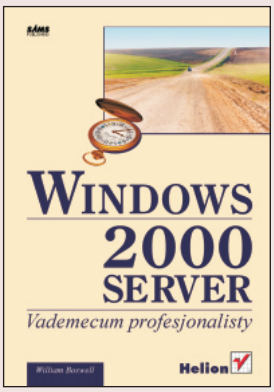
Windows 2000 Server.
Vademecum profesjonalisty



Autor: William Boswell
Tłumaczenie: zbiorowe
ISBN: 83-7197-281-4
Tytuł oryginału: Inside Windows 2000 Server
Format: B5, stron: 1338

Każdy administrator i projektant systemu musi znać odpowiedź na cztery następujące pytania dotyczące technologii Windows 2000 Server:

- W jaki sposób zostały zaprojektowane wszystkie ważniejsze właściwości systemu?
- W jaki sposób należy z nich korzystać?
- Co może być przyczyną błędów systemu?
- Jak należy usunąć powstałe błędy?

W książce „Windows 2000 Server. Vademecum profesjonalisty" znajdziesz odpowiedzi na wszystkie pytania. Autor książki – William Boswell – jest specjalistą w dziedzinie administrowania sieciowymi systemami operacyjnymi Windows NT/2000 (należy zaznaczyć, że Boswell jest nie tylko doświadczonym specjalistą w dziedzinie oprogramowania sieciowego, lecz również specjalizuje się w dziedzinie sprzętu sieciowego). W oparciu o wieloletnie doświadczenie, autor zamieścił w książce wiele odpowiedzi na pytania dotyczące typowych i nietypowych problemów. Przedstawiając rozwiązania problemów w formie zadań, w książce udostępnione zostały strategie instalowania, konfigurowania, rozprzestrzeniania i zarządzania serwerami i stacjami roboczymi Windows 2000.

Jeżeli projektujesz, zarządzasz albo rozwiązujesz problemy sieciowe na platformie systemowej Windows 2000, książka pomoże Ci w:

- Zarządzaniu zabezpieczeniami i replikacjami aktywnego katalogu
- Administrowaniu udostępnionymi zasobami, środowiskiem operacyjnym użytkownika, zdalnym dostępem i routingiem internetowym
- Konfigurowaniu DNS i DHCP
- Uaktualnianiu do domen bazujących na Active Directory
- Zrozumieniu odwzorowywania nazw NetBIOS
- Odzyskiwaniu plików po awarii systemowej
- Konfigurowaniu zasad zabezpieczeń użytkownika
- Czerpaniu korzyści ze wspomagania sprzętowego Plug-and-Play
- Eksplorowaniu najważniejszych protokołów, takich jak np. TCP/IP
- Publikowaniu udostępnionych zasobów
- Konfigurowaniu sieciowych usług routingu i dial-up

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

Spis treści

Rozdział 8.
Projektowanie domen Windows 2000

W poprzednim rozdziale omówiona została struktura Active Directory, ten natomiast poświęcony będzie sposobom korzystania z aktywnej usługi katalogowej oraz tworzeniu domen Windows 2000. Zanim jednak przejdziemy do zagadnienia projektowania domen, warto zastanowić się, czy w ogóle istnieje taka potrzeba.

Przyznam szczerze, że czytając różnego rodzaju dokumentacje objaśniające szczegóły nowych technologii zazwyczaj pomijam w nich rozdziały takie jak ten. Uważam, że problemy, z którymi spotykam się na co dzień są tak niepowtarzalne, że ich rozwiązanie z pewnością szybciej znajdę w praktyce, niż w trakcie przeglądania ogólnych założeń projektowych. Wielu moich kolegów podziela tę opinię. W większości przypadków ich przygoda z Windows 2000 rozpoczęła się od dysku instalacyjnego CD, a nie od rysunków przedstawiających architekturę systemu. Z tego też powodu starałem się zamieścić w tym rozdziale tylko informacje praktyczne i przedstawić je w jak najbardziej zwięzły sposób.

Cele projektowania

Active Directory jest częścią technologii, którą porównać można do klocków lego. Korzystając z niej można zbudować niemal wszystko, lecz należy zadać sobie pytanie — po co? Każdy administrator wie, że sieć nie została wymyślona w celu prezentowania technologii komputerowej, ale po to, by użytkownicy mieli dzięki niej dostęp do zdalnych plików, drukarek i aplikacji klient-serwer. Marzenie użytkownika to w jak najprostszy sposób dotrzeć do zasobów sieciowych; jeżeli dany zasób nie jest dostępny już po dwóch kliknięciach myszki, użytkownik może zacząć się denerwować. Każdy administrator i operator pomocy technicznej doskonale zna historie niecierpliwych użytkowników, którzy rozgłaszali wszem i wobec, jakie to niesamowite problemy czyhają podczas mapowania dysków, podłączania drukarek, znajdowania skrzynek odbiorczych e-mail, itp.

Użytkownicy nie lubią również męczyć się ze skomplikowanymi procedurami zabezpieczeń. Oczywiście, większość z nich zdaje sobie sprawę ze znaczenia systemów bezpieczeństwa (szczególnie, gdy przechowują na serwerze osobiste informacje), ale jednocześnie chce, by owe zabezpieczenia były jak najmniej uciążliwe. Użytkowników nie

obchodzą rewelacje technologiczne, jakimi są usługi katalogowe, czy system uwierzytelniania — chcą, by znajomość jednego hasła (najwyżej dwóch) wystarczała do odpowiedniego zabezpieczenia ich danych. Informacje o szczegółach technologicznych, takich jak partycje obszaru nazw albo konteksty jednostki organizacyjnej, zupełnie ich nie interesują.

Biorąc pod uwagę wszystkie powyższe argumenty wydaje się, iż właściwy projekt domeny powinien uwzględniać przede wszystkim najprostszy dostęp do jej zasobów. Pozostaje jeszcze tylko spełnienie wymagań administratorów systemu i można zabierać się do pracy. Punkt widzenia administratorów jest nieco inny niż punkt widzenia użytkowników, wymagania dotyczą następujących zagadnień.

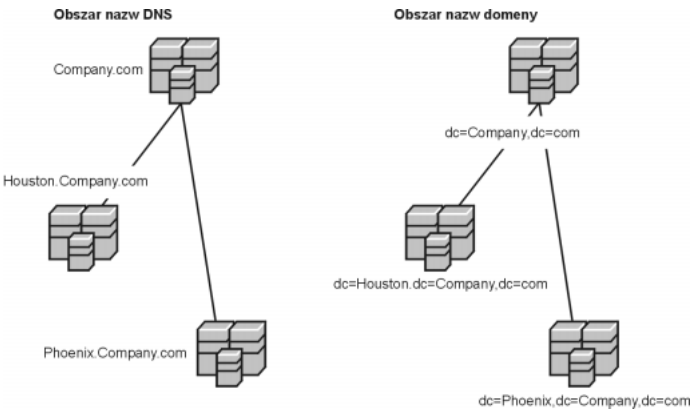
- *Zabezpieczenie*. Protokoły zabezpieczeń służące do kontroli dostępu do domeny i jej zasobów muszą być wystarczająco „silne", by zabezpieczyć dane i sprzęt warte miliony. Bezpieczeństwo jest najważniejsze, projekt domeny musi więc dążyć do maksymalnego utrudnienia dostępu do domeny użytkownikowi nieupoważnionemu, a zarazem do możliwie najprostszego uzyskania dostępu przez użytkownika upoważnionego. Musi również wspomagać kontrolowanie, aby jak najszybciej wykrywać wszystkie wykroczenia i od razu zapobiegać zniszczeniu danych. Idealny system zabezpieczeń powinien pracować szybko i całkowicie niezauważalnie.
- *Stabilność*. Sieciowy system operacyjny nie zostanie zaakceptowany, jeżeli będzie zachowywał się w sposób nieprzewidywalny, bowiem jego praca będzie niestabilna. Usługi kontrolowane przez domenę przez cały czas muszą być wykonywane w dokładnie ten sam sposób.
- *Niezawodność*. Dobry projekt potrafi wyeliminować wszystkie miejsca awarii systemu. Jeżeli danego miejsca nie da się wyeliminować, projekt powinien to uwzględnić i udostępnić dodatkowe rozwiązanie zmniejszające prawdopodobieństwo awarii.
- *Prostota zarządzania*. Zarządzanie domeną nie może angażować całych zastępów inżynierów. Idealnie byłoby, gdyby całą domeną mógł zarządzać jeden administrator, znajdujący się w centrum.
- *Współdziałanie*. Żaden administrator nie uniknie pracy z kilkoma systemami operacyjnymi zainstalowanymi na różnych komputerach. Dobry projekt powinien zminimalizować wszystkie niezgodności pomiędzy systemami.
- *Zdolność do odzyskiwania*. Domena Windows 2000 w całości opiera się na bazie danych Active Directory. Nie ma bazy danych, która byłaby całkowicie odporna na zniszczenie, błędy i inne różnego rodzaju awarie. Musi zatem istnieć metoda jej odzyskiwania i odbudowywania, która powinna być bardzo dobrze udokumentowana.
- *Wydajność*. Operacje wykonywane przez domeny potrzebują zasobów sieciowych, takich jak pasmo komunikacji i osprzęt serwera. Projekt powinien lokalizować strumień danych katalogu i kierować nielokalne strumienie danych do najszybszej linii przesyłania, ponosząc przy tym jak najmniejszy koszt. Projekt powinien również minimalizować wszystkie przewidywane koszty.

Oprócz podanych wyżej, istnieją również mniej definiowalne, lecz równie ważne wskazówki projektowe, takie jak żywotność, ciekawy wygląd i prostota obsługi. Wskazówki te bez wątpienia wpływają bardziej na wygląd niż na strukturę projektu, lecz warto pamiętać także i o nich. Biorąc pod uwagę wszystkie powyższe punkty nie pozostaje nic innego, jak zastanowić się nad tym, które z nich wydają się najistotniejsze i na których warto skupić największą uwagę.

DNS i obszary nazw Active Directory

Domeny Windows 2000 muszą korzystać z TCP/IP — od tego wymagania nie ma żadnego wyjątku. Jeżeli korzystasz z protokołu transportowego innego niż TCP/IP, musisz ponownie zaprojektować całą swoją infrastrukturę. Jeszcze kilka lat temu wymaganie to mogłoby być w niektórych przypadkach trudne do zrealizowania, lecz obecnie — dzięki Internetowi — trudno znaleźć organizację, która nie mogłaby zarządzać przesyłaniem danych za pośrednictwem TCP/IP. Oczywiście wciąż pojawiają się takie sytuacje, lecz jest ich stosunkowo mało. Zdarzają się one w małych firmach, którym niepotrzebny jest stały dostęp do Internetu, w związku z czym bazują na protokole IPX albo NetBUI, LAT, DECnet, czy też LANtactic AILANBIO. Jeżeli masz przyjemność pracować w firmie, która właśnie nabyła nowy produkt Windows 2000 Server, chcąc nie chcąc musisz zainstalować TCP/IP, DNS i prawdopodobnie DHCP. Aby umiejętnie zainstalować nowe składniki systemu, musisz albo zapłacić swojemu dostawcy komputerów, albo nauczyć się samodzielnie instalować nowe protokoły.

Active Directory używa DNS jako szkieletu dla obszaru nazw, od tej reguły nie ma żadnych wyjątków. Każda domena Windows 2000 musi posiadać nazwę pasującą do odpowiadającej domeny DNS. Na rysunku 8.1 przedstawiony został przykład drzewa DNS i odpowiadające mu drzewo domeny Windows 2000.



Rysunek 8.1. *Odwzorowanie nazw domeny Windows 2000 i DNS*

Zewnętrzny i wewnętrzny DNS

Musisz być absolutnie pewny niezawodności połączeń pomiędzy serwerami DNS, a kontrolerami domeny Windows 2000. Prawie wszystkie problemy z Active Directory

zaczynają się od awarii DNS. Serwery DNS muszą wspomagać dynamiczne rejestracje hostów — tak, jak zostało to zdefiniowane w RFC 2136 „Dynamic Updates in the Domain Name System (DNS UPDATE)". Nie będzie można promować serwera Windows 2000 do roli kontrolera domeny, jeżeli strefa DNS nie będzie przyjmować dynamicznych aktualizacji opisanych w RFC 2136.

Jeżeli aktualnie nie posiadasz DNS, Twoje zadanie będzie stosunkowo proste. Musisz określić wygląd domeny Windows 2000 i zgodnie z nim zaprojektować system DNS. Jeżeli posiadasz już obszar nazw DNS, musisz zadać sobie kilka pytań. Po pierwsze — czy kontrolujesz serwery DNS wewnętrznie, czy też zamawiasz usługi DNS poprzez dostawcę usług internetowych *ISP (Internet Services Provider)* albo dostawcę usług sieciowych *NSP (Network Service Provider)*. Jeżeli bazujesz na dostawcy zewnętrznym, jego serwery DNS prawdopodobnie nie będą wspomagać dynamicznego DNS. A nawet jeśli będą wspomagać, to prawdopodobnie dostawca i tak nie pozwoli na rejestrację Twoich serwerów. Przy zabezpieczaniu dynamicznego DNS komunikacja ISP/NSP jest nieco ryzykowna.

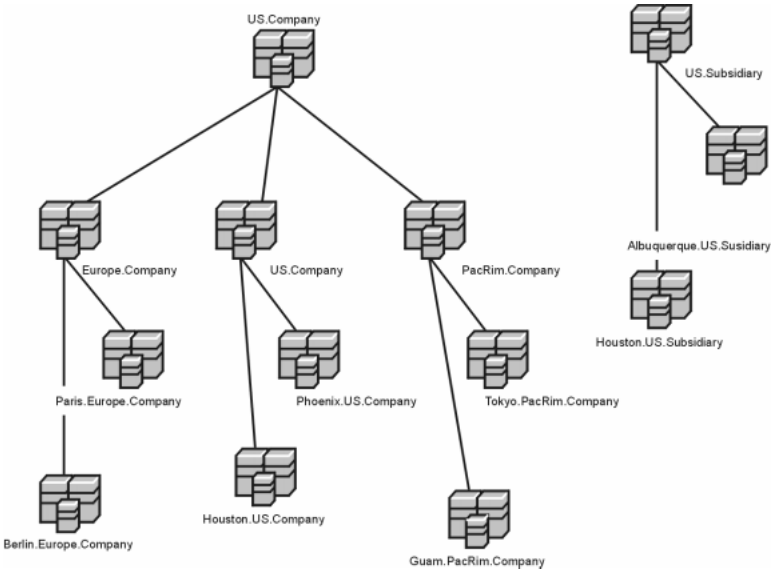
Nawet jeżeli Twój dostawca usług pozwoli na rejestrację hostów na dynamicznych serwerach DNS, możesz być niezadowolony z połączeń WAN, ponieważ bardzo łatwo można utracić dostęp do serwera Yahoo! lub AOL, gdy łącze ISDN albo linia T-1 ulegnie przerwaniu lub przeciążeniu. Z tego powodu zaleca się przed utworzeniem domeny Windows 2000 skonfigurowanie własnego serwera DNS Windows 2000. Nawet jeżeli dany serwer przechowuje już rekordy SRV dla Twojej domeny i przekazuje wszystkie inne zapytania do serwera dostawcy usług DNS, utworzenie własnego serwera jest wciąż warte zachodu.

