Po prostu o sieciach

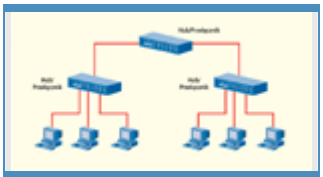
Żeby mieć serwer, trzeba mieć najpierw sieć. Można ją zbudować z wielu różnych elementów i na wiele sposobów. Tylko cel pozostaje zawsze ten sam. Sieć ma dostarczać do naszego stanowiska pracy wszystkie możliwe narzędzia i usługi, które pracę tę będą ułatwiać.

Dostarczanie narzędzi i usług to zadania pakietu SBS 2003. Natomiast zbudowanie platformy sprzętowej, na której system będzie działał, należy całkowicie do nas (pomijając, oczywiście, możliwość zlecenia tej pracy komuś innemu). Poniżej zamieszczamy krótki wstęp do zagadnień budowy sieci komputerowych.

Sieci lokalne Ethernet

Najbardziej rozpowszechnionym standardem sieci lokalnych jest **Ethernet**, który definiuje zarówno zasady łączenia urządzeń, jak i przesyłania danych. W swojej już dość długiej - jak na skalę komputerową - historii standard stale ewoluował, a szybkość transmisji wzrastała, przy czym ostatnio są to zmiany nawet o rząd wielkości.

Obecnie sieci ethernetowe buduje się, wykorzystując kable miedziane i światłowody. Kable miedziane stosuje się zazwyczaj w sieciach lokalnych, gdzie króluje **skrętka**, czyli kabel złożony z czterech par skręconych przewodów. Skrętka jest wygodna, ponieważ kabel jest elastyczny i można go prawie dowolnie układać. Jednocześnie łatwo podłącza się urządzenia za pomocą tych kabli, ponieważ są to zwykłe połączenia elektryczne, które przypominają rozwiązania stosowane w telefonii analogowej. **Światłowody** mają trochę większe wymagania. Nie można ich zginać (bo albo pękną, albo światło się źle odbije), a do przycinania konieczne są specjalne narzędzia. Również same końcówki są bardziej skomplikowane i dużo droższe. Jednak za pomocą światłowodów łatwiej osiągać szybsze transmisje, a ze względu na mniejsze straty sygnał można przesłać na większą odległość (2 km), podczas gdy skrętka umożliwia przesyłanie danych tylko na odległość 100 m. Skrętka jest też łatwiejsza do podsłuchania i bardziej podatna na zakłócenia. Niemniej to właśnie cena i wygoda zadecydowały o jej powszechnym stosowaniu w sieciach lokalnych. Obecnie większość sieci Ethernet pracuje z prędkością 100 Mb/s, a powoli standardem staje się Gigabit Ethernet, w którym dane przesyłane są z prędkością 1000 Mb/s.



Rys. 1. Najbardziej rozpowszechnione sieci Ethernet mają strukturę gwiazdy, mimo że w rzeczywistości przekaźnik komunikacyjny stanowi jedną wspólną, wielodostępną szynę do transmisji danych.

Topologia sieci, a więc sposób łączenia ze sobą urządzeń, w przypadku Ethernetu ma strukturę gwiazdy. Komputery i inne urządzenia sieciowe podłącza się do wspólnego węzła. Każda komunikacja między dwoma urządzeniami przechodzi więc przez ten centralny punkt. Nic nie stoi na przeszkodzie, aby węzły były urządzeniami końcowymi innych węzłów. W ten sposób można zbudować hierarchiczną strukturę, która łączy ze sobą wiele pojedynczych struktur gwiaździstych i sama ma strukturę gwiazdy. W takim przypadku sygnał wysłany z jednego komputera, zanim dojdzie do drugiego, może przejść przez wszystkie węzły, ale nie musi - to zależy od odległości między komputerami. Jeśli znajdują się w obrębie jednego węzła, będzie on jedynym pośrednikiem w transmisji.

Zanim przejdziemy do omawiania urządzeń sieciowych, konieczne jest wyjaśnienie pojęcia segmentu sieci oraz poznanie sposobu, w jaki urządzenia komunikują się ze sobą w jego obrębie. Otóż segment jest to fragment sieci ograniczony ze względu na maksymalną odległość między dwoma urządzeniami, a także maksymalną liczbę urządzeń pośredniczących. Ograniczenia te wynikają z fizycznych cech stosowanych przewodów i sygnałów oraz zasad

komunikacji. W Ethernecie wszystkie urządzenia są równouprawnione, jeśli chodzi o dostęp do transmisyjnego kabla. Każde urządzenie może w dowolnym momencie zacząć nadawać dane. Może zatem dojść do kolizji, gdy dwa urządzenia zaczną nadawać w tym samym momencie. Jeżeli tak się zdarzy, każde odczeka chwilę (czas dobierany jest losowo) i spróbuje ponownie. Co więcej, ponieważ wszystkie urządzenia podłączone są do tego samego kabla, to każde może odbierać wszystkie przesyłane w sieci informacje. Mówimy tu jednak na razie o odbieraniu sygnałów elektrycznych. Za chwilę przekonamy się, że możliwość ta jest różnymi sposobami ograniczana.

Teraz możemy się przyjrzeć urządzeniom sieciowym. Pomijając karty sieciowe zainstalowane w komputerach, jednym z najprostszych urządzeń sieciowych jest **hub**. Pełni funkcję węzła, do którego podłącza się pozostałe urządzenia. Zasada działania huba jest prosta. Po otrzymaniu dowolnego sygnału na jednym z portów (port rozumiemy na razie jako gniazdo, które stanowi jednocześnie wejście i wyjście sygnału, natomiast później, podczas omawiania protokołów sieciowych, port będzie miał inne znaczenie), wysyła ten sygnał do wszystkich pozostałych portów. Można sobie wyobrazić, że wszystkie gniazda są ze sobą po prostu zwarte.

Rys. 2. Mosty przekazują ramki z jednej sieci do drugiej i są przezroczyste dla transmisji danych. Komunikujące się komputery nie mogą stwierdzić, że są podłączone do dwóch różnych sieci.

Do zbudowania najprostszej sieci Ethernet, w której działają co najmniej trzy komputery, oprócz trzech kart sieciowych potrzebny jest właśnie hub (dwa komputery można ze sobą połączyć bez huba specjalnym, tzw. skrosowanym kablem). Skoro już mamy sieć, spójrzmy, w jaki sposób urządzenia przesyłają do siebie dane.

Adresy MAC, pakiety i ramki

Każde urządzenie końcowe sieci Ethernet ma przypisany unikatowy 48-bitowy adres. Jest to tzw. **adres MAC**. Producenci sprzętu numerują każdy egzemplarz swojego urządzenia w ramach przyznanej im puli numerów, co zapewnia, że numery są unikatowe w skali światowej. Może się wydawać, że nie jest to konieczne, ponieważ jedna sieć Ethernet i tak nie oplotłaby całej Ziemi, ale przecież może się zdarzyć, że w jednej sieci znajdą się urządzenia produkowane na dwóch końcach świata.

Jeżeli za jednostkę informacji przyjmiemy pojedynczy bit, to pakietem nazwiemy ciąg bitów o określonej długości. Ogólnie rzecz biorąc, **pakiet** to porcja danych. Jednak w przypadku Ethernetu zamiast pakietu stosuje się pojęcie **ramki**. Urządzenia sieciowe przesyłają więc między sobą ramki. Oprócz informacji ramka zawiera też adres nadawcy i adres odbiorcy. Są to wspomniane adresy MAC.

Karty sieciowe w komputerach mają więc przypisane unikatowe adresy IP i mogą przesyłać do siebie ramki informacji. Jedynym warunkiem jest znajomość adresu odbiorcy, ponieważ karty sieciowe w domyślnym trybie pracy odbierają tylko ramki dla nich przeznaczone. Pozostałe ramki są odbierane przez kartę, ale nieprzekazywane do komputera - zostają pominięte. Wyjątkiem jest rozgłaszanie, czyli wysyłanie ramki do wszystkich odbiorców. W takim razie jako adres odbiorcy w ramce wpisany jest tak zwany adres rozgłoszeniowy, co powoduje, że każda karta sieciowa (znów w domyślnej konfiguracji) odbierze taką ramkę.

Zatem po sieci krąży wiele ramek, a każde urządzenie odbiera tylko te, które są do niego przeznaczone.

W małej sieci nie sprawia to żadnego problemu, ale w bardziej złożonych konfiguracjach może być przyczyną zbędnego ruchu. Ramki będą trafiać również do tych węzłów sieci, do których nie jest podłączony odbiorca. Rozwiązaniem problemu są **przełączniki**, czyli następne - stojące w hierarchii zaraz po hubach - urządzenia sieciowe.

Przełączniki charakteryzuje to, że odbierane przez nie ramki nie są rozsyłane do wszystkich innych urządzeń. Przełącznik, odbierając ramkę, sprawdza jej adres odbiorcy i przekazuje tylko do tego portu, który prowadzi do odbiorcy. Tylko skąd przełącznik wie, do którego portu podłączony jest dany odbiorca? Rzeczywiście na początku nie wie, ale na podstawie obserwacji adresów nadawcy nadchodzących ramek z czasem buduje tablicę wiążącą poszczególne porty z adresami komputerów. W efekcie przełączniki łączą ze sobą tylko nadawcę i odbiorcę, a zatem zmniejszają zbędny ruch w sieci. Dodatkowo transmisja wykorzystująca dwa wybrane porty przełącznika nie blokuje transmisji w pozostałych portach. Sieć z przełącznikami, w przeciwieństwie do sieci opartej na hubach, umożliwia równoległe komunikowanie się wielu urządzeń.

Obok hubów i przełączników w sieciach lokalnych ważną funkcję pełnią też **mosty**. Dotyczy to zwłaszcza większych sieci, w których występują znaczne odległości między urządzeniami. Most łączy dwa segmenty sieci Ethernet i jego zadaniem jest przekazywanie wszystkich ramek z jednego segmentu do drugiego w obu kierunkach. Most można porównać z komputerem wyposażonym w dwie karty sieciowe, z których obie odczytują wszystkie ramki pojawiające się w jednym segmencie i wysyłają je do drugiego segmentu. Różnica polega na tym, że most, wysyłając ramkę do drugiego segmentu zachowuje oryginalny adres nadawcy ramki. Odbiorca nie może zatem stwierdzić, że w przekazanej do niego ramce pośredniczył most. Most jest urządzeniem przezroczystym dla transmisji danych. Podobnie jak w przypadku przełączników, większość mostów buduje tablice adresów MAC dla obu segmentów sieci i przekazuje tylko te ramki, które rzeczywiście powinny trafić do drugiego segmentu.

Sieć mniejszych sieci

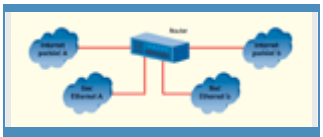
Sieci lokalne Ethernet z adresowaniem MAC dobrze się sprawdzały w zamkniętych, odizolowanych ośrodkach, jak laboratoria badawcze, uczelnie czy zwykłe firmy. Budowane wtedy aplikacje użytkowe bezpośrednio komunikowały się z kartami sieciowymi i wysyłały ramki do odbiorców identyfikowanych przez ich adresy MAC, zwane również adresami fizycznymi. Z czasem pojawiła się potrzeba zapewnienia komunikacji między tymi ośrodkami. Niezbędna była sieć, która połączyłaby ze sobą wszystkie sieci lokalne. Ich bezpośrednie połączenie nie wchodziło w grę, ponieważ często nie były ze sobą całkowicie zgodne, po pierwsze dlatego, że standard Ethernet ewoluował, a po drugie dlatego, że nie był jedynym stosowanym rozwiązaniem, jeśli chodzi o budowę sieci lokalnej.

Sieci lokalne połączył Internet, który w rzeczywistości jest siecią sieci. Mógł połączyć wszystkie zgodne i niezgodne ze sobą sieci lokalne, wprowadzając swojego rodzaju warstwę abstrakcji. Został nadbudowany nad sieciami lokalnymi i wprowadził własny format pakietu, zasady transmisji i adresowanie, jednym słowem - nowy protokół komunikacyjny, nazwany **protokołem IP** (**Internet Protocol** - w rzeczywistości jest to cała grupa protokołów). Adresy stosowane w Internecie nazywa się adresami IP dla odróżnienia na przykład od adresów MAC. Zatem bez względu na architekturę sieci lokalnej wszystkie komputery podłączone do różnych sieci lokalnych znalazły się jednocześnie w jednej wielkiej sieci Internet.

Internet można nazwać siecią logiczną nadbudowaną nad siecią fizyczną, ponieważ transmisja danych i tak odbywa się na najniższym poziomie sieci lokalnych, które posługują się różnymi formatami ramek, sposobami połączeń i zasadami transmisji. Informacja przesyłana pomiędzy dwoma odległymi komputerami w Internecie może przejść przez wiele sieci lokalnych różnego typu i być przesyłana za pomocą najróżniejszych formatów ramek, nawet o różnej długości. W jaki sposób pakiety IP znajdują swoich odbiorców, skoro sieć jest w pewnym sensie abstrakcją sieci działających pod spodem? Otóż pracuje na to cały zestaw protokołów IP, które tłumaczą **adresy IP** na adresy wykorzystywane w danej sieci lokalnej i odwrotnie oraz sterują przekazywaniem pakietów z jednej sieci lokalnej do drugiej. W końcu pakiet trafia do takiej

sieci, w której jeden z komputerów, oprócz swojego fizycznego adresu MAC, ma przypisany również adres IP zgodny z adresem IP odbiorcy pakietu. W naszej analizie sieci doszliśmy więc do etapu jednej globalnej sieci, w której przesyła się pakiety i która wykorzystuje adresowanie IP.

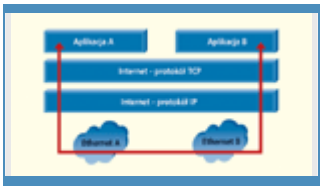
Adresy IP, podsieci i protokoły



Rys. 3. Co prawda routery fizycznie łączą ze sobą sieci Ethernet, ale połączenie logiczne dotyczy dwóch podsieci Internetu.

Obecnie w Internecie stosuje się **32-bitowe adresy IP**, zapisywane dla wygody w postaci oddzielonych kropkami czterech liczb (czterech bajtów) z zakresu 0-255, np. 127.0.0.1. Adresy IP identyfikują każde urządzenie, które może nadawać lub odbierać dane. Adresy IP nadawcy i odbiorcy są elementem pakietu przesyłanego w Internecie. Mimo wprowadzenia globalnej sieci, umożliwiającej komunikację dowolnych dwóch urządzeń, zdecydowano się podzielić całą przestrzeń adresową na podsieci. Dzięki temu fragmenty Internetu stały się znów sieciami lokalnymi, przy czym można łatwo przekazywać pakiety pomiędzy nimi, ponieważ nie mamy już do czynienia z różnymi formatami ramek i różnymi fizycznymi urządzeniami. Podsieci ułatwiają przy tym zarządzanie i przydzielanie adresów. Również wysłanie pakietu rozgłoszeniowego, czyli do wszystkich, dotyczy tylko sieci lokalnej a nie całego świata.

Na początku rozwoju Internetu wprowadzono sztywny podział na **klasy sieci A, B** i **C**. Ustalono, że w **sieci klasy A** pierwszy bajt określa numer sieci, a pozostałe trzy bajty numer komputera w tej sieci. Bajt może przyjmować 256 różnych wartości, ale wartości 0 i 255 są zarezerwowane. Mogły być zatem 254sieci klasy A, a w każdej ponad 16 milionów komputerów (dokładnie 256 x 256 x 254). W **sieci klasy B** dwa bajty przypadały na numer sieci i dwa na numer komputera. Mogło więc być ponad 65 tysięcy (256 x 254) takich sieci, a w każdej z nich również ponad 65 tysięcy komputerów. Natomiast **sieci klasy C**, gdzie trzy bajty określały numer sieci, a jeden pozostawał na numer komputera, mogło być ponad 16 milionów, przy czym w każdej mogły być tylko 254 komputery. Powyższe obliczenia byłyby prawdziwe tylko w przypadku, gdyby wszystkie sieci były jednego rodzaju. W rzeczywistości sieci trzech klas występowały jednocześnie, a zatem wspólnie korzystały z dostępnej 32-bitowej przestrzeni adresowej, a w konsekwencji sieci każdej klasy mogło być znacznie mniej. Ponieważ obecnie prawie całkowicie zrezygnowano ze stosowania klas i wprowadzono maski podsieci, dodamy tylko, że rozpoznawanie typu sieci odbywało się na podstawie kilku pierwszych bitów adresu sieci.



Rys. 4. Aplikacje komunikują się za pomocą protokołów TCP/IP, jednak przesyłanie informacji i tak odbywa się na najniższym poziomie Ethernetu.

Maski podsieci zlikwidowały sztywny podział. Zamiast klas, w których podział adresu IP na numer sieci i numer komputera odbywał się zawsze na granicy bajtów, wprowadzono podział na granicy pojedynczych bitów. Maski podsieci to również liczby 32-bitowe, przy czym w swojej reprezentacji binarnej składają się z dwóch **podciągów**. Pierwszy, złożony z samych jedynek, określa, że bity na odpowiadających pozycjach w adresie IP oznaczają adres sieci. Natomiast drugi podciąg, złożony z samych zer, określa, że bity na odpowiadających pozycjach w adresie IP oznaczają adres komputera w danej podsieci. W ten sposób, dysponując adresem IP i maską, można na podstawie operacji logicznych wyznaczyć adres sieci, adres komputera w sieci oraz adres rozgłoszeniowy, czyli wszystkich komputerów w danej podsieci.

Znów mamy do czynienia z oddzielonymi sieciami lokalnymi. Tym razem jednak wszystkie mówią tym samym językiem, a przekazywanie pakietów z jednej sieci do drugiej jest dużo łatwiejsze. Zadanie to wykonują **routery**, które zawsze są podłączone do co najmniej dwóch sieci i w najprostszym przypadku przekazują pakiety z jednej do drugiej. Od mostów w sieciach Ethernet różni je, po pierwsze, działanie w wyższej warstwie wykorzystującej protokół IP, a po drugie inna zasada odbierania pakietów ze źródłowej podsieci. O ile most zbiera wszystkie ramki, które krążą po segmencie sieci, o tyle pakiety przeznaczone do wysłania przez router trzeba mu przekazać.

Jeżeli komputery w danej podsieci chcą wysyłać do siebie nawzajem pakiety, łączą się bezpośrednio. Jeżeli natomiast odbiorcą pakietu ma być komputer w innej podsieci, to pakiet musi zostać do niej przekazany przez router. Komputery w danej podsieci oprócz swojego adresu IP znają również maskę podsieci (a więc i numer sieci) oraz adres tzw. bramy domyślnej, czyli routera łączącego z innymi sieciami, dlatego mogą łatwo stwierdzić, czy dany pakiet wysłać do komputera, czy też do routera.

Docelowa podsieć może być też bardzo oddalona od sieci źródłowej. Wtedy wysłany pakiet będzie musiał przejść przez wiele kolejnych routerów, zanim dotrze do odbiorcy. Każdy z tych routerów sprawdzi adres odbiorcy pakietu i przekaże go do kolejnego routera, o którym wiadomo, że prowadzi do podsieci docelowej. A skąd wiadomo? Otóż tak jak mosty w sieci Ethernet budują tablice adresów, tak routery budują tablice tras do innych sieci. W przypadku Internetu może być wiele różnych tras prowadzących do sieci docelowej. Do wyboru najbardziej odpowiedniej wykorzystuje się różne algorytmy routingu (np. najkrótszej drogi albo najkrótszego czasu).

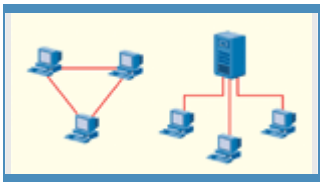
Analiza drogi, którą przebywają pakiety, może nasuwać następującą wątpliwość. Jeżeli pakiet wysyłany do odległej sieci ma wpisany adres odbiorcy w tej właśnie odległej sieci, to w jaki sposób wysłać go pod adres routera, który przecież znajduje się w sieci lokalnej? Trzeba pamiętać, że Internet jest warstwą leżącą nad fizyczną siecią lokalną, a rzeczywiste transmisje odbywają się np. w sieci Ethernet. Zatem pakiet przeznaczony do wysłania przez router, będzie miał, co prawda, wpisany adres odbiorcy z sieci odległej, ale ramka zostanie wysłana pod fizyczny adres lokalny routera. Router odbierze pakiet, mimo że adres odbiorcy nie jest zgodny z jego adresem IP, i przekaże go do kolejnych routerów lub do sieci docelowej, jeśli łączy się z nią bezpośrednio.

Przekazywanie pakietów to jeszcze za mało, aby zbudować wydajną i niezawodną sieć. Protokół IP zapewnia na razie jedynie komunikację między dwoma wybranymi punktami sieci. Potrzebny jest jeszcze sposób kontroli przesyłania danych oraz format, w jakim powinny być przygotowane dane użytkownika. Wprowadzono zatem dwa **protokoły UDP** i **TCP**, które wykorzystują protokół IP. Pierwszy to prosty protokół do przesyłania pojedynczych pakietów, który charakteryzuje się dużą szybkością przesyłania danych. Nie gwarantuje jednak ich dostarczenia, jeśli po drodze nastąpi awaria. TCP jest protokołem bardziej zaawansowanym. Zamiast wysyłać niezależnie pojedyncze pakiety, tworzy najpierw połączenie i kontroluje jego stan. Sprawdza też, czy pakiet został pomyślnie dostarczony, i ewentualnie sygnalizuje błąd. Protokoły UDP i TCP nazywane są protokołami transportowymi w odróżnieniu od protokołu komunikacyjnego IP oraz protokołów niższego poziomu, stosowanych w sieciach lokalnych (np. Ethernet) przy fizycznych połączeniach urządzeń.

Porty, usługi i serwery

Protokoły transportowe pozwalają przesyłać dane już nie tylko między komputerami, ale także pomiędzy działającymi na nich aplikacjami. Ponieważ na jednym komputerze może działać więcej niż jedna aplikacja, pojawiła się konieczność ich rozróżniania. Adres IP jest jeden dla całego komputera (w przypadku pojedynczej karty sieciowej), więc na jego podstawie nie można zidentyfikować aplikacji. Problem rozwiązują porty, które są liczbami 16-bitowymi, a więc na jednym komputerze może być 65 tysięcy portów. Para składająca się z adresu IP oraz numeru portu tworzy tzw. gniazdo, poprzez które aplikacje mogą się ze sobą komunikować. W ten sposób wiele aplikacji na jednym komputerze może się równocześnie komunikować z wieloma aplikacjami na innym komputerze.

W ten sposób doszliśmy do pojęcia **usługi**. Usługi w sieciach komputerowych to właśnie aplikacje, o których wiadomo, że są dostępne pod konkretnym, znanym numerem portu oraz że czekają na zgłoszenia klientów, którzy chcą z nich skorzystać. Usługi mogą zazwyczaj obsługiwać jednocześnie więcej niż jednego klienta, ale wymaga to wykorzystania wielu portów. Ale przecież usługa musi być zawsze dostępna pod tym samym numerem portu! Rozwiązanie jest następujące. Usługa pod znanym numerem portu jedynie nasłuchuje, czy nie nadchodzą zgłoszenia od nowych klientów. Gdy tylko takie zgłoszenie nadejdzie, uruchamia dla niego oddzielne połączenie, wykorzystuje inny numer portu, natomiast sama nadal czeka na kolejne zgłoszenia klientów.



Rys. 5. W sieciach równorzędnych każdy komputer udostępnia zasoby wszystkim pozostałym i sam pilnuje uprawnień, natomiast w sieciach z serwerem wszystko zgromadzone jest w jednym miejscu.

Klienci korzystają zatem z usług udostępnianych przez specjalnie do tego przeznaczone komputery - serwery. Wiele usług nie wymaga jednak specjalnego serwera. Mogą działać na stacjach roboczych klientów i nawzajem udostępniać sobie swoje usługi. Sieci takie nazywa się równorzędnymi, a ich charakterystyczną cechą jest decentralizacja zarządzania, lokalna kontrola dostępu, indywidualne zasady bezpieczeństwa oraz niezależna konfiguracja każdej stacji. Model równorzędny sprawdza się jedynie w bardzo małych sieciach, złożonych z kilku komputerów. Jednak już przy kilkunastu maszynach sama możliwość globalnego zarządzania stacjami przemawia na korzyść sieci z tzw. dedykowanym serwerem. Jeżeli dodamy do tego możliwość bezpiecznego składowania danych, precyzyjną kontrolę dostępu do zasobów, wymuszenie stosowania zasad bezpieczeństwa oraz możliwość świadczenia przez serwer bardzo wielu dodatkowych, dużo bardziej złożonych usług, argumentów za stosowaniem sieci równorzędnych po prostu brak. Na kolejnych stronach pokazujemy, jak osiągnąć maksimum korzyści ze stosowania sieci z dedykowanym serwerem na przykładzie sieciowego systemu operacyjnego Microsoft Windows Small Business Server 2003.

SBS pod lupą

Wiadomo, że SBS 2003 to system sieciowy do małych przedsiębiorstw, ale odpowiedź na pytanie, jakie konkretnie korzyści daje firmie, która postanowi zbudować na nim swój system informatyczny, zajmie już trochę więcej miejsca.

Najbardziej zwięźle system SBS 2003 można zdefiniować jako oparty na Windows Server 2003, przeznaczony do małych przedsiębiorstw kompletny system sieciowy ze zintegrowanym serwerem pocztowym Exchange Server 2003, narzędziami do pracy grupowej, serwerem plików, druku, faksów i dostępu do Internetu, wyposażony dodatkowo w specjalne narzędzia ułatwiające zarządzanie, a jednocześnie pakiet aplikacji, którego duża funkcjonalność w połączeniu ze stosunkowo niskim kosztem dostarcza argumentów za stosowaniem systemu SBS nawet w całkiem niedużych firmach.

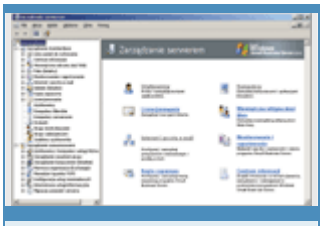
Microsoft Windows Small Business Server 2003 to atrakcyjna oferta dla większości małych firm chociażby ze względu na korzystny stosunek ceny do możliwości. SBS 2003 nie tylko dostarcza kluczowe elementy najnowszych technologii Microsoftu, ale - co nawet ważniejsze - oferuje taki podzakres ich pełnej funkcjonalności, który pokrywa się z najczęstszymi zastosowaniami systemu sieciowego w małej firmie.

Dwie wersje systemu

Dalsze dopasowanie możliwości pakietu do rzeczywistych potrzeb można uzyskać, wybierając edycję Standard albo Premium. Ta ostatnia zawiera serwer baz danych Microsoft SQL Server 2000 oraz zaawansowany firewall Microsoft ISA Server 2000, podczas gdy wersja Standard wykorzystuje wbudowaną zaporę w postaci usługi Routing and Remote Access Services (RRAS).

Do utrzymywania firmowego intranetu, edycja Premium zawiera również FrontPage 2003 z licencją pozwalającą zainstalować program na jednym, wybranym kliencie (nie dotyczy wersji ewaluacyjnej).

Nowoczesne technologie



Rys. 1. Charakterystyczny dla SBS zestaw kreatorów znacznie ułatwiających administrowanie systemem.

SBS 2003 daje firmom dostęp do najnowszych technologii usprawniających działanie przedsiębiorstwa. Główną rolę odgrywa tu Exchange Server 2003 obsługujący firmową pocztę wewnętrzną i zewnętrzną, który dzięki usprawnionej usłudze Microsoft Connector for POP3 Mailboxes może działać także jako pośrednik kont pocztowych utrzymywanych na publicznych serwerach w Internecie. Pracownicy firmy otrzymują przy tym ujednolicony dostęp do wszystkich rodzajów poczty poprzez nowy Outlook 2003, który podobnie jak IE 6.0 (oraz łaty systemowe), jest automatycznie dostarczany do wszystkich stacji klienckich. Natomiast użytkownicy przebywający dużo poza biurem, zawsze mogą dotrzeć do swoich wiadomości, korzystając z technologii Outlook Web Access, która w SBS 2003 została gruntownie przekonstruowana i obecnie umożliwia dostęp do poczty praktycznie z dowolnego miejsca, znajdującego się w zasięgu HTTP. Dotyczy to także urządzeń przenośnych - w szczególności komputerów PocketPC, które komunikują się z serwerem Exchange poprzez Outlook Mobile Access. Pracownikom zdalnym SBS 2003 oferuje także dostęp przez VPN lub usługi terminalowe.

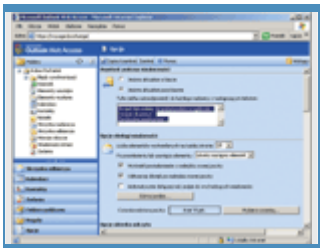
Uproszczona instalacja

Rys. 2. Bezpieczne logowanie do serwera Exchange za pomocą połączenia szyfrowanego.

Instalacja jest prawie całkowicie zautomatyzowana, a liczbę okien dialogowych ograniczono do absolutnego minimum. Na pierwszym etapie instalowany jest sam system operacyjny, co trwa około 40 minut. W tym czasie użytkownik musi jedynie wybrać rozmiar partycji systemowej, podać nazwę komputera i hasło administratora. Drugi etap (około 30 minut) to wstępna konfiguracja systemu, która również nie wymaga od nas dużej aktywności - trzeba podać nazwę domeny oraz domyślne dane kontaktowe dla nowo tworzonych użytkowników.

Jeśli serwer będzie pełnił funkcję zapory i ma dwie karty sieciowe, dodatkowo trzeba wskazać połączenie wykorzystywane w komunikacji z siecią lokalną. Aby serwer pełnił tylko funkcję routera i mógł udostępniać połączenie internetowe, wystarczy jedna karta sieciowa. Ostatni, najdłuższy etap (około 90 minut) to instalacja i konfiguracja komponentów usługowych serwera, takich jak Exchange, SQL Server Desktop Engine, SharePoint Services oraz narzędzia administracyjne. Również i tu interakcja z użytkownikiem jest minimalna, a jego jedynym zadaniem jest wybór instalowanych składników i akceptacja domyślnych lokalizacji folderów. Instalacja i konfiguracja SBS 2003 przypomina więc bardziej instalację pakietu Office niż serwera systemu sieciowego.

Wbudowany system pomocy



Rys. 3. Zdalny dostęp do skrzynki rozwiąże

problemy z nieplanowanym przedłużeniem urlopu.

Można śmiało powiedzieć, że SBS 2003 to więcej niż suma jego elementów, ponieważ oprócz wyboru najważniejszych komponentów systemu sieciowego zawiera spoiwo w postaci licznych kreatorów, które automatyzują wykonywanie typowych czynności administracyjnych. Przykładem jest chociażby sam program instalacyjny, który niepostrzeżenie instaluje katalog Active Directory i konfiguruje go do współpracy z serwerem Exchange oraz usługami SharePoint.

Najbardziej charakterystycznym dla SBS 2003 kreatorem jest Lista zadań do wykonania, która pojawia się po zakończeniu instalacji i konfiguracji serwera oraz aplikacji usługowych. Zawiera zadania administracyjne wypisane w prawidłowej kolejności ich wykonywania - np. przed podłączeniem serwera do Internetu zaleca się przeczytanie informacji o konsekwencjach i związanych z tym potencjalnych zagrożeniach. Zresztą nie tylko tutaj, ale prawie na każdym kroku znajdują się odnośniki do dodatkowych informacji, które pozwolą również niewtajemniczonym prawidłowo skonfigurować serwer.

Centralne zarządzanie

Oprócz możliwości administrowania systemami klientów, które wynikają bezpośrednio z zastosowania modelu domenowego i Active Directory, w SBS 2003 dostępna jest też funkcja dostarczania oprogramowania do komputerów użytkowników. Obejmuje ona instalację przeglądarki Internet Explorer 6, klienta pocztowego Outlook 2003, klienta usługi obsługującej faksy, programu ActiveSync do komunikacji z urządzeniami mobilnymi oraz uaktualnień systemu w postaci Service Pack.

Praca grupowa i zdalny dostęp

Rys. 4. Rozbudowany system pomocy jest zintegrowany z kreatorami pakietu i dlatego prawie w każdym momencie dostępna jest pomoc kontekstowa.

Za współpracę użytkowników i wymianę dokumentów odpowiada Microsoft Windows SharePoint Services - kolejna usługa, która korzysta z najnowszych technologii budowy intranetów oraz przechowywania danych, a konkretnie z serwera WWW Microsoft Internet Information Services 6.0 z obsługą ASP.NET oraz serwera baz danych Microsoft SQL Server 2000 (w wersji Desktop Engine). SharePoint stanowi wygodną - dostępną za pomocą przeglądarki - platformę współdzielenia dokumentów i wymiany informacji. W rzeczywistości jest to firmowa strona intranetowa, która służy jako miejsce wymiany dokumentów i komunikacji zespołów oraz pełni funkcję publicznej tablicy informacyjnej i magazynu danych. Użytkownicy mogą korzystać z globalnych bibliotek i/lub specjalnych list dokumentów związanych tylko z określonym zadaniem, odbierać faksy przekazywane do współdzielonego folderu przez usługę Fax routing i wymieniać informacje organizacyjne. Usługi SharePoint pozwalają też automatycznie informować wszystkich zainteresowanych o zmianie lub pojawieniu się nowych dokumentów i/lub faksów, które obecnie obsługiwane są tak łatwo, jak zwykłe listy elektroniczne.

Zdalny dostęp do sieci firmowej można zrealizować na wiele sposobów w zależności od potrzeb. SBS 2003 oferuje łatwą do uruchomienia usługę serwera dla połączeń VPN oraz zdalnego dostępu poprzez modem. Usługi Remote Web Workplace oraz Connection Manager automatyzują podłączania zdalnego komputera (znajdującego się w dowolnym miejscu w Internecie) do lokalnej sieci - na pulpicie pojawia się dodatkowa ikona, która błyskawicznie nawiązuje połączenie. Z kolei usługa Remote Desktop Web Connection pozwala w oknie przeglądarki (konieczne jest zainstalowanie kontrolki ActiveX) zrealizować podłączenie zdalnego pulpitu nie tylko do serwera SBS, ale i do stacji roboczych. Umożliwia to użytkownikom zdalną

pracę na własnych maszynach, a administratorom - zdalne zarządzanie serwerem oraz firmowym intranetem.

Bezpieczeństwo serwera i sieci

W SBS 2003 bardzo poważnie potraktowano kwestię bezpieczeństwa systemu. Windows Server 2003 ma wbudowany wewnętrzny firewall, co oczwiście nie przeszkadza mu współpracować z dodatkowymi zabezpieczeniami zewnętrznymi. Internet Information Services 6.0 odpowiedzialny za udostępnianie stron internetowych został całkowicie przebudowany i aspiruje do miana najszybszego i najbezpieczniejszego obecnie serwera WWW. Poza tym cały system jest już na wstępie skonfigurowany jako maksymalnie bezpieczny, z uruchomionym minimalnym zestawem usług. Wszystkie pozostałe administrator musi świadomie włączyć, przyjmując do wiadomości informacje o konsekwencjach i koniecznych działaniach profilaktycznych.

Wygodne licencjonowanie

Kupując SBS 2003, oprócz licencji na sam serwer dostajemy również pięć licencji dla klientów (CAL), przy czym mogą być to licencje dla użytkowników lub na urządzenie. Pojedyncza licencja dla użytkownika zezwala mu na dostęp do serwera za pomocą dowolnie wielu urządzeń (komputerów, palmtopów, telefonów komórkowych), natomiast licencja na urządzenie umożliwia wykorzystywanie go przez dowolną liczbę osób. Nie wszystkie licencje muszą być tego samego rodzaju, ale ich suma nie może przekroczyć całkowitej liczby licencji CAL (początkowo pięciu). Dodatkowe licencje można, oczywiście, dokupić, ale ze względu na limit formalny SBS 2003 może obsługiwać do 75 stacji roboczych (istotny wzrost w stosunku do 50 licencji w SBS 2000).

Nowa jakość tworzenia witryn

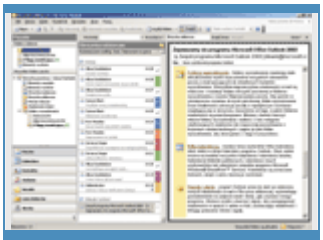
Rys. 5. Strona główna portalu SharePoint w trybie edycji. Zarządzanie układem strony sprowadza się do przeciągania gotowych elementów.

Dodatkowym składnikiem pakietu w wersji Premium jest edytor witryn internetowych Microsoft FrontPage 2003, który został przebudowany z uwzględnieniem próśb i potrzeb zgłoszonych przez użytkowników poprzednich wersji. Znacznie udoskonalono przede wszystkim ergonomię pracy. Edycja kodu i aplikowanie szablonów graficznych, czyli motywów, są dużo wygodniejsze. Ekran może być podzielony na część graficzną i podgląd kodu. Ponadto FrontPage 2003 oferuje inne udoskonalenia: możliwość wyświetlania znaczników w trybie graficznym, lepszą obsługę stylów, siatkę do pozycjonowania elementów, znacznie większe możliwości konfiguracji edytora, funkcjonalne paski narzędzi, funkcję podglądu w różnych przeglądarkach i z różną rozdzielczością, a także optymalizację i kontrolę poprawności kodu.

Wśród najciekawszych właściwości FrontPage 2003 należy wymienić możliwość dołączenia dynamicznego szablonu do zestawu stron, które powinny mieć identyczny układ. Dynamiczne szablony pozwalają nie tylko zdefiniować niezmienne obszary strony, takie jak nagłówki czy elementy nawigacyjne, ale precyzyjnie określić całą strukturę dokumentu, wydzielając obszary automatycznie wypełniane treścią oraz przeznaczone do edytowania przez autorów. W połączeniu z mechanizmem warstw otrzymujemy wygodne narzędzie do tworzenia coraz bardziej złożonych serwisów internetowych, a także firmowego portalu SharePoint. Własne rozszerzenia tej witryny mogą łatwo zachowywać spójny charakter całości.

Budowa stron internetowych coraz bardziej przypomina tworzenie aplikacji multimedialnych, ale narzędziami dużo prostszymi w użyciu. Zestaw rozszerzeń, kreatorów i automatycznych generatorów kodu programu FrontPage 2003 skłania do zastanowienia, czy w ogóle warto cokolwiek programować ręcznie. FrontPage sam generuje skrypty, zarządza arkuszami stylów, tworzy efektowne przyciski i dodaje efekty graficzne. Witryny tworzone za pomocą programu FrontPage mogą też wykorzystywać gotowe kontrolki Web Part, importować informacje z baz danych, przetwarzać dane dostępne w formacie XML czy dołączać elementy portalu SharePoint.

Klient poczty elektronicznej



Rys. 6. Nowy układ interfejsu programu Outlook 2003 zaprojektowano, mając na uwadze wygodę użytkowników.

Domyślnym klientem poczty elektronicznej jest Microsoft Outlook 2003, który instaluje się automatycznie na stacjach roboczych w trakcie podłączania ich do serwera. Najbardziej widoczna w programie zmiana, to nowy układ okien, który pozwala jednocześnie wyświetlać na ekranie więcej informacji. Wiadomości są automatycznie grupowane na przykład na podstawie daty otrzymania i można nimi grupowo zarządzać. Dzięki temu wyszukiwanie i porządkowanie wiadomości odbywa się znacznie szybciej.

Outlook 2003 ma wbudowany nowoczesny filtr wiadomości, który analizuje nadchodzącą pocztę elektroniczną i automatycznie ją klasyfikuje. Niechciane wiadomości trafiają do specjalnego folderu przeznaczonego na wiadomości-śmieci. W podejmowaniu decyzji o przepuszczeniu wiadomości wykorzystywanych jest wiele różnych parametrów, takich jak czas nadania, adres nadawcy czy rodzaj zawartości. Przeprowadzana jest również zaawansowana analiza struktury listu, której wyniki służą do wyciągnięcia wniosków dotyczących charakteru wiadomości.

Usprawnienia dotyczące obsługi programu polegają na wprowadzeniu nowego okna nawigacji, które oprócz wyświetlania listy folderów, pozwala ją także dostosowywać do własnych wymagań. Można na przykład dodawać ulubione foldery i umieszczać je na początku listy albo łatwo przeglądać wszystkie dostępne foldery kontaktów. Okno odczytu ułatwia podgląd wiadomości bez ich otwierania. Z kolei system szybkich znaczników pozwala sprawnie sklasyfikować wiadomości, kiedy nie możemy na nie odpowiedzieć od razu. W ten sposób na podstawie znaczników dotrzemy do wszystkich ważnych wiadomości później. Bardzo wygodnym rozwiązaniem jest też grupowanie wiadomości według wątków, co pozwala oddzielić od siebie wiadomości dotyczące spraw, którymi zajmujemy się równolegle.

Wygodę obsługi oraz elastyczność klienta Outlook 2003 zwiększają także nowe mechanizmy komunikacyjne stosowane przez program podczas połączeń z serwerem Exchange. Oprócz dostępu za pomocą protokołu HTTP, który opakowuje wywołania RPC i przez to umożliwia podłączanie do serwera pocztowego z najbardziej odległych lokalizacji bez używania usługi Outlook Web Access, Outlook 2003 obsługuje też tzw. tryb buforowany serwera Exchange, który pozwala na pracę z serwerem pocztowym nawet przy niepewnych połączeniach sieciowych. Zawartość skrzynki pocztowej i list adresowych jest wtedy okresowo synchronizowana z danymi na serwerze, a zerwanie połączenia nie uniemożliwia dalszej pracy.

Instalacja SBS 2003

Serwer SBS może współpracować z siecią lokalną na kilka sposobów. Wybór któregoś z nich zależy od funkcji, jaką serwer ma pełnić w sieci, oraz od możliwości dodatkowego zainwestowania w sprzęt. Również przygotowanie samej sieci przebiega według różnych scenariuszy w zależności od jej obecnej topologii oraz docelowego kształtu.

Praktycznie każda firma musi mieć jakieś połączenie z Internetem, aby w ogóle funkcjonować. Od rodzaju tego połączenia zależy miejsce serwera w sieci firmowej. Poniżej omówimy najczęściej spotykane konfiguracje.

Przygotowanie sieci

Możliwe konfiguracje

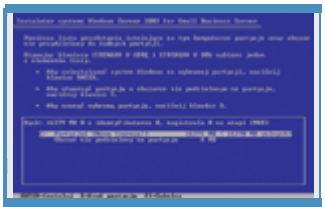
Jeżeli łączymy się z Internetem przez modem, to w serwerze wystarczy zainstalować jedną kartę sieciową do komunikacji z siecią lokalną. Do połączenia z siecią zewnętrzną wykorzystamy

wewnętrzny lub zewnętrzny modem lub kartę ISDN. Serwer będzie pełnił wtedy funkcję bramy do Internetu dla wszystkich pozostałych komputerów w sieci. Karta sieciowa serwera, podobnie jak karty sieciowe wszystkich komputerów, będzie podłączona do wspólnego huba lub przełącznika.

Jeżeli natomiast wykorzystujemy łącze stałe, to na końcu kabla łączącego z dostawcą Internetu na pewno zostanie zainstalowane jakieś urządzanie dostępowe. Zazwyczaj podłącza się je do komputera zwykłym kablem sieciowym, ale zdarzają się też modele np. z interfejsem USB. W przypadku USB urządzenie podłączamy do komputera, podobnie jak zewnętrzny modem. Zwykle trzeba jednak zainstalować w serwerze drugą kartę sieciową do komunikacji z urządzeniem dostępowym.

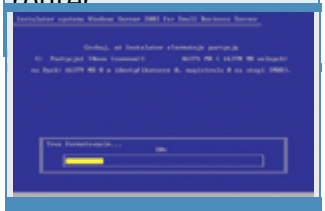
Routery szerokopasmowe

W przypadku routera szerokopasmowego możemy wyróżnić dwie konfiguracje. Po pierwsze, router może bezpośrednio łączyć komputer z Internetem. Wtedy karcie przeznaczonej do komunikacji z siecią zewnętrzną przypisuje się publiczny adres IP i serwer jest widoczny w Internecie. Na takim serwerze powinien bezwzględnie działać programowy firewall, a nie zaszkodzi też wbudowana sprzętowa zapora. Filtrowanie pakietów już na routerze odciąży serwer, który oprócz ochrony przed atakami ma przecież wykonywać mnóstwo operacji związanych z działalnością firmy.



Rys. 4. Aby utworzyć nową partycję, naciskamy klawisz [C] i podajemy jej rozmiar. Jeżeli chcemy na system przeznaczyć cały dysk, wystarczy nacisnąć [Enter].

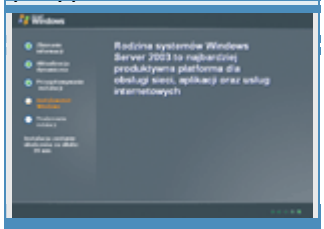
W opisanych dotychczas przypadkach serwer ma dwa interfejsy komunikacyjne (choć nie zawsze są to dwie karty sieciowe) i jest widoczny w Internecie. Może zatem udostępniać swoje usługi klientom zewnętrznym. Ponieważ jednocześnie stanowi bramę do połączeń z Internetem dla komputerów w sieci lokalnej, może kontrolować dostęp użytkowników sieci wewnętrznej do różnych zasobów Internetu. Komputery w sieci lokalnej nie są widoczne w Internecie, ponieważ wykorzystują prywatne adresy IP, a cała komunikacja ze światem zewnętrznym odbywa się za pośrednictwem serwera. Stosując translację adresów (NAT), serwer przesyła pakiety z komputerów lokalnych do Internetu i odwrotnie - pakiety nadchodzące z sieci zewnętrznej przesyła do odpowiednich komputerów w sieci lokalnej.



Rys. 5. Nowa partycja musi zostać sformatowana jako NTFS.

Druga konfiguracja dotyczy routerów szerokopasmowych, które na swoim zewnętrznym interfejsie mają nadal adres publiczny, natomiast na wewnętrznym interfejsie stosują już adresy prywatne. Routery takie sprzętowo realizują translację adresów (NAT) i pełnią funkcję bramy internetowej oraz zapory dla sieci lokalnej. Zazwyczaj mają też wbudowany przełącznik - najczęściej czteroportowy.

W przypadku takiego routera możemy określić, czy chcemy korzystać z serwera jako dodatkowego pośrednika w komunikacji z Internetem. Jeżeli ustawimy go między routerem a siecią lokalną i wyposażymy w dwie karty sieciowe, to uzyskamy podwójne tłumaczenie adresów (NAT). Po raz pierwszy między Internetem a siecią lokalną, a po raz drugi między siecią lokalną a siecią wewnętrzną firmy. Jednocześnie zwiększmy ochronę komputerów użytkowników w sieci wewnętrznej, ponieważ po przejściu przez zaporę sprzętową trzeba będzie się jeszcze przedostać przez zabezpieczenia serwera.



Rys. 6. Środowisko instalacyjne Windows Server 2003.

Przekazywanie portów

Powyższa konfiguracja powoduje jednak pewien problem. Ponieważ serwer znajduje się w sieci lokalnej, nie jest widoczny z Internetu. Nie może zatem udostępniać usług klientom zewnętrznym. Aby serwer, mimo że ma prywatny adres na zewnętrznym interfejsie, był widziany w Internecie, trzeba na

routerze uruchomić przekazywanie portów. Większość routerów ma taką funkcję. Mogą albo przekazywać wszystkie otrzymywane pakiety do wskazanego komputera w sieci lokalnej bez względu na związany z pakietem numer portu, albo działać bardziej wybiórczo, tj. przekazywać pakiety odbierane na określonym porcie do tego samego lub innego portu wskazanego komputera lub nawet różnych komputerów w sieci lokalnej. W pierwszym przypadku wykorzystuje się tzw. port DMZ, natomiast druga usługa określana jest mianem serwerów wirtualnych.

Jeżeli wykorzystujemy router z lokalnym adresem IP, możemy zrezygnować z podwójnej translacji adresów kosztem mniejszego bezpieczeństwa. Serwer nie będzie potrzebował w tym wypadku drugiej karty sieciowej, ale nie będzie mógł też pełnić funkcji zapory internetowej dla sieci lokalnej. Jedynym zabezpieczeniem sieci lokalnej pozostanie prosty sprzętowy firewall wbudowany w router. Programowy firewall zainstalowany na serwerze będzie mógł chronić tylko sam serwer, co i tak jest bardzo ważne, ponieważ po włączeniu przekazywania portów na routerze serwer będzie nadal świadczył usługi dla klientów zewnętrznych.

Aktualizacja, migracja czy nowy serwer?

Jeżeli sieci komputerowej jeszcze nie ma, to najlepiej ją zbudować na podstawie jednego z powyższych modeli (np. rys. 1). Gdy mamy już sieć lokalną, ale bez serwera, to trzeba zdecydować, czy serwer będzie pośrednikiem w komunikacji z Internetem (rys. 1 lub rys. 2), czy też ma być na pozycji równorzędnej względem pozostałych klientów (rys. 3), a następnie przekształcić ją do jednego z powyższych modeli. Jeżeli mamy serwer, pozostaje jedynie zainstalować na nim system SBS 2003. W zależności od używanego systemu operacyjnego serwera stosujemy uaktualnienie lub migrację.

Uaktualnienie z zachowaniem ustawień będzie możliwe, jeśli na serwerze działa Small Business Server 2000, Windows 2000 Server lub Windows Server 2003. Migracja, polegająca na dostawieniu na czas instalacji dodatkowego komputera, na którym zostanie instalowany SBS 2003, i przeniesieniu ustawień ze starego systemu, będzie możliwa, jeżeli na starym serwerze działa jeden z następujących systemów: Small Business Server 4.5, Small Business Server 2000, Windows NT 4.0 Server lub Windows 2000 Server.

Ostatnia możliwość to pozostawienie starego serwera (pod warunkiem, że nie jest kontrolerem domeny, lecz samodzielnym serwerem), dostawienie nowego komputera przeznaczonego na serwer i zainstalowanie na nim nowego systemu Small Business Server 2003.

Instalacja nowego systemu

Instalacja systemu operacyjnego serwera

Instalacja SBS 2003, niebędąca uaktualnieniem bieżącego systemu operacyjnego, przebiega podobnie, jak każdego innego systemu z serii Windows NT. Po uruchomieniu komputera ze startowej płyty CD pojawia się znajome środowisko tekstowe z ekranem powitalnym.

W przypadku wersji ewaluacyjnej ekran powitalny zostanie poprzedzony informacją o wbudowanym mechanizmie ograniczającym czas działania systemu oraz możliwości jego wykorzystywania jedynie w celach testowych.
Na kolejnych ekranach wybieramy opcję instalacji nowego systemu, czytamy uważnie umowę licencyjną i wybieramy partycję lub tworzymy nową. Jej zalecany minimalny rozmiar to 6 GB.

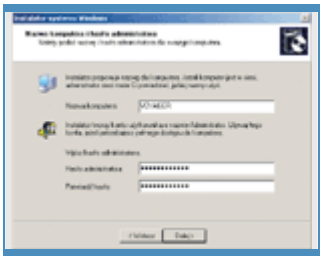
Następnie wybraną partycję formatujemy, zakładając system plików NTFS (wybór NTFS jest konieczny, ponieważ serwer będzie kontrolerem domeny z usługą Active Directory).

Po skopiowaniu podstawowych plików instalacyjnych i ponownym uruchomieniu komputera pojawi się winieta systemu Windows Server 2003, a następnie charakterystyczne graficzne środowisko instalacyjne.

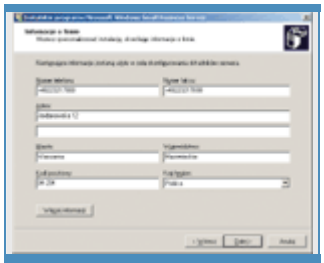
Kolejne standardowe okna dialogowe wymagają zatwierdzenia ustawień regionalnych, podania danych identyfikujących właściciela systemu, podania klucza produktu oraz wpisania wstępnej nazwy komputera (będzie można ją zmienić na drugim etapie instalacji) i hasła administratora (ze względów bezpieczeństwa powinno to być tzw. mocne hasło, składające się z liter, cyfr i niestandardowych znaków).

Po zatwierdzeniu lokalnej strefy czasowej nastąpi właściwa instalacja systemu operacyjnego (na razie tylko Windows Server 2003), która potrwa około 40 minut i zakończy się ponownym uruchomieniem komputera. Wtedy też automatycznie uruchomi się program instalacyjny SBS 2003, który poprowadzi przez kolejne etapy instalacji.

Konfiguracja serwera sieci lokalnej



Rys. 7. Wstępna nazwa komputera i hasło administratora.



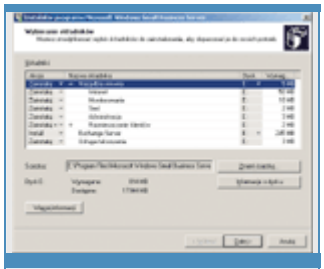
Rys. 8. Podanie danych firmy ułatwi później dodawanie użytkowników.

Rys. 9. Nazwa domeny wewnętrznej powinna mieć rozszerzenie .local.

Drugi etap rozpoczyna się od sprawdzenia, czy system operacyjny spełnia wymagania instalacji systemu SBS 2003. Na początku możemy zobaczyć informację o zalecanej minimalnej ilości pamięci operacyjnej (384 MB) oraz braku drugiej karty sieciowej. Oba ostrzeżenia nie uniemożliwiają dalszej instalacji, ale trzeba pamiętać, że w przypadku konfiguracji z jedną kartą sieciową serwer będzie mógł udostępniać połączenie internetowe, ale nie będzie mógł działać jako firewall.

Rys. 10. Zaznaczamy kartę sieciową wykorzystywaną do komunikacji z siecią lokalną.

Kolejny ekran pozwala wpisać informacje kontaktowe firmy, w której instalowany jest serwer. Są one wykorzystywane później przez różne narzędzia administracyjne. Zdefiniowanie globalnych danych adresowych dla całej firmy pozwala zautomatyzować dodawanie do systemu nowych użytkowników (rys. 8).



Rys. 11. Instalujemy wszystkie możliwe składniki.

Konfiguracja wewnętrznej domeny sprowadza się do podania jej nazwy, najlepiej z rozszerzeniem **.local**, dla odróżnienia od domeny zewnętrznej. Lokalna nazwa domeny jest całkowicie niezależna od domeny zewnętrznej, zarejestrowanej w Internecie. Dla przykładowej domeny zewnętrznej **idg.pl**, domenę wewnętrzną możemy nazwać **idg.local**. Na podstawie lokalnej nazwy domeny DNS kreator automatycznie utworzy odpowiadającą jej nazwę NetBIOS domeny. Nazwę DNS wykorzystują komputery z systemami Windows 2000, XP i 2003, natomiast klienty z systemami Windows NT i 9x wymagają nazwy NetBIOS. Pełnej nazwy DNS domeny używają również serwer pocztowy Exchange 2003 oraz usługi SharePoint, czyli wewnętrzny portal firmowy. Kreator prosi także o wpisanie nazwy serwera. W naszej przykładowej konfiguracji będzie to **voyager** (rys. 9).

W tym momencie warto przełączyć się z programu instalacyjnego do Panelu sterowania i sprawdzić konfigurację kart sieciowych. Kilkamy ikonę Połączenia sieciowe i staramy się zidentyfikować zainstalowane karty. Jeżeli w komputerze zainstalowane są dwie karty sieciowe (a taka konfiguracja jest zalecana), to powinniśmy zobaczyć co najmniej dwa połączenia. W nowszych komputerach, wyposażonych w porty FireWire, dostępne będzie jeszcze trzecie połączenie - właśnie za pomocą interfejsu sieciowego IEEE 1394. Jeżeli jest aktywne, to najlepiej je w tym momencie wyłączyć. Pozostałe dwa połączenia, związane z dwiema kartami sieciowymi służącymi do komunikacji z siecią wewnętrzną oraz Internetem, powinniśmy odpowiednio nazwać - np. połączenie lokalne dla karty łączącej serwer z siecią lokalną oraz np. połączenie sieciowe dla karty łączącej z Internetem. Następnie sprawdzamy, czy karty mają przypisane odpowiednie adresy IP. Jeżeli dostawca usług internetowych automatycznie przydziela adresy albo zewnętrzna karta sieciowa została podłączona do lokalnego routera z aktywną usługą DHCP, to adres zewnętrznego interfejsu prawdopodobnie jest poprawny. W przeciwnym wypadku wpisujemy go ręcznie. Dla karty łączącej z siecią lokalną najczęściej ustawimy adres z puli adresów prywatnych, np. 192.168.0.1. Jeżeli oba interfejsy sieciowe mają przypisane poprawne adresy, możemy powrócić do programu instalacyjnego.

Jeżeli wiemy, która karta sieciowa łączy serwer z siecią lokalną, a która z siecią Internet, musimy o tym poinformować instalator systemu SBS, który na kolejnym ekranie poprosi o wskazanie karty wykorzystywanej do komunikacji z siecią lokalną.

W naszym przypadku będzie to karta z prywatnym adresem 192.168.0.1. Druga skonfigurowana karta ma przypisany publiczny adres 202.232. 198.216 i łączy serwer bezpośrednio z siecią Internet.

Po wybraniu karty sieciowej przeznaczonej do komunikacji z siecią lokalną instalator pozwoli zmienić przypisany jej adres, sugerując jednocześnie typowe wartości dla sieci firmowej. Zostawiamy więc sugerowany adres 192.168.0.1 bez zmian i przechodzimy do kolejnego okna.

Ponieważ w trakcie instalacji system trzeba kilka razy ponownie uruchamiać, instalator oferuje możliwość wpisania hasła administratora i skorzystania z automatycznego logowania. Dzięki

temu kolejna (30-minutowa) instalacja nie wymaga nadzorowania przez użytkownika, bo system sam uruchomi konto administratora. Jednocześnie, ponieważ komputer nie będzie musiał czekać na podanie hasła przez użytkownika, cała instalacja zakończy się nieco szybciej. W trakcie tego "bezobsługowego" etapu zostaną zatwierdzone wpisane wcześniej parametry domeny, sprawdzone karty sieciowe i skonfigurowane protokoły. Zainstalowane będą także: serwer usług internetowych IIS 6.0, usługa SMTP do wymiany poczty elektronicznej oraz usługi SharePoint. Następny etap to przekształcenie serwera w kontroler domeny i zainstalowanie usługi Active Directory na macierzystym poziomie funkcjonalnym zgodnym z Windows 2000, co oznacza, że pozostałe kontrolery domeny (w przypadku systemu SBS mogą być najwyżej dwa) muszą pracować pod kontrolą systemów Windows 2000 Server lub Windows Server 2003.

Instalacja aplikacji pakietu SBS

Po zainstalowaniu Active Directory i ponownym uruchomieniu systemu instalator przedstawi listę wybranych do zainstalowania składników systemu. Wszystkie możliwe komponenty są domyślnie zaznaczone. Po zatwierdzeniu dokonanych wyborów oraz zaakceptowaniu domyślnych folderów instalacyjnych dla poszczególnych aplikacji program instalacyjny pokaże podsumowanie składników i rozpocznie instalację.

Potrwa to około 90 minut, a jedynym zadaniem użytkownika w tym czasie będzie okazjonalna wymiana płyt CD (tu ewidentna przewaga edycji DVD). W ramach tego etapu zainstalowany zostanie serwer pocztowy Exchange 2003 oraz kreatory konfiguracji poczty, połączenia internetowego i dostępu zdalnego, a także konsole zarządzania i usługa faksowania. Następnie za pomocą usługi SharePoint zostanie utworzony intranet. Serwer przygotuje też aplikacje przeznaczone do maszyn klientów, tj. Internet Explorer 6, Outlook Express 2003 oraz program klienta faksu. Po ponownym uruchomieniu systemu i zalogowaniu na konto Administrator będziemy mogli rozpocząć indywidualną konfigurację systemu. Specjalny kreator przedstawi listę zadań do wykonania i przeprowadzi przez podstawowe czynności administracyjne.

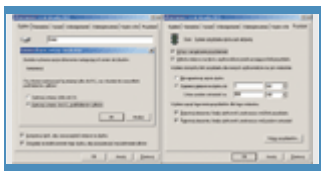
System gotowy

Proces instalacyjny systemu SBS 2003 nie jest najkrótszy, ale instalator dobrze wykorzystuje swój czas. Administrator musi tylko okazjonalnie zmienić płytę lub podać wymagane informacje. Po zakończeniu instalacji system jest w dużym stopniu dostosowany do potrzeb małej firmy.

Przyjrzyjmy się, jakie elementy są instalowane i automatycznie konfigurowane w ramach systemu SBS 2003, jakie usługi są dostępne zaraz po instalacji oraz na czym polega przystosowanie poszczególnych komponentów serwera do pracy w środowisku sieciowym małej firmy.

Pierwszym etapem instalacji pakietu SBS 2003 jest instalacja systemu Windows Server 2003. Wtedy wykonywane są wszystkie standardowe operacje, związane z przygotowywaniem partycji, formatowaniem, wykrywaniem sprzętu czy podstawową konfiguracją sieci.

System operacyjny



Jedno z zadań instalatora SBS 2003 to zidentyfikowanie kart wykorzystywanych do komunikacji z siecią lokalną i z Internetem. Karcie sieciowej, która łączy z siecią lokalną, przypisywany jest stały adres IP. Nie może być przydzielany dynamicznie ze względu na charakter usług udostępnianych przez serwer pozostałym komputerom w sieci. Jako centralny punkt sieci, serwer musi być łatwy do zlokalizowania dla wszystkich klientów.

Rys. 1. Aby nie zabrakło miejsca, dane na partycjach NTFS można kompresować. Można też ograniczyć użytkownikom dostępne dla nich miejsce na dysku.

System operacyjny instalowany jest na partycji NTFS. Wybór tego systemu plików jest konieczny z dwóch powodów. Po pierwsze, na serwerze instalowana jest usługa Active Directory i komputer staje się kontrolerem domeny. Po drugie, instalowany jest serwer pocztowy Exchange 2003. Założenie systemu plików NTFS, oprócz tego, że jest wymuszone przez instalowane aplikacje, przynosi wiele korzyści, takich jak obsługa większych partycji, efektywne zarządzanie przestrzenią dysku oraz zwiększone bezpieczeństwo danych poprzez szyfrowanie, rejestrowanie oraz system uprawnień do folderów i plików.

Active Directory

Active Directory to globalny katalog obiektów sieci. Przechowuje informacje o użytkownikach, grupach, komputerach, drukarkach czy udostępnionych zasobach i jako usługa katalogowa udostępnia je w sieci. Dzięki temu aplikacje mogą szybko wyszukać potrzebne informacje, a usługi sieciowe mogą działać bardziej efektywnie. Użytkownikom łatwiej jest uzyskiwać dostęp do zasobów, a administratorom wygodniej zarządzać siecią, której wszystkie elementy uporządkowane są w jedną logiczną strukturę (rys. 2).

Rys. 2. Globalny katalog obiektów sieciowych pozwala sprawnie zarządzać całą organizacją i zawiera zaawansowane narzędzia, jak np. modelowanie zasad grup, które znacznie ułatwiają to zadanie.

Podczas instalacji konfigurowanych jest wiele parametrów Active Directory, które wpływają na funkcjonowanie sieci. Tworzona jest domena wewnętrzna do obsługi sieci lokalnej. Jej domyślnym rozszerzeniem jest .local, co pozwala oddzielić ją od domeny zewnętrznej, zarejestrowanej w Internecie. W efekcie ten sam system widziany jest od strony sieci lokalnej poprzez jedną nazwę domeny, a od strony Internetu poprzez drugą. Stosowanie rozszerzenia .local nie jest konieczne, ale zalecane, ponieważ to nazwa niezarejestrowana w sieci Internet. Stosując taką nazwę, unika się potencjalnych problemów z rozpoznawaniem nazw.

W przypadku awarii serwera konieczne jest uruchomienie systemu w specjalnym trybie awaryjnym, tzw. trybie przywracania usług katalogowych. Zazwyczaj potrzebne jest do tego oddzielne hasło administratora, które w przypadku systemu SBS jest jednak zsynchronizowane z hasłem głównym konta administratora.

Parametry domeny

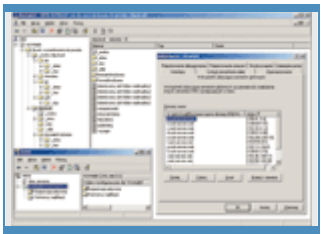
W trakcie instalacji systemu SBS domena Active Directory ustawiana jest na macierzysty poziom funkcjonalności systemu Windows 2000, co oznacza, że na wszystkich pozostałych serwerach, które również są kontrolerami domeny, musi być zainstalowany system Windows 2000 Server lub Windows Server 2003. Nie można zatem wykorzystać w tym celu komputerów z systemem Windows NT 4.0 Server. Ustawienie takiego poziomu funkcjonalnego pozwala wykorzystywać zaawansowane możliwości Active Directory, takie jak członkostwo w grupach uniwersalnych i zagnieżdżonych.

Aby umożliwić budowanie większych sieci i łatwe łączenie przedsiębiorstw, oprócz domeny, która zazwyczaj obejmuje swoim zasięgiem sieć w jednej firmie, wprowadzono drzewa domen, a nawet lasy. Drzewa to grupa lub w ogólności hierarchiczny układ domen, natomiast las to grupa lub hierarchiczny układ drzew. Rozważania te są w przypadku systemu SBS czysto teoretyczne, ponieważ jest przeznaczony do małych firm i przedsiębiorstw.

Domena systemu SBS nie może być domeną podrzędną innej domeny, lecz musi być pojedynczym drzewem w pojedynczym lesie, co więcej w domenie tej może działać tylko jeden komputer z systemem SBS (pewnym wyjątkiem jest migracja z poprzedniej wersji systemu SBS, kiedy to w ograniczonym czasie mogą równolegle działać dwa serwery). Sprzęt, na którym instalujemy system SBS, musi być zatem odpowiednio wydajny, ponieważ prawie wszystkie usługi sieciowe będą dostępne za pomocą tego jednego komputera, a do pomocy mamy jedynie dwa dodatkowe kontrolery domen. Między domeną systemu SBS a dowolną inną nie można ustanowić relacji pozwalającej użytkownikom z jednej domeny na dostęp do zasobów udostępnionych w drugiej domenie, czyli tzw. relacji zaufania.

Serwer DNS

Bardzo ważnym elementem sieci obsługiwanej przez system SBS jest serwer DNS. W ogólnym przypadku serwer DNS może służyć do tłumaczenia nazw na adresy IP i odwrotnie zarówno dla komputerów w sieci lokalnej, jak i w Internecie. W przypadku SBS serwer DNS jest konfigurowany jedynie do obsługi sieci lokalnej. Natomiast zapytania dotyczące zasobów internetowych przesyła do serwerów DNS dostawcy usług internetowych. W ten sposób serwer działa szybciej, obsługując klientów lokalnych, ponieważ nie musi się zajmować zapytaniami dotyczącymi zasobów zewnętrznych (rys. 3).



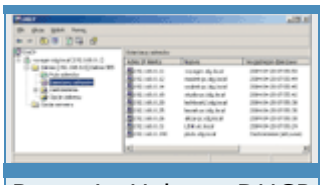
Rys. 3. Serwer DNS zajmuje się tłumaczeniem nazw w sieci lokalnej i przekazywaniem zgłoszeń do serwerów internetowych. Komputery ze starszymi systemami operacyjnymi do tłumaczenia nazw w sieci lokalnej używają WINS.

Aby odizolować serwer DNS od Internetu, usuwana jest tzw. strefa główna, a serwer nie odbiera zgłoszeń pochodzących z sieci zewnętrznej, lecz odpowiada tylko na zapytania pochodzące z sieci lokalnej. Taka konfiguracja zwiększa bezpieczeństwo sieci firmowej, ponieważ informacje o niej nie są dostępne na zewnątrz. Aby przesyłanie zapytań do serwerów internetowych działało poprawnie, adres serwera DNS zewnętrznej karty sieciowej ustawiany jest na adres IP wewnętrznej karty sieciowej. W ten sposób zawsze, gdy system będzie chciał poznać adres IP odpowiadający konkretnej nazwie komputera w Internecie, wyśle zapytanie do własnego serwera DNS, który przekaże je dalej do serwera DNS dostawcy usług internetowych. Adresy serwerów DNS dostawcy muszą być, oczywiście, podane w postaci adresów IP, żeby uniknąć nieskończonej pętli w rozpoznawaniu nazw.

Serwer DHCP

Komputery w sieci lokalnej nie potrzebują stałych adresów IP, można zatem przydzielać je automatycznie. Usługą, która to umożliwia, jest serwer DHCP. Oprócz adresu IP rozsyła też inne informacje związane z konfiguracją sieci i przydatne dla klientów, np. adres serwera DNS, serwera WINS czy adres bramy domyślnej.

W systemie SBS nie trzeba wykorzystywać usługi DHCP instalowanej razem z pozostałymi usługami i aplikacjami, lecz można wykorzystać już będący w sieci serwer DHCP. Wybranie odpowiedniego wariantu zależy od konfiguracji sieci. Jeżeli sieć lokalna jest podłączona do Internetu poprzez router, który pełni funkcję bramki internetowej i ma wbudowaną usługę DHCP, to możemy nadal ją wykorzystywać, a wyłączyć usługę DHCP instalowaną razem z systemem SBS.

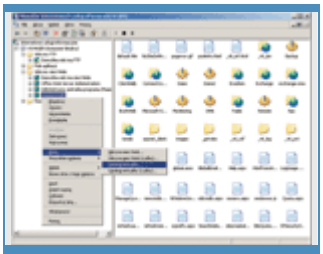


Rys. 4. Usługa DHCP dynamicznie przydziela klientom adresy IP, a także pozostałe informacje umożliwiające im korzystanie z sieci. Dzięki zastrzeżeniom komputery, które potrzebują stałego adresu IP, mogą otrzymywać zawsze ten sam adres.

Pozostaje tylko taki router odpowiednio skonfigurować, np. żeby wysyłał do komputerów klienckich adres wewnętrznej karty sieciowej serwera SBS jako adres serwera DNS. Jeżeli router obsługuje technologię Universal Plug and Play (UPnP), instalator SBS może sam skonfigurować router. W przeciwnym razie trzeba wykonać tę operację ręcznie albo wyłączyć funkcję DHCP w urządzeniu i wykorzystywać usługę DHCP serwera SBS. Jeżeli pozwolimy instalatorowi skonfigurować usługę DHCP, to komputery klienckie na pewno będą otrzymywały prawidłowe informacje. Od liczby kart sieciowych w serwerze zależy, jaki adres będzie wykorzystywany jako bramka internetowa. Jeżeli mamy dwie karty, to serwer pośredniczy w transmisji, a wszystkim komputerom klienckim jako adres bramki podawany jest adres karty sieciowej serwera przeznaczonej do komunikacji z siecią lokalną. Jeżeli w serwerze zainstalowano tylko jedną kartę, adresem bramki będzie adres wewnętrznego interfejsu sieciowego routera (rys. 4).

Serwer DHCP dba również o komputery ze starszymi systemami operacyjnymi. Aby usługi rozpoznawania nazw były dla nich dostępne, otrzymują adres serwera WINS, który działa na serwerze SBS. Z kolei dla urządzeń wymagających stałego adresu IP, takich jak np. drukarki sieciowe, usługa DHCP rezerwuje domyślnie pierwsze 10 adresów z puli adresów wewnętrznych przeznaczonych do dystrybucji. Używanie adresów statycznych dla komputerów z systemami Windows 2000 Professional i Windows XP Professional nie jest zalecane, ponieważ uniemożliwia m.in. automatyczną konfigurację narzędziami serwera SBS.

Serwer WWW



Rys. 5. Menedżer internetowych usług informacyjnych (IIS) stanowi centrum zarządzania witrynami WWW i FTP. Tutaj również uaktywniamy rozszerzenia serwera, umożliwiające budowanie dynamicznych serwisów.

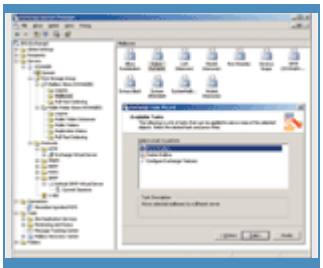
Internetowe usługi informacyjne, czyli serwer IIS w systemie SBS 2003 występuje w najnowszej wersji 6.0, która wprowadza wiele bardzo pozytywnych zmian. Nowy serwer IIS został w dużej części napisany od nowa, dzięki czemu jest szybszy i bardziej bezpieczny. Zastosowano w nim także zaawansowane rozwiązania, które znacznie poprawiły stabilność. Jednym z takich rozwiązań jest separacja witryn, która pozwala aplikacjom wykonywać się w oddzielnych, niedostępnych dla siebie obszarach pamięci, co powoduje, że uszkodzona aplikacja, nie jest w stanie zagrozić żadnej innej ani też samemu serwerowi WWW.

Serwer IIS jest podstawą nie tylko internetowej witryny WWW. Dzięki niemu działa także wewnętrzny portal SharePoint, możliwy jest dostęp do serwera pocztowego Exchange 2003 za pomocą technologii Outlook Web Access oraz Outlook Mobile Access, a także usługa Dostęp do zdalnego miejsca pracy w sieci Web (rys. 5).

W ramach konfiguracji serwera IIS do pracy w systemie SBS uruchamiane są m.in. dwie dodatkowe witryny WWW, jedna do obsługi portalu SharePoint, a druga do administrowania nim, przy czym obie odpowiadają tylko na zgłoszenia z sieci lokalnej. Aby zapewnić bezpieczną transmisję danych pomiędzy serwerem a przeglądarką, włączana jest obsługa protokołu SSL. Zakładane są też specjalne filtry, które potrafią wymusić stosowanie bezpiecznych połączeń. Gdy użytkownik próbuje połączyć się z serwerem WWW za pomocą zwykłego protokołu HTTP, a usługa, z której chce skorzystać, wymaga stosowania połączeń szyfrowanych, filtr skieruje żądanie do innego portu, tak żeby wykorzystywana była szyfrowana transmisja HTTPS. Jeżeli jako zapora internetowa wykorzystywany jest serwer ISA, to przejmuje on nasłuchiwanie w portach przypisanych zwykle do serwera IIS. W zależności od zdefiniowanych zasad dostępu przekazuje żądania do serwera WWW lub je blokuje.

Serwer poczty

Instalator SBS konfiguruje również serwer pocztowy Exchange. Oprócz zwykłego dostępu poprzez sieć lokalną uaktywniane są połączenia poprzez serwer IIS, a więc technologie OWA i OMA. Ponadto uruchamiana jest także usługa RPC przez serwer proxy HTTP, która pozwala programowi Outlook 2003 łączyć się z serwerem pocztowym Exchange poprzez Internet. Nie jest to jednak standardowe binarne połączenie RPC, które wymaga otwierania niestandardowych portów w zaporach. Są to wywołania RPC opakowane tekstowym protokołem HTTP, który przechodzi przez wszystkie zapory przepuszczające ruch w sieci WWW, a więc wszędzie tam, gdzie jest Internet, choćby korzystanie z niego miało się ograniczać do możliwości przeglądania sieci WWW. Eliminuje to potrzebę łączenia się przez OWA lub tworzenia połączeń wirtualnych sieci prywatnych (VPN). Znakomitym uzupełnieniem różnych metod dostępu do serwera jest wbudowany w program Outlook 2003 specjalny tryb pracy, tzw. tryb buforowany, który zmniejsza do minimum ilość informacji przesyłanych między klientem a serwerem Exchange. Wiadomości są ściągane z serwera i przechowywane w lokalnym buforze. Dzięki temu można na nich pracować bez utrzymywania stałego połączenia z serwerem, a dane i tak będą aktualne, gdyż co pewien czas automatycznie wykonywana jest synchronizacja.



Rys. 6. Exchange System Manager wykonuje wszystkie zadania związane z pocztą elektroniczną, od aktywacji poszczególnych usług serwera po odzyskiwanie skrzynek pocztowych użytkowników.

Jeśli chodzi o ustawienia istotne dla końcowych użytkowników poczty, wspomnieć należy, że limit wielkości skrzynki zostaje ustawiony na 200 MB, przy czym przy 175 MB wysyłany jest odpowiedni komunikat informujący o ograniczeniu pojemności. Trwale usunięte wiadomości serwer przechowuje jeszcze przez 30 dni od ich skasowania, a nieaktywne sesje użytkowników są rozłączane po 10 minutach. Serwer może też automatycznie usuwać załączniki określonego typu i zapisywać je we wskazanym folderze. Natomiast prawo przekazywania wiadomości przez serwer pocztowy dostają tylko klienci łączący się z serwerem z sieci wewnętrznej lub użytkownicy uwierzytelnieni. Zabezpiecza to serwer pocztowy przed możliwością wykorzystania go do rozsyłania obcej poczty elektronicznej (rys. 6).

Aby ułatwić użytkownikom łagodne przejście od skrzynek pocztowych przechowywanych u dostawców Internetu do skrzynki na serwerze Exchange lub korzystanie z obu rodzajów kont pocztowych jednocześnie, instalowany jest tzw. Łącznik POP3, który umożliwia regularne pobieranie wiadomości ze wskazanych skrzynek pocztowych i zapisywanie ich w skrzynce serwera Exchange.

Rys. 7. W wewnętrznym portalu firmowym automatycznie tworzone są szablony do przechowywania różnego rodzaju dokumentów.

Aby za bardzo nie obciążać serwera SBS, który oprócz obsługi zgłoszeń zewnętrznych, pochodzących z Internetu, obsługuje jeszcze całą sieć lokalną, zarówno w przypadku witryny WWW, jak i serwera pocztowego Exchange, liczba jednoczesnych połączeń przychodzących została ograniczona do pięciuset. Liczba połączeń wychodzących serwera pocztowego została natomiast ograniczona do dziesięciu, aby Exchange nie zmniejszał znacząco przepustowości łącza.

Portal firmowy

Do potrzeb małej firmy zostaje wstępnie przystosowany również firmowy portal SharePoint. Aby zademonstrować swoje możliwości, SharePoint tworzy przykładową firmową witrynę z bibliotekami dokumentów, folderem faksów przychodzących, punktem pomocy, kalendarzem wakacji, albumem fotografii i oczywiście narzędziami do zarządzania.

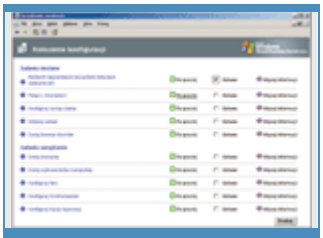
Konfiguracja

Pierwsze zadania administracyjne wykonamy tuż po instalacji za pomocą specjalnego kreatora. Dostępne narzędzia konfigurują zainstalowane usługi, wyświetlają cenne wskazówki dotyczące bezpieczeństwa i pomagają podłączyć do serwera komputery użytkowników.

Podczas pierwszego logowania do nowo zainstalowanego systemu powita nas kreator kończenia

konfiguracji, który przedstawi listę zadań administracyjnych do wykonania. Ponieważ nie wszystkie wykonamy od razu, warto wiedzieć, jak dostać się do tej listy później. Podczas każdego kolejnego logowania na konto Administrator standardowo uruchamiane jest narzędzie Zarządzanie serwerem. Jeśli na liście folderów w lewej części okna podświetlona jest pozycja Strona główna, to po prawej widzimy listę skrótów do narzędzi wykonujących typowe zadania administracyjne. Natomiast Lista zadań do wykonania jest pierwszą pozycją w folderze Zarządzanie standardowe. Lista zadań nie tylko sugeruje prawidłową kolejność wykonywania operacji, ale ułatwia też dostęp do odpowiednich narzędzi, pozwala kontrolować postęp prac administracyjnych i dostarcza szczegółowych informacji o każdym zadaniu.

Lista zadań do wykonania

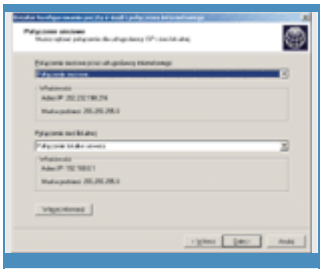


Rys. 1. Lista zadań administracyjnych do wykonania po instalacji systemu. Najpierw powinniśmy koniecznie przeczytać informacje związane z bezpieczeństwem serwera i sieci.

Nie bez przyczyny pierwszą pozycją na liście zadań jest wyświetlenie najważniejszych wskazówek dotyczących zabezpieczeń. Lektura tego dokumentu pozwoli się zorientować w możliwych niebezpieczeństwach i zdobyć informacje, w jaki sposób zabezpieczyć serwer przed zewnętrznymi zagrożeniami, z Internetu, oraz zagrożeniami wewnętrznymi, dotyczącymi sieci lokalnej. Dowiemy się, jak skonfigurować zaporę internetową, zdefiniować zasady haseł, zapewnić zdalnym użytkownikom bezpieczny dostęp do serwera i jak globalnie zmienić nazwę konta Administrator, aby ograniczyć możliwość włamania na to konto po odgadnięciu hasła.

Wśród zaleceń dotyczących sieci lokalnej znajdziemy informacje o instalowaniu narzędzi antywirusowych, konfiguracji automatycznych kopii zapasowych, mechanizmach aktualizacji oprogramowania, wykorzystaniu oferowanych przez Microsoft dodatkowych narzędzi (np. skaner MBSA), które pozwalają utrzymać bezpieczny system. Poruszono także zagadnienia konfiguracji praw użytkowników, kontroli dostępu do serwera czy ograniczenia dostępnej dla użytkowników przestrzeni dyskowej. Pilne przestrzeganie tych reguł, a także stałe monitorowanie pracy systemu za pomocą wbudowanych narzędzi znacząco zwiększą jego bezpieczeństwo, dlatego warto poświęcić chwilę na przeanalizowanie podanych tu informacji.

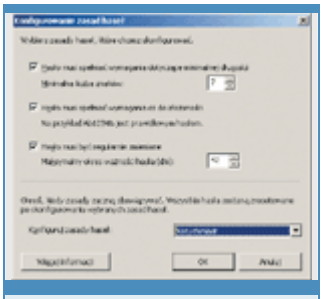
Połączenie z Internetem



Rys. 2. Kreator prawidłowo identyfikuje interfejsy sieciowe wykorzystywane do połączeń lokalnych i internetowych.

Szczegółowy opis podłączania serwera do Internetu przez router szerokopasmowy za pomocą tego kreatora znajduje się w artykule "Na straży SBS", dotyczącym konfiguracji zapory internetowej za pomocą usługi RRAS oraz serwera ISA 2000. Tutaj powiemy jedynie, jakie czynności należy wykonać, aby skonfigurować połączenie internetowe w naszej przykładowej sieci. Zakładamy klasyczną sytuację, w której serwer jest wyposażony w dwie karty sieciowe. Jedna służy do komunikacji z siecią lokalną, a druga bezpośrednio z Internetem. Struktura sieci wygląda tak, jak na rysunku 1 w artykule "Instalacja SBS 2003". Najpierw jako typ połączenia wybieramy Szerokopasmowe, a następnie Bezpośrednie połączenie szerokopasmowe. Ponieważ karty sieciowe skonfigurowaliśmy już podczas instalacji, kreator prawidłowo identyfikuje nazwy połączeń wykorzystywane do komunikacji z Internetem i siecią lokalną. Jeżeli nadaliśmy połączeniom sugerowane wcześniej nazwy, to Połączenie sieciowe łączy nas z dostawcą usług internetowych, natomiast Połączenie lokalne serwera służy do komunikacji z siecią wewnętrzną.

Następnie kreator oferuje możliwość wpisania lub poprawienia adresu IP bramy domyślnej u dostawcy oraz adresów serwerów DNS. Znów potwierdzamy wcześniej wpisane parametry i w kolejnym oknie wybieramy Włącz zaporę. Ponieważ nie zainstalowaliśmy jeszcze aplikacji dodatkowych dostarczanych w edycji Premium pakietu SBS 2003, a konkretnie serwera ISA 2000, teraz konfigurujemy zaporę podstawową, dostępną w ramach usługi RRAS. Po zainstalowaniu serwera ISA 2000 ten sam kreator będzie służył do wstępnej konfiguracji zapory zaawansowanej, oferowanej właśnie przez serwer ISA 2000. W kolejnym oknie określamy usługi dostępne dla użytkowników zewnętrznych. Do wybory mamy opcje: E-mail, Wirtualna sieć prywatna (VPN), Usługi terminalowe i FTP. Na razie chcemy jedynie uzyskać dostęp do Internetu dla klientów sieci lokalnej, dlatego możemy wszystkie opcje odznaczyć, zwłaszcza że dobrą zasadą jest domyślne wyłączenie wszystkich usług, a następnie włączanie tylko potrzebnych. Opcję E-mail zaznaczymy przy okazji konfigurowania poczty elektronicznej w firmie w artykule "Poczta firmowa i internetowa", a połączenia VPN, korzystanie z usług terminalowych i konfigurację serwera FTP opisujemy w artykule "Wszechobecna sieć". Na razie nie pozwolimy też nikomu z zewnątrz korzystać ze strony WWW. Wybieramy Nie zezwalaj na dostęp do witryny sieci Web z Internetu i klikamy Dalej. Następnie wybieramy Nie zmieniaj konfiguracji internetowej poczty e-mail, Dalej i Zakończ. Po zakończeniu pracy kreatora zobaczymy informację o nieskonfigurowanych zasadach haseł z propozycją włączenia zasad haseł. Powinniśmy odpowiedzieć Tak i ustawić wymagania dotyczące haseł, takie jak minimalna długość, odpowiedni stopień złożoności oraz jak często hasło powinno być zmieniane.



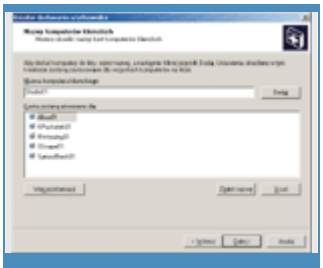
Rys. 3. Długie, złożone i często zmieniane hasła zwiększą bezpieczeństwo systemu.

W tym momencie dostęp do Internetu powinien być możliwy zarówno z samego serwera, jak i z każdego komputera sieci lokalnej, znajdującego się w tej samej podsieci, z którą połączony jest serwer za pomocą swojego interfejsu wewnętrznego. Komputery nie muszą być jeszcze zarejestrowane w domenie, a ich użytkownicy nie muszą korzystać z kont domenowych. Wystarczy, że karty sieciowe komputerów w sieci lokalnej będą miały wpisany adres naszego serwera jako adres bramy domyślnej i jednocześnie jako adres serwera DNS. Jeżeli w konfiguracji kart sieciowych komputerów lokalnych wybrano opcję automatycznego uzyskiwania adresu IP, to karty powinny mieć wszystkie parametry ustawione prawidłowo. Powodem jest to, że podczas instalacji serwera SBS uruchamiana jest usługa DHCP, która automatycznie przydziela adresy komputerom w sieci lokalnej, natomiast serwer DNS jest konfigurowany do przekazywania żądań rozwiązywania nazw internetowych do serwera DNS dostawcy.

Rys. 4. Grupowo tworzymy nowe konta na podstawie wspólnego szablonu.

Dostęp do Internetu za pośrednictwem serwera SBS dla klientów, którzy nie są członkami domeny, zostanie wyłączony bezpośrednio po zainstalowaniu serwera ISA 2000, który domyślnie wymaga, aby użytkownicy łączący się z Internetem podawali informacje uwierzytelniające. Opcję tę można jednak wyłączyć, edytując właściwości serwera w narzędziu ISA Management.

Zdalny dostęp do sieci



Rys. 5. Utworzone zostaną konta dla wszystkich wymienionych komputerów, natomiast podłączenie do domeny trzeba wykonać osobno na każdym z nich.

Opcja Konfiguruj dostęp zdalny uruchamia kreatora, który uaktywnia dostęp do sieci firmowej poprzez połączenie VPN lub przez modem. W przypadku VPN konfiguracja sprowadza się do podania pełnego adresu serwera (czyli jego nazwy wraz z nazwą domeny zewnętrznej), który będzie używany do nawiązywania zdalnych połączeń przez Internet. W naszej przykładowej konfiguracji będzie to voyager.idg.pl. Konfiguracja modemu to wybór zainstalowanego w systemie urządzenia, podanie numeru linii telefonicznej oraz ewentualnego numeru dodatkowego. Kreator włączy przekazywanie ruchu VPN przez zaporę, uaktywni połączenia modemowe i skonfiguruje usługę DHCP do nadawania klientom zdalnym adresów z puli przeznaczonej do sieci lokalnej. Wybranie w Kreatorze dostępu zdalnego dostępu za pomocą VPN spowoduje, że w Kreatorze konfigurowania poczty e-mail i połączenia internetowego, który omawialiśmy w części "Połączenie z Internetem", uaktywniona zostanie dla klientów zewnętrznych usługa Wirtualna sieć prywatna (VPN).

Drukarki, licencje i aktywacja

Kolejna pozycja na liście zadań do wykonania to aktywacja serwera. Nie różni się od procesu aktywacji systemu Windows XP. W najprostszej wersji wymaga jedynie czynnego połączenia z Internetem, choć możliwa jest także aktywacja przez telefon. Następnie powinniśmy dodać kolejne licencje dla użytkowników, ponieważ z pakietem SBS 2003 dostajemy tylko pięć licencji CAL. Tę operację również można wykonać przez Internet albo telefonicznie. Na tym kończymy tzw. zadania sieciowe i przechodzimy do zarządzania.

Pierwszym zadaniem jest zainstalowanie drukarki podłączonej do serwera. Instalowanie drukarki, uruchamiane kliknięciem Dodaj drukarkę, przebiega podobnie, jak w innych systemach Windows, tyle że drukarka zostaje automatycznie udostępniona i opublikowana w katalogu Active Directory, aby klienci mogli ją wyszukać na podstawie różnych kryteriów, np. czy drukuje w kolorze.

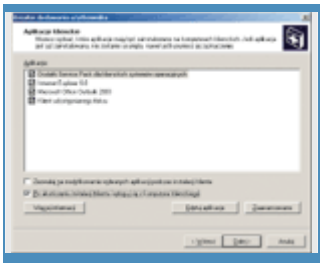
Konfiguracja

Dodawanie użytkowników i komputerów

Na liście zadań do wykonania znajduje się opcja Dodaj użytkowników i komputery, uruchamiająca Kreator dodawania użytkownika. To wygodne narzędzie automatyzuje: zakładanie nowego konta oraz powiązanej z nim skrzynki pocztowej, tworzenie prywatnego folderu, ustawianie członkostwa w grupach zabezpieczeń i w grupach dystrybucyjnych, konfigurowanie dostępu do witryny SharePoint, ustawianie limitów przestrzeni dyskowej, a także tworzenie kont komputerów i dołączanie ich do domeny. Użytkowników dodajemy na podstawie predefiniowanego szablonu (tworzenie i modyfikowanie szablonów opisujemy w artykule "Administracja"), a do wyboru mamy najprostszy User Template, następnie Mobile User Template i Power User Template oraz dający największe uprawnienia Administrator Template.

Szablony standardowe

Konto utworzone na podstawie User Template będzie miało dostęp do współdzielonych folderów, drukarek, faksów, poczty elektronicznej i Internetu. Korzystając z takiego konta będzie można też łączyć się z innymi komputerami za pomocą usługi zdalnego pulpitu, ale tylko w przypadku, gdy będą to systemy Windows XP. Użytkownik nie będzie mógł, oczywiście, połączyć się tą metodą z pulpitem serwera.



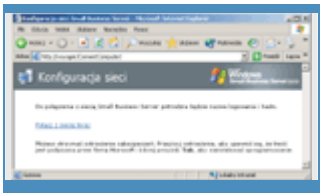
Rys. 6. Zaznaczone aplikacje będą automatycznie dostarczane do komputerów użytkowników po podłączeniu ich do domeny.

Szablon dla użytkowników mobilnych rozszerza możliwości zwykłego użytkownika o uzyskiwanie zdalnego dostępu do serwera przez połączenie VPN albo przez linię telefoniczną, natomiast szablonu użytkownika zaawansowanego używa się, chcąc określonym osobom zlecać niektóre zadania administracyjne. Użytkownicy zaawansowani mogą się w tym celu zdalnie zalogować na komputerze, na którym działa serwer SBS.

W następnym oknie dodajemy kolejne nazwy kont użytkowników, które zostaną utworzone na podstawie wybranego szablonu. Gdy skończymy, kreator zapyta, czy utworzyć również konta komputerów. Odpowiadamy twierdząco i akceptujemy bądź modyfikujemy zaproponowane nowe nazwy komputerów.

Dystrybucja aplikacji w sieci

Dwa ostatnie okna kreatora dotyczą aplikacji instalowanych na komputerach klientów w ramach automatycznej dystrybucji oprogramowania. Bezpośrednio po podłączeniu komputera do domeny instalator automatycznie instaluje na nim zestaw aplikacji i uaktualnień. Ten sam mechanizm może być później wielokrotnie wykorzystywany do instalowania na stacjach roboczych nowych aplikacji. Standardowy zestaw, dostępny tuż po instalacji systemu SBS, obejmuje dodatki Service Pack do systemów Windows 2000 oraz Windows XP (odpowiednio SP4 i SP1), przeglądarkę Internet Explorer 6.0 SP1, Outlook 2003 oraz klienta udostępnionego na serwerze faksu, który pozwala wysyłać faksy i zarządzać nimi z dowolnych komputerów sieci lokalnej (faksy przychodzące mogą trafiać do udostępnionego folderu, do witryny SharePoint lub do skrzynek pocztowych użytkowników).

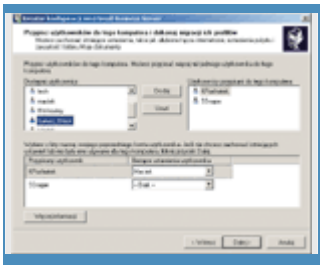


Rys. 7. Klikamy łącze Połącz z siecią teraz, żeby uruchomić kreatora podłączania komputera do domeny.

Zaznaczenie opcji Zezwalaj na modyfikowanie wybranych aplikacji podczas instalacji klienta pozwala użytkownikom podłączanych komputerów ingerować w przebieg instalacji dostarczonych automatycznie aplikacji. Ingerencja może polegać na zmianie domyślnej lokalizacji kopiowanych plików lub zrezygnowaniu z instalowania określonych aplikacji. Druga opcja, czyli Po ukończeniu instalacji klienta wyloguj się z komputera klienckiego, jest użyteczna, gdy wykonujemy instalację bez nadzoru użytkownika, ponieważ zabezpiecza dostęp do komputera po wykonaniu wszystkich czynności instalacyjnych.

Warto też czasami wyłączyć niektóre domyślne ustawienia konfiguracyjne stacji roboczych. Po naciśnięciu przycisku Zaawansowane będziemy mogli odznaczyć te opcje, które chcemy pominąć. Jeżeli jednak zaakceptujemy wszystkie modyfikacje, to w komputerach klienckich zostanie wprowadzonych niemało zmian.

Specjalnie do komputerów przenośnych lub innych urządzeń, które z siecią będą się łączyły sporadycznie, przygotowano aplikację Menedżer połączeń, konfigurującą na komputerach klienckich połączenia z serwerem SBS ze zdalnych lokalizacji. Jeżeli więc podłączamy do domeny np. notebook, warto zaznaczyć opcję Zainstaluj Menedżera połączeń, a jeżeli zamierzamy również synchronizować dane w urządzeniu przenośnym i komputerach w sieci lokalnej lub na serwerze, to dodatkowo zaznaczmy opcję Zainstaluj ActiveSync 3.7. Po kliknięciu Dalej i Zakończ, kreator utworzy konta użytkowników i komputerów, założy katalogi domowe, ustawi członkostwo w odpowiednich grupach zabezpieczeń wynikających z zastosowanego szablonu i poprosi administratora o ręczne podłączenie każdego z komputerów klienckich do domeny.



Rys. 8. Do komputera przypisujemy dwóch użytkowników. Pierwszy to KPuchatek, który przejmie profil lokalnego użytkownika Maciek, a drugi SSnape, dla którego utworzony zostanie nowy domyślny profil.

Podłączanie klientów i migracja profilów

Podłączanie komputerów najłatwiej przeprowadzić za pomocą przeglądarki. Wystarczy w tym celu na komputerze klienta wpisać adres //<nazwa_serwera>/ConnectComputer. W naszym przypadku będzie to //voyager//ConnectComputer.

Po kliknięciu Połącz z siecią teraz musimy podać nazwę i hasło użytkownika, którego komputer konfigurujemy. Ponieważ przed podłączeniem komputera do domeny ktoś mógł na nim już pracować, kreator oferuje możliwość przeniesienia ustawień pulpitu, kolekcji Ulubionych czy zawartości folderu Moje dokumenty na nowe konto. Do jednego komputera możemy przypisać kilku użytkowników i dla każdego indywidualnie przenieść ustawienia profilu z ich obecnych kont.

Rys. 9. Instalację przypisanych do komputera aplikacji możemy odłożyć na później.

Po zatwierdzeniu w kolejnym oknie nowej nazwy komputera, klikamy Dalej oraz Zakończ i czekamy, aż kreator skonfiguruje komputer. Po krótkiej chwili komputer zostanie uruchomiony ponownie, po czym system automatycznie zaloguje się na specjalne tymczasowe konto, za pomocą którego przeniesie profil i ponownie zrestartuje komputer. Wtedy komputer będzie już podłączony do domeny i można się już zalogować na swoje nowe konto domenowe. Gdy to zrobimy, pojawi się okno proponujące instalację aplikacji, które przypisaliśmy do stacji podczas konfigurowania kont komputerów na serwerze.

Po zainstalowaniu wszystkich przypisanych aplikacji komputer jest członkiem domeny i może być globalnie zarządzany. To już zadania dla administratora, który może je wykonywać zdalnie. Natomiast lokalny użytkownik ma już wszystko, czego potrzebuje, i może się wziąć do pracy.

Ustawienia komputerów klienckich

Po zakończeniu konfiguracji przeglądarka będzie przygotowana do współpracy z serwerem ISA 2000 jako serwerem proxy (gdy zostanie zainstalowany), do Ulubionych zostaną dodane przydatne skróty (np. do usługi Outlook Web Access), natomiast strona główna zostanie ustawiona na http: //companyweb/, czyli adres wewnętrznej witryny SharePoint. Automatycznie dostarczony do komputera Outlook 2003 będzie skonfigurowany do współpracy z serwerem pocztowym Exchange i profil ten stanie się domyślny. Skonfigurowane będzie również wysyłanie faksów bezpośrednio z lokalnego programu pocztowego za pomocą faks-modemu zainstalowanego na serwerze.

W folderze Moje miejsca sieciowe pojawią się skróty do kolekcji dokumentów ogólnych w witrynie SharePoint oraz do przechowywanego na serwerze folderu domowego aktualnie zalogowanego użytkownika. Instalowane są również co najmniej dwie drukarki: przekazująca dokumenty na serwer do wysłania faksem oraz zwykła, podłączona do serwera, wcześniej

opublikowana w Active Directory i udostępniona dla klientów. Na komputerach klienckich aktywowane są także usługi Pulpit zdalny i Pomoc zdalna.

Administracja

Small Business Server 2003 jest przeznaczony do niedużych firm. Małe przedsiębiorstwa nie potrzebują wyszukanych metod administracji tysiącami użytkowników i ogromem informacji. Wymagają natomiast narzędzi pozwalających na łatwe zarządzanie zasobami.

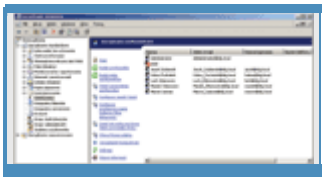
Platformą systemową pakietu Small Business Server 2003 jest Windows Server 2003. Jego duża skalowalność pozwala na pracę w ogromnych korporacjach. Na potrzeby pakietu SBS Windows Server 2003 został wyposażony w wiele narzędzi do łatwego i skutecznego administrowania serwerem. Osoba, której powierzymy opiekę nad systemem, nie musi mieć pakietu certyfikatów dokumentujących jej rozległą wiedzę. Wystarczy znajomość kilku okienkowych kreatorów Windows. Nie oznacza to jednak, że Small Business Server 2003 zawiera niepełnowartościowe produkty. Mając mniej doświadczenia, można korzystać z kreatorów, ale pakietem SBS można administrować tak, jak systemem Windows Server 2003.

Kreator, kreatora, kreatorem

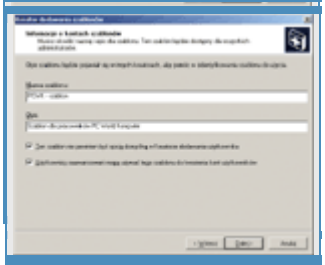
SBS 2003 ma trafić do niewielkich, dynamicznie rozwijających się firm. Jedną z cech małych przedsiębiorstw jest brak wyspecjalizowanego działu IT. Czynności związane z administracją wykonują firmy partnerskie lub pracownicy bardziej obyci z komputerem. Aby maksymalnie uprościć zarządzanie, pakiet SBS wyposażono w zestaw prostych narzędzi, które po bliższym poznaniu może obsługiwać prawie każdy użytkownik sieci.

Administracja poszczególnymi komponentami systemu odbywa się za pomocą czytelnych kreatorów. Użytkownik jest prowadzony za rękę przez kolejne okna konfiguracyjne. Każde okno zawiera nagłówek ze specyfikacją wykonywanej czynności, czytelny opis zaznaczanych opcji lub wprowadzanych danych. Dostępny dodatkowo przycisk Więcej informacji szczegółowo wyjaśnia, do czego służą określane parametry. Zanim kreator wprowadzi skonfigurowane lub zmienione ustawienia, wyświetla informacje o tym, co zostanie wykonane.

Zarządzanie serwerem i Active Directory



Rys. 3. Zawartość folderu Użytkownicy.



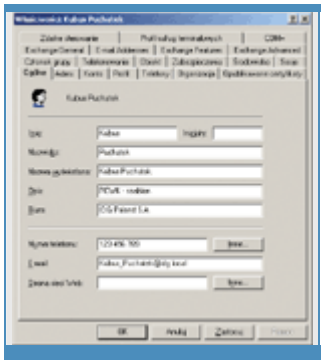
Rys. 4. Tworzenie nowego szablonu.

Rys. 2. Zawartość folderu Szablony użytkownika.

Jeśli system został poprawnie zainstalowany (patrz: "Instalacja SBS 2003") i skonfigurowany (patrz: Konfiguracja"), codzienne zadania administratora ograniczają się do czynności typowo konserwacyjnych. Chodzi o takie zadania, jak monitorowanie działania systemu i aplikacji, wykonywanie kopii zapasowych (patrz: "Współdzielenie zasobów"), instalacja uaktualnień, zarządzanie zasobami sieci oraz rozwiązywanie bieżących problemów. Każda ze wskazanych czynności wymaga użycia właściwego narzędzia. Aby administrator nie błądził po systemie w poszukiwaniu odpowiednich modułów konfiguracyjnych, zostały one zgrupowane pod nazwą Zarządzanie serwerem. Uruchamiając Start | Narzędzia administracyjne | Zarządzanie serwerem, uzyskujemy dostęp do centrum zarządzania SBS 2003.

Rys. 5. Wszystkie karty właściwości konta.

Moduł Zarządzanie serwerem składa się z dwóch paneli. W lewym odnajdziemy dwie grupy folderów: Zarządzanie standardowe i Zarządzanie zaawansowane. Zarządzanie standardowe zawiera listę najczęściej wykonywanych zadań administracyjnych. Umieszczono tu większość kreatorów ułatwiających pracę administratora. Wymienione w folderze moduły: Użytkownicy, Grupy dystrybucyjne, Grupy zabezpieczeń i Szablony użytkownika służą do wykonywania najprostszych zadań. Folder Zarządzanie zaawansowane jest, jak się łatwo domyślić, zbiorem zaawansowanych narzędzi do administrowania aplikacjami oraz serwerem. Moduły: Użytkownicy i komputery usługi Active Directory lub Zarządzanie komputerem to standardowe narzędzia instalowane razem z Windows Server 2003. Zarządzanie zaawansowane, w przeciwieństwie do Zarządzania standardowego, nie jest jedynie zbiorem kreatorów i odnośników do najczęściej wykonywanych zadań. Administrator znający interfejs i przeznaczenie narzędzi umieszczonych w tym folderze może wykonywać wszelkie czynności konfiguracyjne Windows 2003 lub Exchange 2003.



Rys. 6. Miejsce na dane osobowe użytkownika.

Zarządzanie serwerem jest centrum dowodzenia pakietem SBS 2003. Warto jednak pamiętać, że po kliknięciu menu Start, uzyskujemy dostęp do folderu Narzędzia administracyjne, który zawiera listę modułów do zarządzania wszystkimi komponentami Windows Server 2003. Są w nim odnośniki do administracji takimi usługami, jak DNS, DHCP, DFS itd. Jeśli zainstalowaliśmy dodatkowe komponenty pakietu SBS, np. Exchange 2003, czy SQL 2000, w menu Wszystkie programy umieszczane są foldery związane z tymi aplikacjami. Sięgając do nich, możemy uzyskać dostęp do dodatkowych informacji lub narzędzi.

Zarządzanie użytkownikami

Konto jest identyfikatorem użytkownika pakietu SBS 2003. Jest ono wykorzystywane przez wiele komponentów i aplikacji systemu. Po utworzeniu konta możemy konfigurować dostęp do plików, drukarek, limity przydziałów dyskowych, adresy poczty elektronicznej, ograniczenia czasu logowania i wiele innych komponentów. Identyfikator ten jest wykorzystywany przez system podczas generowania raportów i zdarzeń. Założenie konta jest prostym działaniem opisanym w artykule: "Konfiguracja". Ponieważ sieć komputerowa to "żywy" organizm, po pewnym czasie może wystąpić konieczność zmodyfikowania właściwości kont.

W celu maksymalnego uproszczenia konfiguracji środowiska oraz uprawnień klientów sieci, SBS opiera się na szablonach użytkowników. Mając przygotowany szablon, możemy w łatwy sposób przenieść wszystkie jego parametry na zakładane lub modyfikowane konta. Do konfiguracji szablonów służy folder Szablony użytkownika. Po jego zaznaczeniu możemy utworzyć nowy szablon oraz importować lub eksportować ustawienia szablonów. Jeśli zaznaczymy jeden z gotowych obiektów, dostępne są opcje zezwalające na modyfikację ustawień lub usuwanie szablonu.

Tworzenie nowego szablonu rozpoczynamy od kliknięcia opcji Dodaj szablon. Po kliknięciu Dalej definiujemy nazwę oraz opis szablonu. Jeżeli zakładamy obiekt na przykład dla pracowników PCWK, w pole Nazwa szablonu wpisujemy np. PCWK - szablon, a w pole Opis: Szablon dla pracowników PC World Komputer. Dodatkowe parametry służą do określenia, czy szablon ma być domyślnym szablonem w kreatorze Dodaj użytkownika oraz czy członkowie grupy Domain

Power Users mogą korzystać z tego szablonu podczas tworzenia nowych kont. W następnym oknie kreatora wskazujemy grupy zabezpieczeń, do których mają przynależeć użytkownicy założeni za pomocą szablonu. Przykładowo może to być grupa RedakcjaPCWK. Oprócz grup zabezpieczeń ściśle związanych szablonem do listy warto dodać grupy ogólnego przeznaczenia, takie jak Użytkownicy domeny lub Użytkownicy. Następne okno jest również przeznaczone do określania członkostwa w grupach, ale w tym wypadku są to grupy dystrybucyjne. Jeśli chcemy, żeby zakładane konta użytkowników domyślnie należały do grupy dystrybucyjnej, wybieramy ją z listy i klikamy przycisk Dodaj. Kolejne okno, które pojawi się po naciśnięciu Dalej, pozwala ustawić domyślne członkostwo w grupach witryn portalu SharePoint. Możemy np. określić, że użytkownicy, których konta zostały utworzone na podstawie tego szablonu, będą mogli jedynie przeglądać portal firmowy bez możliwości edycji zawartości (opcja Czytelnik). Naciśnięcie Dalej wyświetla okno służące do wprowadzania informacji adresowych. Jego modyfikacja jest przydatna, gdy konta zakładane na podstawie szablonu będą miały inne dane adresowe niż reszta firmy, np. gdyby redakcja PCWK miała siedzibę w innym miejscu niż wydawnictwo IDG. Kolejne okno służy do wprowadzenia informacji o limitach dyskowych. SBS 2003 domyślnie udostępnia jeden z folderów dla klientów pakietu. Limity dyskowe będą nałożone na wolumin, na którym znajduje się udostępnienie. Wprowadzone wartości będą obowiązywały konta założone na podstawie szablonu. Po kliknięciu Dalej wyświetlane jest okno podsumowujące i kreator kończy działanie. Warto pamiętać, że szablony upraszczają zarządzanie, ale nie pozwalają na konfigurację wielu ustawień. Wszystkie parametry określimy, korzystając z modułu Użytkownicy i komputery usługi Active Directory.

Administracja

Modyfikacja parametrów kont

Najprostsza metoda zmiany konfiguracji konta to skorzystanie z serii skrótów do najczęściej wykonywanych zadań z folderu Użytkownicy. Wybranie odpowiedniej opcji pozwala łatwo zmienić nazwę konta czy zmienić hasło, dodać użytkownika do grupy, skonfigurować przekierowanie folderu Moje dokumenty lub zablokować konto. Żadna z tych operacji nie wymaga ani zaawansowanej wiedzy, ani skomplikowanych narzędzi. Wystarczy wybór jednej z opcji lub wpisanie właściwych wartości.

Wprowadzenie nieco bardziej zaawansowanych zmian jest możliwe po skorzystaniu z kreatora Zmień uprawnienia użytkownika. Jego działanie polega na przeniesieniu na modyfikowane konto parametrów przypisanych do jednego z wcześniej utworzonych szablonów. Aby uruchomić kreator, aktywujemy moduł Zarządzanie serwerem i przechodzimy do folderu Użytkownicy. Tam na liście narzędzi odnajdujemy i klikamy opcję Zmień uprawnienia użytkownika. Po uruchomieniu kreatora jesteśmy proszeni o wskazanie, z jakiego szablonu będziemy korzystać, modyfikując uprawnienia. Dalej określamy konto lub konta objęte modyfikacją i gotowe. Jest to bardzo prosta metoda, przeznaczona do wąskiej grupy operacji.

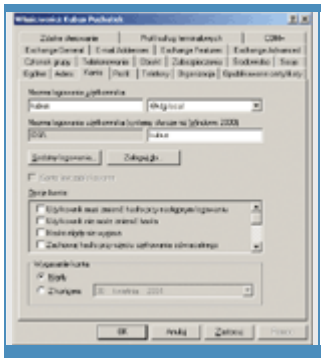
Jeżeli chcemy wprowadzić dodatkowe informacje do kont użytkowników lub gdy trzeba zmienić ich właściwości, kreatory nie wystarczą. W celu edytowania parametrów konta możemy się posłużyć skrótem Zmień właściwości użytkownika z folderu Użytkownicy lub odnaleźć użytkownika w Użytkownicy i komputery usługi Active Directory i z menu podręcznego wybrać Właściwości.

Właściwości kont użytkowników

Okno opisujące cechy konta zawiera kilka rzędów kart przeznaczonych do określenia dodatkowych parametrów środowiska użytkownika. Gdy skorzystamy ze skrótu Zmień właściwości użytkownika, część kart jest niewidoczna. Jeśli chcemy zobaczyć wszystkie, należy w module Użytkownicy i komputery usługi Active Directory z menu Widok wybrać Opcje zaawansowane.

Rys. 7. Konfiguracja wygasania konta.

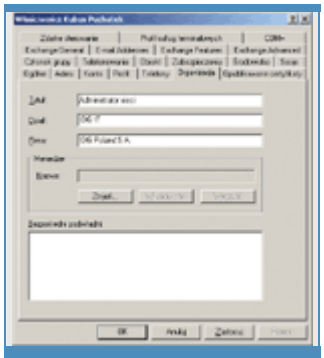
Omawianie każdej z kart właściwości użytkownika nie jest konieczne. Grupa kart obejmująca ustawienia Exchange zostanie przedstawiona w artykule "Poczta firmowa i internetowa". Część ustawień kont należy konfigurować jedynie w przypadku wykorzystywania specyficznych usług systemu. Na przykład karty Zdalne sterowanie, Profil usług terminalowych, Sesje i Środowisko służą do określania cech użytkowników będących klientami usług terminalowych, a karta Telefonowanie jest przydatna podczas definiowania uprawnień do zdalnego dostępu do serwera. Również i te parametry kont zostaną szerzej opisane w dalszych częściach przewodnika po SBS 2003.



Rys. 8. Karta Konto.

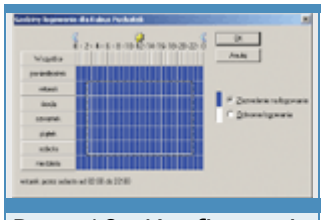
SBS wykorzystuje Active Directory do przechowywania informacji o atrybutach użytkowników, które mogą być przydatne innym pracownikom firmy. To, co zostanie wprowadzone na kartach Ogólne, Adres, Telefony i Organizacja, nadaje się do wykorzystania w opcji Wyszukaj (menu Start).

Na karcie Ogólne znajdują się informacje o danych osobowych użytkownika. Użycie kreatora SBS do zakładania konta spowodowało wypełnienie jedynie trzech pól: Imię, Nazwisko i Nazwa wyświetlana. Na tej karcie dodatkowo możemy wprowadzić takie dane, jak opis użytkownika, miejsce zatrudnienia, telefon, adres poczty elektronicznej oraz adres witryny internetowej. Jeśli w kreatorze wprowadziliśmy adres e-mail, wówczas i to pole nie będzie wymagało aktualizacji. Dane adresowe konta (Adres) służą do gromadzenia informacji o miejscu zatrudnienia pracownika. SBS 2003 automatycznie wypełnia tę kartę na podstawie danych wpisanych podczas instalacji pakietu.



Rys. 9. Miejsce na informacje o stanowisku użytkownika.

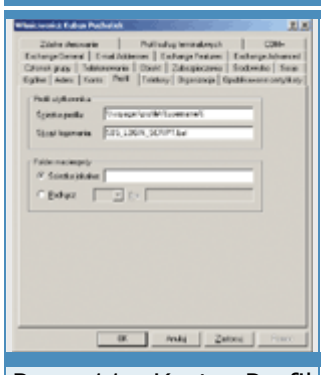
Karta Telefony to miejsce na podanie kontaktowych numerów telefonicznych. Oprócz telefonu domowego, możemy wprowadzić numery telefonu komórkowego, pagera, faksu oraz dane telefonu IP. Pole Uwagi jest przeznaczone na dodatkowe informacje, np. o godzinach pracy pracownika. Organizacja jest ostatnią kartą informacyjną. Wprowadzamy na niej dane związane z zajmowanym stanowiskiem, działem i o firmie pracownika. Dolna część karty jest przeznaczona na informacje o przełożonym pracownika oraz raportowaniu. Dane te dla firm pracujących z pakietem SBS 2003 mogą mieć marginalne znaczenie.



Rys. 10. Konfiguracja godzin logowania.

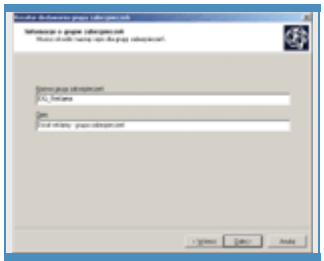
Właściwości karty Konto

Bardzo ważną kartą właściwości konta jest Konto. Zgrupowane na niej parametry nie są dostępne przez kreatory SBS. Okno karty zostało podzielone na trzy części. Pierwsza zawiera nazwy kont wykorzystywane podczas logowania, druga - dodatkowe parametry konta, a trzecia - datę wygaśnięcia konta. Opcje Nazwa logowania użytkownika oraz Nazwa logowania użytkownika (systemy starsze niż Windows 2000) służą do wpisania nazwy logowania użytkownika. Podanie różnych nazw do systemów wcześniejszych i późniejszych od Windows 2000 może być konieczne wtedy, gdy nazwa logowania użytkownika będzie długa. Dodatkowo systemy operacyjne typu Windows NT lub Windows 98 nie potrafią prawidłowo uwierzytelnić użytkownika posługującego się nazwą typu: nazwa_konta@nazwa_domeny . Dla tych systemów zrozumiała jest wyłącznie notacja: nazwa_domeny\nazwa_użytkownika.



Rys. 11. Karta Profil właściwości konta.

Klikając przyciski Godziny logowania oraz Zaloguj do, możemy zdefiniować dodatkowe ograniczenia konta. Przycisk Godziny logowania służy do ustalenia godzin pracy użytkownika, natomiast Zaloguj do - do wskazania komputerów, z których będzie można zalogować się do domeny pakietu SBS.



Rys. 12. Tworzenie grupy zabezpieczeń.

Grupa ustawień zgromadzona w sekcji Opcje konta jest wykorzystywana do określenia dodatkowych parametrów konta. Pierwsza część ustawień wiąże się z konfiguracją haseł. Opcja Użytkownik musi zmienić hasło przy następnym logowaniu wymusza zmianę hasła. Stosujemy ją zwykle wtedy, gdy chcemy zapobiec używaniu przez dłuższy czas tego hasła, które przypisał administrator. Opcję Użytkownik nie może zmienić hasła zaznaczamy na kontach współdzielonych przez wielu klientów lub wykorzystywanych przez oprogramowanie. Parametr Hasło nigdy nie wygasa pozwala uniknąć kłopotów związanych z zasadami haseł. Jest przeznaczony do kont wykorzystywanych przez aplikacje i usługi. Opcja Zachowaj hasło przy użyciu szyfrowania odwracalnego jest zaznaczana, gdy klienci logują się z komputerów Apple lub gdy korzystamy z uwierzytelnienia metodą Digest z Internetowych Usług Informacyjnych. Ze względów bezpieczeństwa nie należy włączać tego parametru. Opcja Konto jest wyłączone blokuje konto. Opcja Logowanie interakcyjne wymaga karty inteligentnej jest stosowana wtedy, gdy trzeba wymusić stosowanie kart inteligentnych podczas logowania do domeny. Logowanie interakcyjne to takie, w którym użytkownik jawnie wprowadza nazwę konta oraz hasło. Następne dwie opcje, Konto jest zaufane w kwestii delegowania i Konto jest poufne i nie może być delegowane obejmują ustawienia związane z usługami Windows Server 2003. Delegowanie zezwala na uzyskiwanie dostępu do zasobów sieciowych w kontekście uprawnień konta użytkownika przez usługi systemowe. Zaznaczenie parametrów Użyj typów szyfrowania DES dla tego konta oraz Nie jest wymagane wstępne uwierzytelnianie protokołu Kerberos jest wykorzystywane podczas integracji uwierzytelniania z innymi systemami operacyjnymi stosującymi Kerberos. Opcje konta należy stosować z rozwagą, gdyż ich pochopne zaznaczenie może przysporzyć kłopotów z uwierzytelnieniem lub bezpieczeństwem systemu.

Wygasanie konta określamy wtedy, gdy konfigurujemy konta dla pracowników tymczasowych lub zatrudnionych na okres próbny. Wprowadzenie daty dla opcji Z końcem, powoduje, że nie musimy pamiętać o zablokowaniu konta po wygaśnięciu umowy pracownika (rys. 7).

Karta Profil

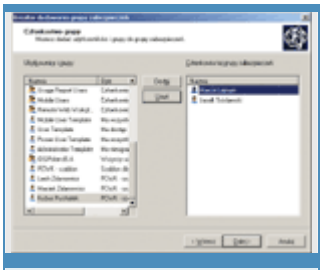
Karta Profil pozwala na ustawienie parametrów obejmujących profile, katalogi domowe oraz skrypty logowania. Standardowo profile klientów sieci są przechowywane na stacjach lokalnych. Jeśli użytkownik zmieni komputer, każdorazowo będzie miał utworzony nowy profil. W pole Ścieżka profilu wpisujemy ścieżkę wskazującą na położenie profilu mobilnego użytkownika. Po określeniu ścieżki ustawienia użytkownika są pobierane z serwera SBS. Ścieżkę wprowadzamy zgodnie ze składnią UNC (Universal Naming Convention). Obejmuje ona nazwę serwera oraz nazwę udostępnienia zapisane w formie \\nazwa_serwera\nazwa_udostępnienia. Na końcu ścieżki powinniśmy wprowadzić nazwę konta użytkownika lub zmienną %UserName%.

Przypisanie skryptów logowania przy użyciu opcji Skrypt logowania wykonujemy niezwykle rzadko. Lepsze rozwiązania oferują zasady grupy, które umożliwiają skonfigurowanie skryptów logowania, wylogowania użytkownika oraz startu i zamykania systemu operacyjnego. Nie oznacza to, że opcja Skrypt logowania jest całkowicie zbędna. Doskonale sprawdza się wtedy, gdy klientami są komputery ze starszymi systemami operacyjnymi, takimi jak Windows 98 lub NT Workstation. SBS stosuje ją podczas instalacji środowiska klienta, uruchamiając plik SBS_LOGIN_SCRIPT.bat

Karta Profil pozwala również na określenie położenia folderów macierzystych. Możemy skonfigurować jedną z dwóch opcji: przypisanie ścieżki lokalnej lub podłączenia do udostępnienia sieciowego. Konfiguracja lokalizacji sieciowej znacznie ułatwia zarządzanie dokumentami użytkowników. SBS 2003 stosuje inną technikę obsługi plików użytkowników sieci. W folderze Użytkownicy w grupie Zarządzanie standardowe modułu Zarządzanie serwerem, znajduje się skrót Konfiguruj przekierowywanie folderów Moje dokumenty. Korzystając z jego opcji, zmieniamy położenie folderu Moje dokumenty.

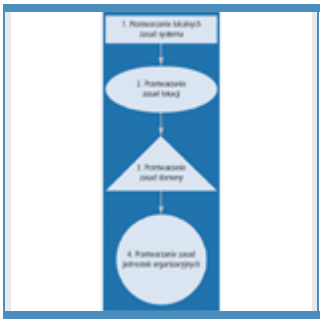
Grupy użytkowników

Konfiguracja parametrów kont służy do określenia właściwości użytkowników pakietu SBS. W module Zarządzanie serwerem są dwa foldery do konfiguracji grup klientów sieci. Grupy tworzy się w celu uproszczenia zarządzania uprawnieniami i prawami użytkowników lub w celu wysyłania wiadomości przeznaczonych do wielu kont. Szybciej i łatwiej skonfigurujemy dostęp grupy do zasobu niż dostęp poszczególnych kont z osobna. Więcej informacji na temat konfiguracji uprawnień zawiera artykuł "Współdzielenie zasobów". SBS pozwala na utworzenie Grup zabezpieczeń i Grup dystrybucyjnych. Typy grup są stosowane do określania przeznaczenia grupy.



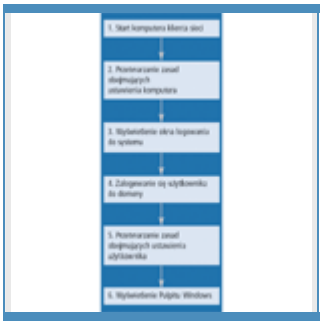
Rys. 13. Dodawanie użytkowników do grupy.

Grupy zabezpieczeń służą do gromadzenia kont o wspólnych uprawnieniach. Po założeniu grupy oraz dodaniu do niej użytkowników, możemy stosować ją do nadawania uprawnień drukarek, rejestru, Active Directory czy systemu plików NTFS. Grupy dystrybucyjne służą do gromadzenia kont, którym będziemy przekazywać wiadomości poczty elektronicznej. Grupom tego typu nie można przypisywać uprawnień. Ponieważ mogą również pełnić funkcję grup dystrybucyjnych, najczęściej korzystamy z pierwszego typu.



Kolejność przetwarzania zasad.

Utworzenie grupy użytkowników to łatwa operacja. Po uruchomieniu modułu Zarządzanie serwerem przechodzimy do folderu Grupy zabezpieczeń, gdzie klikamy Dodaj grupę zabezpieczeń. W pierwszym oknie kreatora naciskamy Dalej, a następnie wprowadzamy nazwę i opis grupy, na przykład RedakcjaPCWK, a w opisie Konta pracowników redakcji PC World Komputer. W kolejnym oknie wybieramy konta, które będą należeć do grupy. Po zaznaczeniu konta naciskamy Dodaj i klikamy Dalej. Jeśli chcemy dodać więcej niż jedno konto, klikamy lewym przyciskiem myszy, naciskając jednocześnie [Shift] (w przypadku kont leżących obok siebie) lub [Ctrl] (w przypadku kont rozproszonych). Naciśnięcie Zakończ kończy pracę kreatora. Tworząc grupy dystrybucyjne, postępujemy analogicznie.

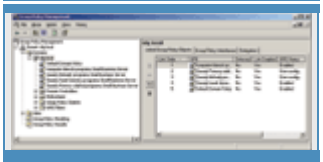


Kolejność przetwarzania zasad na stacji.

Jeśli chcemy zmodyfikować parametry grup, po zaznaczeniu folderu Grupy zabezpieczeń lub Grupy dystrybucyjne wskazujemy grupę i klikamy Zmień właściwości grupy. W oknie właściwości grupy są karty: Ogólne, Członkowie, Członek grupy i Zarządzany przez. Karta Ogólne gromadzi dane informacyjne, takie jak nazwa, opis lub e-mail. Dodatkowo służy do określania zakresu i typu grupy. Zakresy grup: Lokalny w domenie, Globalny lub Uniwersalny służą do wyznaczania widoczności grupy w środowiskach wielodomenowych. Np. grupy z zakresu Globalny mogą mieć przypisywane uprawnienia do zasobów znajdujących się w innych domenach. W systemie SBS nie mają większego znaczenia i należy pozostawić taki zakres, jaki proponuje kreator. Karta Członkowie służy do zarządzania członkostwem grupy. Korzystając z przycisków Dodaj i Usuń, dodajemy lub usuwamy konta użytkowników. Karta Członek grupy zawiera listę grup, do których należy wskazana grupa. Chociaż system Windows Server 2003 dopuszcza zagnieżdżanie grup, w niewielkim środowisku pakietu SBS działania te nie są uzasadnione. Ostatnia karta, Zarządzany przez, służy do wskazania konta, które zarządza daną grupą. W małych sieciach, wskazanie to ma charakter czysto informacyjny i w większości przypadków pole Nazwa możemy pozostawić puste.

Kolejność przetwarzania skryptów.

Zasady grupy



Narzędzie Group Policy Management.

Windows Server 2003 jest oferowany łącznie z bardzo przydatnym narzędziem do kompleksowego zarządzania środowiskiem klientów sieci. Nawet przy niedużej liczbie komputerów, wykonując te same czynności administracyjne na wielu stacjach, tracimy czas i pieniądze. Dzięki zastosowaniu Zasad grupy, możemy łatwo wpływać na zabezpieczenia oraz konfigurację komputerów i użytkowników pakietu SBS 2003. Głównym zadaniem Zasad

grupy jest scentralizowanie, ujednolicenie i usprawnienie zadań związanych z administracją sieci. Osoba zarządzająca komputerami definiuje zbiór parametrów, zwanych obiektem zasad, które obejmują konfigurację różnych komponentów systemów klienckich, np. parametrów zabezpieczeń, usług systemowych lub Internet Explorera. Następnie ustawienia te są wiązane z obiektami Active Directory. W ten sposób wskazujemy systemowi, na które komputery lub użytkowników mają zostać przeniesione skonfigurowane zasady.

Zbiór zdefiniowanych obiektów zasad jest przypisywany do obiektów przechowywanych w Active Directory. Muszą to być obiekty typu pojemnik: jednostka organizacyjna, domena lub lokacja. Systemy operacyjne Windows XP lub Windows 2000 pozwalają również na definiowanie oddzielnych zasad w swoich macierzystych stacjach. Lokalne ustawienia nie wykraczają jednak poza komputer, w którym zostały założone. Dodatkowo ustawienia przenoszone z usługi Active Directory zastępują lokalną konfigurację systemu. Struktura usług katalogowych jest wielopoziomowa. Domena może obejmować wiele lokacji. W domenie zakładamy również obiekty typu jednostka organizacyjna. Gdy w takiej jednostce umieścimy kolejną jednostkę, powstanie konstrukcja przypominająca drzewo katalogów. Do każdego z wymienionych obiektów mogą być przypisywane odmienne zasady. Jeśli ustawienia będą definiowane w nieprzemyślany sposób, doprowadzimy do konfliktów, w których kolejne zasady będą zmieniać ustawienia narzucone przez poprzednie. Dlatego warto poznać kolejność przypisywania obiektów zasad. Najpierw dodaje się zasady związane z lokacją, potem zasady domenowe, następnie na systemy klientów przenoszone są zasady z jednostek organizacyjnych. Jeśli jednostka zawiera inne jednostki, zasady najbardziej zagnieżdżonego obiektu są dodawane na końcu.

Definicje obiektów związanych z zasadami grupy

Lokacja - jedna lub wiele podsieci IP połączonych wydajnym łączem. Definicja wydajnego łącza nie może być precyzyjna dlatego, że o wydajności decydują potrzeby firmy. Odmienne potrzeby będzie miała firma intensywnie eksploatująca połączenie rozległe, a inne taka, w której ruch na liniach WAN będzie sporadyczny. Lokacje służą do usprawnienia uwierzytelnienia klientów sieci oraz do nadzoru nad replikacją pomiędzy kontrolerami domeny. Konfiguracja wielu lokacji w przypadku pakietu SBS jest sporadyczna, ale w pełni możliwa. Zasady grupy przypisane do lokacji obejmują wszystkie stacje i konta przynależące do związanej z lokacją podsieci.

Jednostka organizacyjna - to rodzaj kontenera do grupowania obiektów o podobnej charakterystyce. Mogą zawierać na przykład użytkowników z określonego działu, lokalizacji lub wykonujących zbliżone czynności. Ich zadanie można porównać do roli katalogu w systemie plików. Ze względu na ograniczoną liczbę klientów (do 75), zakładanie wielu jednostek organizacyjnych dla pakietu SBS 2003 jest rzadko spotykane. Zasady grupy przypisane do jednostki organizacyjnej obejmują wszystkie obiekty umieszczone bezpośrednio w jednostce i wszystkich podjednostkach.

Domena - zbiór zasobów należących do jednej organizacji. Informacja o zasobach jest przechowywana we współdzielonej bazie Active Directory. W przypadku pakietu SBS 2003 najczęściej będzie to grupa wszystkich zasobów firmy. Zasady grupy przypisane do domeny obejmują wszystkie obiekty wewnątrz domeny.

Administracja

Jacek Ścisławski
10 maja 2004
PC World Komputer

Każda zasada umożliwia określenie parametrów użytkowników i komputerów. Jeśli skonfigurujemy obiekty zasad dotyczące użytkowników, wszystkie konta klientów objęte zasadami będą miały takie same ustawienia. Zalogowanie się do innego komputera nie będzie miało większego znaczenia. Przykładem parametru podążającego za użytkownikiem może być ukrycie ikony Ekran z Panelu sterowania. Przypisanie konfiguracji do obiektu typu komputer oznacza, że konfigurowane są parametry systemu operacyjnego niezależne od użytkownika

albo obejmujące wszystkie klienty stacji. Przykładem może być automatyczne włączenie przydziałów dysków w komputerach lokalnych lub wyłączenie raportowania błędów.

Przetwarzanie i rodzaje zasad

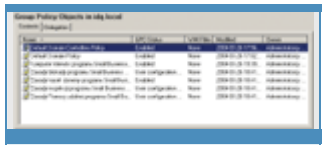
Obiekty zasad są tworzone i przechowywane w kontrolerze domeny. Jest to komputer z zainstalowanym pakietem SBS 2003. Implementacja ustawień odbywa się w komputerach klientów sieci. Jeśli założymy zasadę i przypiszemy ją do np. do jednostki organizacyjnej SBSComputers (jest to pojemnik domyślnie przeznaczony na konta stacji roboczych), wówczas w czasie startu wszystkie komputery klienckie trzymają parametry ustawione w obiekcie zasad. Gdyby konto komputera nie znajdowało się w pojemniku SBSComputers, nie byłoby objęte zasadami. Podobnie jest z kontami użytkowników. Jeśli konto zostanie założone za pomocą kreatora pakietu SBS, wówczas jest umieszczane w pojemniku SBSUsers, zawartym w jednostce organizacyjnej MyBusiness. Przypisanie obiektu zasad do pojemnika SBSUsers, spowoduje, że skonfigurowane w nim parametry zostaną przypisane do każdego konta umieszczonego w tym pojemniku.

Ustawienia komputera są dodawane w czasie startu komputera, natomiast ustawienia związane z użytkownikami - po zalogowaniu do sieci. Parametry konfiguracyjne zasad pozwalają też na określenie interwału automatycznego odświeżania ustawień. Dzięki temu wprowadzenie zmian w obiektach zasad nie wymaga przelogowania lub restartu komputera. Naniesione modyfikacje i tak trafią do swoich odbiorców. Wśród parametrów zasad odnajdziemy również wywoływane po wystąpieniu pewnych zdarzeń. Administrator może przypisać wywoływanie skryptów do komputerów lub użytkowników. Dla obiektu użytkownik dostępne są skrypty przetwarzane podczas logowania i wylogowania. Skrypty związane z obiektem typu komputer, będą uruchamiane zawsze podczas startu lub wyłączania stacji.

Rys. 19. Raport o parametrach jednej z zasad.

Rys.15. Karta Group Policy Inheritance.

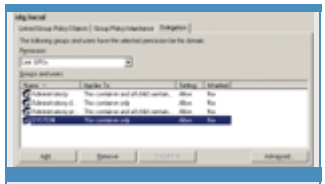
Podczas instalacji pakietu SBS instalator tworzy obiekty zasad przypisane do domeny oraz jednostki organizacyjnej Domain controlers. Chcąc skonfigurować dodatkowe parametry przenoszone na wszystkich użytkowników lub komputery, należy zmodyfikować domyślną zasadę domeny. Alternatywnym rozwiązaniem jest utworzenie nowego obiektu zasad i związanie go z domeną tak, żeby parametry nowego obiektu nie wchodziły w konflikt z ustawieniami przenoszonymi przez inne zasady. Do zakładania nowych obiektów oraz obserwacji rezultatów działania zasad służy narzędzie Group Policy Management.



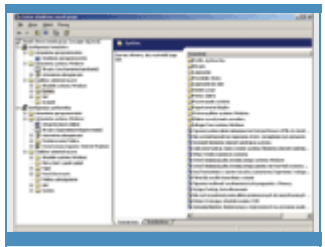
Rys. 16. Zawartość folderu Group Policy Objects.

Narzędzia do konfiguracji zasad

Pakiet SBS 2003 zawiera nowe narzędzie do konfigurowania zasad grupy, Group Policy Management. W folderze Zarządzanie zaawansowane modułu Zarządzanie serwerem odnajdziemy je pod nazwą Zarządzanie zasadami grupy. Natomiast bezpośrednio z Narzędzi administracyjnych jest ono dostępne jako Group Policy Management. Udostępnia informacje o właściwościach wszystkich obiektów zasad utworzonych w lesie Active Directory. Las domen Active Directory to grupa domen powiązanych relacjami zaufania. Ponieważ działanie pakietu Small Business jest ograniczone do jednej domeny, w praktyce Zarządzanie zasadami grupy nie sięga poza tę strukturę.



Rys. 17. Karta Delegation.



Rys. 18. Okno Edytora obiektów zasad grupy.

Interfejs modułu do zarządzania obiektami zasad może się wydawać mało czytelny, ale to mylne wrażenie. Za jego pomocą łatwo skonfigurujemy i przeanalizujemy nawet bardzo zagmatwane i wielopoziomowe zasady. Jedynym warunkiem skutecznego posługiwania się GPM jest zrozumienie sposobu funkcjonowania i przypisywania zasad grupy.

Zasadami możemy zarządzać również tak, jak na serwerze Windows 2000. W module Użytkownicy i komputery usługi Active Directory, we właściwościach obiektów typu Domena lub Jednostka organizacyjna znajduje się karta Group Policy. Możemy ją wykorzystać do konfiguracji obiektów zasad oraz ich właściwości. Ostatnim sposobem jest dodanie do konsoli MMC modułu Edytor obiektów zasad grupy.

Oprócz narzędzi z interfejsem graficznym są też narzędzia wiersza poleceń. Najbardziej popularne to GPResult i GPUpdate. Ponieważ Group Policy Management jest najlepsze, przede wszystkim należy się posługiwać tym narzędziem.

Obsługa Group Policy Management

Po uruchomieniu modułu GPM widoczny jest identyfikator lasu domeny. Po jego rozwinięciu ukazują się cztery foldery: Domains, Sites, Group Policy Modeling oraz Group Policy Results. Rozpocznijmy od opisu zawartości folderu Domains.

Rozwinięcie folderu wyświetla listę domen. W przypadku pakietu SBS 2003 lista będzie zawierać domenę założoną w trakcie instalacji. W dużych korporacjach listę domen można rozszerzyć. Zaznaczenie nazwy domeny powoduje wyświetlenie w prawym panelu listy przypisanych do niej zasad. Jeśli dodatkowo, kliknięciem plusa, rozwiniemy domenę, oprócz dodanych obiektów zasad zostaną wymienione jednostki organizacyjne wewnątrz domeny oraz foldery Group Policy Objects i WMI Filters. Lista jednostek organizacyjnych nie zawiera wbudowanych folderów Active Directory, takich jak Users i Computers, ponieważ nie możemy przypisać im żadnych zasad. Dalsza nawigacja opiera się na rozwijaniu i zwijaniu jednostek organizacyjnych w celu sprawdzenia, jakie obiekty zasad są do nich przywiązane.

Zaznaczenie w lewym panelu jednego z obiektów typu pojemnik, np. domeny, powoduje wyświetlenie w prawym panelu okna, które zawiera trzy karty: Linked Group Policy Objects, Group Policy Inheritance oraz Delegation. Po zaznaczeniu pierwszej zobaczymy listę zasad oraz ich właściwości. Gdy zaznaczony obiekt nie ma przypisanego obiektu zasad, lista będzie pusta. Jeśli do domeny lub jednostki organizacyjnej przypiszemy wiele zasad, klikanie przycisków nawigacyjnych: Move link to top, Move Link up, Move link down i Move link to bottom pozwala na zmianę kolejności implementacji obiektów. Najwyższy priorytet będzie miała pierwsza zasada na liście. Warto pamiętać, że nie jest to równoznaczne z pierwszeństwem w implementacji. Ostatni obiekt zasad zastosowany do użytkownika lub komputera jest najważniejszy, bo to jego ustawienia mogą zastąpić przekazane wcześniej parametry. Przesunięcie zasady na pierwsze miejsce, wbrew pozorom, oznacza, że będzie stosowana na końcu. Listę właściwości zasad omówimy nieco dalej. Karta Group Policy Inheritance wyświetla listę zasad odziedziczonych po obiektach nadrzędnych lub przypisanych bezpośrednio. Parametry zasad, podobnie jak uprawnienia w systemie plików NTFS, są dziedziczone. Oznacza to, że jeśli do domeny przypiszemy zasadę ukrywającą polecenie Uruchom z menu Start, to użytkownicy, których konta są zlokalizowane w wewnętrznych jednostkach organizacyjnych lub ich podjednostkach, po zalogowaniu nie zobaczą polecenia Uruchom. Ostatnia karta, Delegation, wyświetla listę kont grup lub użytkowników, którzy mogą zarządzać uprawnieniami do obiektów zasad w zaznaczonym pojemniku.

Rozwinięcie w lewym panelu ikony reprezentującej domenę wyświetla listę przywiązanych zasad, jednostek organizacyjnych oraz dwa dodatkowe foldery: Group Policy Objects oraz WMI Filters. Po zaznaczeniu pierwszego wyświetlana jest lista wszystkich obiektów zasad zdefiniowanych w Active Directory. WMI Filters zawiera listę wszystkich filtrów WMI. Foldery te pomagają uzyskać dane o każdym z założonych obiektów. Poszczególne obiekty zasad mogą być związane z wieloma pojemnikami, tak jak w systemie plików może być wiele skrótów do jednego pliku. Jeśli zmodyfikujemy obiekt zasad, wówczas skutki tej zmiany obejmą wszystkie pojemniki, z którymi zasada jest powiązana.

Administracja

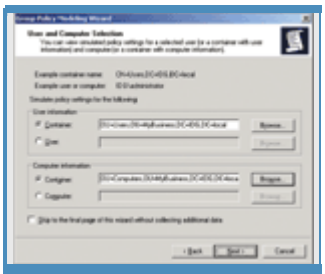
Jacek Ścisławski
10 maja 2004
PC World Komputer

Właściwości obiektów zasad

Każdy obiekt zasad ma grupę opisujących go właściwości. Jedną z nich jest opisywane już dowiązanie. Pojedyncza zasada może być związana z wieloma obiektami. Jest to efektywne, ponieważ nie musimy wielokrotnie dublować ustawień konfiguracyjnych. Inną cechą obiektów zasad jest filtrowanie zabezpieczeń. Konfiguracja filtrowania oznacza wskazanie, do których kont użytkowników, grup lub komputerów zasada ma zostać przypisana. Jeśli chcemy zastosować zasadę tylko do określonego komputera lub użytkownika, należy zastosować filtrowanie. Podobne rezultaty ma zastosowanie filtrów WMI. Każdy obiekt zasad może mieć przypisany filtr WMI, zawężający zakres obiektów podlegających zasadzie.

Standardowa zasada zawiera parametry przenoszone na użytkowników oraz na komputery. Jeśli tworzymy zasadę przeznaczoną do jednostki organizacyjnej zawierającej wyłącznie komputery, przetwarzanie ustawień związanych z użytkownikiem nie jest konieczne. Podobnie będzie w przypadku pojemników, w których umieścimy jedynie konta użytkowników. Konfigurując właściwości obiektu zasad, możemy określić jego stan. Do wyboru mamy jedno z czterech ustawień: All settings disabled, Computer configuration settings disabled, User configuration settings disabled i Enabled. Konfigurując te parametry, wskazujemy, jak system ma przetwarzać zasady. Dodatkowo, gdy wykonujemy testy implementacji zbioru zasad, możemy poszczególne chwilowo wyłączyć.

Powiązania zasad również mają swoje właściwości. W miarę potrzeb, stan każdego z powiązań możemy określić jako włączony lub wyłączony. Wówczas tylko wskazane powiązanie przestaje być aktywne. Innym parametrem powiązań jest wymuszanie przypisywania. O kolejności przetwarzania zasad decyduje poziom obiektu, z którym zostały powiązane, a przy wielu zasadach dotyczących tego samego pojemnika - kolejność powiązania. Enforced służy do wymuszenia przypisania ustawień zawartych w obiekcie zasad, bez względu na kolejność, poziom i ewentualne konflikty. Jeśli na przykład powiążemy zasadę z domeną, jest ona przetwarzana wcześniej niż zasady jednostek organizacyjnych. Parametry zasad jednostek mogą zmienić ustawienia domenowe, ponieważ są dodawane później. Aby zapobiec niechcianym zmianom, należy w powiązaniu domeny z obiektem zasad, włączyć opcję Enforced.



Rys. 22. Okno kreatora raportu.

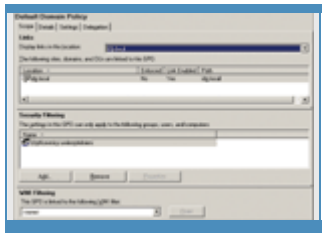
Rys. 23. Raport o wynikowym zestawie zasad.

Parametry zabezpieczeń.

Parametry obiektów i dowiązań zasad są wyświetlane po ich zaznaczeniu w lewym panelu Group Policy Management.

Tworzenie nowej zasady

Utworzenie nowego obiektu zasad nie jest skomplikowane. Po uruchomieniu modułu GPM przechodzimy do folderu Group Policy Objects i z menu Akcja wybieramy New. Wpisujemy nazwę zasady i naciskamy OK. Nowo utworzona zasada nie zawiera żadnych ustawień. Jeśli chcemy wprowadzić nowe parametry, z menu kontekstowego wybieramy polecenie Edit. Spowoduje to wyświetlenie edytora obiektów zasad.



Rys. 21. Karta Scope obiektu zasad.

Okno edytora jest podzielone na dwa panele. Lewy zawiera ustawienia użytkownika i komputera wraz z podfolderami grupującymi opcje zasad. W prawym panelu są opcje konfiguracyjne. Przy każdym z parametrów znajduje się opis jego działania. Trzeba zwracać uwagę na umieszczone w opisie wymagania systemowe, gdyż niektóre z ustawień mogą być przenoszone wyłącznie do nowszych systemów operacyjnych, np. Windows XP i Server 2003.

Konfiguracja poszczególnych opcji polega na wprowadzeniu odpowiedniej wartości parametru lub określeniu położenia przełącznika. Aby zmienić ustawienie, klikamy dwukrotnie wybrany obiekt. W wypadku większości parametrów związanych z zabezpieczeniami wpisujemy żądaną wartość lub wybieramy ją z listy. W ten sposób określamy na przykład minimalną liczbę znaków w haśle systemu. Nieco inaczej modyfikujemy parametry w Szablonach administracyjnych. Określenie ustawień polega na zmianie stanu przełącznika. System daje do wyboru trzy

wartości: Nie skonfigurowano, Włączone i Wyłączone. Pierwsza opcja wskazuje, że ustawienie jest neutralne i nie będzie brane pod uwagę podczas implementacji zasad. Następne włączają lub wyłączają wskazane parametry. Konfigurując ustawienia Włączone i Wyłączone, nie wolno wchodzić w konflikt z zasadami dotyczącymi innych pojemników lub poziomów.

Konfiguracja zasad zabezpieczeń

Zalety zasad grupy najlepiej ukazuje zastosowanie ich do konfiguracji zabezpieczeń sieci. Po określeniu zasad domeny w folderze Konfiguracja komputera | Ustawienia systemu Windows | Ustawienia zabezpieczeń znajdziemy grupę ustawień, które mają znaczny wpływ na zabezpieczenia całej sieci. Lista folderów jest długa i obejmuje grupy: Zasady konta, Zasady lokalne, Dziennik zdarzeń, Grupy z ograniczeniami, Usługi systemowe, Rejestr, System plików, Zasady sieci bezprzewodowej (IEEE 802.11), Zasady kluczy publicznych, Zasady ograniczeń oprogramowania oraz Zasady zabezpieczeń IP w Usłudze Active Directory. Omawianie każdego z parametrów nanoszonych przez te ustawienia wykracza poza ramy artykułu. Krótki opis przeznaczenia poszczególnych folderów zawiera tabela.

Próbka możliwości zasad grupy jest zdefiniowana w parametrach folderu Użytkownicy w module Zarządzanie serwerem. W folderze Użytkownicy, jedna z opcji to Konfiguruj zasady haseł. Kliknięcie skrótu wyświetla możliwe do skonfigurowania parametry haseł klientów sieci. Przypisane w oknie opcje są w rzeczywistości ustawieniami wprowadzonymi do Zasady haseł domeny programu Small Business Server. W ten łatwy sposób możemy centralnie narzucać parametry klientów sieci.

Określanie rezultatu działania zasad

Przeglądanie ustawień zasad w edytorze obiektów nie jest najlepszym pomysłem. Mnogość parametrów sprawia, że ustalenie faktycznie nanoszonych przez zasadę opcji byłoby niewygodne i czasochłonne. Zarządzanie zasadami grupy oferuje kilka czytelnych sposobów raportowania parametrów zasad.

