MINISTERSTWO EDUKACJI
i NAUKI

Tomasz Krupa

Administrowanie systemem operacyjnym Windows opartym na technologii NT
312[01].Z4.01

Poradnik dla ucznia

Wydawca
Instytut Technologii Eksploatacji – Państwowy Instytut Badawczy
Radom 2005

„Projekt współfinansowany ze środków Europejskiego Funduszu Społecznego”

Recenzenci:

mgr inż. Ireneusz Przybyłowicz

mgr inż. Grzegorz Smigielski

Opracowanie redakcyjne:
mgr inż. Katarzyna Maćkowska

Konsultacja:
dr inż. Bożena Zając

Korekta:
mgr inż. Tomasz Sułkowski

Poradnik stanowi obudowę dydaktyczną programu jednostki modułowej 312[01].Z4.01 Administrowanie systemem operacyjnym Windows opartym na technologii NT zawartego w modułowym programie nauczania dla zawodu technik informatyk.

Wydawca
Instytut Technologii Eksploatacji – Państwowy Instytut Badawczy, Radom 2005

SPIS TREŚCI

1. WPROWADZENIE

Podręcznik ten będzie Ci pomocny w uzyskaniu umiejętności niezbędnych do pracy w zawodzie technika informatyka. Podręcznik obejmuje zagadnienia dotyczące jednostki modułowej zajmującej się administrowaniem systemem operacyjnym Windows opartym na technologii NT.

W podręczniku zamieszczono:

- wykaz literatury, z jakiej możesz korzystać podczas nauki,
- wykaz umiejętności, jakie powinieneś mieć przed przystąpieniem do nauki w wybranym przez Ciebie zawodzie,
- wykaz umiejętności, jakie ukształtujesz podczas pracy z tym podręcznikiem,
- materiał nauczania,
- zestawy pytań kontrolnych,
- ćwiczenia, które mają na celu wykształcenie Twoich umiejętności praktycznych,
- sprawdzian postępów.

Materiał nauczania obejmuje zagadnienia dotyczące pracy w środowisku sieciowym, zarządzania systemem, tworzenia kont użytkowników, udostępniania plików i folderów, bezpieczeństwa systemu.

2. WYMAGANIA WSTĘPNE

Przystępując do realizacji tej jednostki modułowej powinieneś umieć:

- poszukiwać informacje w różnych źródłach,
- selekcjonować, porządkować i przechowywać informacje,
- dokumentować, notować i selekcjonować informacje,
- posługiwać się podstawowymi pojęciami z zakresu dokumentacji technicznej, a także bezpieczeństwa i higieny pracy.

3. CELE KSZTAŁCENIA

W wyniku realizacji tej jednostki modułowej powinieneś umieć:

- zaplanować i utworzyć konta użytkowników,
- skonfigurować profile i polisy użytkowników,
- zaplanować skrypty logowania dla użytkowników,
- zaplanować i utworzyć grupy lokalne i globalne,
- zaplanować wykorzystanie grup wbudowanych,
- zastosować programy do zarządzania kontami użytkowników,
- zastosować programy do zarządzania kontrolerami domeny i hierarchiczną strukturą Active Directory,
- zaplanować udostępnianie folderów,
- zaplanować i przypisać uprawnienia NTFS,
- zastosować programy do zarządzania uprawnieniami,
- zainstalować drukarki lokalne i sieciowe,
- zastosować programy do inspekcji zasobów i zdarzeń,
- zaplanować archiwizację i odtwarzanie danych z taśmy,
- zainstalować system Windows, w tym workstation i serwer,
- skonfigurować Windows dla osiągnięcia zadanej efektywności,
- zainstalować wybrane urządzenia i programy w Windows,
- skonfigurować system Windows do współpracy z innymi systemami operacyjnymi,
- zastosować rejestry do konfiguracji Windows,
- zastosować skrypty do automatyzacji pracy w środowisku Windows,
- zastosować przepisy bezpieczeństwa i higieny pracy.

4. MATERIAŁ NAUCZANIA

4.1. Windows NT

4.1.1. Materiał nauczania

Windows NT to rodzina 32- i 64-bitowych systemów operacyjnych firmy Microsoft, przeznaczonych do zastosowań profesjonalnych.

System Windows z technologią NT działa wielozadaniowo i z wywłaszczeniem. Daje się przenosić na różne platformy procesorów.

Podstawowe zalety systemu to:

- przenośność,
- bezpieczeństwo,
- wieloprocesorowość,
- rozszerzalność,
- adaptacje międzynarodowe,
- deklarowana zgodność z aplikacjami MS-DOS.

W systemie NT zastosowano architekturę mikrojądrową, dzięki czemu daną część systemu można ulepszać bez zbytniego naruszania jego innych części. System NT od wersji 2000 jest wielodostępowy (wcześniejsze wersje nie - do wersji 4).

Systemy operacyjne NT można podzielić na dwie wersje w zależności od przeznaczenia komputera, na którym jest instalowana: stacja robocza Windows NT oraz serwer Windows NT. Obie korzystają z tego samego jądra i kodu systemu operacyjnego, lecz oprogramowanie serwera NT jest skonfigurowane do pracy z aplikacjami typu klient–serwer i może działać jako serwer aplikacji w sieciach lokalnych Microsoft. Wersja 4.0 serwera NT zawiera oprogramowani internetowe serwera WWW oraz interfejs użytkownika systemu Windows 95 . W 1996 r. sprzedano więcej licencji serwera NT niż wszystkich licencji różnych komercyjnych wersji systemu Unix. Najnowsza wersja stacji roboczej NT to Windows XP, a wersja serwerowa to Windows Server 2003.

Powszechnie podaje się, że literki NT w nazwie Windows NT oznaczają New Technology. Prawda jest trochę inna. Pod koniec 1988 r. Microsoft rozpoczynał pracę nad nowym systemem Windows. Miała ona działać na procesorze RISC i860. Microsoft używał emulatora tego procesora. Emulator ten miał nazwę kodową N-Ten. I stąd wzięła się nazwa Windows NT. Później marketingowcy przemianowali skrót NT na New Technology.

System plików

Podstawowa cecha wyróżniającą systemy w wersji NT jest system plików NTFS **(NT File System)**

Podstawowymi parametrami opisującymi dyski twarde są sektory i jednostki alokacji.

Dane na dysku zapisywane są w sektorach. Każdy sektor ma rozmiar 512 bajtów. Na dysku o pojemności 100 GB utworzonych jest około 210 milionów sektorów. Kontrola tak dużej liczby sektorów może być dla systemu plików zadaniem niewykonalnym. Z tego powodu sektory zostały połączone w grupy zwane jednostkami alokacji (ang. clusters).

Rozmiar jednostki alokacji jest równy liczbie sektorów w tej jednostce. Jeśli plik nie zapełni całkowicie jednej lub kilku jednostek alokacji, to pozostała część powierzchni dyskowej przypisana niezapełnionej jednostce alokacji nie jest już wykorzystywana. Najefektywniejsze jest utworzenie jednostek alokacji o rozmiarze jednego sektora.

Stopień wykorzystania dysku maleje wraz ze wzrostem rozmiaru jednostki alokacji. Z drugiej strony zwiększenie jednostki alokacji poprawia wydajność pracy dysku twardego.

Z systemami plików związane są następujące pojęcia:

- Sektory i jednostki alokacji. Jest to podstawowy podział danych na dysku. Sektory są określone poprzez geometrię dysku i ustalone przez producenta najczęściej jako 512-

bajtowe. Jednostka alokacji jest to logiczne połączenie sektorów w większą strukturę, co poprawia wydajność systemu plików.

- Partycje i woluminy. Logiczny podział dysku lub zestawu dysków tworzący granice dla systemu plików. W poprzednim rozdziale dokonano rozróżnienia na partycję i wolumin, ponieważ jest to istotne dla działania Menedżera Dysków Logicznych (Logical Disk Manager – LDM), jednak na poziomie abstrakcji reprezentowanym przez system plików, pojęcia te są równoznaczne.
- Sektor rozruchowy (Boot Sector). Pierwszy sektor partycji zawierający informacje o systemie plików oraz część programu ładującego.
- Blok parametrów BIOS (BIOS Parameter Block – BPB). Fragment sektora rozruchowego zawierający informacje właściwe systemowi plików na danej partycji.

