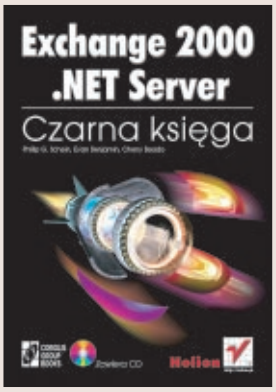
Exchange 2000.NET Server. Czarna księga



Autorzy: Philip G. Schein, Evan Benjamin, Cherry Beado
Tłumaczenie: Marcin Jędrysiak
ISBN: 83-7197-698-4
Tytuł oryginału: Exchange 2000.NET Server
Format: B5, stron: 718

Książka zawiera gotowe rozwiązania typowych problemów, jakie możesz napotkać w czasie zarządzania nowym systemem obsługi wiadomości i pracy grupowej, stanowiącym integralną część platformy .NET. W tej książce przedstawiono krok po kroku procedury implementacji usług i zarządzania nimi. Możesz tu znaleźć także plany tworzenia przepływów pracy oraz wyczerpujące informacje na temat platformy Exchange 2000.

- Najważniejsze dane o topologii sieci, strukturze organizacyjnej, potrzebach użytkowników i celach projektu
- Konfiguracja i wdrażanie usług Exchange 2000 w celu obsługi pracy grupowej i zarządzania usługami czasu rzeczywistego
- Optymalizacja wydajności Exchange 2000 w większym środowisku Windows 2000
- Zaawansowane funkcje architektury .NET, które pozwalają na zwiększenie niezawodności, skalowalności i wydajności
- Rozszerzanie zakresu dostępnych funkcji przy użyciu takich języków jak ASP i XML
- Uzyskiwanie dostępu do zasobów wiedzy w Web Storage System

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

Spis treści

Rozdział 9.

Kwestie związane z serwerem Exchange

Wprowadzenie

We wcześniejszych rozdziałach tej książki omówiliśmy pewnie zagadnienia związane z implementacją różnych komponentów serwera, takich jak magazyny skrzynek pocztowych i grupy magazynowania. Aby można było lepiej zrozumieć strukturę serwera Exchange 2000, została przedstawiona także obsługa wiadomości. Nie zapomnieliśmy o kwestii przywracania pracy serwera po wystąpieniu różnego rodzaju katastrof. Czytelnik poznał zalety architektury Exchange 2000 oraz sposób wyboru usług dla różnych środowisk pracy.

Ten rozdział stanowi uzupełnienie wcześniejszych rozdziałów książki, w których skupiliśmy się na projektowaniu serwera w zakresie poszczególnych komponentów. Teraz skoncentrujemy się na trasowaniu wiadomości i administracji systemem. Większość instalacji Exchange 2000 może być podzielona według następujących typów wykonywanych czynności:

- *Zabezpieczenia* — te czynności są związane z wdrażaniem lub rozszerzaniem narzędzi zabezpieczeń, które zostały stworzone specjalnie dla Exchange 2000; służą one m.in. do zarządzania treścią, wykrywania włamań, wykrywania i usuwania wirusów, a także do blokowania niepożądanej poczty reklamowej (tak zwany spam). W tym rozdziale omówimy szczegółowo MIME i S/MIME (Secure MIME), a także planowanie zarządzania treścią poczty elektronicznej i zabezpieczeniami antywirusowymi.
- *Sieć* — te działania obejmują konfigurację i zarządzanie usługą DNS dla serwera Exchange 2000, a także kwestie związane z integracją Exchange 2000 z modelem komunikacji sieciowej TCP/IP. W rozdziale przyjrzymy się dokładnie integracji DNS z Exchange 2000 oraz portom TCP/IP, które są niezbędne dla tej platformy.
- *Adresaci* — czynności związane z ogólną konfiguracją i zarządzaniem obiektów adresatów, takich jak magazyny skrzynek pocztowych, grupy magazynowania i magazyny folderów publicznych. Wspomnimy także o implementacji tych obiektów do celów kontroli dostępu i zarządzania uprawnieniami. Zostanie przedstawiona kwestia implementacji grup magazynowania i grup administracyjnych, włączając w najlepsze sposoby zarządzanie procesem delegacji uprawnień w firmie.

- *Migracja* — czynności związane z migracją i aktualizacją wcześniejszych wersji serwera Exchange 5.5, a także z zapewnieniem koegzystencji Exchange 2000 i wcześniejszych wersji platform Exchange. Skupimy się na umożliwieniu obsługi folderów publicznych w Exchange 5.5 i Exchange 2000, włączając w to właściwy sposób użycia łącznika ADC (Active Directory Connector).

W tym rozdziale znajduje się wiele przydatnych rozwiązań, które z pewnością będziesz mógł wykorzystać we własnym środowisku.

Kwestie związane z bezpieczeństwem serwera

Bezpieczeństwo stanowi jedno z największych zmartwień każdego administratora poczty elektronicznej, a administracja serwerem Exchange nie jest tu wyjątkiem. Podobnie jak inne systemy pocztowe, serwery Exchange muszą być zabezpieczone przed wieloma zagrożeniami, takimi jak złośliwe elementy sterujące ActiveX i szkodliwe wirusy. Zabezpieczając serwery Exchange 2000, należy wykorzystać rozwiązania zarówno sprzętowe, jak i programowe. Obejmuje to między innymi:

- Użycie sprzętowych firewalli do blokowania niepożądanego ruchu internetowego, który może zawierać szkodliwe wirusy sprzętowe lub inne niepotrzebne rzeczy.
- Użycie szyfrowania i uwierzytelniania dla zewnętrznych klientów internetowych, którzy próbują uzyskać dostęp do serwera Exchange w sieci lokalnej. Dostępne technologie to, na przykład, S/MIME i szyfrowanie SSL (Secure Sockets Layer).
- Instalacja na serwerach Exchange oprogramowania do zarządzania treścią, co pozwoli na filtrowanie niepożądanych załączników lub emaili zawierających niebezpieczny kod VBScript i elementy sterujące ActiveX.
- Instalacja oprogramowania antywirusowego na wszystkich serwerach Exchange w celu usunięcia wszystkich wirusów pochodzących z zainfekowanych serwerów zewnętrznych.
- Wdrożenie systemu wykrywania włamań, który będzie monitorował potencjalne ataki typu DoS (odmowa świadczenia usługi). Takie ataki są czasami rozpoczynane przez złośliwe wirusy komputerowe lub aplikacje zawierające konie trojańskie.

Wirus komputerowy to program, który jest ukryty wewnątrz innej aplikacji, i który wykonuje replikację własnego kodu lub innych plików w celu wykonania szkodliwych zadań, takich jak wymazanie dysku twardego. Z kolei koń trojański to niereplikujący się złośliwy program, który czyni coś szkodliwego; gdyby użytkownicy wiedzieli o istnieniu takiego konia w systemie, nie aprobowaliby jego działania. W niektórych przypadkach wirus może być odmianą konia trojańskiego, ponieważ może zarażać inne programy (czyli również przekształcać je w konie trojańskie).

We wcześniejszych rozdziałach zasugerowano pewne procedury pozwalające na zwiększenie bezpieczeństwa. Takie rozwiązania obejmują zarówno użycie skomplikowanych haseł składających się z kombinacji liter i cyfr, jak i wykorzystanie metod uwierzytelniania w Windows 2000, włączając w to metodę Digest Authentication, która zapewnia szyfrowanie haseł. Jednakże hasła nie stanowią pełnego rozwiązania zabezpieczeń w organizacji. Administratorzy dobrze wiedzą, iż konieczne jest zastosowanie innych środków ochronnych w celu pełnej ochrony zasobów. Wymaga to implementacji narzędzi sprzętowych i programowych, które zostały zaprojektowane specjalnie w tym celu.

Kwestia użycia firewalli oraz ochrony przed atakami DoS została już omówiona w poprzednich rozdziałach tej książki, teraz więc skoncentrujemy się na zbadaniu innych tematów, takich jak dokładne omówienie protokołu MIME i użycie oprogramowania do zarządzania treścią w czasie wdrożenia Exchange 2000.

Użycie zabezpieczeń wiadomości

Ruch emailowy jest zwykle chroniony przy użyciu *zabezpieczeń sesji* lub *zabezpieczeń wiadomości*. Pierwsza metoda wykorzystuje, na przykład, szyfrowanie SSL do stworzenia bezpiecznych tuneli lub kanałów pomiędzy serwerem pocztowym (takim jak Exchange 2000) i klientem (na przykład, Outlook 2000). W czasie procesu dostarczania wiadomości wykorzystywane jest uwierzytelnianie i szyfrowanie. Z kolei zabezpieczenia wiadomości obejmują raczej metody ochrony treści wiadomości, a nie kanału, przez który jest ona przesyłana. Infrastruktura klucza publicznego (PKI) zapewnia oba rodzaje zabezpieczeń. PKI jest połączeniem wielu komponentów, włączając w to ośrodki certyfikacji (CA) i inne ośrodki, które pomagają w uwierzytelnieniu użytkowników zaangażowanych w proces wymiany danych. PKI wykorzystuje różne technologie, takie jak podpisy cyfrowe i pieczętowanie wiadomości, w celu usunięcia wszelkich potencjalnych zagrożeń bezpieczeństwa poczty elektronicznej.

Rozważając kwestie zaawansowanych zabezpieczeń w Exchange 2000, bardzo łatwo jest pomylić ze sobą różne technologie. Dla przykładu, SSL i S/MIME są zwykle wymieniane wspólnie, ale tak naprawdę są używane do kompletnie różnych zastosowań. SSL jest niezbędny w czasie szyfrowanej komunikacji między serwerami frontonu a zdalnymi klientami internetowymi, którzy uzyskują dostęp do skrzynek pocztowych na zabezpieczonych serwerach zaplecza. S/MIME to standardowy protokół internetowy, który pozwala na wymianę podpisanych wiadomości przy użyciu dowolnego klienta obsługującego ten protokół (na przykład, Outlook Express). S/MIME to bezpieczna metoda przesyłania poczty elektronicznej przy użyciu systemu szyfrowania RSA (Rivest-Shamir-Adleman). RSA jest stosowany w większości przeglądarek internetowych Microsoftu i Netscape, aczkolwiek zapewnia tylko podstawowe zabezpieczenia w porównaniu z innymi metodami, takimi jak 3DES (Triple Data Encryption Standard) ze 168-bitowym szyfrowaniem lub uwierzytelnianie SHA-1. S/MIME został zaproponowany zespołowi IETF jako standard; konkurencję stanowi dla niego protokół znany jako PGP/MIME (Pretty Good Privacy/Multipurpose Internet Mail Extensions). Zrozumienie protokołu MIME pozwoli docenić zabezpieczenia wiadomości przy użyciu S/MIME.

Protokół MIME jest opisany w RFC 1521 i definiuje sposób organizacji wiadomości. Różnica między MIME i S/MIME polega na tym, iż ten drugi protokół definiuje sposób, w jaki informacje o szyfrowaniu i cyfrowe certyfikaty mogą stanowić część treści wiadomości emailowych.

Protokół S/MIME korzysta z tej samej składni, co Public-Key Cryptography Standard format #7.

MIME stanowi rozszerzenie protokołu internetowego SMTP i pozwala na użycie go do wymiany poprzez Internet różnych plików danych, takich jak dźwięk i wideo. Celem MIME było rozszerzenie prostego standardu SMTP, tak aby klient pocztowy mógł obsłużyć różne typy danych, a nie tylko zwyczajny tekst w formacie ASCII. Serwery Exchange zwykle dołączają nagłówek MIME na początku każdej transmisji danych przez Internet.

Programy pocztowe, jak na przykład Outlook 2000, używają nagłówka MIME w celu wybrania właściwej aplikacji dla danych zdefiniowanych przez ten nagłówek. Może wystąpić konieczność pobrania odpowiedniego typu aplikacji, na przykład odtwarzacza MP3, jeśli taki typ danych został opisanych w nagłówku, a klient lub przeglądarka nie ma wbudowanych odpowiednich funkcji. Wszystkie nowe typy danych MIME, jakie się pojawiają, są rejestrowane przez Private Internet Corporation for Assigned Names and Numbers (ICANN), znany wcześniej jako IANA (Internet Assigned Numbers Authority).

Więcej szczegółów na temat specyfikacji MIME można znaleźć w RFC 1521 i RFC 1522, które są modyfikacją oryginalnej specyfikacji protokołu SMTP, zdefiniowanego przez RFC 821. RFC znajduje się na witrynie internetowej IETF pod adresem *www.ietf.org/rfc.html*.

We wcześniejszych wersjach serwera Exchange wszystkie wiadomości MIME były natychmiast konwertowane do formatu MAPI. Nie był to jednak jedyny format wiadomości emailowych, ponieważ zależało to od miejsca, skąd wysyłano pocztę. Dostępne formaty poczty elektronicznej obejmowały:

- *EDB* — ten typ pliku reprezentował bazy danych Information Store w Exchange 5.5.
- *MAPI* — standard definiujący interfejsy programu oraz właściwości używane do wyświetlenia wiadomości emailowej. Wiadomość MAPI nie może być jednocześnie pokazywana jako macierzysta wiadomość MIME.
- *MIME* — standard używany do przedstawienia nagłówka, treści lub załączników wiadomości.
- *MTA* — agent MTA w Exchange 5.5 używany do trasowania wiadomości między serwerami. Exchange 2000 do tego celu korzysta z protokołu SMTP, a MTA służy do łączenia się z klasycznymi serwerami Exchange 5.5.
- *NNTP* — standardowy protokół internetowy używany do pobrania wiadomości z grup dyskusyjnych.
- *POP3* — standardowy protokół internetowy używany tylko do pobrania wiadomości.
- *SMTP* — standardowy protokół internetowy służący do wysyłania wiadomości emailowych.

Po konwersji wiadomości do formatu MAPI, oryginalny format MIME zostaje usunięty na zawsze. Jeśli jednak klient POP3 zażąda takiej wiadomości, to, w zależności od konfiguracji, serwer Exchange dokona ponownej konwersji do MIME. Exchange 2000 zmienił ten sposób postępowania, gdyż przechowywane są oryginalne wiadomości MIME bez konieczności konwersji do formatu MAPI. Jest to możliwe, gdyż wszystkie wiadomości MIME pobrane przez protokoły SMTP, NNTP lub HTTP są automatycznie umieszczane w pliku z rozszerzeniem *.stm*. Ten plik to w rzeczywistości baza danych, w której składowana jest zawartość MIME dla wszystkich wiadomości użytkowników (włączając w to magazyny danych skrzynek pocztowych i folderów publicznych).

Funkcja magazynowania wiadomości w formacie MIME stała się bardzo popularna, ponieważ użytkownicy mogą zobaczyć wiadomości dokładnie tak, jak zostały wysłane. Nie ma możliwości utraty części danych z powodu błędnej konwersji.

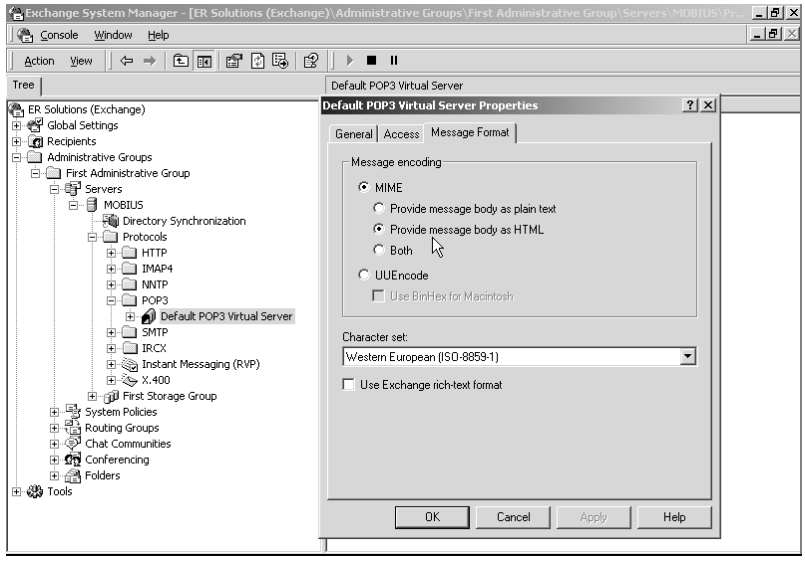
Należy pamiętać, iż na każdą skrzynkę pocztową składają się dwa pliki — EDB i SMT. Kiedy usługa SMTP w Exchange 2000 otrzymuje wiadomość, jej zawartość MIME jest umieszczana w pliku STM. Usługa odczytuje następnie wszystkie nagłówki wiadomości

i umieszcza jej pola (takie jak *Od* i *Temat*) w pliku EDB jako właściwości MAPI (plik EDB zawiera tabelę *Messages* do przechowywania takich informacji). Plik EDB posiada wskaźnik do pliku STM, dzięki czemu wszystkie komponenty otrzymują informacje, gdzie należy odczytać macierzystą zawartość MIME dla użytkownika.

Ponieważ koncentrujemy się tu na porównaniu MIME i MAPI, trzeba rozważyć kilka scenariuszy, kiedy wiadomości są, lub nie są, konwertowane do macierzystego formatu MIME (idealna sytuacja). Użytkownicy Outlooka powinni wiedzieć, iż ten program tworzy wiadomości jako zestaw właściwości MAPI, a Exchange konwertuje taki zestaw do MIME — w zależności od miejsca docelowego wiadomości. Nawet Outlook Web Access (OWA) 2002 nie potrafi utworzyć lub odczytać wiadomości w macierzystym formacie MIME. Taka konwersja jest wykonywana, jeśli odbiorca poczty jest oddalony lub znajduje się na tym samym serwerze, co nadawca. Jeśli nadawca i odbiorca są umieszczeni w tym samym magazynie skrzynek pocztowym (a więc w tej samej grupie magazynowania), wszystkie wiadomości są doręczane do adresata jako zestaw właściwości MAPI, a nie w formacie MIME.

Ciekawostką jest, że wiadomości kierowane do innych serwerów Exchange 5.5 były wysyłane przez MTA jako zestaw właściwości MAPI. Jeśli poczta była kierowana do odbiorców SMTP znajdujących się poza organizacją, łącznik Internet Mail Connector (IMC) wykonywał jej konwersję do MIME.

Protokoły NNTP, HTTP, POP3 i IMAP4 pozwalają na żądanie wiadomości w formacie MIME. Jeśli wykorzystywany jest NNTP, wszystkie wiadomości są automatycznie konwertowane do tego formatu (wiadomości MIME są wysyłane bez konwersji). W przypadku protokołu HTTP wiadomości MAPI są konwertowane do formatu MIME, a wiadomości MIME są przesyłane strumieniowo do przeglądarki internetowej bez żadnych modyfikacji. Jeśli używane są protokoły POP3 lub IMAP4, wiele zależy od wybranych ustawień serwera. Kontrola konfiguracji serwerów wirtualnych POP3 lub IMAP4 może być wykonana poprzez przystawkę MMC *System Manager* (zobacz rysunek 9.1). Dostępne opcje pozwalają na przesyłanie treści wiadomości w formacie tekstowym, HTML lub jako połączenie obu tych metod.



Rysunek 9.1. *Zakładka formatu wiadomości dla serwera wirtualnego POP3 w System Managerze*

Microsoft wprowadził nowy format wiadomości o nazwie *Transport Neutral Encapsulation Format* (TNEF), który występuje tylko w Exchange 2000. TNEF pozwala na przedstawienie danych typu rich-text w wiadomościach Outlooka 2000 w formacie MIME. Ten nowy format stanowi binarny załącznik do wiadomości; tylko klienci MAPI (Outlook 2000 lub wcześniejsze wersje) znają sposób dekodowania tego formatu. Kiedy wiadomości są wysyłane między serwerami w różnych organizacjach, trudno jest zagwarantować integralność danych typu rich-text w Outlooku, a niektóre dane (takie jak obiekty OLE) nie mogą być użyte w standardowym formacie MIME. W takich sytuacjach pomóc może format TNEF. W zakładce *Internet Message Format* w System Managerze możliwe jest skonfigurowanie konwersji wychodzących wiadomości do formatów MIME, UUEncode (Unix-to-Unix Encode) lub TNEF. Należy tylko pamiętać, iż ta konfiguracja odnosi się wyłącznie do wiadomości MAPI, gdyż macierzyste wiadomości MIME nie są nigdy konwertowane przy użyciu tych opcji.

Ponieważ Exchange 2000 do komunikacji między serwerami wykorzystuje protokół SMTP, konieczna jest konwersja wszystkich wiadomości MAPI do formatu TNEF przed przesłaniem do innego serwera. Jeśli wiadomość w formacie TNEF jest przesyłana przy użyciu protokołów HTTP, NNTP lub SMTP, jest ona umieszczana w pliku EDB bazy danych wiadomości, a nie w pliku STM.