Raport o konfiguracji każdej zasady znajdziemy, klikając kartę Settings we właściwościach obiektu lub powiązania. Przy użyciu poleceń Show all, Show i Hide możemy swobodnie poruszać się po ustawieniach. Raport zawiera informacje tylko o tych opcjach zasad, które mają określone wartości lub przypisane wartości Enabled lub Disabled. Wszystkie elementy z wartością Not configured są pomijane.

Raport o poszczególnych zasadach na niewiele się przyda, jeśli do domeny lub jednostek organizacyjnych przypiszemy wiele obiektów zasad. Wiedząc, co zmienia każdy z obiektów, administrator i tak musiałby analizować zagnieżdżenia pojemników oraz priorytety zasad. Biorąc dodatkowo pod uwagę możliwość blokowania dziedziczenia lub wymuszanie przypisywania zasad, byłoby to niezmiernie trudne. W narzędziu Group Policy Management znajdują się dwa foldery Group Policy Modeling oraz Group Policy Results, które pozwalają na szczegółową analizę przetwarzania zasad grupy.

Group Policy Modeling służy do analizowania planowanych zmian w zasadach grupy. Dzięki tej opcji możemy łatwo ustalić, jakie będą skutki przeniesienia konta użytkownika do nowej jednostki organizacyjnej, wpływ priorytetów zasad na przetwarzanie kont komputera i użytkownika itp.

Narzędzie Group Policy Results pozwala na analizowanie faktycznych rezultatów stosowania zasad grupy do określonego konta użytkownika lub komputera. Raport o dodawanych ustawieniach otrzymamy po uruchomieniu kreatora przetwarzania zasad. Na przykład w celu ustalenia, jakie ustawienia będą dodane do komputera Sekretariat z domeny IDG.local, należy przejść do modułu Zarządzanie zasadami grupy, następnie rozwinąć las idg.local i zaznaczyć folder Group Policy Results. Potem z menu kontekstowego wybieramy Group Policy Results Wizard i klikamy Dalej. W nowym oknie wprowadzamy nazwę Sekretariat. Chcąc ponadto ustalić, jakie ustawienia będą dodawane do użytkowników pracujących przy stacji Sekretariat, po kliknięciu Dalej wskazujemy konto klienta sieci. Kolejne naciśnięcie Dalej spowoduje wygenerowanie raportu o wynikowym zestawie zasad, który zostanie wyświetlony po kliknięciu Zakończ. Natomiast akceptując wszystkie domyślne ustawienia kreatora, wygenerujemy raport dotyczący naszego serwera i konta administratora, na którym pracujemy.

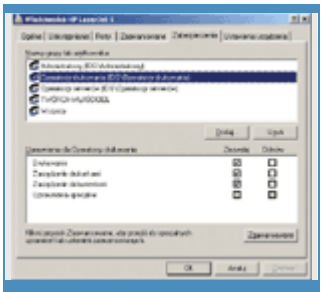
Współdzielenie zasobów

Maciej Zdanowicz
10 maja 2004
PC World Komputer
Najbardziej oczywistą przewagą sieci z serwerem nad sieciami równorzędnymi jest dostępna dla wszystkich możliwość korzystania z podłączonych do serwera urządzeń, globalnego zarządzania prawami dostępu, a także scentralizowanego i bezpiecznego przechowywania danych.

Pierwsze współdzielone zasoby zostały udostępnione użytkownikom zaraz po instalacji systemu, w trakcie wykonywania kolejnych zadań administracyjnych z Listy zadań do wykonania. Użytkownicy otrzymali wtedy możliwość współdzielenia połączenia internetowego, a nieco później również zainstalowanej właśnie drukarki. Z kolei podczas tworzenia kont użytkowników założony został dla nich specjalny katalog na serwerze, zwany folderem macierzystym. Użytkownikom zostały nadane także, wynikające z zastosowanego szablonu, prawa dostępu do firmowej witryny SharePoint.

Dane na dyskach

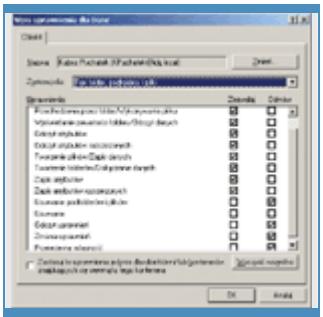
Sensowny system kontroli dostępu do plików i folderów da się zrealizować praktycznie dopiero wtedy, gdy do przechowywania danych wykorzystujemy system plików NTFS. W przeciwieństwie do systemów FAT umożliwia bowiem nadawanie użytkownikom uprawnień do określonych plików lub katalogów. Obiekty w systemie NTFS, czyli np. pliki lub foldery, mają skojarzone ze sobą listy kontroli dostępu, określane w skrócie jako ACL (Access Control List). Listy te zawierają nazwy użytkowników lub grup oraz przypisane im uprawnienia. Konfigurację uprawnień do danego folderu lub pliku przeprowadza się na karcie Zabezpieczenia we właściwościach wybranego obiektu. Skonfigurowane w ten sposób zasady dostępu mają zastosowanie do użytkowników zalogowanych w lokalnym systemie i bezpośrednio obsługujących dany komputer lub np. logujących się zdalnie za pomocą usługi zdalnego pulpitu.



Rys. 1. Karta Zabezpieczenia służy do nadawania użytkownikom uprawnień do plików lub katalogów.

Uprawnienia dostępne na karcie Zabezpieczenia to w rzeczywistości nazwy zestawów uprawnień głębszego poziomu, tzw. uprawnień specjalnych, których jest, po pierwsze, więcej, a po drugie, umożliwiają bardziej precyzyjną kontrolę. Wśród uprawnień, nazwijmy je podstawowych, znajdziemy Pełna kontrola, Modyfikacja, Zapis i wykonanie (właściwie powinno być Odczyt i wykonanie, ponieważ w oryginalnej wersji mamy Read and Execute), Wyświetlanie zawartości folderu, Odczyt, Zapis i Uprawnienia specjalne. Ostatnia opcja określa, czy zastosowano bardziej precyzyjną kontrolę dostępu do danego obiektu. Aby zmienić uprawnienia specjalne do obiektu, należy kliknąć Zaawansowane, wybrać z listy użytkownika lub grupę i kliknąć Edytuj. Korzystanie z zaawansowanych zabezpieczeń jest przydatne zwłaszcza wtedy, gdy musimy nadać użytkownikom bardzo specyficzne lub szczególnie restrykcyjne uprawnienia. Na przykład nadanie użytkownikowi KPuchatek uprawnień specjalnych jak na rysunku 2, spowoduje, że będzie mógł przeglądać zawartość folderu Dane oraz tworzyć nowe pliki i foldery. Będzie również mógł otwierać pliki (odczytywać ich zawartość) oraz je usuwać, ale tylko w przypadku, gdy będą to pliki utworzone przez niego. Nie wolno mu będzie natomiast odczytać ani usunąć pliku utworzonego przez innego użytkownika. Taka konfiguracja może się okazać przydatna na przykład przy udostępnianiu publicznego folderu, poprzez który zewnętrzni użytkownicy będą dostarczali materiały do firmy.

Uprawnienia NTFS są zorganizowane w strukturę drzewa, w której domyślnie obiekty podrzędne dziedziczą ustawienia po obiektach nadrzędnych. Mechanizmem tym steruje opcja Zezwalaj na propagowanie dziedziczonych uprawnień w oknie Zaawansowane ustawienia zabezpieczeń (które pojawia się po kliknięciu opcji Zaawansowane na karcie Zabezpieczenia). Jeżeli jest włączona, to każdy kolejny folder lub plik utworzony w bieżącym folderze (którego właściwości edytujemy), przejmie te ustawienia, które bieżący folder otrzymał od folderu nadrzędnego oraz wszystkie nowe, które zostały zdefiniowane tylko dla bieżącego folderu.



Rys. 2. Przykładowa konfiguracja uprawnień specjalnych do folderu udostępnionego użytkownikom zewnętrznym.

Gdy wyłączymy tę opcję dla folderu, który dotychczas dziedziczył ustawienia uprawnień, system zapyta, czy chcemy skopiować zestaw zasad, który aktualnie wynika z dziedziczenia. Jeżeli chcemy modyfikować dotychczasowe uprawnienia, to powinniśmy skopiować uprawnienia. W przeciwnym razie wszystkie zasady dostępu będziemy musieli tworzyć od nowa. Druga opcja, Zamień wpisy uprawnienia na wszystkich obiektach podrzędnych, pozwala globalnie zmienić uprawnienia do wszystkich plików i podkatalogów folderu bieżącego.

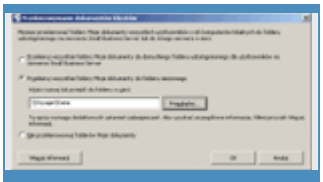
Ponieważ użytkownik może należeć do więcej niż jednej grupy, zdarza się, że jednej grupie nadano prawa zapisu i odczytu w konkretnym folderze, podczas gdy drugiej grupie nadano jedynie prawo odczytu. W efekcie użytkownik należący do obu grup będzie miał do danego folderu jedynie prawo odczytu. Podczas obliczenia tzw. efektywnych uprawnień w pierwszej kolejności brane są pod uwagę wszystkie ograniczenia, zatem wynikowe uprawnienia są najbardziej restrykcyjną kombinacją uprawnień nadanych różnym grupom.

Sytuacja wygląda podobnie w przypadku dostępu do danych poprzez udziały sieciowe, które mają własny zestaw uprawnień. Przy określaniu praw dostępu brane są pod uwagę zarówno uprawnienia do udziału (dostępne wartości to Pełna kontrola, Zmiana oraz Odczyt), jak i uprawnienia NTFS do folderu. Dostęp do udziału zostanie przyznany użytkownikowi tylko wtedy, gdy oba zestawy uprawnień na to pozwolą. Uprawnienia danego udziału stosowane są do wszystkich jego plików i podkatalogów - przeciwnie niż uprawnienia NTFS, które można edytować na dowolnym poziomie hierarchii. Dlatego do bardziej szczegółowej kontroli dostępu stosuje się uprawnienia do udziałów wspólnie z uprawnieniami NTFS.

Rys. 3. Centralne zarządzanie wszystkimi udostępnionymi folderami.

Wygodnym narzędziem do zarządzania udostępnionymi folderami jest konsola Zarządzanie serwerem. Po zaznaczeniu pozycji Udziały (lokalne) w folderze Zarządzanie standardowe, zobaczymy listę folderów na serwerze, które zostały udostępnione. Opcja Dodaj folder udostępniony uruchamia kreatora, który tworzy nowy folder, uaktywnia udział i nadaje predefiniowane, standardowe zestawy uprawnień. Cały czas jest też możliwa bezpośrednia edycja zaawansowanych ustawień.

Domyślnym miejscem przechowywania danych użytkowników jest lokalny folder Moje dokumenty. Dobrze by jednak było, żeby dokumenty te były dostępne z każdego komputera, przy którym użytkownik może pracować. Oprócz oczywistego rozwiązania, jakim jest zapisywanie danych na serwerze, można wykorzystać funkcję przekierowania folderu Moje dokumenty do folderu użytkownika na serwerze. W ten sposób z punktu widzenia aplikacji zapisującej dokument folder Moje dokumenty będzie zwykłym folderem lokalnym, a jednocześnie na wszystkich komputerach będzie dostępna jego aktualna wersja. Folder Moje dokumenty domyślnie przekierowywany jest do katalogu macierzystego dostępnego poprzez udział Users, ale można podać dowolną ścieżkę sieciową, niekoniecznie na serwerze.



Rys. 4. Foldery Moje dokumenty możemy przekierować również na dodatkowy serwer, który np. często wykonuje kopię zapasową.

Uprawnienia do plików i folderów

Pełna kontrola - umożliwia wykonywanie operacji wynikających ze wszystkich pozostałych uprawnień, a dodatkowo pozwala usuwać pliki i podkatalogi w danym folderze, zmieniać uprawnienia i przejmować pliki lub foldery na własność.

Modyfikacja - użytkownik może wykonywać wszystkie możliwe operacje oprócz dostępnych jako dodatkowe w przypadku pełnej kontroli, a więc bez usuwania plików i podkatalogów oraz bez zmiany uprawnień i przejmowania na własność.

Odczyt i wykonanie - składa się na nie możliwość wyświetlania zawartości folderu, odczytywanie danych, uprawnień, synchronizowanie, uruchamianie programów i przechodzenie przez folder. To ostatnie uprawnienie specjalne stosuje się wówczas, gdy użytkownik musi przejść przez szereg folderów nadrzędnych, aby dostać się do określonego pliku. Działanie tej funkcji zależy od ustawień zasad grup.

Wyświetlenie zawartości folderu - praktycznie to samo, co Odczyt i wykonanie, ale w odniesieniu do folderów. W przypadku plików nie pojawia się na liście uprawnień.

Odczyt - odczytywanie danych z plików, odczytywanie atrybutów i atrybutów rozszerzonych wykorzystywanych przez aplikacje oraz wyświetlanie zawartości folderów bez możliwości uruchamiania programów.

Zapis - tworzenie plików i folderów, zapis danych i modyfikacja plików, zapis atrybutów i atrybutów rozszerzonych.

Uprawnienia do udziałów sieciowych

Odczyt - domyślne uprawnienie nadawane wszystkim w momencie tworzenia udziału sieciowego. Pozwala przeglądać foldery, odczytywać pliki i uruchamiać programy.

Zmiana - przyznaje użytkownikowi uprawnienia odczytu oraz możliwość tworzenia plików i podkatalogów, zapisywania danych w plikach oraz usuwania plików i podkatalogów.

Pełna kontrola - uprawnienie automatycznie przyznawane użytkownikom z grupy Administratorzy na komputerze lokalnym. Oprócz wykonywania operacji wynikających z uprawnień Odczyt i Zmiana, użytkownik może też zmieniać uprawnienia - oczywiście tylko w przypadku, gdy udostępniony folder znajduje się na partycji NTFS.

Współdzielenie zasobów

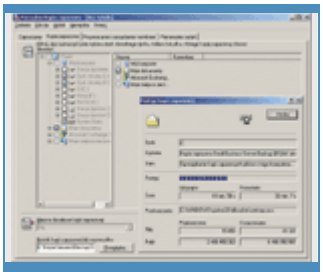
Maciej Zdanowicz
10 maja 2004
PC World Komputer

Dodatkową zaletą wynikającą z przekierowywania folderów Moje dokumenty jest uzyskanie łatwego w obsłudze mechanizmu odzyskiwania dokumentów. We właściwościach folderu oraz jego plików i podkatalogów pojawia się dodatkowa karta Poprzednie wersje, która pozwala użytkownikom powracać do wcześniejszych wersji dokumentów i odzyskiwać usunięte pliki bez angażowania administratora.

Kopie zapasowe

Konfigurację kopii zapasowych powinniśmy przeprowadzić jak najwcześniej po instalacji systemu, gdyż wpływa ona zarówno na bezpieczeństwo danych użytkowników, jak i całego systemu serwera. Skrót do odpowiedniego kreatora znajduje się na Liście zadań do wykonania. Najpierw możemy wybrać rodzaj nośnika wykorzystywanego do przechowywania kopii. Może to być dowolna lokalizacja, np. drugi twardy dysk, ścieżka sieciowa do innego komputera, ale najlepiej, gdyby był to nośnik wymienny, który można przechowywać w bezpiecznym miejscu.

W kolejnych oknach układamy harmonogram kopii: w które dni tygodnia ma być wykonywana i o jakiej porze. Ustalamy też liczbę przechowywanych kopii zapasowych, jak długo będą przechowywane usunięte wiadomości pocztowe (domyślnie 30 dni) oraz ilość miejsca przeznaczoną na tzw. okresowe migawki udostępnionych folderów użytkowników. Ta ostatnia opcja jest szczególnie przydatna, ponieważ uaktywnia odzyskiwanie poprzednich wersji dokumentów oraz usuniętych plików np. z folderu Moje dokumenty, za pomocą wspomnianej wcześniej karty Poprzednie wersje.

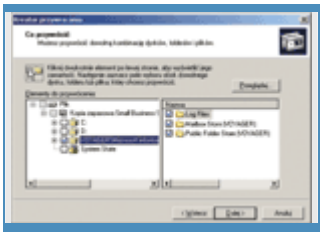


Rys. 5. Kopia zapasowa wykonuje się w tle, w trakcie zwykłej pracy serwera.

Przywracanie systemu

Częste wykonywanie kopii zapasowych pozwala nie tylko odzyskiwać utracone przypadkowo dokumenty, ale może też znacznie zminimalizować straty wynikające z ewentualnej awarii serwera. Informacje o stanie systemu podczas wykonywania ostatniej kopii zapasowej, można wykorzystać do przywrócenia całego systemu.

Przywracanie systemu jest wieloetapową procedurą, ale za to dobrze udokumentowaną. Szczegółowe instrukcje krok po kroku dostępne są w pomocy systemu SBS, a także w Internecie. W razie awarii skorzystamy raczej z tej drugiej możliwości, chociaż procedury odzyskiwania systemu powinny być znane i przetestowane, zanim jeszcze wystąpi awaria.

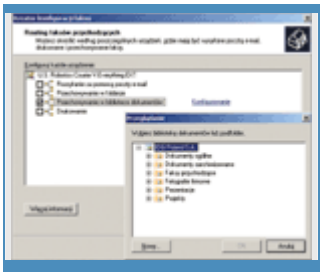


Rys. 6. Możemy przywrócić dowolną kombinację dysków, folderów i plików, z wyjątkiem danych serwera Exchange, które muszą być przywracane w oddzielnej operacji.

Wbudowane w system mechanizmy zabezpieczeń, których najbardziej widoczną konsekwencją jest konieczność aktywacji, mają wpływ również na proces przywracania serwera. Komputer, na który chcemy przywrócić system, powinien być praktycznie nierozróżnialny od komputera, który uległ awarii. W szczególności nowy komputer powinien mieć ten sam chipset i liczbę procesorów oraz podobny układ partycji. Najlepiej mieć w zapasie drugi, identyczny serwer. Problemy te oczywiście nie występują, gdy awarii ulegnie np. twardy dysk. Wtedy wymieniamy go na taki sam lub większy i przywracamy system na tym samym komputerze.

Procedura przywracania systemu precyzyjnie określa, jakie kroki wykonać w szczególnych okolicznościach, np. gdy SBS 2003 był instalowany jako uaktualnienie poprzedniej wersji tego systemu. Przedstawimy zatem jedynie ogólny zarys tego procesu.

Pierwsze dwa etapy przywracania systemu przebiegają dokładnie tak samo, jak instalacja nowego systemu. W pierwszej części uruchamiamy komputer z pierwszej płyty startowej SBS 2003 i pracujemy w tekstowym środowisku instalacyjnym. Zakładamy partycje, formatujemy je w systemie NTFS, czekamy na skopiowanie plików instalacyjnych i po raz pierwszy ponownie uruchamiamy komputer. Druga część instalacji odbywa się już w środowisku graficznym. Tu wprowadzamy typowe informacje, jak nazwa komputera, hasło administratora, ustawienia regionalne, klucz produktu i zwracamy uwagę, aby ustawienia daty i godziny były prawidłowe. Po zakończeniu etapu Finalizowanie instalacji komputer zostanie ponownie uruchomiony. W trakcie ładowania systemu, jeszcze zanim pojawi się ekran logowania, naciskamy [F8], żeby przejść do Menu opcji zaawansowanych. Następnie wybieramy Tryb przywracania usług katalogowych i logujemy się do systemu na konto Administrator.



Rys. 7. Przychodzące faksy możemy automatycznie zapisywać w bibliotece dokumentów portalu firmowego.

Po zalogowaniu, korzystając z narzędzia Zarządzanie dyskami, podłączamy i konfigurujemy pozostałe twarde dyski. Podłączamy też dysk wymienny, na którym zrobiliśmy kopię zapasową, albo wkładamy odpowiednią taśmę do napędu. Jeżeli chcemy odzyskiwać dane przez sieć, sprawdzamy, czy jest dostępny udział sieciowy, na którym przechowujemy kopię. Następnie z menu Start wybieramy Uruchom i wpisujemy ntbackup, żeby uruchomić znane już narzędzie Kopia zapasowa. Za jego pomocą najpierw określamy, jakie elementy systemu i które

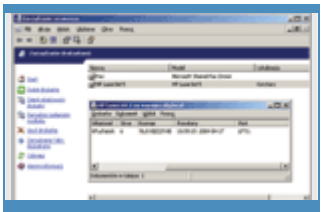
ustawienia powinny zostać przywrócone. Następnie zaznaczamy, że dane powinny zostać zapisane w swojej oryginalnej lokalizacji i rozpoczynamy przywracanie. Na koniec analizujemy raport, żeby sprawdzić, czy wszystkie pliki zostały pomyślnie odzyskane i przeprowadzamy krótki test funkcjonalny serwera - sprawdzamy połączenie internetowe, pocztę elektroniczną, portal firmowy itp.

Faks dla wszystkich

Rys. 8. Kompletny zestaw narzędzi do administrowania urządzeniami, dokumentami i stronami tytułowymi.

Kreator konfiguracji faksu dostępny jest z folderu Faks (lokalny) w narzędziu Zarządzanie serwerem lub z Listy zadań do wykonania. Zanim go użyjemy, musimy mieć poprawnie zainstalowany faks-modem. Przechodzimy do Start | Panel sterowania | Opcje telefonu i modemu, wybieramy kartę Modemy i klikamy Dodaj. Kreator dodawania sprzętu może spróbować sam zidentyfikować modem, ale możemy też mu w tym pomóc, zaznaczając Nie wykrywaj mojego modemu, wybiorę go z listy. W kolejnym oknie klikamy przycisk Z dysku i wpisujemy ścieżkę do folderu ze sterownikiem do naszego modemu.

Konfiguracja faksu za pomocą kreatora to cztery proste etapy. Najpierw wpisujemy dane firmy, które będą wykorzystywane podczas tworzenia strony tytułowej. Później wybieramy urządzenia, które mają być wykorzystywane do wysyłania faksów. Jeżeli zaznaczymy więcej niż jedno, to podczas wysyłania faksu system będzie je po kolei sprawdzał, aż znajdzie urządzenie w danej chwili nieużywane. Kolejne okno służy do wyboru urządzeń odbierających faksy. Najlepiej, gdyby były to inne urządzenia niż wykorzystywane do wysyłania. Wtedy wysyłanie faksu nie zablokuje możliwości ich odbierania. Urządzeń odbierających również może być kilka. Co więcej, każde z nich może zapisywać odebrane faksy w innej lokalizacji. Jeżeli chcemy wykorzystać tę możliwość, zaznaczamy Określ specyficzne miejsca docelowe routingu dla każdego urządzenia. W ostatnim oknie ustalamy wtedy, co dane urządzenie ma zrobić z odebranym faksem. Dostępne możliwości to Rozsyłanie za pomocą poczty e-mail, Przechowywanie w folderze, Przechowywanie w bibliotece dokumentów i Drukowanie. W każdym przypadku kliknięcie odnośnika Konfigurowanie pozwoli odpowiednio: wpisać docelowy adres e-mail, ustalić docelowy folder na dysku, wskazać bibliotekę dokumentów firmowego portalu SharePoint albo wybrać drukarkę.



Rys. 9. Do zarządzania dokumentami służą te same narzędzia, co w systemach desktopowych.

Instalacja udostępnionego faksu na stacji roboczej odbywa się automatycznie podczas podłączania komputera do domeny, w ramach dystrybucji aplikacji do klientów. Po kliknięciu Start | Drukarki i faksy zobaczymy nowe urządzenie, np. Fax na voyager, do którego możemy wysyłać dokumenty tak samo, jak do faksu lokalnego lub drukarki. Dostęp do konsoli faksu uzyskamy, klikając Zobacz, co jest drukowane w Zadaniach drukarki. Od tego momentu wszystkie aplikacje, które potrafią drukować dokumenty, będą mogły wysyłać je również jako faksy.

Wspólne drukarki

Instalację drukarki wykonaliśmy już wcześniej jako jedną z czynności z Listy zadań do wykonania. Drukarkami możemy administrować za pomocą narzędzia Zarządzanie serwerem po wybraniu folderu Drukarki. Zaznaczenie konkretnego urządzenia na liście dostępnych urządzeń (drukarek i faksów), aktywuje dwa dodatkowe skróty kreatora, tj. Zmień właściwości drukarki oraz Zarządzaj zadaniami wydruku. Oba otwierają standardowe okna konfiguracyjne, znane z innych systemów Windows i dostępne np. za pomocą Panelu sterowania. Okno zarządzania zadaniami wydruku oferuje standardowe operacje, tj. wstrzymanie lub wznowienie druku albo usunięcie dokumentu z kolejki. Natomiast okno właściwości zawiera kilka ciekawszych opcji, którymi warto się zainteresować, instalując drukarkę na serwerze, z której będzie korzystało wielu użytkowników. Po pierwsze, na karcie Udostępnianie możemy określić, czy drukarka będzie opublikowana w katalogu Active Directory (domyślnie tak), a po kliknięciu przycisku Dodatkowe sterowniki możemy zainstalować sterowniki do innych systemów operacyjnych niż Windows 2000, Windows XP czy Windows

Server 2003. Użytkownicy tych systemów, instalując drukarki sieciowe, będą mogli wtedy ściągnąć odpowiednie sterowniki wprost z serwera.

Współdzielenie zasobów

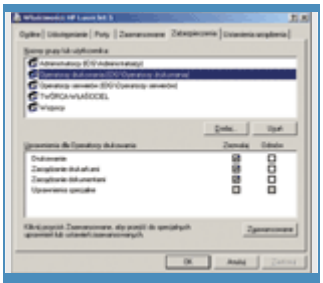
Maciej Zdanowicz
10 maja 2004
PC World Komputer

(Strona 3 z 3)

Druga istotna karta to Zabezpieczenia. Podobnie jak w przypadku folderów, pozwala ustawić uprawnienia związane z drukarkami. Zestaw dostępnych uprawnień jest nieco skromniejszy i zawiera Drukowanie, Zarządzanie dokumentami i Zarządzanie drukarkami. Uprawnienia mogą być przypisywane użytkownikom i grupom, ale jeśli dany użytkownik należy do kilku grup o różnych uprawnieniach, to uprawnienia efektywne są ustalane odmiennie niż w przypadku folderów - wybierana jest kombinacja najmniej restrykcyjna. Jedynie zaznaczenie pola Odmów określonego uprawnienia ma pierwszeństwo przed uprawnieniami wynikającymi z uprawnień efektywnych.

Domyślne uprawnienia, które pozwalają wszystkim użytkownikom drukować, a niektórym grupom również zarządzać drukarką lub dokumentami, są nadawane automatycznie podczas instalowania drukarki.

Dane na odległość



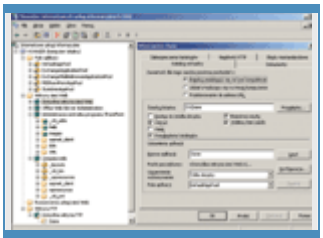
Rys. 10. Dostęp do drukarek jest przyznawany na podstawie oddzielnego zestawu uprawnień.

Wymiana danych w obrębie sieci lokalnej to jedna sprawa, ale czasami trzeba też udostępnić coś na zewnątrz. Jednym z rozwiązań może być uruchomienie serwera FTP. Nie jest on domyślnie instalowany razem z systemem SBS, więc musimy go dodać ręcznie. W tym celu, przechodzimy do menu Start, wybieramy Panel sterowania | Dodaj lub usuń programy, a następnie Dodaj/Usuń składniki systemu Windows. Na liście składników zaznaczamy Serwer aplikacji i klikamy Szczegóły, znajdujemy pozycję Internetowe usługi informacyjne (IIS) i ponownie klikamy Szczegóły. Następnie zaznaczamy pole wyboru przy składniku Usługa FTP (File Transfer Protocol) i klikamy OK. Po zamknięciu dwóch kolejnych okien klikamy Dalej, żeby zaakceptować wprowadzone zmiany. Kreator rozpocznie zapisywanie nowej konfiguracji i poprosi o włożenie pierwszej płyty systemu SBS 2003. Po zakończeniu pracy kreatora uruchomiona zostanie domyślna witryna FTP.

Do konfiguracji witryn WWW i FTP służy Menedżer internetowych usług informacyjnych (IIS). Odpowiedni skrót znajdziemy w Narzędziach administracyjnych. Na liście po lewej stronie znajdziemy następujące pozycje: Pule aplikacji, Witryny sieci Web, Rozszerzenia usługi sieci Web oraz właśnie zainstalowaną - Witryny FTP. Pierwsza służy do definiowania specjalnych kontenerów, w których działają poszczególne serwisy internetowe. Używanie oddzielnych kontenerów np. dla różnych witryn pozwala je skutecznie od siebie odizolować, zapobiegając sytuacji, w której jedna źle działająca witryna zawiesza cały serwer WWW. Folder Witryny sieci Web grupuje wszystkie serwisy WWW, m.in. domyślną witrynę serwera SBS, którą wykorzystujemy, podłączając komputery klienckie do domeny albo łącząc się zdalnie z serwerem. Znajdziemy tu też witrynę obsługującą firmowy portal SharePoint, a także całkiem oddzielną witrynę do zarządzania tym portalem. Folder Rozszerzenia usługi sieci Web służy do konfigurowania rozszerzeń, takich jak strony ASP, dostęp do danych przez ASP.NET, usługi SharePoint czy dostęp do serwera Exchange. Od zdefiniowanych tu ustawień zależy z jednej strony bezpieczeństwo serwera, a z drugiej możliwość używania nowoczesnych technologii, wykorzystywanych do budowy dynamicznych interaktywnych witryn internetowych.

W folderze Witryny FTP znajdziemy natomiast interesującą nas Domyślną witrynę FTP. W standardowej konfiguracji jest ona włączona i wskazuje na katalog \inetpub\

ftproot na dysku systemowym. Aby udostępnić dane poprzez serwer FTP, możemy albo wykorzystać tę domyślną lokalizację albo udostępnić dowolny inny folder, wybierając z menu kontekstowego Domyślnej witryny FTP opcję Nowy | Katalog wirtualny. W pierwszym oknie kreatora podajemy nazwę katalogu wirtualnego, czyli tę, poprzez którą do folderu będą się odwoływali użytkownicy. Następnie określamy ścieżkę do rzeczywistego folderu na dysku i ustawiamy uprawnienia (Odczyt i/lub Zapis). Od tej pory użytkownicy mają dostęp do wskazanego folderu za pomocą klienta FTP.



Rys. 11. Zarządzanie witrynami WWW i FTP w menedżerze IIS.

Druga oprócz FTP możliwość udostępnienia folderu w Internecie to wykorzystanie witryny WWW, a więc protokołu HTTP, który często okazuje się szybszy niż FTP. Aby udostępnić w ten sposób folder, wystarczy w Eksploratorze Windows wyświetlić jego właściwości i wybrać kartę Udostępnianie w sieci Web. W polu Udostępnij na wybieramy witrynę, przez którą folder ma być dostępny - np. Domyślną witrynę sieci Web. Po zaznaczeniu opcji Udostępnij ten folder pojawi się okno Edytowanie aliasu. W pole Alias wpisujemy nazwę katalogu wirtualnego, przez który użytkownicy będą się odwoływali do udostępnianego folderu, podobnie jak w przypadku witryny FTP. W Uprawnieniach dostępu musimy jeszcze zaznaczyć Przeglądanie katalogów i gotowe. Od tej pory użytkownicy mają dostęp do folderu również za pomocą przeglądarki WWW.

W obu przypadkach, jeżeli chcemy udostępniać dane poza firmę, musimy odpowiednio skonfigurować zaporę internetową. W przypadku witryny FTP można w tym celu użyć Kreatora konfigurowania poczty e-mail i połączenia internetowego, który uruchamiamy, klikając Połącz z Internetem w folderze Internet i poczta e-mail narzędzia Zarządzanie serwerem lub na Liście zadań do wykonania. W pierwszym oknie wybieramy Nie zmieniaj typu połączenia, a w drugim Włącz zaporę i zaznaczamy pole przy pozycji FTP. We wszystkich kolejnych oknach zatwierdzamy domyślne ustawienia, a w ostatnim klikamy Zakończ, żeby zaakceptować zmiany.

Rys. 12. Dostęp do tego samego folderu za pomocą dwóch witryn i dwóch protokołów transmisji danych (HTTP i FTP).

Jeżeli jako zaporę wykorzystujemy serwer ISA 2000, używanie kreatora spowoduje wyłączenie niestandardowych filtrów pakietów. Zatem jeżeli zdefiniowaliśmy własne filtry, będziemy musieli je ponownie aktywować za pomocą narzędzia ISA Management po zakończeniu pracy kreatora.

Dodatkowa konfiguracja serwera ISA konieczna jest również w przypadku udostępniania folderów poprzez witrynę WWW. Jeżeli utworzyliśmy katalog wirtualny o nazwie np. Dane, musimy go opublikować, żeby serwer ISA umożliwiał dostęp do tego katalogu użytkownikom zewnętrznym. W narzędziu ISA Management wybieramy Ser-vers and Arrays, następnie nazwę naszego serwera ISA (voyager) i w folderze Policy Elements wybieramy Destination Sets. Klikamy Create a Destination Set i w pole Name wpisujemy np. Folder Dane. Następnie klikamy Add i w kolejnym oknie wypełniamy dwa pola. Jako Destination wpisujemy zewnętrzny adres serwera - np. voyager.idg.pl, a w pole Path wpisujemy /Dane/*, co spowoduje, że dostępne będą wszystkie pliki w folderze.

Sam Destination Set definiuje tylko zakres adresów, które serwer ISA będzie obserwować. Musimy go jeszcze poinstruować, co ma zrobić, gdy takie zgłoszenie otrzyma. W folderze Publishing wybieramy więc Web Publishing Rules, a następnie Create a Web Publishing Rule. Wpisujemy nazwę, np. Dostęp do folderu Dane, a w kolejnym oknie wybieramy Specified destination set i podajemy nazwę zdefiniowanego wcześniej zakresu - w naszym przypadku wybieramy Folder Dane. W oknie Client Type zaznaczamy Any request, a w Rule Action zaznaczamy Redirect the request to this internal Web server (name or IP address) i wpisujemy publishing.idg.pl (jest to adres domyślnie przypisywany wewnętrznemu serwerowi WWW podczas instalacji serwera ISA). Zaznaczamy też Send the original host header to the publishing service instead of the actual one (specified above) i klikamy Dalej oraz Zakończ. Po tych zabiegach serwer ISA nie będzie już blokował dostępu do folderu udostępnionego poprzez witrynę WWW.

Usprawnienia do drukarek

Drukowanie - użytkownicy mający to uprawnienie mogą wysyłać dokumenty do drukarki. Domyślnie otrzymują je użytkownicy grupy Wszyscy.

Zarządzanie dokumentami - pozwala wstrzymywać i wznawiać drukowanie, usuwać z kolejki dokumenty lub zmieniać ich kolejność. Dotyczy to dokumentów wszystkich użytkowników. Nadanie uprawnienia konkretnemu użytkownikowi pozwala mu zarządzać wszystkimi nowymi dokumentami, które zostały wysłane do drukarki od momentu zatwierdzenia nowych uprawnień. Dokumenty, które zostały wcześniej wysłane do kolejki, nie będą dla niego dostępne.

Zarządzanie drukarkami - użytkownik ma wszystkie uprawnienia wynikające z zaznaczenia opcji Drukowanie, ale może też w pełni administrować drukarką. Do jego zadań należy zatem udostępnianie drukarki, przyznawanie uprawnień, zatrzymywanie, uruchamianie oraz zmiana właściwości drukarki. Domyślnie otrzymują to prawo użytkownicy należący do grup Administratorzy i Użytkownicy zaawansowani, którzy oprócz tego dysponują również pozostałymi uprawnieniami, a więc mają pełny dostęp do drukarki.

Poczta firmowa i internetowa

Maciej Zdanowicz
10 maja 2004
PC World Komputer
Może się wydawać, że małe firmy ze skromną infrastrukturą sieciową nie potrzebują własnego serwera pocztowego. Wydaje się tak jednak do czasu poznania korzyści płynących z wprowadzenia sprawnego wewnętrznego obiegu informacji.

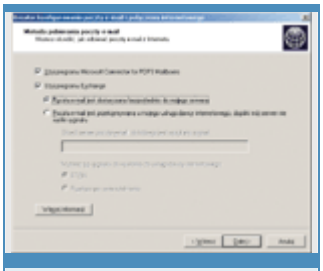
Wewnętrzny serwer pocztowy to nie tylko szybsza wymiana danych wewnątrz firmy. To także zwiększona poufność informacji, ponieważ dokumenty wewnętrzne nie opuszczają ani na chwilę sieci lokalnej. Wszystkie skrzynki pocztowe w jednym miejscu, centralnie zarządzane, wspólnie chronione przed atakami z Internetu i automatycznie archiwizowane, to z kolei bezpieczeństwo informacji. Wewnętrzny obieg poczty elektronicznej może też być bardziej elastyczny, bo daje się dostosować do wymogów przedsiębiorstwa. W sieci lokalnej można ustalić własne ograniczenia wielkości wiadomości lub zastosować specyficzne zasady filtrowania załączników.

Konfiguracja serwera pocztowego

Serwer Exchange 2003, który realizuje wszystkie zadania związane z pocztą elektroniczną, jest automatycznie instalowany razem z pozostałymi aplikacjami pakietu SBS. Wtedy też sam system operacyjny jest konfigurowany i przygotowywany do współpracy z serwerem pocztowym. Jedna z głównych zmian to rozszerzenie schematu Active Directory o elementy związane z funkcjonowaniem poczty elektronicznej.

Kreator konfigurowania poczty

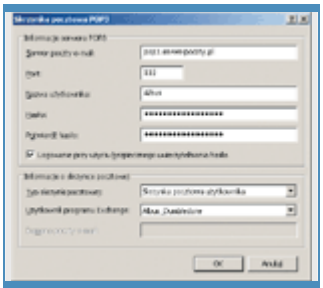
Konfigurację systemu pocztowego, która polega na dostosowaniu serwera do wymagań firmy, wykonujemy już sami. Zadanie to możemy rozpocząć, otwierając znaną już Listę zadań do wykonania. Skrót Połącz z Internetem, którego wcześniej używaliśmy na przykład do konfiguracji połączenia internetowego i ustawiania parametrów zapory, teraz wykorzystamy do skonfigurowania poczty elektronicznej.



Rys. 1. Poczta jest dostarczana bezpośrednio do naszego serwera, do serwera internetowego dostawcy lub do wielu różnych skrzynek na różnych serwerach.

Ponieważ połączenie z Internetem już działa poprawnie, w pierwszym oknie wybieramy Nie zmieniaj typu połączenia. Natomiast nad wyborem odpowiedniej opcji w oknie Zapora, trzeba się już chwilę zastanowić. Jeśli poprzednio skonfigurowaliśmy zaporę do przepuszczania poczty elektronicznej, a więc otworzyliśmy port 25 dla protokołu SMTP, to powinniśmy wybrać Nie zmieniaj konfiguracji zapory. W przeciwnym razie po wybraniu Włącz zaporę trzeba zaznaczyć pole wyboru opcji E-mail. Ponownego konfigurowania zapory, gdy odpowiednie porty są już otwarte, należy unikać, jeśli wykorzystuje się serwer ISA. Użycie kreatora do konfiguracji zapory spowoduje wyłączenie niestandardowych opcji konfiguracyjnych, w szczególności niestandardowych filtrów pakietów, które trzeba będzie później ręcznie aktywować.

Przekazywanie poczty



Rys. 2. Pobieranie poczty z serwerów internetowych za pomocą Łącznika

POP3.

Certyfikat serwera również ustawiliśmy wcześniej, więc przechodzimy do kolejnego okna, w którym zaznaczamy Włącz internetową pocztę e-mail i klikamy Dalej. W oknie Metoda dostarczania poczty e-mail możemy wybrać Użyj DNS do rozsyłania poczty e-mail lub Prześlij dalej wszystkie wiadomości e-mail do serwera poczty e-mail u usługodawcy internetowego. Zaznaczenie pierwszej opcji spowoduje, że nasz serwer będzie próbował nawiązywać bezpośrednie połączenie z serwerem pocztowym właściwym dla odbiorcy każdej wysyłanej wiadomości. W drugim przypadku serwer prześle całą pocztę do wskazanego serwera w Internecie i on dopiero zajmie się rozsyłaniem poczty do konkretnych odbiorców. Wybór odpowiedniej opcji może zależeć od wymagań dostawcy usług internetowych.

Wykorzystywanie dodatkowego serwera do przekazywania poczty wymaga, oczywiście, wykupienia odpowiedniej usługi u dostawcy usług internetowych i odpowiedniej konfiguracji tego serwera, który musi w tym przypadku zezwalać na przekazywanie poczty e-mail.

Poprawnie skonfigurowane serwery pocztowe domyślnie odmawiają nieznanym nadawcom przekazywania poczty. W innym razie niepowołane osoby mogłyby je wykorzystać do rozsyłania niebezpiecznej poczty elektronicznej, np. spamu. Serwer taki szybko trafiłby na czarną listę komputerów, od których pozostałe serwery w ogóle nie odbierają poczty. W konsekwencji nie mógłby już wysyłać nawet zwykłej poczty elektronicznej i stałby się bezużyteczny. Dlatego bardzo istotne jest nadanie tylko wybranym użytkownikom uprawnień do wykorzystywania serwera do przekazywania poczty i kontrolowanie, czy taki użytkownik rzeczywiście jest tym, za kogo się podaje.

Wypełniając pole Serwer poczty e-mail, w kreatorze możemy podać kilka adresów serwerów przekazujących, jeżeli dostawca usług internetowych oferuje taką możliwość.

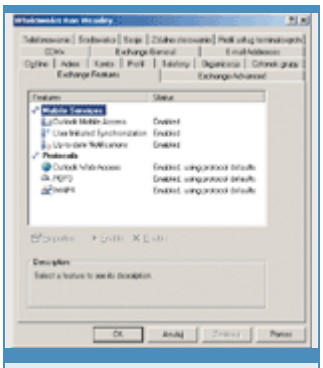
Rekordy MX w DNS

Rys. 3. Użytkownik może mieć wiele adresów pocztowych różnych typów.

Konfigurując nasz serwer pocztowy, wybierzemy pierwszą opcję, czyli Użyj DNS do rozsyłania poczty e-mail, jako bardziej niezależną od dostawcy i dającą pełną kontrolę nad przesyłaniem poczty elektronicznej.

Wykorzystanie systemu DNS do rozsyłania poczty polega na wyszukiwaniu serwerów pocztowych obsługujących daną domenę. Zanim serwer wyśle wiadomość, musi poznać adres serwera pocztowego odbiorcy. Najpierw zidentyfikuje więc domenę internetową odbiorcy, a następnie wyśle zapytanie DNS o tzw. rekord MX dla tej domeny. Rekordy MX (od Mail Exchanger) określają, jakie serwery odbierają pocztę dla wszystkich użytkowników w danej domenie. Jeżeli rekordów MX jest kilka, serwer po kolei próbuje wysłać wiadomości do kolejnych serwerów. Najczęściej stosuje się dwa rekordy MX, jeden dla podstawowego serwera pocztowego oraz drugi dla serwera zapasowego, który odbiera pocztę wtedy, gdy pierwszy jest niedostępny.

Poczta przychodząca



Rys. 4. Uaktywnione usługi i metody dostępu do poczty.

W kolejnym oknie określamy metodę pobierania poczty z Internetu. Opcję Użyj programu Microsoft Connector for POP3 Mailboxes powinniśmy zaznaczyć, jeśli chcemy wykorzystywać indywidualne skrzynki pocztowe użytkowników utrzymywane na serwerach internetowych. Exchange będzie za pomocą wspomnianego łącznika POP3 co jakiś czas sprawdzał, czy w skrzynkach są nowe wiadomości, a jeśli tak, to będzie je ściągał i zapisywał w lokalnej skrzynce pocztowej użytkownika.

Opcja Użyj programu Exchange zakłada, że nasz serwer jest podłączony na stałe do Internetu albo regularnie łączy się z siecią, np. za pomocą modemu. Jeżeli dysponujemy stałym łączem, wybieramy Poczta e-mail jest dostarczana bezpośrednio do mojego serwera i przechodzimy do kolejnego okna.

Odbieranie wiadomości

Jeżeli jednak nasz serwer tylko okazjonalnie podłącza się do Internetu, to do odbierania poczty musimy wykorzystywać serwer pocztowy dostawcy, który jest stale dostępny w sieci. Musimy też poinstruować Exchange, w jaki sposób ma odbierać pocztę od tego serwera. Jeśli wybierzemy opcję Poczta e-mail jest przetrzymywana u mojego dostawcy internetowego, dopóki mój serwer nie wyśle sygnału, w oknie uaktywnione zostaną dodatkowe pola, w których wpisujemy adres serwera pocztowego dostawcy i wybieramy rodzaj sygnału, który serwer Exchange będzie wysyłał do serwera dostawcy, aby zasygnalizować swoją obecność w sieci oraz gotowość do odebrania nowych wiadomości.

Poczta firmowa i internetowa

Maciej Zdanowicz
10 maja 2004
PC World Komputer

Do wyboru mamy sygnały ETRN i TURN. Sygnał ETRN jest bardziej popularny, ale zwykle wymaga, aby nasz serwer pocztowy miał przypisywany statyczny adres IP, co w przypadku połączeń modemowych jest raczej rzadko stosowane. Natomiast sygnał TURN umożliwia korzystanie z dynamicznego adresu IP, ale najczęściej wymaga wcześniejszego uwierzytelnienia. Jeżeli wybierzemy sygnał TURN, zaznaczając opcję Przełącz po uwierzytelnieniu (dość niefortunnie przetłumaczone Turn after authentication), to w kolejnym oknie będziemy musieli wpisać nazwę użytkownika i hasło wykorzystywane do uwierzytelnienia u dostawcy usług internetowych.

W oknie Nazwa domeny poczty e-mail wpisujemy zarejestrowaną w Internecie nazwę zewnętrznej domeny, czyli np. idg.pl. Domena ta musi mieć zdefiniowany przynajmniej jeden rekord MX wskazujący na nasz publiczny adres IP, czyli przypisany do zewnętrznej karty sieciowej naszego serwera.

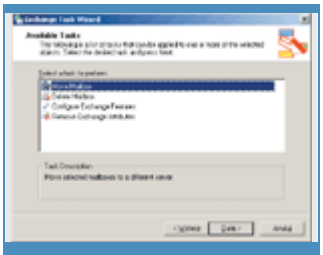
Skrzynki pocztowe POP3

Jeżeli wcześniej zaznaczyliśmy, że będziemy korzystali z łącznika POP3, to teraz mamy szansę skonfigurować odpowiednie konta pocztowe. Klikamy Dodaj i wpisujemy informacje wymagane do połączenia z serwerem POP3 (adres serwera, login i hasło). Natomiast wybory dokonywane w grupie ustawień Informacje o skrzynce pocztowej, zależą od rodzaju internetowej skrzynki pocztowej u dostawcy.

Jeżeli każdy użytkownik, którego wiadomości chcemy odbierać z jego skrzynki internetowej, ma oddzielne konto u dostawcy, to w polu Typ skrzynki pocztowej wybierzemy Skrzynka pocztowa użytkownika, a następnie w polu Użytkownik programu Exchange wskażemy użytkownika lub grupę dystrybucyjną, do której mają trafić odebrane wiadomości.

Dystrybucja poczty

Druga możliwość to wykorzystywanie jednej wspólnej skrzynki pocztowej na serwerze dostawcy dla wszystkich użytkowników. W takiej konfiguracji skrzynka skojarzona jest z adresem pocztowym domeny (np. idg.poczta.pl), a nie konkretnego użytkownika w tej domenie (puchatek@idg.poczta.pl). Wszystkie listy przychodzące pod dowolne adresy pocztowe z tej domeny zapisywane są w tej samej skrzynce pocztowej. Serwer pocztowy Exchange może okresowo pobierać całą zawartość takiej skrzynki, a następnie, analizując poszczególne wiadomości, odczytywać z nich adresy odbiorców i kierować do odpowiednich lokalnych skrzynek pocztowych.



Rys. 5. Zadania serwera pocztowego związane z obiektem użytkownika.

Aby taki mechanizm działał bez żadnych dodatkowych zabiegów, nazwy użytkowników stosowane jako internetowe adresy pocztowe muszą być takie same, jak nazwy

użytkowników skrzynek lokalnych. W przeciwnym razie trzeba zdefiniować dodatkowe reguły routingu, według których będą tłumaczone nazwy użytkowników.

Reguły routingu dla kont POP3

Reguły routingu można zdefiniować dopiero po zakończeniu pracy kreatora, za pomocą narzędzia Zarządzanie serwerem. W folderze Zarządzanie zaawansowane zaznaczamy pozycję Menedżer łącznika POP3 i wybieramy Otwórz Menedżer łącznika POP3. Wybieramy pozycję z listy skrzynek pocztowych POP3 i klikamy Edytuj. W okienku do edycji danych konta, klikamy przycisk Reguły routingu, a następnie wielokrotnie klikając Dodaj, wpisujemy kolejne pary składające się z internetowego adresu pocztowego oraz nazwy użytkownika lokalnej skrzynki pocztowej.

Filtrowanie załączników

Wracamy do Kreatora konfiguracji poczty e-mail i połączenia internetowego. Ostatnie dwa etapy to ustalenie częstotliwości pobierania wiadomości z internetowego serwera pocztowego oraz zmodyfikowanie bądź zaakceptowanie proponowanej listy rozszerzeń załączników, które serwer Exchange będzie usuwał z wiadomości pocztowych. Jeżeli dodatkowo zaznaczymy opcję Zapisz usunięte załączniki wiadomości e-mail w folderze i wskażemy na dysku folder, będziemy mogli odzyskiwać wartościowe załączniki usunięte przez zbyt restrykcyjny filtr.

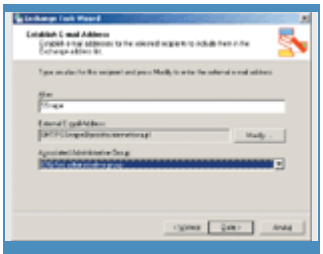
Na tym kończy się podstawowa konfiguracja serwera Exchange, który jest już gotowy do pracy. Skrzynki pocztowe dla użytkowników zostały pozakładane już podczas dodawania nowych kont do systemu, a klient poczty Microsoft Outlook 2003 został skonfigurowany do pracy z serwerem Exchange przy okazji podłączania komputerów do domeny, w ramach automatycznej dystrybucji aplikacji i konfiguracji stacji roboczych. Cały system działa jednak według standardowych ustawień domyślnych. W różnych środowiskach sieciowych i w różnych zastosowaniach może wymagać dalszego dopasowania. Dlatego warto wiedzieć, gdzie szukać poszczególnych opcji konfiguracyjnych i narzędzi do administrowania serwerem.

Konto użytkownika

W związku z obecnością w systemie serwera pocztowego Exchange i rozszerzeniem schematu Active Directory z obiektem użytkownik związanych jest wiele dodatkowych parametrów. Ustawiamy je na dodatkowych kartach właściwości konta. W narzędziu Zarządzanie serwerem przechodzimy do folderu Użytkownicy, zaznaczamy użytkownika na liście i klikamy Zmień właściwości użytkownika. Wśród kilkunastu widocznych kart cztery mają bezpośredni związek z serwerem pocztowym. Są to E-mail Addresses, Exchange General, Exchange Features i Exchange Advanced.

Adresy pocztowe

Karta E-mail Addresses przechowuje przypisane do użytkownika adresy pocztowe i domyślnie zawiera trzy pozycje: lokalny adres pocztowy wykorzystywany podczas przesyłania wiadomości wewnątrz firmy (np. RWeasley@idg.local), internetowy adres pocztowy (np. RWeasley @idg.pl) oraz adres zgodny ze standardem X.400, który oprócz samego adresu pocztowego może zawierać wiele dodatkowych informacji o użytkowniku. Jeden użytkownik może mieć wiele adresów tego samego typu lub różnych typów. Domyślnie ma np. dwa wspomniane adresy SMTP, ale tylko jeden z nich jest adresem głównym. Adresy główne wyświetlane są pogrubioną czcionką. Trzeci adres jest jedynym adresem typu X.400, więc jest jednocześnie adresem głównym X.400 i również jest wyświetlany pogrubioną czcionką.



Rys. 6. Użytkownik może nie mieć lokalnej skrzynki, lecz przypisany adres zewnętrzny.

Za pomocą przycisków New, Edit, Remove, Set As Primary możemy modyfikować adresy, jednak niektóre zmiany mogą zostać pominięte, jeśli zaznaczone jest pole Automatically update e-mail addresses based on recipient policy. W szczególności dotyczy to ustawienia innego adresu głównego niż domyślny. Również usuwanie standardowych adresów niewiele da. Standardowy zestaw zasad serwera Exchange określa, jakie adresy mają być automatycznie tworzone dla użytkownika i które z nich są domyślne. Jeżeli jednak musimy zmienić ten

porządek, to albo wyłączamy opcję automatycznej aktualizacji adresów pocztowych, albo uruchamiamy Exchange System Manager i zmieniamy domyślny zestaw zasad serwera Exchange.

Skrzynka użytkownika

Karta Exchange General służy do modyfikowania parametrów skrzynki pocztowej. W polu Mailbox store zapisana jest lokalizacja skrzynki pocztowej, natomiast pole Alias przechowuje nazwę użytkownika wykorzystywaną do utworzenia adresu pocztowego, która może, oczywiście, być różna od nazwy logowania. Zmiana tej nazwy spowoduje dodanie dwóch nowych adresów SMTP (lokalnego i internetowego) do listy na karcie E-mail Addresses, oraz ustawienie nowego adresu internetowego jako głównego adresu użytkownika.

Za pomocą Delivery Restrictions ustawimy maksymalne rozmiary wysyłanych i odbieranych wiadomości, a także zdefiniujemy grupę nadawców, od których zgadzamy się otrzymywać pocztę. Mogą to być wszyscy, tylko użytkownicy uwierzytelnieni, wybrana grupa lub wszyscy z wyjątkiem wskazanych adresów.

Poczta firmowa i internetowa

Maciej Zdanowicz
10 maja 2004
PC World Komputer

Po kliknięciu przycisku Delivery Options możemy ustawić kilka naprawdę ciekawych parametrów - przede wszystkim wyznaczyć sobie współpracowników, którzy za nas będą wysyłali wiadomości pocztowe. Ponieważ wiadomości są wysyłane w naszym imieniu, odbiorca pomyśli, że sami je wysłaliśmy. Druga opcja to automatyczne przekazywanie wiadomości do dodatkowego odbiorcy. Wskazując w polu Forward to nazwę użytkownika lub grupy oraz zaznaczając Deliver messages to both forwarding address and mailbox, możemy sprawić, aby wszyscy zainteresowani zawsze byli na bieżąco z naszą - wtedy już publiczną - korespondencją. Ostatni parametr to Recipient limit, czyli maksymalna liczba odbiorców naszej wiadomości. Pozostawienie domyślnie zaznaczonej opcji Use default limit sprawi, że obowiązującym limitem będzie wartość zdefiniowana w narzędziu Exchange System Manager na karcie Defaults we właściwościach Global Settings | Message Delivery.

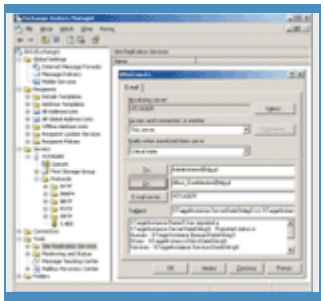
Dostęp do skrzynki

Karta Exchange Features grupuje dostępne dla użytkownika usługi i metody dostępu do skrzynki pocztowej. Opcje zgromadzone w Mobile Services sterują dostępem do serwera Exchange z urządzeń bezprzewodowych, takich jak telefony czy palmtopy. Jeżeli włączymy (Enable) usługę Outlook Mobile Access, użytkownicy będą mogli przeglądać zawartość skrzynki pocztowej na serwerze. Natomiast opcje User initiated Synchronization oraz Up-to-date Notifications umożliwią synchronizację danych w urządzeniu przenośnym z zawartością skrzynki na serwerze oraz zapewnią, że będą one zawsze aktualne.

W grupie Protocols określamy metody zdalnego dostępu do serwera. Włączona usługa Outlook Web Access umożliwi przeglądanie poczty za pomocą przeglądarki, natomiast dwie kolejne POP3 i IMAP4 uaktywnią te protokoły dostępu dla programów pocztowych.

Ustawienia zaawansowane

Exchange Advanced to grupa rzadziej stosowanych parametrów. Pole Simple Display Name pozwala zdefiniować specjalną uproszczoną nazwę użytkownika dla systemów, które nie potrafią zinterpretować wszystkich znaków w zwykłej nazwie użytkownika. Parametr Hide from Exchange address lists pozwala usunąć nazwę użytkownika ze wszystkich list adresowych serwera Exchange. Dzięki temu na serwerze mogą być utrzymywane skrzynki dla dodatkowych użytkowników, np. zewnętrznych, których dane nie muszą lub nie powinny być rozgłaszane w firmie. Opcja Downgrade high priority mail bound for X.400 służy do zachowania zgodności ze standardem w przypadku stosowania adresów X.400.

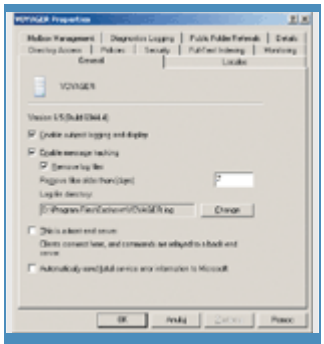


Rys. 7. Powiadamianie pocztą elektroniczną o awarii monitorowanych komponentów serwera.

Na karcie ustawień zaawansowanych możemy też zmienić uprawnienia do skrzynki pocztowej (Mailbox Rights) przypisane poszczególnym użytkownikom lub grupom, takim jak np. Administratorzy domeny czy SBS Mail Operators. Przycisk Custom Attributes pozwala przypisać do konta użytkownika własne dodatkowe informacje, co może okazać się przydatne, jeśli w firmie stosowany jest własny system identyfikacji pracowników. Po kliknięciu ILS Settings możemy podać nazwę serwera oraz konto użytkownika, który korzysta z systemu ILS (Internet Locator Service), pozwalającego wyszukiwać użytkowników podłączonych aktualnie do sieci.

Zadania serwera Exchange

Aby uzyskać dostęp do listy użytkowników systemu SBS najczęściej uruchamiamy narzędzie Zarządzanie serwerem i w folderze Zarządzanie standardowe klikamy Użytkownicy. Jeżeli zaznaczymy konkretną pozycję na liście, to w menu Akcja oraz menu kontekstowym (uruchamianym myszą) pojawią się zadania, które można wykonać na tym obiekcie. Jednak ponieważ folder Użytkownicy służy do uproszczonego zarządzania użytkownikami, lista dostępnych operacji została ograniczona do podstawowych zadań, przewidzianych do wykonywania za pomocą łatwych w obsłudze kreatorów.



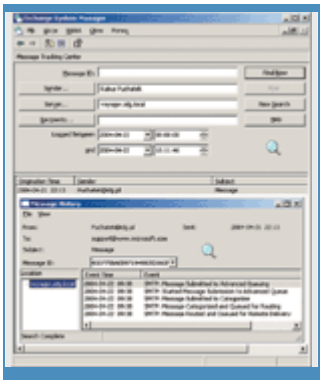
Rys. 8. Chcąc śledzić wiadomości, musimy włączyć zapisywanie dodatkowych informacji do pliku dziennika.

Aby uzyskać dostęp do dodatkowych zadań, musimy zlokalizować ten sam obiekt użytkownika w katalogu Active Directory. W folderze Zarządzanie zaawansowane wybieramy Użytkownicy i komputery usługi Active Directory, a następnie w naszej domenie wewnętrznej idg.local otwieramy kolejno MyBusiness | Users | SBSUsers. SBSUsers jest jednostką organizacyjną, w której domyślnie zakładane są konta użytkowników tworzone za pomocą Kreatora dodawania użytkownika. Na liście w prawym oknie zobaczymy listę użytkowników SBS i szablonów użytkownika. Po zaznaczeniu obiektu w menu Akcja (lub menu kontekstowym) pojawi się rozszerzona lista zadań, m.in. pozycja Exchange Tasks.

Wybranie Exchange Tasks uruchamia kreatora. Dla użytkownika, który ma skrzynkę pocztową Exchange Task Wizard, wyświetli opcje Move Mailbox, Delete Mailbox, Configure Exchange Features oraz Remove Exchange Attributes. Pierwsza służy do przenoszenia skrzynek pocztowych na inne serwery, druga co prawda usuwa skrzynkę, ale pozostawia możliwość jej odzyskania za pomocą specjalnych narzędzi serwera, trzecia otwiera to samo okno konfigurujące usługi oraz metody dostępu, które pojawia się jako jedna z kart właściwości użytkownika, natomiast czwarta usuwa z obiektu użytkownika wszystkie ustawienia związane z pocztą elektroniczną. Użytkownik przestaje pojawiać się na listach adresowych i oczywiście nie ma dostępu do poczty. Opcji nie należy używać, jeśli uruchomione są usługi oparte na Active Directory, zakładające dostępność tych informacji.

Jeżeli uruchomimy kreatora Exchange Task Wizard dla użytkownika, który nie ma skrzynki pocztowej, pojawią się opcje umożliwiające jej utworzenie (Create Mailbox) albo przynajmniej wprowadzenie zewnętrznego adresu pocztowego (Establish E-mail Address) związanego ze skrzynką przechowywaną na jednym z serwerów internetowych.

Zarządzanie serwerem Exchange



Rys. 9. Co się stało z wiadomością po wysłaniu?

Do zarządzania serwerem pocztowym Exchange możemy wykorzystać program System Manager albo posługiwać się standardowym narzędziem Zarządzanie serwerem. Oba otwierają konsolę administracyjną MMC, ale System Manager ogranicza zakres dostępnych folderów i opcji administracyjnych do związanych bezpośrednio z serwerem Exchange. Jeśli zlokalizujemy więc skrzynkę danego użytkownika jako element tzw. Mailbox Store w strukturze serwera Exchange i uruchomimy dla tego obiektu Exchange Task Wizard, to w dostępnych zadaniach nie zobaczymy Remove Exchange Attributes, ponieważ nie będziemy zarządzać w tym momencie bazą Active Directory, lecz tylko serwerem Exchange.

Jeżeli chcemy korzystać z narzędzia Zarządzanie serwerem, to opcje konfiguracyjne znajdziemy w Zarządzanie zaawansowane. Dostępny tam folder Pierwsza organizacja (Exchange) po kliknięciu ujawni zestaw podfolderów i zmieni nazwę na rzeczywistą nazwę organizacji, np. IDG (Exchange). Natomiast program System Manager uruchamiamy, wybierając Start | Programy | Microsoft Exchange | System Manager.

Zasady serwera pocztowego

Bezpośrednio pod IDG (Exchange) zgrupowanych jest sześć folderów. Ustawienia dotyczące wiadomości pocztowych i usług przechowywane są w pierwszym, Global Settings. We właściwościach Internet Message Formats możemy zdefiniować przypisania typów MIME do rozszerzeń plików. Typy MIME wykorzystywane są podczas wysyłania poczty z klientów MAPI (takich jak np. Outlook) do klientów internetowych. Jeżeli wysyłany list ma załączniki, to zostaną one przetworzone na postać tekstową i dołączone do wiadomości. Jednocześnie na podstawie rozszerzeń dołączonych plików w wiadomości zapisane zostaną odpowiadające im identyfikatory typów MIME. W ten sposób klient pocztowy odbierający wiadomość będzie wiedział, jak postępować z załącznikami.

We właściwościach Message Delivery możemy zmienić globalne limity wielkości wysyłanych i odbieranych wiadomości, które w obu przypadkach wynoszą domyślnie 10 MB. Zwiększenie tego parametru ma sens właściwie tylko w przypadku przesyłania danych wewnątrz sieci firmowej, gdzie poczta elektroniczna tworzy podstawowy obieg dokumentów i stanowi swoisty system pracy grupowej. Zasady zdefiniowanie w Message Delivery pomagają także chronić skrzynki pocztowe użytkowników przed niechcianą pocztą. Wiadomości mogą być filtrowanie na podstawie adresu nadawcy lub odbiorcy.

Poczta firmowa i internetowa

Maciej Zdanowicz
10 maja 2004
PC World Komputer

Zasady dotyczące adresów i skrzynek pocztowych definiujemy w folderze Recipients | Recipient Policies. Wstępnie zdefiniowana jest tylko domyślna reguła dotycząca adresów pocztowych. Na jej podstawie każdemu nowo utworzonemu użytkownikowi przypisywane są adresy pocztowe w domenie lokalnej i internetowej. Reguły dotyczące skrzynek pocztowych są wykorzystywane przez menedżera skrzynek przy ich porządkowaniu. Możemy zdefiniować maksymalne wartości dla "wieku" i wielkości wiadomości, po których przekroczeniu podjęte zostaną określone działania, np. wygenerowanie raportu dla administratora albo usunięcie wiadomości lub przeniesienie jej do innego folderu.

Monitorowanie serwera

Utrzymanie serwera pocztowego w pełnej sprawności wymaga monitorowania jego pracy i szybkiego reagowania. Odpowiednie narzędzia znajdziemy w folderze Tools | Monitoring and

Status. Wybierając z menu kontekstowego pozycji Status opcję Connect To, podłączymy się do wskazanego serwera i będziemy mogli odczytać jego stan. Nazwę serwera wpisujemy w standardowym oknie wyszukiwania obiektów w Active Directory lub wybieramy z listy, klikając Zaawansowane | Znajdź teraz. W oknie po prawej stronie zaznaczamy serwer, który chcemy monitorować, i z menu

Akcja wybieramy Właściwości. W nowym oknie zobaczymy pozycję Default Microsoft Exchange Services, stan, w jakim usługa się znajduje (Warning lub Critical) oraz przyczynę, np. Stopped, która oznacza, że jedna z usług składowych nie działa. Po kliknięciu Detail zobaczymy listę usług, które składają się na Default Microsoft Exchange Services oraz stan każdej z nich. Opcja When service is not running change state to określa, jaki powinien być stan usługi nadrzędnej, gdy jedna z usług składowych nie działa. Jest to o tyle istotne, że w zależności od stanu usługi definiuje się powiadomienia administratorów serwera, wysyłane np. pocztą elektroniczną (Tools | Monitoring and Status | Notifications | Nowy | E-mail notification).

Śledzenie wiadomości

Czasami musimy sprawdzić, co się stało z wysłanymi przez nas wiadomościami, które już dawno opuściły program pocztowy, ale ciągle jeszcze nie dotarły do odbiorcy. Aby to stwierdzić, przechodzimy do folderu Servers i rozwijamy pozycję z nazwą naszego serwera pocztowego. Następnie wybieramy Queues i przeglądamy kolejki wiadomości. Jeżeli wysyłaliśmy wiadomość np. do odbiorcy internetowego, to będziemy jej szukali w kolejce Łącznik SMTP pakietu Small Business, Failed message retry queue lub Messages waiting to be routed, wiadomości wewnętrznych będziemy szukać w kolejce Local delivery, natomiast w kolejce Messages awaiting directory lookup znajdziemy wiadomości, które są na etapie rozpoznawania typu odbiorcy. Po zaznaczeniu kolejki możemy kliknąć Find Messages i Find Now, żeby obejrzeć wszystkie wiadomości w kolejce albo wpisać adres nadawcy i/lub odbiorcy i zlokalizować konkretną wiadomość.

Innym przydatnym narzędziem do lokalizowania zagubionych wiadomości jest centrum śledzenia wiadomości (Tools | Message Tracking Centerv). Wykorzystanie go będzie możliwe dopiero po włączeniu usługi śledzenia wiadomości na serwerze. Przechodzimy zatem do folderu Servers, zaznaczamy pozycję z nazwą naszego serwera, np. VOYAGER i z menu Akcja wybieramy Właściwości. Na karcie General zaznaczamy Enable subject logging and display oraz Enable message tracking. Pierwsza opcja powoduje, że tematy wysyłanych wiadomości będą umieszczane w Message Tracking Center, natomiast druga włącza zapisywanie wiadomości w pliku dziennika. Zaznaczając ponadto Remove log files spowodujemy, że pliki dziennika będą usuwane po siedmiu dniach, chyba że wpiszemy własną wartość w pole Remove files older than (days). Klikamy Zastosuj i OK. Od tego momentu cała wysyłana poczta będzie rejestrowana przez centrum śledzenia wiadomości.

W celu znalezienia konkretnej wiadomości przechodzimy do Tools | Message Tracking Center, wpisujemy nazwę nadawcy albo nazwę serwera i klikamy Find Now, żeby wyszukać wiadomości. Dodatkowym kryterium wyszukiwania może być nazwa odbiorcy, identyfikator wiadomości albo przedział czasu, w którym wiadomość została wysłana.

Odzyskiwanie skrzynek pocztowych

Jeżeli usunęliśmy komuś skrzynkę pocztową np. za pomocą Exchange Task Wizard, jest jeszcze szansa jej odzyskania. W folderze Tools znajduje się narzędzie do tego przeznaczone, Mailbox Recovery Center. Po jego zaznaczeniu z menu Akcja wybieramy Add Mailbox Store. Klikamy Zaawansowane | Znajdz teraz, podświetlamy znalezioną pozycję, np. Mailbox Store (VOYAGER) i klikamy OK. Po chwili w prawym oknie pojawi się lista usuniętych skrzynek pocztowych. Zaznaczamy interesującą nas skrzynkę i z menu Akcja wybieramy Find Match, żeby znaleźć w bazie Active Directory użytkownika, któremu należy przypisać odzyskiwaną skrzynkę. Następnie wybieramy Resolve Conflicts, aby przygotować skrzynkę do połączenia z użytkownikiem, aż w końcu Reconnect, żeby ostatecznie ją podłączyć. Podczas podłączania skrzynki może się okazać, że np. użytkownik ma nadany zewnętrzny adres pocztowy, który koliduje z adresem skojarzonym ze skrzynką. Wtedy musimy zlokalizować takiego użytkownika w Active Directory i za pomocą Exchange Tasks usunąć (Delete E-mail Addresses) przypisany adres, a następnie ponownie podłączyć skrzynkę.

Łączniki SMTP i POP3

W folderze Connectors znajdziemy dwa łączniki serwera Exchange. Pierwszy to Łącznik SMTP pakietu Small Business, który Exchange wykorzystuje do komunikacji z serwerami internetowymi. Większość właściwości łącznika SMTP została skonfigurowana za pomocą Kreatora konfigurowania poczty e-mail i połączenia internetowego. Pozostałe są istotne, jeśli zamierzamy wprowadzić bardziej rygorystyczną politykę bezpieczeństwa. Na poszczególnych kartach definiujemy listy nadawców, których wiadomości mają być akceptowane bądź automatycznie odrzucane. Możemy także spowodować, że będą przesyłane tylko wiadomości z ustawionym wysokim priorytetem.

Menedżer łącznika POP3 również został automatycznie skonfigurowany wcześniej. Wśród dostępnych tu użytecznych dodatkowych funkcji, należy wymienić: możliwość pobrania wiadomości ze zdefiniowanych skrzynek na żądanie (przycisk Pobierz teraz karty Planowanie), ustalenia niestandardowego harmonogramu pobierania wiadomości oraz poziomu rejestrowania komunikatów w systemowym dzienniku zdarzeń.

Wirtualne serwery

Po rozwinięciu w folderze Servers pozycji z nazwą naszego serwera pojawi się folder Protocols, który grupuje protokoły dostępowe (nazywane właśnie wirtualnymi serwerami) wykorzystywane w komunikacji z serwerem pocztowym. Protokół HTTP obsługuje technologie Outlook Web Access i Outlook Mobile Access, protokoły POP3 i IMAP4 zapewniają dostęp zdalnym klientom pocztowym, natomiast SMTP służy do komunikacji z internetowymi serwerami pocztowymi. Po wybraniu z menu Akcja opcji Właściwości obiektu Default SMTP Virtual Server, powinniśmy na kartach Access oraz Delivery skonfigurować warunki przyznawania dostępu do serwera na podstawie rodzaju danych uwierzytelniających i/lub adresów internetowych komputerów, a także ograniczyć możliwości wykorzystywania naszego serwera do przekazywania zewnętrznej poczty.

Pozytywna kolaboracja

Jacek Ścisławski
10 maja 2004
PC World Komputer
''Kupą, mości Panowie!'', hasło to na pierwszy rzut oka wydaje się nie mieć związku z pakietem Small Business Server 2003 i technologiami informatycznymi. Warto jednak wiedzieć, że SBS 2003 zawiera nowoczesne centrum usługowe umożliwiające efektywną pracę zespołową. Cóż to jest? SharePoint Services!

Nawet pobieżna analiza oprogramowania wchodzącego w skład Small Business Server 2003 wskazuje, że jest to produkt spełniający wymagania małej, a nawet średniej nowoczesnej firmy. Jeśli przedsiębiorstwo zatrudnia grupę osób do wykonywania zadań o podobnym charakterze, wydajna współpraca personelu może mieć kluczowe znaczenie w osiągnięciu rynkowego sukcesu. Jednym z lepszych sposobów na efektywny obieg informacji wewnątrz firmy jest zbudowanie portalu intranetowego. Dla użytkowników pakietu SBS 2003 Microsoft przygotował gotowe rozwiązanie, które bezproblemowo można zaimplementować na potrzeby firm o różnym profilu działania. Rozwiązaniem tym są usługi Microsoft Windows SharePoint Services.

SharePoint, czyli centrum wymiany informacji

Serwery poczty elektronicznej oraz serwery plików są z założenia systemami obsługującymi wymianę informacji. Centralne składowanie plików lub przesyłanie wiadomości to sprawdzone od lat, standardowe funkcje sieci komputerowych, jednak rozwiązania te zmuszały użytkowników do niewygodnego w praktyce korzystania z oddzielnych narzędzi. W celu odnalezienia potrzebnych plików trzeba sięgnąć do otoczenia sieciowego lub Eksploratora Windows, a do odebrania wiadomości należy uruchomić np. Outlook. I chociaż wewnątrzfirmowe witryny intranetowe stanowią uznane, bardzo dobre i elastyczne źródło informacji, to jak pokazują statystyki, ich utrzymanie - zwłaszcza w niewielkich firmach - było i nadal jeszcze często jest znacznym obciążeniem finansowym. Rozwiązanie SharePoint to zestaw

usług usprawniających wymianę informacji między klientami sieci systemu SBS 2003. Co więcej, dostęp do portalu nie musi być ograniczony do sieci lokalnej. Po przeprowadzeniu nieskomplikowanej konfiguracji systemu, pracownicy mobilni będą mogli sięgać do SharePointa z Internetu przez usługę Remote Web Workplace (patrz artykuł "Wszechobecna sieć")

SharePoint jest zintegrowaną platformą do współdzielenia i zarządzania dokumentami, dostępem do informacji, takich jak kalendarz, kontakty, anonsy, komunikaty, zadania i ankiety. Dzięki temu zespoły handlowców czy projektantów mogą efektywniej współpracować, bo potrzebują tylko przeglądarki internetowej. Niezbędne informacje są dostarczane błyskawicznie, a chaos związany z poszukiwaniem dokumentów zostaje praktycznie eliminowany. Integracja portalu z pakietem Office sprawia, że tworzone arkusze, prezentacje lub pisma mogą być zapisywane bezpośrednio do intranetu.

Nie bez znaczenia jest również łatwość modyfikowania oraz zarządzania modułem SharePoint. Administratorzy systemu mają dostęp do czytelnego środowiska konfiguracji portalu. Zmiana wyglądu witryny albo uprawnień dostępu sprowadza się do kilku kliknięć myszą.

Witryna SharePoint


Rys. 1. Strona główna witryny SharePoint.

Dostęp do portalu usług SharePoint jest realizowany przez przeglądarkę internetową. W dokumentacji producenta znajdujemy informację, że wymagane jest użycie Internet Explorera w wersji powyżej 5.01 z zainstalowanym drugim pakietem serwisowym lub co najmniej Netscape Navigatora 6.2. Możliwa jest również praca z takimi przeglądarkami, jak Opera lub Mozilla. Po uruchomieniu Internet Explorera w pole adresu wprowadzamy http: //CompanyWeb i naciskamy Enter. Jeśli instalacja klienta pakietu Small Business Server została przeprowadzona w sposób zalecany przez Microsoft, w przeglądarce internetowej stroną powitalna będzie http: //CompanyWeb. Witryna SharePoint otworzy się wtedy automatycznie. Ponieważ strony CompanyWeb mają skonfigurowane uwierzytelnienie zintegrowane, pracownicy firmy nie muszą podawać nazwy konta i hasła w celu uzyskania dostępu do portalu. Jeśli użytkownik zalogował się już poprawnie do domeny, informacje wprowadzone w oknie Logowanie do systemu Windows są wykorzystywane do sprawdzenia uprawnień do witryny SharePoint.

Witryna powitalna nie wyróżnia się niczym szczególnym. Przypomina jedną z wielu standardowych stron, które otwieramy, surfując po Internecie. Górna część witryny zawiera pasek odnośników związanych z administrowaniem portalem. Klikając kolejne opcje, będziemy mogli zarządzać dokumentami i listami, tworzyć nowe biblioteki dokumentów, listy lub strony WWW oraz modyfikować ustawienia witryny. Lewy panel strony powitalnej gromadzi skróty do poszczególnych komponentów SharePoint. Klikając dowolny z odnośników, zostaniemy przeniesieni do bibliotek dokumentów, list dyskusyjnych lub ankiet. Pozostały obszar witryny jest podzielony na dwie części. Domyślnie po lewej stronie umieszczane są wiadomości firmowe. Prawa część portalu przedstawia logo firmy oraz listę łączy do określonych przez administratora witryn. Po pierwszym uruchomieniu witryny są to łącza do pomocy dla użytkownika, dostępu do poczty przez przeglądarkę oraz zdalnego zarządzania serwerem.

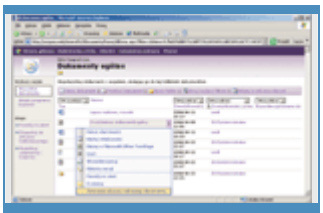
Instalacja i konfiguracja portalu SharePoint

Instalacja usług SharePoint, podobnie jak większość instalowanych komponentów pakietu SBS 2003, przebiega automatycznie. Administrator systemu nie musi wykonywać dodatkowych czynności związanych z konfiguracją portalu lub internetowych usług informacyjnych. Ponieważ Internet Explorer klientów sieci jest ustawiony na automatyczne otwieranie witryny intranetowej, przypisywanie ustawień na stacjach roboczych również nie jest konieczne. Administrator sieci jest zwolniony ze wstępnego definiowania uprawnień dostępu do witryny. Jeśli konta użytkowników są zakładane za pomocą kreatora dodawania kont, każdy nowo utworzony pracownik może korzystać z portalu. Zwiększone uprawnienia użytkowników, związane np. z możliwością zarządzania witryną, są konfigurowane oddzielnie. I jeszcze uwaga: moduł SharePoint domyślnie wykorzystuje port 80.

Jeśli jest to konieczne, dodatkowe czynności konfiguracyjne przeprowadza przeglądarka. Projektanci SBS 2003 nie zapomnieli o umieszczeniu odpowiednich skrótów w narzędziu

Zarządzanie serwerem. Po uruchomieniu tego modułu przechodzimy do folderu Wewnętrzna witryna sieci Web, gdzie wyświetlana jest grupa skrótów do przeprowadzania podstawowych oraz zaawansowanych czynności konfiguracyjnych. Większość ustawień obecnych w Zarządzaniu serwerem to odnośniki uruchamiające Internet Explorer w połączeniu z odpowiednim komponentem administracyjnym SharePointa. Wyjątek stanowi Kreator importu plików, który pozwala na przeniesienie grupy plików do jednej z bibliotek dokumentów. Zmiana ustawień portalu może być wykonywana z pominięciem narzędzia Zarządzanie serwerem. Po otworzeniu strony głównej witryny CompanyWeb klikamy odnośnik Ustawienia witryny i uruchamiamy skrót Przejdź do administracji witryny. Z tego miejsca administratorzy systemu mogą wykonywać wiele zmian ustawień. Dostęp do centralnej strony zarządzania SharePointem uzyskujemy po wpisaniu w przeglądarce adresu: http:// nazwa_serwera:8081, np. http:// voyager:8081.

Konfiguracja i zastosowanie bibliotek dokumentów



Rys. 2. Widok biblioteki Dokumenty ogólne.

W każdej firmie można odnaleźć wiele pism lub arkuszy, wykorzystywanych przez wiele osób. Jedną z głównych zalet witryny SharePoint jest możliwość współdzielenia dokumentów. Pracownicy zatrudnieni w poszczególnych działach firmy mogą centralnie składować ważne pliki ogólnego przeznaczenia. Mogą to być np. podania o urlop, wzory umów, szablony pism kierowanych do kontrahentów lub urzędów państwowych. Korzystając z witryny SharePoint, pracownicy mogą tworzyć, edytować, kopiować oraz usuwać wspólne lub własne pliki.

W panelu szybkiego uruchamiania SharePointa znajduje się grupa odnośników zatytułowana Dokumenty. Oferuje ona dostęp do takich elementów, jak Dokumenty ogólne, Projekty, Prezentacje, Dokumenty zarchiwizowane oraz Faksy przychodzące. Łącza te przenoszą użytkowników do bibliotek dokumentów. Jeśli klikniemy na przykład odnośnik Projekty, przejdziemy do miejsca, w którym możemy zapisywać pliki przeznaczone dla klientów firmy.

Pozytywna kolaboracja

Jacek Ścisławski
10 maja 2004
PC World Komputer

Każda z domyślnych bibliotek służy do gromadzenia odpowiedniego typu dokumentów. W Dokumentach ogólnych przechowywane są pliki związane z pracą zespołową całej firmy. Do biblioteki Projekty możemy przenosić dokumenty wykorzystywane do pracy z klientami firmy. Po założeniu oddzielnego folderu dla każdego kontrahenta zapisujemy w nim wszystkie pliki związane z daną firmą, np. projekty, plany lub oferty. Biblioteka Dokumenty zarchiwizowane służy do gromadzenia archiwalnych zbiorów danych. Podobnie jak w bibliotece Projekty, można utworzyć w niej foldery związane z firmami, dla których projekty zostały już zrealizowane lub foldery reprezentujące minione lata. W bibliotece Prezentacje zapisujemy pliki będące prezentacjami firmy. Folder ten można wykorzystywać jako źródło szablonów plików. W takim przypadku prezentacje utworzone na potrzeby indywidualnych kontrahentów zapisujemy

w bibliotece Projekty. Ostatnia z bibliotek utworzonych po instalacji modułu SharePoint to Faksy przychodzące. Odbierane przez firmę faksy mogą być automatycznie zapisywane w tym folderze. Dzięki temu rozwiązaniu każdy z pracowników będzie mógł łatwo sprawdzić, czy przyszedł oczekiwany faks.

Zawartość bibliotek

Po otwarciu dowolnej z wyżej wymienionych bibliotek, np. Dokumenty ogólne, ujawni się lista dokumentów oraz pasek narzędzi do zarządzania nimi. W lewym panelu umieszczone są skróty do zmiany widoku lub akcji wykonywanych w bibliotece. Po kliknięciu jednej z ikon paska narzędzi możemy utworzyć nowy dokument, przenieść plik lub grupę plików do biblioteki,

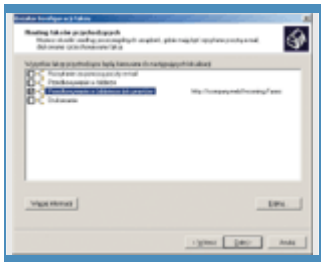
utworzyć nowy folder, przefiltrować pliki lub edytować zasoby w arkuszu danych.

Kliknięcie skrótu Nowy dokument powoduje wywołanie odpowiedniej aplikacji i otworzenie czystego dokumentu, np. dla biblioteki Dokumenty ogólne jest to Microsoft Word związany z szablonem template.doc. Przy tworzeniu nowej biblioteki możemy określić, który z szablonów będzie związany z kliknięciem opcji Nowy dokument. Lista opcji zawiera takie aplikacje, jak Excel, Word, FrontPage czy PowerPoint. Skrót Przekaż dokument jest związany z przekazywaniem dokumentów do biblioteki. Jeśli pracownik utworzył plik na swojej stacji lokalnej, po kliknięciu Przekaż dokument może umieścić go w centrum SharePoint. Na stronie przekazywania dokumentów znajduje się pole edycji, w którym wprowadzamy ścieżkę do pliku. Po kliknięciu przycisku Browse przechodzimy do właściwego folderu i wskazujemy przekazywany plik. Naciśnięcie opcji Zapisz i zamknij spowoduje umieszczenie tego dokumentu w bibliotece. Warto zwrócić uwagę na skrót Przekaż wiele plików, który pozwala na jednorazowe przeniesienie do witryny grupy plików. Zastosowanie opcji Nowy folder nie wymaga żadnego komentarza. Jeśli biblioteka dokumentów zawiera np. kilkaset plików, możliwość filtrowania wyświetlanej zawartości jest nieoceniona. W celu nałożenia filtru na wyświetlane elementy klikamy opcję Filtruj. Okno listy dokumentów zostanie wzbogacone o listy rozwijane, umieszczone nad nagłówkami kolumn. Użytkownik będzie mógł ograniczyć widok dokumentów do tych, które są określonego typu (np. *.doc, *.htm), mają wskazanego właściciela lub zostały zmodyfikowane we wskazanym terminie. Dodatkowo, po kliknięciu nagłówka na przykład kolumny Typ pliki zostaną posortowane rosnąco lub malejąco. Ciekawą opcją paska narzędzi jest możliwość zmiany widoku listy dokumentów. Po kliknięciu w arkuszu danych parametru Edytuj okno portalu przypomina arkusz aplikacji Microsoft Excel. Wśród dodatkowych możliwości widoku dostępna jest na przykład funkcja budowania niestandardowych filtrów lub obliczania sum wartości kolumn.

Każdy z umieszczonych w bibliotece dokumentów ma swoje właściwości. Jeśli korzystamy z widoku standardowego, należy zatrzymać na chwilę wskaźnik myszy na nazwie dokumentu, aby pojawił się znacznik dostępu do listy rozwijanej. Po rozwinięciu listy możemy wybrać takie opcje, jak Pokaż właściwości, Edytuj właściwości, Edytuj w Microsoft Office Word (dla plików *.doc), Usuń, Wyewidencjonuj, Historia wersji, Prześlij mi alert, Dyskutuj oraz Tworzenie nowego obszaru roboczego. Na uwagę zasługuje opcja Wyewidencjonuj, która ma uniemożliwić jednoczesne wprowadzanie zmian do dokumentu przez użytkowników.

Lewy panel biblioteki pozwala na wybranie widoku Wszystkie dokumenty lub Widok programu Explorer. Domyślnie użytkownicy korzystają z widoku Wszystkie dokumenty. Po wybraniu Widok programu Explorer możemy zarządzać plikami tak, jak podczas pracy z Eksploratorem Windows. Jeśli wybierzemy Menu kontekstowe pliku lub okna, będziemy mogli kopiować, wklejać, tworzyć nowe dokumenty, wybierać sposób wyświetlania, korzystać z opcji Wyślij do, zmieniać nazwę itp. W dolnej części lewego panelu biblioteki dokumentów umieszczono grupę odnośników typu Akcje. Opcje tej grupy pozwalają na skonfigurowanie Alertów, eksport listy do arkusza kalkulacyjnego lub zmodyfikowanie ustawień biblioteki. Chcąc na przykład, żeby w bibliotece Dokumenty ogólne domyślnym widokiem był Widok programu Explorer, po przejściu do biblioteki klikamy odnośnik Modyfikuj ustawienia i kolumny. W nowym oknie wyszukujemy opcję Widoki i klikamy Widok programu Explorer. Następnie zaznaczamy pole wyboru Uczyń ten widok domyślnym i klikamy przycisk OK.

Faksy



Opcje związane ze współdzieleniem dokumentów zawierają jeszcze jedno przydatne w wielu firmach łącze, Faksy przychodzące. Pakiet Small Business Server 2003 zawiera dodatkową usługę, która pozwala na zaawansowane zarządzanie wysyłaniem i odbieraniem faksów. Usługi współdzielenia faksu mogą integrować swoje działanie z portalem SharePoint tak, że każdy przychodzący faks będzie automatycznie umieszczany w bibliotece Faksy przychodzące witryny.

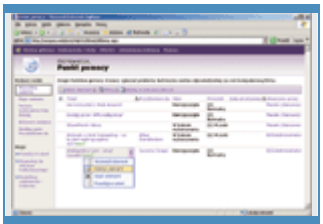
Rys. 3. Okno konfiguracji przekierowania faksów do biblioteki portalu SharePoint.

Konfiguracja integracji z SharePointem jest przeprowadzana w folderze Faks narzędzia Zarządzanie serwerem. Po zaznaczeniu folderu należy uruchomić Kreator konfiguracji faksu. Pierwsze okna kreatora służą do wprowadzenia danych umieszczanych na stronach tytułowych faksów oraz wskazania urządzeń służących do wysyłania i odbierania wiadomości. W oknie Routing faksów przychodzących określamy, gdzie będą kierowane faksy przychodzące do firmy. Wśród dostępnych opcji znajduje się pole wyboru Przechowywanie w bibliotece dokumentów. Po jego zaznaczeniu naciskamy przycisk Edytuj i wskazujemy bibliotekę Faksy przychodzące. W oknie podsumowującym działania kreatora klikamy Zakończ.

Poprawne skonfigurowanie przekazywania faksów owocuje przekazywaniem odebranych wiadomości do biblioteki Faksy przychodzące. Pracownicy firmy przeglądający zawartość portalu będą mogli sprawdzać, czy oczekiwany przez nich faks został odebrany. Umieszczone w bibliotece opcje filtrowania widoków pozwalają na łatwe wyszukiwanie potrzebnych informacji, z uwzględnieniem nadawców lub godziny odbioru. Dodatkowo dzięki usługom alertowania informacje o nadejściu nowego dokumentu będą przekazywane przez system bezpośrednio do skrzynki pocztowej pracownika.

Obrazy

Obrazy swoją zawartością bardzo przypominają biblioteki dokumentów. Podczas instalacji SharePointa system tworzy jedną przykładową bibliotekę, nazwaną Fotografie firmowe. Możemy zapisać tam zdjęcia przedstawiające obrazy z życia firmy lub prywatne fotografie pracowników. Jeśli pakiet SBS 2003 jest używany w agencji reklamowej, pracowni projektowej lub firmach o podobnym profilu, rozbudowa Obrazów o kolejne biblioteki będzie bardzo potrzebna.



Rys. 4. Zawartość listy Punkt pomocy.

Po otwarciu strony Fotografii firmowych nie widzimy na niej żadnych obiektów. Nowe obrazy należy przekazać tak, jak pliki wgrywane do bibliotek dokumentów. Różnicę stanowi możliwość podglądu wstawianych obrazów. Oprócz opcji Nowy folder, Filtruj oraz Usuń zawartość biblioteki została wzbogacona o grupę bardzo przydatnych funkcji, np. Pobierz lub Wyślij do. Po zainstalowaniu pakietu Microsoft Office 2003 bezpośrednio z witryny SharePoint możemy edytować obrazy oraz umieszczać je w dokumentach Worda, PowerPointa czy Excela. Dodatkowo po kliknięciu Opcje ustalamy jeden z proponowanych rozmiarów pobieranego obrazu, np. 800x600 pikseli.

Kolejne udogodnienia odnajdziemy w panelu zawierającym opcje Widok i Akcje. W Widoku wybieramy sposób prezentowania obrazów. Do wyboru mamy Szczegóły, Miniatury oraz Przezrocze. W zależności od wskazanej opcji witryna wyświetla odmienne informacje. Właściwości Akcji oferują możliwość wyświetlania obrazów w pokazie slajdów. Na nowo otwartej stronie możemy swobodnie nawigować pomiędzy prezentowanymi obrazami.

Pozytywna kolaboracja

Jacek Ścisławski
10 maja 2004
PC World Komputer

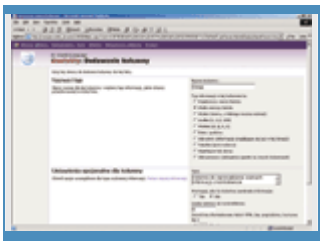
Praca z listami

Praca nad wieloma dokumentami oraz centralne współdzielenie plików stanowi o sile SharePointa. Kolejnym atutem portalu jest możliwość wykorzystania list. Do list witryny

zaliczamy: Anonse, Kontakty, Łącza, Punkt pomocy, Problemy, Kalendarz wakacji oraz Zadania. Każdy z wymienionych obiektów oferuje dodatkowy sposób przekazywania informacji w zespole pracowników. Okno powitalne serwera zawiera odnośniki do Punktu pomocy i Kalendarza wakacji oraz anonsowanych wiadomości.

Korzystając z Punktu pomocy, użytkownicy sieci zgłaszają problemy związane z aplikacjami, sprzętem lub działaniem systemu operacyjnego. Publikowane ogłoszenia nie muszą być związane z kłopotami w działaniu systemów informatycznych, mogą dotyczyć innych technicznych lub organizacyjnych problemów pracowników. Po przejściu do witryny Punkt pomocy, naciskając przycisk Nowy element, tworzymy ogłoszenie. Każda z opublikowanych informacji ma przypisywany priorytet i termin wykonania. Zgłaszając problem, określamy, kogo prosimy o pomoc oraz jaki jest bieżący stan usuwania usterki. Klikając Widok na pasku szybkiego uruchamiania, oglądamy wszystkie lub własne zadania, elementy aktywne oraz te, których termin mija w dniu przeglądania portalu.

Kalendarz wakacji jest przeznaczony do umieszczania informacji o planowanym wypoczynku. Ponieważ do kalendarza może sięgać każdy klient portalu, pozostali użytkownicy sieci wiedzą, kiedy ich współpracownicy są nieobecni. Jeśli na komputerze jest zainstalowany Outlook 2003, informacje o urlopach można łatwo importować do programu jako dodatkowy kalendarz. Wprowadzając nowy termin, określamy nazwę, datę rozpoczęcia i zakończenia urlopu oraz jeśli to konieczne, cykl występowania wydarzenia. Klikając przyciski Wyświetl według dni, Wyświetl według tygodni, Wyświetl według miesięcy możemy wybrać pożądany sposób prezentacji danych.



Rys. 5. Modyfikacja ustawień listy Kontakty.

Pracownikom działu handlowego lub marketingu przyda się współdzielenie informacji o kontaktach z klientami. Jeśli chcielibyśmy do portalu SharePoint dodać listę Kontaktów, należy skorzystać z odnośnika Utwórz umieszczonego w górnej części okna powitalnego. Na nowej stronie odszukujemy listę Kontakty i klikamy jej ikonę. Następnie wprowadzamy nazwę, opis i decydujemy, czy należy dodać listę do paska szybkiego uruchamiania. Po naciśnięciu OK zostaje dodany nowy obiekt. Jeśli chcemy skopiować dane o kontrahentach wprowadzone wcześniej do programu Outlook 2003, klikamy łącze Importuj kontakty. Zaawansowaną konfigurację ustawień listy wykonujemy po kliknięciu Ustawienia witryny | Modyfikuj zawartość witryny. Po wybraniu kontaktów możemy określić uprawnienia innych użytkowników lub zmodyfikować liczbę i ustawienia kolumn opisujących dane klientów.

Dwoma istotnymi elementami witryny SharePoint są Anonse oraz Łącza. Obiekty te domyślnie są umieszczone na głównej stronie portalu. Zadaniem anonsów jest informowanie pracowników firmy o ważnych wydarzeniach, terminach lub spotkaniach. Pod opublikowanymi ogłoszeniami znajduje się odnośnik do tworzenia nowych wiadomości. W dodawanych anonsach wprowadzamy tytuł, treść oraz datę wygaśnięcia. Ogłoszenia, które wygasną, przestaną być widoczne na głównej stronie portalu. Jeśli serwer IIS obsługuje dodatkowe witryny firmy lub pracownicy często sięgają do stron internetowych, administrator może opublikować łącza do przydatnych użytkownikom stron sieci WWW. Domyślnie pierwsza strona portalu zawiera odnośniki do pomocy (Informacje i odpowiedzi), zdalnego dostępu do poczty e-mail oraz zdalnego zarządzania serwerem. Dodanie nowego elementu polega na kliknięciu skrótu Dodaj nowe łącze i wprowadzeniu adresu URL witryny.

Ankiety i dyskusje

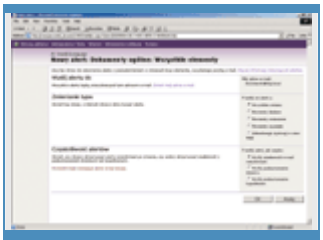
Podejmowanie ważnych decyzji dotyczących produktów czy projektów firmy może być poparte opiniami lub uwagami pracowników. Aby nie tracić czasu na długotrwałe, przegadane zebrania, wystarczy sięgnąć do Ankiet witryny SharePoint. Definiowanie nowego sondażu jest bardzo proste. Po kliknięciu przycisku Utwórz umieszczonego na górnym pasku łączy wyszukujemy i uruchamiamy odnośnik Ankieta. Następnie wprowadzamy nazwę sondażu i konfigurujemy parametry związane z nawigacją oraz opcjami ankiety. Możemy na przykład zezwalać użytkownikom na udzielanie wielu odpowiedzi na to samo pytanie. Po kliknięciu przycisku Następny wpisujemy treść pytania oraz wybieramy jego typ. Do wyboru mamy na przykład pojedynczy wiersz tekstu, liczbę, pole wyboru TAK/NIE czy listę opcji. Dalsze ustawienia zależą od wybranego typu. Jeśli zaznaczyliśmy opcję Wybór (menu, z którego można wybrać), wpisujemy poszczególne punkty odpowiedzi, określamy typ przycisków, wartość domyślną itp.

Gdy ankieta ma zawierać wiele pytań, klikamy przycisk Następne pytanie. Po dodaniu wszystkich pytań naciskamy Zakończ. Utworzone sondaże są umieszczane na pasku szybkiego uruchamiania. Po kliknięciu nazwy ankiety użytkownicy są przenoszeni do okna, w którym mogą udzielić odpowiedzi na pytania lub sprawdzić wyniki głosowania. Kliknięcie łącza Odpowiedz na tę ankietę rozpoczyna pracę z sondażem.

Jeśli grupa użytkowników sieci pracuje nad dużym projektem, często konieczna jest wymiana opinii na temat proponowanych rozwiązań. Sposobem na sprawne jej zorganizowanie jest skorzystanie z Dyskusji. Wymianę zdań rozpoczyna założenie tematu (wątku). Następnie, użytkownicy, którzy chcą wziąć udział w dyskusji, zaznaczają wybrany wątek i ogłaszają odpowiedzi. Strona z publikowanymi wątkami zawiera temat, treść wiadomości, liczbę odpowiedzi, nazwę użytkownika oraz czas publikacji. Utworzenie dyskusji rozpoczynamy od założenia tablicy dyskusyjnej. Zastosowanie tablic pomaga w czytelnym podziale tematów poruszanych przez użytkowników. Tablicę zakładamy, klikając na stronie głównej portalu łącze Dyskusje. Następnie wybieramy skrót Utwórz tablicę dyskusyjną i wpisujemy nazwę tablicy. Dalsze postępowanie jest proste. Na kolejnej stronie klikamy łącze Nowa dyskusja i wprowadzamy temat oraz treść dyskusji. Opcja Zapisz i zamknij zatwierdza naszą wypowiedź.

Alerty

Praca wielu użytkowników nad jednym bądź grupą dokumentów sprawia, że pliki są często modyfikowane. Gdy firma podpisuje ważny kontrakt, na projekt umowy prawnicy lub handlowcy mogą systematycznie nanosić zmiany. Jeśli użytkownicy sieci chcieliby wiedzieć, kiedy nastąpiło uaktualnienie pliku, należy się posłużyć alertami. Po skonfigurowaniu alertów do zasobów użytkownicy będą otrzymywali e-maile o dodawaniu, zmianach lub usuwaniu plików. Możemy konfigurować alerty dotyczące bibliotek dokumentów, listów, dyskusji lub ankiet.



Rys. 6. Dodawanie nowego alertu.

Jeśli w folderze Microsoft biblioteki Projekty umieścimy np. plik: Propozycje artykułów do numeru PCWK Special - SBS 2003.doc i chcielibyśmy, aby system informował nas o zmianach wprowadzonych w dokumencie przez członków redakcji, musimy dodać nowy alert. W tym celu przechodzimy do folderu Microsoft, tam rozwijamy listę opcji dokumentu Propozycje artykułów do numeru PCWK Special - SBS 2003.doc i wybieramy Prześlij mi alert. Na nowej stronie określamy, pod jaki adres ma zostać przesłana informacja. Następnie określamy typ zmian uruchamiających alert oraz termin przesyłania alertów. Na przykład przy typach zaznaczamy Wszystkie zmiany, a w częstotliwości Wyślij wiadomość e-mail natychmiast. Adresu pocztowego nie musimy zmieniać, gdyż system domyślnie proponuje adres użytkownika zalogowanego do portalu. Po naciśnięciu OK, alert jest dodany.

Zmiana konfiguracji alertów może być wykonywana na dwa sposoby. Pierwszy jest przeznaczony dla zwykłych użytkowników portalu i dotyczy wprowadzania zmian ustawień do tych alertów, które odbierają. Druga z opcji jest adresowana do administratorów i pozwala na zarządzanie alertami użytkowników SharePointa. Indywidualne parametry alertów są konfigurowane w opcji Ustawienia witryny. Przechodzimy do nich, klikając odnośnik na głównej stronie portalu. W ustawieniach Zarządzanie moimi informacjami znajduje się skrót Moje alerty w tej lokacji. Jeśli klikniemy odnośnik, będziemy mogli zobaczyć listę alertów i modyfikować ich właściwości. Dostęp do konfiguracji alertów wszystkich użytkowników portalu wymaga przejścia do innej opcji Ustawień. Tym razem klikamy łącze Przejdź do administracji witryny i w części Zarządzanie i statystyka wybieramy Zarządzaj alertami użytkownika. W nowym oknie wskazujemy pracownika, którego ustawienia chcemy zmodyfikować. Po naciśnięciu Aktualizuj wyświetlana jest lista alertów klienta portalu SharePoint. Warto pamiętać, że do zarządzania ustawieniami związanymi z innymi użytkownikami witryny należy mieć uprawnienia administracyjne. Jeśli nie mamy takich uprawnień, przed wprowadzeniem zmian będziemy proszeni o podanie właściwej nazwy konta oraz hasła.

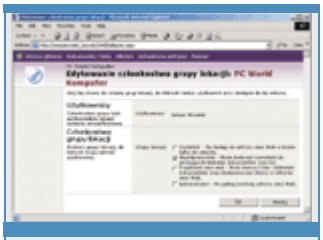
Rys. 7. Okno zarządzania ustawieniami SharePointa w narzędziu Zarządzanie serwerem.

Pozytywna kolaboracja

Jacek Ścisławski
10 maja 2004
PC World Komputer

Folder Wewnętrzna witryna sieci Web

Narzędzie Zarządzanie serwerem zostało zaprojektowana tak, aby nawet mniej doświadczeni użytkownicy pakietu mogli administrować SBS 2003. Uruchamiana przez przeglądarkę centralna strona konfiguracyjna zawiera wiele zaawansowanych ustawień, ale ich stosowanie zalecane jest dopiero po nabyciu pewnego doświadczenia w pracy z modułem SharePoint.



Rys. 8. Zarządzanie uprawnieniami użytkowników.

Zarządzanie portalem intranetowym należy rozpocząć od konfiguracji uprawnień dostępu do modułu SharePoint. Ustawienia nanosimy, uruchomiając skrót Zarządzaj dostępem. Po kliknięciu łącza uruchamiany jest Internet Explorer i zostajemy przeniesieni na stronę Zarządzanie użytkownikami, zawierającą listę kont wraz z przypisanymi im uprawnieniami. Uprawnienia wyznaczane są przez przynależność do Grupy lokacji. Konto klienta może należeć do grup typu Administrator, Projektant sieci Web, Współpracownik oraz Czytelnik. Przynależność do grupy Administrator pozwala użytkownikom na zarządzanie wszystkimi funkcjami portalu. Projektant może tworzyć i konfigurować listy lub biblioteki SharePointa. Konto należące do grupy Współpracownik jest uprawnione do dodawana dokumentów i zawartości do list. Ostatnia z grup - Czytelnik - ma do portalu dostęp w trybie tylko do odczytu. Po instalacji pakietu SBS 2003 każde nowe konto klienta jest automatycznie uprawnione do korzystania z witryny CompanyWeb w trybie Projektanta. Chcąc zmienić domyślne ustawienia, zaznaczamy konto lub grupy kont i klikamy łącze Edytowanie grup lokacji wybranych użytkowników. Na wyświetlonej stronie zaznaczamy grupę, do której chcemy przypisać konta. Większości pracowników firmy wystarcza uprawnienie przynależności do grupy Współpracownik. Aby zmienić domyślne ustawienia nowych klientów pakietu SBS 2003, należy zmodyfikować uprawnienia kont szablonów. Dla standardowych użytkowników szablonem jest User Template.

Po skonfigurowaniu uprawnień możemy rozpocząć wypełnianie portalu firmy dokumentami. Korzystamy z Kreatora importu plików. Umieszczanie dokumentów w witrynie opiera się na prostej technice kopiowania danych. Po uruchomieniu kreatora w oknie Lokalizacja plików i biblioteki dokumentów wypełniamy dwa pola ścieżek do zasobów: Kopiuj pliki z oraz Kopiuj pliki do. Po wprowadzeniu lokalizacji klikamy Dalej i Zakończ.

Następnie należy przystosować portal do potrzeb firmy. Klikając łącze Zmień nazwę szybko można określić tytuł witryny oraz opisać jej zawartość. Po wprowadzeniu danych identyfikatory stron portalu będą zawierać nadaną nazwę. Dalsze działania mogą polegać na korekcie wyglądu głównej strony SharePointa. Do wykonania tego zadania narzędzie Zarządzanie serwerem oferuje dwa skróty Zmień układ strony głównej oraz Zarządzaj wewnętrzną witryną sieci Web. Zmiana układu strony głównej polega na dodawaniu do niej list, dyskusji lub bibliotek dokumentów. Zaawansowane posługiwanie się łączem Zmień układ wymaga zapoznania się z pomocą SharePointa. Kliknięcie Zarządzaj wewnętrzną witryną sieci Web przeniesie nas do strony Ustawienia witryny. Po kliknięciu odnośnika Zastosuj motyw witryny administrator otrzymuje do wyboru jeden z dwudziestu schematów modyfikujących czcionki i kolory portalu. Rezultat przypisania każdego z motywów można obejrzeć w oknie podglądu. Naciśnięcie Zastosuj powoduje automatyczne wprowadzenie ustawień. Innym przykładem prostych modyfikacji witryny jest zmiana znaku firmowego portalu. Po otwarciu powitalnej strony SharePointa widzimy logo pakietu Small Business Server 2003. Zastąpienie tego elementu własnym znakiem graficznym jest bardzo proste. Po wejściu na stronę główną klikamy łącze Modyfikuj stronę udostępnioną i wybieramy po kolei Modyfikuj udostępnione składniki Web Part | Obraz witryny. Następnie wprowadzamy adres URL lub ścieżkę do pliku zawierającego znak firmy. Naciśnięcie Zastosuj zmienia logo. Przedstawione powyżej drobne i przede wszystkim szybkie zmiany wyglądu witryny są jedynie niewielką próbką możliwości konfiguracji portalu. Więcej informacji można odnaleźć w pomocy SharePointa lub na jednej z wielu stron internetowych opisujących ten produkt. Dużo interesujących rozwiązań jest publikowanych na

stronach Microsoftu, np. www.sharepointcustomization.com lub www.microsoft.com/sharepoint .

Na straży SBS

Jacek Ścisławski
10 maja 2004
PC World Komputer

Konfiguracja serwera połączonego z Internetem wymaga wiele uwagi. Jeden mały błąd może spowodować poważne problemy. Oprogramowanie wchodzące w skład pakietu SBS 2003 Premium to seria aplikacji działających nie tylko w środowisku sieci lokalnych. Na szczęście zawiera produkty skutecznie zabezpieczające system przed intruzami.

Pakiet SBS 2003 to grupa serwerów świadcząca usługi dla wewnętrznych i zewnętrznych klientów. Zainstalowanie na jednym komputerze usługi Active Directory, serwera pracy grupowej, baz danych, usług internetowych, DHCP, DNS i np. FTP musi budzić obawy o bezpieczeństwo całego systemu. SBS oferuje usługi lub aplikacje pozwalające na łatwe zabezpieczanie przed nieautoryzowanym dostępem i zarządzanie serwerem. Jeśli firma zdecydowała się na zakup pakietu SBS 2003 Standard, komunikacją zarządza zapora usługi RRAS (Routing i dostęp zdalny). Pakiet SBS 2003 Premium zawiera oddzielną aplikację Internet Security and Acceleration Server 2000 do kompleksowego konfigurowania dostępu do Internetu oraz dostępu z sieci zewnętrznej do zasobów firmy.

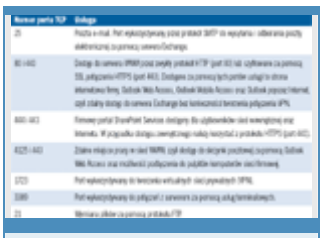
Komponenty komunikacji TCP/IP

Głównym protokołem komunikacyjnym wykorzystywanym do łączności z serwerem SBS 2003 jest TCP/IP, natomiast platformą systemową - Windows Server 2003. Kreatory pakietu sięgają do ustawień systemu i konfigurują wymagane komponenty sieciowe. Zanim przejdziemy do opisu sposobu zabezpieczania serwera, niezbędne jest przypomnienie kilku podstawowych pojęć związanych z komunikacją.

Rys. 1. Właściwości wewnętrznego interfejsu sieciowego.

Wymiana danych z innymi komputerami wymaga prawidłowo skonfigurowanego interfejsu sieciowego. Do zarządzania interfejsami służy folder Połączenia sieciowe z Panelu sterowania. Tam określamy parametry kart sieciowych, a także w miarę potrzeb dodajemy zdefiniowane połączenia i zarządzamy nimi. Warto pamiętać, że podczas konfiguracji serwera SBS najczęściej mamy do czynienia z dwoma interfejsami sieciowymi: wewnętrznym i zewnętrznym. Wewnętrzny służy do komunikacji z klientami sieci lokalnej, a zewnętrzny do wysyłania i odbierania pakietów z Internetu.

Każdy z interfejsów sieciowych serwera musi mieć przypisany jednoznaczny identyfikator w postaci adresu IP. W czasie instalacji Small Business Server 2003 wskazujemy interfejs wykorzystywany do komunikacji z lokalną siecią komputerową. Może to być np. 192.168.0.1, należący do grupy tzw. adresów prywatnych, które są specjalnie przeznaczone do adresowania sieci lokalnych. Podczas ewentualnej zmiany adresu zalecane jest wybranie identyfikatora z zakresu 10.x.x.x, 172.16.x.x-172.31.x.x lub 192.168.x.x. Przypisanie adresu wykraczającego poza wskazane grupy może spowodować konflikty z adresami używanymi w Internecie. Parametry IP drugiego interfejsu zależą od sposobu realizacji połączenia i topologii sieci. Z reguły usługodawca internetowy odpowiada za przekazanie informacji o ustawieniach adresu IP, maski podsieci oraz adresu domyślnej bramy. Adres zewnętrzny nosi nazwę publicznego adresu IP.



Numer portu TCP

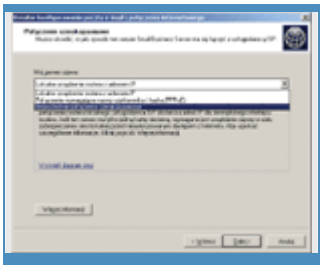
Podczas wymiany danych użytkownicy sieci lokalnej i Internetu korzystają z odpowiednich aplikacji. Chcąc na przykład odebrać wiadomości pocztowe, uruchamiamy klienta poczty, podczas przeglądania witryn korzystamy z Internet Explorera lub innej przeglądarki WWW . Oprogramowanie klienta łączy się z usługą sieciową uruchomioną na serwerze. Pakiety odebrane przez serwer zawierają takie informacje, jak źródłowy adres IP, docelowy adres IP, oznaczenie protokołu warstwy transportowej TCP/IP oraz numery

portów źródłowego i docelowego. Protokoły warstwy transportowej to TCP oraz UDP. Określają one metodę dostarczania danych. Zanim dojdzie do wymiany informacji przez TCP, komputery muszą zestawić sesję. Do komunikacji opartej na UDP zestawienie sesji nie jest konieczne, ponieważ UDP nie wymaga potwierdzenia odebrania danych przez stację docelową. Komputer, w którym uruchamiamy usługę sieciową, np. serwer FTP, otwiera port pełniący funkcję identyfikatora aplikacji działającej na serwerze. Każdy z portów ma przypisany indywidualny numer z zakresu od 0 do 65535. Są dwa typy portów: TCP i UDP, np. serwer FTP standardowo wykorzystuje porty TCP o numerach 20 i 21.

Zabezpieczanie serwera

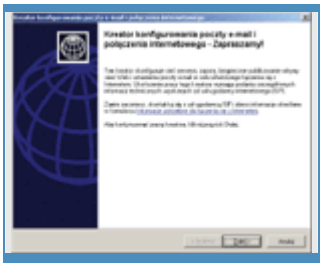
Jeśli serwer SBS 2003 będzie pośrednikiem w komunikacji między siecią zewnętrzną a wewnętrzną lub będzie świadczył usługi dla klientów internetowych, należy zadbać o skuteczną ochronę zasobów systemu. Zabezpieczanie dostępu do serwera opiera się na filtrowaniu pakietów. Dzięki temu administrator SBS 2003 może określić, kto, kiedy i na jakich warunkach dostanie pozwolenie na komunikację z serwerem.

Pakiety są filtrowane na podstawie utworzonych przez administratora reguł komunikacyjnych. Właściwości reguł zawierają informację o typie pakietów odrzucanych lub przyjmowanych przez serwer. Informacje odbierane przez system są analizowane pod kątem takich danych, jak źródłowy lub docelowy adres IP, numer portu, kierunek komunikacji itp.



Rys. 2. Wybór sposobu realizacji połączenia z Internetem.

Zabezpieczenia serwera SBS 2003 mogą być konfigurowane na dwa sposoby. Prostszym rozwiązaniem jest firewall umieszczony w usłudze Rou-ting and Remote Access, zabezpieczenie podobne do oferowanej w systemie Windows XP zapory połączenia internetowego. Tak jak w XP, możemy określać, z których usług uruchomionych na serwerze będą mogli korzystać użytkownicy Internetu. Dostępna jest także karta ICMP pozwalająca na konfigurację przetwarzania pakietów ICMP. Zaletą zapory usługi RRAS jest możliwość tworzenia szczegółowych zasad filtrowania wychodzących i przychodzących pakietów. Szybką konfigurację firewalla wykonujemy przy użyciu kreatora połączenia internetowego. Ustawienia zaawansowane nanosimy, korzystając z menedżera usługi RRAS (opcja Routing i dostęp zdalny) umieszczonego w Narzędziach administracyjnych.



Rys. 3. Okno powitalne kreatora połączeń internetowych i konfiguracji poczty elektronicznej.

Drugim i zdecydowanie zalecanym sposobem zabezpieczenia serwera pakietu SBS 2003 jest instalacja ISA 2000. Internet Security and Acceleration Server to szereg usług, łączących możliwości zapory internetowej oraz buforowania pobieranych witryn. Wbudowany w serwer firewall zawiera złożone mechanizmy ochrony dostępu do zasobów firmy oraz kontroli pakietów wysyłanych z sieci lokalnej. Zaporą zarządza się intuicyjnie i szybko, a możliwość określania dostępu do poszczególnych witryn, plików czy protokołów zwiększa elastyczność administrowania. Co więcej, dostęp może być kontrolowany na poziomie indywidualnych użytkowników lub ich grup. Zastosowanie serwera ISA nie ogranicza się do zapory internetowej. Dodatkowe usługi to buforowanie witryn, raportowanie oraz alarmowanie w przypadku wykrycia potencjalnego zagrożenia. Niestety, serwer ISA jest dostępny wyłącznie w wersji Premium pakietu SBS 2003.

Kreator konfigurowania poczty e-mail i połączenia internetowego

Pakiet SBS 2003 jest przeznaczony do niewielkich firm. Użytkownicy sieci najczęściej mają nieduże doświadczenie w konfigurowaniu zabezpieczeń i zapór internetowych. Aby ułatwić im zadanie oraz zmniejszyć ryzyko pomyłki parametry firewalla są określane za pomocą prostego kreatora, natomiast zaawansowane właściwości można modyfikować za pomocą odpowiednich narzędzi administracyjnych. Kreator jest wywoływany kliknięciem odnośnika Połącz z Internetem w folderze Internet i poczta E-mail modułu Zarządzanie serwerem.

Pracę z kreatorem rozpoczyna wyświetlenie okna powitalnego. Po kliknięciu Dalej przechodzimy do określenia typu połączenia z Internetem. Oferowane są dwie możliwości: dostęp wdzwaniany oraz szerokopasmowy. Połączenie wdzwaniane wybieramy, jeśli łączymy się za pomocą modemu analogowego lub ISDN. Jeśli korzystamy z łącza stałego (np. SDI, Neostrada), należy zaznaczyć opcję Szerokopasmowe. Po kliknięciu Dalej określamy sposób połączenia z Internetem (rys. 2).

Rys. 4. Parametry podawane podczas konfiguracji połączenia z Internetem.

Do wyboru są trzy opcje: połączenie z wykorzystaniem lokalnego routera, połączenie wymagające podania nazwy użytkownika i hasła oraz bezpośrednie, z wykorzystaniem takich urządzeń, jak modem DSL lub kablowy. Aby ułatwić określenie opcji odpowiedniej do konfiguracji sieci, kreator zawiera grupę diagramów ilustrujących różne modele połączeń. Wyświetlamy je, klikając Wyświetl diagram sieci. Na podstawie wskazanego sposobu połączenia, kreator wyświetla kolejne okna. Jeśli wybierzemy Lokalne urządzenie routera z adresem IP, zostaniemy poproszeni o podanie takich parametrów, jak adres IP routera oraz preferowany i alternatywny adres serwera DNS usługodawcy internetowego. Gdy wskażemy opcję Bezpośrednie połączenie szerokopasmowe, musimy określić właściwości adresowania połączenia z Internetem. Na przykład do połączenia przez modem kablowy podajemy adres IP, maskę podsieci oraz adres domyślnej bramy, uzyskany od dostawcy usług internetowych.

Na straży SBS

Jacek Ścisławski
10 maja 2004
PC World Komputer

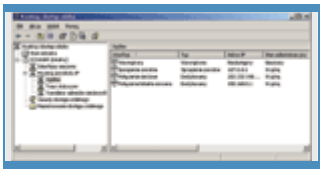
(Strona 2 z 4)

Po zebraniu informacji o właściwościach sieci, kreator połączenia internetowego przystępuje do konfiguracji zabezpieczeń serwera. W oknie Zapora możemy włączyć lub wyłączyć zaporę oraz pozostawić jej konfigurację bez zmian. Bezpośrednio po zainstalowaniu serwera należy koniecznie włączyć i skonfigurować parametry firewalla. Wybieramy Włącz zaporę | Dalej. Okno Konfiguracja usług sieci Web służy do wskazania, które z usług uruchomionych na serwerze SBS 2003 mają być udostępnione klientom zewnętrznym. Domyślnie lista zawiera takie pozycje, jak poczta elektroniczna, wirtualne sieci prywatne, usługi terminalowe oraz FTP. Umieszczenie znacznika przy jednym z elementów włącza dostęp do usługi. Jeśli chcemy wprowadzić dodatkowe wpisy, należy kliknąć przycisk Dodaj. W oknie Dodawanie lub edytowanie usługi wpisujemy nazwę usługi, jej protokół i numer portu. Pełną listę reguł komunikacyjnych można obejrzeć, korzystając z narzędzia Routing i dostęp zdalny.

Rys. 5. Okno Konfiguracja usług sieci Web.

Po zaznaczeniu wybranych usług, klikamy Dalej i przechodzimy do okna Konfiguracja usługi sieci Web. Określamy w nim, z jakich usług serwera WWW mogą korzystać klienci internetowi. Opcje pozwalają zabronić dostępu do witryn z zewnątrz, szczegółowo wskazać, która z usług będzie udostępniona, oraz zezwolić na dostęp do wszystkich komponentów serwera. Chcąc na przykład umożliwić sprawdzanie wiadomości poczty elektronicznej przez przeglądarkę internetową, należy zaznaczyć opcję Outlook Web Access. Klikając Dalej, przechodzimy do okna Certyfikat serwera sieci Web. Certyfikat serwera WWW jest wykorzystywany podczas zestawiania bezpiecznych połączeń SSL między klientem a serwerem. Kreator pozwala na wygenerowanie nowego certyfikatu lub zastosowanie otrzymanego od jednej z komercyjnych firm oferujących tego typu usługi, np. VeriSign. Jeśli generujemy nowy certyfikat, w pole Nazwa serwera sieci Web należy wprowadzić nazwę wykorzystywaną przez klientów do połączenia z serwerem, np. voyager.idg.pl. Po kliknięciu Dalej przechodzimy do konfiguracji ustawień serwera Exchange oraz poczty elektronicznej. Szersze omówienie tych ustawień zawiera artykuł: "Poczta firmowa i internetowa". Wprowadzenie parametrów serwera Exchange 2003 kończy działanie kreatora połączeń internetowych.

Szczegółowa konfiguracja zapory RRAS



Rys. 6. Okno konfiguracyjne usługi RRAS.

Kreator konfiguracji poczty i połączenia internetowego definiuje podstawowe parametry zabezpieczeń serwera. Jeśli chcemy zmodyfikować automatyczne ustawienia systemu, musimy sięgnąć do odpowiednich narzędzi. Do konfiguracji uproszczonej zapory internetowej służy moduł Routing i dostęp zdalny, dostępny w Narzędziach administracyjnych. Głównym przeznaczeniem usługi RRAS jest konfiguracja zasad zdalnego dostępu do serwera SBS. Uruchamiany wcześniej kreator połączenia internetowego wprowadza ustawienia związane z wąskim zakresem działań usługi. Modyfikacja parametrów zabezpieczeń jest ograniczona do właściwości folderu Translator adresów sieciowych / zapora podstawowa.

Po uruchomieniu modułu po kolei rozwijamy foldery: <nazwa_serwera> i Routing protokołu IP. Następnie zaznaczamy opcję Translator adresów sieciowych / zapora podstawowa. W prawym panelu zostanie wyświetlona lista interfejsów sieciowych serwera. Konfiguracja zabezpieczeń dostępu do sieci polega na modyfikacji ustawień interfejsu zewnętrznego. Zaznaczamy go, a następnie z menu Akcja lub z menu kontekstowego wybieramy Właściwości. W wyświetlonym oknie są cztery karty: Translator adresów sieciowych / zapora podstawowa, Pula adresów, Usługi i porty oraz Protokół ICMP.

Rys. 7. Okno właściwości interfejsu zewnętrznego.

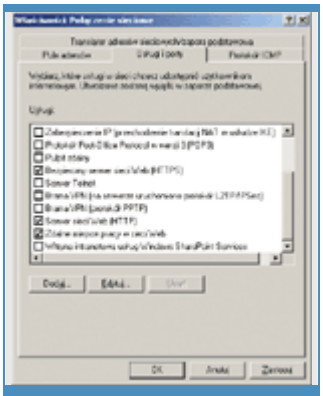
Do zabezpieczania serwera najmniej potrzebna jest karta Pula adresów. Wykorzystujemy ją do konfiguracji zakresu zewnętrznych adresów IP. Zwykle realizacja połączenia z Internetem odbywa się przez jeden adres publiczny i usługę NAT. Jeśli dostawca usług internetowych przydzielił firmie więcej adresów publicznych, karta Pula adresów służy do wprowadzenia przyznanej grupy IP.

Karty Usługi i porty oraz Protokół ICMP zawierają listę ruchu sieciowego przepuszczanego do sieci lokalnej. Karta Protokół ICMP określa typ pakietów protokołu ICMP, na które będzie odpowiadał serwer. Domyślnie włączone jest odpowiadanie na żądania echa, które mogą być przesyłane na przykład przez program Ping. Na karcie Usługi i porty są zaznaczone te usługi, które zostały wybrane w kreatorze połączenia internetowego. Najczęściej zależy nam na dopuszczaniu do serwera ruchu związanego z dostępem do witryn lokalnych (HTTP i HTTPS), poczty (SMTP, POP3), zdalnego pulpitu itp. Zezwolenie na dostęp do serwera polega na zaznaczeniu jednej z wymienionych usług. Jeśli w sieci lokalnej zostanie uruchomiona usługa lub aplikacja, której nie ma na liście, korzystając z przycisku Dodaj, możemy zdefiniować własne parametry komunikacji.

W celu skonfigurowania zaawansowanych ustawień zapory, należy na karcie Translator adresów sieciowych / zapora podstawowa określić dodatkowe parametry zapory dla ruchu przychodzącego i wychodzącego, korzystając z przycisków Filtry przychodzące i Filtry wychodzące. Okna uruchamiane po naciśnięciu dowolnego z przycisków są identyczne. Pole Filtry zawiera definicję komunikacji, natomiast opcje: Odbierz wszystkie pakiety oprócz tych, które spełniają poniższe kryteria i Porzuć wszystkie pakiety oprócz tych, które spełniają poniższe kryteria służą do określania akcji podejmowanej przez serwer po odebraniu konkretnego pakietu. Kryteria mogą być budowane przez wskazanie adresu IP sieci źródłowej i docelowej, typu protokołu oraz portu źródłowego i docelowego.

Instalacja serwera ISA

Po zainstalowaniu podstawowych komponentów pakietu należy zadbać o bezpieczeństwo serwera oraz sieci lokalnej. Edycja Premium pakietu SBS 2003 zawiera serwer Microsoft ISA 2000 Standard Edition. Aby go zainstalować, należy skorzystać z płyty Premium Technologies. Po umieszczeniu CD w napędzie uruchamia się aplikacja autostartu i wyświetlane jest okno zawierające skróty do zapisanych na płycie aplikacji. Oprócz odnośnika do instalatora serwera ISA możemy rozpocząć instalację serwera SQL 2000. Pozostałe skróty to przewodnik omawiający sposób instalacji aplikacji, odnośnik do przeglądania zawartości płyty oraz instalacji Service Pack 3a do serwera SQL. Kliknięciem Zainstaluj Microsoft Internet Security and Acceleration Server 2000 rozpoczynamy instalację.



Rys. 8. Okno konfigurowania dostępu do usług serwera.

Następne trzy okna to ekran powitalny, okno z identyfikatorem aplikacji oraz okno wyświetlające treść licencji. Aby rozpocząć określanie parametrów serwera ISA, naciskamy Continue | OK | I Agree. W nowym oknie możemy wybrać typ oraz miejsce instalacji serwera. Osobom, które mają niewielkie doświadczenie z ISA, zaleca się pozostawienie ścieżki domyślnej i kliknięcie opcji Typical Installation. Następny ekran służy do wyboru trybu pracy serwera: Firewall mode, Cache mode oraz Integrated mode. Wyjaśnienie różnic pomiędzy poszczególnymi typami można odnaleźć w ramce "Tryby pracy serwera ISA 2000". Domyślnie zaznaczona jest opcja Integrated mode i z reguły nie należy jej zmieniać. Po kliknięciu Continue może zostać wyświetlony komunikat związany z rekonfiguracją serwera IIS. Ponieważ po zainstalowaniu serwera ISA należy uruchomić Kreator konfigurowania poczty e-mail i połączenia internetowego, zmiana ustawień IIS nie jest konieczna.

Tabele serwera ISA

LAT (Local Address Table) - zawiera listę adresów IP przypisywanych w wewnętrznej sieci firmy. Klienty sieci sięgają do tabeli w celu określenia, czy pakiety wychodzące z ich komputerów przekazać bezpośrednio do serwera ISA.

LDT (Local Domain Table) - zawiera listę nazw domen sieci wewnętrznej obsługiwanych przez serwer ISA. W wypadku pakietu SBS będzie to jedna domena.

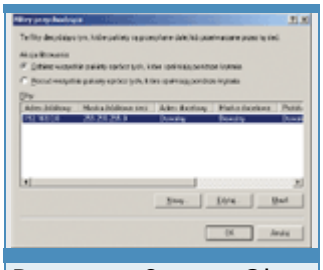
Tryby pracy serwera ISA

Firewall mode - tryb pracy serwera ISA, w którym funkcjonuje on jako zapora zabezpieczająca serwer przed nieautoryzowanym dostępem z zewnątrz. Cały ruch sieciowy przychodzący spoza sieci lokalnej jest kontrolowany za pomocą reguł zdefiniowanych przez administratora.

Cache mode - tryb pamięci podręcznej wykorzystywany na serwerach, które pośredniczą podczas pobierania danych z Internetu przez klienty sieci lokalnej. Magazynowanie plików powoduje, że nie trzeba wielokrotnie ściągać zawartości tych samych witryn. Jeśli w pamięci podręcznej znajduje się kopia strony WWW, przeglądarka klienta pobierze ją z serwera ISA. Oprócz buforowania witryn pobieranych przez klienty sieci lokalnej serwer obsługuje również buforowanie publikowania WWW . Opcja ta jest wykorzystywana, gdy serwer WWW zostanie umieszczony wewnątrz sieci lokalnej, a ISA będzie pośrednikiem w ruchu między zewnętrznym klientem a serwerem WWW .

Integrated mode - tryb pracy mieszanej. Serwer ISA łączy kontrolę dostępu z jednoczesnym magazynowaniem pobranych danych.

Jeżeli wybraliśmy zintegrowany tryb działania, naciśnięcie OK powoduje wyświetlenie okna konfiguracji ustawień pamięci podręcznej. Konfiguracja buforowania w czasie instalacji wymaga podania napędu, na którym umieszczony będzie cache, oraz ilości miejsca przeznaczonego na bufor. Systemem plików pamięci podręcznej musi być NTFS. Po wskazaniu partycji w pole Cache size wprowadzamy odpowiedni rozmiar bufora. W niedużej sieci wystarcza zwykle przedział 100-500 MB. Zatwierdzenie rozmiaru polega na naciśnięciu przycisków Set i OK.



Rys. 9. Okno konfigurowania kryteriów komunikacji.

W następnym oknie wprowadzamy zakresy lokalnych adresów IP. Zwykle sieć wewnętrzna obejmuje adresy od 192.168.0.0 do 192.168.0.255. Wpisujemy je w pola From i To. Gdy nie jesteśmy pewni, jakie wartości wprowadzić w oknie z adresami IP, należy skorzystać z opcji Construct Table. Podczas budowy tabeli system pozwala na zaznaczenie dwóch pól wyboru. Pierwsze dodaje do tabeli LAT (patrz ramka), grupę adresów prywatnych o identyfikatorach 10.x.x.x, 172.16.x.x-172.31.x.x, 192.168.x.x oraz adresy 169.254.x.x, wykorzystywane przez automatyczne adresowanie prywatne w sieciach Microsoft. W miejsce x podstawiane są liczby z przedziału od 0 do 255. Druga opcja wprowadza adresy IP na podstawie analizy tabeli routingu Windows Server 2003. Jeśli uprzednio skonfigurowaliśmy wszystkie interfejsy sieciowe komputera, należy zaznaczyć wyłącznie kartę z adresami lokalnymi. Zatwierdzenie wpisów tabeli LAT rozpoczyna kopiowanie plików, a po wykonaniu wszystkich czynności konfiguracyjnych kończy instalację produktu. W oknie wieńczącym proces instalacji naciskamy OK. Opcja Start the ISA Server Getting Started wizard powinna pozostać pusta. Następnie system automatycznie uruchomi Kreator konfigurowania poczty e-mail i połączenia internetowego. Jego konfiguracja nie różni się od ustawień nadawanych przy zastosowaniu zapory z narzędzia Rou-ting i dostęp zdalny.

Rodzaje klientów serwera ISA

Web Proxy - konfiguracja klienta polega na wprowadzeniu adresu i portu serwera ISA we właściwościach przeglądarki w polu Serwer Proxy. Klient jest wykorzystywany do przyśpieszenia pobierania witryn, gdyż żądania pobrania stron są przesyłane bezpośrednio do serwera ISA.

SecureNAT - konfiguracja klienta polega na wprowadzeniu w pole Domyślna brama adresu serwera ISA. Najprostszym sposobem przypisania właściwych ustawień jest skorzystanie z opcji serwera DHCP. W wypadku tego rodzaju klienta wszelkie żądania komunikacji sieciowej przechodzą przez serwer ISA. Klient obsługuje buforowanie i filtrowanie. Bez autentykacji na poziomie użytkownika.

Firewall - konfiguracja klienta wymaga instalacji dodatkowego oprogramowania. Wysiłek ten jest nagradzany możliwością elastycznego określenia dostępu do zasobów Internetu na poziomie użytkownika.

Rodzaje elementów zasad serwera ISA

Schedules - folder z elementami wykorzystywanymi do określania harmonogramu aktywności reguł. Utworzone w nim obiekty mogą być używane w regułach filtrów, zawartości i miejsca oraz protokołów.

Bandwidth Priorities - folder z elementami wykorzystywanymi do określania priorytetów połączeń. Zakres wprowadzanych wartości stanowi liczba z przedziału 1-200, gdzie 200 to najwyższy priorytet.

Destination Sets - folder z elementami wykorzystywanymi do identyfikowania ścieżki, komputera lub grupy komputerów. Hosty mogą być identyfikowane za pomocą nazwy oraz adresu IP. Obiekty umieszczone w tym folderze są stosowane w regułach zawartości i miejsca.

Client Address Sets - folder z elementami wykorzystywanymi do identyfikowania nazw, adresów lub grup adresów IP klientów sieci lokalnych.

Protocol Definitions - folder z elementami wykorzystywanymi do określania dozwolonych lub zabronionych protokołów. Domyślną zawartość stanowi zestaw definicji większości spotykanych w Internecie usług. Administrator może rozbudowywać zawartość folderu przez wprowadzenie nowych nazw.

Content Groups - folder z elementami wykorzystywanymi do identyfikowania dozwolonej lub niedozwolonej zawartości pobieranej z Internetu. Po instalacji serwera folder zawiera grupę najczęściej spotykanych zestawów rozszerzeń, np. pliki audio lub pliki wideo.

Dial-up Entries - folder zawiera definicje połączeń wdzwanianych podczas dostępu do Internetu.

Instalacja klienta ISA

Po zainstalowaniu serwera ISA administrator musi przeprowadzić jeszcze jedną kluczową czynność. Aby użytkownicy sieci mogli korzystać z serwera proxy, należy odpowiednio skonfigurować ich stacje. ISA serwer obsługuje trzy rodzaje klientów: Web Proxy, SecureNAT oraz Firewall.

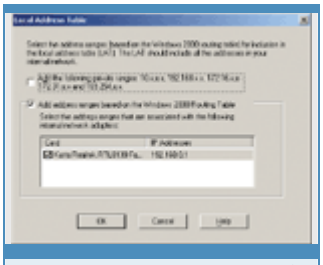
Rys. 10. Okno instalacyjne dysku Premium Techologies.

Dla sieci pracującej pod kontrolą pakietu SBS najbardziej odpowiedni jest klient Firewall, ale niezbędna jest instalacja oprogramowania na komputerach użytkowników. Ponieważ SBS 2003 oferuje proste narzędzie do dystrybucji aplikacji na stacje sieciowe, instalacja wymaga jedynie kilku kliknięć. Warunkiem powodzenia automatycznej dystrybucji oprogramowania jest uprzednie założenie konta komputera w domenie oraz skojarzenie komputera klienckiego z tym konkretnym kontem. Jeżeli konto komputera nie zostało jeszcze założone, należy skorzystać z Kreatora konfigurowania komputera w module Zarządzanie serwerem. Następnie należy podłączyć komputer do domeny. Można do tego wykorzystać narzędzia serwera SBS albo wykonać tę operację ręcznie. Podłączenie komputera do domeny narzędziami SBS odbywa się poprzez przeglądarkę. Na stacji roboczej klienta wpisujemy adres //nazwa_serwera/ConnectComputer i po załadowaniu strony wybieramy opcję Podłącz do sieci. Podłączenie ręczne wymaga wybrania Właściwości obiektu Mój komputer lub ikony System z Panelu sterowania. W obu przypadkach wybieramy kartę Nazwa komputera i naciskamy przycisk Identyfikacja sieciowa albo Zmień. Dalej wprowadzamy nazwę domeny, konto i hasło użytkownika sieci i restartujemy komputer. Zakładanie kont komputerów zostało opisane w artykule "Konfiguracja".


Rys. 11. Wybór trybu pracy serwera ISA.

Następne operacje wykonujemy na serwerze SBS. Uruchamiamy moduł Zarządzanie serwerem i przechodzimy do folderu Komputery klienckie. W prawym panelu, wśród dostępnych zadań odnajdujemy i klikamy Konfiguruj aplikacje klienckie. W oknie powitalnym kreatora klikamy Dalej. Następne okno zawiera listę aplikacji dostępnych dla klientów sieci. Ponieważ lista domyślnie nie zawiera oprogramowania klienckiego serwera ISA, naciskamy przycisk Dodaj. Okno dodawania aplikacji zawiera dwa pola edycji. W pierwsze wprowadzamy nazwę programu, w drugie ścieżkę do pliku wykonywalnego. Ponieważ instalator serwera ISA założył i udostępnił folder z oprogramowaniem klienckim, nie musimy wgrywać żadnych plików i konfigurować udziałów. Wystarczy w odpowiednie pola wpisać: Klient serwera ISA oraz "\\nazwa_serwera_SBS\

MspClnt\setup.exe". Trzeba pamiętać o uwzględnieniu cudzysłowów podczas wpisywania ścieżki sieciowej. Następnie klikamy OK, Dalej oraz Zakończ i kreator kończy działanie.



Rys. 12. Konstruowanie tabeli LAT.

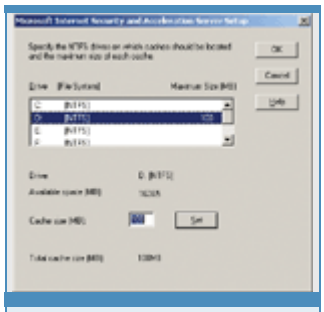
Po dodaniu nowego oprogramowania należy wskazać docelowe klienty instalacji. W tym celu uruchamiamy kreator Przypisz aplikacje do komputerów klienckich. Po naciśnięciu Dalej wybieramy, do których stacji ma trafić aplikacja klienta ISA. Domyślnie powinna dotrzeć do wszystkich komputerów, dlatego w następnym oknie klikamy Dodaj wszystkie. Następnie w oknie Aplikacje klienckie zaznaczamy Klient serwera ISA i w pozostałych oknach kreatora naciskamy Dalej. Teraz wystarczy, aby użytkownicy sieci się przelogowali, a na ich pulpicie pojawi się skrót Kliknij tutaj, aby zainstalować Klient serwera ISA. Naciśnięcie tej opcji spowoduje zainstalowanie oprogramowania. Opisany sposób jest skuteczny w wypadku komputerów z systemami Windows XP oraz Windows 2000 Professional. Jeśli w sieci są wykorzystywane starsze systemy operacyjne, wówczas należy przeprowadzić ręczną instalację klienta. Nie jest to dużym kłopotem, ponieważ wystarczy podłączyć się do udostępnienia MspClnt i uruchomić plik Setup.exe.

Instalacja klienta ISA sprawia, że podczas odwoływania się do adresów zewnętrznych system operacyjny przesyła wywołania sieciowe do serwera SBS 2003. Zarządzanie środowiskiem klienta jest realizowane przez umieszczone w Panelu sterowania narzędzie Firewall Client. Zawiera opcje pozwalające na czasowe wyłączenie klienta oraz aktualizację informacji o adresach wewnętrznych umieszczonych w tabeli LAT.

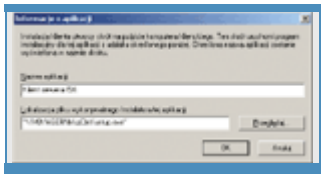
Na straży SBS

Jacek Ścisławski
10 maja 2004
PC World Komputer

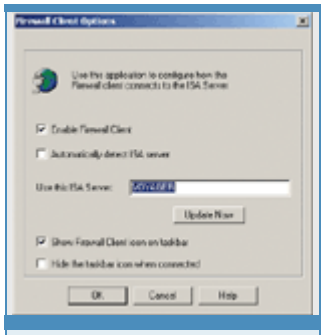
Narzędzie do konfiguracji ISA



Rys. 13. Konfiguracja pamięci podręcznej serwera ISA.



Rys 14. Okno dodawania aplikacji klienta ISA.



Rys. 15. Okno narzędzia Firewall Client.

Kreator konfigurowania poczty e-mail i połączenia internetowego jest wykorzystywany do przypisania podstawowych parametrów serwera ISA. Zaawansowane ustawienia zapory oraz buforowania konfigurujemy narzędziem ISA Management. Możemy je odnaleźć, klikając Start | Programy | Microsoft ISA Server. Moduł do zarządzania serwerem na pierwszy rzut oka wydaje się skomplikowany. Liczba folderów i podfolderów konfiguracyjnych wzbudza lekki niepokój. Wystarczy jednak poznać sposób działania serwera ISA, a lęk przed nieznanym znika.

Dwa podstawowe foldery do zarządzania zabezpieczeniami systemu to Access Policy oraz Policy Elements. Pierwszy zawiera zbiór reguł dotyczących zezwalania lub niezezwalania na dostęp do zasobów sieci i Internetu. Reguły te zostały podzielone na trzy grupy: Site and Content rules, Protocol rules i IP Packet Filters. Ich zastosowanie wyjaśniamy w ramce "Rodzaje reguł dostępu".

Reguły określone przez politykę dostępu są przetwarzane w ustalonym porządku. Jeśli użytkownik sieci będzie chciał zestawić połączenie ze zdalnym hostem, serwer ISA najpierw sprawdzi, czy są reguły, które zabraniają lub zezwalają na wypuszczenie protokołu. Gdy są reguły zabraniające lub nie ma reguł zezwalających, żądania komunikacji są odrzucane. Następnie na podobnej zasadzie weryfikowane są ustawienia zasad witryn i zawartości. Tylko jawne zezwolenie na komunikację ze wskazanymi witrynami zestawia połączenie z zewnętrznym hostem. Na końcu sprawdzane są reguły filtrowania pakietów. Gdy nie ma filtrów blokujących określony ruch, żądania klienta są przekazywane do sieci zewnętrznych.

W celu uproszczenia sposobu konfigurowania zabezpieczeń serwer ISA posługuje się elementami zasad. Policy Elements to zbiór komponentów, z których składamy reguły dostępu do sieci: godziny ich obowiązywania, priorytety ruchu, adresy klientów i hostów, definicje protokołów oraz grup użytkowników. Po wejściu do folderu Policy Elements widzimy grupę podfolderów, z których każdy służy do definiowania nowych obiektów zasad. Ponieważ po zainstalowaniu serwera ISA administrator ma przygotowany pokaźny zestaw zasad nadających się do budowy reguł dostępu, tworzenie nowych obiektów jest bardzo proste.

Rodzaje reguł dostępu serwera ISA

Site and Content rules - zasady określania, do jakich witryn lub domen mogą sięgać klienci Web Proxy. Dodatkowo reguły pozwalają na definiowanie ograniczeń pobieranej zawartości stron. Np. zezwolenie na dostęp do wszystkich witryn domeny idg.pl.

Protocol rules - zasady wykorzystywane do określenia, jakie protokoły sieciowe mogą być używane przez klienty sieciowe do komunikacji z siecią zewnętrzną, np. dostęp do zewnętrznych serwerów grup dyskusyjnych z wykorzystaniem protokołu NNTP.

IP Packet Filters - zasady szczegółowego określania, jakie pakiety są wpuszczane przez serwer lub wypuszczane do Internetu. Filtry obejmują ustawienia protokołu, portu, kierunku, źródła i przeznaczenia, np. zezwolenie na wysyłanie i odbieranie pakietów protokołu ICMP przez wszystkie stacje lokalne do wszystkich

---

ISA w praktyce

Maciej Zdanowicz
10 maja 2004
PC World Komputer

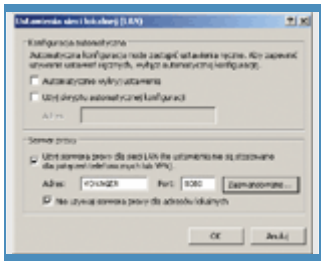
Korzystanie z kreatorów do konfiguracji systemu na pewno ułatwia pracę i przyspiesza wykonywanie zadań administracyjnych. Taka metoda dobrze sprawdza się w typowych czynnościach. Zaawansowana konfiguracja wymaga jednak nieco większego zaangażowania użytkownika.

Dokładne poznanie narzędzia oraz mechanizmów, według których działa, jest szczególnie istotne wtedy, gdy od prawidłowego posługiwania się nim zależy bezpieczeństwo systemu. Tak właśnie jest w przypadku Internet Security and Acceleration Server 2000.

Z poprzednich artykułów znamy już możliwości serwera ISA i potrafimy go zainstalować. Wiemy, że łączy funkcję zapory internetowej w przypadku dostępu klientów zewnętrznych do zasobów sieci lokalnej oraz zapory kontrolującej dostęp użytkowników lokalnych do zasobów w Internecie, a także serwera buforującego - również działającego w obydwu kierunkach. Jako serwer proxy ISA zmniejsza ruch internetowy, przechowując kopie już raz ściągniętych stron, a jednocześnie zmniejsza obciążenie wewnętrznych serwerów WWW, dostarczając klientom zewnętrznym kopie stron już raz wygenerowanych na komputerach w sieci lokalnej.

Poznaliśmy też zasady definiowania reguł, według których serwer ISA kontroluje dostęp oraz sposoby współpracy klientów sieci lokalnej z serwerem. Do wstępnej konfiguracji wykorzystywaliśmy Kreator konfigurowania poczty e-mail i połączenia internetowego, który wprowadzał podstawowe ustawienia do serwera ISA. Obecnie przyjrzymy się domyślnym ustawieniom serwera obowiązującym bezpośrednio po instalacji, zobaczymy, jakie zmiany wprowadza wspomniany kreator i na jakim poziomie zabezpieczeń znajduje się serwer po zakończeniu wstępnego procesu konfiguracyjnego. Dysponując tą wiedzą, będziemy mogli zacząć świadomie tworzyć własne dodatkowe reguły, które współpracując z pozostałymi ustawieniami, pozwolą nam zawsze uzyskiwać oczekiwane i prawidłowe rezultaty. Wprowadzanie dodatkowych reguł prześledzimy na przykładach praktycznych, pokazujących, w jaki sposób osiągnąć wymagane działanie zapory internetowej w określonych okolicznościach.