Podstawową funkcją systemu plików jest lokalizacja plików, czyli katalogowanie miejsca przechowywania na dysku. System DOS wprowadził tablicę alokacji plików – FAT, która określała strukturę plików i ich rozmieszczenie na dysku. Tablicę FAT można sobie wyobrazić jako mapę dysku wskazującą, które jednostki alokacji są w użyciu i w której jednostce alokacji zapisany jest dany plik.

Starsze systemy operacyjne stosowały systemy plików FAT 16 i FAT 32.

System plików FAT 16 wykorzystuje adresowanie 16-bitowe, oznacza to, że możliwe jest zaadresowanie maksymalnie 65 535 jednostek alokacji. Rozmiar jednostki alokacji jest stały i zostaje określony na podstawie wielkości dysku podczas jego formatowania.

System FAT 16 charakteryzuje się następującymi parametrami:

- maksymalny rozmiar partycji dysku mniejszy niż 2 GB,
- kompatybilność ze starszymi systemami operacyjnymi firmy Microsoft,
- maksymalny rozmiar jednostki alokacji mniejszy niż 64 KB.

W systemie Windows XP również można zastosować system plików FAT 16. Wielkość dysku w tym przypadku może przekroczyć 2 GB, jednak systemy DOS i Windows 95 nie będą miały do niego dostępu.

Wraz ze wzrostem wielkości dysków pojawiła się konieczność zastosowania systemu plików pozwalających na ich obsługę. Wprowadzono system plików FAT 32, który mógł być zastosowany już przy systemie Windows 95 OSR2. Ten system plików wykorzystuje trzydziestodwubitową tablicę FAT powiększając maksymalny rozmiar dysku.

Teoretycznie maksymalny rozmiaru dysku FAT 32 wynosi 8 TB, praktyczne maksymalny rozmiar dysku FAT 32 dla Windows XP wynosi 32 GB. Umożliwia to zapis całej tablicy FAT w pamięci podręcznej i poprawę wydajność dysku twardego.

System FAT 32 cechuje:

- maksymalny rozmiar partycji dysku mniejszy niż 32 GB,
- mniejszy rozmiar tworzonych jednostek alokacji,
- rozmiar jednostki alokacji większy niż 4 KB i mniejszy niż 32 KB.

NTFS to zdecydowanie inne rozwiązanie.

System plików NTFS jest podstawą bezpieczeństwa Windows NT. Partycja NTFS rozpoczyna się sektorem inicjującym. Nie jest to, jednak, pojedynczy sektor, ale może być to nawet 16 pierwszych sektorów (zależnie od potrzeb systemu).

Po sektorze inicjującym występuje nadrzędna tabela plików (MFT – Master File Table), czyli po prostu indeks plików systemowych. W aktualnej wersji systemu NT na pliki systemowe wymienione w MFT składają się:

- kopia MFT,
- plik logów,
- informacje o wolumenie (w tym etykieta wolumenu i numer wersji NTFS),
- tablica definicji atrybutów (nazwy, numery identyfikacyjne, objaśnienia),
- katalog główny,

- mapa bitowa klastrów (opis zajętości partycji),
- kopia Boot sektora partycji,
- tabela uszkodzonych klastrów,
- tabela konwersji małych liter na duże odpowiedniki Unicode.

Oprócz zaawansowanego, systemu bezpieczeństwa jedną z ważnych cech NTFS jest kompresja „w locie". W odróżnieniu od rozwiązań typu DriveSpace (dla VFAT) możemy kompresować nie tylko całe wolumeny, ale nawet w standardowo niekompresowanym wolumenie pojedyncze pliki lub katalogi.

To, czy dany element ma być kompresowany ustala się za pomocą klasycznego ustalania atrybutów (w ten sam sposób jak ustala się atrybut „tylko – do – odczytu" czy też „ukryty"). Jedynym ograniczeniem kompresji NTFS jest to, że rozmiar klastra nie może być większy niż 4 KB. W systemie plików NT zastosowano adresowanie 64-bitowe. Teoretycznie umożliwia to utworzenie dysku o wielkości około 16 eksabajtów, ale w praktyce stosuje się ograniczenie maksymalnego rozmiaru woluminu do 2 TB.

System NTFS cechuje:

- maksymalny rozmiar partycji dysku przekraczający 32 GB,
- odporność na błędy – system jest w stanie wykryć uszkodzone sektory, przenieść dane w inny obszar dysku i oznaczyć te sektory jako uszkodzone, co spowoduje, że nie będą dłużej używane,
- zwiększone bezpieczeństwo – dzięki nadawaniu praw do plików i folderów oraz dzięki możliwości zaszyfrowania danych przechowywanych na dyskach z systemem plików NTFS, informacje są chronione przed dostępem niepowołanych osób,
- zarządzanie wolnym miejscem – na dyskach z systemem plików NTFS można zakładać limity ograniczające maksymalną ilość przechowywanych przez danego użytkownika danych,
- lepsze wykorzystanie przestrzeni dysku – jednostki alokacji w systemie NTFS są do ośmiu razy mniejsze niż w przypadku systemu FAT 32 (w zależności od wielkości woluminu).

NTFS szczyci się następującymi nowymi, ważnymi funkcjami (w porównaniu ze swoim poprzednikiem):

- obsługuje długie nazwy plików (do 255 znaków),
- szyfrowanie – NTFS jest w stanie automatycznie szyfrować i deszyfrować dane plików podczas odczytu i zapisu na dysk,
- przydziały dyskowe (disk quotas) – administratorzy mogą ograniczyć ilość przestrzeni dyskowej, którą mogą zająć użytkownicy, dla poszczególnych użytkowników i woluminów. Trzy poziomy limitów to: brak ograniczenia, ostrzeżenie i ograniczenie,
- rozproszone śledzenie łączy – pozwala na zachowanie skrótów przy przenoszeniu plików z jednego woluminu na drugi lub do innego komputera,
- reparse point i węzły montowania woluminów – jednym z zastosowań reparse point jest funkcjonalność montowania woluminów, pozwalająca przekierować odczyt i zapis danych z foldera do innego woluminu lub dysku fizycznego,
- rozszerzanie woluminów bez restartu – daje możliwość dodawania nieprzydzielonej przestrzeni dyskowej bez konieczności restartu komputera,
- właściciele obiektów NTFS mogą udostępnić innemu użytkownikowi obiekt, przyznając mu odpowiednie uprawnienia.

NTFS jest rozwiązaniem zalecanym dla systemów Windows od wersji NT 4.0 Workstation/Server. Ten system plików daje następujące zalety w porównaniu z systemem plików FAT:

- zabezpieczenia plików,

– kompresja i szyfrowanie dysku,
– lepsza skalowalność dla dużych dysków.

Tylko systemy Windows od wersji NT są w stanie bezpośrednio czytać dane z lokalnych dysków NTFS. Każdy system operacyjny może czytać z woluminów NTFS przy dostępie przez sieć. Istnieją programy, które umożliwiają odczyt i zapis partycji NTFS w systemach Windows 9x. Są to jednak dodatkowe aplikacje, nieobecne w systemie. Windows NT obsługuje NTFS w wersji 4, nowsze wersje Windows NTFS w wersji 5.

Tab.1. Wielkości klastrów w różnych systemach plików

Rozmiar partycji		FAT16	FAT32	NTFS
0 - 32	MB	0,5 kB	-	0,5 kB
33 - 64	MB	1 kB	-	0,5 kB
65 - 127	MB	2 kB	-	0,5 kB
128 - 255	MB	4 kB	-	0,5 kB
256 - 511	MB	8 kB	-	0,5 kB
512 - 1023	MB	16 kB	4 kB	1 kB
1 - 2	GB	32 kB	4 kB	2 kB
2 - 4	GB	64 kB	4 kB	4 kB
4 - 8	GB	-	4 kB	8 kB
8 - 16	GB	-	8 kB	16 kB
16 - 32	GB	-	16 kB	32 kB
pow 32	GB	-	32 kB	64 kB

4.1.2. Pytania sprawdzające

Odpowiadając na pytania sprawdzisz, czy jesteś przygotowany do wykonania ćwiczeń.

1. Ilobitowym systemem jest Windows rodziny NT?
2. Jakie systemy plików stosowane są w Windows NT?
3. Co to jest MFT?
4. Jakie ograniczenia ma FAT 32?
5. Co to jest BOOT Sektor?