Jeżeli posiadasz tylko jeden serwer pracujący w klasycznym systemie NT albo zupełnie innym systemie operacyjnym, możesz zainstalować i skonfigurować DNS równocześnie z zainstalowaniem Windows 2000. Jeżeli zlekceważysz tę czynność, kreator promowania kontrolera domeny zaproponuje instalację DNS. Więcej informacji na ten temat znajdziesz w rozdziale 5. „Zarządzanie usługami DNS i DHCP".

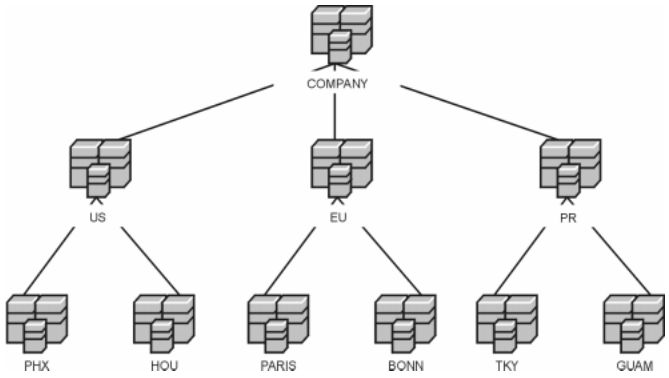
Prywatny albo publiczny obszar nazw

Jeżeli posiadasz już własne zaplecze DNS, kolejnym problemem jest obszar nazw. Twoja firma może nie chcieć używać publicznej strefy DNS do wspomagania wewnętrznych systemów sieciowych, takich jak Active Directory. Kierownictwo firmy może woleć wewnętrzny obszar nazw DNS chroniony przez zaporę sieciową (firewall). Rysunek 8.2 przedstawia diagram prywatnego obszaru nazw DNS.

Prywatny obszar nazw DNS może nie pasować do struktury domeny Windows 2000 tak dobrze, jak ten przedstawiony na rysunku. Jeżeli na przykład posiadasz „płaski" obszar nazw DNS, może on zostać zaakceptowany tylko wtedy, gdy planujesz utworzenie pojedynczej domeny Windows 2000. Gdybyś chciał utworzyć hierarchię domen, musiałbyś najpierw mieć odpowiednie domeny DNS. Diagram domeny na rysunku 8.2 odpowiada projektowi obszaru nazw DNS na rysunku 8.3.



Rysunek 8.2. *Prywatny obszar nazw DNS dla firmy z globalnym dostępem do sieci*



Rysunek 8.3. *Projekt Active Directory korzystający z prywatnego obszaru nazw DNS*

Współpraca Active Directory z DNS nie zawsze przebiega poprawnie. Może zaistnieć sytuacja, w której z powodu funkcjonowania wielu różnych działów w przedsiębiorstwie obszar roboczy DNS zostanie podzielony na wiele stref, których współpraca może przyprawić o ból głowy. Na przykład obszar roboczy DNS dla uniwersytetu może zostać podzielony na oddzielne strefy dla administracji, wydziału biologii, chemii, fizyki, sztuk pięknych, prawa, wychowania fizycznego, matematyki, informatyki, marketingu, językoznawstwa, biblioteki (z poddomenami działu techniki, prawa, medycyny, itd.), nie wspominając nawet o akademikach (z ich olbrzymią liczbą poddomen) czytelniach, ogólnodostępnych pracowniach komputerowych, itp.

Jeżeli zatem Twoja organizacja ma wewnętrzną architekturę DNS, na podstawie której zostanie zaprojektowana domena Windows 2000, upewnij się, czy dany obszar nazw jest odpowiedni dla Twoich potrzeb. Na przykład — system prywatnego obszaru nazw DNS firmy może istnieć samodzielnie w celu wspomagania małej organizacji intranetowej posiadającej kilka serwerów sieci Web w małej strefie DNS *wlasnasiecWeb.inc*. Jeżeli spróbujesz oprzeć usługę Active Directory na tym obszarze nazw DNS, zobaczysz, że zbyt prosta architektura nazw nie będzie się zbytnio do tego nadawać. Nie ma

sensu zajmować się projektem domeny tylko po to, by odkryć, że standardowe nazwy nie pasują do oczekiwań użytkowników. Pozornie prosty obszar nazw może być przyczyną olbrzymich problemów. Aby zmienić jego konwencję podczas rozprzestrzeniania, trzeba „zdeklasować" kontrolery domeny Windows 2000 i zmienić nazwę domeny. Czynność ta może jednak znacznie wpłynąć na Twoją popularność...

Korzystanie z istniejącej strefy DNS albo tworzenie nowej

Możesz zdecydować się na to, by nie korzystać z istniejącego obszaru nazw DNS i utworzyć nowy — tylko dla Windows 2000. W takiej sytuacji musisz wykonać dwa zadania projektowe. Załóżmy przykładowo, że komputery klientów w biurze są skonfigurowane do używania serwera o adresie 10.1.1.1 — jest to ich podstawowy serwer DNS. Jeżeli serwer posiada wersję DNS bez wspomagania dynamicznej rejestracji, Twoim pierwszym zadaniem będzie aktualizacja systemu albo jego usunięcie i ponowne zainstalowanie prawidłowej wersji. Może to być DNS Windows 2000, DNS NetWare 5 albo inny produkt przedstawiony w rozdziale 5.

Aby umożliwić tworzenie nowego obszaru DNS dla domeny Windows 2000, musisz utworzyć przydział dla obszaru już istniejącego. Najlepszym rozwiązaniem byłoby posiadanie kopii dwóch tablic strefowych — istniejącej i nowej strefy — na serwerze dynamicznego DNS. W ten sposób klienty zwracając się do jednego tylko serwera DNS mogłyby otrzymać adresy hostów w obu domenach. Jeżeli chcesz przechowywać istniejącą strefę na osobnym serwerze, masz do wyboru dwie możliwości. Możesz skonfigurować jeden serwer DNS tak, aby przekazywał informacje do drugiego (trzeba w tym miejscu zaznaczyć, że rozwiązanie to może cechować się niestabilnością, a w dodatku jest trudne w zarządzaniu) albo skonfigurować klienty DNS tak, aby kierowały się do obu serwerów — to rozwiązanie pociąga jednak za sobą problem ponownej konfiguracji, jeżeli zdecydujesz się na zmianę serwerów DNS.

Ostatni problem dotyczy przyszłości — zamierzasz połączyć ze sobą intranet, Internet, pocztę elektroniczną, połączenia telefoniczne, zdalny dostęp i technologie sieciowe, ale nie wiesz, co jeszcze nowego pojawi się w ciągu następnych 5 lat. Użytkownicy sieci chcieliby posiadać tylko jeden identyfikator dla wszystkich wymienionych wyżej technologii. Wyobraź sobie, jacy byliby szczęśliwi, gdybyś przed rozpoczęciem instalowania Windows 2000 stanął przed nimi i nalegał na połączenie obszaru nazw DNS, a co za tym idzie, utworzenie wspólnego obszaru nazw Windows 2000 dla całej organizacji. Pod koniec dyskusji mógłbyś w firmie już nie mieć żadnego przyjaciela, ale to zupełnie inna historia.

Jeżeli nawet Twój aktualny obszar nazw DNS wydaje się być odpowiedni dla domeny Windows 2000, zastanów się, jaka sytuacja panuje w pozostałych częściach firmy. Jeden lokalny dział biura może uważać, że utworzenie domeny Windows 2000 w prywatnym obszarze nazw DNS jest najlepszym rozwiązaniem (nazwijmy ją *Phoenix.Company*), podczas gdy inny dział może twierdzić, że należałoby utworzyć publiczny obszar nazw i zbudować ich domenę Windows 2000 wokół *Houston.US.Company.com*. W tym czasie centralna grupa techników informatycznych postanowiła połączyć trzy globalne domeny Windows 2000 w jeden publiczny obszar nazw — *US.Company.com*, *Europe. Company.com*, *Pacrim.Company.com*. Co gorsza administratorzy jednego z biur dowiedzieli się

o tym projekcie i zaplanowali utworzyć jedno drzewo pod katalogiem com dla swojej domeny *Subsidiary.com* oraz domeny firmy *Company.com*. W takiej sytuacji pułapki czyhają dosłownie wszędzie.

- Administratorzy w domenie *Phoenix.Company* nie mogą utworzyć swojej domeny jako podrzędnej wobec *US.Company.com*, gdyż ich obszary DNS różnią się od siebie.
- Administratorzy w *Houston.US.Company.com* unikną problemu obszaru nazw używając publicznej nazwy DNS, lecz nie będą mogli przyłączyć się do istniejącej domeny *US.Company.com*, gdyż Windows 2000 nie posiada żadnych narzędzi łączenia. Jedynym rozwiązaniem jest utworzenie nowej podrzędnej domeny w *US.Company.com*, ręczne przeniesienie wszystkich użytkowników, grup i komputerów do nowej domeny, usunięcie wszystkich kontrolerów ze starej i ponowne promowanie ich w nowej, podrzędnej domenie. Szczegóły dotyczące scalania domen zostaną przedstawione w następnym rozdziale.
- Administratorzy *Subsidiary.com* również będą niemile zaskoczeni, gdy zorientują się, że domena InterNIC podczas tworzenia drzewa Windows 2000 nie zachowuje się jak węzeł główny. Windows odrzuci konfigurację domeny z jedną nazwą węzła głównego — dotyczy to zarówno domen InterNIC, takich jak *com*, *org* i *gov*, jak również domen prywatnych, takich jak *Company*. Domena DNS będąca węzłem głównym dla domeny Windows 2000 musi mieć pełną nazwę zawierającą przynajmniej dwa składniki — np. *US.Company*, *Company.com*, *University.edu*.

Wnioski płynące z pracy z NDS

Niektórzy administratorzy NetWare zauważą, że niezdolność Windows 2000 do łatwej modyfikacji obszaru nazw jest bardzo podobna do cechy ujawnianej przez wczesne wersje NDS. Dość dużo operacji rozprzestrzeniania NDS 4.0 kończyło się potrzebą ich wznowienia w całości z powodu zmiany nazw albo nieodpowiedniego zaplanowania podziału domeny. Zanim w Windows 2000 pojawi się lepsze narzędzie zarządzania kontekstem nazw, należy szybko wyciągnąć wniosek, że lepiej wstrzymać wdrożenie niż przeprowadzić tylko jego część, a następnie być zmuszonym do ponownego utworzenia nazw domeny.

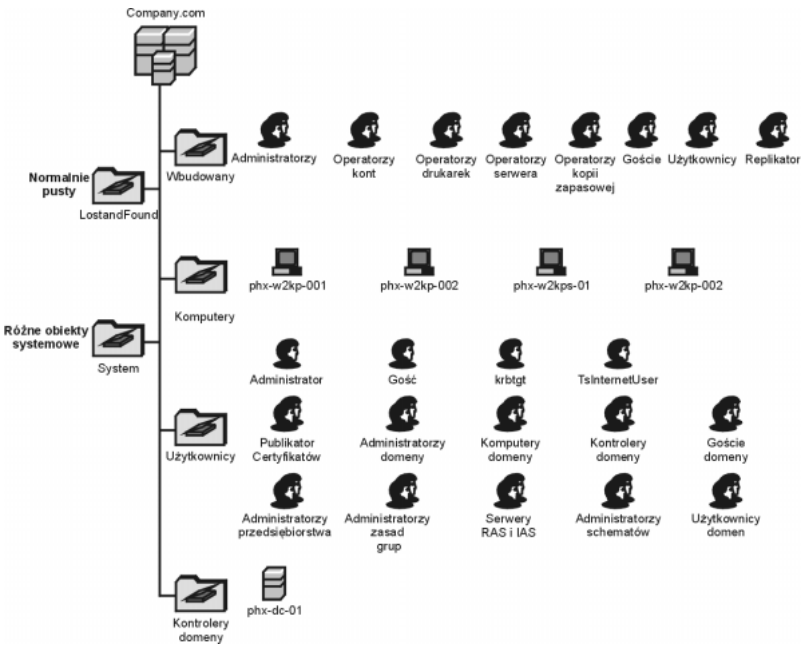
Analizując przytoczone poprzednio przykłady można zauważyć, że domena *Subsidiary .com* posiada zdolność tworzenia drzewa za pomocą relacji zaufania z *US.Company*, z którą może utworzyć las. Aby to umożliwić, *US.Company* musi najpierw utworzyć swoją domenę. Może ona zostać przyłączona do lasu tylko wtedy, gdy promowany jest jej pierwszy kontroler. Windows 2000 nie udostępnia żadnych narzędzi, które mogłyby utworzyć las z jego dwóch niezależnych domen.

Lasy katalogowe także posiadają pewne ograniczenia związane z głębokim przeszukiwaniem LDAP. Obszary nazw „mieszanych" domen mogą również stanowić problem dla użytkowników przeszukujących zasoby w zaufanych domenach — naprawdę można się zirytować po usłyszeniu od pomocy technicznej następującego wyjaśnienia: „Zasoby, których poszukujesz, znajdują się na serwerze w biurze w Salt Lake City. Należą one do domeny *Company*, dlatego musisz otworzyć katalog w folderze Moje miejsca sieciowe, rozwinąć drzewo rozpoczynając od gałęzi *Company*, a nie *Subsidiary*. Tak, wiem, to jest trochę poplątane i rozumiem, że masz na głowie znacznie ważniejsze sprawy niż rozszyfrowywanie sieci komputerowej. Ale cóż... Dziękuję za wezwanie pomocy technicznej Company Inc. Polecamy się na przyszłość. Miłego dnia!".

Mój ulubiony autor, Kurt Vonnegut Jr., mógłby zauważyć, że tworzenie stref DNS Windows 2000 jest jak brnięcie przez wyraz „chronosynclasticinfidibulum" — kończysz daną czynność będąc wszędzie, a zarazem stojąc w punkcie wyjścia. Jeżeli wydaje Ci się, że projekt obszaru nazw DNS masz już gotowy, przedstaw go innym fachowcom i pozwól na surową krytykę.

Wstępne strategie projektowania

Na rysunku 8.4 przedstawiona została domyślna struktura kontekstu nazw domeny Windows 2000, z prostoty której korzystają standardowe kontenery. Uzasadnione jest korzystanie z niej w mniejszych organizacjach, lecz struktura taka z pewnością nie jest wystarczająca dla organizacji posiadających ogromne liczby użytkowników, podzielonych według kryterium potrzeb operacyjnych. Jeżeli zamierzasz używać funkcji zarządzania delegacjami na zewnątrz organizacji, będziesz prawdopodobnie chciał uniknąć korzystania ze standardowych kontenerów. Jeżeli natomiast rozpoczniesz pracę z kontenerami standardowymi, szybko zauważysz, że warto utworzyć nowe. Im szybciej tego dokonasz, tym łatwiej unikniesz sytuacji, w której administratorzy zarządzający różnymi obiektami i prawami będą nawzajem utrudniać sobie życie.



Rysunek 8.4. *Domyślne kontenery dla kontekstu nazw domeny Windows 2000*

Jedynym obiektem ogólnego przeznaczenia wykorzystywanym do tworzenia nowych kontenerów katalogu jest *OU* (*Organizational Unit* — jednostka organizacyjna); bardzo ogólna klasa Container (kontener) dostępna jest tylko dla systemu. Klasy Country (państwo), Organization (organizacja) i Locality (lokalizacja) wchodzą w skład schematu, jednakże Active Directory nie korzysta z nich.