Przy korzystaniu z OWA 2000 trzeba wiedzieć, iż nie potrafi on odczytać ani utworzyć żadnych wiadomości w macierzystym formacie MIME. OWA pozwala przeglądarkom internetowym (takim jak IE 5) na wysłanie żądania wiadomości z dowolnego serwera Exchange; serwer dokonuje konwersji wiadomości emailowych do formy strony internetowej w celu wyświetlenia w przeglądarce. Końcowy format wiadomości dla OWA to MAPI, a nie MIME. Administrator powinien znać również typy formatów, jakie Exchange 2000 wykorzystuje do składowania wiadomości w bazach danych. W każdym momencie wiadomość istnieje w trzech podstawowych formatach — MIME, skonwertowane MIME i MAPI. Należy pamiętać o następujących kwestiach:

- Jeśli klient MAPI żąda wiadomości MIME, Exchange 2000 dokonuje jej konwersji do stanu przekonwertowanego MIME i tworzy wpis w tabeli załączników bazy danych EDB. Oryginalna zawartość MIME pozostaje w pliku MIME w magazynie skrzynki pocztowej.
- Ponieważ każda skrzynka pocztowa ma pliki EDB i STM, powinno się pamiętać, iż właściwości treści wiadomości w pliku EDB nie zawierają samej treści. Pliki EDB wskazują położenie zawartości oryginalnej wiadomości (w formacie MIME) w pliku STM dla skrzynki pocztowej.
- Pełny format MIME oznacza, iż plik STM przechowuje oryginalną zawartość MIME wszystkich wiadomości. W pliku EDB znajdują się nagłówki i inne właściwości.
- Tryb przekonwertowanego MIME oznacza, iż plik STM zawiera oryginalną zawartość wiadomości, a w pliku EDB znajdują się wszystkie jej nagłówki. Właściwości wszystkich załączników są umieszczane w tabeli załączników, która również stanowi część pliku EDB dla każdej skrzynki pocztowej.
- Pełny format MAPI oznacza, iż treść wiadomości i wszystkie inne właściwości znajdują się w tabeli wiadomości w pliku EDB dla skrzynki pocztowej. Wszystkie załączniki i dane wiadomości są umieszczone w tabeli załączników w pliku EDB.

Poznanie tych formatów pozwoli na zrozumienie sytuacji, kiedy klienci modyfikują wiadomości emailowe. W przypadku klientów MAPI wiadomość pozostaje w formacie MAPI, a wszystkie dane odnoszące się do wiadomości są przenoszone z pliku STM. Cała wiadomość — treść i załączniki — jest zapisywana w formacie MAPI w magazynie skrzynki pocztowej. Jeśli do modyfikacji wiadomości użyto protokołów zgodnych z MIME, wiadomość pozostaje w formacie MIME. Należy jednak wiedzieć o sytuacjach, kiedy nie jest możliwy dostęp do macierzystej zawartości MIME. Niektórzy administratorzy korzystają z narzędzia Exchange 5.5 o nazwie Move Mailbox do przenoszenia użytkowników między serwerami. W takim przypadku wszystkie wiadomości mają format MIME, ale wiadomości przechodzące przez łącznik X.400 są konwertowane do formatu MAPI. Podsumowując, Exchange 2000 obsługuje wiadomości MIME w całkowicie odmienny sposób niż wcześniejsze wersje Exchange. O wiele rzadziej wykonywana jest konwersja do formatu MAPI, a ponadto zapewniona jest większa integralność poczty.

Jeśli format MIME decyduje o sposobie organizacji wiadomości, to S/MIME wpływa na sposób dołączenia do treści wiadomości informacji o szyfrowaniu i cyfrowych certyfikatach. Wykorzystanie S/MIME oznacza konieczność wdrożenia PKI, czyli systemu używającego ośrodka certyfikacji i cyfrowych certyfikatów do uwierzytelnienia wszystkich użytkowników komunikacji elektronicznej, włącznie z pocztą emailową. Usługi certyfikatów Windows 2000 pozwalają na instalację PKI. Wdrożenie S/MIME dla klientów Outlook 2000 jest możliwe dzięki usłudze Key Management (KM) w Exchange 2000. Outlook jest odpowiedzialny za szyfrowanie (lub pieczętowanie) i podpisywanie wszystkich wiadomości.

Cyfrowe certyfikaty to obiekty zawierające dwie ważne informacje — klucz publiczny i właściciela certyfikatu. Ośrodek certyfikacji (CA) próbuje zweryfikować powiązanie między kluczem publicznym i organizacją, do której należy właściwy klucz prywatny. PKI w Windows 2000 używa certyfikatów zgodnych ze standardem X.509 v3, aczkolwiek istnieją jeszcze inne formy certyfikatów (na przykład, zgodne ze standardem Pretty Good Privacy). CA to godna zaufania organizacja, która wystawia innym organizacjom certyfikaty na podstawie ustalonych kryteriów, nazywanych *zasadami*. Takie zasady są publikowane w odpowiednim dokumencie opisującym proces certyfikacji. Główne typy ośrodków certyfikacji, jakie są używane przez infrastrukturę PKI (a jednocześnie przez protokół S/MIME), to:

- Macierzysty ośrodek certyfikacji — ekwiwalent samopodpisanego CA, w którym klucz publiczny certyfikatu jest jednocześnie kluczem używanym do jego weryfikacji. Wystawca certyfikatu jest nazywany właścicielem. Wszystkie macierzyste ośrodki certyfikacji są bezwarunkowo godne zaufania klientów, a samopodpisany CA jest automatycznie macierzystym ośrodkiem certyfikacji.
- Podległy ośrodek certyfikacji — sytuacja, w której klucz publiczny certyfikatu różni się od klucza używanego do jego weryfikacji.

Zarządzanie treścią

Zarządzanie pocztą elektroniczną nabiera coraz większego znaczenia, ponieważ każdego dnia zwiększa się liczba wirusów komputerowych w wiadomościach emailowych i załącznikach. Najpierw omówimy znaczenie implementacji aktywnego schematu zarządzania treścią, a następnie pokażemy sposoby ochrony przez złośliwymi wirusami, które mogą spowodować chaos w systemie obsługi wiadomości.

Zarządzanie zawartością poczty elektronicznej to coś więcej, niż tylko próba powstrzymania epidemii wirusów. Specjalne oprogramowanie potrafi odfiltrować niewłaściwą treść lub kod zawarty w wiadomości lub jej załączniku. Administratorzy tworzą filtry w taki sposób, aby przechwycić niektóre słowa kluczowe — od tylko denerwujących, aż po bardzo obelżywe. Programy do zarządzania treścią mogą również blokować niepożądane wiadomości, dzięki czemu użytkownicy nie są bombardowani bezużytecznymi reklamami. Innym sposobem wykorzystania tego oprogramowania jest filtrowanie słów powiązanych z witrynami internetowymi tylko dla dorosłych lub z materiałami pornograficznymi. Możliwe jest także filtrowanie poczty wychodzącej, dzięki czemu wrażliwe informacje firmowe nie są przypadkiem wysłane na zewnątrz organizacji.

Wiele organizacji wprowadza obecnie własne zasady, które definiują typ i formę danych, jakie mogą być przesyłane do osób na zewnątrz firmy. Wszyscy użytkownicy, podpisując umowę o zatrudnieniu, muszą zapoznać się z tymi zasadami.

Zarządzanie treścią może być wprowadzone na bramach SMTP w organizacji lub bezpośrednio na serwerach Exchange 5.5 lub Exchange 2000. Możliwe jest również włączenie odpowiednich funkcji w programach pocztowych użytkowników. Większość produktów została stworzona w taki sposób, aby obsługiwać zarządzanie treścią na bramach SMTP połączonych bezpośrednio z serwerem Exchange 2000. Coraz większa grupa producentów tworzy jednak oprogramowanie działające bezpośrednio na serwerach Exchange 2000.

Autorzy tej książki używali z powodzeniem programu MailSweeper firmy Baltimore Technologies. MailSweeper może być zainstalowany na większości serwerów SMTP, które łączą się z Exchange 2000 poprzez łącznik SMTP. Inne produkty tego typu to, na przykład, Mail Essentials for Exchange Server firmy GFI (*www.gfi.com/me/mailessentials.htm*) oraz InterScan VirusWall firmy Trend Micro (*www.antivirus.com/products/isem*).

Jeśli koszt oprogramowania do zarządzania zawartością wydaje się być zbyt wysoki, do tego celu można wykorzystać funkcje umieszczone w kliencie Outlook 2000 (nazwane *Kreator reguł* i *Asystent skrzynki odbiorczej*). Outlook zapewnia także filtry niepożądanej poczty (*Wiadomości-śmieci*) i treści dla osób dorosłych, które identyfikują wiadomości na podstawie wybranych słów kluczowych. Takie filtry nie zapewniają jednak pełnej skuteczności, co sprawia, iż w niektórych organizacjach konieczne jest wdrożenie komercyjnego oprogramowania do zarządzania treścią. Choć Outlook pozwala na oznaczenie kolorem niepożądanych wiadomości ze źródeł zewnętrznych, to konieczna jest implementacja tej funkcji dla każdego klienta oddzielnie, przez co taka procedura jest mało wygodna dla dużych organizacji.

Zasady poczty przychodzącej w Outlooku nie będą nigdy tak skuteczne, jak umieszczone na serwerze komercyjne oprogramowanie do zarządzania treścią. Dzieje się tak, gdyż zasady Outlooka są stosowane, tylko jeśli ten program pocztowy działa na komputerze użytkownika. Nie jest również możliwe przeniesienie wiadomości do osobistego magazynu wiadomości lub pliku PST (takie pliki znajdują się na komputerze lokalnym). Te zasady nie będą działały w przypadku klienta OWA, ponieważ nie jest możliwa konfiguracja zasad przy użyciu OWA.

Znajdujące się na końcu tego rozdziału rozwiązanie *Wybór właściwego oprogramowania do zarządzania treścią* zawiera najważniejsze informacje związane z wybraniem programu oferującego niezbędny zakres funkcji. Takie funkcje nie zawsze są obecne w programach antywirusowych, przez co nie należy przekazywać tym programom zadania zarządzania

treścią (choć obecnie niektóre narzędzia antywirusowe zawierają właściwe wtyczki do tego celu). Programy antywirusowe zwykle nie skanują informacji zaszyfrowanych w jakikolwiek sposób (na przykład, plików ZIP zabezpieczonych hasłem). Dobre oprogramowanie do zarządzania treścią może filtrować pliki tego typu, co pozwala na wykonanie dalszych analiz lub podjęcie odpowiednich działań.

Jeśli w wyniku użycia oprogramowania do zarządzania treścią można zaobserwować nadmierną liczbę niepożądanych wiadomości reklamowych, należy założyć, iż serwer Exchange 2000 jest używany jako serwer spamowy lub typu open-relay. Oznacza to, iż jakiś zewnętrzny użytkownik wykorzystuje ten serwer pocztowy do trasowania swojej poczty. W najgorszym przypadku może to świadczyć o użyciu serwerów firmowych do przeprowadzania ataków DoS na innych serwerach zewnętrznych.

Zabezpieczenia antywirusowe

Wirusy przesyłane przez systemy pocztowe tylko w 1999 r. spowodowały straty firm w wysokości 8 miliardów dolarów. Należy doliczyć do tego także koszty usunięcia tych złośliwych programów. Większość programów antywirusowych koncentruje się na stronie klienckiej, jednak coraz więcej organizacji poszukuje programów serwerowych działających na skalę całej organizacji. Dzieje się tak, gdyż rosnąca liczba wirusów jest rozprzestrzeniana w sieciach LAN i WAN oraz poprzez bezpośrednie połączenia między serwerami. Oprogramowanie antywirusowe powinno być zainstalowane w różnych miejscach organizacji, podobnie zresztą jak programy do zarządzania treścią.

Administratorzy powinni zapoznać się z zasadami wyszukiwania wirusów, włączając w to kwestię mechanizmu antywirusowego i sygnatur wirusów. Mechanizm antywirusowy zajmuje się wyszukiwaniem wirusów w całej pamięci systemu, podczas gdy plik sygnatur wirusów dostarcza dla niego wzory kodu wirusów. Większość programów antywirusowych używa mechanizmu wyszukiwania w celu znalezienia wirusów zgodnych ze wzorcem sygnatury wirusa. Należy jednak pamiętać, iż spora część takich programów nie zapobiega rozprzestrzenianiu się koni trojańskich w organizacji, co powoduje konieczność użycia innych narzędzi do tego celu. Największym problemem dla administratorów jest szybkie tempo replikacji i rozprzestrzeniania się wirusów, przez co klienci nie mają czasu na aktualizację sygnatur wirusów. Z tego powodu niektórzy producenci udostępniają serwery aktualizacji takich sygnatur, dzięki czemu aktualizacja oprogramowania na wielu komputerach odbywa się prawie natychmiast.

Microsoft wprowadził w Exchange 5.5 z zestawem SP3 nowy interfejs API do wyszukiwania wirusów. Ten interfejs został stworzony pod kątem architektury Exchange i obsługuje funkcje specyficzne dla tej platformy, jak, na przykład, istnienie jednego egzemplarza wiadomości w Information Store.

Ten interfejs jest używany tylko w Exchange 5.5 z SP3 oraz w Exchange 2000. W tym drugim przypadku konieczna jest instalacja zestawu Service Pack 2 dla Windows 2000.

Interfejs API pozwala programistom Exchange na stworzenie własnych programów, które wykrywają wszystkie niebezpieczne wiadomości na serwerze Exchange 2000. Interfejs ma postać biblioteki DLL, do której dostęp uzyskuje Web Storage System (WSS). Podsumowując, interfejs wyszukujący wirusy rozpoczyna działanie po załadowaniu do pamięci biblioteki DLL i uruchomieniu Information Store (lub Web Store). Jeśli taka biblioteka

zostanie zainstalowana na każdym serwerze Exchange 2000, widoczny stanie się spadek wydajności, ponieważ biblioteka będzie skanowała wszystkie wiadomości docierające do WSS. Załączniki są zapisywane w tabeli załączników, a użytkownicy chcący uzyskać załącznik mogą użyć odpowiedniego wskaźnika.

Wielu producentów nie stworzyło jeszcze oprogramowania antywirusowego, które mogłoby być zainstalowane bezpośrednio na serwerze Exchange 2000, i które byłoby kompatybilne z interfejsem API do wyszukiwania wirusów. Z tego powodu zalecane jest wdrożenie programów antywirusowych na wszystkich proxy lub bramach SMTP, a nawet na samych stacjach roboczych. W Exchange 2000 nie jest możliwe zapisywanie informacji o wiadomościach zawierających wirusy, a co gorsza, zaszyfrowane wiadomości nie będą skanowane przez interfejs API, chyba że zostaną one odszyfrowane wraz z załącznikami.

Lepszym rozwiązaniem jest instalacja oprogramowania antywirusowego lub śledzącego konie trojańskie bezpośrednio na serwerach, a nie na stacjach roboczych, ponieważ działanie procesu skanowania na serwerze powoduje redukcję ruchu sieciowego. Drugą przyczyną jest fakt, iż obecność wirusa w załączniku wiadomości wysyłanej do wielu osób spowoduje wywołanie tylko jednego alarmu, a nie wielu (co może się zdarzyć, jeśli zarażone wiadomości dotrą do komputerów użytkowników).

Należy upewnić się, czy wszyscy pracownicy firmy mają niezbędną wiedzę na temat wirusów i sposobów ich rozprzestrzeniania się przy użyciu typowych programów pocztowych, takich jak Outlook 2000 i Outlook Express. Nie wszystkie wirusy mogą rozprzestrzeniać się poprzez pocztę elektroniczną, ponieważ zostały napisane w językach skryptowych (na przykład JavaScript lub VBScript). Użytkownicy powinni znać różnicę pomiędzy wirusami i robakami. Robak to program, który automatycznie rozprzestrzenia się poprzez połączenia sieciowe (bez bezpośredniego wpływu użytkownika). Konie trojańskie wymagają wykonania jakiejś czynności przez użytkownika, takiej jak kliknięcie pliku EXE, dzięki czemu możliwe będzie uruchomienie złośliwej aplikacji w środowisku sieciowym. Większość istniejących obecnie wirusów ma formę robaka lub konia trojańskiego; ironią jest to, iż wiele programów antywirusowych nie pozwala na dokładne wyszukiwanie koni trojańskich, które mogą zawierać złośliwego robaka zarażającego automatycznie i bez wiedzy użytkownika wrażliwe systemy komputerowe.

Aby lepiej poznać różnice między poszczególnymi typami wirusów, zalecamy odwiedzenie stron internetowych producentów oprogramowania, na przykład *www.mcafee.com* lub *www.symantec.com*. Aktualne informacje na temat kwestii zabezpieczeń można znaleźć na stronie *www.symantec.com/avcenter/security*.

Wyszukiwanie wirusów na stacjach roboczych użytkowników jest praktyką wykonywaną przez większość administratorów Exchange. Wiele klienckich programów antywirusowych próbuje sprawdzać wszystkie zapisywane na dysk pliki pod kątem obecności w nich znanych sygnatur wirusów. Zalecane jest użycie programów pocztowych z wbudowanymi funkcjami zabezpieczeń, jak, na przykład, Outlook. Jeśli wykorzystywany jest Outlook 2000 SR-1, możliwe jest automatyczne zapisywanie na dysku niektórych plików załączników przed ich otwarciem przez użytkownika. Niezależnie od wykorzystywanego programu pocztowego, należy pamiętać o aktualizacji oprogramowania antywirusowego; na przykład firma Symantec udostępnia funkcję LiveUpdate do aktualizacji programów na komputerach z dostępnym połączeniem internetowym.

Ponieważ wirusy zyskały tak wielką popularność, Microsoft wprowadził w 1999 r. poprawkę Attachment Security Patch dla Outlooka w wersjach 97, 98 i 2000, która wymusza zapisanie na dysku niektórych załączników przed ich uruchomieniem lub otwarciem. W czerwcu 2000 r. Microsoft udostępnił aktualizację Outlook Email Security Update, która nie tylko blokuje dostęp użytkowników do złośliwych typów plików, ale wyświetla ostrzeżenia przy próbie uzyskania dostępu do informacji w Outlooku przez złośliwy kod. Ta aktualizacja zapewnia następujące funkcje zabezpieczeń:

- Zwiększony poziom domyślnych zabezpieczeń — domyślne ustawienie strefy zabezpieczeń internetowych zostało zmienione z *Internet* na *Witryny z ograniczeniami*. Na tym poziomie wyłączone są domyślnie aktywne skrypty.
- Dozór modelu obiektu — wyświetlane jest ostrzeżenie, jeśli zewnętrzny program próbuje uzyskać dostęp do książki adresowej Outlooka.
- Zabezpieczenia załączników emailowych — uniemożliwia dostęp do niektórych typów plików, jeśli zostały one wysłane w formie załączników emailowych. Obejmuje to pliki wykonywalne oraz pliki *.vbs* (pliki skryptów VBScript).

Użycie Outlook Email Security Update spowoduje spadek wydajności Outlooka, ponieważ zapewniany jest wyższy poziom zabezpieczeń. Należy jednak zauważyć, iż ta aktualizacja nie rozwiązuje pewnych słabych punktów w samym Outlooku.

Należy pamiętać, iż bezpieczeństwo Outlooka jest zależne od używanej wersji i zainstalowanych aktualizacji. Przykładem może być Outlook 2000, który jest bardziej wrażliwy na zagrożenia, gdyż udostępnia więcej funkcji programowania, niż wcześniejsze wersje. Outlook 97 nie potrafi interpretować nawet prostych poleceń HTML, dzięki czemu ryzyko zarażenia wirusem jest o wiele niższe niż w przypadku Outlooka 2000. Przeglądanie wiadomości tekstowych lub w formacie RTF (Rich Text Format) jest zawsze bezpieczne; zagrożenie mogą spowodować jedynie załączniki do takiej poczty. Wiadomości HTML stanowią znaczne zagrożenie, chyba że strefy zabezpieczeń w przeglądarce internetowej zostaną prawidłowo skonfigurowane. Wiadomości tego typu mogą zawierać złośliwe skrypty lub elementy sterujące ActiveX, które są ukrytymi wirusami. Elementy ActiveX będą zawsze uruchamiane automatycznie, chyba że zostanie wyłączona odpowiednia opcja w ustawieniach przeglądarki.

W celu zabezpieczenia systemu należy wyłączyć domyślne działanie plików VBScript (z rozszerzeniem *.vbs*) oraz zablokować Windows Script Host, który stanowi bramę wejściową dla robaków VBS. Więcej informacji na temat tych czynności można znaleźć na stronie *www.zdnet.com/zdhelp/stories/main/0,5594,2568111,00.html*.

Kwestie związane z DNS i TCP/IP

W czasie monitorowania i rozwiązywania problemów związanych z Exchange 2000 należy pamiętać o powiązaniach i zależnościach między serwerem Exchange i usługą DNS zapewnianą przez Windows 2000 Server. Zarówno DNS, jak i serwer Exchange korzystają z usług stosu protokołów TCP/IP. Nie jest możliwa instalacja Exchange 2000 bez Active Directory, a Active Directory nie będzie działać prawidłowo bez DNS. Istnieją jednak również inne przyczyny, dla których Exchange 2000 jest zależny od tej usługi. Serwery Exchange wykorzystują usługę DNS do przeszukiwania serwerów katalogu globalnego w lesie Windows 2000, a także do wyszukiwania adresów innych serwerów obsługi

wiadomości. DNS jest niezbędny za każdym razem, kiedy Exchange wysyła wiadomość. Inne zastosowania usługi DNS obejmują trasowanie wiadomości, komunikację między frontonem i zapleczem, a także obsługę błyskawicznych wiadomości.

Użycie DNS do zapytań Active Directory

Wszystkie obiekty w środowisku obsługi wiadomości znajdują się w bazie danych Active Directory na serwerze Windows 2000. Obejmuje to wszystkie serwery skrzynek pocztowych, foldery publiczne, użytkowników i łączniki. Serwery Exchange regularnie wykorzystują te informacje poprzez usługę DNS w celu wyszukania konkretnych rekordów zasobów (rekordy SRV) oraz poprzez zapytania serwerów protokołu LDAP. Większość serwerów katalogu globalnego jest używana do jednoczesnej obsługi rekordów SRV i protokołu LDAP. Nie jest wprawdzie wymagane użycie serwera katalogu globalnego do obsługi LDAP, ale Exchange będzie szukał serwera tego typu. Z tego powodu wielu administratorów łączy wszystkie te funkcje na jednym serwerze katalogu globalnego. Taki serwer przechowuje rekordy właściwości i informacje odnoszące się do struktury Active Directory, włączając w to nazwy lokalizacji i domen. Serwer Exchange 2000 wyszukujący rekordy SRV na serwerze DNS „wie", iż zawierają one pełną złożoną nazwę domeny kontrolera domeny, który działa jako serwer katalogu globalnego. Zapytanie o nazwę serwera katalogu globalnego zwraca również jego adres IP.