4.1.3. Ćwiczenia

Ćwiczenie 1

Załóż na dysku jedną partycję z systemem plików FAT 32 – sformatuj partycję.

Sposób wykonania ćwiczenia

Aby wykonać ćwiczenie powinieneś:

1) uruchomić komputer,
2) ustawić odpowiednią kolejność bootowania w BIOS'ie,
3) uruchomić komputer ponownie korzystając z dyskietki systemowej zawierającej programy narzędziowe „fdisk" i „format",
4) uruchomić program „fdisk",
5) sprawdzić konfigurację dysku (istniejące partycje – w razie potrzeby usunąć istniejące partycje),

6) założyć na dysku jedną partycję zajmującą całą dostępną pojemność dysku,
7) nadać partycji atrybut „aktywna”,
8) wyjść z programu „fdisk” i zresetować komputer w celu zapamiętania zmian,
9) uruchomić komputer ponownie przy pomocy dyskietki,
10) sformatować dysk,
11) nadać partycji etykietę „system”.

Wyposażenie stanowiska pracy:
- komputery z dyskami przeznaczonymi do formatowania,
- dyskietka systemowa z programami narzędziowymi „fdisk” i „format”.

Ćwiczenie 2

Załóż na dysku trzy partycje z systemem plików FAT 32 – sformatuj wszystkie partycje.

Sposób wykonania ćwiczenia

Aby wykonać ćwiczenie powinieneś:
1) uruchomić komputer,
2) ustawić odpowiednią kolejność bootowania w BIOS’ie,
3) uruchomić komputer ponownie korzystając z dyskietki systemowej zawierającej programy narzędziowe „fdisk” i „format”,
4) uruchomić program „fdisk”,
5) sprawdzić konfigurację dysku (istniejące partycje – w razie potrzeby usunąć istniejące partycje),
6) założyć dwie nowe partycje, każda po 50% pojemności dysku,
7) założyć na drugiej partycji dwa dyski logiczne, każdy po 50% pojemności drugiej partycji,
8) nadać pierwszej partycji atrybut „aktywna”,
9) wyjść z programu „fdisk” i zresetować komputer w celu zapamiętania zmian,
10) uruchomić komputer ponownie przy pomocy dyskietki,
11) sformatować wszystkie partycje dysku,
12) nadać partycji pierwszej etykietę „system”, drugiej „dane”, trzeciej „rozrywka”.

Wyposażenie stanowiska pracy:
- komputery z dyskami przeznaczonymi do formatowania,
- dyskietka systemowa z programami narzędziowymi „fdisk” i „format”.

Ćwiczenie 3

Zainstaluj w systemie nowy wolumin z systemem plików NTFS.

Sposób wykonania ćwiczenia

Aby wykonać ćwiczenie powinieneś:
1) uruchomić komputer z systemem operacyjnym Windows XP,
2) zalogować się do systemu z prawami administratora,
3) uruchomić konsolę zarządzania komputerem,
4) wybrać w konsoli zarządzania opcję „Zarządzanie dyskami”,

5) wskazać dysk przeznaczony do formatowania,
6) utworzyć nową pojedynczą partycję na całej dostępnej powierzchni dysku,
7) sformatować dysk z zastosowaniem systemu plików NTFS.

Wyposażenie stanowiska pracy:
- komputer z systemem Windows XP,
- podłączony dysk przeznaczony do formatowania.

Ćwiczenie 4

Zainstaluj w systemie nowy wolumin z mieszanym systemem plików NTFS/FAT32.

Sposób wykonania ćwiczenia

Aby wykonać ćwiczenie powinieneś:
1) uruchomić komputer,
2) zalogować się do systemu z prawami administratora,
3) uruchomić konsolę zarządzania komputerem,
4) wybrać w konsoli zarządzania opcję „Zarządzanie dyskami”,
5) wskazać dysk przeznaczony do formatowania,
6) utworzyć na dysku dwie partycje, każda po 50% powierzchni dysku, na drugiej partycji utworzyć dwa dyski logiczne, każdy po 50% pojemności tej partycji,
7) sformatować stworzone partycje:
   - pierwszą z systemem plików NTFS,
   - drugą z systemem plików FAT32,
   - trzecią z systemem plików NTFS z opcją szybkiego formatowania i kompresji,
8) nadać partycji pierwszej etykietę „system”, drugiej „dane”, trzeciej „rozrywka”.

Wyposażenie stanowiska pracy:
- komputer z systemem Windows XP,
- podłączony dysk przeznaczony do formatowania.

4.1.4. Sprawdzian postępów

Czy potrafisz?

		Tak	Nie
1)	wymienić zalety systemu opartego na technologii NT?	☐	☐
2)	wymienić jakie ograniczenia ma system plików FAT32?	☐	☐
3)	wymienić jakie zalety ma system plików NTFS?	☐	☐
4)	wymienić jakie zalety ma kompresja w systemie plików NTFS?	☐	☐
5)	powiedzieć, której wersji NTFS używa Windows XP?	☐	☐

4.2. Windows 2003 Server

4.2.1. Materiał nauczania

System Windows Server 2003 Enterprise Edition jest przeznaczony dla średnich i dużych firm.

System Windows Server 2003 Enterprise Edition współpracuje z najnowszymi modelami sprzętu opartymi na platformach 32- i 64-bitowych. Takie rozwiązanie zapewnia optymalną elastyczność i skalowalność. Kolejną zaletą jest bardzo wydajna infrastruktura zoptymalizowana pod kątem wszystkich aplikacji i usług kluczowych.

Zabezpieczenia C2

Bezpieczeństwo systemu – Certyfikacja Common Criteria.

Pojęcie bezpiecznego systemu operacyjnego zostało sformułowane już około 15 lat temu, gdy ogłoszono amerykańską Orange Book, czyli kryteria TCSEC . Kryteria te zostały opracowane właśnie dla ochrony informacji niejawnych (w USA classified), a w szczególności w celu ułatwienia instytucjom rządowym i wojskowym wyboru systemów operacyjnych i aplikacji (na przykład systemów zarządzania bazami danych). Zdecydowano, że takie systemy powinny być oceniane zarówno pod kątem wbudowanych funkcji jak i wiarygodności sposobu ich opracowania (pewności). Podobne podejście, ale bardziej elastyczne zaproponowano w europejskich kryteriach ITSEC.

W zakresie zapewnienia pewności systemu kryteria TCSEC rozróżniają następujące elementy:

- właściwa architektura systemu (np. ukrywanie przetwarzanych danych, wydzielenie jądra TCB),
- spójność systemu,
- testy zabezpieczeń,
- weryfikacja modelu systemu,
- analiza ukrytych kanałów,
- wiarygodne zarządzanie (na przykład rozdzielenie ról administratora),
- wiarygodny powrót do normalnego stanu,
- wiarygodna dystrybucja,
- zarządzanie konfiguracją.

Kryteria TCSEC stanowią, że w systemie operacyjnym powinny być zaimplementowane następujące funkcje zabezpieczające:

- identyfikacja i uwierzytelnienia,
- kontrola dostępu (sterowanie dostępem) w tym,
- DAC – uznaniowa kontrola dostępu polegająca na przyznawaniu dostępu do katalogów, plików oraz uzyskiwaniu uprawnień od ich dotychczasowego użytkownika,
- MAC – narzucona kontrola dostępu polegająca na przypisywaniu etykiet wszystkim elementom aktywnym (użytkownicy, programy) i pasywnym (katalogi, urządzenia, pliki, dane, okna, rekordy) oraz uzyskiwaniu uprawnień do dostępu jedynie w ramach określonej polityki bezpieczeństwa,
- rozliczalności i audytu,
- ponownego wykorzystywanie obiektów.

Konieczne jest również zaimplementowanie funkcji poufności opartej na szyfrach, funkcjach skrótu, podpisach cyfrowych i generatorach liczb pseudolosowych.

Kryteria TCSEC definiują siedem klas bezpieczeństwa D, C1, C2, B1, B2, B3 i A1 włączając do nich różne z powyższych elementów funkcjonalnych i zapewniających zaufanie zgodnie z ogólną zasadą, że klasa wyższa zawiera elementy niższej oraz dodatkowe elementy podwyższające poziom bezpieczeństwa. Z kolei kryteria ITSEC definiują pięć kompatybilnych z powyższymi klas funkcjonalności F-C1, F-C2, F-B1, F-B2, F-B3.