Obiekt OU odgrywa bardzo istotną rolę w projektowaniu Active Directory. Przechowuje on obiekty zasad grup, które zawierają zasady zabezpieczeń, skrypty logowania, rozprzestrzenianie programowe pakietów oraz zasady kontrolujące środowisko komputera. OU stanowi naturalne ograniczenie dla przyznawania praw przechowywanym przez niego obiektom.

Jeżeli zdecydujesz się na używanie swoich kontenerów w strukturze katalogów, możliwe, że zechcesz usunąć kontenery standardowe. Niestety, nie można ich usunąć ani przenieść do innej lokalizacji. Wszystko co możesz zrobić, to zacząć je ignorować.

Zalety i wady pojedynczej domeny

Po przebrnięciu przez wstępny etap projektowania, zastanów się nad użyciem pojedynczej domeny. Nawet jeżeli odnosisz wrażenie, że nie będzie ona odpowiednia dla Twojej organizacji (z powodu dużej liczby użytkowników albo obaw związanych z rozprzestrzenianiem rozległej pojedynczej domeny), warto pamiętać, że korzystanie z pojedynczej domeny ma kilka zalet.

- Pojedynczą domenę łatwiej przeszukiwać. Pamiętaj, że użytkownicy odczuwają wobec struktury sieci taki sam strach, jak przed wejściem do mrocznych katakumb. Im prostszą strukturę katalogów zaprojektujesz, tym bardziej zostaniesz przez nich doceniony.
- DNS jest znacznie prostszy w konfiguracji, gdy korzystasz z pojedynczej domeny Active Directory. Klienty aktywnej usługi katalogowej lokalizują kontrolery domeny usługi Active Directory za pomocą rekordów SRV. Jeżeli posiadasz wiele domen w złożonej konfiguracji nadrzędno-podrzędnej, odwołania pomiędzy strefami mogą być stosunkowo trudne w konfiguracji. DNS jest główną przyczyną problemów z usługą Active Directory. Im DNS jest prostszy, tym lepiej.
- Zarządzanie replikacją jest znacznie prostsze w przypadku pojedynczej domeny, gdyż topologia replikacji nie musi uwzględniać pomieszania lokacji i domen.
- W Active Directory komplikacje pojawiają się podczas obsługi wyszukiwań LDAP w różnych kontekstach nazw. W przypadku istnienia wielu domen posiadanie serwerów *katalogu globalnego* niemalże jest niezbędne. Jeżeli dana strona nie udostępnia serwera katalogu globalnego, użytkownicy mogą nawet nie mieć możliwości zalogowania się. Pojedyncza domena natomiast nie jest zależna od serwera katalogu globalnego, gdyż każdy jej kontroler posiada replikę wszystkich kontekstów nazw.
- Wdrożenie zabezpieczeń jest znacznie prostsze w pojedynczej domenie, gdyż przechodnie relacje zaufania Kerberos pozwalają na bezproblemowy dostęp do zaufanych domen (nie oznacza to jednak, że relacje te są proste w zarządzaniu). Koszmarem administratora jest dokładne sprawdzanie listy członkowskiej setek grup w celu rozwiązania problemu prawa dostępu do pliku albo katalogu. Sytuacja ta jest szczególnie trudna w Windows 2000, gdyż system zawiera trzy różne typy grup, które są zagnieżdżane i mieszane w zróżnicowany sposób.

Jedyną wadą posiadania pojedynczej domeny może być rozmiar bazy danych Active Directory. Im więcej obiektów umieścisz w jednej domenie, tym większe prawdopodobieństwo napotkania problemów ze stabilnością i replikacją systemu. Bazowanie na jednej domenie podczas obsługi sieci posiadającej tysiące użytkowników i komputerów może być bardzo ryzykowne. Przechowywanie, aktualizowanie, replikowanie i przeszukiwanie bazy danych Active Directory obsługującej ponad 100 000 użytkowników może „skołować" pamięć kontrolera domeny tak, jak piwo potrafi „skołować" umysł nastolatka. Globalne replikowanie tak dużej bazy danych poprzez sieć WAN jest bardzo podatne na różnego rodzaju awarie.

Microsoft co prawda przeprowadził testy dla domeny zawierającej 1,5 miliona użytkowników, lecz tylko czas i nabycie większego doświadczenia mogą pomóc w określeniu jej optymalnego rozmiaru. Alternatywą posiadania jednej domeny jest podział całego katalogu na oddzielne domeny. Każda z nich ma oddzielny kontekst nazw, który jest replikowany osobno. Serwery katalogu globalnego przechowują repliki wszystkich domen, ale ponieważ zawiera on tylko ok. 60 atrybutów, więc informacjami przechowywanymi w nim stosunkowo łatwo zarządzać.

Dla sieci posiadającej najwyżej 10 000 użytkowników zalecana jest pojedyncza domena. Jeżeli jednak użytkowników będzie więcej niż 20 000, zapoznaj się z kolejną częścią tego rozdziału pt. „Zalety i wady wielu domen". Jeżeli liczba użytkowników sieci mieści się w przedziale 10 000 — 20 000, spróbuj zaprojektować oba rozwiązania — dla jednej i wielu domen, a następnie zdecyduj, które z nich wydaje się lepsze.

Liczba informacji przechowywanych w Active Directory

Obliczanie ile informacji przechowywanych jest w Active Directory nie jest tak skomplikowane, jak obliczanie rozmiaru bazy SAM dla domeny NT4. Poniżej zamieszczonych zostało kilka danych, które powinny być pomocne w szacowaniu rozmiaru:

- obiekty użytkownika z obowiązującym zestawem atrybutów — 3,5 kB,
- obiekty użytkownika z pełnym zestawem atrybutów — 4,5 kB,
- obiekty OU (jednostka organizacyjna) — 1 kB,
- obiekty grupy — różne, w zależności od liczby członków grupy.

Zgodnie z powyższym, baza danych przechowująca informacje dla pół miliona użytkowników i komputerów z pełnym kompletem grup, serwerów, stron i zasad wspomagających bazę może posiadać 2,5 GB.

Zalety i wady wielu domen

Każdy wysiłek włożony w projektowanie powinien zmierzać do ujęcia całej organizacji w jedną domenę. Niestety, im większa domena, tym większa baza danych Active Directory, a co za tym idzie, większa podatność na problemy ze stabilnością i replikowaniem danych. Rozmiar produktu wpływa bezpośrednio na jego trwałość — jeśli nie wierzysz, spytaj projektantów *Hindenberga* i *Titanica*.

Mechanizm bazy ESENT może przechowywać milion obiektów w 17-terabajtowym obszarze — teoretycznie jest on wystarczający do przechowywania kilku milionów użytkowników razem z ich komputerami, grupami, składnikami infrastruktury i obiektami aplikacji dostarczonymi przez różnych producentów. Administratorzy muszą jednak brać przede wszystkim pod uwagę wydajność i praktyczność domeny Windows 2000. Każdy system posiada pewien punkt, w którym jego wydajność jest największa. Zanim jednak zostanie on znaleziony w systemie Windows 2000, z pewnością upłynie rok albo dwa lata.

Olbrzymie organizacje, takie jak np. U.S. Postal Service (licząca blisko 900 000 pracowników), prawdopodobnie nie będą mogły w najbliższym czasie korzystać z usługi Active Directory. Międzynarodowi dostawcy internetowi obsługujący miliony użytkowników, również nieprędko zechcą skorzystać z nowej technologii aktywnego katalogu (podobnie zresztą jak administratorzy sieci NetWare i UNIX). Nie oznacza to, że Microsoft nie będzie próbował sprzedać Windows 2000 tego typu organizacjom, lecz strategia którą się kieruje prowadzi z dołu do góry, a nie z góry na dół. Jeżeli system sprawdzi się w mniejszych sieciach, będzie można wdrożyć go w sieciach obsługujących więcej użytkowników.

Zasada projektowania domeny: jeżeli katalog ma przybierać bardzo duże rozmiary, skorzystaj z oddzielnych domen — staraj się jednak zminimalizować ich liczbę.

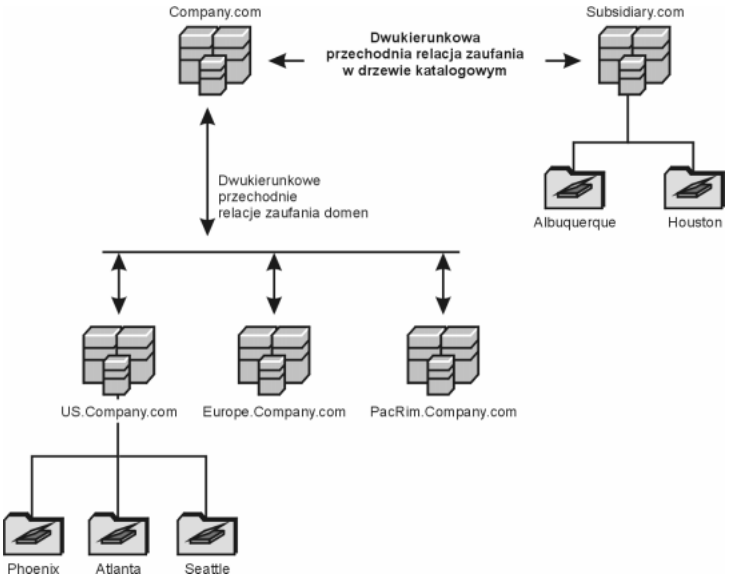
Jedynym sposobem na ograniczenie rozmiaru bazy danych katalogu jest jej podział na pojedyncze domeny. Jeżeli jesteś początkującym użytkownikiem Windows 2000, możesz mieć kłopoty z przewidywaniem, czy jedna domena będzie wystarczająco efektywna dla Twojej organizacji. Oto rada: jeżeli sieć posiada ponad 15 000 użytkowników, rozważ możliwość korzystania z oddzielnych domen. Jeżeli zaś posiada ponad 50 000 użytkowników, nie ma się nad czym zastanawiać i należy zaprojektować oddzielne domeny. Lepiej zarządzać kilkoma domenami niż czekać na nieprzewidziane zachowania aktywnego katalogu. Musisz tylko pamiętać, że domeny reprezentują oddzielne konteksty nazw, komplikują nieco replikacje, a hierarchia domen wyświetlana w interfejsie Eksploratora może być dla użytkowników myląca.

Pojedyncza domena będzie prawdopodobnie znacznie prostsza w obsłudze, a już na pewno łatwiejsza do zaprojektowania (jeżeli nie wykorzystujesz jej do zarządzania olbrzymią organizacją). Może się jednak zdarzyć, że pojedyncza domena nie będzie wystarczająca, i to wcale nie z powodu ograniczeń technicznych. Administratorzy klasycznego systemu NT byliby bardzo zadowoleni z możliwości korzystania z autonomicznych zaufanych domen. Gdybyś zaproponował utworzenie podrzędnej domeny z drzewie katalogowym, mógłbyś napotkać na opór — często zdarza się, że lokalni administratorzy wolą zarządzać stosunkowo *szerokim lasem* niż *wysokim drzewem* katalogowym.

Może zdarzyć się sytuacja, w której liczba utworzonych domen przekracza potrzeby danej organizacji. Nie powinieneś pozwalać lokalnym administratorom na zbyt dużą dowolność w podejmowaniu decyzji, które mogą niekorzystnie wpłynąć na wydajność i stabilność całego systemu. Jeżeli sam jesteś lokalnym administratorem, spróbuj zaprojektować domenę i zastanowić się nad potrzebą tworzenia większej ich liczby. Pojedyncza domena daje wystarczająco duże pole działania — na przykład: w lesie katalogowym może znajdować się tylko jeden schemat i jeden kontekst nazw, dlatego nie musisz dokonywać żadnych wysłań obciążających katalog. Na dodatek wyszukiwanie

LDAP poprzez drzewo relacji zaufania nie jest tak wydajne jak wyszukiwanie w pojedynczej domenie. Więcej informacji dotyczących wyszukiwania LDAP znajdziesz w rozdziale 7., „Usługi Active Directory".

Na rysunku 8.5 przedstawiony został przykład drzewa katalogowego, w którym regiony globalne zostały podzielone na osobne podrzędne domeny. Oprócz tego duże biura zostały podzielone na domeny podrzędne, a nie na obiekty OU. Jeżeli zdecydujesz się na korzystanie z tego projektu, zapoznaj się z zagadnieniem rozprzestrzeniania obszaru nazw DNS. Istnieje kilka spraw, o których należy pamiętać podczas projektowania, np. umieszczenie na karcie projektowej ikony *Phoenix.US.Company.com* albo przekonanie lokalnych administratorów do utworzenia nowych stref DNS i zmodyfikowania ich plików hostów i konfiguracji klientów.



Rysunek 8.5. *Nadrzędne kontenery katalogu korzystające z wielu domen*

Po zaprojektowaniu obiektów OU pomyśl o granicach, które mogą być potrzebne, gdy zostaniesz zmuszony do podzielenia swojego terenu na osobne domeny. Bądź również ostrożny przy tworzeniu nazewnictwa — zamiast długich nazw miast, staraj się używać ich skrótów. Użytkownik z pewnością nie będzie zadowolony, jeżeli jego nazwa będzie wyglądać następująco: *user@Albuquerque.NewMexico.UnitedStates.NorthAmerica.Company.com*.

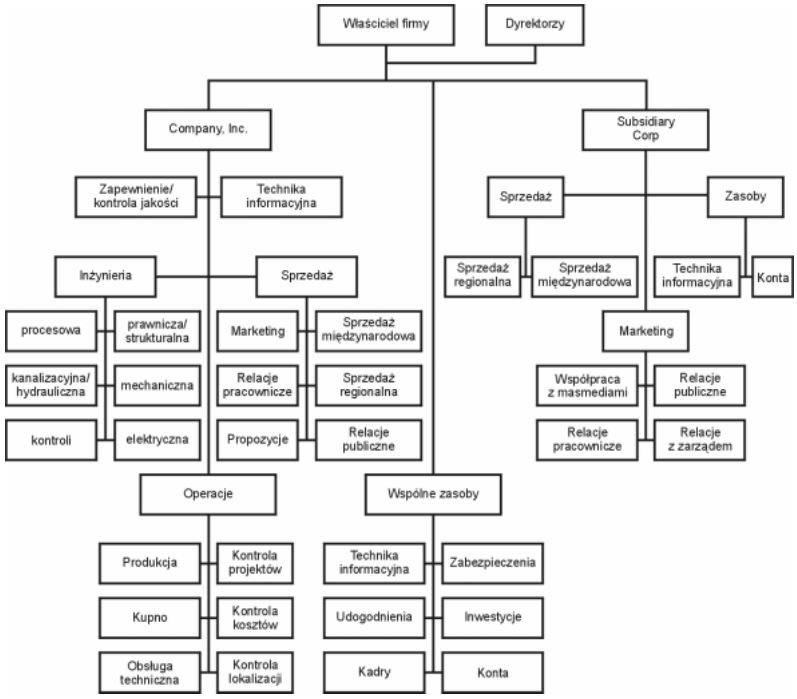
To, że użytkownik może logować się do sieci i przeglądać jej zasoby dzięki przechodnim relacjom zaufania Kerberos nie oznacza, że posiada on dostęp do wszystkich jej zasobów. Zostawmy teraz „górną" strukturę katalogu i zajmijmy się sposobem uzyskiwania dostępu do kontenerów znajdujących się na jego „spodzie". Za chwilę Twój talent dyplomatyczny oraz umiejętność projektowania zostaną sprawdzone.