Większość zapytań DNS jest zwykle umieszczana w pamięci podręcznej serwera Exchange, dzięki czemu kolejne zapytania serwera DNS będą trwały krócej. Ten okres jest znany jako czas życia (ang. *Time To Live* — TTL); TTL decyduje o czasie ważności odpowiedzi na zapytanie DNS.

DNS używany w konfiguracji frontonu i zaplecza

Architektura frontonu i zaplecza może być wprowadzona, jeśli wielu użytkowników uzyskuje dostęp do serwera skrzynek pocztowych lub folderów publicznych poprzez firewall lub serwer proxy. Taka konfiguracja frontonu i zaplecza wykorzystuje DNS do zapytań Active Directory o serwer zawierający skrzynkę pocztową użytkownika lub folder publiczny. Wyobraź sobie, iż serwer frontonu otrzymuje poprzez Internet wiadomość od jednego z pracowników, który pracuje w domu i używa połączenia modemowego w celu połączenia się z siecią. Serwer frontonu próbuje znaleźć właściwy serwer zaplecza ze skrzynką pocztową tego użytkownika, dzięki czemu może przekazać dalej wiadomość. Jest to wykonywane poprzez wysłanie zapytania do Active Directory i przeszukanie DNS w celu znalezienia serwera LDAP (jak wspomniano wcześniej, prawdopodobnie będzie to serwer katalogu globalnego). Serwer frontonu wysyła zapytanie do serwera DNS o nazwę i adres IP serwera zaplecza lub wykorzystuje przyczółkowy serwer pocztowy do przekazania wiadomości do odpowiedniej skrzynki. Serwery frontonu nie tylko przekazują wiadomości odebrane z Internetu, ale również odczytują wiadomości bezpośrednio z serwera zaplecza. Zdarza się to za każdym razem, kiedy użytkownik, korzystając z protokołów HTTP, POP3 lub IMAP4, uzyskuje dostęp do informacji już zapisanych w Information Store na serwerze ze skrzynką pocztową użytkownika. Serwer frontonu wyszukuje w Active Directory nazwę serwera zaplecza, a następnie pobiera jego adres IP z serwera DNS. Jeśli uzyska się odpowiednie informacje, nawiązana zostaje bezpośrednia komunikacja między serwerami frontonu i zaplecza (pod warunkiem iż połączenie klienta pozostaje aktywne).

Integracja usługi Active Directory z istniejącymi serwerami DNS

Czasami konieczna będzie integracja usług Active Directory z istniejącym serwerem opartym na systemie Windows NT lub innym systemie operacyjnym. W takim przypadku konieczne jest zapewnienie obsługi Active Directory i powiązanych rekordów SRV przez serwer DNS. Dobrym pomysłem będzie także zaplanowanie funkcji dynamicznej aktualizacji DNS w Windows 2000. Wprowadzenie usług Active Directory do istniejącej infrastruktury DNS oznacza konieczność wykorzystania nowej przestrzeni nazw Active Directory. Ta nowa przestrzeń nazw może albo zostać dołączona do już istniejącej przestrzeni nazw DNS, albo ją zastąpić. Wybór właściwej drogi jest zależny od tego, czy usługi DNS są zapewniane przez serwer z systemem Windows NT 4, czy też komputer z inną wersją oprogramowania do obsługi DNS.

Przykładem oprogramowania do obsługi DNS, które nie pochodzi z Microsoftu, jest pakiet METAIP 4.1 DHCP/DNS firmy Checkpoint Software, który integruje usługi DHCP i DNS na jednym komputerze, zapewniając jednocześnie uwierzytelnianie RADIUS oraz funkcję przeszukiwania LDAP.

Jeśli w organizacji wykorzystywane są usługi DNS systemu Windows NT 4, zalecana jest aktualizacja sieci do Windows 2000. Implementacja DNS Microsoftu jest oparta na oprogramowaniu Berkeley BIND 8.x. Jeśli usługi DNS są zapewniane przez oprogramowanie innych firm, należy sprawdzić możliwość aktualizacji do wersji Windows 2000, która obsługuje rekordy SRV i dynamiczną aktualizację. W przypadku gdy taka możliwość nie występuje, może być konieczne dodanie kolejnego serwera DNS, który zapewnia takie funkcje, a następnie delegacja niektórych stref DNS do nowego serwera.

Rekordy SRV w DNS odnoszą się do rekordów zasobów, które wskazują położenie serwera konkretnego protokołu oraz domeny. Ten typ rekordu DNS pozwala administratorom na użycie wielu serwerów w danej domenie, dzięki czemu możliwe jest przenoszenie usług między serwerami bez większego wysiłku. Możliwe jest również wyznaczenie jednego komputera jako głównego serwera dla danej usługi (na przykład, FTP), a pozostałych serwerów w domenie jako serwerów zapasowych. Rekordy SRV rozwiązują problem związany z koniecznością posiadania dokładnego adresu serwera w celu skontaktowania się z nim.

Jeśli w sieci znajdują się serwery DNS nie oparte na systemie Microsoftu (na przykład, serwery Unix), należy powoli wprowadzać serwery DNS Windows 2000 jako serwery drugorzędne, dzięki czemu będzie możliwy transfer stref. Taki proces powinien zakończyć się bez zniszczenia lub uszkodzenia powiązanych rekordów zasobów. Po wykonaniu procesu transferu możliwa jest aktualizacja drugorzędnych stref DNS do strefy zintegrowanej z Active Directory, a następnie bezpieczne usunięcie z sieci głównych serwerów DNS. Wybierając lub konfigurując strefy, należy pamiętać, iż dostępne są następujące typy stref:

- *Standardowa strefa główna* — główna kopia nowej strefy zapisana w standardowym pliku tekstowym. Możliwe jest zarządzenie strefą główną na tym samym komputerze, na którym została utworzona.
- *Standardowa strefa drugorzędna* — replika lub kopia istniejącej strefy; strefy tego typu mają atrybut tylko do odczytu i są zapisane w standardowym pliku tekstowym. Nie jest możliwa konfiguracja strefy drugorzędnej bez wcześniejszej konfiguracji strefy głównej. Tworząc strefę zapasową, należy podać główny serwer, który może przekazać informacje strefy do serwera DNS zawierającego standardową strefę drugorzędną.

- *Strefa zintegrowana z Active Directory* — główna kopia nowej strefy; wykorzystuje usługi Active Directory do replikacji plików strefy. W przypadku tego typu strefy nie występują standardowe transfery strefy, gdyż pliki strefy są replikowane wraz z replikacją bazy danych Active Directory.

Przy wdrażaniu Exchange 2000 w nowym środowisku Active Directory lub Windows 2000 z DNS celem administratora powinno być zaprojektowanie wydajnej topologii replikacji, przy jednoczesnej minimalizacji ogólnego ruchu replikacji. Można to osiągnąć poprzez właściwą konfigurację domeny i topologii lokalizacji w taki sposób, aby każda domena Active Directory była powiązana z jedną strefą DNS. Takie strefy są zwykle umieszczane na serwerze DNS, który działa na kontrolerze domeny lub serwerze katalogu globalnego w tej domenie. Wszystkie strefy powinny być zintegrowane z Active Directory (opisano to w ostatnim punkcie wcześniejszej listy). Serwery DNS należy zaplanować z uwzględnieniem kwestii odporności na awarie. Oznacza to użycie co najmniej dwóch kontrolerów domeny w każdej domenie (lub co najmniej jednego kontrolera domeny w każdej lokalizacji Windows 2000).

Exchange 2000 i TCP/IP

Wszystkie usługi wykorzystywane przez Exchange 2000 są zależne od działania stosu protokołów TCP/IP. Nawet macierzysty protokół transportowy SMTP jest członkiem takiego stosu, podobnie jak NNTP i HTTP. Proste problemy z połączeniami z innymi komputerami mogą być rozwiązane przy użyciu narzędzia wiersza poleceń PING. Do tego celu konieczne jest podanie znanego adresu IP, co przedstawiono na poniższym przykładzie:

```
c:/>PING 10.2.24.128
```

Systemy Exchange 5.5 i Exchange 2000 korzystają z różnych portów TCP i UDP (zobacz tabela 9.1).

Tabela 9.1. *Porty używane przez Exchange 5.5 i Exchange 2000*

Numer portu	Nazwa protokołu lub usługi korzystającej z tego portu
25	Usługa SMTP
53	Usługa DNS
80	Protokół HTTP
102	Usługa X.400
135	Usługa RPC (zdalne wywołanie procedury)
143	Usługa IMAP4
110	Usługa POP3
119	Usługa NNTP
389	Protokół LDAP
443	HTTP z SSL
465	SMTP z SSL
563	NNTP z SSL
993	IMAP4 z SSL
995	POP3 z SSL
6667	Protokół IRC

Wiedza na temat portów używanych przez różne usługi i protokoły jest bardzo przydatna przy rozwiązywaniu problemów z niektórymi usługami, które nie działają prawidłowo. Taka sytuacja może wystąpić, jeśli dwie usługi korzystają z portu o tym samym numerze lub jeśli używany jest port zarezerwowany dla innej usługi. W ramce poniżej przedstawiono numery portów wykorzystywane przez konie trojańskie, takie jak Deep Throat i Happy99.

Porty używane przez znane konie trojańskie

Konie trojańskie mogą wykorzystać dowolny port TCP lub UDP na większości systemów komputerowych, ale część z nich kieruje się do zarezerwowanych portów TCP i UDP, takich jak 31337 lub 12345. Czasami można wykryć również próby ataku na porty TCP i UDP, które zwykle nie są używane. Może świadczyć to o obecności złośliwego użytkownika, który próbuje połączyć się z koniem trojańskim wewnątrz sieci lokalnej. Tabela 9.2 przedstawia niektóre domyślne porty używane przez niektóre dobrze znane konie trojańskie (stan na początek 2001 r.). Nie oznacza to, iż ta lista jest pełna; więcej informacji na temat numerów portów używanych przez konie trojańskie można znaleźć na stronie *www.sans.org*.

Dla przykładu, protokół POP3 z SSL korzysta z portu 995, podobnie jak protokół IRC z SSL. Możliwa jest zmiana numerów portów w przypadku powstania konfliktu lub jeśli wybrana grupa użytkowników ma łączyć się przy użyciu określonego protokołu, takiego jak X.400. Administrator może nawet skonfigurować firewall w taki sposób, aby odrzucane były wszystkie próby uzyskania dostępu do portu używanego domyślnie przez serwer Exchange (przykład takiego rozwiązania można znaleźć w podrozdziale *Ustawienie numerów portów TCP/IP dla firewalla w środowisku Exchange w trybie mieszanym*). Tabela 9.3 przedstawia listę portów TCP/IP, które są używane wyłącznie przez Exchange 2000 i Windows 2000.

Kwestie związane z delegacją praw

W tym podrozdziale zostaną omówione trzy tematy odnoszące się do przekazania kontroli nad serwerem Exchange 2000 dla wybranych użytkowników w organizacji. Omówiona zostanie również kwestia zabezpieczenia środowiska Exchange poprzez przyznanie użytkownikom ograniczonego dostępu do informacji znajdujących się na serwerze.

Wszystko zaczęło się od projektu Active Directory...

Każde wdrożenie Exchange 2000 rozpoczyna się od właściwego zaplanowania Active Directory. Przedstawiliśmy już kwestie tworzenia domen, lokalizacji i jednostek organizacyjnych, a także wyjaśniliśmy różnice między fizycznym obiektem Active Directory (takim jak domena) a logicznym obiektem (na przykład, jednostka organizacyjna). Zakładamy, iż organizacja została zaprojektowana z uwzględnieniem struktury *geopolitycznej*. Domeny zostały utworzone zgodnie z rozmieszczeniem lokalizacji, co pomogło w utworzeniu jednostek organizacyjnych wewnątrz tych domen. Skonfigurowano następnie kreatora *Delegation of Control Wizard* w celu przydzielenia wybranym użytkownikom lub grupom uprawnień do tych obiektów jednostek organizacyjnych. Infrastruktura Active Directory nabrała kształtu. W czasie fazy projektowania Active Directory uwzględniono następujące kwestie:

Tabela 9.2. *Numery portów używane przez niektóre konie trojańskie*

Nazwa konia trojańskiego	Używany port TCP
Death	port 2
Senna Spy FTP Server	port 20
Blade Runner	port 21
Fire HacKer	port 23
Happy99, Antigen	port 25
Deep Throat	port 41
DMSetup	port 59
Firehotcker	port 79
CGI Backdoor, RingZero	port 80
Hidden Port	port 99
ProMail Trojan	port 110
Happy99	port 119
NetTaxi	port 142
Infector	port 146
Backage	port 334
TCP Wrappers Trojan	port 421
RPC Backdoor	port 514
Net Administrator, Phase Zero	port 555
Secret Service	port 605
Attack FTP, Cain & Abel	port 666
AimSPY	port 777
Dark Shadow	port 911
Doly Trojan	porty 1010, 1011, 1012, 1015 i 1016
WinHole	porty 1080, 1081, 1082 i 1083
Remote Administration Tool (RAT)	porty 1095, 1097, 1098 i 1099
BackDoor-G, SubSeven	port 1243
VooDoo Doll	port 1245
Matrix	port 1269
Millenium Worm	port 1338

- Utworzono globalne grupy zabezpieczeń wewnątrz jednostek organizacyjnych, dzięki czemu przydzielanie uprawnień jest prostym zadaniem; użytkownicy mogą być z łatwością dodawani lub usuwani z grup.
- Wszystkie serwery komunikujące się ze sobą umieszczono w tej samej lokalizacji Windows 2000, ponieważ wymagają one szybkiego połączenia między sobą; dzięki takiemu postępowaniu zredukowano również ruch replikacji.
- W każdej lokalizacji Active Directory umieszczono co najmniej dwa serwery katalogu globalnego w celu obsługi procesu logowania oraz zapewnienia odporności na awarie.

Tabela 9.3. *Lista portów używanych przez Exchange 2000 i Windows 2000 Server*

Numer portu	Nazwa protokołu lub usługi korzystającej z tego portu
80	Usługa IM otwierająca sesję przy użyciu protokołu RVP (Rendezvous Protocol)
88	Protokół uwierzytelniania Kerberos
379	Usługa replikacji lokalizacji korzystająca z protokołu LDAP
522	Usługa User Locater dla Microsoft NetMeeting
691	Usługa aktualizacji informacji stanu łącza
995	Protokół POP3 lub IRC z SSL
1720	Usługa wideokonferencji
1731	Usługa audiokonferencji
3268	Wyszukiwanie LDAP na serwerach katalogu globalnego
3269	Wyszukiwanie LDAP na serwerach katalogu globalnego z włączonym SSL

- Zawsze wybierano hierarchię jednostek organizacyjnych, a nie hierarchię domeny, ponieważ przenoszenie użytkowników lub grup między różnymi jednostkami organizacyjnymi jest łatwiejsze, niż przenoszenie tych obiektów między różnymi domenami. Łatwiejszy jest również proces przydzielania uprawnień dla jednostki organizacyjnej, niż dla domeny.

... po czym nadeszło zarządzanie systemem Exchange

Po wdrożeniu wszystkich elementów Active Directory kolejna logiczna faza instalacji Exchange 2000 koncentruje się wokół tworzenia i wdrożenia grup administracyjnych i grup magazynowania w celu dalszej delegacji uprawnień do serwera Exchange. Schemat Active Directory został zaktualizowany poprzez uruchomienie programu instalacyjnego z przełącznikiem */ForestPrep*. W ten sposób zostały utworzone wszystkie grupy serwera Exchange, a także obiekt *Organization* w kontekście nazewnictwa Active Directory. Instalacja Exchange 2000 utworzyła również domyślną grupę administracyjną o nazwie *First Administrative Group*, która nie była widoczna aż do momentu włączenia jej we właściwościach obiektu organizacyjnego w przystawce MMC *System Manager*. Lokalizacje Exchange 5.5 nie będą funkcjonowały już jako zakresy administracyjne w organizacjach z Exchange 2000, ponieważ zostały zastąpione przez grupy administracyjne z serwerami. Zarządzanie systemem obejmuje teraz tworzenie jednostki organizacyjnej, tworzenie grupy wewnątrz tej jednostki, umieszczenie w grupie kont do zarządzania, a następnie przydzielenie tej grupy do grupy administracyjnej. Po rozmieszczeniu grup administracyjnych możliwe jest przekazanie kontroli nad nimi różnym administratorom w organizacji poprzez użycie kreatora *Delegation of Control Wizard* dla każdej grupy administracyjnej w System Managerze. Dla każdej grupy tego typu możliwe jest przydzielenie jednej z trzech ról administracyjnych:

- *Exchange View Only Administrator* — pozwala użytkownikom na przeglądanie informacji konfiguracji, ale nie umożliwia dokonywania jakichkolwiek zmian.
- *Exchange Administrator* — pozwala użytkownikom na pełną administrację serwerem Exchange, ale bez możliwości modyfikacji uprawnień.

- *Exchange Full Administrator* — pozwala użytkownikom na pełną administrację serwerem Exchange oraz na modyfikację uprawnień. Dzięki tej opcji użytkownicy mogą kontrolować dostęp do Exchange 2000.

Delegacja kontroli

Kreator *Delegation of Control Wizard* kontroluje dostęp do Exchange, nie przyznając nikomu lokalnego dostępu administracyjnego ani praw do modyfikacji lokalnego rejestru. Jeśli użytkownik potrzebuje takich praw, musi stać się członkiem grupy lokalnych administratorów dla komputera, którym chcą zarządzać. Delegacja kontroli do użytkownika lub grupy nie oznacza jednak, iż ten użytkownik lub grupa muszą być członkiem globalnej grupy zabezpieczeń, takiej jak Domain Admins lub Enterprise Admins. Należy jednak kontrolować poziom, na jakim delegowane są uprawnienia, ponieważ użycie kreatora *Delegation of Control Wizard* na poziomie *Organization* oznacza, iż użytkownicy uzyskają pewne prawa administracyjne w całej strukturze organizacji.

Oprócz trzech opisanych wcześniej ról możliwe jest także przydzielenie użytkownikom lub grupie roli *menedżera skrzynki pocztowej*, dzięki czemu będą mogli włączać obsługę skrzynek pocztowych dla innych użytkowników i grup. Aby uzyskać tę rolę, należy jednak umieścić użytkownika w lokalnej grupie zabezpieczeń Account Operators.

Konieczne jest również zdefiniowanie limitów dostępu i zasad w grupach magazynowania na każdym serwerze. Grupy magazynowania pozwalają na umieszczenie wielu prywatnych i publicznych baz danych na każdym serwerze. Każdy serwer może zawierać nie więcej niż cztery takie grupy, a w każdej grupie może znaleźć się maksymalnie pięć baz danych. Każdy serwer Exchange 2000 uruchamia tylko jeden egzemplarz usługi *Store.exe*, w ramach której mogą funkcjonować grupy magazynowania. Każda grupa stanowi pojedynczy egzemplarz struktury bazy danych ESE (Extensible Storage Engine). Obsługuje on wszystkie bazy danych w danej grupie magazynowania. Niezależnie od liczby baz danych w grupie, każda grupa musi być powiązana tylko z jednym zestawem plików dziennika transakcji. Każda grupa magazynowania powinna zawierać inną klasę użytkowników lub grup i być skonfigurowana dla różnych odbiorców i zasad serwera. Dostępne zasady obejmują ustawienia maksymalnej wielkości wiadomości i skrzynek pocztowych, a także okres przechowywania usuniętych wiadomości. Głównym celem tej fazy zarządzania serwerem jest umieszczenie w grupach magazynowania wszystkich użytkowników według ich typu, w efekcie czego zostanie zachowana funkcja Exchange pozwalająca na magazynowanie wyłącznie jednego egzemplarza. Dzięki takiemu postępowaniu każdy magazyn Information Store będzie zawierał tylko jedną kopię fizyczną każdej wiadomości, podczas gdy adresaci będą korzystali ze wskaźników do tych wiadomości.

Jeszcze bardziej szczegółowa kontrola nad Exchange 2000

Możliwe jest zdefiniowanie kontroli nad elementami Active Directory i obiektami Exchange 2000, takimi jak grupy magazynowania i jednostki administracyjne. Jeszcze bardziej szczegółowe poziomy dostępu mogą być skonfigurowane poprzez ograniczenie sposobów, w jaki wybrani użytkownicy mogą przeglądać informacje. Aby tego dokonać, konieczne jest zarządzanie widokami globalnej listy adresowej (GAL) i widokami folderów publicznych.

Model kontroli dostępu wykorzystywany przez Exchange 2000 przypomina model znany już z Windows 2000 Server. Ten system operacyjny umożliwia kontrolę dostępu do większości obiektów w sieci poprzez przydzielenie *deskryptorów zabezpieczeń* dla obiektów w Active Directory. Taki deskryptor zawiera listę wszystkich użytkowników, którzy mają dostęp do obiektu, a także uprawnienia przyznane tym osobom. Model kontroli dostępu w Exchange 2000 różni się od modelu w Exchange 5.5; kontrola jest możliwa na różnych poziomach obiektu, włączając w to poziom kontenera, elementu lub właściwości. Główna różnica między metodami kontroli dostępu w obu tych systemach obsługi wiadomości polega na tym, iż Exchange 2000 korzysta z bardziej bezpośredniego powiązania pomiędzy kontem użytkownika w Active Directory i skrzynką pocztową dla tego konta, która znajduje się na serwerze Exchange.