Rzecz jasna pojęcie bezpiecznego systemu operacyjnego jest szersze niż tylko jego klasa bezpieczeństwa. System musi być jeszcze prawidłowo skonfigurowany i poprawnie eksploatowany. Prawidłowa konfiguracja systemu opiera się między innymi na wymuszaniu na użytkownikach określonych działań, takich jak:

- zmiana haseł co określony czas,
- stosowanie haseł o złożonej postaci (odpornych na atak słownikowy),
- stosowanie wygaszaczy ekranu, zabezpieczanych hasłem,
- blokowanie nieużywanych kont,
- ograniczanie wyjść z systemu (na przykład blokada stacji dysków elastycznych FDD),
- stosowanie systemu plików NTFS zamiast FAT (NTFS w systemach Windows z technologią NT),
- wyłączanie niebezpiecznych usług (niezabezpieczony Telnet, ftp, rlogin, rsh, rcp w UNIX).

Godnym uwagi jest fakt, że jeśli system uzyskał certyfikat, poświadczający posiadanie klasy bezpieczeństwa według TCSEC lub klasy funkcjonalności według ITSEC, to sprawozdanie badawcze powinno i zazwyczaj zawiera odpowiednie zalecenia oraz zastrzeżenia dotyczące bezpiecznej konfiguracji.

Większość instalacji komputerowych posiada jeden lub więcej systemów programów użytkowych, które mogą umożliwiać obchodzenie zabezpieczeń w systemie i aplikacjach. Istotne jest, aby korzystanie z takich systemowych programów użytkowych było ograniczane i ściśle kontrolowane. Tam, gdzie jest to możliwe powinno się stosować następujące regulacje (zabezpieczenia):

- ochrona systemowych programów użytkowych przy użyciu haseł,
- oddzielanie systemowych programów użytkowych od oprogramowania aplikacyjnego,
- ograniczanie korzystania z systemowych programów użytkowych do minimalnej liczby zaufanych, uprawnionych użytkowników,
- autoryzowanie wykorzystywania ad hoc innych systemowych programów użytkowych,
- ograniczanie dostępności systemowych programów użytkowych, na przykład jedynie na czas trwania uprawnionych zmian,
- zapisywanie w dziennikach zdarzeń wszystkich przypadków wykorzystywania systemowych programów użytkowych,
- definiowanie i dokumentowanie poziomów uprawnień do korzystania z systemowych programów użytkowych,
- usuwanie zbędnych programów użytkowych i oprogramowania.

System operacyjny jako podstawowa platforma zarządzania zasobami informatycznymi musi być narzędziem ochrony informacji niejawnych dla administratora systemu i innych osób za te ochronę odpowiedzialnych (pion ochrony, w szczególności inspektor bezpieczeństwa TI, przełożeni administratora). Narzędzie to musi i powinno:

- posiadać klasę bezpieczeństwa, która potwierdza jego odpowiedniość w zakresie funkcjonalnym i zakresie pewności (uzasadnienia zaufania),
- być właściwie skonfigurowane,
- być poprawnie eksploatowane zgodnie z treścią dokumentu procedurami bezpiecznej eksploatacji.

Klasa C2

Systemy posiadające klasę C2 wymuszają odpowiedzialność użytkownika za wykonywane przez siebie operacje sieciowe, stosując procedury logowania, wykrywając zdarzenia związane z bezpieczeństwem oraz izolując poszczególne zasoby sieciowe.

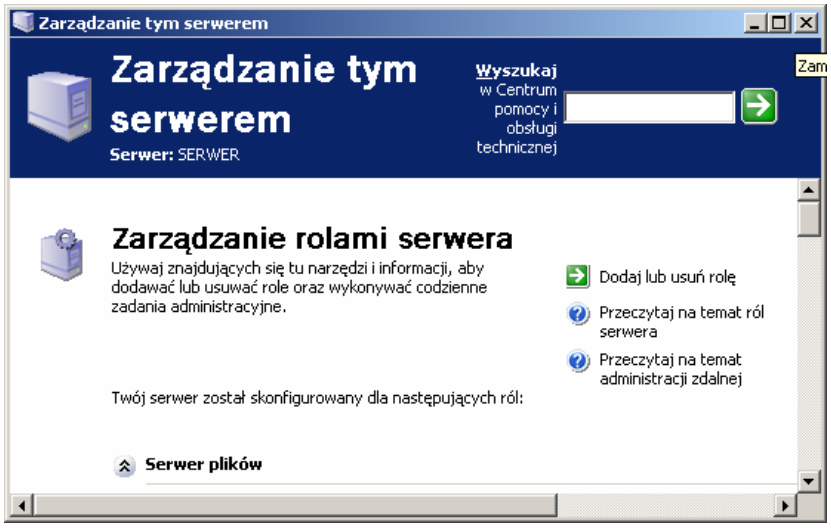
Wymagania dla systemów klasy C2 (muszą spełniać także wymagania dla klasy C1):

- określony i kontrolowany dostęp nazwanych użytkowników do nazwanych obiektów (zasada klasy C1),
- system identyfikujący i sprawdzający hasła, decydujący o przyznaniu użytkownikom dostępu do informacji w sieci komputerowej (zasada klasy C1),
- można decydować o dostępie grup i indywidualnych użytkowników,
- mechanizm kontrolowania dostępu ogranicza replikację praw dostępu,
- uznaniowy mechanizm kontrolowania dostępu domyślnie lub na podstawie jawnego żądania użytkownika uniemożliwia nieautoryzowany dostęp do obiektów,
- mechanizm kontrolowania dostępu może dopuszczać lub ograniczać dostęp użytkowników do określonych obiektów,
- system identyfikowania może rozpoznać każdego użytkownika, który się zaloguje do sieci,
- system operacyjny wykonuje wszystkie operacje zlecane przez poszczególnych użytkowników zgodnie z nadanymi im prawami,
- sieć może śledzić dostęp do obiektów w sieci.

Systemy Windows oparte na technologii NT poddają się z sukcesem certyfikacji poziomu zabezpieczeń C2.

Instalacja Windows 2003 Server

Instalacja Windows 2003 Server nie nastręcza, podobnie jak inne zaawansowane systemy Windows (na przykład XP) większych kłopotów. W przypadku większości zestawów sprzętowych instalator Windows 2003 Server, rozpoznaje urządzenia zainstalowane w komputerze (karty grafiki, karty sieciowe, kontrolery USB i IDEE, IEE 1394...). Urządzenia, które nie zostały rozpoznane podczas instalacji można doinstalować w późniejszym czasie. Inaczej rzecz się ma z systemami OEM, czyli do sprzedaży tylko z nowymi komputerami, jak na przykład SBS (Small Bussines Serwer, oparty na Windows Server), który w swoich kolejnych wersjach dedykowany jest na konkretną platformę sprzętową. Może się okazać, że na komputerze, który posiadamy instalacja systemu w wersji OEM będzie praktycznie niemożliwa. Sprzęt zgodny ze specyfikacją Microsoft wpisywany jest na listę HCL (Hardware Compatibility List). W przypadku pełnej wersji systemu praktycznie jedyne pytania dotyczą nazwy serwera, nazwy domeny. Po zainstalowaniu systemu pozostaje nam doinstalowanie ról serwera. Instalacja ról serwera pozostawiona została administratorowi ze względu na różne potrzeby użytkowników (nie wszyscy potrzebują kompletu ról).