ISA po instalacji

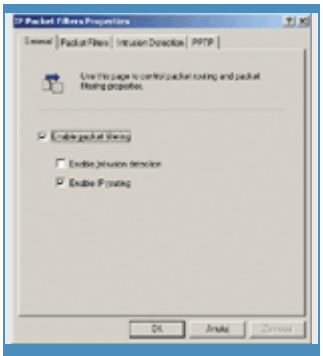


W trakcie instalacji serwera ISA, witryny WWW są zatrzymywane w Menedżerze internetowych usług informacyjnych (IIS) i konfigurowane tak, aby były powiązane z wewnętrznymi interfejsami sieciowymi. Zostaną ponownie uaktywnione po uruchomieniu Kreatora konfigurowania poczty e-mail i połączenia internetowego. Zmiany w konfiguracji kart sieciowych są konieczne dlatego, że to serwer ISA ma w pierwszej kolejności odbierać wszystkie zgłoszenia i dopiero na podstawie zdefiniowanych reguł decydować, czy należy je przekazać dalej.

Rys. 1. Zamiast ściągać strony z Internetu, przeglądarka przesyła wszystkie żądania do serwera proxy. Nie dotyczy to adresów lokalnych, które są dostępne bezpośrednio.

Komputery klientów, które zostały dołączone do domeny serwera SBS, otrzymały zestaw domyślnych ustawień konfiguracyjnych. Jednym z nich jest wpis w przeglądarce, który określa serwer buforujący wykorzystywany przy dostępie do Internetu. W programie Internet Explorer wybieramy Narzędzie | Opcje internetowe i wybieramy kartę Połączenia. Klikamy Ustawienia sieci LAN i w grupie Serwer proxy widzimy wpisany adres serwera ISA (np. VOYAGER) i numer portu, na który mają być kierowane zgłoszenia (8080). Zaznaczona jest też druga opcja Nie używaj serwera proxy dla adresów lokalnych. Gdybyśmy uruchomili w Menedżerze IIS np. wewnętrzną witrynę firmową, to po wpisaniu w przeglądarce adresu http: //companyweb/ zobaczylibyśmy stronę główną wewnętrznego portalu SharePoint. Witryna byłaby dostępna tylko dlatego, że zgłoszenie zostało wysłane bezpośrednio do witryny WWW z pominięciem serwera ISA, ponieważ adres http: //companyweb/ jest adresem lokalnym. Gdybyśmy natomiast wyłączyli opcję Nie używaj serwera proxy dla adresów lokalnych, to wszystkie zgłoszenia przechodziłyby przez serwer ISA, a więc byłyby kierowane na port 8080. Jednocześnie byłyby to zgłoszenia sformułowane dla serwera proxy, a nie dla serwera WWW, który w związku z tym nie potrafiłby na nie odpowiedzieć. Wobec braku jakichkolwiek reguł zezwalających na dostęp do witryny, zamiast oczekiwanej strony otrzymalibyśmy komunikat serwera ISA HTTP 502 Proxy Error - The ISA Ser-ver denies the specified Uniform Resource Locator (URL). (12202) Internet Security and Acceleration Server.

W obecnej konfiguracji, tj. tuż po instalacji, serwer ISA nie ma zdefiniowanych żadnych reguł, a więc zapora nie przepuszcza żadnego ruchu. Pomijając to, że w związku z instalacją ISA do czasu skonfigurowania zapory wyłączona została również zewnętrzna karta sieciowa, dostęp do Internetu z komputerów klientów jest niemożliwy na podstawie samych ustawień serwera.



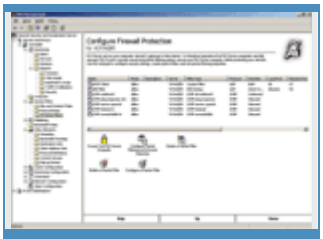
Rys. 2. Zalecana konfiguracja serwera ISA. Filtrowanie ruchu i przekazywanie pakietów włączone.

Zanim uruchomimy kreatora

Przyjrzyjmy się konfiguracji serwera ISA przed wprowadzeniem ustawień za pomocą narzędzi pakietu SBS, a konkretnie Kreatora konfigurowania poczty e-mail i połączenia internetowego. Uruchamiamy narzędzie ISA Management (menu Start | Programy | Microsoft ISA Server | ISA Management). Wszystkie ustawienia znajdują się w folderach dostępnych po przejściu do Servers And Arrays i rozwinięciu pozycji z nazwą serwera, w naszym przypadku VOYAGER.

Reguły dostępu znajdują w folderze Access Policy. W Site and Content Rules jest tylko jedna reguła o nazwie Allow rule. W jej właściwościach dowiemy się, że reguła zezwala (Allowed na karcie Action) na przekazywanie ruchu do wszystkich adresów (All destinations na karcie Destinations), o każdej porze (Always na karcie Schedule) dla wszystkich zgłoszeń niezależnie od adresu nadawcy zgłoszenia (Any request na karcie Applies To). Na karcie HTTP Content wybrana jest ponadto opcja All content groups, żeby zaznaczyć, że reguła nie dotyczy konkretnego rodzaju danych przesyłanych za pomocą protokołu HTTP, lecz dowolnych transmisji.

Podstawowe filtry



Rys. 3. Podstawowy zestaw filtrów w serwerze ISA. Kreator połączenia internetowego pakietu SBS wprowadzi tu wiele dodatkowych filtrów.

Reguły w Site and Content Rules działają w połączeniu z Protocol Rules. Dopiero gdy odpowiednie reguły w obu tych miejscach zezwolą na przekazywanie ruchu i nie będą zdefiniowane filtry blokujące w IP Packet Filters, dostęp zostanie przyznany. Ponieważ w Protocol Rulet nie ma żadnej reguły, dostęp do jakichkolwiek zasobów internetowych nie jest możliwy.

W przypadku połączeń wychodzących brak reguł blokujących w IP Packet Filters zazwyczaj umożliwia przekazywanie pakietów do Internetu. W przypadku protokołu ICMP trzeba jednak wyraźnie na to zezwolić. Dlatego na liście IP Packet Filters jest już kilka gotowych reguł. Pierwszy aktywny DNS filter zezwala na komunikację z zewnętrznymi serwerami DNS, otwierając połączenia ze zdalnym portem 53, natomiast następne pięć dotyczy protokołu ICMP. Reguły te zezwalają na przesyłanie zapytań poleceniem **ping** (filtr ICMP outbound) i odbieranie odpowiedzi pozytywnej zdalnego systemu (ICMP ping response) oraz odbieranie odpowiedzi informujących o błędach lub sytuacjach wyjątkowych (ICMP timeout in, ICMP unreacheable in, ICMP source quench).

Dodawanie filtrów

Konfiguracja protokołu ICMP zezwala na wysyłanie zapytań za pomocą **ping** i umożliwia ich odbieranie. Jednak próba użycia polecenia **ping** do zlokalizowania naszego serwera z zewnątrz zakończy się niepowodzeniem, ponieważ brakuje reguły, która pozwoliłaby komputerowi odpowiadać na zapytania ICMP. Aby ją zdefiniować, w folderze IP Packet Filters klikamy skrót Create a Packet Filter albo jeśli ustawiony mamy widok zaawansowany (menu Widok, opcja Advanced), wybieramy Akcja | Nowy | Filter. Pojawia się okno New IP Packet Filter Wizard, w którym najpierw wpisujemy nazwę filtru, np. ICMP query in. Klikamy Dalej, zaznaczamy Allow packet transmission i ponownie Dalej. W oknie Filter Type zaznaczamy Predefined i z listy wybieramy **ICMP ping query**. W kolejnych oknach zatwierdzamy domyślne wybory Default IP addresses for each external interface on the ISA Server computer oraz All remote computers. Po kliknięciu Zakończ utworzona zostanie nowa reguła i serwer zacznie odpowiadać na zapytania programu ping.

ISA w praktyce

Maciej Zdanowicz
10 maja 2004
PC World Komputer

Precyzyjna selekcja pakietów

Opcje sterujące filtrowaniem pakietów w serwerze ISA dostępne są po kliknięciu Configure Packet Filtering and Intrusion Detection w folderze IP Packet Filters. Na karcie General możemy ponadto włączyć wykrywanie ataków (Enable Intrusion detection), a także przekazywanie pakietów do sieci wewnętrznej (Enable IP routing), przy czym druga opcja jest włączana przez Kreatora konfigurowania poczty e-mail i połączenia internetowego.

Konfiguracja wykrywania ataków, oprócz określenia ich rodzajów na karcie Intrusion Detection, wymaga dodatkowo ustawienia alertów (Monitoring | Alerts), które określą, jaką akcję serwer ma podjąć w przypadku ataku. Czy ma to być np. zapis w dzienniku, wysłanie wiadomości pocztowej, zamknięcie połączenia albo wyłączenie usługi.

Mechanizmy Packet filtering i IP routing są ze sobą ściśle powiązane. Zaznaczenie opcji Enable packet filtering powoduje, że wszystkie pakiety nadchodzące do serwera z zewnątrz są automatycznie odrzucane, chyba że zostały zdefiniowane filtry albo reguły dostępu, które zezwalają na przekazywanie konkretnych typów pakietów. Włączenie opcji IP routing przy wyłączonym filtrowaniu pozwala serwerowi ISA działać jak zwykły router i przekazywać pakiety

do wewnątrz sieci. Natomiast najlepszą konfiguracją dla serwera SBS jest włączenie IP rou-ting wraz z Packet filtering, co pozwoli zapewnić sieci bezpieczeństwo, a jednocześnie udostępniać usługi również poza siecią lokalną.

Wśród właściwości grupy IP Packet Filters dostępnych po kliknięciu Configure Packet Filtering and Intrusion Detection znajduje się także karta Packet Filters. Istotne z punktu bezpieczeństwa są opcje Enable filtering of IP fragments oraz Enable filtering IP options. Pierwsza powoduje, że odrzucane będą wszystkie pakiety, które zostały podzielone na mniejsze, ponieważ ich wielkość przekroczyła maksymalny dopuszczalny rozmiar porcji przesyłanych danych (MTU). Opcji nie należy włączać, jeżeli zamierzamy przesyłać przez zaporę dane audio lub wideo. Druga opcja odrzuca wszystkie pakiety, których nagłówek zawiera dodatkowe parametry, tzw. IP header options.

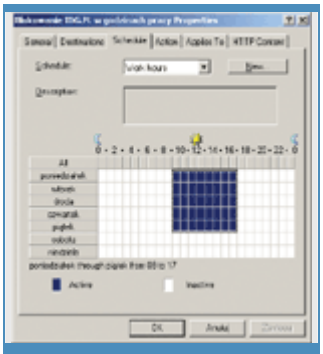
Zmiany wprowadzane przez kreatora

Po uruchomieniu Kreatora konfigurowania poczty e-mail i połączenia internetowego do konfiguracji serwera ISA wprowadzonych zostaje wiele nowych filtrów. Wśród nich filtry zezwalające na komunikację za pomocą protokołu FTP oraz odpowiadanie na zapytania programu Ping (wcześniej pokazaliśmy, jak je zdefiniować ręcznie). Pozostałe filtry umożliwiają komunikację z serwerem terminali, a więc tworzenie połączeń zdalnego pulpitu, przekazywanie ruchu SMTP serwera pocztowego, nawiązywanie połączeń VPN za pomocą PPTP, ściąganie wiadomości z internetowych serwerów POP3, a także zdalne połączenia z usługą Remote Web Workplace. Tworzony jest też dodatkowy filtr zezwalający na komunikację z serwerami WWW w Internecie. Filtr jest domyślnie wyłączony, ponieważ wszystkie przeglądarki w sieci lokalnej konfigurowane są do korzystania z serwera ISA jako serwera proxy, a nie łączenia bezpośrednio z serwerem internetowym.

W folderze Protocol Rules kreator połączenia internetowego tworzy tylko jedną regułę, Small Business Internet Access Protocol Rule, i zezwala na dostęp wszystkim użytkownikom należącym do grupy SBS Internet Users. Oznacza to, że z zasobów internetowych będą mogli korzystać tylko uwierzytelnieni użytkownicy.

Natomiast w folderze Site and Content Rules pojawiły się dwie nowe reguły. Obie zezwalają wszystkim uwierzytelnionym użytkownikom pobierać dane z Internetu. Jedna daje dostęp do wszystkich zasobów, druga tylko do serwerów z aktualizacjami systemu. Przy włączonej pierwszej regule druga jest oczywiście zbędna, ale jej obecność sprawia, że gdy zechcemy zablokować pracownikom firmy dostęp do Internetu, nie pozbawimy się tym samym możliwości aktualizowania systemu.

Blokowanie dostępu

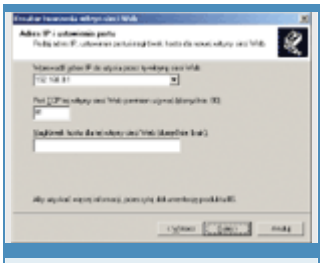


Rys. 4. Blokowanie dostępu tylko w określonych godzinach.

Dysponując takim zestawem reguł, możemy spróbować zablokować dostęp do konkretnej witryny dla określonych użytkowników. Ponieważ chcemy zablokować jedną wybraną witrynę, musimy utworzyć tzw. Destination Set, definiujący jej adres. W folderze Policy Elements wybieramy zatem Destination Sets i klikamy Create a Destination Set. Wprowadzamy nazwę, np. Witryna IDG, i ewentualnie także opis, po czym klikamy Add, wpisujemy www.idg.pl w pole Destination i klikamy OK. Następnie przechodzimy do folderu Site and Content Rules i tworzymy nową regułę, klikając Create a Site and Content Rule. W oknie kreatora wpisujemy nazwę, np. **Blokowanie idg.pl w godzinach pracy**, i klikamy Dalej. W oknie Rule Action wybieramy Deny, w kolejnym z listy Apply this rule to wybieramy Specified destination set, a w polu Name wskazujemy **Witryna IDG**. Klikamy Dalej i w polu Use this schedule wybieramy Work hours. Następnie dwukrotnie przechodzimy dalej, zatwierdzając domyślną opcję Any request i kończymy pracę kreatora. Od tego momentu użytkownicy nie mogą wchodzić na stronę www.idg.pl w godzinach 10-16 od poniedziałku do piątku, ponieważ tak został zdefiniowany plan Work hours. Oczywiście nic nie stoi na przeszkodzie, aby zdefiniować własny plan dostępu (godziny, dni), przechodząc do Policy Elements | Schedules i wybierając Create a Schedule.

Publikowanie serwisów

Preferowaną metodą udostępniania serwisów w Internecie jest ich publikowanie na serwerze ISA, w odróżnieniu od przypisania witrynie zewnętrznego adresu IP i zdefiniowania filtru pakietów zezwalającego na przekazywanie ruchu do serwera. Mechanizm publikowania wymaga, aby udostępnianym serwisom przypisany był adres lokalnej karty sieciowej.



Rys. 5. Nowa witryna musi nasłuchiwać na porcie 81 wewnętrznego interfejsu, ponieważ port 80 jest zajęty przez wewnętrzną stronę WWW serwera.

Podczas instalacji ISA do bazy DNS dodawany jest nowy wpis o nazwie publishing i adresie IP lokalnej karty sieciowej. Zgłoszenia przychodzące na zewnętrzny interfejs sieciowy odbiera serwer ISA i w zależności od zdefiniowanych reguł przekazuje np. do serwera o nazwie publishing. Oczywiście może to być też dowolny inny serwer w sieci lokalnej.

W folderze Publishing znajdują się dwa kolejne foldery, Web Publishing Rules i Server Publishing Rules. Pierwszy przystosowany jest do publikowania witryn WWW (protokół HTTP), podczas gdy drugi obsługuje dowolne protokoły.

Kreator konfigurowania poczty e-mail i połączenia internetowego wprowadza do serwera ISA kilka reguł publikujących usługi, które tym samym stają się dostępne dla użytkowników zewnętrznych. Zdefiniowane reguły umożliwiają przekazywanie ruchu do poszczególnych katalogów wirtualnych domyślnej witryny WWW . Dzięki temu użytkownicy mogą zdalnie pracować za pomocą Remote Web Workplace czy korzystać z Outlook Web Access. Użytkownicy mają też dostęp do systemu pomocy a administratorzy również do raportów o stanie serwera. Reguła Business Card Publishing Rule daje dostęp do katalogu głównego witryny, a więc sprawia, że użytkownicy zewnętrzni po wpisaniu **voyager.idg.pl** zobaczą główną stronę naszego serwera. W niektórych przypadkach zaleca się jej wyłączenie, np. gdy nie chcemy afiszować się ze swoją działalnością, a zamierzamy umożliwić pracownikom firmy pracę zdalną. W takim przypadku, aby podłączyć się do Remote Web Workplace, użytkownicy będą musieli wpisać adres **voyager.idg.pl/Remote/**, zamiast korzystać z domyślnej witryny.

Z funkcji publikowania usług WWW możemy też skorzystać, udostępniając dodatkową witrynę. W tym celu przechodzimy najpierw do Menedżera IIS. Zaznaczamy folder Witryny sieci Web i z menu Akcja wybieramy Nowy | Witryna sieci Web. W kreatorze wpisujemy nazwę witryny, np. **Witryna dla klientów**, w polu Wprowadź adres IP do użycia przez tę witrynę sieci Web wybieramy adres lokalny, np. **192.168.0.1**, natomiast domyślny numer portu (80) musimy zmienić, ponieważ jest już wykorzystywany przez domyślną witrynę WWW . Wpisujemy więc np. **81**. Pole Nagłówek hosta dla tej witryny sieci Web pozostawiamy pusty, ponieważ dostęp do witryny będzie się odbywał poprzez nazwę katalogu wirtualnego dopisaną do adresu serwera. W innym razie konieczna byłaby rejestracja dodatkowej nazwy domenowej w systemie DNS.

ISA w praktyce

Maciej Zdanowicz
10 maja 2004
PC World Komputer

W kolejnym oknie wpisujemy ścieżkę do folderu na dysku, który stanowi katalog główny witryny, np. **D:\Inetpub\wwwroot\Klienci**. Następnie zezwalamy na anonimowy dostęp do witryny (pole wyboru domyślnie zaznaczone), a na kolejnym ekranie zatwierdzamy domyślne uprawnienie Odczyt i wyłączamy Uruchamianie skryptów. Klikamy Dalej i Zakończ. Następnie tworzymy katalog wirtualny. Zaznaczamy naszą witrynę i z menu Akcja wybieramy Nowy | Katalog wirtualny. W kreatorze podajemy nazwę **Informacje**, ścieżkę do folderu, np. **D:\Inetpub\wwwroot\Klienci\Informacje**, i ustawiamy prawa odczytu. Kończymy pracę kreatora i do wskazanego folderu na dysku nagrywamy pliki witryny, w szczególności

index.htm. Strona jest gotowa. Trzeba ją jeszcze tylko opublikować w serwerze ISA.

Definiując reguły zezwalające na dostęp do witryny, będziemy się posługiwali tzw. Destination Set, który określi, do jakich adresów dana reguła się odnosi. Ponieważ nie ma jeszcze Destination Set opisującego naszą witrynę, przechodzimy do Policy Elements | Destination Sets i wybieramy Create a Destination Set. W pole Name wpisujemy np. **Informacje dla klientów**. Klikamy Add i w pole Destination wpisujemy **voyager.idg.pl**, natomiast poniżej w pole Path wpisujemy **/Informacje/***. Gwiazdka na końcu powoduje, że możliwy będzie dostęp do wszystkich plików witryny. Dwukrotnie klikamy OK i mamy utworzony Destination Set.

Rys. 6. Zgłoszenia odbierane przez zewnętrzną kartę sieciową trafiają do serwera ISA, który przekazuje je do witryny wewnętrznej.

Przechodzimy do Web Publishing Rules w folderze Publishing i klikamy Create a Web Publishing Rule. Jako nazwę reguły wpisujemy np. Dostęp do informacji dla klientów. Na kolejnym ekranie w polu Apply this rule to wybieramy Specified destination set, a w polu Name poniżej - Informacje dla klientów. Kilkamy Dalej, zatwierdzamy Any request i przechodzimy dalej. W oknie Rule Action wybieramy Redirect the request to this internal Web server i wpisujemy **publishing.idg.local** jako nazwę serwera, na którym przechowywana jest strona. Zgodnie z tym, co powiedzieliśmy wcześniej nazwa publishing jest przypisana do wewnętrznej karty sieciowej. Ponieważ witryna nasłuchuje zgłoszeń na porcie 81, w pole Connect to this port when bridging request as HTTP zamiast domyślnej wartości 80 musimy wpisać **81**.

Oddzielnego komentarza wymaga opcja Send the original host header to the publishing server instead of the actual one (specified above). W naszym przypadku może pozostać niezaznaczona, ponieważ witryna nie sprawdza, spod jakiego adresu została wywołana. Aby dostać się do witryny, użytkownik wpisuje adres **voyager.idg.pl/Informacje/**. Zgłoszenie odbiera serwer ISA i przesyła je do serwera **publishing.idg.local**. Z punktu widzenia witryny zostaje ona wywołana spod adresu **publishing.idg.local/Informacje/**, ale jak powiedzieliśmy nie ma to żadnego znaczenia.

Gdybyśmy jednak zdefiniowali nazwę domenową, np. **informacje.idg.pl**, poprzez którą użytkownicy łączyliby się z witryną, to w jej właściwościach w pole Wartość nagłówka hosta musielibyśmy właśnie tę nazwę wpisać. Witryna odpowiadałaby wtedy tylko na zgłoszenia przychodzące spod adresu **informacje.idg.pl**, natomiast nie reagowałaby na zgłoszenia spod adresu **publishing.idg.local**. W takiej sytuacji zaznaczenie opcji Send the original host header. spowodowałoby ukrycie serwera ISA jako pośrednika. Z punktu widzenia witryny zgłoszenie nadeszłoby z Internetu bezpośrednio do **informacje.idg.pl**.

Po zakończeniu pracy kreatora wszystkie zgłoszenia wysyłane do **voyager.idg.pl/Informacje/** do portu 80 będą przekazywane do **publishing.idg.local/Informacje/** do portu 81 i witryna będzie widoczna w Internecie.

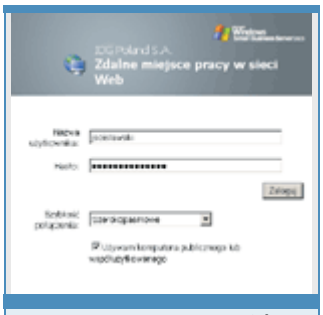
Narzędzie ISA Management może początkowo sprawiać wrażenie skomplikowanego, jednak po poznaniu zasad definiowania reguł i przeznaczenia poszczególnych folderów, a także mechanizmów, według których funkcjonuje, program szybko staje się bardzo wygodnym narzędziem do tworzenia zaawansowanych konfiguracji, w których jednocześnie udostępniane są usługi i zapewnione jest bezpieczeństwo systemu. Pracując z serwerem ISA, zwłaszcza gdy testujemy różne konfiguracje, należy pamiętać, że wprowadzane zmiany stają się aktywne dopiero po pewnym czasie (kilkadziesiąt sekund do kilku minut). Inaczej możemy wielokrotnie doznać niepotrzebnej frustracji.

Wszechobecna sieć

Jacek Ścisławski
10 maja 2004
PC World Komputer
Gwarantowany dostęp do informacji jest dla wielu firm podstawą bytu. Małe przedsiębiorstwa mogą wiele zyskać, jeśli pracownicy lub administratorzy, bez względu na miejsce pobytu lub porę dnia, będą się mogli połączyć z siecią. Grupa

usług związanych ze zdalnym dostępem zawarta w pakiecie SBS 2003 jest bardzo przydatna.

Zdalny dostęp pozwala administratorom i użytkownikom sieci na wydajniejsze wykonywanie zadań. Administrator może szybko zmienić konfigurację Windows, sprawdzić, czy serwer pracuje stabilnie, lub zareagować na awarię jednego z komponentów systemu. Na zdalnym dostępie do zasobów sieci zyskują również użytkownicy - w podróży, hotelu czy nawet w domu często możliwość sięgnięcia do serwera firmy jest niezbędna. Pakiet SBS 2003 zawiera szereg sposobów na łączenie się z siecią przedsiębiorstwa z dowolnego miejsca. Są one uruchamiane po krótkiej i nieskomplikowanej konfiguracji.



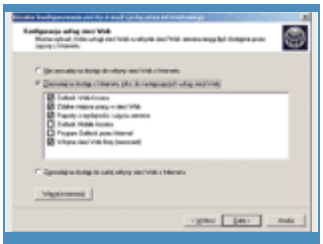
Rys. 1. Okno powitalne witryny Remote Web Workplace.

Możliwości pakietu SBS 2003 w dużej mierze zależą od połączenia z Internetem. Gdy Windows Server 2003 funkcjonuje wyłącznie w obrębie sieci lokalnej, realizacja zdalnego dostępu jest ograniczona. Trochę poprawia sytuację zainstalowanie na serwerze modemu. Dzięki temu można zestawić połączenie dial-up i sięgnąć do zasobów sieci. Niedogodnością jest w tym wypadku mała wydajność przesyłania danych. Gdy komunikacja jest nawiązywana sporadycznie, koszty nie są wysokie. Firmy zatrudniające pracowników mobilnych oczekują rozwiązań dynamicznych i wydajnych, dlatego często wymagane jest stałe połączenie z Internetem. Wówczas zalety zdalnego dostępu są najbardziej widoczne.

Zdalny dostęp do danych serwera SBS 2003 możemy uzyskiwać przy użyciu przeglądarki internetowej lub bezpośrednio po skonfigurowaniu połączenia wdzwanianego albo VPN. Wykorzystanie przeglądarki do połączenia z witryną Remote Web Workplace jest bardzo proste. Jeśli chcemy, żeby użytkownicy łączyli się przez VPN lub dial-up, musimy skonfigurować system i klienty. Oba typy zdalnego dostępu są od siebie niezależne, a ich parametry definiuje się odmiennymi narzędziami.

Remote Web Workplace

Witryna internetowa Remote Web Workplace zapewnia użytkownikom i administratorom sieci dostęp do usług pakietu Small Business Server 2003. Zawiera grupę odnośników umożliwiających odczytanie i wysłanie poczty elektronicznej, podłączenie się do pulpitu lokalnego komputera pracownika, dostęp do współdzielonych aplikacji, dostęp do intranetowej witryny firmy, przeglądanie raportów o obciążeniu serwera oraz zdalną instalację aplikacji Menedżer połączeń.



Rys. 2. Okno kreatora otwierające porty Remote Web Workplace.

Zawartość portalu zależy od przypisanych pracownikom uprawnień. Dla administratorów przygotowano stronę ułatwiającą zarządzanie serwerem. Zwykły użytkownik zobaczy stronę z odnośnikami do usług obejmujących zakres wykonywanych zadań. Ponieważ witryna jest budowana dynamicznie, brak łączy do określonych usług portalu wskazuje, że dana usługa nie została skonfigurowana lub zainstalowana na serwerze SBS.

Do połączenia z witryną zaleca się stosowanie Internet Explorera 6 z zainstalowanym uaktualnieniem SP1. Jeśli klient pracuje z inną przeglądarką lub wcześniejszą wersją Explorera, mogą wystąpić kłopoty z prawidłowym dostępem do wszystkich usług. Korzystanie z Remote Web Workplace zależy od

podania prawidłowego konta i hasła użytkownika domeny. Osoby chcące się zalogować przez przeglądarkę muszą być administratorami systemu lub należeć do grupy zabezpieczeń Remote Web Workplace Users, w przeciwnym wypadku klient zostanie odrzucony.

Instalacja i konfiguracja

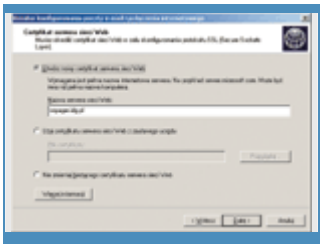
Witryna Remote Web Workplace jest instalowana łącznie z innymi narzędziami administracyjnymi w czasie instalacji serwera SBS. Dla użytkowników zewnętrznych będzie jednak dostępna dopiero po zaznaczeniu odpowiednich opcji w Kreatorze konfigurowania poczty e-mail i połączenia internetowego. Warto zachować odpowiednią kolejność instalacji

oprogramowania. Kreator uruchamiamy po zainstalowaniu serwera ISA. W innym przypadku będziemy musieli włączać go dwukrotnie. Jeżeli korzystamy z zapory podstawowej (RRAS), kreator przypisze odpowiednie reguły dostępu do witryny. Instalacja zapory firm trzecich może przysporzyć nieco więcej kłopotu. Trzeba pamiętać o otwarciu odpowiednich portów, standardowo są to: 80, 443, 3389 i 4125. Port 80 jest wykorzystywany przez protokół HTTP, 443 służy do bezpiecznej komunikacji przez SSL. Port 3389 odpowiada za połączenia przez zdalny pulpit, natomiast 4125 będzie wymagany przy usłudze RWW. Ustawienia portów są wprowadzane do serwera ISA przez kreator konfiguracji zapory. Jeśli chcemy sięgać z Internetu do wewnętrznego portalu intranetowego, musimy ręcznie skonfigurować dostęp do portu 444. Szczegółowa procedura zostanie opisana w dalszej części artykułu.

W oknie Kreatora konfigurowania poczty e-mail i połączenia internetowego, wyświetlanym po konfiguracji ustawień zapory, system proponuje wygenerowanie certyfikatu serwera WWW. Jeśli chcemy korzystać z bezpiecznej komunikacji przez SSL, musimy utworzyć nowy certyfikat. W pole nazwy serwera należy wprowadzić identyfikator wykorzystywany podczas łączenia się z systemem SBS przez Internet. Przykładową nazwą może być voyager.idg.pl.

Zawartość witryny Remote Web Workplace jest tworzona dynamicznie. Wygląd strony oraz odnośniki będą odmienne dla użytkowników i administratorów. Domyślnie administratorzy mogą się łączyć z pulpitem serwera, sprawdzać pocztę oraz przeglądać raporty wydajności i wykorzystania serwera. Dostęp do wewnętrznej witryny firmy oraz witryny pomocy technicznej (Help Desk) wymaga oddzielnej konfiguracji. Pozostali pracownicy firmy po zalogowaniu się do RWW domyślnie zyskują dostęp jedynie do poczty. Praca z portalem SharePoint jest konfigurowana oddzielnie.

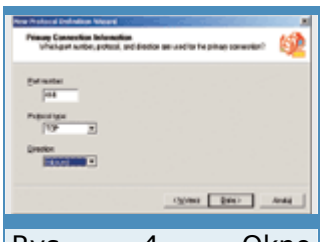
Konfiguracja dostępu do portalu intranetowego



Rys. 3. Okno kreatora służące do utworzenia certyfikatu witryny WWW.

Po zainstalowaniu pakietu SBS połączenie przez Internet z Remote Web Workplace jest możliwe, ale witryna nie oferuje wszystkich usług. Dostęp do portalu wewnętrznego wymaga kilku zmian w parametrach komponentów SBS. Pracę rozpoczynamy od modyfikacji ustawień zapory internetowej. W tym celu otwieramy menedżer serwera ISA (Start | Programy | Microsoft ISA Server | ISA Management). Pierwszym zadaniem jest utworzenie nowej definicji protokołu. Po kolei przechodzimy przez Servers and Arrays | | Policy Elements | Protocol Definitions. Po zaznaczeniu folderu Protocol Definitions z menu Akcja wybieramy Nowy, a następnie Definition.

W oknie kreatora wpisujemy nazwę zasady, np. Dostęp do intranetu 444 IN, i klikamy Dalej. Wartości 444 i IN służą jedynie do celów opisowych i wskazują numer portu oraz kierunek ruchu. Następne okno służy do wprowadzenia informacji o porcie, typie protokołu i kierunku przepływu informacji. Ponieważ naszym zadaniem jest dopuszczenie do sieci komunikacji przychodzącej i skierowanie jej do witryny intranetowej, ustawiamy: Port Number - 444, Protocol type - TCP, Direction - Inbound. Numer 444 nie jest w tym przypadku obowiązujący, stosujemy go ze względu na zgodność z dokumentacją i poradnikami Microsoftu. Po wprowadzeniu danych klikamy Dalej | Zakończ.



Rys. 4. Okno tworzenia definicji protokołu.

Utworzenie definicji protokołu umożliwia konfigurację przekierowania ruchu do witryny wewnętrznej. To konieczne, ponieważ portal intranetowy domyślnie jest związany z adresem IP lokalnego interfejsu sieciowego. Po skonfigurowaniu przekierowania komunikacja adresowana do portu 444 interfejsu zewnętrznego będzie automatycznie przesyłana pod adres wewnętrzny. Modyfikacja ustawień jest wykonywana w folderze Server Publishing Rules (Servers and Arrays | <nazwa_serwera> | Publishing). Po zaznaczeniu folderu z menu Akcja wybieramy Nowy, a następnie Rule. W pierwszym oknie kreatora wprowadzamy nazwę, np. intranet WWW, i klikamy Dalej. Następnie w pole IP address of internal server wpisujemy adres lokalnego interfejsu sieciowego, najczęściej 192.168.0.1. W polu External IP address on ISA Server umieszczamy, otrzymany od dostawcy usług internetowych, publiczny adres serwera. Po kliknięciu Dalej z listy zasad protokołów wybieramy zdefiniowaną poprzednio regułę. W naszym przykładzie jest to Dostęp do intranetu 444 IN. Okno Client Type służy do określenia źródła

komunikacji. Ponieważ najczęściej nie możemy jednoznacznie określić, skąd będą przychodziły żądania dostępu do intranetu, zaznaczamy Any request, a następnie klikamy Dalej i Finish. Jest to ostatnia modyfikacja parametrów serwera ISA. Po zamknięciu menedżera przechodzimy do modułu zarządzania serwerem IIS.

Wszechobecna sieć

Jacek Ścisławski
10 maja 2004
PC World Komputer

Rys. 5. Reguła przekierowania ruchu do witryny intranetowej.

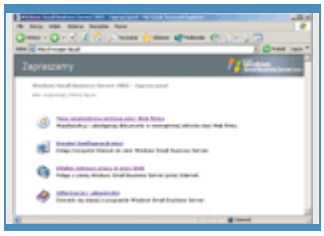
Menedżer internetowych usług informacyjnych jest dostępny w folderze Zarządzanie zaawansowane modułu Zarządzanie serwerem albo bezpośrednio z Narzędzi administracyjnych. Po uruchomieniu menedżera należy przejść do folderu Witryny sieci Web i odnaleźć w nim witrynę companyweb. Następnie z menu Akcja wybieramy Właściwości. Właściwości CompanyWeb zawierają dwie interesujące nas karty. Na początek korzystamy z domyślnie wyświetlonej karty Witryna sieci Web. W pole Port SSL wpisujemy numer portu skonfigurowany na serwerze ISA. W naszym przykładzie będzie to 444. Następnie sięgamy do karty Zabezpieczenia katalogów i naciskamy przycisk Certyfikat serwera. W kreatorze klikamy Dalej i wybieramy Przypisz istniejący certyfikat. Jeżeli opcja Przypisz istniejący certyfikat nie jest dostępna, oznacza to, że witryna ma już przypisany jakiś certyfikat. Usuwamy go zatem, klikając Usuń bieżący certyfikat i ponownie uruchamiamy okno kreatora przyciskiem Certyfikat serwera. Certyfikat utworzyliśmy już wcześniej w Kreatorze konfigurowania poczty E-mail i połączenia internetowego, więc z listy certyfikatów wybieramy właściwy obiekt. Po kliknięciu Dalej serwer proponuje 444 numer portu SSL. Dwukrotne kliknięcie Dalej oraz Zakończ kończy działanie kreatora.

Dopełnienie czynności konfiguracyjnych stanowi edycja Rejestru. Po uruchomieniu edytora poleceniem Regedit przechodzimy do klucza HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\SmallBusinessServer\RemoteUserPortal. Umieszczono w nim dwa podklucze: AdminLinks oraz KWLinks. Ich zawartość stanowi lista odnośników, jakie mają być wyświetlane administratorom i użytkownikom w witrynie Remote Web Workplace. W kluczu AdminLinks przy wpisach STS i HelpDesk zamieniamy 0 na 1. W KWLinks poprzestajemy na zmianie wpisu STS. Zamknięcie edytora kończy konfigurację dostępu do witryny firmy przez Internet.

Rys. 6. Okno konfiguracji certyfikatu witryny CompanyWeb.

Praca z Remote Web Workplace

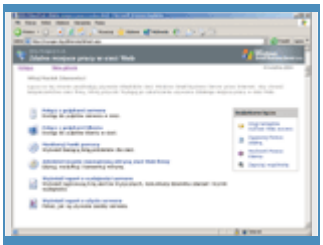
Podłączenie do witryny Remote Web Workplace wymaga jedynie wprowadzenia odpowiedniego adresu w przeglądarce internetowej. Jeśli w czasie tworzenia certyfikatu serwera WWW podaliśmy nazwę voyager.idg.pl, to właśnie ją należy wprowadzić do Internet Explorera. Poprzedzenie jej przedrostkiem https:// nie jest konieczne. Jeśli wprowadzimy samą nazwę, zostanie wyświetlona strona powitalna pakietu SBS. Po kliknięciu łącza Remote Web Workplace połączenie przez SSL zostanie zestawione automatycznie.



Pozostawienie domyślnej strony powitalnej ma pewne wady. Roboty takich wyszukiwarek internetowych, jak Google, mogą odnaleźć odnośnik do witryny zdalnego zarządzania i umieścić go w swoich bazach. Korzystający z Google, wpisując przy zapytaniu ciąg znaków "Remote Web Workplace", otrzymają odpowiedź w postaci listy odnośników do serwerów z zainstalowaną usługą zdalnego zarządzania. Najprostszym obejściem tej niedogodności jest zamiana strony powitalnej na taką, która nie będzie zawierała żadnych odnośników do usług SBS. Po tej operacji trzeba jedynie poinformować użytkowników Remote Web Workplace o pełnym adresie FQDN do zdalnego zarządzania, np. https://voyager.idg.pl/remote.

Rys. 7. Witryna powitalna pakietu SBS 2003.

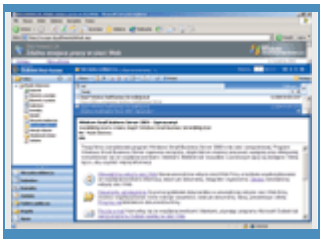
Logując się do witryny zdalnego zarządzania, użytkownik musi podać nazwę konta oraz hasło. Dodatkowo można wprowadzić informacje o przepustowości łącza i rodzaju komputera, z którego się łączymy. Pierwszy parametr ma istotne znaczenie dla działania usługi zdalnego pulpitu oraz Outlook Web Access. Jeśli przepustowość połączenia nie jest wysoka, zakres funkcjonalności obu usług zostanie ograniczony, aby uzyskać lepszą wydajność. Usunięcie znacznika z pola wyboru Używam komputera publicznego lub współużytkowanego w oknie logowania do RWW spowoduje przedłużenie limitu bezczynności sesji do 120 minut. Pozostawienie zaznaczenia spowoduje przerwanie sesji po 20 minutach bezczynności.



Rys. 8. Lista opcji zdalnego zarządzania po zalogowaniu użytkownika.

Po zalogowaniu do witryny Remote Web Workplace użytkownicy mogą sprawdzać pocztę, łączyć się ze swoimi stacjami lokalnymi oraz korzystać z intranetu. Kliknięcie odnośnika Odczytaj moją firmową pocztę e-mail (lub Użyj narzędzia Web Access w przypadku, gdy użytkownik jest administratorem) otwiera klienta programu Outlook. Korzystając z Outlook Web Access użytkownik może wykonywać takie same czynności, jak w czasie pracy ze zwykłą aplikacją. Dostępne są: Kontakty, Kalendarz, Zadania, Foldery publiczne itd. Outlook Web Access może pracować w dwóch trybach: podstawowym i zaawansowanym. Tryb wywołania witryny zależy od prędkości łącza oraz wersji Internet Explorera wybranych w czasie logowania. Przy prędkości powyżej 56 Kb/s i przeglądarce IE 6 z zainstalowanym SP1 uruchamiana jest wersja zaawansowana.

Kolejną opcją dostępną dla użytkowników Remote Web Workplace jest możliwość przejścia do witryny intranetowej firmy. Jeśli użytkownik kliknie odnośnik Użyj mojej wewnętrznej witryny sieci Web firmy (administratorzy zobaczą w tym miejscu odnośnik do zarządzania witryną), zostanie przeniesiony do portalu wewnętrznego. Zanim do tego dojdzie, należy ponownie się uwierzytelnić. Remote Web Workplace nie obsługuje przenoszenia podanych wcześniej danych logowania na witrynę SharePoint.



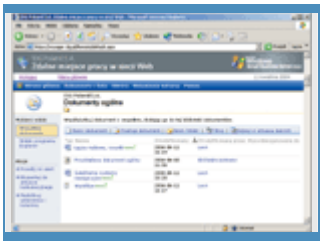
Rys. 9. Zaawansowany widok usługi Outlook Web Access.

Jeśli użytkownicy pakietu SBS będą się chcieli łączyć z siecią firmy przez wirtualne sieci prywatne (VPN) lub dial-up, należy w odpowiedni sposób przygotować ich komputery. Zadanie to realizuje Menedżer połączeń lub odpowiednio przygotowany dysk. Menedżer połączeń można pobrać bezpośrednio z witryny Remote Web Workplace, po skonfigurowaniu serwera SBS do przyjmowania połączeń zdalnych. W tym celu uruchamiamy kreator Konfiguruj dostęp zdalny. Łącze do pobrania programu Menedżer połączeń przez RWW pojawi się dopiero po zakończeniu działania kreatora. Ustawienia przypisywane w trakcie działania Menedżera połączeń zostaną opisane w dalszej części artykułu.

Użytkownicy wykonujący swoje zadania poza siedzibą firmy mogą skorzystać z opcji Połącz z moim komputerem w pracy. Pozwala ona sięgnąć z Internetu do zasobów na lokalnych komputerach użytkowników. Remote Web Workplace pośredniczy między stacją z uruchomioną przeglądarką a komputerem z sieci przedsiębiorstwa, opiera się na usłudze zdalny pulpit i dlatego możemy łączyć się jedynie ze stacjami, które pracują pod kontrolą Windows XP.

Administracja SBS 2003 przez Remote Web Workplace

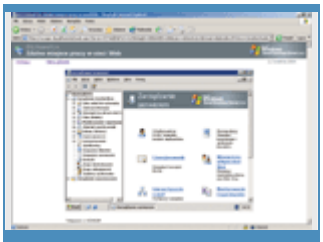
Witryna dla administratorów SBS zawiera wiele przydatnych odnośników. Oprócz dostępu do portalu SharePoint administratorzy mogą konfigurować ustawienia serwera, komputerów klienckich, odbierać pocztę i reagować na zgłoszone awarie.



Rys. 10. Widok listy dokumentów witryny SharePoint.

Opiekunów systemu SBS z pewnością najbardziej ucieszy możliwość zarządzania serwerem za pomocą opcji Połącz z pulpitami serwera. Po kliknięciu odnośnika będzie można tak pracować z pulpitem serwera, jak przy konsoli. W czasie pierwszego dostępu do usługi przeglądarka klienta pobiera i instaluje kontrolkę ActiveX, która umożliwia podłączenie się do pulpitu serwera. Po pobraniu kontrolki można wskazać, z którym serwerem chcemy się połączyć, a także określić opcje komunikacyjne: rozmiar ekranu zdalnego pulpitu, konto wykorzystywane do połączenia, wydruk na drukarkach serwera, transmisję plików pomiędzy serwerem a stacją klienta i odtwarzanie dźwięków ze zdalnego systemu. Zarządzanie Windows Server 2003 przez przeglądarkę internetową jest jedną z najwygodniejszych form zarządzania (rys. 11).

Administrator potrzebuje tylko łączności z Internetem. Inną przydatną funkcją jest skrót do monitorowania zgłoszeń awarii. Kliknięcie Monitoruj Punkt pomocy przenosi do witryny, w której użytkownicy witryny SharePoint wprowadzają informacje o problemach i usterkach. Jeśli systemy klientów sieci to Windows XP Professional, dodatkowo można się łączyć z ich pulpitami i dynamicznie reagować na zgłoszenia awarii.



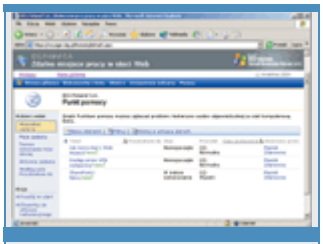
Rys. 11. Okno zdalnego pulpitu w witrynie Remote Web Workplace.

Po podłączeniu się do pulpitu serwera administrator ma dostęp do dzienników podglądu zdarzeń Windows Server 2003. Remote Web Workplace oferuje łatwiejszą metodę kontroli stanu systemu. Kliknięcie łącza Wyświetl raport o wydajności serwera przenosi na stronę zawierającą informacje o błędach i obciążeniu serwera. Pierwsza część raportu przedstawia dane sumaryczne. Klikając Szczegóły przy każdej z grup przechodzimy do sekcji szczegółowych informacji: wydajność serwera, procesy wykorzystujące najwięcej pamięci, procesy najbardziej obciążające procesor, stan sporządzania kopii zapasowej, restart usług i - co najważniejsze - lista błędów z poszczególnych dzienników systemu (rys. 13).

Wszechobecna sieć

Jacek Ścisławski
10 maja 2004
PC World Komputer

Usługi terminalowe



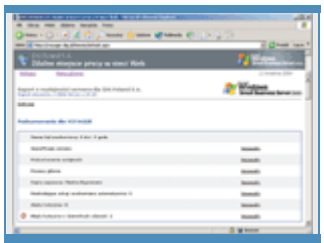
Rys. 12. Okno witryny Punkt pomocy.

Usługa zdalnego pulpitu opiera się na technologii usług terminalowych, a więc każde połączenie zdalnego pulpitu jest w rzeczywistości kolejną sesją uruchamianą na serwerze terminali. Dlatego też, ten sam użytkownik może dwukrotnie zalogować się na tej samej maszynie.

Przebywając poza firmą, możemy połączyć się z witryną internetową naszego serwera, przejść do Zdalnego miejsca pracy w sieci Web, a następnie za pomocą kontrolki ActiveX uruchamianej w lokalnej przeglądarce ustanowić nowe połączenie z serwerem terminali. Możemy także nawiązać połączenie VPN, a następnie uruchomić połączenie zdalnego pulpitu tak samo, jak byśmy znajdowali się w sieci lokalnej firmy.

Jednak żeby nawiązać połączenie zdalnego pulpitu, czy inaczej mówiąc, sesję usług terminalowych, wcale nie potrzebujemy wykorzystywać witryny internetowej czy połączenia VPN. Możemy podłączyć się bezpośrednio do serwera usług terminalowych.

Warunkiem działania takich połączeń jest odpowiednia konfiguracja zapory internetowej, która musi umożliwiać klientom zewnętrznym nawiązywanie połączeń z portem 3389 serwera. Jeżeli do konfiguracji zapory wykorzystamy Kreatora konfigurowania poczty e-mail i połączenia internetowego, to po wybraniu opcji Włącz zaporę, musimy tylko zaznaczyć pole wyboru przy pozycji Usługi terminalowe.

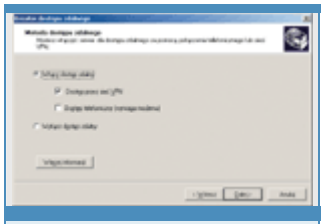


Rys. 13. Widok informacji przedstawianej przez Raport o wydajności serwera.

Z usługami terminalowymi związane są cztery karty właściwości konta użytkownika. Są to: Zdalne sterowanie, Profil usług terminalowych, Sesje i Środowisko. Pierwsza pozwala określić stopień interakcji administratora z sesją uruchomioną przez użytkownika, tj. czy do połączenia wymagana jest zgoda użytkownika i czy administrator jedynie obserwuje jego poczynania, czy też obaj obsługują pulpit wspólnie. Na drugiej karcie określimy miejsce przechowywania profilu użytkownika i zdefiniujemy dla niego folder domowy. Zakładka Sesje określa warunki, w których sesje użytkowników będą zamykane. Przyczyną może tu być np. zerwanie połączenia lub przekroczony limit bezczynności. Ostatnia zakładka Środowisko, służy do określenia aplikacji uruchamianej zaraz po rozpoczęciu sesji, a także podłączania dysków lokalnych i drukarek klienta.

Konfiguracja dostępu przez RAS

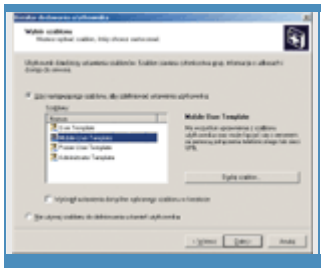
Konfiguracja usługi RAS jest alternatywną metodą uzyskiwania dostępu do danych przechowywanych przez serwer SBS 2003. Dostęp do zasobów sieci może być realizowany przez dial-up lub wirtualne sieci prywatne (VPN). W pierwszym wypadku zarówno serwer, jak i klient muszą mieć zainstalowane i skonfigurowane modemy. Nawiązywanie komunikacji odbywa się przez linie komutowane lub ISDN. Ponieważ łącza telefoniczne są bardzo rozpowszechnione, zestawienie połączenia przez dial-up nie nastręcza wielu problemów. Wadą komunikacji wdzwanianej jest niska wydajność łączy oraz wysokie koszy połączeń na dużą odległość.



Rys. 14. Okno kreatora konfiguracji dostępu zdalnego.

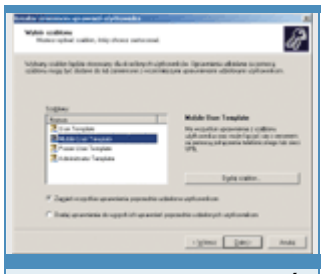
VPN pozwala na zestawienie połączenia z serwerem SBS przez sieci publiczne, takie jak Internet. Sieć pośrednicząca wykorzystywana jest jako nośnik transmisji (wirtualny kabel sieciowy). Rozwiązania oparte na VPN pozwalają wymieniać dane taniej niż dial-up, ponieważ nie trzeba korzystać z drogich połączeń międzymiastowych lub międzynarodowych. Kto chce połączyć się z serwerem SBS, musi mieć dostęp do Internetu. Ponieważ pakiety danych są przesyłane w sieciach ogólnodostępnych, mogą być podsłuchane. W celu ominięcia tego problemu prywatne informacje są kapsułkowane (owijane w inne protokoły) i szyfrowane.

Aby umożliwić użytkownikom sieci pracę przez VPN lub dial-up, trzeba uruchomić kreator połączeń zdalnych. Odnajdziemy go w module Zarządzanie serwerem, w folderze Lista zadań do wykonania albo w Internet i poczta e-mail. Po kliknięciu Konfiguruj dostęp zdalny naciskamy Dalej i rozpoczynamy konfigurację systemu. Najpierw włączamy usługę zdalnego dostępu i określamy jej typ. Do wyboru mamy VPN lub dial-up. Wybranie dial-up wymaga wskazania urządzenia, przez które będziemy się łączyć. Po zaznaczeniu VPN w następnym oknie wprowadzamy nazwę lub adres IP zewnętrznego interfejsu serwera SBS. Jeśli wprowadzimy nazwę, należy pamiętać, że musi to być w pełni kwalifikowana nazwa internetowa (FQDN), np. voyager. idg.pl. Trzeba również zadbać o jej zarejestrowanie na serwerze DNS usługodawcy internetowego, inaczej użytkownicy nie będą mogli komunikować się z systemem. Po naciśnięciu Dalej oraz Zakończ kreator kończy działanie (rys. 14).



Rys. 15. Konfiguracja dostępu przez zastosowanie szablonu Mobile User Template.

Wprowadzenie danych do kreatora trwa tylko chwilę. Mimo określenia ledwie dwóch czy trzech parametrów, modyfikacje ustawień serwera są znaczne. System włącza i konfiguruje usługę Routing i dostęp zdalny, tworzone są odpowiednie filtry pozwalające na dostęp do serwera przez zaporę lub serwer ISA 2000. Ponieważ klienty sieci muszą się komunikować z Windows Server 2003, konfigurowane są parametry nadawania adresów IP. Kreator tworzy również plik klienta Menedżera połączeń. Dzięki niemu użytkownicy zdalnych połączeń będą mogli łatwo przygotować swoje systemy do pracy. Na koniec konfigurowane są odpowiednie zasady dostępu oraz uprawnienia do komunikacji przez usługę zdalnego dostępu.

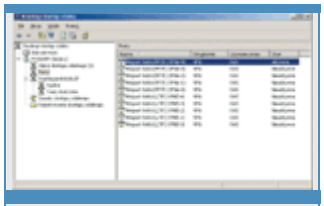


Rys. 16. Wybór szablonu do zmiany uprawnień użytkownika.

Konfiguracja uprawnień klientów sieci

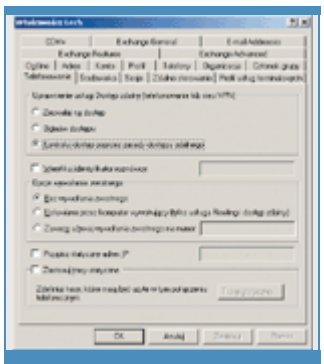
Dostęp zdalny do serwera pakietu SBS 2003 wymaga odpowiednich uprawnień. Domyślnie są konfigurowane przez kreatory. Jeśli będą kłopoty z podłączeniem do sieci, należy sprawdzić, czy dostęp jest dozwolony.

Klienty sieci otrzymują uprawnienia przez przypisanie ich kont do odpowiednich grup. W systemie SBS, dostęp przez usługę dostępu zdalnego (RAS) lub Remote Web Workplace zapewnia członkostwo w grupach Mobile Users i Remote Web Workplace Users. Przy tworzeniu nowego konta kreator Dodaj użytkownika, prosi o wskazanie, który z szablonów użytkownika będzie stanowił podstawę do określenia jego właściwości. Jeśli wybierzemy szablon Mobile User Template, wówczas zakładane konto będzie przypisane do grupy mającej dostęp przez VPN, dial-up i Remote Web Workplace (rys. 15).



Rys. 17. Okno modułu RRAS.

W podobny sposób możemy zmienić uprawnienia użytkownika. Po założeniu konta za pomocą szablonu User Template pracownik nie ma dostępu przez połączenia zdalne. Do zmiany uprawnień służy kreator Zmień uprawnienia użytkownika (rys. 16). Po jego uruchomieniu wskazujemy, który szablon ma być podstawą do zmiany uprawnień i przypisujemy mu konta klientów, np. wybieramy szablon Mobile User Template i przenosimy jego ustawienia na konto Jan Kowalski. Członkostwo w grupach jest zamieniane, a co za tym idzie, uprawnienia Jana Kowalskiego rozszerzają się o możliwość zdalnego dostępu. Szczegółowych modyfikacji ustawień dokonujemy, zmieniając właściwości konta. Po zaznaczeniu użytkownika w folderze Użytkownicy z menu Akcja wybieramy polecenie Właściwości. Okno właściwości konta zawiera karty Członek grupy oraz Telefonowanie. Na karcie Członek grupy określamy, do jakich grup należy użytkownik sieci. Jeśli korzystając z przycisku Usuń, usuniemy grupy Mobile Users oraz Remote Web Workplace Users, wskazane konto nie będzie uprawnione do zdalnego dostępu.



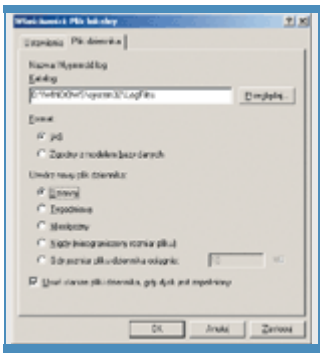
Rys. 18. Właściwości karty Telefonowanie parametrów konta.

Karta Telefonowanie jest przeznaczona do konfiguracji środowiska i uprawnień klientów zdalnych (rys. 18). Grupa ustawień Uprawnienie usługi Dostęp zdalny (telefonowanie lub sieci VPN) jest wykorzystywana do wskazania, czy konto ma dostęp czy nie. Służą do tego opcje Zezwalaj na dostęp i Odmów dostępu. Domyślne zaznaczenie parametru Kontroluj dostęp poprzez zasady dostępu zdalnego powoduje, że o wpuszczeniu użytkownika do sieci decydują zasady określone w usłudze RAS. Opcja Weryfikuj identyfikator rozmówcy pozwala na odrzucenie użytkownika, gdy próbuje się połączyć z innego numeru niż wprowadzony. Sekcja Opcje wywołania zwrotnego jest stosowana do zestawiania połączeń zwrotnych. Jeśli chcemy, żeby koszty połączenia były przenoszone na firmę, we właściwościach konta należy zaznaczyć Ustawiane przez komputer wywołujący lub Zawsze używaj wywołania zwrotnego na numer. W zależności od wskazanej opcji serwer oddzwoni pod określony przez użytkownika numer lub pod numer wprowadzony w pole Zawsze używaj wywołania zwrotnego na numer. Ostatnie dwie opcje, Przypisz statyczny adres IP i Zastosuj trasy statyczne, służą do określania parametrów adresowania IP.

Wszechobecna sieć

Jacek Ścisławski
10 maja 2004
PC World Komputer

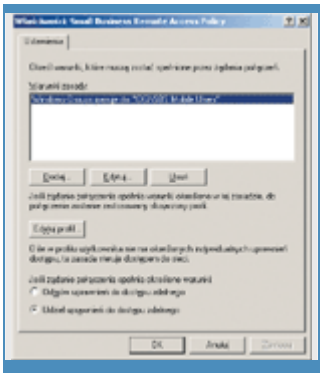
Zaawansowane monitorowanie i konfiguracja usługi RAS



Rys. 19. Okno konfiguracji dzienników.

Parametry nadawane przez kreatory pakietu SBS określają domyślne ustawienia usługi zdalnego dostępu. Jeśli chcemy skonfigurować jej zaawansowane właściwości lub sprawdzić, kto jest aktualnie podłączony, musimy skorzystać z modułu Routing i dostęp zdalny. Uruchamiamy go z Narzędzi administracyjnych Windows Server 2003.

Monitorowanie aktywności zdalnego dostępu jest wykonywane przez folder Klienci dostępu zdalnego. Zaznaczenie folderu spowoduje, że w prawym panelu modułu zostanie wyświetlona lista aktualnie podłączonych klientów. Oprócz nazwy konta klienta możemy zobaczyć, jak długo korzysta z połączenia oraz ile portów zajmuje połączenie. Kliknięcie identyfikatora użytkownika prawym przyciskiem myszy udostępnia opcje przerwania połączenia, wysłania wiadomości do użytkownika oraz wyświetlenia statystycznych informacji o sesji. Kto potrzebuje więcej danych na temat zdalnego dostępu, może skorzystać z dzienników RAS. System dokumentuje pracę usługi w dziennikach Windows Server 2003 oraz plikach tekstowych. Zakres informacji przenoszonych do Podglądu zdarzeń określamy, zaznaczając ikony serwera i wybierając z menu kontekstowego polecenie Właściwości. Po wyświetleniu właściwości serwera należy przejść do karty Rejestrowanie i zaznaczyć wymagany zakres zdarzeń. Dzienniki tekstowe zawierają szczegółowe informacje o wykorzystaniu usługi RAS, a ich konfigurację przeprowadza się w folderze Rejestrowanie dostępu zdalnego. Domyślnie system nie zbiera danych o pracy usługi i dopiero we właściwościach opcji Plik lokalny określamy zakres i format zapisywania danych. Jeśli na serwerze zostanie zainstalowany SQL Server, będziemy mogli dynamicznie przenosić informacje z usługi RAS do zdefiniowanej tabeli serwera. Nazwy pól i typy danych potrzebne do zakładania tabeli określa dokumentacja zdalnego dostępu.

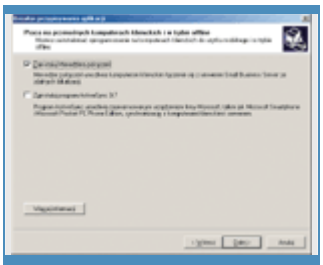


Rys. 20. Okno właściwości zasad dostępu.

Omawiając konfigurację RAS, nie sposób pominąć możliwości tworzenia zasad dostępu zdalnego. Zasady pozwalają dodatkowo wpływać na uwierzytelnienie i środowisko pracy klientów serwera. Po skonfigurowaniu usługi przez kreator zdalnego dostępu tworzona jest zasada Small Business Remote Access Policy. Jej ustawienia zezwalają na dostęp do serwera wyłącznie kontom należącym do grupy Mobile Users (rys. 20). Jeśli trzeba określić inne parametry środowiska klientów usługi, można zdefiniować własne zasady. Każda z nich pozwala na modyfikację takich ustawień, jak metoda uwierzytelnienia, poziom szyfrowania danych, przedziały czasowe dostępu do serwera, filtry wejściowe i wyjściowe, ustawienia IP itd. Listę założonych zasad możemy przeglądać po zaznaczeniu folderu Zasady dostępu zdalnego. Właściwości zasad są wyświetlane po dwukrotnym kliknięciu obiektu z listy. Ponieważ przetwarzanie zasad odbywa się w określonym porządku, ustalenie kolejności wpisów w folderze Zasady dostępu zdalnego ma fundamentalne znaczenie. Do zmiany porządku zasad służą przyciski na pasku narzędzi. Więcej informacji na temat konfiguracji zasad dostępu zawiera dokumentacja usługi RAS.

Konfiguracja klienta usługi RAS

Użytkownicy, którzy chcą się komunikować z serwerem za pomocą połączeń dial-up lub VPN, muszą mieć odpowiednio skonfigurowane komputery. Jak większość procedur konfiguracyjnych pakietu SBS, również przygotowanie stacji klienta do zdalnej pracy zostało maksymalnie uproszczone. Klient usługi RAS może skorzystać z programu Menedżer połączeń lub dyskietki instalacyjnej zdalnego połączenia.



Rys. 21. Okno kreatora przywiązania aplikacji.

Sposób instalacji aplikacji Menedżer połączeń zależy od tego, czy klient jest podłączony do sieci lokalnej, czy nie. Najprostszą metodą dostarczenia programu do systemów użytkowników jest przypisanie aplikacji do konta komputera. Po uruchomieniu modułu Zarządzanie serwerem przechodzimy do folderu Komputery klienckie. Po zaznaczeniu konta komputera, np. Redakcja01, z menu Akcja wybieramy Przypisz aplikacje do tego komputera. W uruchomionym kreatorze klikamy dwukrotnie Dalej. W oknie Praca na przenośnych komputerach klienckich i w trybie offline zaznaczamy opcję Zainstaluj Menedżera połączeń (rys. 21). Następnie, po kolei naciskając Dalej, kończymy pracę kreatora. Podczas następnego logowania użytkownika do stacji roboczej powinien zostać zainstalowany Menedżer połączeń. Jeśli klientami zdalnego dostępu będą systemy starsze niż Windows XP i Windows 2000, musimy zainstalować program ręcznie. Aplikacja jest dostępna przez udostępnienie ClientApps. Po otwarciu udziału przechodzimy do folderu Connection Manager i dwukrotnie klikamy plik sbspackage.exe. Jeśli stacja klienta znajduje się daleko od sieci lokalnej, program można pobrać bezpośrednio z witryny Remote Web Workplace, klikając skrót Pobierz Menedżera połączeń. Inną metodą jest wygenerowanie dyskietki instalacyjnej. Skrót do kreatora dyskietki jest umieszczony w folderze Internet i poczta e-mail modułu Zarządzanie serwerem.

Rys. 22. Okno połączenia z SBS 2003.

Rys. 23. Podłączenie pulpitu zdalnego przez VPN.

Instalacja programu jest prosta i wymaga jedynie uruchomienia pliku wykonywalnego. Jeżeli Menedżer połączeń dotarł do stacji przez przywiązanie aplikacji do komputera, będzie zainstalowany automatycznie. Nawiązanie połączenia z serwerem SBS 2003 polega na kliknięciu skrótu Połącz z serwerem Small Business Server i wpisaniu konta oraz hasła użytkownika.

Zdalny pulpit przez RAS

Jedną z najważniejszych zalet połączeń RAS jest możliwość zarządzania serwerem z każdego miejsca wyposażonego w łącze telefoniczne lub internetowe. Podobnie jak w przypadku usługi Remote Web Workplace, po nawiązaniu łączności z serwerem administrator może uruchomić zdalny pulpit.

Do uruchomienia usługi zdalnego pulpitu potrzebujemy połączenia zdefiniowanego przez program Menedżer połączeń oraz programu Podłączanie pulpitu zdalnego. W przypadku klientów pracujących pod kontrolą systemu Windows XP aplikacja Podłączanie pulpitu zdalnego jest umieszczona w folderze Programy | Akcesoria | Komunikacja. Przed uruchomieniem programu musimy nawiązać połączenie. Następnie uruchamiamy aplikację i wprowadzamy adres IP lub nazwę FQDN serwera.

Przed naciśnięciem przycisku Podłącz należy ustawić właściwości komunikacji. Przycisk Opcje ukrywa grupę parametrów połączenia związanych z optymalizacją wydajności, parametrami ekranu, klawiatury, portów, drukarek oraz dźwięku.

SBS jako magazyn danych

Tomasz Kopacz
10 maja 2004
PC World Komputer
Jednym ze składników SBS 2003 w wersji Premium jest SQL Server 2000. Baza danych to naturalny ''pojemnik'' na wszelkie dane przedsiębiorstwa, a w przypadku SQL Servera wcale nie potrzeba bardzo dużej wiedzy, żeby ją wykorzystać.

Właściciele małych firm mogą się zastanawiać, czy w ogóle zdołają wykorzystać taką bazę. SQL Server to jednak bardzo uniwersalny system baz danych, a przy tym od wielu lat uważany za jeden z prostszych w użyciu. W wielu przypadkach jest niemal "samozarządzający".

Po co mi SQL Server?

Żeby odpowiedzieć na to pytanie, trzeba dokładnie zbadać różnice pomiędzy bazą plikową a silnikiem SQL. W przypadku bazy plikowej to komputer kliencki otwiera plik i wykonuje na nim operacje. Jeśli na przykład baza MDB (Access) jest udostępniona wielu użytkownikom, to w istocie prędkość działania całego rozwiązania zależy od przepustowości sieci oraz najwolniejszego komputera, który używa tej bazy (najwolniejszego komputera klienckiego). Serwer jest tylko serwerem plików i jego moc obliczeniowa jest używana w minimalnym stopniu. W momencie wykonania operacji klient otwiera plik (np. na udziale sieciowym) i samodzielnie przeprowadza modyfikację.

W przypadku prawdziwego serwera SQL przebiega to zupełnie inaczej. Serwer oczekuje na polecenia przesyłane ze stacji klienckich. Po otrzymaniu polecenia wykonuje je, a do klienta przesyła wynik. W ten sposób to serwer zajmuje się obsługą plików bazy danych i odpowiednią optymalizacją polecenia, np. z wykorzystaniem indeksów. Cała operacja wykonywana jest na serwerze, a klient otrzymuje tylko wynikowy zbiór rekordów i dlatego może się zająć przetwarzaniem otrzymanych danych, w pełni wykorzystując swoje zasoby, np. pamięć, procesor itp.

SQL Server jako platforma

SQL Server może służyć jako gotowa platforma wielu różnych zastosowań. Po pierwsze, coraz więcej programów wykorzystuje motor MSDE - bezpłatną edycję SQL Server o nieco ograniczonych możliwościach. Ponieważ MSDE jest całkowicie zgodne z "dużą" bazą danych, aplikacje korzystające z MSDE mogą być łatwo przenoszone (praktycznie dotyczy to tylko plików LDF i MDF) na pełny silnik, pozbawiony ograniczeń wersji bezpłatnej.

Rys. 1. SQL Server, nieodłączny składnik systemu IT nowoczesnej firmy.

Dzięki temu, że SQL Server bez problemu współpracuje z takimi programami, jak Access czy Excel, można użyć go jako platformy do samodzielnego tworzenia prostych aplikacji obsługujących działalność przedsiębiorstwa. W Internecie jest bardzo dużo informacji związanych z praktycznym wykorzystaniem tej bazy.

Często SBS wraz z SQL jest najtańszym sposobem nabycia systemu SQL Server nawet po to, żeby uruchomić dedykowany system na tej platformie.

Również najnowsza wersja programu Płatnik może do przechowywania danych wykorzystywać MSDE. Można taką bazę przenieść na SQL Server (który działa na serwerze SBS) lub po prostu zainstalować go tak, żeby wykorzystywał pracujący już serwer. Pozwoli to na przykład. zarządzać bazą przy użyciu standardowych narzędzi administracyjnych, łatwo tworzyć raporty czy kopie zapasowe.

Na jednym serwerze może działać równolegle wiele instancji bazy SQL Server, co nawet w przypadku SBS może być czasami przydatne. W standardowej instalacji SBS 2003 tworzona jest np. instancja odpowiadająca za monitorowanie serwera. Inny wykorzystywany jest do działania SharePoint Services. Można też doinstalować kolejną, główną instancję, na której będzie działać oprogramowanie obsługujące firmę albo będą tworzone własne bazy.

Instancje są przy tym niemal separowane. Można je niezależnie konfigurować, ustalać parametry działania, wstrzymywać albo uruchamiać ponownie itp.

Możliwości SQL Servera

Podstawą działania baz relacyjnych jest zbiór danych. Wszystkie operacje wykonywane przez silnik bazodanowy są w rzeczywistości przeprowadzane na zbiorach. Jeżeli trzeba zaktualizować dane w bazie, to programista musi określić (przy użyciu warunków) zbiór danych, których ta aktualizacja dotyczy. Podobnie przebiega wybór danych: określane są zasady "przecinania" zbiorów, które wpływają na ostateczny wynik.

Baza relacyjna i T-SQL

SQL Server ma bardzo bogate możliwości programowania, tj. tworzenia tzw. procedur (czy funkcji) przechowywanych działających po stronie serwera. Tego typu programy są pisane w języku T-SQL (który w istocie jest nadzbiorem standardowego SQL i zawiera wiele udogodnień dostosowanych do bazy Microsoftu). Można definiować zmienne odpowiadające zbiorom danych, iteracyjnie przechodzić po wynikach itp. Warto dodać, że w SQL 2000 można zdefiniować funkcję, która zwróci tabelę. W ten sposób dane do tabeli można wygenerować w dowolny sposób, a potem wynik działania takiej funkcji potraktować jak zwykłą tabelę SQL. Jest to bardzo pożyteczne, bo skraca i upraszcza kod prawie każdego programu.

Równocześnie SQL Server sprawdzi, czy zgromadzone dane są spójne, tzn. mają taką strukturę, jaką założył architekt bazy. W wypadku tabel można definiować relacje, które określają, że np. wartość danego pola musi wskazywać wiersz w innej tabeli (tzw. klucz obcy). Można też określać warunki, które muszą spełniać dane wstawiane do bazy (np. data przyjęcia towaru musi być wcześniejsza niż data wydania). Można definiować tabele, indeksy oraz relacje pomiędzy tabelami, a także określać, jakie warunki muszą spełniać poszczególne wartości.

Można definiować także tzw. triggery, czyli specjalne procedury wykonywane po zmianie danych w bazie, a w SQL 2000 dodatkowo zdefiniować tzw. triggery instead of, które pozwalają przechwycić standardowe operacje dopisywania, aktualizacji czy usuwania danych. To umożliwia programiście zdefiniowanie własnych zasad modyfikacji tabel, np. rejestrowanie dodatkowych informacji w momencie zmiany wartości czy modyfikowanie tego, co będzie wstawiane do bazy.

A co najważniejsze - operacje te są wykonywane automatycznie po stronie bazy i jeśli warunki zostaną dobrze określone, dane nie mogą stać się niespójne. Bez względu na to, czy zostaną wprowadzone do tabel ręcznie (np. przy użyciu widoku siatki w Accessie) czy zaimportowane z jakiegoś pliku, zawsze przed dodaniem lub modyfikacją będą sprawdzone.

Z pojęciem baz danych wiąże się także pojęcie transakcji. Transakcja ma cztery podstawowe cechy, tzw. ACID: jest atomowa (jednostkowa), spójna, izolowana i trwała. Innymi słowy, operacja wykonywana na SQL Server albo zakończy się sukcesem i baza będzie spójna (wszystkie dane są prawidłowe) albo w całości zostanie wycofana w celu przywrócenia spójnego stanu sprzed modyfikacji. Dzięki temu, jeśli projekt bazy był prawidłowy, aplikacja pracuje na prawidłowych danych.

Tworząc rozwiązanie do SQL Servera, programista może zamknąć ciąg operacji w transakcji i wtedy albo cały dany ciąg czynności przebiegnie prawidłowo albo w bazie nic się nie zmieni. W SQL Serverze nie ma mowy o reindeksowaniu bazy po zaniku zasilania, co jest zmorą wielu aplikacji opartych na bazach plików.

W przypadku awarii serwer po restarcie analizuje plik LOG, automatycznie przywraca spójny stan bazy i na przykład wycofuje nie do końca zatwierdzone transakcje. W przypadku baz plików właśnie awarie są największym problemem, bo nie wiadomo, jak przywrócić spójny stan plików przechowujących dane.

Wyszukiwanie pełnotekstowe
Bardzo ciekawym mechanizmem w SQL Serverze jest tzw. wyszukiwanie pełnotekstowe (full text search). Pozwala ono - w uproszczeniu - znaleźć rekordy pasujące do określonego ciągu znaków (w pewnym sensie podobnie działają wyszukiwarki internetowe). Dzięki FTS nie trzeba stosować wzorców z symbolami wieloznacznymi (operator LIKE itp.), które dodatkowo spowalniałyby samo wyszukiwanie (wymagają więcej obliczeń). Indeks pełnotekstowy to struktura, która znajduje się obok bazy i musi być okresowo aktualizowana oraz synchronizowana z bazą. Pojedynczy indeks może obejmować wiele pól w tabelach. Właśnie dlatego operacja typu: znajdź wszystkie elementy dotyczące "Adam Mickiewicz Pan Tadeusz Jankiel" jest bardzo prosta do wykonania i sprowadza się niemal do jednego wywołania funkcji T-SQL. Dzięki odpowiedniemu zdefiniowaniu indeksów pełnotekstowych wyszukiwanie będzie dotyczyć wszystkich pól, które mogą zawierać potrzebne informacje. Możemy też nakładać warunki, które określą, że bardziej istotne wyrazy powinny być położone blisko siebie, albo podawać pewne frazy, które mogą być używane wymiennie. W szczególnych przypadkach możemy nawet wyszukiwać w następujący sposób: znajdź wiersze zawierające w którymkolwiek polu tekstowym określony tekst.

SBS jako magazyn danych

Osoby, które znają SQL i wiedzą, jak konstruuje się tak rozbudowane warunki przy użyciu zwykłych poleceń SELECT, zdadzą sobie sprawę, jak wiele ułatwia mechanizm wyszukiwania pełnotekstowego.

Zwracając zestaw wyników, może on także zwrócić liczby określające stopień podobieństwa do poszukiwanego tekstu. Wszystko to sprawia, że jeżeli np. projektujemy witrynę, która ma umożliwiać wyszukiwanie w treści artykułów czy w dokumentach, to FTS bardzo taki projekt uprości. A jest dostępny jako standardowy składnik bazy SQL Server.

Jedną z ważniejszych cech wyszukiwania pełnotekstowego są moduły dostosowujące je do potrzeb konkretnego języka - definiują np. fleksję, krótkie spójniki itp. Niestety, nie ma takich modułów do języka polskiego, ale jeżeli podczas tworzenia indeksu wybrany zostanie "neutralny" język, to mechanizm bardzo dobrze się sprawdzi w przeszukiwaniu np. opisów w języku polskim.

Integracja danych i hurtownie

Mocną stroną SQL Server 2000 jest łatwość integracji danych. W wielu przedsiębiorstwach pracują starsze aplikacje - z bazami DBF lub w innych prostych formatach. SQL Ser-ver może bez większych trudności zintegrować te informacje w swoich bazach. Innymi słowy - dzięki zgromadzeniu wszystkich danych w minihurtowni przedsiębiorstwo zyskuje potężne narzędzie do wszelkiego rodzaju analiz.

SQL Server zawiera wiele elementów pozwalających w prosty sposób przenosić informacje pomiędzy różnymi źródłami danych. Obsługiwane są wszystkie bazy, do których jest sterownik ODBC. Można bez problemu interpretować pliki tekstowe, arkusze Excela czy bazy plikowe - MDB/DBF. Co więcej, podczas analizy importowanych formatów automatycznie może być generowana odpowiednia struktura w SQL. Specjalne kreatory podpowiadają, jak dany schemat został rozpoznany i co dokładnie znajdzie się w bazie SQL Server. Tak więc trudności technicznych właściwie nie ma. Jednak w wypadku hurtowni danych bardzo ważne jest opracowanie właściwych założeń całego projektu, żeby zostały spełnione określone wymagania biznesowe.

Analiza danych za pomocą OLAP

SQL Server 2000 zawiera także serwer OLAP, przeznaczony do wielowymiarowej analizy danych. Tu warto podkreślić różnicę pomiędzy bazą relacyjną a bazą OLAP. Baza relacyjna

zwykle jest systemem typu OLTP, gdzie rejestrowane są dokumenty biznesowe dotyczące operacyjnego funkcjonowania firmy. W przypadku bazy OLAP, na podstawie danych operacyjnych powstaje specjalna struktura - kostka, która upraszcza analizę tych informacji. Zwykle analizy OLAP przeprowadzane są po zgromadzeniu danych w hurtowni, ale można np. bezpośrednio zasilać kostkę danymi z systemu sprzedaży.

Dużą zaletą OLAP w SQL Server jest prosta konfiguracja. Specjalny kreator pozwala administratorowi wskazać tabelę faktów, określić wymiary kostki oraz podać miary, które określą, jakie współczynniki mają być analizowane. Po kilku krokach otrzymana zostanie gotowa kostka OLAP, którą można analizować np. przy użyciu Excela (tak jak zwykle pracuje się z tabelą przestawną). Jeżeli trzeba zmienić definicję kostki, specjalny projektant pozwala łatwo modyfikować strukturę, a równocześnie przeglądać wyniki, czyli dane reprezentowane przez określone przekroje kostek.

Wszystko to sprawia, że SQL Server 2000 naprawdę oferuje coś, co można nazwać Business Intelligence dla ludzi, a w każdym razie BI, które nie wymaga dużych inwestycji ani skomplikowanych operacji administracyjnych.

Warto dodać, że OLAP i świat relacyjny to praktycznie dwa różne obszary działania - z innymi językami programowania i innymi silnikami bazodanowymi. W SQL Server 2000 można np. z poziomu T-SQL odwołać się do bazy OLAP, ale wymaga to utworzenia tzw. referencji OLEDB, co nie jest wcale proste.

Wymagania sprzętowe

Warto się zastanowić nad wymaganiami sprzętowymi SQL Servera. W przypadku systemu SBS, licencja zezwala na instalację oprogramowania na jednym serwerze. Tak więc maszyna (w zależności od przeznaczenia), musi udźwignąć np. Exchange Server, ISA Server oraz SQL Server.

Każdy właściciel firmy musi zdecydować, jaki serwer wybiera. I zwykle głównym kryterium jest cena, tzw. markowe serwery rzeczywiście są drogie. Jednak czasem można zlecić budowę serwera dostosowanego do potrzeb danej firmy. Aby zbudować serwer z dwoma procesorami Intela (Xeon 2.4) z 1 GB RAM, dyskami SCSI 15000 RPM wystarczy 14 tys. zł. Oczywiście w takim przypadku nie dostaniemy gwarancji, jaką daje poważny producent (np. niewiele małych i średnich firm stać na gwarantowany czas naprawy), ale przy wyborze markowych części i odpowiedzialnym podejściu zbudowany serwer będzie godny zaufania.

Dobierając komponenty pod kątem SQL Servera, trzeba wziąć pod uwagę główne zastosowania systemu. Jeżeli mają to być operacje transakcyjne (np. system sprzedaży czy system FK, gdzie rejestrowanych jest dużo dokumentów operacyjnych), warto inwestować w szybki system I/O (czyli twarde dyski oraz kontroler), a prędkość procesora jest mniej ważna. W przypadku systemów analitycznych, gdzie SQL Server wykonuje rozbudowane kwerendy (lub analizy OLAP), procesor staje się ważny.

SQL Server w standardowych ustawieniach dynamicznie dobiera rozmiar używanej pamięci RAM. Jest ona ważnym elementem, wpływającym na wydajność zwłaszcza wtedy, gdy z bazy korzysta wielu użytkowników, a dodatkowo system nie jest opracowany w sposób optymalny (np. nadużywa kursorów serwerowych). Wtedy pamięć staje się bardzo istotnym czynnikiem.

W Windows 2000 procesor pracujący w technologii HyperThreading widziany był jako dwa procesory, natomiast w Windows Server 2003 jest obsługiwany w specjalny sposób. Równocześnie znacznie udoskonalono operacje I/O, a to jeden z ważniejszych czynników mających wpływ na wydajność systemu SQL Server. Zatem jeżeli przejdziemy z SBS 2000 na SBS 2003, to niemal na pewno zwiększy się wydajność serwera SQL.

SQL Server a MSDE

Oprócz pełnej wersji SQL Server 2000, Microsoft oferuje także MSDE - bezpłatną edycję silnika bazodanowego. Baza danych MSDE jest w całkowicie zgodna z silnikiem relacyjnym w SQL Server. Ma jednak pewne ograniczenia. Rozmiar pojedynczej bazy danych nie może przekraczać 2 GB (jednak tak jak w pełnym SQL Server, może ich być 32 767). Pojedyncza instancja bazy

może wykonywać równolegle pięć średnio złożonych zapytań.

MSDE nie zawiera także żadnych graficznych narzędzi administracyjnych (administrator ma do dyspozycji obsługiwany z wiersza poleceń program osql). Brak pełnych usług Analysis Services, ale jest dostępna wersja PivotTable Services (przypomina DOLAP dostępne w Excelu 2000 i nowszych). Nie ma też komponentów do wyszukiwania pełnotekstowego.

MSDE można wykorzystywać tak samo, jak pełny serwer SQL. Do tworzenia rozwiązań dobrze posłuży Access, można też pisać aplikacje w VS.NET i uruchamiać przygotowane skrypty DTS.

W standardowej edycji SBS 2003 MSDE służy m.in. do zasilania portalu Windows SharePoint Ser-vices. Jednak można też zainstalować dodatkową instancję, która będzie funkcjonowała np. jako minibaza SQL do uruchamiania aplikacji.

Zestawienie cech MS SQL

łatwa administracja,
bogaty język T-SQL, który pozwala prosto wyrazić wiele złożo
ych operacji
a zbiorach,
mechanizmy pozwalające na automatyczne dostrojenie bazy,
wygodne mechanizmy do integracji i agregacja danych z dowolnych innych źródeł (DTS, eksport, import itp.),
usługi OLAP (analiza wielowymiarowa),
wyszukiwanie pełnotekstowe,
łatwość programowania i używania,
dobra współpraca z Accessem,
platforma do wielu rozbudowanych systemów obsługujących działanie firmy.</UL< td>

Reporting Services
SBS 2003 wraz z SQL 2000 jest wygodną platformą do gromadzenia wszelkich informacji pochodzących z przedsiębiorstwa. Aby ta wiedza była użyteczna, trzeba opracować mechanizm korzystania z niej.

Problem związany ze sposobem tworzenia i dostarczania raportów dotyczy chyba każdej firmy. Tak naprawdę nie ma złotego sposobu tworzenia i dystrybucji raportów. Poza tym dane trzeba odpowiednio uporządkować, ustalić prawa dostępu, wreszcie poinformować użytkowników, że dany raport jest albo że dane się bardzo zmieniły i na przykład raport finansowy wygląda zupełnie inaczej.

SBS jako magazyn danych

Tomasz Kopacz
10 maja 2004
PC World Komputer

Microsoft udostępnił specjalne narzędzie, które pomaga generować raporty - zarówno w przypadku dużych firm, jak i mniejszych, które stosują SBS z SQL 2000.

Microsoft Reporting Services to zestaw usług oferujących kompletne rozwiązanie do tworzenia, zarządzania i dystrybucji raportów. Jest ściśle związany z SQL Server 2000 i może działać na tym samym serwerze, na którym pracuje SBS 2003.

Administracja, architektura i sposób działania

Definicje raportów są przechowywane centralnie, w jednej bazie konfiguracyjnej SQL Server 2000 i mogą być umieszczane w wirtualnych folderach. Aby ułatwić wyszukiwanie, administrator może dowolnie definiować foldery z raportami oraz różne widoki pokazujące

raporty, które powinny się znaleźć w danej grupie. Do zrobienia kopii zapasowej raportów (lub konfiguracji serwera) wystarczy kopia zapasowa odpowiedniej bazy SQL Server.

Do administrowania serwerem wystarczy przeglądarka internetowa, ale jest też kolekcja skryptów oraz narzędzi uruchamianych z wiersza poleceń, które pozwalają łatwo zautomatyzować często wykonywane operacje. Jednak w praktyce do zarządzania raportami, ich dystrybucją lub uprawnieniami użytkowników wystarczy przeglądarka.

Rys. 2. Query Analyzer może pokazać plan wykonania danej kwerendy SQL. Pozwala to projektantowi dokładnie zobaczyć, z jakich indeksów dane zapytanie korzysta, i odpowiednio je przeformułować, aby było wykonywane najbardziej efektywnie.

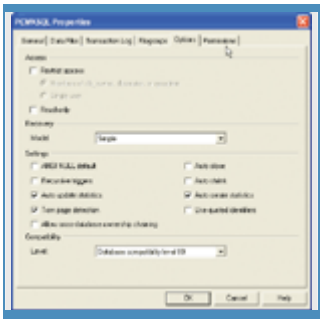
Ciekawą funkcją jest możliwość "prekonfigurowania" raportów. Jeżeli zostanie podana definicja parametrów raportu (w tym np. zakres dat zależny od aktualnej daty), to taki wzorzec można zapisać i udostępnić użytkownikom. Dzięki temu kierownik może po prostu otworzyć "miesięczny raport sprzedaży" i od razu otrzymać gotowe sprawozdanie. A równocześnie ta sama definicja może służyć do wygenerowania "podsumowania rocznego w rozbiciu na handlowców".

Reporting Services - w momencie gdy raport ma być wygenerowany - najpierw tworzą specjalny pośredni format (DataSet), który zawiera zagregowane odwołania do danych. Taki schemat jest następnie prekompilowany. Gdy raport ma zostać wygenerowany, system korzysta z gotowego wzorca (raport jest wykonywany znacznie szybciej). Równocześnie nie ma problemu z tworzeniem jednego raportu w kilku formatach wyjściowych. Można również tak skonfigurować Reporting Services, że raport jest tworzony okresowo, a użytkownik ma dostęp tylko do statycznych widoków. Co ważniejsze, definiując raport, można określić warunki, które spowodują ich unieważnienie. W ten sposób można zrezygnować z każdorazowego tworzenia raportu na życzenie i jednocześnie mieć niemal zawsze aktualny raport.

W tym rozwiązaniu raporty są tworzone zawsze po stronie serwera, natomiast brak modułu, który można uruchomić po stronie klienta. Nawet jeżeli użytkownik wyszukuje coś w raporcie, to odpowiednie żądanie wysyłane jest do serwera, a w odpowiedzi powstaje raport, w którym odpowiedni tekst jest np. podświetlony.

Moduł do definiowania raportów w Microsoft Reporting Services jest zintegrowany z Visual Studio .NET. Projektant definiuje kwerendy pobierające dane oraz wskazuje, gdzie mają być przedstawione - w układzie tabelarycznym lub macierzowym albo swobodnie rozmieszczone na stronie. Dobry pomysł to koncepcja grup czy raczej pewnych wycinków obszaru projektanta, które są traktowane jako całość i można nimi manipulować jak pojedynczym elementem.

Z ciekawostek warto dodać, że układ raportu wraz z definicjami pól może być importowany z programu Access. Microsoft Reporting Services bez problemu współpracuje z wieloma źródłami danych. Co ciekawsze, w jednym raporcie można łączyć informacje pochodzące z relacyjnej bazy SQL Server oraz z kostki OLAP (czyli z Analysis Services). Pakiet zawiera optymalizator, który zawsze odpowiednio wykona zapytanie odwołujące się do różnych baz danych.



Rys. 3. Opcje bazy danych pozwalają określić, jakie operacje automatycznie wykonuje SQL Server, a jakie pozostają w gestii administratora.

W definicji raportu można określać elementy interaktywne, które będą służyć do "zagłębiania się" w niego. Można też definiować odnośniki, których kliknięcie spowoduje otwarcie nowego raportu. Jeżeli trzeba napisać własną funkcję, to do dyspozycji projektant ma VB.NET.

Dużą zaletą jest łatwa parametryzacja raportu. Wystarczy nazwać parametry i powiązać je z danymi, a przed wygenerowaniem raportu Reporting Services poprosi użytkownika o podanie odpowiednich informacji.

Definicja raportu to plik XML zgodny z formatem opracowanym przez Microsoft (XML Report

Definition Language). Obecnie jest w zasadzie tylko jedno narzędzie do projektowania takich raportów, ale dzięki dobrej dokumentacji prawdopodobnie niedługo powstaną narzędzia branżowe, dostosowane do wymagań określonych grup użytkowników.

W Reporting Services łatwo wybiera się wyjściowy format raportów. Projektant, tworząc ich specyfikację (i zapisując ją jako RDL), nie musi się zastanawiać nad tym, w jakim formacie raport będzie dostępny. Automatycznie może być generowana prosta strona HTML, plik PDF czy sformatowany arkusz Excela. Reporting Services zdefiniują też raporty dynamiczne (użytkownik może np. rozwijać określone grupy lub wyszukiwać elementy) wykorzystujące DHTML. Jest także przeglądarka do osadzenia we własnych aplikacjach.

Microsoft SQL Server 2000 Reporting Services to łatwy do wdrożenia system raportujący dla przedsiębiorstwa, bezpłatny dla posiadaczy licencji na SQL Server.

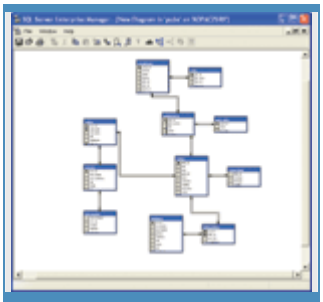
Przyspieszony kurs administracji

Instalacja systemu

SQL Server 2000 jest instalowany z dodatkowej (piątej) płyty CD, wchodzącej w skład SBS 2003 Premium. Użytkownik odpowiada na standardowe pytania instalacyjne oraz musi wybrać tzw. collation, czyli domyślny porządek sortowania znaków w bazie. Określa także zestaw znaków, który można wykorzystywać w nazwach obiektów systemowych. Jednak mimo wybrania lokalizacji polskiej nie zaleca się w nazwach tabel używać polskich znaków.

Warto dodać, że w SQL Server 2000 można wybierać porządek sortowania oddzielnie dla każdej kolumny. Dodatkowo baza w pełni obsługuje Unicode, co pozwala w jednej kolumnie przechować znaki różnych alfabetów.

Podczas instalacji SQL Server 2000 na SBS 2003 warto pamiętać o kilku sprawach. Po pierwsze, na serwerze zwykle są już dwie instancje MSDE. Jedna służy jako moduł pomocniczy narzędzi do monitoringu i administrowania (SBSMONITORING) i nie można go aktualizować do SQL Server 2000.



Rys. 4. Diagram w Enterprise Manager pozwala graficznie pokazać (lub zaprojektować) strukturę bazy.

Drugi jest wykorzystywany przez SharePoint Services. Rozważając instalację pełnej wersji SQL Server 2000, warto od razu uaktualnić instancję wykorzystywaną przez SharePoint. To zwiększy wydajność, a także pozwoli uruchomić mechanizm wyszukiwania pełnotekstowego w portalu SharePoint i znaleźć na przykład wszystkie dokumenty dotyczące określonego zagadnienia (gdy portal wykorzystuje MSDE, mechanizmy wyszukiwania praktycznie nie funkcjonują).

Usługi analityczne OLAP są instalowane oddzielnie. Na piątym CD należy odnaleźć folder SQL2000 i uruchomić program autorun.exe, po czym zainstalować Analysis Services. Po SQL trzeba jeszcze zainstalować SP3A z tego samego CD.

Narzędzia administracyjne

Główne narzędzie do administrowania bazą SQL Server to Enterprise Manager - konsola administracyjna wykorzystująca MMC. Z poziomu konsoli można zarządzać dowolną liczbą serwerów (lub instancji) SQL Server. Chcąc obsługiwać dodatkową instancję bazy SQL Server, należy dodać serwer o nazwie: <nazwa_serwera>/<nazwa_instancji> (np. SERVERSBS/SHAREPOINT).

Wszystkie operacje wykonywane w Enterprise Manager mogą być także wykonane jako skrypty z poziomu kodu T-SQL. Często (np. podczas modyfikacji schematu bazy) Enterprise Manager może automatycznie tworzyć skrypty na podstawie przeprowadzonych zmian.

Inne narzędzie do pracy z bazą SQL Server to SQL Query Analyzer, w zasadzie edytor skryptów SQL, który w specjalnym drzewie pokazuje kluczowe obiekty w bazie. Zawiera zestaw wzorców, które pozwalają np. utworzyć szkielet funkcji lub wstawiać nowy wiersz do podświetlonej tabeli.

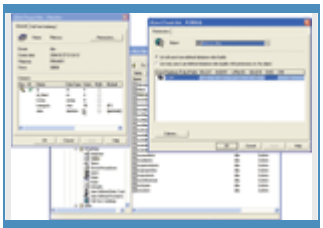
Query Analyzer pozwala także śledzić krok po kroku przechowywaną procedurę lub funkcję. W ten sposób można dokładnie sprawdzić, w jaki sposób działa zaimplementowany algorytm, podejrzeć wartości zmiennych itp. Warto dodać, że aby ten mechanizm działał prawidłowo, podczas instalacji systemu SQL Ser-ver trzeba wybrać opcjonalny interfejs debugera (rys. 2).

Należy także pamiętać o Profilerze, który potrafi podejrzeć polecenia aktualnie wysyłane do serwera. Jeżeli taki ciąg operacji zostanie przechwycony, można je przeanalizować za pomocą Index Tuning Wizard i automatycznie utworzyć indeksy, które przyspieszą daną sekwencję operacji.

Optymalizując SQL Server, warto pamiętać o jednym. SQL Server jest bazą praktycznie samooptymalizującą się. Z dokumentacji wynika, że programista podczas każdej operacji może podpowiedzieć, jaki typ blokad nałożyć na serwer lub jak dokładnie ma działać optymalizator. Jednak zwykle lepiej to zostawić samej bazie. Wtedy wybierana strategia optymalizacji jest właściwa dla danego momentu działania całego systemu komputerowego. Natomiast programista optymalizujący ręcznie zwykle bierze pod uwagę tylko własną aplikację.

Tworzenie nowej bazy

W SQL Serverze dane przechowywane są zwykle w plikach dwóch typów. Plik MDF zawiera dane z bazy, a plik LDF - dziennik transakcji, w którym zapisywane są informacje o aktualnie wykonywanych w niej operacjach. Plik MDF powinien się znajdować na innym dysku niż plik LDF - przestrzeganie tej prostej reguły może kiedyś ułatwić odzyskanie danych.



Rys. 5. Enterprise Manager pozwala zarządzać wieloma serwerami SQL. Tym narzędziem administrator może wykonać niemal wszystkie operacje.

Chcąc przenieść bazę z jednego serwera na drugi, wystarczy odłączyć (opcja Detach) bazę od serwera źródłowego, skopiować pliki MDF/LDF na docelowy serwer, po czym dołączyć je (opcja Attach) do bazy. W ten sam sposób realizuje się migrację pomiędzy MSDE a SQL Serverem.

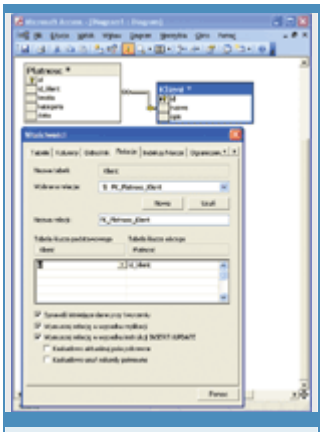
W każdej bazie SQL Server jest kilka opcji, które determinują sposób działania określonej bazy danych. Poniżej przedstawiamy ważniejsze czynniki, które wpływają na wydajność oraz zdolność systemu do automatycznego zarządzania bazą.

Opcja Auto Create Statistics/Auto Update Statistics (warto ją zawsze włączać) powoduje, że system sam okresowo uzupełnia informacje o statystycznym rozkładzie danych w bazie. Dzięki tym wiadomościom optymalizator wie, co zrobić, żeby przy określonym zestawie danych kwerendy wykonywały się optymalnie. Jeżeli ta opcja zostanie wyłączona, administrator musi co jakiś czas ręcznie uaktualniać statystyki.

Zaznaczenie opcji Auto Close powoduje, że jeżeli przez dłuższy czas nikt nie korzysta z danej bazy, to zostanie ona zamknięta, a związane z nią zasoby - zwolnione. Pozwala to zaoszczędzić pamięć serwera, ale wydłuży czas odpowiedzi bazy, gdy ktoś będzie chciał ponownie z niej skorzystać.

Zaznaczenie opcji Auto Shrink sprawia, że jeżeli z bazy zostanie usuniętych dużo rekordów, to po pewnym czasie rozmiar pliku MDF automatycznie się zmniejszy. Jednakże pojawia się problem: gdy dane są często usuwane lub dodawane, to plik stale zmienia rozmiar, co może długo trwać. Równocześnie w momencie zmniejszenia gwałtownie spadnie wydajność bazy.

Recovery Model określa zasady gromadzenia danych w pliku LDF (czyli w pliku dziennika). Gdy zaznaczona jest opcja Simple, plik dziennika przechowuje tylko niezatwierdzone transakcje. Transakcja wycofana (lub potwierdzona) zostaje automatycznie usunięta z pliku LDF. W ten sposób wielkość pliku LDF jest proporcjonalna do liczby równoległych transakcji wykonywanych na bazie danych. W przypadku trybu Full wszystkie transakcje są gromadzone i przechowywane do czasu wykonania kopii zapasowej. Zatem plik LDF stale się zwiększa. Jeżeli administrator zapomni o wykonywaniu takiej kopii i ograniczeniu pliku dziennika, wcześniej czy później cały twardy dysk zostanie zajęty. Jest jeszcze trzecia opcja - Bulk Logged. Po jej zaznaczeniu dodatkowo w pliku dziennika rejestrowane są operacje typu bulk (specjalna opcja importu wielu danych).



Rys. 6. Przykładowa struktura tabel.

Po utworzeniu bazy użytkownik może definiować struktury tabel, relacje między nimi itp. Warto wspomnieć, że w SQL Server ma narzędzie do tworzenia diagramów, które mogą gromadzić wybrane tabele. Odpowiednio dobierając widoki (np. żądając, aby były widoczne typy kolumn i relacje między tabelami), można uzyskać bardzo wygodne sposób przeglądania struktury bazy.

Enterprise Manager umożliwia także podglądanie zależności między obiektami w bazie. Jeżeli baza zawiera np. widok, z którego korzystają przechowywane procedury, to przed usunięciem go można sprawdzić, które obiekty przestaną wówczas działać. Jest to bardzo pożyteczny mechanizm, pozwalający zaoszczędzić dużo czasu.

Prawa w SQL

SQL Server może autoryzować użytkownika na dwa sposoby. W systemie zawsze dostępne jest tzw. logowanie zintegrowane: użytkownik loguje się do domeny i jeśli ma odpowiednie prawa, może uzyskać również dostęp do bazy SQL Server. Drugi tryb logowania - tzw. mieszany (mixed) - można wybrać w opcjach serwera. Pracując w tym trybie, podajemy hasło i nazwę użytkownika, a SQL Server sprawdza, prawo dostępu do serwera. Autoryzacja odbywa się na dwóch poziomach. Najpierw użytkownik uzyskuje prawo dostępu do serwera, a następnie prawo wskazanego użytkownika w bazie danych. Dopiero potem sprawdzane są uprawnienia do wykonywania poszczególnych operacji w danej bazie. Ten sam użytkownik może w jednej bazie mieć prawo db_owner (m.in. pozwala zmieniać strukturę bazy), a w innej na przykład tylko prawo do odczytu.

Oprócz tego użytkownik może mieć przypisane role, które dotyczą całego serwera, np. prawo wykonywania kopii zapasowej - pozwala mu to robić kopie bazy, ale nie zawsze zmieniać przechowywane w niej dane.

Innym sposobem autoryzacji jest przypisanie praw określonej aplikacji. Podczas łączenia się z bazą jedna z opcji to nazwa programu, który nawiązuje połączenie. Można na przykład określić, że do bazy nie ma dostępu program Excel, a ma go określony system sprzedaży.

Monitorowanie pracy serwera

Enterprise Manager pozwala zobaczyć operacje aktualnie wykonywane w bazie danych. Można monitorować połączenia z bazą, śledzić zasoby używane przez dane połączenie, założone blokady, a nawet aktualnie wykonywane polecenie T-SQL.

Po zainstalowaniu bazy SQL Server w systemowym Monitorze wydajności pojawiają się dodatkowe liczniki, które pozwalają oglądać statystyki pracy serwera. Można na przykład zbadać wydajność bufora wewnętrznego SQL albo odczytać liczbę blokad na sekundę. Poza tym w gałęzi Management programu Enterprise Manager znajdują się dzienniki bazy SQL Server. Do dziennika systemowego wysyłane są tylko błędy krytyczne, natomiast uwagi na temat operacji SQL zostają zapisane w tekstowych plikach LOG.

SQL Server Agent

SQL Server Agent to usługa administracyjna towarzysząca instancji SQL Servera. Odpowiada za okresowe wykonywanie operacji w systemie. Jeżeli na przykład co pewien czas trzeba zaimportować lub wyeksportować dane albo utworzyć kopię zapasową, to za wykonywanie takich operacji odpowiada co prawda SQL Server, ale SQL Server Agent je inicjuje. Pozwala też zdefiniować sposoby powiadamiania o sukcesie lub porażce danej operacji administracyjnej, a także określić ciąg ostrzeżeń, które będą uprzedzać administratora o potencjalnych kłopotach.

Poszczególne zadania definiuje się za pomocą programu SQL Server Agent. Ich ręczne tworzenie jest dosyć skomplikowane. Na początek warto uruchomić Database Maintenance Plan Wizard, który pozwala określić, jakie czynności będą wykonywane w celu utrzymania w pełnej sprawności określonego zbioru bazy danych, przy czym jeden plan może dotyczyć wielu różnych baz. Można na przykład wymusić sprawdzanie integralności bazy, przeliczanie statystyk, przesuwanie elementów w plikach MDF tak, aby ich ułożenie było optymalne. Oprócz tego częścią planu utrzymania może być wykonywanie kopii zapasowej. Administrator po założeniu nowej bazy powinien zawsze dołączyć ją do określonego planu utrzymania.

DTS i replikacja

Dużym atutem bazy SQL Server jest łatwość wymiany danych z dowolnym systemem bazodanowym. Elastyczny kreator importu/eksportu pozwala na przykład zaimportować z pliku tekstowego nie tylko dane, ale także strukturę. Z kolei DTS (Data Transformation Services) pozwalają przekształcać dane tak, żeby pasowały do docelowego schematu. Możliwościom importu i eksportu oraz usługom DTS warto się przyjrzeć dokładniej, zwłaszcza że jest specjalny projektant, który pozwala skonstruować rozbudowany pakiet transformacyjny z małych cegiełek i przetestować jego działanie.

SBS jako magazyn danych

Tomasz Kopacz
10 maja 2004
PC World Komputer

Ponieważ SQL Server Agent potrafi uruchamiać zadania DTS, bez trudu można zdefiniować cykliczny import danych - np. z zewnętrznego systemu przechowującego dane w plikach DBF.

Inną ciekawą możliwością bazy SQL Server jest replikacja. Zwykle jest stosowana do synchronizacji dwóch rozdzielonych serwerów bazodanowych, ale może posłużyć także do wysyłania zmian, np. do pliku Excela. W ten sposób zmienione dane byłyby automatycznie zapisywane w ustalonym folderze. W wielu przypadkach może być to bardzo wygodny mechanizm raportujący.

Procedury postępowania

SQL Server to bardzo stabilny silnik bazodanowy. Jeżeli sprzęt pracuje prawidłowo, uruchomiona instancja może działać bez przerwy. Jednak to nie wystarczy, żeby uzyskać niezawodny serwer. Bardzo ważne są też procedury, które określą sposób postępowania w przypadkach krytycznych. Nawet w małej firmie warto sprawdzić, jak dokładnie przebiega odzyskiwanie systemu serwera oraz danych z kopii zapasowej.

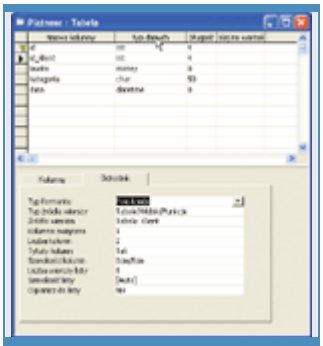
Jeżeli jakaś aplikacja krytyczna dla działania firmy korzysta z SQL, może warto utworzyć oddzielny serwer (wykorzystujący choćby MSDE), który okresowo będzie synchronizował dane z główną bazą na SBS. Pozwoli to aplikacji funkcjonować, gdy serwer SBS wymaga serwisowania lub reinstalacji albo gdy trzeba go odzyskać z kopii. MSDE nie będzie, oczywiście, pracował tak wydajnie, jak "duży" serwer, ale na czas awarii może być dobrym rozwiązaniem, a już na pewno jednym z najtańszych.

Access i SQL

Budowa aplikacji

Access i SQL Server współpracują na dwa sposoby. Po pierwsze, tabele bazy SQL Server mogą być dołączane do projektu MDB jako tabele zewnętrzne. W takim przypadku wszystkie odwołania do SQL Servera przechodzą przez kilka warstw pośrednich, ale rozwiązanie to pozwala połączyć możliwości Accessa z danymi bazy SQL Server. Tego typu tabele funkcjonują jednak zupełnie inaczej niż zwykłe tabele silnika JET.

W Accessie 2000 wprowadzono Microsoft Access Project (ADP), który służy do pisania aplikacji klient/serwer. W tym przypadku plik ADP w ogóle nie zawiera danych, a jedynie część interfejsu użytkownika oraz odwołanie do bazy w SQL Serverze. Jeżeli w takim projekcie tworzymy lub modyfikujemy strukturę bazy danych, to w rzeczywistości modyfikujemy dane na serwerze SQL. Możemy też tworzyć procedury przechowywane, funkcje, widoki, diagramy itp. Utworzenie nowej bazy w Accessie 2000 to dokładnie jeden etap kreatora - wszystkie zbędne szczegóły są ukrywane przed użytkownikiem.



Rys. 7. Definiowanie odnośnika w projekcie ADP. Baza znajduje się na SQL Serverze, ale to niczego nie utrudnia - rozwiązanie można tworzyć tak samo, jak w zwykłym projekcie MDB.

Równocześnie, jeżeli Access jest uruchomiony na tym samym komputerze, co SQL Server, to z jego poziomu możemy wykonywać podstawowe operacje administracyjne - na przykład tworzyć i odzyskiwać kopię zapasową.

Warto tylko pamiętać, że część operacji w Accesie będzie wykonywana na ściągniętym zbiorze rekordów (np. Autofiltr). Ale jeżeli np. zdefiniowana zostanie sparametryzowana kwerenda czy procedura przechowywana, to operację wykona SQL Server, a klient dostanie wyniki. Dzięki temu, że Access pozwala przekazać pewne operacje SQL Serverowi, a równocześnie zawiera bardzo wygodne mechanizmy działające po stronie klienta, względnie łatwo możemy utworzyć nawet rozbudowaną aplikację.

Załóżmy, że chcemy utworzyć prostą bazę, z dwiema tabelami do rejestrowania płatności. Jedna będzie zawierać informacje o kliencie, a druga - o dacie i kwocie płatności.

W Accesie można bez problemu zaprojektować bazę SQL Server, i to w podobny sposób, jak w programie Enterprise Manager, a nawet nieco łatwiej. Dodatkowo, jeśli używamy spolonizowanej wersji Accessa, to cały interfejs projektanta będzie dostępny w języku polskim.

Większość możliwości projektów MDB jest dostępna także w projekcie ADP. Załóżmy, że nie będziemy tworzyć skomplikowanego interfejsu użytkownika, ale chcemy zapewnić możliwość wyboru klienta podczas wprowadzania danych o płatności. Pole id_klient w tabeli Platnosc powinno więc pokazywać informacje z tabeli Klient. Analogicznie jak w plikach MDB, definiujemy w tym celu odnośnik.

Jeżeli po zdefiniowaniu takiego odnośnika za pomocą kreatora wygenerujemy formularz do wprowadzania danych (lub skorzystamy z widoku siatki), automatycznie pojawi się lista wyboru elementu, który może być wprowadzony w pole id_klient.

Oczywiście rozwiązanie przygotowane w Accessie ma mniejsze możliwości niż nowa aplikacja, napisana np. w C#, ale na pewno tworzy się je znacznie szybciej. Pozwala ono wykorzystać zalety wygodnego narzędzia, jakim jest Access, i jednocześnie pozbyć się wad wynikających ze stosowania baz plikowych.

Na marginesie warto wspomnieć o jednej z ciekawszych cech Accessa, a mianowicie stronie dostępu do danych. W zwykłej aplikacji używającej Accessa trzeba zainstalować odpowiednie biblioteki na komputerze, na którym działa. Można jednak zbudować aplikację, w której dostęp do danych nie będzie odbywał się za pomocą bibliotek, lecz poprzez stronę WWW .

Strona dostępu do danych to specjalny dokument HTML, na którym umieszczone są kontrolki wchodzące w skład Office Web Components. Mogą bezpośrednio komunikować się z SQL Serverem i np. wprowadzać informacje bezpośrednio do bazy. W Accessie projektuje się stronę HTML, określając cechy kontrolek. Po opublikowaniu takiej statycznej strony HTML na serwerze

WWW klient automatycznie może pracować z danymi w bazie SQL Server. W momencie wczytania strony do przeglądarki klienta komputer użytkownika nawiązuje połączenie z serwerem SQL. Inaczej odbywa się to przypadku stron ASP czy ASP.NET: serwer WWW komunikuje się z bazą i generuje strony przesyłane do przeglądarki.

Oczywiście tego typu strony dostępu do danych nie mogą być publikowane w Internecie, ale doskonale nadają się do tworzenia rozwiązań intranetowych - równie łatwo je zbudować, jak z nich korzystać.

Excel i OLAP

Czasami nawet mała firma chce dokładnie przeanalizować dane zgromadzone w systemach informatycznych. Jednak problem w tym, że budowa systemu analitycznego jest zwykle kosztowna i często przekracza możliwości małych i średnich firm. Jeżeli jednak na serwerze zainstaluje się Analysis Ser-vices, to budowa prostego systemu analitycznego wykorzystującego SQL Server i np. Excel staje się całkiem realna.

Serwer OLAP, czyli właśnie Analysis Services, jest komponentem systemu SQL Server, przeznaczonym do wielowymiarowej analizy danych. Dzięki niemu można na podstawie informacji zgromadzonych w bazie utworzyć tzw. kostkę, która umożliwi wygodną i rozbudowaną analizę danych np. w Excelu, który począwszy od wersji 2000 może być klientem Analysis Services.

Warto też dodać, że Excel dysponuje własnym silnikiem (tzw. Desktop OLAP), który oferuje podobne funkcje, zatem ten, kto już pracował z tabelą przestawną, dobrze zna większość koncepcji związanych z OLAP.

Szczypta teorii

Przed rozpoczęciem tworzenia struktur typu OLAP warto wyjaśnić kilka kluczowych terminów. Tabela faktów (Fact Table) to główna tabela zawierająca informacje, które chcemy analizować, np. kwoty płatności. Na podstawie danych z tej tabeli określamy, jakie informacje mają być analizowane, np. suma płatności w danym okresie, ale dodatkowo ich liczba. Są to tzw. miary (measures).

Cecha, według której generujemy przekrój kostki, to tzw. wymiar (dimension). Jeżeli mamy zamiar obserwować wysokość płatności w zadanym okresie w zależności od klienta, to kwota płatności jest miarą, a wymiarami są np. nazwa klienta i data. W przypadku niektórych wymiarów ważnym elementem jest poziom (level), określający sposób agregowania danego wymiaru. Najłatwiej to zrozumieć na przykładzie wymiaru "czas". Naturalnymi poziomami mogą być np: lata, kwartały, miesiące, dni. Definiując wymiar z takimi poziomami, możemy na przykład uzyskać sumę płatności w pierwszym kwartale, a potem zagłębić się (operacja drill-down) do poziomu dnia i sprawdzić, jak płatności wyglądały np. 3 lutego.

Oczywiście większość operacji typu OLAP można wykonać, korzystając z języka SQL, lecz wyrażenia takie są bardzo skomplikowane i trudne do skonstruowania. Natomiast silnik OLAP wraz ze specjalnymi projektantami i kreatorami bardzo upraszcza cały proces. Warto dodać, że kostka OLAP bardzo przyspiesza wykonywanie zestawień według założonych miar czy wymiarów. W zależności od typu i rozmiaru danych przyspieszenie może być nawet stokrotne i większe.

W ten sposób kosztem utworzenia pewnej struktury możemy uzyskać natychmiast wyniki analiz, a serwer SQL nie jest niepotrzebnie obciążany.

SBS jako magazyn danych

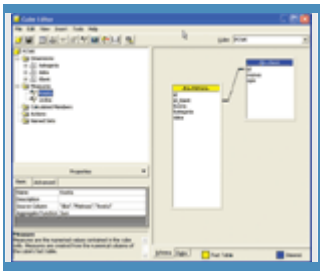
Tomasz Kopacz
10 maja 2004
PC World Komputer

Przed utworzeniem kostek analitycznych zwykle buduje się hurtownię danych, czyli strukturę gromadzącą wszystkie fakty, które później wykorzystuje się do analiz. W naszym przykładzie faza ta zostanie pominięta. Kostka będzie oparta bezpośrednio na dwóch tabelach: Platnosc oraz Klient.

Przykład praktyczny

Do zarządzania Analysis Services służy Analysis Manager. Po jego uruchomieniu musimy się połączyć z serwerem analitycznym (warto sprawdzić, czy na serwerze na pewno działa usługa MSSQLServer-OLAPServices, domyślnie wyłączona). Następnie tworzymy nową bazę (New Database) o nazwie np. PCWK. Następnie określamy źródło danych (New Data Source) i wskazujemy instancję oraz bazę serwera SQL, w której zgromadzone są dane o płatnościach. Jeżeli połączyliśmy się z serwerem, możemy zacząć definiować kostkę OLAP. Wybieramy zatem z menu podręcznego polecenie New Cube | Wizard.

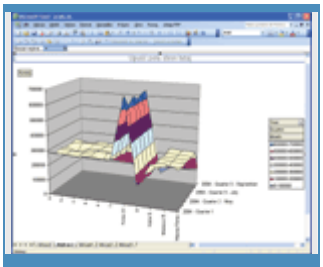
W naszym przypadku tabelą faktów jest Platnosc i ją właśnie wybieramy. Miarą natomiast jest kwota (interesuje nas głównie suma płatności, ale można też wybrać np. kolumnę Id i określić, że miarą dla tej kolumny jest liczba unikatowych wartości kolumny Id w danym zakresie). Następnie definiujemy wymiary. Mamy strukturę przypominającą schemat gwiazdy (Star Schema) i taką opcję wybieramy w kreatorze. Najpierw tworzymy wymiar pola Klient.Nazwa, a potem pola Platnosc.Data, określając jednocześnie, że jest to wymiar dotyczący czasu, czyli Time Dimension. Następnie musimy zainicjować wymiary, żeby zostały wypełnione na podstawie zawartości bazy (rys. 8).



Rys. 8. Edytor kostek pozwala graficznie zaprojektować strukturę OLAP.

Po sprawdzeniu, że kreator wygenerował prawidłową strukturę kostki, inicjujemy ją, wybierając Tools | Process Cube. Ponieważ jest to pierwsze wypełnienie kostki, najpierw musimy uruchomić kreator określający sposób przechowywania agregatów (czyli w jaki sposób kostka będzie fizycznie przechowywana w systemie). Do wyboru mamy opcje: MOLAP, ROLAP i HOLAP. Kostka typu MOLAP zajmuje najwięcej miejsca, ponieważ przechowuje wszystkie agregaty w specjalnej, wielowymiarowej strukturze. Kostka typu ROLAP wykorzystuje bazę relacyjną. Natomiast w przypadku typu HOLAP dane pozostają w bazie relacyjnej, a agregaty umieszczane są w strukturze wielowymiarowej. Zwykle najlepszym wyborem jest kostka MOLAP.

Po wybraniu typu przechowywania kostki zostanie ona wypełniona. Po zakończeniu tego etapu mamy do dyspozycji n-wymiarową (w naszym przypadku trójwymiarową) kostkę zawierającą dane o płatnościach. Dane można podejrzeć od razu w edytorze kostek (po przejściu z karty Schema na kartę Data), ale zwykle użytkownikowi najwygodniej będzie pracować z Excelem.



Rys. 9. Wykres korzysta z danych udostępnianych przez usługi analityczne, ale użytkownik pracuje tak samo, jak ze zwykłą tabelą przestawną.

Aby podłączyć kostkę Analysis Ser-vices do arkusza Excela, należy wstawić nową tabelę przestawną, wybierając Kreator tabeli i wykresów przestawnych z opcją Zewnętrzne źródło danych. Następnie, po kliknięciu Pobierz dane, należy wybrać Moduł OLAP i wskazać serwer OLAP działający w komputerze z zainstalowanym systemem Small Business Server. Po podłączeniu do usług analitycznych można wybrać kostkę (PCWK) i podobnie jak w przypadku zwykłej tabeli przestawnej, określać jej parametry - np. które wymiary mają się znajdować na osiach, jak zaprezentować podsumowania itp.

W arkuszu Excela można też zdefiniować obszar, który będzie wypełniany na podstawie dowolnej tabeli z SQL Server. W wielu przypadkach może to być bardzo wygodny sposób przeglądania danych z bazy. Zwłaszcza, że tego typu dane mogą być przetwarzane tak samo, jak zwykłe komórki Excela. Innymi słowy, możemy zdefiniować skoroszyt, którego jeden arkusz będzie służył do pobierania danych z bazy SQL Server, a drugi będzie wykonywał na tych danych określone operacje.

Rejestracja i aktywacja
Maciej Zdanowicz
10 maja 2004
PC World Komputer
Platformą operacyjną dla pakietu Microsoft Windows Small Business Server 2003 PL jest system Windows Server 2003, który - podobnie jak Windows XP - został wyposażony w mechanizm kontroli oprogramowania. Efektem stosowania tego zabezpieczenia jest konieczność aktywacji systemu. Instalując system SBS 2003, musimy zatem uzyskać klucz aktywacyjny do systemu Windows Server 2003.

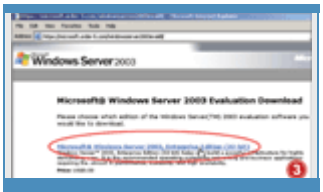
Klucz wymagany jest do zainstalowania systemu SBS 2003 oraz jego pomyślnej aktywacji, którą należy wykonać w ciągu 14 dni od daty zainstalowania i która umożliwi działanie systemu przez 180 dni. Formularz rejestracyjny znajduje się na stronie https://microsoft.order-5.com/windowsserver2003evaldl/ . Połączenie ze stroną jest szyfrowane.

Rejestracja przez Internet

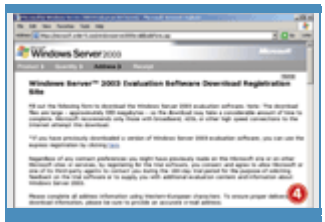
Pierwszy krok to wybór wersji systemu. Wybieramy **Microsoft(r) Windows Server 2003, Enterprise Edition (32-bit)**. Na kolejnym ekranie zatwierdzamy liczbę kopii (1) i dodajemy do koszyka, klikając Add to Basket. Następnie pojawi się podsumowanie zakupów, które powinno zawierać jedną pozycję **Microsoft(r) Windows Server 2003, Enterprise Edition (32-bit)**.

Rys. 1. Potwierdzenie wyboru wersji 32-bitowej i możliwość przeczytania licencji dla użytkownika końcowego. Klikamy przycisk Add to Basket.

Rys. 2. Sprawdzenie poprawności wyboru. Klikamy przycisk Check-out.



Rys. 3. Wybór 32-bitowej wersji Microsoft Windows Server 2003 Enterprise Edition. Aby przejść do następnego etapu, klikamy zakreślone łącze.

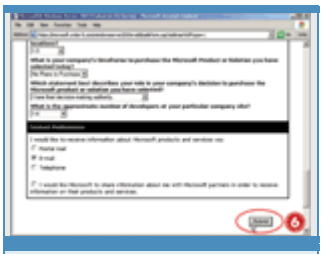


Rys. 4. Informacja o konieczności wypełnienia ankiety/formularza rejestracyjnego. Wypełniamy pola ankiety, pamiętając o podaniu poprawnego

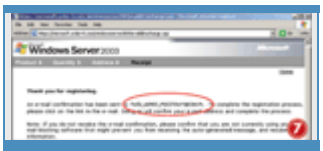
adresu e-mail, pod który zostanie przesłany kod instalacyjny oraz klucz aktywacyjny (już po zainstalowaniu).

Klikamy check-out i na kolejnej stronie wypełniamy formularz rejestracyjny. Po jego wypełnieniu warto jeszcze raz upewnić się, czy wpisany przez nas adres poczty elektronicznej jest prawidłowy, bowiem kliknięcie Submit spowoduje wysłanie listu potwierdzającego rejestrację właśnie pod tym adresem. W treści wiadomości znajdziemy odnośnik do strony internetowej, z której odczytamy klucz aktywacyjny (**Product Key**), który wpiszemy podczas instalacji systemu i który posłuży do aktywacji naszej kopii serwera na jednym komputerze. Klucz aktywacyjny dostaniemy później także pocztą elektroniczną.

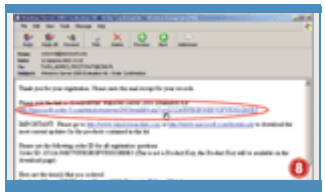
Rys. 5. Pierwsza część formularza. Wypełniamy wszystkie niezbędne pola.



Rys. 6. Druga część formularza. Wypełniamy pozostałe pola i klikamy przycisk Submit.

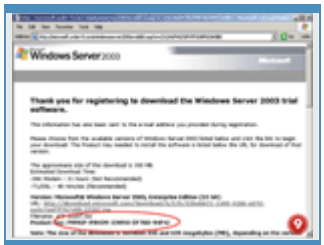


Rys. 7. Potwierdzenie przyjęcia rejestracji i weryfikacja poprawności adresu e-mail użytkownika.



Rys. 8. Ekran z aktywnym łączem do pobrania wersji ewaluacyjnej. Klikamy je tylko w celu uzyskania kodu instalacyjnego, samego obrazu ISO (550 MB).

Problemy z dostępem do formularza rejestracyjnego



Rys. 9. Ekran z informacjami i wygenerowanym, unikatowym dla każdego użytkownika

Gdyby z jakichś przyczyn nie można było wejść bezpośrednio na stronę https://microsoft.order-5.com/windowsserver2003evaldl/ , przedstawiamy całą drogę, jaką trzeba przebyć od strony głównej firmy Microsoft do formularza rejestracyjnego. Otóż po wejściu na www.microsoft.com należy z grupy Product Families po lewej stronie wybrać Servers (można też wybrać opcję Servers z rozwijanego menu górnego All Products), a następnie po prawej stronie w grupie odnośników Products by Name wskazać Windows Server.

kodem instalacyjnym. Informacje znajdujące się na tym ekranie dostępne są także w otrzymanym finalizującym e-mailu.

Na kolejnym ekranie w grupie Quick Links po prawej stronie należy wybrać Evaluation Kit (albo Get the Evaluation Kit na środku strony). Widoczna aktualnie strona powinna być zatytułowana **Windows Server 2003 Evaluation Kit**, a po prawej stronie powinna być dostępna opcja Register to Down-load the Windows Server 2003 Evaluation Kit. W tym momencie istotne jest, aby wybrać rejestrację w celu ściągnięcia programu z sieci (Download File), a nie po to, aby zamówić płyty CD (Order the CD). Po zatwierdzeniu informacji o przekierowaniu pod nowy adres za pomocą szyfrowanego połączenia znajdziemy się na stronie, do której bezpośrednio prowadzi podany wcześniej odnośnik.

Przegląd technologii ethernetowych

Nie można sobie wyobrazić sieci lokalnych bez Ethernetu. Choć ma już 30 lat, jego rozwój jest niepowstrzymany. Objaśnimy sposób działania i przyszłość związaną z Ethernetem 10-gigabitowym.

Pod koniec roku 1972 dr Robert Metcalfe wraz z kilkoma kolegami z Xerox Palo Alto Research Center (PARC - http://www.parc.xerox.com) zainstalował sieć, żeby połączyć kilka maszyn liczących Xerox-Alto - rewolucyjnych na tamte czasy prekursorów komputerów osobistych. W tej sieci, nazwanej początkowo Alto Aloha, zastosowano już protokół CSMA/CD, przejęty przez późniejszy Ethernet.

Częstotliwość przenoszenia wynosiła początkowo tylko 2,94 MHz i była zgodna z częstotliwością taktowania maszyn Alto. Dopiero w roku 1976 Metcalfe nadał sieci nazwę Ethernet. Od tego czasu Ethernet cieszy się wielką popularnością wśród administratorów sieci.

Szczególnie ceni się łatwość instalacji i konserwacji oraz niskie koszty.

Mimo wszystkich zmian, jakich Ethernet doznał od czasu naszkicowania pierwszego schematu blokowego, wciąż opiera się na tych samych zasadach.

CSMA/CD jako podstawa Ethernetu

Protokół Ethernet opiera się na komponentach multiple access, carrier sense i collision detection:

Multiple Access (MA). Wszystkie stacje ethernetowe odwołują się niezależnie od siebie do wspólnego nośnika transmisji.

Carrier Sense (CS). Jeżeli stacja ethernetowa chce wysłać dane, sprawdza najpierw, czy odbywa się inna transmisja. Jeżeli nośnik jest zajęty, stacja czeka do zakończenia transmisji oraz dodatkowo odczekuje jeszcze 9,6 µs. Jeżeli nośnik jest wolny, natychmiast rozpoczyna transmisję.

Collision Detection (CD). Podczas transmisji stacja nadająca kontroluje nośnik, żeby wychwycić ewentualne kolizje. Jeżeli w trakcie nadawania nie wykryje żadnego zakłócenia, które mogłoby być wynikiem kolizji z innym pakietem, uznaje, że pakiet został pomyślnie dostarczony.

Jeżeli stacja nadająca wykryje kolizję:
zrywa transmisję i wysyła sygnał błędu (101010... = AAAAAAAA),
czeka 9,6 ?s oraz przypadkowy okres czasu, zależny od liczby nieudanych prób wysłania tego pakietu (binary backoff) i podejmuje na nowo próbę wysłania pakietu.Taki tryb jest skuteczny i niezawodny tylko wtedy, gdy stacja nadająca jest w stanie wykryć kolizję przed zakończeniem transmisji pakietu. Należy pamiętać, że propagacja sygnału w sieci następuje ze skończoną szybkością. Warunkiem skutecznego funkcjonowania protokołu CSMA/CD jest to, aby podwojony czas przebiegu sygnału między dwiema stacjami był krótszy od czasu przesyłania najmniejszego dopuszczalnego pakietu.

Przy założeniu, że minimalna długość pakietu ethernetowego wynosi 64 bajty (= 512 bitów), maksymalny czas przebiegu sygnału (round trip delay - RTD) nie może przekroczyć 512 "czasów bitowych". Jeśli szybkość transmisji wynosi 10 Mb/s, przesłanie jednego bitu trwa 100 ns, tak więc RTD musi być krótszy niż 51,2 ?s.

Dopuszczalne opóźnienia

Zgodnie ze specyfikacją Ethernetu, różne aktywne i bierne komponenty systemu mogą wnosić opóźnienia. Tabela powyżej zawiera omawiane przykłady.

Późne kolizje

Aby określić, czy połączenie między dwiema stacjami spełnia warunki RTD, należy dodać czasy bitowe wszystkich komponentów transmisji. Suma nie może być większa od minimalnej długości pakietu w bitach (512). Jeżeli warunek ten nie jest spełniony i kolizje występują później, niż po 512 czasach bitowych, mówimy o tzw. późnych kolizjach (late collisions). Nie są one rozpoznawane przez mechanizmy kontrolne Ethernetu, które uznają, że pakiet został przesłany w całości przed wystąpieniem błędu w nośniku. Mimo to sieć działa, ponieważ protokoły wyższych warstw, na przykład TCP, zwykle żądają ponownego przesłania tych pakietów. Jeżeli w czasie następnej próby wysłania nie nastąpi kolizja ze zbyt oddaloną stacją, pakiet może być mimo wszystko skutecznie przesłany. Niemniej pogarsza to wydajność sieci, ponieważ pewna część szerokości pasma jest zużywana na retransmisję pakietów danych.

Format pakietu

Ethernet to sieć z pakietowym przesyłem danych. Oznacza to, że dane do przesłania dzielone są na mniejsze jednostki, nazywane pakietami (packets) lub ramkami (frames). Każdy pakiet sam sobie wyszukuje drogę przez sieć. Poszczególne pakiety są ponownie łączone po stronie odbiorczej.

Ethernet w pierwotnej postaci jest magistralą logiczną, nawet wtedy, gdy implementacja fizyczna nie jest magistralą. Oznacza to, że stacja wysyłająca dane "słyszana jest" przez wszystkich uczestników danej sieci. Kontroler ethernetowy stacji odbiorczej rozstrzyga na podstawie adresu docelowego, czy dana transmisja jest przeznaczona dla niego, czy nie. Wszystkie pozostałe wiadomości są ignorowane.

Adresy MAC

W celu uzyskania pewności, że w sieci nie wystąpią dwa identyczne adresy, adresy ethernetowe (nazywane również adresami MAC) kodowane są sprzętowo przez producentów tegoż sprzętu. Przydział adresów odbywa się według następującego klucza:

Większość kontrolerów ethernetowych może również odbierać pakiety i przesyłać je do wyższych warstw, które nie są dla nich przeznaczone Ten tryb pracy, zwany promiscuous, jest związany z dużym ryzykiem, ponieważ umożliwia pracę snifferów, czyli programów, które mogą obserwować ruch w całej sieci.

Od kabla koncentrycznego do skrętki w układzie gwiaździstym

Pierwotna specyfikacja Ethernetu przewidywała zastosowanie jako nośnika kabla koncentrycznego. W zależności od rodzaju, rozróżnia się gruby kabel (thick coax, 10Base-5) i cienki kabel (thin coax, 10Base-2). Ten ostatni bywa również nazywany cheapernet ze względu na niższe koszty.

Korzystając z kabla koncentrycznego, należy pamiętać, że:
Jest to implementacja magistrali fizycznej, do której przyłączono stacje. Do przyłączenia służą złączki T.
Aby rozpoznać kolizję, stacja nadawcza musi sprawdzić stan sygnału na kablu. Jeżeli panujące tam poziomy sygnału nie zgadzają się z wysłanymi sygnałami, uznaje się, że nastąpiła kolizja.
W związku z tym równie istotne jest zastosowanie właściwych końcówek kabla, pozwalających uniknąć odbić, które w pewnych okolicznościach mogłyby zostać uznane

za kolizje.Kable koncentryczne mają jednak sporo wad, np. dodanie stacji w ekspoatowanej już sieci wymaga przecięcia kabla, co oznacza, że sieć przez jakiś czas jest niedostępna.

Dlatego też w roku 1990 standard 10BaseT rozszerzono o możliwość stosowania skrętki.

Skrętka

Wykorzystanie skrętki jako nośnik pod kilkoma ważnymi względami stanowi odwrót od pierwotnych mechanizmów:
W skrętce kanał nadawczy (transmit - Tx) został oddzielony od kanału odbiorczego (receive - Rx); każdy z nich działa na własnej parze przewodów.
Gdy podczas nadawania na parze przewodów Tx odbierane są pakiety z pary przewodów Rx, uznaje się, że nastąpiła kolizja.
Do komunikacji między dwoma użytkownikami (połączenie punkt-punkt) niezbędne jest połączenie między kanałem nadawczym jednej stacji a kanałem odbiorczym drugiej stacji. Służy do tego tzw. kabel skrętkowy (crossover).
Do komunikacji między większą liczbą użytkowników konieczna jest stacja centralna - hub. W najprostszym przypadku wysyła on sygnał odebrany na parze przewodów Rxa717 jednego portu do par przewodów Tx we wszystkich innych portach. Dzięki temu każda stacja podłączona do tego huba, może odbierać pakiety na swoim kanale Rx.Ważne jest przy tym, żeby hub nie wysłał pakietów z powrotem do portu stacji nadającej, bo wówczas stacja nadająca wykryłaby aktywność na kanale odbiorczym i uznała ją za kolizję.

Jednakże rozdzielenie kanałów umożliwia pracę w trybie pełnego dupleksu, dzięki uzupełniającemu standardowi 802.3x, przyjętemu w roku 1997. Pełny dupleks polega w istocie rzeczy na tym, że zarówno na kanale nadawczym, jak i odbiorczym dozwolona jest transmisja z wyłączeniem rozpoznawania kolizji.

Światłowód w sieci szkieletowej

Wadą zarówno kabla koncentrycznego, jak i skrętki jest ograniczony zasięg transmisji. Skrętka już w odległości 100 m na tyle osłabia sygnał, że musi on być odświeżony przez wzmacniacz. Stosując kabel koncentryczny 100Base-5, uzyskuje się zasięg około 500 m (stąd 5 w oznaczeniu typu), w przypadku kabla 10Base-2 - 185 m (2 w oznaczeniu typu to 1,85 w zaokrągleniu). Im więcej wzmacniaczy w sieci, tym więcej wprowadzają opóźnień, a wówczas dochodzi do kolizji.

W związku z tym kable miedziane nie nadają się na przykład do połączenia siecią szkieletową różnych budynków na terenie kampusu uniwersyteckiego. Z tego względu przyjęto dwa kolejne standardy, które określają warunki przesyłania sygnałów optycznych w sieciach światłowodowych.

W ten sposób można uzyskać zasięg około 2 km bez stosowania dodatkowych wzmacniaczy. Z trzech zatwierdzonych standardów w praktyce rozpowszechnił się tylko jeden - 10Base-FL.

Połączenia światłowodowe można stosować tylko w połączeniach punkt - punkt, zatem 10Base-FL jest również strukturą gwiaździstą.

W stronę 100 Mb/s

Zwiększenie mocy obliczeniowej komputerów w latach dziewięćdziesiątych spowodowało wzrost zapotrzebowania na sieci szerokopasmowe. Z tego względu w roku 1995 wprowadzono standard 100Base-T o przepustowości 100 Mb/s, nazywany Fast Ethernet.

Następujące aspekty zasługują tu na uwagę:
Dozwoloną wartość opóźnienia w przesyłaniu sygnału twórcy standardu pozostawili w niezmienionej wielkości 512 czasów bitowych, ale ze względu na większą szybkość transmisji jeden czas bitowy odpowiada już tylko 10 ns, a zatem należy zwrócić większą uwagę na budżet czasowy. O ile w sieci o przepustowości 10 Mb/s sygnał pokonuje w ciągu jednego czasu bitowego (100 ns) drogę około 8 m, o tyle w sieci 100 Mb/s w kablu kat.5 jest to już poniżej jednego metra. W podobny sposób zwiększają się wymagania wobec aktywnych komponentów (zobacz "Dozwolone czasy opóźnień").
Kabli koncentrycznych nie stosuje się ze względu na ich niewystarczające właściwości elektryczne.
Transmisja za pomocą skrętki również jest trudna dla mechanizmów przesyłowych. Przyjęto w tym zakresie trzy alternatywne standardy: 100Base-Tx, 100Base-T2 i 100Base-T4. Standard 100Base-Tx wymaga zastosowania skrętki kat.5, która umożliwia przesyłanie z częstotliwością do 100 MHz.
Aby umożliwić transmisję również z wykorzystaniem starych kabli kat.3 (częstotliwość graniczna 16 MHz), przyjęto też standardy 100Base-T4 i 100Base-T2. Nie znalazły, co prawda, szerszego zastosowania, są jednak o tyle interesujące, że zastosowane mechanizmy, dzięki którym przesyła się 100 Mb/s kablem o częstotliwości granicznej 16 MHz, zostały również użyte przy okazji kolejnego zwiększania przepustowości sieci, w wersji 1000Base-T.1000Base-Tx

Założenie, że sieć z kablem kat.5 o częstotliwości granicznej 100 MHz automatycznie może przesyłać dane z szybkością 100 Mb/s, jest fałszywe.

Należy przy tym zwrócić uwagę na następujące szczególne aspekty:
W trakcie pracy odbiornik sygnałów musi się zsynchronizować ze strumieniem danych. Długie fazy identycznych sygnałów, przesyłane w paśmie podstawowym, są źródłem problemów, ponieważ nie występują zbocza sygnałów, które mogłyby posłużyć nadajnikowi do ponownej synchronizacji. Problem ten rozwiązano w standardzie 10 Mb/s przez zastosowanie kodowania Manchester. W pierwszej fazie przesyłany jest bit danych, przy czym zmiana zbocza oznacza logiczną 1. Druga faza zapewnia taktowanie w ten sposób, że musi nastąpić co najmniej jedna zmiana zbocza, co gwarantuje, że w każdej fazie nastąpi przynajmniej jedna zmiana poziomu sygnału. Wadą tego rozwiązania jest konieczność dwukrotnego zwiększenia częstotliwości.
Ponieważ w wypadku przesyłu 100 Mb/s podwojenie częstotliwości nie wchodzi w grę, strumień bitowy kodowany jest według wzoru 4B5B. Wzory są przy tym tak dobierane, że w ramach każdego bloku o długości 4 względnie 5 bitów występuje co najmniej jedna zmiana poziomu sygnału. W ten sposób strumień bitowy wydłuża się zaledwie o 25 procent, zaś wynikowa szybkość transferu wynosi 125 Mb/s.
Ponieważ częstotliwość 125 MHz jest w oczywisty sposób większa niż 100 MHz, sygnał przesyłany jest na trzech poziomach (MLT-3 - multi level transmission z poziomami -1, 0 i 1). W ten sposób można przesłać wiele bitów na symbol, a także zmniejszyć częstotliwość przenoszenia.
Częstotliwość podstawowa pustego ciągu bitowego zmniejsza się w ten sposób ze 125 MHz do jednej czwartej i wynosi teraz 31,25 MHz. Ze względu na przemieszanie zakodowanego strumienia danych (scrambling) musi jeszcze nastąpić rozdział pasma częstotliwości. W ten sposób uzyskuje się rozrzut widma mocy emitowanych sygnałów oraz jednocześnie zgodność z przepisami dotyczącymi emisji elektromagnetycznych.100Base-T4

Standard 100Base-TX można określić jako bardzo rozrzutny, ponieważ wykorzystuje tylko dwie z czterech par przewodów, z jakich składa się skrętka. Dzięki temu pozostałe pary przewodów można wykorzystać na przykład do telefonii ISDN. Ponieważ jednak takie rozwiązanie rzadko spotyka się w praktyce, zaproponowano standard 100Base-T4, w którym wykorzystane są wszystkie cztery pary przewodów.

Do przesyłu danych stosuje się trzy pary przewodów, dzięki czemu transmisja rozkłada się na trzy kanały po 33 MHz. Czwarta para przewodów służy do wykrywania kolizji. Dalsze zmniejszenie częstotliwości sygnału uzyskuje się przez zastosowanie kodowania.

W danej chwili możliwa jest tylko transmisja w jednym kierunku. Praca w trybie pełnego dupleksu nie jest możliwa.

100Base-T2

Również w standardzie 100Base-T2 przewidziano procedurę umożliwiającą przesyłanie 100 Mb/s kablem kat.3. 100Base-T2 wykorzystuje jednak tylko dwie pary przewodów, pozostałe dwie pozostawiając do dyspozycji telefonii głosowej. Dla rozwiązania tego problemu opracowano impulsową modulację amplitudy (Pulse Amplitude Modulation - PAM). Zastosowana w 100Base-T2 modulacja PAM 5x5 wykorzystuje pięć różnych poziomów (-2, -1, 0, +1, +2).

Szczególnie interesujące jest przy tym, że obie pary przewodów mogą pracować w trybie pełnego dupleksu. Uzyskano to za pomocą tzw. transceiverów hybrydowych.

Charakteryzują się one dwiema funkcjonalnościami:
W kierunku nadawania linia przenosi jednocześnie sygnał nadawania i sygnał odbioru.
Po stronie odbiorczej należy wydzielić wysłany sygnał z sygnału całościowego, aby otrzymać dane adresowane do odbiorcy.Należy jednak uwzględnić i wyeliminować za pomocą kompensacji echa (echo cancellation) odbite w przewodzie składowe wysłanego sygnału.

Tak więc ten specjalny tryb pełnodupleksowy jest ciekawym przypadkiem ewolucji w historii Ethernetu.
Do kabla koncentrycznego potrzebny jest transceiver. Podczas nadawania musi on jednocześnie kontrolować poziom sygnału na kablu, aby stwierdzić, czy jest zgodny z wysłanym sygnałem. Jeżeli poziomy zbytnio odbiegają od wysłanych sygnałów, uznawane jest to za kolizję.
Do transmisji z użyciem skrętki w standardzie 10Base-T rozdzielono kanały nadawcze i odbiorcze.
Natomiast w standardzie 100Base-T2 również w przypadku przesyłu skrętką kanały odbiorcze i nadawcze są znów wykorzystywane wspólnie, w celu uzyskania wymaganej szybkości transmisji w dostępnej szerokości pasma.Autonegocjacja

Zastosowanie dwóch różnych poziomów szybkości transmisji rodzi pytanie o kompatybilność. Na podstawie podobieństwa cech można zaprojektować grupy komunikujące się z prędkością 10 lub 100 Mb/s do wyboru. Oczywiście jest pożądane, żeby automatycznie negocjowana była największa możliwa szybkość transmisji. W tym celu w ramach standardu Ethernetu opracowano tzw. protokół autonegocjacji (Auto Negotiation Protocol - ANP), oparty na opracowanym przez National Semiconductor protokole Nway. ANP odnosi się do segmentów łączących pomiędzy dwoma uczestnikami komunikacji. Protokół ten wywoływany jest bezpośrednio w chwili inicjacji połączenia i wykorzystuje własny system sygnałów. System ten opiera się na impulsach NLP (Normal Link Pulsem), które urządzenie 10Base-T regularnie wysyła w celu kontroli połączenia. ANP wysyła ciągi sygnałów z impulsami FLP (Fast Link Pulses), których sekwencja jest identyczna z impulsami NLP. Dzięki temu urządzenia 10Base-T mogą się obejść bez ANP, gdyż rozpoznają te sygnały jako NLP. Jeżeli jednak urządzenie obsługuje ANP, to może wczytać z 16 parzystych impulsów FPL 16-bitowy kod Link Code Word, który zawiera informacje o obsługiwanych prędkościach i trybach. Może wówczas wybrać szybkość i tryb z listy kolejnych priorytetów.

Ograniczenia autonegocjacji

Przy szybkościach 10 i 100 Mb/s autonegocjacja jest opcjonalna; w standardzie 100Base obowiązuje w wypadku używania skrętki. W łączach optycznych nie jest możliwa współpraca różnych standardów ze względu na różne długości fali. W Ethernecie gigabitowym ANP jest zapisana w standardzie jako obowiązkowa.

Jeżeli urządzenie nie odpowiada na impulsy FLP, uruchamia się mechanizm wykrywania równoległego, który rozpoznaje standard transmisji na podstawie kształtu sygnału i kodowania. W takim przypadku jednak standardowo wybierany jest tryb półdupleksu.

Może to spowodować problemy, jeżeli drugie urządzenie zostało ręcznie przełączone na tryb pełnego dupleksu.

W ANP jest możliwość przekazania dodatkowych informacji na kolejnych stronach. W ten sposób autonegocjacją można też objąć standardy gigabitowe.

Pewien problem stanowi to, że wspomniana możliwość jest wykorzystywana przez niektórych producentów do zamieszczania specyficznych informacji.

Często zdarza się zatem, że pary sprzętowe różnych producentów nie tolerują się wzajemnie w trakcie ANP. W tym wypadku potrzebna jest ręczna konfiguracja.

Przełączanie

Wraz z przejściem na skrętkę zastąpiono pierwotną fizyczną strukturę magistrali architekturą gwiazdy, w której połączenia punkt-punkt przebiegają przez centralny węzeł.

W architekturze gwiazdy można zrezygnować z zasady dzielonego dostępu do kabla na rzecz znacznie wydajniejszej metody, a mianowicie przełączania:
Gdy centralny węzeł analizuje adresy źródłowe nadchodzących pakietów, z czasem "uczy się", do którego portu jest podłączona każda stacja.
Jeżeli teraz węzeł centralny odbierze na jednym z portów pakiet do "znanej" stacji, wystarczy, że prześle go tylko do portu, do którego podłączona jest stacja docelowa.
Znacznie zwiększa to szerokość pasma, gdyż stacje mogą komunikować się parami między sobą, nie wpływając na komunikację innych stacji.Należy jednak jeszcze wziąć pod uwagę dwa czynniki:

Ponieważ transmisje przechodzą przez matrycę przełącznika równolegle, jego pasmo jest dzielone. Jednak wewnątrz urządzenia można uzyskać znacznie większe szerokości pasma, które przyjmą równoległe strumienie danych.

Jeżeli ruch danych przechodzi najpierw przez określone urządzenie, np. serwer, podziałowi podlega dostępna szerokość pasma połączenia między serwerem a przełącznikiem.

Następny krok - od 100 do 1000 Mb/s

Technologia przełączania zwiększa zapotrzebowanie na szerokość pasma w odniesieniu do niektórych połączeń punkt-punkt. Gdy na przykład połączenie serwera z węzłem ma większą przepustowość, niż łączne zapotrzebowanie wszystkich klientów, ruch będzie odbywał się bez przeszkód. Zapotrzebowanie na szybką transmisję wzrosło również w zakresie sieci szkieletowych. Logiczną konsekwencją stało się zatem opracowanie standardu gigabitowego. Aby przesłać miliard bitów na sekundę jednym kablem, podjęto dwie zasadnicze decyzje:
Transmisja w standardzie 1000Base-X (IEEE 802.3z) opiera się na technikach modulacji, a zwiększenie szybkości transmisji uzyskano głównie dzięki zwiększeniu częstotliwości przenoszenia.

Natomiast w standardzie 1000Base-T (IEEE 802.3ab) zrezygnowano z bezpośredniego skalowania technologii 100Base-TX.W celu uzyskania tej szybkości transmisji w kablu kat.5 na odległość powyżej 100 m zastosowano kombinacje różnych technik, przy czym zarzucono centralne procedury standardów 100Base-T2 i 100Base-T4.

1000Base-X

Standard 1000Base-X wykorzystuje technikę modulacji 8B/10B, zbliżoną do techniki 4B5B ze standardu 100Base-X. Jeden bajt zawierający osiem bitów jest przy tym kodowany do postaci słowa 10-bitowego i dlatego szybkość transmisji danych wzrasta do 1250 Mb/s.

Nośnikiem w standardzie 1000Base-X mogą być różne rodzaje światłowodów lub kabel twinax 150 W o długości do 25 m.

1000Base-TX

Wzrost szybkości transmisji ze 100 do 1000 Mb/s w standardzie 1000 Base-TX można uzyskać według poniższego opisu. Podana kolejność jest przypadkowa.