Główną przyczyną, dla której należy zdefiniować taką kontrolę dla listy GAL, jest fakt, iż domyślnie zawiera ona widok wszystkich obiektów z obsługą poczty w organizacji, a czasami nie wszyscy użytkownicy powinni mieć dostęp do informacji tego typu. Lista GAL pozwala użytkownikom na przeszukiwanie Active Directory przy użyciu LDAP na porcie 389, a także łączy informacje ze wszystkich serwerów katalogu globalnego w lesie Windows 2000. Utworzenie pewnego typu partycji wewnątrz listy GAL spowoduje ograniczenie informacji dostępnych dla użytkowników, dzięki czemu nie będą oni przytłoczeni ogromną liczbą danych w czasie wyszukiwania użytkownika lub grupy. Oznacza to, iż możliwe jest utworzenie wielu list GAL, z których każda będzie zawierała oddzielne zasady kontroli dostępu dla różnych klas użytkowników.

Filtrowanie widoków GAL może ułatwić pracę administratora, aczkolwiek może spowodować pewien problem. Wyobraź sobie, iż Jan i Marek są wewnętrznymi użytkownikami tego samego systemu pocztowego, ale znajdują się w różnych grupach administracyjnych lub jednostkach organizacyjnych. Lista GAL jest filtrowana, dzięki czemu każdy użytkownik widzi w programie Outlook inną część GAL. Kiedy Jan próbuje wysłać wiadomość do Marka, używając tylko jego nazwiska, Outlook odrzuci tę wiadomość, jeśli Marek nie pojawi się na liście GAL Jana. Nadawca może rozwiązać ten problem poprzez użycie adresu proxy SMTP adresata, a nie jego nazwiska.

Także foldery publiczne często sprawiają problemy administratorom, ponieważ służą one za „śmietnik" dla danych, które nie są ważne lub nie powinny znaleźć się w tym miejscu. Użytkownicy postrzegają takie foldery jako miejsce magazynowania niepotrzebnych emaili lub dokumentów. Hierarchia folderów publicznych powinna składać się z folderów macierzystych i potomnych. Dla przykładu, folder macierzysty może otrzymać nazwę Sprzedaż, podczas gdy jego foldery potomne otrzymają nazwy zgodne z regionami działu sprzedaży, takimi jak Północ, Zachód, itp. Exchange 2000 zapewnia wiele sposobów konfiguracji dostępu do folderów publicznych poprzez przeglądanie właściwości każdego folderu w System Managerze. Dostępne opcje obejmują m.in. ukrycie folderu publicznego na wszystkich listach adresowych lub ukrycie go dla wszystkich użytkowników, którzy nie mają właściwych praw dostępu.

Kwestie związane z migracją serwera Exchange 5.5

W tym podrozdziale zostaną omówione kwestie migracji, włączając w to współpracę między serwerami Exchange 5.5 i Exchange 2000, a także planowanie i konfigurację łącznika ADC w Exchange 2000. Obie te kwestie występują w organizacjach Exchange trybu mieszanego i są związane z użyciem obiektów znanych jako *umowy połączenia*.

W organizacji trybu mieszanego używane są serwery zarówno Exchange 2000, jak i Exchange 5.5. Decydując się na aktualizację lub migrację organizacji do najnowszej wersji Exchange, należy przenieść wszystkie informacje katalogowe Exchange 5.5 do bazy danych Active Directory w Windows 2000. Migracja informacji oznacza ręczną replikację lub odtworzenie danych użytkowników i kontaktów, które były obsługiwane przez klasyczne serwery Exchange. Aby pomóc w przeprowadzeniu migracji, Microsoft dostarczył narzędzie ADC (Active Directory Connector), które działa na wszystkich serwerach Windows 2000 i pozwala na synchronizację oraz replikację informacji między katalogami Exchange 5.5 i Windows 2000. Najpierw zajmiemy się skutkami instalacji ADC, a następnie wykorzystamy uzyskane informacje w celu zapewnienia współpracy folderów publicznych w obu systemach obsługi wiadomości.

Łącznik ADC ma wersje dla Windows 2000 i Exchange 2000. Wersja Windows 2000 pozwala na replikację informacji obiektu między Exchange 5.5 i Active Directory, umożliwiając jednocześnie administratorowi Windows 2000 zarządzanie katalogiem Exchange 5.5. Łącznik ADC w Exchange 2000 replikuje te same informacje katalogowe, co wersja dla Windows 2000, ale umożliwia jednocześnie replikację danych konfiguracji między platformami Exchange.

Choć dostępne są dwie wersje łącznika ADC, nie oznacza to, iż należy zainstalować je jednocześnie. Prawdę mówiąc, w czasie instalacji Exchange 2000 łącznik ADC dla Windows 2000 (jeśli istnieje) jest zastępowany wersją dla Exchange 2000.

Konfiguracja replikacji między katalogami jest możliwa dzięki użyciu umowy połączenia. Replikacja takich informacji pozwala użytkownikom na wyszukiwanie w Active Directory obiektów znajdujących się na ich listach GAL. Lista GAL w Exchange 5.5 nie korzysta z Active Directory, ponieważ użytkownicy przeszukują bazę danych katalogu na serwerach Exchange 5.5. Należy pamiętać, iż podstawową funkcją Active Directory jest zastąpienie oryginalnego pliku bazy danych katalogu *DIR.EDB* na wszystkich serwerach Exchange 2000. Łącznik ADC może zarządzać jednocześnie kilkoma umowami połączenia; możliwa jest również konfiguracja wielu takich umów, nawet w przypadku istnienia tylko jednej lokalizacji Exchange 5.5. W idealnej sytuacji wiele umów połączenia powinno komunikować się z wieloma lokalizacjami Exchange 5.5.

Lokalizacja Exchange 5.5 różni się od lokalizacji Windows 2000. Pierwszy typ lokalizacji to fizyczny zakres definiowany przez grupę serwerów Exchange 5.5, które komunikują się ze sobą poprzez szybkie połączenie sieciowe. Lokalizacja Windows 2000 odnosi się do zakresu podsieci IP składających się z serwerów, które także komunikują się poprzez szybkie łącza. Exchange 5.5 umieszcza oddzielne magazyny katalogu na każdym serwerze, podczas gdy Windows 2000 integruje wszystkie obiekty w centralnym katalogu Active Directory.

Wszystkie umowy połączenia zawierają różne informacje, takie jak docelowe serwery, replikowane obiekty oraz terminarz replikacji. Bardzo ważną kwestią jest zdefiniowanie kierunku replikacji, ponieważ możliwe jest wykonanie tego procesu zarówno *z* katalogu Exchange 5.5, jak i *do* niego. Exchange 5.5 jest mniej elastyczny, ponieważ do magazynowania większości danych adresatów używany jest tylko jeden kontener; zwykle jest to kontener *Recipients* w narzędziu Exchange 5.5 Administrator. Exchange 2000 pozwala na utworzenie wielu kontenerów w Active Directory — są to kontenery jednostek organizacyjnych. Ta sytuacja ma wpływ na tworzone umowy połączenia; należy pamiętać, iż administrator nie jest zmuszony do replikacji obiektów tylko do jednego kontenera.

Możliwa jest synchronizacja wielu kontenerów *Recipients* z Exchange 5.5 do jednego kontenera Active Directory oraz replikacja wielu kontenerów Active Directory do jednego kontenera *Recipients* w Exchange 5.5.

Umowy połączenia mogą być definiowane jako jedno- lub dwukierunkowe. Jednokierunkowa umowa oznacza, iż informacje są replikowane z Exchange 5.5 do Active Directory lub odwrotnie. Dwukierunkowa umowa połączenia pozwala na replikację danych w obu kierunkach. W większości przypadków wybierane są umowy jednokierunkowe, co pozwala na automatyczną aktualizację Active Directory po modyfikacji katalogu Exchange 5.5. Tylko jedna umowa połączenia jest wymagana do replikacji całej organizacji Exchange 5.5 do Active Directory, należy jednak rozważyć użycie wielu takich umów ze względu na długi czas replikacji, szczególnie w przypadku dużych lokalizacji Exchange 5.5. Użycie większej liczby umów połączenia do jednoczesnej replikacji grupy obiektów jest bardziej efektywne i redukuje ruch replikacji; ma to duże znaczenie w przypadku zaplanowania replikacji na okres poza szczytem. Zastosowanie umów połączenia oznacza także konieczność podjęcia decyzji o miejscu administracji większością obiektów katalogu. Jeśli zdecydowano się na administrację wszystkimi obiektami bezpośrednio z Active Directory, można do tego celu użyć przystawki *Active Directory Users and Computers*. W takiej sytuacji należy się upewnić, czy umowy połączenia są skonfigurowane jako jednokierunkowe oraz czy każda taka umowa ma prawa zapisu w każdym katalogu Exchange 5.5. To rozwiązanie pozwala na automatyczne zapisywanie i replikację w katalogach Exchange 5.5 wszystkich nowych obiektów utworzonych w Active Directory. Jeśli jednak zdecydowano się na użycie klasycznego programu Exchange 5.5 Administrator do zarządzania użytkownikami i grupami, to wszystkie umowy połączenia powinny być skonfigurowane jako jednokierunkowe do Active Directory; takie umowy nie muszą posiadać uprawnień zapisu do katalogu Exchange 5.5.

Najbardziej elastycznym rozwiązaniem będzie utworzenie w kontenerze *Recipients* w Exchange 5.5 oddzielnych podkontenerów dla użytkowników, grup lub list dystrybucyjnych, a następnie replikacja każdego podkontenera do powiązanego kontenera Active Directory przy użyciu oddzielnej umowy połączenia. Taki schemat pozwala na tworzenie nowych kont zarówno w Exchange 5.5, jak i Exchange 2000, szczególnie w przypadku użycia dwukierunkowych umów połączenia. Umowa tego typu przyznaje każdemu katalogowi uprawnienia zapisu w drugim katalogu. Poniżej przedstawiono najważniejsze zalecenia związane z tworzeniem umów połączenia:

- Jeśli istnieje tylko jedna lokalizacja Exchange 5.5, należy skonfigurować jednokierunkową umowę połączenia w celu zachowania tej samej konfiguracji w Active Directory.
- Każdy użytkownik z prawami Enterprise Admin lub Schema Admin może utworzyć nową umowę połączenia poprzez wskazanie magazynu katalogu Exchange 5.5 oraz usługi Active Directory w Windows 2000 jako dwóch końców połączenia.
- Wdrażając Exchange 2000, należy użyć łącznika ADC z Exchange 2000, ponieważ rozszerza on funkcje prostego łącznika ADC z Windows 2000, który jest instalowany wraz z systemem. ADC w Windows 2000 replikuje dane adresatów, podczas gdy ADC w Exchange 2000 replikuje także informacje konfiguracji.
- Exchange 2000 może bezpośrednio dostarczać wiadomości do serwerów Exchange 5.5 przy użyciu wywołań RPC (a nie protokołu SMTP), ponieważ dzięki specjalnym umowom połączenia Configuration Connection Agreement (ConfigCA) przechowuje informacje o konfiguracji Exchange 5.5.

Umowa ConfigCA replikuje informacje pomiędzy kontenerem *Configuration* w Exchange 5.5 i kontekstem nazewnictwa konfiguracji w Active Directory.

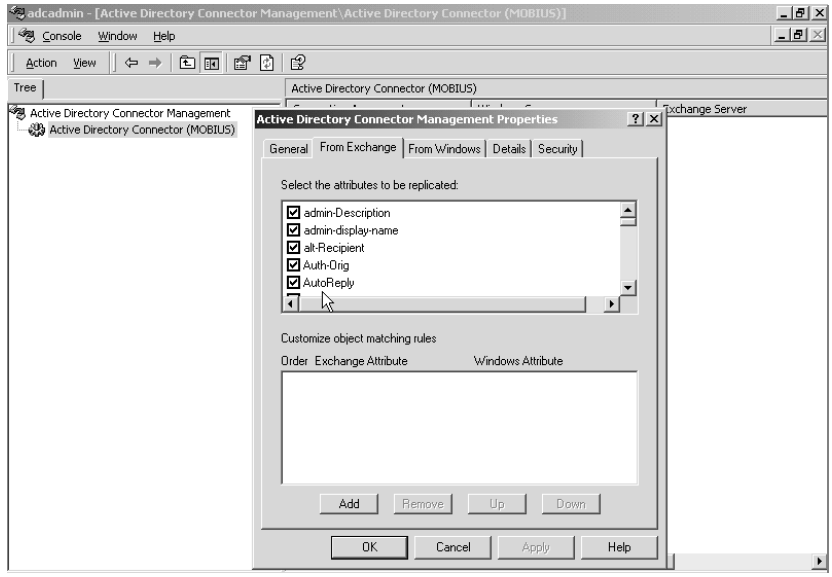
- Umowa ConfigCA jest tworzona automatycznie przy każdej aktualizacji serwera Exchange 5.5 do Exchange 2000 lub w czasie instalacji Exchange 2000 w lokalizacji Exchange 5.5. Tylko łącznik ADC z Exchange 2000 potrafi utworzyć umowę ConfigCA; łącznik ADC z Windows 2000 nie posiada takiej funkcji.
- Administrator powinien zdecydować się na wybór Active Directory lub Exchange 5.5 do zarządzania wszystkimi obiektami. Choć Active Directory potrafi zarządzać wszystkimi obiektami, czasami konieczne będzie użycie mieszanego trybu zarządzania. Jednoczesne użycie narzędzi Exchange 5.5 Administrator i Active Directory Users and Computers do modyfikacji atrybutów tego samego obiektu powoduje powstanie błędów lub konfliktów. W takiej sytuacji wybierane są ostatnie dokonane zmiany.
- Dwa główne typy umów połączenia, jakie są widoczne w przystawce MMC *Connector Management*, to umowy użytkowników i konfiguracji. Umowy połączenia użytkowników replikują obiekty adresatów i ich dane, podczas gdy umowy konfiguracji replikują informacje o konfiguracji Exchange 2000.

Łącznik ADC odgrywa ogromną rolę, ponieważ może być użyty do replikacji i synchronizacji skrzynek publicznych, folderów publicznych i innych ważnych danych systemowych. *Czas* replikacji jest jednak ważniejszy niż to, *co* jest replikowane. Możliwe jest ustawienie ADC na replikację nawet co 5 sekund, co wpływa jednak na wydajność sieci i serwera ze względu na zwiększone obciążenie procesora i większy ruch pakietów. ADC używa protokołu LDAP do uzyskania dostępu do różnych katalogów; częste zapytania LDAP mogą znacznie obniżyć wydajność w dużych sieciach.

Choć Microsoft zdecydowanie to odradza, możliwa jest modyfikacja rejestru w celu modyfikacji domyślnego okresu replikacji (co pięć sekund). Otwórz edytor rejestru i do klucza *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSADC\Parameters* dodaj wartość DWORD o nazwie *Synch Sleep Delay*. Wartość DWORD powinna być wyższa niż 5 sekund (na przykład, 600 sekund, czyli 10 minut), dzięki czemu wydłuża się interwał replikacji Exchange 2000.

Czytelnik może zastanawiać się, czy jest możliwa kontrola mapowania atrybutów indywidualnych obiektów, gdyż głównym celem łącznika ADC jest synchronizacja atrybutów obiektów pomiędzy katalogami Exchange 5.5 i Active Directory. *Atrybuty* to, między innymi, adresy, nazwy i numery telefoniczne dla różnych obiektów, takich jak użytkownicy. Microsoft stworzył przystawkę MMC do obsługi ADC o nazwie *Active Directory Connector Manager*, która zawiera wstępnie zdefiniowany zestaw atrybutów, jakie można włączyć to terminarza synchronizacji. Takie atrybuty (na przykład, nazwy i adresy) mogą być automatycznie synchronizowane z Active Directory po utworzeniu umowy połączenia między kontenerem Exchange 5.5 i docelowym kontenerem w Active Directory (takim jak jednostka organizacyjna). Aby zmienić domyślną listę i dodać własne atrybuty, należy zmodyfikować domyślną zasadę ADC przy użyciu przystawki *Active Directory Connector Manager*. Modyfikacja tej zasady oznacza dodanie atrybutów nie zsynchronizowanych automatycznie, ale także usunięcie atrybutów, które nie będą potrzebne w Active Directory (na przykład, w przypadku ich replikacji z alternatywnego źródła lub katalogu; mogą to być nazwy własnych adresatów, którzy nie będą mieli włączonej obsługi skrzynki pocztowej w Windows

2000). Rysunek 9.2 pokazuje atrybuty, jakie mogą być wybrane w czasie synchronizacji z Exchange 5.5 do Active Directory poprzez zakładkę *From Exchange* w przystawce *Active Directory Connector Manager*.



Rysunek 9.2. *Wybór atrybutów w zakładce From Exchange w przystawce Active Directory Connector Manager*

Wszystkie reguły mapowania atrybutów są definiowane poprzez zasadę *Default ADC Policy*. Łącznik ADC wymusza stosowania tych reguł dla każdej powiązanej umowy połączenia. Należy pamiętać, iż możliwe jest ustawienie oddzielnych reguł mapowania dla każdej konfigurowanej umowy połączenia. W momencie pierwszej instalacji łącznika ADC tworzone są tabele mapowania atrybutów przy wykorzystaniu plików tekstowych umieszczonych na płycie instalacyjnej Exchange 2000. Pliki te mają nazwy *local.map* i *remote.map* i umieszczone są w katalogu *ADC\i386*. W obu tych plikach można znaleźć reguły mapowania, które decydują o różnych atrybutach i ustawieniach zasady *Default ADC Policy*. Dla przykładu, pliki *local.map* decydują o atrybucie *msExchServer2SchemaMap*, który definiuje reguły mapowania atrybutów z Exchange 5.5 do Active Directory. Zwykle nie należy ingerować w reguły mapowania atrybutów powiązane z domyślną zasadą ADC, ponieważ wszystkie atrybuty obiektów w Exchange 5.5 są automatycznie powiązane ze swoimi odpowiednikami w Active Directory. Instalacja łącznika ADC definiuje domyślne mapowanie pomiędzy dwoma usługami katalogowymi.

Koniecznie trzeba zrozumieć różnice między środowiskami trybu mieszanego i macierzystego, gdyż odnoszą się one zarówno do Exchange 2000, jak i do Windows 2000 Server. Domena Windows 2000 trybu mieszanego implikuje obecność w tej samej domenie lub lesie kontrolerów domeny pracujących w systemach starszych niż Windows 2000. Organizacja Exchange 2000 trybu mieszanego implikuje koegzystencję z serwerami Exchange 5.5. Z kolei w domenie Windows 2000 w trybie macierzystym nie występują żadne kontrolery domeny z systemami starszymi niż Windows 2000, podczas gdy organizacja Exchange 2000 w trybie macierzystym oznacza brak jakichkolwiek serwerów Exchange 5.5. Możliwa jest instalacja platformy Exchange trybu mieszanego w macierzystej domenie Windows, podobnie jak instalacja Exchange trybu macierzystego w domenie Windows trybu mieszanego.

Inną ważną kwestią jest współpraca folderów publicznych w Exchange 5.5 i Exchange 2000. Pewne subtelne powiązanie łączy funkcję ADC z koncepcją przydzielania uprawnień do folderów publicznych w Exchange 2000. Aby zrozumieć to powiązanie, należy docenić zmiany w zakresie kontroli dostępu wymagane przez Exchange 2000. W przeciwieństwie do domeny Windows 2000 trybu mieszanego, domena Windows 2000 w trybie macierzystym umożliwia prawidłową administrację folderów publicznych w Exchange 2000.

Administracja folderami publicznymi zmieniła się od czasów Exchange 5.5. Istnienie środowiska Exchange trybu mieszanego wymaga replikacji i migracji folderów publicznych do Exchange 2000. Wcześniejszy opis umów połączenia może być rozciągnięty również na foldery publiczne, ponieważ ADC zapewnia specjalną umowę połączenia dla folderów publicznych (inne umowy połączenia obejmują umowy użytkowników i konfiguracji). Ta umowa połączenia jest odpowiedzialna za synchronizację adresów emailowych folderów publicznych Exchange 5.5 do Active Directory, co pozwala użytkownikom Exchange 2000 z włączoną obsługą skrzynek pocztowych na wysyłanie wiadomości emailowych do tych folderów publicznych (co było możliwe w Exchange 5.5). W czasie replikacji folderów publicznych między Exchange 5.5 i Exchange 2000 mogą wystąpić problemy, jeśli te obiekty służą jako adresaci dla list dystrybucyjnych Exchange 5.5. W trakcie konfiguracji umowy połączenia użytkowników w celu synchronizacji listy dystrybucyjnej Exchange 5.5 z Active Directory tworzony jest specjalny typ obiektu grupy o nazwie *uniwersalna grupa dystrybucyjna*. Nie jest jednak możliwe dołączenie do niej adresu emailowego folderu publicznego, chyba że został on konkretnie zdefiniowany w Active Directory, a umowy połączenia użytkowników nie są w stanie zdefiniować tego adresu. Z tego powodu istnieje konieczność utworzenia oddzielnej umowy połączenia dla folderów publicznych.

Początkowo umowy połączeń oferowały funkcję automatycznej replikacji adresów emailowych folderów publicznych. Niestety, opcja ta została usunięta w ostatniej chwili, co doprowadziło do powstania umów połączenia folderów publicznych.

Umowy połączenia adresów emailowych synchronizują adresy emailowe wszystkich folderów publicznych Exchange 5.5 do Active Directory lub wszystkich folderów publicznych Exchange 2000 do katalogu Exchange 5.5. Takie umowy pomagają również w administracji folderów publicznych Exchange 5.5 przy użyciu przystawki MMC *System Manager* oraz folderów Exchange 2000 poprzez program Exchange 5.5 Administrator. Wszystkie foldery publiczne, które mają adresy emailowe, są w Exchange 5.5 automatycznie z nimi powiązane. Wszystkie wpisy folderów publicznych w katalogu są domyślnie ukryte na liście GAL. Pracując w środowisku Exchange 2000 trybu mieszanego, trzeba zrozumieć wszystkie domyślne zachowania folderów publicznych. Microsoft znacznie ułatwił konfigurację umów połączenia folderów publicznych w porównaniu z takimi umowami dla użytkowników. Wszystkie umowy folderów publicznych są automatycznie konfigurowane jako połączenia dwukierunkowe.