Rys. 1. Dodawanie ról serwera

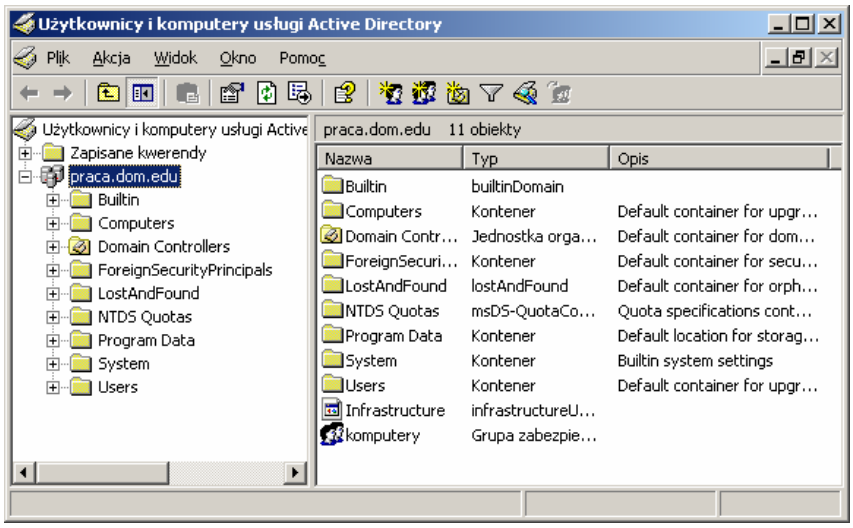
Active Directory

Active Directory to usługi katalogowe dla Windows 2003 Server. Katalog przechowuje informacje o obiektach dostępnych w sieci (drukarkach, komputerach, serwerach bazodanowych, oprogramowaniu). Administrator w postaci Active Directory otrzymuje narzędzie pozwalające na wprowadzenie porządku i określonej, hierarchicznej struktury w sieci.

Zabezpieczenia są zintegrowane z usługą Active Directory za pośrednictwem mechanizmu uwierzytelniania i kontroli dostępu do obiektów w katalogu. Administratorzy mogą zarządzać danymi i organizacją za pośrednictwem sieci. Autoryzowani użytkownicy sieci mogą uzyskać dostęp do zasobów znajdujących się w dowolnych lokalizacjach w sieci.

Usługa Active Directory oferuje chroniony magazyn informacji dotyczących kont użytkowników i grup, korzystając z mechanizmu kontroli dostępu do obiektów i weryfikacji danych identyfikacyjnych użytkowników. Usługa Active Directory przechowuje nie tylko poświadczenia użytkowników, ale również informacje związane z kontrolą dostępu, dlatego użytkownicy logujący się w sieci są uwierzytelniani i autoryzowani w zakresie dostępu do zasobów systemowych. Na przykład podczas logowania użytkownika w sieci system zabezpieczeń uwierzytelnia użytkownika na podstawie informacji przechowywanych w usłudze Active Directory. Następnie, jeżeli użytkownik usiłuje uzyskać dostęp do usługi w sieci, system sprawdza właściwości zdefiniowane na arbitralnej liście kontroli dostępu (DACL) dla danej usługi.

Administratorzy korzystający z usługi Active Directory mogą tworzyć konta grup, a więc z większą efektywnością zarządzać zabezpieczeniami systemu. Na przykład administrator może dostosować właściwości pliku, aby zezwolić wszystkim użytkownikom w grupie na odczytywanie danego pliku. Dostęp do obiektów w usłudze Active Directory jest więc oparty na członkostwie grupy.



Rys. 2. Konsola Active Directory

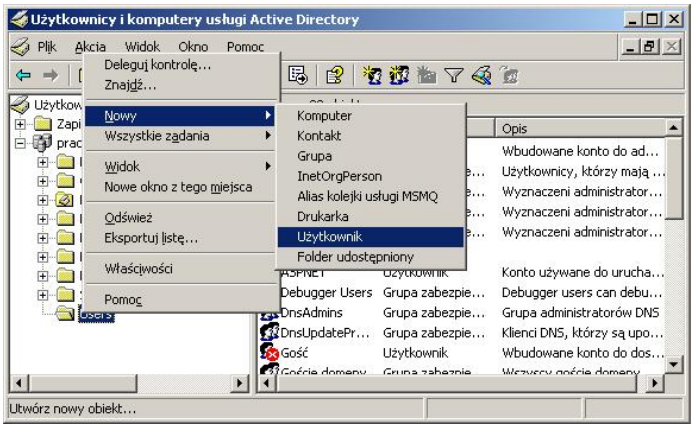
Kreator ułatwia proces konfigurowania usługi Active Directory i oferuje wstępnie zdefiniowane ustawienia dla określonych ról serwera, umożliwiające ujednolicenie metod wstępnego rozmieszczania serwerów przez administratorów.

Katalog Active Directory może działać zarówno na 64- jak i 32-bitowej wersji Windows 2003 Server. Obie edycje bez problemu mogą współpracować ze sobą.

Tworzenie kont użytkowników

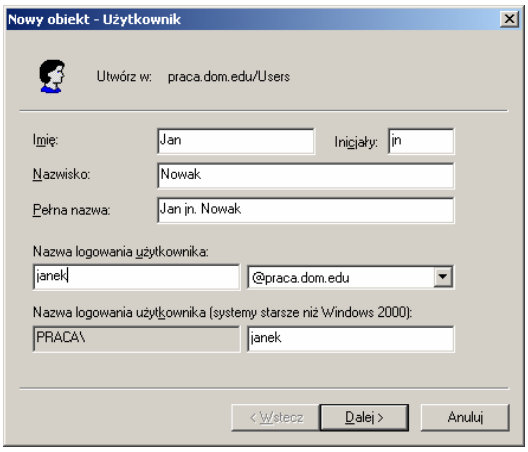
Aby założyć nowe konto użytkownika musimy uruchomić z menu programy: Narzędzia administracyjne/Użytkownicy i komputery usługi Active Directory.

Po kliknięciu w domenę i uaktywnieniu prawym przyciskiem myszy na folderze „Users" menu dialogowego, można dokonać wyboru polecenia: „Nowy/Użytkownik".



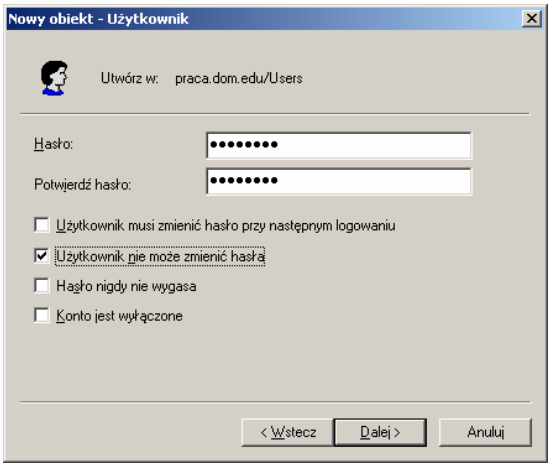
Rys. 3. Zakładanie kont użytkowników

W kolejnym kroku będziemy musieli podać pewne informacje dotyczące nowego użytkownika.



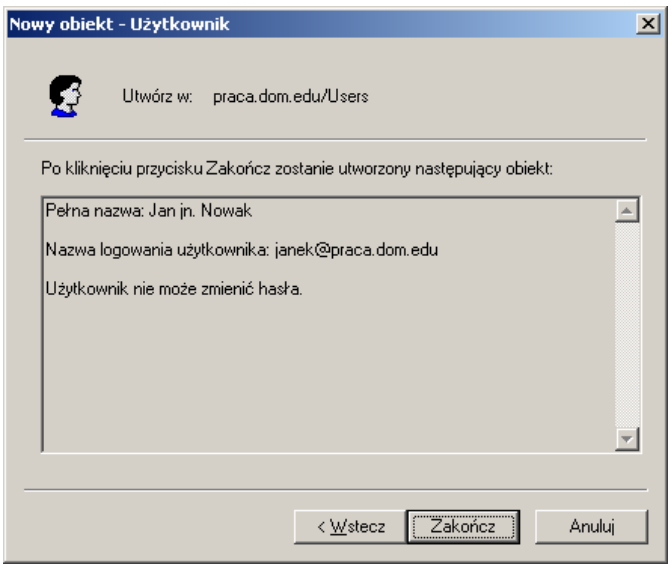
Rys. 4. Konsola tworzenia konta użytkownika

Ostatnim etapem tworzenia konta użytkownika jest określenie jego hasła i warunków podstawowych takich jak okres wygaśnięcia hasła, konieczność zmiany hasła przy pierwszym logowaniu. Możemy również w tym miejscu zablokować konto.



Rys. 5. Ustalanie hasła użytkownika

W końcowej fazie system poinformuje nas o utworzeniu konta.



Rys. 6. Potwierdzenie założenia konta użytkownika

Tworzenie grup użytkowników

Użytkownicy o podobnych uprawnieniach ustanowionych przez administratora, są przydzielani do odpowiednich grup. Grupę może stanowić jeden lub kilku użytkowników. Istnieją trzy rodzaje grup: lokalne, globalne i uniwersalne.

