Projektowanie struktur Active Directory

Autor: Neall Allcot
Tłumaczenie: Adam Jarczyk
ISBN: 83-7197-794-8
Tytuł oryginału: Understanding & Designing Your Active Directory Infrastructure
Format: B5, stron: 294

Active Directory jest złożoną bazą danych i nieodłącznym elementem architektury sieciowej Windows 2000. Pozwala organizacjom skutecznie udostępniać i zarządzać informacjami dotyczącymi zasobów sieciowych i użytkowników. Active Directory gra rolę węzła integrującego ze sobą systemy i pozwalającego na konsolidację zarządzania nimi. W niniejszej książce zawarliśmy doświadczenia nabyte przy implementacji AD:

- Planowanie instalacji AD w terminie i w ramach zaplanowanego budżetu.
- Interakcja AD z innymi usługami sieciowymi: DNS, DHCP, RIS, RRAS i WINS.
- Korzystanie z obiektów zasad grup, praw użytkownika, FSMO i mechanizmów delegowania kontroli.
- Unikanie pułapek w strategiach migracji korzystających z narzędzi migracji Active Directory.
- Administracyjne i polityczne aspekty migracji do AD

W książce Projektowanie struktur Active Directory ponadto znajdziemy:

- Przejrzysty opis AD.
- Wyjaśnienie, dlaczego udane wdrożenie Active Directory wymaga starannego zaplanowania.
- Kilka przykładów pomyślnych implementacji AD.
- Sposoby tworzenia solidnych podstaw dla planowania i implementacji Active Directory.

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

Spis treści

Rozdział 4.

Planowanie Active Directory

W poprzednich rozdziałach przedstawiliśmy, czym jest usługa Active Directory, czym różni się od podobnych produktów i jak jest zorganizowana. Niniejszy rozdział zajmuje się różnymi zagadnieniami, które musimy rozważyć podczas planowania i implementowania AD w organizacji.

Najważniejszą sprawą dotyczącą tych zagadnień, jest to, iż większość z nich jest jedynie w niewielkim stopniu związana ze stroną techniczną. Problemy wynikają z uwarunkowań politycznych, organizacyjnych i komunikacyjnych, które, jeśli nie zostaną prawidłowo zrozumiane i potraktowane, mogą doprowadzić do drastycznych rozbieżności pomiędzy projektem AD a faktycznym środowiskiem pracy.

Możemy pogrupować problemy na różne sposoby, jednak dla naszych celów najwygodniejszy będzie następujący podział:

- **Zagadnienia migracji** — problemy związane z implementacją, które mogą mieć wpływ na strategie *WINS*, *DHCP*, *OU*, użytkowników i grup.
- **Zagadnienia administracyjne** — problemy eksploatacyjne, które mogą wpływać na struktury *OU*, *GPO*, *użytkowników* i *grup*.
- **Zagadnienia bezpieczeństwa** — zagadnienia dostępu i ochrony danych, które mogą oddziaływać na struktury *OU*, *grup* i *GPO*.
- **Zagadnienia instalacji** — problemy organizacyjne i techniczne, które mogą wpłynąć na plan migracji i procedury instalowania serwerów i stacji roboczych.
- **Zagadnienia organizacyjne** — zasady prawne i związane z komunikacją, które mogą oddziaływać na plany wdrażania, projekt zabezpieczeń, projekt dostępu i zasady zarządzania.

Wszelkie porady zawarte w tym rozdziale sprowadzają się do następującego stwierdzenia: należy poznać środowisko przed rozpoczęciem projektowania. Nie wystarczy zrozumienie zagadnień związanych z rozmieszczeniem komputerów; musimy wiedzieć też, jak sieć jest administrowana, jak użytkownicy wykonują swoje zadania i jak należałoby poprawić sieć, by lepiej służyła użytkownikom. Dopiero wtedy możemy zacząć zastanawiać się nad projektem.

Zagadnienia migracji

Na początku procesu planowania AD powinniśmy zatrzymać się i dobrze i uważnie przyjrzeć się istniejącemu środowisku. Czy na pewno rozumiemy, co w nim się dzieje? Czy wiemy, jakimi komputerami dysponujemy? Ile zwykle przychodzi zgłoszeń blokady konta? Jak często usługa WINS nie potrafi poprawnie rozwiązać nazwy? Ile grup posiadamy i jak są one używane? Czy musimy zachować wszystkie istniejące domeny, czy też powinniśmy część z nich scalić, aby uprościć zarządzanie? Na jakich zasadach ustalana jest przynależność do grup?

Lista pytań, jakie możemy zadać, jest niemal nieograniczona. Każda odpowiedź jest fragmentem zbioru danych, który pozwoli zdecydować o sposobie migracji do Active Directory. Mówiąc w skrócie, decyzja ta obejmuje następujące zagadnienia:

- Jak dużą część nakładów pracy administracyjnej chcemy przenieść do nowego środowiska?
- W jakim stopniu istniejąca architektura zaspokaja potrzeby firmy?
- Jak wiele musimy zmienić, by wykorzystać nową funkcjonalność Windows 2000?
- Czy łatwiej będzie zreorganizować istniejące środowisko, czy też zbudować nowe od podstaw?

Aby móc odpowiedzieć na te pytania, musimy znać dostępne opcje. Wobec tego skoncentrujemy się na konsekwencjach każdej z nich, wymienionych poniżej:

- Modernizacja czy migracja równoległa — wybór pomiędzy modernizacją istniejącego środowiska a zbudowaniem nowego i przejściem do niego.
- Tryb mieszany czy macierzysty — wybór pomiędzy szybkim a stopniowym przeniesieniem całości do środowiska zabezpieczeń Windows 2000.
- Modernizacja serwera, odtworzenie serwera czy przeniesienie do nowej domeny — wybór pomiędzy modernizacją serwera do Windows 2000, stworzeniem od zera lub przeniesieniem bez zmian do nowej domeny Windows 2000.
- Modernizacja, reinstalacja czy przeniesienie klienta do domeny — wybór pomiędzy modernizacją klientów do Windows 2000, zbudowaniem systemów od zera lub przeniesieniem w obecnej postaci do nowej domeny Windows 2000.
- Utworzenie czy migracja użytkowników i grup — wybór pomiędzy założeniem wszystkich kont użytkowników i grup na nowo a przeniesieniem istniejących użytkowników i grup za pomocą odpowiedniego narzędzia.

Gdy zrozumiemy konsekwencje każdego wyboru, wówczas możemy podjąć rozsądne decyzje o tym, jak, co z naszych zasobów i kiedy migrować do Windows 2000.

Modernizacja domeny do Windows 2000

Jedną z pierwszych decyzji do podjęcia jest wybór, czy zmodernizować bieżącą strukturę domen czy też zbudować równoległą Active Directory i przenieść do niej użytkowników i zasoby. Ten podrozdział omawia za i przeciw modernizacji; następny przedstawi proces migracji równoległej.

Podczas migracji z modernizacją należy kolejno:

1. Wybrać po jednym BDC z każdej domeny głównej i odłączyć od sieci. To będzie nasz „zapasowy" serwer chroniący bazę danych na wypadek, gdyby wydarzyło się coś bardzo złego.
2. Zmodernizować PCD domen głównych.
3. Zmodernizować serwery infrastruktury (DHCP, WINS i DNS) domen głównych.
4. Zmodernizować BDC w domenach głównych.
5. Zmodernizować PDC w domenach zasobów (jeśli istnieją).
6. Zmodernizować BDC w domenach zasobów.
7. Zmodernizować serwery członkowskie we wszystkich domenach.

Więcej informacji o szczegółowej procedurze migracji zawiera rozdział 8., „Planowanie migracji i dostępne narzędzia".

Postępując w ten sposób, zachowamy bazy danych kont, grupy, ustawienia zabezpieczeń, ustawienia systemów plików i strukturę domen. Zmniejsza to ryzyko przypadkowego przeoczenia ustawień użytkowników, co uniemożliwiłoby im wykonywanie swoich zadań. Ponadto zachowamy stare standardy nazewnicze i ustawień IP; serwery będą dalej funkcjonować pod oryginalnymi nazwami i adresami, co wyeliminuje potrzebę rekonfiguracji klienckich stacji roboczych, aplikacji i usług. Ogólnie mówiąc, ta metoda zdecydowanie ogranicza nakłady pracy potrzebne do skonfigurowania nowej Active Directory.

Ale czy na pewno? Tak, zachowaliśmy wszystkie stare konta. Co więcej, zachowaliśmy wszystkie stare identyfikatory *SID*, co oznacza, że nadal posiadamy uprzednie prawa dostępu, lecz odziedziczyliśmy też wszystkie pomyłki i błędy popełnione w starych domenach. Teraz, zamiast móc poprawnie zbudować nowe środowisko, musimy skontrolować i ewentualnie zmienić stare ustawienia.

Co ważniejsze, mamy niemal pewność, iż zachowane środowisko nie skorzysta z nowych możliwości organizacyjnych i zabezpieczeń systemu Windows 2000. Musimy teraz planować, jak zmienić posiadany system w coś, co będzie korzystać z nowych możliwości. W niektórych przypadkach jest to niemal niemożliwe.

Dodatkowo migracja przez modernizację bardzo utrudnia usprawnienie usług infrastruktury. Aby zyskać organizacyjnie na modernizacji, powinniśmy pozostawić dla większości usług (WINS, DHCP, a ewentualnie nawet DNS) taką samą podstawową konfigurację, jakiej używaliśmy dotychczas. Oznacza to, że w celu poprawy konfiguracji będziemy musieli zaplanować dodatkowe kroki i brać pod uwagę dodatkowe ryzyko. Proszę porównać to ze scenariuszem modernizacji równoległej, w którym zarządzanie tymi zadaniami i zarządzanie ryzykiem są wbudowane w sam projekt.

Pozostają też do rozważenia problemy logistyczne. Po rozpoczęciu modernizacji istniejącej infrastruktury *NT* wycofanie się może być bardzo trudne. Administratorzy muszą zostać bardzo szybko przyuczeni do wykonywania podstawowych zadań związanych z zarządzaniem użytkownikami. Serwery muszą zostać zmodernizowane, aby spełniały

nowe wymagania sprzętowe. Jeżeli dział informatyczny jest scentralizowany, a sieć rozproszona, wówczas ktoś będzie musiał wybrać się do każdej lokalizacji, aby zmodernizować lokalne serwery.

W każdym scenariuszu modernizacji przez zastąpienie czeka nas pewien okres eksploatacji środowiska mieszanego Windows 2000/NT. Może to spowodować bardzo złożone interakcje, zwłaszcza, jeśli dysponujemy większą liczbą domen głównych zawierających konta użytkowników. Dodatkowo, pracownicy pomocy technicznej pierwszego i drugiego poziomu muszą rozumieć i śledzić stan środowiska, które może zmieniać się codziennie. Pracownicy ci potrzebują aktualnych informacji dotyczących przenoszonych kont, zmian w zabezpieczeniach i wszelkich innych zmian w środowisku mających wpływ na społeczność użytkowników.

Musimy też pomyśleć o tym, jakich narzędzi używać do obsługi sieci. Jeśli chcemy zmienić zestawy narzędzi (na przykład zastosować nowe narzędzia kopii zapasowych lub nowy pakiet zarządzania środkami przedsiębiorstwa), jak mamy dokonać zmiany? Czy zostawimy stary pakiet w spokoju i zainstalujemy nowy na przeniesionych serwerach? Czy najpierw zainstalujemy nowy pakiet w starym środowisku (o ile w ogóle będzie działać), a następnie dokonamy modernizacji do Windows 2000?