Strategie projektowania dla wyższych poziomów katalogu

Zadaniem usługi katalogowej jest ułatwienie zarządzania siecią opartą na funkcjonalnych ograniczeniach narzuconych przez organizację. Jest to główne założenie specyfikacji X.500. Nazwy klas obiektów mają za zadanie zachęcić Cię do korzystania ze schematów organizacyjnych ułatwiających projektowanie katalogu. Zastanówmy się dlaczego jest to aż tak istotne.

Na rysunku 8.6 przedstawiony został schemat organizacyjny firmy prowadzącej dwa rodzaje działalności. Trzon firmy nosi jej główną nazwę Company Inc., zaś jego odgałęzienie nazwano Subsidiary Corp. Obie części firmy używają wspólnych biur w tych samych miastach, ich pracownicy jedzą posiłki w tych samych restauracjach, posiadają konta w tych samych bankach, lecz wykonują całkowicie różne prace.

Rysunek 8.6. *Typowy schemat organizacyjny dla firmy o średnich rozmiarach*



Działy informacji technicznej są jednak oddzielne. Administratorzy sieci także stanowią osobne grupy i są przekonani, że zarządzają siecią tysiąc razy lepiej od swoich „sąsiadów" z drugiej części firmy. Firma dysponuje jeszcze małą grupką personelu technicznego, którą zmusza do wykonywania długoterminowych projektów i raportów oraz rozprzestrzeniania ich za pomocą Lotus Notes (zamiast pozwolić na korzystanie z centralnego zarządzania rozprzestrzenianiem).

Problem w zastosowaniu schematu przedstawionego na rysunku 8.6 do zaprojektowania katalogu polega na tym, że przedstawia on tylko ogólnie sposób zarządzania i wykonywania

operacji wewnątrz firmy. Nie odsłania on hierarchii funkcjonalnej, regionalnej i powiązań między częściami firmy, co może istotnie wpłynąć na sposób wykorzystania komputerów w organizacji. Nowoczesne, przyszłościowo myślące organizacje posiadają hierarchiczną strukturę relacji pomiędzy różnymi grupami, dzięki czemu można bardzo szybko uzyskać różne informacje na temat użytkownika. Próba odzwierciedlenia tych relacji jest jednak bardzo niewdzięcznym zadaniem. Jeśli chcesz zaprojektować domenę na podstawie schematu organizacyjnego, przygotuj się na spędzenie wielu, wielu dni na rozmowach z pracownikami firmy w celu ustalenia, czy Twój projekt jest prawidłowy. Każda zmiana operacji wykonywanych w firmie automatycznie powoduje konieczność zmiany Twojego projektu.

Stąd właśnie wynika jedna z głównych zasad projektowania domeny Windows 2000:

> *Zasada projektowania domeny: upewnij się, czy struktura domeny jest odpowiednia dla sposobu, w jaki zorganizowany jest dział IT.*

Podczas pierwszego etapu pracy nie zajmuj się innymi działami. Projektowanie struktury powinieneś zacząć od organizowania działu IT — ludzi, którzy będą posługiwali się narzędziami zarządzania i interfejsami wewnątrz Windows 2000.

Sprostanie wymaganiom co do struktury domeny jest bardzo trudne. Prawdopodobieństwo, że dwa różne działy IT będą zadowolone z tej samej struktury domeny jest bardzo małe. Nawet, jeżeli dyrektorzy firmy włączą się do dyskusji próbując uzyskać kompromis, kłótnia i tak może przybrać pokaźne rozmiary. Podczas takich debat warto zająć miejsce blisko drzwi i upewnić się wcześniej czy są otwarte. Spróbuj dowiedzieć się dokładnie jaki jest podział obowiązków przy zarządzaniu i podziel schemat organizacji pionowo na poszczególne jednostki firmy albo poziomo na regiony. Na koniec pozostaje tylko znaleźć wszystkich administratorów i ich szefów oraz określić relacje pomiędzy nimi.

Nie ograniczaj poszukiwań jedynie do kręgu ludzi z tytułem administratora. Znajdź wszystkie ukryte relacje w firmie i sprawdź, kto jest odpowiedzialny za operacje komputera i sieci. Zaawansowanych użytkowników możesz znaleźć poza formalną strukturą informacji technicznej, czasem odgrywają oni znaczącą rolę w zarządzaniu zasobami sieci. Znajdź osoby, które współpracują z działem IT i posiadają uprawnienia administratora. Krótko mówiąc, znajdź wszystkich, którzy mogą potrzebować uprawnień administracyjnych w domenie albo chcą je posiadać.

Po ustaleniu prawdziwej hierarchii administracyjnej kolejnym zadaniem będzie określenie sposobu wzajemnego współdziałania członków personelu. Musisz zdefiniować uprawnienia administratora, które umożliwiają mu wykonywanie jego pracy. Podziel administratorów na grupy w zależności od posiadanych uprawnień. Na zakończenie zaplanuj wierzchołek katalogu tak, aby zdefiniowane przez Ciebie grupy administracyjne mogły posiadać prawa dostępu do obiektów OU łączących użytkowników, komputery i wspólne zasoby, które podlegają tymże administratorom.

Zagadnienie bezpieczeństwa katalogu zostało szczegółowo omówione w rozdziale 10. „Zarządzanie zabezpieczeniami Active Directory", Windows 2000 wykorzystuje grupy zabezpieczeń na kilka różnych sposobów, dlatego warto poświęcić kilka chwil temu problemowi.

Omówienie funkcji grup zabezpieczeń Windows 2000

Windows 2000 udostępnia dwa typy grup — grupy zabezpieczeń i grupy dystrybucyjne. Grupy dystrybucyjne używane są do zarządzania rozprzestrzenianiem oprogramowania i nie mogą być wykorzystane do kontroli dostępu do obiektów zabezpieczeń.

Istnieją trzy klasy grup zabezpieczeń, a każda z nich posiada własne funkcje i ograniczenia. Zanim te klasy zostaną omówione, zastanówmy się nad charakterystyką operacyjną domen Windows 2000, które wpływają na sposób obsługi grup. Charakterystyka ta potrzebna jest ze względu na wsteczną zgodność z klasycznym systemem NT.

Klasyczna domena NT składa się z podstawowego kontrolera domeny, który posiada dostęp do bazy danych zabezpieczeń oraz jednego lub kilku pomocniczych kontrolerów, które replikują aktualizacje zabezpieczeń z kontrolera podstawowego. W Windows 2000 baza SAM została zastąpiona przez Active Directory. Obiekty aktywnego katalogu (użytkownicy, komputery i grupy), posiadają wartości atrybutów, które symulują części bazy SAM. Kontroler domeny Windows 2000 może replikować te atrybuty do klasycznych pomocniczych kontrolerów domeny, dzięki czemu mogą one być odpowiedzialne za uwierzytelnianie użytkowników i komputerów. Takie wspomaganie klasycznego systemu NT jest niezbędne do zarządzania rozprzestrzenianiem Windows 2000 w istniejącej sieci NT.

Klasyczne kontrolery pomocnicze domeny mogą pobierać repliki tylko z kontrolera podstawowego, który został zdefiniowany w specjalnej relacji zaufania w bazie *LSA (Local Security Authority)* wewnątrz grupy Security w rejestrze systemowym. Natomiast w Windows 2000 każdy kontroler domeny ma dostęp do Active Directory. Dla zachowania zgodności, jeden podstawowy kontroler domeny Windows 2000 oznaczony jest jako kontroler pełniący rolę wzorca. Kontrolę nad operacjami tej domeny może sprawować tylko jeden wzorzec.

Podstawowy kontroler domeny pełniący rolę wzorca jest zazwyczaj kontrolerem domeny NT, który został zaktualizowany dla potrzeb Windows 2000, pomimo to, że istnieje możliwość przesunięcia funkcji wzorca do innego kontrolera owej domeny. Operacja ta podobna jest do promowania pomocniczego kontrolera domeny do kontrolera podstawowego. Wszystkie aktualizacje Active Directory wpływają na atrybuty SAM — są one zapisywane tylko w kontrolerze pełniącym rolę wzorca, a następnie replikowane do klasycznych pomocniczych kontrolerów domeny.

Domena zawierająca klasyczne kontrolery pomocnicze nosi nazwę *trybu mieszanego*. W trybie mieszanym grupy zabezpieczeń są ograniczane wymaganiami klasycznego systemu NT. Grupy globalne nie mogą być zagnieżdżane w innych grupach tego typu, grupy lokalne nie mogą być zagnieżdżane w innych grupach lokalnych, a grupy lokalne z zaufanych domen nie mogą być używane jako priorytety zabezpieczeń w zaufanych domenach.

Współpraca grup zabezpieczeń w domenach trybu macierzystego

Gdy wszystkie kontrolery pomocnicze domeny zostaną zaktualizowane dla potrzeb Windows 2000, zostaje ona określona mianem domeny trybu macierzystego. W takiej sytuacji komputery domeny mogą w pełni brać udział w przechodnich relacjach zaufania Kerberos, umożliwiając w ten sposób większą elastyczność zarządzania systemem. Poniżej przedstawione zostały zasady zarządzania grupami w trybie macierzystym domeny Windows 2000.

- *Lokalne grupy domeny*. Stosowane przy wstecznej zgodności z klasycznym systemem NT. Członkami lokalnych grup domeny mogą być użytkownicy domeny lokalnej oraz użytkownicy, grupy globalne i grupy uniwersalne zaufanych domen. Lokalna grupa domeny może być używana do kontrolowania dostępu do obiektów zabezpieczeń tylko we własnej domenie lokalnej. I tak np. lokalna grupa domeny w domenie *Company.com* nie może być delegowana do kontroli domeny *Branch.Company.com*.
- *Grupy globalne*. Używane są do kontroli dostępu do lokalnych zasobów w domenie. Członkami grupy globalnej mogą być tylko użytkownicy i grupy globalne własnej domeny. Grupa globalna może być używana do kontrolowania dostępu do obiektów zabezpieczeń w domenie lokalnej i domenach zaufanych. Na przykład grupa globalna w domenie *Company.com* może być delegowana do kontrolowania domeny *Branch.Company.com*, zakładając, że pomiędzy domenami istnieje relacja zaufania.
- *Grupy uniwersalne*. Używane są do kontrolowania dostępu do zasobów pomiędzy granicami domen. Grupy uniwersalne dostępne są tylko w domenach trybu rodzimego. Członkiem grupy uniwersalnej może być członek indywidualny pochodzący z dowolnej domeny oraz globalne i uniwersalne grupy z domen zaufanych. Grupa uniwersalna może być używana do kontrolowania dostępu do obiektów zabezpieczeń w dowolnej zaufanej domenie.

Różnica pomiędzy grupami globalnymi i uniwersalnymi polega na sposobie ich przechowywania w katalogu. Obiekt katalogu dla priorytetów zabezpieczeń (użytkowników, komputerów, grup) posiada atrybut Member-Of. Atrybut ten zawiera wyróżnioną nazwę każdej lokalnej domeny i grupy globalnej, do której należy użytkownik. Poniżej przedstawiona została lista wpisów Member-Of użytkownika o nazwie Company User, który jest członkiem trzech grup. Lista została zestawiona za pomocą narzędzia LDIFDE, omówionego wcześniej.

```
dn: CN=Company User, CN=Users, DC=Company, DC=com
memberOf: CN=Phx_Eng, OU=Groups, OU=Phoenix, DC=Company, DC=com
memberOf: CN=Account Operators, CN=Builtin, DC=Company, DC=com
memberOf: CN=Users, CN=Builtin, DC=Company, DC=com
```

Po zalogowaniu użytkownika sprawdzany jest atrybut Member-Of. Skanowany jest lokalny kontekst nazw w celu znalezienia grup, których członkiem jest dany użytkownik. Wszystkie informacje zawarte są w powiązanym z obiektem grupy atrybucie Member. Poniżej przedstawiony jest przykład dla grupy Administrators, uzyskany również za pomocą narzędzia LDIFDE:

```
dn: CN=Administrators, CN=Builtin, DC=Company, DC=com
member: CN=Phx Admin, CN=Users, DC=Company, DC=com
```

```
member: CN=Domain Admins, CN=Users, DC=Company, DC=com
member: CN=Enterprise Admins, CN=Users, DC=Company, DC=com
member: CN=Administrator, CN=Users, DC=Company, DC=com
```

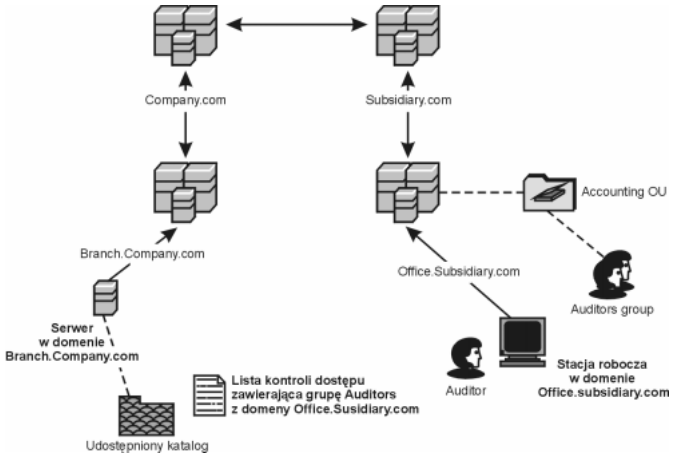
Łączenie wsteczne

Parowanie atrybutów Member/Member-Of jest dość powszechną operacją dokonywaną w katalogu, istnieje wiele tego typu par. Informacja przechowuje łącze dla drugiej bazy danych — bazy LINK, która śledzi parowanie. Jeden ze składników bazy sprawdza jej zgodność według ustalonego harmonogramu (czynność ta wykonywana jest w tle). Istnieje również możliwość ręcznego sprawdzenia zgodności za pomocą narzędzia *NTDSUTIL*, poprzez wykonanie tzw. łączenia wstecznego.

Przegląd operacji grup zabezpieczeń Windows 2000

Rysunek 8.7 przedstawia schemat lasu domen trybu rodzimego. Gdyby były one klasycznymi domenami NT albo domenami Windows 2000 trybu mieszanego, relacja zaufania pomiędzy domeną *Subsidiary* i *Office* mogłaby być niewidoczna dla *Branch* i *Company*. W takiej sytuacji aby uzyskać dostęp do folderu w podrzędnej domenie *Branch*, użytkownik *Auditor* potrzebowałby konta w domenie *Company*. Po przeniesieniu domen do trybu macierzystego i utworzeniu w pełni przechodnich relacji zaufania Kerberos, administrator w domenie *Branch* mógłby umieścić użytkownika *Auditor* na liście kontroli dostępu do danego folderu albo grupy lokalnej w domenie *Branch*.

Rysunek 8.7. *Las domen trybu rodzimego*



Przechodząc do trybu macierzystego niszczysz ostatni pomost łączący Cię z klasycznym systemem NT. Jeżeli z jakichś powodów będziesz musiał skorzystać z klasycznych podstawowych i pomocniczych kontrolerów domeny, będzie to niemożliwe, chyba że przywrócisz je z kopii bezpieczeństwa. Więcej informacji na temat awarii Active Directory znajdziesz w rozdziale 11., „Zarządzanie replikacjami Active Directory".