Lokalne grupy użytkowników mają prawa i uprawnienia lokalnie na komputerach. Grupy globalne są dostępne we własnej domenie i domenach ufających. Grupy globalne mogą zawierać się w grupach lokalnych. Grup uniwersalnych używa się w celu nadania uprawnień w dowolnym miejscu w drzewie lub lesie domen. Mogą one zawierać inne grupy uniwersalne, grupy globalne i pojedynczych użytkowników z dowolnych domen.

Windows 2003 posiada wstępnie zdefiniowane grypy użytkowników.

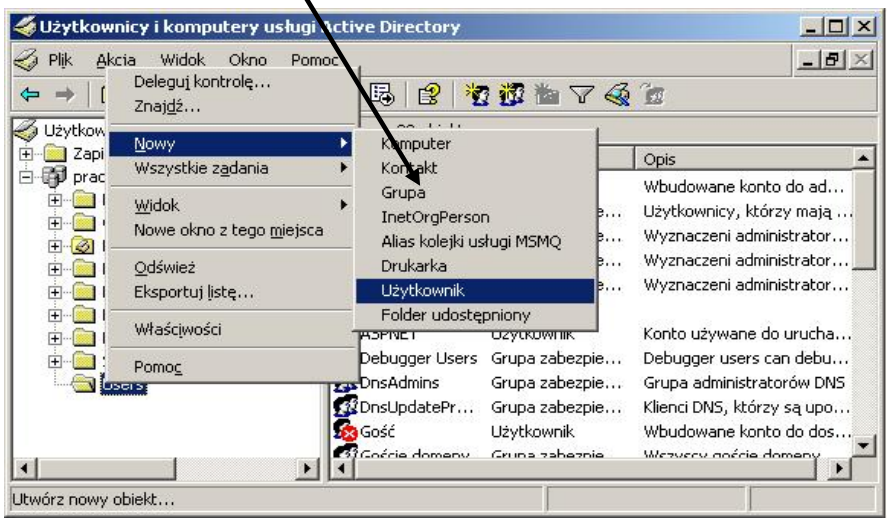
Tab.2. Wstępnie zdefiniowane grupy użytkowników

Grupy lokalne	**Grupy globalne**
Administratorzy	Administratorzy domen
Operatorzy kont	Goście domen
Operatorzy kopii zapasowych	Użytkownicy domen
Goście	Wszyscy
Użytkownicy zaawansowani	
Operatorzy wydruku	
Operatorzy serwerów	
Użytkownicy	

Dodatkowo system posiada kilka grup specjalnych, które nie posiadają żadnych członków. Dotyczą one dowolnego konta korzystającego w określony sposób z komputera. Należą do nich:

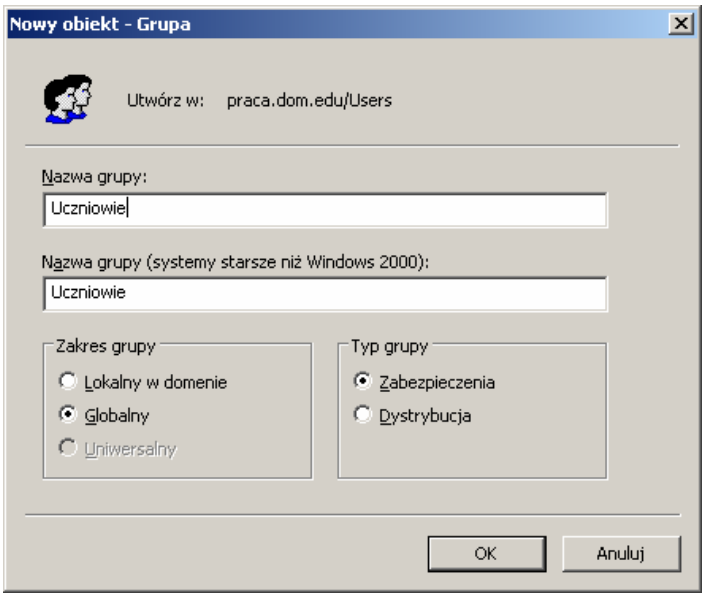
- użytkownicy anonimowi,
- użytkownicy uwierzytelnieni,
- dialup.

Tworzenie grupy rozpoczynamy dokładnie tak samo jak tworzenie użytkownika od uruchomienia panelu Użytkownicy i komputery usługi Active Directory z tym, że należy wybrać opcję Nowy/Grupa



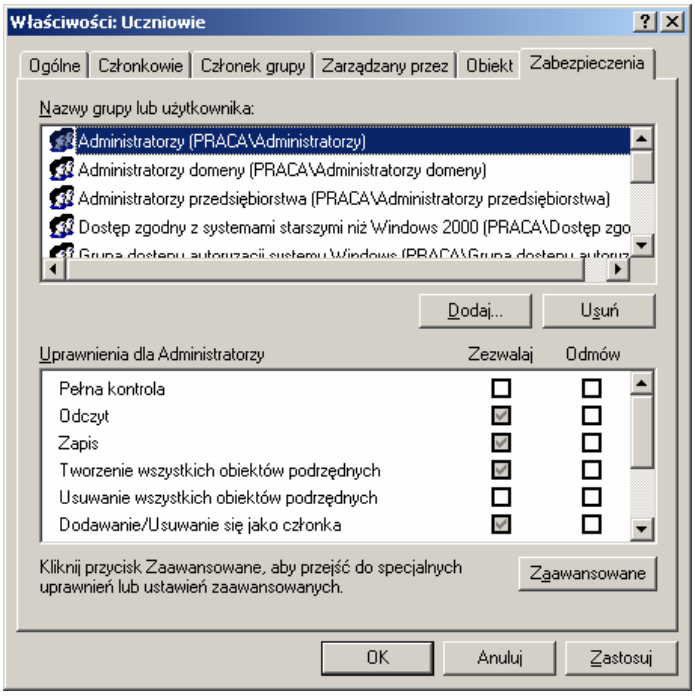
Rys. 7. Zakładanie konta grupy

Dalsze postępowanie polega na wpisaniu nazwy grupy oraz określeniu jej zakresu i typu.



Rys. 8. Konsola zakładania konta grupy

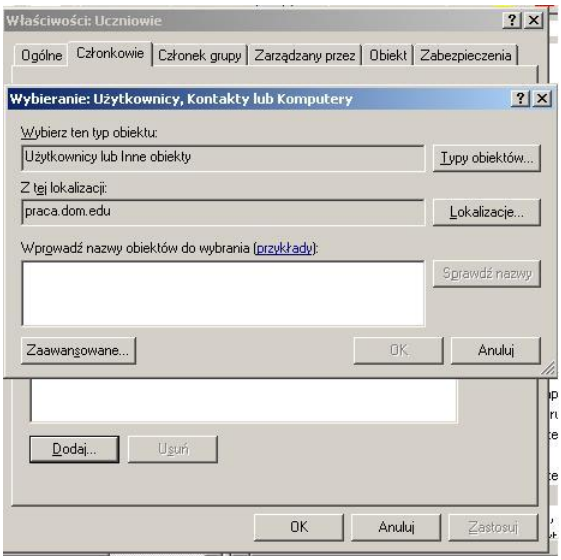
Zabezpieczenia grupy ustawiamy wywołując odpowiedni panel w oknie „użytkownicy i komputery usługi Active Directory". Rozwijamy Menu Akcja/Właściwości (lub klikając na grupie prawym przyciskiem myszy). W tym panelu możemy ustawić zasady zabezpieczeń grupy.