Rozważając te wszystkie pytania, musimy wziąć pod uwagę następujące korzyści, jakie daje modernizacja środowiska:

- Zachowana zostaje baza danych kont, łącznie z identyfikatorami SID. Oznacza to, że nie musimy odtwarzać kont użytkowników, grup i komputerów należących do domeny.
- Zachowany zostaje system plików na wszystkich serwerach. Dzięki temu nie musimy ponownie ustawiać zabezpieczeń dla partycji *NTFS* i udziałów.
- Zachowane zostają istniejące konwencje nazewnicze i adresów IP. Oznacza to, że użytkownicy nie muszą ponownie przypisywać drukarek i udziałów. Co więcej, administrator nie ma potrzeby resetowania adresów podstawowych usług infrastruktury, takich jak *DDNS* i *WINS*.
- Zredukowany jest zakres interakcji zabezpieczeń pomiędzy platformami. Dzięki temu maleje ryzyko wystąpienia poważnych błędów zabezpieczeń podczas migracji, ponieważ większość lub całość informacji o zabezpieczeniach jest przechowywana w środowisku Windows 2000.

Musimy też wziąć pod uwagę ujemne strony opcji modernizacji:

- Błędy popełnione w pierwotnym środowisku pozostają. Oznacza to, że chcąc „posprzątać" środowisko, będziemy musieli radzić sobie z błędami już istniejącymi, zamiast zaczynać od zera.
- Pojawiają się różnice w ustawieniach zabezpieczeń serwerów. Ustawienia dla zmodernizowanych serwerów i stacji roboczych są inne niż dla systemów zainstalowanych od podstaw. Przede wszystkim, zmodernizowane komputery obowiązuje kilka ograniczeń dotyczących zabezpieczania plików systemowych i ustawień Rejestru, co może doprowadzić do niezgodności pomiędzy tym, co wydaje się nam, że instalujemy, a tym, co w rzeczywistości otrzymamy. Problem ten może zostać rozwiązany za pomocą narzędzia *Security Configuration Manager*.

- Występują logistyczne, techniczne i proceduralne problemy, gdy trzeba scentralizować w jeden system kilka katalogów o własnych zabezpieczeniach (np. domeny *NT*, *Novella* i *Kerberosa* w systemie UNIX). W migracji poprzez modernizację, gdy chcemy skoncentrować zabezpieczenia, musimy najpierw przeanalizować i udokumentować zmodernizowane środowisko, a następnie zdefiniować na potrzeby konwersji właściwe relacje. Może to okazać się bardziej czasochłonne niż proste zdefiniowanie stanu idealnego i wykorzystanie posiadanych danych do przejścia do niego.
- Pojawia się konieczność równoległego korzystania z dwóch narzędzi. Oznacza to, że musimy najpierw zastosować w istniejącym środowisku nowe narzędzia. W przeciwnym razie zwiększamy ryzyko błędów w administracji podczas etapu migracji.

Gdy zdecydujemy się na modernizację, musimy dodatkowo odpowiedzieć na następujące pytania:

- Która domena (jeśli mamy więcej niż jedną) będzie modernizowana?
- Jak, kiedy i kto będzie modernizować kontrolery domen i serwery znajdujące się w terenie?
- Jak, kiedy i kto będzie łączyć i optymalizować domeny?
- Jak, kto i kiedy będzie modernizować kolejki drukowania, serwery intranetowe, serwery aplikacji, zabezpieczenia plików i grupy?
- Jakie kryteria zostaną wzięte pod uwagę przy analizie istniejących tożsamości zabezpieczeń (kont użytkowników, grup lokalnych, grup globalnych itp.) do ustalenia, które tożsamości zachować, a które zmienić?
- Jak będzie wyglądać komunikacja z działem obsługi technicznej, pozwalająca zapewnić społeczności użytkowników pomoc podczas migracji?

Nasze środowisko skutecznie migrować przez modernizację, jeśli:

- Posiadamy niewielką liczbę (zwykle poniżej 15) rozrzuconych geograficznie lokalizacji serwerów i uwierzytelniania.
- Istniejące środowisko jest dobrze zorganizowane, udokumentowane i zawiera małą liczbę innych katalogów.
- Właśnie przeszliśmy cykl gruntownej modernizacji sprzętu.
- Dobrze znamy posiadane narzędzia służące do odzyskiwania środowiska po awarii i możemy zapewnić, że będą one działać poprawnie w mieszanym środowisku.

Jeśli nakłady pracy związane z problemami są większe niż korzyści płynące z migracji przez modernizację (zastąpienie), wówczas warto rozważyć inne opcje. Następny punkt zajmuje się drugą z dwóch podstawowych opcji — migracją równoległą.

Migracja równoległa

Niektóre organizacje po przeanalizowaniu ścieżki migracji przez modernizację stwierdzają, że jest ona pełna problemów. Może logistyka jest zbyt trudna. Może stosowanych jest kilka systemów katalogowych, które trzeba połączyć w jeden. Może po prostu lepiej jest uniknąć prac porządkowych związanych z modernizacją starego środowiska i rozpocząć od zera.

Na potrzeby niniejszej książki można przyjąć, że migracja równoległa to taka, w której:

1. Tworzymy nową domenę, drzewo i las Windows 2000.
2. Decydujemy, jak ma wyglądać nowe środowisko.
3. Decydujemy, które informacje należy przenieść ze starego środowiska do nowego.
4. Tworzymy odwzorowanie starego środowiska na nowe.
5. Przenosimy użytkowników, grupy, pliki i serwery zgodnie z odwzorowaniem.

Więcej informacji o szczegółowej procedurze migracji zawiera rozdział 8.

Inaczej mówiąc, tworzymy dziewicze środowisko, do którego migrujemy dane tak, jak nam pasuje. Taka procedura daje szereg korzyści: kontrolę nad danymi, kontrolę nad tempem migracji, zdolność do utworzenia odpowiednich standardów oraz zdolność do wyegzekwowania zgodności z tymi standardami. Wymienione zalety rozwiązują, niemal punkt po punkcie, problemy występujące w migracji przez modernizację.

Na przykład, pomoc techniczna wciąż potrzebuje dokładnych informacji o tym, którzy użytkownicy i które zasoby są zaplanowane do migracji. Jednakże w migracji równoległej rozgraniczenie jest znacznie wyraźniejsze — część z nich istnieje tylko w nowym środowisku, część nie jest przeznaczona w ogóle do przeniesienia, zaś wszystko inne posiada zaplanowane daty migracji. Interakcje mogą być o wiele prostsze; mają zdecydowanie wyraźniejsze granice.

Podobna analiza sprawdza się dla pozostałych punktów. Ponieważ w migracji równoległej dysponujemy dwoma odrębnymi środowiskami, mamy znacznie wyraźniej określone granice pomiędzy procedurami obsługi technicznej, wersjami narzędzi i usługami infrastruktury. Wszystko, co może stać się niejasne w migracji przez modernizację, w migracji równoległej jest bardziej zrozumiałe.

Musimy zarazem bardziej rozważnie decydować, kiedy, jak i dlaczego mamy zmieniać skrypty logowania, odwzorowania drukarek i dokonywać innych podobnych czynności. Modernizacja równoległa stanowi klasyczny proces instalowania infrastruktury, w którym użytkownicy przenoszą się ze starszego środowiska do nowego, czasem diametralnie odmiennego. Zwiększa to ilość zapytań i komentarzy ze strony użytkowników, co może zwiększyć nakłady czasu poświęcone na zarządzanie projektem w ramach procesu instalacji.

Musimy też zdać sobie sprawę z faktu, że migracja równoległa „od podstaw" jest niemal idealnym rozwiązaniem dla scalenia kilku katalogów związanych z zabezpieczeniami w jeden. Na potrzeby analizy weźmy pod uwagę mieszane środowisko systemów Novell i NT. Jeśli bezpośrednio zmodernizujemy Windows NT do Windows 2000, będziemy musieli:

1. Określić idealny stan dla Windows 2000.
2. Ustalić stan obecny.
3. Określić odwzorowanie Windows NT na stan idealny.
4. Określić odwzorowanie Novella na stan idealny.
5. Zmodyfikować Windows NT tak, by zbliżyć się do stanu idealnego.
6. Zaktualizować Windows NT do Windows 2000.
7. Przenieść dane zabezpieczeń z Novella do Windows 2000.

Jeśli stosujemy migrację równoległą od zera, zamiast tego będziemy musieli:

1. Określić stan idealny.
2. Ustalić odwzorowanie Windows NT na stan idealny.
3. Określić odwzorowanie Novella na stan idealny.
4. Migrować odpowiednie dane zabezpieczeń z Novella lub Windows NT, zależnie od tego, które będą lepsze, do środowiska Windows 2000.

Drugim faktem, jaki musimy wziąć pod uwagę, jest ten, iż jedną z podstawowych korzyści migracji przez modernizację (zachowanie SID) możemy uzyskać za pomocą niemal wszystkich istniejących narzędzi migracji. Każda domena działająca w trybie macierzystym posiada dla każdego obiektu atrybut `SIDhistory`, który pozwala nowo utworzonym obiektom posiadać ten sam SID co obiekt, z którego została dokonana migracja.

Gdy zastanawiamy się nad wyborem migracji równoległej, musimy pamiętać o następujących korzyściach z niej płynących:

- Tworzymy wyraźną granicę pomiędzy starym i nowym środowiskiem. Powoduje to mniejszą liczbę interakcji w migrowanym środowisku, prowadząc do aktualizacji bardziej przejrzystej i łatwiejszej do kontrolowania.
- Zachowujemy (stosując odpowiednie narzędzia) SID przenoszonego obiektu. Oznacza to, że możemy migrować dane i ustawienia zabezpieczeń stosunkowo bezkarnie, odkładając porządki na późniejszy termin.
- Mamy bardzo szczegółową kontrolę nad tym, kiedy przenosić zasoby i użytkowników do nowego środowiska. Jest to szczególnie ważne w dużych organizacjach lub w organizacjach mających szczególne wymagania prawne i związane z kontrolami.
- Otrzymujemy dziewicze środowisko, do którego możemy przenieść kilka istniejących dostawców zabezpieczeń, wybierając ten system, który najlepiej spełnia nasze potrzeby.

Musimy też wziąć pod uwagę podstawową wadę modernizacji równoległej, którą jest zapotrzebowanie na znaczące ilości nowego sprzętu. Jeśli modernizacja do Windows 2000 zbiega się ze standardowym okresem odświeżania zasobów sprzętowych, wówczas jest to mniejszym problemem. Jeśli jednak zamierzamy zakupić nowe serwery poza harmonogramem modernizacji sprzętu w celu obsługi Active Directory i innych usług Windows 2000, wówczas powinniśmy dokonać poważnej analizy zysku i kosztów.

Proszę też zdać sobie sprawę, że po przyjęciu opcji modernizacji równoległej musimy odpowiedzieć na poniższe pytania:

- Jak będziemy podczas migracji monitorować i zarządzać interakcjami pomiędzy istniejącym środowiskiem (środowiskami) i domeną Windows 2000? Firma przez jakiś czas będzie korzystać z dwóch systemów, co bez właściwego planowania może wystawić ją na niedopuszczalne ryzyko.
- Jak chcemy odwzorować dane zabezpieczeń z wszystkich istniejących środowisk?
- Jak będziemy zarządzać skryptami logowania, drukarkami, udostępnionymi plikami i wspólnymi zasobami, które mogą ulec zmianie podczas migracji i mogą (jak w przypadku skryptów logowania) wymagać kilku wersji?

Nasze środowisko jest dobrym kandydatem do modernizacji równoległej, jeśli:

- Zbliża się lub właśnie trwa cykl odświeżania zasobów sprzętowych.
- Stosujemy kilka środowisk udostępniających zabezpieczenia, które chcemy skonsolidować w jedną domenę.
- Z powodów technicznych nie możemy bezpośrednio zmodernizować domeny.
- Dysponujemy dużą liczbą lokalizacji fizycznych i potrzebujemy dodatkowej kontroli nad migracją, jaką może nam dać dziewicze środowisko.