Uprawnienia folderów publicznych są obsługiwane w Exchange 2000 inaczej, niż w przypadku Exchange 5.5. Starsza wersja tej platformy używa list kontroli dostępu (ACL) do zarządzania dostępem do folderów publicznych. Lista ACL nie jest uważana za wyróżniającą właściwość folderu publicznego. Z kolei Exchange 2000 traktuje ACL jako bezpośrednią właściwość folderu; jest ona umieszczona w magazynie folderów publicznych i zawiera identyfikatory zabezpieczeń dla wszystkich użytkowników lub grup, które mają prawa do danego folderu publicznego. Exchange 5.5 używa właściwości obiektu o nazwie *Distinguished Name* do identyfikacji wszystkich użytkowników, których uprawnienia do folderu publicznego zostały skonfigurowane poprzez ACL. Z kolei Exchange 2000 używa do tego

samego celu identyfikatora zabezpieczeń obiektu zapisanego w Active Directory, dzięki czemu wszystkie dane ACL są konwertowane, kiedy folder publiczny jest replikowany z Exchange 5.5 do bazy danych magazynu folderu publicznego w Exchange 2000.

Powiązanie między ADC i replikacją folderów publicznych z Exchange 5.5 do Exchange 2000 staje się ważne, ponieważ listy ACL takich folderów korzystały z list dystrybucyjnych. Innymi słowy, listy dystrybucyjne kontrolowały dostęp do folderów publicznych. Jak wspomniano wcześniej, nie oznacza to, iż możliwa jest replikacja listy dystrybucyjnej Exchange 5.5 do Active Directory, ponieważ Exchange 2000 używa teraz pewnych typów grup do kontrolowania dostępu do folderów publicznych.

Dlaczego typy grup sprawiają takie problemy w Windows 2000?

Niektóre obiekty Exchange 5.5 stają się innymi obiektami po replikacji do Exchange 2000. Dla przykładu, obiekt adresata w Exchange 5.5 może stać się w Active Directory obiektem z włączoną obsługą poczty lub skrzynki pocztowej. Jest to zależne od tego, czy nowy obiekt posiada tylko adres emailowy, czy też jest powiązany ze skrzynką pocztową w Active Directory. Własny adresat w Exchange 5.5 zawsze staje się obiektem z *włączoną obsługą poczty*, a nie z *włączoną obsługą skrzynki pocztowej*. Lista dystrybucyjna staje się w Exchange 2000 *obiektem grupy* z włączoną obsługą poczty. Możliwe jest zdefiniowanie różnych obiektów grup w zależności od *typu* lub *zakresu* grupy.

Dwie kategorie *typu* grupy obejmują:

- *Grupy zabezpieczeń* — używane do przydzielania uprawnień do zasobów w strukturze lasu Windows 2000.
- *Grupy dystrybucyjne* — używane w przypadku funkcji nie związanych z zabezpieczeniami. Grupa tego typu może służyć do wysłania wiadomości emailowej jednocześnie do grupy użytkowników i nigdy nie może być użyta do przydzielenia uprawnień do zasobów.

Trzy kategorie *zakresu* grupy obejmują:

- *Grupy lokalnej domeny* — używane do przydzielania uprawnień do zasobów. W grupie mogą znaleźć się użytkownicy z dowolnej domeny w lesie, ale mogą oni uzyskać dostęp jedynie do zasobów ulokowanych w domenie, w której została utworzona grupa.
- *Grupy globalne* — używane do organizacji użytkowników z podobnymi potrzebami w zakresie dostępu. W grupie mogą znaleźć się użytkownicy tylko z domeny, w której została utworzona grupa; członkowie grupy będą mieli dostęp do zasobów dowolnej domeny w lesie.
- *Grupy uniwersalne* — używane do przydzielania zasobów w wielu domenach. W grupie można umieścić użytkowników z dowolnej domeny, którzy będą mieli dostęp do dowolnej domeny w lesie. Grupy uniwersalne mogą być z kolei podzielone na:
  - *uniwersalne grupy zabezpieczeń* — dostępne tylko w środowisku Windows 2000 trybu macierzystego
  - *uniwersalne grupy dystrybucyjne* — dostępne w środowisku Windows 2000 trybu mieszanego lub macierzystego, ale używane głównie w środowisku mieszanym w celu wysyłania wiadomości emailowych jednocześnie do wielu użytkowników.

Typ grupy determinuje *sposób* jej użycia, podczas gdy zakres grupy decyduje o *miejscu w sieci*, gdzie grupa jest użyta. Możliwa jest konwersja wszystkich grup lokalnej domeny i globalnych do grup uniwersalnych, ale tylko w przypadku, gdy Windows 2000 działa w trybie macierzystym (takie grupy nie mogą zawierać innych grup o tym zakresie, jeśli planowana jest konwersja do grupy uniwersalnej). Microsoft zaleca wykorzystanie następującej strategii tworzenia grup w celu zredukowania liczby procesów przydzielania uprawnień w organizacji:

1. Przydziel użytkowników z podobnymi potrzebami do nowej lub istniejącej grupy globalnej.
2. Utwórz grupy lokalnej domeny dla wszystkich zasobów, które będą udostępniane (na przykład, drukarki sieciowe lub pliki).
3. Dodaj grupy globalne do grup domeny lokalnej powiązanych z zasobami, do których potrzebny jest dostęp.
4. Przydziel właściwe uprawnienia do grupy domeny lokalnej z kroku 3.

Być może łatwiejsze wyda się przydzielenie użytkowników bezpośrednio do grupy domeny lokalnej, a następnie przyznanie tej grupie uprawnień do zasobów. Jednakże ta strategia nie pozwoli członkom grupy na użycie zasobów znajdujących się poza domeną lokalną. Tylko członkowie grupy globalnej i uniwersalnej grupy zabezpieczeń mogą uzyskać dostęp do zasobów w dowolnej domenie.

Umieszczenie użytkowników bezpośrednio w grupach dystrybucyjnych i przydzielenie im uprawnień również nie jest praktyczne, ponieważ w tym przypadku wymagana jest praca w trybie macierzystym Windows 2000. W przypadku obecności serwerów Windows NT 4 konieczne są jednak funkcje trybu mieszanego Windows 2000.

Listy dystrybucyjne Exchange 5.5 zostały zastąpione w Exchange 2000 przez grupy uniwersalne z włączoną obsługą poczty. Uniwersalne grupy zabezpieczeń z włączoną obsługą poczty również mogą zastąpić listy dystrybucyjne, ale może się to zdarzyć *tylko* w przypadku organizacji z lasem Windows 2000 trybu macierzystego (zobacz hasło *Dlaczego typy grup sprawiają takie problemy w Windows 2000?*). W lesie Windows 2000 trybu mieszanego możliwa jest praca jedynie z uniwersalnymi grupami dystrybucyjnymi, a nie uniwersalnymi grupami zabezpieczeń. W takich przypadkach częściej stosowane są grupy dystrybucyjne, gdyż możliwe jest uniknięcie sytuacji, w której omyłkowo zostaną przyznane prawa dostępu do ważnych zasobów (co zdarza się automatycznie w przypadku grup zabezpieczeń). Łącznik ADC replikuje wszystkie listy dystrybucyjne Exchange 5.5 z uniwersalnymi grupami dystrybucyjnymi w Active Directory; grupy tego typu nie mogą decydować o dostępie do folderów publicznych w Exchange 2000. Windows 2000 Server pozwala jedynie głównym obiektom zabezpieczeń na kontrolowanie dostępu do synchronizowanych obiektów, a uniwersalne grupy dystrybucyjne nie są uważane za takie obiekty. W niektórych przypadkach grupa tego typu może być przekonwertowana do uniwersalnej grupy zabezpieczeń. Dzieje się tak, kiedy foldery publiczne są aktualizowane do Exchange 2000 lub jeśli Outlook jest używany do przydzielenia uprawnień do folderów publicznych w Exchange 2000. Ponieważ uniwersalne grupy zabezpieczeń mogą wymusić dostęp do folderów publicznych, w czasie replikacji list dystrybucyjnych Exchange 5.5 do Active Directory należy upewnić się, czy wszystkie domeny Windows 2000 pracują w trybie macierzystym. Kiedy tworzona jest umowa połączenia użytkowników w celu replikacji listy dystrybucyjnej, łącznik ADC poinformuje o domenie Windows 2000, która nie pracuje w trybie macierzystym.

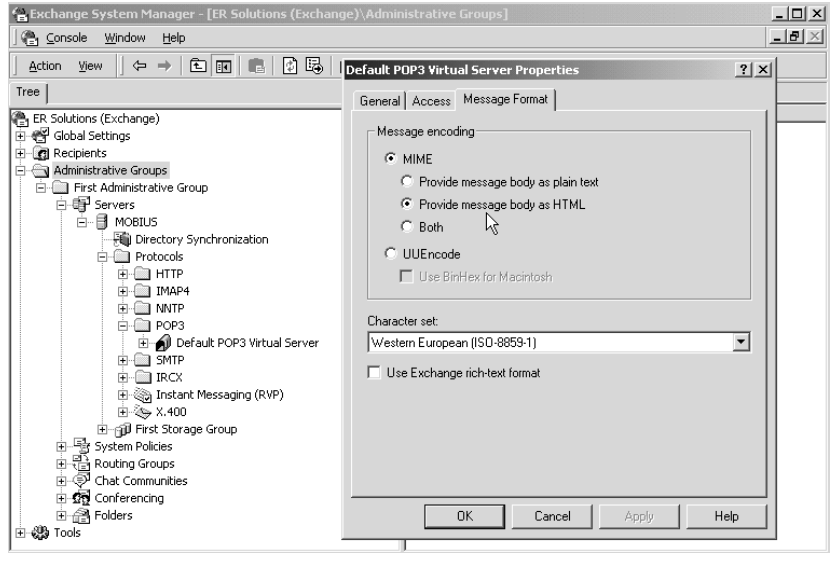
Powiązane rozwiązania	Strona
Planowanie folderów publicznych	
Ustalenie zakresu grup	
Tworzenie grup zabezpieczeń i grup dystrybucyjnych	
Ustalenie zakresu grup Active Directory	
Planowanie grup zabezpieczeń Active Directory	

Gotowe rozwiązania

Konfiguracja formatów wiadomości dla serwera wirtualnego POP3

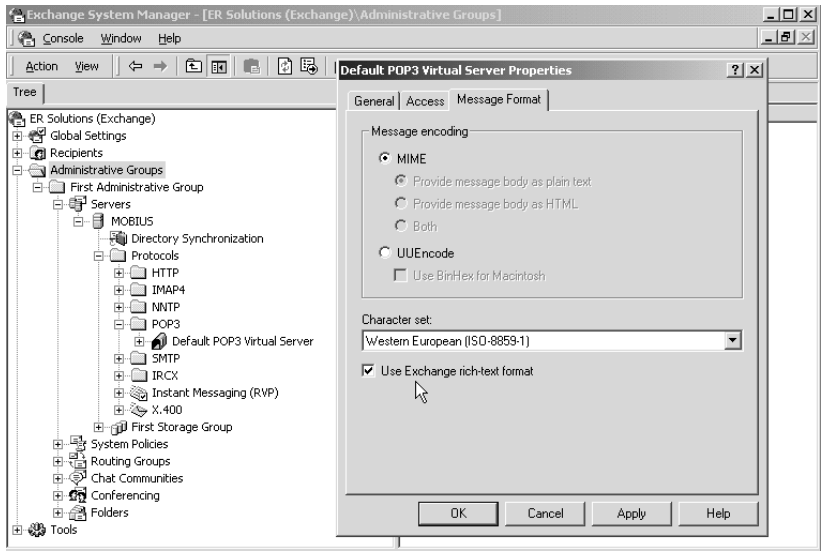
Wszystkie opcje serwera wirtualnego POP3 można skonfigurować poprzez przystawkę MMC *Exchange 2000 System Manager*. Aby tego dokonać:

1. Otwórz przystawkę *System Manager* poprzez wybranie *Start|Programs|Microsoft Exchange| System Manager*.
2. Kliknij symbol + przy ikonie folderu *Administrative Groups*, a następnie symbol + przy kontenerze *First Administrative Group*.
3. W ten sam sposób rozwiń kolejno kontener *Servers*, obiekt logiczny *Server* i podkontener *Protocols*.
4. Rozwiń folder *POP3* wewnątrz kontenera *Protocol*, aby ujawnić obiekt *Default POP3 Virtual Server*. Kliknij prawym przyciskiem myszy ten obiekt i wybierz polecenie *Properties*.
5. Na ekranie pojawi się automatycznie zakładka *General* okna dialogowego *Default POP3 Virtual Server Properties*. Kliknij zakładkę *Message Format* (zobacz rysunek 9.3).



Rysunek 9.3. *Zakładka Message Format w oknie dialogowym Default POP3 Virtual Server Properties*

6. Zauważ, iż domyślnym schematem kodowania MIME jest HTML (opcja *Provide Message Body As HTML*). Kliknij opcję *Exchange Rich-Text Format* (w sposób pokazany przez wskaźnik myszy na rysunku 9.4) i przyjrzyj się domyślnym ustawieniom MIME. Kliknij *OK*, aby powrócić do konsoli *System Manager*.

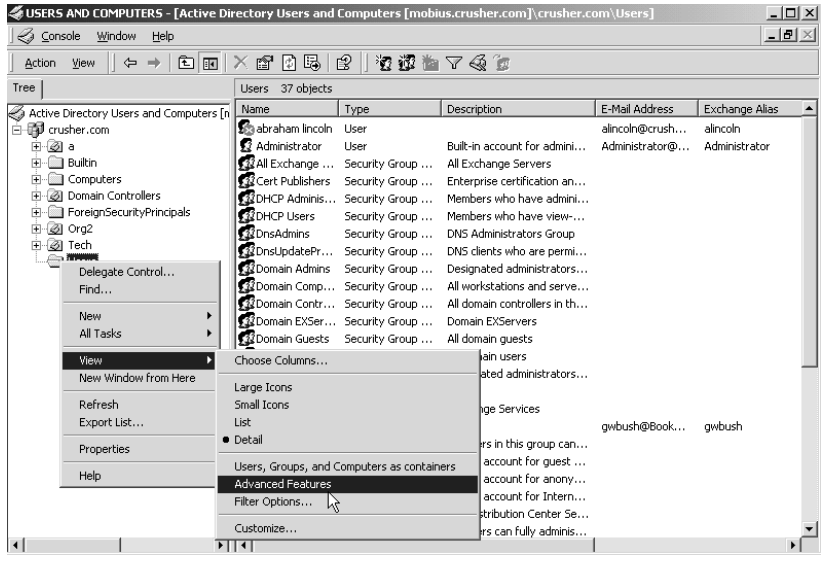


Rysunek 9.4. *Zakładka Message Format pokazująca ustawienie Exchange Rich-Text Format*

Konfiguracja opcji zmiany formatu wiadomości dla poszczególnych użytkowników

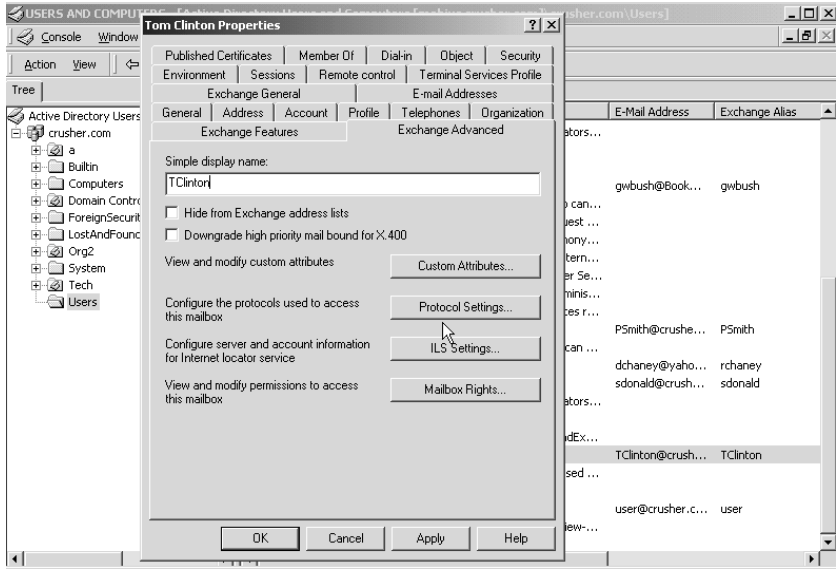
Kiedy użytkownicy żądają przesłania wiadomości poprzez protokół POP3 lub IMAP4, możliwe jest skonfigurowanie opcji dostarczenia wiadomości w formie prostego tekstu lub HTML (lub w obu tych formatach). Możliwa jest również zmiana tych domyślnych ustawień dla poszczególnych użytkowników. Aby tego dokonać:

1. Otwórz przystawkę MMC *Active Directory Users and Computers*.
2. Kliknij kontener *Users*, a następnie kliknij prawym przyciskiem myszy ten kontener i wybierz polecenie *View|Advanced Features* (zobacz rysunek 9.5).



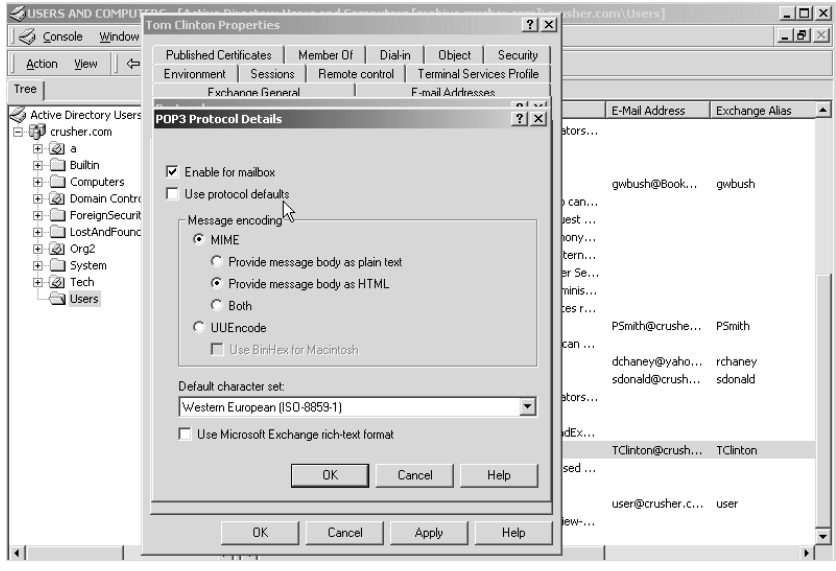
Rysunek 9.5. *Udostępnienie zaawansowanych funkcji dla kontenera Users w przystawce Active Directory Users and Computers*

3. Kliknij dwukrotnie wybranego użytkownika i w pojawiającym się oknie właściwości wybierz zakładkę *Exchange Advanced*. Kliknij następnie przycisk *Protocol Settings* w środkowej części zakładki (zobacz rysunek 9.6).



Rysunek 9.6. *Konfiguracja ustawień protokołu dla użytkownika w zakładce Exchange Advanced w oknie Active Directory Users and Computers*

4. Kliknij dwukrotnie protokół *POP3*, który pojawi się w oknie dialogowym *Protocols*. Poczekaj na pojawienie się okna dialogowego *POP3 Protocol Details* (zobacz rysunek 9.7) i wyłącz opcję *Use Protocol Defaults*. Możesz skonfigurować wybrane opcje dla użytkownika. Po zakończeniu konfiguracji kliknij *OK*, aby powrócić do okna dialogowego *Protocols*.



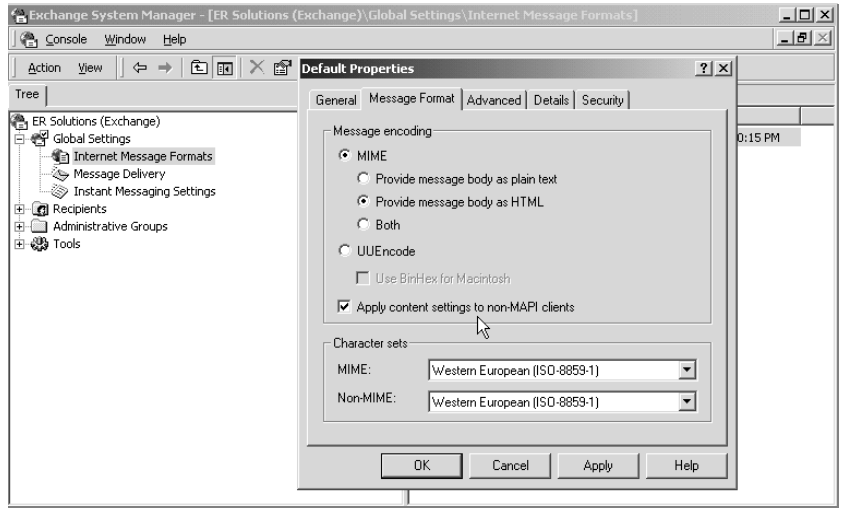
Rysunek 9.7. *Okno dialogowe POP3 Protocol Details*

5. Kliknij *OK*, aby powrócić do okna właściwości użytkownika. Kolejne kliknięcie przycisku *OK* spowoduje powrót do konsoli *Active Directory Users and Computers*. Kliknij symbol X w prawym górnym rogu okna, aby zamknąć interfejs *Active Directory Users and Computers*.