Tworząc strategię domeny pamiętaj o tym, że lokalni administratorzy będą przypisywać lokalne prawa dostępu za pomocą grup zaufanych domen. Jeżeli utworzysz wiele domen, podczas wyszukiwania właściwych grup administratorzy mogą być zdezorientowani, w związku z czym bardzo trudno będzie określić, czy dany użytkownik posiada odpowiednie uprawnienia. Taka sytuacja może być bardzo irytująca.

Poniżej zamieszczony został krótki opis sposobu, w jaki członkostwo grupy używane jest do kontrolowania dostępu do obiektu katalogu. W rozdziale 10. znajdziesz dokładne omówienie tego problemu.

Gdy LSA skanuje kontekst nazw członkostwa grupy, wyszukiwane są również identyfikatory zabezpieczeń odpowiadające każdej grupie związanej z użytkownikiem. Po znalezieniu identyfikatora, zostaje on wysłany do Centrum dystrybucyjnego kluczy *KDC (Key Distribution Center)* Kerberos, którego zadaniem jest wydanie użytkownikowi biletu *TGT (Ticket-Granting Ticket)*.

Atrybut Member-Of obiektu użytkownika w lokalnym kontekście nazw nie zawiera informacji dla grup w zaufanych domenach, wobec tego LSA musi użyć innego mechanizmu określenia członkostwa grupy. Gdyby operacja ta nie została wykonana, użytkownik mógłby otrzymać niepożądany dostęp do zasobów chronionych przez grupę z zaufanej domeny.

Aby uniknąć takiej sytuacji, LSA skanuje również katalog globalny szukając grup uniwersalnych, których członkiem jest dany użytkownik. Katalog globalny, gdyż posiada on kopię każdego kontekstu nazw domeny. Oznacza to, że za każdym razem, gdy użytkownik otrzymuje bilet TGT z centrum KDC, LSA musi wykonać pełne skanowanie całego katalogu globalnego, łącznie z wszystkimi grupami, których członkiem jest dany użytkownik. Skanowanie tych grup jest istotne, ponieważ grupy uniwersalne mogą zagnieżdżać globalne i uniwersalne grupy z dowolnej domeny trybu macierzystego.

Jeżeli LSA znajdzie grupę uniwersalną, której członkiem jest dany użytkownik, dodaje do listy identyfikatorów wysyłanych do centrum KDC identyfikator zabezpieczenia grupy uniwersalnej (również uzyskany z katalogu globalnego). Identyfikatory zawarte w bilecie TGT używane są do tworzenia żetonów lokalnego dostępu do serwerów. Podsumowując powyższe fakty można powiedzieć, że grupy uniwersalne mogą być używane do kontrolowania dostępu do lokalnych zasobów domeny poprzez priorytety zabezpieczeń.

Jeżeli zagadnienie relacji pomiędzy grupami lokalnej domeny, grupami globalnymi i grupami uniwersalnymi wciąż nie jest do końca jasne, spróbuj za pomocą narzędzia LDIFDE wykonać zrzut obiektu z kontrolera domeny w domenie użytkownika nie będącej katalogiem globalnym; z serwera katalogu globalnego w domenie użytkownika oraz z serwera katalogu globalnego nie znajdującego się w domenie użytkownika. Rezultat działania narzędzia może być pomocny w zrozumieniu zagadnienia:

- zrzut LDIFDE obiektu użytkownika z kontrolera domeny nie będącej katalogiem globalnym wyświetla tylko grupy domeny (lokalne, globalne i uniwersalne),
- zrzut z katalogu globalnego w domenie użytkownika wyświetla wszystkie grupy ze wszystkich domen lasu,
- zrzut z katalogu globalnego w zaufanej domenie wyświetla tylko grupy uniwersalne z dowolnej domeny lasu.

Obiekty grupy uniwersalnej w katalogu globalnym muszą posiadać atrybut Member, który należy replikować do każdego katalogu globalnego w lesie. Jeżeli masz tysiące użytkowników w dziesiątkach różnych miejsc na świecie, nie jest to takie nielogiczne.

Podczas definiowania grup kontrolujących dostęp do katalogu i przydzielających przywileje administratora pamiętaj o dwóch zasadach:

- używaj uniwersalnych grup tylko wtedy, gdy priorytety zabezpieczeń z zaufanej domeny będą miały dostęp do obiektu,
- staraj się, aby członkami grup uniwersalnych nie byli indywidualni użytkownicy, oni zbyt często zmieniają członkostwo. Przyporządkuj grupy globalne z każdej zaufanej domeny i zmodyfikuj listę członków grupy globalnej.

Delegowanie i dziedziczenie praw dostępu

Jeżeli kiedykolwiek planowałeś system plików serwera, wiesz, jak wiele różnych sztuczek trzeba stosować, aby prawa dostępu nie zostały przypisane przypadkowo. Sytuacja ta jednak znacznie bardziej komplikuje się w przypadku katalogu.

Klasyczny system NT i Windows 2000 używają wspólnego modelu zabezpieczeń ukierunkowanego na obiekty. Struktury danych, takie jak pliki i katalogi NTFS, klucze rejestru oraz wpisy Active Directory są *obiektami zabezpieczeń*. Deskryptor zabezpieczeń zawiera listę kontroli dostępu *ACL (Access Control List)*, definiującą priorytety zabezpieczeń upoważnianych do dostępu do obiektu. Lista ACL definiuje również *prawa dostępu* przyznawane pryncypiom zabezpieczeń. Podstawowymi prawami dostępu dla obiektów katalogu są:

- *List (pokaż wykaz)*, prawo do przeglądania obiektów w kontenerze,
- *Read (czytaj)*, prawo do przeglądania właściwości (atrybutów) obiektu,
- *Write (zapisz)*, prawo do modyfikowania właściwości obiektu,
- *Create (twórz)*, prawo do tworzenia nowego obiektu,
- *Delete (usuń)*, prawo do usunięcia obiektu,
- *Extended (rozszerz)*, specjalne prawo unikatowe dla danych klas obiektów,
- *Permissions (uprawnienia)*, prawo do zmiany uprawnień dla obiektu.

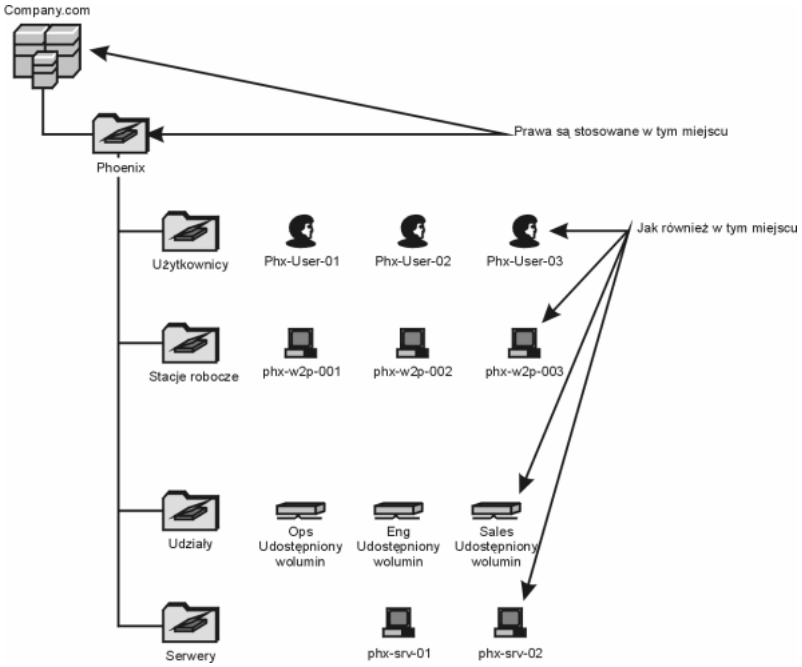
Gdy użytkownik uzyska dostęp do serwera, zostaje mu przyznany *żeton dostępu*. Zawiera on *identyfikator zabezpieczeń*, reprezentuje użytkownika oraz identyfikatory zabezpieczeń wszystkich grup, do których należy. Gdy użytkownik próbuje uzyskać dostęp do obiektu, lokalny podsystem zabezpieczeń *LSASS (Local Security Authority SubSystem)* sprawdza deskryptor zabezpieczeń w obiekcie i żetonie dostępu, a następnie potwierdza, że jeden albo kilka identyfikatorów zabezpieczeń w żetonie pasuje do jednego albo kilku wpisów na liście kontroli dostępu obiektu. W zależności od tego potwierdzenia, użytkownik może otrzymać prawo dostępu do obiektu.

W Windows 2000 funkcje zabezpieczeń pozostają takie same, jak w klasycznym systemie NT; udostępnione zostały natomiast dwie nowe właściwości:

- *Delegacja*. Prawa dostępu przypisane przez wyższe upoważnienie powiązane są z grupą albo indywidualnym użytkownikiem i stosowane są w kontenerze.

- *Dziedziczenie*. Prawa dostępu przypisane do kontenera przechodzą w dół katalogu i odnoszą się do wewnętrznych kontenerów i obiektów kontenera.

Delegacja i dziedziczenie odgrywają bardzo istotną rolę w strukturze katalogów, dlatego warte są szczegółowej analizy (spójrz na rysunek 8.8). Wyobraź sobie firmę średniej wielkości, która chce, abyś zaprojektował jej katalog dla pojedynczej domeny Windows 2000. Pracę tę musisz oczywiście rozpocząć od sprawdzenia struktury zarządzania informacją techniczną.



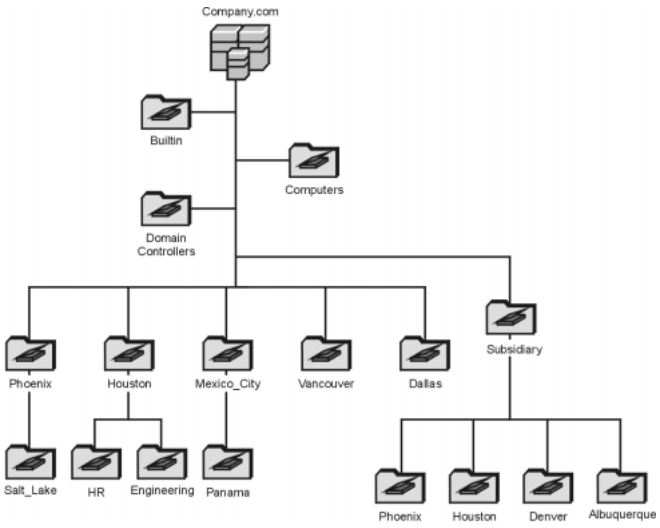
Rysunek 8.8. *Przykład dziedziczenia praw dostępu*

Załóżmy, że mamy do czynienia z firmą, która bazuje na modelu rozproszonego zarządzania informacjami, a indywidualni użytkownicy są odpowiedzialni za udostępniane zasoby. Innymi słowy, system informacyjny firmy jest zarządzany przez niezależne grupy, a ponadto firma nie przeznacza dużych sum na wdrożenie technologii i chce, aby system zarządzania pozostał zdecentralizowany. Większość organizacji posiada swoje własne serwery, infrastrukturę sieci, personel techniczny; potrzebuje tylko dobrego projektanta, który zaplanuje system zarządzania domeną. Nie zrażając się potencjalnymi problemami rozpocznij pracę od zaplanowania struktury wyższego kontenera katalogu.

Przykład struktury wyższego kontenera

Musisz teraz zaprojektować strukturę kontenera, która przyporządkuje użytkowników do grup administracyjnych. Dzięki temu będziesz mógł delegować prawa administratora tak, aby ich dziedziczenie obejmowało tylko określone segmenty użytkowników.

Na rysunku 8.9 przedstawiona została struktura kontenera dla pojedynczej domeny. Obejmuje ona zachodnią część Stanów Zjednoczonych, Meksyk i część Ameryki Środkowej. Firma prowadzi dwa rodzaje działalności. Jeden z nich wykorzystuje zasoby obu biur firmy, posiada też dodatkowe zasoby w dwóch odległych od siebie miastach.



Rysunek 8.9. *Struktura wyższego kontenera dla firmy North American prowadzącej dwa rodzaje działalności i posiadającej pojedynczą domenę*

Firma posiada wiele działów, w których zatrudnia pozornie niezależny od siebie personel informatyczny. Załóżmy, że jeden z jej działów domaga się, by dane przechowywane na jego serwerach i lokalnych dyskach twardych (niektórzy wciąż nie wierzą w zabezpieczenia sieciowe) były całkowicie poufne i dostęp do nich mieli tylko członkowie grupy administracyjnej. Podobne wymagania stawiają też pozostałe działy firmy. Nawet szefostwo, które zażyczyło sobie centralnego systemu zarządzania, również żąda pewnej autonomii i może być niezadowolone z projektu centralnego zarządzania domeną.

Struktura wyższego kontenera dla domeny wyznaczana jest dzięki liniom określającym lokalizację geograficzną biur. Działy, które posiadają niezależny personel informatyczny otrzymują osobne kontenery znajdujące się w obrębie ich biur. Pozwala to na administrowanie podrzędnymi kontenerami przez lokalny personel, dzięki czemu nie muszą być one nadzorowane przez centralną grupę techników. Przykładem odmiennej sytuacji jest obiekt Salt_Lake — lokalny personel mógłby z powodzeniem zająć się administracją własnego obiektu, lecz technicy Phoenix nie zdecydowali się na przyznanie im takich praw.

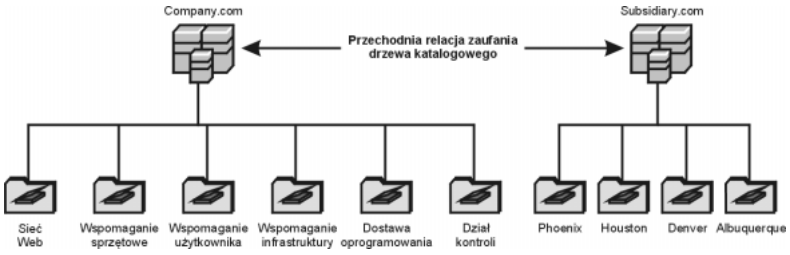
Wyświetlanie specyfikatorów i lokalizacji

W poprzednim rozdziale przedstawione zostały specyfikatory — specjalne obiekty katalogu udostępniające reguły językowe i interpunkcyjne, dzięki którym możliwe jest wyświetlanie obiektów katalogu w różnych wersjach językowych; i tak np., obiekty katalogu w Mexico City będą wyświetlane w języku hiszpańskim, a nie angielskim.

Projekt zakłada umieszczenie prawie wszystkich obiektów OU (jednostki organizacyjnej) na wierzchołku katalogu albo blisko niego. Posiadanie szerokiej struktury katalogu

nie wiąże się z żadnymi konsekwencjami, natomiast sytuacja odwrotna nie jest mile widziana. Należy unikać tworzenia głębokiej struktury katalogu. W bazie danych ESENT indeksowanie i buforowanie dla 10 poziomów wykonywane jest łatwo — jednakże głębsza struktura zdecydowanie nie jest zalecana. Zdecentralizowana organizacja może być kłopotliwa dla utrzymania płytkiej struktury kontenera, dlatego warto skonsultować się z technikami Microsoftu i razem określić konfigurację optymalną dla danej sytuacji.

Struktura kontenera byłaby zupełnie inna, gdyby firma posiadała potężny centralny dział zarządzania, którego personel mógłby często kontrolować i oceniać wydajność wszystkich serwerów sieciowych. W takiej sytuacji mógłbyś wyeliminować wyższe poziomy katalogu i utworzyć strukturę podobną do przedstawionej na rysunku 8.10.