Jeśli możemy sobie na nią pozwolić, migracja równoległa daje wiele korzyści. Proszę jednak zdać sobie sprawę, że przejście z migracji przez modernizację na migrację równoległą może być trudne i wyjątkowo kosztowne. Unikniemy tej pułapki, rozważnie analizując dostępne opcje **przed** rozpoczęciem projektu i trzymając się podjętej decyzji przez cały okres przejściowy.

Domeny w trybie mieszanym i macierzystym

Jedną z najważniejszych kwestii, jakie pojawiają się podczas projektowania Active Directory, a co za tym idzie, która stanowi największe źródło nieporozumień, jest różnica pomiędzy domenami funkcjonującymi w *trybie mieszanym* i *macierzystym*. Ludzie pytają: „Czy powinniśmy przejść na tryb macierzysty?”, traktując to jak swojego rodzaju mistyczną podróż, która, gdy ją już podejmą, zaprowadzi ich do ziemi obiecanej.

Rzeczywiste pytanie, jakie należy zadać w związku z przejściem w tryb macierzysty, nie brzmi „czy”, lecz „kiedy”. Każdy prędzej czy później przechodzi w tryb macierzysty; musimy raczej podjąć decyzję, na jakim etapie migracji zaplanować przejście, a nie czy przechodzić w ogóle.

Wyjaśnijmy najpierw nieporozumienia. Przejście w tryb macierzysty:

- Nie aktywuje obiektów zasad grup.
- Nie zapewnia lepszej replikacji.
- Nie optymalizuje rozmiarów bazy danych AD.
- Nie uniemożliwia logowania ze starszych wersji klientów.
- Nie uniemożliwia stosowania starszych aplikacji.
- Nie zmienia sposobu, w jaki AD współpracuje z innymi systemami Kerberosa.

Tryb macierzysty w zamian za to:

- Aktywuje część obiektów w katalogu.
- Pozwala na stosowanie grup uniwersalnych.
- Pozwala AD na ignorowanie baz danych SAM, omijając dzięki temu ich ograniczenia.

Jeśli planujemy migrację przez modernizację, powinniśmy rozważnie zaplanować przejście w tryb macierzysty. Możemy przełączyć domenę w ten tryb dopiero po zmodernizowaniu do Windows 2000 wszystkich kontrolerów domeny (PDC i wszystkich BDC). W przeciwnym razie możemy mieć do czynienia z klientami nie mogącymi się w ogóle zalogować do domeny, ponieważ kontroler domeny usiłujący dokonać uwierzytelnienia nie będzie mógł już otrzymywać aktualizacji z aktywnych baz danych zabezpieczeń.

Jeśli planujemy migrację równoległą, wówczas powinniśmy przejść w tryb macierzysty najszybciej, jak tylko się da. Pozostawienie katalogu w trybie mieszanym spowoduje, iż większość istniejących narzędzi do migracji (jeśli nawet nie wszystkie) nie będzie w stanie migrować użytkowników do naszej nowej, ślicznej struktury Active Directory.

Migracja serwerów

Przy planowaniu strategii migracji serwerów możemy je podzielić na cztery kategorie: przeznaczone do zastąpienia, do konsolidacji, do modernizacji i do przeniesienia bez zmian.

Każda z kategorii jest przy projektowaniu i planowaniu traktowana nieco inaczej.

Powinniśmy zasadniczo zastąpić serwery, których nie da się zmodernizować do Windows 2000. Może są zbyt stare i nie damy rady rozbudować ich do poziomu minimalnych wymogów sprzętowych, a może skończyła się na nie gwarancja, więc nie chcemy eksploatować systemu bez zabezpieczenia. Niezależnie od powodów, gdy zastępujemy serwer, musimy:

1. Mieć całkowitą pewność, iż znamy usługi świadczone przez dany serwer.
2. Zapewnić dostępność tych usług podczas migracji.
3. Upewnić się, czy usługi działają poprawnie w nowym miejscu.

4. Zastąpić serwer, przetestować i włączyć nowy serwer do środowiska produkcyjnego.
5. Zlikwidować stary serwer.

Powinniśmy konsolidować serwery wykorzystywane w zbyt małym stopniu oraz takie, których koszty utrzymania przekraczają pewną ustaloną wartość. Są to zwykle przestarzałe serwery, które i tak musielibyśmy zmodernizować lub zastąpić, lecz stopień ich wykorzystania jest na tyle niski, że nie usprawiedliwia zakupu nowego. Przygotowując się do konsolidacji kilku serwerów musimy:

1. Zidentyfikować poziom wykorzystania każdego serwera.
2. Upewnić się, czy serwer docelowy jest w stanie obsłużyć sumę obciążenia tych serwerów.
3. Upewnić się, czy wzorce dostępu do różnych konsolidowanych usług nie wchodzą w konflikty. Na przykład, często trudno jest stabilnie skonsolidować usługi pocztowe i bazy danych na pojedynczej platformie *Wintel*.
4. Zaplanować konsolidację na okres nie będący krytyczny dla biznesu.
5. Dokładnie przetestować konsolidację. Połączenie różnych usług w jednym komputerze może wprowadzić nietypowe wzorce wykorzystania powodujące niestabilność.
6. Po dokonaniu konsolidacji monitorować serwer przez okres przynajmniej jednego kwartału.
7. Zlikwidować stary serwer.

Ogólnie mówiąc, powinniśmy modernizować serwery na gwarancji, łatwe w rozbudowie do wymaganego poziomu, wykazujące rozsądne poziomy wykorzystania i nie świadczące usług wymagających starszego środowiska. Przygotowując się do modernizacji serwera, musimy:

1. Zweryfikować, czy wszystkie usługi świadczone przez serwer (aplikacje, bazy danych i tak dalej) są kompatybilne z Windows 2000.
2. Przygotować i przetestować aktualizacje usług niezgodnych z Windows 2000.
3. Zaplanować modernizację na normalne godziny serwisowania.
4. Zmodernizować sprzęt w serwerze, system operacyjny i usługi do Windows 2000 i zgodnych z nim wersji oprogramowania.

Proszę pamiętać, że złożoność migracji przez modernizację nie wynika z systemu operacyjnego, lecz z usług świadczonych przez serwer. Zwłaszcza planowanie przeniesienia baz danych i oprogramowania *ERP* (planowanie zasobów przedsiębiorstwa) może zająć miesiące, a po przeniesieniu możemy poświęcić kolejne miesiące na monitorowanie serwera, by upewnić się, że wszystko poszło dobrze.

Przenoszone są przede wszystkim serwery nie uczestniczące w zabezpieczeniach domeny (jako PDC lub BDC) i obsługujące aplikacje krytyczne dla firmy, a nie posiadające wersji zgodnej z Windows 2000. Wysiłek związany z wycofywaniem krytycznego dla firmy oprogramowania typu *legacy* (przestarzałego) może być większy niż włożony w cały projekt Windows 2000. Przygotowując się do przeniesienia serwera, musimy:

1. Upewnić się, czy stare oprogramowanie nie posiada żadnych zależności od innych serwerów, które modernizujemy, konsolidujemy lub zastępujemy.
2. Zaplanować modernizację na standardowe godziny przeznaczone na serwis.
3. Usunąć serwer ze starej domeny.
4. Przyłączyć serwer do nowej domeny.
5. Sprawdzić, czy ustawienia zabezpieczeń serwera są prawidłowe dla funkcji serwera.
6. Monitorować serwer i stare oprogramowanie przez przynajmniej kwartał od chwili migracji.
7. Przenieść zadania obsługi i monitorowania serwera na personel obsługi technicznej po uznaniu migracji za zakończoną powodzeniem.

Faktyczny harmonogram i kolejność migracji serwerów zależy od rozmiarów organizacji, składu i umiejętności zespołu związanego z projektem oraz od naszej zdolności do szybkiego i dokładnego oszacowania środowiska. Największe ryzyko przekroczenia harmonogramu pochodzi od aplikacji krytycznych dla funkcjonowania przedsiębiorstwa i przestarzałych; ryzyko to możemy zmniejszyć tylko przez utworzenie i wdrożenie planu szczegółowych i stosunkowo czasochłonnych testów.

Migracja klientów

Migrowanie serwerów jest łatwe, ponieważ zasadniczo dobrze wiemy, gdzie się znajdują, co się w nich mieści i jak firma je wykorzystuje. Migracja komputerów klienckich to całkiem inna sprawa.

Logistyka znajdowania, identyfikacji, szacowania, rejestrowania, sortowania, planowania harmonogramu, a na koniec faktycznej migracji komputerów klienckich może bez trudności zająć większość czasu poświęconego na projekt Windows 2000. Zagadnienia te nie mieszczą się w zakresie niniejszej książki.

Nas interesuje ustalenie, jak postąpić ze wszystkimi klientami, gdy już ustalimy, gdzie są, czym są, kto ich używa i do czego. Ogólnie mówiąc, możemy klienty podzielić na trzy kategorie:

- przeznaczone do zastąpienia,
- przeznaczone do modernizacji,
- pozostawione bez zmian.

Klienty przeznaczone do zastąpienia to zwykle te, które są zbyt stare na modernizację do poziomu minimalnych wymogów sprzętowych lub przeznaczone do rychłego złomowania z uwagi na politykę księgową (odświeżenie dzierżawy lub budżetowanie kapitałowe). W przypadku takich komputerów musimy rozważyć logistykę identyfikowania, przenoszenia i wycofywania starego sprzętu, jak również wpływ, jaki ma na użytkownika przydział nowej stacji roboczej. Możemy zapanować nad niebezpieczeństwami instalacji przez wstępne przygotowanie nowego sprzętu, skonfigurowanie i przetestowanie przed przydzieleniem go użytkownikowi.

Klienty przeznaczone do modernizacji spełniają minimalne wymagania sprzętowe (czasami po zakupie dodatkowego sprzętu), lub z powodów księgowych, nie są zaplanowane do wymiany w ciągu roku. W przypadku takich klientów musimy szczególnie rozważnie zaplanować czas modernizacji, metodę instalacji i metody przywracania klienta. Jednym z największych wyzwań w całym projekcie jest w istocie przeniesienie wszystkich ustawień indywidualnych i danych klientów ze starego systemu do nowego.

Klienty pozostawione bez zmian to zwykle te, które obsługują przestarzałe aplikacje absolutnie niezbędne użytkownikowi. Jeśli nie da się znaleźć innego rozwiązania, wówczas użytkownik musi otrzymać nowy PC. Czasami, gdy grupa użytkowników potrzebuje aplikacji tylko od czasu do czasu i to nie równocześnie, możemy pozostawić pojedynczą starą stację roboczą dla grupy użytkowników, co uwolni nas od odpowiedzialności za utrzymanie kilku starych, niezgodnych ze specyfikacjami komputerów.

Migracja użytkowników i grup

Z punktu widzenia planowania i projektowania jednym z najbardziej złożonych zadań, jakie musimy przemyśleć, jest to, jak, kiedy i dlaczego powinniśmy migrować konta użytkowników i grup. Ten problem może bez trudu sparaliżować proces analizy. Istnieją dosłownie setki czynników, jakie powinniśmy wziąć pod uwagę, oraz chyba tysiące wariacji na podstawowe tematy.

Zamiast omawiać godzinami każdą możliwość i odmianę, proszę na chwilę zatrzymać się i przemyśleć, co trzeba tu zaplanować:

- Jeśli modernizujemy domenę, musimy ustalić, jak zmodyfikować istniejące grupy, by pasowały do obecnego projektu.
- Jeśli dokonujemy migracji równoległej, musimy ustalić odwzorowania pomiędzy starą i nową strukturą grup.

W obu przypadkach niezbędna będzie mapa zmian. Ten dokument mówi, co usunąć, co skonsolidować z czym, co utworzyć, a co po prostu przenieść. Sam proces migracji informacji z wykorzystaniem mapy zmian powinien odbyć się przed rozpoczęciem lub po zakończeniu migracji. Dokonanie tej pracy podczas migracji może spowodować nieprzewidywalne zmiany w dostępie pracowników do zasobów, więc nie jest zalecane.

