeny, przechowującym kompletną kopię wszystkich informacji, jakie Active Directory posiada na temat tej domeny. Zarządza on również zmianami w tej kopii i replikuje je do innych kontrolerów domen w tej samej i innych domenach. Informacje o schemacie i infrastrukturze są replikowane pomiędzy wszystkimi kontrolerami domen w lesie.

Serwer członkowski

Mimo że tylko kontrolery domen zawierają obiekty Active Directory, inne serwery Windows 2000 mogą zwiększyć funkcjonalność implementacji Windows 2000.

Serwer członkowski (*member server*) jest serwerem pracującym pod Windows 2000 i będącym członkiem domeny, ale nie jest kontrolerem i nie zawiera Active Directory. Serwery członkowskie współdzielą cechy bezpieczeństwa, takie jak założenia domen oraz prawa użytkowników.

Serwery członkowskie mogą pracować jako:

- serwery plików,
- serwery drukarek,
- serwery internetowe,
- serwery proxy,
- serwery routingu i zdalnego dostępu (RRAS),
- serwery aplikacji, zawierające: serwery składowe, serwery terminalowe, serwery certyfikatów, bazodanowe, pocztowe.

Ponieważ serwer członkowski nie jest kontrolerem domeny, nie obsługuje procesu logowania konta, nie bierze udziału w replikacji ani nie przechowuje informacji o zasadach bezpieczeństwa.

Serwery członkowskie posiadają zestaw wspólnych cech związanych z bezpieczeństwem. Wymieniamy je poniżej.

- Stosują się do zasad grupowych ustawionych dla danej lokacji, domeny lub jednostki organizacyjnej.
- Zasoby dostępne na serwerze członkowskim są tak skonfigurowane, aby zapewniać kontrolę dostępu.
- Użytkownicy serwerów członkowskich mają przydzielone sobie prawa.
- Serwery członkowskie posiadają bazy danych bezpieczeństwa lokalnego, zwane bazami *SAM* (*Security Account Manager*).

Zamiana ról

Serwer wewnątrz domeny może funkcjonować w jednej z dwóch ról: jako kontroler domeny lub jako serwer członkowski.

Ponieważ wymagania użytkowników dotyczące środowisk komputerowych zmieniają się, może pojawić się potrzeba zmiany roli serwera. Za pomocą narzędzia Kreator Instalacji Usługi Active Directory wywoływanego przez polecenie `dcpromo.exe` można wypromować serwer członkowski na kontroler domeny lub też zdegradować kontroler domeny do roli serwera członkowskiego (jak wspomniano wcześniej).

Lokacje

Lokacja jest grupą serwerów mogących komunikować się ze sobą przez stałe, synchroniczne łącza o wysokim poziomie niezawodności i szerokiej przepustowości. Tworzenie lokacji pozwala konfigurować dostęp do Active Directory i topologię replikacji, dzięki czemu można lepiej wykorzystywać fizyczną strukturę sieci. Kiedy użytkownik loguje się, klient Active Directory znajduje serwery z jego lokacji. Ponieważ komputery z tej samej lokacji są, z punktu widzenia sieci, położone blisko siebie, komunikacja pomiędzy nimi jest niezawodna, szybka i efektywna.

Dwa podstawowe powody dla tworzenia lokacji to kontrola ruchu replikacyjnego oraz ruchu związanego z logowaniem się i uwierzytelnianiem użytkowników. Lokacje tworzymy za pomocą modułu *Active Directory Sites and Services* (Lokacje i usługi Active Directory). Nie ma bezpośredniego związku pomiędzy domenami i lokacjami, więc pojedyncza domena może obejmować wiele lokacji i podobnie lokacja może rozciągać się na wiele domen. Zwykle granice lokacji pokrywają się z granicami sieci lokalnej.

Jedną z korzyści płynących z Active Directory jest ta, że domeny mogą obejmować fizyczne lokalizacje o różnych topologiach, powiązane łączami sieci rozległych WAN, ale wciąż są przezroczyste dla użytkownika. Jednym z głównych problemów pozostaje jednak przepustowość łączy sieci WAN.

Lokacje a domeny

Ważne jest zrozumienie faktu, iż lokacje są niezależne od domen. Mapują one fizyczną strukturę sieci, zaś domeny (jeśli używa się więcej niż jednej) zwykle mapują jej strukturę logiczną. Struktury fizyczna i logiczna są od siebie niezależne, co niesie ze sobą następujące konsekwencje.

- Nie musi istnieć połączenie pomiędzy lokacjami i przestrzeniami nazw domen.
- Niekonieczne jest powiązanie pomiędzy fizyczną strukturą sieci a strukturą jej domen. Mimo tego w wielu przypadkach domeny tworzy się tak, aby odtwarzały fizyczną strukturę sieci, ponieważ domeny są partycjami, a partycjonowanie wpływa na replikację — partycjonowanie lasu na liczne pomniejsze domeny może zmniejszyć wielkość ruchu replikacyjnego.
- Active Directory umożliwia wielu domenom pojawianie się w pojedynczych lokacjach, a pojedynczym domenom na zaistnienie w wielu lokacjach.