Rysunek 8.10. *Wyższe kontenery dla wysoce scentralizowanej organizacji, w której gałęzie biznesu są skonfigurowane jako równorzędne domeny w lesie katalogowym*

Warstwa kontenera dla wysoce scentralizowanej organizacji rozdziela prawa zarządzania pomiędzy grupy autonomiczne. Kontenery przechowują użytkowników, grupy, komputery, drukarki i udostępnione foldery kontrolowane przez grupy — bez względu na lokalizację biura. Katalog jest replikowany do wszystkich kontrolerów domeny, dzięki czemu np. kontener Wspomaganie użytkownika może przechowywać obiekty Phoenix, Houston i Mexico City. Zauważ, że administratorzy w domenie *Subsidiary.com* nie ufają centralnej grupie informatyków, lecz posiadają oddzielny obszar nazw, który został przyłączony do lasu katalogowego dzięki relacji zaufania.

Podział wysokiego poziomu obiektów OU dokonany został na podstawie oceny zadań wykonywanych przez personel informatyczny, a nie przez poszczególne działy firmy. Nie wpływa on na funkcjonalność konta użytkownika, dopóki ograniczasz się do pojedynczej domeny. Jeżeli posiadasz jedną globalną domenę, użytkownik może zmienić lokalizację z Phoenix na Seul i nadal będzie posiadał dostęp do tej samej domeny, będzie też mógł używać tego samego identyfikatora logowania do sieci. Zanim jednak zdecydujesz się na zaprojektowanie przedstawionej struktury domeny, zastanów się dobrze, czy dla potrzeb Twojej firmy wystarczająca będzie jedna domena.

Strategie projektowania dla niższych poziomów katalogu

Zasady projektowania niższych poziomów katalogu różnią się trochę od zasad stosowanych przy wyższych poziomach. Na tym etapie musisz wziąć pod uwagę dwie sprawy: po pierwsze maksymalne ułatwienie administratorom zarządzania, po drugie — ułatwienie użytkownikom dostępu do zasobów. Zacznijmy od pierwszego problemu.

Dobre zarządzanie oznacza dobrą strategię delegowania. Nie jest tajemnicą, że upoważnienie do zarządzania powinno znajdować się w organizacji tak nisko, jak to tylko możliwe. Wynika stąd trzecia zasada projektowania:

> *Zasada projektowania domeny: Projektuj z myślą o scentralizowanej kontroli struktury katalogu oraz o lokalnych kontrolach obiektów katalogu.*

Implementacja kontroli zarządzania na niższych poziomach katalogu wymaga zrozumienia idei *zasad grup*. Temat ten został dokładnie omówiony w rozdziale 10. Poniżej znajdziesz najważniejsze informacje, które pomogą zrozumieć rolę zasad grup w projektowaniu katalogu.

Funkcjonalne omówienie zasad grupy

Klasyczne systemy NT i Windows 95 przedstawiły koncepcję założeń systemowych, pozwalających na rozprzestrzenianie aktualizacji rejestru systemowego. Założenia systemowe są zbiorem kluczy i wartości rejestru zebranych w pliku *NTCONFIG.POL* (w przypadku Windows 9x jest to plik *CONFIG.POL*), który jest rozprzestrzeniany podczas logowania (dane są pobierane za pomocą pliku *NETLOGON* z kontrolera domeny).

Zasady grupy Windows 2000 są ulepszoną formą mechanizmu rozprzestrzeniania zasad, które dotyczą skryptów logowania i rozłączania, automatycznego pobierania oprogramowania, konfiguracji zabezpieczeń, przekierowywania folderu i opcji świadectwa kryptograficznego.

Zasady grup dotyczące ustawień rejestru są przechowywane w plikach *REGISTRY.POL*. Pliki te są pobierane podczas logowania i stosowane do lokalnego rejestru. Zasady grup dotyczące ustawień konfiguracji komputera są związane z wpisami w grupie *HKEY_Local_Machine*, a zasady dotyczące ustawień konfiguracji użytkownika w grupie *HKEY_Current_User*.

Jedną, niezmiernie ważną różnicą pomiędzy zasadami grup i założeniami systemowymi jest to, że zasady grup są stosowane w „lotny" sposób. Nie są na stałe zapisywane w rejestrze, tak jak założenia systemowe. Gdy zasada grup zostaje usunięta, pierwotne ustawienia rejestru są ponownie wykorzystywane. Zasady grup są odświeżane co 90 minut, aż do momentu wylogowania użytkownika. Niektóre zasady mogą być używane tylko podczas operacji wylogowania.

Zasady grup są przechowywane w różnych miejscach w zależności od tego, czy są używane tylko do systemu lokalnego, czy też są rozprzestrzeniane z kontrolera domeny do wszystkich komputerów domeny:

- *Zasady lokalne*. Zasady te są przechowywane na twardym dysku w katalogu *\WINNT\System32\GroupPolicy*. Dotyczą lokalnego komputera i użytkowników, którzy logują się do komputera.
- *Zasady Active Directory*. Zasady te są przechowywane w dwóch miejscach. Główne zasady znajdują się w katalogu *\WINNT\Sysvol\Sysvol\<nazwa_domeny>* na każdym kontrolerze domeny. Drugi katalog *Sysvol* jest udostępniony z nazwą *SYSVOL*. Reszta zasad jest przechowywana w katalogu w ustawieniach kontenerów

Group Policy albo obiektów GPC. Zasady te mogą być związane z kontenerem Domain, Site albo dowolnym kontenerem OU. Więcej informacji znajdziesz w rozdziale 7.

Katalog *\WINNT\Sysvol\Sysvol\<nazwa_domeny>* jest replikowany do wszystkich kontrolerów domeny. Za tę czynność odpowiedzialna jest usługa *FRS (File Replication Service — usługa replikacji plików)*, która została szczegółowo omówiona w rozdziale 13. „Zarządzanie systemami plików". W dużym skrócie, FRS jest usługą synchronizującą dane, zaprojektowaną do replikowania plików do docelowych serwerów. Kopiowane są tylko zaktualizowane pliki bazy danych. FRS wymaga jednak używania systemu NTFS5 na wszystkich replikowanych woluminach.

Zasady grup rozprzestrzeniane przez kontrolery domeny posiadają obiekty w katalogu wskazujące na foldery w *SYSVOL*. Obiekty te są przykładami klasy GroupPolicyContainer albo GPC. Klienty Windows 2000 automatycznie wyszukują obiekty GPC i ładują pliki zasad. Zasady grup mogą być połączone z kontenerami OU, Domain-DNS i Sites. Zasady posiadają własną hierarchię, dzięki której rozwiązywane są różne konflikty pierwszeństwa. Zasady OU posiadają priorytet. W dalszej kolejnością znajdują się zasady Domain, Site, Local i System.

Kontener może zawierać wiele zasad grup, jak również jedną zasadę połączoną z więcej niż jednym kontenerem. Zasady są wyświetlane według identyfikatorów GUID, które nie dają niestety zbyt wielu przydatnych informacji.

Operacyjne omówienie zasad grup

Zasady grup są konfigurowane za pomocą konsoli Group Policy (Zasady grupy). Konsola bazuje na edytorze zasad Group Policy Editor — *GPEDIT.DLL*. Edytor może być ładowany za pomocą wielu różnych przystawek, w zależności od lokalizacji zasady:

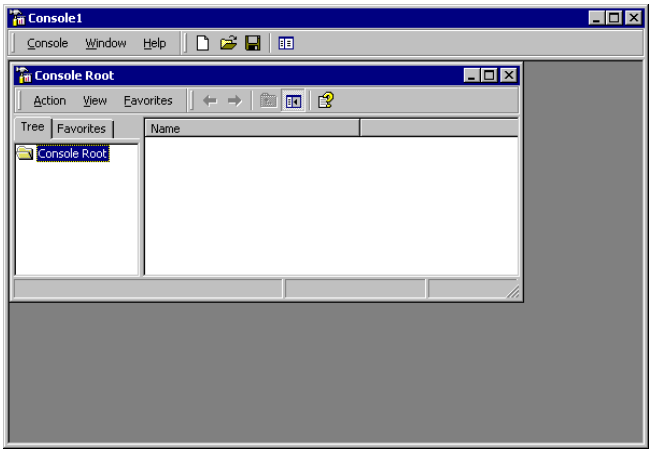
- *Group Policy Editor (Edytor zasad grupy) — GPEDIT.MSC*, jest używana do edycji zasad lokalnych.
- *AD Users and Computers (Użytkownicy i komputery Active Directory) — DSA.MSC*, jest używana do tworzenia i edytowania profili związanych z kontenerem Domain i dowolnymi kontenerami OU.
- *AD Sites and Services (Lokacje i usługi AD) — DSSITE.MSC*, jest używana do tworzenia i edytowania profili związanych z kontenerami Site.

Edytor zasad grup zawiera kilka rozszerzeń przystawek odpowiadających typom zasad, które mogą być edytowane. Wszystkie rozszerzenia są domyślnie ładowane. Możesz również utworzyć niestandardową konsolę Group Policy, która będzie wygodniejsza w użyciu od standardowej konsoli, szczególnie wtedy, gdy zamierzasz rozprzestrzeniać zasady do użytkowników wraz z delegacjami praw administracyjnych. W tym celu wykonaj poniższą instrukcję:

Procedura 8.1.
Tworzenie konsoli GPE

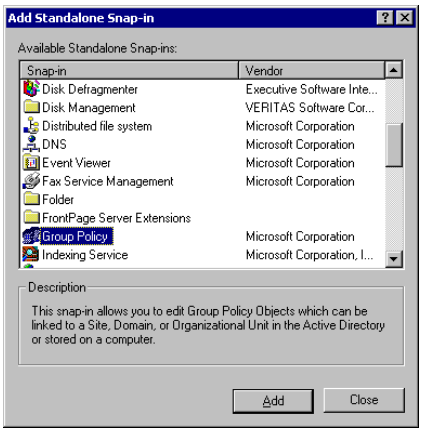
1. Za pomocą menu *Start* otwórz okno *Run (Uruchom)*, wpisz w nim `MMC` i kliknij *OK*. Pojawi się puste okno konsoli *MMC*, tak jak przedstawia to rysunek 8.11.

Rysunek 8.11.
Pusta konsola MMC gotowa do dodawania nowych wstawek

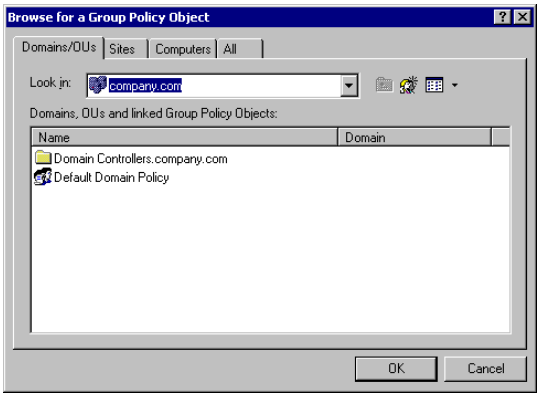


2. Z menu *Console (Konsola)* wybierz *Console (Konsola)|Add/Remove Snap-in (Dodaj/Usuń przystawkę)* — możesz skorzystać ze skrótu *Ctrl+M*. Wyświetlone zostanie okno *Add/Remove Snap-in (Dodaj/Usuń przystawkę)*.
3. Kliknij *Add (Dodaj)*. Wyświetlone zostanie *Add Standalone Snap-in (Dodawanie przystawki autonomicznej)* — rysunek 8.12.

Rysunek 8.12.
Okno Add Standalone Snap-in (Dodawanie przystawki autonomicznej)



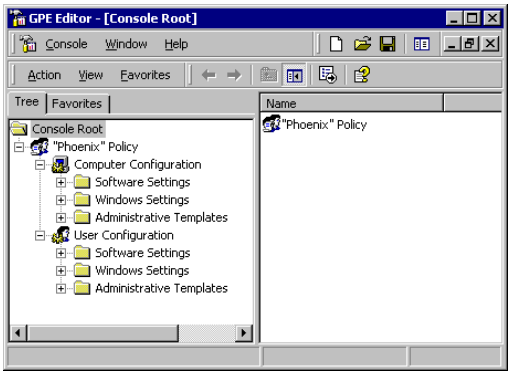
4. Z wyświetlonej listy zaznacz pozycję *Group Policy (Zasady grupy)*. Wyświetlone zostanie okno *Select Group Policy Object (Wybierz obiekt zasad grupy)*. W polu *Group Policy Object (Obiekt zasad grupy)* widoczny jest domyślny wpis — *Local Computer (Komputer lokalny)*.
5. Kliknij przycisk *Browse (Przeglądaj)*. Wyświetlone zostanie okno *Browse for a Group Policy Object (Przeglądanie obiektów zasad grupy)* — rysunek 8.13.



Rysunek 8.13. *Okno Browse for a Group Policy Object (Przeglądanie obiektów zasad grupy) przedstawiające listę dostępnych obiektów dla danej domeny*

- Zakładka *Domains/OUs (Domeny/OU)* wyświetla zasady, które zostały utworzone i połączone z kontenerem OU albo Domain-DNS.
- Zakładka *Sites (Lokacje)* wyświetla zasady, które zostały utworzone i połączone z kontenerem Sites.
- Zakładka *Computer (Komputer)* wyświetla zasady, które zostały utworzone i połączone z danym obiektem Computer.

6. Na zakładce *Domain/OUs (Domeny/OU)* kliknij dwukrotnie pozycję *OU*. Na liście pojawi się powiązany obiekt zasad grup.
7. Jeżeli na liście nie pojawił się żaden obiekt, to znaczy, że nie został on jeszcze utworzony dla tego kontenera OU. W części *Name (Nazwa)* prawym przyciskiem myszy kliknij biały obszar, a następnie z wyświetlonego menu wybierz polecenie *New (Nowy)*. Na liście pojawi się ikona zasady z domyślną nazwą *New Group Policy Object (Nowy obiekt zasad grupy)*.
8. Zmień istniejącą nazwę na bardziej opisową.
9. Kliknij *OK*, aby zapisać nowy wybór i powrócić do okna *Select Group Policy Object (Wybierz obiekt zasad grupy)*.
10. Kliknij *Finish (Zakończ)*, aby zapisać wprowadzone zmiany i powrócić do okna *Add Standalone Snap-in (Dodaj przystawkę autonomiczną)*.
11. Kliknij *Close (Zamknij)*, aby powrócić do okna *Add/Remove Snap-in (Dodaj/Usuń przystawkę)*. Nowy obiekt będzie znajdował się na liście dostępnych obiektów zasad dla tej przystawki.
12. Zaznacz zakładkę *Extensions (Rozszerzenia)*.
13. Upewnij się, czy opcja *Add All Extensions (Dodaj wszystkie rozszerzenia)* jest zaznaczona — wyświetlane są wszystkie dostępne opcje obiektu (rysunek 8.14).
14. Kliknij OK, aby zapisać zmiany i powrócić do okna *Console (Konsola)*. Nowa zasada pojawi się w lewym panelu okna w gałęzi *Console Root (Katalog główny konsoli)*. Jeżeli chcesz zachować te ustawienia dla konsoli MMC, zaznacz *Console (Konsola)|Save as (Zapisz jako)*, a następnie nadaj konsoli nazwę. Konsola zostanie zapisana w pliku z rozszerzeniem *.MSC*.