Podczas tworzenia mapy zmian proszę zwrócić szczególną uwagę na:

- Konta usług i konta administracyjne używane w roli kont usług. W Windows 2000 mogą one wymagać innych uprawnień niż te, do których jesteśmy przyzwyczajeni.
- Konta z uprawnieniami do logowania jedynie do określonych komputerów lub w określonych porach dnia. Jeśli zmieniamy komputer kliencki lub parametry robocze konta, wówczas nieumyślnie zmieniamy zasady zabezpieczeń.
- Grupy mające dostęp do więcej niż jednego zasobu (poprzez uprawnienia do plików lub udziałów). Grupy takie mogą dysponować większym zakresem uprawnień, niż nam się wydaje; należyta staranność w tym miejscu zaoszczędzi w przyszłości mnóstwa telefonów do pomocy technicznej.

Jak już mówiliśmy, zagadnienia związane z migracją mają wpływ na logistykę i na plany zmian. Proszę nie ignorować podczas planowania Active Directory stwarzanych przez nie trudności i możliwości.

Zagadnienia administracyjne

Zza horyzontu migracji wyłania się mityczny stan zwany stanem produkcyjnym. Serwery szumią sobie spokojnie, a użytkownicy pracują radośnie w ochronnej klatce stworzonej przez wydział informatyczny. Zabezpieczenia chronią skutecznie dane przed niepowołanym dostępem. Użytkownicy nigdy nie blokują swoich kont ani nie zapominają haseł.

Gdy to złudzenie już się rozwieje, czeka nas brutalna rzeczywistość — ktoś musi zarządzać zaprojektowaną przez nas Active Directory. Najprawdopodobniej będziemy to my. Wobec tego Czytelnik musi dokładnie wiedzieć, co oznacza zarządzanie siecią i brać to pod uwagę w swoim projekcie.

Aby jak najwięcej wynieść z lektury tego podrozdziału, proszę rozważyć:

- Różnice pomiędzy NT i Windows 2000 — zmiany w systemie operacyjnym, które zmieniają sposób myślenia o administrowaniu.
- Role *jednostek organizacyjnych* (*OU*) — jak ułatwić zadania administracyjne za pomocą OU.
- Jak i kiedy delegować kontrolę — jak wykorzystać możliwość oddelegowania kontroli nad określonymi obiektami katalogowymi w celu uproszczenia administracji.
- Bezpieczeństwo (kto i kiedy) — porównanie potrzeb dostępu z ryzykiem związanym z przyznaniem tego dostępu.
- Zasady grup — ile i do czego je stosować.

Usiłując zrozumieć te zagadnienia, możemy zaprojektować katalog, który nie tylko ładnie wygląda na papierze, lecz będzie można również go obsługiwać. Te dwa warunki nie muszą wykluczać się wzajemnie.

Różnice administracyjne pomiędzy Windows NT i 2000

Na pierwszy rzut oka ten punkt może wydać się bezużyteczny. W końcu wiemy już, że Windows 2000 różni się od Windows NT. Jakby nie było, to jeden z głównych powodów, dla których zdecydowaliśmy się na ten projekt...

Niech i tak będzie, lecz przyda się poświęcić minutę na wyraźne określenie różnic pomiędzy Windows 2000 i Windows NT z punktu widzenia administratora. Dobra znajomość tych różnic pozwoli podjąć rozsądne decyzje dotyczące tego, jak wykorzystać te różnice w przyszłości.

Pierwsza i najważniejsza różnica, jaką musimy wziąć pod uwagę, jest najmniej oczywista. W Windows NT nie możemy zmusić komputera do korzystania z lokalnego kontrolera domeny w środowisku IP. W Windows 2000 komputery wykorzystują dane lokacji, aby znaleźć najbliższy dostępny kontroler w celu zalogowania się.

Dlaczego jest to ważne?

- W bazie danych kont typu *multimaster* (jak w Windows 2000) zmiany nie są propagowane automatycznie. Oznacza to, że musimy albo dokonać zmian w bazie danych położonej najbliżej użytkownika, albo kazać użytkownikom zaczekać na zmiany w ustawieniach konta.
- Jeśli uszkodzenie bazy danych powoduje problemy z logowaniem, wówczas w celu zdiagnozowania problemu musimy zalogować się do systemu sprawiającego kłopoty.
- Musimy uważać na *usługę replikacji plików* (*FRS — File Replication Service*), ponieważ rejestruje ona błędy, gdy nie może prawidłowo zsynchronizować się z kontrolerem domeny. Może to pomóc w diagnozowaniu problemów związanych z zasadami grup i błędami w skryptach logowania, które naprawiliśmy (jak nam się wydawało).

Proszę zwrócić uwagę, że replikacja pomiędzy lokacjami jest procesem zaplanowanym według harmonogramu. Dla większości procedur (jak np. zmiana przynależności do grup) harmonogram decyduje, kiedy zmiany dokonane w danej lokacji mają zostać rozpropagowane do innych dołączonych lokacji. Jeśli w naszej sieci istnieją trasy replikacji z wieloma przeskokami, wówczas replikacja zmian w całym środowisku może zająć tyle czasu, ile potrwa replikacja przez najdłuższą trasę.

Proszę też zdać sobie sprawę, że przynależność do grupy jest propagowana jako pojedynczy blok danych. Oznacza to, że gdy jeden administrator zmieni członkostwo w grupie *foo* z komputera w Wielkiej Brytanii, a drugi dokona zmian w tej samej grupie z komputera w USA, wówczas jedna z informacji zostanie nadpisana.

Weźmy pod uwagę wpływ modelu multimaster na odzyskiwanie kontrolerów domeny. Jeśli katalog nie uległ uszkodzeniu, wówczas w małych organizacjach (powiedzmy, że do 10 000 obiektów) zwykle łatwiej będzie pozwolić kontrolerowi domeny na replikację bazy danych AD zamiast ją odtwarzać. W dużej organizacji musimy bardziej uważać na procedury tworzenia i przywracania kopii zapasowych, ponieważ odebranie pełnej replikacji może zająć więcej czasu, niż możemy pozwolić.

Weźmy jeszcze pod uwagę wpływ narzędzi takich jak *Taskpad* na nasz model administrowania. Odrobina rozważnego planowania pozwoli nam wyposażyć pracowników obsługi technicznej pierwszego stopnia w zbudowane specjalnie dla nich narzędzia, zapewniające im możliwości niezbędne, a ograniczające te uprawnienia, których obsługa mieć nie powinna. Na przykład, możemy zbudować *Taskpad* dający administratorowi dostęp jedynie do zmiany haseł użytkowników, co pozwoli mu wykonywać obowiązki służbowe bez konieczności stosowania przystawki *MMC Użytkownicy i komputery usługi Active Directory*.

Co więcej, powinniśmy planować zmiany tak, jak myślimy o skryptach logowania. W tej chwili możemy tworzyć skrypty uruchamianie przy załączaniu i wyłączaniu komputerów oraz przy logowaniu i wylogowywaniu użytkownika. Po zespoleniu tego z możliwościami *Visual Basica* i *ADSI*, otrzymamy niemal nieograniczone możliwości konfiguracji.

Łatwo pogubić się we wszystkich tych zmianach. Opcje dokonywania zmian są prawie nieograniczone. Jeśli chcemy wdrożyć Windows 2000 w czasie choćby zbliżonym do czasu życia produktu, to musimy ograniczyć zakres początkowej migracji.

Z doświadczenia wynika, że najlepszym ograniczeniem zakresu zmian administracyjnych jest na początek próba odtworzenia istniejącej funkcjonalności. Proszę przenieść skrypty, zapoznać się z narzędziami administracyjnymi i uważać, by nie przekroczyć początkowych możliwości. Dopiero, gdy nauczymy się duplikować oryginalną funkcjonalność, możemy zabrać się za problemy w istniejącym środowisku. Na przykład, gdy mamy poważny problem z niemożliwością zmiany haseł użytkowników przez pomoc techniczną bez przyznania pracownikowi uprawnień administratora domeny, wówczas rozważymy naprawę tego problemu. Po skopiowaniu funkcjonalności i rozwiązaniu problemów możemy przejść do implementowania ulepszeń w zarządzaniu.

Jaką rolę grają OU?

Jednym z najnowszych wynalazków w zestawie narzędzi administracyjnych Microsoftu jest *jednostka organizacyjna* (*OU — Organizational Unit*). OU są logicznymi kontenerami na obiekty katalogowe; możemy je zagnieżdżać praktycznie w nieskończoność i wykorzystywać do reprezentowania prawie wszystkiego, co sobie wyobrazimy.

Pytanie brzmi: co mamy z nimi począć? Możemy grupować użytkowników i komputery na niemal tyle sposobów, ile jest firm i projektantów sieci. Wygląda na to, że nie istnieje jedyna słuszna odpowiedź.

I prawdę mówiąc, nie istnieje jednoznaczna odpowiedź na pytanie o najlepszą strukturę OU. Są jednakże dostępne wytyczne, z których pomocą możemy najefektywniej wykorzystać OU.

Pierwszą i najważniejszą regułą, o której musimy pamiętać przy projektowaniu OU, jest unikanie nadmiernej komplikacji schematu. Nie istnieje teoretyczny limit, jak głęboko możemy zagnieżdżać OU. Możemy zejść 10, 20 lub nawet 30 poziomów w dół, zanim zobaczymy kolejny obiekt. Jednakże w praktyce powinniśmy pilnować, by nie zejść zbyt głęboko poniżej trzeciego poziomu. Głębiej reguły sortowania obiektów w poszczególnych OU stają się bardzo złożone.

Powinniśmy też bardzo uważać na wybór OU. Ponieważ stanowi ona logiczny zbiór komputerów, grup i użytkowników, powinniśmy zadać sobie pytanie: „Jaką rolę spełnia ta jednostka organizacyjna?”. Jeśli nie potrafimy znaleźć dobrej odpowiedzi na to pytanie, wówczas najprawdopodobniej powinniśmy usunąć OU z projektu.

OU nadają się doskonale do tworzenia obszarów ustawień konfiguracji, zasad zabezpieczeń i specjalnych grup. Na przykład, niektóre firmy używają OU dla serwerów WWW, serwerów plików i serwerów aplikacji. Inne stosują OU dla komputerów wymagających

dostępu do zasobów sieciowych, lecz mających zdecydowanie inne potrzeby funkcjonalne niż pozostałe stacje robocze (jak np. PC gromadzący w czasie rzeczywistym dane ze sprzętu laboratoryjnego i publikujący te dane w sieci).

Za dobre przyzwyczajenie przy projektowaniu uznaje się unikanie tzw. „kontenerów" OU — *pustych OU*, których jedynym zadaniem jest przechowywanie innych OU. Weźmy na przykład jednostkę organizacyjną o nazwie Kraje, w której znajdą się OU USA, Francja i Japonia. OU Kraje jest typowym kontenerem. Jaką funkcję spełnia? Czy naprawdę jej potrzebujemy?

Nie znaczy to, że takie OU są bezwzględnie złe. Każdy kontener powinien przejść ten sam proces uzasadnienia jak każda inna OU. Jeśli musimy za pomocą kontenera zorganizować dużą liczbę OU, to potrzeba taka pojawi się podczas tworzenia projektu stosunkowo szybko.

OU dobre są też do wyznaczania stref kontroli w obrębie firmy. Im bardziej przedsiębiorstwo jest zdecentralizowane (z wyboru, ograniczeń prawnych lub konieczności politycznej), tym więcej musi istnieć OU do delegowania kontroli. W całkowicie zdecentralizowanej organizacji działu informatycznego może nawet okazać się potrzebnych więcej geograficznych jednostek organizacyjnych.