Konfiguracja formatów MIME dla domyślnego formatu wiadomości internetowych

Aby poprzez Exchange System Manager skonfigurować formaty MIME dla obiektu *Internet Message Format* w kontenerze *Global Settings* w obiekcie *Organizational*:

1. Otwórz przystawkę MMC *Exchange System Manager* i kliknij symbol + w pobliżu kontenera *Global Settings*. Pojawi się obiekt *Internet Message Formats*.
2. Kliknij ten obiekt, a w panelu szczegółów po prawej stronie pojawi się format *Default* (z podaną nazwą domeny *). Kliknij ten obiekt prawym przyciskiem myszy i wybierz polecenie *Properties*.
3. Pojawi się ekran *Default Properties*. Wybierz zakładkę *Message Format*; domyślnie wybrane tu kodowanie MIME to tekst (*Provide Message Body As Plain Text*). Aby zmienić domyślne kodowanie na HTML, wybierz opcję *Provide Message Body As HTML*, zaznacz *Apply Content Settings To Non-MAPI Clients* (zastosuj ustawienia treści dla klientów innych niż MAPI) i kliknij *OK*, aby powrócić do konsoli *Exchange System Manager* (zobacz rysunek 9.8).



Rysunek 9.8. *Wybór ustawień MIME dla domyślnego formatu wiadomości internetowych w System Managerze*

4. Zamknij konsolę *System Manager* poprzez wybranie z menu polecenia *Console|Exit*.

Użycie kreatora reguł w Outlooku 2000 do zarządzania treścią

Bardzo ważną funkcją każdej aplikacji pocztowej jest możliwość wydajnego przetwarzania zarówno przychodzących, jak i wychodzących wiadomości. Outlook zapewnia taką funkcję przy użyciu *Kreatora reguł*, który pozwala na zdefiniowanie określonych działań wykonywanych dla wiadomości przychodzących i wychodzących. Kreator może być wykorzy-

stany do przydzielenia kategorii dla wiadomości na podstawie ich zawartości. Możliwe jest nawet ustawienie zawiadomień, które będą alarmowały użytkownika po dotarciu ważnej wiadomości do skrzynki pocztowej. Kolejną opcją jest oflagowanie wiadomości pochodzących od wybranych nadawców.

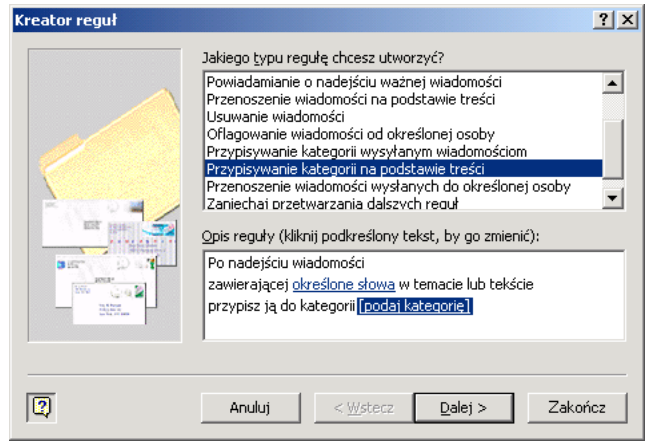
Użytkownicy Outlooka 97 i 98 mogą użyć *Asystenta skrzynki odbiorczej* do emulacji funkcji *Kreatora reguł*. Kreator jest instalowany automatycznie wraz z klientami Outlook 98 i Outlook 2000. W przypadku Outlooka 97 konieczna jest ręczna instalacja.

Kreator reguł może współpracować z *Asystentem skrzynki odbiorczej* w programie Outlook Express, aby filtrować i sortować wiadomości emailowe, które nie spełniają określonych kryteriów. Podstawowa różnica między tymi dwoma narzędziami to fakt, iż *Kreator reguł* przetwarza wiadomości przychodzące i wychodzące, podczas gdy *Asystent skrzynki odbiorczej* obsługuje tylko przychodzącą pocztę, ale może jednocześnie przekazywać dalej wiadomości emailowe bez zmiany jej zawartości. Po pierwszym uruchomieniu *Kreator reguł* w Outlooku 2000 użytkownik zostanie zapytany o chęć konwersji wszystkich istniejących reguł asystenta skrzynki odbiorczej. Aby potwierdzić taką konwersję, kliknij *Tak*, a następnie *OK*. Przekonwertowane zostaną wszystkie reguły z wyjątkiem tych, które zawierają własne warunki formularza.

Jeśli używana jest wersja Exchange wcześniejsza niż 5.5, mogą pojawić się pewne problemy związane z konwersją reguł, ponieważ *Kreator reguł* w Outlooku 2000, oprócz nowych reguł, zachowuje jednocześnie wszystkie stare reguły *Asystenta skrzynki odbiorczej*. Taka kombinacja plików może spowodować niepotrzebne zajęcie cennego miejsca na dyskach twardych serwera.

Aby użyć *Kreatora reguł* w programie Outlook 2000:

1. Uruchom Outlooka i wybierz polecenie *Narzędzia|Kreator reguł*. Pojawi się okno dialogowe *Kreator reguł*. Kliknij *Nowa* i wybierz typ reguły, którą chcesz utworzyć.
2. Kliknij regułę *Przypisywanie kategorii na podstawie treści*. W dużym polu tekstowym pojawi się opis reguły (zobacz rysunek 9.9).



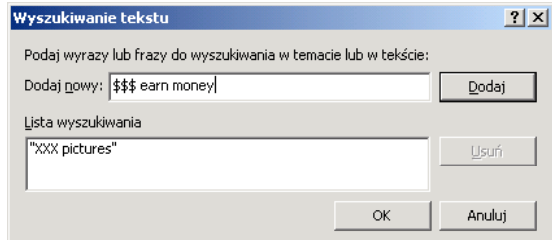
Rysunek 9.9. *Kreator reguł z wybraną regułą Przypisywanie kategorii na podstawie treści*

3. Kliknij *Dalej*, aby wybrać warunek do sprawdzenia. Zauważ, iż automatycznie jest już zaznaczona opcja *zawierającej określone słowa w temacie lub w tekście*; możesz jednak ją wyłączyć. My jednak pozostawimy tę opcję i przyjrzymy się

sposobowi tworzenia opisu reguły w polu tekstowym poniżej. Kliknij podkreślone łącze *określone słowa*, aby podać słowa lub frazy, które będą wyszukiwane w treści lub temacie wszystkich wiadomości emailowych.

4. W polu tekstowym *Dodaj nowy* wpisz *$$$ earn money* i kliknij *Dodaj*, aby dodać te słowa do listy wyszukiwania (zobacz rysunek 9.10). Kliknij *OK*, aby powrócić do okna *Kreator reguł*.

Rysunek 9.10. *Okno dialogowe Wyszukiwanie tekstu pokazujące słowa i frazy, które będą używane jako filtry*



5. Zauważ, iż dodane słowa pojawiły się w polu *Opis reguły* na dole ekranu. Kliknij łącze *podaj kategorię* i wprowadź nazwę kategorii, którą chcesz monitorować (na przykład, *Śmieci*). Jeśli zawartość pola *Opis reguły* wygląda poprawnie, kliknij *Dalej*.

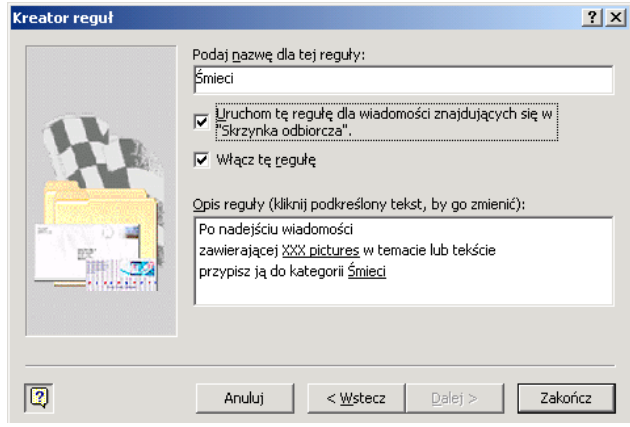
Dodając nowe słowa lub frazy w kroku 4., możesz zostać ostrzeżony, iż te reguły nie będą działały poprawnie w wersjach Outlooka starszych, niż aktualnie używana (w naszym przykładzie używamy Outlooka 2000). Jeśli to akceptujesz, kliknij *Tak*; w przeciwnym przypadku odpowiedz *Nie* na pytanie o chęć utworzenia tej reguły.

6. W kolejnym oknie kreatora wybierz właściwą opcję w odpowiedzi na pytanie o czynność, jaka powinna być wykonana z wiadomością (*Co chcesz zrobić z tą wiadomością?*). Dostępne opcje to m.in. *Przypisz ją do kategorii* lub *Usuń ją*. Kliknij *Dalej*.

7. Zignoruj kolejne okno pytające o wyjątki do reguły — *Podaj ewentualne wyjątki* i kliknij *Dalej*.

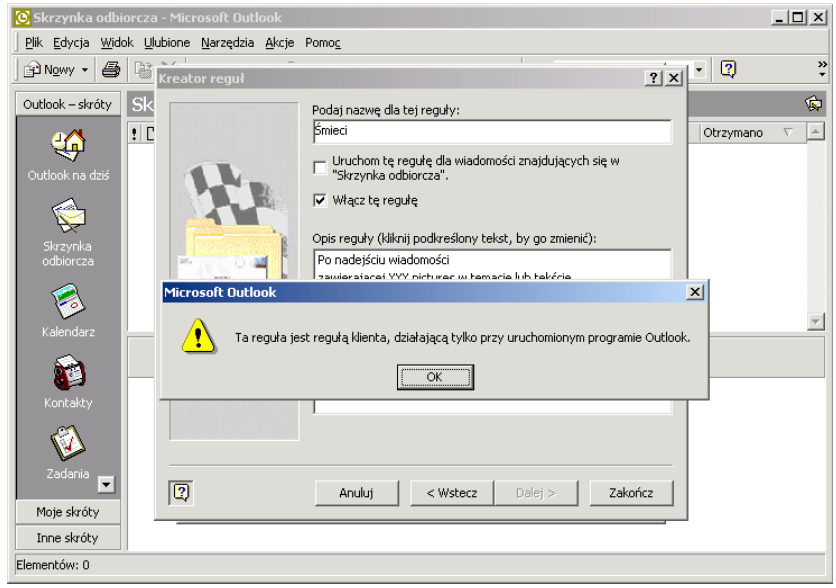
8. W kolejnym oknie podaj nazwę tej reguły poprzez wpisanie w polu tekstowym słów `Śmieci`. Zaznacz opcję *Uruchom tę regułę dla wiadomości znajdujących się w „Skrzynka odbiorcza”*. Opcja *Włącz tę regułę* jest zaznaczona automatycznie (zobacz rysunek 9.11). Kliknij *Zakończ*, aby zakończyć tworzenie reguły.

Rysunek 9.11. *Podanie nazwy nowej reguły i jej włączenie*



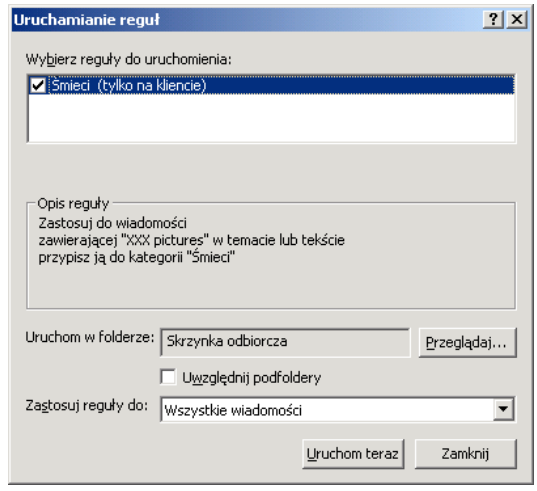
9. Jeśli pojawi się komunikat informujący, iż *Ta reguła jest regułą klienta, działającą tylko przy uruchomionym programie Outlook* (zobacz rysunek 9.12), kliknij *OK*, aby powrócić do okna dialogowego *Kreator reguł*.

Rysunek 9.12. *Okno dialogowe pokazujące status nowej reguły*



10. W pojawiającym się oknie dialogowym przyjrzyj się dostępnym teraz opcjom. Możliwe jest utworzenie nowej reguły lub skopiowanie, modyfikacja, zmiana nazwy i usunięcie właśnie utworzonej reguły. Kliknij przycisk *Uruchom teraz*, aby otworzyć okno dialogowe *Uruchamianie reguł* (zobacz rysunek 9.13).

Rysunek 9.13. *Okno dialogowe Uruchamianie reguł*

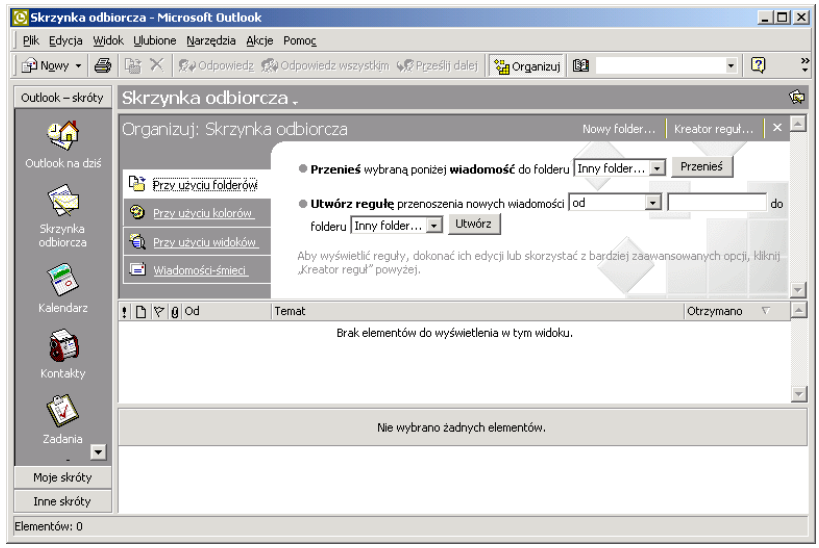


11. Zaznacz pole wyboru w pobliżu nowej zasady i upewnij się, czy w polu tekstowym obok napisu *Uruchom w folderze* pojawił się folder *Skrzynka odbiorcza*. Kliknij przycisk *Uruchom teraz*, a następnie *Zamknij*. Kliknij *OK*, aby zamknąć okno *Kreator reguł* i powrócić do interfejsu Outlooka 2000.

Użycie filtrów treści wiadomości w programie Outlook

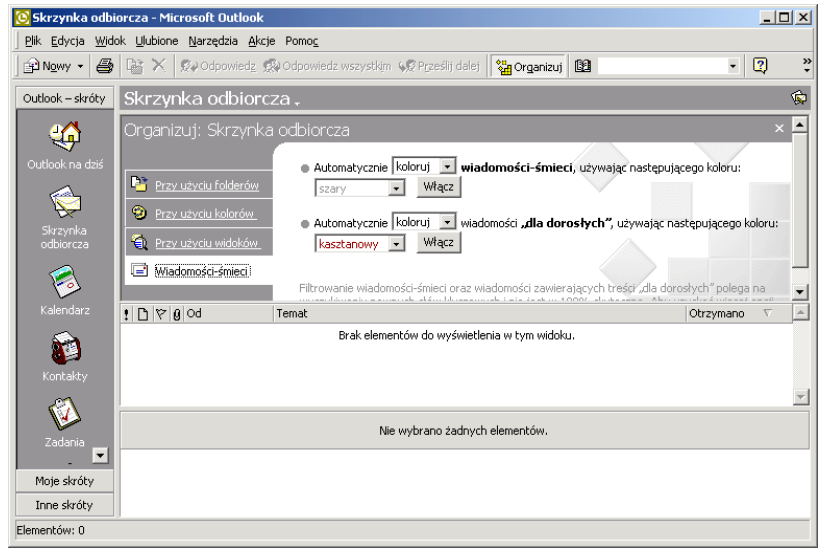
Filtry treści mogą być zastosowane w uzupełnieniu do *Kreatora reguł*, który został opisany we wcześniejszym rozwiązaniu. Aby włączyć te filtry w programie Outlook:

1. Otwórz program pocztowy Outlook i kliknij menu *Widok*. Upewnij się, czy zaznaczono opcję *Pasek Outlook*, a następnie powróć do głównego ekranu Outlooka.
2. Kliknij ikonę *Organizuj* w pasku narzędzi, aby pojawił się ekran pokazany na rysunku 9.14.



Rysunek 9.14. *Ekran Outlooka po kliknięciu przycisku Organizuj w pasku narzędzi*

3. Kliknij łącze *Wiadomości-śmieci* w sekcji *Organizuj: Skrzynka odbiorcza*. Pojawi się ekran podobny do tego, który został przedstawiony na rysunku 9.15.



Rysunek 9.15. *Opcje niepożądanej poczty w Outlooku 2000*

4. Upewnij się, czy w pierwszym wierszu w tej sekcji pojawia się napis *Automatycznie koloruj wiadomości-śmieci*, wybierz kolor czerwony, a następnie kliknij *Włącz*. W drugim wierszu powinien znaleźć się napis *Automatycznie koloruj wiadomości „dla dorosłych”*. Wybierz kolor fioletowy i kliknij *Włącz*.
5. Kliknij ikonę *Organizuj* w pasku narzędzi Outlooka, aby wyłączyć ten ekran.

Wybór właściwego oprogramowania do zarządzania treścią

Wybierając właściwy pakiet oprogramowania do zarządzania treścią, należy upewnić się, czy zawiera pewien minimalny zestaw funkcji. Wybrany pakiet będzie służył nie tylko do prostego blokowania poczty, ale również do inteligentnego trasowania wiadomości w organizacji. Oprogramowanie tego typu powinno być zainstalowane w wielu punktach dostępowych organizacji, włączając w to bramy SMTP i programy pocztowe. Upewnij się, czy wybrany pakiet udostępnia następujące funkcje:

- Kontrola obecności skryptów HTML oraz plików wykonywalnych i *.vbs* — program powinien wyszukiwać wszystkie rodzaje aktywnej treści przychodzących wiadomości, włączając w to pliki wykonywalne, pliki ActiveX oraz pliki z rozszerzeniem *.vbs* (VBScript). Za wprowadzenie szkodliwych wirusów do organizacji często są obciążane właśnie takie skrypty. Niektóre programy antywirusowe posiadają funkcję skanowania wiadomości w poszukiwaniu takiej zawartości.
- Obsługa obcych języków — dobre oprogramowanie do zarządzania treścią powinno rozpoznawać szkodliwe treści w językach innych, niż tylko angielski. Oznacza to konieczność obsługi znaków narodowych dla popularnych języków, włączając w to oczywiście język polski.
- Ochrona zaszyfrowanej komunikacji — większość pakietów antywirusowych nie potrafi skanować zaszyfrowanych informacji, ale większość programów do zarządzania treścią ma funkcję blokowania zaszyfrowanych wiadomości i ich załączników.
- Integracja z Windows 2000 — wybrany pakiet powinien obsługiwać wszystkie funkcje Active Directory i Windows 2000. Oprogramowanie powinno być zarządzane i monitorowane przy użyciu własnej przystawki MMC. Inną opcją jest integracja z już istniejącymi przystawkami Exchange 2000 i Windows 2000.
- Użycie analizy słownikowej — dobre oprogramowanie do zarządzania treścią sprawdza zarówno zawartość wiadomości, jak i wszystkie załączniki. Konieczna jest również funkcja logicznego filtrowania według kombinacji słów.

Pod adresem *www.slipstick.com/addins* znajduje się doskonała strona internetowa, która zawiera omówienie różnych pakietów oprogramowania do zarządzania treścią dla Exchange 2000. Do przeszukania tej strony użyj słów kluczowych *Content Control* lub *Automatic Message Processing*. Wiele z programów działa jako wtyczki lub dodatki do serwera Exchange 2000, podczas gdy inne pakiety działają tylko z programami pocztowymi lub na bramach SMTP. Wiele narzędzi tego typu współpracuje również z narzędziami antywirusowymi oraz oferuje dodatkowe funkcje, takie jak archiwizacja wiadomości.

Niewłaściwe użycie poczty na serwerze Exchange 2000

Niektórzy użytkownicy — poprzez użycie firmowego serwera poczty do przekazywania poczty — mogą wywołać chaos w nie spodziewających się niczego organizacjach. Takie osoby masowo wysyłają pocztę reklamową, podając domenę organizacji jako adres zwrotny. Ponieważ wykorzystana jest nazwa firmowej domeny, odbiorcy spamu mogą uznać daną organizację za źródło wiadomości. Serwer Exchange 2000 będzie musiał obsłużyć wszystkie raporty niedoręczonej poczty (NDR) wygenerowane przez wiadomości, które nie dotarły do miejsca docelowego.

Exchange 2000 nie wykrywa różnicy pomiędzy pocztą elektroniczną wysyłaną do poprawnych i „oszukanych" użytkowników w organizacji. Bardzo trudne jest również filtrowanie całej poczty SMTP, która nie należy do organizacji. Istnieją jednak organizacje (takie jak Mail Abuse Prevention System LLC — MAPS) prowadzące kampanie w celu ochrony systemów pocztowych przed osobami rozsyłającymi spam (takie osoby są nazywane *spamerami*).

Aby uzyskać dodatkowe informacje na temat nie nastawionej na zysk organizacji MAPS, która pomaga śledzić osoby niewłaściwie korzystające z systemów pocztowych, zajrzyj na stronę *http://maps.vix.com*.

Zadaniem administratora jest ochrona serwera przed użyciem go do przesyłania wiadomości przez osoby z zewnątrz organizacji (tzw. open-relay). Zdarza się to, kiedy serwer Exchange 2000 przetwarza wiadomości, których nadawca i odbiorca nie są członkami organizacji. W niektórych przypadkach użycie serwera do przekazywania poczty może jednak pomóc w rozwiązywaniu problemów (na przykład, do przetestowania łączności między wieloma systemami w pojedynczej sieci).