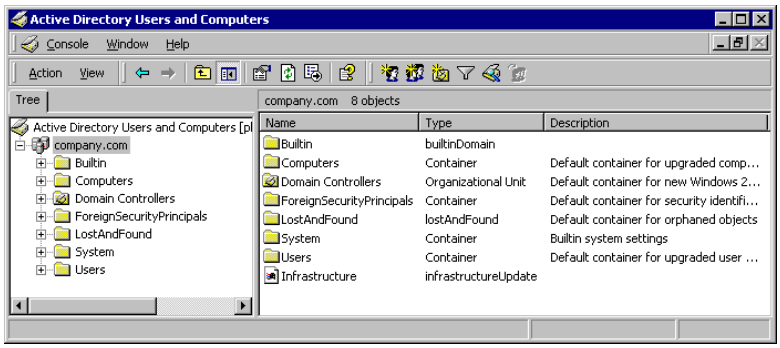
Rysunek 8.14. *Group Policy Editor (Edytor zasad grupy) wraz z załadowanym domyślnym obiektem domeny*

15. Nowa konsola zostanie zapisana w folderze *My Documents (Moje dokumenty)*. Dostęp do folderu możliwy jest m.in. za pomocą menu *Start|Documents (Dokumenty)|My Documents (Moje dokumenty)*.

Przypisywanie zasad grupy do kontenerów

Zbierając informacje o działach firmy i grupach organizacji, zastanów się, czy potrzebują one osobnych zasad. Na przykład menedżer działu Sprzedaż chce mieć pod kontrolą wszystkie komputery swoich pracowników, aby móc kontrolować ich pracę. Dzięki temu menedżer będzie mógł szybko kierować swoje dyrektywy do określonych pracowników: „Natychmiast zakończ grać w sapera i zajmij się swoją pracą!”.

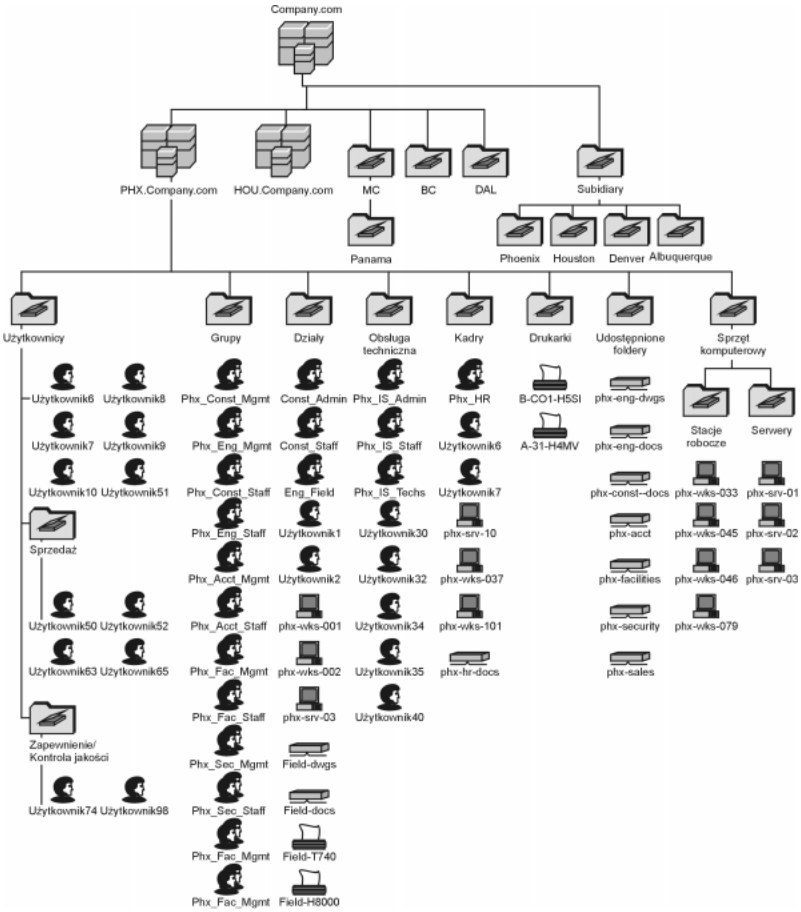
Decydując się na granice zasad, nie zapomnij o lokacjach. Załóżmy na przykład, że uniwersytet ustanowił pewną zasadę dla wszystkich wydziałów i nie zastosował jej jeszcze dla kilku placówek. Zamiast stosowania zasady do pięciu różnych domen, możesz połączyć zasady do obiektu lokacja. Spowoduje to zastosowanie zasady do wszystkich komputerów i użytkowników, którzy zalogowali się do połączonej podsieci IP. Na rysunku 8.15 przedstawiony został przykład konfiguracji globalnej strony. Każda lokacja posiada inną podsieć IP, która prowadzi klienta do właściwych lokalnych kontrolerów domeny.



Rysunek 8.15. *Przystawka Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory) przedstawiająca przykład konfiguracji strony dla globalnego katalogu*

Przykład projektu katalogu niższego poziomu

Stosując zasady projektowe domeny niższego poziomu do omawianego przykładu firmy, projekt kontenera dla niższych poziomów domeny *Company.com* mógłby wyglądać tak, jak przedstawia to rysunek 8.16. Celem diagramu jest przedstawienie jedynie jednego rozwiązania. Samodzielnie możesz zaprojektować całkiem inny schemat i utworzyć całkiem nowy scenariusz. Z pewnością można zaprojektować tysiące struktur domeny *Company.com*. System NetWare 4.x jest obecny na rynku od wielu lat. Z pewnością istnieje kilka milionów węzłów zarządzania siecią, a ja będąc w pełni świadom tego co mówię uważam, że nie ma dwóch identycznych drzew NDS. Projekty domen Windows 2000 z pewnością również będą tak urozmaicone.



Rysunek 8.16. *Struktura kontenera niższego poziomu dla pojedynczej domeny w katalogu zawierającym wiele domen*

Wierzchołek katalogu zachowuje strukturę kontenera przedstawioną w poprzedniej części rozdziału. Niższe kontenery zostały natomiast zaprojektowane w następujący sposób:

- *Użytkownicy*. Kontener przechowuje konta dla wszystkich użytkowników biura Phoenix z wyjątkiem personelu grup Kierownicy i Obsługa techniczna który przyłącza się do sieci poprzez sieć LAN Phoenix. Umieszczenie wszystkich użytkowników w jednym kontenerze sprawia, że możliwe staje się delegowanie

grupy administracyjnej dla tego kontenera. Podrzędny kontener Sprzedaż gromadzi żądania dla różnych zasad grup. Teoretycznie każdy dział mógłby mieć swój własny kontener OU ze specjalnie określonymi dla niego zasadami grup. Taka struktura wymaga jednak wiele czasu i zasobów.

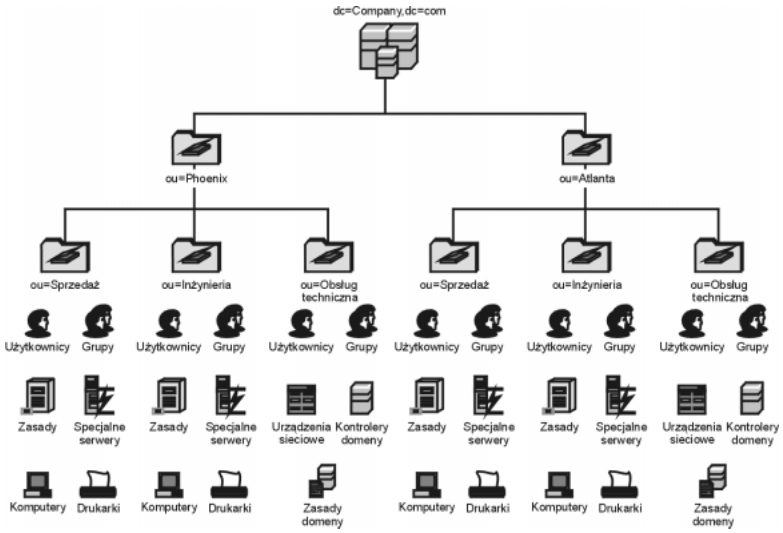
- *Grupy*. Ten kontener ma na celu utrzymanie pewnego porządku w sieci. Przechowywanie obiektów grupy w jednym kontenerze ułatwia ich wyszukanie. Jest problem, gdy musisz zarządzać kilkoma tysiącami grup. Umieszczenie grup w różnych kontenerach nie wpływa na spadek wydajności działania domeny.
- *Działy*. Kontener udostępnia miejsce na przechowanie obiektów ze zdalnych lokalizacji. Dla kontenera najważniejsze są dwie rzeczy: po pierwsze zasady grup dla personelu działu są zazwyczaj mniej ograniczone niż zasady biura, a po drugie za operacje działu często odpowiedzialni są lokalni administratorzy, którzy nie są tak „zmanierowani" jak naczelni administratorzy. Oddzielny kontener umożliwia przypisanie ograniczonych praw administracyjnych użytkownikom i komputerom.
- *Obsługa techniczna i Kadry*. Kontenery udostępniają jednostki zarządzania, które są wystarczające do utrzymania własnej autonomii przez osobny personel. Taka sytuacja niesie oczywiście ze sobą pewne niebezpieczeństwo. Otóż gdy administratorzy działów w jakiś sposób utracą dane z katalogu, administratorzy z głównej grupy technicznej nie będą mogli w żaden sposób ich odzyskać.
- *Drukarki i Udostępnione foldery*. Kontenery posiadają elementy, których użytkownicy szukają wokół wierzchołka struktury kontenera. Im mniej kontenerów użytkownik będzie musiał przeszukać, tym jest większe prawdopodobieństwo, że będzie korzystał z ich zawartości. Jeżeli dostęp do katalogu będzie prosty, użytkownicy z większą chęcią będą z niego korzystać.
- *Sprzęt komputerowy*. Kontener umieszcza obiekty Computer w dwóch oddzielnych kontenerach — jeden w stacjach roboczych, a drugi w serwerach — w których mogą być one zarządzane jako różne elementy. Część administratorów sieciowych może posiadać prawa administracyjne tylko dla stacji roboczych, podczas gdy inna część może posiadać prawa do administracji serwerów. Nie ma żadnej korzyści z umieszczenia w jednym kontenerze obiektów komputerów i ich użytkowników. Znacznie łatwiej znaleźć obiekty w kontenerze zawierającym obiekty tego samego typu.

Po zaprojektowaniu niższego poziomu domeny, należy zająć się zagadnieniem dostępu użytkowników, menedżerów i administratorów. Ta część projektu zabiera trochę czasu, nawet w przypadku małych organizacji. Możesz utworzyć małe środowisko laboratoryjne i sprawdzić w jaki sposób użytkownicy logują się do domeny, korzystają z jej zasobów, i jak sprawdza się struktura kontenerów.

Jeżeli masz do czynienia z małą organizacją, projekt struktury przedstawiony na rysunku 8.16 może być zbyt skomplikowany. W takim przypadku bardziej odpowiedni wydaje się być projekt widoczny na rysunku 8.17.

Gdy liczba personelu działu obsługi technicznej jest ograniczona, lokalni administratorzy zmuszeni są wziąć na siebie więcej obowiązków. Z tego powodu na rysunku 8.16 widoczny jest podział funkcyjny niższych kontenerów. Każdej grupie w każdej jednostce organizacyjnej można przypisać prawa administracyjne, dzięki czemu zarówno lokalni, jak i centralni administratorzy mogą modyfikować grupy.

Rysunek 8.17.
Projekt katalogu dla małej firmy



Bez względu na wybór metody projektowania, najważniejszy jest postęp pracy. Pozostaw sobie pewną przestrzeń, w obrębie której będziesz mógł eksperymentować i nie obawiaj się wprowadzania zmian w sposobie zarządzania administratorów. Jeżeli zmiany nie będą radykalnie wpływać na sposób pracy użytkowników, możesz eksperymentować.

W tym miejscu można zakończyć etap przygotowania projektu domeny i zająć się zagadnieniem rozmieszczenia specjalnych serwerów.

Specjalne serwery

Na zakończenie projektowania domeny, musisz zdecydować się, w którym miejscu umieścić kilka specjalnych serwerów. Są to kontrolery domeny dla różnych domen, serwery katalogu globalnego, pomocnicze serwery DNS i wzorce FSMO. Z tej grupy serwerów zdecydowanie najbardziej „egzotyczne" są wzorce FSMO — zatem od nich zaczniemy omawianie grupy.

Wzorce FSMO

Właściwość replikowania informacji pozwala, by wszystkie kontrolery domeny były sobie równe (posiadały ten sam status). Wciąż jednak z różnych powodów niektóre czynności muszą być przyporządkowane jednemu kontrolerowi domeny. Czynności te są nazywane *operacjami FSMO (Flexible Single Master Operation — elastyczne operacje wykonywane przez serwer pełniący rolę wzorca)*. Kontroler domeny pełniący obowiązki FSMO nosi natomiast nazwę *wzorca FSMO*.

Wzorce FSMO są automatycznie wybierane przez system, jakkolwiek istnieje możliwość przeniesienia funkcji wzorca do innego kontrolera domeny. Możliwość taka jest niezbędna, gdyż w przypadku awarii kontrolera domeny pełniącego funkcję wzorca, musi istnieć sposób przeniesienia funkcji do innego serwera. Przeniesienie to nosi nazwę

przechwycenia funkcji. Zgodnie jednak z ogólnie przyjętą zasadą, nie powinno się przenosić funkcji, dopóki pierwotny kontroler może prawidłowo pracować. Więcej informacji na ten temat znajdziesz w rozdziale 10.

Tożsamość danego wzorca FSMO jest określana przez atrybut FSMORoleHolder związany z obiektem katalogu. Funkcje i obiekty katalogu reprezentują:

- *Domain Naming Master (Wzorzec nazw domeny)*. Kontroluje dodatkowe i zdalne domeny w lesie katalogowym.
- *Schema Master (Wzorzec schematu)*. Kontroluje dostęp do zapisu/odczytu kontekstu nazw schematu. Pozostałe kontrolery domeny w lesie posiadają tylko prawo do odczytu repliki kontekstu nazw.

Tożsamości tych dwóch wzorców muszą być jednoznaczne w lesie katalogowym i muszą znajdować się na tym samym kontrolerze domeny. Ich funkcje różnią się od siebie. Pierwszy promowany kontroler domeny staje się automatycznie wzorcem nazw domeny i wzorcem schematu. Jeżeli te dwie funkcje są niedostępne, wykonywanie standardowych operacji nie zostaje zachwiane, lecz nie ma możliwości dodawania i usuwania domen, jak również nie można modyfikować schematu. Obie funkcje są używane stosunkowo rzadko, więc zazwyczaj jest dużo czasu na naprawę uszkodzonego serwera. Funkcje nie wymagają dużej ilości zasobów i właściwie nie generują żadnego transferu. Z tego powodu powinny być przenoszone tylko wtedy, gdy pojawi się inny kontroler domeny, który będzie znajdował się w dużo lepszej lokalizacji. Należy pamiętać o tym, aby zawsze przypisywać obie funkcje do tego samego kontrolera domeny, w przeciwnym wypadku mogą pojawić się problemy integralności danych w katalogu.