Przyjmując za podstawę transmisję jedną parą przewodów w standardzie 100Base-T4, można wykorzystać wszystkie cztery pary przewodów. W ten sposób szybkość transmisji zwiększa się do 400 Mb/s.

Po rezygnacji z kodowania 4B5B i stałej częstotliwości przenoszenia szybkość transmisji zwiększa się do 500 Mb/s.

Zastosowanie modulacji PAM5x5 ze standardu 100Base-T2 podwaja szybkość transmisji do 1000 Mb/s, przy czym częstotliwość przenoszenia nie zmienia się. rzeba się jednak pogodzić ze zmniejszeniem o 6 dB odstępu sygnału od szumu w wyniku spadku poziomu sygnału; konieczna jest kompensata w postaci dodatkowej korekcji błędów.

Korekcja błędów oparta na modulacji TCM (Trellis-Coded Modulation) odwołuje się do kodowania splotowego, które jest powszechnie stosowane w cyfrowej łączności bezprzewodowej, a także od dawna w rozpoznawaniu mowy i obrazów. Korekcja błędów, o której mowa, jest w istocie jedynym nowym komponentem w standardzie 1000Base-T.

Jednoczesny przesył w obu kierunkach jedną parą przewodów, jak w standardzie 100Base-T2. W ten sposób uzyskuje się 1000 Mb/s w trybie pełnego dupleksu.

Od 1000 do 10 000 Mb/s

Zanim standard 1000Base-T przybrał dojrzałą postać, w marcu 1999 roku powstała grupa robocza w ramach IEEE802.3 Higher Speed Study Group (HSSG, http://grouper.ieee.org). Jej celem było opracowanie standardu transmisji 10 Gb/s. Już wówczas podjęto dwie trafne decyzje, które stały się podstawą dalszego rozwoju Ethernetu. Z jednej strony, chciano zachować sprawdzone właściwości Ethernetu. Chodziło przede wszystkim o format ramek i bezpośrednie dopasowanie do architektury 802.x, co miało umożliwić łatwe pakietowanie wolniejszych ramek ethernetowych na wyższych poziomach szybkości i bezpośrednie przejęcie technik sterowania ruchem. Ponadto specyfikacja miała umożliwiać korzystną cenowo implementację, po kosztach dwu- lub trzykrotnie niższych w porównaniu z Ethernetem gigabitowym.

Z drugiej strony, widać wyraźnie, że rozwój Ethernetu 10G idzie w kierunku sieci MAN (Metropolitan Area Networks). Cechą charakterystyczną jest m.in. to, że połączenia punkt-punkt są obsługiwane tylko w trybie pełnego dupleksu. Szczególne znaczenie uzyskują również nowe w Ethernecie kategorie długości łączy, rzędu 50 kilometrów.

Ponadto współczesne projekty przewidują bezpośrednie dopasowanie do struktur MAN, zaimplementowanych na poodstawie SONET/SDH. Jak przystało na nowy standard, powstała oczywiście grupa 10 Gigabit Ethernet Alliance (10GEA, www.10gea.com). Pierwszy projekt (Draft) standardu został przedstawiony we wrześniu 2000 roku. Ostateczną wersję przyjęto 17 czerwca 2002 roku.

10GBase i 10GBase-LX

Obecnie sa przewidziane dwa typowe warianty 10-gigabitowego Ethernetu, które różnią się wzajemnie przede wszystkim fizycznym interfejsem.

LAN PHY (SX) to wersja ekonomiczna, natomiast WAN PHY (LX) ma zapewnić transmisję na duże odległości i kompatybilność z wykorzystywaną infrastrukturą OC-192WAN.

Oba interfejsy obsługują zarówno transmisję szeregową, jak i czterokrotnie multipleksowaną. W tym kontekście należy dodać, że Ethernet 10-gigabitowy przewiduje wyłącznie transmisję światłowodową. Nie wynikają stąd jednak żadne ograniczenia, ponieważ w obu scenariuszach zastosowań (sieć szkieletowa LAN i sieć brzegowa WAN) można również przewidzieć zastosowanie światłowodów jako nośników.

Fizyczny przekaz w nośniku optycznym stawia znacznie mniejsze wymagania w porównaniu z okablowaniem opartym na miedzi. Można tu jednak odnaleźć niektóre techniki znane z dotychczasowych standardów. W ten sposób chciano umożliwić zastosowanie najprostszych i najtańszych światłowodów. Chodziło również o to, żeby aktywne komponenty pracowały z jak najmniejszą częstotliwością i były jak najprostsze. Rozpatrując dopasowanie poszczególnych składników systemu, trzeba jednak zauważyć, że postęp w technologii półprzewodników i rozmiary podzespołów uzasadniają raczej zastosowanie bardziej zaawansowanej - cyfrowej - obróbki sygnału niż kosztownych, biernych mediów transportowych lub laserów.

Dwa przykłady są ilustracją kontynuacji stosowania znanych technik:
Sprawdzone kodowanie 8B/10B jest nadal stosowane. Aby jednak nie zwiększać dodatkowo szybkości transmisji, szczególnie w wypadku transmisji szeregowej, stosuje się również kodowanie 64B/66B.
Z kolei, aby częstotliwość przenoszenia nie przewyższyła wartości możliwej do obsłużenia za pomocą technologii CMOS, konieczne jest połączenie wielu bitów w kombinowane bloki. Wypróbowano w tym celu różne techniki alternatywne, jednak do współpracy z biernymi i aktywnymi podzespołami najlepiej nadaje się znana skądinąd modulacja PAM5x5.Podsumowanie

Dysponując ekonomicznymi rozwiązaniami na różnych poziomach szybkościach od 10 MB/s do 10 Gb/s standard Ethernet miałby szansę stać się wreszcie dominującym protokołem sieciowym. Tak zresztą się nawet stało, przynajmniej w sieciach lokalnych, zarówno w komunikacji biurowej, jak i w automatyce przemysłowej. W niedalekiej przyszłości Ethernet może umocnić swoją pozycję również w sieciach regionalnych (MAN), gdyż jednolity standard, niewymagający konwersji protokołów, jest prostszy i tańszy od mnogości różnych systemów.

Sen o jednolitym krajobrazie sieciowym nie spełnił się, choć z innych powodów, niż te, które mogli przewidywać twórcy zorientowanej na połączenia i zbyt skomplikowanej sieci ATM.

Przegląd bezprzewodowych sieci LAN

Zbyt wiele standardów sieci bezprzewodowych zabiega o względy klientów. Kto dziś zdecyduje się na określony standard, szybko zabrnie w ślepy zaułek. Omówimy teraz specyficzne zalety i wady poszczególnych technologii sieci bezprzewodowych.

O bezprzewodowej transmisji danych dyskutuje się już od wielu lat. Obecnie dynamika rynku jest duża; wszędzie prezentowane są nowe produkty. Szczególnymi beneficjentami transmisji bezprzewodowej są kieszonkowe urządzenia do komunikacji głosowej i przetwarzania danych.

Zalety sieci WLAN

Sieci bezprzewodowe charakteryzują się wieloma zaletami również w zastosowaniach stacjonarnych:
brak kabli - możesz wreszcie mieć porządek wokół biurka,
brak wtyczek - możesz zapomnieć o niekompatybilnych wtykach,
brak połączeń kablowych w biurze - zależnie od poziomu hierarchii sieciowej, która ma być objęta transmisją bezprzewodową, można uniknąć kosztownej instalacji kabli w pomieszczeniach biurowych czy budynkach prywatnych,
tworzenie sieci ad hoc - potencjalni partnerzy wyszukiwani są aktywnie, a niezbędne protokoły transmisyjne - negocjowane automatycznie,
mobilność - zależnie od charakterystyki danej sieci bezprzewodowej, urządzenia można stosować również w sposób "mobilny". Wielkość komórek sieci i sposób komunikacji z innymi systemami zależą przy tym od wybranej technologii.Wady sieci WLAN

Wszystkie wyżej wymienione zalety nie powinny wywołać bezkrytycznego entuzjazmu, ponieważ sieci bezprzewodowe mają też wady:
koszt szerokości pasma - mimo znaczącego spadku kosztów ta sama szerokość pasma jest w sieciach bezprzewodowych nadal znacząco droższa niż w sieciach kablowych,
dostępna szerokość pasma - jest często mniejsza niż w sieciach kablowych, mimo wyższych kosztów,
zasięg - w wypadku systemów bezprzewodowych jest często poważnie ograniczony, co nie pozwala uzyskać pożądanej funkcjonalności lub wymusza kompromisy.
bezpieczeństwo inwestycji - obecnie na rynku jest wiele rozwiązań, przy czym tylko niektóre mogą liczyć na sukces w perspektywie średniookresowej. Obawa o bezpieczeństwo inwestycji prowadzi w tej sytuacji często do odłożenia decyzji w czasie.Za pomocą inteligentnych rozwiązań wiele z tych atrakcyjnych cech technologii bezprzewodowych można również zrealizować w sieciach kablowych. Dotyczy to szczególnie przypadków, gdy pewne usługi realizowane są w wyższych warstwach protokołu, niezależnie od rodzaju nośnika fizycznego. Ponieważ producenci bezprzewodowych systemów komunikacyjnych po raz pierwszy stosują nowe możliwości konsekwentnie, a nawet w sposób do pewnego stopnia ujednolicony, są one nieraz mylone z sieciami WLAN.

Wielość rozwiązań

Negatywny wpływ na akceptację sieci WLAN ma obecnie wielość dostępnych rozwiązań i wyższy koszt węzła sieci. Duża liczba konkurujących ze sobą rozwiązań tworzy rażący kontrast w stosunku do sieci przewodowych. Tam dominuje standard Ethernetu. Rynek sieci bezprzewodowych znajduje się natomiast dopiero w fazie rozwoju, choć przewiduje się ogromne przyrosty w następnych latach. Dlatego też wielu producentów wypracowuje sobie dogodną pozycję startową, oferując szczególne funkcje czy cechy.

Niemniej wszyscy producenci zdają sobie sprawę z tego, że rozwiązania niestandardowe nie mają szans na sukces - brak współdziałania z innymi urządzeniami stanowiłby barierę

akceptacji rynkowej, a koszty badawczo-rozwojowe i marketingowe byłyby niezwykle wysokie.

Z tych powodów na rynku sieci bezprzewodowych ma miejsce prawdziwy boom konsorcjów. Są to organizacje typu non-profit, które zajmują się koordynacją prac badawczo-rozwojowych i wspólnymi działaniami marketingowymi na rzecz członków organizacji. Jednak niemal wszyscy liczący się producenci półprzewodników, systemów i oprogramowania biorą udział w więcej niż jednym konsorcjum. Są trzy powody takiego stanu rzeczy:
wielcy producenci prowadzą tak zróżnicowaną działalność, że zaangażowanie w różnych konsorcjach jest logicznym tego skutkiem;
rynek sieci bezprzewodowych jest jeszcze na tyle nieprzejrzysty, że sukcesu określonej technologii nie da się przewidzieć, dlatego niektórzy uważają, że warto postawić na więcej niż jednego konia;
po trzecie, obszary zastosowań różnych protokołów mogą różnić się między sobą, a to oznacza różne docelowe segmenty rynku.Rozwiązania niestandardowe

Powyższe stwierdzenia nie oznaczają bynajmniej, że nie ma specyficznych rozwiązań firmowych. Przeważnie chodzi o niestandardowe rozszerzenia eksploatowanych systemów.

Tempo zmian zmusza producentów do jak najszybszego wprowadzania nowych produktów na rynek, nawet za cenę ryzyka, że nie są w pełni zgodne ze standardem.

Urządzenia bezprzewodowe wymagają obecnie bardzo dobrych projektów układów i systemów, dlatego wydajne systemy pierwszej generacji opierają się zwykle na specyficznych rozwiązaniach własnych firm.

Brak współpracy z innymi urządzeniami nie jest rzeczywistą wadą z punktu widzenia producenta. W ten sposób nabywca zmuszony jest do kolejnych inwestycji. Producenci standaryzowanych urządzeń komunikacyjnych nie mają praktycznie żadnej możliwości zróżnicowania swoich produktów pod względem właściwej funkcji komunikacyjnej. Jakąkolwiek wartość dodaną mogą tworzyć jedynie dodatkowe usługi lub funkcje. Większość z nich wiąże się bezpośrednio z funkcją administrowania siecią. To z kolei w istotny sposób ogranicza możliwości wzajemnego współdziałania.

Wydajny standard, jak choćby IEEE802.11, oferujący przepływność do 11 Mb/s, może wyprzeć z rynku firmy oferujące produkt niestandaryzowany. Tak na przykład firma Radiola, jeden z pierwszych producentów szybkich, ale niestandardowych urządzeń, ogłosiła upadłość. Również firma Proxim była jednym z pierwszych dostawców niestandardowych urządzeń bezprzewodowych.

Scenariusze zastosowań i poziomy sieci

W systemach bezprzewodowych są trzy zasadnicze obszary zastosowań: sieci PAN, LAN i sprzężenie sieci. Stosunkowo nowe pojęcie "sieci osobiste" (Personal Area Network - PAN) obejmuje komunikację urządzeń jednego lub nie więcej niż kilku użytkowników na odległość około 10 metrów. Można tu wyróżnić trzy scenariusze.

Sprzężenie urządzeń peryferyjnych. Chodzi o połączenie takich urządzeń, jak drukarki, telefony komórkowe, palmtopy czy aparaty cyfrowe, z komputerem osobistym w celu wymiany lub synchronizacji danych.

Sprzężenie zewnętrznych urządzeń z platformą usługową. Typowym przykładem jest opracowany już dawno przez Ericssona zestaw słuchawkowy do telefonów komórkowych oparty na technologii Bluetooth.

Sprzężenie wielu komputerów PC w celu wymiany danych. Ta architektura jest już bliska klasycznej sieci LAN, można ją więc uznać za przypadek graniczny. W sieciach PAN komunikujące się ze sobą urządzenia znajdują się zwykle w bezpośrednim sąsiedztwie. Przeważnie wystarcza im umiarkowana szerokość pasma. Moduły radiowe urządzeń pracujących w sieciach PAN muszą być bardzo tanie. Tylko wówczas można je implementować w prostych i tanich urządzeniach, uzyskując niezbędną akceptację.

Scenariusze zastosowań - rodzaj ruchu w sieci

Wymagania stawiane sieci muszą zostać sklasyfikowane według różnych rodzajów ruchu. Podstawowe rozróżnienie to transmisja głosu i danych. Widać tu wyraźnie, że sieciom bezprzewodowym przypisuje się coś, czego realizacja sie dotychczas nie udała lub udała się w niewystarczającym stopniu w sieciach przewodowych. Problemy związane z przesyłaniem głosu w sieci Ethernet-IP są powszechnie znane.

Jakość usług sieciowych na poziomie sieci określają zasadniczo cztery parametry: szybkość przesyłu danych, czas opóźnienia, wahania czasu opóźnienia (jitter) i współczynnik strat. Zapewnienie odpowiedniego poziomu tych parametrów w różnych rodzajach ruchu oznacza z reguły spełnienie wymagań różnych protokołów.

W razie wykorzystania do czystej transmisji danych (klasyczne przesyłanie plików) potrzebna jest duża szybkość transferu. Jeżeli chodzi o ewentualne opóźnienia, ważne jest jedynie, aby cały proces zamknął się w akceptowalnym przedziale czasu. Utrata danych jest absolutnie niedopuszczalna. Transmisja mowy wymaga niewielkiej szerokości pasma, ale jednocześnie stawia ona wymagania dotyczące opóźnień i ich wahań. Odpowiedzi rozmówcy powinny docierać bez wyczuwalnej zwłoki. Zwykle daje się to zrealizować tylko poprzez rezerwację wyznaczonych kanałów. Z kolei zrozumiałość mowy niewiele ucierpi w razie utraty pojedynczych bitów w czasie transmisji. Przekaz multimedialny, jako połączenie dźwięku i ruchomego obrazu, np. w wypadku przesyłania filmów, stawia znów inne wymagania - duża przepustowość i niewielkie opóźnieniaa. Bezwzględna wielkość opóźnienia ma przy tym znaczenie drugorzędne. Współczynnik strat jest do pewnego stopnia niekrytyczny, ponieważ oko ludzkie uzupełnia brakujące lub błędnie wyświetlone punkty obrazu.

Standardy sieci mobilnych

Wśród dostępnych na rynku znaczące są następujące technologie:
Bluetooth,
DECT,
IEEE802.11b,
IEEE802.11a,
HiperLAN i,
HomeRF.Rozwiązania oparte na podczerwieni właściwie nie mają przyszłości. Sam sprzęt jest tani, bardzo rozpowszechniony i dobrze współdziała z wieloma urządzeniami, jak notebooki, palmtopy i telefony komórkowe, ale jego podstawową wadą jest konieczność zapewnienia niezakłóconej "widoczności" między urządzeniami, a co za tym idzie, praktyczna niemożność połączenia w sieć więcej niż dwóch.

W dalszym ciągu omówimy poszczególne rozwiązania z punktu widzenia ich potencjalnych zastosowań.

Na rysunku widać, że obecne standardy pokrywają bardzo szeroki zakres szybkości transferu i odległości, a niektóre z nich pokrywają się. Należy jednak poczynić dwa zastrzeżenia. Szybkość transferu to szybkość brutto fizycznej transmisji. Przeważnie do dyspozycji użytkownika pozostaje efektywnie 25 do 50 procent. Zależnie od warunków brzegowych współczynnik ten może być jeszcze mniejszy.

W praktyce systemy nie uzyskują nominalnego zasięgu. Zasięg może się jednak znacznie zwiększyć po zastosowaniu anten o charakterystyce kierunkowej. Jednak zwiększa to koszty oraz zmniejsza komfort użytkowania.

Standard Bluetooth

Niezależnie od wszelkich dyskusji technicznych trzeba przyznać propagatorom systemu Bluetooth, że przeprowadzili najlepszą i najskuteczniejszą kampanię marketingową. Bluetooth Special Interest Group (BSIG) została założona na początku roku 1988 przez pięć firm: IBM, Toshiba, Intel, Ericsson i Nokia, a już niedługo potem standard został zatwierdzony.

Technologia ta bardzo szybko zwróciła na siebie uwagę dzięki zręcznemu wykorzystaniu w marketingu obudów, imitacji urządzeń i prezentacji potencjalnych zastosowań. Korzyści odniosły wszystkie technologie radiowe.

Do najważniejszych cech standardu Bluetooth zaliczają się:

Pasmo częstotliwości. Bluetooth pracuje w powszechnie dostępnym paśmie częstotliwości 2,4 GHz (ISM - industrial, scientific and medical, pasma częstotliwości zarezerwowane pierwotnie do niekomercyjnego wykorzystania w przemyśle, nauce i medycynie).

Technika modulacji. W celu uzyskania niezawodnej transmisji w paśmie zwolnionym z licencjonowania Bluetooth korzysta z techniki skokowej zmiany częstotliwości (frequency hopping). Nadajnik i odbiornik zmieniają w uzgodniony sposób częstotliwość nośną co 625 ?s.

Zasięg systemów. Bez anteny kierunkowej jest on ograniczony do ok. 10 metrów, ale w przyszłości mają być dostępne dodatkowe wzmacniacze; moc wyjściowa wzrośnie z 1 do 100 mW, a zasięg zwiększy się do ok. 100 metrów.

Typy danych i ruchu. Bluetooth obsługuje zarówno synchroniczny, jak i asynchroniczny typ transmisji. Dzięki temu umożliwia przesyłanie mowy w paśmie o szerokości 64 Mb/s w obu kierunkach oraz przesyłanie danych w paśmie o szerokości 865,2 Mb/s.

Usługi. Standard definiuje nie tylko oba najniższe poziomy warstwy protokołów, lecz również usługi opisane na wyższych poziomach. Dzięki temu w komfortowy sposób obsługuje tworzenie tzw. sieci ad hoc.

Obszar zastosowań Bluetooth, ze względu na wymienione cechy kluczowe, to zdecydowanie sieci osobiste (PAN). Tworzenie wydajnych sieci nie jest możliwe ze względu na niską przepustowość i ograniczenia topologii.

Standard DECT

W roku 1982 Europejski Instytut Norm Telekomunikacyjnych (ETSI, http://www.etsi.org) zatwierdził standard europejskich cyfrowych bezprzewodowych sieci telekomunikacyjnych (Digital European Cordless Telecommunications, DECT) ETS 300 175. Standard ten jest bardzo rozpowszechniony w rozwiązaniach firmowych i w gospodarstwach domowych. Do tej pory zainstalowano na całym świecie ok. 300 mln systemów DECT. Techniczne warunki brzegowe:

Pasmo częstotliwości. W większości krajów DECT pracuje w specjalnie wydzielonym paśmie częstotliwości - w Europie pomiędzy 1880 a 1900 MHz. Na innych kontynentach stosuje się również inne pasma, od 1,5 do 3,6 GHz.

Technika modulacji. Podział pasma częstotliwości na poszczególne kanały odbywa się zgodnie z algorytmem MC/TDMA/TDD. Algorytm przydzielania kanałów może podlegać dynamicznym zmianom. Zwiększa to odporność na zakłócenia.

Zasięg. W obrębie budynków zasięg systemów DECT jest ograniczony do około 50 metrów. W otwartej przestrzeni zwiększa się do około 300 metrów. Ponieważ dopuszczalna jest stosunkowo wysoka moc wyjściowa 250 mW, z anteną kierunkową można uzyskać zasięg do 3 km.

Typy danych i ruchu. W podstawowej specyfikacji DECT obsługuje synchroniczną i symetryczną transmisję mowy. Rozszerzenie standardu dodaje ważne usługi do pakietowej transmisji danych. Przy wykorzystaniu wszystkich kanałów można przesłać maksymalnie 20 Mb/s.

Usługi. W celu rozszerzenia oferty na kolejnym etapie zdefiniowano DECT Multimedia Access Profile. Opiera się on na stosowanych już standardach, jak GAP i DPRS, dopuszcza jednak dodatkowe usługi, np. Direct Link Access (DLA), w celu tworzenia połączeń sieciowych ad hoc.

Ze względu na ograniczoną przepustowość DECT nie jest wydajnym rozwiązaniem sieciowym, dlatego należy ją uznać za kolejną technologię z rodziny PAN. Dysponuje bardzo wydajnym mechanizmem do nadzorowania kanałów i zarządzania nimi, które w sieci PAN są właściwie zbędne. Można się na przykład przemieszczać między komórkami sieci bez przerywania połączenia. Opcje te zwiększają koszty urządzeń DECT, mimo to wiele firm, szczególnie niemieckich, oferuje interesujące produkty.

Standard IEEE802.11

Sekcja standaryzacyjna amerykańskiego stowarzyszenia inżynierów IEEE (http://www.ieee.org) opracowała protokół transmisji bezprzewodowej IEEE802.11, podobny do wszechobecnego Ethernetu. Wsparciem marketingowym i działalnością informacyjną zajmuje się Wireless LAN Association (WLANA, http://www.wlana.com). Z kolei Wireless Ethernet Compatibilty Alliance (WECA, http://www.wi-fi.com) certyfikuje urządzenia kompatybilne z 802.11 pod względem wzajemnego współdziałania. Dlatego też urządzenia pracujące w standardzie IEEE.802.11 sprzedawane są również pod nazwą handlową Wi-Fi (Wireless Fidelity).

Oprócz pierwotnego standardu 802.11 są dwa ważne rozszerzenia. 802.11b umożliwia przechodzenie - z uwzględnieniem stosowanych systemów 802.11 - na szybszą transmisję. 802.11a jest standardem podobnym, jednak niekompatybilnym ze względu na inną częstotliwość nośną. Ma on jednak charakteryzować się znacznie wyższą wydajnością.

Oto przegląd najważniejszych cech standardu IEEE802.11:

Pasmo częstotliwości. Nielicencjonowane pasmo ISM 2,4 GHz.

Technika modulacji. 802.11 stosuje dwie: modulacja w widmie rozproszonym ze skokową zmianą używanego kanału (frequency hopping spread spectrum - FHSS) daje w efekcie zmiany częstotliwości nośnej. Modulacja rozproszonego widma z bezpośrednim szeregowaniem bitów (direct sequence spread spektrum - DSSS) rozszerza spektrum częstotliwości poprzez logiczne powiązanie danych z kodem cyfrowym o wyższej szybkości. Dzięki temu możliwa jest praca wielu sieci na jednym obszarze bez wzajemnego zakłócania, zwiększa się także odporność na błędy.

Zasięg. W systemach 802.11 wynosi do 100 metrów. Antena kierunkowa może zwiększyć go do 2 km.

Typy danych i ruchu. 802.11 dysponuje transferem do 2 Mb/s, 802.11b - ponad 11 Mb/s. Głównym zadaniem jest transmisja danych. Metodą rezerwacji odcinków czasowych (convention free periods - CFP) można zapewnić na jednym kanale transmisję bez opóźnień.

Usługi. Standard 802.11 zastępuje kablowe systemy transmisji danych na fizycznym poziomie modelu warstw, co daje gwarancję, że wybór nośnika transmisji jest nieprzezroczysty dla wyższych warstw protokołu.

Parametry - zwłaszcza 802.11b - umożliwiają zastosowanie również w większych sieciach. Obecnie producenci implementują oprócz czystej funkcjonalności transportowej również wiele funkcji do zarządzania siecią i użytkownikami. Wada systemu to jego ukierunkowanie na transmisję danych. Świadczenie usług głosowych jest praktycznie niemożliwe.

Standard HomeRF

Standard HomeRF (RF - radio frequency) próbuje przezwyciężyć słabości standardu IEEE802.11. Równolegle z danymi można w nim przesyłać mowę względnie pakiety multimedialne. Standard HomeRF został opracowany od podstaw przez firmę Proxim, jednak obecnie zajmuje się nim ponad 100 firm. Jest bardzo popularny w Stanach Zjednoczonych. Jak wynika z badania przeprowadzonego przez PC Data w czwartym kwartale 2000 roku, 95 procent wszystkich domowych sieci bezprzewodowych opierało się wówczas na HomeRF. Pierwsza wprowadzona na rynek wersja 1.2 standardu obsługiwała transfer do 1,6 Mb/s. Obecnie dostępna wersja 2.0 uzyskuje transfer danych do 10 Mb/s. Kolejna wersja 2.1 ma osiągać do 20 Mb/s.

Pasmo częstotliwości. HomeRF pracuje w nielicencjonowanym paśmie ISM 2,4 GHz.

Technika modulacji. HomeRF korzysta z techniki skokowej zmiany częstotliwości. Jest 75 kanałów o szerokości pasma 1 MHz; każdym z nich można przesłać 1,6 Mb/s. W nowszych wersjach uzyskuje się wyższy transfer dzięki łączeniu kanałów.

Zasięg. Zasięg systemów HomeRF wynosi 50 metrów.

Typy danych i ruchu. Oprócz transmisji danych HomeRF umożliwia przesyłanie głosu i multimediów o określonych parametrach jakościowych. Uzyskuje się to dzięki zastosowaniu protokołu SWAP-CA (Shared Wireless Access Protocol - Cordless Access), który w regularnych odstępach czasu przydziela użytkownikom zarezerwowane szczeliny czasowe.

Usługi. Opis standardu HomeRF obejmuje dwie najniższe warstwy sieci. Są wyposażone w punkty dostępu do usług w taki sposób, że mogą każdorazowo prawidłowo obsłużyć różne rodzaje ruchu (dane, multimedia, głos).

HomeRF nadaje się do niezbyt skomplikowanych zastosowań w obszarze SOHO. Zaletą systemu jest ekonomiczna realizacja zarówno przesyłu danych, jak i telefonii. Nie był opracowywany do poważniejszych zastosowań biurowych i się do nich nie nadaje. Jego pozycja wydaje się w ten sposób określona, ale są wątpliwości. Jeżeli na przykład stanieją wydajniejsze systemy 802.11, HomeRF gwałtownie straci na atrakcyjności. W dodatku liczba zainstalowanych telefonów bezprzewodowych jest tak duża, że dodatkowa usługa nie stanowi żadnej atrakcji. Jeżeli zaś chodzi o przesyłanie zaawansowanych multimediów, uzyskiwany transfer danych z trudem na to pozwala.

Standard HiperLAN/2

Ponieważ producenci nie byli zainteresowani przełożeniem standardu HiperLAN/1 na konkretne urządzenia, europejski instytut norm telekomunikacyjnych zainicjował w kwietniu 2000 roku jako część projektu BRAN (Broadband Radio Access Network) standaryzację systemu HiperLAN Type 2 (HiperLAN/2). Za cel postawiono zapewnienie dostępu do stałej sieci z prędkością do 155 Mb/s zarówno w warunkach domowych, jak i biurowych. Popularyzacją standardu HiperLAN/2 zajmuje się HiperLAN Global Forum (www.hiperlan2.com). Oto techniczne warunki brzegowe HiperLAN/2:

Pasmo częstotliwości. HiperLAN/2 pracuje w paśmie ISM 5 MHz. Wymaga to jeszcze ścisłych uzgodnień z działaniami IEEE w zakresie 802.11a w Stanach Zjednoczonych i Japonii. Ich wynik jest jeszcze sprawą otwartą.

Technika modulacji. HiperLAN/2 wykorzystuje technikę OFDM (orthogonal frequency division multiplex), podobnie jak ADSL i DAB. OFDM uzyskuje wysoką wydajność również w kanałach rozproszonych, jakie występują w zakresie częstotliwości gigahercowych. Oprócz tego stosuje się modulację typu Multicarrier Modulation. W tej technice dane przesyłane są na niezależnych podnośnych. Każdy kanał dysponuje 48 podnośnymi dla danych i 4 podnośnymi pilotowymi do synchronizacji.

Typy danych i ruchu. HiperLAN/2 uzyskuje na poziomie fizycznej warstwy transportowej przepustowość 54 Mb/s. Jako bezprzewodowy wariant ATM uzyskuje podobną do niego jakość usług.

Usługi. HiperLAN/2 ogranicza się do opisu obu dolnych warstw sieci. Typowa sieć HiperLAN/2 składa się z wielu punktów dostępowych (access points - AP), które łącznie zapewniają dostęp na pewnym obszarze. W tak utworzonych komórkach odbywa się komunikacja mobilnych użytkowników (mobile terminals - MT).

Możliwy jest tryb centralized mode (CM), w którym wszyscy użytkownicy mobilni przesyłają dane przez punkty dostepowe, lub tryb direct mode (DM), w którym użytkownicy mobilni, którzy znajdują się we wzajemnym zasięgu, wymieniają dane bezpośrednio pod kontrolą instancji nadzorującej (central controller - CC).

HiperLAN/2, podobnie jak kablowa sieć ATM, zorientowany jest na połączenia. Przed rozpoczęciem transmisji danych użytecznych konieczne jest nawiązanie połączenia; wariantowo może to być połączenie punkt-punkt, punkt-wiele punktów lub połączenie rozgłoszeniowe.

Rozszerzenia standardu HiperLAN/2

Standard HiperLAN/2 uzupełniają dwa składniki, które otwierają przed nim dodatkowe obszary zastosowań. Hiper-ACCESS ma zapewnić połączenia na odległość do 5 km w architekturze punkt-wiele punktów. Zastosowanie - osiedla mieszkaniowe i łączność z klientami. Protokół ten, Wireless Local Loop, nazwany swego czasu HiperLAN Type 3, ma zapewnić transfer do 27 Mb/s. HiperLINK służy do połączeń punkt-punkt na odległość do 150 m z bardzo dużą szybkością do 155 Mb/s. Szczególną uwagę poświęca się obsłudze współpracy HiperLAN/2 i Hiper-ACCESS na niewielką odległość. Na HiperLINK, nazwany swego czasu HiperLAN Type 4, zarezerwowano pasmo częstotliwości wokół 17 GHz.

W popieranie HiperLAN/2 angażuje się obecnie wielu liczących się producentów, szczególnie w Stanach Zjednoczonych i Japonii, dlatego można przypuszczać, że standard nie podzieli losu swego poprzednika, HiperLAN/1. Ma też dobrą pozycję wyjściową w walce o pasmo częstotliwości 5 GHz.

Przemawiają za nim ponadto możliwości, które wynikają, podobnie jak w ATM, z jakości usług. Jednak dodatkowy nakład na zarządzanie i zwiększony wolumen ruchu utrudniły już sukces rynkowy kablowym systemom ATM.

Podsumowanie

Powyższy przegląd pokazuje wyraźnie, że poszczególne protokoły transmisji bezprzewodowej charakteryzują się różnymi właściwościami i różnorodną jakością. Na możliwości ich popularyzacji mają również wpływ lokalne regulacje w poszczególnych krajach. Odpowiednio do tego różnicują się optymalne obszary zastosowań i rynki docelowe. Jest rzeczą rozsądną odczekać i obserwować, jaka będzie akceptacja rynku dla poszczególnych systemów i który z nich najlepiej sprawdzi się na konkretnym rynku docelowym.

Przegląd portów

Bez portów nie sposób wyobrazić sobie komunikacji za pomocą standardowych protokołów komunikacyjnych Internetu, Transmission Control Protocol (TCP) i User Datagram Protocol (UDP). To właśnie dzięki portom wiele aplikacji może jednocześnie wymieniać dane za pośrednictwem jednego łącza internetowego.

Podstawowa wiedza o portach jest również niezbędna do prawidłowej konfiguracji firewalla. Każdy datagram przechodzi przez pakiet filtrów, który na podstawie określonych reguł decyduje, czy przesłać go dalej, czy nie. Odczytywane są przy tym między innymi informacje z nagłówka, takie jak port nadania i port docelowy. Na podstawie tych reguł firewall może filtrować usługi. Procesy usługowe zawsze korzystają z określonych portów. Wystarczy na przykład odfiltrować pakiety, które mają w nagłówku wpisany port 21, aby zablokować usługi FTP. Równie duże znaczenie ma informacja, z jakiego komputera nawiązano połączenie - z klienta w sieci LAN, czy też z komputera zewnętrznego.

W tym artykule opiszemy funkcjonowanie portów i ich grupy.

Czym są numery portów?

Numery portów są podstawa stosowania protokołów TCP oraz UDP. Gdy dane dotrą już do komputera docelowego, trzeba je jeszcze dostarczyć do właściwej aplikacji.

W trakcie przesyłu informacji przez warstwy sieci potrzebny jest mechanizm, który przede wszystkim zapewnia przekazanie do właściwego w każdym przypadku protokołu.

Łączenie danych pochodzących z różnych źródeł w pojedynczy strumień danych określa się mianem multipleksingu. Protokół internetowy (IP) musi zatem zdemultipleksować dane przychodzące z Internetu. W tym celu IP oznacza protokoły transportowe numerami protokołów. Z kolei same protokoły transportowe wykorzystują numery portów do identyfikacji aplikacji.

Numer protokołu IP znajduje się w jednym bajcie w trzecim słowie nagłówka datagramu. Wartość ta stanowi o przekazaniu do odpowiedniego protokołu warstwy transportowej, na przykład 6 oznacza TCP, zaś 17 - UDP. Protokół transportowy musi przekazać otrzymane dane do właściwej aplikacji. Aplikacje identyfikowane są na podstawie numeru portu o długości 16 bitów, do którego dane przesyłane są po nadejściu do komputera docelowego. Dlatego też pierwsze słowo każdego nagłówka TCP oraz UDP zawiera numer source port (port źródłowy) i destination port (port docelowy). Aplikacja, która chce być dostępna pod określonym numerem portu, informuje o tym stos protokołów TCP/IP.

Gniazda

Kombinacja adresu IP i numeru portu nosi nazwę gniazda. W ten sposób możliwa jest jednoznaczna identyfikacja pojedynczego procesu sieciowego w całym Internecie. Zapis wygląda następująco: adres IP:numer portu, na przykład 62.96.227.70:80. Dwa gniazda definiują połączenie - jedno dla komputera-nadawcy, drugie dla odbiorcy.

TCP i UDP mogą nadawać te same numery portów. Dopiero kombinacja protokołu i numeru portu jest jednoznaczna. Tak więc port numer 53 w protokole TCP nie jest identyczny z portem numer 53 w protokole UDP. O budowie i sposobie funkcjonowania rodziny protokołów TCP/IP piszemy obszernie w artykule "Tak działa TCP/IP i IPv6".

Grupy portów

Do dyspozycji jest ogółem 65 535 portów TCP i UDP. Aby zachować nad nimi kontrolę, a także by móc przydzielać aplikacjom stałe numery, podzielono je na trzy grupy.

Dobrze znane porty (well known ports) - zarezerwowane, standardowe numery portów od 1 do 1023. Ułatwiają nawiązanie połączenia, ponieważ zarówno nadawca, jak i odbiorca z góry wiedzą, że dane muszą być przesłane dla określonego procesu pod określony numer portu. Serwery Telnetu używają na przykład portu nr 23. Dobrze znane porty umożliwiają klientom nawiązywanie połączeń z serwerami bez dodatkowej konfiguracji. Zarządzaniem tymi portami zajmuje się Internet Assigned Numbers Authority (IANA). Listę aktualnie przydzielonych numerów portów można znaleźć pod adresem http://www.iana.org/assignments/port-numbers . Do roku 1992 dobrze znane porty ograniczały się do zakresu 1 do 255. Porty o numerach od 256 do 1023 były stosowane do usług uniksowych.

Zarejestrowane porty (registered ports) - porty o numerach od 1024 do 49.151 przewidziane są dla usług, które zwyczajowo korzystają z określonych portów. Przykładem może być port 3128, często wykorzystywany przez serwery proxy jako alternatywny port HTTP.

Porty przydzielane dynamicznie (dynamically allocated ports, również ephemeral ports) - jak wskazuje nazwa, zawsze przydzielane dynamicznie. Są to porty o numerach od 49.152 do 65.535. Każdy klient może korzystać z nich tak długo, jak długo kombinacja protokołu transportowego, adresu IP i numeru portu jest jednoznaczna. Proces, który potrzebuje dostępu do portu, żąda go od swojego hosta.

Który z portów jest używany?

Jak już wspomnieliśmy, wiedza o portach jest nieodzowna do konfiguracji firewalla. Należy określić, które porty mogą być wykorzystywane do połączeń wychodzących i przychodzących. Jednak często nie wiadomo, z których portów korzysta dana aplikacja. Nieraz dobrze byłoby też wiedzieć, który z portów został już losowo przydzielony aplikacji na komputerze-kliencie.

W celu zdobycia tej wiedzy można się posłużyć się narzędziem Windows, programikiem Netstat. Niestety, jego funkcjonalność jest bardzo ograniczona. Nie podaje ono na przykład informacji o tym, jakie aplikacje używają poszczególnych połączeń.

Godny polecenia jest shareware'owy program Essential NetTools firmy Tamos Software (http://www.tamos.com). Jednym z jego składników jest rozbudowane narzędzie Netstat. Dostarcza ono nie tylko informacji o otwartych portach i połączeniach w systemie, lecz również tekstowych tłumaczeń adresów i portów wraz ze ścieżkami dostępu do odpowiednich aplikacji.

Przykładowe połączenie

W naszym przykładzie załadujemy za pomocą przeglądarki internetowej stronę http://www.tecChannel.de . Przeglądarka utworzy połączenie z adresem IP 62.96.227.70. Na serwerze zostanie użyty port TCP numer 80, dobrze znany port serwerów internetowych. Klient wykorzysta dynamicznie przydzielany port 1897.

Klient, który wywołuje stronę internetową, znajduje się w lokalnej sieci, co można poznać po adresie 192.168.80.99. Dane przechodzą przez router, gdzie stosowana jest maskarada z użyciem Network Address Translation (NAT). Więcej informacji o maskaradzie i komunikacji port-port za pośrednictwem routera poniżej.

Router - maskarada

Jeżeli połączenie z Internetem przechodzi przez router, niemożliwa jest bezpośrednia komunikacja port-port w ramach protokołu TCP/IP. W sieciach lokalnych stosowane są najczęściej prywatne adresy IPv4, ponieważ uzyskanie oficjalnych adresów IPv4 w większych ilościach jest od pewnego czasu znacznie utrudnione. Cały ruch internetowy przechodzi przez router. Jednak mając taki adres, klienty nie mogą się komunikować bezpośrednio z Internetem. Pakiety odpowiedzi nie mogłyby znaleźć właściwej drogi. Skąd zatem serwer w sieci zna właściwy numer portu klienta w sieci LAN?

Ma tu zastosowanie tak zwana maskarada. Chodzi tu o specjalną metodę konwersji adresów, nazywaną również source network address translation (SNAT). W przypadku pakietów wychodzących na zewnątrz adres źródłowy zastępowany jest adresem routera, zaś pierwotny port źródłowy - nowym portem. Dane te zapisywane są w tablicy, dzięki czemu pakiety odpowiedzi mogą być odpowiednio przekonwertowane w drugą stronę. W ten sposób usługa internetowa "nie zauważa", że kontaktuje się z portami routera, a nie klienta.

Router - forwardowanie portów

Ze względu na zasadę działania Network Address Translation (NAT), która jest stosowana w wielu sieciach firmowych, nie można nawiązać z zewnątrz połączenia z komputerem, który znajduje się wewnątrz sieci, za routerem. Stosuje się zatem technikę zwaną forwardowaniem (forwarding) lub odwzorowaniem (mapping) portów. Polega ona na tym, że komputer oczekuje na nawiązanie połączenia pod określonym numerem portu, a następnie przesyła pakiety danych do innego komputera w sieci. W ten sposób możliwa jest praca serwera internetowego na kliencie za routerem.

Odwołania nie następują bezpośrednio do komputera w lokalnej sieci, lecz do określonego portu routera. Router przekazuje odwołanie do odpowiedniego portu komputera docelowego. Pakiety, które odsyła komputer, również wymagają odpowiedniego opracowania. Adres IP i numer portu komputera jest zastępowany adresem IP i forwardowanym numerem portu routera. Można powiedzieć, że forwardowanie jest przeciwieństwem maskarady. Jednak w obu przypadkach klienty są niewidoczne z poziomu Internetu.

Aby lepiej zrozumieć istotę forwardowanie portów, posłużmy się przykładem serwera internetowego. Klient o adresie 192.168.80.99 w sieci lokalnej jest połączony z Internetem za pośrednictwem routera o adresie publicznym 194.246.96.76. Aby umożliwić dostęp do serwera internetowego na kliencie, router jest konfigurowany w ten sposób, że wszystkie pakiety adresowane do portu 4711 przesyła do portu 80 na komputerze 192.168.80.99. Pakiety odpowiedzi z 192.168.80.99:80 przekształcane są przez router na postać 194.246.96.76:4711.

Porty - otwarta brama

Porty TCP i UDP są jednocześnie potencjalnym źródłem zagrożeń. Za ich pośrednictwem robaki i trojany ingerują w systemy lokalne lub tworzą połączenia internetowe. Dlatego też zaleca się stosowanie firewalli, szczególnie w systemach windowsowych.

W niektórych kręgach poszukiwanie na ślepo tylnego wejścia (backdoor) poprzez łączenie z losowo wybranymi adresami IP stało się rodzajem sportu. Używając skanera portów, napastnik może bardzo łatwo ustalić, które z portów w komputerze są otwarte. Skaner nie robi przy tym nic innego, tylko łączy się po kolei ze wszystkimi portami i sprawdza, czy nadejdzie odpowiedź. Jeżeli nadejdzie, oznacza to, że port jest otwarty i można spróbować wykorzystać go do niewłaściwych celów.

Stąd też stosowanie firewalli jest wręcz nieodzowne. W następnym rozdziale opiszemy konfiguracje firewalla na podstawie reguł. Przestrzeganie tych reguł może ochronić przed większością zagrożeń online.

Budowanie firewalla

Za pomocą metajęzyka wyjaśnimy ważne reguły filtrowania, niezbędne do skutecznego funkcjonowania firewalla. Mają one zastosowanie do wszystkich popularnych firewalli. Podstawowa zasada mówi, że należy najpierw zamknąć wszystkie porty, a następnie otworzyć tylko te, które są naprawdę potrzebne. Reguły filtrowania wynikają z wielu opcji, które zebraliśmy w tabeli na sąsiedniej stronie:

Stosujemy następującą notację metajęzyka:

FORWARD/ACCEPT/REJECT/DROP -dir IN/OUT -prot TCP/UDP -src HOST:PORT -dest HOST:PORT

Posługując się adresami IP komputera źródłowego, można zablokować usługi dla określonych komputerów w sieci lokalnej. Dokonując konfiguracji, należy jednak pamiętać, że niektóre usługi nie korzystają z już otwartych połączeń, lecz tworzą nowe. Z tego względu firewall powinien w niektórych przypadkach zezwalać na otwieranie połączeń:

IF FORWARD/ACCEPT/REJECT/DROP -dir IN/OUT -prot TCP/UDP -src HOST:PORT -dest HOST:PORT THEN FORWARD/ACCEPT/REJECT/DROP -dir IN/OUT -prot TCP/UDP -src HOST: PORT -dest HOST:PORT

Wiele pojedynczych reguł tworzy zestawy. Przy każdym zapytaniu z sieci lokalnej lub z Internetu przetwarzany jest cały zestaw reguł. Zestaw reguł bada i filtruje każdy pakiet danych. W naszej przykładowej konfiguracji sieci firmowej wiele klientów połączonych jest z Internetem za pośrednictwem firewalla. Serwer proxy nie jest stosowany.

Usługi standardowe I

Na początek zaleca się skonfigurowanie usług standardowych, potrzebnych do większości połączeń internetowych. Chodzi przede wszystkim o dostęp do witryn internetowych i serwerów FTP.

Domain Name Service - ta reguła umożliwia komputerowi lokalnemu nawiązanie połączenia z serwerem nazw dostawcy usług internetowych. Te dwie reguły będą z całą pewnością potrzebne:

FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:53
FORWARD -dir OUT -prot UDP -src LOCAL_CLIENT:ANY -dest ANY:53

File Transfer Protocol - FTP dopuszcza dwa różne rodzaje połączeń, które wymagają różnych ustawień filtrowania. Zasadniczo zaleca się stosowanie pasywnego FTP, ponieważ w tym przypadku wszystkie połączenia nawiązywane są przez klienta i nie trzeba zezwalać na żadne połączenia inicjowane z zewnątrz. W trybie aktywnym klient tworzy połączenie do portu 21 serwera. Serwer potwierdza połączenie i tworzy nowe ze swojego portu 20 do klienta. Dla pełnej jasności opiszemy oba warianty. W przypadku aktywnego FTP należy tak skonfigurować firewall, aby połączenie mógł nawiązywać tylko ten serwer, z którym klient wcześniej utworzył połączenie przez port 20.

Pasywny FTP:
FORWARD -dir OUT -prot TCP -scr LOCAL_CLIENT:ANY ANY:21

Aktywny FTP:
IF FORWARD -dir OUT -prot TCP -scr LOCAL_CLIENT:ANY FTP_SERVER:21 THEN FORWARD -dir IN -prot TCP -src FTP_SERVER:20 LOCAL_CLIENT:ANY

Usługi standardowe II

SSH Remote Login Protocol umożliwia bezpieczną komunikację i uwierzytelnianie. W tym celu cały proces logowania, łącznie z przekazywaniem haseł, jest szyfrowany. Tę regułę należy stosować tylko w razie potrzeby.

FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:22

Hypertext Transfer Protocol (HTTP) jest standardowym protokołem przeglądarek internetowych i umożliwia dostęp do stron internetowych.

FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:80

Jeżeli w sieci firmowej stosowany jest serwer proxy, regułę należy odpowiednio dostosować.

Hypertext Transfer Protocol over TLS/SSL służy do bezpiecznej transmisji stron internetowych między serwerem internetowym a przeglądarką. Transmisja jest szyfrowana metodą SSL. Protokół HTTPS jest stosowany przez wiele witryn internetowych, na przykład w bankowości internetowej. Dlatego należy otworzyć odpowiednie porty.

FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:443

Poczta elektroniczna i serwisy wiadomości

Należy też otworzyć odpowiednie porty, żeby umożliwić wysyłanie i odbieranie poczty elektronicznej. Simple Mail Transfer Protocol (SMTP) jest z reguły stosowany do wysyłania wiadomości. Możliwa jest taka konfiguracja, że wysyłanie poczty elektronicznej jest dozwolone tylko za pośrednictwem określonego serwera. Przy właściwej konfiguracji pocztę można wysyłać tylko za pośrednictwem firmowego serwera pocztowego.

FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:25

Post Office Protocol Version 3 umożliwia ściąganie poczty elektronicznej z serwerów pocztowych POP3. Również i tutaj można ograniczyć dostęp do wybranych serwerów.

FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:110

Network News Transfer Protocol (NNTP) służy do przekazywania wiadomości USENET-u. Tę regułę należy stosować tylko w razie potrzeby.

FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:119

Internet Message Access Protocol Version 4 - jeżeli dostęp do poczty ma odbywać się za pośrednictwem IMAP4, należy również zastosować odpowiednią regułę.

FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:143

Internet Message Access Protocol Version 4 over TLS/SSL służy do transmisji szyfrowanej SSL między klientami pocztowymi a serwerem IMAP4. Regułę należy stosować tylko wtedy, gdy używany jest również ten protokół.

FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:993

Post Office Protocol Version 3 over TLS/SSL - jeżeli stosowany serwer POP3 obsługuje bezpieczną transmisję SSL, należy zastosować następującą regułę:

FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:995

Audio i wideo I

W tym podrozdziale powiemy, jakie reguły filtrowania trzeba zainstalować, żeby móc korzystać mimo firewalla z popularnych programów do odtwarzania plików audio i wideo, na przykład z Apple Quick Time Playera czy Real Playera. Reguły te należy zainstalować tylko wtedy, gdy jest to niezbędne, i zalecamy ich zastosowanie jedynie do wybranych klientów w sieci LAN.

Real Player tworzy połączenia do serwerów danych strumieniowych za pomocą portów TCP 554, 7070 i 7071. Serwer wysyła strumień audio/wideo z jednego z portów UDP pomiędzy 6970 a 7170. Ponieważ jednak nie jest rozsądne otwieranie wszystkich tych portów, zalecamy otwarcie dla Real Playera tylko jednego portu UDP i wpisanie go w konfigurację oprogramowania. Alternatywnie można odbierać strumienie przez porty TCP, jednak firma Real twierdzi, że jakość jest wówczas gorsza.

FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:554
FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:7070
FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:7071

Port UDP powinien być jednym z portów pomiędzy 6970 a 6997, ponieważ w tej chwili nie są to jeszcze porty zarejestrowane, na przykład:

IF FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY REAL_SERVER:554 THEN FORWARD -dir IN -prot UDP -src REAL_SERVER:6971 -dest LOCAL_CLIENT:ANY

Firewall należy tak skonfigurować, żeby połączenie mógł nawiązać tylko ten serwer, z którym wcześniej połączenie nawiązał odpowiedni klient z sieci lokalnej.

Audio i wideo II

Microsoft Media Player. Media Server wykorzystuje do przesyłu strumieni audio i wideo (ASF) własny, niestandardowy protokół serwerowy, opracowany przez Microsoft. Jest on obsługiwany przez MS Media Server od wersji 4.0 i przez MS Media Player. W celu nawiązania połączenia Media Player kontaktuje się z serwerem przez port TCP 1755. Serwer wysyła strumień do klienta z portu UDP 1755.

FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:1755

IF FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY MEDIA_SERVER:1755 THEN FORWARD -dir IN -prot UDP -src MEDIA_SERVER:1755 -dest LOCAL_CLIENT:ANY

Apple Quick Time, podobnie jak Real Player, wykorzystuje port TCP 554 do nawiązania połączenia z serwerem. Apple Quick Time Player wysyła dane strumieniowe do klienta przez port UDP 6970 do 6999. I w tym przypadku odradzamy otwieranie wszystkich tych portów, natomiast zalecamy odbiór strumieni przez http.

FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:554

Komunikacja i czat

Choć z dużym opóźnieniem, firmy zaczynają doceniać rolę komunikatorów w obrębie przedsiębiorstwa. Jeżeli mają być stosowane, wymaga to opracowania odpowiednich reguł filtrowania.

ICQ - do komunikacji klient-serwer z komputerem login.icq.com program wykorzystuje port TCP 5190. Opcjonalnie można użyć dla tego serwera również portu TCP 443 z szyfrowaniem SSL. Do komunikacji pomiędzy klientami można używać dowolnych portów z zakresu 1024 do 65535. Należy otworzyć tylko jeden port i podać go w opcjach konfiguracji ICQ (http://Web.icq.com).

FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest login.icq.com:5190

W komunikatorze Yahoo! cała komunikacja odbywa się przez port TCP 5050, dlatego w grę wchodzą następujące trzy serwery: http://cs1.yahoo.com , http://cs2.yahoo.com oraz http://cs3.yahoo.com . Należy otworzyć porty dla tych trzech serwerów. Jeżeli nie udaje się nawiązać połączenia z serwerem Yahoo! (http://de.messenger.yahoo.com) przez port 5050, wykorzystywany jest port 80.

FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY cs1.yahoo.com:5050
FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY cs2.yahoo.com:5050
FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY cs3.yahoo.com:5050

Komunikator AOL Instant Messenger (http://www.aol.com), podobnie jak ICQ, korzysta z portu TCP 5190.

FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:5190

Microsoft Instant Messenger wykorzystuje do komunikacji port TCP 1863. Jeżeli ma być użyta funkcja integracji z AOL Instant Messenger, należy dodatkowo otworzyć port TCP 5190:

FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:1863

Integracja z AIM:

FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:5190

ICMP - Internet Control Message Protocol

Internet Control Message Protocol (ICMP) służy do wymiany komunikatów o błędach i komunikatów statusu w przypadku, gdy w transmisji danych za pomocą Internet Protocol (IP) wystąpią błędy. Jeżeli na przykład host jest niedostępny, router wysyła do nadawcy komunikat "destination unreachable". ICMP służy też do kontroli - polecenie ping wykorzystuje pakiety ICMP do ustalenia czasu przebiegu datagramów między dwoma hostami.

Ataki z wykorzystaniem ICMP

Korzystanie z Internet Control Message Protocol przypomina jazdę po brzytwie z balansowaniem między bezpieczeństwem a wydajnością. Godząc się na niewielki spadek wydajności, można całkowicie zablokować ten protokół. W większości przypadków połączenie internetowe powinno mimo to normalnie funkcjonować.

Niebezpieczeństwo polega na tym, że ICMP może być wykorzystany do ataków polegających na wysyłaniu fałszywych komunikatów o błędach. W ten sposób możliwy jest na przykład atak typu denial of service (DoS), który może spowodować zablokowanie niektórych usług lub wręcz unieruchomienie serwera. Za pomocą dostępnych w ICMP

usług Echo i Echo Reply napastnik może też zgromadzić przydatne informacje o budowie sieci, na przykład o liczbie komputerów i ich adresach IP. Informacje te mogą być następnie wykorzystane przez hakerów do kolejnych, celowych ataków.

Komunikaty ICMP I

Jak już wspomnieliśmy, należy najpierw zamknąć wszystkie porty, a następnie otworzyć tylko te, które są naprawdę potrzebne. ICMP dostarcza wielu komunikatów, ale w praktyce potrzebnych jest tylko kilka. Komunikaty ICMP dzielą się na typy. Więcej informacji na temat poszczególnych typów można znaleźć na stronie IANA (http://www.iana.org/assignments/icmp-parameters). Potrzebne reguły filtrowania opisujemy poniżej.

Komunikaty o błędach

Typ 3 - destination unreachable. Ten rodzaj komunikatu jest wysyłany, gdy brama nie może znaleźć odpowiedniej sieci lub komputer docelowy nie może znaleźć protokołu czy portu. Przychodzące pakiety tego rodzaju powinny być akceptowane. Zmniejsza to czas przestojów, gdyż w przeciwnym razie klient musi czekać na time-out.

FORWARD -dir IN -prot ICMP_Typ_3 -src ANY:ANY -dest LOCAL_CLIENT:ANY

Typ 11 - time exceeded. Komunikat dla nadawcy pakietu, że z powodu przekroczenia limitu czasu pakiet nie został dostarczony. Przyczyną może być nadmiar pakietów (zator) na odpowiednim routerze względnie protokół IP na komputerze docelowym nie potrafi połączyć fragmentów w kompletny strumień danych. Przychodzące komunikaty tego rodzaju powinny być akceptowane.

FORWARD -dir IN -prot ICMP_Typ_11 -src ANY:ANY -dest LOCAL_CLIENT:ANY

Komunikaty ICMP II

Typ 12 - parametr problem. Komunikat dla nadawcy datagramu informujący, dlaczego pakiet danych nie mógł być przesłany.

FORWARD -dir IN -prot ICMP_Typ_12 -src ANY:ANY -dest LOCAL_CLIENT:ANY

Typ 4 - source quench. Komunikat dla nadawcy pakietu o problemie z buforem, informujący, dlaczego pakiet nie mógł być przesłany.

FORWARD -dir IN -prot ICMP_Typ_4 -src ANY:ANY -dest LOCAL_CLIENT:ANY

Meldunki informacyjne

Typ 8 - echo / Typ 0 - echo reply. Odbiorca wysyła do nadawcy echo request wszystkie dane zawarte w pakiecie danych. W ten sposób można stwierdzić, czy określony adres IP jest dostępny, czy nie. Wielu hakerów skanuje Internet poleceniem echo w poszukiwaniu komputerów, które odpowiedzą komunikatem echo reply, a następnie szuka w tych komputerach trojanów, dlatego należy zezwolić tylko na echo wychodzące i echo reply przychodzące.

FORWARD -dir OUT -prot ICMP_Typ_8 -src ANY -dest ANY
FORWARD -dir IN -prot ICMP_Typ_0 -src ANY -dest ANY

Narzędzia współdzielenia plików I

Serwisy wymiany plików, jak Gnutella i eDonkey, cieszą się coraz większą popularnością wśród amatorów plików muzycznych czy wideo. Być możem niektórzy szefowie firm zdecydują się na udostępnienie tych usług w sieci przedsiębiorstwa, nawet jeśli nie mają one wiele wspólnego z właściwymi zadaniami pracowników. Dlatego właśnie opiszemy wymagane w tym przypadku reguły filtrowania.

Gnutella to jeden z najbardziej znanych serwisów równorzędnej (peer-to-peer) wymiany plików. Aby dostęp do usług wymiany był możliwy, porty TCP 6346 i 6347 muszą być otwarte dla ruchu wychodzącego.

FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:6346
FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:6347

Więcej informacji o stosowaniu Gnutelli za firewallem można znaleźć na stronach http://www.gnutellanews.com .

Narzędzia współdzielenia plików II

eDonkey wykorzystuje standardowo porty 4661, 4662 i 4665. Jednak do korzystania z serwisu wystarczy otwarcie ruchu wychodzącego w porcie TCP 4662. Port TCP 4661 wykorzystywany jest w trybie serwera i dla trybu klienta nieistotny. Funkcja komunikatora eDonkey korzysta z portu 4665. Więcej informacji można znaleźć pod adresem http://www.edonkey2000.com .

FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:4662

Powyższa reguła jest więc wystarczająca. Jeżeli jednak miałby działać także serwer, a do tego chcielibyśmy się kontaktować z innymi użytkownikami eDonkeya, należałoby ustanowić dodatkowo następujące reguły:

FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:4661
FORWARD -dir IN -prot UDP -src ANY:ANY -dest LOCAL_CLIENT:4662
FORWARD -dir OUT -prot UDP -src LOCAL_CLIENT:ANY -dest ANY:4665

KazaA i Morpheus - oba serwisy peer-to-peer (http://www.kazaa.com , http://www.morpheus.com) wykorzystują do wymiany plików z innymi użytkownikami port TCP 1214.

FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:1214

Gry online I

Wspólne gry przez Internet cieszą się coraz większą popularnością. Poniżej zebraliśmy niezbędne reguły konfiguracji firewalla do gier online. Korzystając z komputera w pracy, upewnij się najpierw, że szef jest skłonny przymknąć oko na sporadyczne gierki.

Battle.net - chyba najbardziej znany portal gier. Umożliwia grę w "StarCraft", "WarCraft II", "Diablo" i "Diablo II". W tym celu należy włączyć ruch przychodzący i wychodzący dla protokołów TCP oraz UDP w porcie 6112.

FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:6112

IF FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY GAME_SERVER:6112 THEN FORWARD -dir IN -prot TCP -src GAME_SERVER:6112 -dest LOCAL_CLIENT:ANY

FORWARD -dir OUT -prot UDP -src LOCAL_CLIENT:ANY -dest ANY:6112

IF FORWARD -dir OUT -prot UDP -src LOCAL_CLIENT:ANY GAME_SERVER:6112 THEN FORWARD -dir IN -prot UDP -src GAME_SERVER:6112 -dest LOCAL_CLIENT:ANY

Gry online II

Microsoft zone.com - MSN (http://www.msn.com) umożliwia na stronie zone.com (http://www.zone.com wspólne gry strategiczne, jak "Age of Empires". W tym celu należy otworzyć odpowiednie porty dla zone.com oraz interfejsu gier DirectX.

Zone.com:
FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:6667
FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:28800-29100

DirectX 8:
FORWARD -dir OUT -prot UDP -src LOCAL_CLIENT:ANY -dest ANY:6073
FORWARD -dir OUT -prot UDP -src LOCAL_CLIENT:ANY -dest ANY:2302-2400

IF FORWARD -dir OUT -prot UDP -src LOCAL_CLIENT:ANY GAME_SERVER:2302-2400 THEN FORWARD -dir IN -prot UDP -src GAME_SERVER:2302-2400 -dest LOCAL_CLIENT:ANY

Microsoft SideWinder Game Voice: urządzenie peryferyjne do komputerów PC umożliwia zarówno bezpośrednią komunikację z innymi graczami za pośrednictwem sieci LAN, jak również sterowanie głosowe grami.

FORWARD -dir OUT -prot UDP -src LOCAL_CLIENT:ANY -dest ANY:9110

Jeżeli komputer w sieci lokalnej ma być również serwerem czatu, należy otworzyć ruch przychodzący w porcie UDP 9110.

FORWARD -dir IN -prot UDP -src ANY:9110 -dest LOCAL_CLIENT:ANY

Tak działa DHCP

Sieci podlegają stałym przemianom - starsze urządzenia idą na złom, przybywa nowych komputerów, mobilni użytkownicy logują się i wylogowują. Ręczna konfiguracja sieci wymagałaby nieprawdopodobnego nakładu pracy. Protokół DHCP (Dynamic Host Configuration Protocol) rozwiązuje ten problem poprzez dynamiczne przydzielanie adresów IP.

W sieci opartej na protokole TCP/IP każdy komputer ma co najmniej jeden adres IP i jedną maskę podsieci; dzięki temu może się komunikować z innymi urządzeniami w sieci. Centralne przydzielanie adresów za pomocą wydzielonego komputera opłaca się już w małej sieci. Administrator uzyskuje w ten sposób kilka korzyści od razu. Konserwacja sieci wymaga mniej czasu, ponieważ odpadają manipulacje przy poszczególnych klientach. Konflikty adresów należą do przeszłości, ponieważ serwer DHCP steruje centralnie przydzielaniem adresów IP.

Protokół DHCP opiera się na protokole BOOTP (Bootstrap Protocol), jednak w stosunku do niego zawiera wiele ulepszeń. Niewątpliwie najbardziej interesującym jest dynamiczne przydzielanie adresów IP. Serwer DHCP korzysta przy tym z predefiniowanego obszaru adresowego (range, czasem nazywany też scope) i przydziela kolejnym klientom, które o to występują, adres IP na określony czas (lease). W czasie trwania okresu lease klient DHCP nie występuje do serwera DHCP podczas startu systemu o nowy adres, a jedynie żąda potwierdzenia istniejącego stanu lease.

Protokół DHCP minimalizuje również możliwe źródła błędów. Na życzenie podaje oprócz adresu IP również inne parametry, jak choćby standardowa brama, czy adresy serwerów nazw. Specyfikacja techniczna protokołu DHCP zawarta jest w RFC 2131.

Interakcja między klientem a serwerem

Już uproszczony opis przydzielania adresów unaocznia cykliczny charakter interakcji między klientem a serwerem. Cały proces uzgadniania i przydzielania jest czteroetapowy.

Klient wysyła do znajdującego się w sieci serwera DHCP wiadomość DHCPDISCOVER. Jej sens można jest mniej więcej taki: "Do wszystkich serwerów DHCP w sieci. Potrzebny mi adres IP". Ponieważ jak dotąd klient nie ma adresu IP, nie może wykorzystywać protokołu TCP/IP do komunikacji z innymi systemami sieciowymi. Z tego względu korzysta z protokołu UDP.

W odpowiedzi na zapytanie klienta serwer DHCP przesyła mu propozycję DHCPOFFER, w której zawarty jest adres IP. Ponieważ w sieciach, szczególnie w dużych sieciach, może się znajdować większa liczba serwerów DHCP, oferta ta ma szczególne znaczenie.

Teraz piłeczka jest po stronie klienta - musi się zdecydować na jeden z zaproponowanych adresów. W tej fazie istotne znaczenie ma rodzaj implementacji DHCP - kryteria wyboru nie są opisane w RFC, lecz różnią się w zależności od platformy systemowej. Gdy klient zdecyduje się już na jeden z adresów, wysyła do serwera DHCP komunikat DHCPREQUEST. Również w tym wypadku protokołem transportowym jest UDP.

Na ostatnim chwilowo etapie piłeczka wraca na pole serwera. Po otrzymaniu komunikatu DHCPREQUEST serwer przydziela klientowi za pomocą DHCPPACK tymczasowy adres IP. Po otrzymaniu tej wiadomości klient z reguły sprawdza, czy adresu nie stosuje inny komputer w sieci. Na koniec klient wpisuje otrzymane parametry sieciowe do konfiguracji swojego systemu.

Odświeżanie DHCP

Nieodłącznym elementem przydzielenia klientowi adresu IP przez serwer DHCP jest przyznanie dodatkowo tzw. czasu użytkowania (lease). Określa on czas ważności ustawień. W tle pracują dwa zegary - T1 odmierza połowę czasu użytkowania, zaś T2 - 87,5 procent pełnego czasu użytkowania. Obie wartości można zmienić w opcjonalnych ustawieniach serwera DHCP - jeśli takie funkcje zostały zaimplementowane.

Po upływie czasu T1 klient wysyła komunikat DHCPREQUEST do serwera i pyta, czy serwer może przedłużyć czas użytkowania. Stan ten określa się jako renewing status. Z reguły serwer odpowiada wiadomością DHCPACK i przydziela nowy czas użytkowania. Serwer resetuje wówczas zegary T1 i T2.

Jeżeli po upływie czasu T2 klient nie otrzyma wiadomości DHCPACK, rozpoczyna się tak zwany rebinding status. Klient musi wysłać komunikat DHCPREQUEST, żeby uzyskać przedłużenie czasu użytkowania. Serwer może odpowiedzieć na to żądanie potwierdzeniem DHCPACK. Jeżeli jednak i to żądanie pozostanie bez odpowiedzi, klient musi zażądać nowego adresu IP. Wkracza wówczas ponownie opisany na początku mechanizm, który rozsyła zapytania do wszystkich serwerów DHCP w sieci.

Obszar adresowy a czas użytkowania

Zanim serwer DHCP będzie w ogóle mógł zacząć przydzielać klientom adresy IP, musi zostać wyposażony w informacje na temat przewidzianego do tych celów obszaru adresowego (range). Obszar adresowy jest zdefiniowany poprzez adres początkowy i końcowy. W zależności od implementacji mogą też być też obszary wykluczone, a więc takie, których serwer nie może przydzielać. Gwarantuje to bezkolizyjne współistnienie w sieci adresów stałych i dynamicznie przydzielanych.

Czas użytkowania określany jest zwykle w dniach, godzinach i minutach. Nie ma w tym względzie żadnej złotej reguły. Parametr ten, jeśli w ogóle jest zaimplementowany w poszczególnych produktach, musi uwzględniać obciążenie serwera, zachowanie klientów i stabilność sieci. Decydujące znaczenie ma liczba potencjalnych klientów. Reguła brzmi: Czas użytkowania powinien być dwukrotnie dłuższy niż czas potrzebny do przywrócenia pracy serwera w razie jego awarii. Uwaga - w przypadku długiego czasu użytkowania odpowiednio później uwzględniane są zmiany opcji DHCP po stronie klientów.

Tak działa TCP/IP i IPv6

Podstawą Internetu jest rodzina protokołów TCP/IP, która zapewnia globalną komunikację między najróżnorodniejszymi komputerami i urządzeniami. Opracowano ją w połowie lat siedemdziesiątych, kiedy to w amerykańskiej Defense Advanced Research Agency (DARPA, http://www.darpa.mil) zainteresowano się budową sieci umożliwiającej wymianę pakietów danych między różnymi systemami komputerowymi w ośrodkach badawczych. TCP/IP tworzy heterogeniczną sieć o otwartych protokołach, które są niezależne od systemów operacyjnych i architektury sprzętowej. Za pomocą protokołów internetowych mogą się komunikować dowolne systemy - domowe, korporacyjne i kieszonkowe.

Protokoły są dostępne dla każdego i traktowane jako własność publiczna. Każdy użytkownik może korzystać z nich bez licencji na własne potrzeby, a także tworzyć na ich podstawie własne aplikacje i usługi. Skrótem TCP/IP określa się całą rodzinę protokołów, tak zwaną "Internet Protocol Suite". Dwa najważniejsze typy, TCP oraz IP, stały się źródłem nazwy dla całej rodziny protokołów.

Dzięki jednolitemu schematowi adresowania każdy komputer w sieci TCP/IP może jednoznacznie zidentyfikować dowolny inny komputer. Standaryzowane protokoły wyższych warstw oddają do dyspozycji użytkownika usługi dostępne w ujednolicony sposób. Dodanie pod koniec lat siedemdziesiątych protokołów TCP/IP do systemu BSD-Unix stało się podstawą do rozwoju Internetu.

Architektura protokołu

Nie ma powszechnej zgody co do sposobu opisu TCP/IP jako modelu warstw. Model OSI jest wprawdzie całkiem użyteczny, ale w dużej części bardzo akademicki. Do zrozumienia budowy TCP/IP potrzebny jest model, który w większym stopniu opiera się na strukturze protokołów.

Amerykańskie ministerstwo obrony (DoD - Department of Defense, http://www.defenselink.mil) opracowało czterowarstwowy model sieci. Każda warstwa składa się z pewnej liczby protokołów, które łącznie tworzą rodzinę TCP/IP. Specyfikację każdego protokołu opisano w jednym lub kilku RFC.

Podobnie jak w modelu OSI, podczas wysyłania dane przechodzą drogę od góry stosu w dół; w trakcie odbioru danych z sieci droga prowadzi przez stos do góry. W celu zapewnienia prawidłowej transmisji danych każda warstwa dodaje swoje dane kontrolne. Informacje te noszą nazwę nagłówka, ponieważ poprzedzają właściwe dane.

Kapsułkowanie danych

Dodawanie informacji kontrolnych nazywa się kapsułkowaniem (encapsulation). W trakcie odbioru danych kapsułkowanie wykonywane jest w odwrotnej kolejności. Każda z warstw usuwa swój nagłówek i przesyła pozostałe dane do warstwy leżącej powyżej.

Podczas przesyłania niewielkiej ilości danych może się zdarzyć, że w wyniku kapsułkowania powstanie więcej danych protokołu niż danych użytecznych. Celowe jest wówczas użycie protokołu UDP (User Datagram Protocol), który przesyła dane, korzystając z minimalnej liczby mechanizmów protokołu.

IP - Internet Protocol

Internet Protocol (IP) jest podstawą rodziny protokołów TCP/IP. Odpowiada za przesyłanie danych. Ogólnie rzecz biorąc, jego zadaniem jest zapewnienie transmisji

danych między sieciami. W tym celu musi przejąć wiele zadań, stawiając je do dyspozycji wyższych warstw w formie usług. Do zadań IP należą:
usługa pakietowania danych,
fragmentacja pakietów danych,
wybór parametrów transmisji,
funkcja adresowania,
routing między sieciami.Internet Protocol nie udostępnia żadnego zabezpieczonego połączenia i nie może przesyłać ponownie utraconych pakietów danych. Każdy pakiet danych IP przesyłany jest do odbiorcy jako niezależny pakiet (datagram). Dla różnych typów sieci określone są różne długości pakietów danych. Wielkość pakietu danych zależy od wielu czynników, w tym od ograniczeń sprzętowych i programowych.

Jeżeli pakiet danych ze względu na wielkość nie może być przesłany w całości, zostaje podzielony na mniejsze fragmenty. Pakiety wysyłane są wprawdzie we właściwej kolejności, niekoniecznie jednak w takiej samej docierają do celu. Ponieważ mogą się przemieszczać różnymi drogami, konieczne są dodatkowe informacje. Umożliwiają one zrekonstruowanie pierwotnego stanu pakietu. W trakcie transmisji każdy pakiet otrzymuje na początku nagłówek.

Nagłówek IP - szczegóły

Nagłówek IP oferuje 14 parametrów i z wykorzystanym polem Opcje ma długość 32 bajtów; w przeciwnym wypadku - 20 bajtów.

Adresy IP

Każdy host w sieci TCP/IP otrzymuje jednoznaczny, 32-bitowy adres, który składa się z dwóch zasadniczych części - adresu sieci i adresu komputera w ramach tej sieci. Jednak format obu części nie jest taki sam we wszystkich adresach IP. W celu łatwiejszej strukturyzacji podzielono całą przestrzeń adresową na wiele klas.

Liczba bitów, które identyfikują sieć, oraz liczba bitów, które identyfikują komputer, zmienia się wraz z klasą, do której należy adres. Ogólnie rzecz biorąc, adresy zapisuje się w postaci czterech liczb dziesiętnych rozdzielonych kropkami. Każda z tych 8-bitowych liczb zawiera się w przedziale od 0 do 255 - wartości, które można przedstawić za pomocą jednego bajta.

IP - klasy adresów i adresy specjalne

Trzy najważniejsze klasy adresów to A, B i C. Aby stwierdzić, do jakiej klasy należy dany adres, oprogramowanie IP odczytuje pierwsze bity adresu. Do określenia klasy, do której należy dany adres, stosuje się następujące reguły:

Jeżeli pierwszym bitem adresu jest 0, mamy do czynienia z adresem klasy A. W pierwszym bicie adresu zakodowana jest jego klasa, kolejne siedem identyfikuje sieć. Pozostałe 24 bity identyfikują komputer w sieci. Ogółem możliwych jest 127 sieci klasy A.

Jeżeli dwa pierwsze bity adresu IP to 10, mamy do czynienia z adresem w sieci klasy B. Dwa pierwsze bity określają klasę, następnych 14 identyfikuje sieć, zaś 16 ostatnich - komputer.

Jeżeli trzy pierwsze bity to 110, chodzi o sieć klasy C. Pierwsze trzy bity określają klasę, 21 kolejnych określa sieć. Osiem ostatnich bitów identyfikuje komputer.

Jeżeli pierwsze trzy bity adresu to 111, chodzi o adres specjalny, zarezerwowany, określany często mianem adresu klasy D. Są to tak zwane adresy grupowe. Można je nadawać grupom komputerów, które korzystają ze wspólnego protokołu.

We wszystkich klasach adresów są numery komputerów zarezerwowanych do specjalnych celów. Adres IP, w którym wszystkie bity identyfikujące komputer mają wartość 0, a więc adres z komputerem o numerze 0, identyfikuje samą sieć. Jeżeli wszystkie bity identyfikujące komputer mają wartość 1, a więc tworzą numer komputera 255, mamy do czynienia z tzw. adresem rozgłoszeniowym. Używa się go do jednoczesnego zaadresowania wszystkich komputerów w sieci.

Również w klasie A są dwa adresy, a mianowicie 0 oraz 127, zarezerwowane do celów specjalnych. Sieć 0 oznacza trasę domyślną (default route), standardową lub predefiniowaną, a sieć 127 to adres zwrotny (loopback address). Trasa domyślna służy do uproszczenia routingu, jaki musi wykonać IP. Adres zwrotny upraszcza aplikacje sieciowe w ten sposób, że komputer lokalny można zaadresować dokładnie tak, jak komputer.

Podsieci

Stosując podmaski sieci można przenieść część adresu IP związaną z numerowaniem komputerów do podsieci. Maska podsieci informuje, który obszar jest interpretowany jako podsieć, a który jako adres komputera. W ten sposób w jednej dużej sieci tworzy się wiele małych, redukując jednak jednocześnie liczbę komputerów, które do niej przynależą. Te małe sieci w ramach dużej nazywa się podsieciami.

I tak na przykład adres klasy A 10.x.y.z, który ma maskę podsieci 255.0.0.0, poprzez maskę podsieci 255.255.0.0 staje się adresem klasy B, a poprzez maskę podsieci 255.255.255.0 staje się adresem klasy C. Decyzja o utworzeniu podsieci ma zwykle rozwiązać problemy topologiczne lub organizacyjne. Podsieci umożliwiają zdecentralizowanie zarządzania siecią komputerową.

Routery IP mogą fizycznie łączyć różne sieci, ale tylko wtedy, gdy każda sieć otrzyma własny, jednoznaczny adres. Tworząc podsieci, dzieli się jeden jednoznaczny adres sieci na wiele jednoznacznych adresów podsieci. W ten sposób każda sieć fizyczna otrzymuje własny adres.

Maski podsieci są zorientowane bitowo i umożliwiają określanie klas pośrednich, np. maska podsieci 255.128.0.0 stanowi adres klasy A. Drugi bajt rozróżnia dwie sieci o adresach 0 do 127 i 128 do 255. W ten sposób sieć klasy A została podzielona na dwie podsieci.

Routing - tak dane docierają do celu

Komputer wysyłający pakiet danych IP zna wprawdzie adres docelowy, ale nie zna drogi do niego. Każda stacja na drodze datagramu do odbiorcy musi podjąć decyzję o wyborze dalszej drogi. Proces ten nosi nazwę routingu. Wybór określonej trasy (route) zależy od wielu kryteriów. Nadawca przekazuje to zadanie standardowemu routerowi, który zajmuje się dostarczaniem pakietów danych do innych sieci.

Miedzy dwoma hostami znajduje się z reguły wiele routerów. Każdy z nich dysponuje tak zwaną tablicą routingu (routing table). To z niej router wybiera kolejną stację na drodze datagramu. Każdy wpis w tablicy routingu zawiera określone informacje (patrz tabela poniżej).

Procedura routingu

Co do zasady, rozróżnia się trzy procedury routingu:
routing statyczny na podstawie stałych wpisów w tablicy routingu,
routing domyślny na podstawie jednego stałego wpisu w tablicy routingu,

routing dynamiczny na podstawie automatycznej aktualizacji tablic routingu.W przypadku routingu statycznego do tablicy routingu komputera wpisywany jest odpowiedni router dla każdej sieci. W ten sposób można dokładnie prześledzić, jaką drogę przeszedł każdy z pakietów danych. W dużych sieciach metoda ta jest niepraktyczna, ponieważ należałoby utrzymywać zbyt wiele wpisów. W routingu domyślnym do tablicy komputera wpisuje się jeden adres, pod który wysyłane są wszystkie pakiety danych, które nie pochodzą z własnego obszaru adresowego sieci.

W routingu dynamicznym komputer i router nieustannie wymieniają między sobą informacje. Dzięki temu komputer "wie", która z tras jest aktualnie najlepsza. Nie trzeba ręcznie prowadzić tablic routingu. Każdy pakiet danych jest wysyłany trasą optymalną w danej chwili. Komunikacja między routerami odbywa się na podstawie specjalnych protokołów routingu, jak RIP (Routing Information Protocol) lub IGRP (Interior Gateway Routing Protocol).

Prywatne adresy IP

Zarządzaniem adresami IP zajmuje się przede wszystkim IANA (Internet Assigned Numbers Authority, http://www.iana.org), która upoważniła trzy organizacje regionalne do przydzielania adresów IP. W Ameryce Północnej i Południowej jest to ARIN (American Registry for Internet Numbers, http://www.arin.net), w Europie RIPE NCC (Réseaux IP Européens, http://www.ripe.net), w Azji APNIC (Asia-Pacific Network Information Center, http://www.apnic.net).

Zasady przydzielania adresów określa RFC 2050. Rezerwacji jednego lub wielu adresów IP dokonuje się zawsze za pośrednictwem dostawcy usług internetowych. Nie wszystkie sieci TCP/IP są wzajemnie połączone za pośrednictwem Internetu, dlatego w RFC 1918 zarezerwowano trzy obszary adresowe w klasach A, B i C na izolowane, lokalne sieci TCP/IP.

Hosty o tych adresach nie mogą być bezpośrednio połączone z Internetem, więc adresy pozostają do dyspozycji dowolnej liczby sieci lokalnych.

Mechanizm kontrolny IP - ICMP

Gdy w trakcie transmisji IP występują błędy, uruchamia się mechanizm Internet Control Message Protocol (ICMP). ICMP rozróżnia komunikaty błędu i komunikaty statusu. Gdy na przykład host jest nieosiągalny, wówczas host lub router wysyła do nadawcy komunikat o błędzie Destination Unreachable. Oprócz wykrywania błędów ICMP wykonuje też funkcje kontrolne - polecenie ping służy do ustalenia czasu przebiegu datagramu między dwoma hostami.

Przesyłanie wiadomości ICMP odbywa się w ramach datagramów IP, składających się z trzech pól nagłówka i bloku danych. Blok nagłówka Type informuje o rodzaju wiadomości. Może to być komunikat o błędzie lub statusie. W polu Code zawarte są kody błędów do danego datagramu. Interpretacja kodów zależy od rodzaju wiadomości. Pole nagłówka Checksum zawiera sumę kontrolną.

Komunikaty ICMP

Są dwie klasy meldunków ICMP:

TCP - Transmission Control Protocol

Aplikacje, dla których istotne jest, żeby dane niezawodnie dotarły do celu, wykorzystują Transmission Control Protocol (TCP). Zapewnia on prawidłowe przesyłanie danych we

właściwej kolejności. Nie zastępuje on protokołu IP, lecz wykorzystuje jego właściwości do nadawania i odbioru.

TCP jest niezawodnym protokołem transmisyjnym, zorientowanym połączeniowo. Komputer po upływie określonego czasu wysyła dane ponownie aż do chwili, gdy otrzyma od odbiorcy potwierdzenie, że zostały poprawnie odebrane. Jednostka czasu, którą posługują się we wzajemnej komunikacji moduły TCP, nosi nazwę segmentu. Każdy segment zawiera przy tym automatycznie sumę kontrolną, która podlega weryfikacji po stronie odbiorcy. W ten sposób sprawdza się, czy dane zostały odebrane poprawnie.

TCP jest zorientowany na połączenia. Protokół tworzy zatem połączenie logiczne komputer-komputer. W tym celu wysyła przed rozpoczęciem właściwej transmisji danych użytecznych pewną ilość informacji kontrolnych, nazywanych handshake.

Handshake wykorzystywany w TCP to 3-Way-Handshake, ponieważ w jego trakcie wymieniane są trzy bloki informacji. Nawiązywanie połączenia rozpoczyna się od tego, że oba komputery ustalają wartość początkową sekwencji numerycznej - Initial Sequence Number (ISN). Oba systemy TCP wymieniają między sobą i potwierdzają te wartości.

3-Way-Handshake

Nawiązywanie połączenia za pomocą 3-Way-Handshake można przedstawić w postaci diagramu. Punktem wyjścia tryb Closed - spoczynku. Za pomocą odpowiedniego polecenia połączenie przechodzi w tryb Listen, w którym można nawiązać kontakt z innym systemem TCP.

Jeżeli system znajduje się w trybie Listen, czeka na nadejście znaku SYN, aby odpowiedzieć kolejnym znakiem SYN, a następnie przejść w tryb SYN Received. Jeżeli znak SYN został wysłany, połączenie przechodzi w tryb SYN Send. System TCP pozostaje w tym trybie aż do otrzymania od drugiego systemu znaku SYN w odpowiedzi.

Jeżeli nadejdzie pozytywna odpowiedź na ten znak SYN, system TCP przechodzi w tryb SYN Received. Po pozytywnym potwierdzeniu znaku SYN (ACK w odpowiedzi na SYN) nadajnik i odbiornik przechodzą w tryb Established - może się rozpocząć transmisja danych między obydwoma komputerami. Po przesłaniu wszystkich danych komputery biorące udział w komunikacji kontynuują procedurę 3-Way-Handshake. W celu zakończenia połączenia wymieniane są segmenty z bitem No more data from sender.

Nagłówek TCP - szczegóły

Nagłówek TCP dysponuje 12 parametrami i ma 32 bajty długości, jeśli wykorzystane jest pole Opcje, lub 20 bajtów w przeciwnym wypadku.

Wszystkie pozostałe informacje, niezbędne do nadawania i odbioru, zawarte są w zakapsułkowanym nagłówku IP.

UDP - User Datagram Protocol

User Datagram Protocol (UDP) zapewnia protokołom wyższego rzędu zdefiniowaną usługę transmisji pakietów danych, zorientowanej transakcyjnie. Dysponuje minimalnymi mechanizmami transmisji danych i opiera się bezpośrednio na protokole IP. W przeciwieństwie do TCP nie gwarantuje kompleksowej kontroli skuteczności transmisji, a zatem nie ma pewności dostarczenia pakietu danych do odbiorcy, nie da się rozpoznać duplikatów ani nie można zapewnić przekazu pakietów we właściwej kolejności.

Mimo to jest wiele istotnych powodów stosowania UDP jako protokołu transportowego. Gdy trzeba przesłać niewiele danych, nakłady administracyjne na nawiązanie połączenia i

zapewnienie prawidłowej transmisji mogą być większe od nakładów niezbędnych do ponownej transmisji wszystkich danych.

Protokoły, porty i gniazda

Gdy dane dotrą już do komputera docelowego, trzeba jeszcze dostarczyć je do właściwej aplikacji. Podczas transportu danych przez poszczególne warstwy TCP/IP niezbędny jest mechanizm, który zagwarantuje przekazanie danych do właściwego w każdym przypadku protokołu. Łączenie danych pochodzących z różnych źródeł w jeden strumień danych to multipleksowanie. IP musi zatem zdemultipleksować dane nadchodzące z sieci. W tym celu oznacza protokoły transportowe numerami. Z kolei same protokoły transportowe wykorzystują numery portów do identyfikacji aplikacji. Niektóre z tych numerów protokołów i portów to tak zwane dobrze znane usługi (well-known services).

Numer protokołu IP znajduje się w jednym bajcie w trzecim słowie nagłówka datagramu. Wartość ta decyduje o przekazaniu datagramu do odpowiedniego protokołu w warstwie transportowej. Na przykład 6 oznacza TCP, a 17 - UDP. Protokół transportowy musi przekazać otrzymane dane do właściwej aplikacji. Aplikacje identyfikowane są na podstawie 16-bitowych numerów portów.

IPv6 - Internet Protocol Version 6

Cztery miliardy dostępnych adresów internetowych przestały wystarczać wobec gwałtownego rozwoju Internetu. Ponieważ niedługo niemal każda kuchenka mikrofalowa i lodówka będą dysponowały własnymi adresami internetowymi, stosowany obecnie protokół IPv4 osiągnął kres możliwości, a w dodatku nie ma on żadnych mechanizmów bezpieczeństwa ani funkcji szyfrowania i nie spełnia wymagań aplikacji posługujących się strumieniową transmisją danych. Dlatego konieczny jest nowy protokół o większej przestrzeni adresowej.

Następca stoi już w blokach startowych. Ma oznaczenie Internet Version Protocol Version 6 (IPv6), a jego wprowadzenie zaleciła na początku lat dziewięćdziesiątych organizacja Internet Engineering Task Force (IETF, http://www.ietf.org). IETF jest główną organizacją zajmującą się technicznym rozwojem i standaryzacją Internetu. Specyfikację zawarto w RFC 1883. IPv6 ma usunąć wiele wad swojego poprzednika.

Pierwsze wersje projektu IPv6 nazwano Internet Protocol next Generation (IPnG). W latach 1995 i 1996 powstało wiele projektów, już pod nazwą Internet Protocol Version 6 (IPv6). W roku 1997 IPv6 stał się już "tymczasowym standardem" (draft standard).

Przegląd cech IPv6

IPv6 jest, podobnie jak jego poprzednik IPv4, protokołem transportowym do przesyłania pojedynczych pakietów w sieci. W celu zagwarantowania kompletnej transmisji IPv6 może wykorzystywać protokoły wyższych warstw, na przykład TCP. Najważniejsze elementy funkcjonalne nowego protokołu to:
adresy IP o długości 128 bitów,
uproszczona struktura nagłówków,
zagnieżdżone nagłówki do przesyłania opcji,
opcje szyfrowania i uwierzytelniania na poziomie IP,
nowa klasyfikacja strumieni danych (flows) w celu optymalizacji przesyłu danych audio i wideo,
uproszczenie ręcznej konfiguracji,
poprawa kontroli przepływu i rozpoznawanie wąskich gardeł,
specjalne mechanizmy do wykrywania i nadzoru sąsiadów w przypadku zastosowania w routerach.Szczegóły nagłówka IPv6

Uproszczenie struktury nagłówka to jedna z najważniejszych nowości w specyfikacji IPv6. W odróżnieniu od swojego odpowiednika z protokołu IPv4 nagłówek IPv6 został zredukowany do niezbędnego minimum. Umożliwia to jego szybszą obróbkę i przyśpiesza transport przez routery.

Nowe adresy

Z kolei niewątpliwie najważniejszą zmianą, jaką przynosi IPv6, jest powiększenie przestrzeni adresowej IP. Długo nie można było znaleźć odpowiedzi na pytanie, ile bajtów tak naprawdę jest potrzebne. Doświadczenia wynikające z przydzielania adresów IPv4 pokazują, że w rzeczywistości wykorzystywany jest tylko ułamek liczby możliwych adresów. Powodem jest przestarzały podział na stałe klasy. W sieci klasy C wykorzystuje się w praktyce zaledwie około 2,5 tysiąca z dostępnych 65 tysięcy adresów.

Zwiększenie długości adresu z 32 do 128 bitów daje 2128 możliwych adresów IP. Oznacza to dokładnie astronomiczną liczbę 340 282 366 920 938 463 463 374 607 431 768 211 456 różnych wartości. Ponieważ przeciętny śmiertelnik nie jest w stanie objąć rozumem takiej liczby, sprytni rachmistrze wymyślili porównanie, które robi nie mniejsze wrażenie - ta liczba wystarcza, aby każdemu kilometrowi kwadratowemu powierzchni Ziemi przypisać 665 570 793 348 866 943 898 599 adresów. Jak widać, nic już nie stoi na przeszkodzie, by każda pralka automatyczna otrzymała swój adres IP.

Format adresów IPv6

Również w czasach stosowania Domain Name System (DNS) użytkownik styka się sporadycznie z adresami IP. W uproszczonej pisowni protokołu IPv4 cztery bajty adresu zapisywane są jako zwykłe liczby dziesiętne. Poszczególne bajty rozdzielane są kropką, na przykład 127.0.0.1. W przypadku nowych, 128-bitowych adresów protokołu IPv6, tak zapisywane adresy miałyby bardzo niepraktyczną postać.

Z tego względu IPv6 korzysta z systemu szesnastkowego. Umożliwia on przedstawienie nawet dłuższych grup liczb w sposób bardziej zwarty. Tworzy się grupy po dwa bajty i rozdziela je dwukropkiem, na przykład 0000:0000:0000:3210:0123:4567:89AB:CDEF. W ramach jednej grupy można pominąć początkowe zera. Aby jeszcze bardziej skrócić ciągle dość długi adres, można zastąpić grupę następujących po sobie zer dwoma dwukropkami.

Zgodnie ze specyfikacją IPv6, można zachować w przestrzeni adresowej dotychczasowe adresy IPv4. W takim przypadku stosuje się zapis mieszany - ::FFFF:127.0.0.1 odpowiada 0:0:0:0:0:FFFF: 7F00:0001.

Rodzaje adresów IPv6

Internet Engineering Task Force (IETF) ustaliła wraz z innymi gremiami, m.in. Internet Architecture Board (IAB, http://www.iab.org i Internet Society (ISOC, http://ww.isoc.org), że adresami IPv6 zarządzać będzie centralnie Internet Assigned Numbers Authority (IANA). Adresy IPv6I, w przeciwieństwie do adresów IPv4, nie są przydzielane raz na zawsze. Nowe bloki adresowe będzie można unieważniać, gdy okaże się to konieczne z przyczyn technicznych lub z powodu nadużycia. IPv6 rozróżnia trzy rodzaje adresów:
Adresy unicast - ten typ adresu jest identyfikatorem interfejsu w komputerze lub routerze. Datagram wysyłany pod adres typu unicast jest dostarczany do interfejsu identyfikowanego za pomocą adresu.
Adresy anycast - identyfikator grupy interfejsów w urządzeniu lub wielu urządzeniach.
Adresy multicast - definiują grupę. Datagram wysłany pod adres typu multicast dociera do wszystkich interfejsów należących do grupy.Bezpieczeństwo i ICMP

Aspekt bezpieczeństwa odgrywał pierwszoplanową rolę od samego początku prac nad IPv6. Zdefiniowano standardy bezpieczeństwa, które mogą być stosowane zarówno w IPv4, jak i IPv6. Dzięki nim możliwe jest zapobieganie atakom z wykorzystaniem zmiany adresu lub podsłuchiwania komunikacji. Poszczególne procedury bezpieczeństwa dzielą się na następujące obszary:
szyfrowanie jako zabezpieczenie przed nieuprawnionym dostępem do wiadomości,
uwierzytelnianie wiadomości za pomocą sumy kontrolnej jako dowód integralności wiadomości,
uwierzytelnianie nadawcy za pomocą podpisu cyfrowego.
Całość ma uniemożliwić osobie nieuprawnionej odczytanie wiadomości na drodze od nadawcy do odbiorcy. Pełne szyfrowanie zapewnia ponadto, że wiadomość nie zostanie zmieniona. Druga z metod nie wymaga szyfrowania danych. Tworzona jest suma kontrolna do bloku danych, zabezpieczanego kluczem. Zastosowanie sumy kontrolnej o wartości znanej tylko nadawcy daje jednocześnie bezpieczną metodę identyfikacji nadawcy.

IPv6 wykorzystuje Internet Control Message Protocol (ICMP) z kilkoma rozszerzeniami. Obecność elementów protokołu ICMP sygnalizuje w wersji 6 wartość 58 w polu Next Najważniejsze zmiany w ICMP to:
nowe formaty tłumaczenia nazw zamiast stosowanego dotychczas Address Resolution Protocol (ARP),
elementy definicji maksymalnej wielkości pojedynczej transmisji (MTU - maximum transmission unit),
nowe elementy sterowania grupami multicast zamiast Internet Group Management Protocol (IGMP) protokołu IPv4.Zastosowania

Co oznacza IPv6 dla użytkownika? Należy, a może wręcz trzeba się postarać o nowy stos TCP/IP do komputera? A może wręcz o nowszą wersję systemu operacyjnego?

W tej chwili można jeszcze spać spokojnie. W Internecie nadal panuje niepodzielnie IPv4 i tak będzie jeszcze przez jakiś czas. Są już wprawdzie pierwsze wdrożenia IPv6, jednak najważniejsze komponenty, serwery DNS i routery, nie zostały jeszcze "przezbrojone".

Tymi problemami użytkownik nie musi się martwić. Mechanizm dual stack (podwójny stos) automatyzuje komunikację z nowymi hostami IPv6 i starymi IPv4 - przynajmniej w teorii. W przypadku poprawnej implementacji IPv6 nie powinny występować problemy. Na pewno jednak pojawią się jakieś niespodzianki.

DNS - nazwy zamiast liczb

Wszystkie komputery w sieci TCP/IP identyfikowane są za pomocą jednoznacznego adresu IP. Jego postać liczbowa o długości 32 bitów jest skomplikowana i łatwo o błąd podczas wpisywania. Z tego powodu już w roku 1984 utworzono system nazw domen - Domain Name System (DNS). To właśnie dzięki niemu można połączyć się z hostem, używając przynależnej nazwy domeny, jak choćby pcworld.pl. DNS to rozproszona baza danych, której głównymi komponentami są serwery nazw. Zarządzają informacjami o odwzorowaniu (mapping), co polega na wzajemnym przyporządkowaniu adresów IP i nazw komputerów.

Gdy jeszcze nie było Internetu obecnej postaci, a ARPAnet łączył kilkaset komputerów, wszystkie informacje o hostach mieściły się w jednym pliku. Plik ten musiał się znajdować w każdym komputerze podłączonym do sieci ARPAnet; zawierał wszystkie informacje związane z odwzorowaniem.

System nazw domen usunął podstawowe wady tablic nazw opartych na plikach:
DNS daje się łatwo rozszerzać,
ma postać rozproszonej bazy danych i gwarantuje, że informacje o nowych komputerach i zmianach w razie potrzeby dotrą do wszystkich użytkowników Internetu.Hierarchiczna struktura DNS

Domain Name System jest rozproszonym, hierarchicznym systemem konwersji nazw komputerów na adresy IP. Nie ma centralnej bazy danych zawierającej całość informacji o komputerach w Internecie. Takich informacji udzielają tysiące tzw. serwerów nazw.

Baza danych DNS ma strukturę drzewa i jest podzielona na strefy; korzenie stanowią odpowiednik katalogu głównego (root). Aby znaleźć informację o jakiejś domenie, trzeba przejść od domeny głównej (root), przez podrzędne, do docelowej. Każdej nazwie domeny odpowiada jeden węzeł w hierarchii DNS.

Bezpośrednio pod domeną główną znajdują się domeny wysokiego poziomu Top Level Domains (TLDs). Są dwa ich rodzaje - geograficzne (według ISO 3166-1, tak zwane ccTLDs), na przykład .pl, oraz organizacyjne. Siedem pierwotnych domen organizacyjnych nazywa się generycznymi TLDs.

Niektóre kraje tworzą domeny drugiego poziomu (second level domains) zgodnie z regułami tworzenia generycznych domen wysokiego poziomu. Przykładem może być co.uk dla przedsiębiorstw komercyjnych w Wielkiej Brytanii. Na stronach www.denic.de można znaleźć zbiór łączy do źródeł z informacjami o historycznym rozwoju domen wysokiego poziomu.

Nazwy domen

Nazwy domen zapisuje się od najniższego poziomu, nazwy komputera, do najwyższego poziomu, czyli Top Level Domain. Domena główna ma postać kropki.

Tego rodzaju nazwę domeny określa się jako absolute domain name lub fully qualified domain name (FQDN). Tak więc pcworld.pl. jest FQDN domeny drugiego poziomu (second level domain) pcworld w domenie wysokiego poziomu (top level domain) .pl. Kończąca nazwę kropka znajduje się tu zamiast domeny głównej. Nazwy domen rzadko pisze się w postaci fully qualified domain name. Kropka na oznaczenie domeny głównej jest z reguły pomijana.

Przydziałem nazw domen zajmuje się wiele firm i instytucji. Zarządzanie geograficznymi domenami wysokiego poziomu znajduje się w gestii poszczególnych krajów. Domeną .pl

zarządza NASK - Naukowa i Akademicka Sieć Komputerowa. Generycznymi domenami wysokiego poziomu, jak .com lub .edu, zarządzają Stany Zjednoczone. Wiele z tych nazw domen może być rejestrowanych tylko przez instytucje działające na terenie Stanów Zjednoczonych. Na przykładu .edu jest zastrzeżone dla amerykańskich instytucji oświatowych. Polski uniwersytet może zarejestrować jedynie nazwę z końcówką .edu.pl.

Rejestracja domen

Ten, kto rejestruje domenę .pl, uzyskuje jedynie prawo użytkowania. Wnioskodawca ponosi odpowiedzialność za naruszenie praw osób trzecich.

Oprócz tego są różne reguły, których należy przestrzegać. Nazwa domeny nie może się rozpoczynać ani kończyć myślnikiem, nie może liczyć więcej niż 63 znaki, dozwolone są tylko znaki alfabetu łacińskiego i cyfry.

Więcej informacji na temat rejestracji domen znajdziesz pod adresem http://www.nask.pl .

Serwery nazw

Wniosek o przyznanie nazwy domeny musi zawierać adresy co najmniej dwóch serwerów nazw, tzw. primary name server oraz secondary name server. Zajmują się obsługą nazwy danej domeny. Jeżeli wniosek o przyznanie domeny zostanie rozpatrzony pozytywnie, w Domain Name System (DNS) zostają wpisane wskaźniki (pointer) do odpowiednich serwerów nazw.

Serwery nazw zawierają informacje o odwzorowaniu tych domen (mapping), których obsługą się zajmują. Polega to na wzajemnym przyporządkowaniu adresów IP do nazw komputerów, podobnie jak we wcześniejszych tablicach nazw.

Primary name server oraz secondary name server muszą działać niezależnie od siebie, a pod względem technicznym być na tyle niezawodne, żeby przynajmniej jeden z nich był zawsze dostępny. Różnica pomiędzy nimi polega na tym, że secondary name server pobiera wszystkie istotne dane z primary name server i w efekcie pracuje jako serwer kopii zapasowej.

Wszelkich zmian dokonuje się zatem tylko na primary name server. Pozostałe serwery aktualizują swoje dane w regularnych odstępach czasu, zwykle co trzy godziny.

Zapytanie serwera nazw

Gdy w przeglądarce internetowej wpiszesz nazwę domeny, z którą chcesz się połączyć, twój komputer wyśle zapytanie do serwera nazw w celu przetłumaczenia nazwy domeny na adres IP. Z reguły jest to serwer nazw twojego dostawcy usług internetowych, za pośrednictwem którego łączysz się z Internetem.

A jeżeli na serwerze nazw nie ma żądanych danych? Musi on przekierować zapytanie do innego serwera nazw, a przy tym nie musi akurat wiedzieć, który z innych serwerów nazw jest właściwy dla tego zapytania lub na którym przechowywane są żądane dane. Wystarczy jednak, że każdy serwer nazw wie, jak skontaktować się z tzw. serwerem głównym (root serwer). Zna on adresy wszystkich autorytatywnych serwerów nazw dla wszystkich domen drugiego poziomu.

Aby zmniejszyć obciążenie sieci, wszystkie serwery nazw dysponują pamięcią cache, w której zapisane jest każde wystosowane zapytanie DNS. Gdy któryś z komputerów zażąda tłumaczenia wcześniej tłumaczonej nazwy, serwer nazw odwołuje się do pamięci

cache. Dane te mają określony czas życia (Time to Live / TTL). Po jego upływie - po dwóch dniach - zapytanie o domenę musi przejść pełną drogę od nowa.

Pamięć cache serwera nazw ma jedną istotną wadę - w przypadku zmiany dostawcy usług internetowych zmieniają się zwykle również serwery nazw.

Może się zatem zdarzyć, że niektóre serwery nazw jeszcze przez dwa dni po zmianie będą przechowywały adresy starych serwerów nazw w pamięci cache. Wszelkie zapytania kierowane do serwerów ze starymi danymi będą więc trafiały w próżnię.

Serwery główne

Jak już wspomniano, każdy primary name server musi znać adresy wszystkich serwerów głównych. Obecnie na całym świecie jest 13 serwerów głównych:

Rozmieszczenie wszystkich serwerów głównych można obejrzeć online pod adresem http://www.wia.org/pub/rootserv.html . Uderzające, że tylko trzy serwery główne znajdują się poza terytorium Stanów Zjednoczonych. To niewątpliwie jeden z przejawów starań, żeby zachować kontrolę nad Internetem.

DNS resolver

Każdy klient sieciowy, który chce odwołać się do hosta internetowego, ale zna tylko jego nazwę domeny, musi, jak wspomniano, skorzystać z pomocy serwera nazw. Odbywa się to za pomocą tak zwanego resolvera.

Należy zwrócić uwagę, że resolver nie jest samodzielnym programem. To raczej biblioteka procedur programowych, kodów tłumaczących; każdy program, który poszukuje adresu, musi połączyć się z tą biblioteką. Właśnie ona "wie", jak formułować zapytania o komputery do serwera nazw.

Resolver ma zasadniczo trzy zadania:
Tworzy zapytanie i przesyła je do serwera nazw. Z reguły jest serwer nazw twojego dostawcy usług internetowych, za którego pośrednictwem łączysz się z Internetem.
Jeśli tłumaczenie się powiedzie, interpretuje odpowiedź serwera nazw.
Na zakończenie resolver przesyła informacje do programu, który zażądał danych, na przykład do przeglądarki internetowej.Pod kontrolą systemów UNIX i Windows resolver wywoływany jest za pomocą poleceń gethostbyname oraz gethostbyaddr. Pierwsze polecenie ustala adres IP nazwy domeny, drugie - główną nazwę domeny znanego adresu IP.

Rekurencyjne i iteracyjne tłumaczenie nazw

Zasadniczo stosuje się dwa typy zapytań - rekurencyjne i iteracyjne tłumaczenie nazw. W obu przypadkach klient przekazuje nazwę hosta i określa typ zapytania.

Najdogodniejsze dla klienta jest postawienie zapytania rekurencyjnego. Wówczas serwer nazw, do którego skierowano zapytanie, odpowiada za kompletne tłumaczenie nazwy. Odpytuje po kolei wszystkie serwery, aż do pełnego przetłumaczenia nazwy. Zalety tego typu zapytania: resolver musi zainicjować tylko jedno zapytanie, przyjąć odpowiedź i przekazać ją do odpowiedniej aplikacji.

W przypadku iteracyjnego tłumaczenia nazw serwer nazw dostarcza jedynie adres serwera, który trzeba zapytać jako następny w kolejności. W związku z tym resolver musi samodzielnie formułować kolejne zapytania do odpowiedniego serwera nazw aż do chwili, gdy nazwa zostanie w pełni przetłumaczona.

Rekordy zasobów usług

System nazw domen (DNS) przechowuje informacje o hostach w tak zwanych rekordach zasobów usług (Resource Records - RRs). Jest 20 rodzajów RRs.

Rekordy zasobów usług przesyłane są do klienta w odpowiedzi na pytanie. W tym celu dołączane są do nagłówka DNS.

Rekord zasobów usług w odpowiedzi DNS zawiera sześć pól:

Są ponadto też tak zwane mail exchange records (MX Records), które mają znaczenie dla wysyłania poczty elektronicznej.

Wiadomości DNS

Resolver i serwer wymieniają zapytania i odpowiedzi w postaci tak zwanych wiadomości DNS. Mają one jednolity format - po nagłówku o długości 12 bajtów następują rekordy zasobów usług.

Domena .in-addr.arpa

Domena .arpa była pierwszą domeną wysokiego poziomu, później zastąpiły ją kolejne. Domena wysokiego poziomu .arpa żyje jednak nadal własnym życiem w połączeniu z domeną drugiego poziomu in-addr. W domenie in-addr.arpa znajdują się wpisy DNS tzw. reverse mapping, za pomocą których można tłumaczyć znane adresy IP na nazwy domen. Zapytania reverse mapping określane są również jako pointer queries.

Domena in-addr.arpa nazywana jest również domeną odwrotną (inverse domain). Tworzy się ją przez odczytanie adresu IP od tyłu i dołączenie ciągu do .in-addr.arpa. Na przykład informacje reverse mapping o adresie IP 62.96.227.70 znajdują się w nazwie domeny 70.227.96.62.in-addr.arpa.

W celu przetłumaczenia adresu IP na nazwę domeny resolver musi sformułować zapytanie w postaci Bure Type = PTR, Query Class = 1 oraz Query Name = 70.227.96.62.in-addr.arpa.

W odpowiedzi serwer zwróci 70.227.96.62.in-addr.arpa = PTR tecchannel.de.

Protokoły - TCP czy UDP?

System nazw domen (DNS) obsługuje zarówno protokół TCP, jak i UDP, w obu przypadkach przez port 53. Powstaje pytanie, kiedy jest stosowany każdy z tych protokołów?

Resolver formułuje zapytania z reguły z użyciem protokołu UDP. Może się jednak zdarzyć, że odpowiedź jest większa niż 512 bajtów. W takim przypadku do nagłówka odpowiedzi wstawiany jest bit TC i przesyłane jest tylko 512 pierwszych bajtów.

Resolver musi wówczas powtórzyć zapytanie z użyciem protokołu TCP/IP, a odpowiedź zostanie przesłana w postaci wielu segmentów.

Protokół TCP jest natomiast generalnie wykorzystywany do uaktualniania informacji między serwerami nazw. Ze względu na dużą ilość danych w tym wypadku tylko wspomniany protokół wchodzi w grę.

Nowe domeny wysokiego poziomu

Od kilku lat trwa ożywiona dyskusja nad uzupełnieniem wykorzystywanych dotąd domen wysokiego poziomu nowymi domenami. Proponowane były między innymi domeny .firm, .shop czy .web.

Zarządzająca nazwami domen organizacja ICANN (http://www.icann.org) zatwierdziła 16 listopada 2000 roku siedem nowych domen wysokiego poziomu. Zestawienie przedstawiamy obok.

Ethernet 10-gigabitowy

Większość sieci lokalnych opiera się na standardach ethernetowych 10Base-T (10 Mb/s; IEEE802.3i) oraz 100Base-TX (100 Mb/s; IEEE802.3u, 1995). Od pewnego czasu coraz większe znaczenie zyskuje też Ethernet gigabitowy. Jego typowe zastosowania to sieć szkieletowa oraz połączenia punkt-punkt między sieciami. Największe znaczenie mają warianty 1000Base-SX i LX z kablem światłowodowym (IEEE802.3z, 1998) oraz 1000Base-T (IEEE802.3ab, 1999) ze skrętką kat. 5.

Nowy standard IEEE 802.3ae, czyli Ethernet 10-gigabitowy, to zwiększenie szybkości transmisji o kolejny rząd wielkości. Technologia zdecydowanie wykracza więc poza zakres zastosowań LAN i w stronę obszaru sieci miejskich (MAN) i rozległych (WAN).

Ethernet 10-gigabitowy w sieciach LAN i WAN

Ethernet 10-gigabitowy ma nad innymi standardami zdecydowaną przewagę - nawet bardzo rozległe topologie sieci można zrealizować w jednolitej technologii, opartej na IP i Ethernecie. Dzięki temu odpada problem konwersji protokołów w warstwie przesyłowej wraz ze wszystkimi związanymi z tym problemami i koniecznymi kompromisami. To nie tylko ułatwia łączenie rozproszonych terytorialnie sieci LAN. Nowa technologia obiecuje również znaczące obniżenie kosztów, na przykład w wyniku łączenia rozproszonych punktów dostępowych (POP) ponadregionalnych dostawców Internetu. W ten sposób Ethernet 10-gigabitowy (10GE) to nie tylko potencjalny zamiennik technologii ATM, która w zakresie niższych szybkości transmisji i tak już znacznie straciła znaczenie. Ethernet 10G konkuruje również z co najmniej tak samo szybkimi technologiami WAN, jak SONET/OC-192 lub SDH/STM-64.

Wymagania i cele

Z licznych wymagań, które odgrywały znaczącą rolę podczas definiowania standardu Ethernetu 10G, trzy najważniejsze cele to: nowa technologia powinna być maksymalnie kompatybilna z obowiązującymi standardami, oferować podobnie korzystną strukturę kosztów, a także wykorzystywać stosowane interfejsy i typy okablowania.

Jako wartość graniczną kosztów przyjęto współczynnik x2-, najwyżej x3 w stosunku do instalacji Ethernetu gigabitowego. W stosunku do typowych dla sieci WAN systemów SONET/SDH oznacza to w każdym razie oszczędność kosztów rzędu minimum 30 procent. Wynika to przede wszystkim z trzech czynników:
Ethernet 10G korzysta z tych samych zasadniczych formatów i technologii Ethernetu, np. transmisja odbywa się nadal asynchronicznie, a ekonomiczne przełączniki typu "store and forward" mogą sprostać wymaganiom ruchu w sieci. Oznacza to także istotne oszczędności zarówno na etapie projektu i produkcji, jak i podczas eksploatacji i administracji.
W zakresie nośników transmisji Ethernet10G ma zaledwie kilka elementarnych wymogów jakościowych.
Zapewnia szereg fizycznych protokołów transportowych, które można zoptymalizować kosztowo zależnie od odległości, jakie mają obejmować łącza.Kompatybilność

Ethernet 10G powinien być kompatybilny z wieloma innymi standardami, w tym z:
składnikami standardu IEEE802.3, jak 802.1p (multicast), 802.3q (VLAN) i 802.3ad (Link Aggregation);
standardami IETF, jak Simple Network Management Protocol (SNMP), Multi-Protocol Label Switching (MPLS) i Remote Monitoring for Ethernet (RMON);
standardami z otoczenia OSI (Open Systems Interconnection). Powiązanie z cechami Ethernetu zapewnia korzyści w stosunku do rozwiązań konkurencyjnych, np. zachowanie formatu i długości ramek IEEE802.3 powoduje, że przełączanie jest szybsze niż w

technologiach WAN, ponieważ nie trzeba dopasowywać zarówno ramek (segmentacja i rekonstrukcja), jak i adresów.Nośnik transportowy światłowód

Już podczas standaryzacji Ethernetu gigabitowego zastanawiano się, czy komercyjne przesyłanie kablami miedzianymi ma sens. Ostatecznie po długich dyskusjach przyjęto w końcu standard 1000Base-T. Umożliwia on przesył skrętką kat. 5 na odległość do 100 m. Jednak już wówczas było dla wszystkich jasne, że następny próg szybkości można będzie, a nawet należy pokonać już tylko z użyciem światłowodów. Stosownie do tych uzgodnień Ethernet 10G przewiduje do topologii gwiaździstych tylko połączenia optyczne punkt-punkt.

Już podczas standaryzacji Ethernetu gigabitowego okazało się ponadto, że wykorzystanie stosowanego okablowania LAN jest warunkiem komercyjnego sukcesu standardu sieciowego. W jeszcze większym stopniu zasada ta odnosi się do okablowania sieci WAN, bo znajduje się ono w domenie publicznej. Ewentualne rozszerzenia lub dostosowania wymagałyby dużych nakładów. Dlatego właśnie Ethernet 10G definiuje aż siedem możliwych interfejsów fizycznych do już eksploatowanych typów okablowania LAN i WAN.

Interfejs niezależny od nośnika

Wielość możliwych interfejsów fizycznych wywołuje skutki przede wszystkim w odniesieniu do aktywnych komponentów sieciowych - interfejsy niezależne od nośnika zyskują znaczenie zarówno dla producentów, jak i użytkowników. Tego rodzaju interfejsy przewidziano już w pierwszych standardach Ethernetu. Miały umożliwiać elastyczne i ekonomiczne sprzężenie ze złączami fizycznymi. Jednak tzw. Attachment Unit Interfaces (AUI) do Ethernetu 10 Mb/s względnie Media Independent Interfaces (MII) do Fast Ethernetu praktycznie nie mają już dziś żadnego znaczenia.

Z wyjątkiem styku LAN-LAN, gdzie ze względu na konieczność pokonania większych odległości stosuje się zwykle światłowody, niemal powszechnym standardem stało się złącze RJ45 na kablu-skrętce. W tej sytuacji długo nie przykładano specjalnej wagi do modularności i elastyczności. Po wprowadzeniu Ethernetu 10G może się to zmienić.

Pełny dupleks jako standard

Pierwotny standard Internetu IEEE 802.3 przewidywał zastosowanie kabla koncentrycznego w topologii magistrali jako fizycznego nośnika. Nośnik fizyczny jest jednocześnie dostępny wszystkim uczestnikom komunikacji (shared medium). Ogranicza to komunikację do trybu półdupleksowego. Wprowadzenie skrętki jako nośnika umożliwiło jednak fizyczne rozdzielenie kanału nadawczego od odbiorczego, a tym samym jednoczesną komunikację w obu kierunkach (pełny dupleks). Dało to znaczne korzyści w zakresie połączeń między aktywnymi węzłami, jak mosty i przełączniki. Pełna szybkość transmisji 10 Gb/s ma obecnie sens chyba tylko pomiędzy aktywnymi komponentami. Dlatego, a ponadto ze względu na przesyłanie wyłącznie kablami światłowodowymi, tryb pełnego dupleksu jest nieodzowny w Ethernecie 10G.

Już w trakcie wprowadzania Ethernetu gigabitowego okazało się, że tryb półdupleks nie ma w praktyce żadnego znaczenia. Niewykluczone, że sytuacja ta może się niedługo zmienić wraz z upowszechnieniem się okablowania gigabitowego bezpośrednio do komputerów. Podobny scenariusz jest jednak z dzisiejszego punktu widzenia nieprawdopodobny w odniesieniu do systemów 10-gigabitowych.

W ten sposób Ethernet 10-gigabitowy kończy erę nasłuchiwania łącza i usuwania kolizji, czyli technikę zwaną CSMA/CD (Carrier Sense with Multiple Access/Collision Detection).

IEEE - tak rodzą się standardy

Standard Ethernetu 10G jest dziełem Standards Association (SA) amerykańskiego stowarzyszenia zawodowego IEEE, czyli Institute of Electrical and Electronics Engineers. Samo opracowanie standardu również polega na przestrzeganiu szeregu standardów. Po wyszukaniu sponsorów projektu i formalnym utworzeniu grupy studialnej oraz roboczej rozpoczyna się odliczanie czteroletniego terminu. W tym okresie standard musi zostać zatwierdzony. Zwykle w tym celu powołuje się jeszcze grupę zadaniową, która dopracowuje szczegóły standardu.

Projekt jest najpierw rozpatrywany przez grupę roboczą, a następnie przekazywany grupie sponsorów pod głosowanie. Jeśli frekwencja w głosowaniu sponsorów wyniesie co najmniej 75 procent i minimum 75 procent głosów będzie na tak, standard uznaje się za formalnie przyjęty i publikuje się go. Harmonogram czynności związanych z zatwierdzeniem standardu IEEE802.3ae przedstawiamy w diagramie.

Standard 802.3ae

Podział standardu Ethernetu 10G na obszary Logical Link Control (LLC), Nośnik Access Control (MAC) i złącze fizyczne jest zgodny z innymi standardami obowiązującymi w ramach IEEE 802.3.

Szczególne znaczenie praktyczne ma przy tym, że wywołanie modułu ethernetowego odbywa się poprzez jednolite dla wszystkich standardów częściowych rodziny IEEE802.3 warstwy LLC. Podobnie jak w dotychczasowych wariantach Ethernetu, podzielono funkcjonalność na różne podwarstwy w celu uzyskania jeszcze większej modularności budowy. W kolejnych rozdziałach przedstawiamy więcej szczegółów na ten temat.

Warstwa MAC

Warstwa MAC realizuje trzy zadania o podstawowym znaczeniu, związane z budową ramki przesyłowej, dopasowaniem stopni szybkości i dostępem do głębiej leżących warstw przekazu fizycznego. Struktura ramek Ethernetu 10G jest przy tym całkowicie zgodna ze strukturą ramek innych wariantów Ethernetu.

Oznacza to, że:
format adresu jest zgodny ze zwyczajowym schematem IEEE,
korekcja błędów (frame checking sequence - FCS) opiera się nadal na 32-bitowym CRC,
mogą być tworzone tzw. ramki jumbo, zawierające do 9000 bajtów,
minimalna długość pakietu, wynosząca 64 bajty, jest zgodna z odpowiednim parametrem systemów 10/100 Mb/s,jak również
możliwy jest podział przestrzeni adresowej w wirtualnych sieciach LAN zgodnie z IEEE802.1q.Aktywne komponenty 10G służą nie tylko do połączeń z szybkością 10 Gb/s, lecz w razie potrzeby obsługują wolniejsze strumienie danych. Chodzi przede wszystkim o Ethernet gigabitowy, możliwe jest jednak również sprzężenie z systemami SONET poziomu OC-192. Niemal identyczna szybkość transmisji (9,5884640 Gb/s) wymaga jedynie niewielkiego dostosowania.

XGMII

Podobnie jak dotychczasowe standardy Ethernetu, 802.3ae zawiera również specyfikację złącza niezależnego od nośnika między warstwami MAC a PHY. Obłożenie poszczególnych kabli złącza 10 Gigabit Medium Independent Interface (XGMII - X to w tym przypadku rzymska liczba 10) zostało przedstawione w tabeli na str. 15. Złącze przesyła dane równolegle, 32-bitowymi magistralami w kierunku nadawania i odbioru. Z uwzględnieniem niezbędnych sygnałów sterujących i taktujących daje to złącze o 74 przewodach.

XAUI

Złożone, zewnętrzne złącze, jak XGMII, to znaczne koszty i wysokie wymagania odnośnie synchronizacji równoległych linii danych. Dlatego też IEEE dodatkowo zdefiniował tzw. XAUI (10 Gigabit Attachment Unit Interface). Ta uproszczona wersja złącza XGMII zadowala się zaledwie 16 przewodami. Samotaktująca magistrala opiera się bezpośrednio na standardzie 1000Base-X, ale przewody danych eksploatowane są z dwuipółkrotną szybkością, a więc 2,5 Gb/s. W ten sposób czterema równoległymi parami przewodów można przesłać 10 Gb/s. Ponadto XAUI wykorzystuje znane z 1000Base-X skuteczne kodowanie 8B/10B. Złącze charakteryzuje się wysoką tolerancją elektromagnetyczną, stosunkowo dużą stabilnością w zakresie różnic czasów przebiegu i odpornością na zakłócenia przesyłu.

Za pomocą obu złączy XGMII i XAUI można wysterować wszystkie przewidziane w standardzie typy PHY, ponadto można bezpośrednio wykorzystać równoległy przekaz XAUI o szerokości 4 bitów w ramach substandardu 10GBase-LX4.

Warstwa PHY

Warstwa PHY Ethernetu 10-gigabitowego dzieli się na cztery podwarstwy PCS, WIS, PMA i PMD. Physical Coding Sublayer (PCS) odpowiada za kodowanie strumienia danych, który ma być przesłany. Physical Nośnik Attachment (PMA) i Physical Nośnik Dependent (PMD) dbają o połączenie z danym nośnikiem. WAN Interface Sublayer (WIS) dostosowuje szybkość transmisji w dalekosiężnych wariantach systemu do szybkości transmisji systemów SONET/SDH. Tabela na następnej stronie przedstawia najważniejsze parametry substandardów w zależności od wyboru nośnika fizycznego i obszaru zastosowań.

LAN-PHY kontra WAN-PHY

Wśród warstw PHY mają swoje warianty. LAN-PHY służy do bezpośredniego zwiększenia szerokości pasma czystych systemów ethernetowych. Ruch odbywa się po nieaktywnych włóknach światłowodowych (dark fiber). Substandardy LAN-PHY można rozpoznać po literze R w nazwie.

Z kolei WAN-PHY łączy systemy ethernetowe i systemy SONET/SDH. Według założeń architektów Ethernetu 10G, wariant ten jest tylko rozwiązaniem etapowym w dążeniu do czystego, globalnego Ethernetu. różni się od wariantu LAN jedynie dodatkową podwarstwą WAN Interface Sublayer (WIS), która w uproszczony sposób tworzy ramki SONET/SDH. Substandardy WAN-PHY wyróżnia litera W w nazwie.

LAN-PHY i WAN-PHY eksploatowane są na tych samych warstwach PMD i w związku z tym uzyskują identyczny zasięg. Rozróżnienie odnosi się zatem nie do uzyskiwanych odległości transmisji, lecz sygnalizuje jedynie, czy wykorzystywana jest infrastruktura WAN. W rzeczywistości w trakcie standaryzacji dyskutowano gorąco, czy rozróżnienie między WAN-PHY a LAN-PHY faktycznie musi mieć wpływ na odległość transmisji (short haul/long haul - krótkodystansowa/długodystansowa). Ostatecznie zdecydowano się na rezygnację z dopasowania odległości. Ogólnie rzecz biorąc, podział na LAN-PHY i WAN-PHY był i jest dyskusyjny, natomiast opracowanie jednolitego modułu fizycznego (Unified PHY) pozostaje nadal sprawą otwartą.

Physical Coding Sublayer

Ponieważ są różne standardy Ethernetu, stosowano już wiele różnych technik kodowania. Ich zakres rozciąga się od kodowania Manchester, pochłaniającego dużą część szerokości pasma, do oszczędnego kodowania Trellis w 1000Base-T. W trakcie definiowania standardu Ethernetu 10G temat ten ponownie wzbudził dyskusje.

Ogólnie rzecz biorąc, przydatność konkretnej metody kodowania zależy z jednej strony od dostępnej szerokości pasma, z drugiej zaś - od wymagań dotyczących stopy błędów bitowych. Poszczególne techniki różnią się zasadniczo stosunkiem liczby bitów informacyjnych do liczby bitów przesyłanych. Im więcej bitów w sumie przypada na bit informacyjny, tym łatwiej uniknąć składowej stałej i uzyskać synchronizację odbiornika. Transmisja bitów nadmiarowych umożliwia dodatkowe rozpoznawanie lub korekcję błędów. Jednak im więcej bitów trzeba przesłać, tym większe są wymagania co do szerokości pasma nośnika transmisji.

Do Ethernetu 10G IEEE wybrał dwie techniki kodowania. W wersji 10GBase-LX4 stosuje się kodowanie 8B/10B, w którym przesyła się 10 bitów na bajt. W wypadku czterech równoległych strumieni danych o użytecznej szybkości transmisji 2,5 Gb/s szybkość brutto wynosi odpowiednio 3,125 Gb/s w każdym z kanałów lub 12,5 Gb/s ogółem. Tak duża nadwyżka nieużyteczna wydawała się nieefektywna w transmisji szeregowej, dlatego stosuje się tam kodowanie 64B/66B, które 64 bity użyteczne kodowane za pomocą 66 bitów, które trzeba przesłać. Potrzebna szerokość pasma przewyższa zatem użyteczny strumień danych zaledwie o 3 procent.

WIS - WAN Interface Sublayer

Podwarstwa WIS stosowana jest tylko w warstwach WAN-PHY. Jej zadaniem jest formatowanie (framing) danych i dostarczanie informacji zarządczych dla systemów SONET/SDH. Chodzi tu przede wszystkim o konwersję pakietów danych między systemami SONET (słowa 16-bitowe) a formatem Ethernetu 10G (słowa 66-bitowe).

PMD/PMA

W trakcie opracowywania fizycznego złącza do Ethernetu 10-gigabitowego musiano przyjąć wiele rozwiązań kompromisowych. Długo rozważano wiele wariantów. Należało rozstrzygnąć z punktu widzenia przyszłych rozwiązań technicznych i zastosowań komercyjnych, czy skoncentrować się na realizacji toru laserowego, czy na cyfrowej obróbce sygnału.

Stosunkowo prostszy tor laserowy wiąże się z większymi problemami w zakresie rozpoznawania i korekcji błędów. Ostatecznie wybrano jednak ten wariant - nie bez przyczyny. Układy CMOS stosowane do cyfrowej obróbki sygnału są skalowalne, co w przyszłości może dać oszczędności. Technika laserowa na to nie pozwala. Początkowo rozważano również zastosowanie MAS (Multi-Level Analog Signaling) z pięcioma możliwymi poziomami sygnału transmisyjnego - rozwiązanie znane z 1000Base-T. Propozycja ta nie uzyskała wystarczającego poparcia.

Obecnie wybrane rozwiązania cechuje przede wszystkim dążenie do wykorzystania w możliwie niezmienionej postaci eksploatowanych łączy światłowodowych. Do dyspozycji jest zatem Wavelength Division Multiplexing, a także techniki transmisji szeregowej.

Physical Medium Dependent

Ethernet 10-gigabitowy wykorzystuje do transmisji światłowodowej trzy popularne "okna optyczne" o długości fali 850, 1310 względnie 1550 nanometrów.

Najbardziej ekonomiczny wariant to transmisja z wykorzystaniem fal o długości 850 nm (oznaczenie literą S). Można w tym przypadku użyć nie tylko względnie taniego włókna wielomodowego, lecz również niedrogiego lasera typu VCSEL (Vertical Cavity Surface-Emitting Laser). Jego zaletą jest to, że pracuje bez dodatkowego chłodzenia. Niestety, jest to również jego wada - w tych warunkach uzyskuje moc zaledwie 0,35 mW. W połączeniu ze stosunkowo dużym tłumieniem w światłowodzie (ok. 3,5 dB/km) sprawia to, że możliwy do uzyskania zasięg nie przekracza 300 m.

Przy długości fali 1310 nm (oznaczenie literą L) możliwa jest transmisja zarówno z wykorzystaniem włókna wielomodowego (MMF), jak i jednodomowego (SMF). W wariancie MMF stosuje się laser FP (Fabry Perot Laser), wariant SMF wymaga lasera DFB (Distributed Feedback Laser). Oba typy lasera uzyskują moc rzędu 6 mW. W połączeniu z mniejszym współczynnikiem tłumienia włókna SMF (0,5 dB/km) pozwala to na uzyskanie zasięgu rzędu 15 km.

Podobne typy laserów pracują w wariancie z falą o długości 1550 nm (oznaczenie literą E). Używane są również w systemach SONET/SDH. Stosuje się tu jeszcze wyższe moce - rzędu 10 mW. Trzeba się jednak liczyć z większym rozproszeniem sygnału lub stosować specjalne, a więc drogie nośniki - DSF, Dispersion Shifted Fiber. Można w ten sposób uzyskać zasięg do 50 km.

Ethernet 10-gigabitowy kontra SONET/SDH

Komitet 10 Gigabit Ethernet Task Force zdefiniował opcjonalne złącze, dostosowane do szybkości transmisji i protokołów SONET OC-192 względnie SDH STM-64. SDH, Synchronous Digital Hierarchy, to podstawa infrastruktury na poziomie szkieletowym w nowoczesnych sieciach telekomunikacyjnych. Stosuje zwielokrotnienie z podziałem czasowym (Time Division Multiplexing, TDM) na łączach szeregowych. Nazwa pochodzi stąd, że wszystkie stacje synchronizowane są wzorcową częstotliwością taktującą, pozyskiwaną zwykle bezpośrednio z zegara atomowego (Stratum Clock). Wynikają stąd bardzo wysokie wymagania odnośnie jittera i synchroniczności sygnału taktującego.

Ethernet 10-gigabitowy stosuje natomiast asynchroniczny protokół transmisyjny, w którym dopasowanie w czasie i parametry synchronizacji obowiązują każdorazowo tylko dla jednego przesyłanego znaku. Każdy aktywny komponent może dokonywać niezależnej synchronizacji. Sprzężenie różnych domen synchronizacyjnych następuje na poziomie urządzeń takich jak mosty, routery i wzmacniaki. Dzięki temu implementacja fizycznych urządzeń transmisyjnych Ethernetu 10-gigabitowego wiąże się z niższymi kosztami niż w przypadku ich odpowiedników SDH.

Protokół transportowy

Pakiety ethernetowe i IP są już od dawna przesyłane za pośrednictwem systemów SONET/SDH. W tym celu wykorzystuje się tzw. transmisję zorientowaną pakietowo w systemach SONET/SDH (Packet-over-SONET/SDH - POS), co polega na umieszczaniu ramek w pakietach POS. Stosowane w tym wypadku protokoły to przede wszystkim High-Level Data Link Layer Control (HDLC) i Point-to-Point Protocol (PPP). W celu uzyskania bezpośredniego sprzężenia z sieciami ethernetowymi, które lepiej wykorzystują dostępną szerokość pasma, IEEE zdefiniował warstwę WAN-PHY. Dzięki temu oparte na pakietach przełączniki IP/ethernetowe mogą również korzystać z infrastruktury SONET/SDH. Używają jej do fizycznej transmisji na warstwie 1., są przy tym prostsze, a przede wszystkim tańsze od czystych komponentów SDH. Niemniej jednak komponenty Ethernetu 10-gigabitowego nie dają się sprzęgać bezpośrednio z infrastrukturą SONET/SDH, a jedynie z aktywnymi komponentami warstwy 1. (Line Terminal Equipment - LTE).

Szybkość transmisji i zarządzanie

Dostosowanie szybkości transmisji rozwiązano za pomocą sztuczki. Przy podłączeniu do WAN-PHY warstwa MAC wstawia pomiędzy pakiety ethernetowe dodatkowe znaki (Inter-Packet Gap - IPG). Po zredukowaniu szybkości transmisji netto te puste znaki zapewniają szybkość transmisji brutto 10 Gb/s. Liczba bajtów w IPG jest przy tym proporcjonalna do długości poprzedzającego pakietu. W kodowaniu 64B/66B dodatkowe bajty są usuwane,

dzięki czemu dalej przesyłany jest strumień netto dostosowany do przepływności SONET/SDH. Obniża to obciążenie po stronie systemu o mniej więcej jeden procent.

W celu zapewnienia ciągłego zarządzania w sieci WAN trzeba jednak dostosować nie tylko szybkość transmisji. Oprócz tego WAN-PHY komponentów Ethernetu 10-gigabitowego musi dostarczyć odpowiednich informacji administracyjnych w standardzie SONET/SDH. Zadanie to wykonuje WAN Interface Sublayer (WIS), który dodatkowo zapewnia konwersję ramek między formatami Ethernetu a SONET/SDH. W czystym Ethernecie stosuje się natomiast dużo prostszy protokół SNMP.

Przykład zastosowania

Za pomocą opisanych mechanizmów można rozszerzyć logicznie sieć Ethernet-LAN na infrastrukturę WAN. Ilustracja poniżej przedstawia konfigurację, w której ruch zorientowany pakietowo przesyłany jest przez SONET/SDH za pomocą 10-gigabitowego routera z WAN-PHY.

Nadchodzące pakiety warstwa IP routera A przesyła najpierw do 10-gigabitowego kontrolera ethernetowego. Tam warstwa MAC gromadzi ramki i przekazuje je do podwarstwy PCS do kodowania 64B/66B. Powstałe w ten sposób słowa 66-bitowe wędrują w postaci logicznie ciągłego strumienia danych do podwarstwy WIS. Ta z kolei przekazuje pakiety jako słowa 16-bitowe do podwarstwy PMD. W tym momencie może się już rozpocząć się transmisja optyczna za pomocą terminalu LTE, zgodnego z SONET/SDH. Terminal LTE dostosowuje bity danych do synchronicznej transmisji SONET/SDH. W tym celu przesyła je do bufora Jitter Elimination Buffer. Dodatkowo terminal LTE gromadzi informacje administracyjne i przesyła strumień danych do sieci SONET/SDH.

Po stronie odbiorczej strumień danych trafia najpierw do tamtejszego terminalu LTE, który przetwarza przede wszystkim informacje administracyjne. Ponieważ timing synchronicznej sieci SONET/SDH jest na znacznie wyższym poziomie, niż w asynchronicznej sieci Ethernetu 10-gigabitowego, odbiorczy terminal LTE może zrezygnować z synchronizacji. Przesyła dane bezpośrednio do podwarstwy PMD routera B, która zamienia sygnały optyczne na elektryczne. Te z kolei przesyłane są w postaci słów 16-bitowych do podwarstwy WIS, która sprawdza i zapisuje informacje zarządcze. Następnie słowa 66-bitowe przesyłane są do podwarstwy PCS, która je odkodowuje i wywołuje warstwę MAC. Warstwa MAC sprawdza bity kontrolne CRC. Jeżeli nie wykryje żadnych błędów transmisji, rozpakowuje ramki ethernetowe i na zakończenie przekazuje pakiet do warstwy IP routera B.

Perspektywy

Firmy, które stworzyły podstawy Ethernetu 10-gigabitowego, zrzeszyły się w organizacji 10 Gigabit Ethernet Alliance (http://www.10gea.org). Do członków-założycieli, 3Com, Cisco, Extreme Networks, Intel, Nortel, Sun i World Wide Packets, dołączyło około 100 firm działających w różnych obszarach, od techniki laserowej do produkcji systemów.

Oceniając produkty, można stwierdzić, że standard IEEE802.3ae został opracowany z uwzględnieniem praktycznej integracji. Producenci PHY uzyskują przepływność do 2,5 Gb/s wyłącznie na podstawie niedrogiej technologii CMOS. Możliwa obecnie do zastosowania technologia 180 nm stawia wprawdzie wysokie wymagania co do projektu układu, nie przekraczają one jednak granic możliwości.

Wiele firm zapowiedziało już - biorąc pod uwagę prototypy - wprowadzenie na rynek pierwszych produktów. Są wśród nich: Cisco z modułami 10-gigabitowymi, względnie kartami linii do przełączników Catalyst 6500 i routerów z serii 7600, a także Enterasys z 10-gigabitowymi modułami rozszerzeń do przełączników z rodziny Matrix E1. Biorąc pod

uwagę koszty rzędu 80 tysięcy dolarów w przypadku produktów Cisco, można przypuszczać, że pierwszymi użytkownikami sprzętu 10-gigabitowego będą operatorzy sieci MAN i WAN.

Tak funkcjonuje e-mail

Mimo nowych możliwości, jakie dają komunikatory, e-mail ciągle zyskuje na popularności i znaczeniu. Z badań rynku przeprowadzonych przez IDC wynika, że w roku 2005 można się spodziewać 36 miliardów e-maili dziennie! W roku 2000 w użyciu było około 505 mln skrzynek poczty elektronicznej, w roku 2005 tą formą komunikacji ma się już posługiwać ok. 1,2 mld użytkowników.

A wszystko zaczęło się w roku 1971 w sposób, który trudno byłoby nazwać spektakularnym. Technik w BBN, Ray Tomlinson, przesłał e-mail między dwoma komputerami, które były połączone w sieci ARPAnet. Poszukując rzadko używanego znaku dla wyróżnienia poczty elektronicznej odkrył @ i w ten sposób ustanowił symbol nowej epoki.

Kolejnym krokiem milowym w historii poczty elektronicznej było opracowane w roku 1981 przez Erica Allmana oprogramowanie Sendmail. Umożliwiło ono po raz pierwszy wysyłanie za pomocą programu pocztowego wiadomości jednocześnie do wielu sieci.

Dzisiejszy sukces e-maila był nie do przewidzenia w roku 1971 i wynalazek Thomlinsona zasłużył sobie tylko na kilka wzmianek w prasie. Dziś nie sposób wyobrazić sobie życia bez poczty elektronicznej, a dla wielu ludzi jest ona wręcz warunkiem funkcjonowania.

Poczta elektroniczna opiera się na trzech protokółach - SMTP do wysyłania oraz POP i IMAP do odbioru. Specyfikację każdego protokołu opisano w jednym lub kilku RFC.

SMTP - Simple Mail Transfer Protocol

Zadaniem Simple Mail Transfer Protocol (SMTP) jest niezawodny i wydajny transport wiadomości. SMTP jest niezależny od protokołu sieciowego; zwykle stosowany jest standardowy protokół Internetu, TCP. Komunikacja odbywa się przez port 25.

Za wymianę wiadomości odpowiadają tzw. mail transfer agents (MTA). Najbardziej znanym MTA jest Sendmail (http://www.sendmail.org). Użytkownik zwykle nie ma z nimi bezpośrednio do czynienia. Dostawą poczty do i z MTA zajmują się klienty pocztowe, takie jak Outlook czy KMail. MTAs komunikują się między sobą za pomocą zwykłych znaków ASCII. Klient wysyła polecenia do serwera, który odpowiada za pomocą kodu numerycznego i opcjonalnego ciągu znaków.

Simple Mail Transfer Protocol ma jednak jedną, istotną wadę - po wysłaniu e-maila nie otrzymuje się żadnej wiadomości o jego dalszych losach. Specyfikacja przewiduje wprawdzie powiadomienie nadawcy w sytuacji, gdy wiadomość nie może być dostarczona. Nie jest określone jednoznacznie, jak taka wiadomość ma wyglądać. Zwykle jest to e-mail z komunikatem o błędzie i nagłówkiem niedostarczonej wiadomości. Ze względu na brak standardu w praktyce rzadko udaje się ustalić, gdzie i dlaczego wystąpił błąd.

Dlatego też opracowano rozszerzenie SMTP, definiujące standardowe powiadomienia o błędach. Ponieważ bardzo niewiele serwerów obsługuje obecnie to rozszerzenie, nie będziemy go bliżej omawiać. Zainteresowani mogą znaleźć więcej informacji w RFC 1891 i 1894.

SMTP - polecenia

Polecenia SMTP definiują przesył e-maili. Zgodnie ze specyfikacją implementacja SMTP musi obsługiwać co najmniej osiem poleceń (patrz tabela).

SMTP - kody odpowiedzi

Kody odpowiedzi SMTP gwarantują, że klient jest na bieżąco informowany o statusie serwera. Każde polecenie wymaga kodu odpowiedzi od serwera. Klient decyduje o sposobie dalszego postępowania wyłącznie na podstawie otrzymanych zwrotnie kodów numerycznych.

W dalszej części opiszemy budowę e-maila.

SMTP - koperta, nagłówek i treść

E-mail składa się z trzech części:
koperty, która zawiera dane nadawcy i odbiorcy wiadomości; koperta jest niezbędna dla mail transfer agents;
nagłówka, w którym klient pocztowy zamieszcza dalsze informacje, jak identyfikator klienta czy wiadomości;
treści, czyli właściwego tekstu wiadomości. Zgodnie z RFC 822, treść ma postać czystego tekstu ASCII.W trakcie wysyłania e-maila za pomocą polecenia DATA klient pocztowy przesyła nagłówek oraz treść oddzieloną od nagłówka jednym pustym wierszem. Żaden przesyłany wiersz nie może być dłuższy niż 1000 bajtów.

Poniżej przykładowy nagłówek:

Received: by xyz.de. id AA00502; Mon, 19 Nov 2001 12:47:32 +0100

Received: from adam1 (715684625313-0001@[192.168.80.201]) by fwd00.xyz.de with smtp id 166Cyz-1KXYRsC; Tue, 20 Nov 2001 16:38:45 +0100
From: adam@xyz.de (Adam)
To: eva@test.de (Eva)
Subject: Beispiel-Mail
Date: Mon, 19 Nov 2001 12:47:31 +0100
Reply-To: adam@xyz.de
Message-ID: <9307191947AA00502.Adam@xyz.de>
MIME-Version: 1.0
Content-Type: text/plain; charset="iso-8859-1"
Content-Transfer-Encoding: 8bit
X-Mailer: Microsoft Outlook IMO, Build 9.0.2416 (9.0.2910.0)

W wierszu "Received" wpisywane są wszystkie serwery SMTP, przez które e-mail przeszedł na drodze od nadawcy do odbiorcy. Każda wiadomość otrzymuje jednoznaczny identyfikator, Message-ID. Jest to najczęściej kombinacja cyfr i liczb, po której następuje adres hosta nadawcy. Wiersze rozpoczynające się od "X" to z reguły informacje dodane przez klienta pocztowego, które nie są niezbędne do przesłania wiadomości. Wiersze "Mime-Version", "Content-Type" oraz "Content-Transfer-Encoding" charakteryzują e-mail zgodny z MIME. Pozostałe wiersze, jak "Date" czy "Subject", nie wymagają chyba oddzielnych objaśnień.

SMTP - przykład wysyłania e-maila

W naszym przykładzie wiadomość licząca trzy wiersze wysyłana jest do dwóch odbiorców:

S: 220 test.de SMTP server ready
C: HELO xyz.de.
S: 250 xyz.de., pleased to meet you
C: MAIL From:<adam@xyz.de>
S: 250 <adam@xyz.de> Sender ok

C: RCPT To:<eva@test.de>
S: 250 <eva@test.de> Recipient ok
C: RCPT TO:<tom@test.de>
S: 250 <tom@test.de> Recipient ok
C: DATA
S: 354 Enter mail
C: Hallo Eva, hallo Tom!
C: Beispiel fŁr den Mail-Versand mit SMTP.
C: Adam
C: .
S: 250 Mail accepted
C: QUIT
S: 221 test.de delivering mail

Do wysłania wiadomości niezbędnych jest pięć poleceń. Klient pocztowy po nawiązaniu połączenia TCP z serwerem SMTP czeka na tekst powitalny z kodem odpowiedzi 220. Następnie klient identyfikuje się poleceniem HELO, a jako argument przesyła fully qualified domain name swojego hosta, w tym przypadku xyz.de. Polecenie MAIL identyfikuje twórcę wiadomości. Polecenie RCPT podaje odbiorcę. Zawartość wiadomości klient przesyła poleceniem DATA. Końcem wiadomości jest wiersz zawierający tylko kropkę. QUIT kończy połączenie, a serwer wysyła wiadomość.

SMTP - Mail Routing i DNS

Gdy serwer SMTP odbierze wiadomość od klienta, odpowiada za routing e-maila. System nazw domen (DNS) odgrywa centralną rolę nie tylko w dziedzinie dostępu do serwerów internetowych i FTP, lecz również w kwestii przesyłania wiadomości elektronicznych. W systemie DNS przewidziano specjalne wpisy dla e-maili - rekordy MX. Serwer identyfikuje komputer docelowy za pomocą tak zwanego mail exchange record domeny. W tym celu pyta serwer DNS i otrzymuje listę serwerów (mail exchanger), które odbierają wiadomości dla tej domeny. Każdy mail exchanger ma określony priorytet o długości 16 bitów. Serwer SMTP próbuje zatem po kolei dostarczyć wiadomość do któregoś z serwerów zgodnie z priorytetem.

Zasadniczo wiadomość może przechodzić przez wiele serwerów SMTP. Wbrew szeroko rozpowszechnionemu mniemaniu, jakoby e-maile mogły kilkakrotnie okrążyć Ziemię, zanim w końcu dotrą do odbiorcy, w rzeczywistości z reguły przechodzą tylko przez dwa serwery SMTP. Zapobieganie powstawaniu takich pętli jest właśnie zadaniem rekordów MX.

Mimo to w wyjątkowych przypadkach może się zdarzyć, że taka pętla powstanie, na przykład w sytuacji gdy informacje routingowe są niekompletne lub nieaktualne. Taki przypadek zachodzi na przykład przy zmianie dostawcy usług internetowych.

SMTP - Extended SMTP

Z biegiem czasu wzrosły wymagania wobec usług poczty elektronicznej. Aby im sprostać, rozszerzono protokół SMTP o kilka poleceń i funkcji. Zostały one ujęte w protokole ESMTP (Extended SMTP). Wszystkie dodane funkcje są kompatybilne w dół, a więc nie mają wpływu na dotychczasowe implementacje.

Jeżeli klient korzysta z rozszerzonych funkcji, identyfikuje się wobec serwera SMTP poleceniem EHLO (zamiast HELO). Jeżeli również serwer jest kompatybilny z rozszerzoną wersją protokołu, odpowiada wielowierszowym kodem odpowiedzi 250. Każdy wiersz zawiera hasło i opcjonalny argument. Hasła informują o rozszerzeniach SMTP, które obsługuje serwer.

220 test.de SMTP server ready
EHLO xyz.de
250-xyz.de, pleased to meet you
250-HELP
250-EXPN
250-8BITMIME
250-SIZE 461544960
250 XADR

Kod odpowiedzi i hasło rozdzielone są myślnikiem, z wyjątkiem ostatniego wiersza, który zawiera spację. Polecenia HELP i EXPN obecne są wprawdzie już w pierwszej specyfikacji SMTP, ponieważ jednak jest ona opcjonalna, często podaje się dodatkowo w ESMTP. Wszystkie hasła rozpoczynające się od X wskazują na lokalne rozszerzenia SMTP.

SMTP - Multipurpose Internet Mail Extension

Jak już wspomnieliśmy, w treści e-maili stosuje się 7-bitowy tekst ASCII. Zawiera on 128 znaków, jednak bez narodowych znaków specjalnych. W tej wersji nie można więc pisać z polskimi ogonkami. RFC 2045 definiuje MIME (Multipurpose Internet Mail Extension), który eliminuje problemy, gdy w e-mailu użyto innego zestawu znaków niż US ASCII.

Treść e-maila MIME może być w dalszym ciągu przesyłana jako tekst ASCII, bez względu na zawartość. Jedynym warunkiem stosowania jest obsługa przez klienta pocztowego. MIME dodaje do nagłówka pewne elementy, które objaśniają odbiorcy strukturę treści (patrz tabelka poniżej).