Czynniki, jakie musimy rozważyć przy projektowaniu struktury OU, są następujące:

- Czy struktura działu informatycznego jest scentralizowana czy zdecentralizowana? Jakie są granice administracyjne (obszary kontroli) organizacji?
- Jak wiele ról funkcjonalnych odgrywają serwery? Przykładami ról są serwery WWW, aplikacji oraz plików i drukowania.
- Jak wiele kategorii ról funkcjonalnych możemy stworzyć dla stacji roboczych? Przykłady to: komputery biurkowe, laptopy, zdalne stacje robocze i sprzęt gromadzący dane.
- Czy organizacja dysponuje stacjami roboczymi, serwerami lub użytkownikami wymagającymi wyłączenia z ogólnego schematu zabezpieczeń domeny, GPO i organizacji? Do przykładów należą: zarząd, pracownicy pomocy technicznej i administratorzy sieci.
- Czy istnieją administracyjne, finansowe lub prawne potrzeby wydzielenia części użytkowników lub komputerów? Do przykładów zaliczają się pracownicy kontraktowi, konta zablokowane i stacje robocze z ograniczeniami (miejsce na stacje robocze o wyjątkowo rygorystycznych wymogach bezpieczeństwa).
- Jak struktura OU wpłynie na wszelkie aplikacje, które w przyszłości będą korzystać z Active Directory? Na przykład, czy istnieją jakieś specjalne zależności w obrębie aktualizacji pakietu ERP, o których powinniśmy wiedzieć?

Pytania te zmuszają do bardzo dokładnego przeanalizowania, do czego zamierzamy wykorzystać poszczególne OU. Im bardziej szczegółowo odpowiemy na te pytania, z tym większym prawdopodobieństwem nasz projekt będzie dobrze dopasowany do środowiska i przyszłych potrzeb administracyjnych.

Delegowanie kontroli

Jedną z najbardziej reklamowanych możliwości Active Directory jest zdolność do szczegółowego przydziału praw administracyjnych, nawet do poszczególnych atrybutów obiektu. Jest to ogromny postęp w stosunku do epoki Windows NT, gdy przydział ograniczonych praw administracyjnych stanowił prawdziwe wyzwanie.

Odrobina planowania pozwoli przydzielić użytkownikom prawa do modyfikowania własnych danych osobistych. Możemy przyznać sekretarce prawa do zmiany danych adresowych dowolnego użytkownika w danym dziale. Możemy dać pracownikom pomocy technicznej prawo do zmiany haseł użytkowników, nie przyznając im równocześnie prawa do dodawania stacji roboczych do domeny. Każdemu możemy przydzielić prawo do czegokolwiek, absolutnie czegokolwiek!

Czy to nie jest fascynujące? Lecz na początek proszę pomyśleć, co dokładnie trzeba delegować i jak tego dokonać. Jest to jedna z tych możliwości, które wymagają bardzo dokładnej analizy, zanim zaczniemy rozdawać uprawnienia wszystkim osobom, które ich mogą potrzebować.

Pierwsze pytanie jest najtrudniejsze: Co musimy oddelegować? Warto sformułować to pytanie inaczej, by spojrzeć na problem z pewnej perspektywy:

Do jakich istotnych, osobistych, poufnych lub związanych z bezpieczeństwem danych chcemy przyznać dostęp?

To jest realne pytanie, jakie sobie musimy zadać. Gdy delegujemy komuś kontrolę nad atrybutem, wówczas dajemy tej osobie możliwość zmiany tego atrybutu. Nadajemy też bezpośrednio prawa administracyjne i prawne do dostępu i kontroli nad tymi danymi.

Musimy też zwracać uwagę na kontrolę nad zmianami w jednostce informatycznej. Jak zamierzamy wykorzystać integralność danych i nadzór nad zmianami w środowisku? Jaki wpływ będą miały te zmiany na integralność danych używanych przez przedsiębiorstwo? Na co powinniśmy zwrócić szczególna uwagę?

Po tym wstępie spójrzmy na różne role pracowników w typowej organizacji działu informatycznego, którym potrzebne są uprawnienia do wykonywania określonych funkcji:

- **Poziom 1. (pomoc techniczna)** — bezpośredni kontakt z użytkownikiem. Pracownicy zmieniają hasła i konta, weryfikują przynależność do grup, rozwiązują problemy z eksploatacją, porządkują kolejki drukowania, stosują podstawowe narzędzia do rozwiązywania problemów ze źle działającym sprzętem i oprogramowaniem oraz pomagają użytkownikom w odnajdowaniu zasobów.
- **Poziom 2. (bezpośrednia obsługa komputerów biurkowych i serwerów)** — pracownicy należący do tego poziomu współdziałają z przedstawicielami poziomu 1. i społecznością użytkowników. Pracują z użytkownikami nad rozwiązaniem problemów leżących poza zakresem uprawnień grupy pracowników poziomu 1. lub wymagających więcej czasu, niż osoby te mogą poświęcić problemowi. Potrzebują dostępu administracyjnego do określonego sprzętu

i uprawnień takich, jakie posiada poziom 1. Większość pracowników musi również mieć możliwość dodawania stacji roboczych do domeny oraz możliwość tworzenia skrzynek pocztowych.

- **Poziom 3. (zaawansowane wsparcie techniczne)** — te osoby rozwiązują złożone problemy dotyczące użytkowników lub całego systemu. Muszą mieć możliwość wykonywania złożonych testów, analizy określonych danych i odczytu dowolnej części zabezpieczeń i informacji katalogowych, aby móc zidentyfikować potencjalne błędy. Większość pracowników technicznych poziomu 3. ma uprawnienia do zmiany przynależności do grup, zmiany haseł i dodawania oraz usuwania serwerów z domeny.
- **Eksploatacja** — osoby zajmujące się procesami wewnętrznymi utrzymującymi funkcjonowanie infrastruktury informatycznej. Monitorują one i zarządzają serwerami, drukarkami, systemami plików, oprogramowaniem przedsiębiorstwa, dystrybucją aplikacji itp. Są zwykle odpowiedzialni za kopie zapasowe, utrzymanie kont, utrzymanie serwerów i oprogramowania oraz, czasem, za telekomunikację i tworzenie zabezpieczeń. W zależności od stopnia fragmentacji tych funkcji możemy potrzebować kilku poziomów zabezpieczeń „eksploatacyjnych" i przydzielać określone prawa tylko pracownikom potrzebującym ich.
- **Architektura** — ta grupa zajmuje się tworzeniem wartości handlowej poprzez integrację ludzi, procesów i technologii. Potrzebuje zwykle dostępu do danych dotyczących wykorzystania sprzętu, dzienników błędów i do przeglądania całej struktury katalogu. Architekci nie muszą potrzebować dostępu do ważnych danych osobistych (np. adresów).
- **Testerzy oprogramowania** — współpracują z grupą architektów nad zapewnieniem, żeby oprogramowanie potrzebne firmie było bezpieczne i obsługiwane przez środowisko. Potrzebują dość szerokiego dostępu do katalogu, serwerów i stacji roboczych, lecz dostęp ten można łatwo ograniczyć do odrębnego środowiska testowego lub pojedynczej jednostki organizacyjnej.
- **Programiści** — mają zwykle specjalne potrzeby, wynikające z używanego środowiska aplikacji. Ponieważ budują i testują aplikacje, więc zazwyczaj potrzebują szerokiego dostępu i sporych uprawnień, aby zajmować się problemami z kodem. Ponieważ dobrze prowadzony projekt programistyczny w bardziej widoczny sposób przynosi zyski niż projekt infrastruktury, programiści zwykle otrzymują szeroki dostęp do środowiska produkcyjnego, chyba że zanim go zażądają, zostaną im zapewnione rozsądne warunki pracy.

Proszę zwrócić uwagę na to, że większość organizacji, tworząc opisy stanowisk, łączy te role. Na przykład, nierzadko spotkamy pomoc techniczną łączącą funkcje poziomu 1. i eksploatacji. Takie zazębianie się kompetencji może być powodem konfliktów pomiędzy poszczególnymi członkami zespołu, jeśli nie będzie zapewniony odpowiedni standard zarządzania, lecz to jest temat na osobną książkę.

Gdy mamy do czynienia ze zdecentralizowaną organizacją, wówczas mnożymy i zwiększamy się liczba liczba pracowników grających określone role oraz złożoność interakcji pomiędzy nimi. Musimy bardzo rozważnie wyznaczać strefy kontroli każdej części organizacji i bezwzględnie wymuszać utrzymywanie tych stref. W przeciwnym razie przytłoczą nas trudności w zarządzaniu katalogiem i problemy z zapewnieniem spójności danych.

Na szczęście Microsoft udostępnia dobre narzędzie pomagające rozdzielanie stref kontroli (nawet w zdecentralizowanej organizacji). Wprawdzie, teoretycznie, można ręcznie przypisywać uprawnienia do każdego atrybutu, lecz większość administratorów wykorzystuje *Kreator delegowania kontroli*, który jest bezpośrednio powiązany z OU.

Co?! Jeśli to prawda, to po co był nam ten cały nudny opis ról i funkcji pracowników? Możemy po prostu rozdawać uprawnienia za pomocą kreatora i tyle. No cóż, sposób podziału uprawnień związanych z zabezpieczeniami ma bardzo dużo wspólnego z tym, jak zbudujemy strukturę OU.

Załóżmy, na przykład, że pomoc techniczna ma szeroki dostęp do serwerów plików i drukowania, lecz żadnego dostępu do serwerów WWW, *Exchange* i aplikacji. Pracownicy pomocy technicznej mogą dodawać użytkowników do grup, zmieniać hasła i odblokowywać konta. Nie mogą jednak dodawać użytkowników, komputerów i grup do domeny oraz nie mają praw do modyfikacji danych użytkowników.

W takim scenariuszu mogą nam być potrzebne OU dla użytkowników, grup, serwerów plików i drukowania, serwerów WWW, serwerów *Exchange* i serwerów aplikacji. W tym przypadku możemy stosować kreator do szczegółowej kontroli dostępu pracowników grupy pomocy technicznej do każdej jednostki organizacyjnej i zawartych w niej obiektów.

Gdy więc zaczynamy rozważać implikacje delegowania kontroli, musimy brać pod uwagę następujące zagadnienia:

- Jaki jest poziom ważności danych, do których możemy przyznać dostęp?
- Jak będziemy nadzorować zmiany danych katalogowych?
- Jaki dostęp jest właściwy dla poszczególnych ról w organizacji?
- Jak te zagadnienia wpływają na projekt jednostek organizacyjnych?

Proszę zawsze pamiętać, że delegowanie uprawnień jest tylko częściowo funkcją działu informatycznego. W większym stopniu jest to zagadnienie biznesowe — kto ma uzasadnione potrzeby dostępu do określonych informacji i kogo należy wyłączyć z dostępu do tej informacji ze względu na funkcjonowanie biznesu.

Bezpieczeństwo

Mamy pełne prawo twierdzić, że dział informatyczny istnieje, by chronić integralność danych organizacji. Istotnie, w wielu organizacjach jest to podstawowa funkcja działu informatycznego. Gdy dane firmy zostaną stracone, zniszczone lub uszkodzone, koszty mogą wynosić miliony dolarów i tysiące straconych roboczogodzin. Ponieważ firmy stają się coraz ściślej połączone ze sobą, niepoprawne dane przekazane od jednego ogniwa łańcucha dostaw do innego mogą zniszczyć cały proces obejmujący wiele przedsiębiorstw, prowadząc do katastrofalnych skutków w wielu firmach.

Pamiętając o tym, powinniśmy podchodzić do bezpieczeństwa danych i katalogu z największą ostrożnością. Jest to jedna z najważniejszych funkcji, jakie możemy zapewniać, i powinna być ona traktowana z odpowiedzialnością.