Tożsamość wzorca nazw domeny jest przechowywana w atrybucie FSMORoleMaster obiektu Partitions. Obiekt Partitions jest przechowywany w kontenerze Configuration. Obiekt nie jest widoczny w standardowych konsolach Active Directory, lecz można go przeglądnąć w następujący sposób:

Procedura 8.2.
Przeglądanie tożsamości wzorca

1. Otwórz przystawkę *AD Domains and Trusts (Domeny i relacje zaufania usługi Active Directory)*.
2. Prawym przyciskiem myszy kliknij ikonę *Domains and Trusts (Domeny i relacje zaufania)* znajdującą się na wierzchołku drzewa.
3. Z wyświetlonego menu wybierz polecenie *Operation Master (Operacje wzorca)*.

Tożsamość wzorca schematu jest przechowywana w atrybucie FSMORoleMaster kontenera Schema. Obiekt ten również nie jest widoczny ze standardowych konsoli Active Directory i może być przeglądany w następujący sposób:

Procedura 8.3.
Ładowanie standardowej konsoli zarządzania Active Directory

1. W oknie *Run (Uruchom)* wpisz `SCHMMGMT.MSC`. Spowoduje to uruchomienie konsoli *Schema Management (Zarządzanie schematem)*.

2. Prawym przyciskiem myszy kliknij ikonę *Schema Manager (Menedżer schematu)* znajdującą się na wierzchołku drzewa.
3. Z wyświetlonego menu wybierz polecenie *Operations Master (Operacje wzorca)*.

Wzorzec identyfikatora względnego

Wszystkie obiekty w Windows 2000 posiadają identyfikatory zabezpieczeń. Identyfikator jest kombinacją identyfikatora zabezpieczeń domeny i sekwencyjnego numeru noszącego nazwę identyfikatora względnego. Kontrolery domeny w Windows 2000 dodają 100 000 numerów do obiektów zabezpieczeń utworzonych przez dany kontroler domeny. W trybie mieszanym domeny tylko jeden kontroler może przyznawać identyfikatory względne — emulator podstawowego kontrolera domeny. W ten sposób wszystkie identyfikatory względne są sekwencyjne, co jest niezbędne dla klasycznych pomocniczych kontrolerów domeny. W trybie macierzystym domeny Windows 2000 dowolny kontroler może przypisać względny identyfikator do pryncypia zabezpieczeń.

W trybie rodzimym obszar identyfikatorów względnych jest przekazywany z jednego kontrolera domeny do drugiego. Gdy kontroler domeny potrzebuje większej liczby identyfikatorów, staje się wzorcem identyfikatora względnego i otrzymuje cały obszar identyfikatorów. Wszystkie numery są przechowywane w obiekcie katalogu o nazwie RID Set za pomocą atrybutu RIDAllocationPool. Obiekt RID jest zlokalizowany w obiekcie Computer kontrolera domeny w kontenerze Domain Controllers. Obiekt ten przechowuje również wartości następnego identyfikatora względnego oraz numer ostatniego pola alokacji, utrzymywanego przez ten kontroler domeny.

Tożsamość wzorca nazw domeny jest przechowywana w atrybucie FSMORoleMaster obiektu RID Manager$ w kontenerze System. Atrybut zawiera nazwę wyróżnioną obiektu NTDS Settings wskazującą na serwer, tak jak zostało to przedstawione poniżej:

```
Ntds Settings, cn=phx-dc-01, cn=Servers, cn=Phoenix, cn=Sites, cn=Configuration,
dc=Company, dc=com.
```

Obiekt ten nie jest widoczny za pomocą standardowych przystawek zarządzania katalogiem. Aby przeglądnąć albo zmienić tożsamość wzorca identyfikatora względnego, otwórz przystawkę *Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory)*, prawym przyciskiem myszy kliknij ikonę *Users and Computers (Użytkownicy i komputery)* znajdującą się na wierzchołku drzewa, a następnie z wyświetlonego menu wybierz *Operations Masters (Wzorce operacji)*.

Wzorzec podstawowego kontrolera domeny

W trybie mieszanym domeny klasyczne pomocnicze kontrolery domeny mogą jedynie pobierać uaktualnione repliki z podstawowego kontrolera domeny. Pomocnicze kontrolery korzystają tylko z kontrolera podstawowego i z żadnego innego. Posiadają specjalny obiekt SAM noszący nazwę LSA Secret, który łączy je z kontrolerem podstawowym za pomocą zdalnej procedury wywołania.

Z tego powodu klasyczny podstawowy kontroler domeny jest zawsze pierwszy promowany do kontrolera Windows 2000 stając się jednocześnie wzorcem. Przesuwając rolę wzorca do innego kontrolera, przeprowadza się jakby operację promowania kontrolera pomocniczego do podstawowego. Wszystkie repliki pobierane są teraz z nowego kontrolera, który uzyskał status wzorca. Rolę wzorca może pełnić tylko kontroler domeny Windows 2000. Gdy jeden z kontrolerów domeny został już promowany do kontrolera Windows 2000, nie ma możliwości powrotu do klasycznego podstawowego kontrolera bez usunięcia promowanego kontrolera.

Tożsamość wzorca nazw domeny jest przechowywana w atrybucie FSMORoleMaster obiektu Domain-DNS, takim jak np. *dc=Company, dc=com*. Atrybut ten zawiera nazwę wyróżnioną obiektu NTDS Settings wskazującą na serwer, tak jak zostało to poniżej przedstawione:

```
Ntds Settings, cn=phx-dc-01, cn=Servers, cn=Phoenix, cn=Sites, cn=Configuration,
dc=Company, dc=com.
```

Atrybut ten nie jest wyświetlany jako właściwość obiektu w konsoli *AD Users and Computers (Użytkownicy i komputery usługi Active Directory)*. Można go natomiast przeglądnąć w następujący sposób:

Procedura 8.4.
Przeglądanie atrybutu FSMORoleMaster

1. Prawym przyciskiem myszy kliknij ikonę *AD Users and Computers (Użytkownicy i komputery usługi Active Directory)* znajdującą się na wierzchołku drzewa.
2. Z wyświetlonego menu wybierz *Operations Masters (Wzorce operacji)*. Wyświetlone zostanie okno *PDC Role Master (Wzorzec podstawowego kontrolera domeny)*.

Wzorzec infrastruktury

Szybkie rozpowszechnianie informacji o członkach grupy w dużej sieci jest niezwykle istotne. Użytkownicy są bardzo niecierpliwi — gdy podczas przyłączania się do danej grupy są zmuszeni długo czekać na uzyskanie dostępu, szybko zaczynają się denerwować. Windows 2000 nadzoruje zmiany członkostwa grupy w pojedynczej domenie FSMO za pomocą wzorca infrastruktury.

Tożsamość wzorca nazw domeny jest przechowywana w atrybucie FSMORoleMaster obiektu Infrastructure w kontenerze Domain-DNS (np. *cn=Infrastructure, dc=Company, dc=com*). Atrybut ten zawiera nazwę wyróżnioną obiektu NTDS Settings wskazującą dany serwer.

Obiekt nie jest domyślnie wyświetlany w konsoli *AD Users and Computers (Użytkownicy i komputery usługi Active Directory)*. Ustawienia te możesz jednak przeglądnąć w następujący sposób:

Procedura 8.5.
Przeglądanie atrybutu FSMORoleMaster

1. Prawym przyciskiem myszy kliknij ikonę *AD Users and Computers (Użytkownicy i komputery usługi Active Directory)* znajdującą się na wierzchołku drzewa.
2. Z wyświetlonego menu wybierz *Operations Masters (Wzorce operacji)*. Wyświetlone zostanie okno *Infrastructure Role Master (Wzorzec infrastruktury)*.

Kontrolery domeny

Każdy kontroler domeny Windows 2000 posiada replikę do odczytu-zapisu kontekstu nazw domeny oraz repliki tylko do odczytu kontekstów nazw schematu i konfiguracji. W przeciwieństwie do NetWare, serwery domeny Windows 2000 nie przechowują zewnętrznych replik katalogu. Gdy użytkownicy uzyskują dostęp do danego serwera, wstępne uwierzytelnianie jest obsługiwane przez Kerberos, a użytkownicy otrzymują odpowiednie żetony dostępu, które umożliwiają (albo i nie) dostęp do obiektów zabezpieczeń. Gdy serwer jest kontrolerem domeny, uwierzytelnianie prawie nie obciąża wydajności serwera.

Określanie liczby kontrolerów domeny i planowanie ich rozmieszczenia wymaga nie tylko wiedzy technicznej, lecz również nieco zmysłu artystycznego. Tolerancja błędu wymaga, aby utworzyć przynajmniej dwa kontrolery w domenie. Podstawowymi kryteriami są wydajność i niezawodność. Jeżeli oczywiście na podstawie raportów wydajności obsługa zapytań przez jeden kontroler domeny jest wystarczająco szybka, nie ma sensu zwiększania liczby kontrolerów aż do momentu, gdy sieciowy system wejścia/wyjścia stanie się tzw. wąskim gardłem. DNS uczestniczy w podziale ładowania danych pomiędzy kontrolerami.

Utwórz zatem przynajmniej dwa kontrolery domeny w każdym dużym biurze (z powodu tolerancji błędu) oraz jeden w każdym mniejszym zdalnym biurze, dla którego nie chcesz, żeby użytkownicy byli uwierzytelniani poprzez sieć WAN. W przypadkach, gdy sieć zawiera tylko kilku użytkowników, a w dodatku posiada bardzo dobre połączenie z siecią WAN, można całkiem zrezygnować z kontrolera domeny. W takiej sytuacji musisz jednak uświadomić wszystkich użytkowników, że awaria sieci WAN powoduje utratę dostępu do ich lokalnego serwera. Bez biletu Kerberos i uwierzytelnienia użytkowników serwer odrzuci próbę połączenia. Awaria sieci WAN będzie odbierana przez użytkownika tak, jakby nastąpiło wygaśnięcie ważności biletu.

W większości przypadków ludzie popełniają ten sam błąd stawiając zbyt wiele kontrolerów domeny. Dzięki możliwości replikacji wszystkie kontrolery domeny współdzielą te same kopie katalogu. Teoretycznie problem wydajności nie powinien pojawić się dla jednego serwera. Im więcej replik kontekstów nazw, tym większe prawdopodobieństwo zniszczenia jednego z nich przez któryś z kontrolerów domeny. Gdy zmieniasz liczbę kontrolerów domeny, dokładnie przeglądaj statystyki wydajności NTDS za pomocą *Monitora wydajności (Performance Monitor)*. Jeżeli zauważysz zwiększanie natężenia przesyłu, oznacza to, że znajdujesz się w tzw. punkcie ekstremalnym charakterystyki wydajności.

Serwery katalogu globalnego

Standardowe kontrolery domeny nie przechowują kopii kontekstów nazw z innych domen. Bez lokalnej kopii kontekstu nazw z zaufanej domeny, klienty zmuszone są do uwierzytelniania poprzez sieć w celu uzyskania dostępu do kontrolera domeny w zaufanej domenie. Kontroler domeny katalogu globalnego rozwiązuje wszystkie problemy przechowywania częściowych replik wszystkich kontekstów nazw w lesie katalogowym. Rozmiar bazy tego typu mógłby być olbrzymi dla dużych sieci, dlatego też katalog zawiera tylko 60 atrybutów. Wyszukiwanie innego atrybutu jest odsyłane do kontrolera domeny przechowującego pełną replikę.

Jeżeli żaden kontroler domeny nie jest dostępny, użytkownicy nie będą mogli zalogować się do domeny. Jest to spowodowane tym, że listy członków grup uniwersalnych w zaufanych domenach są dostępne tylko w serwerach katalogu globalnego. Microsoft zdecydował się na zablokowanie dostępu użytkowników, w przypadku gdy niedostępny jest katalog globalny pozwalający na sprawdzenie ich członkostwa grup. Ograniczenie to nie dotyczy administratorów. Serwery katalogu globalnego ułatwiają wyszukiwanie LDAP poprzez udostępnienie indeksu najczęściej używanych atrybutów w każdej zaufanej domenie. Redukuje to natężenie transferu sieciowego pomiędzy zaufanymi domenami, jak również zwiększa wydajność wyszukiwania.

Promowanie kontrolera domeny do roli serwera katalogu globalnego może znacznie zwiększyć wymagania sprzętowe dla serwera w dużej sieci. Domena podrzędna z 300 użytkownikami może posiadać tablicę NTDS.DIT wielkości 15 – 20 MB, natomiast katalog globalny może być 10, 20 albo nawet 100 razy większy. Nie ma jednak sensu wymagać od mniejszych firm zakupu niesamowicie drogiego sprzętu po to, by postawić serwer katalogu globalnego. Znacznie rozsądniejsze jest zainwestowanie w dobre połączenie z siecią WAN pozwalające na uzyskiwanie z niej potrzebnych informacji. Proces uwierzytelniania w małych firmach nie generuje dużego natężenia sieciowego. W każdej chwili możesz sprawdzić transfer sieciowy za pomocą narzędzia *Network Monitor (Monitor sieci)*.

Pomocnicze serwery DNS

Stabilność i niezawodność domeny Windows 2000 całkowicie zależy od stabilności i niezawodności dynamicznego systemu DNS, który udostępnia usługę odwzorowywania nazw domeny. Umieszczenie kontrolera domeny w firmie bez pomocniczego serwera dynamicznego DNS nie wydaje się być dobrym rozwiązaniem.

Najlepszym sposobem rozprzestrzenienia usług DNS w połączeniu z katalogiem jest wykorzystanie systemu DNS zintegrowanego katalogowo (więcej szczegółów na ten temat znajdziesz w rozdziale 5.). Zintegrowany DNS umieszcza tablicę strefową bezpośrednio w katalogu, do którego ma dostęp każdy kontroler domeny. Wszystko, co musisz zrobić w tej sytuacji, to instalacja usługi DNS na kontrolerze domeny i jej konfiguracja jako pomocniczego systemu zintegrowanego katalogowo. Następnie należy już tylko skonfigurować klienty, aby mogły używać kontrolera domeny jako serwera DNS albo ustawić odpowiednią konfigurację w DHCP.

Podczas korzystania z DNS zintegrowanego katalogowo pojawi się kilka ostrzeżeń. Najważniejsze określa, że serwer DNS musi być również kontrolerem domeny. Jeżeli jesteś przyzwyczajony do przechowywania usług DNS na stacjach roboczych albo serwerach niższego statusu, powinieneś zmienić to przyzwyczajenie, szczególnie wtedy, gdy pracujesz w dużej sieci posiadającej dużą bazę katalogową.

Jeżeli posiadasz serwery różnego typu — serwery DNS Windows 2000 wraz z serwerami DNS innych systemów, jak np. BIND albo NetWare, możesz z powodzeniem używać systemu DNS zintegrowanego katalogowo na swoich serwerach Windows 2000. Musisz się jedynie upewnić, czy są one właściwie skonfigurowane do wysyłania tablic strefowych do serwerów innych niż Windows 2000 (więcej informacji znajdziesz w rozdziale 5.).

Na koniec, jeżeli rozpocząłeś już pracę z domeną Windows 2000 i masz tylko jeden albo dwa kontrolery domeny, możesz zainstalować DNS na serwerze nie będącym kontrolerem domeny i skonfigurować go jako pomocniczy standardowy DNS pobierający strefy z podstawowych serwerów. Będzie to stanowić kopię zapasową dla strefy zintegrowanej katalogowo. Nie ma potrzeby odwoływania żadnych klientów do tego serwera. Serwer ten będzie pełnił rolę tylko serwera kopii zapasowej, która może się przydać, jeżeli nie jesteś pewien konfiguracji Active Directory.