Typy MIME

MIME nie tylko umożliwia przesyłanie e-maili z załącznikami, lecz jednocześnie zapewnia informację, którą klient pocztowy wykorzystuje do wybrania właściwego programu edycyjnego. Służy do tego element nagłówka "Typ zawartości". MIME dzieli typy danych (typy mediów) na siedem grup głównych z wieloma podgrupami. Każde rozszerzenie nazwy pliku przypisane jest do jednego z "typów mediów" (patrz tabelka powyżej).

Odbiór e-maili

Wielu użytkowników łączy się z Internetem za pomocą dial-up. Nie mogą oni w prosty sposób uruchomić na swoich komputerach serwera SMTP do odbioru wiadomości. W tym celu serwer SMTP dostawcy usług internetowych

musiałby przesyłać wiadomości do własnego serwera, a w większości przypadków jest to niemożliwe. Dlatego też wiadomości przeznaczone do odebrania są tymczasowo zapisywane. Zdalny dostęp do tych zbiorów wiadomości umożliwiają dwa protokoły - starszy protokół POP, znany od roku 1984, oraz jego nowsza wersja, POP3; drugi to opracowany w roku 1986 protokół IMAP, dostępny obecnie w rozszerzonej wersji 4rev1.

W strukturze rozproszonej są trzy możliwości odbioru wiadomości, zgodne z RFC 1733:
podczas pracy offline e-maile przesyłane są do serwera. Klient łączy się z serwerem i ściąga wiadomości. Poczta elektroniczna jest przetwarzana lokalnie na komputerze użytkownika.
w trybie online poczta pozostaje na serwerze i tam jest przetwarzana przez klienta.
trzeci wariant to dostęp typu disconnected, będący hybrydą modelu offline i online. W tym przypadku klient łączy się z serwerem, tworzy kopie wiadomości i przerywa połączenie. Gdy użytkownik zakończy przetwarzanie wiadomości, następuje uzgodnienie stanu wiadomości między klientem a serwerem.POP kontra IMAP

W porównaniu protokołem POP, protokół IMAP oferuje szereg korzyści, szczególnie, gdy chodzi o zdalny dostęp do poczty elektronicznej. Zakres funkcjonalny obu protokołów przedstawiliśmy w tabeli.

Na kolejnych stronach przedstawiamy szczegółowy opis obu protokołów POP3 i IMAP4.

POP3 - Post Office Protocol, Version 3

Klient, który chce odebrać wiadomości POP3, tworzy połączenie TCP przez port 110. Gdy połączenie zostaje nawiązane, serwer wysyła komunikat powitalny. Dalsza komunikacja między obydwoma komputerami odbywa się na podstawie poleceń.

Polecenia POP3 składają się z haseł o długości trzech lub czterech znaków i jednego lub kilku argumentów o długości do 40 znaków. Odpowiedzi zawierają wskaźnik statusu, hasło oraz informacje opcjonalne. Są dwa wskaźniki statusu - pozytywny (+OK) i negatywny (-ERR).

Sesja POP3 składa się z wielu etapów. Po wysłaniu przez serwer komunikatu powitalnego rozpoczyna się etap autoryzacji (authorization state). Klient musi uwierzytelnić się na serwerze. Jeżeli uwierzytelnienie zakończy się pomyślnie, rozpoczyna się etap transakcyjny (transaction state). Wykonywane są wszystkie operacje związane z przetwarzaniem wiadomości, jak ich usuwanie i ściąganie. Po wysłaniu przez klienta polecenia QUIT rozpoczyna się etap uaktualniania (update state). Serwer kończy połączenie TCP i wykonuje zmiany, których klient zażądał w trakcie etapu transakcyjnego.

Wiele serwerów POP3 ma dodatkowo zegar czasu bezczynności. Zgodnie ze specyfikacją, musi on być ustawiony na co najmniej 10 minut. Każde polecenie ze strony klienta resetuje zegar. Jeżeli czas bezczynności zostanie przekroczony, połączenie TCP jest natychmiast przerywane, bez przejścia do etapu uaktualniania - serwer nie zapisuje ewentualnych zmian.

POP3 - etap autoryzacji

Gdy klient POP3 nawiąże połączenie TCP z serwerem, ten ostatni wysyła komunikat powitalny do klienta. Może nim być dowolny ciąg:

S: +OK POP3 server ready

Ponieważ jest to już odpowiedź serwera, komunikat zawsze ma status pozytywny (+OK). Połączenie znajduje się teraz na etapie uwierzytelniania. Klient musi zidentyfikować się wobec serwera. Odbywa się to za pomocą poleceń USER i PASS.

POP3 - etap transakcyjny

W przypadku pomyślnej identyfikacji połączenie przechodzi do etapu transakcyjnego. Klient ma do dyspozycji cały szereg poleceń do przetwarzania wiadomości: serwer nie wykonuje polecenia DELE bezpośrednio. Odpowiednie wiadomości są zaznaczane jako przeznaczone do usunięcia i ostatecznie usuwane z serwera odpiera na zakończenie połączenia. Jeżeli jakaś wiadomość została zakwalifikowana do usunięcia, a jednak nie powinna być usunięta, należy wykonać polecenie RSET. Serwer porzuca wszystkie niewykonane dotąd operacje.

POP3 - etap uaktualniania

Gdy klient wyśle polecenie QUIT, połączenie przechodzi do etapu uaktualniania. Serwer rozłącza połączenie TCP i wykonuje wszystkie zapisane zmiany.

Oprócz przedstawionych tu poleceń, niezbędnych do minimalnej implementacji, jest jeszcze szereg kolejnych, które obsługiwane są przez większość klientów i serwerów. Szczegóły opisane są w RFC 1725.

POP3 - przykład ściągania wiadomości

W tym przykładzie prześledzimy przebieg połączenia POP3. Klient uwierzytelnia się na serwerze i pobiera listę zapisanych wiadomości. Następnie klient ściąga pojedynczo kolejne wiadomości, które tym samym zostają zaznaczone na serwerze jako przeznaczone do usunięcia, a połączenie kończy się.

S: +OK POP3 server ready
C: user tecchannel
S: +OK
C: pass ahd635d
S: +OK
C: LIST
S: +OK 2 messages (320 octets)
S: 1 120
S: 2 200
S: .
C: RETR 1
S: +OK 120 octets
S: <Server sendet Nachricht 1>
S: .
C: DELE 1
S: +OK message 1 deleted
C: RETR 2
S: +OK 200 octets
S: <Server sendet Nachricht 2>
S: .
C: DELE 2
S: +OK message 2 deleted
C: RETR 3
S: -ERR no such message
C: QUIT
S: +OK

IMAP4 - Internet Message Access Protocol, Version 4

Klient pocztowy i serwer wymieniają dane IMAP przez port TCP numer 143. Jednak inaczej niż w protokołach SMTP i POP, klient IMAP nie musi czekać po każdym wysłanym poleceniu na bezpośrednią odpowiedź serwera. Klient może wysłać kolejno kilka poleceń, a odpowiedź z serwera może nadejść później. Klient nadaje każdemu poleceniu znacznik (tag), na przykład A001, A002 i dalej kolejno. Serwer może również odpowiedzieć klientowi na kilka sposobów; plus na początku wiersza oznacza, że serwer potrzebuje dodatkowych informacji związanych z poleceniem. W ten sposób sygnalizuje jednocześnie klientowi swoją gotowość do odbioru. Gdy z kolei na początku wiersza znajdzie się gwiazdka, oznacza to, że serwer przesyła klientowi kolejne informacje.

Odpowiedź serwera świadczy o powodzeniu lub błędzie wykonania polecenia: OK - polecenie wykonane z powodzeniem, NO - błąd wykonania, BAD - błąd protokołu; polecenie nieznane lub błąd składni. Odpowiedź zawiera ten sam znacznik, co źródłowe polecenie; w ten sposób klient "wie", którego polecenia dotyczy odpowiedź. Podobnie jak w przypadku protokołu POP, połączenie IMAP składa się z kilku etapów.

Stan nieuwierzytelniony (non-authenticate state) - bezpośrednio po nawiązaniu połączenia. Użytkownik musi zidentyfikować się wobec serwera.
Stan uwierzytelniony (authenticate state) - użytkownik uwierzytelnił się z powodzeniem i teraz musi wybrać skrzynkę pocztową.
Stan wybrany (selected state) - skrzynka pocztowa została wybrana. Na tym etapie odbywa się sprawdzanie skrzynek pocztowych i przetwarzanie poczty.
Stan wylogowania (update state) - połączenie zostaje przerwane, serwer wykonuje zapisane zmiany.W dalszym ciągu opisujemy dokładniej kolejne etapy sesji.

IMAP4 - stan nieuwierzytelniony

Stan nieuwierzytelniony daje użytkownikowi do dyspozycji kilka sposobów identyfikacji. Wiążą się z tym odpowiednie polecenia (patrz tabela).

Przykładowe uwierzytelnienie za pomocą polecenia LOGIN:

C: a001 LOGIN EVA AHD635D
S: a001 OK LOGIN completed

IMAP4 - stan uwierzytelniony

Użytkownik uwierzytelnił się i musi tylko wybrać skrzynkę pocztową, której zawartość będzie przetwarzana podczas tej sesji. Ma w tym celu do dyspozycji między innymi polecenia wymienione w tabeli 2.

Przykład usuwania skrzynki pocztowej za pomocą polecenia DELETE:

C: A683 DELETE FRIENDS
S: A683 OK DELETE completed

IMAP4 - stan wybrany i stan wylogowania

Po wybraniu skrzynki pocztowej klient ma do dyspozycji szereg poleceń do przetwarzania jej zawartości (patrz tabela poniżej).

Przykład szukania określonej wiadomości za pomocą polecenia SEARCH. W odpowiedzi na zapytanie serwer zwraca numery odpowiednich wiadomości.

C: A282 SEARCH SINCE 1-NOV-2001 FROM "ADAM"
S: * SEARCH 2 84 882
S: A282 OK SEARCH completed

Gdy klient zakończy połączenie za pomocą polecenia LOGOUT, serwer przechodzi w stan wylogowania i wykonuje przewidziane zmiany. Oprócz tego w stanach uwierzytelnionym i wybranym jest jeszcze szereg innych poleceń, jednak opis wszystkich funkcji i poleceń daleko przekracza możliwą objętość tego artykułu. Zainteresowanym możemy zasugerować przeczytanie RFC 2060 o objętości 60 stron.

IMAP4 - przykład ściągania wiadomości

Przedstawimy teraz przebieg przykładowego połączenia IMAP4. Klient identyfikuje się względem serwera, wybiera skrzynkę pocztową i ściąga nagłówek wiadomości.

S: * OK IMAP4 Service Ready
C: a001 login eva ahd635d
S: a001 OK LOGIN completed
C: a002 select inbox

S: * 18 EXISTS
S: * FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
S: * 2 RECENT
S: * OK [UNSEEN 17] Message 17 is first new message
S: * OK [UIDVALIDITY 3857529045] is first new message
S: a002 OK [READ-WRITE] SELECT completed
C: a003 fetch 12 rfc822.header
S: * 12 FECH (RFC822.HEADER {346}
S: Date: Wed, 10 Dec 2001 02:23:25 -0700 (PDT)
S: From: Adam <adam@xyz.de>
S: Subject: Beispiel für eine IMAP4-Verbindung
S: To: Eva <eva@test.de>
S: Message-Id: <9307191947AA00502.Adam@xyz.de>
S: Mime-Version: 1.0
S: Content-Type: TEXT/PLAIN; CHARSET=iso-8859-1
S:)
S: a003 OK FETCH completed
C: a004 LOGOUT
S: * BYE IMAP4 server terminating connection
S: a004 OK LOGOUT completed

Po nawiązaniu połączenia TCP z serwerem SMTP klient czeka na komunikat powitalny serwera. Następnie klient identyfikuje się za pomocą polecenia LOGIN, podając jako argument nazwę użytkownika i hasło. Gdy klient wybierze skrzynkę pocztową, serwer przesyła kilka informacji, na przykład liczbę nieprzeczytanych informacji. Za pomocą polecenia FETCH klient żąda przesłania nagłówka wiadomości numer 12. Polecenie LOGOUT kończy połączenie.

Zapobieganie spamowi

Wysyłane w miliardach sztuk listy reklamowe, określane powszechnie jako spam, stają się coraz większym problemem. Niektórzy dostawcy usług internetowych czy firmy oferujące konta pocztowe, blokują w całości pocztę nadchodzącą z adresów uznanych powszechnie za źródło spamu. Tego rodzaju środki mogą jednak w najgorszym razie dotknąć nie tylko spamera, ale zablokować cały ruch pocztowy wychodzący z danego serwera pocztowego. Problem w tym, że nie jest rzeczą łatwą odróżnienie niechcianego listu reklamowego od zamówionej wiadomości o charakterze informacyjnym. Może się zatem zdarzyć, że jedna czy druga ważna wiadomość z serwisu wiadomości utnie w filtrze antyspamowym i nie dotrze do odbiorcy.

Ulubiona metoda, jaką posługują się spamerzy, to wysyłanie poczty z cudzych serwerów pocztowych, czyli tak zwany relaying. W wielu krajach jest to nie tylko nielegalne, ale może spowodować też inne problemy dla właściciela tak zaatakowanego serwera - musi zapłacić za przesłanie cudzych danych, a pojawiające się w milionach sztuk wiadomości mogą zupełnie sparaliżować jego infrastrukturę. Kolejna konsekwencja może być taka, że w przypadku dłużej trwającego nieautoryzowanego relayingu serwer może trafić na tak zwaną czarną listę. Na skutek tego inni dostawcy usług zablokują wszelki ruch przychodzący z tego serwera. W najgorszym przypadku z takiego serwera SMTP nie da się wysłać żadnej wiadomości.

Aby skutecznie obronić się przed nieetycznymi działaniami tego typu pseudospecjalistów od marketingu, należy podjąć działania wyprzedzające.

Zwalczanie spamu - zapobieganie relayingowi

Serwer SMTP powinien rozpoznać nieautoryzowany relaying i obronić się przed nim. Cztery elementy wysyłanej poczty mogą posłużyć do identyfikacji nadawcy i odbiorcy z różnym stopniem pewności:

Pierwsze dwa punkty (HELO i MAIL) mogą mieć dowolną treść. Nie należy więc przywiązywać do nich wagi. Dlatego też serwer powinien zezwalać na relaying na podstawie następującego algorytmu:
adres odbiorcy wiadomości należy do "własnej" domeny;
wiadomości do domeny odbiorcy są zasadniczo przyjmowane i przekazywane dalej (MX Record);
adres IP klienta jest znany i autoryzowany. W ten sposób można uniknąć przynajmniej większości prób nieautoryzowanego relayingu.Zwalczanie spamu - dalsze możliwości

Kolejną możliwością zwalczania nieautoryzowanego relayingu jest uwierzytelnianie SMTP. Serwer pocztowy identyfikuje klienta na podstawie danych dostępowych i tylko w razie prawidłowego ich podania umożliwia przesłanie wiadomości. Dzieje się to przy każdym wysyłaniu wiadomości. Procedura jest zgodna z quasi-standardem RFC 2554, który jest obsługiwany przez popularne klienty pocztowe, jak Microsoft Outlook czy Netscape Messenger.

SMTP

Wielu dostawców usług internetowych nie stosuje uwierzytelniania SMTP, ponieważ nie każdy system je obsługuje. Zamiast tego stosują dynamiczne zezwalanie na relaying. Wiadomości są ściągane z serwera tak, jak dotychczas w POP3 czy IMAP4. Klient identyfikuje się wobec serwera za pomocą nazwy użytkownika i hasła oraz przekazuje swój adres IP. System zezwala na wysyłanie wiadomości tylko spod tego adresu IP, przez określony czas. W przypadku SMTP after POP trzeba więc przynajmniej raz sprawdzić zawartość skrzynki, aby móc wysłać wiadomość.

Wysyłanie poczty a bezpieczeństwo

Wadą SMTP jest niedostateczny poziom bezpieczeństwa. Mail transfer agents komunikują się między sobą "otwartym tekstem". W większości przypadków ruch przechodzi przez jeden lub wiele routerów. Może się zdarzyć, że cały ruch między klientem a serwerem zostanie przechwycony i wykorzystany bez wiedzy i zgody uczestnikow komunikacji. Jedną z możliwości nawiązania bezpiecznej komunikacji jest nawiązanie połączenia SMTP z szyfrowaniem TLS. TLS (Transport Layer Security) to rozwinięcie znanego zabezpieczenia SSl (Secure Socket Layer). Więcej informacji o SMTP over TLS można znaleźć w RFC 2487. W trakcie nawiązywania połączenia serwer informuje klienta za pomocą hasła STARTTLS, że obsługuje szyfrowanie. Jeżeli klient chciałby skorzystać z szyfrowania, wysyła polecenie STARTTLS bez parametru. Oba komputery rozpoczynają wówczas szyfrowanie. Oto przykład połączenia SMTP szyfrowanego TLS:

}
S: 220 test.de SMTP server ready
C: EHLO xyz.de
S: 250-xyz.de, pleased to meet you
S: 250 STARTTLS
S: 220 Go ahead
C: <Start der VerschlŁsselung>
S: + C: <VerschlŁsselung wird abgesprochen>
C: <Client sendet Kommandos zur Bearbeitung von Mails>
...

Również w przypadku POP i IMAP jest ten sam problem: dane - szczególnie dane dotyczące uwierzytelniania - przesyłane są przez Internet w otwartej postaci. Dlatego też

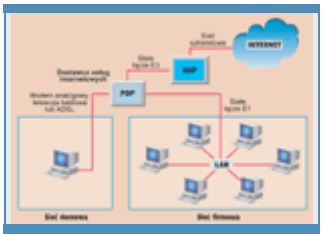
wprowadzono stosowanie TLS również w POP i IMAP. Więcej informacji można znaleźć w RFC 2595.

Routerem w Sieć

Dla internautów Sieć to kłębek kabli oplatających planetę niczym pajęczyna. Niewiele osób zdaje sobie sprawę, że ruch w przewodach odbywa się dzięki niewielkim urządzeniom telekomunikacyjnym, umiejscowionym na stykach różnych sieci.

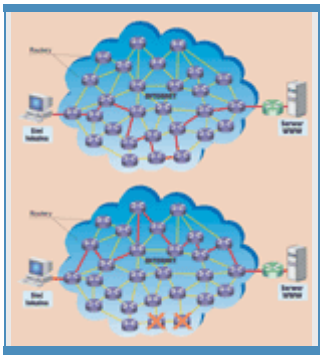
Internet to tak naprawdę setki tysięcy mniejszych i większych sieci lokalnych, podłączonych przez lokalne punkty dostępowe (Point of Presence - POP) do większych sieci, należących do dostawców usług internetowych. Ci z kolei są podłączeni do rozległych sieci szkieletowych (backbone) za pomocą sieciowych punktów dostępowych (Network Access Point - NAP). Tam też stykają się ze sobą sieci szkieletowe należące do różnych organizacji. Ale w jaki sposób dane (np. wiadomości elektroniczne) wysłane do komputera umieszczonego w sieci lokalnej na drugiej półkuli docierają właśnie do niego? Umożliwiają to routery (routers) - urządzenia telekomunikacyjne umieszczane na stykach różnych sieci. Ich zadanie polega między innymi na odczytaniu adresata przechodzącej partii danych i przesłaniu jej pod wskazany adres lub przynajmniej w jego kierunku.

Trochę techniki



Internet stanowi połączenie kilkuset tysięcy sieci lokalnych i korporacyjnych, mających określoną strukturę pionową. Najniżej w hierarchii są sieci lokalne, wchodzące w skład sieci rozległych dostawców usług internetowych, którzy sami korzystają z sieci szkieletowych.

Zasada działania routerów jest prosta. Wystarczy wyobrazić sobie kilka różnych sieci lokalnych podłączonych do jednego routera. Wiadomo, że dane wewnątrz sieci krążą w postaci pakietów, tj. niewielkich strumieni bitów zawierających, oprócz partii danych, informacje dotyczące nadawcy i odbiorcy (ich adresy IP). Ponieważ router stanowi element każdej z podłączonych sieci (ma też własny adres IP i ewentualnie nazwę domeny), to przechodzą przez niego wszystkie pakiety krążące w tych sieciach. Zanim router prześle pakiet dalej, odwołuje się do swojej tablicy konfiguracyjnej (configuration table). Zapisane są w niej informacje, do której części sieci prowadzą określone adresy IP, jaką trasą się tam dostać oraz jak traktować zwykłe pakiety, a jak te o specjalnym znaczeniu (wysokim priorytecie). Każdy pakiet jest analizowany pod kątem tych informacji i dopiero wtedy zostaje podjęta decyzja o przesłaniu go dalej (jeżeli jest skierowany poza sieć lokalną, z której został nadany) lub zatrzymaniu w sieci nadawcy. Jednak zadanie routera na tym się nie kończy - każdorazowo sprawdza, czy dany pakiet dotarł do miejsca przeznaczenia. Jak wiadomo, aby wypełnić wszystkie swoje funkcje, routery korzystają z unikatowych adresów IP, przyporządkowanych do każdego komputera podłączonego do sieci. Ponieważ adresy IP wykorzystywane są przez protokoły trzeciej warstwy modelu referencyjnego OSI (patrz ramka "Fachowa chińszczyzna") często mówi się, że routery są urządzeniami trzeciej warstwy modelu OSI.



Internet jest niezawodny dzięki przełączaniu pakietowemu - jeżeli

jedna z dostępnych dróg jest chwilowo nieczynna, routery natychmiast prześlą pakiety do celu inną drogą, na której nie ma żadnych przeszkód.

Jak wygląda współpraca kilku routerów w dużych sieciach? Przede wszystkim dane o połączeniach w sieci można dostarczyć do tablicy konfiguracyjnej routera na dwa sposoby. Pierwszy to po prostu ręczne wprowadzenie odpowiednich adresów IP przez administratora. Routery zawsze wybierają dla pakietu tę drogę, którą nakazał im administrator (rutowanie statyczne), i w razie awarii części sieci nie mogłyby samodzielnie wybrać innej. Dlatego właśnie są wyposażone w mechanizm pozwalający im co wybrany przedział czasu (najczęściej 15-30 sekund) sprawdzać, jaka jest topologia podłączonej do nich sieci i jakie natężenie ruchu panuje w poszczególnych jej segmentach. W razie tłoku lub awarii router sam decyduje o wybraniu dla pakietu alternatywnej drogi (rutowanie dynamiczne). Setki tysięcy routerów, które tworzą sieć Internet, cały czas na bieżąco monitoruje sytuację na poszczególnych łączach i wzajemnie się o niej informuje. Pakiety kierowane są taką drogą, aby mogły jak najszybciej dotrzeć do adresata. To jedna z najważniejszych cech Internetu - mówi się, że jest siecią o przełączaniu pakietowym (patrz rys. na następnej stronie).

Każdy użytkownik Internetu może osobiście sprawdzić, jaką drogę pokonują zamawiane przez niego pakiety danych. Wystarczy uruchomić tryb MS-DOS (Windows 95/98/Me) lub wiersz poleceń (Windows XP) i wpisać polecenie **tracert** oraz nazwę domeny, z którą chcemy się połączyć (np. **tracert www.pcworld.pl**). Oprócz kolejnych routerów, przez które przechodziły pakiety (liczba tzw. hopów), wyświetlona zostanie informacja, ile czasu zajęło im pokonanie drogi do routera i z powrotem.

Ponieważ w sieciach pracuje bardzo wiele różnych urządzeń telekomunikacyjnych, routery bardzo często mylone są z przełącznikami, mostami i hubami, za pomocą których również można sprzęgać sieci lokalne. Pierwsza i najważniejsza różnica między nimi to warstwa modelu referencyjnego OSI, w której pracują. Rutery opierają się na warstwie trzeciej, przełączniki i mosty na drugiej, a huby na pierwszej.

W praktyce przełączniki rozsyłają pakiety do każdego urządzenia w docelowym segmencie sieci ("przełączają" pakiety z jednej sieci do drugiej), dynamicznie przydzielając dostępne pasmo transmisji (najnowsze z nich, przełączniki warstwy trzeciej, mogą trafić już do konkretnej maszyny, natomiast starsze stosują mostkowanie przezroczyste, tzn. na bieżąco uczą się, gdzie w sieci znajdują się określone maszyny). Mosty powielają odebrane dane do odpowiednich segmentów sieci. Nowsze z nich w trakcie przesyłania strumieni bitów uczą się topologii sieciowej. Huby mogą jedynie fizycznie powielić sygnał do wszystkich przyłączonych do niego sieci (na rynku są również huby przełączające, pozwalające na wysyłanie strumieni bitów do konkretnych segmentów sieci).

Wyższa inteligencja routerów w porównaniu do mostów, przełączników i hubów powoduje, że przesłanie przez nie pakietu danych zajmuje nieco więcej czasu. Aby zwiększyć sprawność sieci, bardzo często łączy się sieć lokalną z routerem za pomocą np. przełącznika. Dane lokalne rozsyłane są w takich sieciach w szybszym tempie. Są również routery z opcją przełączania pakietów (tzn. działające także w drugiej warstwie modelu OSI).

Koszty sieci

Zakładamy, że instalowana jest przewodowa lub bezprzewodowa sieć lokalna składająca się z czterech komputerów, rozmieszczonych na dwóch piętrach budynku. W wypadku okablowania przyjmujemy użycie topologii gwiazdy (wszystkie komputery podłączone będą bezpośrednio do routera, podłączonego z kolei do modemu ADSL). Średnia odległość host-router nie przekracza 25 m. Połączenie bezprzewodowe odbywa się w technologii Wi-Fi.

Sieć **bezprzewodowa**

Koszt instalacji:

- karty sieciowe Linksys Wireless LAN PCI (4 sztuki) - 1800 zł (lub 4 karty sieciowe Linksys Wireless LAN PCMCIA - 1480 zł)
- router bezprzewodowy Linksys BEFW11S4 - 999 zł
- koszt łączny - 2799 zł (2479 zł w wersji dla laptopów)
- koszt jednego stanowiska - 699,75 zł (619,75 zł)

Czas instalacji: jedno popołudnie.

Sieć przewodowa

Koszt instalacji:
- kabel UTP kategorii 5 (4 x 25 m = 100 m) firmy Belden - 270 zł
- końcówki RJ45 (10 sztuk) - 15 zł
- karty sieciowe 10/100 Mb/s D - Link (4 sztuki) - 200 zł (lub 4 karty sieciowe 10/100 Mb/s D - Link PCMCIA - 680 zł)
- router D-Link DI-804v - 855 zł
- koszt łączny - 1340 zł (1820 zł w wersji do laptopów)
- koszt jednego stanowiska - 335 zł (455 zł)

Czas instalacji: od jednego dnia do tygodnia, w zależności od uzdolnień manualnych administratorów i warunków terenowych.

Routerem w Sieć

Poradnik konsumenta

Alternatywą dla sieci przewodowych stają się sieci bezprzewodowe działające w technologii Wi-Fi, pozwalające na uzyskanie przepływności 11 Mb/s. Punkt dostępowy Linksys BEFW11S4 to najnowsze rozwiązanie technologiczne, charakteryzujące się również estetycznym wyglądem i przystępną ceną.

Wybór routera do sieci domowej lub małej sieci firmowej nie jest łatwy. Z góry założymy tutaj, że będzie ona podłączona do Internetu. W podjęciu odpowiedniej decyzji na pewno pomoże zamieszczona na końcu tabela "Wybrane modele routerów" oraz udzielenie odpowiedzi na trzy zasadnicze pytania:

Z jakiego łącza internetowego będziesz korzystać?
Ilu użytkowników będzie pracowało w sieci?
Ile pieniędzy przeznaczasz na budowę sieci?

Pierwsze z pytań jest o tyle ważne, że każdy router jest przeznaczony do określonego rodzaju połączenia z Internetem. Użytkownicy prywatni najczęściej wykorzystują analogowe łącza modemowe, łącza telewizji kablowej lub ADSL (w Polsce przykładem tego typu usługi jest Neostrada Plus w sieci TP S.A.). W tabeli, w części "Sieci domowe" wymieniono kilka urządzeń wykorzystujących powyższe technologie. Należy pamiętać, że komputery użytkowników prywatnych będą podłączone do routera, który z kolei będzie połączony z modemem kablowym lub modemem ADSL. W wypadku sieci domowych nie trzeba inwestować w urządzenia obsługujące kilka rodzajów łączy internetowych, gdyż wystarczy jedna technologia. Inaczej jest w wypadku małych firm, które przy pewnych profilach działalności muszą mieć możliwość połączenia alternatywnego na wypadek awarii łącza pierwotnego. W tabeli w części "Niewielkie sieci firmowe" zaproponowaliśmy urządzenia pozwalające na jednoczesne połączenie łączem stałym i przez telefonię cyfrową ISDN. Firmy, które nie muszą być stale obecne w sieci, mogą skorzystać z routerów współdziałających z modemami kablowymi, modemami ADSL lub łączami stałymi.

Kolejnym ważnym czynnikiem wpływającym na wybór routera jest liczba komputerów tworzących sieć i współdzielących łącze internetowe. Zarówno osoby prywatne, jak i firmy, w których jest niewielu użytkowników sieci, powinny wybrać tańsze modele, mające do czterech portów komunikacyjnych.

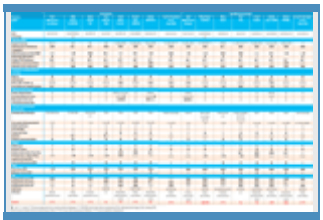
W wypadku większych sieci należy rozważyć zakup albo modelu z większą liczbą portów, albo urządzenia, które można łączyć z innymi routerami (skalowalnego). Pozwoli to złożyć kilka segmentów sieci lokalnej w jedną całość. Również do większych sieci wybiera się model przełączający pakiety (patrz część "Trochę technologii") - znacznie przyspieszy to działanie routera. Można również kupić sprzęt pozwalający na zdalne połączenie z routerem (np. za pomocą linii telefonicznej). W wypadku firm bardzo ważnym czynnikiem wyboru odpowiedniego modelu powinna być obsługa wirtualnych sieci prywatnych (Virtual Private Network - VPN). Im więcej algorytmów szyfrujących ma dany router i im więcej protokołów obsługuje, tym bezpieczniej można się połączyć z siecią firmową za pośrednictwem Internetu.

W przeciwieństwie do niewielkich routerów pracujących w sieciach lokalnych, sieci szkieletowe tworzące Internet muszą być połączone za pomocą niezwykle wydajnych urządzeń. Cisco 12404 Internet Router obsługuje wiele milionów pakietow w ciągu jednej sekundy.

Ostatnią, ale równie istotną kwestią jest cena urządzeń. Użytkownicy prywatni oraz firmy powinny rozważyć dwie możliwości - połączenie tradycyjne za pomocą skrętki czteroparowej (przepustowość standardowo 10 Mb/s lub 100 Mb/s) lub połączenie bezprzewodowe (obecnie najpopularniejsza i najefektywniejsza jest technologia Wi-Fi, pozwalająca na osiąganie przepustowości do 11 Mb/s w paśmie 2,4 GHz). Technologia bezprzewodowa będzie niezastąpiona np. w starych budynkach, gdzie niemożliwe jest zainstalowanie kabli, lub w wypadku dużej mobilności poszczególnych hostów w sieci (tzn. gdy duża część komputerów w sieci to laptopy). Standardowe okablowanie z pewnością będzie potrzebne tam, gdzie niezbędne są duże przepustowości (np. przy grach sieciowych, przesyłaniu dużych plików). Przykładowe koszty budowy sieci przewodowych i bezprzewodowych dla czterech użytkowników znajdują się w ramce "Koszt sieci". Po wybraniu technologii należy się zorientować, czy routery obsługują odpowiednią przepustowość (w wypadku okablowania) oraz jakiego rodzaju antenę oraz protokół WEP zastosowano w routerach bezprzewodowych (dobre są anteny zewnętrzne i co najmniej 64-bitowe protokoły). Więcej informacji na temat Wi-Fi można znaleźć w artykule "Sieci bez kabli i kłopotów", dostępnym w portalu PC World Komputer On-line pod adresem www.pcworld.pl/artykuly/24752.html .

Pożyteczne dodatki

Warto zwrócić uwagę na kilka dodatkowych elementów. Pierwszy to sposób, w jaki można administrować routerem. Im więcej, tym lepiej, choć podstawą powinno być połączenie z okna przeglądarki (jest najwygodniejsze). Kolejną pożyteczną cechą routera jest obsługa DHCP (Dynamic Host Configuration Protocol), czyli dynamicznego przydzielania adresów IP. Jeżeli router ma opcję *DHCP Serwer*, będzie automatycznie przydzielał adresy IP hostom znajdującym się w sieci lokalnej (z reguły administrator musi podać przewidywaną liczbę hostów). Znacznie upraszcza to procedurę budowy sieci i ułatwia jej zarządzanie. Opcja *Klient DHCP* przyda się, jeżeli dostawca usług internetowych dynamicznie przydziela adresy IP swoim klientom - router nie będzie mu w tym przypadku przeszkadzał. Jeżeli użytkownicy przywiązują dużą wagę do bezpieczeństwa sieci lokalnej, warto zainwestować w router z firewallem, chroniący przed atakami z zewnątrz. Dobry firewall powinien pozwalać na filtrowanie portów (administrator określa, z których usług w Internecie mogą korzystać użytkownicy lokalni - np. ftp, http lub telnet), pozwalać na zabezpieczenie komunikacji przez porty (opcja port forwarding) oraz umożliwiać tworzenie tzw. strefy zdemilitaryzowanej (DMZ), w której umieszcza się serwery ogólnodostępne. Profesjonalne firewalle umożliwiają zabezpieczenie poprzez specjalne algorytmy filtrowania pakietów, podnoszące znacząco bezpieczeństwo sieci lokalnych (triggered maps oraz stateful inspection). Więcej o technologii stosowanej w firewallach można przeczytać w numerze 1/2003 PC World Komputera.



Wybrane modele routerów

Na koniec warto wspomnieć o routowaniu statycznym i dynamicznym (patrz część "Trochę teorii"). Wybrany router powinien bezwzględnie obsługiwać obydwa standardy.

Fachowa chińszczyzna

Hop - przejście pakietu danych z jednej sieci do drugiej przez węzeł (router, przełącznik).

Host - urządzenie zainstalowane w środowisku sieciowym.

Hub - bardzo proste urządzenie komunikacyjne, działające w pierwszej warstwie modelu referencyjnego ISO/OSI, służące do rozgałęziania strumienia danych w sieciach LAN. Po prostu przesyła strumienie danych do wszystkich przyłączonych segmentów sieci. Nowsze modele potrafią imitować przełączniki, tzn. przesyłać sygnał do segmentu zawierającego docelową stację.

Model ISO/OSI - model referencyjny połączonych systemów otwartych, standard opracowany w celu ułatwienia połączeń otwartych systemów komputerowych bez względu na pracujący na nich system operacyjny. Model referencyjny dzieli sesję telekomunikacyjną na siedem warstw funkcjonalnych, według naturalnej sekwencji zdarzeń w niej zachodzących. Wyróżniono warstwy: fizyczną, łącza danych, sieciową, transportową, sesji, prezentacji oraz aplikacji. Warstwy od pierwszej do trzeciej umożliwiają dostęp do sieci, a warstwy od czwartej do siódmej są odpowiedzialne za komunikację końcową.

Most (bridge) - jedno z prostszych urządzeń telekomunikacyjnych stosowane do łączenia odrębnych sieci lub do sprzęgania segmentów jednej sieci LAN. Działa na poziomie drugiej warstwy modelu referencyjnego ISO/OSI. Podczas transmisji ramek "uczy się" lokalizacji określonych segmentów sieci i na podstawie tej wiedzy podejmuje później decyzje o przesłaniu ramek danych do odpowiedniego segmentu. Najnowsze wersje mostów wykrywają szkodliwe pętle (pakiety odsyłane pomiędzy mostami).

Przełącznik (switch) - urządzenie telekomunikacyjne umożliwiające przesyłanie danych z wykorzystaniem drugiej warstwy modelu referencyjnego ISO/OSI. W przeciwieństwie do huba, pozwala poszczególnym hostom na wykorzystanie całego dostępnego pasma transmisyjnego. Najprostszy przełącznik rozsyła pakiety do wszystkich maszyn w sieci. Przełącznik stosujący przezroczyste mostkowanie (transparent bridging) "uczy się", w której części sieci znajdują się poszczególne hosty, i tam wysyła pakiety.

Rutowanie (routing) - sposób przesyłania i filtrowania pakietów w sieciach zawierających routery. Najczęściej bywa statyczne lub dynamiczne. W pierwszym wypadku administrator sieci ręcznie wprowadza do pamięci routera parametry sieci (możliwe ścieżki wędrowania pakietów) i w razie awarii sam je modyfikuje. W rutowaniu dynamicznym router co pewien czas automatycznie pobiera dane dotyczące wszystkich możliwych połączeń i sam wybiera optymalną drogę dla pakietów.

Router - urządzenie telekomunikacyjne, które wraz z załączonym oprogramowaniem służy do łączenia sieci (przesyłania danych między sieciami). Działanie routera opiera się na trzeciej (sieciowej) warstwie modelu referencyjnego ISO/OSI.

Routery dysponują informacją o adresach docelowych urządzeń, więc mogą wybrać optymalną trasę przesłania danych.

Podstawy VPN

Problem jest znany od dawna. Zadanie może polegać na przesłaniu dużej ilości danych do innego komputera. Może to być aktualizacja bazy danych, projekt strony tytułowej lub choćby kolekcja cyfrowych zdjęć z wakacji. Droga przez e-mail odpada, choćby ze względu na ograniczoną pojemność skrzynki pocztowej. Wysłanie danych przez FTP wymaga zainstalowania serwera FTP i tymczasowego zapisania w Internecie na jednym z wielu serwerów usługowych, co dla wielu użytkowników jest nie do zaakceptowania ze względów bezpieczeństwa.

Alternatywą może być bezpośrednie przesłanie danych do komputera docelowego przez modem, jednak komputer docelowy musi po pierwsze być w ogóle wyposażony w modem, po drugie musi być skonfigurowany jako serwer RAS (Remote Access Services). Ponadto niebagatelne znaczenie maja koszty, zwłaszcza w przypadku połączeń międzymiastowych. Jeżeli oba komputery są połączone z Internetem, można rzecz załatwić za pomocą udostępniania plików Windows. Użytkownicy uzyskują wówczas dostęp do plików na komputerze odległym w dokładnie taki sam sposób, jak na komputerze lokalnym. Ogromna wada tego rozwiązania polega na tym, że taki komputer można porównać do stodoły z otwartymi wrotami. Chyba trudno byłoby o bardziej komfortową sytuację dla hakera.

Należy zatem sięgnąć po tak zwane VPNs - wirtualne sieci prywatne. Istota ich działania polega na tym, że za pomocą mechanizmów szyfrowania tworzą małą, wydzieloną sieć w wielkiej sieci. Tylko ci użytkownicy, którzy znają właściwe adresy i hasła, mogą kontaktować się za pośrednictwem takiej sieci. Bardzo zapobiegliwi administratorzy mogą je nawet instalować w sieci LAN, choćby w celu zapewnienia bezpiecznej komunikacji zarządowi firmy lub niektórym wydziałom. Haker może wprawdzie nadal przechwycić strumień danych za pomocą programów zwanych snifferami, lecz nie jest w stanie odczytać samych danych.

Czym jest VPN?

Wirtualna sieć prywatna łączy dwa komputery lub dwie sieci, korzystając z innej sieci jako nośnika. Przykładem może być połączenie między oddziałem firmy we Wrocławiu a centralą firmy w Gdańsku za pośrednictwem Internetu. Użytkownik postrzega sieć VPN jako normalne połączenie sieciowe z komputerem docelowym; rzeczywisty nośnik pozostaje dla niego niewidoczny.

Aby to umożliwić, VPN oddaje do dyspozycji użytkownika wirtualny adres IP. Dane do przesłania są szyfrowane przez klienta, łączone w pakiety i przesyłane do serwera VPN za pośrednictwem sieci publicznej. W przypadku Internetu jest to znów pakiet IP.

Serwer VPN odszyfrowuje pakiet i przetwarza go dalej. Sugestywną, animowaną grafikę ilustrującą ten proces można znaleźć na stronie www.wown.com/w_baeten/gifani/vpnani.gif. Opisany sposób postępowania nazywany jest też "tunelowaniem", ponieważ właściwe dane przesyłane są do komputera docelowego przez tunel utworzony w sieci publicznej.

Jest wiele możliwości implementacji VPN. Najbardziej popularne to:
Point-to-Point Tunneling Protocol (PPTP), nadaje się do przesyłu pakietów IP, IPX lub NetBEUI w sieci IP.
Layer 2 Tunneling Protocol (L2TP), nadaje się do przesyłu pakietów IP, IPX lub NetBEUI w dowolnym nośniku, który obsługuje transmisję datagramów punkt-punkt. Jako przykłady można podać IP, X.25, Frame Relay lub ATM.
IP Security Protocol (IPsec), nadaje się do przesyłu danych IP za pośrednictwem nadrzędnej sieci IP.Protokoły w tunelu

Tunelowanie może odbywać się na dwóch różnych poziomach modelu warstw OSI. PPTP i L2TP wykorzystują warstwę łącza danych (poziom 2) i pakują pakiety danych w ramki protokołu PPP (Point to Point Protocol). Mogą przy tym korzystać ze wszystkich funkcji protokołu PPP, jak choćby uwierzytelnianie użytkownika, dynamiczne przydzielanie adresu (np. DHCP), kompresja danych i ich szyfrowanie.

Szczególnie ważne jest uwierzytelnianie użytkownika, gdyż zadaniem VPN jest bezpieczna transmisja danych. Często stosuje się uwierzytelnienie CHAP, w którym dane użytkownika są szyfrowane. Można też uzyskać wyższy poziom bezpieczeństwa, stosując call-back (oddzwanianie). W tej procedurze połączenie jest przerywane po zakończonym powodzeniem uwierzytelnieniu. Następnie serwer obsługujący połączenie oddzwania pod określony numer, by nawiązać właściwe połączenie służące do transmisji danych. Pakiety danych do przesłania (IP, IPX lub NetBEUI) pakowane są w ramki PPP, następnie rozpakowywane w komputerze docelowym w celu dalszego przetwarzania.

PPTP pakuje ramki PPP przed przesłaniem w pakiety IP i przesyła je siecią IP do węzła docelowego. Protokół został opracowany w roku 1996 przez takie firmy, jak Microsoft, Ascend, 3Com i US Robotics.

Ograniczenie polegające na tym, że PPTP pracuje tylko w sieciach IP, legło u podstaw kolejnego opracowania z roku 1998. L2TP pracuje również w sieciach X.25, Frame Relay i bardzo wówczas cenionych sieciach ATM. Przewaga L2TP nad PPTP polega na tym, że może być przesyłany różnymi nośnikami WAN oraz opcjonalnie drogą okrężną przez IP.

IPsec - VPN tylko do Internetu

W przeciwieństwie do PPTP i L2TP, IPsec pracuje w warstwie sieci (poziom 3). Szyfruje on pakiety danych do przesłania łącznie ze wszystkimi informacjami, jak dane odbiorcy i meldunki o statusie, następnie dodaje normalny nagłówek IP, który przesyłany jest na drugi koniec tunelu. Tamtejszy komputer usuwa dodatkowy nagłówek IP, deszyfruje oryginalny pakiet i kieruje go do właściwej stacji odbiorczej.

W IPsec można skonfigurować dwie różne techniki tunelowania. W przypadku tak zwanego tunelu dobrowolnego klient tworzy najpierw normalne połączenie z Internetem, a następnie korzysta z tego kanału do utworzenia wirtualnego połączenia z właściwym serwerem docelowym. Aby było to możliwe, klient musi mieć zainstalowany odpowiedni protokół. W normalnym przypadku komunikację inicjuje użytkownik, który łączy się z Internetem. Jednak również komputery w sieci LAN mogą tworzyć połączenia VPN. Ponieważ połączenie IP już jest, w takim przypadku zachodzi jedynie potrzeba utworzenia połączenia VPN.

W przypadku tak zwanego tunelu obowiązkowego to nie klient odpowiada za utworzenie tunelu, lecz dostawca usług internetowych. Klient musi połączyć się jedynie z dostawcą usług internetowych, zaś tunel do stacji docelowej jest tworzony automatycznie przez dostawcę. Potrzebna jest w tym celu odpowiednia umowa z dostawcą usług internetowych.

Zagadnienia bezpieczeństwa w IPsec

IPsec posługuje się nagłówkiem uwierzytelniającym (AH - authentication header), by zagwarantować, że odebrany pakiet pochodzi rzeczywiście od właściwego nadawcy, a nie na przykład od hakera, który ingeruje w proces komunikacji, a także że nie został on zmieniony, a więc nie została naruszona jego integralność. Nagłówek uwierzytelniający zawiera informacje służące do uwierzytelnienia, a także numer kolejny, który ma zapobiegać atakom powtórzeniowym z użyciem starych pakietów (replay attack). Niestety, nie jest on szyfrowany.

Szyfrowanie można uzyskać za pomocą Encapsulation Security Header (ESH). W tej wersji dane użytkowe są w pełni szyfrowane, zaś ESH przekazuje sieci VPN informacje o metodzie szyfrowania. ESH zawiera również mechanizmy uwierzytelniania i ochrony integralności danych, a więc nagłówek AH staje się zbędny.

Nie jest jednoznacznie określona metoda szyfrowania i uwierzytelniania. Niemniej, IETF (www.ietf.org) ustalił pewne algorytmy jako obowiązkowe do wdrożenia IPsec, co ma zapewnić wzajemne współdziałanie różnych produktów. Należą do nich między innymi MD5, DES i Secure Hash Algorithm. IPsec wykorzystuje między innymi następujące standardy i procedury:
szyfrowany protokół Diffiego-Hellmana do wymiany kluczy między dwiema stacjami biorącymi udział w komunikacji;
szyfrowanie metodą klucza publicznego do podpisywania wymienianych kluczy i weryfikacji tożsamości stacji biorących udział w komunikacji;
algorytmy szyfrowania, takie jak DES, do zabezpieczenia właściwej wymiany danych;
algorytmy do uwierzytelniania poszczególnych pakietów danych;
podpisy cyfrowe w charakterze cyfrowych dowodów osobistych.IPsec bez tunelowania

W porównaniu z innymi rozwiązaniami IPsec ma jeszcze jedną zaletę - może być stosowany jako "normalny" protokół transportowy. Inaczej niż w trybie tunelowania, nie szyfruje się całego pakietu IP i nie pakuje się go w kolejny pakiet. Zamiast tego szyfrowane są czyste dane użytkowe. Oryginalny nagłówek z danymi nadawcy i odbiorcy pozostaje niezmieniony. W związku z tym do przesłania jest mniej dodatkowych danych (overhead), a więc zmniejsza się obciążenie nośnika.

W ten sposób haker może jednak stwierdzić, skąd pochodzą dane i dla kogo są przeznaczone. Ponieważ jednak informacje powyżej warstwy 3 w modelu OSI są szyfrowane, haker nie może ustalić, czy chodzi tu o komunikację z serwerem pocztowym, czy też o inny rodzaj komunikacji.

Przebieg połączenia IPsec

Zanim dwie stacje zaczną wymieniać dane, korzystając z IPsec, trzeba poczynić pewne przygotowania.

Na początek należy ustalić zakres procedur bezpieczeństwa. Stacje muszą uzgodnić, czy stosowane będzie szyfrowanie, uwierzytelnianie/weryfikacja integralności, czy też wszystkie trzy procedury na raz.

Następnie uzgadniają konkretne algorytmy, na przykład DES do szyfrowania i MD5 do weryfikacji integralności.

Następnie stacje muszą wymienić klucze sesji.

IPsec stosuje do zabezpieczenia komunikacji tak zwane security association - (SA), opis stosunków między dwiema stacjami, zawierający między innymi informacje o usługach zastosowanych do zabezpieczenia komunikacji. SA identyfikowane są jednoznacznie za pomocą security parameter index (SPI). SPI składa się z liczby losowej i adresu docelowego.

Oznacza to, że między dwiema stacjami są zawsze dwa SPI - jeden do komunikacji z A do B i drugi w odwrotną stronę. Jeżeli stacja chce rozpocząć bezpieczną transmisję, sprawdza uzgodnione SA ze stacją docelową i przetwarza pakiet danych zgodnie z uzgodnionymi procedurami. Na koniec wpisuje SPI do nagłówka pakietu i wysyła go pod adres docelowy.

Zarządzanie kluczami w IPsec

IPsec zakłada co prawda niejako "z góry" istnienie SA nie zapewnia jednak żadnych mechanizmów do ich tworzenia. Zadanie to IPsec ceduje na IKE (Internet Key Exchange), objawiające się w postaci Key Management Protocol (IKMP). W celu wytworzenia SA obie stacje muszą się najpierw uwierzytelnić. IKE jest bardzo elastyczne, gdy chodzi o to porozumienie. Obecnie używa się przede wszystkim następujących procedur:

Klucze współdzielone - na obu komputerach jest wstępnie zainstalowany klucz. Z tego klucza IKE tworzy wartość hasz i wysyła ja do komputera docelowego. Jeżeli obie stacje mogą utworzyć tę wartość, obie dysponują kluczem i są uwierzytelnione.

Szyfrowanie z użyciem klucza publicznego - każda ze stron generuje liczbę losową, szyfruje ją kluczem publicznym drugiej strony i wysyła do niej. Jeżeli druga strona może zdeszyfrować liczbę za pomocą swojego klucza prywatnego i odesłać ją do nadawcy, jest uwierzytelniona. W tym przypadku obecnie obsługiwany jest obecnie tylko algorytm RSA.

Podpis cyfrowy - w tej metodzie każda ze stron podpisuje cyfrowo blok danych i przesyła go drugiej stronie. Obecnie obsługiwany jest algorytm RSA i Digital Signature Standard (DSS).

W celu zabezpieczenia tej wymiany danych obie strony muszą najpierw uzgodnić wspólny klucz sesji. Ustala się go za pomocą protokołu Diffie-Hellman. Jeżeli uwierzytelnianie zakończy się powodzeniem, obie stacje uzgadniają klucz, który będzie stosowany w dalszej komunikacji. Możliwe są przy tym dwa warianty - zastosowanie użytego już do uwierzytelniania klucza Diffie-Hellman (szybsze) lub utworzenie nowego klucza (bezpieczniejsze).

Podsumowanie

Wymiana danych przez Internet niesie pewne ryzyko. Niemal każdy, kto znajdzie się w odpowiednim miejscu i czasie, może przechwycić dane i wykorzystać je w sobie tylko wiadomy sposób, choćby po to, by komuś zaszkodzić. Wirtualne sieci prywatne w znacznym stopniu przynajmniej utrudniają to zadanie. Wobec integracji technologii VPN z systemem Windows praktycznie nie ma przeszkód w jej stosowaniu. Mimo to, jest ona względnie rzadko stosowana. Podobnie zresztą, jak szyfrowanie poczty elektronicznej.

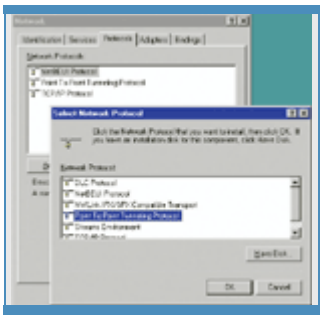
VPN w Windows

PC World Komputer

Internet w coraz większym stopniu sprawdza się jako sieć transportowa. Od dawna już oferuje znacznie więcej, niż tylko dostęp do witryn i pocztę elektroniczną. Niewielkim nakładem pracy można nawet połączyć dwa komputery, które stoją na różnych kontynentach. Oba komputery mają przy tym "wrażenie", jakby pracowały w tej samej sieci LAN. W ten sposób obaj użytkownicy unikają kłopotliwej wymiany danych za pomocą poczty elektronicznej lub drogich połączeń modemowych z komputerem docelowym.

Zasadniczym minusem tego rozwiązania jest to, że oba komputery są wydane na łaskę i niełaskę hakerów, czy w celu przeprowadzenia ataku, czy w celu podsłuchu komunikacji. Wirtualne sieci prywatne (VPN) oferują cały szereg zabezpieczeń przed atakiem hakerów. O podstawach funkcjonowania sieci VPN możesz przeczytać w poprzednim artykule. Teraz opiszemy, jak w łatwy sposób uruchomić własną sieć VPN w środowisku Windows. Nie potrzeba do tego nawet specjalnego oprogramowania, gdyż Microsoft dostarcza niezbędne sterowniki wraz z systemami operacyjnymi lub udostępnia je do ściągnięcia na swojej stronie internetowej.

Wymagania



Pierwszy etap - Point-to-Point Tunneling Protocol to podstawa funkcjonowania serwera VPN.

Aby dwa komputery mogły łączyć się przez VPN, jeden z nich musi pracować pod kontrolą Windows NT lub 2000. Jest on wówczas serwerem VPN; komputer działający pod Windows 9x/Me może być tylko klientem VPN.

Ponadto serwer VPN musi mieć statyczny adres IP. W rozdziale "Rozwiązywanie problemów" powiemy też, jak postawić serwer VPN bez statycznego adresu IP.

Oczywiście oba komputery muszą być połączone z Internetem - jest przy tym obojętne, czy jest to połączenie wdzwaniane, czy poprzez sieć LAN połączoną z Internetem. Serwer VPN musi w każdym razie być dostępny pod publicznym adresem IP, by klient mógł nawiązać z nim połączenie również z zewnątrz. W sieciach lokalnych korzysta się najczęściej z prywatnych adresów IP (np. 192.168.X.X). W takim przypadku można utworzyć sieć VPN jedynie w obrębie sieci LAN, jakkolwiek w określonych przypadkach również i to ma sens - można choćby zabezpieczyć połączenia między określonymi komputerami zapobiegając w ten sposób podsłuchiwaniu przez współpracowników.

Trzeci etap - w konfiguracji RAS należy dodać adapter VPN jako urządzenie Remote Access.

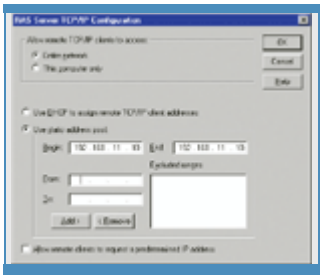
Jeżeli klient VPN ma pracować pod kontrolą Windows 95, należy najpierw pobrać i zainstalować uaktualnienie 1.3 Dial-Up Networking - (www.microsoft.com/windows95/downloads/contents/WURecommended/S_WUNetworking/dun13win95/Default.asp) Zawiera ono sterowniki, które są niezbędne do funkcjonowania VPN. Dochodzi do tego jeszcze uaktualnienie związane z problemem roku 2000 (www.microsoft.com/windows95/downloads/contents/WURecommended/S_WUNetworking/dunwinsky2k/Default.asp) oraz dodatkowe uaktualnienie VPN - www.microsoft.com/windows95/downloads/contents/WURecommended/S_WUNetworking/vpn/Default.asp , które zdanie Microsoftu zwiększa stabilność i szybkość działania połączeń VPN.

Czwarty etap - na karcie Network Configuration należy określić, które protokoły są dozwolone.

Instalacja serwera VPN

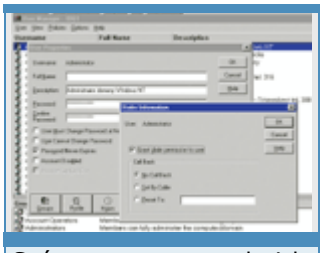
Na komputerze pracującym pod kontrolą Windows NP należy najpierw zainstalować Point-to-Point Tunneling Protocol (we właściwościach otoczenia sieciowego).

Na kolejnym etapie pojawi się pytanie o liczbę jednocześnie utrzymywanych, możliwych połączeń VPN. W przypadku serwerowej wersji NT może to być maksymalnie 256 połączeń. Stacja robocza obsługuje tylko jedno połączenie, ponieważ stacja robocza NT zezwala na tylko jedno połączenie RAS.



Piąty etap - jeżeli w sieci VPN mają być dozwolone również połączenia TCP/IP, koniecznych jest kilka dodatkowych ustawień.

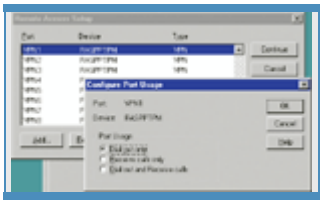
Ponieważ system uznaje połączenie VPN za połączenie typu remote access, Windows NT uruchamia automatycznie okno dialogowe konfiguracji RAS (Remote Access Server). Jeżeli RAS nie jest jeszcze zainstalowany, Windows NT czyni to automatycznie. W oknie konfiguracyjnym należy dodać adapter VPN jako port dostępowy. Jeżeli ma być obsługiwanych więcej połączeń VPN, punkt ten należy powtórzyć dla każdego adaptera VPN.



Szósty etap - każdy użytkownik, który ma mieć dostęp przez VPN, musi otrzymać odpowiednie uprawnienia.

Konfiguracja serwera RAS

Adapter VPN należy tak skonfigurować, by akceptował połączenia przychodzące. Na następnym etapie na karcie "Konfiguracja sieci" należy zaznaczyć dozwolone protokoły dla połączeń VPN. Należy tutaj również określić rodzaj szyfrowania oraz to, czy klient ma mieć dostęp tylko do komputera NT, czy też do całej sieci LAN, w której ten pracuje. Jeżeli jest to możliwe, serwer VPN działa również jako router.



Uwaga - w przypadku klienta VPN adapter musi zezwalać na połączenia wychodzące.

Dla podwyższenia stopnia bezpieczeństwa można zezwolić wyłącznie na stosowanie protokołu NetBEUI i zabronić odległemu komputerowi dostępu do sieci LAN. W takim układzie klient VPN może odwoływać się wyłącznie do udostępnionych zasobów serwera VPN. Sieć LAN i usługi internetowe są niewidoczne dla klienta. W ten sposób kończy się instalacja i konfiguracja protokołu.

W przypadku VPN opartym na TCP/IP koniecznych jest jeszcze kilka czynności konfiguracyjnych. Jeżeli nie zainstalowałeś serwera DHCP, przypisz statyczny obszar adresowy. Używaj jednak tylko prywatnych, a nie publicznych adresów IP. Obszar

adresowy musi zawierać co najmniej dwa adresy serwera VPN oraz dla klienta.

Użytkownik, który chce uzyskać dostęp do serwera za pośrednictwem VPN, musi wykazać się stosownymi uprawnieniami. W tym celu w opcjach Właściwości użytkownika aktywuj w menu Dostęp dostęp zdalny.

Na końcu należy uruchomić Remote Access Server, co spowoduje utworzenie połączeń VPN.

Klient VPN - Windows NT

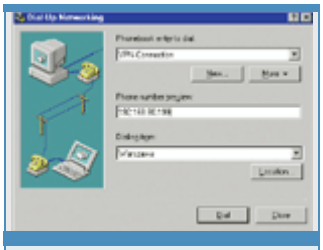
Instalacja klienta VPN w Windows NT jest identyczna z instalacją serwera VPN. Najpierw należy zrealizować cztery pierwsze etapy, identyczne z opisanymi w instalacji serwera. A więc:

- zainstalować PPTP,
- ustalić liczbę połączeń,
- dodać adapter VPN jako urządzenie RAS,
- skonfigurować adapter VPN w RAS Jedyna różnica polega na konfiguracji adaptera VPN.

Należy tu zezwolić na połączenia przychodzące, zamiast na wychodzące.

Następnie zapisz ustawienia i poczekaj, aż komputer ponownie się uruchomi. Następnie otwórz Dial Up Networking i utwórz nowe połączenie. Jako urządzenie podaj adapter VPN, jako numer telefonu - adres IP serwera VPN.

W ten sposób konfiguracja klienta VPN w Windows NT została zakończona, a wirtualna sieć prywatna - utworzona.



Konfiguracja połączenia z serwerem VPN.

Gotowe - połączenie z serwerem VPN zostało utworzone.

VPN w Windows

Mike Hartmann
1 sierpnia 2003
PC World Komputer

Klient VPN - Windows 2000

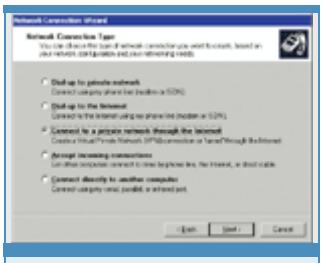
Utworzenie klienta VPN jest dużo prostsze, niż w przypadku serwera. W Windows 2000

należy przejść do właściwości otoczenia sieciowego i za pomocą asystenta utworzyć nowe połączenie.

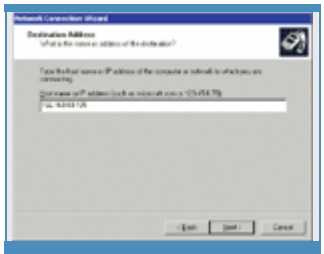
Zazwyczaj asystent wymaga podania adresu IP serwera VPN. Należy tu podać normalny adres IP, nie zaś adres sieci VPN.

W ten sposób została skonfigurowana sieć VPN, a połączenie zostanie za chwilę utworzone. W celu uwierzytelnienia na komputerze NT należy podać nazwę użytkownika i hasło tego użytkownika, któremu przyznano prawa zdalnego dostępu (remote access).

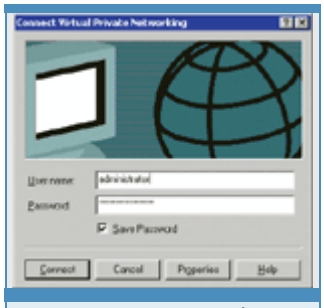
Na zakończenie Windows 2000 tworzy natychmiast połączenie - wirtualna sieć prywatna jest kompletna.



Pierwszy etap - w Windows 2000 konfigurację VPN ułatwia asystent.



Drugi etap - wystarczy podać adres IP serwera VPN.



Trzeci etap - na koniec pozostają już tylko formalności związane z załogowaniem.

Gotowe - połączenie z serwerem VPN zostało utworzone.

Klient VPN - Windows 9x

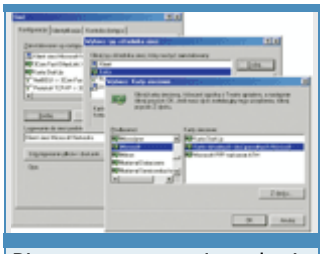
Instalacja klienta VPN w Windows 95, 98 i Me jest identyczna. Najpierw należy zainstalować obsługę VPN. W przeciwieństwie do NT, nie jest tu instalowany protokół, a jedynie adapter sieciowy.

Windows 9x instaluje automatycznie wszystkie potrzebne komponenty, na przykład Dial Up Networking, oraz tworzy powiązania z odpowiednimi protokółami. W ten sposób instalację sterowników mamy za sobą. Następnie należy utworzyć nowe połączenie w Dial Up Networking. Jako urządzenie trzeba wybrać adapter VPN.

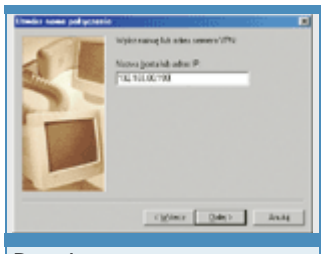
System operacyjny Windows 9x pyta poprawnie o adres IP dla serwera VPN. Nie ma więc mowy o zamieszaniu - numer telefonu czy adres IP?

W ten sposób konfiguracja klienta VPN jest zakończona i można nawiązać połączenie. Wystarczy podać nazwę użytkownika i hasło dla komputera NT.

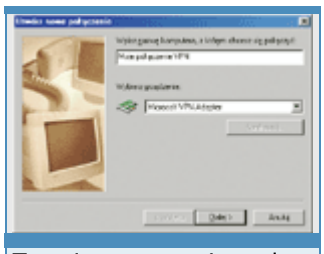
Windows 9x tworzy teraz połączenie internetowe i tunel, którym będą przesyłane prywatne dane.



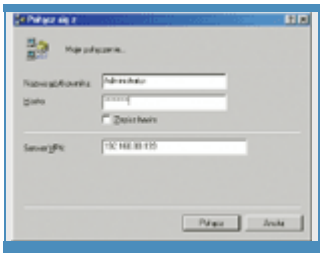
Pierwszy etap - instalacja adaptera VPN.



Drugi etap - nowe połączenie z adapterem VPN.

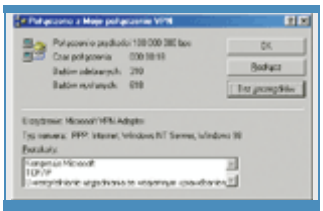


Trzeci etap - wpisz adres IP serwera VPN.



Czwarty etap - w celu uzyskania dostępu do serwera VPN należy podać nazwę użytkownika i hasło.

Rozwiązywanie problemów



Gotowe - połączenie między Windows 9x jako klientem a Windows NT jako serwerem VPN zostało nawiązane.

Jeżeli chcesz utworzyć połączenie VPN między komputerem w biurze (klient VPN) a komputerem w domu (serwer VPN), napotykasz dwa problemy.

komputer domowy nie jest stale połączony z Internetem (chyba, że masz stałe łącze);
klient VPN oczekuje adresu IP. Tego adresu nigdy nie znasz z góry, ponieważ większość dostawców usług internetowych przydziela adres IP dynamicznie.

Interesującym rozwiązaniem tego problemu jest OnlineJack (www.mailjack.de/onlinejack/). To niewielki program, który można zainstalować na komputerze domowym. Następnie za pośrednictwem strony OnlineJack, posługując się nazwą użytkownika i hasłem, można spowodować, że komputer domowy nawiąże połączenie z Internetem. W tak zwanym kokpicie (cockpit) możesz po chwili ustalić adres IP, który twój dostawca przydzielił komputerowi w domu. Posługując się tym adresem, skonfigurujesz i uruchomisz klienta VPN.

Dwa ograniczenia: OnlineJack funkcjonuje tylko wtedy, gdy komputer jest podłączony do Sieci przez ISDN i jest zainstalowany CAPI 2.0. Oprócz tego musi być, oczywiście włączony.

Klient sieci

Sieć komputerowa składa się nie tylko z serwera, ale także klienckich stacji roboczych. Konfiguracja serwera jest niezmiernie ważna, lecz warto pamiętać, że jego zadaniem jest świadczenie usług użytkownikom sieci. Dlatego poprawne przygotowanie stacji roboczych daje solidne podstawy do wydajnej pracy.

Windows Server 2003 może współpracować z różnymi klientami. Wśród dostępnych usług systemu odnajdziemy takie, które pozwalają na komunikację z systemami Windows, Unix i Macintosh. Naturalnie klientami najlepiej przystosowanymi do pracy w domenie będą stacje wyposażone w najnowsze systemy operacyjne potentata z Redmond, takie jak: Windows 2000 Professional oraz Windows XP Professional. Pozostałe, np. Windows NT 4.0, są albo przestarzałe, albo przeznaczone do zastosowań domowych i ich integracja z sieciami Microsoft jest możliwa tylko w ograniczonym zakresie.

Konfiguracja poszczególnych systemów do pracy w domenie Windows Server 2003 opiera się na podobnych zasadach. Ustawienia systemów 2000 i XP różnią się nieznacznie, ale rozbieżności między Windows 98, Me i NT są już nieco większe. Na szczegółowy opis wszystkich możliwych konfiguracji nie starczy nam miejsca, więc przykłady będą obejmowały wyłącznie stacje robocze z zainstalowanym Windows XP Professional. Pominiemy również tematykę związaną z fizyczną instalacją sieci oraz kart sieciowych.

Komunikacja sieciowa

Komunikacja sieciowa jest możliwa tylko wtedy, gdy są odpowiednie warunki. Stacje robocze i serwer sieciowy powinny być wyposażone w sprzęt zapewniający transmisję danych - zwykle jest to tania i prosta w instalacji karta sieciowa. Oprócz interfejsu sieciowego należy zadbać o niezawodne połączenie kablowe oraz co najmniej jedno urządzenie aktywne, np. koncentrator lub przełącznik. Jeśli powyższe warunki są spełnione, możemy przejść do konfiguracji serwera i klienckich stacji roboczych w sieci.

Mając fizyczne możliwości wymiany informacji, należy zadbać o właściwe ustawienia systemów operacyjnych. Oprócz zainstalowania karty sieciowej trzeba będzie ustawić takie parametry, jak klient sieci, protokół oraz odpowiednie usługi sieciowe. Konfiguracja odbywa się we właściwościach połączeń sieciowych. Aby się do nich dostać na przykład w Windows XP, należy wybrać Start | Ustawienia | Połączenia sieciowe, wskazać połączenie i wybrać Właściwości.

Protokół komunikacyjny można porównać do języka, jakim posługuje się komputer w czasie dialogu z innymi stacjami roboczymi. Dzięki niemu komputery będą mogły zrozumieć przekazywane w sieci informacje. Windows Server 2003 obsługuje wiele protokołów, ale najkorzystniejsze jest zastosowanie TCP/IP. Ponieważ stał się standardem w większości sieci, korzystanie z niego umożliwia komunikację z innymi systemami, np. Linuksem czy NetWare. Ponadto niektóre kluczowe usługi oferowane przez Windows Server 2003, np. Active Directory, wymagają jego wykorzystania.

Kolejnym komponentem koniecznym do pracy w domenach Windows Server 2003 jest Klient sieci Microsoft Networks. Nie wymaga od użytkownika żadnej konfiguracji, ale to właśnie dzięki niemu można uzyskiwać dostęp do zasobów oferowanych przez inne komputery w sieci. Domyślnie składnik ten jest instalowany i uruchamiany. Jeśli nie jest potrzebny, łatwo go wyłączyć. Dostęp do zasobów oferowanych przez lokalny komputer oferuje składnik o nazwie Udostępnianie plików i drukarek w sieciach Microsoft Networks. Gdy go brak, inne stacje nie będą mogły korzystać z naszych udostępnień i drukarek. Serwery plików i drukarek bezwzględnie wymagają tego składnika, natomiast stacje sieciowe tylko wtedy, gdy dane komputery oferują swoje zasoby, np. lokalnie podłączone drukarki.

Adresowanie IP - podstawa komunikacji

Jeśli komunikacja będzie oparta na TCP/IP, trzeba wybrać najlepszy do swojej sieci sposób konfiguracji adresowania protokołu. Każdy system wysyłający lub odbierający dane musi mieć przypisany unikatowy adres IP. Służy on do jednoznacznej identyfikacji systemu w sieci i składa się z czterech części, tzw. oktetów, oddzielonych kropkami. Każdy z nich może przybierać wartości z zakresu 0-255, przykładowy adres to 192.168.0.1. Niedopuszczalne jest dublowanie adresów, każdy identyfikator musi być unikatowy w obrębie tzw. podsieci, czyli wydzielonego fizycznego fragmentu sieci. Pomyłka w adresie sprawia, że dany komputer nie będzie mógł poprawnie komunikować się z innymi stacjami.

Drugi bardzo istotny element adresowania, maska podsieci, to również cztery oddzielone kropkami liczby, które muszą jednak przyjmować z góry ustalone wartości, np. 255.255.255.0 albo 255.255.0.0. Ta część adresowania IP pozwala na określenie, gdzie zlokalizowany jest odbiorca wysyłanych informacji - w lokalnej sieci, czy poza nią. W niektórych oknach konfiguracyjnych systemu Windows maska podsieci jest zapisywana w inny sposób. Zamiast oktetów należy wprowadzić wartość odpowiadającą liczbie bitów przeznaczonych na maskę. Adres IP 192.168.1.1 z maską 255.255.255.0 będzie przedstawiony jako 192.168.1.1/24. Zapis ten oznacza, że na maskę przeznaczono 24 bity. Dla przypomnienia: 255 binarnie równa się 11111111, co zajmuje osiem bitów. Podanie adresu IP oraz maski podsieci jest niezbędne do komunikacji.

Gdy system pracuje w grupach roboczych lub poza Internetem, wypełnienie pola związanego z adresem serwera DNS nie jest obowiązkowe, ale zalecamy to, bo przygotowujemy klienta do pracy w środowisku domenowym. Klienty korzystają z rozwiązywania nazw DNS w czasie wyszukiwania innych systemów w sieci, co ma bardzo duże znaczenie w czasie logowania do domeny. Informacje o kontach przechowywane są w Active Directory, użytkownik po wpisaniu swojej nazwy i hasła musi być uwierzytelniony przez kontroler domeny, czyli w naszym przypadku Windows Server 2003. W tym celu system klienta powinien zgłosić się do serwera i poprosić go o "wpuszczenie" do sieci. Żeby móc to zrobić, trzeba zlokalizować komputer z Windows Server 2003. Szybkie wyszukiwanie kontrolera domeny jest realizowane właśnie poprzez DNS. Klient wysyła zapytanie do serwera i w odpowiedzi otrzymuje listę adresów IP kontrolerów. Jeśli nie podamy preferowanego serwera DNS, system klienta odnajdzie kontroler, korzystając z emisji (broadcastu), jednak będzie to długo trwało. Pozostałe parametry TCP/IP, takie jak adres bramy domyślnej lub adres serwera WINS w opcjach zaawansowanych, konfigurujemy w razie potrzeby.

W wypadku sieci lokalnych, w których komputery nie oferują zasobów klientom z zewnątrz firmy, np. internetowym, zalecane jest stosowanie adresowania prywatnego, obejmującego grupy adresów niewykorzystywanych publicznie w Internecie. Identyfikatory sieci prywatnych przedstawiają się następująco: 10.0.0.0/8, 172.16.0.0/12 i 192.168.1.0/16. Oznacza to, że na potrzeby firmy możemy wybrać adresowanie z jednego z przedstawionych wyżej zakresów, przypisując komputerom np. w małej firmie adresy od 192.168.1.1 do 192.168.1.20 z maską 255.255.255.0. Nie trzeba przy tym sprawdzać, czy są gdziekolwiek stosowane do adresowania serwerów internetowych.

Sposoby przydzielania adresów

Windows Server 2003 oraz Windows XP pozwalają na wybranie różnych strategii konfigurowania protokołu TCP/IP. Najprostsza to ręczne przypisanie każdej stacji właściwego adresu. W tym celu należy wypełnić odpowiednie pola we właściwościach protokołu TCP/IP. Naturalnie adres i jego parametry należy wpisywać uważnie. W celu

uniknięcia bałaganu warto odnotowywać przydzielane adresy na osobnym arkuszu, a w większych firmach - w bazie danych.

Ręczne zarządzanie adresami IP ma dużo wad. Do najważniejszych zaliczamy trudności z ich modyfikacją oraz prawdopodobieństwo pomyłek podczas wprowadzania. Jeśli trzeba zaadresować na przykład 150 stacji, konfiguracja będzie trwała długo. Administrator lub grupa administratorów musi dojść do każdego komputera i nadać mu odpowiedni adres, więc prawdopodobieństwo popełnienia pomyłki jest znaczne. Zamiana dowolnej cyfry w adresie, masce podsieci lub adresie serwera DNS powoduje zakłócenia w komunikacji.

W celu usprawnienia tej procedury w wielu sieciach stosuje się adresowanie automatyczne. Instalowany i uruchamiany jest serwer DHCP, którego działanie polega na przydzielaniu klientom sieci adresów IP na żądanie. Stacja robocza w czasie startu wysyła prośbę o adres do serwera, który wybiera jeden z puli i nadaje go klientowi na okres ustalany przez administratora. W naszym przypadku funkcję serwera może z powodzeniem pełnić Windows Server 2003. Ponieważ adresy są nadawane automatycznie, administrator nie musi odwiedzać każdego z komputerów na wypadek modyfikacji ustawień. Jeśli chcemy wprowadzić inne parametry adresu, związane np. z serwerem DNS, dzięki centralnej konfiguracji dotrą one bez kłopotu do wszystkich klientów sieci. Problemem może być oczywiście awaria serwera DHCP, ale jeśli skorzystamy z dostępnej w Windows XP funkcji alternatywnego adresowania, ten kłopot zostanie ominięty.

Ostatni z możliwych sposobów to automatyczne adresowanie prywatne, dostępne w systemach operacyjnych Microsoftu od Windows 98 SE, z wyjątkiem - uwaga! - Windows NT. Polega na samoistnym przypisaniu adresu IP wtedy, gdy nie można go uzyskać w inny sposób. Jeśli stacja ma na przykład skonfigurowane pobieranie adresu z serwera DHCP, ale serwer z dowolnej przyczyny jest nieosiągalny, wówczas system sam przypisze sobie adres. Będzie to identyfikator ze z góry narzuconego zakresu od 169.254.0.1 do 169.254.255.254, z maską 255.255.255.0. Adresowanie to stosuje się w bardzo małych grupach roboczych po to, żeby oszczędzić użytkownikom konieczności zapamiętania reguł adresowania IP i zminimalizować skutki awarii, podczas których nie można przydzielać klientom adresów IP.

Przykładowe rozwiązanie adresowania w sieci

W przykładowej konfiguracji sieci wykorzystujemy ręczne przydzielanie adresów IP. Ustawienia związane z DHCP zostaną opisane po omówieniu tej usługi. Zakładamy, że nasza sieć nie przekroczy jednej lokalizacji i będzie w niej wykorzystywanych najwyżej 100 systemów. W takim wypadku z powodzeniem możemy wykorzystać jedną z grup adresów prywatnych, np. sieć 192.168.1.0 z maską 255.255.255.0.

Pracę należy rozpocząć od wprowadzenia parametrów TCP/IP Windows Server 2003. W tym celu klikamy Start | Panel sterowania | Połączenia sieciowe. Następnie wybieramy połączenie związane z kartą sieciową. Jeśli na serwerze jest tylko jedna karta sieciowa, to domyślnie otrzymuje nazwę Połączenie lokalne. Gdy jest wiele interfejsów sieciowych, w celu zwiększenia czytelności zaleca się zmianę nazwy, np. na LAN lub LocalNet (opcję Zmień nazwę znajdziesz w menu podręcznym połączenia lokalnego). Kliknięcie wybranego połączenia otwiera okno Stan.

We właściwościach tego okna wyświetlana jest lista składników sieciowych związanych z połączeniem. W celu zmiany ustawień TCP/IP należy zaznaczyć ten protokół oraz kliknąć Właściwości. Karta Ogólne zawiera pola związane z adresowaniem IP oraz adresami serwerów DNS. Konfiguracja Windows Server 2003 wymaga ręcznego ustawienia adresów. Zgodnie z założeniami, w polu adresu IP wprowadzamy: 192.168.1.1, a jako maskę podsieci 255.255.255.0. Następnie przechodzimy do pola Preferowany serwer DNS i wpisujemy odpowiedni adres. Zakładamy, że serwerem DNS jest serwer lokalny i

dlatego wpisujemy 192.168.1.1. Jeśli sieć nie jest ograniczona do zasobów lokalnych i wymaga dostępu np. do Internetu, należy również wypełnić pole Brama domyślna. Powinno zawierać adres IP systemu lub urządzenia będącego routerem. W schematach adresowania stosowanych w sieciach lokalnych bramy oznaczane są najczęściej jedynką, np. 10.0.0.1, ale jest to rozwiązanie zwyczajowe i nie musimy go stosować. Jeśli zmieniamy adres na funkcjonującym serwerze, trzeba zwrócić uwagę na ustawienia usług sieciowych, które mogą wymagać rekonfiguracji. Dzieje się tak na przykład w przypadku usługi DHCP.

Zakończenie konfiguracji serwera pozwala na przejście do stacji klienckich. Na komputerach pracujących pod kontrolą Windows XP przypisanie parametrów protokołu TCP/IP przebiega bardzo podobnie. We właściwościach połączenia sieciowego odnajdujemy składnik TCP/IP, w którym wypełniamy te same pola. Oczywiście maska oraz adres serwera DNS pozostają takie same - w naszym przypadku 255.255.255.0, DNS: 192.168.1.1. Modyfikacji podlega jedynie adres IP. Aby uniknąć problemów, przydzielone adresy należy odnotowywać w pliku tekstowym lub odpowiednim arkuszu. Rekonfiguracja adresu nie wymaga restartu komputera. Na koniec warto sprawdzić, czy nasze działania są skuteczne. W tym celu wystarczy posłużyć się poleceniem ping z parametrem będącym adresem serwera. Jeśli po uruchomieniu wiersza poleceń i wpisaniu: ping 192.168.1.1 otrzymamy pozytywną odpowiedź, będzie to oznaczać poprawną konfigurację protokołu TCP/IP, zarówno po stronie serwera, jak i stacji XP.

Automatyzacja adresowania przez DHCP

Automatyczne adresowanie może zdecydowanie ułatwić pracę administratora. Do konfiguracji adresowania tego typu będziemy potrzebować serwera DHCP. Ponieważ w skład usług sieciowych dostarczanych z Windows Server 2003 wchodzi protokół dynamicznej konfiguracji hosta (DHCP), wystarczy odpowiednio przygotować serwer.

Działanie serwera DHCP jest stosunkowo proste. Komputery klienckie w sieci podczas startu systemu sprawdzają lokalną konfigurację TCP/IP. Jeśli w parametrach protokołu zaznaczona jest opcja Uzyskaj adres IP automatycznie, system operacyjny musi się postarać o przydzielenie adresu. Najpierw należy zlokalizować serwer DHCP. Ponieważ na początku system nie wie, która stacja pełni to zadanie, do wszystkich komputerów w sieci wysyłana jest prośba o zgłoszenie się serwera DHCP. Na tę prośbę odpowiadają jedynie maszyny z uruchomioną usługą DHCP. W naszym przypadku będzie to Windows Server 2003. Otrzymana odpowiedź zawiera ofertę adresu IP. Klient potwierdza przyjęcie oferty, wysyłając odpowiednią informację do sieci. Na koniec serwer, którego oferta została przyjęta, odsyła klientowi potwierdzenie nadania adresu. Od tej chwili stacja staje się pełnoprawnym dzierżawcą adresu i parametrów IP. Opisane działanie odbywa się podczas pierwszego kontaktu z serwerem DHCP. Jeśli stacja już otrzymała adres, powtórne odwołania do serwera wyglądają nieco inaczej. Komputer "wynajmujący" adres może się nim posługiwać w wyznaczonym przez administratora okresie. Domyślnie jest to osiem dni. Po upływie połowy czasu dzierżawy lub podczas każdego restartu komputera stacja kontaktuje się z serwerem DHCP w celu odnowienia dzierżawy i związanych z nią parametrów. Jeśli system nie będzie mógł odnaleźć usługodawcy, DHCP będzie używał adresu do czasu jego wygaśnięcia.

Podstawowa konfiguracja serwera DHCP opiera się na założeniu i uaktywnieniu zakresu adresów. Zakres to przedział adresów IP, jakim będą się posługiwały klienty sieci. Definicja zakresu zawiera nazwę, adres początkowy, adres końcowy, maskę podsieci, czas dzierżawy oraz dodatkowe opcje związane z innymi parametrami przekazywanymi klientom sieci, np. adres domyślnej bramy lub serwera DNS. Zanim klienty sieci będą mogły wykorzystać zakres, należy go uaktywnić. Jeśli na serwerze wyczerpie się pula adresów dla klientów, kolejne zgłaszające się komputery nie otrzymają adresu. W takim wypadku należy albo zwiększyć pulę, albo skrócić czas dzierżawy.

Dodatkowe parametry DHCP

Zanim przejdziemy do przykładowej konfiguracji serwera DHCP na potrzeby naszej sieci, powinniśmy poznać kilka dodatkowych szczegółów związanych z jego pracą. Pierwszą istotną czynnością, jaką należy wykonać po zainstalowaniu serwera, jest autoryzacja DHCP w usłudze Active Directory. Ponieważ klienty usługi DHCP nie mogą decydować, z którego serwera będą pobierały adres IP, pojawienie się w sieci nieznanych serwerów sprawia wiele problemów. Część stacji po otrzymaniu niewłaściwego adresu nie będzie mogła się komunikować z pozostałymi komputerami. Aby ograniczyć możliwość powstania tego typu trudności, wprowadzono autoryzację serwerów, która wymaga obecności w sieci usługi Active Directory. Active Directory utrzymuje listę zarejestrowanych serwerów, które mogą świadczyć usługi DHCP. W czasie uruchamiania usługi DHCP w Windows Server 2003 lub Windows 2000, systemy te weryfikują swoją obecność na liście uprawnionych komputerów. Jeśli serwer nie jest autoryzowany, nie będzie przydzielał adresów klientom sieci. Autoryzacja nie potrafi zablokować przyznawania IP przez serwery na przykład z systemem Linux czy Windows NT.

W większości sieci konfiguracja adresowania IP nie kończy się na przypisaniu adresu i maski podsieci. Często klienty muszą mieć określone dodatkowe parametry, takie jak adres routera lub adres serwera WINS. W przypadku domen Active Directory konieczne jest również dostarczenie adresu serwera DNS. DHCP byłaby bardzo mizerną usługą, gdyby nie potrafiła przekazać dodatkowych parametrów IP. W Windows Server 2003 możemy zdefiniować wiele poziomów opcji, które będą przenoszone na klienty sieci. Opcje mogą być nadawane z poziomu serwera, zakresu, zastrzeżenia albo klas zdefiniowanych przez administratora lub dostawców. Najczęściej wykorzystywane są opcje zakresu, obejmujące klienty z określonej grupy adresów IP. Po zdefiniowaniu opcji, np. DNS, wszystkim stacjom pobierającym adres z zakresu będzie nadany adres IP i maska podsieci oraz zostanie dla nich ustawiony adres serwera DNS. Opcje DHCP możemy konfigurować w czasie tworzenia zakresu albo w dowolnym terminie późniejszym. Zmiana wartości opcji zostanie automatycznie przypisana komputerom klientom sieci w czasie odnawiania dzierżawy adresu.

Kolejnym przydatnym ustawieniem DHCP jest możliwość wykonywania rezerwacji i wykluczeń adresów. Ponieważ DHCP przydziela adresy dynamicznie, może się zdarzyć, że co pewien czas stacje otrzymają różne adresy IP. Jeśli zależy nam na tym, aby określony komputer miał zawsze przydzielany ten sam adres, należy skonfigurować rezerwację. Działanie rezerwacji polega na powiązaniu adresu IP z adresem fizycznym karty sieciowej klienta. Gdy do serwera zgłosi się komputer z zastrzeżonym adresem MAC, serwer przydzieli mu skojarzony IP. Wykluczenia to ustawienia, które rozwiązują problemy innego rodzaju. Jeśli w sieci działa już grupa urządzeń lub komputerów z przypisanymi ręcznie adresami IP, może dojść do tego, że zakresy obejmują już przydzielone adresy. W takim wypadku należałoby wykluczyć z zakresu zajęte IP. Wprowadzanie wykluczeń jest możliwe w trakcie tworzenia zakresu albo w dowolnym momencie pracy serwera.

Przykładowa konfiguracja DHCP

Konfigurację serwera DHCP rozpoczynamy od instalacji usługi dynamicznego przydzielania adresów. W tym celu należy przejść do Panelu sterowania na serwerze i dwukrotnie kliknąć opcję Dodaj lub usuń programy. Następnie klikamy ikonę Dodaj/Usuń składniki systemu Windows. W oknie Kreatora składników systemu Windows wyszukujemy Usługi sieciowe. Po zaznaczeniu tej opcji klikamy przycisk Szczegóły, w nowym oknie umieszczamy znacznik w polu Protokół dynamicznej konfiguracji hosta (DHCP) i naciskamy OK. System zainstaluje odpowiednie pliki i zakończy instalację.

Do konfiguracji usługi służy przystawka DHCP. Ponieważ interfejs konsoli przeznaczonych do zarządzania jest zunifikowany, dla tych, którzy poznali już takie narzędzia, jak: Użytkownicy i komputery usługi Active Directory czy chociażby Eksplorator Windows,

obsługa przystawki będzie bardzo prosta. Jak zwykle okno jest podzielone na dwa panele: w lewym są zgrupowane obiekty będące odpowiednikami pojemników na informacje, a prawy zawiera szczegółowe dane gromadzone przez te pojemniki. Jeśli na przykład w lewym panelu zaznaczymy obiekt Dzierżawy adresów, w prawym zostanie wyświetlona lista "wynajętych" adresów IP wraz z dodatkowymi informacjami o nazwie komputera, terminie wygaśnięcia dzierżawy itp.

Zgodnie z opisanymi wcześniej sposobami funkcjonowania serwera DHCP, powinniśmy rozpocząć od autoryzacji usługi w Active Directory. W tym celu zaznaczamy w lewym panelu ikonę reprezentującą serwer, a następnie z menu Akcja wybieramy opcję Autoryzuj. Po odświeżeniu obrazu strzałka w ikonie serwera powinna być skierowana ku górze. Następnie wybieramy menu Akcja | Nowy zakres. Nowy zakres tworzymy, używając Kreatora nowych zakresów. W oknie powitalnym kreatora klikamy przycisk Dalej. Najpierw należy podać nazwę zakładanego zakresu. W naszym przykładzie posłużymy się nazwą SiećLokalna. Pole Opis możemy pozostawić puste. Jeśli serwer DHCP będzie obsługiwał więcej zakresów, ich przejrzyste opisywanie przyda się na przykład innym pracownikom działu IT. Po kliknięciu Dalej przechodzimy do konfiguracji zakresu adresów. W polu Początkowy adres IP wprowadzamy np. 192.168.1.10, a w polu Końcowy adres IP: 192.168.1.109.

System automatycznie zaproponuje nam maskę podsieci do tego zakresu. Jeśli nie będzie nam odpowiadała, możemy ją zmodyfikować, wpisując bitową długość maski albo wartość dziesiętną. W przykładowej sieci posługujemy się maską 24-bitową, dlatego możemy zaakceptować propozycję serwera i kliknąć Dalej. Kolejne okno służy do określania ewentualnych wykluczeń. Gdy to konieczne, należy wypełnić pola Początkowy adres IP i Końcowy adres IP. Pomijamy te ustawienia i przechodzimy do ustawień czasu dzierżawy. Nasza testowa sieć obsługuje wyłącznie klienty lokalne, dlatego możemy ustalić miesięczny okres wynajmowania adresów. W polu Dni zmieniamy wartość na 30 i klikamy Dalej. Następnie kreator pyta, czy chcemy skonfigurować dodatkowe opcje serwera. W naszym przykładzie powinniśmy ustawić przekazywanie klientom adresu serwera DNS, więc pozostawiamy zaznaczenie opcji Tak, chcę teraz skonfigurować te opcje i przechodzimy do następnego okna. Określa się w nim adres routera, a ponieważ założyliśmy wcześniej, że sieć ogranicza się do zasobów lokalnych, pole Adres IP pozostawiamy puste. Następne okno służy do konfiguracji parametrów związanych z usługą DNS. W pole Domena nadrzędna wpisujemy nazwę naszej domeny. Tak jak poprzednio, będzie nią pl.idg.com. Oczywiście musimy również wprowadzić adres serwera DNS, w naszym przypadku 192.168.1.1. Klikamy Dodaj i przechodzimy do kolejnego okna.

Służy ono do konfiguracji przekazywania klientom adresu serwera WINS. Ponieważ nie będziemy konfigurować tej usługi, pole adresu pozostawiamy puste i klikamy Dalej. W ostatnim oknie kreatora decydujemy, czy konfigurowany zakres ma zostać uaktywniony. Uaktywnienie zakresu uruchamia obsługę klientów zgłaszających się do serwera i kończy działanie kreatora. Jeśli chcemy zmodyfikować lub do założonego zakresu dodać nowe opcje, należy w lewym panelu rozwinąć zakres, następnie zaznaczyć go i z menu Akcja wybrać polecenie Konfiguruj opcje.

Ostatnią operacją przykładowej konfiguracji będzie dodanie rezerwacji klienta. Załóżmy, że komputer w sekretariacie powinien mieć zawsze przypisany adres 192.168.1.25. Do ustawienia zastrzeżenia będziemy potrzebować fizycznego adresu karty sieciowej tej stacji. Możemy go ustalić na kilka sposobów. Jeśli jesteśmy blisko, wystarczy podejść do komputera i w wierszu polecenia wpisać:

ipconfig /all. Adres MAC będzie wyświetlony w polu Adres fizyczny. Jeśli system pobrał już adres z DHCP, na liście wydzierżawianych adresów znajduje się pole Unikatowy identyfikator, które zawiera fizyczny adres karty sieciowej klienta. Gdy mamy adres MAC, konfiguracja rezerwacji jest prosta. Rozwijamy zakres, następnie zaznaczamy obiekt

Zastrzeżenia i wybieramy menu Akcja | Nowe zastrzeżenie. W wyświetlonym oknie wprowadzamy nazwę rezerwacji, np. Sekretariat, dalej wpisujemy adres IP, który będzie zarezerwowany dla tego komputera. Zgodnie z założeniami, jest to 192.168.1.25. W pole adresu MAC wpisujemy adres fizyczny karty sieciowej. Pole Opis jest opcjonalne. Naciśnięcie przycisku Dodaj zatwierdza konfigurację rezerwacji. Na koniec przestawiamy ustawienia TCP/IP klientów na automatyczne pobieranie adresu IP i adresu serwera DNS.

Zadania i działanie DNS

DNS jest usługą zwykle kojarzoną z Internetem. Jej integracja z domenami Windows 2000 i 2003 to dla wielu użytkowników nowość. Głównym zadaniem serwerów DNS jest rozwiązywanie nazw w sieciach pracujących pod kontrolą protokołu TCP/IP. Najczęściej obserwujemy ich działanie w czasie przeglądania witryn internetowych. Jeśli w przeglądarce wprowadzamy nazwę, np. www.pcworld.pl, w celu dotarcia do serwera WWW system musi ją zamienić na adres IP. Jeśli nie będzie mógł tego zrobić, witryna nie zostanie otwarta. Alternatywnym sposobem kojarzenia nazw z adresami IP jest wykorzystanie pliku Hosts. Możemy go odnaleźć w %systemroot%\system32\Drivers\Etc. To zwykły plik tekstowy, który zawiera proste odwzorowanie: adres IP - nazwa, np. "194.69.207.64 www.idg.pl". System najpierw sprawdza, czy określona nazwa znajduje się w pliku Hosts, a dopiero później korzysta z usług DNS. Różne sposoby rozwiązywania nazw są stosowane dlatego, że o wiele prościej jest posługiwać się nazwami niż ciągami liczb. O wiele łatwiej zapamiętać "www.idg.pl" niż "194.69.207.67". Ponadto w przypadku stosowania usługi DNS o zmianie adresu serwera nie trzeba informować wszystkich stacji klienckich, wystarczy uaktualnić ustawienia DNS.

Działanie usługi DNS polega na odbieraniu zapytań od stacji klienckich w sieci, przetwarzaniu ich i zwracaniu odpowiedzi. Jeśli wprowadzimy dowolną nazwę w przeglądarce, to zanim przejdziemy do określonej witryny, do serwera DNS zostanie wysłana prośba o odnalezienie skojarzonego z nią adresu IP. DNS gromadzi informacje w rekordach, które zawierają nazwę, adres lub inne przydatne dane. Rekordy DNS mogą być różnego typu, np. A, MX, PTR, SRV. W czasie realizacji zapytania oprogramowanie klienta wyszukuje określone adresy, nazwy lub typy rekordów. W zależności od konfiguracji, jeśli serwer nie będzie mógł udzielić odpowiedzi, pytanie przejdzie do innego usługodawcy DNS lub zostanie zwrócony komunikat o nieodnalezieniu rekordu.

W domenach pracujących pod kontrolą Active Directory celem serwerów DNS jest udzielenie odpowiedzi na zapytania o adres IP systemów, które oferują usługi związane z Windows Server 2003. Informacje o usługach są przechowywane w rekordach SRV, dlatego serwer musi je rozpoznawać. Starsze serwery DNS, np. dostarczane razem z Windows NT 4.0, nie obsługują rekordów SRV, dlatego nie nadają się do Active Directory. Usługa ta może korzystać z serwerów DNS pracujących z innymi systemami operacyjnymi, jeśli będą rozpoznawały wymienione rekordy. Zalecane jest posługiwanie się serwerami Windows 2000 lub 2003. W czasie instalacji kontrolera domeny niezbędne wpisy związane z Active Directory są dodawane automatycznie. Nie musimy się więc martwić o właściwe zarządzanie rekordami wykorzystywanymi przez domenę.

Domenowa przestrzeń nazw

Omawiając usługę Active Directory, niejednokrotnie stosowaliśmy określenie "domena", termin ten jest również szeroko wykorzystywany w Internecie. Mimo zbieżności nazwy chodzi o różne zagadnienia. Domena Active Directory to grupa komputerów wskazanych przez administratora sieci, która należy do bazy usług katalogowych i korzysta z niej. Domeny DNS są związane z przestrzenią nazw, do których się odwołujemy, przeglądając strony internetowe. Przestrzeń ta może być również wykorzystywana na potrzeby Active Directory.

W systemie plików mamy do czynienia z katalogiem głównym, podkatalogami i plikami, a w systemie DNS są: korzeń, domeny, poddomeny i rekordy. Główną różnicę stanowi rozproszenie przestrzeni nazw na wiele serwerów. Nazwy DNS biorą swój początek z katalogu głównego, czyli korzenia. Jest reprezentowany przez kropkę na końcu używanej nazwy, np. idg.com. Poniżej znajdują się znane wszystkim domeny wysokiego poziomu, takie jak com, edu, org, net czy pl. Określają kraj lub przeznaczenie przechowywanych przez nie nazw. Na kolejnym poziomie przestrzeni umieszczane są nazwy-domeny - rejestrowane przez firmy, użytkowników lub organizacje, np. pcworld lub computerworld. Domeny mogą mieć swoje poddomeny, te z kolei - swoje poddomeny itd. Dokładnie tak, jak katalogi mogą mieć podkatalogi. W domenach lub poddomenach możemy zakładać rekordy wskazujące na zasoby (hosty). Najczęściej są nimi komputery oferujące określone usługi, takie jak np. ftp. Nazwy domen wysokiego poziomu, domen oraz hostów tworzą nazwy FQDN (w pełni kwalifikowane nazwy domen). Można je porównać do ścieżek dostępu w systemie plików, np. nazwą FQDN jest puchatek.pcworld.pl, oznaczająca, że w domenie wysokiego poziomu (pl) została założona domena pcworld, w której jest host puchatek. Warto zwrócić uwagę, że - w przeciwieństwie do nazw plików - nazwy DNS są odczytywane od końca.

Innym pojęciem ściśle związanym z usługą DNS jest strefa, czyli wydzielony na potrzeby administracyjne fragment przestrzeni nazw. Ich funkcja jest oczywista - trudno sobie wyobrazić jeden serwer, na którym byłyby nanoszone i modyfikowane wszystkie nazwy. Aby ułatwić zarządzanie i utrzymywanie całej struktury nazw, jej poszczególne części są rozpraszane na wiele serwerów DNS. Jeśli firma jest duża, może mieć własny serwer DNS zajmujący się gromadzeniem informacji związanych z jej zasobami. Domenami mniejszych przedsiębiorstw zajmują się dostawcy internetowi. W czasie instalacji usługi definiujemy jeden z dwóch rodzajów stref. Windows Server 2003 pozwala na założenie strefy wyszukiwania do przodu oraz strefy wyszukiwania wstecznego. Pierwsza jest przeznaczona do odpowiadania na zapytania związane z nazwą. Klient przysyła nazwę, np. www.pcworld.pl, i w odpowiedzi oczekuje adresu IP. Strefy wyszukiwania wstecznego realizują działania odwrotne: w odpowiedzi na otrzymany od klienta adres IP wysyłana jest skojarzona z nim nazwa. Ponieważ DNS to usługa wielopoziomowa i rozproszona, tzn. hierarchia domen jest utrzymywana na wielu serwerach, strefy muszą być ze sobą powiązane. Jeśli klient będzie chciał na przykład rozwiązać nazwę hosta test.idg.pl, a firma IDG ma własny serwer DNS ze strefą obejmującą nazwę idg, najpierw trzeba będzie zapytać jeden z serwerów korzenia o domenę pl, a następnie serwer odpowiedzialny za domenę pl o idg. Aby było to możliwe, serwer DNS przechowujący dane o domenie pl musi zawierać informacje, które pozwolą odesłać stacje klienckie do serwera IDG. Jeśli usługa DNS jest wykorzystywana wyłącznie na potrzeby Active Directory, nie trzeba się łączyć z korzeniem lub serwerami przechowującymi domeny wysokiego poziomu. Na lokalnym serwerze wymagana jest jedynie obecność strefy związanej z własną domeną.

Każdy z rodzajów stref dzielimy również ze względu na dostępność wprowadzania danych i sposób magazynowania informacji. Możemy zakładać takie strefy wyszukiwania do przodu, jak podstawowe, pomocnicze oraz skrótowe. Dodatkowo należy określić, czy strefy te będą przechowywane w plikach tekstowych na serwerze, czy zintegrowane z usługą Active Directory. Decyzja o typie zakładanej strefy zależy od wielu czynników, np. zakresu wykorzystania nazwy (lokalne czy globalne), rodzaju serwerów DNS (tylko Windows Server 2003 czy również Linux), rozmiar sieci (lokalny czy rozległy) itp. W naszym przykładzie należy założyć strefę wyszukiwania do przodu, podstawową, przechowywaną w usłudze Active Directory.

Instalacja i konfiguracja DNS

Przygotowanie DNS do świadczenia usług klientom sieci może być realizowane na dwa sposoby. Najprostszy z nich został już opisany w poprzednich artykułach. Dla przypomnienia: w czasie instalacji kontrolera domeny należy zaznaczyć opcję związaną z

instalacją usługi DNS. Jeśli to zrobimy, kreator instalacji Active Directory zainstaluje i skonfiguruje DNS na lokalnym serwerze Windows Server 2003. Sposób ten zalecamy administratorom z mniejszym doświadczeniem. Naturalnie automatyczna instalacja nie przeszkadza w późniejszej zmianie parametrów usługi za pomocą odpowiednich narzędzi.

Ręczna instalacja DNS jest nieco lepszym rozwiązaniem, gdyż pozwala na szczegółową konfigurację wszystkich niezbędnych parametrów usługi. Jeśli DNS jest uruchamiany wyłącznie na potrzeby Active Directory, nie ma zbyt wielu ustawień konfiguracyjnych. Po zainstalowaniu usługi w narzędziach administracyjnych pojawia się skrót do modułu zarządzania serwerem DNS. Narzędzie DNS ma standardowy interfejs administracyjny. W lewym panelu w postaci folderów wyświetlane są serwery i założone w nich strefy. Kliknięcie jednej ze stref wyświetla w prawym panelu założone w niej rekordy. Jeżeli chcemy założyć nową strefę, klikamy prawym przyciskiem folder Strefy wyszukiwania do przodu lub Strefy wyszukiwania wstecznego i wybieramy opcję Nowa strefa. Potem wprowadzamy dane związane z rodzajem strefy oraz jej parametrami. Innym, łatwiejszym sposobem ustawienia serwera DNS jest skorzystanie z kreatora. Uruchamiamy go, klikając prawym przyciskiem ikonę serwera, następnie wybieramy opcję Konfiguruj serwer DNS.

Tworząc strefę związaną z nazwą domeny Active Directory, przygotowaliśmy swego rodzaju pojemnik do przechowywania właściwych rekordów DNS. Żeby usługa była w pełni funkcjonalna należy w domenie umieścić odpowiednie rekordy. Informacje w nich zawarte są wykorzystywane do lokalizacji właściwych zasobów. W niewielkich sieciach pracujących pod kontrolą Windows Server 2003 najlepiej zastosować automatyczne wprowadzanie rekordów do DNS. W tym celu musimy odpowiednio przygotować zarówno serwer, jak i stacje klienckie w sieci. Konfiguracja serwera jest stosunkowo łatwa. Po pierwsze, trzeba sprawdzić, czy w parametrze TCP/IP - Użyj następujących adresów serwerów DNS - jest wprowadzony lokalny adres IP. Jeśli tak, sprawdzamy z kolei, czy we właściwościach strefy wyszukiwania do przodu, związanej z naszą domeną, jest włączona aktualizacja dynamiczna. Odpowiednią listę rozwijaną znajdziemy na karcie Ogólne (np. właściwości strefy pl.idg.com). W przypadku stref zintegrowanych z Active Directory dostępne są trzy opcje: Brak, Niezabezpieczone i zabezpieczone oraz Tylko zabezpieczone. Zalecane jest wybranie ostatniej opcji.

Jeżeli w sieci nie ma innych klientów niż systemy Windows XP, możemy przejść do weryfikacji ustawień stacji roboczych. Ponieważ podczas instalacji komponentów sieciowych Windows automatycznie konfigurowany jest protokół TCP/IP z opcją Zarejestruj adresy tego połączenia w DNS, nasze zadanie polega jedynie na sprawdzeniu, czy opcja ta jest włączona. Prowadzi do niej następująca ścieżka Start | Panel sterowania | Połączenia sieciowe | Właściwości interfejsu sieciowego | Protokół internetowy TCP/IP | Właściwości | Zaawansowane | Karta DNS. Jeśli wszystkie wspomniane wyżej opcje są skonfigurowane, klienty będą dynamicznie rejestrowały swoje nazwy w usłudze DNS.

Jednym z ważniejszych zadań serwera DNS jest dostarczanie informacji o kontrolerach domeny. Potrzebne w tym celu rekordy są automatycznie dodawane do strefy. Za te czynności odpowiada usługa Logowanie do sieci (Netlogon). Administrator nie musi dodawać żadnych wpisów ręcznie.

Przykładowa konfiguracja DNS na potrzeby Active Directory

W celu dodania DNS do usług uruchomionych w Windows Server 2003 należy kliknąć Panel sterowania | Dodaj/Usuń programy | Dodaj/Usuń składniki systemu Windows | Usługi sieciowe | Szczegóły. W nowym oknie zaznaczamy System DNS (Domain Name System) i wybieramy OK. Kliknięcie przycisku Dalej powoduje instalację usługi, a naciśnięcie Zakończ zamyka kreator.

Najprostszym i najszybszym sposobem konfiguracji usługi DNS jest wykorzystanie kreatora. Uruchamiamy dostępną w narzędziach administracyjnych przystawkę DNS, zaznaczamy ikonę serwera IDGTEST i klikamy prawym przyciskiem myszy. Z listy wybieramy opcję Konfiguruj serwer DNS. Po uruchomieniu kreatora klikamy Dalej. W oknie Wybierz akcję konfiguracji zaznaczamy Utwórz strefę wyszukiwania do przodu (zalecane w małych sieciach) | Dalej. W następnym oknie pozostawiamy zaznaczone Ten serwer przechowuje strefę. Po naciśnięciu Dalej wpisujemy nazwę strefy. Nasza przykładowa sieć powinna mieć założoną taką strefę, jak nazwa domeny, czyli pl.idg.com. Następne okno służy do konfiguracji typu aktualizacji dynamicznych tu również pozostawiamy zaznaczoną opcję Zezwalaj tylko na zabezpieczone aktualizacje dynamiczne. Ponieważ serwer ma być wykorzystywany jedynie w małej sieci lokalnej, bez połączeń zewnętrznych, w oknie Usługi przesyłania dalej należy zaznaczyć opcję Nie, nie powinien przesyłać kwerend dalej. Naciśnięcie przycisku Zakończ sprawia, że serwer DNS może realizować zapytania klientów sieci.

Konfiguracja klientów sieci

Jeśli serwer został należycie przygotowany do swojej roli, możemy przejść do konfiguracji klientów sieci. Najpierw warto poświęcić kilka chwil na rozstrzygnięcie, który z systemów operacyjnych najlepiej nadaje się do pracy z Windows Server 2003. W niewielkiej sieci, w której komputery mają już zainstalowane oprogramowanie, często spotykamy wiele wersji systemów operacyjnych. Niejednorodność środowiska sprawia, że administrator musi na konfigurację i zarządzanie systemami klienckimi poświęcić nieco więcej czasu. Optymalne środowisko pracy to takie, w którym wszystkie komputery sieciowe działają pod kontrolą takiego samego systemu operacyjnego, nawet jeśli będzie to starszy Windows 98 SE. Eliminuje to wiele problemów, związanych np. z automatyzacją ustawień dotyczących stacji roboczych.

Jeżeli sieć powstaje od podstaw i możemy określić, jakie oprogramowanie będzie potrzebne, bezwzględnie należy wybrać jeden z nowszych systemów operacyjnych: Windows XP Professional albo Windows 2000 Professional. To bardzo uprości administrowanie siecią. Dodatkowo będziemy mogli w pełni wykorzystać wszystkie zalety Windows Server 2003, takie jak Zasady grupy lub IPSec.

Naszymi przykładowymi stacjami będą komputery z zainstalowanym systemem Windows XP Professional. Warto pamiętać, że Windows XP Home nie jest przeznaczony do pracy w sieciach, bo nie oferuje wielu istotnych w takich środowiskach funkcji. System XP Home na przykład niełatwo dodać do domeny Active Directory.

Możliwość współpracy systemu z innymi komputerami w domenie zależy od prawidłowego skonfigurowania ustawień komunikacyjnych. Ponieważ w Windows XP Professional określanie ustawień sieciowych nie różni się od tego, co oferuje Windows Server 2003, poprawne nadanie parametrów jest proste. Dodatkowo XP automatycznie wykrywa karty sieciowe i uruchamia połączenia lokalne, zatem jeśli nie ma kłopotów ze sterownikiem, konfiguracja może polegać tylko na weryfikacji ustawień. Na początku artykułu omówiliśmy konfigurację odpowiednich parametrów TCP/IP w Windows Server 2003. W wypadku Windows XP ustawienia są identyczne. Po wybraniu właściwości TCP/IP sprawdzamy, czy opcja automatycznego pobierania adresu z serwera DHCP jest zaznaczona.

Praca stacji w domenie

Zanim rozpoczniemy pracę w domenie, musimy się do niej "zapisać". W przypadku systemu Windows XP Professional "zapisanie" polega na założeniu w bazie Active Directory konta komputera sieciowego oraz skonfigurowaniu w Windows XP przynależności do domeny. Operacje te mogą być wykonywane oddzielnie lub - co jest nieco wygodniejsze - łącznie z poziomu stacji roboczej.

Dodawanie komputera do domeny można przeprowadzić na kilka sposobów. Jeśli instalujemy system Windows XP na stacji roboczej, już w czasie konfiguracji możemy "zapisać" komputer do domeny. Jeśli Windows jest już zainstalowany, należy skorzystać z karty Nazwa komputera, dostępnej po dwukrotnym kliknięciu ikony System w Panelu sterowania. Na tej karcie są dwa przyciski: Identyfikator sieciowy i Zmień. Służą do konfigurowania podobnych ustawień systemu, ale są między nimi drobne różnice. Kliknięcie przycisku Identyfikator sieciowy powoduje uruchomienie kreatora przypisującego komputer do domeny oraz konfigurującego ustawienia kont domenowych w lokalnej bazie użytkowników. W oknie wyświetlonym po naciśnięciu przycisku Zmień można zmienić nazwę komputera, sufiks domeny DNS oraz przynależność do grupy roboczej lub domeny.

Zakładając konto komputera oddzielnie, możemy określić lokalizację konta w odpowiednim pojemniku bazy Active Directory. Ma to duże znaczenie, jeśli chcemy korzystać z zalet konfiguracji Zasad grup, pozwalających na automatyczne przekazywanie ustawień komputera w zależności od pojemnika, w którym znajduje się jego konto. Na przykład inne ustawienia mogą przejść z serwera na stacje założone w jednostce organizacyjnej NetWorld, niż na te, które umieścimy w PCWorld. Jeśli będziemy łącznie dodawać konto i "zapisywać" komputer do domeny, system automatycznie umieści konto stacji w jednostce organizacyjnej Computers. Ponieważ jest to pojemnik wbudowany, nie możemy przypisać mu ustawień Zasad grupy. Oczywiście nic nie stoi na przeszkodzie, żeby korzystając z opcji Przenieś, umieścić konto w innym pojemniku, ale wymaga to dodatkowych czynności. Zanim zaczniemy konfigurować środowisko robocze dla stacji, powinniśmy wybrać najwygodniejszy sposób postępowania.

Aby uniknąć przykrych niespodzianek, przed fizycznym dodaniem stacji do domeny należy zapoznać się z zagadnieniami związanymi z bezpieczeństwem. Dodawanie komputerów do Active Directory oraz zmiana lokalnych ustawień Windows XP jest możliwa wtedy, gdy mamy odpowiednie uprawnienia. Dostęp do karty Nazwa komputera w Windows XP jest ograniczony do kont należących do lokalnej grupy Administratorzy. Pracując na innym koncie, należy skorzystać z opcji Uruchom jako. Aktywujemy ją, zaznaczając ikonę System i naciskając klawisz [Shift] oraz prawy przycisk myszy. Podajemy nazwę i hasło konta z grupy Administratorzy. W czasie dodawania komputera do domeny system łączy się z Windows Server 2003 i wprowadza konto do bazy Active Directory. Domyślne ustawienia serwera pozwalają na wykonanie tych czynności użytkownikom będącym członkami domeny. Zanim konto zostanie dodane, należy podać właściwą nazwę konta, hasło oraz nazwę domeny. Każdy uwierzytelniony użytkownik domeny może założyć do dziesięciu kont komputerów. Ograniczenie to nie jest, oczywiście, związane z kontem administratora Windows Server 2003.

Przykładowa konfiguracja klientów sieciowych

Konfigurację stacji roboczej rozpoczynamy od weryfikacji poprawności parametrów interfejsu sieciowego. W tym celu należy się zalogować na koncie z uprawnieniami administracyjnymi i wybrać Panel sterowania | Połączenia sieciowe | Połączenie lokalne | Właściwości. Ustawienia interfejsu powinny obejmować następujące usługi: Klient sieci Microsoft, Udostępnianie plików i drukarek oraz Protokół internetowy TCP/IP. Udostępnianie plików i drukarek jest potrzebne, jeśli dana stacja robocza będzie oferowała swoje zasoby innym klientom sieci, czyli na przykład wtedy, gdy z lokalnej drukarki korzystają inni pracownicy firmy. Do współpracy z systemem Windows Server 2003 potrzebujemy protokołu i klienta sieci.

W naszej przykładowo konfigurowanej sieci do zarządzania adresami IP służy serwer DHCP, dlatego we właściwościach tego protokołu powinna być zaznaczona opcja Uzyskaj adres IP automatycznie. Automatycznie powinien być również pobierany adres serwera

DNS. Jeśli obie opcje są zaznaczone, ustawienia interfejsu sieciowego można uznać za poprawne.

Następnie do domeny należy dodać komputer. W tym celu możemy uruchomić Kreator identyfikacji sieciowej lub skorzystać z przycisku Zmień. Obie opcje odnajdziemy po wybraniu System panelu sterowania | Nazwa komputera. Wydajniejszym rozwiązaniem jest skorzystanie z przycisku Zmień, ale jeśli ktoś woli łatwiejsze sposoby konfiguracji, może się posłużyć kreatorem. Po naciśnięciu przycisku Zmień, w oknie Zmiana nazwy komputera przenosimy znacznik z opcji Grupa robocza na Domena i wprowadzamy nazwę domeny zgodną ze standardem DNS. W naszym przypadku będzie to PL.IDG.COM. Naciśnięcie przycisku OK sprawia, że stacja kontaktuje się z serwerem DNS w celu uzyskania listy adresów IP kontrolerów domeny. Po udanym odnalezieniu serwera Windows Server 2003 nasza stacja jest dodawana do domeny. Przed zakończeniem operacji trzeba jeszcze w oknie Zmiana nazwy komputera podać właściwy identyfikator i hasło użytkownika domeny.

O powodzeniu tej operacji informuje komunikat "Witamy w domenie pl.idg.com". Aby wszystkie ustawienia działały poprawnie, należy zrestartować Windows XP. Po ponownym uruchomieniu użytkownicy stacji roboczej będą się już logowali do domeny pl.igd.com.

Testowanie komunikacji i pracy w domenie

Konfiguracja Windows Server 2003 i stacji roboczych jest niezbyt skomplikowana, ale zdarzają się pewne problemy. Jeśli wystąpią błędy, trzeba umieć szybko zlokalizować miejsce awarii oraz usunąć ją. Zacznijmy od eliminacji tych problemów, które występują najczęściej, czyli błędów komunikacyjnych.

Jeśli zawiedzie komunikacja, przekonamy się o tym bardzo szybko. Nie będziemy się mogli podłączyć do serwera sieciowego, wydrukować dokumentu na drukarce sieciowej czy wysłać poczty. Ustalanie źródła błędu należy zacząć od sprawdzenia działania fizycznej części sieci. Najczęściej nie trzeba śledzić ciągłości kabla lub czołgać się pod biurkiem. Do wyciągnięcia kilku istotnych wniosków na temat sieci wystarczy zaznaczyć pole wyboru opcji Pokaż ikonę w obszarze powiadomień podczas połączenia, dostępnej we właściwościach interfejsów sieciowych zarówno Windows Server 2003, jak i stacji pracującej pod kontrolą XP. Po zaznaczeniu tej opcji w obszarze powiadomień pojawi się ikona sygnalizująca obecność lub przerwanie połączenia. Jej dwukrotne kliknięcie pozwala na uzyskanie informacji o właściwościach i aktywności połączenia. Jeśli zawiedzie okablowanie lub urządzenie aktywne, poinformuje nas o tym zmiana w wyglądzie ikony oraz odpowiedni komunikat.

Z reguły w celu usunięcia awarii wystarczy sprawdzić, czy nie wysunął się kabel z karty sieciowej lub czy działa koncentrator względnie przełącznik. Jeśli to nie wystarczy, trzeba sprawdzić, czy kabel nie jest uszkodzony.

Jeśli ikona informująca o stanie interfejsu nie sygnalizuje błędów, należy przejść do weryfikacji konfiguracji stacji lub serwera. Łatwo da się ustalić, czy mamy kłopoty z serwerem, czy z komputerem lokalnym. Jeżeli inne stacje również nie mogą się podłączyć do plików serwera, z dużym prawdopodobieństwem awaria dotknęła Windows Server 2003. W innym przypadku mamy problemy z Windows XP. Do testowania konfiguracji służy pokaźna grupa narzędzi, zarówno tekstowych, jak okienkowych. W podstawowej diagnostyce systemu wystarczy zastosowanie trzech narzędzi wiersza poleceń: IPCONFIG, PING oraz NSLOOKUP. Każde z nich może być wykorzystane do weryfikacji poprawności działania poszczególnych usług.

Wyszukiwanie błędów rozpoczynamy od polecenia, które może natychmiast zdiagnozować poprawność pracy. Jeśli zastosujemy ping, będziemy mogli od razu wyeliminować dużą część potencjalnych źródeł błędów. Gdy rezultatem polecenia z

parametrem w postaci nazwy Windows Server 2003 będzie odpowiedź systemu, wówczas wiemy, że poprawnie działa usługa DHCP oraz DNS. Jeżeli w odpowiedzi otrzymamy na przykład komunikat "Upłynął limit czasu żądania" lub "Żądanie polecenia Ping nie może odnaleźć hosta idgtest.pl.idg.com. Sprawdź nazwę i ponów próbę.", nasze dalsze czynności mogą iść w różnych kierunkach. Najczęściej źródłem kłopotów jest konfiguracja adresowania lub problemy z rozwiązywaniem nazw.

Polecenie IPCONFIG służy do sprawdzania lokalnych ustawień adresowania TCP/IP. Jest przydatne do określenia, czy kłopoty wynikają z nieprawidłowego działania sieci, czy serwera DHCP. Po wpisaniu w wierszu poleceń IPCONFIG /ALL otrzymamy informacje o bieżących ustawieniach adresowania. W czasie rozwiązywania problemów najcenniejszymi danymi zwróconymi przez IPCONFIG są: DHCP włączone, Adres IP oraz Serwery DNS. Ponieważ zdecydowaliśmy się na automatyczną dystrybucję adresów IP, parametr DHCP powinien wyświetlać Tak. Jeśli jest inaczej trzeba, przejść do właściwości protokołu TCP/IP interfejsu sieciowego i zmienić jego konfigurację. Pole Adres IP powinno zawierać adres z zakresu zdefiniowanego w Windows Server 2003. Gdy ten warunek nie jest spełniony, należy sprawdzić, czy działa DHCP, sieć lub czy nie pojawił się "obcy" serwer DHCP. Może tak być na przykład po włączeniu usługi udostępniania połączenia internetowego. Ostatnie wskazane pole - Serwery DNS - w naszym przypadku powinno zawierać adres IP Windows Server 2003. Jeśli wartość tego pola jest inna, powinniśmy sprawdzić konfigurację opcji serwera DHCP.

Do testowania funkcjonowania serwera DNS służy polecenie NSLOOKUP. Nam będzie potrzebne do sprawdzenia, czy możemy się połączyć z usługodawcą DNS i czy serwer ten zawiera rekordy potrzebne do prawidłowego funkcjonowania sieci. NSLOOKUP może działać w dwóch trybach: interaktywnym i wsadowym. Tryb interaktywny uzyskujemy po wprowadzeniu nazwy polecenia i naciśnięciu klawisza [Enter]. Powoduje to przejście do powłoki NSLOOKUP, w której możemy wydawać najróżniejsze polecenia. Lista poleceń jest dostępna po wpisaniu ? i naciśnięciu klawisza [Enter]. Tryb wsadowy polega na wpisaniu NSLOOLUP z odpowiednim parametrem i wystarcza do weryfikacji komunikacji z lokalnym serwerem DNS. Jeśli wpiszemy NSLOOKUP idgtest.pl.idg.com i otrzymamy odpowiedź, będzie to oznaczało poprawną pracę DNS. Podobnie możemy postąpić, sprawdzając, czy system jest w stanie odpowiedzieć na pytania o rekordy SRV.

Po wyeliminowaniu z grupy wadliwie działających konfiguracji protokołu TCP/IP, usługi DHCP i DNS, należy rozpocząć inne testy. Jeśli na podstawie komunikatów systemu ustalimy, że kłopot nie polega na błędnym skonfigurowaniu uprawnień, trzeba dokładnie przejrzeć dzienniki w poszukiwaniu innych źródeł problemów. Warto również pamiętać, że pomoc Windows Server 2003 zawiera serię przydatnych przewodników, wspomagających testowanie ustawień systemu.

IDG.PL
Konfiguracja wstępna
PC World Komputer

wersja do wydruku
|strona główna | wersja oryginalna|

Poprawnie zainstalowany system operacyjny to dopiero połowa sukcesu. Kolejny bardzo ważny etap to przygotowanie go do pełnienia roli serwera sieci. Pokazujemy, jak zwiększyć wydajność, poprawić bezpieczeństwo i przekształcić serwer w kontroler domeny.

Windows Server 2003 pozwala na uruchamianie wielu aplikacji w jednym czasie. Każdy z programów wymaga odpowiednich zasobów sprzętowych. Do zasobów tych zaliczamy również pamięć RAM. Po uruchomieniu aplikacji system przydziela jej odpowiednią ilość pamięci, jednocześnie dbając o to, żeby nie doszło do naruszenia przestrzeni adresowej zajętej przez inny program. Jednostką pamięci, którą posługuje się Windows, jest tzw. strona. Ma ona rozmiar 4 KB. Jeśli aplikacje wymagają więcej pamięci RAM, niż jest zainstalowane w komputerze, następuje stronicowanie: Menedżer pamięci przenosi na dysk część pamięci, żeby mogła zostać przydzielona tej aplikacji, która zgłosiła zapotrzebowanie. Plik zawierający te dane to pagefile.sys, domyślnie umieszczony w katalogu głównym pierwszej partycji, np. C:.

Dla wydajności systemu niebagatelne znaczenie ma zarówno położenie tego pliku, jak i jego rozmiar. Najlepszym rozwiązaniem jest przeniesienie pliku wymiany z partycji systemowej na inny dysk, choć ogranicza to możliwość wykonywania tzw. zrzutów pamięci podczas błędów zatrzymania (blue screen). Jeśli trzeba wykonywać zrzuty, należy utworzyć dwa pliki wymiany. Jeden, niewielkich rozmiarów, umieszczamy na partycji systemowej. Drugi, będący podstawowym plikiem wymiany, na innym dysku. Zalecany rozmiar pliku to 150 procent pamięci RAM. Gdy system ma np. 512 MB RAM-u, podczas instalacji będzie utworzony plik o rozmiarze początkowym 768 MB. Kolejnym zaleceniem jest założenie stałego pliku wymiany, czyli pliku o takim samym rozmiarze początkowym, jak końcowym, ponieważ podczas startu system stara się zaalokować ciągłą przestrzeń na plik, co zapobiega rozproszeniu danych na dysku.

Rozmiarem i położeniem pliku pagefile.sys zarządza się po otworzeniu obiektu System z Panelu sterowania. Na karcie Zaawansowane wybieramy związany z wydajnością przycisk Ustawienia. Na następnej karcie Zaawansowane klikamy przycisk Zmień. Okno Pamięć wirtualna pozwala na wybór dysku i rozmiaru pliku. Po wpisaniu zmian naciskamy przycisk Ustaw. Aby zmiany zostały wprowadzone w życie, trzeba zrestartować serwer.

Uwaga. Korzystając z dokumentacji dotyczącej Windows Server 2003, należy zwrócić uwagę na różnice w nazewnictwie partycji. Partycją systemową jest ta, z której Windows startuje (ta, na której znajdują się pliki ntldr, ntdetect.com itp), natomiast startową ta, na której są przechowywane pliki systemu operacyjnego (najczęściej katalog o nazwie Windows).

Konfiguracja środowiska startowego

Ważnym elementem przygotowania systemu do pracy jest konfiguracja środowiska startowego: ustawienia związane z uruchamianiem serwera oraz z jego działaniem w wypadku awarii.

Jeśli Windows Server 2003 nie jest jedynym systemem zainstalowanym na naszym komputerze, podczas uruchamiania stacji musimy wybrać, który system chcemy uruchomić. Zwykle po 30 sekundach ładowany jest domyślny system operacyjny. Konfiguracja Windows związana z wystąpieniem błędów zatrzymania obejmuje takie parametry, jak wysyłanie alertów administracyjnych, miejsce i rozmiar zrzutu pamięci. Jeśli serwer "padnie", informacja o tym zdarzeniu będzie umieszczona w Podglądzie zdarzeń. Dodatkowo zostanie wysłany komunikat ostrzegawczy i w pliku memory.dmp zostanie zapisana pełna zawartość pamięci systemu. Ustawienia startowe i awaryjne możemy w prosty sposób zmodyfikować.

W celu zmiany bieżących parametrów Windows Server 2003 należy we właściwościach obiektu System w Panelu sterowania kliknąć kartę Zaawansowane i nacisnąć przycisk Ustawienia, związany z opcją Uruchamianie i odzyskiwanie. Tam też znajdują się przełączniki konfigurujące opisywane wcześniej parametry. Jeżeli nie chcemy, aby po wystąpieniu błędu zatrzymania Windows zapisywał pełną informację o debugowaniu, należy wybrać opcję Zrzut pamięci jądra lub całkowicie wyłączyć zapisywanie. Na karcie

Zaawansowane znajduje się również przycisk Raportowanie błędów. Gdy w dowolnej z aplikacji wystąpi błąd, pojawi się okno z pytaniem, czy przesłać raport do Microsoftu. Jeśli system nie jest podłączony do Internetu lub nie chcemy wysyłać żadnych informacji, należy wyłączyć raportowanie o błędach.

Konfiguracja partycji i dysków

Podczas tekstowego etapu instalacji systemu założyliśmy partycję przeznaczoną do Windows Server 2003, teraz przyszła pora na przygotowanie pozostałych partycji lub dysków do pracy. Ponieważ serwer pełni istotną funkcję w strukturze sieci, jednym z najważniejszych zadań jest należyte zabezpieczenie systemu przed awarią. Oprócz przestrzegania bezwzględnego wymogu częstego wykonywania kopii zapasowych trzeba zadbać o ochronę danych na wypadek uszkodzenia dysków.

Jednym ze sposobów zabezpieczenia systemu przed uszkodzeniami są macierze dysków. Ich działanie opiera się na nadmiarowości zapisu. Oznacza to, że dane, w zależności od wersji macierzy, są zapisywane na dwóch lub więcej dyskach. Najprostsza macierz to odbicie lustrzane tzw. RAID 1. Rozwiązanie to stosuje dwa dyski, a zapis odbywa się równolegle na każdy z nich. W wypadku uszkodzenia jednego dysku przed utratą danych ochrania nas jeszcze drugi. Innym często stosowanym zabezpieczeniem jest RAID 5. W tym wypadku wykorzystywane są co najmniej trzy dyski, a każdy z nich, oprócz danych, wylicza i zapisuje informacje o parzystości. Jeśli jeden z dysków ulegnie awarii, Windows kontynuuje pracę, odtwarzając potrzebne dane z parzystości pozostałych dysków. Zmniejsza się wydajność systemu, ale to, co najcenniejsze, jest bezpieczne. W Windows Server 2003 możemy stosować macierze zarówno sprzętowe, jak i programowe. Pierwsze wymagają zakupu kontrolera RAID, działanie drugich opiera się na odpowiedniej konfiguracji systemu. Ze względu na wydajność zalecane są rozwiązania sprzętowe, jednak z powodów ekonomicznych wiele firm decyduje się na skonfigurowanie programowej odporności na uszkodzenia.

Do konfiguracji dysków i partycji służy przystawka Zarządzanie dyskami, dostępna oddzielnie, po załadowaniu konsoli mmc, albo w przystawce Zarządzanie komputerem. Najprościej ją uruchomić, wpisując w wierszu polecenia (menu Start | Uruchom) diskmgmt.msc. Chcąc założyć nową partycję, należy kliknąć prawym przyciskiem myszy obszar dysku oznaczony etykietą "Nieprzydzielone", z menu podręcznego wybrać opcję Nowa partycja, a następnie zdecydować, czy założyć partycję podstawową, rozszerzoną, czy dysk logiczny. W czasie konfiguracji można określić dodatkowe parametry partycji, takie jak oznaczenie literowe, system plików czy rozmiar jednostki alokacji. Biorąc pod uwagę wydajność oraz bezpieczeństwo, podczas formatowania powinniśmy wybierać system NTFS.

Jeżeli naszym celem jest skonfigurowanie jednej z metod odporności na uszkodzenia, wówczas pierwszym zadaniem będzie konwersja dysków na dyski dynamiczne. Jest to konieczne, ponieważ Windows pozwala na utworzenie RAID 1 lub 5 tylko wówczas, gdy używamy dysków dynamicznych. W celu przeprowadzenia konwersji klikamy prawym przyciskiem myszy etykietę dysku (np. "Dysk 0") i z menu podręcznego wybieramy opcję Konwertuj na dysk dynamiczny. Jeśli modyfikujemy ustawienia dysku, na którym znajduje się system, konieczne jest ponowne uruchomienie serwera. Dalsze postępowanie zależy od rodzaju konfigurowanej odporności na uszkodzenia. Zakładając dublowanie, należy kliknąć prawym przyciskiem myszy partycję, którą chcemy "mirrorować", i wybrać opcję Dodaj dublowanie. Jeżeli naszym celem jest konfiguracja RAID 5, to zaznaczamy nieprzydzieloną przestrzeń na jednym z dysków i wybieramy opcję Nowy wolumin. W kreatorze zakładania woluminu wskazujemy RAID 5. Do utworzenia tej formy ochrony przed awarią musimy mieć co najmniej trzy dyski z nieprzydzieloną przestrzenią o mniej więcej tym samym rozmiarze. W tym wypadku do przechowywania danych wykorzystane będzie 2/3 pojemności, a 1/3 zostanie przeznaczona na informację o parzystości.

Role i zarządzanie serwerem

Doświadczeni użytkownicy serwerowych systemów firmy Microsoft, po zakończeniu instalacji dodają i konfigurują tylko usługi niezbędne. Jeśli nie mamy dużego doświadczenia, możemy skorzystać z któregoś kreatora konfiguracji.

Bezpośrednio po zainstalowaniu systemu wyświetlane jest okno Zarządzanie tym serwerem. Będzie ono pomocne w przygotowaniu systemu do wypełniania określonych zadań. Klikając odnośnik Dodaj lub usuń rolę, możemy wybrać jedną z licznych funkcji, które chcemy przypisać komputerowi. Jeśli klikając Dalej, wybierzemy konfigurację niestandardową, wyświetlana jest lista ról serwera, m.in.: serwer plików, serwer wydruku, serwer poczty czy kontroler domeny. Zaznaczenie jednej z funkcji i kliknięcie Dalej uruchamia kreator związany z ustawieniami danej roli. Na przykład kreator serwera plików pozwala na ustawienia związane z przydziałami dysków, usługą indeksowania, udostępnieniami, plikami offline oraz uprawnieniami do udostępnień. Po skonfigurowaniu określonej roli możemy dodatkowo wykorzystać podpowiedzi opisujące kolejne zadania, żeby zwiększyć funkcjonalność serwera lub właściwie zabezpieczyć dane.

Po zainstalowaniu jednej lub kilku ról okno Zarządzanie tym serwerem zawiera listę wybranych funkcji wraz z odnośnikami do narzędzi pozwalających na konfigurację systemu. Jeśli wybraliśmy na przykład rolę serwera plików, kliknięcie odnośnika Zarządzaj tym serwerem plików przeniesie nas do przystawki z listą udostępnień, sesji, otwartych plików oraz narzędziami do defragmentacji i zarządzania dyskami.

Jeśli chcemy, aby na serwerze zainstalowana była usługa Active Directory, powinniśmy rozpocząć konfigurację ról od opcji Konfiguracja standardowa dla pierwszego serwera lub od wyboru roli Kontroler domeny. Nie ma sensu definiowania parametrów serwera plików lub serwera wydruku, ponieważ po instalacji Active Directory będziemy mieli do czynienia z innymi kontami grup i użytkowników. Więcej informacji o domenach oraz instalacji Active Directory przedstawimy w dalszej części artykułu. Okno Zarządzaj tym serwerem jedynie ułatwia wstępną konfigurację systemu. Wszystkie parametry Windows Server 2003 można określić za pomocą odpowiednich przystawek umieszczonych w module Narzędzia administracyjne.

Domeny i grupy robocze

Podczas instalacji Windows Server 2003 instalator pytał, czy chcemy, żeby system pracował w środowisku domeny, czy grupy roboczej. Było to związane z przyłączeniem się do jednego z już funkcjonujących środowisk. Po zakończeniu instalacji możemy utworzyć własną domenę Active Directory lub kontynuować pracę w grupie roboczej. Zanim podejmiemy właściwą decyzję, należy poznać różnice oraz wady i zalety obu wymienionych środowisk.

Grupy robocze są prostym zbiorem systemów komputerowych korzystających nawzajem ze swoich zasobów. Współdzielą tę samą nazwę i są umieszczone w tym samym pojemniku modułu Moje miejsca sieciowe. Ich najważniejszą cechą jest brak centralnej administracji. Konta użytkowników są zakładane na każdym z komputerów należących do grupy roboczej i dlatego zarządzanie nimi jest mocno utrudnione. Problemy związane z administracją takim środowiskiem są główną przyczyną ograniczania grup roboczych do sieci liczących maksymalnie 10 stacji.

Domeny charakteryzuje całkowicie odmienne podejście do zarządzania siecią. Ich administracja jest uproszczona przez umieszczenie w jednej bazie informacji o kontach użytkowników, zabezpieczeniach i zasobach sieci. Za jej obsługę i udostępnianie odpowiada usługa Active Directory. Chcąc założyć domenę, należy na jednym z serwerów Windows Server 2003 lub Windows 2000 zainstalować Active Directory. Od tej pory

komputer ten będzie nazywany kontrolerem domeny. Baza zasobów może być replikowana na dodatkowe serwery, dzięki czemu awaria jednego z komputerów nie prowadzi do paraliżu sieci.

Centralne zarządzanie nie jest jedyną zaletą środowiska domenowego. Użytkownicy są uwierzytelniani przez kontrolery domeny, więc nie trzeba tworzyć wielu kont dla tego samego klienta sieci. Korzystanie z wszystkich zasobów wymaga jednego logowania, przy czym nie ma znaczenia liczba komputerów w sieci. Jeśli serwer będzie wystarczająco mocny, może obsłużyć uwierzytelnienie kilkuset stacji. Naturalnie ze względów bezpieczeństwa zaleca się instalację co najmniej dwóch kontrolerów domeny. Ponieważ w przypadku domen nie ma ograniczeń związanych z liczbą przechowywanych kont, znajdują one zastosowanie zarówno w małych biurach, jak i dużych firmach. Firma może mieć jedną domenę, która będzie obejmować rozległy obszar geograficzny, np. centralę i filie rozproszone po całej Polsce.

Instalacja domeny

Zalety domen sprawiają, że usługa Active Directory jest instalowana w większości sieci opartych na Windows 2000 i 2003. Instalację domeny możemy rozpocząć na wiele sposobów. Najprostszy to wybranie opcji Konfiguracja standardowa dla pierwszego serwera w oknie Zarządzanie tym serwerem. Kreator zadaje kilka pytań, a następnie instaluje usługi Active Directory, DNS i DHCP. Dla administratorów z niewielkim doświadczeniem to najprostsza i najszybsza metoda. Jeśli jednak zależy nam na określeniu szczegółowych parametrów instalowanej usługi, powinniśmy skorzystać z roli Kontroler domeny, dostępnej w Niestandardowej konfiguracji opcji Zarządzanie tym komputerem. Innym sposobem uruchomienia instalatora domeny w Windows Server 2003 jest wprowadzenie polecenia dcpromo.exe po kliknięciu menu Start | Uruchom.

Instalacja roli kontrolera domeny uruchamia kreator dodawania usługi Active Directory. Po uruchomieniu kreatora najpierw należy odpowiedzieć na pytanie o typ kontrolera domeny. W każdej domenie powinny być co najmniej dwa serwery przechowujące bazę Active Directory, dla pierwszego z nich zaznaczamy opcję Kontroler domeny dla nowej domeny, natomiast dla drugiego opcję Dodatkowy kontroler domeny dla istniejącej domeny. Instalując serwer zapasowy, powinniśmy najpierw sprawdzić, czy mamy wystarczające uprawnienia do zakładania dodatkowych kontrolerów. Operacje związane z konfiguracją usługi Active Directory zawsze wymagają uprawnień administratora domeny. Następne okno służy do określenia typu tworzonej domeny. Serwery Windows Server 2003 mogą budować środowiska domenowe na olbrzymią skalę. Potrafią łączyć zasoby przedsiębiorstw o zasięgu globalnym, które mają filie rozproszone na wielu kontynentach. Podstawową jednostką administracji jest domena, natomiast dla wspomnianych firm można tworzyć drzewa lub lasy domen. Drzewo Active Directory to grupa domen powiązanych relacją zaufania oraz współdzielących tę samą przestrzeń nazw. Graficznie przypomina to odwrócone drzewo, które ma domenę nadrzędną (tzw. korzeń) i wychodzące z niej domeny podrzędne (patrz ilustracja).

Las liczy wiele drzew. Elementem wyróżniającym lasy jest brak wspólnej przestrzeni nazw, dlatego służą do grupowania zasobów korporacji, w których skład wchodzi wiele firm. Podczas instalacji pierwszego kontrolera domeny należy wybrać opcję Domena w nowym lesie.

Kolejne pytanie kreatora wiąże się z usługą DNS. Ponieważ Active Directory korzysta z tej usługi do rozwiązywania nazw oraz lokalizacji kontrolerów domeny, należy zainstalować lokalny serwer DNS. Jeśli nie wiemy, jak go skonfigurować do współpracy z Active Directory, warto wybrać opcję Nie, zainstaluj i skonfiguruj DNS na tym komputerze. Kreator automatycznie przeprowadzi wówczas integrację systemu z DNS.

W oknie Nazwa nowej domeny wprowadzamy nazwę zakładanej struktury, zgodną ze standardem DNS. Nie musimy się posługiwać zarejestrowaną nazwą internetową - może być dowolna, np. IDG.localAD. Wybór właściwej nazwy ma istotne znaczenie, dlatego zanim ją wprowadzimy, należy zapoznać się z odpowiednimi akapitami pomocy do systemu Windows Server 2003. W następnym oknie podajemy nazwę netbiosową domeny. Jest to konieczne ze względu na wykorzystywanie mechanizmów NetBIOS do realizacji niektórych połączeń sieciowych. Nazwa powinna mieć maksymalnie 15 znaków i wiązać się z wprowadzaną przez nas nazwą DNS. Jeśli nazwiemy domenę IDG.localAD, to dobrą nazwą NetBIOS będzie IDG.

Kolejne okna monitują o określenie lokalizacji plików i katalogów przechowujących Active Directory. Najczęściej nie ma istotnej potrzeby zmiany tych ustawień. W przedostatnim oknie wybieramy poziom zgodności uprawnień. Jeśli do domeny będą się podłączać klienci starszych systemów operacyjnych, powinniśmy wybrać opcję zgodności ze starszymi systemami. Niesie to ze sobą ryzyko odczytywania pewnych informacji o domenie przez użytkowników anonimowych. Należy jednak pamiętać, że po ustawieniu restrykcyjnych uprawnień w niektórych przypadkach starsi klienci będą mieli problemy z podłączeniem się do domeny. Na koniec należy podać hasło do trybu przywracania Active Directory. Jest ono wykorzystywane do uruchomienia systemu podczas awarii usługi katalogowej. Parametr ten kończy instalację domeny i możemy zrestartować system. Po powtórnym uruchomieniu serwer jest w pełni funkcjonalnym kontrolerem domeny. Dodatkowo w narzędziach administracyjnych pojawiają się skróty do przystawek związanych z Active Directory.

Aktywacja produktu

Jeśli z sukcesem zakończyliśmy przygotowanie systemu do pracy, jedną z ostatnich czynności będzie aktywacja serwera. W serwerze zastosowano ten sposób zabezpieczenia przed nielegalnym użytkowaniem, co w Windows XP lub produktach z rodziny Office. Sam proces aktywacji nie jest zbyt uciążliwy i nie wymaga dużo czasu. Jeśli w firmie dużo oprogramowania wymaga aktywacji, należy się zastanowić się nad wykorzystaniem proponowanych przez Microsoft programów licencji grupowej. Licencjonowanie to nie wymaga aktywacji na przykład w wypadku reinstalowania systemu po awarii dysku.

Windows Server 2003 można aktywować na dwa sposoby. Pierwszy wymaga połączenia z Internetem, jest automatyczny i trwa kilka sekund. Jeśli Internet nie jest dostępny, należy zadzwonić do regionalnego centrum aktywacji. Po podaniu przedstawicielowi centrum wygenerowanego przez Windows Server 2003 identyfikatora otrzymujemy ciąg znaków, który wprowadzamy do wyświetlonego okna. W tym momencie aktywacja jest zakończona.

Aktualizacja Windows

Konfiguracja Windows nie kończy się wraz z zainstalowaniem Active Directory oraz przeprowadzeniem drobnych modyfikacji systemu. Serwer to komputer szczególnie narażony na niebezpieczeństwo i dlatego należy zadbać o instalację wszystkich niezbędnych poprawek. Jeśli firma jest nieduża i serwer ma połączenie z Internetem, najwygodniej w tym celu posłużyć się usługą automatycznej aktualizacji Windows. Pozwala ona na automatyczne lokalizowanie oraz instalację poprawek systemowych, łatek, a także uaktualnień sterowników. Windows Server 2003 co określony czas łączy się z serwerami internetowymi i kontroluje, czy jego bieżąca konfiguracja nie wymaga doinstalowania poprawek.

Najbardziej zawodnym "elementem" zabezpieczania systemu jest administrator sieci, który najczęściej przez nieuwagę lub brak czasu zaniedbuje szybką instalację uaktualnień, dlatego aktualizacja automatyczna niewątpliwie ułatwia zarządzanie

bezpieczeństwem. O pojawieniu się nowych łatek Windows Server 2003 poinformuje nas samoistnie.

Aby uruchomić automatyczne aktualizowanie Windows, należy we właściwościach obiektu Mój komputer na karcie Aktualizacje automatyczne zaznaczyć opcję Aktualizuj mój komputer. Jeśli to ustawienie zostanie wyłączone... itd. Z dostępnych ustawień, dodatkowo możemy wybrać powiadamianie użytkownika przed pobraniem aktualizacji, powiadamianie użytkownika przed zainstalowaniem poprawek lub wykorzystanie do uaktualnień zdefiniowanego harmonogramu.

Instalacja poprawek nie musi być wykonywana automatycznie. Jeśli wolimy sami wpływać na to, które z uaktualnień instalować, oraz ręcznie sprawdzać obecność aktualizacji, należy się posłużyć skrótem do internetowej witryny Windows Update. Odnajdziemy go z łatwością w menu Programy. Na poświęconych bezpieczeństwu stronach Microsoftu (http://www.microsoft.com/security) można się zapoznać z najnowszymi informacjami o zagrożeniach oraz zaprenumerować biuletyn informujący o nowych poprawkach.

IDG.PL
Administracja od podstaw
PC World Komputer

Instalacja Windows Server 2003 nie nastręcza użytkownikom większych trudności. Przygotowanie systemu do funkcji serwera plików lub serwera wydruku również nie jest wyjątkowo skomplikowane. Kilkanaście minut klikania sprawi, że Windows Server 2003 będzie można przekazać w użytkowanie klientom sieci.

Wraz z rozwojem technologii informatycznych zmieniają się wymagania wobec sieci komputerowych. Jeszcze nie tak dawno sieć oferowała przede wszystkim dostęp do zasobów przechowywanych na wielu stacjach oraz współdzielenie aplikacji. Obecnie w wielu firmach służy dodatkowo do udostępnienia połączenia z Internetem, a także do informacji potrzebnych partnerom handlowym. W tym artykule zajmiemy się konfiguracją serwera umożliwiającą bezpieczny i wygodny dostęp do zasobów. Dowiemy się także, jak przygotować system do funkcji serwera plików oraz serwera wydruku.

Funkcje serwera

W celu ułatwienia wykonywania czynności administracyjnych programiści Microsoftu opracowali specjalny panel do wstępnej konfiguracji Windows Server 2003. Po każdorazowym logowaniu do konsoli wyświetlane jest okno - Zarządzanie tym serwerem. Służy ono do szybkiego określania, jakie usługi ma świadczyć komputer. Ponieważ umieszczono w nim sporo skrótów do narzędzi potrzebnych administratorowi, można je potraktować jako główną konsolę do sterowania systemem. Jeśli zdecydujemy się na skorzystanie z okna Zarządzania tym serwerem, uruchomiona będzie grupa kreatorów łagodnie wprowadzająca w niezbędne ustawienia komputera. Mniej doświadczeni administratorzy, będą mogli po kolei ustawić te funkcje systemu, które mają fundamentalne znaczenie dla konfigurowanych systemów. Należy jednak zaznaczyć, że niektóre czynności administracyjne wykonywane przez kreatory są mocno uproszczone. W celu porównania poznamy zarówno prostszy, jak i drobiazgowy sposób określania ustawień Windows Server 2003.

Jeśli okno Zarządzanie tym serwerem nie spełnia naszych oczekiwań, możemy łatwo wyeliminować jego wyświetlanie przez zaznaczenie opcji: Nie wyświetlaj tej strony przy logowaniu. Nie oznacza to, że nie możemy do niego wrócić. W celu powtórnego uruchomienia okna należy wejść w narzędzia administracyjne i kliknąć odpowiedni skrót.

Zanim przejdziemy do dodawania roli serwera plików, musimy wykonać szereg czynności wstępnych. Rozpoczynamy od przygotowania podsystemu dysków oraz od założenia odpowiednich kont dla pracujących w sieci użytkowników.