Przy tym poważnym tonie dobrą wiadomością jest to, że mamy do dyspozycji szereg jasno sprecyzowanych reguł, których możemy się trzymać, aby chronić użytkowników przed nadmiernymi szkodami:

- Stosuj zasadę minimalnego dostępu.
- Twórz procedury nadzoru i rejestracji.
- Równoważ potrzebę ograniczeń i potrzeby pracowników.
- Zawsze zdobywaj odpowiednie upoważnienia.
- Obejmij schematem zabezpieczeń plany przywracania danych i ciągłości działania firmy.

Zasada minimalnego dostępu mówi, iż użytkownik powinien otrzymać dostęp jedynie do danych i usług, które są mu w uzasadniony sposób potrzebne do wykonywania obowiązków służbowych. Dostęp do reszty danych jest zakazany, niezależnie od politycznej lub organizacyjnej pozycji użytkownika.

W Windows 2000 możemy zastosować zasadę minimalnego dostępu, tworząc z OU linie funkcjonalne i zapewniając przez to, aby jedynie zasoby przeznaczone do powszechnego wykorzystania w przedsiębiorstwie posiadały w profilach zabezpieczeń przypisaną im grupę Użytkownicy domeny, oraz rozważnie kontrolując, które grupy mają dostęp do poszczególnych zasobów. Kontrola doskonała pozwala na doskonałą ochronę.

Niestety żaden schemat zabezpieczeń nie jest idealny. Organizacje informatyczne są projektowane, budowane i obsługiwane przez ludzi i dla ludzi. Oznacza to, że błędy mogą się zdarzać. Jedynym sposobem identyfikacji i naprawiania pomyłek jest utworzenie jasnych procedur nadzoru i rejestracji dla tworzenia wystawców zabezpieczeń (tworzenia kont użytkowników), dostępu do zabezpieczonych zasobów (dzienniki pomyślnych i nieudanych prób dostępu) i dla zmian w zasadach zabezpieczeń (dodawanie osoby do grupy).

Szczegółowość i częstość kontroli informacji muszą być dostosowane do zdolności działu informatycznego do rozsądnego przetwarzania danych. Niewiele daje gromadzenie setek megabajtów szczegółowych danych, których nikt nie czyta. Musimy zastosować kilka zdroworozsądkowych reguł, aby ograniczyć powódź danych, z jaką możemy się spotkać:

- W pierwszej kolejności monitoruj punkty dostępu do ważnych danych.
- Monitoruj grupy mające dostęp do tych punktów.
- Kontroluj zakładanie użytkowników i grup.
- Pozwalaj tylko zaufanym administratorom nadawać uprawnienia do wyznaczonych zabezpieczonych udziałów.

Oprócz monitorowania pozostaje jeszcze jeden element układanki dostępu do danych, który musimy przemyśleć: jak bardzo ostrożni powinniśmy być? Moglibyśmy zamknąć zabezpieczane dane w sejfie, wrzucić sejf do kadzi z betonem, a całość do najbliższej rzeki. Wprawdzie dane byłyby bezpieczne, lecz nikt nie mógłby ich użyć do wytworzenia jakiejkolwiek wartości.

Jako profesjonalista z branży informatycznej Czytelnik powinien równoważyć potrzebę ochrony danych i potrzeb dostępu ze strony użytkowników. Możemy spotkać się z niezliczonymi sugestiami metod, jak to osiągnąć: analiza wymierna, analiza „6 sigma" i zamknięcie wszystkiego pod klucz.

Zdecydowanie najefektywniejszą jak dotąd metodą jest *zdefiniowanie procesu* (i postępowanie zgodnie z nim), w którym wymagane jest uwierzytelnienie ze strony wyznaczonych właścicieli danych przed przyznaniem dostępu do danych. Na przykład, jeśli pewien udział zawiera wszystkie dane finansowe przedsiębiorstwa, wówczas wyznaczonym właścicielem danych powinien być zapewne główny księgowy. Nikt nie zostanie dodany do grupy mającej dostęp do udziału bez bezpośredniego zezwolenia głównego księgowego. Proces autoryzacji może być zautomatyzowany (do właściciela danych będzie wysyłany list e-mail), oparty na dokumentach papierowych (właściciel danych otrzymuje formularz), lub bezpośredni (właściciel danych żąda dostępu w imieniu użytkownika, który go potrzebuje).

Powinniśmy też przygotować się na reagowanie w sposób zorganizowany na uszkodzenia, usunięcie lub zniszczenie danych. Oznacza to, że nie tylko musimy planować przywracanie usług, lecz również mityczny stan zwany „ciągłością działania przedsiębiorstwa", w którym organizacje mogą na jakimś poziomie funkcjonować mimo niedostępności krytycznych dla przedsiębiorstwa systemów komputerowych.

Proszę uważać, by nie potraktować zbyt lekko znaczenia zagadnień bezpieczeństwa. Łatwo jest, podczas projektowania Active Directory, prześlizgnąć się po problemach z tym związanych, lecz wystawia to organizację na niedopuszczalne ryzyko, które prędzej czy później będziemy sami musieli zmniejszać.

Zasady grup

Obiekty *zasad grup* (*GPO — Group Policy Object*) są jedną z tych funkcjonalności, które bez właściwego zaplanowania i wdrożenia mogą łatwo wymknąć się spod kontroli. Prosto z pudełka dostajemy 600 ustawień, co w połączeniu z nieograniczonymi możliwościami rozbudowy i modyfikacji ich funkcjonalności pozwoli nam bez trudu stworzyć strukturę administracyjną tak złożoną, że nigdy dokładnie nie ustalimy, co się w niej dzieje.

GPO są przede wszystkim metodą na modyfikowanie Rejestru w sposób przewidywalny i możliwy do opanowania. Pozwalają one administratorowi sieci wymuszać określone ustawienia konfiguracji, zapewniając przewidywalne zachowanie niezależnych systemów. GPO może być skojarzony z kilkoma OU lub lokacjami i łatwo filtrowany w oparciu o przynależność do grup.

Podczas budowania GPO powinniśmy pamiętać o kilku podstawowych zasadach. Ułatwią one znacznie implementację i rozwiązywanie problemów z projektem:

- Zdecyduj na początku projektu, czy kojarzyć pojedyncze GPO z pojedynczymi OU czy też stosować filtrowanie GPO.
- Używaj możliwie najmniejszej liczby GPO.

- Nakładaj jak najmniej GPO.
- Konfiguruj tylko te ustawienia, które będą egzekwowane.
- Ustawiaj parametry, które mają być wyegzekwowane, jak najbliżej obiektu docelowego w łańcuchu GPO.

Istnieją dwa podstawowe sposoby stosowania GPO wobec użytkowników i komputerów: kojarzenie jednego GPO z jedną jednostką organizacyjną oraz kojarzenie wielu GPO z jedną OU, a następnie filtrowanie na podstawie przynależności do grup. Obie opcje mają swoje wady i zalety; ważne jest, by zdecydować się na jedną i stosować ją konsekwentnie. Jeśli zdecydujemy, by łączyć jeden GPO z jedną OU, wówczas możemy potrzebować większej liczby OU, aby zapewnić użytkownikom i komputerom wymagane ustawienia. Jeśli zdecydujemy się łączyć wiele GPO z pojedynczą OU, wówczas potrzebnych będzie mniej OU, lecz więcej grup zabezpieczeń do segregacji ról użytkowników i komputerów.

Nie wymieniliśmy w tym rozdziale idei łączenia pojedynczego GPO z wieloma OU. Wprawdzie jest to jak najbardziej możliwe, lecz nie jest to rozwiązanie zbyt korzystne. Ponieważ trudno ustalić, z którą OU GPO jest skojarzony, więc łączenie GPO z wieloma OU może łatwo doprowadzić do powstawania niezamierzonych interakcji i nieprawidłowo skonfigurowanych ustawień.

Kolejnym sposobem na uniknięcie niezamierzonych interakcji jest unikanie tworzenia dużej liczby GPO. Przy tworzeniu struktury GPO stosujmy *brzytwę Ockhama*: gdy wybieramy jedną z opcji, to ta najprostsza jest zwykle najlepszą. Nie tylko chroni to nas przed koniecznością śledzenia uprawnień poprzez szereg GPO, lecz również ogranicza czas przetwarzania podczas procesów logowania i wylogowywania.

Jeśli po wybraniu najprostszej ścieżki przez szereg różnych zagadnień otrzymamy dużą liczbę GPO, powinniśmy spróbować stworzyć możliwie najkrótszy łańcuch GPO. Oznacza to, że należy próbować nałożyć możliwie jak najmniej GPO na użytkownika lub komputer, tak by wymogi projektu i zabezpieczeń pozostały spełnione. Krótki łańcuch zmniejsza też czas przetwarzania GPO podczas logowania i wylogowania, w niektórych przypadkach bardzo silnie wpływając na czas reakcji systemu na działania użytkownika.

Powody, dla których należy podawać tylko wartości, jakie zamierzamy zmienić, są bardzo zbliżone do wymienionych powyżej. Ponieważ przetwarzanie GPO odbywa się domyślnie co 45 minut oraz podczas logowania i wylogowania, więc im mniej ustawień zmienimy w GPO, tym mniej wartości trzeba będzie przetwarzać. Jeśli na przykład w części GPO dotyczącej użytkownika nie ma żadnych aktywnych ustawień, wówczas przetwarzanie tej części GPO jest wyłączane.

Ponieważ ustawienia GPO kumulują się jako suma wszystkich zastosowanych GPO, a obiekt najbliżej użytkownika lub komputera jest przetwarzany jako ostatni, powinniśmy pilnować, by umieścić ustawienia dotyczące konkretnego konta w GPO położonym najbliżej tego konta.

Innym sposobem na wyegzekwowanie określonej funkcji jest wymuszenie zastosowania GPO. Proszę ostrożnie posługiwać się tą funkcjonalnością — cały GPO zostanie wymuszony, uniemożliwiając dostosowanie ustawień w dalszej części łańcucha. Funkcję tę

należy stosować tylko dla ustawień charakterystycznych dla określonej lokacji (specjalne powiadomienie o bezpieczeństwie w zabezpieczonym ośrodku) lub dla ustawień stosujących się do bardzo dużego podzbioru użytkowników (np. ustawienia obowiązujące całą domenę).

GPO są dla administratora wyjątkowo przydatnym narzędziem, lecz bez rozważnego przeanalizowania i planowania mogą stać się koszmarem administracyjnym. Stosując rozsądnie brzytwę Ockhama, możemy zabezpieczyć się przed niebezpieczeństwem utworzenia skomplikowanego systemu i zmniejszyć prawdopodobieństwo niezamierzonego uniemożliwienia użytkownikom wykonywania swoich zadań.

Zagadnienia bezpieczeństwa

Jak już napomknęliśmy w tym rozdziale, zapewnienie bezpieczeństwa danych należy do podstawowych obowiązków pracowników działu informatyki. Spora część zadań administratora polega na zapewnieniu społeczności użytkowników dostępu na czas do potrzebnych danych oraz zagwarantowania, że dane nie zostały zmienione lub uszkodzone od chwili opublikowania w sieci.

Bieżący podrozdział omawia szczegółowo część zagadnień dostępu do danych, które mogą wpłynąć na projekt Windows 2000 i Active Directory. Położymy nacisk na:

- Dostęp do danych Active Directory — kto powinien mieć dostęp i w jakim kontekście?
- Zarządzanie Active Directory — kto powinien mieć możliwość zarządzania i sprawowania kontroli nad obiektami AD?
- Publikowanie udziałów i drukarek w AD — jakie są konsekwencje widoczności i zabezpieczeń danych?
- Przeszukiwanie Active Directory — co powinno być dostępne, a co nie?

Podobnie jak w każdym z zagadnień dotyczących bezpieczeństwa i tutaj obowiązuje zasada minimalnego dostępu. Zastosowana łącznie z rozsądnym schematem nadzoru i kontroli zmian, zasada ta tworzy solidne podłoże zabezpieczeń, na którym może rozwijać się organizacja.