Spamerzy korzystają z otwartych serwerów do rozprzestrzeniania niepożądanej poczty w Internecie. Oznacza to, iż wiele serwerów Exchange może stać się ofiarą takich planów. Należy powstrzymać wszystkie takie próby, ponieważ mogą one spowodować poważne problemy systemów pocztowych poprzez niepotrzebne zajęcie pasma sieciowego lub wykorzystanie mocy procesora. W najgorszym przypadku dana organizacja może znaleźć się na czarnej liście organizacji MAPS, która zawiera dane dostawców usług internetowych przyczyniających się do rozsyłania spamu. Zmiany na liście dokonują się w czasie rzeczywistym, przez co dostawca usług może znaleźć się na niej natychmiast po otrzymaniu spamu. Czarna lista została umieszczona na serwerze *http://maps.vix.com*. Warto również odwiedzić stronę projektu *Anti-Spam Project* pod adresem *www.bitgate.com/spam*. Można tam znaleźć listę domen rozsyłających spam, a także narzędzie do filtrowania poczty o nazwie BlackMail. Po zainstalowaniu program filtruje pocztę przychodzącą, wykorzystując zdefiniowane kryteria.

Microsoft już w sierpniu 1999 r. rozwiązał kwestię serwerów pocztowych przekazujących spam, publikując poprawkę o nazwie *Exchange 5.5 post-SP2 hotfix*. Ta poprawka usunęła możliwość przekazywania poczty oraz zamknęła lukę w zabezpieczeniach, która pozwalała na użycie usługi IMS (Internet Mail Service) do przesyłania kapsułkowanych wiadomości SMTP. Większość środków ochronnych powinna być zgodna z RFC 2505, które zawiera rekomendacje antyspamowe dla agentów MTA SMTP. To RFC zidentyfikowało problemy związane ze spamem i opisało funkcje MTA SMTP, które zredukują efekty spamu.

Jeśli organizacja została dodana do czarnej listy MAPS z serwerami, które są otwarte na przekazywanie poczty przez osoby z zewnątrz, to członkowie organizacji nie będą mogli wysyłać żadnej poczty, nawet jeśli wcześniej było to możliwe. Ta czarna lista jest dostępna na stronie MAPS pod adresem *www.mailabuse.org*. Administrator może skontaktować się z usługą MAPS Relay Spam Stopper w celu usunięcia serwera z czarnej listy. MAPS przetestuje serwer i sprawdzi, czy usunięto wszystkie dziury w zabezpieczeniach, a następnie usunie serwer z listy.

Aktualizacja zabezpieczeń poczty w Outlooku 2000

Możliwe jest zabezpieczenie programu pocztowego Outlook przed potencjalnie niebezpiecznymi robakami i wirusami, ale wiele zależy od używanej wersji programu i zastosowanych poprawek zabezpieczeń. Wirusy mają wpływ na trzy różne obszary Outlooka:

- *Panel podglądu* — wyłączenie tego panelu nie zabezpiecza przed atakiem wirusów na system. Wszystkie elementy sterujące ActiveX uruchamiają się automatycznie w tym panelu. Panel podglądu w Outlooku jest znacznie bezpieczniejszy, niż w Outlooku 98, ponieważ cała aktywna zawartość (włączając w to elementy sterujące ActiveX i Active Scripting) jest wyłączana niezależnie od ustawień strefy zabezpieczeń.
- *Otwarte wiadomości* — otwarcie wiadomości tekstowej lub RTF jest zawsze bezpieczne. Otworzenie wiadomości HTML może już spowodować problemy, ponieważ może ona zawierać kod Active Scripting lub elementy sterujące ActiveX z wirusami.
- *Załączniki* — jest to część wiadomości, która stwarza najwięcej zagrożeń. Załączniki nie mogą być otwarte bez wiedzy użytkownika, gdyż wymagają wykonania określonej czynności. Office 2000 w wersji SR-1 wyświetla zapytanie w przypadku próby uruchomienia plików wykonywalnych w Outlooku. Monitorowanych jest około 20 typów plików i rozszerzeń, włączając w to rozszerzenia *.vbs*, *.bat* i *.zip*.

Ze względu na coraz większą liczbę niebezpiecznych wirusów, takich jak *ILOVEYOU.VBS*, Microsoft opublikował poprawkę Outlook Email Security Update dla Outlooka 98 i Outlooka 2000, która rozwiązała wiele dziur w zabezpieczeniach. W skład poprawki weszły następujące komponenty:

- Komponent uniemożliwiający użytkownikom otwarcie lub zapisanie plików, które mogą zawierać niebezpieczny lub złośliwy kod. Zaufani użytkownicy mogą otrzymać uprawnienia dostępu do niektórych typów załączników lub uprawnienia do użycia klienta OWA. Użytkownicy, którzy nie zostali utworzeni na serwerze Exchange, nie mogą w żaden sposób uzyskać dostępu do tych załączników przy użyciu Outlooka.
- Komponent konfigurujący strefy zabezpieczeń Outlooka i blokujący wykonanie niektórych skryptów w formularzach Outlooka, chyba że te formularze zostaną umieszczone w bibliotece formularzy.
- Komponent Outlook Object Model Guard, który zapewnia kod blokujący dostęp do książki adresowej Outlooka.

Przed opublikowaniem Email Security Update Microsoft przedstawił poprawkę o nazwie Attachment Security, która uniemożliwiała użytkownikom otwarcie załączników w Outlooku. Ta wersja została jednak wycofana po wprowadzeniu podobnych funkcji w wersji Office 2000 SP-1. Ciągle dostępna jest jednak poprawka Attachment Security dla Outlooka 98.

Poprawka Email Security Update wyświetla ostrzeżenie przy próbie uruchomienia załącznika z określonym rozszerzeniem, ale nie wykrywa ani nie usuwa wirusów z zarażonych plików; jeśli taki plik zostanie zapisany na dysku i uruchomiony, w systemie znajdzie się wirus. Ta poprawka nie będzie miała żadnego wpływu na macierzyste dokumenty Office z rozszerzeniami *.doc*, *.xls* i *.ppt*, podobnie jak na pliki z rozszerzeniem *.shs* (obiekt wycinka) lub *.vbs* (pliki skryptów).

Ta poprawka definiuje określone poziomy załączników na podstawie rozszerzenia plików. Dla przykładu, załączniki poziomu 1 są uważane za niebezpieczne; w tej grupie znalazły się wszystkie rozszerzenia plików powiązane ze skryptami. Oznacza to, iż *nie jest możliwy dostęp do załączników*, jeśli zainstalowano tę poprawkę. Niektóre niebezpieczne typy plików zostały przedstawione w tabeli 9.4.

Tabela 9.4. *Rozszerzenia plików uważane za niebezpieczne w Outlooku 2000*

Nazwa rozszerzenia pliku	Typ rozszerzenia pliku
.adp	Projekt Access 2000
.bas	Moduł klasy Visual Basic
.cmd	Skrypt poleceń Windows NT/2000
.com	Plik wykonywalny MS-DOS
.exe	Dowolny plik wykonywalny
.hlp	Dowolny plik pomocy
.js	Dowolny plik JavaScript
.lnk	Dowolny plik skrótu
.mdb	Dowolny program Access 97/2000
.msi	Pakiet instalatora Windows
.mst	Plik źródłowy Microsoft Visual Test
.pif	Plik Microsoft Program Information (skrót do programu MS-DOS)
.scr	Dowolny plik wygaszacza ekranu
.url	Dowolny adres internetowy
.vbs	Dowolny plik lub program VBScript
.wsh	Dowolny plik Windows Script Host

W przeciwieństwie do poziomu 1, załączniki poziomu 2 nie są uważane za niebezpieczne, wymagają jednak wysokiego poziomu zabezpieczeń. Po otrzymaniu załącznika poziomu 2 użytkownik zostanie zapytany o chęć zapisania go na dysku; nie jest możliwe uruchomienie lub przeglądania załącznika z samej wiadomości. Ta aktualizacja będzie działała, tylko jeśli w systemie zainstalowano Outlooka w wersji SR-1. Należy pamiętać, iż poprawka stanowi integralny komponent Outlooka; aby ją usunąć, należy odinstalować cały pakiet, którego część stanowi Outlook, czyli Microsoft Office 2000 (lub Microsoft Office 97).

Poniżej przedstawiono uwagi końcowe dotyczące poprawki Outlook Email Security Update:

- W *All Public Folders* należy utworzyć folder najwyższego poziomu o nazwie *Outlook Security Settings*. Outlook bada wszystkie formularze umieszczone w tym folderze dla ustalenia ustawień zabezpieczeń dla każdego użytkownika.
- Jeśli wiadomość z niebezpiecznym załącznikiem poziomu 1 zostanie przekazana dalej (forward), to załącznik nie zostanie dołączony. Ta funkcja może być używana w celu usunięcia wszystkich niebezpiecznych załączników z otrzymanej wiadomości emailowej. Przesłanie wiadomości do samego siebie usuwa załącznik, ponieważ przekazane wiadomości nie zawierają załączników.
- Jeśli na stacji roboczej zainstalowano samodzielną wersję Outlooka 2000, a następnie zostanie wykonana próba aktualizacji tego komputera do pełnej wersji Office SR-1, instalacja poprawki Outlook Email Security Update nie powiedzie się. Dzieje się tak, ponieważ nie uruchomiono wcześniej aktualizacji Office 2000 SR-1 Update w celu wymuszenia aktualizacji Outlooka do wersji SR-1. Dopiero po wykonaniu tej czynności można zainstalować Outlook Email Security Update.
- Jeśli poprawka zostanie instalowana dla klienta Outlook 98, a następnie odbędzie się próba jego aktualizacji do Outlooka 2000, to zabezpieczenia nie zostaną zaktualizowane. Konieczna jest ręczna instalacja Outlook Email Security Update w wersji dla Outlooka 2000.

Łączenie Exchange 2000 z Internetem przy użyciu statycznego adresu IP

Administrator może skonfigurować serwer Exchange 2000 przy użyciu statycznego adresu IP, jaki został przyznany przez dostawcę usług internetowych. Nie jest konieczna rejestracja nazw DNS dla tego adresu IP, ale wykonanie tej czynności i skonfigurowanie właściwych rekordów wymiany poczty (MX) w bazie danych DNS oznacza, iż możliwe jest użycie „przyjaznych" nazw DNS, zamiast „nieprzyjaznych" adresów IP (zobacz ramka *Konfiguracja DNS dla poczty emailowej*). Aby zarejestrować nazwę domeny, odwiedź stronę *www.nask.pl*.

Konfiguracja DNS dla poczty emailowej

Poniższy przykład ilustruje sposób funkcjonowania serwera DNS w zakresie poczty elektronicznej, a w szczególności pod względem rekordów MX. Wyobraź sobie, iż konfigurowany jest serwer pocztowy o nazwie *Orion* (z serwerem Exchange) dla firmy o nazwie Caramel. W firmie działa również serwer DNS na komputerze z Windows 2000 Server o nazwie *Fantom*. Zewnętrzny użytkownik Tomasz chce wysłać dwie wiadomości emailowe do szefa firmy, którego adres to *Malinowski@Caramel.com* (nazwa *Malinowski* została skonfigurowana na tym serwerze pocztowym jako obiekt adresata z włączoną obsługą skrzynki pocztowej). W jaki sposób te dwa emaile odnajdą serwer pocztowy *Orion*, dzięki czemu zostaną dostarczone na adres *Malinowski@Caramel.com*?

Odpowiedź na to pytanie może być ustalona dopiero po zrozumieniu struktury Internetu. W Sieci umieszczone są serwery najwyższego poziomu, które znają położenie każdego serwera DNS z informacjami o domenie **.com* (co oznacza każdą nazwę domeny, która kończy się przyrostkiem *.com*). Serwer pocztowy na komputerze Tomasza (zewnętrzny użytkownik wysyłający wiadomości) zapyta serwer sieci szkieletowej o informacje dotyczące domeny *Caramel.com*. Serwer odpowie, iż ta domena jest obsługiwana przez serwer domeny umieszczony pod adresem *Fantom.Caramel.com*.

Po znalezieniu serwera DNS dla domeny *Caramel.com* komputer Tomasza zapyta go o informacje na temat tej domeny. Serwer nazw zainstalowany na Fantomie sprawdzi swoje rekordy zasobów i wyśle odpowiedź do komputera Tomasza w zewnętrznej domenie. Wysłane informacje obejmują rekordy MX i A oraz wskazują, iż wszystkie wiadomości dla domeny *Caramel.com* powinny być przesłane na serwer *Orion.Caramel.com*. Tym razem dostarczony zostanie również adres TCP/IP tego serwera. Używając tego adresu, Tomasz może skierować swoje wiadomości emailowe do serwera *Orion.Caramel.com*, który następnie przekaże je na adres *Malinowski@Caramel.com*.

Obecność rekordów MX w bazie danych DNS jest wymagana, jeśli serwer ma odbierać pocztę emailową bezpośrednio z Internetu, ponieważ informują one inne serwery pocztowe o sposobie trasowania poczty. Rekordy MX dokonują konwersji domen, które nie wskazują żadnego konkretnego serwera, do pełnej złożonej nazwy domeny, a także trasują wiadomości z danego serwera do innego serwera obsługującego serwer pocztowy (na przykład, Exchange 2000).

Poniżej przedstawiono sposób tworzenia rekordu MX (wraz z powiązanym rekordem zasobu A, który przekształca nazwę serwera pocztowego do adresu IP) w bazie danych na serwerze DNS o nazwie *Fantom*. Pierwszy wiersz to wpis rekordu MX, drugi wiersz zawiera wpis dla rekordu A, który identyfikuje adres IP serwera pocztowego *Orion* (którego adres IP to 192.168.10.5).

```
Caramel.com              IN     MX     10
Orion.Caramel.com
Orion.Caramel.com        IN     192.168.10.5
```

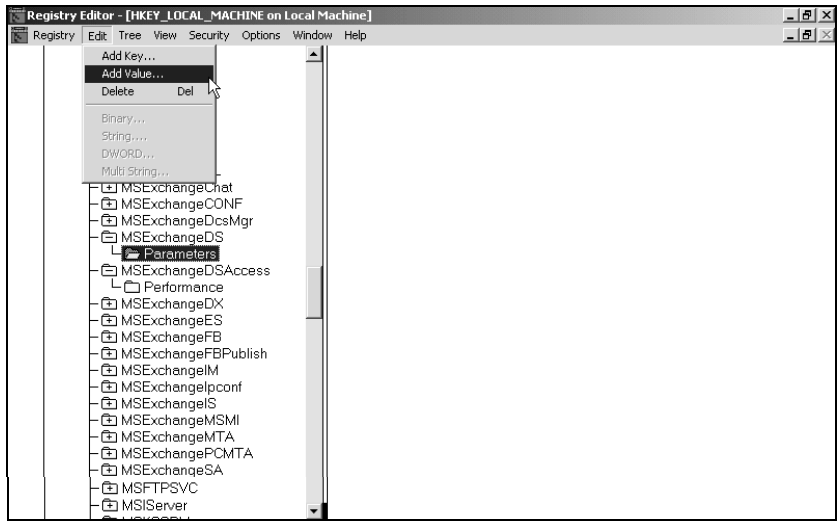
Szczegółowe informacje na temat rekordów MX znajdują się pod adresem *http://supportnet.merit.edu/m-spectop/t-dns/mx.html*. Możesz również przeczytać RFC 974, aby poznać sposób, w jaki systemy poczty internetowej trasują wiadomości na podstawie informacji zapewnianych przez systemy DNS (co opisano w RFC 882 i RFC 883). RFC 974 jest umieszczony pod adresem *www.faqs.org/rfcs974.html*.

Ustawienie numerów portów TCP/IP dla firewalla w środowisku Exchange trybu mieszanego

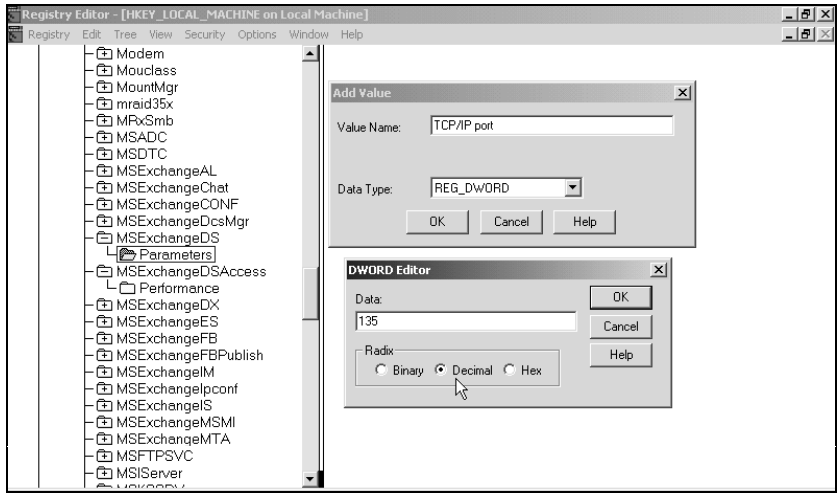
W czasie instalacji firewalla lub routera internetowego może wystąpić konieczność konfiguracji Information Store w Exchange 5.5 i usług katalogowych w celu użycia wstępnie zdefiniowanych numerów portów TCP. Niektóre firewalle mogą mieć problemy z akceptacją numerów portów TCP, jakie są wymagane przez serwer Exchange do komunikacji RPC. W takiej sytuacji konieczne jest dodanie do konfiguracji firewalla lub listy dostępowej portu o numerze 135, a następnie konfiguracja Exchange na pracę z portami dozwolonymi przez firewall.

Konfiguracja portu RPC dla Information Store w Exchange 5.5 może być wykonana przy użyciu edytora rejestru (*regedit* lub *regedt32.exe*). Aby zmienić port RPC dla usługi katalogowej w Exchange 5.5:

1. Uruchom edytor rejestru poprzez kliknięcie *Start|Run* i wpisanie `regedt32.exe` w polu *Open*.
2. Przejdź do podklucza *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeDS\Parameters*. Wybierz z menu polecenie *Edit|Add Value* w sposób pokazany na rysunku 9.16.
3. Pojawi się okno dialogowe *Add Value*; jako wartość *DWORD* podaj `TCP/IP port` i kliknij *OK*. W kolejnym oknie dialogowym *DWORD Editor* wybierz opcję *Decimal* i podaj numer portu (taki jak 135). Przykład pokazano na rysunku 9.17.



Rysunek 9.16. *Dodanie nowej wartości do istniejącego klucza rejestru*



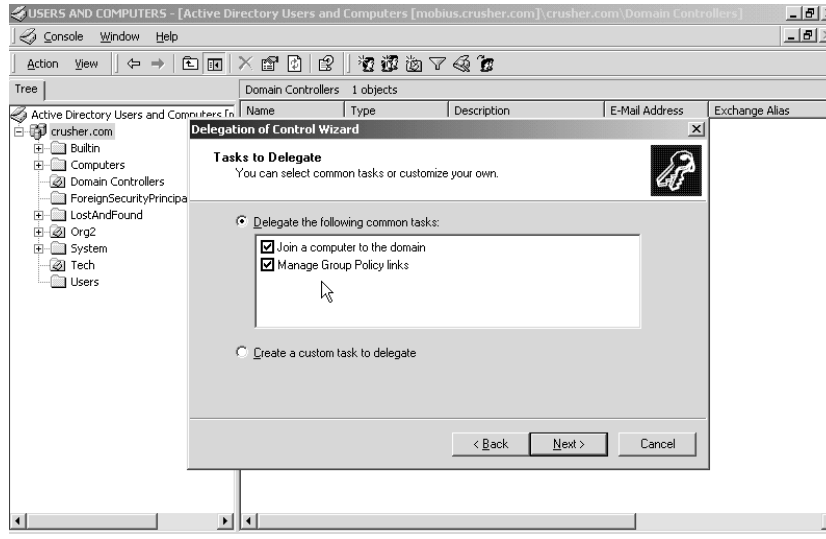
Rysunek 9.17. *Okno dialogowe Add Value oraz okno dialogowe DWORD Editor dla nowej wartości rejestru*

4. Po zakończeniu zamknij edytor rejestru poprzez wybranie polecenia *Registry|Exit*.

Użycie kreatora Delegation of Control do przydzielenia uprawnień

Możliwa jest delegacja kontroli nad obiektami w Windows 2000 dla niektórych użytkowników, co pozwoli na wykonanie zadań administracyjnych dla tych obiektów. Do celów delegacji kontroli nad różnymi obiektami w Windows 2000 i Exchange 2000 służy kreator *Delegation of Control Wizard*. Użyj tego kreatora do przydzielenia użytkownikom lub grupom odpowiednich uprawnień, dzięki czemu możliwe będzie utworzenie obiektów w jednostce organizacyjnej. Możliwe jest również przydzielenie uprawnień dla użytkowników, przez co uzyskają oni prawo modyfikacji uprawnień do atrybutów obiektu (na przykład, prawo do zmiany haseł innych użytkowników w jednostce organizacyjnej). Aby tego dokonać:

1. Otwórz przystawkę *Active Directory Users and Computers* (wybierz *Start|Programs|Administrative Tools|Active Directory Users and Computers*).
2. Wybierz obiekt, dla którego chcesz przekazać kontrolę (możesz wybrać obiekt domeny lokalizacji lub jednostki organizacyjnej). Kliknij prawym przyciskiem myszy obiekt domeny i wybierz polecenie *Delegate Control*.
3. Pojawi się okno powitalne *Welcome To The Delegation Of Control Wizard*. Kliknij *Next*.
4. W oknie dialogowym *Users Or Groups* kliknij przycisk *Add*, aby wybrać użytkowników lub grupy, którym zostanie przekazana kontrola.
5. Pojawi się okno dialogowe *Select Users, Computers, Or Groups*. Kliknij użytkownika lub grupę, którym chcesz przekazać kontrolę (użyj klawisza *Ctrl*, aby wybrać kilku użytkowników lub kilka grup), a następnie kliknij przycisk *Add* w środkowej części okna. Kliknij *OK*, aby powrócić do okna *Users Or Groups*.
6. Kliknij *Next*, dzięki czemu pojawi się okno *Tasks To Delegate*, które zostało pokazane na rysunku 9.18. Tutaj możliwe jest zdefiniowanie delegowanych zadań.