Konfiguracja dysków

Jeśli Windows Server 2003 ma pełnić funkcję serwera plików, kluczowym zadaniem jest właściwe przygotowanie dysków. Komputer powinien być należycie zabezpieczony przed awarią aparatu przechowywania, a partycje trzeba skonfigurować tak, żeby nie zabrakło na nich miejsca. Windows Server 2003 obsługuje programowe funkcje ochrony przed awarią dysków, jednakże zalecane jest korzystanie z rozwiązań sprzętowych. Najczęściej w celu zapobieżenia uszkodzeniom stosuje się macierze RAID-5, ale ze względów ekonomicznych, w wypadku niewielkich serwerów plików, z powodzeniem można zastosować dublowanie danych, czyli popularny "mirroring". Płyty główne z wbudowanym kontrolerem RAID są bardzo popularne oraz coraz tańsze.

Przydziały dyskowe przypisują użytkownikom serwera limity przestrzeni dyskowej. Dzięki temu możemy spokojnie zakładać np. foldery domowe dla klientów bez obawy, że dysk się "zatka". Konfiguracja ograniczeń związanych z zapisywaniem danych jest wykonywana na poszczególnych partycjach systemu. Trzeba pamiętać, że przydziały dyskowe wymagają systemu plików NTFS i jeśli korzystamy z FAT lub FAT32, musimy wykonać konwersję systemu. W tym celu należy w wierszu poleceń wprowadzić polecenie CONVERT z parametrem wskazującym partycję, którą chcemy poddać konwersji, np. Convert D: /fs:ntfs. Jeśli systemem plików jest NTFS, możemy przejść do konfiguracji przydziałów dyskowych. W tym celu należy otworzyć Eksplorator Windows, zaznaczyć partycję, na którą chcemy nakładać ograniczenie, i z menu Plik wybrać jej właściwości. Następnie przechodzimy do karty Przydział. Domyślnie przydziały dysków nie są włączone i jeśli chcemy uruchomić tę usługę, należy zaznaczyć opcję Włącz zarządzanie przydziałami. Warto zaznaczyć, że samo włączenie zarządzania nie powoduje ograniczania przestrzeni. Służy ono jedynie do monitorowania działalności użytkowników. Dopiero zaznaczenie drugiej opcji, Odmów miejsca na dysku użytkownikom przekraczającym limit przydziału, sprawia, że klienty Windows Server 2003 nie mogą zapisywać więcej, niż mają dozwolone. Bezpośrednio we właściwościach przydziałów określamy limity przestrzeni dyskowej dla nowych użytkowników. Dotyczą one miejsca na dysku oraz poziomu ostrzeżeń. Dodatkowo, administrator może zaznaczyć opcje związane z rejestrowaniem w dzienniku systemu zdarzeń o przekroczeniach limitów. Przycisk Wpisy przydziałów służy do monitorowania oraz konfigurowania ograniczeń dla indywidualnych użytkowników. Jeśli przekroczony zostanie poziom ostrzeżeń dla dowolnego z kont, w oknie wpisów pojawi się odpowiedni komunikat.

Konta użytkowników

Wszystkie sieciowe systemy operacyjne w celu identyfikowania poszczególnych klientów posługują się kontami użytkowników. Windows Server 2003 nie jest tutaj wyjątkiem. Stosowanie kont oferuje wiele istotnych mechanizmów związanych z zabezpieczeniami lub zwiększeniem funkcjonalności systemu. Założenie konta każdemu użytkownikowi sieci pozwala, między innymi, na określenie uprawnień do zasobów czy ograniczenie miejsca zajmowanego przez jego dane na dysku. Do każdego konta system przypisuje unikatowy identyfikator, tzw. SID, wykorzystywany do ustalania praw do wykonywania zadań w systemie, takich jak zmiana czasu systemowego lub możliwości zarządzania, odczytu czy też zapisu informacji gromadzonych przez system plików, rejestr, Active Directory itd.

Użytkownicy, którzy chcą korzystać z zasobów sieci, muszą zostać uwierzytelnieni. W tym celu należy podać nazwę konta oraz wprowadzić związane z nim hasło. Podanie błędnej nazwy lub hasła wiąże się z brakiem dostępu do sieci. O ile w przypadku takich systemów, jak Windows 95 czy 98, dostęp do zasobów innych komputerów mógł być określany wyłącznie przez hasło, o tyle w Windows XP czy Server 2003 niezbędne jest posługiwanie się kontem. Niekiedy czynność ta odbywa się automatycznie i nie jest widoczna dla użytkownika. Tak się zdarza na przykład w wypadku dostępu do zasobów systemów, w których jest włączone konto Gość (proste udostępnianie plików Windows XP).

Konta mogą gromadzić i udostępniać informacje adresowe, organizacyjne i kontaktowe o klientach sieci. Dzięki kontom możemy również konfigurować takie właściwości użytkownika, jak uprawnienia do zdalnych połączeń z serwerem przedsiębiorstwa, godziny logowania lub dostęp do sieci z określonych stacji. Po zainstalowaniu domeny za przechowywanie kont odpowiada baza usługi Active Directory.

Jak tworzyć konta użytkowników?

Utworzenie konta użytkownika jest wyjątkowo proste. Wystarczy podać kilka niezbędnych informacji, takich jak nazwa konta lub początkowe hasło. Konto zostanie utworzone i użytkownik będzie mógł się zalogować do sieci. Zanim jednak przejdziemy do tego etapu, należy określić, jakie założenia muszą spełniać konta. Trzeba opracować zasady tworzenia nazw kont, haseł oraz lokalizacji użytkowników w odpowiednich jednostkach organizacyjnych. Wyznaczenie tych prostych strategii przed rozpoczęciem tworzenia obiektów pozwala uniknąć niespójności i bałaganu.

Klienci sieci posługują się nazwą konta w czasie logowania. Windows Server 2003 wyróżnia dwie nazwy kont. Zwykła (standardowa) zawiera nazwę konta użytkownika, "małpkę" oraz przyrostek będący DNS-ową nazwą domeny, np. użytkownik o nazwie JNowak założony w domenie idg.pl będzie posługiwał się nazwą JNowak@idg.pl. Ten rodzaj zapisu nazywamy główną nazwą użytkownika lub UPN (User Principal Name). Jak widać, składnia nazwy jest taka sama, jak stosowana w adresach poczty elektronicznej. Dzięki temu łatwo daje się zintegrować nazwę konta użytkownika z nazwą konta pocztowego. W takim wypadku klienci sieci nie będą musieli zapamiętywać różnych nazw i różnych haseł do każdego z systemów. Po zintegrowaniu kont trzeba koniecznie zadbać o bezpieczne przekazywanie haseł do serwerów pocztowych, gdyż zwykle uwierzytelnienie przebiega "czystym tekstem" i łatwo je "podsłuchać". Druga nazwa konta jest utrzymywana w celu zachowania zgodności ze starszymi systemami operacyjnymi, takimi jak Windows 95, 98 czy NT. Systemy te nie potrafią poprawnie zinterpretować wpisów typu JNowak@idg.pl i dlatego należy stosować oddzielne wprowadzanie nazwy użytkownika oraz domeny, do której chcemy się zalogować. Starsze systemy nie obsługują nazw przekraczających 20 znaków. Podczas tworzenia konta powinniśmy unikać zakładania odmiennych nazw, gdyż logując się do sieci z różnych systemów, użytkownik będzie musiał wprowadzać inne nazwy.

Konwencja nazewnicza przyjęta w czasie zakładania nowych kont powinna być przejrzysta i spełniać wymagania firmy. Należy określić standardy postępowania oraz sposoby reagowania na tzw. szczególne przypadki. Standardy obejmują budowę konta, liczbę części składowych i na przykład zakaz używania polskich znaków. Raczej wyjątkowo do firmy trafią użytkownicy o takich samych imionach i nazwiskach, praktykanci, pracownicy tymczasowi, goście itp. Najczęściej stosowana konwencja to tworzenie nazwy konta z pierwszej litery imienia i całego nazwiska, np. kpuchatek. Ma to wiele zalet, na przykład łatwość połączenia z nazwami kont pocztowych, małe prawdopodobieństwo przekroczenia limitu starszych systemów, czyli maksymalnie 20 znaków w nazwie.

Inne konwencje, np. imię plus nazwisko, już nie są tak elastyczne. Dodatkowo zbyt długie nazwy są męczące dla użytkowników. Sławny Grzegorz Brzęczyszczykiewicz miałby konto łamiące limit 20 znaków, o nazwie np. Grzegorz_Brzeczyszczykiewicz@idg.com.pl. Zakładając konta dla pracowników tymczasowych lub praktykantów, warto rozważyć zastosowanie przedrostków wyróżniających wymienione grupy. Podane przykłady nie wyczerpują wszystkich możliwości nazewnictwa kont. Każda z firm może opracować własną, odpowiadającą jej strategię.

Przed utworzeniem identyfikatorów sieciowych warto przemyśleć również strategię nadawania i utrzymywania haseł. W tym przypadku duże znaczenie ma specyfika działania firmy. Inną politykę bezpieczeństwa będą stosowały banki czy organizacje rządowe, a inną małe biura z kilkoma lub kilkunastoma pracownikami. Ponieważ podczas zakładania konta należy przypisać hasło początkowe, powinniśmy rozważyć, czy hasłami zarządzają właściciele kont, czy za generowanie i przypisywanie haseł odpowiada administrator. W niewielkich firmach wystarczą domyślne ustawienia Windows Server 2003, polegające na tym, że system wymusza stosowanie haseł spełniających wymagania co do złożoności. Określają one, że hasło musi mieć co najmniej sześć znaków. Dodatkowo musi zawierać znaki należące do trzech z czterech proponowanych kategorii: wielkie litery, małe litery, cyfry oraz znaki niealfanumeryczne, np. !, #, %, ^ itp. Warto pamiętać, że Windows Server 2003 pozwala również między innymi na kontrolowanie okresu ważności hasła (np. minimum 1 dzień, maksimum 60 dni) oraz ograniczenie powtarzalności haseł (np. pięć pamiętanych haseł).

Jednostki organizacyjne

Wykorzystywana do przechowywania informacji o zasobach sieci usługa Active Directory pozwala na wielopoziomową budowę hierarchii domeny Windows Server 2003. Oznacza to, że możemy zakładać wiele obiektów spełniających funkcję pojemnika do przechowywania innych obiektów, tak jak foldery służą do gromadzenia plików. Funkcję pojemników w Active Directory wypełniają jednostki organizacyjne. Oprócz logicznego porządkowania obiektów, mają one jeszcze jedną, bardzo istotną zaletę. Możemy przypisać im zespół ustawień modyfikujących parametry pracy obiektów umieszczonych w tych jednostkach. Ustawienia te noszą nazwę zasad grupy. Ponieważ konfiguracja zasad grupy jest bardzo szerokim zagadnieniem, zostanie omówiona w oddzielnym artykule.

Możliwość implementacji zasad grupy zmusza administratorów do należytego przemyślenia schematu jednostek organizacyjnych. Jeśli będzie dobry, w znacznym stopniu ułatwi zarządzanie. Planując rozmieszczenie jednostek, najczęściej, choć nie zawsze, posługujemy się modelem geograficznym firmy. Oznacza to, że na najwyższym poziomie struktury znajdują się jednostki obrazujące poszczególne filie firmy. Dla przykładu, jeśli przedsiębiorstwo ma trzy oddziały: Kraków, Łódź i Gdańsk, głównymi jednostkami organizacyjnymi powinny być właśnie te trzy obiekty. W nich należałoby umieścić konta użytkowników, grup i komputerów. Należy pamiętać, że jest to tylko proponowane rozwiązanie i w wypadku niektórych firm lepszy byłby inny układ jednostek. Jeśli zakładamy domenę Windows Server 2003 w niewielkiej firmie, mającej jedną siedzibę i kilkunastu pracowników, stosowanie jednostek organizacyjnych nie jest chyba uzasadnione.

Narzędzie do zarządzania kontami użytkowników

Po zainstalowaniu Active Directory zespół narzędzi administracyjnych rozszerzany jest o grupę przystawek do zarządzania tą usługą, w tym o narzędzie Użytkownicy i komputery usługi Active Directory. Służy ono do tworzenia, zarządzania i usuwania obiektów typu użytkownik, komputer, grupa itd. Zanim przejdziemy do zakładania nowych kont, powinniśmy przyjrzeć się interfejsowi przystawki.

Charakterystyka większości narzędzi wykorzystywanych do konfiguracji systemu Windows Server 2003 jest podobna. Dzięki temu poznanie sposobu zarządzania systemem nie nastręcza trudności i po kilku chwilach większość użytkowników dobrze sobie radzi z wykonywaniem podstawowych czynności. Okno narzędzia Użytkownicy i komputery usługi Active Directory jest podzielone na dwa panele. Panel lewy przedstawia widok folderów. W przypadku Active Directory są nimi domena oraz obiekty typu jednostka organizacyjna. W prawym panelu są wyświetlane te obiekty, które znajdują się w zaznaczonym pojemniku lewego panelu. Poruszanie się po przystawce do złudzenia przypomina nawigację po Eksploratorze Windows.

Do modyfikacji ustawień służą polecenia paska menu, menu kontekstowego lub właściwości każdego z obiektów. Na przykład jeśli chcemy dodać nowego użytkownika, należy najpierw zaznaczyć folder, w którym zamierzamy umieścić konto np. Users, a następnie z menu Akcja wybrać Nowy | Użytkownik. Tę samą czynność możemy wykonać, klikając prawym przyciskiem myszy folder Users i wskazując Nowy | Użytkownik. Podobnie jak w Eksploratorze, pasek menu zawiera polecenia Plik, Widok, Okno i Pomoc. Na szczególną uwagę zasługują dwie opcje dostępne w menu Widok: Użytkownicy, grupy i komputery jako kontenery i Opcje zaawansowane. Pierwsza wyświetla dodatkowe obiekty, które mogą być ukryte np. pod obiektem typu komputer. Druga opcja odkrywa foldery systemowe, np. System lub LostAndFound. Dodatkowo we właściwościach obiektów wyświetlane są niewidoczne dotąd karty, np. Zabezpieczenia.

Zakładanie konta użytkownika

Zakładanie kont dla nowych użytkowników sieci nie jest skomplikowane. Najpierw należy wskazać macierzystą jednostkę organizacyjną, a potem z menu Akcja wybrać polecenie Nowy | Użytkownik. Windows uruchomi prosty kreator, w którym wpisujemy kilka niezbędnych informacji.

W pierwszym oknie wprowadzamy imię, inicjały, nazwisko oraz nazwę konta użytkownika. Windows Server 2003 wykorzysta te dane i sam wypełni pole Pełna nazwa. Podobnie jest podczas wprowadzania nazwy logowania użytkownika - wypełnienie pola Nazwa logowania użytkownika sprawia, że te same informacje są przenoszone do Nazwy logowania użytkownika w systemach wcześniejszych niż Windows 2000. Jeśli chcemy posługiwać się nazwą zgodną ze standardem UPN, możemy również podać odpowiadający nam sufiks. Alternatywne sufiksy do nazwy logowania można określić, korzystając z narzędzia Domeny i relacje zaufania usługi Active Directory. Pozwala to na zastosowanie nazwy logowania innej niż nazwa domeny. Jeśli cała organizacja należy do jednej struktury (np. idg.com) i polski oddział ma założoną domenę pl.idg.com, zastosowanie alternatywnego sufiksu, np. idg.pl, umożliwia logowanie się użytkowników z nazwą np. kpuchatek@idg.pl i integrację nazw z systemem pocztowym.

Po wprowadzeniu danych związanych z nazwami użytkownika należy kliknąć przycisk Dalej. W następnym oknie określamy dodatkowe parametry konta. Pierwsze dwa pola służą do wprowadzenia początkowego hasła użytkownika. Windows Server 2003 ma domyślnie włączone wymuszanie wprowadzania haseł o wysokim poziomie skomplikowania. Oznacza to, że podczas definiowania hasła musimy podać ciąg znaków spełniający opisane wcześniej wymagania co do złożoności (sześć znaków, wielkie i małe litery, cyfry lub znaki typu %, *, ! itp.). Po wpisaniu hasła przechodzimy do konfiguracji następnych parametrów. Pierwszy z nich - Użytkownik musi zmienić hasło przy następnym logowaniu - służy do wymuszenia zmiany hasła początkowego. W większości sieci nowo zakładane konta otrzymują narzucane przez administratora początkowe hasła. Część użytkowników, przez lenistwo czy przez nieuwagę, pracuje z tymi hasłami, nie zmieniając ich. Może to poważne zagrozić bezpieczeństwu sieci, bo początkowe hasła najczęściej są takie same. Aby zapobiec tej sytuacji, należy zaznaczyć opisywane pole wyboru. Podczas pierwszego logowania do sieci każdy użytkownik będzie musiał zmienić

hasło na wybrany przez siebie ciąg znaków. Funkcja ta działa najlepiej w połączeniu z opcją pamiętania historii haseł, ponieważ nowo wprowadzane hasło nie będzie mogło być takie samo, jak stare. Pozostałe dwie opcje: Użytkownik nie może zmienić hasła oraz Hasło nigdy nie wygasa, są z reguły zaznaczane przy kontach wykorzystywanych przez aplikacje (np. Exchange, SQL) lub usługi systemu. Uniemożliwienie zmiany hasła sprawdza się również, jeśli stosujemy konta współdzielone przez wielu użytkowników, np. jedno konto logowania dla określonej grupy. W praktyce należy unikać takich sytuacji, gdyż stanowi to naruszenie zasad bezpieczeństwa. Parametr związany z wygasaniem hasła należy zaznaczyć w odniesieniu do kont usługowych, jeśli polityka bezpieczeństwa firmy wymusza zmianę hasła co określony czas, np. co 60 dni. Konieczność zmiany haseł do kont użytkowników jest jak najbardziej zasadna, natomiast w wypadku kont usługowych i aplikacyjnych będzie kłopotliwa dla administratora. Użytkownik konta, który nie zmieni hasła po określonym czasie, nie będzie mógł się uwierzytelnić, co spowoduje zatrzymanie działania usługi lub aplikacji. Ostatni parametr - Konto jest wyłączone, należy stosować, gdy chcemy czasowo zapobiec wykorzystywaniu danego konta, ale nie chcemy go usuwać z bazy Active Directory. Tak bywa na przykład w przypadku dłuższej choroby pracownika lub pracy z kontami tymczasowymi. Kliknięcie przycisku Dalej wyświetla okno podsumowujące nasze działania i kończące zakładanie nowego użytkownika.

Właściwości kont użytkowników

Kliknięcie przycisku Zakończ zakłada nowe konto użytkownika. Pozostałe parametry określamy przez wybranie właściwości kont. W tym celu klikamy prawym przyciskiem obiekt użytkownika lub po jego zaznaczeniu korzystamy z menu Akcja i wskazujemy Właściwości. Wyświetlone okno przedstawia pokaźną grupę kart służących do dodatkowej konfiguracji użytkownika. Domyślnie część z nich jest niewidoczna. Jeśli chcemy zobaczyć wszystkie dostępne karty, należy w menu Widok wybrać Opcje zaawansowane.

Omawianie po kolei każdej z kart właściwości użytkownika mija się z celem, ponieważ część z nich należy konfigurować jedynie w przypadku wykorzystywania specyficznych usług systemu. Na przykład karty Zdalne sterowanie, Profil usług terminalowych, Sesje i Środowisko służą do określania cech użytkowników będących klientami usług terminalowych, a karta Telefonowanie jest przydatna podczas definiowania uprawnień do zdalnego dostępu do serwera. Wymienione usługi zostaną szerzej opisane w dalszych częściach przewodnika po Windows Server 2003.

Karty właściwości użytkownika służą do konfigurowania jego konta w systemie oraz do gromadzenia informacji o użytkowniku. Na początek zobaczmy, co można wprowadzić na kartach informacyjnych.

Informacje o użytkowniku

Usługa Active Directory służy do przechowywania informacji o cechach zasobów sieciowych. W przypadku użytkowników to, co zapiszemy w atrybutach konta, może być wykorzystywane w procesach komunikacyjnych wewnątrz firmy. Inni użytkownicy sieci będą się nimi posługiwać na przykład w celu odnalezienia informacji o miejscu pracy danej osoby, zajmowanym stanowisku itp. W przypadku małych sieci nie jest to istotne, jednak przydatne w dużych korporacjach.

Do wprowadzania danych o pracowniku służą następujące karty: Ogólne, Adres, Telefony i Organizacja. Na karcie Ogólne znajdują się znane już informacje o danych osobowych użytkownika. Możemy wprowadzić lub poprawić takie pola, jak Imię, Inicjał oraz Nazwisko. Dalej istnieje możliwość wprowadzenia opisu użytkownika, a także miejsca zatrudnienia. Dane kontaktowe obejmują telefon, adres poczty elektronicznej oraz adres witryny internetowej. Jeśli w tym miejscu wpiszemy e-mail i adres serwera WWW, będziemy mogli skorzystać z dwóch opcji menu podręcznego obiektu Użytkownik, takich

jak Wyślij pocztę oraz Otwórz stronę główną. W danych adresowych konta możemy zamieścić informację o miejscu zatrudnienia pracownika. Personel innych oddziałów firmy będzie wiedział, gdzie kierować korespondencję przeznaczoną dla danego użytkownika.

Na karcie Telefony znajdują się pola pozwalające na podanie kontaktowych numerów telefonicznych. Oprócz telefonu domowego jest tu miejsce na wprowadzenie informacji o telefonie komórkowym, pagerze, faksie oraz telefonie IP. Przewidziano także miejsce na dodatkowe uwagi, na przykład w jakich godzinach pracownik jest osiągalny pod danym numerem. Na karcie Organizacja można podać, jakie stanowisko zajmuje, w jakim dziale i jakiej firmie. Oddzielne pola służą do wprowadzenia informacji o podległości służbowej oraz raportowaniu.

Konfiguracja profili użytkowników

Karta Profil, zawarta we właściwościach użytkownika, pełni jedną z ważniejszych funkcji przy konfigurowaniu konta. Znajduje się na niej miejsce na ustawienia obejmujące profile, katalogi domowe oraz skrypty logowania.

Profil użytkownika to zespół ustawień określających parametry środowiska Windows. Uwzględnia preferencje związane ze sprzętem (mysz, klawiatura), pulpitem, menu Start i Programy itp. Profile są tworzone w czasie pierwszego logowania użytkownika do stacji roboczej. Domyślnie są tam również przechowywane. Dzięki temu użytkownicy po modyfikacji swoich preferencji, takich jak np. przystosowanie myszy dla leworęcznych, mogą z nich korzystać po każdorazowym zalogowaniu do komputera. Jeśli ktoś zmieni miejsce pracy, w nowym systemie będzie musiał ustawiać swoje parametry od początku. W Windows Server 2003, podobnie jak w Windows NT i 2000, można skonfigurować profile mobilne. Dzięki ich zastosowaniu zmiana komputera nie zmusza użytkownika do rekonfiguracji systemu. Opcja ta jest możliwa, ponieważ profile nie są przechowywane lokalnie, lecz na serwerze. Podczas logowania do sieci profil jest pobierany z serwera, a podczas wylogowywania jest na nim zapisywany. Przed konfiguracją profili mobilnych powinniśmy założyć i udostępnić odpowiedni katalog na serwerze, najlepiej na innej partycji niż system operacyjny, bezwzględnie zalecane jest zastosowanie systemu plików NTFS. Pozwala to na szczelne zabezpieczenie dostępu do profili poszczególnych użytkowników.

Na karcie Profil znajduje się pole służące do wpisywania, skąd system ma pobierać profil użytkownika. W ścieżce do profilu należy podać lokalizację folderu z profilem. Ścieżkę wprowadzamy zgodnie ze składnią UNC (Universal Naming Convention). Obejmuje ona nazwę serwera oraz nazwę udostępnienia, zapisane w formie \\nazwa_serwera\nazwa_udostępnienia. Na końcu ścieżki powinniśmy wprowadzić nazwę logowania użytkownika lub zmienną %UserName%. Wpisanie zmiennej jest przydatne, jeśli ustawiamy parametry profili wielu użytkowników i nie możemy jawnie podać ich nazwy. %UserName% zostanie automatycznie zamienione na nazwę konta. Po wpisaniu ścieżki i naciśnięciu przycisku OK system skonfiguruje również odpowiednie uprawnienia do folderów każdego z użytkowników. Jest to możliwe pod warunkiem, że partycja, na której przechowywane są profile, wykorzystuje system plików NTFS. Przedstawiony sposób konfiguracji pozwala na utworzenie profili mobilnych, które mogą być modyfikowane przez użytkowników.

Jeśli chcemy narzucić klientom sieci profile obowiązkowe, musimy wykonać kilka dodatkowych czynności. Profile z zakazem modyfikacji mogą być wykorzystywane w firmach, które chcą ujednolicić pulpity pracowników. Każdy użytkownik (choć najczęściej grupa użytkowników) może mieć przygotowany profil zawierający skróty do aplikacji, elementy pulpitu, elementy menu Start oraz tapety przeznaczone wyłącznie dla niego. Administrator określa standardy konfiguracji dla handlowców, księgowych, marketingu itp. W celu utworzenia profili obowiązujących należy najpierw utworzyć profile referencyjne. Realizujemy to, logując się na konto użytkownika, które będzie szablonem

profilu. Następnie modyfikujemy ustawienia tak, żeby były odpowiednie dla określonej grupy pracowników (np. dział marketingu). Po zakończeniu konfiguracji profilu wylogowujemy się. W ten sposób powstał nowy profil referencyjny. Logujemy się na konto z uprawnieniami administratora, w Panelu sterowania otwieramy obiekt System i klikamy kartę Zaawansowane | Profile użytkowników. Lista profili będzie zawierać utworzony profil referencyjny. Po zaznaczeniu musimy go skopiować do odpowiedniego udostępnienia na serwerze oraz określić uprawnienia do profilu. Obie czynności wykonujemy kolejno po wybraniu przycisku Kopiuj do. Następnie wprowadzamy lokalizację sieciową albo korzystamy z przycisku Przeglądaj. Uprawnienia modyfikujemy, naciskając przycisk Zmień w polu Pozwolenie na używanie. Zmiana typu profilu z dopuszczającego modyfikacje na obowiązkowy polega na zmianie nazwy pliku Ntuser.dat, znajdującego się w miejscu, do którego skopiowaliśmy profil. Jeśli skopiowaliśmy profil użytkownika ProfilRef na przykład do udostępnienia \\IDGTEST\Profiles, Ntuser.dat będzie się znajdował w folderze ProfilRef, umieszczonym w tym udostępnieniu. Konfiguracja profilu obowiązkowego to zmiana Ntuser.dat na Ntuser.man. Jeśli nie można zlokalizować pliku Ntuser.dat, należy sprawdzić, czy w opcjach folderów skonfigurowane jest wyświetlanie ukrytych obiektów. Konfigurację profili obowiązkowych kończy wpisanie pełnej ścieżki do profilu we właściwościach konta lub kont użytkowników.

Dodatkowe parametry karty Profil

Zawartość karty Profil nie ogranicza się do ustawień związanych z profilami użytkowników. W tym miejscu możemy skonfigurować jeszcze dwie istotne właściwości konta: skrypt logowania i ścieżka do folderu domowego użytkownika.

Konfiguracja skryptu na karcie profilu użytkownika to pozostałość po systemie Windows NT. W tym miejscu określano lokalizację skryptów przetwarzanych podczas logowania do domeny. Obecnie bardziej elastyczne rozwiązanie oferują Zasady grupy, które pozwalają na skonfigurowanie skryptów logowania, wylogowania użytkownika oraz startu i zamykania systemu operacyjnego. Nie oznacza to, że opcja Skrypt logowania jest całkowicie zbędna. Należy ją stosować wtedy, gdy klientami sieciowymi są komputery ze starszymi systemami operacyjnymi, takimi jak Windows 98 lub NT Workstation, oraz gdy przypisanie Zasad grupy nie spełnia wymagań administratora. Konfiguracja jest bardzo prosta, wystarczy napisać odpowiedni skrypt, następnie na karcie Profil umieścić jego nazwę, np. Logon.bat. W przeciwieństwie do profilu nie podajemy ścieżki, a jedynie nazwę. Skrypt należy zapisać w folderze katalog_główny_systemu\SYSVOL\sysvol\nazwa_domeny\scripts. Jako parametr katalog_główny_systemu z reguły podajemy Windows, a jako nazwę domeny - jej DNS-ową nazwę, np. pl.idg.com. W nazwie katalogu głównego tkwi pewnego rodzaju pułapka, na którą warto zwrócić uwagę. Poprzednie systemy serwerowe, takie jak Windows NT i 2000, domyślnie instalowały się w folderze WINNT, a nie w Windows. Administratorzy przenoszący skrypty ze starszych wersji powinni zwracać uwagę na tę zmianę.

Jedną z opcji konfiguracji serwera plików jest konfiguracja folderów macierzystych użytkowników. Ich głównym zadaniem jest przechowywanie plików klientów sieci. Standardowo dane zapisywane są w folderze Moje dokumenty na komputerach lokalnych. Zaletą takiego rozwiązania jest szybkość zapisu, niezależność i brak obciążenia sieci. Najpoważniejszą wadę stanowi trudność wykonywania kopii zapasowych. Najczęściej stacje robocze nie są wyposażone w sprzęt do sporządzania kopii zapasowych, a jeśli nawet są, to użytkownicy często zaniedbują regularną archiwizację swoich danych. Centralne składowanie dokumentów osobistych umożliwia proste rozwiązanie tego problemu. Za sporządzanie kopii odpowiada administrator, a ponieważ powinien przeprowadzać również archiwizację systemu i aplikacji, jest to tylko dodatkowa partia danych. Zalecane jest również połączenie konfiguracji folderów domowych z narzuceniem Przydziałów dyskowych. Ograniczymy w ten sposób przestrzeń zajmowaną przez użytkowników.

Karta Profil pozwala na określenie położenia folderów macierzystych. Do wyboru mamy ścieżkę lokalną albo podłączenie do udostępnienia sieciowego. Ścieżka lokalna powinna zawierać informacje o lokalizacji folderu na stacji roboczej, np. d:\home\users. Konfiguracja lokalizacji sieciowej wymaga założenia i udostępnienia odpowiedniego katalogu na serwerze. Tak jak w przypadku profili mobilnych, zalecane jest założenie folderu na innej partycji niż systemowa. Przykładowa konfiguracja może wyglądać następująco. Otwieramy Eksplorator Windows. Na partycji D: wybieramy menu Plik | Właściwości | Udostępnianie i przenosimy znacznik z Nie udostępniaj tego folderu na Udostępnij ten folder. Klikamy przycisk Uprawnienia. W oknie Uprawnienia dla Home, usuwamy grupę Wszyscy i klikając Dodaj, przypisujemy grupie Użytkownicy domeny uprawnienia Zmiana i Odczyt. Dwukrotne naciśnięcie przycisku OK zamyka otwarte okna. Na koniec przechodzimy do narzędzia Użytkownicy i komputery usługi Active Directory i wyszukujemy użytkownika, któremu chcemy przypisać folder macierzysty. Otwieramy właściwości użytkownika, wybieramy kartę Profil i klikamy Podłącz. Z listy oznaczeń dyskowych wybieramy odpowiadającą nam literę (najczęściej H:), a w pole Do wprowadzamy ciąg znaków \\nazwa_komputera\home\%UserName%. Kliknięcie OK kończy konfigurację folderów macierzystych.

Karta Konto

To kolejna karta, której należy poświęcić nieco więcej uwagi. Zawiera wiele istotnych parametrów konfiguracyjnych związanych z kontem i jego opcjami. Górna grupa ustawień pozwala na zmianę nazwy logowania. Jest to nazwa, którą przypisaliśmy do konta w czasie jego tworzenia.

Przyciski Zaloguj do oraz Godziny logowania otwierają okna, w których można wprowadzać ograniczenia miejsca i czasu dostępu do sieci. W oknie Godziny logowania wskazujemy, w jakich dniach i o jakiej porze użytkownik może się zalogować do sieci. Kolor niebieski oznacza zezwolenie na pracę, biały - brak możliwości podłączania się do zasobów sieciowych. Domyślnie użytkownik, który przekroczy przypisane mu ograniczenia, nie jest natychmiastowo odłączany od serwera, lecz nie może korzystać z kolejnych zasobów sieciowych, np. drukarki czy udostępnienia. Warto pamiętać, że nowo założone konta nie mają wprowadzonych ograniczeń związanych z godzinami logowania do sieci. W oknie Zaloguj do wyznaczamy te stacje, z których użytkownik ma prawo zalogować się do domeny. Domyślnie dozwolona jest praca z każdego stanowiska. Aby przypisać konto do określonych komputerów, należy przenieść znacznik z opcji Wszystkie komputery na Następujące komputery i wprowadzić ich nazwy. Warto pamiętać, że po zainstalowaniu systemu Windows Server 2003 lokalnie na serwerze nie mogą się logować zwykli użytkownicy sieci. Prawo takie mają jedynie administratorzy oraz konta wyznaczone do pełnienia zadań administracyjnych.

W sekcji Opcje konta jest seria pól wyboru, w których ustawiamy dodatkowe parametry konta. Część elementów poznaliśmy już w czasie tworzenia nowego użytkownika. Takie opcje, jak Użytkownik nie może zmienić hasła czy Hasło nigdy nie wygasa, zostały już omówione wcześniej. Warto jednak przyjrzeć się kilku nowym parametrom. Opcja Zachowaj hasło przy użyciu szyfrowania odwracalnego jest najczęściej stosowana w przypadku logowania z komputerów Apple lub przy uwierzytelnieniu metodą Digest z poziomu internetowych usług informacyjnych. Ze względów bezpieczeństwa nie należy włączać tego parametru. Parametru Logowanie interakcyjne wymaga karty inteligentnej używa się, chcąc wymusić stosowanie kart inteligentnych podczas logowania do domeny. Logowanie interakcyjne to takie, podczas którego użytkownik jawnie wprowadza nazwę konta oraz hasło. Następne dwa parametry: Konto jest zaufane w kwestii logowania i Konto jest poufne i nie może być delegowane, obejmują ustawienia związane z usługami Windows Server 2003. Delegowanie oznacza możliwość uzyskiwania dostępu do zasobów sieciowych przez usługi w kontekście uprawnień konta użytkownika. Na koniec pozostały nam opcje związane z dodatkową konfiguracją uwierzytelnienia za pomocą protokołu Kerberos. Ustawienie znaczników przy Użyj typów szyfrowania DES dla tego konta oraz

Nie jest wymagane wstępne uwierzytelnienie protokołu Kerberos jest wykorzystywane podczas integracji uwierzytelniania z innymi systemami operacyjnymi stosującymi Kerberos. Omawiane opcje należy zaznaczać jedynie w razie konieczności.

Wygasanie konta jest ostatnim parametrem karty Konto. Domyślne ustawienie (Nigdy) zmieniamy wtedy, gdy konfigurujemy konta dla pracowników tymczasowych, zatrudnionych na okres próbny lub na określony czas. Zaleca się korzystanie z tego parametru, bo zwalnia z konieczności pamiętania o blokowaniu konta po odejściu pracownika z firmy.

Grupy użytkowników

Oprócz indywidualnych kont użytkowników, Windows Server 2003 pozwala również na zakładanie grup. Grupy tworzymy w celu uproszczenia przypisywania uprawnień lub praw. O wiele szybciej i łatwiej skonfigurujemy dostęp do zasobu grupowego niż każdego konta z osobna. Dla początkujących użytkowników posługiwanie się grupami może być nieco kłopotliwe. Nie jest to związane z zakładaniem lub konfigurowaniem grup, lecz z odpowiednim zaplanowaniem struktury i rodzaju tworzonych obiektów. Windows Server 2003 posługuje się różnymi typami i zakresami grup. Dodatkowo, w zależności od trybu pracy, funkcjonalność tworzonych grup może się różnić.

Każdą zakładaną grupę cechuje zakres oraz typ. W wypadku usługi Active Directory są trzy zakresy grup: lokalny w domenie, globalny i uniwersalny. Utworzone konta użytkowników należy dodawać do grup globalnych. Są przeznaczone do gromadzenia kont pełniących podobne funkcje w firmie, np. Marketing, lub znajdujących się w jednej lokalizacji np. Pracownicy_Opole. Grupy lokalne służą do przypisywania uprawnień i zakładamy je tam, gdzie znajduje się zasób sieci. Jeśli chcemy nadać uprawnienia wszystkim pracownikom firmy do drukowania na drukarce podłączonej do serwera o nazwie Pepek, powinniśmy założyć na serwerze grupę Drukarka_Users i przypisać jej uprawnienie Wydruk. Do utworzonej grupy dodajemy grupę globalną Użytkownicy domeny. W ten sposób każdy pracownik firmy będzie mógł korzystać z drukarki, ponieważ domyślnie wszystkie konta użytkowników należą do grupy Użytkownicy domeny. Jest prosta strategia posługiwania się grupami, której zastosowanie znacznie ułatwia administrację. Jeśli to możliwe, należy dodawać konta do grup globalnych, a grupy te przypisywać do grup lokalnych. Grupy lokalne są zakładane tam, gdzie zasób, i to im nadajemy uprawnienia dostępu. Inne rozwiązania, np. przypisywanie uprawnień bezpośrednio do pojedynczych kont, utrudniają zarządzanie, zwłaszcza w większych firmach.

Główną różnicę między grupami lokalnymi a globalnymi stanowi ich zasięg. Grupy lokalne nie mogą opuścić własnej domeny, mogą natomiast gromadzić grupy globalne z wielu domen. Grupy globalne są widoczne z każdej domeny, ale należą do nich wyłącznie konta z własnej domeny. Grupy uniwersalne są połączeniem obu zakresów i powinny być stosowane tylko w rozległych środowiskach wielodomenowych, ponadto domena nie może pracować w środowisku mieszanym, czyli z kontrolerami domeny opartymi na NT 4.0 Serwer.

Typy służą do określania przeznaczenia grupy. Podczas zakładania grupy wskazujemy, czy chodzi o zabezpieczenia, czy o dystrybucję. Domyślnie zaznaczony jest typ Zabezpieczenia, co oznacza, że tworzone konto służy do wyznaczania uprawnień. Nadając uprawnienia do drukarek, rejestru czy plików w systemie NTFS, korzystamy właśnie z grup tego typu. Typ Dystrybucja służy do przekazywania wiadomości poczty elektronicznej. Na grupy tego typu nie można nakładać uprawnień. Ponieważ grupy zabezpieczeń mogą również pełnić funkcję grup dystrybucyjnych, korzystamy przeważnie z nich.

Utworzenie grupy użytkowników to łatwa operacja. Najprościej posłużyć się narzędziem Użytkownicy i komputery usługi Active Directory. Po uruchomieniu przystawki musimy zaznaczyć tę jednostkę organizacyjną, w której zamierzamy utworzyć grupę - na przykład jednostkę PCWK, gromadzącą wszystkich pracowników PC Worlda. Następnie z menu Akcja wybieramy Nowy | Grupa. W wyświetlonym oknie musimy wprowadzić nazwę grupy. Podobnie jak podczas zakładania nowego konta użytkownika, również w przypadku grup należy podać dwie nazwy, właściwą oraz nazwę systemów starszych niż Windows 2000. Naturalnie zaleca się, żeby obie nazwy się nie różniły i były niezbyt długie. Następnie określamy zakres i typ grupy. Jeśli chcemy na przykład założyć konto zawierające pracowników PCWK, w nazwie wpisujemy PracownicyPCWK, a następnie zaznaczamy zakres Globalny i typ Zabezpieczenia. Kliknięcie OK powoduje utworzenie grupy. Na koniec dodajemy do grupy konta użytkowników. Możemy to zrobić na dwa sposoby. Pierwszy to wybranie właściwości grupy i naciśnięcie przycisku Dodaj na karcie Członkowie. Drugi sposób to zaznaczenie myszą (przy wciśniętym przycisku [CTRL]) kont użytkowników i wybranie menu Akcja | Dodaj do grupy. W wyświetlonym oknie wprowadzamy nazwę lub początek nazwy grupy i naciskamy OK. Wszystkie zaznaczone konta są w tym momencie umieszczane we wskazanej grupie.

Konfiguracja uprawnień NTFS

Jeśli Windows Server 2003 ma pracować jako serwer plików, powinien być w nim stosowany jedynie system NTFS. Oprócz zwiększonej wydajności oferuje on możliwość nadawania uprawnień dostępu. Właśnie ta cecha jest w naszym przypadku kluczowa. Ważna może być również wbudowana kompresja oraz konfiguracja przydziałów dyskowych.

Uprawnienia NTFS możemy nadawać zarówno plikom, jak i folderom. W celu ustalenia, kto może uzyskiwać dostęp do plików i folderów, system NTFS korzysta z list Access Control List (ACL). Zawierają one nazwy użytkowników lub grup oraz przypisane im uprawnienia. Aby uzyskać dostęp do danych, użytkownik albo grupa, do której należy, musi być wymieniona na liście uprawnionych. W przeciwnym wypadku system wyświetli komunikat "Odmowa dostępu". Ten sam komunikat obejrzymy, jeśli będziemy mieli jawnie przypisane uprawnienie z zaznaczeniem opcji Odmów. Windows Server 2003 sumuje nadane uprawnienia. Będąc członkami dwóch grup, z których jedna ma przypisane uprawnienie Odczyt, a druga Zapis, możemy zarówno czytać, jak i zapisywać dane. Wyjątkiem jest wspomniana wyżej odmowa dostępu. Po jej zastosowaniu inne uprawnienia nie mają znaczenia. Jeśli grupa, do której należymy, lub nasze konto mają ustawioną odmowę dostępu, staje się ona efektywna nawet, jeśli jesteśmy członkami grup mających uprawnienia zezwalające na dostęp.

Kolejną właściwością NTFS jest dziedziczenie uprawnień. Przypisane do folderu uprawnienia domyślnie przenoszą się na wszystkie znajdujące się w nim podfoldery i pliki. W efekcie użytkownik, który ma uprawnienia dostępu do folderu np. APPS, będzie mógł sięgnąć do wszystkich zapisanych w nim danych. Dziedziczenie jest szczególnie przydatne, gdy chcemy szybko zapewnić dostęp do szerszej struktury plików. Nadanie nowych uprawnień na wyższym poziomie drzewa folderów nie zastępuje tych, które już się w nim znajdują. Nowe zasady dostępu są dodawane do poprzednich. W oknie konfiguracji zabezpieczeń odziedziczone uprawnienia są zacieniowane. Jeśli dziedziczenie przeszkadza nam we właściwym nadaniu uprawnień, możemy je wyłączyć. W tym celu na karcie Zabezpieczenia pliku lub folderu należy kliknąć przycisk Zaawansowane. W dolnej części okna są dwie opcje związane z dziedziczeniem. Pierwsza, Zezwalaj na propagowanie dziedziczonych uprawnień, ma domyślnie ustawiony znacznik i dzięki temu uprawnienia "spływają" w dół. Usunięcie znacznika przerywa dziedziczenie i w zależności od naszej decyzji kopiuje bieżące ustawienia na obiekty wewnątrz lub je usuwa. Druga opcja, Zamień wpisy uprawnienia na wszystkich obiektach, pozwala na szybkie "oczyszczenie" uprawnień na obiektach wewnętrznych. Ustawienie znacznika i wybranie

przycisku Zastosuj, przenosi uprawnienia z bieżącego okna na podfoldery i pliki, z jednoczesnym usunięciem innych, jawnie nadanych uprawnień.

Znajomość podstawowych właściwości systemu NTFS wystarcza do prawidłowego skonfigurowania uprawnień. Ponieważ naszym zadaniem jest skonfigurowanie serwera plików, omówimy na prostym przykładzie, jak należy przypisać uprawnienia do folderu zawierającego wersje instalacyjne firmowego oprogramowania.

Rozpoczynamy od założenia odpowiedniej struktury folderów. Dane powinniśmy zapisać na innej partycji niż system operacyjny, np. D:. Następnie przechodzimy do utworzenia katalogów. Aby przypisanie i zarządzanie uprawnieniami nie było zbyt skomplikowane, zakładamy jeden folder do gromadzenia aplikacji. Możemy go nazwać np. Instalacje. Po jego zaznaczeniu z menu Plik wybieramy opcję Właściwości albo Udostępnienia i zabezpieczenia. Następnie przechodzimy do karty Zabezpieczenia, podzielonej na dwie sekcje. Pierwsza służy do wyznaczania użytkowników lub grup, którym chcemy przypisać dostęp do zasobu. Druga pozwala na określenie poziomu nadawanych uprawnień. Jeśli chcemy dodać nowe konto, naciskamy przycisk Dodaj i wprowadzamy nazwę lub początek nazwy konta. Jeśli nie pamiętamy, jaką nazwę nosi dany użytkownik lub grupa, po naciśnięciu przycisku Zaawansowane, możemy wybrać Znajdź teraz i otrzymamy pełną listę kont. Po wprowadzeniu początku nazwy, która występuje wielokrotnie, system przedstawi listę kont spełniających wymagania. Jeśli chcemy przypisać uprawnienia grupie PracownicyPCWK, wystarczy wpisać ciąg Pracownicy, a system automatycznie doda tę grupę do okna uprawnionych albo wyświetli grupy spełniające wprowadzony warunek. Po dodaniu grupy w dolnej części okna ustalamy poziom uprawnień. Ponieważ folder ma gromadzić instalacje aplikacji, zwykły użytkownik nie powinien móc modyfikować danych, a najwyżej odczytywać jego zawartość. W takim wypadku najlepszym uprawnieniem będzie Odczyt i wykonanie. Nadajemy je, zaznaczając opcję Zezwalaj przy tym uprawnieniu. Warto zwrócić uwagę, że automatycznie zaznaczają się uprawnienia Wyświetlanie zawartości folderu oraz Odczyt. Kliknięcie przycisku OK zatwierdza wykonaną operację. Nadanie uprawnień w folderze Instalacje powoduje, że każdy zakładany folder podrzędny będzie je dziedziczył. Jeśli utworzymy katalogi np. Office, Benchmarki lub AntyWir, każdy z nich będzie miał już skonfigurowane właściwe zakresy dostępu.

Konfiguracja udostępnień

Głównym zadaniem serwera plików jest udostępnianie klientom sieci zapisywanych na nim danych. Udostępniać można: foldery macierzyste, profile mobilne, foldery z aplikacjami, sterowniki itp. Utworzenie udostępnienia nie jest wyjątkowo skomplikowane.

Jeśli chcemy udostępnić użytkownikom jeden z folderów umieszczonych na serwerze, powinniśmy skorzystać z Eksploratora Windows. Zakładamy bądź odnajdujemy w nim katalog przeznaczony do udostępnienia, zaznaczamy go, a następnie z menu Plik wybieramy opcję Udostępnianie i zabezpieczenia. W oknie właściwości folderu na karcie Udostępnianie przenosimy znacznik z opcji Nie udostępniaj tego folderu na Udostępnij ten folder. System domyślnie proponuje, aby nazwą udziału była nazwa folderu. Jeśli propozycja ta nam nie odpowiada, w pole Nazwa udziału wpisujemy nową wartość. Opcjonalnie możemy wprowadzić opis zawartości katalogu oraz limit użytkowników, którzy mogą korzystać z udostępnienia. Warto pamiętać, że domyślnie limit ten równa się liczbie licencji "na serwer", skonfigurowanych w opcji Licencjonowanie Panelu sterowania.

Ostatnim i najważniejszym elementem konfiguracji udostępnień jest przypisanie uprawnień do korzystania z zasobu. Po kliknięciu przycisku Uprawnienia wyświetlane jest okno służące do nadawania uprawnień. Sposób określania poziomu dostępu jest niemal identyczny, jak zabezpieczeń systemu NTFS. Interfejs okna podzielono na dwie części - pierwsza służy do wskazania grupy lub użytkownika, a druga do przypisania uprawnienia. Inny jest rodzaj nadawanych uprawnień. Dostępne są jedynie trzy opcje: Pełna kontrola,

Zmiana i Odczyt. Ich nazwy są tak intuicyjne, że w zasadzie nie trzeba opisywać, do czego służą. Po wyborze grupy i typu uprawnienia naciśnięcie przycisku OK zatwierdza nadane uprawnienia.

Właściwe posługiwanie się uprawnieniami do udostępnień wymaga dodatkowych informacji. W wypadku udostępnień obowiązują podobne zasady konfiguracji, jak przy systemie NTFS. Jeśli użytkownicy występują w kilku grupach wymienionych w oknie uprawnionych, ich możliwości sumują się. Zastosowanie odmowy dostępu nadpisuje wszelkie zezwolenia. Należy bezwzględnie pamiętać, że uprawnienia udostępnień i NTFS współpracują ze sobą. Efektywne jest zawsze ustawienie bardziej restrykcyjne.

Dodawanie roli serwera plików i serwera wydruku

Po zainstalowaniu Windows Server 2003 uruchamiany jest panel konfiguracji ról serwera. Wśród dostępnych opcji znajduje się również możliwość przypisania roli serwera plików. Odpowiedni kreator pozwala na zdefiniowanie przydziałów dyskowych, indeksowania oraz udostępnień sieciowych. Jego możliwości są dość ubogie, ale wystarczy do wstępnej konfiguracji systemu. Dodatkowe ustawienia należy przeprowadzić samemu. Zaletą skonfigurowania roli serwera plików jest utworzenie specjalnej przystawki do zarządzania serwerem. Ułatwia ona początkującym administratorom poruszanie się po zakamarkach Windows Server 2003.

Dodawanie roli serwera wydruku jest jeszcze łatwiejsze. Zadanie właściwie sprowadza się do dodania nowej drukarki. Po wybraniu roli Serwer wydruku w Kreatorze konfigurowania serwera, zaznaczamy jakiego rodzaju klienci będą korzystali z udostępnianych drukarek. Jeżeli będą to systemy Windows 2000 i nowsze uruchomiony zostanie standardowy kreator dodawania nowej drukarki. Jeżeli natomiast zaznaczymy opcję Wszyscy klienci systemu Windows, po zainstalowaniu sterowników podstawowych uruchomiony zostanie Kreator dodawania sterowników drukarek, który zainstaluje sterowniki do wybranych dodatkowych systemów operacyjnych. Po tym pozostaje jedynie nadać użytkownikom odpowiednie uprawnienia na karcie Zabezpieczenia.

IDG.PL
Klient sieci
PC World Komputer

Sieć komputerowa składa się nie tylko z serwera, ale także klienckich stacji roboczych. Konfiguracja serwera jest niezmiernie ważna, lecz warto pamiętać, że jego zadaniem jest świadczenie usług użytkownikom sieci. Dlatego poprawne przygotowanie stacji roboczych daje solidne podstawy do wydajnej pracy.

Windows Server 2003 może współpracować z różnymi klientami. Wśród dostępnych usług systemu odnajdziemy takie, które pozwalają na komunikację z systemami Windows, Unix i Macintosh. Naturalnie klientami najlepiej przystosowanymi do pracy w domenie będą stacje wyposażone w najnowsze systemy operacyjne potentata z Redmond, takie jak: Windows 2000 Professional oraz Windows XP Professional. Pozostałe, np. Windows NT 4.0, są albo przestarzałe, albo przeznaczone do zastosowań domowych i ich integracja z sieciami Microsoft jest możliwa tylko w ograniczonym zakresie.

Konfiguracja poszczególnych systemów do pracy w domenie Windows Server 2003 opiera się na podobnych zasadach. Ustawienia systemów 2000 i XP różnią się nieznacznie, ale rozbieżności między Windows 98, Me i NT są już nieco większe. Na szczegółowy opis

wszystkich możliwych konfiguracji nie starczy nam miejsca, więc przykłady będą obejmowały wyłącznie stacje robocze z zainstalowanym Windows XP Professional. Pominiemy również tematykę związaną z fizyczną instalacją sieci oraz kart sieciowych.

Komunikacja sieciowa

Komunikacja sieciowa jest możliwa tylko wtedy, gdy są odpowiednie warunki. Stacje robocze i serwer sieciowy powinny być wyposażone w sprzęt zapewniający transmisję danych - zwykle jest to tania i prosta w instalacji karta sieciowa. Oprócz interfejsu sieciowego należy zadbać o niezawodne połączenie kablowe oraz co najmniej jedno urządzenie aktywne, np. koncentrator lub przełącznik. Jeśli powyższe warunki są spełnione, możemy przejść do konfiguracji serwera i klienckich stacji roboczych w sieci.

Mając fizyczne możliwości wymiany informacji, należy zadbać o właściwe ustawienia systemów operacyjnych. Oprócz zainstalowania karty sieciowej trzeba będzie ustawić takie parametry, jak klient sieci, protokół oraz odpowiednie usługi sieciowe. Konfiguracja odbywa się we właściwościach połączeń sieciowych. Aby się do nich dostać na przykład w Windows XP, należy wybrać Start | Ustawienia | Połączenia sieciowe, wskazać połączenie i wybrać Właściwości.

Protokół komunikacyjny można porównać do języka, jakim posługuje się komputer w czasie dialogu z innymi stacjami roboczymi. Dzięki niemu komputery będą mogły zrozumieć przekazywane w sieci informacje. Windows Server 2003 obsługuje wiele protokołów, ale najkorzystniejsze jest zastosowanie TCP/IP. Ponieważ stał się standardem w większości sieci, korzystanie z niego umożliwia komunikację z innymi systemami, np. Linuksem czy NetWare. Ponadto niektóre kluczowe usługi oferowane przez Windows Server 2003, np. Active Directory, wymagają jego wykorzystania.

Kolejnym komponentem koniecznym do pracy w domenach Windows Server 2003 jest Klient sieci Microsoft Networks. Nie wymaga od użytkownika żadnej konfiguracji, ale to właśnie dzięki niemu można uzyskiwać dostęp do zasobów oferowanych przez inne komputery w sieci. Domyślnie składnik ten jest instalowany i uruchamiany. Jeśli nie jest potrzebny, łatwo go wyłączyć. Dostęp do zasobów oferowanych przez lokalny komputer oferuje składnik o nazwie Udostępnianie plików i drukarek w sieciach Microsoft Networks. Gdy go brak, inne stacje nie będą mogły korzystać z naszych udostępnień i drukarek. Serwery plików i drukarek bezwzględnie wymagają tego składnika, natomiast stacje sieciowe tylko wtedy, gdy dane komputery oferują swoje zasoby, np. lokalnie podłączone drukarki.

Adresowanie IP - podstawa komunikacji

Jeśli komunikacja będzie oparta na TCP/IP, trzeba wybrać najlepszy do swojej sieci sposób konfiguracji adresowania protokołu. Każdy system wysyłający lub odbierający dane musi mieć przypisany unikatowy adres IP. Służy on do jednoznacznej identyfikacji systemu w sieci i składa się z czterech części, tzw. oktetów, oddzielonych kropkami. Każdy z nich może przybierać wartości z zakresu 0-255, przykładowy adres to 192.168.0.1. Niedopuszczalne jest dublowanie adresów, każdy identyfikator musi być unikatowy w obrębie tzw. podsieci, czyli wydzielonego fizycznego fragmentu sieci. Pomyłka w adresie sprawia, że dany komputer nie będzie mógł poprawnie komunikować się z innymi stacjami.

Drugi bardzo istotny element adresowania, maska podsieci, to również cztery oddzielone kropkami liczby, które muszą jednak przyjmować z góry ustalone wartości, np. 255.255.255.0 albo 255.255.0.0. Ta część adresowania IP pozwala na określenie, gdzie zlokalizowany jest odbiorca wysyłanych informacji - w lokalnej sieci, czy poza nią. W niektórych oknach konfiguracyjnych systemu Windows maska podsieci jest zapisywana w inny sposób. Zamiast oktetów należy wprowadzić wartość odpowiadającą liczbie bitów

przeznaczonych na maskę. Adres IP 192.168.1.1 z maską 255.255.255.0 będzie przedstawiony jako 192.168.1.1/24. Zapis ten oznacza, że na maskę przeznaczono 24 bity. Dla przypomnienia: 255 binarnie równa się 11111111, co zajmuje osiem bitów. Podanie adresu IP oraz maski podsieci jest niezbędne do komunikacji.

Gdy system pracuje w grupach roboczych lub poza Internetem, wypełnienie pola związanego z adresem serwera DNS nie jest obowiązkowe, ale zalecamy to, bo przygotowujemy klienta do pracy w środowisku domenowym. Klienty korzystają z rozwiązywania nazw DNS w czasie wyszukiwania innych systemów w sieci, co ma bardzo duże znaczenie w czasie logowania do domeny. Informacje o kontach przechowywane są w Active Directory, użytkownik po wpisaniu swojej nazwy i hasła musi być uwierzytelniony przez kontroler domeny, czyli w naszym przypadku Windows Server 2003. W tym celu system klienta powinien zgłosić się do serwera i poprosić go o "wpuszczenie" do sieci. Żeby móc to zrobić, trzeba zlokalizować komputer z Windows Server 2003. Szybkie wyszukiwanie kontrolera domeny jest realizowane właśnie poprzez DNS. Klient wysyła zapytanie do serwera i w odpowiedzi otrzymuje listę adresów IP kontrolerów. Jeśli nie podamy preferowanego serwera DNS, system klienta odnajdzie kontroler, korzystając z emisji (broadcastu), jednak będzie to długo trwało. Pozostałe parametry TCP/IP, takie jak adres bramy domyślnej lub adres serwera WINS w opcjach zaawansowanych, konfigurujemy w razie potrzeby.

W wypadku sieci lokalnych, w których komputery nie oferują zasobów klientom z zewnątrz firmy, np. internetowym, zalecane jest stosowanie adresowania prywatnego, obejmującego grupy adresów niewykorzystywanych publicznie w Internecie. Identyfikatory sieci prywatnych przedstawiają się następująco: 10.0.0.0/8, 172.16.0.0/12 i 192.168.1.0/16. Oznacza to, że na potrzeby firmy możemy wybrać adresowanie z jednego z przedstawionych wyżej zakresów, przypisując komputerom np. w małej firmie adresy od 192.168.1.1 do 192.168.1.20 z maską 255.255.255.0. Nie trzeba przy tym sprawdzać, czy są gdziekolwiek stosowane do adresowania serwerów internetowych.

Sposoby przydzielania adresów

Windows Server 2003 oraz Windows XP pozwalają na wybranie różnych strategii konfigurowania protokołu TCP/IP. Najprostsza to ręczne przypisanie każdej stacji właściwego adresu. W tym celu należy wypełnić odpowiednie pola we właściwościach protokołu TCP/IP. Naturalnie adres i jego parametry należy wpisywać uważnie. W celu uniknięcia bałaganu warto odnotowywać przydzielane adresy na osobnym arkuszu, a w większych firmach - w bazie danych.

Ręczne zarządzanie adresami IP ma dużo wad. Do najważniejszych zaliczamy trudności z ich modyfikacją oraz prawdopodobieństwo pomyłek podczas wprowadzania. Jeśli trzeba zaadresować na przykład 150 stacji, konfiguracja będzie trwała długo. Administrator lub grupa administratorów musi dojść do każdego komputera i nadać mu odpowiedni adres, więc prawdopodobieństwo popełnienia pomyłki jest znaczne. Zamiana dowolnej cyfry w adresie, masce podsieci lub adresie serwera DNS powoduje zakłócenia w komunikacji.

W celu usprawnienia tej procedury w wielu sieciach stosuje się adresowanie automatyczne. Instalowany i uruchamiany jest serwer DHCP, którego działanie polega na przydzielaniu klientom sieci adresów IP na żądanie. Stacja robocza w czasie startu wysyła prośbę o adres do serwera, który wybiera jeden z puli i nadaje go klientowi na okres ustalany przez administratora. W naszym przypadku funkcję serwera może z powodzeniem pełnić Windows Server 2003. Ponieważ adresy są nadawane automatycznie, administrator nie musi odwiedzać każdego z komputerów na wypadek modyfikacji ustawień. Jeśli chcemy wprowadzić inne parametry adresu, związane np. z serwerem DNS, dzięki centralnej konfiguracji dotrą one bez kłopotu do wszystkich klientów sieci. Problemem może być oczywiście awaria serwera DHCP, ale jeśli

skorzystamy z dostępnej w Windows XP funkcji alternatywnego adresowania, ten kłopot zostanie ominięty.

Ostatni z możliwych sposobów to automatyczne adresowanie prywatne, dostępne w systemach operacyjnych Microsoftu od Windows 98 SE, z wyjątkiem - uwaga! - Windows NT. Polega na samoistnym przypisaniu adresu IP wtedy, gdy nie można go uzyskać w inny sposób. Jeśli stacja ma na przykład skonfigurowane pobieranie adresu z serwera DHCP, ale serwer z dowolnej przyczyny jest nieosiągalny, wówczas system sam przypisze sobie adres. Będzie to identyfikator ze z góry narzuconego zakresu od 169.254.0.1 do 169.254.255.254, z maską 255.255.255.0. Adresowanie to stosuje się w bardzo małych grupach roboczych po to, żeby oszczędzić użytkownikom konieczności zapamiętania reguł adresowania IP i zminimalizować skutki awarii, podczas których nie można przydzielać klientom adresów IP.

Przykładowe rozwiązanie adresowania w sieci

W przykładowej konfiguracji sieci wykorzystujemy ręczne przydzielanie adresów IP. Ustawienia związane z DHCP zostaną opisane po omówieniu tej usługi. Zakładamy, że nasza sieć nie przekroczy jednej lokalizacji i będzie w niej wykorzystywanych najwyżej 100 systemów. W takim wypadku z powodzeniem możemy wykorzystać jedną z grup adresów prywatnych, np. sieć 192.168.1.0 z maską 255.255.255.0.

Pracę należy rozpocząć od wprowadzenia parametrów TCP/IP Windows Server 2003. W tym celu klikamy Start | Panel sterowania | Połączenia sieciowe. Następnie wybieramy połączenie związane z kartą sieciową. Jeśli na serwerze jest tylko jedna karta sieciowa, to domyślnie otrzymuje nazwę Połączenie lokalne. Gdy jest wiele interfejsów sieciowych, w celu zwiększenia czytelności zaleca się zmianę nazwy, np. na LAN lub LocalNet (opcję Zmień nazwę znajdziesz w menu podręcznym połączenia lokalnego). Kliknięcie wybranego połączenia otwiera okno Stan.

We właściwościach tego okna wyświetlana jest lista składników sieciowych związanych z połączeniem. W celu zmiany ustawień TCP/IP należy zaznaczyć ten protokół oraz kliknąć Właściwości. Karta Ogólne zawiera pola związane z adresowaniem IP oraz adresami serwerów DNS. Konfiguracja Windows Server 2003 wymaga ręcznego ustawienia adresów. Zgodnie z założeniami, w polu adresu IP wprowadzamy: 192.168.1.1, a jako maskę podsieci 255.255.255.0. Następnie przechodzimy do pola Preferowany serwer DNS i wpisujemy odpowiedni adres. Zakładamy, że serwerem DNS jest serwer lokalny i dlatego wpisujemy 192.168.1.1. Jeśli sieć nie jest ograniczona do zasobów lokalnych i wymaga dostępu np. do Internetu, należy również wypełnić pole Brama domyślna. Powinno zawierać adres IP systemu lub urządzenia będącego routerem. W schematach adresowania stosowanych w sieciach lokalnych bramy oznaczane są najczęściej jedynką, np. 10.0.0.1, ale jest to rozwiązanie zwyczajowe i nie musimy go stosować. Jeśli zmieniamy adres na funkcjonującym serwerze, trzeba zwrócić uwagę na ustawienia usług sieciowych, które mogą wymagać rekonfiguracji. Dzieje się tak na przykład w przypadku usługi DHCP.

Zakończenie konfiguracji serwera pozwala na przejście do stacji klienckich. Na komputerach pracujących pod kontrolą Windows XP przypisanie parametrów protokołu TCP/IP przebiega bardzo podobnie. We właściwościach połączenia sieciowego odnajdujemy składnik TCP/IP, w którym wypełniamy te same pola. Oczywiście maska oraz adres serwera DNS pozostają takie same - w naszym przypadku 255.255.255.0, DNS: 192.168.1.1. Modyfikacji podlega jedynie adres IP. Aby uniknąć problemów, przydzielone adresy należy odnotowywać w pliku tekstowym lub odpowiednim arkuszu. Rekonfiguracja adresu nie wymaga restartu komputera. Na koniec warto sprawdzić, czy nasze działania są skuteczne. W tym celu wystarczy posłużyć się poleceniem ping z parametrem będącym adresem serwera. Jeśli po uruchomieniu wiersza poleceń i

wpisaniu: ping 192.168.1.1 otrzymamy pozytywną odpowiedź, będzie to oznaczać poprawną konfigurację protokołu TCP/IP, zarówno po stronie serwera, jak i stacji XP.

Automatyzacja adresowania przez DHCP

Automatyczne adresowanie może zdecydowanie ułatwić pracę administratora. Do konfiguracji adresowania tego typu będziemy potrzebować serwera DHCP. Ponieważ w skład usług sieciowych dostarczanych z Windows Server 2003 wchodzi protokół dynamicznej konfiguracji hosta (DHCP), wystarczy odpowiednio przygotować serwer.

Działanie serwera DHCP jest stosunkowo proste. Komputery klienckie w sieci podczas startu systemu sprawdzają lokalną konfigurację TCP/IP. Jeśli w parametrach protokołu zaznaczona jest opcja Uzyskaj adres IP automatycznie, system operacyjny musi się postarać o przydzielenie adresu. Najpierw należy zlokalizować serwer DHCP. Ponieważ na początku system nie wie, która stacja pełni to zadanie, do wszystkich komputerów w sieci wysyłana jest prośba o zgłoszenie się serwera DHCP. Na tę prośbę odpowiadają jedynie maszyny z uruchomioną usługą DHCP. W naszym przypadku będzie to Windows Server 2003. Otrzymana odpowiedź zawiera ofertę adresu IP. Klient potwierdza przyjęcie oferty, wysyłając odpowiednią informację do sieci. Na koniec serwer, którego oferta została przyjęta, odsyła klientowi potwierdzenie nadania adresu. Od tej chwili stacja staje się pełnoprawnym dzierżawcą adresu i parametrów IP. Opisane działanie odbywa się podczas pierwszego kontaktu z serwerem DHCP. Jeśli stacja już otrzymała adres, powtórne odwołania do serwera wyglądają nieco inaczej. Komputer "wynajmujący" adres może się nim posługiwać w wyznaczonym przez administratora okresie. Domyślnie jest to osiem dni. Po upływie połowy czasu dzierżawy lub podczas każdego restartu komputera stacja kontaktuje się z serwerem DHCP w celu odnowienia dzierżawy i związanych z nią parametrów. Jeśli system nie będzie mógł odnaleźć usługodawcy, DHCP będzie używał adresu do czasu jego wygaśnięcia.

Podstawowa konfiguracja serwera DHCP opiera się na założeniu i uaktywnieniu zakresu adresów. Zakres to przedział adresów IP, jakim będą się posługiwały klienty sieci. Definicja zakresu zawiera nazwę, adres początkowy, adres końcowy, maskę podsieci, czas dzierżawy oraz dodatkowe opcje związane z innymi parametrami przekazywanymi klientom sieci, np. adres domyślnej bramy lub serwera DNS. Zanim klienty sieci będą mogły wykorzystać zakres, należy go uaktywnić. Jeśli na serwerze wyczerpie się pula adresów dla klientów, kolejne zgłaszające się komputery nie otrzymają adresu. W takim wypadku należy albo zwiększyć pulę, albo skrócić czas dzierżawy.

Dodatkowe parametry DHCP

Zanim przejdziemy do przykładowej konfiguracji serwera DHCP na potrzeby naszej sieci, powinniśmy poznać kilka dodatkowych szczegółów związanych z jego pracą. Pierwszą istotną czynnością, jaką należy wykonać po zainstalowaniu serwera, jest autoryzacja DHCP w usłudze Active Directory. Ponieważ klienty usługi DHCP nie mogą decydować, z którego serwera będą pobierały adres IP, pojawienie się w sieci nieznanych serwerów sprawia wiele problemów. Część stacji po otrzymaniu niewłaściwego adresu nie będzie mogła się komunikować z pozostałymi komputerami. Aby ograniczyć możliwość powstania tego typu trudności, wprowadzono autoryzację serwerów, która wymaga obecności w sieci usługi Active Directory. Active Directory utrzymuje listę zarejestrowanych serwerów, które mogą świadczyć usługi DHCP. W czasie uruchamiania usługi DHCP w Windows Server 2003 lub Windows 2000, systemy te weryfikują swoją obecność na liście uprawnionych komputerów. Jeśli serwer nie jest autoryzowany, nie będzie przydzielał adresów klientom sieci. Autoryzacja nie potrafi zablokować przyznawania IP przez serwery na przykład z systemem Linux czy Windows NT.

W większości sieci konfiguracja adresowania IP nie kończy się na przypisaniu adresu i maski podsieci. Często klienty muszą mieć określone dodatkowe parametry, takie jak

adres routera lub adres serwera WINS. W przypadku domen Active Directory konieczne jest również dostarczenie adresu serwera DNS. DHCP byłaby bardzo mizerną usługą, gdyby nie potrafiła przekazać dodatkowych parametrów IP. W Windows Server 2003 możemy zdefiniować wiele poziomów opcji, które będą przenoszone na klienty sieci. Opcje mogą być nadawane z poziomu serwera, zakresu, zastrzeżenia albo klas zdefiniowanych przez administratora lub dostawców. Najczęściej wykorzystywane są opcje zakresu, obejmujące klienty z określonej grupy adresów IP. Po zdefiniowaniu opcji, np. DNS, wszystkim stacjom pobierającym adres z zakresu będzie nadany adres IP i maska podsieci oraz zostanie dla nich ustawiony adres serwera DNS. Opcje DHCP możemy konfigurować w czasie tworzenia zakresu albo w dowolnym terminie późniejszym. Zmiana wartości opcji zostanie automatycznie przypisana komputerom klientom sieci w czasie odnawiania dzierżawy adresu.

Kolejnym przydatnym ustawieniem DHCP jest możliwość wykonywania rezerwacji i wykluczeń adresów. Ponieważ DHCP przydziela adresy dynamicznie, może się zdarzyć, że co pewien czas stacje otrzymają różne adresy IP. Jeśli zależy nam na tym, aby określony komputer miał zawsze przydzielany ten sam adres, należy skonfigurować rezerwację. Działanie rezerwacji polega na powiązaniu adresu IP z adresem fizycznym karty sieciowej klienta. Gdy do serwera zgłosi się komputer z zastrzeżonym adresem MAC, serwer przydzieli mu skojarzony IP. Wykluczenia to ustawienia, które rozwiązują problemy innego rodzaju. Jeśli w sieci działa już grupa urządzeń lub komputerów z przypisanymi ręcznie adresami IP, może dojść do tego, że zakresy obejmują już przydzielone adresy. W takim wypadku należałoby wykluczyć z zakresu zajęte IP. Wprowadzanie wykluczeń jest możliwe w trakcie tworzenia zakresu albo w dowolnym momencie pracy serwera.

Przykładowa konfiguracja DHCP

Konfigurację serwera DHCP rozpoczynamy od instalacji usługi dynamicznego przydzielania adresów. W tym celu należy przejść do Panelu sterowania na serwerze i dwukrotnie kliknąć opcję Dodaj lub usuń programy. Następnie klikamy ikonę Dodaj/Usuń składniki systemu Windows. W oknie Kreatora składników systemu Windows wyszukujemy Usługi sieciowe. Po zaznaczeniu tej opcji klikamy przycisk Szczegóły, w nowym oknie umieszczamy znacznik w polu Protokół dynamicznej konfiguracji hosta (DHCP) i naciskamy OK. System zainstaluje odpowiednie pliki i zakończy instalację.

Do konfiguracji usługi służy przystawka DHCP. Ponieważ interfejs konsoli przeznaczonych do zarządzania jest zunifikowany, dla tych, którzy poznali już takie narzędzia, jak: Użytkownicy i komputery usługi Active Directory czy chociażby Eksplorator Windows, obsługa przystawki będzie bardzo prosta. Jak zwykle okno jest podzielone na dwa panele: w lewym są zgrupowane obiekty będące odpowiednikami pojemników na informacje, a prawy zawiera szczegółowe dane gromadzone przez te pojemniki. Jeśli na przykład w lewym panelu zaznaczymy obiekt Dzierżawy adresów, w prawym zostanie wyświetlona lista "wynajętych" adresów IP wraz z dodatkowymi informacjami o nazwie komputera, terminie wygaśnięcia dzierżawy itp.

Zgodnie z opisanymi wcześniej sposobami funkcjonowania serwera DHCP, powinniśmy rozpocząć od autoryzacji usługi w Active Directory. W tym celu zaznaczamy w lewym panelu ikonę reprezentującą serwer, a następnie z menu Akcja wybieramy opcję Autoryzuj. Po odświeżeniu obrazu strzałka w ikonie serwera powinna być skierowana ku górze. Następnie wybieramy menu Akcja | Nowy zakres. Nowy zakres tworzymy, używając Kreatora nowych zakresów. W oknie powitalnym kreatora klikamy przycisk Dalej. Najpierw należy podać nazwę zakładanego zakresu. W naszym przykładzie posłużymy się nazwą SiećLokalna. Pole Opis możemy pozostawić puste. Jeśli serwer DHCP będzie obsługiwał więcej zakresów, ich przejrzyste opisywanie przyda się na przykład innym pracownikom działu IT. Po kliknięciu Dalej przechodzimy do konfiguracji zakresu adresów. W polu Początkowy adres IP wprowadzamy np. 192.168.1.10, a w polu Końcowy adres IP: 192.168.1.109.

System automatycznie zaproponuje nam maskę podsieci do tego zakresu. Jeśli nie będzie nam odpowiadała, możemy ją zmodyfikować, wpisując bitową długość maski albo wartość dziesiętną. W przykładowej sieci posługujemy się maską 24-bitową, dlatego możemy zaakceptować propozycję serwera i kliknąć Dalej. Kolejne okno służy do określania ewentualnych wykluczeń. Gdy to konieczne, należy wypełnić pola Początkowy adres IP i Końcowy adres IP. Pomijamy te ustawienia i przechodzimy do ustawień czasu dzierżawy. Nasza testowa sieć obsługuje wyłącznie klienty lokalne, dlatego możemy ustalić miesięczny okres wynajmowania adresów. W polu Dni zmieniamy wartość na 30 i klikamy Dalej. Następnie kreator pyta, czy chcemy skonfigurować dodatkowe opcje serwera. W naszym przykładzie powinniśmy ustawić przekazywanie klientom adresu serwera DNS, więc pozostawiamy zaznaczenie opcji Tak, chcę teraz skonfigurować te opcje i przechodzimy do następnego okna. Określa się w nim adres routera, a ponieważ założyliśmy wcześniej, że sieć ogranicza się do zasobów lokalnych, pole Adres IP pozostawiamy puste. Następne okno służy do konfiguracji parametrów związanych z usługą DNS. W pole Domena nadrzędna wpisujemy nazwę naszej domeny. Tak jak poprzednio, będzie nią pl.idg.com. Oczywiście musimy również wprowadzić adres serwera DNS, w naszym przypadku 192.168.1.1. Klikamy Dodaj i przechodzimy do kolejnego okna.

Służy ono do konfiguracji przekazywania klientom adresu serwera WINS. Ponieważ nie będziemy konfigurować tej usługi, pole adresu pozostawiamy puste i klikamy Dalej. W ostatnim oknie kreatora decydujemy, czy konfigurowany zakres ma zostać uaktywniony. Uaktywnienie zakresu uruchamia obsługę klientów zgłaszających się do serwera i kończy działanie kreatora. Jeśli chcemy zmodyfikować lub do założonego zakresu dodać nowe opcje, należy w lewym panelu rozwinąć zakres, następnie zaznaczyć go i z menu Akcja wybrać polecenie Konfiguruj opcje.

Ostatnią operacją przykładowej konfiguracji będzie dodanie rezerwacji klienta. Załóżmy, że komputer w sekretariacie powinien mieć zawsze przypisany adres 192.168.1.25. Do ustawienia zastrzeżenia będziemy potrzebować fizycznego adresu karty sieciowej tej stacji. Możemy go ustalić na kilka sposobów. Jeśli jesteśmy blisko, wystarczy podejść do komputera i w wierszu polecenia wpisać:

ipconfig /all. Adres MAC będzie wyświetlony w polu Adres fizyczny. Jeśli system pobrał już adres z DHCP, na liście wydzierżawianych adresów znajduje się pole Unikatowy identyfikator, które zawiera fizyczny adres karty sieciowej klienta. Gdy mamy adres MAC, konfiguracja rezerwacji jest prosta. Rozwijamy zakres, następnie zaznaczamy obiekt Zastrzeżenia i wybieramy menu Akcja | Nowe zastrzeżenie. W wyświetlonym oknie wprowadzamy nazwę rezerwacji, np. Sekretariat, dalej wpisujemy adres IP, który będzie zarezerwowany dla tego komputera. Zgodnie z założeniami, jest to 192.168.1.25. W pole adresu MAC wpisujemy adres fizyczny karty sieciowej. Pole Opis jest opcjonalne. Naciśnięcie przycisku Dodaj zatwierdza konfigurację rezerwacji. Na koniec przestawiamy ustawienia TCP/IP klientów na automatyczne pobieranie adresu IP i adresu serwera DNS.

Zadania i działanie DNS

DNS jest usługą zwykle kojarzoną z Internetem. Jej integracja z domenami Windows 2000 i 2003 to dla wielu użytkowników nowość. Głównym zadaniem serwerów DNS jest rozwiązywanie nazw w sieciach pracujących pod kontrolą protokołu TCP/IP. Najczęściej obserwujemy ich działanie w czasie przeglądania witryn internetowych. Jeśli w przeglądarce wprowadzamy nazwę, np. www.pcworld.pl, w celu dotarcia do serwera WWW system musi ją zamienić na adres IP. Jeśli nie będzie mógł tego zrobić, witryna nie zostanie otwarta. Alternatywnym sposobem kojarzenia nazw z adresami IP jest wykorzystanie pliku Hosts. Możemy go odnaleźć w %systemroot%\system32\Drivers\Etc. To zwykły plik tekstowy, który zawiera proste odwzorowanie: adres IP - nazwa, np. "194.69.207.64 www.idg.pl". System najpierw sprawdza, czy określona nazwa znajduje

się w pliku Hosts, a dopiero później korzysta z usług DNS. Różne sposoby rozwiązywania nazw są stosowane dlatego, że o wiele prościej jest posługiwać się nazwami niż ciągami liczb. O wiele łatwiej zapamiętać "www.idg.pl" niż "194.69.207.67". Ponadto w przypadku stosowania usługi DNS o zmianie adresu serwera nie trzeba informować wszystkich stacji klienckich, wystarczy uaktualnić ustawienia DNS.

Działanie usługi DNS polega na odbieraniu zapytań od stacji klienckich w sieci, przetwarzaniu ich i zwracaniu odpowiedzi. Jeśli wprowadzimy dowolną nazwę w przeglądarce, to zanim przejdziemy do określonej witryny, do serwera DNS zostanie wysłana prośba o odnalezienie skojarzonego z nią adresu IP. DNS gromadzi informacje w rekordach, które zawierają nazwę, adres lub inne przydatne dane. Rekordy DNS mogą być różnego typu, np. A, MX, PTR, SRV. W czasie realizacji zapytania oprogramowanie klienta wyszukuje określone adresy, nazwy lub typy rekordów. W zależności od konfiguracji, jeśli serwer nie będzie mógł udzielić odpowiedzi, pytanie przejdzie do innego usługodawcy DNS lub zostanie zwrócony komunikat o nieodnalezieniu rekordu.

W domenach pracujących pod kontrolą Active Directory celem serwerów DNS jest udzielenie odpowiedzi na zapytania o adres IP systemów, które oferują usługi związane z Windows Server 2003. Informacje o usługach są przechowywane w rekordach SRV, dlatego serwer musi je rozpoznawać. Starsze serwery DNS, np. dostarczane razem z Windows NT 4.0, nie obsługują rekordów SRV, dlatego nie nadają się do Active Directory. Usługa ta może korzystać z serwerów DNS pracujących z innymi systemami operacyjnymi, jeśli będą rozpoznawały wymienione rekordy. Zalecane jest posługiwanie się serwerami Windows 2000 lub 2003. W czasie instalacji kontrolera domeny niezbędne wpisy związane z Active Directory są dodawane automatycznie. Nie musimy się więc martwić o właściwe zarządzanie rekordami wykorzystywanymi przez domenę.

Domenowa przestrzeń nazw

Omawiając usługę Active Directory, niejednokrotnie stosowaliśmy określenie "domena", termin ten jest również szeroko wykorzystywany w Internecie. Mimo zbieżności nazwy chodzi o różne zagadnienia. Domena Active Directory to grupa komputerów wskazanych przez administratora sieci, która należy do bazy usług katalogowych i korzysta z niej. Domeny DNS są związane z przestrzenią nazw, do których się odwołujemy, przeglądając strony internetowe. Przestrzeń ta może być również wykorzystywana na potrzeby Active Directory.

W systemie plików mamy do czynienia z katalogiem głównym, podkatalogami i plikami, a w systemie DNS są: korzeń, domeny, poddomeny i rekordy. Główną różnicę stanowi rozproszenie przestrzeni nazw na wiele serwerów. Nazwy DNS biorą swój początek z katalogu głównego, czyli korzenia. Jest reprezentowany przez kropkę na końcu używanej nazwy, np. idg.com. Poniżej znajdują się znane wszystkim domeny wysokiego poziomu, takie jak com, edu, org, net czy pl. Określają kraj lub przeznaczenie przechowywanych przez nie nazw. Na kolejnym poziomie przestrzeni umieszczane są nazwy-domeny - rejestrowane przez firmy, użytkowników lub organizacje, np. pcworld lub computerworld. Domeny mogą mieć swoje poddomeny, te z kolei - swoje poddomeny itd. Dokładnie tak, jak katalogi mogą mieć podkatalogi. W domenach lub poddomenach możemy zakładać rekordy wskazujące na zasoby (hosty). Najczęściej są nimi komputery oferujące określone usługi, takie jak np. ftp. Nazwy domen wysokiego poziomu, domen oraz hostów tworzą nazwy FQDN (w pełni kwalifikowane nazwy domen). Można je porównać do ścieżek dostępu w systemie plików, np. nazwą FQDN jest puchatek.pcworld.pl, oznaczająca, że w domenie wysokiego poziomu (pl) została założona domena pcworld, w której jest host puchatek. Warto zwrócić uwagę, że - w przeciwieństwie do nazw plików - nazwy DNS są odczytywane od końca.

Innym pojęciem ściśle związanym z usługą DNS jest strefa, czyli wydzielony na potrzeby administracyjne fragment przestrzeni nazw. Ich funkcja jest oczywista - trudno sobie

wyobrazić jeden serwer, na którym byłyby nanoszone i modyfikowane wszystkie nazwy. Aby ułatwić zarządzanie i utrzymywanie całej struktury nazw, jej poszczególne części są rozpraszane na wiele serwerów DNS. Jeśli firma jest duża, może mieć własny serwer DNS zajmujący się gromadzeniem informacji związanych z jej zasobami. Domenami mniejszych przedsiębiorstw zajmują się dostawcy internetowi. W czasie instalacji usługi definiujemy jeden z dwóch rodzajów stref. Windows Server 2003 pozwala na założenie strefy wyszukiwania do przodu oraz strefy wyszukiwania wstecznego. Pierwsza jest przeznaczona do odpowiadania na zapytania związane z nazwą. Klient przysyła nazwę, np. www.pcworld.pl, i w odpowiedzi oczekuje adresu IP. Strefy wyszukiwania wstecznego realizują działania odwrotne: w odpowiedzi na otrzymany od klienta adres IP wysyłana jest skojarzona z nim nazwa. Ponieważ DNS to usługa wielopoziomowa i rozproszona, tzn. hierarchia domen jest utrzymywana na wielu serwerach, strefy muszą być ze sobą powiązane. Jeśli klient będzie chciał na przykład rozwiązać nazwę hosta test.idg.pl, a firma IDG ma własny serwer DNS ze strefą obejmującą nazwę idg, najpierw trzeba będzie zapytać jeden z serwerów korzenia o domenę pl, a następnie serwer odpowiedzialny za domenę pl o idg. Aby było to możliwe, serwer DNS przechowujący dane o domenie pl musi zawierać informacje, które pozwolą odesłać stacje klienckie do serwera IDG. Jeśli usługa DNS jest wykorzystywana wyłącznie na potrzeby Active Directory, nie trzeba się łączyć z korzeniem lub serwerami przechowującymi domeny wysokiego poziomu. Na lokalnym serwerze wymagana jest jedynie obecność strefy związanej z własną domeną.

Każdy z rodzajów stref dzielimy również ze względu na dostępność wprowadzania danych i sposób magazynowania informacji. Możemy zakładać takie strefy wyszukiwania do przodu, jak podstawowe, pomocnicze oraz skrótowe. Dodatkowo należy określić, czy strefy te będą przechowywane w plikach tekstowych na serwerze, czy zintegrowane z usługą Active Directory. Decyzja o typie zakładanej strefy zależy od wielu czynników, np. zakresu wykorzystania nazwy (lokalne czy globalne), rodzaju serwerów DNS (tylko Windows Server 2003 czy również Linux), rozmiar sieci (lokalny czy rozległy) itp. W naszym przykładzie należy założyć strefę wyszukiwania do przodu, podstawową, przechowywaną w usłudze Active Directory.

Instalacja i konfiguracja DNS

Przygotowanie DNS do świadczenia usług klientom sieci może być realizowane na dwa sposoby. Najprostszy z nich został już opisany w poprzednich artykułach. Dla przypomnienia: w czasie instalacji kontrolera domeny należy zaznaczyć opcję związaną z instalacją usługi DNS. Jeśli to zrobimy, kreator instalacji Active Directory zainstaluje i skonfiguruje DNS na lokalnym serwerze Windows Server 2003. Sposób ten zalecamy administratorom z mniejszym doświadczeniem. Naturalnie automatyczna instalacja nie przeszkadza w późniejszej zmianie parametrów usługi za pomocą odpowiednich narzędzi.

Ręczna instalacja DNS jest nieco lepszym rozwiązaniem, gdyż pozwala na szczegółową konfigurację wszystkich niezbędnych parametrów usługi. Jeśli DNS jest uruchamiany wyłącznie na potrzeby Active Directory, nie ma zbyt wielu ustawień konfiguracyjnych. Po zainstalowaniu usługi w narzędziach administracyjnych pojawia się skrót do modułu zarządzania serwerem DNS. Narzędzie DNS ma standardowy interfejs administracyjny. W lewym panelu w postaci folderów wyświetlane są serwery i założone w nich strefy. Kliknięcie jednej ze stref wyświetla w prawym panelu założone w niej rekordy. Jeżeli chcemy założyć nową strefę, klikamy prawym przyciskiem folder Strefy wyszukiwania do przodu lub Strefy wyszukiwania wstecznego i wybieramy opcję Nowa strefa. Potem wprowadzamy dane związane z rodzajem strefy oraz jej parametrami. Innym, łatwiejszym sposobem ustawienia serwera DNS jest skorzystanie z kreatora. Uruchamiamy go, klikając prawym przyciskiem ikonę serwera, następnie wybieramy opcję Konfiguruj serwer DNS.

Tworząc strefę związaną z nazwą domeny Active Directory, przygotowaliśmy swego rodzaju pojemnik do przechowywania właściwych rekordów DNS. Żeby usługa była w pełni funkcjonalna należy w domenie umieścić odpowiednie rekordy. Informacje w nich zawarte są wykorzystywane do lokalizacji właściwych zasobów. W niewielkich sieciach pracujących pod kontrolą Windows Server 2003 najlepiej zastosować automatyczne wprowadzanie rekordów do DNS. W tym celu musimy odpowiednio przygotować zarówno serwer, jak i stacje klienckie w sieci. Konfiguracja serwera jest stosunkowo łatwa. Po pierwsze, trzeba sprawdzić, czy w parametrze TCP/IP - Użyj następujących adresów serwerów DNS - jest wprowadzony lokalny adres IP. Jeśli tak, sprawdzamy z kolei, czy we właściwościach strefy wyszukiwania do przodu, związanej z naszą domeną, jest włączona aktualizacja dynamiczna. Odpowiednią listę rozwijaną znajdziemy na karcie Ogólne (np. właściwości strefy pl.idg.com). W przypadku stref zintegrowanych z Active Directory dostępne są trzy opcje: Brak, Niezabezpieczone i zabezpieczone oraz Tylko zabezpieczone. Zalecane jest wybranie ostatniej opcji.

Jeżeli w sieci nie ma innych klientów niż systemy Windows XP, możemy przejść do weryfikacji ustawień stacji roboczych. Ponieważ podczas instalacji komponentów sieciowych Windows automatycznie konfigurowany jest protokół TCP/IP z opcją Zarejestruj adresy tego połączenia w DNS, nasze zadanie polega jedynie na sprawdzeniu, czy opcja ta jest włączona. Prowadzi do niej następująca ścieżka Start | Panel sterowania | Połączenia sieciowe | Właściwości interfejsu sieciowego | Protokół internetowy TCP/IP | Właściwości | Zaawansowane | Karta DNS. Jeśli wszystkie wspomniane wyżej opcje są skonfigurowane, klienty będą dynamicznie rejestrowały swoje nazwy w usłudze DNS.

Jednym z ważniejszych zadań serwera DNS jest dostarczanie informacji o kontrolerach domeny. Potrzebne w tym celu rekordy są automatycznie dodawane do strefy. Za te czynności odpowiada usługa Logowanie do sieci (Netlogon). Administrator nie musi dodawać żadnych wpisów ręcznie.

Przykładowa konfiguracja DNS na potrzeby Active Directory

W celu dodania DNS do usług uruchomionych w Windows Server 2003 należy kliknąć Panel sterowania | Dodaj/Usuń programy | Dodaj/Usuń składniki systemu Windows | Usługi sieciowe | Szczegóły. W nowym oknie zaznaczamy System DNS (Domain Name System) i wybieramy OK. Kliknięcie przycisku Dalej powoduje instalację usługi, a naciśnięcie Zakończ zamyka kreator.

Najprostszym i najszybszym sposobem konfiguracji usługi DNS jest wykorzystanie kreatora. Uruchamiamy dostępną w narzędziach administracyjnych przystawkę DNS, zaznaczamy ikonę serwera IDGTEST i klikamy prawym przyciskiem myszy. Z listy wybieramy opcję Konfiguruj serwer DNS. Po uruchomieniu kreatora klikamy Dalej. W oknie Wybierz akcję konfiguracji zaznaczamy Utwórz strefę wyszukiwania do przodu (zalecane w małych sieciach) | Dalej. W następnym oknie pozostawiamy zaznaczone Ten serwer przechowuje strefę. Po naciśnięciu Dalej wpisujemy nazwę strefy. Nasza przykładowa sieć powinna mieć założoną taką strefę, jak nazwa domeny, czyli pl.idg.com. Następne okno służy do konfiguracji typu aktualizacji dynamicznych tu również pozostawiamy zaznaczoną opcję Zezwalaj tylko na zabezpieczone aktualizacje dynamiczne. Ponieważ serwer ma być wykorzystywany jedynie w małej sieci lokalnej, bez połączeń zewnętrznych, w oknie Usługi przesyłania dalej należy zaznaczyć opcję Nie, nie powinien przesyłać kwerend dalej. Naciśnięcie przycisku Zakończ sprawia, że serwer DNS może realizować zapytania klientów sieci.

Konfiguracja klientów sieci

Jeśli serwer został należycie przygotowany do swojej roli, możemy przejść do konfiguracji klientów sieci. Najpierw warto poświęcić kilka chwil na rozstrzygnięcie, który z systemów operacyjnych najlepiej nadaje się do pracy z Windows Server 2003. W niewielkiej sieci, w

której komputery mają już zainstalowane oprogramowanie, często spotykamy wiele wersji systemów operacyjnych. Niejednorodność środowiska sprawia, że administrator musi na konfigurację i zarządzanie systemami klienckimi poświęcić nieco więcej czasu. Optymalne środowisko pracy to takie, w którym wszystkie komputery sieciowe działają pod kontrolą takiego samego systemu operacyjnego, nawet jeśli będzie to starszy Windows 98 SE. Eliminuje to wiele problemów, związanych np. z automatyzacją ustawień dotyczących stacji roboczych.

Jeżeli sieć powstaje od podstaw i możemy określić, jakie oprogramowanie będzie potrzebne, bezwzględnie należy wybrać jeden z nowszych systemów operacyjnych: Windows XP Professional albo Windows 2000 Professional. To bardzo uprości administrowanie siecią. Dodatkowo będziemy mogli w pełni wykorzystać wszystkie zalety Windows Server 2003, takie jak Zasady grupy lub IPSec.

Naszymi przykładowymi stacjami będą komputery z zainstalowanym systemem Windows XP Professional. Warto pamiętać, że Windows XP Home nie jest przeznaczony do pracy w sieciach, bo nie oferuje wielu istotnych w takich środowiskach funkcji. System XP Home na przykład niełatwo dodać do domeny Active Directory.

Możliwość współpracy systemu z innymi komputerami w domenie zależy od prawidłowego skonfigurowania ustawień komunikacyjnych. Ponieważ w Windows XP Professional określanie ustawień sieciowych nie różni się od tego, co oferuje Windows Server 2003, poprawne nadanie parametrów jest proste. Dodatkowo XP automatycznie wykrywa karty sieciowe i uruchamia połączenia lokalne, zatem jeśli nie ma kłopotów ze sterownikiem, konfiguracja może polegać tylko na weryfikacji ustawień. Na początku artykułu omówiliśmy konfigurację odpowiednich parametrów TCP/IP w Windows Server 2003. W wypadku Windows XP ustawienia są identyczne. Po wybraniu właściwości TCP/IP sprawdzamy, czy opcja automatycznego pobierania adresu z serwera DHCP jest zaznaczona.

Praca stacji w domenie

Zanim rozpoczniemy pracę w domenie, musimy się do niej "zapisać". W przypadku systemu Windows XP Professional "zapisanie" polega na założeniu w bazie Active Directory konta komputera sieciowego oraz skonfigurowaniu w Windows XP przynależności do domeny. Operacje te mogą być wykonywane oddzielnie lub - co jest nieco wygodniejsze - łącznie z poziomu stacji roboczej.

Dodawanie komputera do domeny można przeprowadzić na kilka sposobów. Jeśli instalujemy system Windows XP na stacji roboczej, już w czasie konfiguracji możemy "zapisać" komputer do domeny. Jeśli Windows jest już zainstalowany, należy skorzystać z karty Nazwa komputera, dostępnej po dwukrotnym kliknięciu ikony System w Panelu sterowania. Na tej karcie są dwa przyciski: Identyfikator sieciowy i Zmień. Służą do konfigurowania podobnych ustawień systemu, ale są między nimi drobne różnice. Kliknięcie przycisku Identyfikator sieciowy powoduje uruchomienie kreatora przypisującego komputer do domeny oraz konfigurującego ustawienia kont domenowych w lokalnej bazie użytkowników. W oknie wyświetlonym po naciśnięciu przycisku Zmień można zmienić nazwę komputera, sufiks domeny DNS oraz przynależność do grupy roboczej lub domeny.

Zakładając konto komputera oddzielnie, możemy określić lokalizację konta w odpowiednim pojemniku bazy Active Directory. Ma to duże znaczenie, jeśli chcemy korzystać z zalet konfiguracji Zasad grup, pozwalających na automatyczne przekazywanie ustawień komputera w zależności od pojemnika, w którym znajduje się jego konto. Na przykład inne ustawienia mogą przejść z serwera na stacje założone w jednostce organizacyjnej NetWorld, niż na te, które umieścimy w PCWorld. Jeśli będziemy łącznie dodawać konto i "zapisywać" komputer do domeny, system automatycznie

umieści konto stacji w jednostce organizacyjnej Computers. Ponieważ jest to pojemnik wbudowany, nie możemy przypisać mu ustawień Zasad grupy. Oczywiście nic nie stoi na przeszkodzie, żeby korzystając z opcji Przenieś, umieścić konto w innym pojemniku, ale wymaga to dodatkowych czynności. Zanim zaczniemy konfigurować środowisko robocze dla stacji, powinniśmy wybrać najwygodniejszy sposób postępowania.

Aby uniknąć przykrych niespodzianek, przed fizycznym dodaniem stacji do domeny należy zapoznać się z zagadnieniami związanymi z bezpieczeństwem. Dodawanie komputerów do Active Directory oraz zmiana lokalnych ustawień Windows XP jest możliwa wtedy, gdy mamy odpowiednie uprawnienia. Dostęp do karty Nazwa komputera w Windows XP jest ograniczony do kont należących do lokalnej grupy Administratorzy. Pracując na innym koncie, należy skorzystać z opcji Uruchom jako. Aktywujemy ją, zaznaczając ikonę System i naciskając klawisz [Shift] oraz prawy przycisk myszy. Podajemy nazwę i hasło konta z grupy Administratorzy. W czasie dodawania komputera do domeny system łączy się z Windows Server 2003 i wprowadza konto do bazy Active Directory. Domyślne ustawienia serwera pozwalają na wykonanie tych czynności użytkownikom będącym członkami domeny. Zanim konto zostanie dodane, należy podać właściwą nazwę konta, hasło oraz nazwę domeny. Każdy uwierzytelniony użytkownik domeny może założyć do dziesięciu kont komputerów. Ograniczenie to nie jest, oczywiście, związane z kontem administratora Windows Server 2003.

Przykładowa konfiguracja klientów sieciowych

Konfigurację stacji roboczej rozpoczynamy od weryfikacji poprawności parametrów interfejsu sieciowego. W tym celu należy się zalogować na koncie z uprawnieniami administracyjnymi i wybrać Panel sterowania | Połączenia sieciowe | Połączenie lokalne | Właściwości. Ustawienia interfejsu powinny obejmować następujące usługi: Klient sieci Microsoft, Udostępnianie plików i drukarek oraz Protokół internetowy TCP/IP. Udostępnianie plików i drukarek jest potrzebne, jeśli dana stacja robocza będzie oferowała swoje zasoby innym klientom sieci, czyli na przykład wtedy, gdy z lokalnej drukarki korzystają inni pracownicy firmy. Do współpracy z systemem Windows Server 2003 potrzebujemy protokołu i klienta sieci.

W naszej przykładowo konfigurowanej sieci do zarządzania adresami IP służy serwer DHCP, dlatego we właściwościach tego protokołu powinna być zaznaczona opcja Uzyskaj adres IP automatycznie. Automatycznie powinien być również pobierany adres serwera DNS. Jeśli obie opcje są zaznaczone, ustawienia interfejsu sieciowego można uznać za poprawne.

Następnie do domeny należy dodać komputer. W tym celu możemy uruchomić Kreator identyfikacji sieciowej lub skorzystać z przycisku Zmień. Obie opcje odnajdziemy po wybraniu System panelu sterowania | Nazwa komputera. Wydajniejszym rozwiązaniem jest skorzystanie z przycisku Zmień, ale jeśli ktoś woli łatwiejsze sposoby konfiguracji, może się posłużyć kreatorem. Po naciśnięciu przycisku Zmień, w oknie Zmiana nazwy komputera przenosimy znacznik z opcji Grupa robocza na Domena i wprowadzamy nazwę domeny zgodną ze standardem DNS. W naszym przypadku będzie to PL.IDG.COM. Naciśnięcie przycisku OK sprawia, że stacja kontaktuje się z serwerem DNS w celu uzyskania listy adresów IP kontrolerów domeny. Po udanym odnalezieniu serwera Windows Server 2003 nasza stacja jest dodawana do domeny. Przed zakończeniem operacji trzeba jeszcze w oknie Zmiana nazwy komputera podać właściwy identyfikator i hasło użytkownika domeny.

O powodzeniu tej operacji informuje komunikat "Witamy w domenie pl.idg.com". Aby wszystkie ustawienia działały poprawnie, należy zrestartować Windows XP. Po ponownym uruchomieniu użytkownicy stacji roboczej będą się już logowali do domeny pl.igd.com.

Testowanie komunikacji i pracy w domenie

Konfiguracja Windows Server 2003 i stacji roboczych jest niezbyt skomplikowana, ale zdarzają się pewne problemy. Jeśli wystąpią błędy, trzeba umieć szybko zlokalizować miejsce awarii oraz usunąć ją. Zacznijmy od eliminacji tych problemów, które występują najczęściej, czyli błędów komunikacyjnych.

Jeśli zawiedzie komunikacja, przekonamy się o tym bardzo szybko. Nie będziemy się mogli podłączyć do serwera sieciowego, wydrukować dokumentu na drukarce sieciowej czy wysłać poczty. Ustalanie źródła błędu należy zacząć od sprawdzenia działania fizycznej części sieci. Najczęściej nie trzeba śledzić ciągłości kabla lub czołgać się pod biurkiem. Do wyciągnięcia kilku istotnych wniosków na temat sieci wystarczy zaznaczyć pole wyboru opcji Pokaż ikonę w obszarze powiadomień podczas połączenia, dostępnej we właściwościach interfejsów sieciowych zarówno Windows Server 2003, jak i stacji pracującej pod kontrolą XP. Po zaznaczeniu tej opcji w obszarze powiadomień pojawi się ikona sygnalizująca obecność lub przerwanie połączenia. Jej dwukrotne kliknięcie pozwala na uzyskanie informacji o właściwościach i aktywności połączenia. Jeśli zawiedzie okablowanie lub urządzenie aktywne, poinformuje nas o tym zmiana w wyglądzie ikony oraz odpowiedni komunikat.

Z reguły w celu usunięcia awarii wystarczy sprawdzić, czy nie wysunął się kabel z karty sieciowej lub czy działa koncentrator względnie przełącznik. Jeśli to nie wystarczy, trzeba sprawdzić, czy kabel nie jest uszkodzony.

Jeśli ikona informująca o stanie interfejsu nie sygnalizuje błędów, należy przejść do weryfikacji konfiguracji stacji lub serwera. Łatwo da się ustalić, czy mamy kłopoty z serwerem, czy z komputerem lokalnym. Jeżeli inne stacje również nie mogą się podłączyć do plików serwera, z dużym prawdopodobieństwem awaria dotknęła Windows Server 2003. W innym przypadku mamy problemy z Windows XP. Do testowania konfiguracji służy pokaźna grupa narzędzi, zarówno tekstowych, jak okienkowych. W podstawowej diagnostyce systemu wystarczy zastosowanie trzech narzędzi wiersza poleceń: IPCONFIG, PING oraz NSLOOKUP. Każde z nich może być wykorzystane do weryfikacji poprawności działania poszczególnych usług.

Wyszukiwanie błędów rozpoczynamy od polecenia, które może natychmiast zdiagnozować poprawność pracy. Jeśli zastosujemy ping, będziemy mogli od razu wyeliminować dużą część potencjalnych źródeł błędów. Gdy rezultatem polecenia z parametrem w postaci nazwy Windows Server 2003 będzie odpowiedź systemu, wówczas wiemy, że poprawnie działa usługa DHCP oraz DNS. Jeżeli w odpowiedzi otrzymamy na przykład komunikat "Upłynął limit czasu żądania" lub "Żądanie polecenia Ping nie może odnaleźć hosta idgtest.pl.idg.com. Sprawdź nazwę i ponów próbę.", nasze dalsze czynności mogą iść w różnych kierunkach. Najczęściej źródłem kłopotów jest konfiguracja adresowania lub problemy z rozwiązywaniem nazw.

Polecenie IPCONFIG służy do sprawdzania lokalnych ustawień adresowania TCP/IP. Jest przydatne do określenia, czy kłopoty wynikają z nieprawidłowego działania sieci, czy serwera DHCP. Po wpisaniu w wierszu poleceń IPCONFIG /ALL otrzymamy informacje o bieżących ustawieniach adresowania. W czasie rozwiązywania problemów najcenniejszymi danymi zwróconymi przez IPCONFIG są: DHCP włączone, Adres IP oraz Serwery DNS. Ponieważ zdecydowaliśmy się na automatyczną dystrybucję adresów IP, parametr DHCP powinien wyświetlać Tak. Jeśli jest inaczej trzeba, przejść do właściwości protokołu TCP/IP interfejsu sieciowego i zmienić jego konfigurację. Pole Adres IP powinno zawierać adres z zakresu zdefiniowanego w Windows Server 2003. Gdy ten warunek nie jest spełniony, należy sprawdzić, czy działa DHCP, sieć lub czy nie pojawił się "obcy" serwer DHCP. Może tak być na przykład po włączeniu usługi udostępniania połączenia internetowego. Ostatnie wskazane pole - Serwery DNS - w naszym przypadku powinno zawierać adres IP Windows Server 2003. Jeśli wartość tego pola jest inna, powinniśmy sprawdzić konfigurację opcji serwera DHCP.

Do testowania funkcjonowania serwera DNS służy polecenie NSLOOKUP. Nam będzie potrzebne do sprawdzenia, czy możemy się połączyć z usługodawcą DNS i czy serwer ten zawiera rekordy potrzebne do prawidłowego funkcjonowania sieci. NSLOOKUP może działać w dwóch trybach: interaktywnym i wsadowym. Tryb interaktywny uzyskujemy po wprowadzeniu nazwy polecenia i naciśnięciu klawisza [Enter]. Powoduje to przejście do powłoki NSLOOKUP, w której możemy wydawać najróżniejsze polecenia. Lista poleceń jest dostępna po wpisaniu ? i naciśnięciu klawisza [Enter]. Tryb wsadowy polega na wpisaniu NSLOOLUP z odpowiednim parametrem i wystarcza do weryfikacji komunikacji z lokalnym serwerem DNS. Jeśli wpiszemy NSLOOKUP idgtest.pl.idg.com i otrzymamy odpowiedź, będzie to oznaczało poprawną pracę DNS. Podobnie możemy postąpić, sprawdzając, czy system jest w stanie odpowiedzieć na pytania o rekordy SRV.

Po wyeliminowaniu z grupy wadliwie działających konfiguracji protokołu TCP/IP, usługi DHCP i DNS, należy rozpocząć inne testy. Jeśli na podstawie komunikatów systemu ustalimy, że kłopot nie polega na błędnym skonfigurowaniu uprawnień, trzeba dokładnie przejrzeć dzienniki w poszukiwaniu innych źródeł problemów. Warto również pamiętać, że pomoc Windows Server 2003 zawiera serię przydatnych przewodników, wspomagających testowanie ustawień systemu.

W serwerach sieciowych duże znaczenie ma wygoda klientów sieci. Nie mniej ważne jest sprawne zarządzanie systemem. Do realizacji tego zamierzenia niezbędna jest grupa narzędzi o szerokich możliwościach i przejrzystym interfejsie. Po bliższym poznaniu Windows Server 2003 wydaje się, że administrowanie systemem to całkiem przyjemne zadanie.

Jednym z celów, jaki sobie stawiają twórcy kolejnych wersji oprogramowania, jest zwiększenie komfortu pracy użytkowników. Przekonajmy się, czy narzędzia dostarczone z Windows Server 2003 są przydatne do sprawnego zarządzania i monitorowania działań systemu i użytkowników.

Dla każdego coś miłego

Microsoft przyzwyczaił użytkowników Windows do administrowania z wykorzystaniem narzędzi okienkowych. Standardowo, w celu zmiany konfiguracji systemu, należy skorzystać z odpowiedniego narzędzia i wybrać kilka opcji. Wraz z pojawieniem się Windows 2000 znacznie zwiększyły się możliwości zarządzania za pomocą programów wiersza poleceń. W Windows Server 2003 wprawny administrator wykona w ten sposób prawie wszystko. Dodatkowo dzięki możliwościom języków skryptowych, automatyzacja często wykonywanych czynności nie jest niczym skomplikowanym.

Zwiększenie liczby narzędzi tekstowych nie zmniejsza znaczenia podstawowego środowiska zarządzania systemem, czyli konsoli MMC oraz jej przystawek. W starszych systemach operacyjnych konfiguracja Windows była wykonywana przy użyciu programów stanowiących oddzielne narzędzia administracyjne. Na przykład w celu zarządzania kontami użytkowników i grup w domenach Windows NT należało uruchomić program usrmgr.exe. Począwszy od Windows 2000, głównym sposobem modyfikacji konfiguracji

systemu stało się uruchomianie przystawek konsoli MMC. Warto pamiętać, że w tym wypadku mechanizm zarządzania wykorzystuje dwa elementy. Pierwszy to przystawka, która służy do zmiany ustawień poszczególnych komponentów systemu. Są oddzielne przystawki do zarządzania zasadami grup, lokacjami i usługami Active Directory itp. Drugim elementem jest konsola MMC. Stanowi ona środowisko, w którym uruchamiane są napisane przez programistów przystawki. Bez nich konsola jest bezużyteczna. Wprowadzone przez Microsoft rozszerzenia sposobu zarządzania oferują wiele korzyści, m.in. elastyczność, łatwość modyfikacji, prostą dystrybucję oraz możliwość tworzenia uproszczonych konsoli, przeznaczonych dla mniej zaawansowanych użytkowników. Firmy oferujące oprogramowanie do systemów okienkowych mogą dostarczać własne przystawki do zarządzania aplikacjami.

Administratorzy systemu Windows Server 2003, którzy chcą pracować zdalnie lub zautomatyzować często wykonywane czynności, znajdą dla siebie wiele przydatnych funkcji. Do zdalnego zarządzania można wykorzystać usługi zdalnego pulpitu. Ich konfiguracja nie jest niczym kłopotliwym. Jeżeli nie odpowiada nam tryb graficzny, możemy wykorzystać narzędzia wiersza poleceń. Na przykład grupa poleceń rozpoczynających się od ds*.*, np. Dsadd, Dsmod czy Dsrm, służy do administracji Active Directory. Oczywiście, narzędzia te z powodzeniem mogą być wykorzystywane do tworzenia skryptów. W efekcie powtarzanie takich samych czynności w odniesieniu do wielu serwerów może zostać bardzo uproszczone.

Wykorzystanie konsoli MMC

Konsola MMC pełni funkcję interfejsu przystawek służących do zarządzania systemem. Po zainstalowaniu Windows Server 2003 w grupie narzędzi administracyjnych znajdują się skróty do najczęściej wykorzystywanych przystawek. Dodatkowo po skonfigurowaniu jednej z dostępnych ról serwera, kreator przygotowuje konsole zarządzania wybranymi rolami - tak jest na przykład po dodaniu roli serwera plików. W folderze narzędzi administracyjnych pojawia się konsola Zarządzanie serwerem plików. Interfejs większości oferowanych przystawek podzielony jest na trzy części. Pierwsza z nich to pasek menu oraz pasek narzędzi. Poniżej obu pasków są dwa panele. Lewy przedstawia widok folderów, a prawy - szczegóły związane z zaznaczonym obiektem. Klasycznym przykładem konsoli zawierającej takie przystawki jest Zarządzanie serwerem plików.

Automatyczne przygotowanie przez Kreator konfiguracji ról odpowiednich przystawek ułatwia zarządzanie serwerem. Jeśli jednak efekty działań kreatora nie są satysfakcjonujące, możemy zbudować własną konsolę, zawierającą potrzebne przystawki. W tym celu należy uruchomić konsolę MMC, wywołując polecenie Uruchom i wpisując mmc. Po naciśnięciu OK jest wyświetlana pusta konsola.

W celu przyłączenia nowej przystawki, z menu Plik wybieramy polecenie Dodaj/Usuń przystawkę. Podobny efekt przyniesie naciśnięcie kombinacji klawiszy [Ctrl M]. W nowym oknie klikamy Dodaj i z listy przystawek wybieramy te, które nam odpowiadają.

Uwaga! Jeśli chcemy, żeby lista zawierała wszystkie przystawki związane z administracją Windows Server 2003, należy zainstalować na serwerze pakiet narzędzi administracyjnych - Adminpak.msi. Odnajdziemy go w folderze I386 płyty instalacyjnej systemu.

W czasie dodawania przystawki możemy określić jej dodatkowe parametry. Najczęściej dotyczą wyświetlanych komponentów lub komputera, którym chcemy zarządzać. Zaletą stosowania konsoli MMC jest to, że w pojedynczej możemy umieścić grupę przystawek do administrowania tymi samymi komponentami systemu różnych stacji sieciowych. Naciśnięcie przycisku Zakończ zamyka właściwości dodawanej przystawki. Okno z listą elementów nie jest zamykane. Jeśli trzeba, możemy umieszczać w konsoli następne przystawki. Wybór przycisku Zamknij, a następnie OK kończy dodawanie obiektów.

Ponieważ przystawki nie muszą być rozmieszczane jedna pod drugą, możemy zbudować podobną do struktury folderów na dysku, kaskadową hierarchię obiektów.

Umieszczanie grup przydatnych przystawek w jednej konsoli nie jest jedyną zaletą MMC. W miarę potrzeb administrator może kształtować jej wygląd. Oprócz standardowych modyfikacji związanych z wyświetlaniem lub ukrywaniem poszczególnych pasków jest opcja pozwalająca na tworzenie tzw. widoków bloków zadań. Widok bloku zadań to przystawka tak przekształcona, że korzystający z niej mogą wykonywać czynności konfiguracyjne w uproszczony sposób. Tworzenie bloków zadań przydaje się, jeśli chcemy powierzyć część zadań związanych z administracją komponentami systemu tym użytkownikom, którzy nie mają dużego doświadczenia w zarządzaniu Windows. Prosty blok zadań może zawierać dokładnie opisane ikony będące wyzwalaczami pojedynczych funkcji lub poleceń. Zamiast standardowego widoku przystawki z wszystkim obiektami, opcjami, parametrami, użytkownik będzie widział tylko te elementy, które chcemy mu pokazać. Dodatkowo możemy ograniczyć liczbę operacji, które będą wykonywane na wyświetlonych obiektach. W czasie zapisywania przygotowanej konsoli MMC określamy tryb jej uruchamiania. Są cztery tryby uruchamiania: autorski, użytkownika z pełnym dostępem, użytkownika z ograniczonym dostępem z możliwością wyświetlania wielu okien i użytkownika z ograniczonym dostępem z możliwością wyświetlania jednego okna. Administrator, któremu dostarczymy konsolę, będzie mógł ją uruchomić w wybranym przez nas trybie. Jeśli nie będzie to tryb autora, wówczas wprowadzanie modyfikacji do konsoli jest zabronione. Tryb autorski wywołujemy, stosując przełącznik /a podczas uruchamiania konsoli z wiersza poleceń lub wybierając z menu podręcznego konsoli opcję Autor. Warto pamiętać, że ograniczenia te nie zapewniają skutecznego zabezpieczania konsoli przed modyfikacją. Dopiero odpowiednie zmiany ustawień profilu użytkownika lub właściwa konfiguracja Zasad grupy, sprawiają, że użytkownicy nie mogą modyfikować konsoli.

Przykładowa konfiguracja widoku bloku zadań przystawki

Jednym z najbardziej obrazowych przykładów tworzenia bloku zadań konsoli MMC jest wykorzystanie przystawki Usługi. Na początek należy uruchomić konsolę MMC. W tym celu klikamy przycisk Start, następnie wybieramy Uruchom i wpisujemy mmc. Po naciśnięciu OK uruchomi się pusta konsola. Następną czynnością jest dodanie przystawki Usługi. Z menu Plik wybieramy Dodaj/Usuń przystawkę. W nowym oknie klikamy Dodaj i na liście przystawek odnajdujemy Usługi. Ostatnim parametrem jest określenie komputera, którego usługami ma zarządzać przystawka. W naszym przypadku można pozostawić domyślną opcję - Komputer lokalny. Klikanie po kolei Zakończ | Zamknij | OK sprawia, że właściwa przystawka jest pomyślnie dodana. Warto zaznaczyć, że nic nie stoi na przeszkodzie, aby w większych sieciach zbudować sobie przystawkę do zarządzania usługami z kilku serwerów lub stacji roboczych.

Jeśli udało się dodać nową przystawkę, możemy przejść do konfiguracji widoku bloku zadań. W tym celu należy w lewym panelu zaznaczyć folder Usługi i wybrać menu Akcja | Nowy widok bloku zadań. W Kreatorze nowego widoku klikamy Dalej i przechodzimy do okna służącego do określenia, jak system ma wyświetlać tworzony przez nas blok. Tutaj możemy wybrać styl okienka szczegółów oraz styl opisu zadań. Dla usług odpowiedni będzie styl Lista pionowa lub Lista pozioma. Ponieważ okno usług zawiera wiele kolumn, Lista pozioma wydaje się lepszym rozwiązaniem. W celu ułatwienia posługiwania się widokiem podczas konfiguracji stylu opisu zadań wybieramy opcję Porada, a z listy rozmiaru opcję Duża. Kliknięcie Dalej otwiera kolejne okno kreatora, w którym wskazujemy, do jakich elementów drzewa przystawki (w lewym panelu) będzie się odnosił tworzony widok. Jeśli zaznaczymy Wybrany element drzewa, wówczas blok zadań wpłynie tylko na przystawkę Usługi. Jeżeli konsola zawierałaby przystawki do zarządzania usługami z kilku komputerów, należałoby zaznaczyć opcję Wszystkie elementy drzewa, będące tego samego typu co wybrany element drzewa. Zastosowanie tej opcji sprawi, że

ominie nas żmudne powtarzanie konfiguracji wielu przystawek. Nadanie nazwy i opisu kończy pierwszą część budowy bloku zadań.

Okno wieńczące pracę Kreatora nowego widoku zawiera opcję Uruchom Kreatora nowego zadania. Nowy kreator służy to tworzenia zadań - ilustrowanych ikonami i opisami - dla użytkowników. W powitalnym oknie Kreatora nowego zadania klikamy Dalej i przechodzimy do wyboru rodzaju poleceń. Okno Typ polecenia zawiera trzy opcje: Polecenie menu, Polecenie powłoki oraz Nawigacja. Jeśli pierwszą pozostawimy wybraną, po kliknięciu Dalej zobaczymy listę obiektów oraz poleceń. W przypadku wybranej przez nas przystawki Usługi, będzie to lista usług systemowych (Aktualizowanie automatyczne, Alertowanie itd.) oraz grupa poleceń związanych z serwisami (Uruchom, Zatrzymaj itd.). Zaznaczmy Uruchom | Dalej. Okno Nazwa i opis służy do wprowadzenia wyświetlanej użytkownikowi informacji o obiekcie. System sam podpowiada tekst związany z poleceniem i jego opisem. Jeśli nie chcemy niczego modyfikować, możemy nacisnąć Dalej. W przedostatnim oknie kreatora wybieramy ikonę, która ma ilustrować zadanie. Ponieważ wybraliśmy polecenie Uruchom, najbardziej odpowiednia do naszych celów będzie ikona Otwórz. Po jej odnalezieniu na liście ikon klikamy Dalej.

Okno kończące działanie kreatora zawiera opcję Uruchom tego kreatora ponownie. Jeśli chcemy wprowadzić kolejne polecenia, np. Zatrzymaj, Uruchom ponownie, powinniśmy ją zaznaczyć i nacisnąć Zakończ. Po wyborze wszystkich niezbędnych zadań z menu Plik wybieramy Opcje i przełączamy tryb konsoli na Tryb użytkownika - ograniczony dostęp, jedno okno. Następnie wybieramy menu Widok | Dostosuj i usuwamy wszystkie zaznaczenia. Na koniec zapisujemy konsolę (Plik | Zapisz jako). Tak przygotowany widok bloku zadań możemy dystrybuować do użytkowników.

Obszary zarządzania systemem

Administrator Windows Server 2003 odpowiada za poprawną i bezawaryjną pracę serwera. Jego codzienne działania opierają się przede wszystkim na kontrolowaniu funkcjonowania, wykonywaniu kopii bezpieczeństwa oraz rozwiązywaniu bieżących problemów użytkowników. Jeśli system jest w pełni wdrożony, takie czynności, jak zakładanie kont, konfiguracja sprzętu, oprogramowania, wykonuje się sporadycznie.

Warto pamiętać, że zarządzanie systemem jest ściśle związane z pełnionymi przez serwer funkcjami. Administrowanie serwerem poczty, zdalnego dostępu, plików czy baz danych będzie wymagało nadzorowania i konfigurowania innych komponentów Windows Server 2003. Nie bez znaczenia pozostaje również środowisko pracy. Administratorzy systemów wielodomenowych będą skazani na rozwiązywanie problemów dotyczących np. replikacji oraz funkcjonowania Active Directory. Jeśli pod naszą opieką będzie nieduża sieć biurowa, ustawienia usług katalogowych najczęściej ograniczą się do zarządzania użytkownikami oraz uprawnieniami i nie musimy się martwić o działanie replikacji. Więcej informacji na temat administrowania usługą Active Directory przedstawimy w artykule poświęconym Zasadom grupy. W dalszej części będziemy się koncentrowali na standardowych komponentach wykorzystywanych do śledzenia działania Windows Server 2003.

Monitorowanie działania systemu

Serwer sieciowy jest komputerem z którego zasobów korzysta wielu użytkowników lokalnych lub klientów przedsiębiorstwa. Awarie oraz spadki wydajności głównego komputera firmy mogą mieć istotne znaczenie dla całej organizacji. Administrator Windows Server 2003 powinien wiedzieć, w jakim stanie jest jego ulubiona maszyna, czy pracuje poprawnie i czy nie wymaga szybkiej renowacji. System oferuje wiele narzędzi do badania bieżącej sprawności - jednym z najważniejszych jest Podgląd zdarzeń.

Przystawkę Podgląd zdarzeń lub jej pojedyncze dzienniki możemy odnaleźć w wielu narzędziach administracyjnych. Jeśli uruchamiamy Zarządzanie komputerem albo przystawkę DNS, znajdujemy dzienniki informujące o działaniu Windows. Jeśli coś idzie nie tak, informacje o wystąpieniu problemu zostaną umieszczone w Podglądzie zdarzeń. Warto pamiętać, że od tego narzędzia powinniśmy rozpoczynać obserwację funkcjonowania serwera.

Jeśli musimy skorzystać z innych metod monitorowania i diagnozowania Windows Server 2003, możemy się posłużyć na przykład Menedżerem zadań, Diagnostyką sieci, przystawką Wydajność lub Monitorem sieci. Znaczna grupa narzędzi oferuje dodatkowe mechanizmy przenoszenia informacji o swoim działaniu do plików tekstowych. Wśród nich możemy wymienić np. DNS, DHCP, Routing i dostęp zdalny lub popularną Zaporę połączenia internetowego. Informacje zapisywane do plików tekstowych są z reguły o wiele bardziej szczegółowe.

Podgląd zdarzeń

Podgląd zdarzeń jest narzędziem, do którego uruchomione aplikacje oraz Windows Server 2003 przesyłają informacje o działaniu systemu. W celu ułatwienia nawigacji zdarzenia są zapisywane w różnych dziennikach. Typ informacji wyznacza miejsce zapisu. Jeśli na przykład wystąpi zdarzenie związane z próbą nieuprawnionego dostępu do systemu, zostanie ono wpisane do dziennika Zabezpieczenia. W zależności od tego, jakie komponenty są zainstalowane lub jaką funkcję pełni serwer, w Podglądzie zdarzeń można odnaleźć inną liczbę dzienników. Trzy z nich są zawsze: Aplikacje, System i Zabezpieczenia. Pozostałe trzy: Serwer DNS, Usługa katalogowa i Usługa replikacji plików, występują wtedy, gdy mamy zainstalowany serwer DNS oraz gdy system jest kontrolerem domeny.

Dla administratorów jednym z najważniejszych dzienników jest System. Gromadzone w nim dane obejmują wydarzenia odnoszące się do funkcjonowania Windows Server 2003. Jeżeli w czasie uruchamiania systemu wystąpi błąd lub zdarzenie, które może spowodować potencjalną niestabilność pracy, informacje o nim są umieszczane właśnie w dzienniku System. Kolejnym ważnym dziennikiem są Zabezpieczenia, gromadzące zdarzenia związane z bezpieczeństwem Windows Server 2003. Należą do nich, między innymi, informacje o udanym lub nieudanym logowaniu do domeny, dostępie do plików lub drukarek, modyfikacji konfiguracji systemu czy starcie lub zatrzymaniu serwera. Administrator może określić typ i kategorię zdarzenia umieszczanego w dzienniku. Domyślnie po zainstalowaniu Windows Server 2003 monitorowane są takie komponenty, jak dostęp do usługi katalogowej, zarządzanie kontami, zmiana zasad, zdarzenia systemowe, logowanie i logowanie na kontach. Ostatnim z kluczowych dzienników są Aplikacje. Trafiają do niego informacje wygenerowane przez uruchamiane w systemie oprogramowanie - wbudowane, np. instalator, lub zewnętrzne, np. MS SQL czy Exchange.

Aby ułatwić rozpoznanie poziomu zdarzenia, zapisy w dziennikach są podzielone na pięć kategorii. Każda ma inny symbol graficzny. W dziennikach Aplikacje, System, Usługa katalogowa, Serwer DNS i Usługa replikacji plików występują trzy typy zdarzeń: informacja (dymek z literą i), ostrzeżenie (trójkąt z wykrzyknikiem) i błąd (znak "Stop"). Dziennik Zabezpieczenia zawiera informacje o niepowodzeniu (ikona z kłódką) lub sukcesie (ikona z kluczykiem) wykonania jednej z operacji.

Korzystanie z dzienników i administrowanie nimi

Uruchomienie Podglądu zdarzeń jest bardzo proste. Najczęściej korzystamy z Narzędzi administracyjnych lub z przeglądania Zarządzania komputerem. W razie potrzeby można tę przystawkę dołączać do tworzonych konsoli administracyjnych. Przeglądanie każdego z dzienników rozpoczynamy od zaznaczenia go w lewym panelu przystawki. W prawym

panelu zostanie wówczas przedstawiona lista zdarzeń posortowanych w kolejności wystąpienia. Jeśli chcemy, możemy zastosować własny sposób uporządkowania. Realizujemy to kliknięciem jednego z nagłówków kolumn, np. Źródło. Dodatkowo menu Widok zawiera polecenia pozwalające na filtrowanie i wyszukiwanie wyznaczonych zdarzeń.

Dwukrotne kliknięcie poszczególnego zdarzenia powoduje wyświetlenie jego właściwości. Zawierają one szczegółowe informacje na temat daty i czasu zajścia zdarzenia, jego typu, konta użytkownika związanego z zajściem, miejscem wystąpienia wydarzenia, a także kategorią i źródłem informacji. Dla administratorów przeglądających komunikaty, najważniejsze są pola Identyfikator i Opis zdarzenia. Treść opisu pozwala na rozpoznanie przyczyny wystąpienia zdarzenia, natomiast identyfikator doskonale sprawdza się wtedy, gdy poszukujemy dodatkowych informacji na stronach Microsoftu (http://support.microsoft.com) lub grupach dyskusyjnych (http://group.google.pl).

Menedżer zadań

Zanim przejdziemy do omówienia szczegółowych sposobów monitorowania poszczególnych elementów systemu, warto wspomnieć o niewielkim, ale za to bardzo przydatnym narzędziu, jakim jest Menedżer zadań. Program ten pomaga w bieżącym monitorowaniu wykorzystania Windows Server 2003, a zawarte w nim polecenia umożliwiają szybkie rozwiązywanie niektórych problemów.

Jednym ze sposobów na uruchomienie Menedżera zadań jest naciśnięcie przycisków [Ctrl Shift Esc]. Inne to na przykład wybranie opcji Menedżer zadań po kliknięciu prawym przyciskiem paska zadań lub po naciśnięciu [Alt Ctrl Del]. Menedżer składa się z pięciu kart: Aplikacje, Procesy, Wydajność, Sieć i Użytkownicy. Każda z nich informuje o różnych elementach działania systemu. Na karcie Aplikacje znajduje się lista oraz stan uruchomionych programów konsoli. Z tego miejsca możemy zakończyć działanie zablokowanych zadań albo uruchomić nową aplikację. Karta Procesy zawiera listę i właściwości procesów Windows Server 2003. Zawartość listy możemy w łatwy sposób zmodyfikować, wybierając menu Widok | Wybierz kolumny. Dla administratorów serwera szczególnie ważne jest to, że na karcie Procesy można zamykać poszczególne procesy oraz zmieniać ich priorytet.

UWAGA! Niektóre usługi działające w systemie, np. Przeglądarka komputera, nie są uruchamiane jako oddzielne procesy. Mogą współdzielić proces svchost.exe. Aby wyświetlić zawartość każdego podprocesu svchost, należy w wierszu poleceń wpisać Tasklist z parametrem /svc.

Karta Wydajność pozwala na obserwację bieżącego wykorzystania serwera. Wśród dostępnych informacji odnajdziemy użycie procesora i pamięci, a także dodatkowe dane o ilości pamięci jądra, fizycznej i zadeklarowanej.

Począwszy od Windows XP, Menedżer zadań zawiera dwie dodatkowe karty pozwalające na monitorowanie sieci i użytkowników. Na karcie Sieć przedstawione jest wykorzystanie poszczególnych interfejsów sieciowych. Podobnie jak na karcie Procesy, menu Widok zawiera polecenie Wybierz kolumny. Dzięki niemu możemy włączyć wyświetlanie różnych przydatnych informacji statystycznych. Ostatnia karta Menedżera zadań pozwala na zarządzanie podłączonymi do serwera użytkownikami i monitorowanie ich. Po zaznaczeniu jednego z użytkowników możemy wysłać do niego wiadomość, odłączyć go od serwera lub wylogować. To, jakie operacje będzie mógł wykonywać administrator, zależy od typu podłączenia do serwera. W przypadku użytkowników podłączonych przez zdalny pulpit dostępne są opcje Odłącz, Wyloguj, Wyślij wiadomość i Podłącz.

Monitorowanie dostępu

Jeśli serwer sieciowy ma obsługiwać wielu klientów lokalnych lub zewnętrznych, administrator musi mieć możliwość obserwowania tego, co użytkownicy robią lub robili w systemie. Dane te są niezmiernie istotne dla bezpieczeństwa serwera sieci. Windows Server 2003 zawiera wbudowaną obsługę monitorowania działań użytkowników. Jest nią Inspekcja, a poza tym specjalna przystawka wyświetlająca bieżące połączenia z serwerem.

Inspekcja, zwana czasami audytem, pozwala na gromadzenie danych o działalności użytkowników. Jednym z obszarów, jakie możemy monitorować, jest dostęp do zasobów serwera - są to drukarki, Rejestr lub przechowywane na partycjach NTFS pliki i foldery. Oprócz zasobów możemy obserwować czynności użytkowników Windows Server 2003. Ten zakres audytu zbiera, między innymi, informacje o dostępie do systemu, usług katalogowych lub modyfikacji zasad grupy.

Informacje z inspekcji są zapisywane w dzienniku, więc niewygodnie jest wykorzystywać je do obserwacji aktualnych poczynań użytkowników. Aby łatwo sprawdzić na przykład, jakie pliki są w danej chwili pootwierane przez klientów sieci, należy skorzystać z narzędzia Zarządzanie komputerem lub przystawki Foldery udostępnione. Jeśli skonfigurowaliśmy Windows Server 2003 do pełnienia funkcji serwera plików i drukarek, wygenerowana przez system konsola nadaje się najlepiej do obserwacji działań klientów.

Inspekcja

Inspekcja jest elementem stosowanym w serwerach Windows od dawna. Jednak poprzednio administrator musiał ją włączyć ręcznie. Ze względów bezpieczeństwa w Windows Server 2003 inspekcja jest włączona domyślnie. Oznacza to, że w dzienniku Zabezpieczenia zaraz po zakończeniu instalacji pojawiają się wpisy związane z działaniem użytkowników. Dzięki temu pewne poczynania są odnotowywane od samego początku pracy serwera.

Zanim przejdziemy do omówienia sposobów konfiguracji poszczególnych komponentów audytu, należy się zapoznać z zasadami funkcjonowania inspekcji. Powyżej została opisana przystawka Podgląd zdarzeń. Narzędzie to jest jednym z kluczowych elementów działania inspekcji. Ponieważ audyt funkcjonuje na podstawie zdarzeń w systemie, informacje o nich trafiają do Podglądu zdarzeń. Dane inspekcji są przechowywane w dzienniku Zabezpieczenia. Aby docierały do niego odpowiednie informacje, należy włączyć monitorowanie interesujących nas elementów systemu. W innym wypadku do dziennika trafią tylko dane, których zbieranie zostało włączone domyślnie.

Należy pamiętać, że dzienniki charakteryzują się pewnymi właściwościami. W celu uniknięcia kłopotów, na przykład z powodu ich przepełnienia lub za dużych rozmiarów, trzeba ustawić odpowiednie parametry dziennika Zabezpieczenia. W tym celu klikamy prawym przyciskiem folder dziennika w Poglądzie zdarzeń i wybieramy Właściwości. Na karcie Ogólne znajdziemy informacje o aktualnej pojemności i lokalizacji dziennika. Dodatkowo możemy wyczyścić go z wpisów, ustawić maksymalny rozmiar oraz określić akcje podejmowane przez system w razie przepełnienia się dziennika.

Gdzie włączyć inspekcję?

Instalacja systemu operacyjnego uruchamia samoczynnie tylko część zasad inspekcji. Jeśli dodatkowo chcemy wiedzieć, jak eksploatowane są zasoby albo kto bezskutecznie usiłował się podłączyć do serwera, musimy włączyć te działania audytu. W tym celu wybieramy Start | Narzędzia administracyjne | Zasady zabezpieczeń kontrolera domeny i zmieniamy parametry folderu Ustawienia zabezpieczeń | Zasady lokalne | Zasady inspekcji.

W zależności od tego, co chcemy obserwować, należy dwukrotnie kliknąć odpowiednią opcję. We właściwościach zaznaczamy Definiuj następujące ustawienia zasad i wybieramy Sukces lub Niepowodzenie. Naturalnie podczas uruchamiania zasad musimy wiedzieć, jaki typ zdarzenia nas interesuje. W niektórych przypadkach bardziej uzasadnione jest obserwowanie prób zakończonych sukcesem, np. inspekcja zmian zasad. Niekiedy warto odnotowywać niepowodzenia, np. nieudane próby logowania. W razie potrzeby możemy przenosić do dziennika informacje zarówno o sukcesach, jak i o niepowodzeniach.

Uruchomienie audytu po zaznaczeniu sukcesu lub niepowodzenia powoduje zapisywanie informacji w Poglądzie zdarzeń. Od tej reguły są wyjątki. Jeśli chcemy śledzić dostęp do zasobów serwera lub Active Directory, samo włączenie zasad inspekcji nie wystarcza. Dodatkowo musimy poinformować system, jakie zasoby ma monitorować. Oprócz źródła danych należy jeszcze określić, kogo i w jakim zakresie monitorujemy.

Możemy włączyć na przykład monitorowanie dostępu do pliku cmd.exe (źródło) przez użytkowników z grupy Wszyscy, na poziomie powodzenia i niepowodzenia prób wykonywania (uruchomiania), usuwania lub zmiany uprawnień. Parametry te określamy we właściwościach zasobu, w wypadku plików wybieramy Właściwości | Zabezpieczenia | Zaawansowane | Inspekcja.

W celu włączenia audytu Rejestru uruchamiamy edytor Regedit.exe. Następnie zaznaczamy gałąź lub klucz, który chcemy obserwować, i z menu wybieramy Edycja | Uprawnienia | Zabezpieczenia | Zaawansowane | Inspekcja i dodajemy określone obiekty. Ustawienia monitorowania drukarek przebiegają dość podobnie. Otwieramy folder Drukarki i faksy, zaznaczamy odpowiednią drukarkę i z menu wybieramy Właściwości. Na koniec w znany już sposób przechodzimy przez kartę Zabezpieczenia | Zaawansowane | Inspekcja. Nieco więcej kłopotu przysparza ustawienie audytu w obiektach usługi Active Directory. Uruchamiamy przystawkę Użytkownicy i komputery usługi Active Directory. Ponieważ domyślnie karta Zabezpieczenia jest ukryta, aby dostać się do inspekcji, musimy najpierw zaznaczyć Opcje zaawansowane w menu Widok. Dalej wszystko pójdzie jak z płatka. Zaznaczamy domenę, obiekt lub jednostkę organizacyjną i przechodzimy przez Zabezpieczenia | Zaawansowane | Inspekcja.

Przed omówieniem przykładowej konfiguracji inspekcji podamy jeszcze kilka godnych uwagi szczegółów. Audyt związany z folderami i plikami jest możliwy wyłącznie w systemie plików NTFS. Konfiguracja inspekcji dostępu do obiektów oraz do usługi katalogowej powinna być gruntownie przemyślana. Uruchomienie obserwacji zbyt wielu obiektów może generować dużo zdarzeń i zmniejszyć wydajność systemu. Interpretacja zdarzeń inspekcji i wyszukanie interesujących informacji może być kłopotliwe. W przypadku trudności z interpretacją zdarzenia warto sięgnąć do opublikowanego na stronach Microsoftu dokumentu: Windows Server 2003 Security Guide. Natomiast podczas wyszukiwania pamiętajmy o dostępnych w Poglądzie zdarzeń filtrach oraz opcji Znajdź. Dzięki nim szybko odnajdziemy istotne informacje. Jeśli zdarzeń jest naprawdę wiele, zawartość dziennika można wyeksportować do pliku tekstowego (TXT) lub rozdzielanego przecinkami (CSV), a następnie zaimportować do dowolnego arkusza lub bazy danych.

Przykładowa konfiguracja inspekcji

Najważniejszym zaleceniem przed fizyczną konfiguracją zasad inspekcji jest określenie zakresu monitorowania. W wypadku narażonych na niebezpieczeństwo serwerów inspekcja powinna dotyczyć przede wszystkim zasad: logowania (sukces, niepowodzenie), zarządzania kontami (sukces, niepowodzenie), zmiany zasad (sukces, niepowodzenie), zdarzeń systemowych (sukces, niepowodzenie), użycia uprawnień (niepowodzenie) i części plików systemowych (niepowodzenie).

W celu włączenia monitorowania wskazanych zasad po kolei klikamy Start | Narzędzia administracyjne| Zasady zabezpieczeń kontrolera domeny | Ustawienia zabezpieczeń | Zasady lokalne | Zasady inspekcji. Tutaj rozpoczynamy od dwukrotnego kliknięcia opcji Przeprowadź inspekcję dostępu do obiektów, następnie zaznaczamy Definiuj następujące ustawienia zasad oraz Sukces i Niepowodzenie. W ten sposób konfigurujemy zalecane wyżej ustawienia lub te, które nam najbardziej odpowiadają. Po zamknięciu przystawki możemy jeszcze odświeżyć zasady poleceniem wiersza poleceń gpudate.

Powyższe ustawienia wymagają jeszcze wskazania zasobów objętych audytem. To, jakie zasoby będą monitorowane, zależy od specyfiki firmy. Niektóre z przedsiębiorstw chcą śledzić dostęp do krytycznych plików, np. procedur czy list płac, inne, zwłaszcza oferujące dostęp klientom z zewnątrz - szczególnie ważne pliki systemowe Windows, np. cmd.exe.

Monitorowanie dostępu do udostępnianych folderów

Uruchomienie inspekcji dostarcza informacji o działaniach podejmowanych przez użytkowników sieci. Jeśli jednak chcielibyśmy poznać aktualne wykorzystanie systemu, audyt niezbyt się przyda. Oprócz wskazanej już wcześniej karty Użytkownicy (Podgląd zdarzeń) Windows oferuje oddzielną przystawkę Foldery udostępnione do monitorowania połączeń z serwerem. Po jej uruchomieniu widoczne są trzy podfoldery. Każdy z nich pozwala na monitorowanie lub zarządzanie odrębnymi elementami systemu udostępnień.

Pierwszy folder to Udziały. Administratorowi, który ma sprawnie zarządzać systemem, bardzo się przyda. Jeśli na serwerze utworzona zostanie pokaźna grupa udostępnień, obejmujących umieszczone na różnych wolumenach lub dyskach katalogi, obserwacja czy chociażby wyświetlenie listy wszystkich udziałów może sprawić kłopot. W folderze Udziały mamy podaną jak na dłoni listę udostępnień, łącznie z ich właściwościami. Wyświetlane są informacje o nazwie udziału, ścieżce do folderu, typie udostępnienia, liczbie podłączonych klientów oraz zawarte w opisie dodatkowe dane. Stamtąd możemy również wydawać polecenia administracyjne związane z tworzeniem nowych udziałów lub zarządzaniem ich właściwościami. Jeśli chcemy udostępnić nowy folder, z menu Akcja wybieramy polecenie Nowy udział. Dalej, krok po kroku, jesteśmy prowadzeni przez Kreator udostępniania folderu. Pracę rozpoczynamy, naciskając przycisk Dalej.

W kolejnym oknie kreatora wpisujemy ścieżkę do udostępnianego katalogu. Jeśli go nie ma, możemy wskazać lokalizację, korzystając z przycisku Przeglądaj, a następnie kliknąć Utwórz nowy folder. Po naciśnięciu Dalej podajemy nazwę udziału, opcjonalny opis oraz ustawienia trybu offline. Następne okno daje możliwość określenia uprawnień dostępu użytkowników lub administratorów. Jeżeli domyślne opcje nas nie zadowalają, wybieramy Użyj niestandardowych uprawnień udziału i folderu. Naciśnięcie Dalej wyświetla listę podsumowującą nasze działania i kończy pracę kreatora. Natomiast wcześniejsze konfiguracje modyfikujemy, klikając udział i wybierając menu Akcja | Właściwości. Po wywołaniu menu kontekstowego dowolnego udostępnienia możemy bezpośrednio przejść do udostępnionego folderu (polecenie Otwórz) albo zlikwidować udział poleceniem Zatrzymaj udostępnianie.

Folder Sesje służy do zarządzania tymi użytkownikami, którzy już nawiązali połączenie z serwerem. W kolumnach wyświetlane są: nazwa użytkownika, nazwa komputera, z którego nawiązano połączenie, typ połączenia, liczba otwartych plików, czas trwania połączenia, czas bezczynności oraz informacja, czy połączenie zostało nawiązane na podstawie uprawnień konta Gość. Oprócz monitorowania bieżących sesji administrator może odłączyć od sesji Windows poszczególnych lub wszystkich użytkowników.

Do śledzenia, z których plików korzystają użytkownicy serwera, służy folder Otwarte pliki. Za jego pomocą administrator może dokładnie kontrolować zasoby Windows Server 2003. Oprócz informacji o nazwie zasobu podawane są: nazwa użytkownika, typ, liczba

blokad oraz tryb otwierania. Pliki mogą być blokowane na przykład przez aplikacje w związku z ograniczeniem dostępu do zasobu lub ograniczeniem wykonywania pewnych operacji na zasobie, np. usuwania pliku. Ograniczenia te dają pewność, że w danym momencie do pliku sięga tylko jeden użytkownik albo że nie zostanie zmodyfikowany plik używany przez inną osobę. Tryb otwierania określa sposób dostępu do danych, np. Odczyt lub Zapis i odczyt.

Na koniec warto zwrócić uwagę na zastosowanie konsoli Zarządzanie serwerem plików. Zawiera ona wszystkie omówione wcześniej foldery związane z udziałami i dodatkowo moduły Defragmentator dysków oraz Zarządzanie dyskami. Oferuje też nowe polecenia związane z podłączaniem się do innych komputerów oraz wysyłaniem komunikatów konsoli.

Zdalny pulpit

W sieciach lokalnych część operacji związanych z administracją możemy wykonywać, podłączając się do maszyny za pomocą odpowiednich przystawek konsoli MMC. Ten typ zarządzania nakłada pewne ograniczenia, na przykład po załadowaniu przystawki Zarządzanie komputerem dla zdalnego systemu nie możemy wykonać żadnych czynności związanych ze sterownikami urządzeń. Jedną z istotnych zalet Windows Server 2003 jest możliwość zdalnego zarządzania systemem za pomocą usługi Zdalny pulpit, szczególnie istotnej dla administratorów starszych systemów, którzy zwykle korzystali z bezpłatnej - nie najgorszej zresztą - aplikacji VNC lub oprogramowania komercyjnego typu pcAnywhere. Możliwość zdalnego zarządzania serwerem przydaje się zarówno w zarządzaniu z sieci lokalnej, jak i przez sieć rozległą. Umiejscowienie serwera nie ma większego znaczenia. Zdalny pulpit korzysta z dostępnych w systemie usług terminalowych. Co prawda, usługi te były oferowane już w Windows 2000 oraz dystrybuowane z Windows NT jako oddzielna wersja systemu, ale zdalny pulpit Windows Server 2003 oferuje wiele ulepszeń. Do najważniejszych zaliczamy unowocześniony protokół komunikacyjny Remote Desktop Protocol 5.2 (serwer) i 5.1 (klient) oraz zmiany związane z lepszymi zabezpieczeniami.

Aby móc zdalnie administrować serwerem, najpierw należy włączyć usługę Zdalny pulpit. W tym celu należy wyświetlić właściwości obiektu Mój komputer lub kliknąć ikonę System, przejść do karty Zdalny i zaznaczyć opcję Zezwalaj użytkownikom na zdalne łączenie się z tym komputerem. Warto przy tym zwrócić uwagę na przycisk Wybierz użytkowników zdalnych, służący do określania, którzy użytkownicy mogą zdalnie administrować systemem. W Windows 2000 zarządzanie za pośrednictwem usług terminalowych było dozwolone domyślnie wyłącznie dla użytkowników należących do grupy Administratorzy. W systemach Windows XP oraz Windows Server 2003 jest nowa grupa: Użytkownicy pulpitu zdalnego. Za jej pośrednictwem można dodawać inne konta uprawnione do zdalnej administracji.

UWAGA! Jeśli Windows Server 2003 został skonfigurowany jako kontroler domeny, domyślnie tylko członkowie grupy Administratorzy mogą nim zdalnie zarządzać. Jeśli chcemy zezwolić na to również członkom grupy Użytkownicy pulpitu zdalnego, należy zmienić ustawienia Zasad grup w folderze Przypisywanie praw użytkownika. Trzeba również pamiętać, że Windows Server 2003 ma wbudowane ograniczenie do dwóch równoległych sesji pulpitu zdalnego.

Działanie zdalnego pulpitu opiera się na wykorzystaniu komponentów klienta i serwera. Jak już zaznaczono, komponentem serwera są usługi terminalowe. Jeśli nie zostaną uruchomione, nikt nie będzie mógł się podłączyć do Windows Server 2003. Komponentem klienta jest aplikacja Podłączenie pulpitu zdalnego (mstsc.exe), instalowana automatycznie w stacjach roboczych pracujących pod kontrolą Windows XP Professional. Łatwo go odnajdziemy w menu Komunikacja (Programy | Akcesoria). Jeśli chcemy zarządzać serwerem z innych systemów operacyjnych, musimy zainstalować

odpowiednie oprogramowanie. Do tego celu będzie potrzebne albo połączenie sieciowe z serwerem, albo płyta instalacyjna Windows Server 2003. W folderze katalog_główny_systemu/system32/clients/tsclient/win32 znajduje się instalator aplikacji Podłączanie pulpitu zdalnego. Jeśli chcemy, żeby klienci sieci instalowali ten program bezpośrednio z serwera, należy udostępnić folder tsclient. Jeżeli wolimy zrobić to osobiście w wybranych komputerach, wystarczy wziąć płytę instalacyjną i po autostarcie wybrać Wykonaj zadania dodatkowe | Konfiguruj podłączanie pulpitu zdalnego.