Przechowywanie danych

Dane w Active Directory przechowywane są w pliku bazodanowym *Ntds.dit*. Dwie kopie pliku *Ntds.dit* istnieją na danym kontrolerze w osobnych lokalizacjach:

- *%SystemRoot%\NTDS\Ntds.dit* — kopia przechowująca bazę danych, zawierającą informacje o domenie oraz replikę danych o lesie,

- *%SystemRoot%\System32\Ntds.dit* — kopia dystrybucyjna domyślnego katalogu używanego podczas promowania komputera opartego na Windows 2000 na kontroler domeny. Podczas trwania procesu promowania plik *Ntds.dit* jest kopiowany z katalogu *%SystemRoot%\System32* do ustawionego jako domyślny katalogu *%SystemRoot%\NTDS*.

Active Directory przechowuje dane dla całego lasu. „Katalog" i „Las" można w tym wypadku uznawać za synonimy. Mimo że katalog jest jeden, magazyny danych są rozprowadzane pomiędzy jedną lub więcej domenami, gdzie spójne dane są utrzymywane w lesie odnoszącym się do wielu domen. Active Directory jest partycjonowane i replikowane. Aby mogło obsługiwać dziesiątki milionów obiektów, jest partycjonowane na segmenty logiczne. Każda partycja logiczna replikuje swoje zmiany oddzielnie pomiędzy tymi kontrolerami domen w lesie, które przechowują kopie tych samych partycji katalogowych, aby zapewnić obsługę i dostępność dla tysięcy klientów.

Niektóre partycje katalogowe przechowują informacje o konfiguracji z całego lasu oraz o schemacie, inne magazynują dane dotyczące tylko pojedynczych domen, takich jak: użytkownicy, grupy i jednostki organizacyjne. Partycje katalogowe przechowujące informacje katalogowe są replikowane tylko do kontrolerów z tej samej domeny. Partycje katalogowe dysponujące danymi o konfiguracji i schemacie są replikowane do kontrolerów we wszystkich domenach. Kontrolery skonfigurowane jako serwery GC przechowują pełne repliki jednej partycji domenowej oraz częściowe repliki wszystkich innych domen w lesie. Od kontrolera GC można żądać odnalezienia jakiegokolwiek obiektu w lesie.

Jest różnica pomiędzy partycją katalogową a partycją bazodanową. Baza danych Active Directory nie jest partycjonowana. Partycjonowane jest tylko drzewo katalogowe, będące logiczną reprezentacją danych przechowywanych przez kontroler domenowy.

Dystrybucja Active Directory w drzewie katalogowym może być podsumowana następująco.

- Dystrybucja pomiędzy domenami:
  - dane dotyczące tylko danej domeny są przechowywane w partycji domenowej,
  - pełna, zapisywalna replika partycji domenowej jest replikowana do każdego kontrolera w domenie, włączając w to wszystkie serwery GC w domenie.
- Dystrybucja w lesie:
  - dane dotyczące całego lasu są przechowywane w dwóch partycjach katalogowych: partycji konfiguracji oraz partycji schematu; kontener *Cofiguration* (kontener konfiguracji) jest nadrzędnym obiektem partycji konfiguracji a kontener *Schema* (kontener schematu) jest nadrzędnym obiektem partycji schematu,
  - pełne, zapisywalne repliki partycji konfiguracji i partycji schematu są replikowane do każdego kontrolera w lesie,

- w kontrolerach pełniących role serwerów GC przechowywane są pełne, zapisywalne repliki pojedynczej domeny (tej, dla której kontener domeny jest nadrzędny) oraz częściowe, przeznaczone tylko do odczytu repliki każdej innej partycji domenowej w lesie; te ostatnie repliki nazywamy częściowymi, ponieważ przechowują tylko niektóre atrybuty każdego obiektu.

Kiedy Active Directory po raz pierwszy instalowane jest na komputerze z Windows 2000 Server, wszystkie pełne repliki są replikowane w celu utworzenia katalogu. Następnie replikowane są już tylko zmiany w obiektach katalogowych (zmiany atrybutów oraz tworzenie i usuwanie obiektów).

Podsumowanie

Architektura Active Directory (zbyt złożona dla tej książki) jest znacznie bogatsza w porównaniu do poprzednich wersji systemów NT. Struktura logiczna Active Directory tworzy kopie lustrzane systemów DNS, jest do nich podobna i wypełnia ich standardy. Active Directory składa się logicznie z obiektów, domen i drzew, zaś fizycznie z kontrolerów domen i lokacji.