Rysunek 9.18. *Ekran Tasks To Delegate w kreatorze Delegation Of Control*

7. W sekcji *Delegate The Following Common Tasks* zaznacz dwie opcje o nazwach *Join A Computer To The Domain* (przyłącz komputer do domeny) oraz *Manage Group Policy Links* (zarządzaj łączami zasad grup). Kliknij *Next*.
8. Pojawi się końcowe okno kreatora *Completing The Delegation Of Control Wizard*. Możesz przejrzeć tu wszystkie informacje zawarte w podsumowaniu. Kliknij *Finish*, aby zakończyć pracę kreatora *Delegation Of Control*, po czym powrócisz do konsoli *Active Directory Users and Computers*.

Ta sama procedura może być wykonana w przystawce MMC *Exchange System Manager* do przydzielenia użytkownikom lub grupom ról administracyjnych dla grup administracyjnych. Możliwa jest delegacja kontroli do użytkowników bez konieczności umieszczenia ich w ważniejszych grupach, takich jak globalna grupa zabezpieczeń Domain Admins.

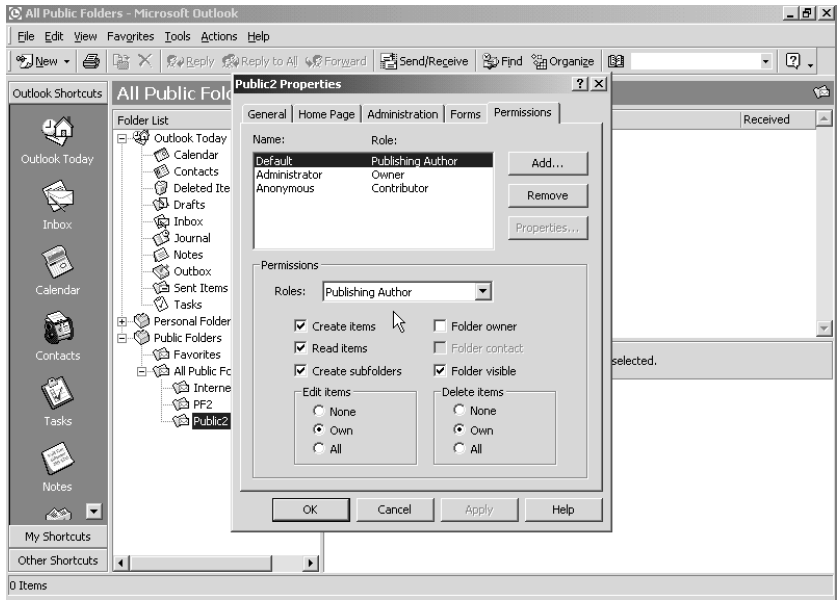
Delegacja kontroli może odbywać się również na poziomie organizacyjnym lub grupy administracyjnej. Przy użyciu kreatora można przydzielić następujące uprawnienia:

- *Exchange Administrator* — użytkownik lub grupa mogą w pełni administrować informacjami systemowymi serwera Exchange, ale bez kontroli dostępu do organizacji lub możliwości modyfikacji uprawnień do innych obiektów.
- *Exchange Full Administrator* — użytkownik lub grupa mogą w pełni administrować informacjami systemowymi serwera Exchange oraz modyfikować uprawnienia.
- *Exchange View Only Administrator* — użytkownik lub grupa mogą przeglądać informacje konfiguracji Exchange.
- *Mailbox Manager* — użytkownik lub grupa mogą włączać obsługę skrzynki pocztowej innym użytkownikom, grupom lub kontaktom; konieczne jest jednak dodanie takiego użytkownika lub grupy również do właściwej grupy zabezpieczeń Windows 2000, jak, na przykład, Account Operators. Ta opcja pojawia się tylko w przypadku konfiguracji uprawnień na poziomie grupy administracyjnej.

Ograniczenie dostępu do folderów publicznych w Outlooku 2000

Foldery publiczne mogą być utworzone przy użyciu przystawki MMC *Exchange System Manager* lub programu Outlook. W obu tych przypadkach właściwości folderu publicznego mogą być skonfigurowane w taki sposób, aby ograniczyć dostęp dla niektórych użytkowników lub grup w celu delegacji uprawnień. Aby tego dokonać:

1. Uruchom Microsoft Outlook 2000 i na liście *Folders* rozwiń kontener *Public Folders*. Kliknij prawym przyciskiem myszy *All Public Folders* i wybierz polecenie *New Folder*.
2. W polu *Create New Folder* wprowadź nazwę `Public2` dla nowego folderu publicznego, w polu *Folder Contains* wybierz *Mail Items*, a następnie w wyświetlonej poniżej hierarchii folderów kliknij *All Public Folders*. Kliknij *OK*.
3. Kliknij *No*, kiedy zostaniesz zapytany o chęć utworzenia skrótu dla tego folderu publicznego w pasku narzędzi Outlooka.
4. Kliknij prawym przyciskiem myszy nowy folder publiczny w drzewie *All Public Folders* i wybierz polecenie *Properties*. Kliknij zakładkę *Permission* i przyjrzyj się domyślnym właściwościom (zobacz rysunek 9.19).
5. Na liście *Name* zaznacz konto *Administrator*, a następnie rozwiń listę *Roles* w celu wyświetlenia ról dla tego folderu publicznego, które mogą być przydzielone dla użytkowników lub grup:
   - *Owner* — przyznaje wszystkie uprawnienia do tego folderu, dzięki czemu użytkownicy mogą czytać, tworzyć, modyfikować i usuwać wszystkie elementy w tym folderze.
   - *Publishing Editor* — przyznaje użytkownikom uprawnienia do tworzenia, modyfikacji, czytania i usuwania wszystkich elementów w tym folderze, a także do tworzenia podfolderów.



Rysunek 9.19. *Zakładka Permissions dla nowego folderu publicznego w Outlooku 2000*

- *Editor* — przyznaje użytkownikom uprawnienia do tworzenia, modyfikacji, czytania i usuwania wszystkich elementów w tym folderze.
- *Publishing Author* — przyznaje użytkownikom uprawnienia do tworzenia i czytania elementów w tym folderze lub do modyfikacji i usuwania utworzonych przez nich elementów.
- *Author* — przyznaje użytkownikom uprawnienia do tworzenia i czytania elementów w tym folderze, a także do modyfikacji i usuwania utworzonych przez nich elementów.
- *Nonediting Author* — przyznaje użytkownikom uprawnienia do tworzenia i czytania elementów w tym folderze.
- *Reviewer* — przyznaje użytkownikom uprawnienia tylko do odczytu tego folderu.
- *Contributor* — przyznaje użytkownikom uprawnienia do tworzenia elementów w tym folderze publicznym bez możliwości przeglądania jego zawartości.
- *None* — brak jakichkolwiek uprawnień do tego folderu.

6. Wybierz rolę *Publishing Editor* i przyjrzyj się opcjom dla tej roli. Zauważ także, iż ten użytkownik może teraz edytować i usuwać wszystkie elementy. Folder może stać się „niewidzialny” dla tego użytkownika poprzez usunięcie opcji *Folder Visible*.
7. Kliknij *OK*, aby powrócić do ekranu Outlooka 2000.

Konwersja uniwersalnych grup dystrybucyjnych do uniwersalnych grup zabezpieczeń w celu zabezpieczenia dostępu do folderów publicznych

Listy dystrybucyjne były używane do kontroli dostępu do folderów publicznych w Exchange 5.5. Takie listy zostały zastąpione przez uniwersalne grupy dystrybucyjne Active Directory w Windows 2000. Konwersją list dystrybucyjnych Exchange 5.5 zajmuje się łącznik ADC. Choć uniwersalne grupy dystrybucyjne mogą rozwijać listy adresów emailowych podobnie jak listy dystrybucyjne, to nie mogą być zakwalifikowane jako główny obiekt zabezpieczeń w Windows 2000. Z tego powodu takie grupy nie mogą być użyte do przydzielania uprawnień do folderów publicznych. Aby zabezpieczyć dostęp do folderów publicznych w Exchange 2000, konieczne jest utworzenie uniwersalnych grup zabezpieczeń.

Uniwersalna grupa dystrybucyjna może być przekonwertowana do uniwersalnej grupy zabezpieczeń, tylko jeśli domena Windows 2000 działa w trybie macierzystym. Istnieją pewne warunki, które umożliwiają taką konwersję grup w celu zapewnienia dostępu do folderów publicznych:

- Jeśli folder publiczny Exchange 5.5 jest replikowany do Exchange 2000, a lista ACL tego folderu wykorzystuje uniwersalną grupę dystrybucyjną, to łącznik ADC tworzy tymczasową uniwersalną grupę dystrybucyjną w Windows 2000 przed jej konwersją do uniwersalnej grupy zabezpieczeń.
- Jeśli aktualizowany jest magazyn folderów publicznych Exchange 5.5, a lista ACL tego obiektu wykorzystuje uniwersalną grupę dystrybucyjną, to magazyn folderów publicznych Exchange 2000 dokona konwersji wszystkich uniwersalnych grup dystrybucyjnych, jakie zostaną utworzone przez ADC, do uniwersalnych grup zabezpieczeń.
- Jeśli do listy ACL folderu publicznego w Exchange 2000 zostanie dodana uniwersalna grupa dystrybucyjna, to magazyn folderów publicznych przekonwertuje tę grupę do uniwersalnej grupy zabezpieczeń.

Jeśli uniwersalna grupa dystrybucyjna nie zostanie przekonwertowana do uniwersalnej grupy zabezpieczeń (gdy proces konwersji nie powiódł się), magazyn folderów publicznych Exchange 2000 będzie próbował powtórzyć ten proces, kiedy jakiś użytkownik spróbuje uzyskać dostęp do folderu. Może się to zdarzyć, jeśli uniwersalna grupa dystrybucyjna działa w domenie Windows 2000 trybu mieszanego. Administrator może natknąć się w Exchange 2000 na problemy, jeśli uniwersalna grupa dystrybucyjna została przekonwertowana do uniwersalnej grupy zabezpieczeń, a następnie ręcznie przekształcona z powrotem do grupy dystrybucyjnej. Kiedy użytkownik spróbuje uzyskać dostęp do tego folderu publicznego, to tym razem uniwersalna grupa dystrybucyjna nie zostanie automatycznie przekonwertowana do grupy zabezpieczeń. W tym celu należy zmienić odpowiednie uprawnienia grupy dystrybucyjnej.

Magazyn folderów publicznych nie dokona konwersji uniwersalnej grupy dystrybucyjnej, która została dodana do istniejącej uniwersalnej grupy zabezpieczeń.

Instalacja łącznika ADC z umową połączenia w środowisku Exchange trybu mieszanego

W czasie migracji do Exchange 2000 bardzo ważna jest konsolidacja dwóch elementów — skrzynki pocztowej Exchange 5.5 i jej głównego konta Windows NT 4 — w jeden obiekt użytkownika z włączoną obsługą poczty lub skrzynki pocztowej w Windows 2000. Przed wdrożeniem pierwszego serwera Exchange 2000 w bazie danych Active Directory należy umieścić obiekty użytkowników z Exchange 5.5. Jest to konieczne, ponieważ Exchange 2000 nie ma bezpośredniego dostępu do bazy danych katalogu Exchange 5.5. Aby migracja systemu powiodła się, należy zapewnić wzajemną synchronizację między katalogiem Exchange 5.5 i Active Directory w Windows 2000.

Aby tego dokonać, konieczna jest instalacja i konfiguracja łącznika ADC z Exchange 2000. Łącznik będzie wymagany aż do momentu aktualizacji wszystkich serwerów Exchange 5.5 do Exchange 2000. Od tej chwili organizacja z Exchange 2000 będzie działała w trybie macierzystym.

Aby zainstalować łącznik ADC z Exchange 2000, należy spełnić następujące wymagania:

- Łącznik ADC jest instalowany na serwerze członkowskim z Windows 2000 i Exchange 2000. Konieczna jest również instalacja zestawu SP-1 dla Windows 2000 Server.
- Konto Windows 2000 używane do instalacji łącznika ADC nie jest kontem usługi Exchange 5.5, ale musi być zalogowane w tej samej domenie, co serwer Exchange.
- Konto używane do instalacji łącznika ADC musi mieć uprawnienia Exchange 2000 Enterprise Admins do serwera członkowskiego, a także prawa Domain Admins do wszystkich domen, z którymi będzie się łączył ADC. To konto wymaga również uprawnień Server Operator dla serwera Exchange 5.5.
- Konieczne jest wdrożenie wszystkich niezbędnych usług Windows 2000 i DNS, włączając w to funkcję dynamicznej aktualizacji DNS.
- Docelowy punkt końcowy ADC powinien zawierać serwer Exchange 5.5 z zestawem poprawek SP-3.

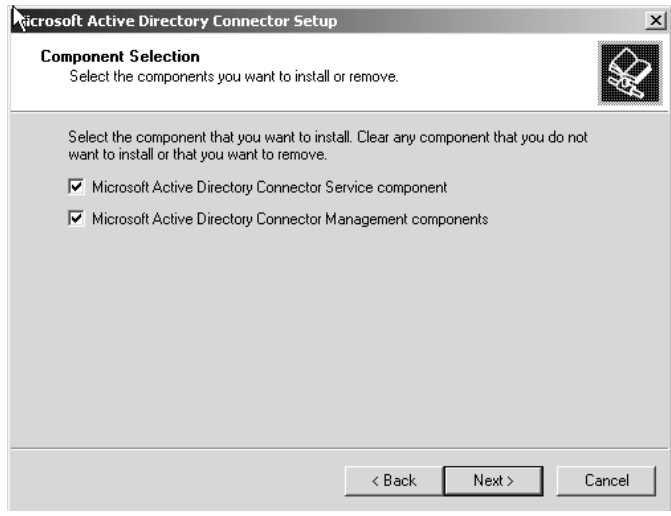
Aby zainstalować i skonfigurować łącznik ADC:

1. Umieść płytę instalacyjną Exchange 2000 w napędzie CD-ROM i kliknij *Start|Run*. W oknie dialogowym *Open* podaj ścieżkę do pliku wykonywalnego ADC na płycie, wpisując następujące polecenie (podaj literę dysku dla napędu CD):

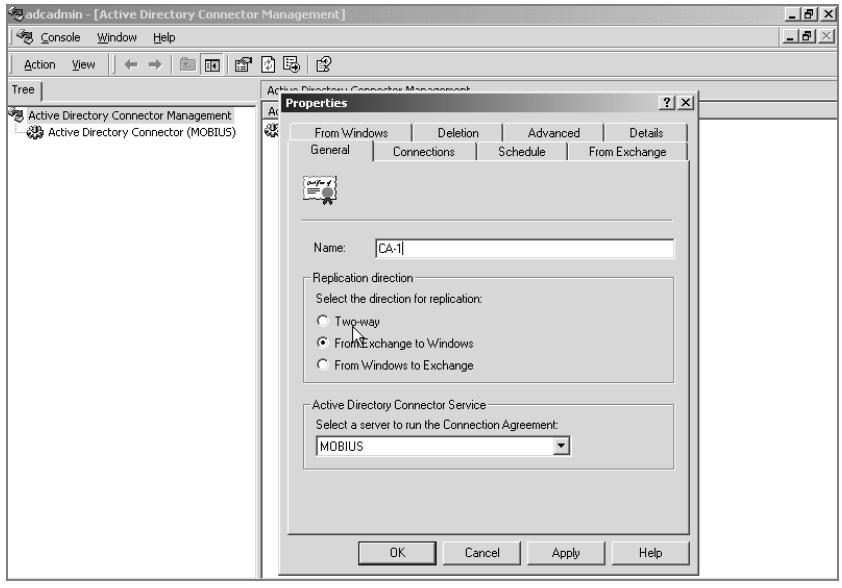
   ```
   litera_dysku:\ADC\I386\SETUP.EXE
   ```

2. Kliknij *OK*, aby kontynuować.
3. Kiedy pojawi się ekran powitalny *Active Directory Connector Setup Wizard*, kliknij *Next*. Na kolejnym ekranie *Component Selection* wybierz opcje *Microsoft Active Directory Connector Service Component* i *Microsoft Active Directory Connector Management Components*, a następnie kliknij *Next* (zobacz rysunek 9.20).

Rysunek 9.20. *Ekran wyboru komponentów w kreatorze Active Directory Connection Setup Wizard*



4. Na ekranie *Install Location* zaakceptuj domyślne położenie ADC (*C:\Program Files\MSADC*) i kliknij *Next*.
5. Na ekranie *Service Account* podaj nazwę użytkownika i hasło, jakie będzie używane do uruchomienia łącznika ADC. Kliknij *Next*.
6. Na kolejnym ekranie pojawi się pasek postępu instalacji łącznika ADC. Jest to dowód aktualizacji schematu Windows 2000. Po zakończeniu tego etapu instalacji pojawi się końcowe okno *Completing The Active Directory Connector Installation Wizard*. Kliknij *Finish*.
7. Otwórz narzędzie ADC poprzez wybranie *Start|Programs|Microsoft Exchange|Active Directory Connector*. Pojawi się konsola *Active Directory Connector Management*.
8. Kliknij prawym przyciskiem myszy łącznik ADC w panelu po lewej stronie konsoli i wybierz polecenie *New|Connection Agreement*. Pojawi się ekran *Properties*.
9. W polu *Name* zakładki *General* wpisz nazwę `CA-1` i kliknij opcję *Two-way* (replikacja dwukierunkowa) w sekcji *Replication Direction* (zobacz rysunek 9.21). Wybranie tej opcji spowoduje wyświetlenie nowego okna komunikatu, w którym należy podać konto Windows 2000 z uprawnieniami do zapisu w katalogu Exchange 5.5. Kliknij *OK*.
10. Wybierz zakładkę *Connections* i sprawdź, czy w polu *Windows Server Information* znajduje się właściwy serwer, oraz czy wybrany sposób uwierzytelniania (*Authentication*) to *Windows Challenge/Response*.
11. W sekcji *Connect As* kliknij *Modify*. Pojawi się okno dialogowe *Connect As (Windows Server)*. Wpisz nazwę konta *Administrator* i podaj hasło administratora. Kliknij *OK*.
12. W sekcji *Exchange Server Information* w zakładce *Connections* podaj nazwę serwera Exchange 5.5 i zmień numer portu na `390` (nie 389).



Rysunek 9.21. *Ekran właściwości dla nowej umowy połączenia ADC*

13. W sekcji *Connect As* kliknij ponownie *Modify*. W kolejnym oknie dialogowym *Connect As (Exchange Server)* wpisz `Administrator` i podaj hasło administratora Exchange. Kliknij *OK*.

14. Wybierz zakładkę *Schedule* i wybierz przełącznik *Always* (zawsze) jako terminarz replikacji. Zaznacz również opcję *Replicate The Entire Directory The Next Time The Agreement Is Run* (wykonaj replikację całego katalogu, kiedy umowa zostanie następnym razem uruchomiona).

Ostatnia część procedury instalacji i konfiguracji łącznika ADC jest związana z wyborem kontenerów, które będą źródłem i miejscem docelowym dla replikacji obiektów. Aby tego dokonać:

1. W zakładce *From Exchange* kliknij *Add*, aby wybrać kontener *Recipient*, z którego pobierane będą aktualizacje obiektów. Kiedy pojawi się okno dialogowe *Choose A Container*, przejdź do serwera Exchange 5.5 i wybierz kontener *Recipients*. Kliknij *OK*.

2. Kliknij *Modify* w sekcji *Default Destination* (domyślne miejsce docelowe), a następnie wybierz *Users Container* w oknie dialogowym *Choose A Container*. Przejdź do zakładki *From Windows*.

3. Kliknij *Add*, aby wybrać kontener jednostki organizacyjnej, z którego będą pobierane aktualizacje. Kiedy pojawi się okno dialogowe *Choose A Container*, zaznacz jednostkę organizacyjną *Users* i kliknij *OK*.

4. Kliknij *Modify* w sekcji *Default Destination*, a następnie wybierz kontener *Recipients* w oknie dialogowym *Choose A Container*. Kliknij *OK*. Na dole okna zaznacz również opcję *Replicate Secured Active Directory Objects To The Exchange Directory* (replikuj zabezpieczone obiekty Active Directory do katalogu Exchange) i kliknij *OK* po raz ostatni.

W tym momencie łącznik ADC jest już zainstalowany i skonfigurowany. Być może pojawią się okna dialogowe potwierdzające następujące kwestie (potwierdź je, klikając *OK*):

- Pierwsze okno dialogowe informuje, iż jest to pierwsza umowa połączenia w organizacji.
- Kolejne okno dialogowe informuje, iż domena Windows 2000 działa w trybie mieszanym.
- Ostatnie okno dialogowe informuje, że Exchange 2000 utworzył uniwersalne grupy zabezpieczeń dla ADC.

Skonfigurowana umowa połączenia umożliwia replikację obiektów użytkowników między katalogiem Exchange 5.5 i Active Directory poprzez utworzenie wyłączonych kont Windows 2000 dla każdej skrzynki pocztowej Exchange 5.5, która nie jest powiązana z obiektem Active Directory. Po zakończeniu tej procedury możesz zamknąć konsolę *ADC Management* (lub *adcadmin.exe*).