Dostęp do Active Directory

Active Directory jest repozytorium zabezpieczeń i informacji o tożsamościach organizacji. Możemy o AD myśleć jak o gigantycznej książce adresowej, wypełnionej danymi, które mogą być komuś potrzebne. Im więcej danych zapiszemy w Active Directory, tym większe istnieje prawdopodobieństwo, że wiele grup wewnątrz przedsiębiorstwa, często o sprzecznych interesach, będzie potrzebować dostępu do przechowywanych w niej informacji.

Istnieją trzy podstawowe metody dostępu do informacji w Active Directory:

- poprzez narzędzia administracyjne dostarczone przez Microsoft,
- wykorzystując skrypty *ASDI*, szukające określonych informacji o dostępnych obiektach,
- generując zapytania *LDAP*, wykorzystujące klienty z obsługą standardu LDAP.

Dostępne są tuziny książek i setki publikacji o tym, jak korzystać z tych narzędzi w celu uzyskania dostępu do informacji w Active Directory. Niestety, większość z nich pomija najważniejszą kwestię.

Kwestia ta jest prosta, lecz ważna:

Komu i po co potrzebny jest dostęp do danych?

Zanim nie odpowiemy na te pytania, nie możemy nawet zacząć rozważać, jak zapewnić bezpieczeństwo danych.

Zatrzymajmy się na chwilę i spójrzmy na informacje, które w rzeczywistości obecne są w AD dla większości obiektów:

- **Dane identyfikacyjne** — adres, telefon, imię i nazwisko, bezpośredni przełożony.
- **Dane o lokalizacji** — położenie fizyczne i w sieci, pozycja w przedsiębiorstwie.
- **Dane grup** — przynależność użytkownika do grup.
- **Dane systemowe** — hasła, skrypty logowania, katalogi macierzyste i podobne informacje.
- **Dane własne** — wszelkie atrybuty, jakie dodaliśmy do obiektów.

Jakie usługi potrzebują dostępu do tych informacji? Kto w organizacji i do czego potrzebuje powyższych danych? Skąd pochodzą dane i kto jest odpowiedzialny za ich zmiany?

Ogólnie mówiąc, odpowiedzi na te pytania są następujące:

- **Dane identyfikacyjne** — kontrolowane przez dział spraw osobowych i zmieniane przez dział eksploatacji. Mogą służyć systemom typu *ERP* do tworzenia jednolitych tożsamości użytkowników.
- **Dane o lokalizacji** — kontrolowane przez dział spraw osobowych i zmieniane przez dział eksploatacji. Wykorzystywane przez sprzęt sieciowy i serwery do poprawnego przesyłania danych.
- **Dane grup** — kontrolowane przez właścicieli danych i zmieniane przez dział eksploatacji. Mogą być używane przez oprogramowanie *ERP*, bazy danych i inne aplikacje do przyznawania odpowiednich praw dostępu.
- **Dane systemowe** — kontrolowane zarówno przez użytkownika, jak i przez działy architektury i eksploatacji. Dane używane są przez aplikacje w celu przyznawania odpowiedniego dostępu, mogą też służyć innym dostawcom zabezpieczeń do przyznawania dostępu do swoich zasobów.

- **Dane własne** — kontrolowane przez wyznaczonych właścicieli danych; mogą być prywatne lub poufne. Z danych tych zwykle korzystają systemy *ERP* i inne aplikacje. Z dostępem do nich mogą być związane zagadnienia prawne.

Proszę uważnie przeanalizować, kto i po co potrzebuje dostępu do konkretnych danych. W typowej sieci należy przyznać prawa do odczytu pracownikom, którzy muszą powoływać się na dane, prawa do modyfikacji tym, którzy mają prawo zmieniać dane, zaś pełną kontrolę *tylko* właścicielowi danych.

Zarządzanie AD

Zarządzanie Active Directory w rzeczywistości nie różni się od zarządzania innymi systemami sieciowymi. Narzędzia są inne, lecz reguły i ograniczenia pozostają takie same.

Active Directory jednakże daje możliwość bardzo precyzyjnego dopasowania dobrych zasad do projektu sieci. W przeciwieństwie do systemu Windows NT, w którym większość zasad było dyktowanych przez ograniczenia systemu, AD jest wyjątkowo elastyczna pod względem organizacji, przyznawania dostępu do określonych funkcji i rozdzielania zadań.

To jest kolejne zagadnienie, w którym najbardziej przydatnym narzędziem jest brzytwa Ockhama — zachowanie jak największej prostoty przy równoczesnym spełnianiu wymogów bezpieczeństwa. Należy unikać zbędnych kroków, warstw i złożoności oraz ograniczać liczbę etapów pomiędzy właścicielem danych (kimkolwiek by nie był) a osobami zarządzającymi dostępem, bez poświęcania niezbędnej zdolności do monitorowania.

Udziały i drukarki w AD

Możliwe jest publikowanie w Active Directory informacji o udziałach i drukarkach. Teoretycznie ułatwia to użytkownikom znajdowanie i korzystanie z potrzebnych zasobów, gdy zajdzie taka konieczność.

W praktyce publikowanie udziałów w Active Directory nie zawsze jest rozsądnym pomysłem. Chodzi tu nie tyle o możliwość ochrony danych przez ukrycie przed osobami, które nie powinny mieć do nich dostępu, lecz po prostu istnieje szereg lepszych sposobów na obsługę wyszukiwania tych informacji przez użytkowników. Wiele firm posiada sieci intranetowe, systemy zarządzania dokumentami, rozproszony system plików (*DFS — Distributed File System*) lub udostępnione dyski poszczególnych działów. Lista rozwiązań nie ma końca i jest o wiele elastyczniejsza od publikowania w AD.

Z drugiej strony, publikowanie drukarek może być wysoce przydatne dla społeczności użytkowników. Zamiast dawać użytkownikom pozornie niekończącą się listę tajemniczo brzmiących nazw drukarek, możemy dla ułatwienia dostępu posortować je według lokalizacji. Użytkownicy mogą wówczas szukać drukarek lokalnych lub położonych gdzieś indziej, gdyby chcieli wydrukować dokument dla współpracownika w innej części firmy.

Ogólnie mówiąc, problemy dostępu do danych związane z drukarkami w Active Directory są mało znaczące. Ryzyko skojarzone z drukarkami po prostu nie jest wystarczająco wysokie, by wymagać szczegółowego ustawiania zabezpieczeń w sieci. Większość

drukarek wymaga jednakże pewnego poziomu zabezpieczeń fizycznych, ponieważ użytkownicy mogą drukować dokumenty zawierające poufne informacje, które należy chronić przed niepowołanym dostępem.

Przeszukiwanie AD

Użytkownicy mogą przeszukiwać Active Directory w celu znajdowania innych użytkowników, komputerów lub drukarek. Ogólnie mówiąc, jest to funkcja, którą warto popularyzować — im więcej informacji użytkownicy mogą znaleźć, z tym większą sprawnością będą mogli wypełniać swoje obowiązki.

Jednakże w środowisku złożonym z wielu domen musimy pilnować, by zamieścić w serwerach wykazu globalnego wszystkie atrybuty, które mogą być potrzebne użytkownikom w operacjach wyszukiwania. Więcej informacji na ten temat zawiera rozdział 3., „Składniki Active Directory".

Zagadnienia instalacji

Organizacja instalacji może skomplikować najlepiej zaprojektowaną Active Directory. To, jak szybko możemy zaimplementować określone funkcje, zachować i migrować funkcjonalność i zmniejszyć ryzyko utraty danych, jest kluczem do ustalania w projekcie etapów wdrożenia.

Ten podrozdział omawia dwa podstawowe narzędzia:

- Usługę instalacji zdalnej — pozwala uruchamiać stacje robocze przez sieć lokalną i reinstalować z wykorzystaniem określonego obrazu systemu operacyjnego.
- Zastosowanie GPO do dystrybucji oprogramowania — możemy za pomocą GPO dystrybuować pakiety oprogramowania do użytkowników i komputerów, w oparciu o położenie w strukturze OU.

Bieżący rozdział nie obejmuje opisu skryptów i CD służących do zautomatyzowanej instalacji oraz narzędzi innych producentów. Narzędzia te zostaną dokładnie omówione w rozdziale 8.

Wykorzystanie usługi instalacji zdalnej

Usługa *instalacji zdalnej* (*RIS — Remote Instalation Service*) jest wprowadzoną w Windows 2000 metodą rozsyłania przez *adresowanie grupowe* (*multicasting*) obrazu stacji roboczej do kilku instalowanych klientów. Usługa ta znacząco obciąża sieć i dyski twarde i czasami jest trudna do zarządzania.

Ogólnie mówiąc, usługa RIS jest stosowana w małych środowiskach (poniżej 100 stacji roboczych), w których usługi DHCP i RIS mieszczą się na dwóch lub kilku odrębnych serwerach. Pozwala ona na równoczesne szybkie instalowanie kilku komputerów.

RIS możemy też stosować w centralnym ośrodku przygotowawczym, w którym większa liczba stacji roboczych jest instalowana równocześnie z obrazu systemu operacyjnego, w procesie przygotowania do rozmieszczenia w przedsiębiorstwie. Może to ogromnie przyspieszyć migrację stacji roboczych, lecz tylko wtedy, gdy logistyka przenoszenia stacji roboczych do centralnego ośrodka nie zajmuje więcej czasu i koordynacji niż proste przygotowanie komputera w pobliżu miejsca przeznaczenia.

Instalowanie oprogramowania poprzez GPO

W zależności od tego, jaką strukturę GPO wybraliśmy, może to być opcja wyjątkowo przydatna lub poboczna funkcjonalność, którą na razie zignorujemy.

Jest ona przydatna, gdy musimy w całej organizacji rozprowadzić poprawki do oprogramowania, programy właściwe dla określonej lokacji lub profilu zabezpieczeń albo też pakiety aplikacji, które ulegają regularnym zmianom i mają wpływ na dużą część organizacji.

Instalowanie oprogramowania przez GPO jest mniej przydatne, gdy organizacja zarządza dostępnością aplikacji według użytkowników, a nie według profili zabezpieczeń lub grup. Ponieważ GPO są egzekwowane na poziomie grup i OU, więc nie najlepiej nadają się do rozsyłania aplikacji do poszczególnych użytkowników.

Z punktu widzenia idealnego zarządzania dobrze byłoby, gdyby organizacja wprowadziła zarządzanie aplikacjami na podstawie profilu zabezpieczeń lub przynależności do grup. Niestety, nie zawsze jest to możliwe ze względów politycznych i czasami podejście to nie ma większego sensu, ponieważ w niektórych środowiskach profile zabezpieczeń poszczególnych użytkowników i potrzeby firmy są na tyle różne, by uzasadnić indywidualne zarządzanie.

Zagadnienia polityczne

Przez jedno z tych niemiłych zrządzeń losu, jakie czasem zdarzają się w życiu, informatycy nie mogą po prostu zignorować reszty świata i bawić się swoimi komputerami. Nasza praca odbywa się w szerszym kontekście, który obejmuje praktyki handlowe, wymagania prawne, kulturę przedsiębiorstwa, złożone łańcuchy dostaw i politykę międzynarodową.

Bieżący podrozdział usiłuje przeprowadzić Czytelnika przez pokłady żargonu i zidentyfikować zagadnienia, które bezpośrednio wpływają na projekt Active Directory. Możemy podzielić część tych zagadnień na następujące kategorie:

- **Zagadnienia administracyjne** — kadry, kontrola dostępu i wymagania proceduralne pochodzące od potrzeb biznesowych.
- **Zagadnienia przestrzeni nazw domen** — kwestia tożsamości przedsiębiorstwa, marki i wewnętrznego marketingu.

- **Dostęp do zawartości katalogu** — kwestie prawne, które wymuszają określone działania ze strony projektantów sieci.
- **Problemy ze schematem** — problemy prawne lub inne wymagające dodania lub dezaktywacji określonych obiektów i atrybutów.
- **Zagadnienia handlu światowego** — przepisy mogące mieć wpływ na bezpieczeństwo, szyfrowanie i zasady administracyjne.