Parametry zdalnego zarządzania również mogą być konfigurowane po dwóch stronach. Od strony klienta konfigurujemy m.in. opcje użytkownika, ekranu, optymalizację szybkości połączenia oraz mapowanie zasobów lokalnych. Dostęp do ustawień uzyskujemy przyciskiem Opcje w oknie programu Podłączanie pulpitu zdalnego. Do zmiany konfiguracji serwera służy narzędzie Konfiguracja usług terminalowych, a do monitorowania połączeń z Windows Server 2003 - Menedżer usług terminalowych. Skróty do nich odnajdziemy w Narzędziach administracyjnych. W przypadku wykorzystania zdalnego pulpitu do administracji serwerem, zarządzanie tą usługą musi się opierać przede wszystkim na uważnym ustawieniu opcji związanych z bezpieczeństwem systemu. Zalecane jest skonfigurowanie wysokiego poziomu szyfrowania komunikacji, wymuszania każdorazowego podawania hasła przez osoby łączące się z komputerem oraz automatycznego zrywania bezczynnych sesji. Opcje te modyfikujemy we właściwościach protokołu RDP serwera (Konfiguracja usług terminalowych | Połączenia | Właściwości połączenia RDP-Tcp. Kluczowym obowiązkiem jest również częste monitorowanie kont uprawnionych do zarządzania serwerem. Do administrowania powinniśmy założyć oddzielne, specjalne konto, które w żadnym wypadku nie powinno należeć do grupy Administratorzy. Po uruchomieniu zdalnego pulpitu z uprawnieniami zwykłego użytkownika, w celu administrowania poszczególnymi komponentami systemu trzeba się posłużyć opcją Uruchom jako.

Przykładowa konfiguracja zdalnego pulpitu

Przykładową konfigurację zdalnego zarządzania rozpoczniemy od założenia konta przeznaczonego do obsługi zdalnego pulpitu. W tym celu uruchamiamy narzędzie Użytkownicy i komputery usługi Active Directory. Następnie zaznaczamy jeden z folderów. W naszym przypadku może to być Users. Z menu Akcja wybieramy Nowy | Użytkownik. Po nadaniu kontu nazwy, np. ZdalnyPulpit, powinniśmy bezwzględnie przypisać mu dobre hasło (powyżej ośmiu znaków, w tym cyfry i znaki typu #, %, ! itp.) oraz odznaczyć opcję zmiany hasła podczas następnego logowania. Potem dodajemy użytkownika do wbudowanej grupy Użytkownicy pulpitu zdalnego. Do kompletu brakuje modyfikacji ustawień zabezpieczeń kontrolera domeny. Jest to konieczne ze względu na wspomniane wcześniej ograniczenia kontrolerów domeny, w których jedynie członkowie grupy administratorzy mogą pracować ze zdalnym pulpitem. Modyfikacja ustawienia zasad dotyczących serwera zajmie nie więcej niż minutę. Klikamy Start | Narzędzia administracyjne | Zasady zabezpieczenia kontrolera domeny. Po uruchomieniu konsoli MMC kolejno wybieramy Ustawienia zabezpieczeń | Zasady lokalne | Przypisywanie praw użytkownika. Edytujemy opcję Zezwalaj na logowanie za pomocą usług terminalowych, następnie zaznaczamy Definiuj następujące ustawienia zasad i dodajemy grupę Użytkownicy pulpitu zdalnego. Po naciśnięciu OK wykonujemy jeszcze jedną zmianę. Ponieważ zwykli użytkownicy sieci domyślnie nie mają dostępu do konsoli serwera, musimy ustawić interakcyjne logowanie do Windows Server 2003. W tym celu klikamy Zezwalaj na logowania lokalne i do listy uprawnionych dodajemy grupę Użytkownicy pulpitu zdalnego. Po zamknięciu konsoli możemy dla pewności odświeżyć zasady, wpisując gpupdate w poleceniu Uruchom.

Po prawidłowym założeniu i skonfigurowaniu konta użytkownika, możemy włączyć usługę Zdalny pulpit. W tym celu klikamy Start | Panel sterowania | System, następnie przechodzimy do karty Zdalny i zaznaczamy opcję Zezwalaj użytkownikom na zdalne łączenie się z tym komputerem. Naciśnięcie przycisku OK pozwala na pracę ze zdalnym

pulpitem. Ostatnie działania polegają na skonfigurowaniu właściwości protokołu RDP. Po kolei klikamy Start | Narzędzia administracyjne | Konfiguracja usług terminalowych | Połączenia | Właściwości połączenia RDP-Tcp. Tu na karcie Ogólne zmieniamy poziom szyfrowania na Wysoki, na karcie Ustawienia logowania zaznaczamy opcję Zawsze monituj o podanie hasła. Wreszcie na karcie Sesje wymuszamy zastępowanie ustawień użytkownika parametrami Limit czasu bezczynności sesji (np. 5 minut) i Zakończ sesję po osiągnięciu limitu. Naciśnięcie OK kończy konfigurację serwera.

Jeśli klientami naszej sieci są systemy Windows XP Professional, nie musimy instalować oprogramowania do zdalnego zarządzania. Do rozpoczęcia administracji wystarczy kliknąć Start | Wszystkie programy | Akcesoria | Komunikacja i uruchomić Podłączanie pulpitu zdalnego. Zanim jednak przejdziemy do nawiązywania łączności, warto się bliżej przyjrzeć ustawieniom klienta. Po naciśnięciu przycisku Opcje możemy ustawić kilka przydatnych właściwości. Jeśli nie zarządzamy z sieci lokalnej, warto zmienić konfigurację związaną z optymalizacją wydajności. W tym celu klikamy kartę Wrażenia i ustawiamy odpowiednią szybkość łącza lub ręcznie modyfikujemy widoczne tam opcje.

Wykonywanie kopii zapasowej

Nawet najlepiej zarządzany serwer może ulec awarii. Konsekwencje związane z bezpowrotną utratą danych często wiążą się z utratą klientów, a w krańcowych przypadkach z upadkiem firmy. Administrator systemu powinien zadbać o skuteczne sporządzanie kopii zapasowych, żeby w razie awarii lub przypadkowego usunięcia danych zminimalizować wynikające z tego problemy. Fizyczne wykonanie kopii bezpieczeństwa jest stosunkowo łatwe. Zanim jednak omówimy narzędzie do backupu, należy starannie przemyśleć strategie jego sporządzania. W wypadku ochrony danych na stacjach lokalnych i w komputerach domowych kopiowanie plików z reguły dotyczy niewielkiej ilości informacji, ale czynnikami decydującymi o sposobie backupu na serwerach są: rozmiar, czas sporządzania oraz czas odtwarzania. Większość firm w celu ochrony danych wyposaża serwery w napędy taśmowe. Zadaniem administratora jest opracowanie takiej strategii sporządzania backupu, żeby jego wykonanie nie trwało wieki, a odtworzenie danych było szybkie i niezawodne.

Windows Server 2003 pozwala na wybór jednego z pięciu rodzajów sporządzania kopii zapasowej. Mamy do dyspozycji kopię zwykłą, kopiującą, przyrostową, różnicową oraz codzienną. Wyjaśnienie różnic pomiędzy metodami backupu wymaga przypomnienia wiadomości o jednym z atrybutów plików. Pliki zapisywane na wolumenach FAT i NTFS oprócz tak ewidentnych cech, jak nazwa, rozmiar i czas utworzenia, mają jeszcze atrybuty. W systemie FAT są to: Tylko do odczytu, Ukryty, Systemowy i Archiwalny. W systemie NTFS dodatkowo funkcjonują Zaszyfrowany i Skompresowany. Atrybut Archiwalny występuje w obu systemach. Jego głównym zastosowaniem jest oznaczenie, czy plik należy archiwizować, czy nie. Utworzenie oraz każdorazowa modyfikacja pliku automatycznie nadają ten atrybut. W zależności od wybranego przez administratora typu backupu, system zdejmuje lub pozostawia w nienaruszonym stanie nadany atrybut archiwizacji.

Typ Normalny kopii bezpieczeństwa archiwizuje wszystkie wybrane do backupu dane i - co bardzo ważne - usuwa atrybut Archiwalny. Strategię ochrony danych rozpoczyna się zwykle od wykonania zwykłej kopii, natomiast w wypadku metody różnicowej archiwizowane są tylko te pliki, które zostały utworzone lub uległy zmianie od ostatniego zwykłego backupu. Atrybut Archiwalny nie jest usuwany. Zaletą tej metody jest zmniejszenie liczby kopiowanych danych i skrócenie czasu sporządzania kopii. Wadę stanowi wydłużenie czasu odtwarzania zasobów, bo administrator musi odtworzyć najpierw kopię zwykłą, a później różnicową. Backup przyrostowy, podobnie jak różnicowy, polega na wykonaniu kopii jedynie tych elementów, które zostały utworzone lub zmodyfikowane po ostatnim zwykłym backupie. Skopiowane pliki pozbawia się atrybutu Archiwalny. Powoduje to istotną zmianę podczas tworzenia oraz odtwarzania

danych. Każdy backup przyrostowy zachowuje tylko te dane, które zmieniły się od czasu wykonania poprzedniej kopii zapasowej.

Stosując metodę różnicową zawsze kopiuje się to, co podlegało zmianom w okresie między wykonaniem kopii a zwykłą archiwizacją. Oznacza to, że pierwsze kopie utworzone metodą różnicową lub przyrostową są takie same, natomiast wszystkie następne różnią się rozmiarem i czasem wykonania. Archiwizacja przyrostowa jest szybsza i z reguły wymaga mniejszych objętości nośników niż różnicowa. W czasie odtwarzania, wymaga jednak kolejnego przetwarzania wszystkich archiwów, począwszy od kopii zwykłej. Wydłuża to czas odtwarzania i zwiększa prawdopodobieństwo błędu podczas kolejnych operacji. Backup kopiujący jest stosowany do obsługi kombinacji typów zwykłych i przyrostowych. Polega na archiwizowaniu wszystkich zaznaczonych elementów. W czasie wykonywania tej kopii atrybut Archiwalny jest pomijany. Jeśli łączymy model zwykły z przyrostowym, zastosowanie backupu kopiującego, np. w środku tygodnia, zmniejsza liczbę kopii koniecznych do odtworzenia w przypadku awarii. Ostatni model kopii - archiwizacja codzienna - opiera swoje działanie na dacie wykonywania. Archiwizowane są wszystkie zaznaczone do backupu dane, które zostały zmodyfikowane w danym dniu. Znacznik atrybutu Archiwalny nie jest modyfikowany.

Podczas uruchamiania Kreatora kopii zapasowych administrator jest pytany, czy ma być wykonana kopia stanu systemu. Stan systemu nie jest typem archiwizacji, lecz zbiorem danych potrzebnych do odtworzenia Windows Server 2003. W jego skład wchodzą: Rejestr, pliki systemowe, baza komponentów COM+ oraz pliki rozruchowe. Dodatkowo, w zależności od konfiguracji serwera, skład stanu systemu może zawierać kopię Active Directory, metabazy usługi IIS oraz bazę usług certyfikatów.

Zaawansowane parametry kopii zapasowej

Wybór plików oraz metoda wykonywania kopii zapasowej jest jednym z parametrów określanych przez administratora po uruchomieniu kreatora archiwizacji. Podczas tworzenia kopii możemy określić jeszcze kilka ważnych opcji backupu. Jeśli serwer nie jest wyposażony w napęd taśmowy, archiwizacja może być wykonana w pliku, następnie zapisanym na płycie DVD lub CD-R.

Archiwizację systemu należy wykonywać cyklicznie oraz w czasie najmniejszego obciążenia Windows Server 2003. Po wybraniu zaawansowanych opcji kreatora możemy określić, kiedy system ma uruchomić kopię zapasową. Planowanie archiwizacji pozwala na wykonanie jej raz, codziennie, co tydzień, co miesiąc, podczas uruchamiania systemu, logowania oraz w okresie bezczynności. Możemy również określić datę rozpoczęcia, datę zakończenia, powtarzalność oraz dodatkowe parametry związane np. z reakcją systemu na wypadek zapętlenia się zadania.

Pozostałe parametry obejmują: weryfikację danych po wykonaniu archiwizacji, jeśli pozwala na to napęd taśm, włączenie kompresji sprzętowej oraz wyłączenie kopiowania woluminów w tle. Podczas odtwarzania danych pliki mogą zostać zapisane w poprzedniej albo w nowej lokalizacji. Konfigurując backup, nie należy zapominać o uprawnieniach. Aby wykonać lub odtworzyć kopię zapasową w systemie Windows Server 2003, trzeba mieć odpowiednie uprawnienia. Domyślnie do realizowania tych czynności uprawnieni są członkowie grupy Administratorzy, Operatorzy serwerów oraz Operatorzy kopii zapasowych. W celu umożliwienia wskazanemu użytkownikowi uruchomienia backupu należy dodać jego konto do jednej z wymienionych grup. Naturalnie, ze względów bezpieczeństwa, nie jest zalecane przypisywanie go do grupy Administratorzy.

Przykładowe wykonanie kopii zapasowej

Użytkowników, którzy chcą wykonać kopię zapasową danych, czeka niespodzianka związana z lokalizacją narzędzia do archiwizacji. Nie jest ono umiejscowione ani w Panelu

sterowania, ani w Narzędziach administracyjnych. W celu przeprowadzenia backupu, należy kliknąć Wszystkie programy | Akcesoria | Narzędzia systemowe | Kopia zapasowa.

Jeśli Kopia zapasowa jest uruchamiana po raz pierwszy, rozpoczyna ją łatwy w użyciu Kreator kopii zapasowych lub przywracania. Dla administratorów, którzy chcą konfigurować archiwizację ręcznie, w pierwszym oknie umieszczono opcję Zawsze uruchamiaj w trybie kreatora. Usunięcie znacznika przełączy widok w tryb bez kreatora. W celu kontynuacji tworzenia kopii należy kliknąć przycisk Dalej. Pracę rozpoczynamy od określenia, czy chcemy wykonać kopię, czy odtworzyć dane z archiwum. Jeśli wybierzemy utworzenie backupu, następne pytanie związane jest z zakresem archiwizowanych danych. Możemy skopiować je wszystkie albo określić zakres backupu ręcznie. Zaznaczenie opcji Pozwól mi wybrać, co ma zawierać kopia zapasowa, powoduje wyświetlenie okna podobnego do Eksploratora Windows, w którym wskazujemy elementy przeznaczone do archiwizacji. W naszym prostym przykładzie zaznaczymy przykładowy folder Public. Po kliknięciu Dalej przechodzimy do określenia miejsca zapisywania kopii oraz jej nazwy. Jeśli serwer nie jest wyposażony w napęd taśmowy, jedyną lokalizacją kopii jest plik. W celu uproszczenia przykładu wskażmy dysk D:, a archiwum nazwijmy FolderPublic. W rzeczywistym środowisku sieciowym należałoby przygotować oddzielny folder do backupu i odpowiednio nazwać archiwum. Kliknięcie przycisku Dalej wyświetla okno kończące prace kreatora i po wybraniu Zakończ rozpoczyna się wykonywanie kopii.

Jeśli chcemy określić dodatkowe parametry kopii zapasowej, należy kliknąć znajdujący się w ostatnim oknie przycisk Zaawansowane. Będziemy mogli wówczas wybrać typ archiwizacji (zwykła, przyrostowa itp.), a także określić inne, omówione wcześniej zaawansowane parametry. Na koniec warto pamiętać, że co pewien czas należy przeprowadzić testowe odtwarzanie danych. Dzięki temu upewnimy się, czy przygotowana strategia chroni przed poważnymi skutkami awarii.

Marzenie każdego administratora to sieć, której zarządzanie jest całkowicie zautomatyzowane. Brak konieczności mozolnego klikania tych samych opcji na wielu komputerach zmniejsza ryzyko pomyłki, a dodatkowo oszczędza mnóstwo czasu. Windows Server 2003 ma wbudowane mechanizmy, które pozwalają w dużym stopniu zoptymalizować wykonywanie nudnych zadań.

Kiedy firma rozwija się dynamicznie, sieć komputerowa rozrasta się razem z nią. Zwiększenie liczby użytkowników i komputerów nie wprawia w dobry nastrój administratora sieci. Rachunek jest prosty - im więcej kont i stacji, tym więcej obowiązków. Trzydziestoma stacjami można zarządzać bez problemów, ale jeśli komputerów jest sto pięćdziesiąt, kłopoty narastają. Nadmiar obowiązków wiąże się z ryzykiem popełniania błędów. Niewłaściwe przypisanie uprawnień dostępu lub zezwolenie na posługiwanie się pustymi hasłami może negatywnie wpłynąć na zabezpieczenia sieci. W Windows Server 2003 zarządzanie domeną jest wspomagane przez zasady grupy. Ich zastosowanie w znaczny sposób ułatwia administrację serwerami, komputerami klientów i

grupami użytkowników. Poprawna konfiguracja zasad grupy nie jest trudna, a daje znaczne korzyści.

Funkcja zasad grupy

Zarządzanie sieciami komputerowymi nie ogranicza się do poprawnego skonfigurowania Windows Server 2003. Wydajne i bezawaryjne działanie głównego komputera firmy jest bardzo ważne, ale większość codziennych zadań administratora wiąże się z konfiguracją oraz obsługą klientów sieci. Główną funkcją zasad grupy jest scentralizowanie, ujednolicenie i usprawnienie zarządzania siecią.

Zasady grupy to zespół parametrów konfiguracyjnych sformułowanych przez klienta, a następnie automatycznie przenoszonych do systemów operacyjnych klientów domeny pracującej pod kontrolą serwera z Windows Server 2003. Usługa Active Directory pozwala na wykorzystanie zasad grupy do zarządzania komputerami i użytkownikami sieci. Parametry konfiguracyjne mogą być przenoszone zarówno na wszystkie konta użytkowników i komputerów, jak i na te, które zostaną jednoznacznie określone. Głównym zadaniem zasad grup jest ujednolicenie i zabezpieczenie środowiska pracy użytkowników. Dodatkowo pozwalają instalować oprogramowanie w sieci oraz wypływać na to, do jakich komponentów systemu Windows będą mieli dostęp klienci domeny.

Obiekty zasad grupy

Windows Server 2003 świadczy usługi klientom sieci. Za przechowywanie informacji o zasobach odpowiada usługa Active Directory. Po jej zainstalowaniu administrator zakłada konta użytkowników oraz komputerów, korzystając z odpowiednich narzędzi. Po zalogowaniu pracownicy identyfikują się, podając podczas uwierzytelnienia nazwę konta. Ponieważ konta komputerów również mają nazwy, łatwo ustalić, przy jakiej stacji pracuje klient sieci. Prosta identyfikacja użytkownika i komputera daje wiele korzyści związanych z zarządzaniem zasobami. Funkcjonowanie zasad grupy opiera się właśnie na obiektach przechowywanych przez Active Directory. Zestaw zasad to zbiór parametrów przekazywanych kontom użytkowników i komputerów. Pojedynczy zestaw nazywamy obiektem zasad grupy.

Parametry przenoszone na konta komputerów zawierają ustawienia środowiska systemu niezwiązane z profilem użytkownika. Ustawienia nadane komputerowi są uwzględniane niezależnie od tego, czy ktokolwiek zalogował się do stacji. Za przykład może służyć automatyczne włączenie przydziałów dysków w komputerach lokalnych lub wyłączenie usług związanych z aktualizacją oprogramowania.

Ustawienia użytkowników, takie jak konfiguracja oprogramowania, zabezpieczeń, składników systemu Windows, są odmienne dla każdego z kont. Stosujemy je do określania cech przenoszonych na środowisko pracy klientów sieci. Przykładem parametru związanego z użytkownikiem jest ukrycie ikony Ekran w Panelu sterowania. Zalogowanie się klienta do innego komputera niczego nie zmieni. W dalszym ciągu konfiguracja ekranu będzie niedostępna. Jeśli użytkownik zakończy pracę, zamiast niego zaloguje się inny pracownik, dostęp do konfiguracji ekranu będzie zależał od ustawień zasad nowego klienta. Parametry ekranu mogą być np. na powrót włączone.

Rodzaje ustawień przenoszonych przez zasady

Ustawienia użytkownika oraz komputera dotyczą zabezpieczeń, systemu operacyjnego, oprogramowania oraz środowiska pracy. Mimo podobieństw zakresu zazębiają się sporadycznie, a w dodatku parametry kont klientów i stacji są wysyłane do systemu oddzielnie. Najpierw wprowadzane są ustawienia komputera, a dopiero po zalogowaniu się klienta do domeny stosowane są zasady użytkowników.

Konfiguracja oprogramowania dotyczy dystrybucji aplikacji i uaktualnień w domenie Windows Server 2003. Przypisanie programów do obiektu komputer sprawia, że oprogramowanie jest dostępne dla wszystkich klientów sieci pracujących przy danej stacji. Jeśli związemy aplikację z obiektem użytkownik, wówczas oprogramowanie będzie "podążało" za pracownikiem do każdej stacji, do której się zaloguje. Dzięki temu zmiana miejsca pracy nie spowoduje utraty dostępu do programów. W zależności od ustawień, aplikacje mogą być instalowane automatycznie lub na żądanie klienta.

W sekcji konfiguracji Windows znajdują się parametry środowiska pracy użytkownika: zabezpieczeń, indywidualnych skryptów logowania i wylogowania obiektu użytkownik oraz skryptów startu i zamykania systemu dla komputera. Dla kont klientów dodatkowo przewidziano możliwość zmiany położenia m.in. folderów Moje dokumenty lub Pulpit, ustawień parametrów Internet Explorera oraz usług instalacji zdalnej.

Zasady zabezpieczeń są zawarte w grupie konfiguracji Windows. Obejmują konfigurację haseł, praw, uprawnień do zasobów, parametrów infrastruktury kluczy publicznych (PKI), protokołu Kerberos i zabezpieczeń przez IPSec. Zastosowanie zasad zabezpieczeń do wszystkich stacji lub użytkowników w domenie pozwala na wprowadzenie spójnych i jednolitych ustawień w całej sieci.

Do konfiguracji środowiska pracy służą foldery szablonów administracyjnych. Zawierają dużą grupę parametrów wpływających na wygląd i ustawienia pulpitu, składników systemu Windows, udostępnień, Panelu sterowania itp. Zmiana poszczególnych parametrów pozwala na skonfigurowanie standardowego i bezpiecznego systemu operacyjnego dla całej domeny lub wybranych oddziałów firmy.

Narzędzia do administrowania zasadami grupy

Administrator Windows Server 2003 otrzymuje kilka wygodnych konsoli do zarządzania ustawieniami zasad grupy oraz narzędzia do monitorowania i konfiguracji parametrów z poziomu wiersza poleceń. Z witryny Microsoftu można pobrać dodatkowe, zaawansowane narzędzia i przystawki.

Podstawowymi narzędziami graficznymi są moduły MMC. Zarządzanie zasadami grupy można podzielić na dwie oddzielne czynności. Pierwsza to tworzenie i konfigurowanie obiektów zasad. Korzystając z Edytora obiektów zasad grupy, konfigurujemy poszczególne konta komputerów i użytkowników. Druga czynność to zarządzanie utworzonymi obiektami zasad: wiązanie obiektów zasad z obiektami w Active Directory, określanie właściwości powiązań oraz monitorowanie wynikowych rezultatów powiązań. Obiekty zasad łączy się z obiektami usługi Active Directory po to, żeby zawarte w zasadach ustawienia były przenoszone na konta zgromadzone w domenie, lokalizacji lub jednostce organizacyjnej. Do wiązania ustawień służą moduły Użytkownicy i komputery usług Active Directory oraz Lokacje i usługi Active Directory.

Windows Server 2003 pozwala na oddzielne zarządzanie systemowymi parametrami konfiguracji zabezpieczeń. Są one przenoszone za pomocą modułów wchodzących w skład Narzędzi administracyjnych - Zasad zabezpieczeń domeny lub Zasad zabezpieczeń kontrolerów domeny. Dla administratorów dużych sieci znacznym usprawnieniem i ułatwieniem konfiguracji bezpieczeństwa będzie wykorzystanie szablonów zabezpieczeń. Do nanoszenia ustawień służą moduły Szablony zabezpieczeń oraz Konfiguracja i analiza zabezpieczeń. Nie zapomniano również o module pozwalającym na analizę parametrów wprowadzanych przez zasady grupy. Aby wyświetlić zasady stosowane do komputerów i użytkowników, należy się posłużyć modułem Wynikowy zestaw zasad. Chcąc otworzyć trzy ostatnio wymienione moduły, należy wczytać pustą konsolę MMC i dodać wskazany element z listy modułów autonomicznych.

Biorąc pod uwagę liczbę narzędzi do zarządzania zasadami grupy, ich konfiguracja oraz monitorowanie wydają się skomplikowane. Istotnie, przy wielu obiektach zasad oraz domenach o złożonej strukturze, nadzorowanie i bezproblemowe wdrażanie usług zasad grupy nie jest proste. W celu ułatwienia Microsoft przygotował specjalną konsolę do kompleksowego zarządzania zasadami. Group Policy Management Console gromadzi w jednym miejscu większość funkcji konfiguracyjnych oraz oferuje dodatkowe opcje, m.in. tworzenia zapasowych kopii zasad. Moduł (na razie jest tylko w wersji angielskiej) należy pobrać z witryny http://www.microsoft.com/downloads . Ponieważ konfiguracja zasad przy użyciu konsoli Group Policy Management jest znacznie wygodniejsza, opis zarządzania zasadami grupy będzie dotyczył tego narzędzia.

Edytor obiektów zasad grupy

Podstawowym narzędziem do tworzenia i modyfikowania obiektów zasad jest Edytor obiektów zasad grupy. Może być uruchamiany bezpośrednio po otworzeniu pustego modułu MMC lub z którejś konsoli łączącej pojemniki usługi Active Directory (domena, lokacja, jednostka organizacyjna) z obiektami zasad. Chcąc wywołać edytor z poziomu modułu Użytkownicy i komputery usługi Active Directory, należy zaznaczyć jeden z pojemników, np. domenę pl.idg.com, i z menu Akcja wybrać Właściwości. Następnie przechodzimy do karty Zasady grupy i naciskamy przycisk Edytuj. Kliknięcie Edytuj otwiera moduł do konfiguracji ustawień komputera i użytkownika. Wywołanie edytora z konsoli GPMC wymaga nieco więcej kliknięć. Po uruchomieniu modułu po kolei rozwijamy foldery Forest: nazwa_lasu, Domains i nazwa_domeny. Następnie przechodzimy do folderu Group Policy Objects i z menu Action wybieramy New. Wpisujemy nazwę zasady i naciskamy OK. Nowo utworzona zasada nie zawiera żadnych ustawień. Jeśli chcemy wprowadzić nowe parametry, powinniśmy wybrać z menu Action polecenie Edit. Spowoduje to wyświetlenie edytora obiektów zasad.

Po uruchomieniu narzędzia do edycji zasad wyświetlane są dwa foldery. Pierwszy zawiera ustawienia przekazywane komputerom, drugi użytkownikom. Podział ten jest skutkiem oddzielnego reprezentowania obiektów w Active Directory. Rozbicie konfiguracji stacji i klientów na dwa oddzielne foldery ma dodatkowe zalety. Środowisko pracy użytkowników najczęściej jest ściśle związane z przypisanymi im stacjami roboczymi, ale czasem z jednego stanowiska korzysta wiele osób lub pracownicy wykonujący swoje obowiązki przemieszczają się od komputera do komputera. Wymaga to odpowiedniej obsługi ze strony systemu operacyjnego. Oddzielna konfiguracja zasad grupy pozwala na proste rozwiązywanie problemów związanych z wielodostępem. Podział ten wynika również ze sposobu utrzymywania informacji o konfiguracji Windows. Rejestr systemu składa się z kilku oddzielnych części, tzw. gałęzi. Gałąź HKEY_LOCAL_MACHINE zawiera ustawienia stacji, natomiast HKEY_CURRENT_USER parametry profilu zalogowanego użytkownika. W profilach zawarte są informacje o indywidualnych preferencjach osób korzystających z Windows, np. parametry ekranu, myszy itp.

Rozwijając poszczególne obiekty, podobnie jak w Eksploratorze Windows, poruszamy się po folderach zawierających odpowiednie opcje. Klikając np. folder Szablony administracyjne, w prawym panelu wyświetlamy jego zawartość. Poszczególne opcje zmieniają wybrane parametry systemu, np. Ukryj i wyłącz wszystkie elementy pulpitu. Jeśli nazwa ustawienia jest nieczytelna lub mało mówiąca, należy ją zaznaczyć. Spowoduje to wyświetlenie opisu oraz wymagań systemowych. Warto zwracać uwagę na umieszczone w opisie wymagania systemowe, gdyż niektóre z ustawień mogą być przenoszone wyłącznie do nowszych systemów operacyjnych, np. Windows XP i Server 2003.

Konfiguracja poszczególnych opcji polega na wprowadzeniu odpowiedniej wartości parametru lub określeniu położenia przełącznika. Aby zmienić ustawienie, klikamy dwukrotnie wybrany obiekt. W wypadku większości parametrów związanych z zabezpieczeniami wpisujemy żądaną wartość lub wybieramy ją z listy. W ten sposób

określamy na przykład minimalną liczbę znaków w haśle systemu. Nieco inaczej zmieniamy parametry w Szablonach administracyjnych. Określenie ustawień polega na zmianie stanu przełącznika. System daje do wyboru trzy wartości: Nie skonfigurowano, Włączone i Wyłączone. Pierwsza opcja wskazuje, że ustawienie jest neutralne i nie będzie brane pod uwagę podczas implementacji zasad. Następne włączają lub wyłączają wskazane parametry. Konfigurując ustawienia Włączone i Wyłączone, trzeba uważać, żeby nie wchodzić w konflikt z zasadami z innych pojemników.

Instalacja konsoli do zarządzania zasadami

Przed rozpoczęciem konfiguracji ustawień zasad powinniśmy zainstalować konsolę GPMC. Instalacja konsoli nie jest obowiązkowa. Bez większych przeszkód możemy się posługiwać poprzednimi sposobami zarządzania zasadami grupy. Warto jednak pamiętać, że funkcjonalność i możliwości modułu GPMC są znacznie większe, dlatego jej instalacja jest bardzo zalecana.

Pobrany z witryny Microsoftu plik konsoli to GPMC.MSI. Instalację rozpoczynamy od uruchomienia pliku, a następnie postępujemy zgodnie z zaleceniami kreatora. W oknie powitalnym klikamy Next. Jeśli zgadzamy się z warunkami licencji, wybieramy opcję I Agree i przechodzimy do następnego okna. System instaluje odpowiednie komponenty modułu i wyświetla okno z przyciskiem Finish. Konsola jest domyślnie instalowana w folderze GPMC zawartym w Program Files partycji startowej Windows Server 2003. Warto wiedzieć, że na dysku zapisywany jest również folder Scripts, zawierający grupę skryptów przydatnych do zarządzania zasadami skryptów.

Po zainstalowaniu konsoli zarządzania zasadami poprzedni sposób konfigurowania obiektów zasad grupy zostaje wyłączony. Jeśli sięgniemy do modułu Użytkownicy i komputery usługi Active Directory i przejdziemy do karty Zasady grupy, odnajdziemy tam informację o przeniesieniu sposobu zarządzania zasadami na konsolę Group Policy Management. Klikając przycisk Open, możemy bezpośrednio wywołać moduł GPMC.

Moduł Group Policy Management

Zainstalowaną konsolę do zarządzania zasadami grupy uruchamiamy, klikając skrót umieszczony w Narzędziach administracyjnych. W głównym oknie konsoli widoczny jest identyfikator lasu Active Directory oraz jego nazwa. Nazwę tę definiujemy podczas instalacji usług katalogowych. Więcej informacji dotyczących instalacji Active Directory można znaleźć w artykułach "Instalacja wprost" oraz "Konfiguracja wstępna". Po rozwinięciu folderu z nazwą lasu usług katalogowych zobaczymy cztery foldery: Domains, Sites, Group Policy Modelling oraz Group Policy Results. Podczas wstępnej konfiguracji zasad grupy najważniejsza jest zawartości folderu Domains.

Rozwinięcie folderu Domains wyświetla listę domen. W przypadku domeny testowej będzie to pl.idg.com. W sieciach korporacyjnych, które grupują wiele domen, lista obiektów mogłaby być znacznie szersza. Zaznaczenie nazwy domeny powoduje wyświetlenie w prawym panelu listy obiektów zasad związanych ze wskazanym pojemnikiem. W tym przypadku będzie to grupa zasad przywiązanych do domeny. Jeśli dodatkowo, klikając plus, rozwiniemy folder domeny pl.idg.com, zostaną wyświetlone skróty do obiektów zasad, jednostki organizacyjne wewnątrz domeny oraz foldery Group Policy Objects i WMI Filters. Lista jednostek organizacyjnych nie zawiera wbudowanych folderów Active Directory, takich jak Users, Builtin lub Computers. Windows Server 2003 nie pozwala na przypisywanie zasad tym pojemnikom.

W folderze reprezentującym domenę odnajdziemy podfolder Group Policy Objects. Zawiera on listę obiektów zasad utworzonych w domenie. Po instalacji Windows Server 2003 znajdują się tam jedynie dwa obiekty. Default Domain Policy to domyślna zasada,

gromadząca ustawienia z całej domeny, obiekt Default Domain Controller Policy przechowuje ustawienia wszystkich kontrolerów domeny.

Wiązanie obiektów zasad z pojemnikami usług katalogowych

Ustawienia określane przez zasady grupy dotyczą kont użytkowników i stacji roboczych umieszczonych w Active Directory. Jedną z zalet tej usługi jest możliwość odwzorowywania struktury organizacyjnej firmy na wielopoziomowe grupy pojemników zawierających użytkowników i komputery. Na przykład dla firmy mającej oddziały w trzech miastach (np. Kalisz, Kielce, Katowice) możemy założyć jednostki organizacyjne odpowiadające nazwom miast, a następnie umieścić w nich komputery i konta z danej lokalizacji. Takie zagnieżdżenia ułatwiają zarządzanie oraz zwiększają czytelność informacji o zasobach sieci. Kontenery na obiekty mogą być wykorzystywane podczas stosowania zasad grupy. Przeniesienie w tym przykładzie ustawień na wszystkie konta użytkowników z Kalisza polega na przypisaniu do jednostki organizacyjnej Kalisz utworzonego i skonfigurowanego obiektu zasad.

Zasady grupy mogą być związane z czterema rodzajami obiektów. Trzy z nich to pojemniki usługi Active Directory, czwartym są zasady lokalne. Do kontenerów usług katalogowych zaliczają się: wspomniana już jednostka organizacyjna oraz domena i lokalizacja. Struktura Active Directory może być wielopoziomowa - jedna domena będzie obejmować wiele lokalizacji oraz jednostek organizacyjnych. Gdy w jednostce organizacyjnej umieścimy kolejną jednostkę, powstanie konstrukcja przypominająca drzewo katalogów. Do każdego z wymienionych obiektów mogą być przypisywane odmienne zasady. Zasady przypisane do pojemników przenoszą się na wszystkie zawarte w nich obiekty. Oznacza to, że jeśli związemy zasadę z obiektem typu domena, wówczas wszystkie konta komputerów i użytkowników będą miały takie ustawienia, jakie przenosi zasada. Zasady określone lokalnie dotyczą środowisk komputerów z uruchomionymi systemami Windows XP i Windows 2000. Ustawienia te nie wykraczają poza komputer, w którym zostały założone.

Warto poznać kolejność implementacji zasad, ponieważ mogą one być wiązane z różnymi typami obiektów. Najpierw wprowadzane są lokalne zasady stacji roboczych klientów sieci, potem zasady złączone z lokalizacją, ustawienie domenowe i na końcu zasady dotyczące jednostek organizacyjnych. Jeśli jednostka zawiera inne jednostki, zasady najbardziej zagnieżdżonego obiektu są dodawane na końcu. Warto pamiętać, że poszczególne obiekty zasad mogą nanosić przeciwne ustawienia, np. zasada domenowa będzie ukrywała Panel sterowania, a zasada jednostki organizacyjnej będzie go pokazywała. W takim wypadku ostatnia wprowadzana zasada nanosi obowiązujące parametry. Domyślnie reguła ta obowiązuje, ale administrator może wskazać zasady, które mają być najważniejsze.

Tworzenie i wiązanie przykładowego obiektu zasad

Poznanie podstawowych sposobów zarządzania zasadami grupy pozwala na przejście do praktycznego wdrożenia ustawień. Rozpoczynamy od budowy założenia niezbędnych obiektów usługi Active Directory. Prezentacja funkcjonowania zasad wymaga kilku jednostek organizacyjnych oraz kont komputerów i użytkowników. Korzystając z modułu Użytkownicy i komputery usługi Active Directory, załóżmy szybko trzy jednostki organizacyjne, np. PCWorld, NetWorld i IT. W każdej umieśćmy po jednym koncie użytkownika i komputera. Użytkownikami niech będą: Jan Kowalski, Piotr Nowak i Adam Michalak, komputery to PCWK1, NW1 i IT1. Szczegółowy opis tworzenia kont i jednostek dostępny jest w pierwszych trzech artykułach.

Domena ma już przypisany jeden obiekt zasad, Default Domain Policy. Zawarte w nim ustawienie są dziedziczone przez wszystkie jednostki organizacyjne i konta. Drugi obiekt to zasada wpływająca na konfigurację kontrolerów domeny i związana z pojemnikiem

Domain Controlers. Naszym zadaniem będzie utworzenie dwóch zasad: przypisanej do domeny oraz związanej z pojemnikiem IT. Zasadę domenową wykorzystamy do konfiguracji środowiska roboczego klientów domeny, natomiast zasadę jednostki organizacyjnej do dystrybucji oprogramowania dla działu IT. Po utworzeniu obiektów w Active Directory uruchamiamy konsolę Group Policy Management. Następnie przechodzimy do folderu Group Policy Objects, umieszczonego w domenie pl.idg.com, i z menu Akcja wybieramy New. W nazwie tworzonego obiektu wpisujemy np. Ustawienia standardowe IDG. Ponieważ mamy utworzyć dwa obiekty, czynność powtarzamy. Drugi obiekt nazywamy np. Dystrybucja oprogramowania IT. Po założeniu zasad lista obiektów w pojemniku Group Policy Objects rozszerzyła się o dwa elementy.

Kolejną czynnością jest powiązanie obiektów zasad z pojemnikami. Zasadę Ustawienia standardowe IDG musimy przypisać do domeny pl.idg.com, natomiast Dystrybucję oprogramowania IT do jednostki organizacyjnej IT. Klikamy ikonę reprezentującą domenę i z menu Akcja wybieramy Link an Existing GPO. W oknie Select GPO zaznaczamy zasadę Ustawienia standardowe IDG i klikamy OK. W ten sposób połączyliśmy obiekt zasad z domeną IDG. Ponieważ musimy połączyć jeszcze drugą zasadę, przechodzimy do folderu IT i powtarzamy poprzednią czynność. Naturalnie w tym przypadku wskazujemy obiekt Dystrybucja oprogramowania IT. Po naciśnięciu OK mamy założone i przypisane dwa puste obiekty zasad grupy. W celu skonfigurowania ustawień zasad należy zaznaczyć zasadę i z menu Akcja wybrać Edit.

Konfiguracja ustawień komputera

Po otwarciu edytora obiektów zasad zobaczymy dwa foldery: ustawienia komputera i ustawienia użytkownika. Kliknięcie folderu Konfiguracja komputera wyświetla trzy podfoldery: Ustawienia oprogramowania, Ustawienia systemu Windows oraz Szablony administracyjne. Konfiguracja dystrybucji oprogramowania oraz ustawienia systemu Windows zostaną opisane oddzielnie, natomiast teraz zajmiemy się zawartością folderu Szablony administracyjne.

Po jego kliknięciu zobaczymy foldery Składniki systemu Windows, System, Sieć oraz Drukarki. Umieszczone w nich ustawienia konfigurują wybrane parametry środowiska pracy komputera w domenie, np. po rozwinięciu folderu Składniki systemu Windows widać serię podfolderów zmieniających ustawienia komponentów: Internet Explorer, Zgodność aplikacji, Harmonogram zadań, Usługi terminalowe, Windows Update itd. Przechodząc do folderu System, możemy skonfigurować parametry Profili użytkownika, Skryptów, Logowania, Przydziałów dysków, Logowania do sieci, Ochrony plików systemowych, Raportowania błędów itd. Folder Sieć służy do zmiany parametrów sieciowych komputera. Korzystając z tych ustawień, administrator może zmienić konfigurację takich elementów, jak Klient DNS, Połączenia sieciowe lub Pliki trybu offline. Ostatni z folderów - Drukarki - jest przeznaczony do przypisywania parametrów związanych ze współpracą usługi Active Directory ze środowiskiem wydruku komputera.

Należy pamiętać, że modyfikacja ustawień komputera nie zależy od użytkownika zalogowanego do danej stacji. Skonfigurowanie parametrów na przykład przydziałów dyskowych będzie dotyczyło każdego z pracowników. Przypisując ustawienia komputera, należy dokładnie zapoznać się z funkcjonowaniem parametru oraz konsekwencjami jego włączenia.

Konfiguracja zasad użytkownika

Ustawienia dotyczące kont użytkowników sieci są podobne do parametrów komputerów. Przy konfiguracji użytkowników również odnajdziemy trzy foldery: Ustawienia oprogramowania, Ustawienia systemu Windows oraz Szablony administracyjne. Parametry w nich zawarte mają niewielką część wspólną i zwykle określają inne ustawienia systemu operacyjnego.

Szablony administracyjne zawierają grupę elementów konfigurujących środowisko pracy użytkownika. Parametry przenoszone przez szablony są wplatane w część Rejestru systemu Windows, przechowującą profil użytkownika. Podobnie jak w przypadku komputera, po rozwinięciu folderu Składniki systemu Windows możemy zmodyfikować konfigurację komponentów typu Internet Expolorer, NetMeeting, Windows Update itd. Ustawienia nie są jednak takie same. W przypadku Internet Explorera możemy ukrywać opcje menu, paski narzędzi oraz zabraniać modyfikacji środowiska przeglądarki. W Składnikach systemu Windows pojawia się folder Eksploratora Windows. Wprowadzone w nim parametry pozwalają na wyłączanie niektórych z opcji Eksploratora, np. usunięcie karty Zabezpieczenia przy przeglądaniu właściwości plików i folderów systemu NTFS.

Grupa folderów Sieć, Pulpit, Panel sterowania i Menu Start oraz Pasek zadań jest przeznaczona do ukrywania i zabraniania dostępu do poszczególnych części systemu. Na przykład włączenie opcji Ukryj i wyłącz wszystkie elementy pulpitu opróżnia pulpit klientów domeny. Jeśli nie chcemy, żeby użytkownicy ingerowali w lokalne ustawienia Windows, zaznaczamy opcję Zabroń dostępu do Panelu sterowania. W folderze Sieć ustalamy dostęp do parametrów połączeń sieciowych i plików trybu offline, np. możliwość zmiany zaawansowanej konfiguracji protokołu TCP/IP. W folderze System określamy właściwości przetwarzania skryptów, zasad grupy, profili użytkownika lub logowania. Dostępne tu opcje pozwalają między innymi na wyłączenie dostępu do Menedżera zadań lub opcji Zablokuj komputer.

Przekierowanie folderów

Umieszczony w parametrach użytkownika folder Ustawienia systemu Windows zawiera bardzo interesującą grupę parametrów - przekierowanie folderu. Domyślnie takie foldery, jak Moje dokumenty, są przechowywane na stacjach roboczych klientów sieci. Wykonywanie kopii zapasowych, monitorowanie zawartości czy przestrzeni dyskowej jest wówczas bardzo utrudnione. Przekierowanie pozwala na przeniesienie grupy osobistych folderów klientów sieci do jednego, centralnego miejsca, np. wolumenu na serwerze. Konfiguracja tych ustawień pozwala na uniknięcie kłopotów z rozproszeniem danych użytkowników, dodatkowo dostęp do plików jest gwarantowany nawet wtedy, gdy pracownik loguje się na innym komputerze.

Administrator sieci może przekierować takie foldery, jak: Dane aplikacji, Moje dokumenty, Pulpit oraz Menu Start. Po wskazaniu miejsca przechowywania plików, użytkownicy będą automatycznie zapisywali swoje dokumenty na dysku serwera. Jeśli użytkownik otworzy skrót Moje dokumenty na pulpicie, zostanie przekierowany do folderu na serwerze. Naturalnie każdy z pracowników może mieć indywidualny folder na swoje dokumenty. Nie musimy się wówczas martwić o ryzyko nieuprawnionego dostępu do zasobów. Jeżeli dane zapisywane są na partycji NTFS, system automatycznie zabezpiecza pliki, nadając odpowiednie uprawnienia. Włączenie przekierowania folderów Menu Start i Pulpit pozwala na ustandaryzowanie ich elementów u wszystkich pracowników firmy. Po wskazaniu centralnego źródła danych o folderach Pulpit i Menu Start, należy skopiować do niego skróty do aplikacji lub narzędzi i przypisać użytkownikom uprawnienia do odczytu zawartości.

Przekierowanie każdego z folderów jest konfigurowane indywidualnie. Po zaznaczeniu np. folderu Moje dokumenty z menu Akcja wybieramy polecenie Właściwości. Okno konfiguracyjne zawiera dwie karty: Miejsce docelowe i Ustawienia. Domyślnie na karcie Miejsce docelowe zaznaczona jest opcja Nie skonfigurowano. W celu przekierowania folderu należy wybrać odpowiednią wartość z listy rozwijanej: Podstawowe - Przekierowuj wszystkie foldery do tej samej lokalizacji lub Zaawansowane - Określaj lokalizacje dla różnych grup użytkowników. Pierwszy parametr pozwala na wskazanie jednej z czterech lokalizacji: Przekieruj do katalogu macierzystego użytkownika, Utwórz folder dla każdego użytkownika w ścieżce katalogu głównego, Przekieruj do następującej lokalizacji i

Przekieruj do lokalnej lokalizacji profilu użytkownika. Najczęściej korzystamy z opcji trzeciej, ponieważ możemy określić dokładne położenie danych użytkowników. Po wyborze lokalizacji w polu Ścieżka do katalogu głównego wpisujemy informacje o położeniu dokumentów. Ścieżkę wprowadzamy zgodnie z notacją UNC w postaci \\nazwa_serwera\nazwa_udostępnienia, przy czym udostępnienie musi być założone wcześniej. Na końcu ścieżki należy wprowadzić zmienną %username%, dzięki temu dla każdego z użytkowników zostanie utworzony oddzielny folder do przechowywania dokumentów. Przykładowy wpis może wyglądać następująco \\W2k3SRV\UserDoc\%username%. Po wyborze zaawansowanych ustawień przekierowania, możemy skonfigurować odmienne ścieżki dla różnych grup zabezpieczeń domeny Windows Server 2003.

Konfiguracja skryptów zasad grupy

W zasadach grupy umieszczono jeszcze jedną funkcję pozwalającą na kontrolowanie środowiska komputera i użytkownika. Korzystając ze skryptów, administrator zrealizuje te zadania konfiguracyjne, których nie można wykonywać, korzystając z szablonów lub innych ustawień zasad grupy. Windows Server 2003 pozwala na skonfigurowanie pięciu rodzajów skryptów. Najstarszy sposób został już opisany przy okazji omawiania właściwości kont użytkowników, patrz artykuł "Administracja od podstaw". Teraz przejdziemy do pozostałych typów skryptów administracyjnych.

Okno konfiguracyjne folderu Ustawienia systemu Windows zawiera podfolder Skrypty. Jest dostępny zarówno w konfiguracji komputera, jak i użytkownika. Dla stacji możemy uruchamiać skrypty uruchamiania i zamykania systemu, dla kont klientów sieci - logowania i wylogowania. Jeśli skryptów będzie więcej niż jeden, domyślna kolejność ich uruchamiania nie jest taka sama. Skrypty komputera są przetwarzane synchronicznie w kolejności występowania w oknie właściwości typu skryptu, zatem jeśli są na przykład dwa, pierwszy musi zakończyć działanie, aby został uruchomiony kolejny. Gdy użytkownik się loguje, skrypty są przetwarzane asynchronicznie, czyli kolejność rozpoczęcia i kończenia działania nie ma znaczenia. W skryptach możemy umieszczać polecenia systemu operacyjnego (pliki z rozszerzeniem BAT lub CMD) lub polecenia środowiska Windows Scripting Host dla plików VBS lub JS.

Obiekty zasad grupy są uwzględniane w określonej kolejności. Każdy może przechowywać ustawienia użytkownika oraz komputera. Ustawienia te nie są wprowadzane w tym samym czasie. W momencie startu systemu, przed pojawieniem się okna logowania, ładowana jest część zasad dotycząca maszyny. Dopiero po zalogowaniu, kiedy Windows wie, kto się uwierzytelnił, dodawane są zasady konta użytkownika. Ponieważ są cztery typy skryptów, każdy z nich jest również uruchamiany w innym momencie: najpierw skrypty uruchamiania komputera, a po udanym uwierzytelnieniu klienta skrypty logowania. Podczas kończenia pracy z Windows najpierw przetwarzane są skrypty wylogowywania, a dopiero po nich zamykania systemu.

Konfiguracja zabezpieczeń

Do najważniejszych zadań zasad grupy możemy zaliczyć konfigurację zabezpieczeń. Centralne zarządzanie bezpieczeństwem domeny pozwala administratorom na szybkie przenoszenie kluczowych ustawień do komputerów wewnątrz sieci. Głównym sposobem szybkiego skonfigurowania ochrony zasobów domeny jest modyfikacja parametrów w folderze Ustawienia zabezpieczeń konfiguracji komputera.

Dostęp do folderu uzyskujemy przez Edytor obiektów zasad grupy. Microsoft umieścił również dodatkowe skróty do zasad związanych z bezpieczeństwem w Narzędziach administracyjnych. Klikając Start | Narzędzia administracyjne odnajdziemy konsole Zasady zabezpieczeń domeny oraz Zasady zabezpieczeń kontrolera domeny. Każda z nich przenosi do parametrów konfiguracji zabezpieczeń, przy czym pierwsza modyfikuje

wbudowaną domyślną zasadę domeny, a druga domyślną zasadę stosowaną do jednostki organizacyjnej Domain Controllers.

Po przejściu do ustawień zabezpieczeń lub uruchomieniu jednego z modułów widzimy grupę folderów konfiguracji bezpieczeństwa różnych komponentów systemu: Zasady konta, Zasady lokalne, Dziennik zdarzeń, Grupy z ograniczeniami, Usługi systemowe, Rejestr, System plików, Zasady sieci bezprzewodowej, Zasady kluczy publicznych, Zasady ograniczeń oprogramowania oraz Zasady zabezpieczeń IP.

Zasady konta

W zabezpieczaniu komputerów niebagatelną rolę odgrywają hasła dostępu. Im mocniejsze hasło, tym trudniej je złamać. Domyślnie Windows Server 2003 wymusza stosowanie mocnych haseł. Ich ustawienia konfigurowane są w Zasadach konta. W folderze tym możemy również określić parametry blokowania dostępu do stacji oraz zasady protokołu Kerberos.

Domyślnie przypisane zasady haseł mogą irytować niecierpliwych klientów sieci. Jeśli hasło musi być złożone i liczyć co najmniej siedem znaków, to pracownicy muszą się naprawdę postarać, żeby system zaakceptował ich hasła. Jeśli opcja Hasło musi spełniać wymagania co do złożoności jest zaznaczona, użytkownicy muszą ustawiać takie hasła, które spełniają trzy z podanych niżej czterech warunków: zawierać co najmniej jedną wielką literą, małą literę, cyfrę lub znak spoza grupy znaków alfanumerycznych. Pozostałe parametry dotyczą takich elementów jak: minimalny i maksymalny okres ważności oraz pamiętanie historii wprowadzanych haseł.

Kolejny folder zawiera zasady blokady konta. Ich modyfikacja ogranicza możliwość popełnienia przez użytkowników błędów przy logowaniu. Umieszczono w nim jedynie trzy opcje: czas trwania blokady konta, próg blokady oraz czas, po jakim licznik blokady konta ma zostać wyzerowany. Jeśli określimy, że próg blokady to pięć pomyłek, a czas wynosi 30 minut, to klienci logujący się do domeny, w ciągu 30 minut będą mogli się pomylić jedynie cztery razy, piąta pomyłka zakończy się zablokowaniem konta na pół godziny. Po zablokowaniu konta klient musi odczekać ustalony czas lub powiadomić administratora domeny. Administrator może odblokować konto, usuwając zaznaczenie opcji Konto jest zablokowane, umieszczonego we właściwościach konta w module Użytkownicy i komputery usługi Active Directory. Konto administratora nie jest blokowane nawet po wielu błędach logowania.

Zasady protokołu Kerberos dotyczą parametrów protokołu domyślnie wykorzystywanego przez serwer do uwierzytelniania użytkowników domeny. Przenoszonych przez zasady ustawień nie należy modyfikować bez wyraźnej potrzeby.

Zasady lokalne i dziennik zdarzeń

Folder Zasady lokalne zawiera jedne z bardziej istotnych ustawień związanych z bezpieczeństwem domeny Windows Server 2003 - oferuje możliwość konfiguracji zasad inspekcji, praw użytkowników oraz przypisania opcji zabezpieczeń.

Prawa użytkowników określają, jakie czynności w systemie operacyjnym mogą wykonywać użytkownicy lub ich grupy. Nie należy mylić praw z uprawnieniami do obiektów. Uprawnienia są ściśle związane z czynnościami dozwolonymi przy dostępie do plików w systemie NTFS, rejestru, drukarek itd. Prawa możemy traktować jako przywileje wykonywania działań w obrębie całego komputera, np. prawo do wykonywania kopii zapasowych lub zmiany czasu systemowego. W wypadku domen Windows Server 2003 centralne zarządzanie prawami daje znaczne korzyści, np. łatwo zdefiniować, kto jest uprawniony do wykonywania kopii stacji roboczych. Zarządzanie prawami wymaga

ostrożności, ponieważ prawa określone na poziomie domeny zastępują parametry lokalne.

Folder Opcje zabezpieczeń zawiera dodatkowe parametry zwiększające bezpieczeństwo systemu. Ustawienia są podzielone na kilka grup związanych z domeną, dostępem sieciowym, logowaniem itd. Warto na przykład włączyć dwie opcje: Logowanie interakcyjne: nie wyświetlaj nazwy ostatniego użytkownika i Konta: Stan konta gościa. Zastosowanie zasad inspekcji omówiliśmy w poprzednich artykułach. Warto tylko przypomnieć, że zmiana ustawień folderu pozwala na wskazanie, jakie działania i zasoby systemu mają być monitorowane przez Windows. Zdarzenia odnotowywane przez system zapisywane są w dziennikach Podglądu zdarzeń. Modyfikacja zasad inspekcji na poziomie domeny spowoduje automatyczną modyfikację ustawień we wszystkich stacjach przynależących do domeny.

Dziennik zdarzeń jest folderem narzucającym konfigurację dzienników przechowywanych przez Podgląd zdarzeń. Dostępne w nim zasady służą do określania takich parametrów, jak maksymalny rozmiar dziennika, czas przechowywania informacji przez dzienniki, dostęp do informacji dla grupy goście oraz sposoby postępowania systemu na wypadek przepełnienia się dzienników. Ponieważ domyślnie na każdej stacji są dzienniki systemu, aplikacji oraz zabezpieczeń, parametry mogą być określane oddzielnie dla każdego z nich.

Konfiguracja uprawnień, usług i grup zabezpieczeń

Kolejne modyfikacje ustawienia zabezpieczeń przeprowadza się w folderach Grupy z ograniczeniami, Usługi systemowe, Rejestr i System plików. Dużej uwagi wymaga konfiguracja Grup z ograniczeniami, bo pozwala określić, które konta użytkowników mają należeć do grup zabezpieczeń. Jeśli chcemy na przykład, żeby członkiem grupy Użytkownicy zaawansowani na wszystkich stacjach roboczych był wyłącznie Jan Kowalski, należy wpisać nazwę grupy, a następnie dodać do niej konto Jana Kowalskiego. Grupy z ograniczeniami należy konfigurować bardzo ostrożnie, bo system nie tylko dodaje konta do grupy, ale również usuwa z nich użytkowników, którzy nie zostali wymienieni. W ten sposób możemy przez przypadek usunąć wszystkie konta z grup lokalnych.

W folderze Usługi systemowe administrator domeny konfiguruje parametry usług w systemach klientów sieci. W ten sposób można określić, które usługi mają być uruchamiane automatycznie w czasie startu stacji, a które wyłączone. Dodatkowo dostępne są parametry pozwalające na zdefiniowanie uprawnień do wskazanych usług. W celu zwiększenia wydajności systemu administrator może np. centralnie wyłączyć usługę Kompozycje.

W folderach Rejestr oraz System plików modyfikujemy uprawnienia dostepu do Rejestru oraz zasobów przechowanych na partycjach NTFS. Jeśli w każdym komputerze w firmie jest zainstalowana ta sama usługa (aplikacja) i chcemy, żeby dostęp do jej folderu był ściśle określony, możemy posłużyć się ustawieniami zabezpieczenia plików. Po skonfigurowaniu zasad grupy uprawnienia zostaną przekazane wskazanym plikom i folderom. Administrator nie będzie musiał przypisywać ich ręcznie na każdym z komputerów w domenie. Uprawnienia do kluczy w Rejestrze są implementowane w ten sam sposób - dodajemy klucz i określamy uprawnienia. Nadane parametry zostaną automatycznie przekazane stacjom klientów.

Pozostałe foldery ustawień zabezpieczeń

W domenach Windows Server 2003 folder Zasady kluczy publicznych jest wykorzystywany wtedy, gdy stosujemy certyfikowanie lub system szyfrowania plików (EFS). Po utworzeniu zasad kluczy publicznych administratorzy domeny mogą elastyczniej zarządzać wydawaniem certyfikatów lub wdrażaniem systemu szyfrowania

plików. W folderze Zasady kluczy publicznych jest grupa podfolderów przeznaczonych do konfiguracji komponentów PKI. Na przykład w folderze System szyfrowania plików można zdefiniować nowe agenty odzyskiwania plików zaszyfrowanych przez użytkowników domeny, których konta zostały usunięte.

Zastosowanie zasad ograniczeń oprogramowania pozwala administratorom na określenie, które aplikacje użytkownicy mogą uruchamiać na swoich stacjach, a których nie. Dostęp do Internetu wiąże się z możliwością automatycznego instalowania i uruchamiania szkodliwych programów, zatem opcja ta jest wyjątkowo przydatna. Aplikacje są konfigurowane według reguł określonych przez administratora.

Zasady zabezpieczeń IP poprzez protokół IPSec pozwalają na ochronę informacji przesyłanych przez sieć. Jeżeli możliwe jest podsłuchiwanie komunikacji sieciowej, administratorzy domeny powinni zdefiniować odpowiednie reguły weryfikujące integralność lub szyfrujące przesyłane dane. Domyślnie system oferuje trzy rodzaje zasad protokołu IPSec: Server (Request Security), Client (Respond Only) oraz Secure Server (Require Security). Każda przypisuje odmienne sposoby wdrażania bezpiecznej komunikacji. Aby włączyć zasadę, należy zaznaczyć odpowiednie opcje i wybrać z menu Akcja polecenie Przypisz.

Ostatni z folderów zabezpieczeń to Zasady sieci bezprzewodowej. Jeśli dostęp do zasobów jest w firmie realizowany przez sieci bezprzewodowe, administrator może zdefiniować zasadę globalnie konfigurującą ustawienia klientów. Jej parametry służą do określenia takich elementów, jak konfiguracja ustawień połączenia, sposób uwierzytelniania klientów czy wskazanie preferowanej sieci bezprzewodowej.

Konfiguracja zasad dystrybucji oprogramowania

Zasady grupy Windows Server 2003 zawierają jeszcze jedną bardzo interesującą usługę. Administratorzy domeny mogą instalować oprogramowanie klientów sieci bez podchodzenia do komputerów pracowników. Dystrybucja oprogramowania do klientów domeny może być realizowana przez konfigurację zasad użytkownika lub komputera. Jeśli aplikacja zostanie przypisana do ustawień komputera, wówczas będzie dostępna dla wszystkich pracowników korzystających z danej stacji. Przywiązanie oprogramowania do ustawień użytkownika sprawia, że aplikacja jest dostępna tylko dla danego klienta.

Oprogramowanie jest dostarczane klientom domeny za pomocą odpowiednio przygotowanych pakietów. Pakiety mogą mieć rozszerzenie MSI lub ZAP. Pliki MSI są związane z usługą Windows Installer, której zadaniem jest zarządzanie, zautomatyzowanie instalacji i deinstalacji oprogramowania. Pakiety instalatora można porównać do bazy przechowującej instrukcje i dane na temat oprogramowania. Dzięki temu aplikacje mogą być dynamicznie diagnozowane, naprawiane i reinstalowane. Jeśli wersja instalacyjna oprogramowania nie zawiera pakietów MSI, administrator sieci, używając dodatkowego komercyjnego oprogramowania, może je przygotować ręcznie. Innym rozwiązaniem jest zastosowanie plików ZAP. Więcej informacji o tworzeniu pakietów ZAP zawiera witryna www.microsoft.com/technet.

Są dwa sposoby dystrybucji oprogramowania: przywiązanie oraz publikacja. Przywiązanie aplikacji do obiektu komputer powoduje, że jest ona instalowana automatycznie w czasie startu stacji klienta. Przed wyświetleniem okna logowania widoczny jest wówczas komunikat informujący o instalacji oprogramowania. Jeśli przywiążemy aplikacje do obiektu użytkownik, instalacja pakietu nastąpi wówczas, gdy klient sieci kliknie rozszerzenie skojarzone z aplikacją np. DOC do Worda lub XLS do Excela. Publikowanie oprogramowania instaluje pakiety w nieco inny sposób. Opublikowanie aplikacji dla obiektu komputer sprawia, że jest dostępna po kliknięciu rozszerzenia związanego z aplikacją. Publikacja związana z obiektem użytkownik udostępnia informację o możliwości instalacji programu w Dodaj/Usuń programy.

Konfiguracja dystrybucji oprogramowania jest procesem kilkuetapowym. Najpierw należy założyć i udostępnić katalog, który będzie gromadził wersje instalacyjne aplikacji. Może to być np. folder Aplikacje na partycji D. Następnie w konsoli Group Policy Management wybieramy obiekt, do którego chcemy przypisać aplikację, i wywołujemy edytor zasad grupy. Omawialiśmy w tym artykule zakładanie obiektu Dystrybucja oprogramowania IT, przypisanego do jednostki organizacyjnej IT. Jeśli chcemy, aby wszyscy pracownicy tego działu mieli dostęp do narzędzi administracyjnych, należy przejść do obiektu Dystrybucja oprogramowania IT i z menu podręcznego wybrać Edit. Do instalacji modułów zarządzania systemem wykorzystamy pakiet Adminpack.msi, dostępny na płycie instalacyjnej Windows Server 2003. Najbardziej aktualna wersja tego pakietu jest umieszczona w witrynie download.microsoft.com. Ponieważ kontom pracowników działu IT chcemy przyznać dostęp do narzędzi administracyjnych, pakiet należy skonfigurować w folderze Instalacja oprogramowania obiektu Konfiguracja użytkownika. Po otworzeniu edytora przechodzimy do ustawień użytkowników, zaznaczamy folder Instalacja oprogramowania i z menu Akcja wybieramy Nowy | Pakiet. W nowym oknie należy wskazać ścieżkę do pakietu adminpak.msi. Jeśli w domenie będziemy dystrybuować wiele aplikacji, powinniśmy założyć oddzielny folder na każdy z programów, np. AdminPak, i tam umieścić pobrany z Internetu pakiet. Następnie wprowadzamy ścieżkę do pliku zgodnie ze standardem UNC, w naszym przykładzie będzie to \\idgtest\aplikacje\adminpak\adminpak.msi. Po wprowadzeniu ścieżki określamy metodę rozmieszczenia pakietu: opublikowanie, przypisanie lub zaawansowane. Dodatkowe parametry dystrybucji pakietu możemy skonfigurować we właściwościach adminpak.msi. Zamknięcie wszystkich okien kończy konfigurację publikacji oprogramowania.

Zaawansowana konfiguracja ustawień zasad

Jeśli domena Windows Server 2003 obejmuje wiele stacji i kont użytkowników, konfiguracja zasad grupy może wymagać dodatkowych działań administracyjnych. Wszystkie przeprowadzamy, modyfikując właściwości zasad w module Group Policy Management. Zaznaczenie w lewym panelu jednego z obiektów typu pojemnik, np. domeny pl.idg.com, powoduje wyświetlenie w prawym panelu okna, które zawiera trzy karty: Linked Group Policy Objects, Group Policy Inheritance oraz Delegation. Pierwsza karta przedstawia listę zasad oraz ich właściwości. Jeśli do domeny lub jednostki organizacyjnej przypiszemy wiele zasad, istotne znaczenie ma kolejność wdrażania obiektów. Przyciskami Move link to top, Move Link up, Move link down i Move link to bottom możemy zmienić kolejności implementacji. Najwyższy priorytet będzie miała pierwsza zasada na liście. Warto pamiętać, że nie jest to równoznaczne z pierwszeństwem w implementacji. Ostatni obiekt zasad zastosowany do użytkownika lub komputera jest najważniejszy, bo to jego ustawienia mogą zastąpić przekazane wcześniej parametry. Przesunięcie zasady na pierwsze miejsce oznacza, że będzie ona stosowana na końcu. Karta Group Policy Inheritance wyświetla listę zasad odziedziczonych z obiektów nadrzędnych lub przypisanych bezpośrednio. Parametry zasad, podobnie jak uprawnienia w systemie plików NTFS, są dziedziczone. Oznacza to, że jeśli do domeny przypiszemy zasadę ukrywającą polecenie Uruchom z menu Start, to użytkownicy, których konta są zlokalizowane w wewnętrznych jednostkach organizacyjnych lub ich podjednostkach, po zalogowaniu nie zobaczą polecenia Uruchom. Ostatnia karta - Delegation - wyświetla listę kont grup lub użytkowników, którzy mogą zarządzać uprawnieniami do obiektów zasad w zaznaczonym pojemniku.

Rozwinięcie w lewym panelu ikony reprezentującej domenę wyświetla listę związanych z nią zasad, jednostek organizacyjnych oraz dwa dodatkowe foldery: Group Policy Objects oraz WMI Filters. Po zaznaczeniu pierwszego zobaczymy listę wszystkich obiektów zasad, zdefiniowanych w Active Directory. WMI Filters zawiera listę filtrów WMI. Foldery te pomagają uzyskać informacje o każdym z założonych obiektów. Poszczególne obiekty zasad mogą być związane z wieloma pojemnikami. Tak jak w systemie plików, jeden plik

może mieć wiele skrótów. Jeśli zmodyfikujemy obiekt zasad, wówczas skutki tej zmiany obejmą wszystkie pojemniki, z którymi zasada jest związana.

Zaznaczenie obiektu zasad w lewym panelu Group Policy Management wyświetla karty opisujące jego właściwości. Na karcie Scope są informacje na temat listy powiązanych z obiektem pojemników, filtrowaniem zabezpieczeń oraz filtrami WMI. Konfiguracja filtrowania oznacza wskazanie, do których kont użytkowników, grup lub komputerów zasada ma zostać przypisana. Podobne rezultaty daje zastosowanie filtrów WMI. Każdy obiekt zasad może mieć dodany filtr WMI, który będzie zawężał zakres obiektów podlegających zasadzie na przykład do stacji pracujących pod kontrolą Windows XP.

Standardowa zasada zawiera parametry przenoszone na użytkowników oraz na komputery. Jeśli ustanawiamy zasadę dotyczącą jednostki organizacyjnej zawierającej wyłącznie komputery, przetwarzanie ustawień związanych z użytkownikiem nie jest konieczne. Podobnie będzie w wypadku pojemników, w których umieścimy jedynie konta użytkowników. Na karcie Details możemy określić stan obiektu zasad. Do wyboru mamy jedno z czterech ustawień: All settings disabled, Computer configuration settings disabled, User configuration settings disabled i Enabled. Przypisując jeden z parametrów, wskazujemy sposób przetwarzania zasad.

Swoje właściwości mają także dowiązania obiektów zasad. Podobnie do skrótów do plików i folderów, ikonę reprezentującą dowiązanie rozpoznajemy po małej strzałce umieszczonej w lewym dolnym rogu. Każde z dowiązań możemy włączyć lub wyłączyć. Wówczas tylko wskazane dowiązanie, a nie cała zasada przestaje być aktywne. Innym parametrem dowiązań jest wymuszanie implementacji. Parametr Enforce wymusza przypisanie ustawień zawartych w obiekcie zasad, bez względu na kolejność, poziom i ewentualne konflikty. Jeśli na przykład powiążemy zasadę z domeną, jest ona przetwarzana wcześniej niż zasady jednostek organizacyjnych. Parametry zasady jednostek mogą zmienić ustawienia domenowe, ponieważ są dodawane później. Aby zapobiec niechcianym zmianom, należy w dowiązaniu do domeny włączyć opcję Enforced. Właściwości dowiązań konfigurujemy, zaznaczając ikonę dowiązania i wybierając odpowiednie polecenie z menu Akcja.

Monitorowanie i testowanie zasad grupy

Rezultaty implementacji zasad monitorujemy, korzystając z Group Policy Management lub grupy narzędzi wiersza poleceń. Zastosowanie konsoli zarządzania zasadami jest najlepszym rozwiązaniem. Raport o ustawieniach przenoszonych przez każdą z zasad odnajdziemy, klikając kartę Settings we właściwościach obiektu lub dowiązania. Przy użyciu poleceń show all, show i hide możemy sprawdzać, co konfiguruje zakres użytkownika, komputera lub cała zasada. Raport zawiera informacje o ustawieniach zasad, które mają wprowadzone wartości lub przypisane ustawienia Enabled lub Disabled. Wszystkie elementy z parametrem Not configured są pomijane.

Jeśli w domenie jest wiele obiektów, raport o ustawieniach pojedynczych zasad będzie mało przydatny. Znając ustawienia wprowadzane przez każdy z obiektów, administrator i tak musiałby kolejno analizować priorytety i zagnieżdżenia każdej z zasad. Jeśli dodatkowo uwzględnimy możliwość blokowania dziedziczenia lub wymuszanie przypisywania zasad, wywnioskowanie efektywnych ustawień byłoby niezmiernie trudne. Group Policy Management zawiera foldery Group Policy Modeling oraz Group Policy Results, które pozwalają na szczegółową analizę wszystkich dodawanych obiektów zasad grupy.

Group Policy Results to narzędzie do analizy faktycznych rezultatów stosowania zasad grupy dla określonego konta użytkownika lub komputera. Raport o dodawanych ustawieniach otrzymamy po uruchomieniu kreatora przetwarzania zasad. W celu ustalenia, jakie ustawienia będą dodane do ustawień komputera i użytkownika, należy

uruchomić kreator i wprowadzić nazwy analizowanych kont. Po kilku chwilach mamy wygenerowany raport o wynikowym zestawie zasad.

Opcja Group Policy Modeling służy do analizowania planowanych zmian w zasadach grupy. Pozwala łatwo ustalić skutki przeniesienia konta użytkownika do nowej jednostki organizacyjnej, wpływ priorytetów zasad podczas przetwarzania kont komputera i użytkownika itp.

Jacek Ścisławski

IDG.PL
Uzdolnienia sieciowe Windows Server 2003
PC World Komputer

wersja do wydruku
|strona główna | wersja oryginalna|

Serwery firmowe muszą być uniwersalne jak scyzoryk szwajcarskiej armii. Lista zadań stawianych przed sieciowym systemem operacyjnym może być niewyobrażalnie długa. Oprócz obsługi potrzeb lokalnych klientów, trzeba wykonywać inne, narzucone przez administratora czynności. Zobaczmy, czy Windows Server 2003 nie pozostaje w tyle za konkurencją.

Udostępnianie plików i drukarek, uwierzytelnianie użytkowników, ochrona zasobów, centralne zarządzanie, to tylko niektóre z wielu zadań, jakie stawiane są przed sieciowym systemem operacyjnym. Realizacja dodatkowych usług sieciowych umożliwiających zdalny dostęp do serwera, automatyczną dystrybucję uaktualnień do komputerów sieciowych czy swobodną wymianę informacji to zalety Windows Server 2003, o których nie należy zapominać. Konfiguracja każdego z komponentów jest realizowana przez serię przyjaznych kreatorów.

Usługi sieciowe Windows Server 2003

Serwer jest komputerem, którego zadaniem jest świadczenie usług dla klientów sieci. Funkcje związane z udostępnianiem plików i drukarek są traktowane jako absolutne minimum obowiązków systemu sieciowego. Nowoczesne firmy oczekują od systemu operacyjnego serwera, znacznie szerszej oferty usług. Większe możliwości pozwalają

osiągnąć przedsiębiorstwu lepsze efekty. Nowoczesny produkt musi oferować bezpieczny i uniwersalny dostęp do informacji, niezależnie od miejsca, z którego łączy się użytkownik.

Z danych przechowywanych przez serwer najczęściej korzystają klienci sieci lokalnej. Lokalne usługi sieciowe są stale rozbudowywane o nowe, dodatkowe opcje ułatwiające prace użytkownika lub administratora. Twarde podziały środowisk na LAN i WAN powoli zanikają. Do znanych od lat serwerów DNS, WINS czy DHCP, dodawane są usługi zapewniające dostęp do Internetu, zabezpieczające przed utratą danych lub chroniące przesyłane informacje. Działanie Windows Server 2003 jako serwera plików, DNS czy DHCP już omówiliśmy. Obecnie sięgniemy do oferty rozszerzającej funkcjonalność serwera o usługi zdalnego dostępu, automatyczną aktualizację oprogramowania oraz aplikację ułatwiającą wymianę informacji w sieci lokalnej i rozległej, jaką jest SharePoint.

Rola serwera dostępu zdalnego/sieci VPN

Rola serwera zdalnego dostępu jest związana z uruchomieniem usługi Routing i dostęp zdalny. Głównym zadaniem stawianym przed tą usługą jest zapewnienie pracownikom mobilnym dostępu do sieci komputerowej firmy. W zależności od sposobu nawiązywania komunikacji, klienci mogą łączyć się przez wirtualne sieci prywatne lub za pomocą modemu telefonować do serwera. Działanie usługi RRAS (Routing and Remote Access) nie ogranicza się do przyjmowania połączeń z sieci rozległej. Jej dodatkowymi atutami jest możliwość trasowania pakietów między dwoma sieciami pracującymi z protokołem TCP/IP lub IPX/SPX, zapewnienie podstawowej ochrony dostępu przez filtrowanie pakietów i zaporę połączenia internetowego, a także funkcjonowanie jako serwer pośredniczący w komunikacji klientów sieci z Internetem.

Konfiguracja Windows Server 2003 jako serwera dostępu zdalnego nie jest procesem trudnym, wymaga jednak od administratora określenia właściwych parametrów w kilku komponentach systemu. Zmiana właściwości komputera powinna być naniesiona po rozważnej analizie potrzeb i możliwości firmy. Podstawowym zadaniem jest dobór odpowiednich sposobów nawiązywania połączenia. Dostęp do zasobów sieci może być realizowany przez połączenia typu Dial-up lub wirtualne sieci prywatne (VPN). Do zestawienia pierwszego typu połączenia, serwer oraz klient muszą mieć zainstalowane i skonfigurowane modemy analogowe lub ISDN. Łączność odbywa się przez linie komutowane lub cyfrowe. Zaletą komunikacji wdzwanianej jest nieograniczony dostęp do łączy telefonicznych. Połączenia Dial-up mogą być nawiązywane bez większych kłopotów z każdego zakątka kraju. Problemem przy łączności modemowej jest słaba wydajność łączy oraz wysokie koszy połączeń międzynarodowych i międzymiastowych. Jeśli pracownik będzie sporadycznie łączył się z firmą z różnych miejsc i przesyłał małe porcje informacji, połączenia Dial-Up mogą być wystarczające. Komunikacja wdzwaniana często znajduje zastosowanie jako forma zabezpieczenia przed awarią. Gdy uszkodzeniu ulegnie główny nośnik przekazywania informacji, alternatywnym rozwiązaniem jest łączność modemowa.

Wirtualne sieci prywatne oferują możliwość zestawienia połączenia z Windows Server 2003 poprzez sieci publiczne, takie jak Internet. Sieć pośrednicząca jest traktowana jako nośnik informacji dla komunikacji z serwerem firmy. Rozwiązania oparte na VPN pozwalają na wymianę danych przy mniejszych kosztach połączenia, ponieważ eliminują konieczność wykorzystania drogich linii modemowych. Ponieważ pakiety danych są przesyłane w sieciach publicznych, istnieje poważne ryzyko podsłuchania komunikacji. W celu ominięcia tego problemu prywatne informacje są zabezpieczane przez silne szyfrowanie. Gdy siecią publiczną jest Internet, pracownicy korzystający z modemów mogą bez problemów łączyć się z serwerem. Jedyne, czego potrzebują, to zestawienie połączenia z lokalnym dostawcą internetowym. Zamiast dzwonić do firmy oddalonej o setki kilometrów, wystarczy zadzwonić pod numer dostępowy i przez Internet dostać się do serwera firmy.

Konfiguracja połączeń zdalnego dostępu wymaga ustawienia parametrów komunikacji na serwerze oraz w systemach operacyjnych klienta. Zestawienie połączenia będzie zakończone sukcesem dopiero po określeniu właściwości urządzeń sieciowych, adresowania IP, uprawnień, uwierzytelnienia oraz profili zdalnego dostępu. Ponieważ liczba możliwych wariantów konfiguracji połączeń jest znaczna, opis usługi Zdalnego dostępu ograniczymy do prezentacji ustawień serwera pracującego z wirtualnymi sieciami prywatnymi. Warto pamiętać, że w takim przypadku co najmniej jeden interfejs sieciowy Windows Server 2003 powinien być podłączony do Internetu i mieć adres IP widoczny z sieci zewnętrznej.

Instalacja serwera zdalnego dostępu

Pierwszą czynnością związaną z instalacją usługi zdalnego dostępu jest dodanie odpowiedniej roli serwera RRAS do Windows Server 2003. Rozpoczynamy od uruchomienia przystawki Zarządzanie tym serwerem. Następnie klikamy odnośnik Dodaj lub usuń rolę. Kreator konfigurowania serwera przeprowadza test parametrów serwera i wyświetla okno z listą dostępnych ról. Po zaznaczeniu opcji Serwer dostępu zdalnego/sieci VPN, naciskamy przycisk Dalej. Program instalatora poinformuje nas o konieczności uruchomienia kolejnego kreatora i po kliknięciu Dalej przejdziemy do Kreatora instalacji serwera routingu i zdalnego dostępu.

Wywołany kreator wyświetla okno powitalne, a następnie listę wariantów konfiguracyjnych usługi RRAS. Przy nadawaniu roli serwera zdalnego dostępu przez wirtualne sieci prywatne, odpowiednimi pozycjami są: Dostęp zdalny (połączenie telefoniczne lub sieć VPN) oraz Dostęp prywatnej sieci wirtualnej (VPN) i translacja adresów sieciowych (NAT). W zależności od potrzeb firmy wybieramy właściwą opcję. Administratorzy, którzy znają interfejs przystawki usługi zdalnego dostępu mogą zaznaczyć pole Konfiguracja niestandardowa. Po wskazaniu konfiguracji niestandardowej wybieramy aktywację jednej z usług komunikacyjnych serwera. Pozostałe okna kreatora są pomijane i właściwości pracy Windows Server 2003 należy przypisać samodzielnie. W naszym przykładzie zaznaczamy Dostęp zdalny (połączenie telefoniczne lub sieć VPN) i klikamy Dalej.

Kolejne okno służy do określania sposobu uzyskiwania dostępu do serwera. Wyświetlone pola wyboru pozwalają na ustawienie przyjmowania połączeń telefonicznych lub VPN. Jeśli klienci będą się łączyć zarówno przez Internet, jak i modemy, umieszczamy znaczniki w obu polach. Po zaznaczeniu opcji Serwer sieci VPN, przechodzimy do okna Połączenie sieci VPN. W tym miejscu wskazujemy, który z interfejsów Windows Server 2003 łączy system z Internetem. Żeby się nie pogubić, warto wcześniej sprawdzić adresy IP kart sieciowych. Innym, lepszym rozwiązaniem jest zmiana nazw interfejsów. Domyślnie każdy z nich ma nadawane mało znaczące nazwy Połączenie lokalne i Połączenie lokalne 2. Kartę wewnętrzną możemy nazwać np. LAN, a zewnętrzną WAN lub INet. Zmianę nazwy wykonujemy w Panelu sterowania w opcji Połączenia sieciowe. Następnie zaznaczamy ikonę reprezentująca interfejs sieciowy i z menu Plik wybieramy Zmień nazwę.

Przy wskazywaniu karty sieciowej w Kreatorze instalacji serwera routingu i dostępu zdalnego, warto zaznaczyć opcję Włącz zabezpieczenia na wybranym interfejsie poprzez ustawienie statycznych filtrów. Pozwala ona na ograniczenie dostępu z Internetu przez automatyczne zdefiniowanie grupy filtrów przekazywania protokołu IP. Jeśli pominiemy zakładanie filtrów przez kreatora, parametry filtrowania mogą zostać ustawione we właściwościach interfejsu zewnętrznego w przystawce Routing i dostęp zdalny. Po naciśnięciu przycisku Dalej, przechodzimy do konfiguracji parametrów adresowania klientów zdalnych. Jeśli na serwerze jest zainstalowana usługa DHCP należy zaznaczyć opcję Automatycznie. W ostatnim oknie kreatora konfigurujemy sposób uwierzytelnienia żądań połączeń. Jeśli w sieci pracuje wiele urządzeń zdalnego dostępu można przesyłać

prośby o uwierzytelnienie do serwera protokołu RADIUS. W małych sieciach, najczęściej uwierzytelnienie pozostawia się w gestii usługi Routing i dostęp zdalny. Po wyświetleniu ekranu podsumowującego wprowadzane parametry kreator jest zamykany.

W celu zakończenia określania parametrów adresowania IP należy dodatkowo skonfigurować Agenta przekazywania serwera DHCP. Agent przekazywania jest wykorzystywany do pobierania adresów z serwera usługi DHCP i przekazywania ich klientom łączącym się przez wirtualne sieci prywatne. Ustawienia związane z Agentem są dostępne w przystawce Routing i dostęp zdalny. Przystawkę uruchamiamy, wchodząc w Start | Programy | Narzędzia administracyjne | Routing i dostęp zdalny. Następnie po kolei rozwijamy foldery: Nazwa_serwera | Routing protokołu IP i Agent przekazywania. Po zaznaczeniu Agenta przekazywania, z menu Akcja wybieramy Właściwości i w polu Adres serwera wpisujemy IP wewnętrznej karty sieciowej.

Konfiguracja zasad zdalnego dostępu

Dostęp zdalny do Windows Server 2003 wymaga odpowiednich uprawnień. Uprawnienia te mogą być konfigurowane na dwa różne sposoby. Pierwszy z nich pozwala na zdalny dostęp tym klientom sieci, którzy mają jawnie wyrażoną zgodę na dostęp. Drugim sposobem jest przeniesienie odpowiedzialności za umożliwienie dostępu do sieci na zasady dostępu zdalnego. Konfigurację jawnej zgody na połączenia przez VPN wykonujemy we właściwościach konta użytkownika w przystawce Użytkownicy i komputery usługi Active Directory. Umieszczona tam karta Telefonowanie jest przeznaczona do konfiguracji środowiska i uprawnień klientów zdalnych. Grupa ustawień Uprawnienie usługi Dostęp zdalny (Telefonowanie lub sieci VPN) jest wykorzystywana do wskazania, czy dany użytkownik może uzyskiwać dostęp, czy jest on zabroniony. Służą do tego opcje Zezwalaj na dostęp i Odmów dostępu. Kontroluj dostęp przez zasady zdalnego dostępu wskazuje, że o dostępie decydują zasady określone w usłudze RRAS. Pozostałe parametry karty zajmują się dodatkowymi ustawieniami środowiska użytkownika. Opcja Weryfikuj identyfikator rozmówcy pozwala na odrzucenie użytkownika, gdy próbuje zadzwonić do serwera z innego niż wprowadzony w polu edycji numer. Grupa ustawień Opcje wywołania zwrotnego jest stosowana wtedy, gdy chcemy by serwer oddzwaniał do telefonującego użytkownika. Koszty połączenia pokrywa wówczas firma. Po zaznaczeniu wybranej opcji serwer oddzwoni pod określony przez użytkownika numer lub pod numer wprowadzony w polu Zawsze używaj wywołania zwrotnego na numer. Ostatnie dwa ustawienia: Przypisz statyczny adres IP i Zastosuj trasy statyczne, służą do określania dodatkowych parametrów adresowania IP. Jeśli chcemy umożliwić dostęp do zasobów firmy większej liczbie użytkowników zdalnych, zalecane jest założenie grupy zabezpieczeń np. VPNUsers i przypisanie jej wszystkich kont mogących łączyć się z sieci zewnętrznej.

Jeśli uprawnienia są określone przez zasady zdalnego dostępu, modyfikujemy je w przystawce Routing i dostęp zdalny. W czasie instalacji usługi RRAS zakładane są dwie zasady domyślne, które zabraniają dostępu do Windows Server 2003. Jeśli chcemy, aby klienci sieci mogli komunikować się z firmą przez wirtualne sieci prywatne, należy zmodyfikować lub zastąpić zasady wymienione w przystawce. Obiekty te odnajdziemy po wejściu do folderu Zasady dostępu zdalnego. W celu szybkiego skonfigurowania usługi RRAS zmienimy ustawienia domyślnej zasady o nazwie Połączenia z serwerem usługi routingu i dostępu zdalnego firmy Microsoft. Po zaznaczeniu obiektu, z menu Akcja wybieramy Właściwości. Następnie usuwamy wpisy w polu Warunki zasady i wprowadzamy własne ustawienia. Po kliknięciu Dodaj, z listy atrybutów wybieramy Windows-Groups. Kliknięcie kolejnego Dodaj, pozwala nam na wskazanie grup, którym chcemy udzielić uprawnień do zdalnego dostępu przez VPN. W następnym oknie wpisujemy nazwę grupy lub wyszukujemy ją za pomocą kombinacji przycisków Zaawansowane | Znajdź teraz. Nie powinniśmy zapomnieć o przestawieniu opcji Odmów uprawnień do dostępu zdalnego na Udziel uprawnień do dostępu zdalnego.

Zaawansowane parametry zasad ustawiamy po wejściu w profil zasad. Po kliknięciu przycisku Edytuj profil możemy zmienić konfigurację uwierzytelnienia, szyfrowania, adresowania IP, nałożyć dodatkowe ograniczenia na połączenia lub zmienić ustawienia łącza wielokrotnego. Jeśli chcemy zwiększyć zabezpieczenia systemu zalecane jest wybranie silnego szyfrowania i uwierzytelnienia na poziomie MS-CHAPv2 lub EAP. Po skonfigurowaniu zasady należy upewnić się, że jest ona umieszczona na pierwszej pozycji listy zasad. Każdy użytkownik należący do grupy wskazanej w obiekcie zasad, np. VPNUsers, będzie mógł bez kłopotu łączyć się z serwerem.

Konfiguracja klienta usługi RRAS

Klienci, którzy chcą komunikować się z serwerem za pomocą połączeń VPN, muszą mieć odpowiednio skonfigurowane komputery. Na stacjach roboczych lub laptopach pracujących pod kontrolą systemu Windows XP, należy wejść do folderu Połączenia sieciowe umieszczonego w Panelu sterowania. Następnie uruchamiamy Kreatora nowego połączenia. W oknie powitalnym kreatora wybieramy Dalej i z listy typów połączeń wskazujemy: Połącz z siecią w miejscu pracy. Po kliknięciu Dalej, zaznaczamy Połączenie wirtualnej sieci prywatnej. W kolejnym oknie definiujemy nazwę połączenia np. IDG, a w wyborze serwera sieci VPN, podajemy adres IP lub nazwę serwera Windows 2003. Jeśli wprowadzimy nazwę hosta, musi być to nazwa FQDN zarejestrowana w serwerach DNS.

Po naciśnięciu Dalej ustalamy, czy konfigurowane połączenie będzie dostępne wyłącznie dla konta przez które zostało utworzone, czy dla wszystkich użytkowników komputera. W oknie finalizującym pracę kreatora, zaznaczamy Dodaj skrót do tego połączenia na pulpicie, a następnie klikamy Zakończ. Po zamknięciu kreatora Windows Server 2003 automatycznie wyświetli okno dialogowe do nawiązania połączenia z serwerem. Dzięki temu będzie można natychmiast sprawdzić, czy konfiguracja klienta była przeprowadzona prawidłowo. Jeśli po wprowadzeniu nazwy konta i hasła zostaniemy poprawnie uwierzytelnieni, należy uznać, że ustawienia są prawidłowe. Zmianę parametrów komunikacji VPN realizujemy przez wywołanie właściwości połączenia.

Pracę z wykorzystaniem wirtualnych sieci prywatnych rozpoczynamy tak, jak przy standardowej sieci lokalnej. W oknie logowania musimy dodatkowo zaznaczyć pole wyboru: Zaloguj używając połączenia telefonicznego. Jeśli pracujemy poza siecią lokalną, ręczne uruchomienie połączenia nie będzie funkcjonować poprawnie i mimo zestawienia połączenia możemy mieć kłopoty z podłączeniem się do udostępnionych zasobów. Warto również pamiętać, że podczas pracy z sieciami wirtualnymi usługi przeglądania komputerów (computer browser) nie funkcjonują tak samo, jak przy połączeniu lokalnym. Bezproblemowe posługiwanie się nazwami, np. \\nazwa_komputera będzie możliwe dopiero po uruchomieniu usługi WINS na serwerze i przekazaniu klientowi dodatkowych parametrów w adresie IP.

Zaawansowane monitorowanie i konfiguracja usługi RRAS

Parametry nadawane przez kreatory Windows Server 2003 określają domyślne ustawienia usługi zdalnego dostępu. Jeśli chcemy ustalić, kto jest aktualnie podłączony, skonfigurować zaawansowane właściwości RRAS lub określić parametry filtrowania IP, musimy skorzystać z przystawki Routing i dostęp zdalny.

Parametry połączenia konfigurujemy we właściwościach serwera RRAS. Po zaznaczeniu ikony reprezentującej serwer, z menu Akcja wybieramy Właściwości. Na kartach Ogólne, Zabezpieczenia, Protokół IP oraz PPP możemy zmienić globalne ustawienia serwera. Parametry urządzeń obsługujących połączenia przychodzące i wychodzące określamy w folderze Porty. Po zaznaczeniu folderu i wybraniu Właściwości system wyświetla listę urządzeń, które mogą być wykorzystane do komunikacji przez VPN. Jeśli w kreatorze konfiguracji usługi dostępu zdalnego wybraliśmy rolę serwera wirtualnych sieci prywatnych, system automatycznie tworzy po 128 portów protokołów PPTP i L2TP.

Zmniejszenie liczby portów wykonujemy przez zaznaczenie jednego z urządzeń, np. Miniport WAN L2TP, i naciśnięcie przycisku Konfiguruj. W oknie konfiguracji urządzenia możemy określić, czy dany port będzie wykorzystywany do połączeń przychodzących, czy przychodzących i wychodzących.

Monitorowanie aktywności łączy jest wykonywane przez folder Klienci dostępu zdalnego. Zaznaczenie folderu spowoduje, że w prawym panelu przystawki zostanie wyświetlona lista aktualnie podłączonych klientów. System prezentuje informacje o nazwie klienta, czasie połączenia oraz liczbie portów zajmowanych przez połączenie. Po kliknięciu prawym przyciskiem identyfikatora użytkownika dostępne są opcje pozwalające na zakończenie połączenia, wysłanie wiadomości do użytkownika oraz wyświetlenie statystycznych informacji o sesji. Dodatkowe dane o wykorzystaniu zdalnego dostępu otrzymamy z dzienników usługi RRAS. System dokumentuje pracę serwera w dziennikach oraz plikach tekstowych. Zakres informacji przenoszonych do Podglądu zdarzeń określamy przez zaznaczenie ikony serwera i wybranie z menu Akcja polecenia Właściwości. Po wyświetleniu nowego okna należy przejść do karty Rejestrowanie i zaznaczyć wymagany zakres monitorowanych zdarzeń. Dzienniki tekstowe zawierają szczegółowe informacje o wykorzystaniu połączeń VPN.

Konfiguracja dzienników jest wykonywana w folderze Rejestrowanie dostępu zdalnego. Domyślnie system nie zbiera danych na temat pracy usługi. Dopiero po wejściu we właściwości obiektu Plik lokalny określamy zakres i format zapisywania danych. Jeśli na serwerze jest zainstalowany silnik bazy danych SQL Server, będziemy mogli dynamicznie przenosić informacje z usługi zdalnego dostępu do zdefiniowanej tabeli serwera. Opisane powyżej zaawansowane parametry konfiguracji serwera RRAS stanowią jedynie wąski fragment ustawień, jakie można przypisać w systemie Windows Server 2003. Szczegółowy opis dodatkowych parametrów zawierają pliki pomocy serwera.

Portal pracy grupowej

Wśród usług oferowanych przez Windows Server 2003 można odnaleźć dodatkowe, bezpłatne rozwiązania zwiększające efektywność pracy firmy. Bardzo ciekawą ofertą jest możliwość pobrania z witryny firmy Microsoft usług wspierających pracę grupową SharePoint. Usługi SharePoint to gotowy szablon portalu intranetowego, który bardzo łatwo można przystosować do bieżących potrzeb firmy.

Zadaniem intranetu jest wyeliminowanie wielu niedogodności standardowych sieci komputerowych. W celu wymiany informacji pracownicy firmy korzystają z niezwiązanych ze sobą programów. Jeśli użytkownik chce wysłać wiadomość pocztową, musi uruchomić klienta poczty. Gdy chce sięgnąć do szablonu pisma firmowego lub współdzielonego arkusza kalkulacyjnego, otwiera i przeszukuje otoczenie sieciowe itd. Umieszczenie wszelkich informacji w centralnym miejscu oraz współdzielenie dokumentów zdecydowanie usprawnia wymianę informacji między klientami sieci lokalnej. Jeśli dodamy do tego możliwość łączenia się z witryną lokalną z Internetu, zalety SharePointa są znaczne.

SharePoint jest zintegrowaną platformą do składowania dokumentów, dostępu do takich informacji, jak kontakty, zadania i kalendarz. Poszczególne działy firmy mogą publikować ankiety związane z oceną produktów lub prowadzić dyskusje na wybrany temat. Kadry, marketing lub zarząd mają możliwość łatwego publikowania ogłoszeń dotyczących ważnych spraw organizacyjnych. Wszyscy użytkownicy sieci otrzymują dostęp do centrum zgłaszania awarii. Instalacja, konfiguracja i zarządzanie portalem nie jest trudne. Administratorzy systemu mają dostęp do kreatorów zmieniających ustawienia, wygląd oraz uprawnienia do witryny.

Instalacja i wstępna konfiguracja portalu SharePoint

Usługi SharePoint nie są dostarczane łącznie z Windows Server 2003. Administratorzy sieci zainteresowani wdrożeniem portalu w swojej firmie, muszą pobrać pakiet instalacyjny usług ze strony firmy Microsoft. Po uruchomieniu przeglądarki, wprowadzamy adres http://www.microsoft.com/downloads i w opcji Search wpisujemy SharePoint Services. W odnalezionych rezultatach odnajdujemy i klikamy odnośnik Windows SharePoint Services. W otworzonym przez przeglądarkę oknie możemy nacisnąć Download i pobrać pakiet instalacyjny. Należy zwrócić uwagę na język pobieranego pakietu. Wśród dostępnych znajduje się również polski. Po wybraniu właściwej wersji klikamy na przycisk Pobierz i spokojnie czekamy na skopiowanie pakietu. Plik instalacyjny usług SharePoint zajmuje niecałe 35 MB.

Kiedy pobieranie zostanie zakończone rozpoczynamy instalację. Uruchamiamy plik stsv2.exe i czekamy na wyświetlenie powitalnego okna kreatora instalacji. Warto pamiętać, że SharePoint jest witryną intranetową i wymaga obecności w systemie internetowych usług informacyjnych (IIS) oraz składnika ASP.NET. Jeśli do momentu instalacji usług SharePoint IIS nie był zainstalowany na serwerze, należy uruchomić przystawkę Zarządzanie tym serwerem i dodać rolę serwera aplikacji. Przy okazji dodawania roli system zapyta nas o dodanie składnika ASP.NET. W pierwszym oknie instalacji należy przeczytać i zaakceptować umowę licencyjną, a następnie wybrać sposób instalowania usług SharePoint. Kreator oferuje dwa typy instalacji. Wersja typowa jest przeznaczona do większości środowisk sieciowych. Po jej zaznaczeniu system zainstaluje witrynę SharePointa i dodatkowo wersję WMSDE programu SQL Serwer 2000. Drugi typ - Farma serwerów, jest przeznaczony do sieci z wieloma serwerami WWW. Po zaznaczeniu instalacji typowej należy kliknąć Dalej oraz Zakończ. Instalator rozpocznie proces kopiowania i konfigurowania witryny programu SharePoint. Otworzenie strony powitalnej oznacza koniec instalacji portalu.

Przed rozpoczęciem pracy z witryną należy przeprowadzić wstępną konfigurację SharePointa. Proces ten powinniśmy rozpocząć od ustawienia parametrów poczty elektronicznej. Dzięki temu przy zakładaniu nowych użytkowników będziemy mogli bez problemu rozsyłać wiadomość o przyznaniu dostępu do SharePointa. Konfigurację ustawień poczty wykonujemy po kliknięciu skrótu Administracja centralna programu SharePoint umieszczonego w Narzędziach administracyjnych. Na stronie Administracja centralna klikamy łącze: Konfiguruj domyślne ustawienia serwera e-mail. Następnie wprowadzamy adres serwera poczty wychodzącej (SMTP), adresy Od i Odpowiedz do oraz określamy używany zestaw znaków. Pola adresów Od oraz Odpowiedz do informują, od kogo jest e-mail oraz do kogo należy wysłać odpowiedź. Dane te są automatycznie wypełniane przy wysyłaniu wiadomości przez serwer do użytkowników witryny.

Po skonfigurowaniu ustawień poczty możemy przejść do dodania użytkowników portalu. Wprowadzanie nowych kont wykonujemy w domyślnej witrynie SharePointa. Do jej otworzenia wystarczy w przeglądarce wprowadzić adres serwera, np. http://w2k3idg. Następnie należy kliknąć odnośnik Ustawienia witryny. Odnajdziemy go bez trudu na górnym pasku strony powitalnej. W nowym oknie klikamy skrót Zarządzaj użytkownikami, a następnie Dodaj użytkowników. Wprowadzenie nowego użytkownika portalu polega na określeniu grupy parametrów podzielonych na oddzielne kroki. Najpierw wpisujemy nazwę konta domenowego zgodnie z notacją nazwa_domeny\nazwa_konta np. idg\jscislawski. Jeśli chcemy dodać wielu użytkowników, możemy wprowadzić wiele nazw kont rozdzielonych średnikami. Następnie określamy uprawnienia użytkownika w witrynie, które są wyznaczane przez przynależność do Grupy lokacji. Konto klienta może należeć do grup typu: Administrator, Projektant sieci Web, Współpracownik oraz Czytelnik. Administrator to grupa przeznaczona do zarządzania wszystkimi funkcjami portalu. Projektant może tworzyć i konfigurować listy lub biblioteki SharePoint. Konto należące do grupy Współpracownik jest uprawnione do dodawana dokumentów i zawartości list. Ostatnia z grup - Czytelnik, pozwala na dostęp do portalu w trybie tylko do odczytu. Po zaznaczeniu wybranej opcji naciskamy przycisk Następny. Lista dostępnych pól obejmuje właściwości adresowania e-

mail oraz nazwy wyświetlane w portalu. Ostatni etap w dodawaniu kont SharePointa pozwala na wysłanie wiadomości pocztowej do nowych użytkowników z informacją o skonfigurowaniu dostępu do portalu.

Kolejnymi czynnościami powinny być działania przystosowujące portal do potrzeb firmy. Przeprowadzamy je za pomocą grupy opcji Dostosowywanie w Ustawieniach witryny. Klikając łącze: Zmień tytuł i nazwę witryny, w szybki sposób możemy przypisać stały identyfikator portalu. Odnośnik Zastosuj motyw w lokacji otworzy stronę umożliwiającą wybór jednego z dwudziestu schematów modyfikujących czcionki i kolory portalu. Rezultat przypisania każdego z motywów można obejrzeć w oknie podglądu. Klikając odnośnik Modyfikuj zawartość witryny, dostosowujemy widok i rozmieszczenie elementów na stronie głównej Intranetu. Prezentacja zaawansowanych możliwości zarządzania i konfiguracji stron intranetowych znacznie wykracza poza zakres artykułu. Czytelny przewodnik administratora SharePointa oraz przykładowe zastosowania można pobrać ze strony firmy Microsoft. Po gruntownym zapoznaniu się z możliwościami programu, administrator jest w stanie przygotować portal na potrzeby najbardziej wymagającej firmy.

Prezentacja możliwości portalu

Zadaniem SharePointa jest ułatwienie współdzielenia informacji wewnątrz firmy. Witryna startowa zawiera odnośniki do takich zasobów portalu jak: Dokumenty, Obrazy, Listy kontaktów i zadań, Dyskusje oraz Zadania. W środkowej części witryny publikowane są informacje o ważnych wydarzeniach i anonsach. Prawa strona umożliwia publikowanie łączy przenoszących użytkowników portalu do innych witryn przedsiębiorstwa lub przydatnych stron internetowych. Zawartość strony głównej może być praktycznie dowolnie rozszerzana. Po kliknięciu łącza Utwórz umieszczonego na górnym pasku skrótów, jesteśmy przenoszeni do strony z listą gotowych do umieszczenia w portalu szablonów. Jednym z ciekawszych przykładów jest lista Problemy. Po dodaniu listy do strony głównej będziemy mogli zgłaszać problemy ze sprzętem lub oprogramowaniem do administratorów sieci. Dodatkowo każda z opublikowanych informacji ma przypisywany priorytet i termin wykonania. Zgłaszając problem wskazujemy, którego z użytkowników prosimy o wsparcie. Wracając do listy Problemy po jakimś czasie, możemy obserwować, bieżący stan usuwania usterki wyrażony w procentach.

W prawym panelu SharePointa znajduje się przykładowy odnośnik Dokumenty współużytkowane. Oferuje dostęp do ogólnodostępnej biblioteki dokumentów firmy. W tym miejscu możemy centralnie składować ważne pliki przeznaczone dla wszystkich pracowników. W zależności od specyfiki firmy będą to np. wzory umów, szablony pism lub arkusze danych. Gdy pojawi się potrzeba podzielenia współdzielonych dokumentów na oddzielne listy, bez przeszkód założymy dodatkowe biblioteki gromadzące oddzielnie projekty, prezentacje i arkusze. Korzystając z witryny SharePoint, pracownicy mogą tworzyć, edytować, kopiować oraz usuwać pliki bezpośrednio ze strony intranetowej. Po wejściu do biblioteki Dokumenty współużytkowane widzimy listę dokumentów oraz pasek narzędzi do zarządzania plikami. W lewym panelu umieszczone są skróty do zmiany widoku lub akcji wykonywanych w bibliotece. Po kliknięciu jednej z ikon możemy utworzyć nowy dokument, przenieść plik lub grupę plików do biblioteki, założyć folder, przefiltrować pliki lub edytować zasoby w arkuszu danych. Warunkiem bezpośredniego tworzenia dokumentów jest obecność właściwej aplikacji pakietu Office na stacji klienta.

Pracownikom działu handlowego lub marketingu przyda się współdzielenie informacji o kontaktach z klientami. Jeśli chcielibyśmy do portalu SharePoint dodać listę kontaktów, należy po raz kolejny skorzystać z odnośnika Utwórz. Na nowej stronie odszukujemy listę Kontakty i klikamy jej ikonę. Następnie wprowadzamy nazwę, opis i zaznaczamy, czy należy dodać listę do paska szybkiego uruchamiania. Po naciśnięciu OK zostaje dodany nowy obiekt. Jeśli chcemy skopiować dane o kontrahentach wprowadzone wcześniej do programu Outlook 2003, klikamy łącze Importuj kontakty. Zaawansowaną konfigurację

ustawień listy wykonujemy przez łącze Ustawienia witryny | Modyfikuj zawartość witryny. Po wybraniu kontaktów możemy określić uprawnienia innych użytkowników lub zmodyfikować liczbę i ustawienia kolumn opisujących klientów.

Podejmowanie ważnych decyzji dotyczących produktów czy projektów firmy może być wspierane przez zbieranie opinii lub uwag pracowników. Aby nie tracić czasu na długotrwałe, spotkania wystarczy sięgnąć do ankiet witryny SharePoint. Definiowanie nowego sondażu jest bardzo proste. Po kliknięciu przycisku Utwórz wyszukujemy i uruchamiamy odnośnik Ankieta. Następnie wprowadzamy nazwę sondażu i konfigurujemy parametry związane z nawigacją oraz opcjami ankiety. Możemy zezwalać użytkownikom na wiele odpowiedzi na to samo pytanie. Po kliknięciu przycisku Następny, wpisujemy treść oraz wybieramy typ pytania. Do wyboru mamy np. pojedynczy wiersz tekstu, liczbę, TAK/NIE czy listę opcji. Dalsze ustawienia zależą od wybranego typu. Jeśli zaznaczyliśmy opcję: Wybór (menu, z którego można wybrać), wpisujemy poszczególne punkty odpowiedzi, określamy typ przycisków, wartość domyślną itp. Gdy ankieta ma zawierać wiele pytań, klikamy przycisk Następne pytanie. Po dodaniu wszystkich pytań naciskamy Zakończ. Utworzone sondaże są umieszczane na pasku szybkiego uruchamiania. Po kliknięciu nazwy ankiety, użytkownicy są przenoszeni do okna, w którym mogą udzielić odpowiedzi na pytania lub sprawdzić wyniki głosowania. Kliknięcie łącza Odpowiedz na tę ankietę rozpoczyna pracę z sondażem.

Aktualizacje, aktualizacje, aktualizacje....

Blaster i Sasser to słowa, które wywołały znaczny popłoch wśród administratorów sieci na całym świecie. Niedawne nasilenie ataków wirusów na systemy operacyjne firmy Microsoft wymusza nieustanne dbanie o właściwe zabezpieczanie serwerów i stacji roboczych. Jeśli łata zostanie zainstalowana szybko, ryzyko zainfekowania sieci jest radykalnie zminimalizowane. Windows Server 2003 oferuje grupę usług pozwalającą na szybkie i proste aktualizowanie systemu. Administrator może wybrać, ten sposób wgrywania łatek, który będzie dla niego najbardziej odpowiedni.

Pierwszym ze składników systemu umożliwiającym łatwe uaktualnienie serwera jest witryna Windows Update. Odnośnik przenoszący nas do strony zarządzającej poprawkami jest umieszczony bezpośrednio w menu Start. Po naciśnięciu Start i kliknięciu łącza Windows Update, możemy sprawdzić czy Windows nie wymaga uaktualnienia. Przy pierwszym połączeniu z witryną należy zainstalować komponent Windows Update, dzięki któremu będzie można ustalić, jakie poprawki są już zainstalowane na serwerze, a jakie należy doinstalować. Po wyświetleniu okna powitalnego, za pomocą przycisku Skanuj w poszukiwaniu aktualizacji, uruchamiamy program sprawdzający bieżący stan systemu. Gdy skaner odnajdzie nowe poprawki, zostanie wyświetlona lista z proponowanymi aktualizacjami. Jeśli z opisu łaty wynika, że jej obecność nie jest konieczna, za pomocą przycisku Usuń możemy pominąć instalację. Kliknięcie przycisku Zainstaluj teraz, rozpoczyna proces pobierania i implementacji poprawek. Po instalacji łatek regułą jest ponowne uruchomienie komputera. Zaletą korzystania z Windows Update jest możliwość prostego przeglądania zawartości nowych uaktualnień oraz wybierania do instalacji tylko tych, które są naprawdę niezbędne. Do największych wad należy zaliczyć to, że administrator musi pamiętać o cyklicznym odwiedzaniu portalu, aby sprawdzić, czy nie pojawiła się jakaś nowość. Jeśli przegapimy instalację aktualizacji, skutki mogą być opłakane.

Kolejnym komponentem, który pozwala na szybkie importowanie i wdrażanie łatek jest usługa Aktualizacja automatyczna. Dzięki niej Windows Server 2003 będzie na bieżąco pobierał i instalował najnowsze uaktualnienia. Dostęp do konfiguracji usługi uzyskujemy po wejściu we właściwości ikony System umieszczonej w Panelu sterowania. Aby Windows Server 2003 automatycznie łączył się z Internetem i pobierał aktualizacje, należy zaznaczyć pole: Aktualizuj mój komputer. Jeżeli to ustawienie zostanie włączone, oprogramowanie witryny Windows Update... itd. W grupie Ustawienia możemy określić

dodatkowe parametry wgrywania łatek. Najbardziej asekuracyjną opcją jest Powiadom mnie przed pobraniem aktualizacji i powiadom ponownie przed zainstalowaniem ich na komputerze. Zaznaczenie tego pola powoduje, że administrator sieci musi wskazać aktualizacje do pobrania oraz zaakceptować ich instalację. Informacje o dostępności nowych łatek są wyświetlane w obszarze powiadomień systemu Windows. Jest to pole na pasku zadań, umieszczone przy zegarze, w lewym dolnym rogu ekranu. Parametr Pobierz aktualizacje automatycznie i powiadom mnie, kiedy będą gotowe do zainstalowania, zmienia nieco zachowanie systemu. Eliminowane jest powiadomienie o dostępności nowych aktualizacji. Administrator serwera musi jednak zaakceptować każdą łatę zanim zostanie zainstalowana. Ostatnia opcja Pobierz aktualizacje automatycznie i zainstaluj je zgodnie z ustalonym harmonogramem, daje możliwość określenia, kiedy mają być instalowane uaktualnienia do systemu. Jeśli zaznaczymy ten parametr, aktualizacje są pobierane automatycznie, ale instalacja czeka do wskazanej godziny. Komunikat o pobraniu łatek pojawia się w obszarze powiadomień. Jeśli nie wskażemy, które z aktualizacji chcemy zainstalować, o wyznaczonej porze zostaną zainstalowane wszystkie dostępne łaty. Korzystając z aktualizacji automatycznych, nie musimy pamiętać o systematycznym wchodzeniu na witrynę Windows Update. System wykona te operacje za nas. Ważne jest jednak, aby nie instalować całkowicie zbędnych i obciążających system dodatków. Zanim zaznaczymy komponent do zainstalowania należy dokładnie zapoznać się z zawartością opisu łaty.

Miły SUS

Przy niewielkiej ilości komputerów, czynności związane z zarządzaniem poprawkami nie są uciążliwe. Jeśli jednak stacji jest kilkadziesiąt lub kilkaset, pojawia się potrzeba implementacji innych rozwiązań. Dla administratorów opiekujących się sieciami firm średniej wielkości, Microsoft oferuje usługę zajmująca się automatycznym instalowaniem aktualizacji na stacjach roboczych klientów. Usługą tą jest Software Update Services. Konfiguracja SUS wymaga więcej pracy, ale w zamian za to sieć jest aktualizowana w sposób bardziej wydajny i elastyczny. Omawiane wcześniej wykorzystanie witryny Windows Update oraz aktualizacje automatyczne charakteryzują się pewną niedogodnością. Wszyscy klienci sieci muszą mieć dostęp do Internetu. Dodatkowo, każda z łatek jest pobierana wielokrotnie. Jeśli w firmie pracuje 200 stacji, pojedynczy komputer na własny rachunek, ściąga te same pliki aktualizacyjne. Gdy wydajność łącza zewnętrznego nie jest zbyt wysoka, może mieć to istotne znaczenie. Wskazane problemy można łatwo ominąć przez zastosowanie SUS. Działanie usługi uaktualniania oprogramowania polega na automatycznym pobieraniu przez wskazany serwer wszystkich łatek, a następnie na udostępnieniu ich stacjom sieciowym. Łączność z Internetem musi mieć jedynie serwer z zainstalowaną usługą SUS. Klienci sieci nie łączą się z komputerami zewnętrznymi, lecz z serwerem zlokalizowanym w sieci lokalnej.

Aby skorzystać z usługi Software Update Services musimy mieć komputer z systemem Windows Server 2003 lub Windows 2000 Server z SP 2 oraz odpowiednią ilością pamięci i miejsca na dysku. Konfiguracja sprzętowa jest ściśle związana z liczbą obsługiwanych klientów i ich wersją językową. Jeśli w sieci znajdują się systemy pracujące wyłącznie z polskimi systemami operacyjnymi, nie musimy pobierać i przechowywać uaktualnień związanych np. z chińskim Windows XP. Oprócz odpowiedniej mocy procesora, pamięci i zasobów dyskowych, serwer SUS wymaga partycji NTFS, obecności Internetowych Usług Informacyjnych (IIS) w wersji, co najmniej 5.0 oraz minimum Internet Explorer 6.0. Zanim przejdziemy do opisu instalacji SUS, musimy pobrać odpowiednie oprogramowanie z witryny Microsoftu. Po wpisaniu w przeglądarce adresu http://www.microsoft.com/downloads , w wyszukiwarce oprogramowania wpisujemy SUS i klikamy OK. Wybieramy Software Update Services 1.0 with Service Pack 1. W oknie opisującym pakiet klikamy Download i wskazujemy, gdzie należy zapisać pobierane oprogramowanie. Usługa aktualizacji oprogramowania jest dostępna bez ponoszenia dodatkowych opłat.

Instalacja usługi jest bardzo prosta. Ponieważ Internetowe Usługi Informacyjne nie są domyślnie zainstalowane w Windows Server 2003, pracę należy rozpocząć od dodania serwera IIS. W tym celu otwieramy umieszczoną w Narzędziach administracyjnych, przystawkę Zarządzanie tym serwerem. Następnie klikamy przycisk Dodaj lub usuń rolę. Po przejściu do okna Role serwera, wskazujemy Serwer aplikacji (IIS, ASP.NET) i klikamy Dalej. Okno Opcje serwera aplikacji pozwala na wybór dodatkowych narzędzi IIS, takich jak Rozszerzenia serwera FrontPage oraz ASP.NET. Nie są one potrzebne do instalacji usługi SUS. Po dwukrotnym kliknięciu: Dalej, kreator prosi o umieszczenie płyty instalacyjnej Windows Server 2003 w napędzie CD i po skopiowaniu potrzebnych plików kończy pracę. Jeśli Internetowe Usługi Informacyjne są obecne na serwerze, możemy przejść do instalacji usługi SUS. Rozpoczynamy ją od dwukrotnego kliknięcia pobranego z Internetu pakietu SUS10SP1.exe. W czasie instalacji oprogramowania określamy podstawowe parametry usługi. Należą do nich takie opcje jak: katalog składowania uaktualnień, wersje językowe pobieranych aktualizacji oraz ustawienia związane z akceptowaniem nowych poprawek. W pierwszym oknie kreatora instalacji naciskamy przycisk Next, po czym czytamy i akceptujemy licencję użytkownika końcowego. Następnie wybieramy sposób instalacji. Co prawda program instalujący pozwala na wskazanie opcji Typical, ale ponieważ dodajemy oprogramowanie do serwera, ustawienia domyślne mogą nam nie odpowiadać. Po kliknięciu przycisku Custom wskazujemy folder, w którym będą przechowane poprawki. Domyślnie instalator proponuje partycja_startowa/SUS, np. C:/SUS. Usługi uaktualnienia oprogramowania można skonfigurować tak, by aktualizacje nie były składowane lokalnie. Za zarządzanie uaktualnieniami w dalszym ciągu będzie odpowiedzialny serwer SUS, lecz zamiast pobierać łaty z komputera z Windows Server 2003, klienci sieci będą odsyłani do serwerów internetowych. Rozwiązanie to oszczędza lokalną przestrzeń dyskową, ale zwiększa obciążenie łącza. W kolejnym oknie instalacji oprogramowania wskazujemy wersje językowe poprawek obsługiwanych przez SUS.

W celu ograniczenia miejsca zajmowanego przez poprawki, zalecane jest wskazanie wyłącznie potrzebnych języków. W tym celu umieszczamy wskaźnik w polu Specific Languages i klikamy Choose Languages. Po wyświetleniu okna z obsługiwanymi przez SUS wersjami językowymi, zaznaczamy Polish oraz, jeśli jest to konieczne English. W ostatnim oknie konfiguracyjnym instalatora, należy wskazać sposób zarządzania instalacją poprawek. Aktualizacja systemów sieciowych powinna być przeprowadzana uważnie. Zanim nowa łatka zostanie przekazana klientom, należy sprawdzić, czy jej instalacja nie wpłynie negatywnie na działanie komputerów lub lokalnego oprogramowania użytkowników. Okno konfiguracyjne instalatora SUS pozwala na określenie automatycznego lub ręcznego akceptowania nowych wersji zaakceptowanych uprzednio poprawek. Jest to bardzo wygodne, ale warto pamiętać, że nie zawsze wygodniejsze rozwiązania są bezpieczne. Na zakończenie instalacji system wyświetla okna informujące o adresach witryny do pobierania uaktualnień oraz zarządzania serwerem i kończy pracę.

Po zainstalowaniu pakietu należy skonfigurować parametry pobierania i instalowania poprawek. Zarządzanie usługą SUS jest przeprowadzanie przez przeglądarkę internetową. Po uruchomieniu Internet Explorera na stacji roboczej, wprowadzamy adres http://nazwa_serwera_lokalnego_SUS/SUSAdmin. Konfiguracja usługi SUS może zostać przeprowadzona także bezpośrednio po zakończeniu instalacji, ponieważ automatycznie uruchamiana jest witryna administracyjna. Wszelkie czynności administracyjne wykonujemy klikając jeden z odnośników umieszczonych w lewym panelu witryny. Jeśli przy określaniu ustawień uaktualniania oprogramowania, została wybrana opcja lokalnego przechowywania łatek, Windows Server 2003 czeka dużo pracy. System musi podłączyć się do witryny firmy Microsoft, zawierającej wszystkie uaktualnienia i skopiować je do folderu macierzystego. Pobieranie rozpoczynamy od kliknięcia łącza Synchronize server lewego panelu, a następnie Synchronize now. Ponieważ ilość pobieranych plików jest znaczna, operacje kopiowania możemy odłożyć na czas mniejszego obciążenia łącza.

W tym celu, zamiast Synchronize now, klikamy Synchonization Schedule i określamy dzień oraz godzinę rozpoczęcia synchronizacji. W oknie harmonogramu należy ustawić również odpowiednią liczbę ponowień pobierania na wypadek utraty połączenia. Jeśli zaznaczyliśmy wyłącznie polskie wersje pakietów uaktualnień system pobiera znacznie ponad 600 MB danych. Jeśli z sukcesem uda się skopiować dane z Internetu, możemy przejść do procedury akceptowania aktualizacji. Dopiero po uzyskaniu zezwolenia na instalację, łaty będą mogły dotrzeć do stacji roboczych klientów sieci. Początkowa akceptacja poprawek jest nieco męcząca. Miłym ułatwieniem jest możliwość posortowania pobranych uaktualnień według statusu, daty, tytułu i platformy. Każdą wybraną do instalacji poprawkę należy po prostu zaznaczyć. Zatwierdzanie aktualizacji przeprowadzamy po kliknięciu łącza Approve Update. Na zakończenie konfiguracji serwera warto pamiętać, że modyfikacja ustawień usługi SUS jest wykonywana po kliknięciu odnośnika Set options. Zmiana parametrów usługi będzie przydatna np. przy dodatkowym pobieraniu pakietów aktualizacyjnych do innych wersji językowych.

Jeśli SUS jest instalowany w komputerze z uruchomioną witryną SharePoint, domyślna strona zarządzania usługami uaktualnienia oprogramowania jest zablokowana. W celu odblokowania witryny należy wykonać następujące czynności. Korzystając ze skrótu w Narzędziach administracyjnych, otwieramy witrynę zarządzania portalem SharePoint. Następnie po kolei klikamy odnośniki Konfiguruj ustawienia serwera wirtualnego | Domyślna witryna sieci Web | Definiuj zarządzane ścieżki. W polu Dodaj nową ścieżkę wprowadzamy ciąg znaków SUSAdmin i zaznaczamy opcję Wykluczona ścieżka. Po kliknięciu OK, powtarzamy czynność, tym razem wykluczając ścieżki autoupdate i dictionaries. Po wykonaniu tych czynności witryna http://nazwa_serwera/SUSAdmin powinna zostać uruchomiona bez żadnych problemów.

Konfiguracja klientów usługi SUS

Przygotowanie serwera usług aktualizacji systemów nie jest ostatnim etapem konfiguracji SUS. Uaktualnianie oprogramowania będzie funkcjonowało poprawnie dopiero po skonfigurowaniu stacji roboczych. W tym celu najłatwiej skorzystać z usług oferowanych przez zasady grupy. Praca z zasadami grupy została opisana w oddzielnym artykule, dlatego też obecnie zajmiemy się wyłącznie sposobami skonfigurowania zasad do współpracy z usługami uaktualniania oprogramowania. Jeśli uaktualnienia mają trafiać na wszystkie komputery klientów domeny, najlepiej będzie skorzystać z zasady Default Domain Policy. Żeby się do niej dostać, należy otworzyć przystawkę do zarządzania zasadami, czyli Edytor Obiektów Zasad Grupy. W zależności od konfiguracji serwera, dostęp do edytora uzyskamy przez konsolę Group Policy Management Console lub przystawkę Użytkownicy i komputery usługi Active Directory. Dla GPMC będzie to ścieżka Start | Programy | Narzędzia administracyjne | Group Policy Management. W uruchomionej przystawce rozwijamy foldery Forest | Domains | Nazwa_domeny i zaznaczamy zasadę Default Domain Policy. Następnie z menu Akcja wybieramy Edit. Gdy nie mamy zainstalowanej konsoli, po kolei uruchamiamy Start | Programy | Narzędzia administracyjne | Użytkownicy i komputery usługi Active Directory. Następnie zaznaczamy ikonę reprezentującą domenę i z menu Akcja wybieramy Właściwości. Po przejściu do karty Zasady grupy, naciskamy przycisk Edytuj.

Niezależnie od wykorzystywanej przystawki, w edytorze zasad po kolei rozwijamy ustawienia Konfiguracja komputera | Szablony administracyjne | Składniki systemu Windows | Windows Update. W folderze związanym z uaktualnieniami oprogramowania dostępne są cztery ustawienia: Konfigurowanie aktualizacji automatycznych, Określ lokalizację intranetową usługi aktualizującej firmy Microsoft, Zaplanuj ponownie zaplanowane instalacje aktualizacji automatycznych oraz Bez automatycznego uruchamiania ponownego dla zaplanowanych instalacji aktualizacji automatycznych. Wymienione ustawienia należy kolejno zmodyfikować na potrzeby usługi SUS. Parametry Konfigurowania aktualizacji automatycznych zawierają opcje dotyczące planowania i

harmonogramu pobierania aktualizacji. Nie różnią się one niczym od opisywanych wcześniej elementów karty Aktualizacje automatyczne ikony System w Panelu Sterowania. Ta część usługi SUS, która jest uruchamiana po stronie klienta, funkcjonuje właśnie w oparciu o Aktualizacje automatyczne. Główną różnicą w konfiguracji jest to, że stacja robocza nie łączy się z serwerem wewnętrznym, a z serwerem intranetowym. Adres serwera lokalnego jest wprowadzany w drugim ustawieniu foldera Windows Update. Po umieszczeniu znacznika przy opcji włączone, do pól edycji wpisujemy nazwę DNS lub adres IP komputera z Windows Server 2003. Ustawienia związane z ponownym planowaniem instalacji oraz wyłączające automatyczne uruchamianie są bardzo przydatne. Pierwsze z nich pozwala na ponawianie instalacji poprawek, jeśli aktualizacja zgodna z harmonogramem nie doszła do skutku. Wydarzenia takie mają miejsce jeśli np. komputer klienta był wyłączony.

Niektóre z uaktualnień wymagają restartu systemu. Jeśli system operacyjny klienta automatycznie zainstaluje taką poprawkę, może dojść do niespodziewanego restartu Windows. Włączenie ostatniej opcji foldera Windows Update, pozwala na wyeliminowanie tego problemu. Po ustawieniu wszystkich ustawień na włączone, zamknięcie edytora zasad grupy kończy proces konfiguracji. Przy następnym restarcie na komputery klientów zostaną przekazane właściwe parametry.

Awaria serwera może się przytrafić każdemu. Dobry administrator powinien wiedzieć, co robić w przypadku problemów. Jeśli zostaliśmy całkowicie zaskoczeni, a o sporządzaniu kopii zapasowych czytaliśmy tylko w mądrych podręcznikach, mamy poważny kłopot. Nie wszystko jednak jest stracone. Gdy mamy odrobinę szczęścia, możemy spróbować zmusić Windows Server 2003 do ponownego, poprawnego działania.

Pierwsze kilka godzin pracy po mile spędzonym weekendzie może się okazać "czarnym poniedziałkiem". Jeżeli po uruchomieniu serwera, zamiast okna z prośbą o naciśnięcie klawiszy [Ctrl Alt Delete], system wyświetli koszmarny błękitny ekran, nasz organizm na 90 procent przejdzie w stan przedzawałowy. Żeby do tego nie dopuścić, warto poznać kilka funkcji zabezpieczających Windows Server 2003 przed awarią lub przywracających system do życia po jej wystąpieniu.

Źródła awarii systemu

Rozważając przyczyny awarii systemów operacyjnych, możemy wskazać dwa główne źródła problemów: sprzęt oraz "czynnik ludzki". Wyczucie momentu wystąpienia awarii sprzętowej jest bardzo trudne. Czasami komputer przekazuje pewne sygnały w postaci np. błędów zapisu na dysku, ale najczęściej sprzęt psuje się nagle. Są sposoby minimalizowania lub zapobiegania skutkom awarii. Wersja Standard, Enterprise oraz Datacenter systemu Windows Server 2003 obsługuje łączenie serwerów w klastry. Niestety, są to drogie rozwiązania, przeznaczone do firm, w których nieprzerwany dostęp do zasobów jest wyjątkowo ważny. Wiele sprzedawanych serwerów umożliwia wymianę dysków "na gorąco", zawiera sprzętowe macierze dysków oraz nadmiarowe zasilacze awaryjne. Małe firmy, dla których koszty mają fundamentalne znaczenie, mogą skorzystać z oferowanego przez Windows Server 2003 programowego zabezpieczenia

przed awarią dysków. Funkcja ta nie uchroni systemu przed skutkami usterek płyty głównej czy zasilacza, ale zadba o bezpieczeństwo danych.

Wadliwe działanie poszczególnych komponentów systemu może powodować utratę stabilności Windows. Jeśli uszkodzone są pamięć lub twardy dysk, liczba zawieszeń systemu oraz błękitnych ekranów znacznie wzrasta. Gdy obserwujemy nasilenie błędów, powinniśmy skorzystać z dowolnego programu testującego sprzęt. Najczęściej oprogramowanie diagnostyczne jest oferowane przez producenta danego komponentu, choć nie brakuje specjalistycznych aplikacji testujących kompleksowo cały serwer. Serwery podłączone na stałe do Internetu są narażone na inny rodzaj niebezpieczeństw. Głównym problemem administratora jest właściwe zabezpieczenie systemu przed atakami z zewnątrz. Jeśli atak będzie skuteczny i komputer przestanie poprawnie funkcjonować, należy zastosować takie rozwiązania, które skrócą lub zminimalizują skutki przestoju pracy serwera.

Czynnikiem, którego znaczenia nie można bagatelizować, są błędy ludzkie. Pracownicy serwisów dystrybutorów oraz sklepów komputerowych przekonali się o tym niejednokrotnie. Zdarzenia te dotyczą zwłaszcza domowych użytkowników pecetów, choć występują również przy systemach serwerowych. Dlatego warto się zabezpieczyć przed skutkami nieuwagi lub lekkomyślności - najlepiej zapoznać się z usługami zawartymi w Windows Server 2003, które pozwalają w krótkim czasie przywrócić poprawne funkcjonowanie systemu.

Poznanie przyczyny problemu

Jeśli Windows Server 2003 z uporem maniaka zamiast okna powitalnego wyświetla tzw. blue screen, awaria staje się faktem. Skuteczność kontrataku ze strony administratora jest uzależniona od właściwego rozpoznania przeciwnika. Gdy w serwerze zepsuje się pamięć, wówczas nawet dziesięć kopii zapasowych będzie mało przydatne. W innym przypadku problemy związane ze środowiskiem startowym zawsze wymagają natychmiastowego wezwania serwisu lub naprawy komputera. Zanim zastosujemy właściwą strategię przywracania systemu, musimy ustalić, co jest przyczyną kłopotów.

W poprawnym zdiagnozowaniu serwera pomoże treść wyświetlanych przez system komunikatów, zawartość wpisów w dziennikach Aplikacje oraz System, a także wiedza o ostatnio wykonanych operacjach. Bardzo często zainstalowanie niewłaściwych sterowników lub zmiana parametrów urządzeń powodują problemy podczas restartu serwera. Jeśli ostatnie działania administratora w pewien sposób przyczyniły się do powstania awarii, należy się zastanowić, jak przywrócić poprzednie ustawienia lub wyłączyć urządzenie sprawiające kłopot. Chcąc sprawdzić, czy konfiguracja sprzętu jest poprawna, wystarczy wejść we właściwości ikony System, a następnie przejść do karty Sprzęt i kliknąć przycisk Menedżer urządzeń. Jeśli przy ikonach reprezentujących komponenty komputera zobaczymy wykrzyknik, należy sprawdzić poprawność funkcjonowania urządzenia lub zainstalować właściwy sterownik. Do diagnostyki systemu można zastosować narzędzie Informacje o systemie. Uruchamia się je, wpisując bezpośrednio w wierszu poleceń MSInfo32 albo standardowo pokonując ścieżkę: Start | Wszystkie programy | Akcesoria | Narzędzia systemowe | Informacja o systemie. Po rozwinięciu opcji Składniki odnajdziemy pozycję Urządzenia powodujące problemy. Jeśli w serwerze są wadliwie działające komponenty, zostanie wyświetlona ich lista.

Powyższe metody sprawdzenia poprawności działania systemu są całkowicie nieskuteczne, jeśli Windows nie daje się uruchomić. Wtedy należy skorzystać z trybu awaryjnego. Pewne informacje o przyczynach awarii zawiera komunikat wyświetlany w wypadku błędu krytycznego (blue screeen). Dane przekazywane przez błąd zatrzymania są bardzo skromne. Otrzymujemy numer oraz parametry błędu i jeśli to możliwe, dane o sterowniku, będącym prawdopodobną przyczyną problemu. Po zanotowaniu numeru błędu najlepszym rozwiązaniem jest próba odnalezienia na stronie internetowej

Microsoftu informacji dotyczącej danego problemu. Innym bardzo dobrym źródłem wiedzy są grupy dyskusyjne.

Kopia zapasowa

Systemy, których działanie jest niezmiernie ważne dla firmy, należy zabezpieczać, często wykonując kopie zapasowe. To jedna z najczęściej stosowanych i najbardziej pewnych metod ochrony danych. Kopie należy wykonywać regularnie, zgodnie z wybraną strategią archiwizacji. Bardzo ważne jest sprawdzenie możliwości skutecznego odtworzenia danych. Jeśli nie przetestujemy przywracania systemu, może się okazać, że archiwizacja była pozorna, bo i tak nie można odzyskać wszystkich niezbędnych danych.

Wykonując kopię zapasową danych, administrator musi zarchiwizować dwa typy informacji. Dla pracowników firmy najważniejsze są ich zasoby. Jeśli przypadkowo zostaną usunięte ważne dokumenty lub arkusze, trzeba szybko przywrócić pliki z kopii zapasowej. Niestety, nawet najbardziej dokładna archiwizacja danych użytkowników nie pomoże odtworzyć konfiguracji Windows Server 2003. Aby odzyskać ustawienia kont, parametry usług sieciowych albo Zasad grupy, należy skopiować ustawienia systemu operacyjnego. Dane te można zarchiwizować za jednym zamachem, wykonując kopię Stanu systemu. Stan systemu to grupa plików potrzebna do odtworzenia Windows Server 2003. W przypadku kontrolera domeny zaliczamy do nich takie informacje konfiguracyjne, jak Rejestr, bazę danych COM+, bazę Active Directory, folder SysVol, pliki systemu operacyjnego oraz pliki rozruchowe. Jeśli na serwerze dodatkowo zainstalowane są Internetowe usługi informacyjne oraz Usługi certyfikatów, w skład stanu systemu wchodzi również kopia bazy danych certyfikatów oraz metabazy aplikacji IIS.

Archiwizacja stanu systemu jest prostą operacją. Po uruchomieniu w trybie kreatora narzędzia Kopia zapasowa zaznaczamy Wykonaj kopię zapasową plików i ustawień | Dalej | Pozwól mi wybrać, co ma zawierać kopia zapasowa. W oknie Elementy do zapisania w kopii zapasowej rozwijamy folder Mój komputer i zaznaczamy obiekt System State. Po naciśnięciu Dalej określamy lokalizację i nazwę kopii. Ponieważ archiwizacja stanu systemu powinna być wykonywana systematycznie, w ostatnim oknie należy kliknąć przycisk Zaawansowane. Umożliwi to określenie harmonogramu sporządzania kopii. Jeśli nie posługujemy się kreatorem, sporządzenie archiwizacji jest jeszcze prostsze. Po uruchomieniu narzędzia Kopia zapasowa przechodzimy do karty o tej samej nazwie i zaznaczamy obiekt System State w folderze Mój komputer. Warto pamiętać, że wykonanie kopii zapasowej stanu systemu to automatyczny backup rejestru do folderu katalog_systemu\repair. Będzie on potrzebny podczas próby naprawy systemu. Jeśli chcemy odtworzyć dane o systemie na komputerze z zainstalowaną usługą Active Directory, należy uruchomić Windows w Trybie odzyskiwania usług katalogowych.

Automatyczne odzyskiwanie systemu

Użytkownicy Windows XP mogą być nieco rozczarowani uszczupleniem Windows Server 2003 o jedną z ważniejszych usług odzyskiwania systemu. Pracując z serwerem, nie można korzystać z Punktów odzyskiwania. Administratorowi pozostaje tylko użycie Automatycznego odzyskiwania systemu. ASR jest funkcją wspierającą przywracanie Windows Server 2003 po awarii. Jeśli system operacyjny będzie poważnie uszkodzony i próba odtworzenia Windows przez Ostatnią znaną dobrą konfigurację lub tryby awaryjne zakończy się niepowodzeniem, może być konieczna reinstalacja systemu. Operacja ta jest czasochłonna. Trzeba od nowa zainstalować Windows, potem urządzenia i dopiero wtedy odtworzyć dane z kopii zapasowej stanu systemu. Znacznym uproszczeniem przywracania jest skorzystanie z danych skopiowanych przez ASR. Do odtworzenia Windows będziemy potrzebowali jednej dyskietki, kopii danych sporządzonych przez kreatora Automatycznego odzyskiwania systemu oraz płyty instalacyjnej Windows Server 2003.

Kopię danych niezbędnych do automatycznego odzyskiwania systemu wykonujemy narzędziem Kopia zapasowa. W celu sporządzenia archiwizacji klikamy Start | Wszystkie programy | Akcesoria | Narzędzia systemowe | Kopia zapasowa. Jeśli po włączeniu narzędzia zostanie uruchomiony Kreator kopii zapasowych, w poszczególnych oknach zaznaczamy: Wykonaj kopię zapasową plików i ustawień | Dalej | Wszystkie informacje na tym komputerze | Dalej. W oknie Typ kopii wskazujemy lokalizację i nazwę archiwum, a następnie klikamy Zakończ. Po wykonaniu kopii zapasowej system poprosi o umieszczenie w stacji czystej dyskietki, na której zostaną zapisane dane o odtwarzanym systemie. Jeśli do sporządzania archiwizacji nie wykorzystujemy trybu kreatora, na karcie Zapraszamy klikamy przycisk Kreator automatycznego odzyskiwania systemu lub to samo polecenie wybieramy z menu Narzędzia. Zapisane na dyskietce informacje są ściśle związane z wykonaną kopią zapasową. Do każdej archiwizacji ASR należy przygotować inną dyskietkę.

Odtworzenie Windows Server 2003 z wykorzystaniem Automatycznego odzyskiwania systemu rozpoczynamy od uruchomienia serwera z płyty instalacyjnej. Po wyświetleniu komunikatu dotyczącego dodatkowych sterowników na dolnym pasku ekranu możemy zaobserwować kolejny komunikat: "Naciśnij klawisz F2, aby uruchomić automatyczne odzyskiwanie systemu (ASR)". Po naciśnięciu przycisku należy umieścić dyskietkę w napędzie i system rozpocznie odtwarzanie. W pierwszej fazie zakładana jest od początku partycja systemowa. Dalsze operacje przywracania systemu przypominają proces instalacji. Sprawdzany jest dysk, instalator kopiuje pliki z płyty i wykonuje restart. Po ponownym uruchomieniu Windows, rozpoznaniu sprzętu i wskazaniu źródła archiwum ASR rozpoczyna się odtwarzanie systemu operacyjnego z kopii zapasowej. Dane źródłowe odzyskiwania zajmują ponad 1 GB. Najlepiej przechowywać je na zapasowym dysku podłączonym do serwera w czasie przywracania albo na płycie DVD. Kolejny restart kończy odzyskiwanie systemu Windows.

Naprawa instalacji systemu

Jeśli awaria Windows Server 2003 przydarzy się administratorowi, który zapomniał wykonać jakąkolwiek kopię zapasową, możemy spróbować przywrócić system, naprawiając instalację. Operacja ta jest bardzo prosta, ale może się nie powieść.

Rozpoczynamy od uruchomienia systemu z płyty instalacyjnej. Cierpliwie czekamy na pojawienie się ekranu z prośbą o wskazanie dalszego przebiegu instalacji. Następnie naciskamy klawisz [Enter] i akceptujemy warunki licencji. Nie należy wybierać klawisza [R], który umożliwia naprawę systemu za pomocą Konsoli odzyskiwania. Ta metoda zostanie opisana w dalszej części artykułu. Przed rozpoczęciem reinstalacji Windows instalator podejmuje próbę odszukania i naprawienia znajdujących się na dysku systemów. Jeśli chcemy naprawić uszkodzoną instalację, klawisz [R] naciskamy dopiero w kolejnym oknie, które zawiera listę zainstalowanych systemów operacyjnych. Gdy instalator nie wykryje systemu, naprawa instalacji jest niemożliwa.

Dalszy przebieg przywracania systemu przypomina instalację Windows. Kopiowane są pliki systemowe, a po restarcie gromadzone są informacje o konfiguracji. Musimy także ponownie wprowadzić numer klucza Windows. Jeśli wszystko pójdzie dobrze, system jest naprawiony.

Programowy RAID

Regularne wykonywanie kopii zapasowych pozwala na skuteczną ochronę plików na wypadek awarii sprzętowej. Archiwizacja danych nie jest jedynym sposobem na unikanie poważnych problemów. Niewielkie firmy, instalujące Windows Server 2003 na niedrogich serwerach, mogą zastosować programowy RAID, oferowany przez system operacyjny. Stosując jeden z wariantów nadmiarowego zapisywania danych, możemy ochronić zasoby

gromadzone na dysku serwera. Windows Server 2003 pozwala na skonfigurowanie dwóch rodzajów odporności na uszkodzenia: woluminy dublowane oraz woluminy RAID 5.

Woluminy dublowane to inne określenie znanego mirroringu dysków lub odbicia lustrzanego. Zabezpieczenie przed awarią wymaga wyposażenia systemu w dwa dyski. Po skonfigurowaniu dublowania dane przechowywane na woluminie są zapisywane równolegle na dwóch dyskach. Dzięki temu awaria jednego z urządzeń nie powoduje utraty informacji. Woluminy RAID 5 działają w odmienny sposób. Do zabezpieczenia plików potrzeba co najmniej trzech dysków. Każdy z nich przechowuje dane oraz tzw. parzystość, czyli wyliczaną wartość, stosowaną do rekonstrukcji danych na wypadek awarii dysku. Jeśli jedno z urządzeń ulegnie uszkodzeniu, Windows Server 2003 odtwarza potrzebne informacje, sięgając do pozostałych dysków. Każdy ze wskazanych sposobów ochrony zasobów ma wady i zalety. Za zastosowaniem dublowania przemawia możliwość zabezpieczenia partycji rozruchowych i systemowych. Warto pamiętać, że partycja rozruchowa to obszar dysku zawierający pliki systemu Windows, natomiast partycja systemowa to miejsce, w którym zapisane są pliki potrzebne do uruchomienia systemu, np. NtDetect.com, Boot.ini oraz Ntldr. W większości komputerów będzie to ta sama partycja, np. C:. Drugą zaletą dublowania woluminów jest niższy koszt początkowy. Aby zabezpieczyć dane, należy kupić jeden dodatkowy dysk. Zastosowanie woluminów RAID 5 wymaga większych wydatków, ale koszt ochrony jednego MB informacji jest niższy. Woluminy RAID 5 mają większą wydajność odczytu niż mirroring. Podczas zapisywania danych wydajność spada, ponieważ system musi obliczyć parzystość.

Implementacja woluminów dublowanych oraz RAID 5 nie jest trudna. Najpierw należy skonwertować dyski serwera na dyski dynamiczne. Standardowe partycje podstawowe i rozszerzone nie pozwalają na ochronę danych przez RAID. W celu wykonania konwersji uruchamiamy moduł Zarządzanie komputerem (Narzędzia administracyjne). Następnie przechodzimy do folderu Zarządzanie dyskami i zaznaczamy dysk podstawowy. Po kliknięciu prawym przyciskiem myszy z menu podręcznego wybieramy Konwertuj na dysk dynamiczny. Jeśli konwertowana jest partycja rozruchowa lub systemowa, należy ponownie uruchomić komputer.

Uwaga! Konwersja dysku podstawowego na dynamiczny sporadycznie może się nie powieść. Przed operacją zmiany typu należy bezwzględnie wykonać kopię zapasową danych. Po skonwertowaniu na dysk dynamiczny system posługuje się woluminami, a nie partycjami. Jeśli chcemy powrócić do standardowych partycji podstawowych i rozszerzonych, należy wykonać pełną archiwizację danych, usunąć wszystkie woluminy, przekonwertować dysk na podstawowy, utworzyć partycje i odtworzyć pliki z kopii zapasowej.

Po konwersji w opisie dysku widoczny jest typ Dynamiczny, a partycja zmienia się w Wolumin prosty. Dalszy przykład zilustruje tworzenie woluminu dublowanego. Ponieważ dublowanie wymaga dwóch dysków dynamicznych, w opisany wcześniej sposób konwertujemy kolejny dysk. Następnie klikamy prawym przyciskiem ten wolumin, który będziemy dublować, i z menu podręcznego wybieramy polecenie Dodaj dublowanie. W nowym oknie wskazujemy lokalizację dublowania i klikamy Dodaj. Po odczekaniu kilku chwil na synchronizację danych woluminów mirror jest zestawiony. Z takim zabezpieczeniem systemu Windows Server 2003, jeśli jeden z dysków ulegnie awarii, można skorzystać z danych w drugim urządzeniu.

Zaawansowane opcje uruchamiania systemu

Ochrona informacji przechowywanych na serwerze jest fundamentalnym zadaniem administratora. Mozolne archiwizowanie oraz nadmiarowe rozwiązania dyskowe mogą się okazać mało przydatne, jeśli Windows Server 2003 po prostu nie będzie chciał się uruchomić. Część administratorów stosuje wówczas przywracanie systemu przez ASR, a

jeśli nie ma kopii odtwarzania, wybiera inny sprawdzony sposób - reinstalację. Warto pamiętać, że te rozwiązania należy traktować jako ostateczność. Windows Server 2003 pozwala na zastosowanie innych, mniej czasochłonnych i łatwiejszych sposobów reanimacji systemu. Najprościej skorzystać z serii przydatnych opcji zaawansowanego uruchamiania Windows. Jeśli w czasie początkowej fazy ładowania systemu naciśniemy przycisk [F8], zostanie wyświetlona lista trybów uruchamiania Windows Server 2003. Wybór jednej z opcji pozwala na ominięcie najczęstszych problemów startowych systemu operacyjnego. O tym, czy którykolwiek z trybów pomoże uniknąć kłopotów, decyduje rodzaj usterki Windows. Z "leczniczych" właściwości przycisku [F8] korzystamy wtedy, gdy zainstalowaliśmy niewłaściwy sterownik, skonfigurowaliśmy błędne parametry wyświetlania lub określiliśmy złe parametry startowe usług lub urządzeń.

Jeśli w czasie startu systemu pojawią się problemy związane z urządzeniami albo usługami, należy zastosować jeden z trzech trybów awaryjnych. Windows Server 2003 jest uruchamiany zgodnie z parametrami określonymi w Rejestrze. Zawarte tam wpisy określają zestaw kontrolny wykorzystywany podczas startu systemu. Zestaw kontrolny obejmuje: kolejność, typ i moment ładowania plików, sterowników urządzeń oraz usług systemowych. Jeśli jeden z elementów zawiedzie, rozruch Windows może się nie powieść. Wybór trybu awaryjnego pozwala na włączenie ograniczonej liczby urządzeń i usług. Dzięki temu eliminowane są potencjalne źródła problemów. Można również łatwo ustalić, który z komponentów sprawia problemy. Najczęściej uruchamiamy standardowy Tryb awaryjny. Zestaw kontrolny tego trybu zawiera listę urządzeń i usług niezbędnych do wystartowania systemu. Jeśli po jego wybraniu Windows uruchomi się bez błędów, sytuacja jest opanowana. Dalsze działania polegają na stopniowym ustalaniu, który ze sterowników albo usług jest przyczyną problemów. W tym celu możemy posłużyć się modułem usługi, kartą Sprzęt, dostępną we właściwościach Systemu czy programem MSCONFIG.EXE. Pozostałe typy awaryjnego rozruchu zawierają dodatkowe opcje startowe. Po wskazaniu ładowania Trybu awaryjnego z obsługą sieci oprócz minimalnego zestawu kontrolnego uruchamiane są urządzenia związane z komunikacją sieciową. Wybranie Trybu awaryjnego z wierszem polecenia powoduje, że po zalogowaniu użytkownika ładowana jest powłoka tekstowa, a nie Eksplorator Windows.

Kolejne opcje menu startowego pozwalają na rozwiązywanie problemów dotyczących szczegółowych ustawień systemu. Rozruch Windows z parametrem Włącz tryb VGA ładowanie zainstalowanego przez użytkownika sterownika karty graficznej z najniższą obsługiwaną rozdzielczością. Zapobiega to problemom wynikającym z błędnych ustawień parametrów wyświetlania. Gdy uruchamiamy system za pomocą wymienionych wcześniej trybów awaryjnych, Windows startuje z podstawowym sterownikiem wideo. Opcja Włącz rejestrowanie rozruchu służy do śledzenia przebiegu procedury startowej Windows Server 2003. W czasie uruchamiania system zapisuje przebieg rozruchu w pliku dziennika. Jeśli podczas startu wystąpią kłopoty, możemy sięgnąć do pliku i zobaczyć, który z komponentów powoduje błędy. Domyślnie plik dziennika nosi nazwę ntbtlog.txt i jest zapisywany w folderze Windows. Jeśli serwer pełni funkcję kontrolera domeny, w przypadku problemów związanych z usługą Active Directory, niezbędny jest Tryb przywracania usług katalogowych. Po uruchomieniu systemu z użyciem tej opcji możemy odtwarzać Active Directory z kopii zapasowej oraz przeprowadzać zaawansowane operacje naprawcze przy użyciu narzędzia wiersza poleceń NTDSUTIL.EXE. W przypadku poważnej awarii serwera administrator może się posłużyć trybem debugowania. Jego zastosowanie pozwala na szczegółowe monitorowanie rozruchu systemu z jednoczesnym przesyłaniem zebranych informacji do innego komputera. Dzięki temu pracownicy obsługi technicznej będą mogli dokładnie zlokalizować problem. Informacje diagnostyczne są przesyłane kablem szeregowym podłączonym do portu COM1.