Rys. 9. Konsola ustawiania zabezpieczeń grupy

Przydzielanie użytkowników do grup

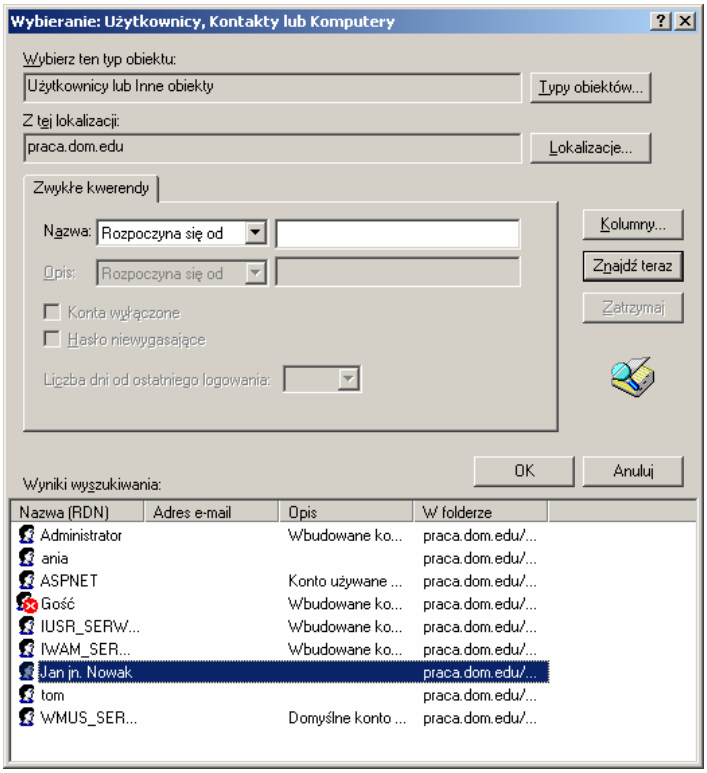
Kolejnym krokiem w organizacji jest przydzielenie użytkowników do grup. Przydzielanie użytkowników do tworzonej grupy odbywa się również za pośrednictwem usługi Active Directory – Menu Akcja/Właściwości. W drugiej zakładce „Członkowie" możemy wybrać użytkowników, których dołączymy do danej grupy.



Rys. 10. Konsola przydzielania użytkownika do grupy

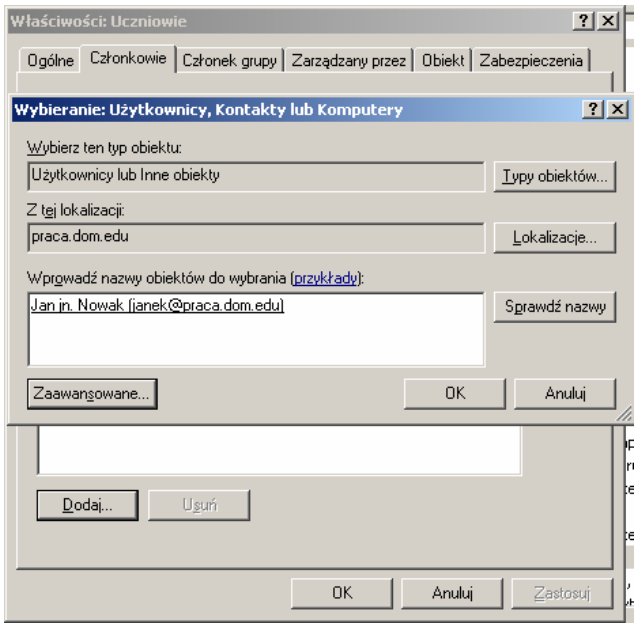
Wybierając przycisk „Dodaj" uruchamiamy kolejny panel umożliwiający odnalezienie użytkowników, których chcemy dołączyć do grupy.

Wybieramy kolejno zaawansowane/znajdź teraz. Następnie odszukujemy użytkownika którego chcemy przydzielić do grupy i wybór potwierdzamy przyciskiem „OK".



Rys. 11. Konsola wyszukiwanie użytkownika

Kolejne „OK" powoduje przypisanie Użytkownika.



Rys. 12. Widok konsoli z wybranym użytkownikiem

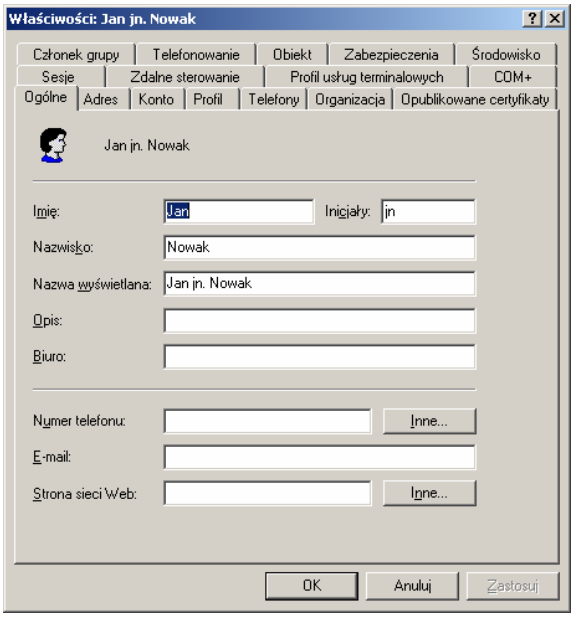
Zarządzanie właściwościami kont użytkowników

Po utworzeniu i przydzieleniu użytkownika do grupy mamy nadal możliwość modyfikacji jego konta. Aby to zrobić musimy wybrać z menu programy: Narzędzia administracyjne/Użytkownicy i komputery usługi Active Directory i znaleźć użytkownika. Po kliknięciu prawym przyciskiem myszy w wybranego użytkownika i z menu podręcznego wybieramy polecenie „Właściwości".

W tym panelu możemy dokonać odpowiednich modyfikacji w kolejnych zakładkach okna.

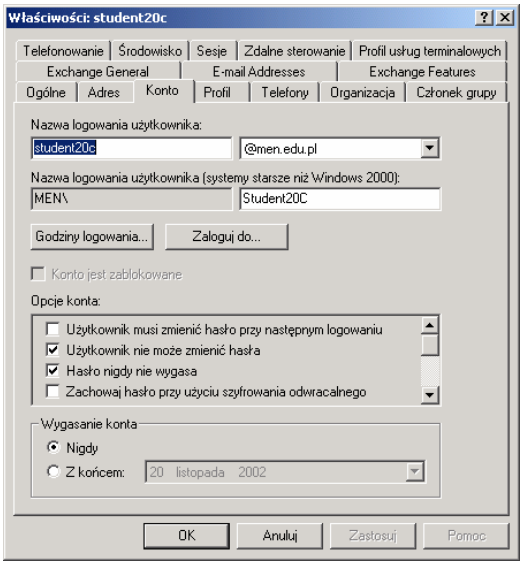
Ogólne – główne dane o użytkowniku.

Adres – dane dotyczące adresu użytkownika.



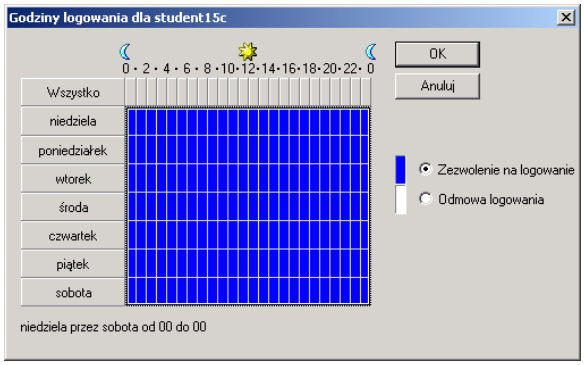
Rys. 13. Konsola zarządzania właściwościami użytkownika

Konto – zawiera informacje na temat wymagań, dotyczących hasła i konta użytkownika.



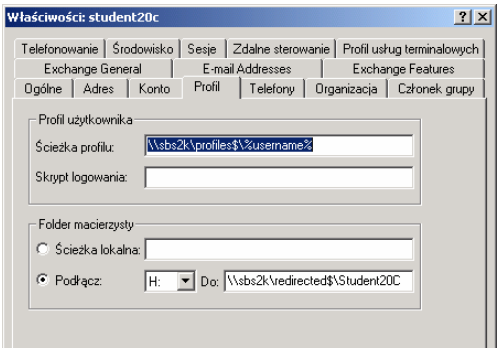
Rys. 14. Ustawianie właściwości konta

Przycisk godziny logowania pozwala na określenie, w których godzinach dany użytkownik może logować się do sieci.