Dla każdego z tych problemów najlepiej sformułować odpowiednie pytania i przekazać użytkownikom z dziedziny biznesu, którzy zajmują się tymi zagadnieniami, aby znaleźli odpowiedzi. Prawo, polityka i kultura przedsiębiorstwa są same w sobie złożonymi dziedzinami i, jeśli Czytelnik nie jest biegły w nich wszystkich, to potrzebna nam będzie pomoc z zewnątrz w rozwiązaniu problemów.

Zagadnienia administracyjne

Każdy dział gospodarki ma inne wymogi prawne związane z kontrolami, składowaniem i szybkim udostępnianiem odpowiednim władzom informacji o użytkownikach, plikach, komputerach itp.

Pytania, jakie musimy zadać:

- Jakie organizacje wymagają od nas informacji, kiedy i w jakiej postaci?
- Jakie prawne wymogi kontroli i raportowania obowiązują naszą organizację?
- Przez jaki okres musimy przechowywać historyczne dane katalogowe? Skąd pochodzi ten wymóg i w jakim formacie powinniśmy składować dane?
- Czy w dziale informatycznym pracują osoby, które, z jakiegokolwiek powodu, nie powinny mieć praw dostępu zwykle przyznawanych z uwagi na wykonywaną pracę?
- Czy firma zatrudnia jakieś osoby które wymagają specjalnego traktowania z powodów prawnych, proceduralnych lub politycznych?
- Jeśli firma posiada placówki międzynarodowe, czy dla poszczególnych krajów obowiązują różne wymogi dotyczące składowania, kontrolowania i prezentacji danych?

Dysponując odpowiedziami na te pytania, zaczniemy pojmować, jakich żądań możemy spodziewać się w przyszłości.

Zagadnienia przestrzeni nazw domen

Gdy proponujemy *przestrzeń* nazw domeny (domen), musimy zadać następujące pytania:

- Czy nazwa jest zgodna z wewnętrzną tożsamością firmy?
- Czy nazwa jest zastrzeżona przez inną firmę?

- Czy nazwa w obcym języku znaczy coś, czego chcielibyśmy raczej uniknąć? Na przykład, samochód Chevrolet Nova podobno sprzedawał się źle w krajach hiszpańskojęzycznych, ponieważ po hiszpańsku „no va" oznacza „nie idzie".
- Czy jakaś umowa partnerska lub inna ogranicza wybór przestrzeni nazw?
- Jak proponowana nazwa współgra ze znanymi i planowanymi działaniami marketingowymi przedsiębiorstwa?
- Czy przypadkowo nie wybraliśmy nazwy niosącej negatywne skojarzenia w naszym środowisku?
- Czy potrzeby polityczne lub biznesowe organizacji mogą wymagać założenia nowej domeny?
- Czy organizacja zawiera jednostki, które oddzielą się od większej grupy w ciągu najbliższego półrocza lub roku? Jeśli tak, to czy przejmą swoje zasoby informatyczne podczas odłączenia od firmy?

Zajmując się tymi problemami, powinniśmy też zwracać uwagę na zdanie zarządu organizacji. Jeśli nie wyjaśnimy dokładnie, co robimy i dlaczego chcemy tak właśnie postąpić, kierownictwo raczej nie będzie zainteresowane naszymi „technicznymi" problemami.

Dostęp do zawartości katalogu

Dostęp do informacji zawartych w Active Directory może być ograniczony z uwagi na problemy prawne, etyczne lub proceduralne. Musimy tu zadać następujące pytania:

- Które dane wymagają specjalnego traktowania ze względów politycznych?
- Które dane jesteśmy prawnie zobowiązani chronić?
- Które dane są poufne dla poszczególnych działów?
- Które dane są poufne dla całej firmy?

Problemy te mogą ujawnić się na szereg sposobów. Na przykład w szpitalu kusząca może być możliwość umieszczenia w Active Directory wskaźników do danych pacjentów przypisanych do konkretnego lekarza. Active Directory może grać rolę pośrednika zabezpieczeń, udostępniając dostęp do różnych systemów zawierających dane pacjenta. Jednakże osobiste informacje o stanie zdrowia są chronione przez prawo i dostęp do nich bez właściwego upoważnienia może prowadzić do kar pieniężnych, pozbawienia wolności i wydalenia ze stanowisk związanych ze zdrowiem. Nie są to dane, jakie powinny być składowane w dostępnym dla wszystkich katalogu.

Lub weźmy przykład firmy odpowiedzialnej za oczyszczenie składowiska odpadów. Pracuje ona ciężko nad zniwelowaniem szkód spowodowanych przez odpady, a zarazem nad ochroną reputacji swojej i firmy odpowiedzialnej za zanieczyszczenie. Nagle nazwy grup służących do zabezpieczenia informacji o lokalizacji mogą stać się poufną informacją, ponieważ sprawdzenie przynależności kogoś do grupy jest zadaniem dość trywialnym..., nawet jeśli dane są chronione.

Problemy ze schematem

Schemat Active Directory w Windows 2000 jest bogatym źródłem informacji o firmie lub organizacji, jeśli ktoś poświęci trochę czasu na analizę schematu. Które atrybuty zapełniliśmy danymi? Jakie atrybuty zostały dodane? Jakie obiekty? Z jakich aplikacji ERP korzystamy? Z jakiego oprogramowania pocztowego? Jakie inne katalogi istnieją w naszym środowisku? Krótki wywiad za pomocą klienta *LDAP* może udzielić dowolnemu napastnikowi odpowiedzi na te pytania i wiele innych.

Przy planowaniu dostępu do schematu musimy zadać sobie następujące pytania:

- Kto powinien mieć możliwość przeglądania informacji ważnych i poufnych?
- Kto może wiedzieć, jak organizujemy informacje?
- Jakie informacje musimy kategorycznie ukryć?
- Czy istnieją problemy związane z kadrami lub przepisami, które musimy wziąć pod uwagę podczas tworzenia obiektów reprezentujących ludzi w naszym środowisku?

Zagadnienia handlu i dostępu na skalę światową

Po przekroczeniu granicy międzynarodowej trudności, jakie nas czekają przy ustalaniu wymogów prawnych i biznesowych, wzrastają wykładniczo. Nie tylko musimy martwić się o przepisy prawne dwóch (lub kilku!) krajów, lecz musimy też brać pod uwagę umowy handlowe, umowy międzynarodowe i organizacje używające takich skrótów, jak *WTO* i *ONZ*. A jeszcze nie doliczyliśmy problemów, na które możemy natknąć się przy tłumaczeniu różnorodnych dokumentów z jednego języka na drugi.

Ogólnie mówiąc, musimy zadać następujące pytania:

- Jak nasze różne operacje międzynarodowe są ze sobą związane?
- Czy w którymś kraju istnieją wymogi prawne zmuszające do rozdzielenia naszych struktur domen?
- Czy możemy napotkać na problemy prawne lub związane z bezpieczeństwem dotyczące handlu zastrzeżonymi lub tajnymi informacjami z określoną placówką?
- Czy nasze systemy zawierają dane nie zaklasyfikowane jako poufne, lecz uznawane za poufne przez umowy międzynarodowe?
- Czy katalog zawiera dane uznawane w innym kraju za poufne lub chronione?
- Czy istnieją ograniczenia finansowe lub prawne określające, gdzie musi zostać zakupiony sprzęt?
- Czy nasz katalog jest dobrze przygotowany do potrzeb kontroli i raportowania w innym kraju?

Biorąc pod uwagę ogromną złożoność niektórych z tych problemów, łatwo byłoby odrzucić wszystkie pytania i pójść dalej. Proszę się nie poddawać, tylko zadawać pytania i projektować dalej. Niech prace analityczne nie obciążają projektu. Zawsze możemy w razie konieczności dostosować projekt do potrzeb, nawet po wdrożeniu go do produkcji.

Podsumowanie

Bieżący rozdział został poświęcony zagadnieniom projektowania i implementacji Active Directory. Wiele z zagadnień omówionych w nim opiera się na problemach politycznych, logistycznych i związanych z komunikacją. Problemy te muszą zostać dobrze zrozumiane i przeanalizowane, aby móc stworzyć praktyczny i funkcjonalny projekt Active Directory.

Rozdział ten omówił zagadnienia migracji, jak np. wpływ i współpracę Active Directory z innymi usługami sieciowymi — *WINS*, *DNS* i *DHCP*. Zostały również omówione kwestie administracyjne, takie jak *OU*, grupy i *GPO*.

Do innych problemów zaliczają się zagadnienia bezpieczeństwa i instalacji. Zagadnienia bezpieczeństwa zostały przedyskutowane, aby pomóc Czytelnikowi w ustaleniu najlepszych sposobów ochrony danych i struktur OU, grup i GPO. Na koniec omówiliśmy zagadnienia logistyczne i techniczne, które mogą mieć wpływ na implementację Active Directory.

W praktyce

Nauka na przykładzie: przedsiębiorstwo „Molly Pitcher Pharmaceuticals, Inc.”

Po przeanalizowaniu przykładu firmy Molly Pitcher zostało jeszcze do rozważenia kilka problemów.

Zagadnienia migracji: w przypadku firmy Molly Pitcher jedną z pierwszych decyzji projektowych jest wybór sposobu migracji ze środowiska Windows NT 4 do środowiska Active Directory Windows 2000.

Jednym z wymagań postawionych przez Molly Pitcher jest wyeliminowanie modelu domen z pojedynczą domeną główną. Aby to osiągnąć, możemy wybrać migrację i reorganizację istniejącego środowiska lub zbudowanie nowego. Ponieważ dostępna jest pojedyncza domena główna, w której mieszczą się wszystkie konta użytkowników, możemy wybrać modernizację domeny głównej. Domeny zasobów mogą zostać przeniesione do Windows 2000 później i przekształcone na OU w nowej domenie.

Tryb mieszany czy macierzysty: ponieważ dokonujemy modernizacji przez zastąpienie, na początku będziemy pracować w środowisku mieszanym. Trzeba tu nadmienić, iż firma Molly Pitcher zainstalowała już Windows 2000 Professional we wszystkich klienckich komputerach biurkowych i przenośnych. Z tego powodu wystarczy zapewnić modernizację wszystkich kontrolerów domen (PDC i BDC) przed przejściem w tryb macierzysty. Jeśli przełączymy tryb przed przeniesieniem wszystkich kontrolerów domen, wówczas być może część klientów nie będzie mogła zalogować się do domeny.

Migracja serwerów: Molly Pitcher wykorzystuje szereg serwerów udostępniających usługi plików i drukowania, przesyłania wiadomości i usług intranetowych. Firma posiada też kilka odmian serwerów aplikacji. Wszelkie serwery nie spełniające wymogów sprzętowych Windows 2000 muszą zostać zastąpione. Musimy też upewnić się, czy wszystkie aplikacje używane w tych serwerach są kompatybilne z Windows 2000. Jeśli nie, musimy skontaktować się ze sprzedawcą oprogramowania i zapytać o możliwość modernizacji lub znaleźć innego producenta.

Migracja klientów: firma Molly Pitcher zainstalowała już Windows 2000 Professional na wszystkich komputerach klienckich w całym środowisku. Wobec tego nie ma żadnych problemów związanych z migracją klientów.

Zagadnienia administracyjne: Na koniec musimy przemyśleć problemy administracyjne i zadania, jakie czekają dział informatyczny Molly Pitcher po wprowadzeniu Active Directory do fazy produkcyjnej. Pracownicy działu informatycznego muszą zostać przeszkoleni w zakresie Active Directory, łącznie ze sposobami wykorzystania OU, delegowania zadań i uprawnień innym pracownikom (na przykład zatrudnionym w poszczególnych działach), oraz w sposobach implementacji i zarządzania zasadami grup.