Parametr Ostatnia znana dobra konfiguracja to szybki sposób na doraźne kłopoty. W czasie uruchamiania serwera system korzysta z zestawu kontrolnego przechowywanego w Rejestrze. W odpowiednich kluczach Rejestru przechowywany jest również zapasowy zestaw startowy, zapisywany w czasie ostatniego poprawnego logowania do konsoli

Windows Server 2003. Skuteczne uwierzytelnienie jest dla systemu zwieńczeniem prawidłowego rozruchu. Jeśli po zalogowaniu administrator zmienia konfigurację systemu na taką, która powoduje kłopoty z uruchomieniem serwera, możemy skorzystać z alternatywnych ustawień rozruchowych. Wybieramy je, zaznaczając opcję Ostatnia znana dobra konfiguracja. Należy pamiętać, że wskazanie tego parametru nie uchroni nas przed kłopotami związanymi z usunięciem lub zamianą plików systemowych. Jeśli uruchomimy Windows Server 2003 w trybie znanej dobrej konfiguracji, wszystkie zmiany wprowadzone przed ostatnim zamknięciem systemu są zastępowane ustawieniami zapisanymi w zapasowym zestawie startowym.

Konsola odzyskiwania

Zaawansowane parametry startowe pomagają rozwiązać wiele kłopotów z rozruchem Windows. Są jednak problemy, których nie rozwiąże zastosowanie trybu awaryjnego czy ostatniej znanej dobrej konfiguracji. Jeśli usuniemy ważny plik systemowy albo wirus uszkodzi sektor rozruchowy, niezbędne będzie zastosowanie Konsoli odzyskiwania Windows Server 2003.

Konsola odzyskiwania jest alternatywną metodą uruchamiania systemu. W przeciwieństwie do opisywanych wcześniej opcji, dostępnych po naciśnięciu przycisku [F8], po jej włączeniu nie jest uruchamiany system operacyjny, lecz tekstowe środowisko naprawcze. Środowisko to zawiera narzędzia do usuwania najpoważniejszych problemów rozruchowych. Za jego pomocą możemy przywrócić pliki systemowe, naprawić środowisko startowe, konfigurować parametry startowe usług, testować stan dysków komputera, zarządzać partycjami Windows Server 2003 itp.

Konsolę można uruchomić na dwa sposoby. Jeśli zależy nam na stałej możliwości korzystania ze środowiska odzyskiwania, należy zainstalować konsolę. Instalację rozpoczyna uruchomienie z katalogu I386 płyty instalacyjnej systemu polecenia WINNT32 z parametrem /CMDCONS. Rezultat można zaobserwować w czasie następnego uruchomienia Windows. System wyświetli menu pozwalające na start serwera przy użyciu konsoli odzyskiwania. Jeśli stały dostęp do konsoli nie jest wymagany, dostęp do środowiska naprawczego można uzyskać, uruchamiając Windows Server 2003 z płyty instalacyjnej.

Niezależnie od sposobu uruchomienia konsoli obowiązuje logowanie do Windows. Po wyświetleniu listy systemów operacyjnych zainstalowanych na serwerze należy wskazać ten, do którego chcemy się zalogować, a następnie wprowadzić hasło administratora. Korzystając z konsoli odzyskiwania, nie możemy się zalogować na dowolne konto. Jeśli serwer ma zainstalowane usługi katalogowe, w celu dostępu do konsoli, należy podać hasło definiowane podczas instalacji Active Directory jako hasło administratora do trybu przywracania usług katalogowych. Po uwierzytelnieniu system wyświetla znak zgłoszenia i można wprowadzać dowolne polecenia konsoli odzyskiwania. Pełną listę poleceń uzyskujemy po wpisaniu HELP. Do najbardziej przydatnych poleceń zaliczamy: CHKDSK, BOOTCFG, FIXBOOT, FIXMBR, COPY i EXPAND. Pozwalają one na sprawdzenie partycji oraz podstawowych operacji naprawczych systemu operacyjnego. Na koniec warto zwrócić uwagę na ustawienia Zasad grupy, które zwiększają elastyczność posługiwania się konsolą odzyskiwania. Domyślnie system operacyjny nie pozwala na stosowanie symboli wieloznacznych typu *, ogranicza dostęp do katalogów na partycji z systemem operacyjnym oraz nie pozwala na kopiowanie danych na urządzenia przenośne. W celu wyłączenia tych ograniczeń dla kontrolerów domeny, należy przejść do Narzędzi administracyjnych i uruchomić moduł Zasady zabezpieczeń kontrolera domeny. Następnie trzeba wybrać kolejno Ustawienia systemu Windows | Ustawienia zabezpieczeń | Zasady lokalne | Opcje zabezpieczeń. W grupie Opcje zabezpieczeń odnajdziemy dwa parametry związane z Konsolą odzyskiwania: Konsola odzyskiwania: zezwalaj na kopiowanie na dyskietkę oraz dostęp do wszystkich dysków i folderów oraz Konsola odzyskiwania: zezwalaj na automatyczne logowanie administracyjne. Zezwolenie na

kopiowanie wydajemy, zaznaczając opcję Definiuj następujące ustawienia zasad oraz Włącz. Drugiego ustawienia ze względów bezpieczeństwa nie należy stosować. W celu sprawdzenia i ewentualnej zmiany konfiguracji rozszerzeń konsoli należy po jej uruchomieniu posłużyć się poleceniem SET.

Jacek Ścisławski

Skuteczne zabezpieczenie systemu to jedno z najważniejszych zadań administratora. W sieciach komputerowych, gdzie trzeba chronić wiele komputerów, jego realizacja jest utrudniona. Windows Server 2003 umożliwia centralne zarządzanie ustawieniami zabezpieczeń, a następnie jednoczesne dostarczenie konfiguracji do stacji klientów.

Zarządzanie zabezpieczeniami systemów sieciowych powinno być bezproblemowe i sprawne. Windows Server 2003 zawiera grupę narzędzi, za pomocą których administrator może zmienić ustawienia na wszystkich serwerach i stacjach roboczych bez odchodzenia od swojego komputera. System zawiera przystawki pozwalające na szybką weryfikację, czy wprowadzane zmiany nie kolidują z bieżącymi parametrami serwera. Centralne przekazywanie ustawień zabezpieczeń jest realizowane przez Zasady grupy. Są jednak prostsze mechanizmy konfigurujące komputery pracujące w sieci. Dodatkowo administrator może szybko przygotować szablony ustawień, a następnie w prosty sposób zaimportować je do wybranych komputerów lub obiektów zasad grupy.

Uproszczone mechanizmy konfiguracji zabezpieczeń

Zasady grupy są dobrym i elastycznym rozwiązaniem, pozwalającym na szybkie skonfigurowanie środowiska pracy klientów sieci. Dużym organizacjom implementacja złożonych obiektów zasad umożliwia nadzorowanie sieci rozległych, składających się z setek komputerów. Niewielkim firmom zakładanie skomplikowanej struktury domen, jednostek organizacyjnych i lokalizacji nie jest potrzebne. Administratorów bardziej

interesuje szybkie i skuteczne zabezpieczenie sieci oraz serwera. Do realizacji tego celu otrzymują dwie proste przystawki.

Po wyświetleniu zawartości folderu Narzędzia administracyjne wśród wielu skrótów odnajdujemy Zasady zabezpieczeń kontrolera domeny, Zasady zabezpieczeń domeny oraz Zasady zabezpieczeń lokalnych. Przystawki te służą do błyskawicznego określenia parametrów bezpieczeństwa wszystkich kontrolerów domeny, wszystkich komputerów w sieci i lokalnego serwera. Każde z narzędzi jest fragmentem ustawień, które możemy przypisać w obiektach Zasad grupy. Jeśli Windows Server 2003 pełni funkcję kontrolera domeny, podczas instalacji usługi Active Directory zakładane są dwa obiekty zasad, Default Domain Policy oraz Default Domain Controllers Policy. Pierwszy jest związany z instalowaną domeną, drugi obejmuje ustawienia kont komputerów umieszczonych w jednostce organizacyjnej Domain Controllers. Domyślnie są w niej tworzone konta kontrolerów domeny. Zmiany parametrów przystawek Zasady zabezpieczeń kontrolera domeny i Zasady zabezpieczeń domeny są w rzeczywistości modyfikacjami jednego z domyślnych obiektów zasad. Przystawka Zasady zabezpieczeń lokalnych służy do konfiguracji lokalnego środowiska serwera.

Jeżeli administrator chce zmienić parametry zabezpieczeń sieci, nie musi uruchamiać narzędzia Użytkownicy i komputery usługi Active Directory albo Group Policy Managment Console, wywoływać Edytora obiektów zasad i błądzić po ustawieniach komputerów. Wystarczy uruchomienie przystawki Zasady zabezpieczeń domeny. W wyświetlonej konsoli będzie można nanosić wszelkie parametry zabezpieczeń oraz definiować skrypty uruchamiania i zamykania komputerów.

Uwaga! Podczas konfiguracji zabezpieczeń kontrolerów domeny należy uważać na konflikty z ustawieniami zawartymi w Zasadach zabezpieczeń lokalnych. Jeśli parametry lokalne będą zastąpione przez zasady domenowe, system poinformuje nas o tym, przez wyświetlenie odpowiedniej ikony.

Przykładowa konfiguracja zasad ograniczeń oprogramowania

Zabezpieczenia ustawiane przez Zasady grupy zawierają bardzo atrakcyjną funkcję nadzorującą uruchamianie oprogramowania na stacji lokalnej. Usługa ta jest niezmiernie przydatna, jeśli chcemy się zabezpieczyć przed automatycznym uruchamianiem wirusów lub zabronić pracownikom korzystania z niedozwolonych programów typu komunikator internetowy.

Windows Server 2003 oferuje serie parametrów wpływających na ograniczenia oprogramowania. Po pierwsze, możemy zezwalać na uruchamianie wszystkich aplikacji z wyjątkiem zakazanych albo odwrotnie, tylko tych programów, które wskażemy. System pozwala również na wskazanie następujących reguł identyfikacji aplikacji: mieszania, certyfikatów, ścieżki oraz strefy internetowej. W zależności od właściwości programu dobieramy odpowiednią regułę. Do ograniczania specyficznego pliku uruchamiającego aplikację najlepiej nadaje się reguła mieszania. Stosuje specjalny algorytm hashowania, który wylicza wartość bezbłędnie identyfikującą plik lub program, trzeba jednak pamiętać, że po ukazaniu się nowej wersji aplikacji wartość obliczana przez algorytm może się zmienić i reguła przestaje skutkować.

Bardzo bezpiecznym sposobem konfigurowania stacji sieciowych jest wyraźne wskazanie, jakie aplikacje mogą być uruchamiane. Nie trzeba wówczas dodawać każdego zabronionego programu do listy ograniczeń. Po przygotowaniu zbioru dozwolonych aplikacji i nadaniu odpowiednich uprawnień w systemie plików komputer będzie dobrze zabezpieczony. Powiemy teraz, jak wprowadzić ograniczenie zakazujące wszystkim użytkownikom domeny uruchamiania gry "Pasjans".

Jeśli chcemy ograniczyć uruchamianie oprogramowania w całej domenie, uruchamiamy przystawkę Zasady zabezpieczeń domeny i przechodzimy do folderu Zasady ograniczeń oprogramowania. Po zaznaczeniu folderu z menu Akcja wybieramy polecenie: Nowe zasady ograniczeń oprogramowania, zaznaczamy folder Reguły dodatkowe i z menu Akcja wybieramy Nowa reguła mieszania. W wyświetlonym oknie wskazujemy plik, który chcemy mieszać. W naszym przykładzie będzie to sol.exe. Alternatywnie można zabronić uruchamiania gry, wskazując ścieżkę, w której domyślnie jest przechowywany plik wykonywalny. W takim wypadku należy posłużyć się opcją: Nowa reguła ścieżki. Metoda mieszania stosunkowo dobrze eliminuje niepożądane oprogramowanie i jest skuteczna nawet wtedy, gdy użytkownicy zmienią domyślną ścieżkę lub nazwę pliku wykonywalnego.

Ograniczenia dotyczące oprogramowania można konfigurować na poziomie komputerów lub użytkowników. Zasady nałożone na komputery przenoszą parametry na wszystkich klientów pracujących przy danej stacji. Ustawienia związane z użytkownikami przechodzą na konta objęte kontenerem. Dla zasad zabezpieczenia domeny nie ma to większego znaczenia, ale jeśli w domenie zostały założone jednostki organizacyjne, przypisanie ograniczeń dla kont użytkowników umieszczonych w pojemnikach zawęzi obszar przenoszenia zasad do wskazanego zakresu.

Szablony zabezpieczeń

Konfiguracja parametrów obejmujących bezpieczeństwo serwerów i stacji roboczych wymaga zaznaczenia odpowiedniej opcji w przystawce Zasady zabezpieczeń kontrolerów domeny lub Zasady zabezpieczeń domeny. Sposób określania ustawień Zasad grupy nie jest skomplikowany, ale jeśli zdarza się dużo zmian - bez wątpienia uciążliwy. Sprawne przeszukiwanie ponad setki parametrów, szczegółowe wczytywanie się w pomoc dotyczącą każdej opcji, wymaga czasu. Chcąc ujednolicić ustawienia i wykorzystać w wielu domenach albo stacjach pracujących w grupach roboczych, należy przygotować szablon zabezpieczeń, czyli plik tekstowy zawierający ustawienia wprowadzane do Zasad zabezpieczeń.

W skład szablonu wchodzą ustawienia znane z narzędzi do implementacji zasad. Po otworzeniu dowolnego pliku określamy parametry Zasad konta, Zasad lokalnych, Dziennika zdarzeń, Grup z ograniczeniami, Usług systemowych, Rejestru oraz Systemu plików. Zawartość szablonów możemy modyfikować odpowiednio do potrzeb, a następnie zapisać je pod własną nazwą. Dla przykładu: po zainstalowaniu systemu operacyjnego tworzony jest plik domyślnych ustawień uprawnień do plików systemowych Windows Server 2003. Szablon może być zmodyfikowany i zapisany, a następnie importowany do ustawień innego serwera lub do wybranego obiektu zasad grupy domeny.

System operacyjny jest dostarczany z grupą gotowych szablonów zawierających ustawienia kontrolerów domeny, serwerów członkowskich oraz stacji roboczych. Do każdego typu komputera oferowany jest inny poziom zabezpieczeń, od domyślnego, standardowego, do wyższego, wymuszającego mocne zabezpieczenia. Folder C:\WINDOWS\security\templates zawiera grupę wbudowanych szablonów. Są tam zarówno pliki o standardowym poziomie zabezpieczeń (DC Security.inf), umożliwiające bezproblemowe uruchamianie aplikacji na stacjach roboczych (compatws.inf), jak i podnoszące poziom zabezpieczeń (securedc.inf), wprowadzające mocną ochronę (hisecdc.inf). Szablony iesacls.inf, setup security.inf oraz rootsec.inf określają ustawienia kluczy rejestru Internet Explorera, zabezpieczeń plików systemu po instalacji oraz plików zapisanych w głównym katalogu.

Narzędzie do konfiguracji szablonów

Podstawowe narzędzie do administrowania szablonami to przystawka Szablony zabezpieczeń. Nie jest dostępna bezpośrednio z folderu Narzędzia administracyjne, jej

uruchomienie wymaga kilku prostych operacji. Zaczynamy od wpisania MMC w wierszu polecenia. Naciśnięcie OK otworzy pustą konsolę. Następnie z menu Plik wybieramy Dodaj/Usuń przystawkę i klikamy Dodaj. Na liście przystawek autonomicznych wskazujemy Szablony zabezpieczeń. Na koniec klikamy Dodaj | Zamknij | OK. Administratorzy, którzy będą często sięgali do ustawień szablonów, mogą zapisać konsolę. Z menu Plik wybieramy Zapisz jako, po czym określamy nazwę i lokalizację konsoli.

Po otwarciu konsoli widzimy folder opisujący ścieżkę do plików szablonów. Wstępną zawartość przystawki stanowią szablony dostępne po instalacji Windows Server 2003. Ustawienia każdego z szablonów możemy łatwo przeglądać, kolejno rozwijając umieszczone w nim foldery. Szblon - zależnie od typu - zawiera od kilku do kilkudziesięciu zdefiniowanych zasad. Przy parametrach neutralnych wyświetlany jest opis Nie zdefiniowane. Chcąc założyć nowy szablon, zaznaczamy folder opisany przez ścieżkę C:\WINDOWS\security\templates i z menu Akcja wybieramy polecenie Nowy szablon. Po wprowadzeniu nazwy oraz opisu szablonu zakładany jest obiekt niezawierający żadnych zasad. Często wystarczy odpowiednio zmodyfikować zawartość szablonów, zamiast konfigurować parametry zabezpieczeń od początku. W celu przeprowadzenia takiej operacji zaznaczamy jeden z szablonów, a następnie z menu Plik wybieramy Zapisz jako. Po nadaniu nazwy otrzymujemy nowy obiekt, zawierający wszystkie ustawienia modelu. Następnie zmieniamy zasady odpowiednio do potrzeb.

Sugerowana przez system ścieżka do przechowywania szablonów nie jest obowiązkową lokalizacją plików. Na wielu stronach internetowych, w tym również Microsoftu, są gotowe pliki konfigurujące zabezpieczenia nie tylko do systemu Windows Server 2003, ale także do Windows 2000 oraz Windows XP. Po pobraniu pliku warto sprawdzić, jakie parametry systemu są przez niego modyfikowane. Aby otworzyć skopiowany szablon w przystawce, zaznaczamy folder Szablony zabezpieczeń i z menu Akcja wybieramy Ścieżka wyszukiwania nowego szablonu. Następnie odnajdujemy pobrany z Internetu plik i klikamy OK. Zobaczmy, jak przeprowadzić tę operację na przykładzie przewodnika o zabezpieczeniach Windows Server 2003, pobranego z witryny firmy Microsoft.

Rozpoczynamy od pobrania interesujących nas danych z Internetu. Wchodzimy na stronę www.microsoft.com/dowloads, następnie w polu Keywords wprowadzamy ciąg znaków: Server 2003 Security Guide. Pierwszą pozycją z listy odnalezionych odnośników powinien być przewodnik zabezpieczania systemu Windows Server 2003 (Windows Server 2003 Security Guide). Kliknięcie łącza otwiera stronę pobierania danych. W czasie pisania tego artykułu najnowsza wersja poradnika miała numer 1.3. W celu zapisania na dysku pliku instalacyjnego klikamy łącze Windows_Server_2003_Security_Guide_v1_3.exe. W wypadku połączenia o przeciętnej wydajności pobranie pliku nie powinno trwać dłużej niż kilkadziesiąt sekund. Kolejny etap to rozpakowanie pobranego przewodnika. Zapisujemy go w dowolnym miejscu. Grupę interesujących szablonów odnajdziemy w ścieżce: folder_do_którego_rozpakowaliśmy_plik\Tools and Teplates\Security Guide\Security Teplates. Ścieżkę tę podajemy jako lokalizację szablonów w przystawce Szablony zabezpieczeń. Po wprowadzeniu ścieżki do plików konsola będzie zawierała dwie lokalizacje szablonów, starą: C:\WINDOWS\SECURITY\TEMPLATES oraz nową. Ustawienia zawarte w pobranych plikach możemy przeglądać w standardowy sposób. Jeśli chcemy porównać ich parametry z bieżącymi ustawieniami Windows Server 2003, musimy posłużyć się inną przystawką.

Przystawka porównująca i testująca szablony zabezpieczeń

Niewłaściwe przygotowanie własnego szablonu lub bezkrytyczne korzystanie z plików pobranych z Internetu może przynieść opłakane skutki. Zanim ustawienia zostaną zastosowane w sieci, należy je dokładnie zweryfikować. Funkcje sprawdzania ustawień szablonów oferuje narzędzie Konfiguracja i analiza zabezpieczeń. Przystawkę

uruchamiamy tak samo, jak Szablony zabezpieczeń. W celu ułatwienia sobie pracy najlepiej połączyć obie przystawki w jedną konsolę administracyjną.

Bezpośrednio po uruchomieniu przystawka nie wyświetla analiz ustawień szablonów. Widzimy opis tworzenia lub otwierania nieznanej bazy danych. Baza danych analizy zabezpieczeń jest źródłem informacji potrzebnych do porównania ustawień zawartych w szablonie z parametrami obowiązującymi w Windows Server 2003. Dlatego najpierw jesteśmy proszeni o utworzenie lub otwarcie bazy. Niezależnie od tego, czy zakładamy nowy plik porównania, czy korzystamy z już utworzonego, dostęp do bazy uzyskujemy po kliknięciu folderu Konfiguracja i analiza zabezpieczeń i wybraniu z menu Akcja polecenia Otwieranie bazy danych. Pierwsze uruchomienie przystawki wymaga założenia pliku. Jest to prosta czynność, polegająca na nazwaniu bazy i kliknięciu Otwórz. Ponieważ jednym z zadań przystawki jest analiza zabezpieczeń, do pliku porównawczego trzeba zaimportować wybrany szablon. Szablon odszukujemy i wskazujemy w następnym oknie. Kliknięcie po raz kolejny Otwórz kończy zakładanie bazy. Dalsze postępowanie zależy od tego, czy chcemy analizować ustawienia szablonu i systemu, czy mamy zamiar natychmiast wprowadzić zasady szablonu do systemu Windows Server 2003.

Analizę zabezpieczeń włączamy, wybierając w menu Akcja polecenie Analizuj komputer teraz. Po wybraniu analizy system prosi o wskazanie położenia tekstowego dziennika błędów. Po naciśnięciu OK rozpoczynamy porównywanie ustawień. Rezultat testu nie jest dostrzegalny na pierwszy rzut oka. Przydatne informacje otrzymujemy dopiero podczas rozwijania kolejnych folderów, np. zasad konta, zasad lokalnych itd. Wyświetlane są znaczniki informujące o wynikach analizy poszczególnych parametrów szablonu. Czerwony X oznacza, że pomiędzy ustawieniami bazy i Windows wystąpiły różnice. Dzieje się tak np. wtedy, gdy minimalna długość hasła w systemie wynosi siedem znaków, a w bazie pięć. Zielone V wskazuje na zgodność ustawień Windows i bazy. Ostatnie dwa oznaczenia to wykrzyknik oraz znak zapytania. Znak zapytania informuje, że zasada nie była określona w bazie i dlatego nie jest analizowana, a wykrzyknik - że baza zawiera ustawienie, którego nie ma w systemie Windows Server 2003.

Jeśli nie mamy ochoty wędrować po folderach szablonu i przypatrywać się każdemu z parametrów, możemy skorzystać z informacji zgromadzonych w dzienniku analizy. Zawartość dziennika jest wyświetlana bezpośrednio w konsoli. Dostęp do danych uzyskujemy po zaznaczeniu folderu Konfiguracja i analiza zabezpieczeń i wybraniu z menu Akcja polecenia Wyświetl plik dziennika.

Po dokładnym przeanalizowaniu i zakceptowaniu zmian, które wprowadza szablon, możemy zastosować je w systemie. Służy do tego polecenie Konfiguruj komputer teraz. Zanim wskażemy tę opcję, należy jeszcze raz sprawdzić, czy zdefiniowane parametry są określone poprawnie, bo konfiguracja powoduje natychmiastowe wprowadzenie ustawień do serwera. Szablony zabezpieczeń możemy stosować również do obiektów zasad grupy. Po otworzeniu jednej z zasad, np. Zasady zabezpieczeń domeny, zaznaczamy folder Ustawienia zabezpieczeń i z menu Akcja wybieramy Importuj zasady. W nowym oknie wskazujemy nazwę szablonu i klikamy Otwórz.

Dodawanie własnych zasad do szablonu

Na pierwszy rzut oka szablony zabezpieczeń wydają się mało elastyczne. Można konfigurować określone przez administratora uprawnienia do systemu plików, kluczy w rejestrze oraz członkostwo w grupach z ograniczeniami, ale pozostałe ustawienia wyglądają na statyczne. Okazuje się, że bez większych kłopotów możemy umieszczać w szablonach własne zasady.

Duża część parametrów zabezpieczeń jest przenoszona na stacje klientów metodą dodania odpowiednich wpisów w rejestrze systemu operacyjnego. W ten sposób na komputery trafia większość ustawień związanych z Szablonami administracyjnymi

konfigurowanymi przez Zasady grupy. Jeśli chcemy dodać własne wpisy do szablonu, musimy wiedzieć, jaki parametr rejestru ma być przenoszony na stacje sieciowe oraz poznać notację wprowadzania ustawień do plików *.inf. Dodawanie wpisów do szablonów najlepiej zilustrować na przykładzie.

Pobrane z Internetu dodatkowe szablony zabezpieczeń zawierają ustawienia zwiększają bezpieczeństwo Windows Server 2003, np. w pliku High Security - Member Server Baseline ukryty jest wpis zwiększający bezpieczeństwo automatycznej ochrony systemu po okresie bezczynności. Domyślnie Windows Server 2003 ma skonfigurowany wygaszacz ekranu, uruchamiany po czasie określonym w parametrach wyświetlania. Start wygaszacza wiąże się z zablokowaniem konsoli serwera. Warto wiedzieć, że domyślnie następuje krótki, kilkusekundowy okres przejściowy pomiędzy uruchomieniem wygaszacza a blokadą konsoli. W celu zwiększenia bezpieczeństwa należy wyzerować opóźnienie. Szablon High Security - Member Server Baseline (oraz kilka innych) zawiera wpis ustawiający opóźnienie na 0 sekund. Parametru tego nie widać jednak w przystawce przeznaczonej do konfigurowaniu opcji zabezpieczeń. Za pomocą kilku prostych operacji możemy usunąć tę niedogodność. Na początku ustalmy, jaki wpis w rejestrze modyfikuje parametry wygaszacza. Za zerowe opóźnienia odpowiada ScreenSaverGracePeriod, typ ciąg znaków, wartość 0. Parametr ten umieszczamy w kluczu HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon. W celu dodania opcji wygaszacza do szablonu zabezpieczeń należy klucz rejestru dopisać do pliku Sceregvl.inf. Odnajdziemy go w folderze katalog_systemowy\inf, np. C:\Windows\inf. Przed modyfikacją pliku należy, na wszelki wypadek utworzyć jego kopię. Po otwarciu pliku w Notatniku odnajdujemy nagłówek [Register Registry Values]. Pod nagłówkiem znajduje się opis składni wprowadzania danych oraz klucze Rejestru. Za ostatnim kluczem dopisujemy: MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ ScreenSaverGracePeriod,1,%SCREENSAVER%,1. Następnie przechodzimy do nagłówka [Strings] i na jego końcu dodajemy wpis: SCREENSAVER="Wygaszacz ekranu: ustaw opóźnienie między uruchomieniem wygaszacza a blokadą konsoli (zalecane 0 sekund)". Dodane wiersze oznaczają, że w folderze Opcje zabezpieczeń szablonów ma zostać umieszczona zasada: Wygaszacz ekranu: ustaw opóźnienie między uruchomieniem wygaszacza a blokadą konsoli (zalecane 0 sekund). Pierwszy parametr, w naszym przykładzie równy 1, określa typ wartości rejestru. %SCREENSAVER% to etykieta opisu wprowadzonego w nagłówku [Strings]. Ostatni parametr wskazuje na sposób wyświetlania zasady w szablonie. Ponieważ opóźnienie wygaszacza jest wyrażane w sekundach, kolejna cyfra 1 wskazuje, że wyświetlany ma być typ numeryczny. Po zapisaniu pliku Sceregvl.inf w menu Plik Eksploratora Windows wybieramy Zainstaluj. Ostatnią operacją jest kliknięcie Start | Uruchom i wpisanie polecenia Regsvr32 scecli.dll. Po naciśnięciu OK możemy przejść do przystawki z szablonami i w folderze Opcje zabezpieczeń odnajdziemy nowy wpis dotyczący wygaszacza ekranu.

Jacek Ścisławski

wersja do wydruku
|strona główna|wersja oryginalna|

IDG.PL
Wyjście na świat
PC World Komputer

Administrator sieci to osoba czuwająca nad poprawną pracą systemów komputerowych oraz urządzeń komunikacyjnych firmy. Windows Server 2003 zawiera usługę Routing i dostęp zdalny, którą z powodzeniem możemy nazwać wbudowanym administratorem sieci. Jej zadaniem jest realizacja oraz nadzorowanie wchodzącej i wychodzącej transmisji danych w systemie Windows Server 2003.

Wykorzystanie systemu Windows Server 2003 w niewielkich firmach powoduje, że serwer musi wykonywać więcej zadań, m.in. obsługa połączeń zewnętrznych. Usługa Routing i dostęp zdalny oprócz przyjmowania połączeń przychodzących od mobilnych pracowników przedsiębiorstwa (patrz artykuł: "Uzdolnienia sieciowe Windows Server 2003") umożliwia współdzielenie połączenia internetowego lokalnym pracownikom firmy.

Brama do Internetu

Jednym z podstawowych zastosowań usług komunikacyjnych wbudowanych w Windows Server 2003 jest pełnienie funkcji bramy wyjściowej do Internetu, możliwe na dwa sposoby. Dla wielu niewielkich firm zdecydowanie najlepszym rozwiązaniem jest Udostępnianie połączenia internetowego (Internet Connection Sharing, ICS). Drugi ze sposobów to Translacja adresów sieciowych. NAT pozwala na dodatkowe ustawienie szeregu istotnych właściwości połączenia.

ICS jest łatwym i co bardzo ważne, szybkim sposobem na zapewnienie połączenia internetowego w niewielkich firmach. Administrator włączający udostępnianie wykonuje tylko kilka kliknięć, a o resztę parametrów połączenia martwi się system. Prostota konfiguracji dla mniej doświadczonych użytkowników jest ważną zaletą, jednak niewielkie możliwości wpływania na ustawienia połączenia nie ucieszą administratorów, którzy chcą narzucać bardziej wyrafinowane parametry.

Jeśli administrator sieci wymaga większej elastyczności przy zarządzaniu komunikacją z siecią zewnętrzną, powinien pomyśleć o skorzystaniu z NAT. Konfiguracja translacji jest nieco bardziej skomplikowana, ale w zamian uzyskujemy np. możliwość definiowania własnych parametrów adresowania IP, korzystania z wielu adresów publicznych, zaawansowanego filtrowania ruchu sieciowego itd.

Interfejsy sieciowe

Przed przystąpieniem do konfiguracji jakichkolwiek połączeń internetowych należy odpowiednio przygotować ustawienia sieci. Ponieważ liczba możliwych wariantów interfejsów komunikacyjnych jest znaczna, opis usług ICS, NAT oraz zdalnego dostępu ograniczymy do prezentacji ustawień serwera pracującego z dwoma kartami sieciowymi. Warto pamiętać, że w takim przypadku jeden interfejs Windows Server 2003 powinien być podłączony do Internetu i mieć adres IP widoczny z sieci zewnętrznej.

Drugiej karcie należy przypisać identyfikator z puli adresów prywatnych albo - jeśli będziemy stosować ICS - określić adresowanie automatyczne.

Żeby się nie pogubić podczas konfiguracji usług sieciowych, warto przypisać odpowiednie nazwy wszystkim interfejsom. Domyślnie każdy z nich ma niewiele mówiącą etykietę Połączenie lokalne i Połączenie lokalne 2. Kartę wewnętrzną można nazwać LAN lub SiecLokalna, a zewnętrzną WAN lub Internet. Zmianę nazwy wykonujemy po wejściu w Panel sterowania i Połączenia sieciowe. Następnie zaznaczamy ikonę reprezentującą interfejs sieciowy i z menu Plik wybieramy Zmień nazwę.

Oprócz nazw karty sieciowe powinny mieć odmienne właściwości. Rozpocznijmy od parametrów interfejsu zewnętrznego. Na karcie WAN nie należy włączać takich składników, jak Klient sieci Microsoft Networks oraz Udostępnianie plików i drukarek w sieciach Microsoft Networks. Wyłączenie tych usług wykonujemy przez usunięcie znaczników we właściwościach połączenia WAN. Ustawienia adresowania IP zależą od informacji przekazanych przez usługodawcę internetowego. Jeśli przyznano nam stały adres IP, we właściwościach protokołu TCP/IP wprowadzamy otrzymane parametry. W niektórych przypadkach adres zewnętrzny może być przyznawany dynamicznie. W takim przypadku należy ustawić opcję Uzyskaj adres IP automatycznie. Bardzo ważne jest prawidłowe skonfigurowanie adresowania serwerów DNS. Błędne wskazanie usługodawcy DNS może doprowadzić do kłopotów z rozwiązywaniem nazw internetowych lub problemami podczas logowania do domeny. Więcej informacji o ustawieniach DNS zawiera następny akapit. Konfiguracja interfejsu wewnętrznego może być wykonana przez administratora Windows Server 2003 lub - jeśli włączymy Udostępnianie połączenia internetowego - będzie określona automatycznie przez system. Przypisując parametry ręcznie, do adresowania IP należy użyć jednego z adresów prywatnych, np. 10.0.0.1/24 lub 192.168.0.1/24.

Ustawienie DNS do pracy z Internetem

Jeśli podczas dodawania roli kontrolera domeny w systemie Windows Server 2003 kreator instalacji otrzymał polecenie automatycznego zainstalowania i skonfigurowania usługi DNS, musimy wykonać kilka zmian przygotowujących tę usługę do współpracy z Internetem. Domyślne ustawienia wprowadzane przez kreatora zakładają lokalnie strefę główną (root). W takim przypadku klienci wysyłający do Windows Server 2003 prośby o rozwiązanie nazwy internetowej, np. www.pcworld.pl, zostaną odprawieni z kwitkiem. Serwer sprawdzi, czy są wpisy związane z domeną pcworld.pl, a ponieważ ich nie znajdzie, odpowie klientowi komunikatem Nie odnaleziono nazwy. Jeśli Windows Server 2003 będzie funkcjonował jednocześnie jako brama do Internetu i kontroler domeny, należy usunąć strefę główną oraz skonfigurować Usługi przesyłania dalej w serwerze DNS.

Strefę główną usuwamy w przystawce DNS. Odnajdziemy ją w Narzędziach administracyjnych. Po otwarciu przystawki przechodzimy do foldeu Strefy wyszukiwania do przodu i zaznaczamy strefę .(główny). Następnie z menu Akcja wybieramy Usuń. Po potwierdzeniu operacji usunięcia możemy zamknąć przystawkę.

Dalsze czynności administracyjne są związane z konfiguracją usług przesyłania dalej. Po usunięciu strefy głównej serwer DNS może rozwiązywać nazwy internetowe, wysyłając prośby o rozwiązanie nazw do ogólnoświatowych serwerów root. Lepsze jest ustawienie przekazywania zapytań do serwera DNS usługodawcy internetowego. W tym celu otwieramy przystawkę DNS i zaznaczamy ikonę przedstawiającą serwer. Następnie z menu Akcja wybieramy właściwości. Po przejściu do karty Usługi przesyłania dalej, w polu Lista adresów IP wybranych usług przesyłania dalej domeny wpisujemy adres IP serwera DNS usługodawcy. Następnie naciskamy przycisk Dodaj i zamykamy okno oraz przystawkę. Od tej chwili wszystkie nazwy, których nie będzie umiał rozwiązać lokalny Windows Server 2003, zostaną przesłane do wskazanego serwera DNS.

Konfiguracja Udostępniania połączenia sieciowego

Uruchomienie udostępniania połączenia internetowego jest bardzo prostą operacją. W Panelu sterowania otwieramy Połączenia sieciowe i zaznaczamy interfejs zewnętrzny (WAN). Następnie z menu Plik wybieramy Właściwości. We właściwościach połączenia przechodzimy do karty Zaawansowane i umieszczamy znacznik w polu Zezwalaj innym użytkownikom sieci na łączenie się poprzez połączenie internetowe tego komputera. Po naciśnięciu OK udostępnianie jest włączone. Warto pamiętać, że do modyfikacji ustawień Windows Server 2003 należy mieć odpowiednie uprawnienia i wykonanie powyższych czynności po zalogowaniu na konto należące do grupy Użytkownicy lub Użytkownicy domeny nie będzie możliwe.

ICS jest przeznaczony do małych firm lub biur. Po włączeniu usługi udostępniania system przypisuje karcie LAN adres 192.168.0.1 z maską 255.255.255.0. Dodatkowo Windows Server 2003 uruchamia automatycznie uproszczoną wersję serwera DHCP, który odpowiada za dostarczenie parametrów adresowania IP klientom sieci. W takim wypadku komputery pracujące w sieci powinny mieć ustawione automatyczne uzyskiwanie adresu IP. Stacjom roboczym przydzielane są adresy z zakresu od 192.168.0.2 do 192.168.0.254. Jeśli którakolwiek ze stacji będzie miała nadany adres statyczny, nie połączy się z Internetem. Gdy ustawimy ręcznie adres z tego samego zakresu, którym posługuje się serwer, mogą wystąpić konflikty adresów IP.

Chociaż ICS ma do minimum ograniczoną konfigurację, można zmienić pewne parametry do zmiany we właściwościach Udostępniania połączenia internetowego. Na karcie Zaawansowane umieszczony jest przycisk Ustawienia. Służy do określania usług dostępnych dla klientów łączących się z serwerem przez interfejs WAN. Domyślnie Windows Server 2003 nie pozwala na połączenia przychodzące od strony karty zewnętrznej. Po kliknięciu przycisku Ustawienia system wyświetla okno przeznaczone do zmiany parametrów domyślnych. Na liście usług dostępne są takie, opcje jak Serwer sieci Web, Serwer FTP czy Pulpit zdalny. Jeśli administrator chciałby zarządzać serwerem z zewnątrz, wystarczy zaznaczyć np. usługę Pulpit zdalny i gotowe. Gdy serwer oferuje usługi, których nie ma na liście, możemy skorzystać z przycisku Dodaj i skonfigurować parametry połączenia. Warto pamiętać, że ICS jest prościutką usługą, przeznaczoną raczej do serwerów grup roboczych. Do kontrolerów domeny lepiej użyć translacji adresów sieciowych (NAT). Dodatkowo nie należy zapominać o ochronie dostępu do serwera. Absolutne minimum to włączenie Zapory połączenia internetowego. Niemniej zalecane jest zastosowanie innego, bogatszego w możliwości firewalla.

Translacja adresów (NAT)

Usługa NAT opiera się na translacji adresów. Klienci sieci, którzy chcą komunikować się z Internetem, kierują pakiety do komputera z Windows Server 2003. Serwer mający interfejs publiczny i prywatny odbiera dane przez kartę LAN, następnie zmienia adres źródłowy pakietu na adres karty WAN i tak zmodyfikowaną informację wysyła do Internetu. Po nadejściu odpowiedzi odbywa się tłumaczenie odwrotne i dane trafiają do klienta sieci wewnętrznej.

Pierwszą czynnością związaną z instalacją usługi translacji adresów sieciowych jest dodanie odpowiedniej roli serwera w systemie Windows Server 2003. Rozpoczynamy od uruchomienia przystawki Zarządzanie tym serwerem. Następnie klikamy odnośnik Dodaj lub usuń rolę. Kreator konfigurowania serwera testuje parametry serwera i wyświetla okno z listą dostępnych ról. Po zaznaczeniu opcji Serwer dostępu zdalnego/sieci VPN naciskamy przycisk Dalej. Program instalatora informuje o konieczności uruchomienia kolejnego kreatora i po kliknięciu Dalej przechodzimy do Kreatora instalacji serwera routingu i zdalnego dostępu. W oknie powitalnym naciskamy Dalej i trafiamy do okna związanego z wyborem konfiguracji serwera. W celu włączenia translacji sieciowej

możemy wybrać jedną z trzech opcji: Translację adresów sieciowych (NAT), Dostęp prywatnej sieci wirtualnej (VPN) i translację adresów sieciowych (NAT) lub Konfigurację niestandardową. Po zaznaczeniu opcji związanej z translacją adresów klikamy Dalej. W oknie Połączenie internetowe NAT wskazujemy, która z kart sieciowych służy do komunikacji z Internetem. Jeśli do zestawiania połączenia serwer wykorzystuje modem, zaznaczenie opcji Utwórz nowy interfejs wybierania numeru na żądanie do Internetu umożliwia założenie interfejsu aktywowanego automatycznie podczas zestawiania połączenia przez klienta. Zaznaczenie pola wyboru Włącz zabezpieczenia na wybranym interfejsie poprzez ustawienie zapory podstawowej włącza firewall na karcie WAN. Po naciśnięciu Dalej kreator wyświetla ekran podsumowujący i kończy działanie.

Kliknięcie Zakończ może sprawić, że translacja adresów zacznie natychmiast funkcjonować. Wszystko zależy od tego, czy klienci dostaną adresy IP i czy będą potrafili rozpoznać nazwy internetowe. Odpowiedzialność standardowo spoczywa na usługach DHCP i DNS. DHCP może pomóc w konfigurowaniu zaawansowanych opcji dynamicznego adresowania w sieciach lokalnych. Chociaż nie jest niezbędna do translacji adresów, dodanie serwera DHCP znacznie ułatwia pracę administratora. W małych sieciach usługę DNS odnajdziemy z pewnością na serwerze Active Directory. Jeżeli w opcjach DNS skonfigurujemy Usługę przesyłania dalej, rozwiązanie nazw będzie działać bez kłopotów. Gdy w sieci nie ma serwera DHCP lub DNS, zadania wykonywane przez te usługi weźmie na siebie NAT. Parametry translacji konfigurujemy w przystawce Routing i dostęp zdalny. Po uruchomieniu przystawki przechodzimy do folderu Routing protokołu IP i zaznaczamy Translator adresów sieciowych/zapora podstawowa. Następnie z menu Akcja wybieramy Właściwości. Na karcie Przypisywanie adresu zaznaczamy opcję Automatycznie przypisz adresy IP, używając programu przydzielania DHCP i wprowadzamy parametry adresowania. System samoczynnie sugeruje adresy do sieci 192.168.0.0 z maską 255.255.255.0. Korzystając z przycisku Wyklucz, możemy wprowadzić identyfikatory IP, które są już przypisane w sieci prywatnej. Pamiętajmy, że ustawienia karty Przypisywanie adresu powinny być wprowadzane jedynie wtedy, gdy w sieci nie ma serwera DHCP, a systemy klientów są skonfigurowane na automatyczne pobieranie adresu IP.

Pozostałe parametry usługi NAT ustawiamy we właściwościach interfejsów LAN i WAN umieszczonych w folderze Translator adresów sieciowych/zapora podstawowa. Po wybraniu Właściwości interfejsu LAN możemy określić statyczne filtry pakietów przychodzących i wychodzących. Opcja ta nadaje się doskonale do wykluczania niechcianego ruchu generowanego przez stacje sieciowe. Właściwości interfejsu WAN oferują więcej interesujących ustawień. Wyświetlone okno zawiera cztery karty: Translator adresów sieciowych/zapora podstawowa, Pula adresów, Usługi i porty, Protokół ICMP. Rozpocznijmy od Puli adresów. Karta ta jest wykorzystywana do konfiguracji zakresu publicznych adresów IP. Najczęściej realizacja połączenia z Internetem odbywa się przez jeden adres zewnętrzny. Jeśli usługodawca internetowy przydzielił firmie więcej adresów publicznych, na karcie Pula adresów wprowadzamy otrzymane adresy IP.

Karty Usługi i porty oraz Protokół ICMP zawierają ustawienia zapory internetowej konfigurowanej do usługi NAT. Karta Protokół ICMP określa typ żądań informacji o stanie i błędach, na które będzie odpowiadał serwer. Jeśli zaznaczymy parametr Przychodzące żądanie echa, komputery komunikujące się z Windows Server 2003 przez interfejs WAN będą mogły sprawdzić obecność systemu np. poleceniem ping. Na karcie Usługi i porty zaznaczone są te usługi, które mają być dostępne dla klientów internetowych. Zezwolenie na dostęp do serwera polega na zaznaczeniu jednej z wymienionych usług. Ważne jest to, że systemem oferującym FTP lub WWW nie musi być komputer z uruchomioną usługą NAT. Po wejściu we właściwości dowolnej opcji możemy wskazać adres prywatny serwera sieci lokalnej, np. 192.168.0.6. Jeśli w sieci lokalnej zostanie uruchomiona usługa lub aplikacja, której nie ma na liście, korzystając z przycisku Dodaj, możemy zdefiniować własne parametry komunikacji.

Na ostatniej karcie właściwości interfejsu zewnętrznego dostępne są filtry pakietów. Tak samo jak na karcie LAN, korzystając z przycisków Filtry przychodzące i Filtry wychodzące, określamy dodatkowe parametry zapory komunikacji sieciowej. Po naciśnięciu dowolnego z przycisków kliknięciem opcji Nowy określamy reguły filtrowania ruchu. Kryteria mogą być budowane przez wskazanie adresu IP sieci źródłowej i docelowej, typ protokołu oraz port źródłowy i docelowy. Po dodaniu filtru określamy akcję filtrowania. Możemy odrzucać lub przyjmować wszystkie pakiety oprócz wskazanych.

Jacek Ścisławski

Określenie serwer aplikacji do niedawna kojarzone było przede wszystkim z rozwiązaniami opartymi na platformie J2EE. Połączenie systemu Windows Server 2003 z serwerem Internet Information Services 6.0 oraz technologią .Net zaowocowało pojawieniem się alternatywnej, mocno konkurencyjnej platformy.

Internet Information Services 6.0 w stosunku do swoich poprzednich wersji jest wydaniem rewolucyjnym pod wieloma względami. Jako efekt inicjatywy budowy niezawodnych platform komputerowych, stanowi przy tym jeden z najbardziej wyraźnych dowodów na poważne traktowanie kwestii bezpieczeństwa. Aby osiągnąć zamierzone cele, cały kod źródłowy serwera IIS poddano wnikliwej analizie, a duża jego część została po prostu napisana od nowa.

Architektura IIS

Efektem jest nowoczesny, stabilny, wydajny i bezpieczny serwer aplikacji, który w dodatku jest łatwy do programowania dzięki wprowadzeniu ASP.NET. Aby zapewnić serwerowi możliwość długotrwałej bezawaryjnej pracy, zmieniono jego wewnętrzną

strukturę. Obecnie serwer oraz jego witryny działają w dwóch odseparowanych obszarach. Specjalny sterownik obsługujący protokół HTTP odbiera zgłoszenia od użytkowników zewnętrznych i kieruje je do odpowiednich kolejek, które z kolei przekazują je do odpowiednich procesów obsługujących konkretne witryny. Istotny z punktu widzenia bezpieczeństwa i stabilności jest fakt, że sterownik HTTP działa w trybie jądra, a procesy, wewnątrz których działają poszczególne witryny, uruchamiane są już w trybie użytkownika. Efekt jest taki, że źle działająca witryna nie może zakłócić pracy samego serwera, a więc nie wyrządzi żadnych poważniejszych szkód. Zamknięcie nieprawidłowo działającej witryny przypomina zamykanie aplikacji, która przestała reagować na polecenia użytkownika.

Izolacja witryn

Poszczególne serwisy nie tylko działają niezależnie od serwera IIS, ale także niezależnie od siebie. Służą do tego tzw. pule aplikacji. Każda związana jest z oddzielnym obszarem pamięci, który może być wykorzystywany tylko przez aplikacje uruchomione w ramach tej jednej puli. Wewnątrz danej puli działa tzw. Worker Process, widoczny w Menedżerze zadań jako w3wp.exe, a dopiero w nim działa konkretna aplikacja obsługująca witrynę. Domyślnie w jednej puli aplikacji uruchamiany jest jeden proces roboczy, który może jednak obsługiwać kilka witryn. Liczbę procesów roboczych w puli aplikacji można zwiększyć, ale traci się w ten sposób izolację obszarów pamięci. Lepiej utworzyć nową pulę aplikacji (z nowym procesem roboczym) i przypisać do niej witrynę.

Stała dostępność usług

Pracę serwera IIS stale nadzoruje specjalna usługa, która zarządza pulami aplikacji i procesami roboczymi. Do jej zadań należy śledzenie aktywności procesów roboczych, zamykanie procesów po przekroczeniu limitów (czasu działania, wykorzystanej pamięci, czasu bezczynności). Dzięki funkcjonowaniu wspomnianych wcześniej kolejek żądań możliwe jest zamknięcie wadliwie działającego procesu i w zamian otwarcie nowego albo, co ciekawsze, utworzenie dodatkowego procesu, który przejmie jego kolejkę. Dzięki temu stary proces nie jest już wykorzystywany przez użytkowników i można go wykorzystać do zlokalizowania błędu w działaniu serwisu. Wszystkie te operacje odbywają się automatycznie i bez wiedzy użytkowników, dla których witryna jest cały czas dostępna.

Bezpieczeństwo systemu

Samo uruchomienie usługi WWW na serwerze, który pełni równocześnie inne zadania w sieci lokalnej, jest pewnym zagrożeniem dla jego bezpieczeństwa i m.in. dlatego usługi IIS nie są domyślnie instalowane w systemie Windows Server 2003. Z kolei po ich zainstalowaniu serwer IIS działa w trybie podstawowym, w którym serwer może dostarczać klientom tylko statyczną zawartość. Wszystkie dynamiczne rozszerzenia są domyślnie zablokowane, a procesy robocze działają z ograniczonymi prawami konta USŁUGA SIECIOWA. Jednak nawet jeśli uruchomimy możliwość dostarczania dynamicznej zawartości poprzez aplikacje ASP.NET, serwer i tak będzie znacznie bezpieczniejszy niż w przypadku ASP, ponieważ platforma .NET zawiera wiele wbudowanych mechanizmów kontroli kodu, które mogą zablokować niedozwolone operacje.

Instalacja IIS

Najłatwiejszym sposobem instalacji IIS jest wykorzystanie Kreatora konfigurowania serwera. Wybieramy Start | Zarządzanie tym serwerem | Dodaj lub usuń rolę | Dalej, na liście możliwych ról zaznaczamy Serwer aplikacji (IIS, ASP.NET) i klikamy Dalej. W następnym oknie Opcje serwera aplikacji mamy możliwość zainstalowania dodatkowych składników serwera IIS, tj. Rozszerzeń serwera FrontPage (dość niefortunne tłumaczenie, w rzeczywistości są to rozszerzenia serwera WWW, które umożliwiają m.in. publikowanie zawartości w witrynie bezpośrednio z programu FrontPage, bez potrzeby stosowania FTP)

oraz ASP.NET. Drugi składnik zaznaczymy prawie zawsze, ponieważ ASP.NET - następca Active Server Pages - znacznie upraszcza tworzenie dynamicznych serwisów i jest wykorzystywany np. przez Windows SharePoint Services. Kliknięcie Dalej rozpocznie kopiowanie plików, podczas którego system upomni się o płytę z Windows Server 2003.

Podstawą serwera aplikacji jest serwer WWW, ale IIS 6.0 ma większe możliwości. Może bowiem utrzymywać witryny FTP i pełnić funkcję serwera pocztowego. Funkcje te nie są jednak instalowane podczas dodawania roli serwera aplikacji. Aby je dodać ręcznie, wybieramy Start | Panel sterowania | Dodaj lub usuń programy | Dodaj/Usuń składniki systemu Windows. Następnie przechodzimy kolejno do szczegółów składnika Serwer aplikacji i Internetowe Usługi Informacyjne (IIS) i zaznaczamy pozycje: Usługa FTP (File Transfer Protocol) oraz Usługa SMTP. Dwukrotne kliknięcie OK, a następnie Dalej, rozpocznie instalację dodatkowych komponentów i konfigurację serwera. Po zakończeniu tego procesu obie usługi są praktycznie gotowe do działania. Pozostaje jedynie ich bezpieczna konfiguracja za pomocą wielu kart właściwości w menedżerze serwera IIS.

Menedżer IIS

Do zarządzania serwerem IIS służy Menedżer internetowych usług informacyjnych (IIS), dostępny jako folder w przystawce Serwer aplikacji, uruchamianej skrótem Zarządzaj tym serwerem aplikacji narzędzia Zarządzanie tym serwerem lub jako samodzielna konsola, uruchamiana poprzez Narzędzia administracyjne. Główny folder z nazwą komputera zawiera w domyślnej konfiguracji podfoldery Pule aplikacji, Witryny sieci Web oraz Rozszerzenia usługi sieci Web. Jeżeli instalując IIS za pomocą Dodaj lub usuń programy, zaznaczyliśmy usługi FTP i SMTP, znajdziemy tu również dodatkowe foldery Witryny FTP i Domyślny serwer wirtualny SMTP.

Aby założyć nową witrynę, zaznaczamy pozycję Witryny sieci Web i z menu Akcja wybieramy Nowy | Witryna sieci Web. Wpisujemy nazwę, np. Strona główna, i klikamy Dalej. Jako adres IP możemy zostawić (Wszystkie nieprzypisane). Domyślny numer portu dla usługi WWW to numer 80, przy czym na serwerze działa już Domyślna witryna sieci Web, która nasłuchuje zgłoszeń w tym samym porcie. W jaki sposób użytkownicy mają uzyskać dostęp do nowej witryny? Możemy wybrać niestandardowy numer portu, który klienci będą musieli wpisywać w przeglądarce zaraz za adresem strony, wybrać inny adres IP - np. gdy mamy w serwerze kilka kart sieciowych, lub przypisać do adresu IP dodatkową nazwę domenową w serwerze DNS i wpisać ją w polu Nagłówek hosta dla tej witryny sieci Web. Wtedy w zależności od wpisanego przez klienta adresu (nazwy) serwera, IIS uruchomi odpowiednią witrynę. Jeżeli jednak adres serwera podamy w postaci numeru IP, załaduje się ta witryna, której nagłówek hosta nie został zdefiniowany. Standardowo jest to Domyślna witryna sieci Web. W kolejnych oknach wskazujemy ścieżkę do katalogu głównego witryny i klikając Dalej, zatwierdzamy domyślnie zaznaczoną opcję Zezwalaj na anonimowy dostęp do witryny sieci Web. Na początek wystarczą też domyślne uprawnienia: Odczyt i Uruchamianie skryptów. Naciśnięcie Dalej kończy pracę kreatora.

Aby przypisać witrynę do konkretnej puli aplikacji, zaznaczamy nazwę witryny w folderze Witryny sieci Web i wybieramy z menu Akcja opcję Właściwości. Na karcie Katalog macierzysty definiujemy Nazwę aplikacji, ustalamy Uprawnienia wykonywania i wybieramy Pulę aplikacji. Aby umieścić witrynę w nowej puli, musimy ją wcześniej utworzyć. W tym celu wystarczy wcześniej przejść do folderu Pule aplikacji, z menu Akcja wybrać Nowy | Pula aplikacji i zaakceptować domyślne ustawienia albo skopiować je z innej puli aplikacji.

Szyfrowanie i certyfikaty

Na wysoką jakość usług dostarczanych użytkownikom serwisu duży wpływ ma zarówno zabezpieczenie samego serwera, jak i zapewnienie poufności przesyłanych informacji. W

realizacji drugiego zadania przydatna okaże się karta Zabezpieczenia katalogów. Oprócz włączenia kontroli dostępu i wybrania metody uwierzytelniania (przy dostępie anonimowym użytkownicy korzystają z konta IUSR_NAZWAKOMPUTERA) oraz ograniczenia zakresu adresów IP komputerów, z których można nawiązywać połączenia z serwerem, na karcie Zabezpieczenia katalogów możemy skonfigurować bezpieczne połączenia SSL i nadać certyfikat naszemu serwerowi. Aby umożliwić połączenia HTTPS, klikamy Certyfikat serwera | Dalej | Utwórz nowy certyfikat | Przygotuj żądanie teraz, ale wyślij później. Po wpisaniu danych identyfikujących naszą firmę oraz nazwy domenowej witryny zapisujemy zgłoszenie nadania certyfikatu w pliku. Po uzyskaniu certyfikatu z urzędu certyfikacji (funkcję urzędu certyfikacji może pełnić Windows Server 2003 - odpowiednie narzędzia dostępne Narzędziach administracyjnych po zainstalowaniu składnika Usługi certyfikacji w Dodaj/Usuń składniki systemu Windows) na karcie Zabezpieczenia katalogów ponownie wybieramy Certyfikat serwera, a następnie Przetwarzaj oczekujące żądanie i zainstaluj certyfikat. Wskazujemy plik z certyfikatem, zatwierdzamy domyślny numer portu dla transmisji SSL (443), klikamy Dalej i kończymy pracę kreatora. Od tej pory z witryną można się łączyć również za pomocą bezpiecznego protokołu, poprzedzając adres internetowy witryny ciągiem znaków https://. Jeżeli chcemy wymusić stosowanie bezpiecznych połączeń i zablokować zwykłe połączenia http://, na karcie Zabezpieczenia katalogów klikamy Edytuj, a następnie zaznaczamy Wymagaj bezpiecznego kanału (SSL) i Wymagaj szyfrowania 128-bitowego.

System operacyjny Windows Server 2003 został wyposażony w znany już z Windows XP mechanizm zabezpieczający przed nieuprawnionym wykorzystywaniem, czego efektem jest konieczność aktywacji zainstalowanego produktu. Klucz aktywacyjny trzeba jednak podać już na etapie instalacji systemu. Pokazujemy, w jaki sposób uzyskać klucz aktywacyjny ze strony firmy Microsoft.

Klucz aktywacyjny wymagany jest do zainstalowania systemu Windows Server 2003 oraz jego pomyślnej aktywacji, którą należy przeprowadzić w ciągu 14 dni od daty zainstalowania i która umożliwi działanie systemu przez 180 dni. Formularz rejestracyjny znajduje się na stronie https://microsoft.order-5.com/windowsserver2003evaldl/ . Połączenie ze stroną jest szyfrowane.

Pierwszy krok to wybór wersji systemu. Wybieramy więc Microsoft® Windows Server 2003, Enterprise Edition (32-bit). Na kolejnym ekranie zatwierdzamy liczbę kopii (1) i dodajemy do koszyka, klikając Add to Basket. Następnie pojawi się podsumowanie zakupów, które powinno zawierać jedną pozycję MicrosoftR Windows Server 2003, Enterprise Edition (32-bit). Klikamy check-out i na kolejnej stronie wypełniamy formularz rejestracyjny. Po wypełnieniu formularza warto się jeszcze raz upewnić, czy wpisany adres poczty elektronicznej jest prawidłowy, bo kliknięcie Submit spowoduje wysłanie listu potwierdzającego rejestrację właśnie pod ten adres. W treści wiadomości znajdziemy odnośnik do strony internetowej, z której odczytamy klucz aktywacyjny (Product Key), który wpiszemy podczas instalacji systemu i który posłuży do aktywacji naszej kopii serwera na jednym komputerze. Klucz aktywacyjny dostaniemy później także pocztą elektroniczną.

Problemy z dostępem do formularza rejestracyjnego

Przedstawiamy całą drogę, jaką trzeba przebyć od strony głównej firmy Microsoft do formularza rejestracyjnego, gdyby z jakichś przyczyn nie dawało się wejść bezpośrednio na stronę https://microsoft.order-5.com/windowsserver2003evaldl/ . Po wejściu na stronę http://www.microsoft.com należy z grupy Product Families po lewej stronie wybrać Servers (można też wybrać opcję Servers z rozwijanego menu górnego All Products), a następnie po prawej stronie w grupie odnośników Products by Name wskazać Windows Server. Na kolejnym ekranie w grupie Quick Links po prawej stronie

należy wybrać Evaluation Kit (albo Get the Evaluation Kit na środku strony). Aktualna strona powinna być zatytułowana Windows Server 2003 Evaluation Kit, a po prawej stronie powinna być dostępna opcja Register to Download the Windows Server 2003 Evaluation Kit. W tym momencie istotne jest, aby wybrać rejestrację w celu ściągnięcia programu z sieci (Download File), a nie w celu zamówienia płyty CD (Order the CD). Po zatwierdzeniu informacji o przekierowaniu pod nowy adres przy użyciu szyfrowanego połączenia znajdziemy się na stronie, do której bezpośrednio prowadzi podany wcześniej odnośnik.

Usługi katalogowe - zasada działania

Coraz więcej przedsiębiorstw buduje globalne, zdecentralizowane sieci firmowe. Często korzysta się przy tym z aplikacji rozproszonych. Mogą one pracować na komputerach w lokalnej sieci, w intranecie lub w Internecie.

Wiele informacji dostępnych w sieci można wymieniać między poszczególnymi aplikacjami i użytkownikami. Są też jednak dane, które powinny być chronione przed nieautoryzowanym dostępem i modyfikacjami. Dlatego właśnie tak ważne jest ekonomiczne, nieskomplikowane, a zarazem skuteczne administrowanie informacjami o użytkownikach i innych zasobach sieci. Warunkiem funkcjonowania tak zarządzanej sieci jest integracja usług katalogowych. Dzięki niej informacje zorganizowane są w ujednolicony sposób. Dodatkowo użytkownicy uzyskują dostęp do wszystkich zasobów sieci za pomocą jednego loginu. Ta procedura nosi nazwę pojedynczego logowania (single sign-on).

W dalszym ciągu wyjaśnimy, czym są usługi katalogowe oraz przedstawimy zarysy koncepcji i architektury usług katalogowych X.500, LDAP, Novell eDirectory oraz Microsoft Active Directory.

Katalogi i usługi katalogowe

Katalog to lista informacji o obiektach, zapisana w uporządkowanej formie. Najlepszy przykład to książka telefoniczna - nazwiska są uporządkowane alfabetycznie, adres i numer telefonu to szczegółowe informacje o obiektach.

W sferze komputerów katalog to specjalny rodzaj bazy danych, która zawiera informacje o obiektach posortowane według typów. Na przykład zapisane są dane o drukarce wraz z dodatkowymi informacjami, np. jej lokalizacja i wydajność w stronach na minutę.

Katalogi umożliwiają użytkownikom i aplikacjom wyszukanie zasobów o określonych właściwościach. Można na przykład przeszukiwać spis użytkowników według adresów poczty elektronicznej lub numerów faksu. W innym katalogu można wyszukiwać informacje o najbliższej dostępnej drukarce.

Jeżeli nazwa obiektu jest znana, na przykład nazwisko osoby lub nazwa drukarki, można łatwo znaleźć przynależne do obiektu właściwości, jak numer telefonu czy wydajność druku. Jeżeli natomiast nazwa jest nieznana, poszukujemy w katalogu obiektu, który spełnia określone warunki. Można to porównać do poszukiwania określonego rzemieślnika w branżowej książce telefonicznej.

Katalog sam w sobie jest jedynie zbiorem informacji, które muszą być dostępne. Dostęp może polegać na wyszukiwaniu, modyfikacji lub dodawaniu informacji. Interfejs programistyczny (Application Programming Interface - API), który umożliwia ten dostęp, to właśnie usługa katalogowa.

Przykładowy katalog

Katalog to w rozumieniu normy ISO 9594-1 zbiór danych o strukturze drzewa. Ma cechę szczególną: zawartość jest w dużej mierze statyczna, a na każdym poziomie może być dowolnie wiele wpisów. Każdemu wpisowi można z kolei przyporządkować dowolnie wiele atrybutów.

W tym przykładzie mamy siedem wpisów do katalogu na trzech poziomach wraz z ich atrybutami.

Liśćmi drzewa są pracownicy, ponad nimi są odpowiednie działy firmy, w których pracują. Korzeniem drzewa jest sama firma.

Klasyk X.500

X.500 to usługa katalogowa zalecana przez międzynarodową unię telekomunikacyjną (International Telecommunication Union, ITU, http://www.itu.int) w ramach serii X (Data Networks and Open System Communications).

Zalecenie ukazało się po raz pierwszy w roku 1988. Jednym z głównych zadań ITU jest proponowanie międzynarodowych standardów globalnej komunikacji.

Zalecenie w sprawie X.500 składa się z dziesięciu dokumentów. Wszystkie zostały też przyjęte jako standard ISO 9594-1...10 przez międzynarodową organizację standaryzacyjną (International Organization for Standardization, ISO, http://www.iso.org).

Wielu użytkowników może znać zalecenia ITU dotyczące typoszeregu V (Data Communication over the Telephone Network). Dotyczą one kompatybilnych technicznie połączeń modemowych. Znane standardy tego typoszeregu to choćby V.90 czy V.32bs.

Budowa katalogu X.500

Ideą przewodnią X.500 jest globalny, rozproszony katalog, z dostępem z dowolnego miejsca. Ma on strukturę drzewa, u podstawy którego znajduje się niemający nazwy obiekt główny (root). Udostępniane przez katalog dane noszą nazwę Directory Information Base (DIB), zaś drzewo - Directory Information Tree (DIT).

Dla poszczególnych wpisów zdefiniowano klasy obiektów, przy czym każdy wpis musi należeć przynajmniej do jednej z klas. W każdej klasie obiektów musi być przynajmniej jeden atrybut. W ten sposób każdy wpis w katalogu X.500 należy do jednej lub wielu klas obiektów oraz zawiera jedną lub wiele wartości poszczególnych typów atrybutów. Szczególnym rodzajem wpisów są aliasy, umożliwiające umieszczenie takiego samego wpisu w różnych miejscach drzewa. Dzięki takiemu rozwiązaniu zmiana dokonana w jednym wpisie powoduje odpowiednie zmiany we wszystkich aliasach.

Przykładowe drzewo katalogu X.500

Nasz przykład przedstawia wycinek z katalogu X.500. Każdy wpis należy do jednej klasy obiektów. Klasa podaje wartość typu atrybutu głównego, primary distinguished value. Wpis "C=PL" należy więc do klasy obiektów "Country". Typem atrybutu głównego jest zatem "C" jak Country, zaś wartością jest "PL" jak Polska.

Wpis "CN=Stefan Malinowski" przynależy natomiast do klasy obiektów "Osoba", a "Stefan Malinowski" jest wartością typu atrybutu głównego "Common Name" (CN).

Wpisy w drzewie katalogu muszą być jednoznaczne, dlatego każdy wpis musi mieć nazwę (distinguished name - DN). Powstaje ona w wyniku odwzorowania wszystkich obiektów w drzewie katalogu, od danego wpisu aż do korzenia. W tym celu wykorzystuje się wartość primary distinguished value głównej klasy obiektów (distinguished value). W naszym przykładzie byłoby to dla pana Stefana Malinowskiego: CN=Stefan Malinowski, OU=Dyrektor ds. handlowych, O=Zarząd, C=PL.

Nie jest jednoznacznie określone, jaką postać ma mieć DN. W tym przypadku postać CN jest zgodna ze wzorem ustalonym w RFC 1779.

Obok DN jest jeszcze relative distinguished name (RDN). To część nazwy, która sama jest atrybutem obiektu. W poprzednim przykładzie RDN obiektu brzmi: CN=Stefan Malinowski. RDN obiektu nadrzędnego brzmi: OU=Dyrektor ds. handlowych.

X.500 - dostęp użytkownika

X.500 oferuje dla usług katalogowych cały szereg operacji. Umożliwiają one dostęp do katalogu za pośrednictwem directory user agent (DUA).

Jak już wspomnieliśmy, dostęp do katalogu powinien być możliwy z każdego miejsca. Zasada ta nie musi jednak dotyczyć wszystkich danych - poufne dane muszą być chronione. Można zatem określić, do których wpisów i atrybutów mają dostęp poszczególne obiekty. Możliwe jest "proste" uwierzytelnianie za pomocą haseł lub "mocne" - za pomocą certyfikatów elektronicznych. W ten sposób część drzewa katalogu może być dostępna tylko dla określonych osób.

X.500 - praca w sieci

X.500 definiuje katalog rozproszony, dlatego dane nie muszą być przechowywane centralnie. Jest sieć serwerów, z których każdy zarządza tylko częścią drzewa. W razie potrzeby kontaktują się ze sobą, na przykład w celu przesłania do innego serwera zapytania nieodnoszącego się do własnego zasobu danych. Poszczególne serwery określa się mianem directory system agents (DSA).

Replikacja

Aby przyśpieszyć odczyt katalogu X.500, warto w niektórych przypadkach udostępnić część struktury drzewa na kilku serwerach. Dodatkowo wzrasta poziom odporności na awarie odpowiedniej części drzewa (dane są replikowane). Jest jeden serwer master, na którym tworzy się i utrzymuje zasoby danych, oraz jeden lub kilka serwerów slave, na których znajdują się kopie zasobów danych. Serwery slave kontaktują się w określonych odstępach czasu z serwerem master i aktualizują swoje zasoby danych.

X.500 - protokoły

Specyfikacja X.500 definiuje różne protokoły, które udostępniają usługi katalogowe. Opierają się one na siedmiu warstwach modelu warstw OSI (patrz tabela obok).

Implementacje X.500

Większość dostępnych dzisiaj usług katalogowych opiera się na specyfikacji X.500. Dotyczy to również eDirectory Novella i Active Directory Microsoftu, które opiszemy bliżej w dalszej części artykułu. LDAP opracowano z myślą o komunikacji klientów z serwerami X.500.

DirX Siemensa jest również kompatybilny z X.500. Ten ostatni nadaje się między innymi do zarządzania numerami telefonów i faksów, adresami e-mail, danymi personalnymi, adresami komputerów, profilami użytkowników i wieloma innymi zasobami sieciowymi. Obecnie dostępny jest w wersji do Windows NT/2000 i wszystkich popularnych wariantów UNIX-a. Dostęp do DirX możliwy jest za pomocą przeglądarki internetowej poprzez bramę internetową DirXweb, za pomocą przeglądarki WAP przez DirXwap lub za pomocą klienta Siemensa lub innego, dowolnego klienta LDAP.

LDAP (Lightweight Directory Access Protocol)

Początkowo X.500 nie cieszył się zbyt wielkim uznaniem m.in. dlatego, że specyfikacja wymaga kompletnej implementacji modelu warstw OSI. Eksploatowane protokoły

komunikacyjne, jak TCP/IP, nie są obsługiwane. Jest to szczególnie niekorzystne w przypadku komunikacji między DUA a DSA, bo również po stronie klientów konieczne są dodatkowe nakłady na wdrożenie. Ponieważ jednak było duże zainteresowanie usługą katalogową w rodzaju X.500, opracowano w roku 1993 Lightweight Directory Access Protocol, LDAP. Pierwsza jego wersja została zdefiniowana w RFC 1487 ("X.500 Lightweight Directory Access Protocol") i była uproszczoną wersją Directory Access Protocol (DAP) z X.500.

Później opracowano RFC 1777. W tej chwili jest już wersja 3 LDAP, zdefiniowana w RFC 2251, "Lightweight Directory Access Protocol (v3)". Specyfikacja obejmuje opis kompletnego protokołu, który umożliwia klientom opartym na TCP/IP dostęp do katalogów X.500 za pośrednictwem serwerów LDAP. Lightweight Directory Access Protocol, wprawdzie zdefiniowany w uznawanych w skali międzynarodowej RFC, nie jest jednak oficjalnym standardem. Można jednak powiedzieć, że LDAP jest standardem de facto.

LDAP - protokół czy usługa katalogowa?

Czym jest LDAP - protokołem czy usługą katalogową? Formalnie rzecz biorąc, LDAP definiuje protokół komunikacyjny. Opisany jest sposób przesyłu i format wiadomości, który klient musi zastosować w celu uzyskania dostępu do usługi katalogowej zgodnej z X.500. Tak więc protokół nie specyfikuje właściwej usługi katalogowej, lecz jedynie sposób dostępu do niej.

Klient LDAP uzyskuje dostęp do usługi katalogowej, wywołując API LDAP. Dla serwera X.500 te wiadomości klienta są niezrozumiałe. Klient LDAP i serwer X.500 używają różnych protokołów komunikacyjnych - klient korzysta z TCP/IP, serwer opiera się na stosie protokołów OSI. Dlatego też klient komunikuje się z tak zwaną bramą LDAP, która przekazuje zapytania do serwera X.500, a sama jest z kolei klientem dla serwera X.500. Serwer LDAP musi więc mieć zaimplementowany protokół TCP/IP oraz stos protokołów OSI.

Samoistny serwer LDAP

Wraz z popularyzacją LDAP opracowano usługi katalogowe, z których można korzystać bezpośrednio za pomocą klienta LDAP. Sprawiło to, że serwer X.500 stał się w zasadzie zbędny. Tak więc serwer LDAP może korzystać z katalogu bezpośrednio, zamiast być jedynie bramą.

Serwer LDAP, który może pracować bezpośrednio z katalogami, określa się mianem samoistnego serwera LDAP. "Samoistność" serwera polega na jego niezależności od serwera X.500. Z punktu widzenia klienta każdy serwer, który ma zaimplementowany protokół LDAP, jest serwerem usług katalogowych LDAP, niezależnie od tego, czy jest serwerem "samoistnym", czy służy tylko jako brama. Tak wykorzystywane katalogi określa się mianem katalogów LDAP.

Jednym z najbardziej znanych samoistnych serwerów LDAP jest slajd, implementacja z otwartym dostępem do kodu źródłowego autorstwa OpenLDAP (http://www.openldap.org).

Architektura LDAP

Jak już wspomniano, Lightweight Directory Access Protocol opiera się na modelu klient-serwer. Z upływem lat uzyskał mocną pozycję. Sukces LDAP nie bierze się z przypadku. W stosunku do X.500 czy Directory Access Protocol (DAP) oferuje następujące korzyści:
Korzysta z protokołu TCP/IP, a nie ze stosu protokołów OSI. TCP/IP oszczędniej korzysta z zasobów i jest dostępny na niemal wszystkich komputerach.

Jest prostszy, a zatem jego implementacja jest łatwiejsza.
Wykorzystuje dla danych ciągi zamiast składni o skomplikowanej strukturze, jak ASN.1 (Abstract Syntax Notation One), stosowanej w X.500.LDAP definiuje zawartość wiadomości między klientem a serwerem. Wiadomości specyfikują, jakie operacje chce wykonać klient, jak choćby Search czy Modify, a także stosowną odpowiedź serwera. Dodatkowo jest też dokładnie określone, w jaki sposób mają być przesłane w wiadomości właściwe dane katalogowe. Ponieważ LDAP opiera się na TCP/IP, a więc protokole zorientowanym na połączenia, przeprowadzane są też stosowne operacje związane z nawiązaniem i zakończeniem połączenia. Więcej informacji o TCP/IP można znaleźć w artykule "Tak działa TCP/IP i IPv6".

Novell eDirectory

Novell Directory Service (NDS) jest usługą katalogową opartą na X.500, służącą do zarządzania użytkownikami, prawami dostępu i innymi zasobami sieciowymi. NDS 8, opublikowany po raz pierwszy z Netware 5, a jakiś czas temu przemianowany ze względów strategiczno-marketingowych na eDirectory, oferuje, zdaniem producenta, znacznie większą funkcjonalność niż wszystkie poprzednie wersje.

W ramach swojej strategii "One Net" Novell (http://www.novell.pl) udostępnia serwer usług katalogowych do wszystkich ważniejszych platform: Netware od wersji 5, Windows NT/2000, Linux i Solaris.

eDirectory upraszcza zarządzanie użytkownikami i zasobami w sieciach pracujących pod kontrolą systemów Windows NT/2000, Netware oraz UNIX/Linux. Usługa obsługuje eksploatowane standardy, jak LDAP, DNS, LDIF (Lightweight Data Interchange Format), XML, XSL, XSLT, ADSI (Active Directory Service Interface, niestandardowy API Microsoftu), ODBC oraz JDBC. Architektura eDirectory Novella opiera się na dwóch głównych komponentach.

Podstawowe komponenty serwera to Directory Service Agents (DSAs). Przechowują one informacje o katalogu, replikacjach oraz same dane. Aplikacje i usługi odwołują się do DSAs za pomocą standardowych protokołów, jak choćby LDAP, lub też za pośrednictwem Novell Directory Access Protocol (NDAP), niestandardowego protokołu dostępu do usług katalogowych autorstwa Novella.

Directory Clients to komponenty oprogramowania klienckiego Novella. Umożliwiają dostęp do eDirectory również innym produktom Novella, jak choćby ZENworks.

Architektura eDirectory

eDirectory opiera się na trzech "poziomach", za pomocą których można opisać architekturę usługi katalogowej: Logical Plane, Physical Plane i Schema Plane. Każdy z tych poziomów pokrywa pewną część całości usług katalogowych.

Physical Plane opisuje fizyczną budowę i organizację oraz sposób replikacji w bazie danych usług katalogowych. Drzewo eDirectory można utworzyć jako jedno wielkie drzewo częściowe na jednym serwerze lub w postaci wielu mniejszych drzew na wielu serwerach. Poszczególne drzewa częściowe określa się mianem partycji. Każde z nich może mieć jedną lub wiele kopii, zwanych replicas.

Logical Plane jest tym, co widzi administrator w trakcie zarządzania eDirectory za pomocą przewidzianych do tego narzędzi, wśród których są między innymi ConsoleOne oraz NWAdmin. Niezależnie od sposobu zapisu usługi katalogowej, zarządza się nią zawsze jako jednym, logicznym katalogiem.

Schema Plane opisuje między innymi, jakiego rodzaju obiekty mogą się znajdować w eDirectory, a także rodzaj atrybutów i sposób ich replikacji. Dodatkowo określona jest tu wielkość i rodzaj danych.

Obiekty eDirectory

Usługa katalogowa Novella może zarządzać wieloma obiektami, które reprezentują urządzenia i zasoby w sieci. Są to na przykład użytkownicy, grupy, drukarki, bazy danych, aplikacje i serwery plików. Poprzez rozbudowę schematu katalogu można dodawać dowolnie wiele nowych obiektów, takich jak serwery faksowe czy routery.

Obiekty w eDirectory można podzielić na dwie kategorie.

Leaf objects, obiekty typu liść - reprezentują użytkowników i zasoby sieciowe w rodzaju serwerów, drukarek i routerów. Obiekt typu liść nie może zawierać innych obiektów ani być jedynym obiektem danej partycji. Container objects, obiekty kontenerowe - mogą zwierać inne obiekty, zarówno typu liść, jak i inne obiekty kontenerowe. Dodanie obiektu kontenerowego do niego samego określa hierarchię i upraszcza dostęp. Obiekty kontenerowe są najmniejszą jednostką partycji i replikacji.

Microsoft Active Directory

Wraz z Windows 2000 Microsoft po raz pierwszy wprowadził na rynek usługę katalogową zgodną z X.500 - Active Directory. Umożliwia ona replikację i wyszukiwanie zgodnie ze standardami internetowymi LDAP, DNS i DDNS (Dynamic DNS). Jednak Active Directory jest dostępna jedynie do Windows.

Oto cechy usługi katalogowej Microsoftu:

Centralna administracja. Katalog jest zbudowany hierarchicznie, zgodnie ze specyfikacją X.500. Wszystkie stosunki zaufania są przechodnie ze względu na stosowany protokół bezpieczeństwa Kerberos. Zmniejsza to liczbę stosunków zaufania pomiędzy domenami. Stosunek przechodni oznacza, że gdy domena A ufa domenie B i domena C ufa domenie B, wówczas domena A ufa również domenie C.

Wspólne zasady i reguły. Schemat Active Directory jest rozszerzalny i daje możliwość definiowania nowych obiektów i właściwości.

Kontrola i definicja bezpieczeństwa. Dostęp do obiektów w katalogu kontrolowany jest przez Access Control Lists (ACLs). Lista dozwolonych odwołań replikowana jest w skali całej hierarchii, aż do poziomu obiektu.

Rozszerzone możliwości zapytań. Dzięki Global Catalog Server katalog Active Directory oferuje poszerzone możliwości formułowania zapytań i rozbudowany mechanizm zapytań sieciowych. Global Catalog Server można porównać do indeksu; obsługuje zapytania dotyczące każdego obiektu w katalogu.

Komponenty Active Directory

Budowa Active Directory jest porównywalna z koncepcją DNS. Przestrzeń nazw jest nazwą lub grupą nazw zdefiniowanych według pewnej konwencji. Internet posługuje się hierarchiczną przestrzenią adresową, która dzieli nazwy na domeny wysokiego poziomu, na przykład .com lub .org. Active Directory stosuje ten sam model hierarchiczny do budowy sieci.

Podczas instalacji Active Directory tworzy hierarchię, w której każda domena, każda jednostka organizacyjna i każdy zasób otrzymuje jednoznaczną nazwę w przestrzeni

nazw. Każdy obiekt w Active Directory jest naznaczony unikatową nazwą, zagnieżdżoną w hierarchicznej strukturze katalogu. Podobnie jak w eDirectory Novella, można integrować inne usługi katalogowe z użyciem mechanizmu LDAP.

Elementy logiczne Active Directory

W Active Directory są trzy różne elementy logiczne.

Obiekty. Są to składniki mające wiele atrybutów. Przykładowe obiekty to użytkownicy lub drukarki. Obiekt może być również kontenerem dla innych obiektów.

Atrybuty obiektu. Wszystkie obiekty w katalogu mają atrybuty lub właściwości. W Microsoft Active Directory oba pojęcia używane są zamiennie. Atrybut to pewna ilość informacji. Obiekty znajdujące się w tym samym kontenerze mają te same atrybuty.

Klasy obiektów. Active Directory grupuje obiekty według ich atrybutów. Wszystkie obiekty są kategoryzowane właśnie w ten sposób, na przykład jako użytkownicy lub drukarki. Tego rodzaju grupowanie logiczne odpowiada za organizację zasobów w katalogu.

Komponenty strukturalne

Oprócz obiektów typu liść w Active Directory są też komponenty strukturalne. Pomagają one w budowie hierarchii katalogu. Zaliczają się do nich kontenery, czyli pojemniki na inne obiekty w katalogu. Rozróżnia się dwie różne kategorie kontenerów.

Domeny. Stanowią granicę bezpieczeństwa w pojedynczej sieci komputerowej. Active Directory składa się z jednej lub wielu domen. W samodzielnej stacji roboczej domeną jest sam komputer. Domena może być czymś więcej, niż tylko fizyczną lokalizacją - każda dysponuje własnymi wytycznymi co do bezpieczeństwa w kontaktach z innymi domenami. Jeżeli kilka domen jest połączonych stosunkami zaufania i wykorzystują wspólną konfigurację, mówimy o strukturze domen.

Jednostki organizacyjne. Stanowią kolejny podział struktury katalogu. Możliwe są dowolne hierarchie w ramach jednej domeny.

Komponenty relacyjne Active Directory

Kolejne ważne jednostki podziału struktury określają relacje między domenami. Należą do nich:

Drzewo. Wiele przedsiębiorstw utrzymuje kilka domen, choć nie jest to niezbędne z technicznego punktu widzenia. Zastosowanie wielu domen tworzy hierarchię, która ma współzależną przestrzeń nazw i określana jest mianem drzewa. Drzewo tworzy logiczną strukturę wysokiego poziomu, w której domeny są wzajemnie relacyjnie powiązane. W obrębie drzewa domeny są wzajemnie powiązane stosunkami zaufania.

Las. Obecnie często jedne przedsiębiorstwa są przejmowane przez inne. Microsoft opracował koncepcję "lasu", który umożliwia zachowanie struktur, którymi można nadal zarządzać. Rzecz polega na współistnieniu dwóch różnych przestrzeni nazw.

Global Katalog Server. Wspominaliśmy o nim już wcześniej. Powstaje w wyniku replikacji usługi katalogowej i zawiera kopie wszystkich obiektów drzewa. Można powiedzieć, że ten serwer jest indeksem całej sieci. Zapisuje kopię każdego obiektu w katalogu.

Podsumowanie

Oprócz przedstawionych powyżej najważniejszych usług katalogowych jest wiele innych. Ich ewentualny opis daleko wykracza poza ramy tego tekstu. eDirectory, Active Directory oraz LDAP opieraja się na X.500, wspólnej specyfikacji katalogów i usług katalogowych. LDAP można określić mianem "dodatku" lub najmniejszego wspólnego mianownika, ponieważ ten protokół komunikacyjny umożliwia dostęp do wszystkich usług.

Active Directory - do czego użyć

Active Directory to usługi katalogowe do Windows Server 2003. Katalog przechowuje informacje o obiektach dostępnych w sieci - czy są to udziały sieciowe, drukarki, komputery, czy też wyspecjalizowane serwery bazodanowe, czy inne oprogramowanie serwerowe.

Przy użyciu Active Directory można odwzorować strukturę przedsiębiorstwa (np. podział na jednostki organizacyjne, działy itp). Dzięki temu, że obiekty "należą" do określonego węzła drzewa (lub - lasu), można precyzyjnie definiować łańcuch uprawnienia lub delegować "prawa administracyjne".

Usprawnienia w usługach katalogowych w Windows Server 2003 obejmują chyba każdy aspekt działania Active Directory. Nowa usługa działa szybciej i nawet na analogicznym sprzęcie może obsłużyć więcej użytkowników. Katalog jest znacznie bardziej elastyczny w stosunku do tego, który był dostępny w Windows 2000 Server. Można niemal dowolnie zmieniać schemat katalogu (czyli strukturę określającą, w jaki sposób opisywane są obiekty umieszczane w drzewie AD). W ten sposób można na przykład dodatkowo opisać informacje o koncie użytkowników lub o zainstalowanych specjalistycznych drukarkach. Niewykorzystywane obiekty schematu mogą być np. ukrywane.

Warto dodać, że aby edytować schemat, należy zarejestrować specjalne biblioteki oraz utworzyć własną konsolę administracyjną (np. używając polecenia mmc /a); szczegóły opisane są w pomocy Windows Server 2003).

Mechanizmy replikacji mogą przesyłać tylko zmiany, nawet gdy zmodyfikowany został schemat katalogu (wykorzystywana jest technologia Inter-Site Topology Generator - ISTG), gdzie minimalizowana jest ilość przesyłanych informacji.

Logowanie do domeny Windows Server 2003 odbywa się znacznie szybciej. Klient może przechowywać w pamięci podręcznej informacje pozwalające zalogować się do domeny (które w Windows 2000 znajdują się w tzw. Global Catalog). Ułatwia to wykorzystanie Active Directory, gdy łącze pomiędzy zdalnym biurem a centralą nie jest pewne (nie trzeba w każdym oddziale instalować kopii GC).

W Windows Server 2003 można zainstalować specjalną konsolę do zarządzania polisami grupowymi (GPMC). Konsola pozwala przypisywać uprawnienia na dowolnym "węźle" drzewa. Instalacja nowej polisy sprowadza się do przeciągnięcia obiektu na dany węzeł. GPMC pozwala także na praktyczne przetestowanie działania polis - można wygenerować "wynikowy" zestaw uprawnień, a nawet przetestować, jakie operacje da się wykonać po nałożeniu określonych ograniczeń w różnych węzłach drzewa.

Dzięki Active Directory administrator ma potężne narzędzie pozwalające na wprowadzenie porządku i określonej, hierarchicznej struktury w sieci.

Równocześnie jest to bardzo interesująca struktura, pozwalająca zapisać informacje na potrzeby własnych aplikacji, rozwijanych wewnątrz przedsiębiorstwa (czy też wdrażanych w firmie). Jednak w niektórych scenariuszach wdrożeń instalacja pełnej infrastruktury katalogowej może być niepotrzebna. Firma może już mieć katalog Active Directory, a aplikacja wymaga na przykład tylko mechanizmu do przechowania tymczasowych danych. Jeżeli zostaną umieszczone w "dużym" katalogu, to będą podlegać replikacji itp., a nie zawsze jest to potrzebne.

Wreszcie czasami w małej firmie może w ogóle nie być takich informacji, które nie muszą być replikowane w całej strukturze Active Directory.

W Windows Server 2003 dostępny jest specjalny "tryb" działania Active Directory, pozwalający wydzielić fragment katalogu na potrzeby danej aplikacji. Taka partycja często bywa przydatna. Można określić, że np. nie będzie ona replikowana pomiędzy kolejnymi serwerami AD. W ten sposób każdy oddział, pracujący na własnych aplikacjach przechowujących dane w wydzielonej partycji AD nie będzie niepotrzebnie wysyłał informacji do innych serwerów.

Dostępna jest także specjalna wersja usług Active Directory - Active Directory Application Mode (ADAM). Tego typu katalog może być instalowany "obok" głównej instalacji AD; nawet w środowisku Windows XP. Na jednym serwerze może obok siebie działać kilka niezależnych instancji ADAM.

ADAM może być wykorzystane np. jako repozytorium informacji o użytkownikach w przypadku serwera WWW. Dzięki temu serwer byłby w ogóle "poza" główną instalacją AD (instalacja serwera WWW w ramach AD zawsze jest niepotrzebnym ryzykiem).

Warto dodać, że pakiet (do pobrania ze stron Microsoftu) zajmuje 16 MB.

Dla programisty do obsługi "dużego" Active Directory, jak i ADAM dostępne są dwa interfejsy programistyczne. ADSI jest specjalnym API opracowanym przez Microsoft do obsługi Active Directory. Równocześnie do operacji na katalogu można wykorzystywać zapytania zgodne z LDAP (uniwersalny schemat kwerend przeznaczony do odpytywania struktur katalogowych).

W Windows Server 2003 obsługiwane są wirtualne listy elementów. Klient, który chce odczytać duży zestaw obiektów, może utworzyć po stronie serwera specjalny tymczasowy obiekt - listę, po czym przeglądać kolejno informacje, ściągając je małymi partiami. Jest to rozszerzenie LDAP opracowane przez IETF. W LDAP w Windows Server 2003 można wykorzystać bezpieczną komunikację przy użyciu TLS (zgodnie z RFC 2830) oraz autoryzację typu diggest, jak to opisuje RFC 2829.

Interfejs ADSI bezproblemowo może być wykorzystywany z poziomu aplikacji pisanych w .NET. Dostępne są specjalne biblioteki, zatem z punktu widzenia programisty obsługa katalogu sprowadza się praktycznie do używania dwóch obiektów: opisującego encję AD oraz pośrednika w wyszukiwaniu informacji.

Więcej źródeł OLAP

Do BusinessObjects 5.0 zostanie dodana obsługa technologii zawartych w Microsoft SQL Server 7.0.

Dla wielu przedsiębiorstw przechowujących krytyczne informacje w serwerach OLAP podstawowym wyzwaniem okazuje się połączenie w ramach jednego raportu informacji znajdujących się w serwerach OLAP i innych źródłach danych.

BusinessObjects OLAP Access Packs pozwala na przetwarzanie danych z serwera OLAP z poziomu BusinessObjects. Użytkownicy w ramach jednego raportu mogą analizować informacje pochodzące z wielowymiarowych baz danych i innych źródeł, takich jak hurtownie danych, relacyjne i wielowymiarowe tematyczne hurtownie danych, pakiety zintegrowane i pliki osobiste.

BusinessObjects 4.1 jest obecnie zintegrowany z popularnymi serwerami OLAP: Hyperion Essbase, IBM DB2 OLAP Server, Informix MetaCube i Oracle Express. Kolejna wersja BusinessObjects 5.0, która ma być dostępna jeszcze w pierwszej połowie br., będzie wspierała nowe technologie hurtowni danych zawarte w Microsoft SQLServer 7.0, łącznie z OLE DB for OLAP, funkcjonalnością OLAP Services i Microsoft Repository do współdzielenia danych. Oznacza to, że użytkownicy Business Objects będą mogli uzyskiwać informacje z serwerów wspierających OLAP Services, np. Baan Enterprise Decision Manager. Ponadto Business Objects będzie wspierał zestaw funkcji Microsoft OLE DB for OLAP API. W ten sposób jego użytkownicy mogą łączyć się z innymi źródłami danych OLE DB for OLAP, np. SAP BW.

Informacje z serwera OLAP są automatycznie przesyłane do Business Objects, gdzie są składowane, wraz z innymi danymi raportu, w postaci dynamicznych "mikrokostek". Tym samym niezależnie od źródła danych, użytkownicy Business-Objects mają dostęp do pełnego zakresu funkcjonalności business inteligence.

Bazodanowe rozwiązania OLAP

Praktycznie wszyscy producenci relacyjnych baz danych oferują narzędzia analityczne OLAP. W środowisku open source ciągle nie ma stabilnego rozwiązania OLAP.

Systemy Business Intelligence, będące coraz powszechniejszym elementem systemów informatycznych przedsiębiorstw, są oparte na analitycznych systemach OLAP. Zwykłe bazy transakcyjne nie dają możliwości wyliczania skomplikowaagregatów, są bowiem projektowane w taki sposób, że większość wynikowych informacji nie jest przechowywana. Jeżeli jakaś wartość zostanie wyznaczona na podstawie zawartości kolumn w bazie, to nie musi być ona trwale przechowywana w bazie. W przypadku baz OLAP postępowanie jest odwrotne - projektant określa strukturę kostki OLAP, tzn. wskazuje, jakie informacje mają być gromadzone i agregowane, a następnie motor OLAP wylicza żądane statystyki, które są przechowywane obok informacji bazowych.

Klasycznym przykładem zastosowania kostki OLAP jest analiza wartości sprzedaży. W tym przypadku wymiarami kostki może być typ towaru, region sprzedaży, data sprzedaży czy też nazwa kanału dystrybucyjnego, w którym dany towar był dostępny. By zasilić taką kostkę z systemu OLTP (przetwarzania transakcyjnego), pobiera się informacje dotyczące bieżących obrotów i zapisuje w strukturze OLAP. Nie jest to tylko proste kopiowanie wartości - kostki można zasilać wyliczonymi danymi. Przykładowo, można określić różne poziomy szczegółowości danych (np. grupa towaru, kraina geograficzna czy przedział czasowy: rok, miesiąc, tydzień). Podczas wypełniania kostki motor wylicza np. sumaryczną wartość sprzedaży na całym świecie w określonym roku, a następnie w rozbiciu na poszczególne kontynenty i miesiące. Chociaż zasilanie kostki jest procesem czasochłonnym, to musi być ona aktualizowana w określonym cyklu (np. raz dziennie).

System analityczny może potem szybko czerpać informacje z tak skonstruowanej struktury kostek, tj. wykonywać określone przekroje, np. wybrać dane o wartości sprzedaży w Europie w maju 2002 r., a następnie je uszczegółowić i podać wartość sprzedaży w pierwszym tygodniu maja. Teoretycznie tego typu operacje można wykonać za pomocą bazy OLTP, jednak taka kwerenda mogłaby łatwo spowodować przeciążenie systemu transakcyjnego (zwłaszcza w przypadku jej równoległego wykonywania dla wielu użytkowników). Zastosowanie gotowych agregatów powoduje, że uszczegółowienie wyszukiwania sprowadza się w zasadzie tylko do odczytania zawartości podkostki.

W konkretnej implementacji można tworzyć kostki OLAP, które nie będą przechowywały informacji bazowych, tylko np. ograniczone do określonego poziomu szczegółowości. W przypadku, gdy użytkownik zażąda informacji, które nie są zgromadzone w kostce, motor OLAP pobierze dane źródłowe np. z bazy relacyjnej. Nawet w takim przypadku obciążenie bazy relacyjnej jest małe, bo wybierany jest tylko określony fragment bazy OLTP.

Jakość danych

Tak jak w przypadku hurtowni danych, przy konstrukcji kostek bardzo ważne jest zapewnienie jakości wprowadzanych informacji - sprawdzenie, czy np. nie są błędnie wpisywane nazwy miejscowości, czy adres jest zapisywany w spójnej postaci itp. Bardzo dobrym rozwiązaniem przeznaczonym do kontroli wprowadzanych danych jest mechanizm DTS zawarty Microsoft SQL Server. Pozwala on elastycznie tworzyć mechanizmy przepływu informacji z bazowego systemu OLTP poprzez komponenty (np. kontrolujące poprawność zapisu informacji metodą słownikową) aż do tabel tymczasowych, wykorzystywanych do zasilania kostek OLAP. Działanie DTS nie jest ograniczone tylko do bazy Microsoftu - może czerpać informacje z dowolnego systemu, pod warunkiem że jest w nim dostępny sterownik ODBC/OLEDB.

Niezgodność zapytań

Nie rozwiązanym problemem pozostaje sposób dostępu do danych OLAP-owych. O ile w przypadku danych relacyjnych praktycznie obowiązuje SQL, o tyle w zakresie OLAP niemal każdy producent stosuje odmienne dialekty API, własne metody przechowywania i obróbki metadanych. Microsoft opracował OLEDB for OLAP oraz język MDX. Obecnie duża część niezależnych producentów rozwiązań OLAP dostarcza sterowniki zgodne z tym standardem. Równolegle Hyperion we współpracy z Microsoftem i SAS Institute opracowali XML For Analysis, w którym kwerendy mają składnie podobną do stosowanej w XPatch czy XQuery. W świecie Javy powstał standard JOLAP, pozwalający (przynajmniej w założeniach) na ujednolicony dostęp do danych OLAP z poziomu dowolnego serwera aplikacyjnego zgodnego z J2EE.

Otwartą pozostała kwestia połączenia składni SQL oraz składni zapytań skierowanych do kostki OLAP. W wielu sytuacjach wygodnym rozwiązaniem jest bowiem umieszczenie obok prostego polecenia "Select" określonego agregatu pochodzącego z bazy OLAP. Wyrafinowane rozwiązanie opracował Oracle - jeżeli we frazie where wystąpi słowo OLAP_TABLE, wtedy dany fragment zapytania zostanie przesłany do motoru przetwarzającego dane OLAP. Równocześnie można pobrać relacyjny widok struktury OLAP w taki sposób, aby był on widziany jak normalna tabela SQL. Daje to duże możliwości operowania danymi w bazie.

W Microsoft SQL Server, od wersji 7.0, możliwe jest łączenie wyrażeń OLAP i MDX. Zastosowano w nim mechanizm otwierania dowolnego zbioru rekordów, który może być dostarczony za pośrednictwem sterownika OLEDB, który może łączyć się z serwerem OLAP.

Wszyscy mówią OLAP

Praktycznie wszyscy producenci relacyjnych baz danych oferują jakieś rozwiązania OLAP. W przypadku Microsoft SQL Server 2000 stanowi to integralną część bazy danych. Oracle OLAP jest opcjonalnym składnikiem Oracle Enterprise Edition. IBM DB2 OLAP Server to produkt IBM, oparty na Hyperion Essbase OLAP Server. W ten sposób dowolna aplikacja, która może współpracować z Essbase, może także działać w ramach serwera OLAP IBM.

Sybase nie ma oddzielny serwer OLAP. Natomiast rozwiązania hurtowni danych (np. Adaptative Server IQ Multiplex) mogą przechowywać dane w kostkach razem z agregatami. Informacje są przechowywane w strukturze relacyjnej, jednak nie jest to taka sama baza relacyjna, jak Sybase Adaptative Server, baza Multiplex została bowiem zoptymalizowana do wszelkiego rodzaju operacji związanych z zastosowaniami Business Intelligence.

W środowisku open source praktycznie nie ma stabilnego rozwiązania OLAP. Obecnie trwają prace nad serwerem OLAP napisanym w Javie, który będzie implementował większość popularnych standardów API - MDX, JOLAP oraz XML for Analysis. Obecnie jest dostępna wersja 0.5 tego pakietu - numer wersji dobrze oddaje stopień jego przygotowania.

Prezentacje, prezentacje...

Kostka OLAP jest tworem wielowymiarowym, w związku z tym także wynik zapytania, rzadko jest jedną liczbą - zazwyczaj ma kilka wymiarów. Mimo tych potencjalnych możliwości, ciągle jeszcze wszystkie sposoby prezentacji wyglądają bardzo podobnie - po określeniu ciągu warunków, wybierany jest płaski widok, gdzie ewentualnie na przecięciu kolumn znajduje się kilka liczb, które obrazują kolejne poziomy agregacji.

Informacja dla mas - OLAP

Dołączenie do SQL Server 7 produktów do wspomagania decyzji umożliwia przedsiębiorstwom wdrożenia niewielkim kosztem rozwiązań z zakresu informacji zarządczej.

Pojawienie się OLAP Services wraz z SQL Server 7 zmieniło rynek informacji zarządczej (business intelligence). Wprawdzie roczna obecność na rynku OLAP Services nie wpłynęła znacząco na pozycję dostawców narzędzi analitycznych i produktów do eksploracji danych takich jak Holos, Hyperion czy SAS, ale uderzyła jednak w producentów tańszych rozwiązań. Ci, by nie konkurować bezpośrednio z Microsoftem, muszą różnicować swoje narzędzia, szukać rynków niszowych.

MS OLAP jest czymś więcej niż tylko zestawem analitycznym klient/serwer. Wielu niezależnych producentów baz danych zaadaptowało bowiem interfejs dostępu używany w MS OLAP, zaś wiele firm programistycznych skorzystało z możliwości wbudowanych w MS Office 2000 i Visual Studio do tworzenia własnych spec-jalizowanych aplikacji analitycznych.

SQL Server w hurtowni

Aplikacja do wspomagania procesów podejmowania decyzji składa się z trzech elementów: hurtowni danych "na zapleczu", serwera OLAP w pośredniej warstwie oraz programów klienckich dostępu do danych, analizy i prezentacji. Optymalna realizacja zestawu OLAP Services wymaga dwóch komputerów z Windows NT, na których zainstaluje się hurtownię danych i serwer analityczny MS OLAP Server. Klientem może być komputer z Win 95/98/NT i jednym z licznych programów analitycznych.

Realizacja hurtowni wymaga zaprojektowania schematu i jego implementacji, stworzenia skryptów do pobrania danych z baz operacyjnych, dokonania niezbędnych transformacji danych i załadowania ich do hurtowni. Hurtownię danych opartą na SQL Serverze można zaprojektować i utworzyć, posługując się programem SQL Enterprise Manager, modułem zestawu Microsoft Management Console (MMC). Enterprise Manager graficznie tworzy i modyfikuje obiekty hurtowni oraz generuje skrypt dla SQL Servera dla dokonania niezbędnych operacji w bazie produkcyjnej lub testowej. Do modelowania gwiazdowej struktury hurtowni w bazie relacyjnej może służyć Visual Database Designer.

Najtrudniejszy problem realizacji hurtowni polega na sprecyzowaniu, jakie dane należy pobrać, jak je przekształcić z formatu operacyjnego na postać obowiązującą w hurtowni i jak załadować dane do hurtowni. MS SQL Server 7 do wykonania tych operacji oferuje narzędzie Data Transformation Services (DTS). Pozwala ono na pobieranie danych z baz SQL Ser-ver i Oracle lub z dowolnego źródła zgodnego z ODBC. Wynikowy zbiór danych może być załadowany do SQL Servera lub innej bazy ODBC.

DTS tworzy zadania do dokonywania operacji pobierania, transformacji i ładowania w formie skryptów Transact SQL (dialekt używany przez MS SQL Server i Sybase), VBScript, JavaScript i komend Perl. DTS może dokonywać licznych operacji na danych, w tym wyliczyć nowe wartości z połączenia kolumn lub agregacje. Struktury danych, skrypty do pobierania, transformacji i ładowania danych oraz inne metadane (np. odwzorowanie nazw tabel na określenia biznesowe) są przechowywane w repozytorium Microsoft, ważnym elemencie projektu każdej hurtowni danych.

Warstwa pośrednia - OLAP Services

OLAP Services mogą współpracować z różnymi bazami danych, nie tylko SQL Server. Nie można ich kupić jako oddzielnego produktu, natomiast można je instalować niezależnie od serwera Microsoftu.

Kluczowym obiektem MS OLAP jest sześ-cian danych - struktura służąca do zapamiętywania wielowymiarowych danych zagregowanych. Analiz OLAP dokonuje się przez zadawanie zapytań (dokonywanie selekcji, obrotów i przekrojów) do tego sześ-cianu. Edytor sześcianów pozwala na ich tworzenie przez wybranie jednej tabeli faktów (danych numerycznych, takich jak dochód czy koszt) oraz kluczy wymiarowych z dowolnymi poziomami szczegółowości (np. czas podawany w dniach, tygodniach, miesiącach i latach), określającymi jak dane się agreguje i tworzy przekroje. Projekt hurtowni powinien uwzględniać specyfikę tworzenia sześcianów przez MS OLAP, możliwie ściśle dopasowując się do teoretycznego modelu gwiazdy lub płatka śniegu.

Sześcian danych można przechowywać w relacyjnej bazie danych (relacyjny model OLAP), w bazie wielowymiarowej (MOLAP) lub hybrydowej (HOLAP, podzielony między bazę wielowymiarową i relacyjną). SQL Server pozwala na realizację każdej z tych możliwości. W celu osiągnięcia dobrej wydajności analiz OLAP wskazane jest zapisywanie danych w strukturach MOLAP; na dysku taka struktura wymaga jednak wielokrotnie więcej miejsca niż wynosi rozmiar danych. Jeżeli natomiast w sześcianie jest bardzo dużo danych, relacyjny model pozwala na partycjonowanie danych, a każda partycja może mieć inny model zapamiętywania.

Ponieważ agregowanie powoduje gwałtowny przyrost rozmiaru przestrzeni dyskowej, MS OLAP oferuje możliwość definiowania, które agregacje będą zapisywane na dysku, a które będzie można obliczać na bieżąco w trakcie wykonywania zapytania. Ponadto pozwala na definiowanie w sześcianie innych pól wczytywanych z dodatkowych tabel lub wyliczanych (za pomocą funkcji napisanych przez użytkownika) w trakcie realizacji zapytania.

Aplikacje klienckie

Na rynku istnieje wiele uniwersalnych narzędzi analitycznych współpracujących z MS OLAP, obecnie dostarcza je ponad 10 firm, w tym Cognos (NovaView), Seagate Software (Worksheet i Analyzer), OLAP@Work, Portola, Knosys (ProClarity). Część z nich jest bezpłatna, koszt innych jest znikomy. Również Excel 2000 może stanowić uniwersalny interfejs do MS OLAP.

Język Visual Basic for Applications, wbudowany w Microsoft Office 2000 Developer Edition, nadaje się do tworzenia analitycznych rozszerzeń programów biurowych o możliwości analityczne dla określonych zastosowań. Pakiet Visual Studio 6 umożliwia korzystanie z OLE DB for OLAP, pozwalając na operowanie na wielowymiarowych obiektach danych i buforowanie w pamięci, pobieranie z repozytorium informacji o zawartości i strukturze hurtowni, istniejących sześcianach danych.

Operowanie na danych

Architektura OLAP Services jest otwarta. Pozwala operować na sześcianach danych za pomocą zestawu funkcji Decision Support Objects API, służących do rozszerzania właściwości pakietu administracyjnego OLAP Manager. Rozszerzenia komponentów ActiveX Data Objects MD służą do tworzenia interfejsu aplikacji klienckich do sześcianów danych. Język Multidimensional Expression (MDX) stanowi wielowymiarowe rozszerzenie SQL o funkcje zdefiniowane przez Microsoft w OLE DB for OLAP. Funkcja obracanej tabeli PivotTable pozwala na dwukierunkową wymianę danych wielowymiarowych z aplikacją kliencką. Wszystko to powoduje, że MS OLAP jest raczej zestawem programistycznym do opracowania aplikacji niż produktem OLAP "z półki".

SQL Server 7 z OLAP Services jest dostępny od stycznia 1999 r. Od tego czasu Microsoft ulepszył m.in. wydajność SQL Servera w zakresie wykonywania operacji analitycznych. Następna wersja, nazwana SQL Server 2000, będzie dostępna w połowie br.

Obecnie dostępne są dwie wersje SQL Server - Standard i Enterprise. Obie zawierają relacyjny motor danych, pełną replikację danych, DTS oraz repozytorium Meta Data Repository 2.0. W wersji standardowej nie ma możliwości partycjonowania danych wielowymiarowych. Koszt wersji Enterprise wynosi: od 1400 USD (dla 5 użytkowników) do 29 tys. USD (dla 250 użytkowników).

Pamięciowa analiza OLAP

Applix TM1 to kolejny, dostępny na polskim rynku, pakiet analityczny OLAP.

Firma Applix postawiła sobie cel stworzenie wielowymiarowego serwera analitycznego OLAP o dużej szybkości działania, pozwalającego na dokonywanie agregacji, przekrojów i obrotów. Dużą szybkość działania można osiągnąć jedynie przez załadowanie całej wielowymiarowej bazy do pamięci RAM serwera.

Wadą tego rozwiązania jest mały rozmiar bazy, którą można poddawać analizie. Dodanie do hurtowni danych serwera Applix TM1 OLAP Server pozwoli na analizę jedynie ograniczonego do kilku lub kilkunastu megabajtów wycinka danych. Dokonanie analiz na innych wymiarach wymaga utworzenia nowej struktury wielowymiarowej.

W pakiecie TM1 OLAP Server dane do analizy (hipersześcian danych) są wprawdzie zapisywane na dysk do użycia w przyszłości, ale wszystkie analizy wykonywane są na bazie w całości załadowanej do pamięci RAM. TM1 OLAP Server umożliwia korzystanie z danych przez wielu użytkowników, zapewnia replikację na inne serwery.

Ładowanie danych do bazy TM1 ułatwia narzędzie TM1 Data Control, służące do projektowania struktury bazy (hierarchii, wymiarów, elementów) i zapełniania jej danymi. Narzędzie TM1 Architect służy do tworzenia i przechowywania modeli danych, zarządzania serwerem TM1, replikacji do innych serwerów i synchronizacji danych oraz określania uprawnień użytkowników.

Narzędzia analityczne

Jak dowodzą badania rynkowe, najpopularniejszym narzędziem analitycznym są arkusze obliczeniowe. Applix proponuje więc narzędzia analityczne rozszerzające możliwości analityczne Excela i 1-2-3 w zakresie dokonywania przekrojów, agregowania i drążenia danych.

Inne rozwiązanie to TM1 Perspectives, jednostanowiskowa wersja OLAP do komputerów PC, zarówno klient serwera TM1 OLAP jak i samodzielne narzędzie analityczne w przypadku pracy na lokalnej wersji wielowymiarowej bazy danych bez połączenia z serwerem OLAP.

Zgodny z OLE DB for OLAP

Opublikowanie przez Microsoft specyfikacji dostępu do wielowymiarowych baz danych OLE DB for OLAP umożliwiło firmie Applix opracowanie serwera OLAP zgodnego z tą specyfikacją, konkurencyjnego w stosunku do serwera Plato, dostarczanego przez Microsoft wraz z SQL Server 7.0.

Serwer ten może bezpośrednio współpracować z wieloma dostępnymi narzędziami analitycznymi zgodnymi z OLE DB for OLAP, takimi jak Seagate Worksheet czy Cognos NovaView. Applix poinformował o przeniesieniu pod system operacyjny Linux aplikacji klienckiej TM1 OLAP for Linux, która może działać jako samodzielny system jednostanowiskowy lub korzystać z danych przechowywanych przez serwer wielowymiarowej bazy danych TM1 OLAP Server (działający na innych platformach). Program Applix TM1 OLAP for Linux wymaga zainstalowania arkusza obliczeniowego z pakietu aplikacji Applixware w wersji dla Linuxa.

Applix TM1
Platformy: Windows NT, 95, Sun Solaris, HP i IBM Unix

Internet i serwer aplikacyjny

Nowa wersja Internet Information Services (IIS) w Windows Server 2003 została zupełnie inaczej zaprojektowana niż wcześniejsze. Praktycznie zmieniły się zupełnie zasady zarówno instalacji (domyślnie IIS w ogóle nie jest instalowany na serwerze; administrator musi go wybrać, a dodatkowo określić, jakie rozszerzenia będą dostępne w IIS). Główna zmiana związana jest z zupełnie inną architekturą serwera.

W Windows 2000, gdy przychodzi żądanie do serwera WWW, jest ono najpierw przetwarzane na poziomie jądra (gdzie następuje obsługa m.in. gniazd TCP/IP). Następnie dane przesyłane są do procesu IIS, gdzie następuje analiza nagłówka HTTP. W zależności od wyników analizy żądanie przekierowywane jest do konkretnego procesu CGI czy ASP, który obsługuje daną witrynę.

W Windows Server 2003, w jądrze moduł HTTP.SYS odpowiada za pełną obsługę protokołu HTTP. Dzięki temu jądro od razu może przeanalizować żądanie i wywołać odpowiedni proces roboczy, który ma je obsłużyć. Na poziomie jądra odbywa się także obsługa pamięci podręcznej, co jeszcze bardziej przyspiesza działanie serwera. Należy podkreślić, że jest także druga strona medalu - do jądra Windows Server 2003 wprowadzony został dodatkowy komponent, potencjalne źródło problemów.

IIS 6.0 wykorzystuje zupełnie nowy model izolacji procesów, który z jednej strony zapewnia większy poziom bezpieczeństwa, a z drugiej - lepiej wykorzystuje zasoby serwera.

W IIS 5 dostępne były dwa sposoby izolacji aplikacji WWW działających na serwerze. Aplikacja mogła funkcjonować jako oddzielny proces albo wszystkie aplikacje WWW były gromadzone w jednym procesie (w takim trybie znacznie mniejsze jest zużycie zasobów). Jednak w tym trybie wadliwie działająca aplikacja mogła zakłócić pracę innych witryn, a nawet głównego procesu IIS, co jest niedopuszczalne, na przykład gdy na serwerze są hostowane witryny różnych klientów.

W IIS 6.0 dostępny jest dodatkowy model izolacji aplikacji. Można utworzyć dodatkową instancję "zestawu" - tzw. pulę czy "web garden". Proces inetinfo.exe (główny proces serwera WWW) jest zupełnie oddzielony, nie zawiera żadnego kodu aplikacji WWW uruchamianych na IIS. W ten sposób znacznie zwiększono stabilność serwera - praktycznie błędnie napisana aplikacja nie może spowodować zawieszenia inetinfo.exe.

Wydzielenie wątków roboczych zwiększyło elastyczność konfiguracji serwera WWW - można grupować określone serwisy WWW w wybranych, oddzielnych procesach. Każdy z tych procesów może mieć oddzielne uprawnienia. Konfigurując pulę., można ustawiać m.in., maksymalny rozmiar pamięci oraz zdefiniować sytuacje, w których aplikacje będą automatycznie restartowane.

W IIS 6.0 można także podać, ile procent mocy procesora mają maksymalnie zająć wątki robocze działające w ramach puli (ten mechanizm może być wykorzystany, gdy serwer pełni także inną funkcję oprócz serwera WWW). W ten sposób administrator może skonfigurować taki serwer, który poradzi sobie nawet z błędnie napisanymi witrynami. Warto dodać, że podczas restartu puli (a więc i danej aplikacji) nie jest tracona sesja użytkownika. Innymi słowy, jeżeli internauta dokonywał zakupów w sklepie, gdzie sesja jest wykorzystywana do przechowywania informacji o koszyku, to nie zauważy restartu puli - nadal będzie miał dostępny swój koszyk itp.

Jednak w razie konieczności administrator może włączyć tryb zgodności z IIS 5.0 - ta opcja przydaje się, jeżeli wspomnianego modelu izolacji wymagają aplikacje uruchamiane na danym serwerze.

W IIS 6.0 konfiguracją serwera zarządza oddzielny komponent WAS (Web Administration Service). Odpowiada on za dynamiczną zmianę konfiguracji IIS w trakcie działania serwera. WAS może także zatrzymać zbyt długi nieużywany wątek roboczy. W zależności od opcji mogą być dynamicznie wykrywane zmiany w metabazie (pliku XML), który określa konfigurację serwera. Administrator ma do wyboru korzystanie z administracyjnego GUI albo ręczne edytowanie pliku tekstowgo z konfiguracją. Równocześnie dzięki XML-owi wszystkie ustawienia można zapisać w pliku (np. konfiguracje katalogów wirtualnych).

Internet Information Server ma wbudowaną obsługę autoryzacji przy użyciu Microsoft Passport. Dotychczas dostępne były metody wykorzystywania zintegrowanej autoryzacji Windows, autoryzacji typu diggest oraz podstawowego mechanizmu, gdzie hasło i nazwa użytkownika przesyłane były w niezakodowanej postaci. Warto dodać, że aby logować się w witrynie przy użyciu Microsoft Passport, trzeba skonfigurować odpowiednio Passport Manager Authorization i zarejestrować system.

Warto też dodać, że użytkownicy serwera FTP są izolowani od użytkowników WWW.

IIS 6.0 jest bardzo wydajnym serwerem plików HTML (czyli informacji statycznych). Obsługuje także najnowszą wersję rozszerzeń FrontPage oraz SharePoint Portal Server. Na IIS 6.0 można uruchamiać zarówno strony dynamiczne ASP, jak i napisane przy użyciu technologii .NET - ASP.NET.

W wypadku .NET administrator ma bardzo duże możliwości kontroli uruchamianego kodu. Program w .NET (np. kod obsługujący witrynę ASP.NET) umieszczany jest w tzw. pakietach (assembly). Taki pakiet może być podpisany cyfrowo przez autora. Administrator może określić, że "ufa" pakietom podpisanym przez danego programistę albo że na serwerze mogą działać tylko te aplikacje, które są podpisane danym kluczem. Można też dokładnie określić, jakie operacje są dozwolone dla danego pakietu (czy też pakietu o danej sygnaturze).

Ustawienie uprawnień dla pakietów .NET obejmuje chyba każdy aspekt działania. Można ograniczać prawa zapisu w określonych miejscach na dysku, blokować dostęp do Active Directory, określać zasady komunikacji sieciowej, MSMQ itp. Można też zabronić dostępu do API systemowego (pakiety .NET działają w specjalnym, izolowanym środowisku). Wszystko to sprawia, że omawiana technologia jest dosyć bezpieczna i administrator może określić, co będzie działać na "jego" serwerze.

Administrator może bardzo precyzyjnie określić uprawnienia jakich udziela danemu pakietowi .NET.

Microsoft Windows Server 2003

Choć przy każdej premierze nowego systemu Microsoftu dowiadujemy się, że jest on najbezpieczniejszy ze wszystkich do tej pory opracowanych, to za każdym razem kilka następnych miesięcy weryfikuje te stwierdzenia. Doświadczeni administratorzy decydują się na zmianę systemu dopiero wtedy, gdy pojawią się pierwsze poważne uaktualnienia. Czy Windows Server 2003 będzie wyjątkiem od tej reguły? Pierwsze wrażenia sugerują, że jest to możliwe.

Czy to możliwe w sytuacji, gdy aktualne produkty z rodziny Windows korzystają z tego samego jądra, a podstawowe części systemów są tak podobne do siebie? Legendarne już luki zabezpieczeń wcześniejszych systemów musiały przecież w końcu zmusić Microsoft do gruntownego zajęcia się problemem bezpieczeństwa. Jeżeli jednak udało się poprawić bezpieczeństwo, to w jakim stopniu kosztem funkcjonalności i wygody użytkowania?

Windows Server 2003 ma być początkiem nowej, licznej rodziny produktów, określanej mianem Windows Serwer System. Microsoft zapowiada sukcesywne pojawianie się takich produktów, jak Office 2003, BizTalk Server, Exchange Server 2003, Real-Time Communication Server, Windows SharePoint Services, Rights Management Services, Automated Deployment Services, Small Business Server i wreszcie narzędzie do zarządzania całością, System Center. Dzięki zaawansowanej strukturze plików i systemowi zarządzania tożsamością ma to być zintegrowane środowisko świadczące wszystkie usługi, jakich oczekuje użytkownik, a może nawet o krok wyprzedzające jego potrzeby.

Praktycznie wszystkie istniejące produkty Microsoftu doczekają się nowych wersji, przy czym najdłużej będziemy musieli czekać na nową wersję SQL Servera. Ich liczbę szacuje się na około dwadzieścia.

Opis systemu

Windows Server 2003 to uniwersalny system operacyjny, który może pełnić różnorodne funkcje serwerowe, zależnie od potrzeb użytkownika i wersji, którą się posługuje. Poszczególne wersje przeznaczone są oczywiście dla różnych grup użytkowników:

Windows Server 2003, Standard Edition. Dla małych organizacji, zawiera zmodernizowane mechanizmy w zakresie udostępniania plików i drukarek, zapewnia bezpieczne połączenia z Internetem i scentralizowane zarządzanie komputerem. Wydajna, niezależna, skalowalna i bezpieczna platforma.

Windows Server 2003, Enterprise Edition. Dla średnich organizacji do stosowania na serwerach, na których pracują aplikacje sieciowe, biznesowe, komunikacyjne, bazy danych itp. Wyższą stabilność i wydajność zapewnia wersja 64-bitowa, dostępna obok 32-bitowej.

Windows Server 2003, Datacenter Edition. Dla firm wymagających najwyższego poziomu dostępności i stabilności serwera. Najbardziej wydajna wersja systemu Windows Server 2003, doskonała do utrzymywania dużych baz danych, dysków i pracy skomplikowanych aplikacji. Dostępna w wersjach 32-bitowej i 64-bitowej.

Windows Server 2003, Web Edition. Do budowy i utrzymania aplikacji internetowych, witryn oraz usług XML. Zapewnia optymalne warunki do usług internetowych.

Obecnie dostępne wersje i ich podstawowe parametry przedstawiamy w tabeli na następnej stronie.

Windows Server 2003 zastosował najlepsze technologie systemu Windows Server 2000, wzbogacając go jednocześnie o właściwości platformy Microsoft .NET, która ułatwia udostępnianie informacji, systemów i urządzeń oraz współpracę i komunikację między użytkownikami.

System może pracować w trybie scentralizowanym lub rozproszonym, a jego podstawowe funkcje to:
serwer plików i wydruków,
serwer sieci Web i serwer aplikacji sieciowych,
serwer pocztowy,
serwer terminalowy,
serwer dostępu zdalnego/wirtualnej sieci prywatnej (VPN),
serwer usług katalogowych, systemu DNS, protokołu DHCP i usługi WINS,
serwer do obsługi multimediów przesyłanych strumieniowo.Dzięki zastosowanym technologiom Windows Serwer 2003 może pracować w firmach o dowolnej wielkości, elastycznie dostosowując się do zmieniających się obciążeń. Wśród podstawowych zalet systemu Microsoft wymienia:

Niezawodność. System może charakteryzować się wysoką dostępnością dzięki wbudowanej i rozszerzonej obsłudze klastrowania. Obsługuje do ośmiu węzłów, realizuje równomierny rozkład obciążeń, a w razie awarii jednego z węzłów inne natychmiast przejmują w trybie awaryjnym jego funkcje. System jest podwójnie skalowalny - w pionie, dzięki obsłudze wieloprocesorowości, oraz w poziomie, dzięki możliwości budowy klastrów. System już w trakcie projektowania został bardzo dokładnie sprawdzony pod kątem niezawodności. Robert Short, wiceprezes departamentu Windows Core Technology, powiedział w wywiadzie udzielonym serwisowi ZDNet, że do testowania "szczelności" systemu zatrudniono około dziesięciu najlepszych programistów, którzy wcielili się w rolę hakerów nieustannie włamujących się do systemu. Miał wśród nich być jeden były prawdziwy haker, którego nakłoniono do współpracy. Ponieważ coraz więcej firm musi korzystać z Sieci, było to zagadnienie kluczowe. Zmniejszono więc do minimum liczbę luk wynikających z błędów w konstrukcji systemu, a sam system weryfikuje aplikacje i przypisane im uprawnienia, eliminując ryzyko uruchomienia złośliwego kodu. Poziom zabezpieczeń internetowych usług informacyjnych (IIS 6.0) domyślnie ustawiony jest na maksimum, co zwiększa bezpieczeństwo pracy w Sieci.

Wydajność. Wraz z postępującym rozproszeniem sieci firmowych w wyniku dołączania ekstranetów i udziału Internetu poważnym problemem staje się efektywne zarządzanie zasobami plików i wydrukami. Zwiększa się też obciążenie sieci ze względu na wzrost liczby użytkowników zdalnych (pracownicy mobilni, partnerzy handlowi). Usługa Active Directory logicznie i hierarchicznie porządkuje zasoby informacji, a nowe narzędzia ułatwiające zarządzanie, w tym Software Update Service, wspomagają codzienną obsługę sieci. Poprawione zostało zarządzanie pamięciami masowymi, wykonywanie kopii zapasowych i odzyskiwanie danych. Usługi terminalowe umożliwiają zdalne uruchamianie aplikacji nawet z poziomu urządzeń, na których nie można uruchomić systemu Windows.

Elastyczność w zastosowaniach sieciowych. Usługi IIS 6.0 to szybka i niezawodna platforma, umożliwiająca bezpieczne korzystanie z zasobów przez pracowników biurowych, mobilnych i partnerów handlowych. Zadbano o elastyczność, wydajność i bezpieczeństwo - to ostatnie przecież od zawsze było powodem największych cięgów, jakie Microsoft zbierał od użytkowników. Ponadto Windows Serwer 2003 oferuje efektywne mechanizmy przesyłania mediów strumieniowych, których znaczenie ciągle przecież rośnie.

Bezpieczeństwo. Zmiany związane z poprawą bezpieczeństwa mają wreszcie charakter jakościowy, to znaczy wynikają z innego sposobu myślenia. Przede wszystkim zupełnie inny jest domyślny poziom bezpieczeństwa systemu tuż po instalacji. Poprzednio instalowane były domyślnie niemal wszystkie składniki, teraz - tylko potrzebne do

pełnienia funkcji przypisanej serwerowi. Mimo że IIS 6.0 jest uznawany za znacznie bezpieczniejszy od wersji 5.0, nie jest on domyślnie instalowany, a w dodatku tylko wtedy, gdy serwerowi przypisano funkcję serwera aplikacyjnego. Niektóre z usług IIS 6.0 wymagają z kolei instalacji odpowiednich rozszerzeń ISS 6.0, co wymusza na administratorze świadome postępowanie. Podobnie jest z dostępem do plików. O ile w Windows 2000 Server do nowo utworzonego udziału sieciowego domyślnie wszyscy użytkownicy mieli pełny dostęp, o tyle obecnie domyślny dostęp daje tylko prawo do odczytu. Coraz trudniej będzie tłumaczyć błędy nieświadomością lub zaniechaniem. I taka właśnie była intencja.

Od początku

Instalacja przebiega w sposób znany z Windows XP. Użytkownika wita znany ekran powitalny, oczywiście jeśli rozpoczyna się instalację z jednej z poprzednich wersji Windows, a nie od uruchomienia systemu z instalacyjnej płyty CD.

Oczywiście, możliwe jest uaktualnienie wersji np. Standard do Enterprise. Kolejne czynności również są standardowe - klucz CD, ustawienia regionalne, położenie katalogu Windows. Dostępne są również ułatwienia w postaci lupy i narracji głosowej. Następnie trzeba podjąć decyzję o wyborze systemu plików - jeżeli system jest instalowany na komputerze z systemem FAT32, można pozostawić ten system plików, można też przejść na system plików NTFS. Jeśli system instalowany jest z Windows XP, instalator może się połączyć z Internetem i ściągnąć od razu potrzebne poprawki.

Po restarcie komputera pojawia się już interfejs, tekstowy tym razem, znany również z Windows XP. Kolejne etapy to wczytywanie sterowników, pytanie o partycję, sprawdzenie dysku(ów), kopiowanie plików i wreszcie uruchomienie interfejsu graficznego.

Dochodzimy do chwili, kiedy instalator pyta o rodzaj licencji. Licencja per server dotyczy zwykle pojedynczego serwera; w takim modelu klient otrzymuje licencję na serwer oraz tyle licencji na klienty, ile jest równoczesnych połączeń do serwera. Drugi wariant to licencja per seat: klient otrzymuje licencję na każdą stację roboczą. Ta licencja pozwala użytkownikowi na dostęp do każdego serwera znajdującego się w sieci. W dużych sieciach z kilkoma serwerami model ten pozwala na znaczne zmniejszenie kosztów. Jeśli będzie potrzebny dodatkowy serwer, klient dokupuje wyłącznie pojedynczą licencję na jeden serwer. Możliwa jest późniejsza zmiana warunków licencji.

Kolejne rutynowe czynności to podanie nazwy komputera i hasła administratora. W tym ostatnim przypadku, inaczej niż w Windows XP, hasło musi spełniać określone, minimalne parametry: składać się co najmniej z sześciu znaków, zawierać małe i wielkie litery, cyfry oraz znaki specjalne. Wreszcie kolejno użytkownik konfiguruje strefę czasową i datę, a także składniki sieciowe. Instalator wykrywa wszystkie systemy operacyjne znajdujące się na komputerze i jak zwykle, ostatni instalowany system umieszcza się na pierwszym miejscu menu wyboru jako system niejako domyślny. Zaawansowani użytkownicy mogą wyedytować plik boot.ini w celu zmiany ustawień lub skorzystać z ustawień zaawansowanych we właściwościach systemu.

Podstawowa instalacja systemu jest równie prosta, jak i poprzednich systemów Windows. Niestety, jest równie czasochłonna - na wszystkie czynności, w tym głównie oczekiwanie, należy przeznaczyć niemal godzinę.

"Goły" system tuż po instalacji uruchamia się dość długo - prawie dwa razy dłużej niż skonfigurowany i obarczony różnymi aplikacjami Windows XP. W miarę obrastania w aplikacje i sterowniki czas ten jeszcze nieco wzrasta, co można uznać za rzecz oczywistą.

W trakcie uruchomienia konieczny jest "trójpalcowy salut" [Ctrl+Alt+Del], po którym jesteśmy proszeni o wprowadzenie hasła. Microsoft tłumaczy to względami

bezpieczeństwa. Jedna z opcji Local Security Policy (Local Policies | Security Options | Interactive Logon: do not request CTRL+ALT+DEL) umożliwia wyłączenie tej funkcji; można też na karcie Screen Saver we właściwościach ekranu wyłączyć żądanie podania hasła po zadziałaniu wygaszacza ekranu, które po instalacji domyślnie jest włączone.

Kolejny ekran to Manage Your Server, umożliwiający dodanie usług sieciowych dostępnych na serwerze i będący w praktyce konsolą sterowania. Zanim z niej skorzystamy, musimy skonfigurować podstawowe parametry, a później można zaznaczyć opcję, która powoduje, że okno nie pojawia się po uruchomieniu.

Po zamknięciu okna Manage Your Server użytkownikowi ukazuje się... pusty pulpit. Jedynym "ozdobnikiem" jest ikona kosza, nie wiedzieć czemu, uznawana we wszystkich wersjach Windows za tak ważną, że musi pojawiać się bezpośrednio po instalacji.

Znana z Windows XP powłoka LUNA, do której wielu może już zdążyło się przyzwyczaić, jest również dostępna, chociaż jej aktywacja wymaga nieco zachodu. Należy w tym celu przejść do Administrative Tools | Services i uruchomić usługę Themes. Z pewnością nieco bardziej spartańska standardowa powłoka Windows Server 2003 pochłania trochę mniej zasobów komputera. Równie podobne do Windows XP jest Menu Start, podzielone na kilka stref i wyposażone w rozwijane listy. Okna My Computer i Control Panel również nie sprawią kłopotu nikomu, kto zna wcześniejsze wersje Windows.

Czas na Internet

Skoro mamy już skonfigurowane podstawy systemu, a zajęło to trochę czasu, chciałoby się zajrzeć do Sieci. Jeżeli połączenie sieciowe nie zostało skonfigurowane wcześniej, można to zrobić teraz - Control Panel | Network Connections | New Connections Wizzard. Po wpisaniu odpowiednich wartości można sprawdzić efekt - w oknie Local Area Connection wyświetlany jest status połączenia. Ponieważ wskaźnik statusu pokazuje Connected, uruchamiamy Internet Explorer i... nic.

Windows Server 2003 jest tak restrykcyjnie zabezpieczony, że mimo czynnego połączenia nie ładują się strony, nie działa też poczta elektroniczna. Na szczęście, jeżeli zdezorientowany użytkownik będzie wystarczająco cierpliwy, doczeka się stosownego komunikatu. Musi wówczas otworzyć Control Panel | Add or Remove Programms, a następnie wybrać opcję Add/Remove Windows Components. Kolejne kroki to odszukanie opcji Internet Explorer Enhanced Security Configuration, naciśnięcie przycisku Details i odznaczenie obu dostępnych opcji. Dwukrotne naciśnięcie przycisku OK zatwierdzi zmiany, dostęp do stron WWW stoi otworem. Być może, nieco powiększył się też "otwór" do naszego komputera, jednak w końcu dostęp do Internetu to jeden z ważniejszych powodów używania komputerów.

Dookoła Windows

Jest cechą charakterystyczną systemów Windows, że z biegiem czasu i z kolejnymi wersjami obrastają w coraz większą liczbę aplikacji pomocniczych - głównie multimedialnych i komunikacyjnych. Choć Windows Server 2003 jest z założenia systemem serwerowym, nie jest przecież praktycznie uboższy w dodatki. Nie znajdziemy tu wprawdzie komunikatorów Windows Messenger/MSN Messenger, zaś dołączony Internet Explorer nie ma rozszerzenia MSN, nie znaczy to jednak, że system serwerowy nie może służyć do multimediów i gier. Łatwo natomiast zauważyć, że po instalacji systemu domyślnie wyłączone są lub ustawione na niewielką wydajność akceleratory i wspomaganie sprzętowe. Dotyczy to na przykład akceleracji sprzętowej karty graficznej oraz akceleracji DirectX. Standardowe sterowniki kart graficznych dołączone do Windows Server 2003 mogą odmówić posłuszeństwa w grach, szczególnie 3D. W końcu jednak przygotowano je do pracy w środowisku serwerowym, a nie na potrzeby fanów gier.

Jest więc Windows Media Player w wersji 9, z możliwością kopiowania plików z płyt CD do formatów MP3 i WMA, oraz nagrywania plików z twardego dysku na płyty CD-RW. Funkcja obsługi nagrywarek jest domyślnie wyłączona, można ją jednak oczywiście aktywować w usługach (IMAPI CD-Burning COM Service).

Windows Workstation 2003?

I oto dochodzimy do wniosku, że właściwie nic nie stoi na przeszkodzie (poza ceną - patrz ramka), by zastosować Windows Server 2003 jako system domowy. Aby się o tym przekonać, wystarczy zainstalować zamieszczoną przez nas na płycie, 180-dniową wersję testową tego systemu.

Taka adaptacja wymaga wszakże kilku zabiegów. O czterech była już mowa - trzeba "odblokować" dostęp do Internetu, włączyć obsługę nagrywarki, wyłączyć żądanie podawania hasła podczas logowania i po zadziałaniu wygaszacza ekranu. Kolejna funkcja, która może irytować użytkownika, to konieczność podawania powodu restartu lub wyłączenia komputera. Aby się jej pozbyć, należy wpisać gpedit.msc w wierszu poleceń, uruchamiając w ten sposób Group Policy Object Editora. W jego oknie należy przejść kolejno: Computer Configuration | Administrative Templates | System i po prawej stronie kliknąć dwukrotnie pozycję Display Shutdown Event Tracker. Zaznaczenie opcji Disabled i zatwierdzenie kliknięciem OK uwolni nas od drobnych, acz uciążliwych czynności.

Kolejna przykra, choć możliwa do usunięcia niespodzianka, to brak dźwięku. Nawet jeśli karta dźwiękowa została poprawnie zainstalowana, z głośników nie wydobędzie się żaden dźwięk. Obsługa dźwięku jest domyślnie wyłączona - to kwestia bezpieczeństwa i stabilności systemu. Aby ją włączyć, należy wykonać następujące czynności: Start | Administrative Tools| Services, następnie przejść do usługi Windows Audio, kliknąć ją prawym przyciskiem myszy i jako Startup Type wybrać Automatic. Na koniec: Apply | OK | Start the service. Niestety, lista obsługiwanych kart dźwiękowych jest bardzo krótka (różne wersje można znaleźć w Internecie). Można też wypróbować sterowniki Windows XP. Na oficjalnej stronie Microsoftu, poświęconej zgodności sprzętu, nie ma w chwili pisania tego tekstu żadnej karty dźwiękowej do Windows Server 2003.

Kolej na DirectX i kartę graficzną. Jak wspomniano, akceleracja jest w obu wypadkach domyślnie wyłączona. Aby zmienić ustawienia DirectX, należy z wiersza poleceń uruchomić narzędzie dxdiag i na karcie Display w polu DirectX Features, kliknąć kolejno przyciski Enable. Dostępne są również dwa przyciski do przetestowania działania DirectX - Test DirectDraw oraz Test Direct3D.

Podobnie należy zmienić ustawienia akceleracji karty graficznej - domyślnie wykorzystane jest 20 procent potencjału akceleracji. W tym celu należy kliknąć prawym przyciskiem myszy wolny fragment ekranu, następnie kliknąć Properties i na karcie Settings kliknąć Advanced. Na karcie Troubleshoot należy przeciągnąć suwak w skrajnie prawe położenie.

Jak zwykle w takich przypadkach, można spróbować poszukać nowszego sterownika karty graficznej.

Bardziej zaawansowani i dociekliwi użytkownicy mogą jeszcze wyłączyć lub przełączyć na uruchamianie ręczne zbędne lub/i niebezpieczne usługi - Start | Administrative Tolls | Services. Szczegółowy opis usług sytemu Windows XP, którym można posłużyć się i w tym przypadku, zamieściliśmy w numerze PCWK PRO IT Security. Pozostałe komponenty - oprogramowanie antywirusowe, firewalle, aplikacje multimedialne etc. to już wyłącznie sprawa fantazji i stopnia zaawansowania użytkownika. Trzeba jednak szukać najnowszych produktów, najlepiej obsługujących Windows Server 2003, w ostateczności Windows XP. Należy się liczyć z tym, że w przeciwnym razie system odmówi instalacji oprogramowania lub sprzętu, względnie może mimo wszystko pracować niestabilnie.

Wydaje się, że praca z minimalnymi parametrami, szczególnie procesora, wymagałaby ze strony użytkownika przysłowiowej świętej cierpliwości. Rozsądnie jest przyjąć, że wymagania minimalne to właściwie zalecane.

We właściwej roli

Jednak Windows Server 2003 jest prawdziwym systemem serwerowym, a więc powiedzmy, co jeszcze ma do dyspozycji administrator.

Rozbudowane narzędzie Backup Utility umożliwia tworzenie kopii zapasowych we wszelkich możliwych wariantach, a więc od "zrzutu" całego komputera, poprzez pliki, napędy i dane sieciowe aż do skromnej kopii zapasowej systemu. Dostępna jest opcja Shadow Copy, czyli kopiowanie w tle. Z kolei opcja Automated System Recovery tworzy dwuczęściową kopię zapasową - dyskietkę systemową oraz zapasową kopię właściwych danych na innym nośniku. Dostępne są kopie normalne, dzienne, przyrostowe i różnicowe, a całość można łatwo zaplanować za pomocą wygodnego kalendarza. Tak rozbudowany system kopii zapasowych musiał, oczywiście, spowodować, że znikła wygodna, choć za skromna, jak na system serwerowy, opcja System Restore, znana z Windows XP.

Miłym dodatkiem jest funkcja tworzenia kopii zapasowej hasła systemu na dyskietce. Jest dostępna po naciśnięciu klawiszy [Ctrl Alt Del], następnie polecenia Change Password. Pozostaje tylko dobrze schować dyskietkę...

Na odwrotnym biegunie jest z kolei opcja Automatic Updates, dostępna na karcie Control Panel. Można zaprogramować automatyczne pobieranie i instalowanie dostępnych uaktualnień, również z uwzględnieniem harmonogramu i powiadamiania. To stoi w pewnej sprzeczności z restrykcyjną polityką bezpieczeństwa, skoro wiadomo na przykład, że niektóre poprawki Microsoftu bardzo spowolniały pracę systemu. Co dziwniejsze, funkcja jest domyślnie włączona po instalacji, choć na poziomie powiadamiania - instalację poprawek trzeba zatwierdzić.

Bardzo ważna z punktu widzenia bezpieczeństwa jest opcja Event Viewer, która bardzo dokładnie gromadzi wszelkie zdarzenia z zakresu pracy aplikacji, systemu i bezpieczeństwa. To doskonały sposób na wykrycie błędów i potencjalnych zagrożeń.

Niewątpliwie najważniejsze narzędzie administratora, jeśli chodzi o zarządzanie funkcjami serwerowymi, to zintegrowany interfejs Manage Your Server. To swoiste centrum nadzoru, kontroli i zarządzania. Uzupełnieniem tego centrum jest rozbudowany kreator wraz z systemem pomocy i podpowiedzi, który prowadzi użytkownika krok po kroku, informując o warunkach, jakie trzeba spełnić, by przypisać serwerowi daną rolę, oraz konsekwencjach, jakie się z tym wiążą.

Trzeba jednak zwrócić uwagę na pewną pułapkę, jaką stanowią rozbudowane kreatory, dostępne niemal w każdym miejscu systemu. Instalacja i konfiguracja jest wręcz przyjemna, to prawda, ale niesie ryzyko bezmyślnego poddania się sugestiom komputera. Na dłuższą metę grozi popadnięciem w rutynę, a to już niebezpieczne. Na szczęście, system zawiera też bardzo funkcjonalny wiersz poleceń, więc żaden wytrawny administrator, szczególnie z nawykami z systemów UNIX/Linux, nie powinien narzekać.

Podstawowe, "serwerowe" komponenty są pod względem swoich funkcji właściwie oczywiste, jednak zostały w mniejszym lub większym stopniu zmodernizowane, niektóre wręcz radykalnie. Dotyczy to szczególnie Internet Information Services 6.0, które w Windows Server 2003 zostały zaprojektowane praktycznie od nowa, ze szczególnym uwzględnieniem wydajności i bezpieczeństwa. To dobra wiadomość, bo stanowią podstawę obsługi stron WWW, serwera FTP, serwerów pocztowych (POP3 i SMTP) oraz

aplikacji sieciowych. Jednym z ważniejszych zastosowanych mechanizmów jest nowa wersja izolacji procesów. Nie wdając się w skomplikowane szczegóły, wystarczy powiedzieć, że efektem jest zwiększenie wydajności serwera, zmniejszenie zapotrzebowania na zasoby sprzętowe, zwiększenie bezpieczeństwa i zmniejszenie ryzyka zakłóceń w jego pracy. IIS 6.0 stanowią trzon wersji Windows Server 2003 Web Edition, przeznaczonej do wyspecjalizowanych serwerów webowych, ale są też standardowym składnikiem wszystkich wersji systemu.

Nowy, opcjonalny składnik systemu to usługi Windows Media Services 9 Series, mechanizmy dystrybucji danych strumieniowych zarówno w intranetach, jak i w Internecie. Możliwa jest zarówno transmisja na żywo, jak i rozsyłanie treści zarejestrowanych wcześniej, również przy użyciu programów kodujących firm trzecich. Windows Media Services wyposażono w wiele dodatkowych mechanizmów, przyśpieszających rozpoczęcie transmisji bez oczekiwania na zapełnienie bufora oraz zwiększających bezpieczeństwo i poprawiających stopień wykorzystania przepustowości sieci. Rozszerzalna o wtyczki architektura daje programistom praktycznie nieograniczone możliwości.

System plików i kompatybilność

Właściwy system plików Windows Server 2003 to NTFS, choć obsługiwany jest także system FAT 32. System NTFS oferuje, oczywiście, dodatkowe możliwości szyfrowania plików i folderów. Narzędzie zwane Program Compatibility Wizard pozwala wymusić uruchamianie programów zgodnych wstecz aż do Windows 95. Ciekawe, że administrator może bez ograniczeń zezwolić użytkownikom na stosowanie tego narzędzia.

Wspomnieliśmy już o kłopotach z kartami dźwiękowymi. W tym względzie prawdopodobnie niewiele się zmieni, ponieważ Microsoft uznaje sterowniki kart dźwiękowych za poważną przyczynę niestabilności systemu. Cóż, dostarczanie idealnego dźwięku przestrzennego niewątpliwie nie jest podstawowym zadaniem serwera.

Z pewnością mogą też być pewne kłopoty ze starszymi sterownikami różnych urządzeń. Perfekcjoniści powinni stosować sterowniki certyfikowane przez Microsoft, jedyne gwarantujące stabilność pracy systemu.

Warto dodać, że system jest już do pewnego stopnia kompatybilny "w górę", gdyż ma zaimplementowaną obsługę protokołu IPv6, praktycznie jeszcze niestosowanego - skala trudności związanych z przejściem na nowy protokół jest tak olbrzymia, że najprawdopodobniej dopiero poważny brak przestrzeni adresowej wymusi pierwszy krok. Zapewne potrwa to jeszcze kilka lat. System jest wyposażony w dwa ciekawe mechanizmy - 6to4 oraz Intra-site Automatic Tunnel Addressing Protocol (ISATAP), które umożliwiają opakowanie danych IPv6 w otoczkę IPv4 i przesłanie kanałem, który nie obsługuje nowego protokołu.

Zaleca się uaktualnienie Windows Server 2000 Microsoft za pomocą odpowiednich narzędzi, ale w przypadku NT 4.0 celowe jest raczej formatowanie dysków i instalacja systemu na czystej partycji. Uboczna korzyść to zwykle przyśpieszenie pracy napędów.

Warto też pamiętać, że nie da się uaktualnić systemu np. Windows 2000 Advanced Server do Windows Server 2003 Standard Edition. Windows Server 2003 Web Edition w ogóle nie ma odpowiednika w wersji 2000.

Podsumowanie

Przed premierą mówiło się, że Windows Server 2003 będzie po prostu przerośniętą wersją Windows Server 2000. Może tak by się stało, jednak zainicjowana przez Microsoft akcja Trustworthy Computing (Wiarygodne technologie komputerowe), która zresztą

spowodowała opóźnienie premiery, wymusiła najprawdopodobniej znaczne zmiany, jak choćby gruntowna modernizacja IIS 5.0 do wersji 6.0. Dbałość o bezpieczeństwo widoczna jest praktycznie na każdym kroku. System pracuje stabilnie, a rozbudowane funkcje kontroli i raportowania umożliwiają wychwycenie potencjalnych zagrożeń.

Bardzo rozbudowany jest system pomocy (Help and Support Center). Z jednej strony, dostępny jest obszerny katalog - zbiór dokumentów poświęconych różnym tematom, z drugiej zaś - system pomocy interaktywnej, który umożliwia uzyskanie jej zdalnie od innych użytkowników, specjalistów Microsoftu lub społeczności użytkowników systemu.

Podstawowa obsługa wydaje się wręcz zbyt komfortowa, jak na system serwerowy, który powinien przecież wymagać przynależności do kasty wtajemniczonych guru. To rzecz jasna pozory - gdy zagłębić się w funkcje, parametry, itd. żarty się kończą.

Trzeba będzie zaprzyjaźnić się z tym systemem na kilka lat. Następcy Windows XP doczekamy się zapewne około roku 2006, a już dzisia jsłyszymy, że wersja serwerowa pojawi się mniej więcej rok później. Biorąc jednak pod uwagę liczbę nowych technologii i rozwiązań, które mają się tam pojawić, jest to chyba wariant optymistyczny.

Czy to się sprzeda?

Jak wynika z informacji publikowanych przez sam Microsoft, Windows NT 4.0, liczący sobie już siedem lat, wciąż jeszcze obsługuje 35-40 procent serwerów windowsowych na świecie. Microsoft zachęca klientów do przejścia na Windows Server 2003 w dość oryginalny sposób, świadczący o specyficznym poczuciu humoru. Otóż przyznaje, że możliwości łatania dziur w NT 4 wyczerpały się - architektura systemu nie pozwala na więcej. Za to Windows Server 2000 spisuje się jeszcze nieźle.

Co więc powinien zrobić klient, skoro już trzy razy odraczano premierę nowego systemu, pierwotnie planowaną na październik 2001? Jak zwykle przy takich okazjach, wiele firm prędzej czy później przejdzie na nowy system, ale niemal na pewno odczekają minimum dwa lata, aż dojrzeje, a większość najpoważniejszych dziur zostanie załatana. Doświadczenia zgromadzone przy okazji premier innych systemów wyraźnie wskazują, że użytkownicy biznesowi rzadko decydują się na zakup nowego systemu przed ukazaniem się pierwszego service pack.