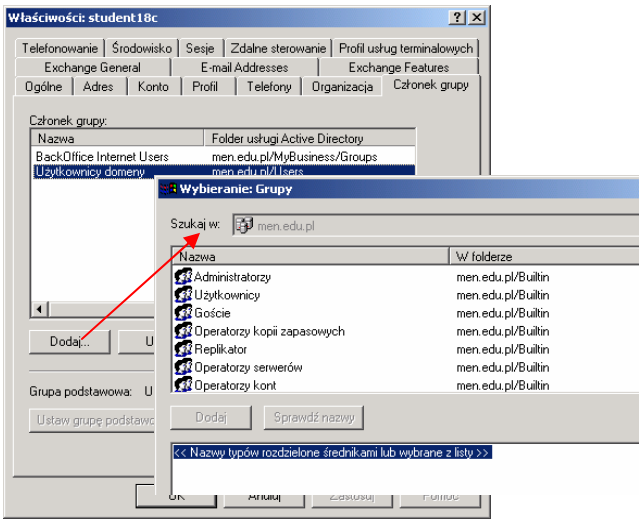
Rys. 15. Konsola ustalania godzin logowania

Profil – zawiera informacje o ścieżce dojścia do profilu, skryptu logowania, folderu macierzystego.



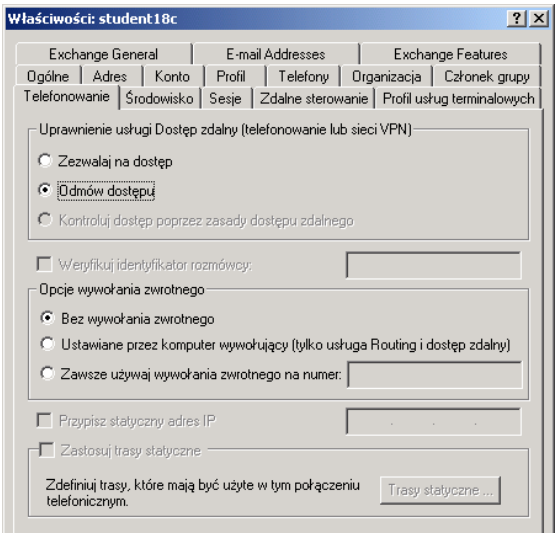
Rys. 16. Konsola ustawiania parametrów profilu

Członek grupy – pozwala na przydzielenie użytkownika do danej grupy. Poprzez przycisk Dodaj można uaktywnić okno z listą istniejących grup.



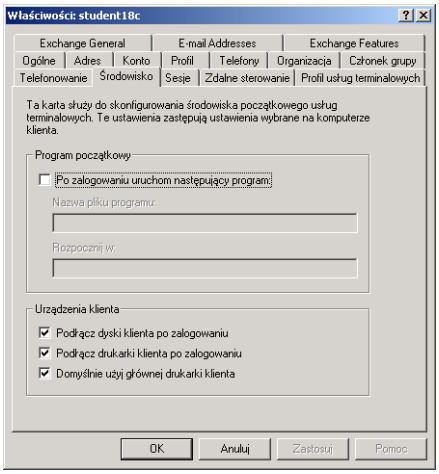
Rys. 17. Konsola przydzielania użytkownika do grupy

Telefonowanie – zakładka ta umożliwia przydzielenie uprawnienia zdalnego logowania się poprzez modem.



Rys. 18. Konsola konfiguracji zdalnego logowania użytkownika

Środowisko – zakładka służy do skonfigurowania środowiska początkowego usług terminalowych dla danego użytkownika.



Rys. 19. Konsola ustalania środowiska użytkownika

Profile

Profil jest to kolekcja ustawień środowiska użytkownika, do których zmiany użytkownik ma pełne prawo.

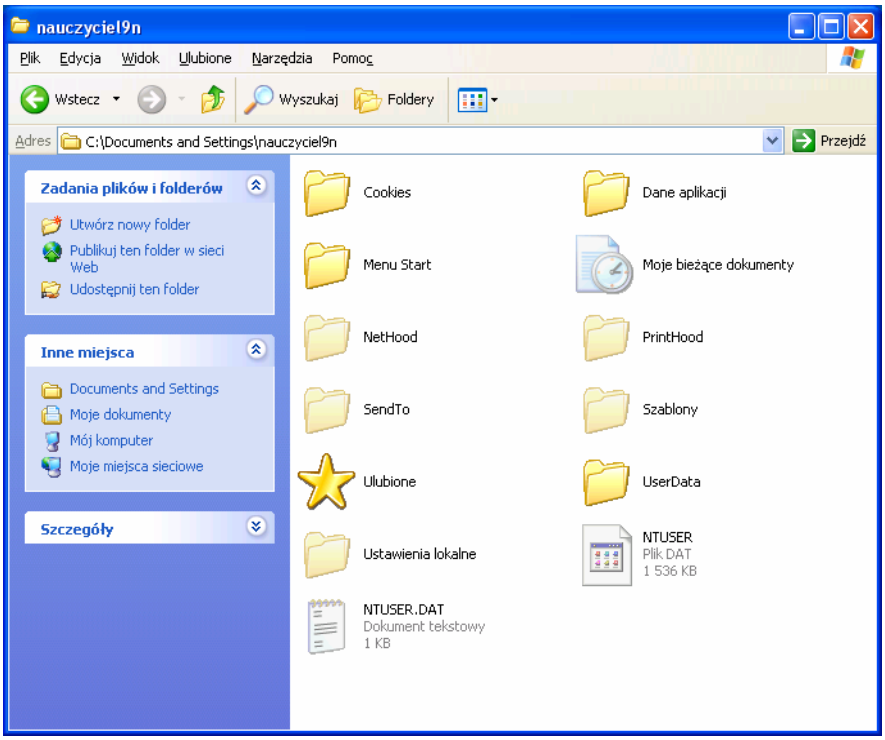
Na komputerach z systemami operacyjnymi Windows Server 2003 profile użytkownika umożliwiają automatyczne tworzenie i zachowywanie ustawień pulpitu dotyczących środowiska pracy każdego użytkownika na komputerze lokalnym. Profil użytkownika jest utworzony dla każdego użytkownika, gdy loguje się on na danym komputerze po raz pierwszy.

Typy profilów użytkownika:

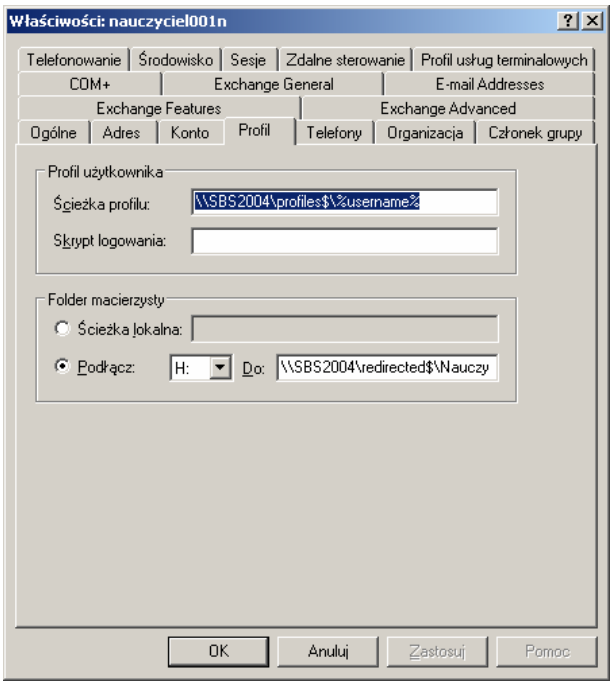
- **lokalny** (local user profile) – jest tworzony podczas pierwszego logowania do komputera i przechowywany na lokalnym dysku twardym komputera. Każda zmiana lokalnego profilu użytkownika dotyczy jedynie komputera, na którym została wprowadzona,
- **mobilny** (roaming user profile) – jest tworzony przez administratora systemu i przechowywany na serwerze. Ten profil jest dostępny podczas każdego logowania na dowolnym komputerze w sieci. Zmiany mobilnego profilu użytkownika są wprowadzane na serwerze. Zmian może dokonywać użytkownik,
- **obowiązkowy** (mandatory user profile) – to profil mobilny, który może określać konkretne ustawienia dla pojedynczych użytkowników i całych grup. Tylko administratorzy systemu mogą wprowadzać zmiany w obowiązkowym profilu użytkownika,
- **tymczasowy** (temporary user profile) – jest wydawany, jeśli błąd uniemożliwia załadowanie profilu użytkownika. Tymczasowe profile są usuwane pod koniec każdej sesji. Zmiany wprowadzone przez użytkownika w ustawieniach pulpitu i w plikach są tracone po wylogowaniu się użytkownika.

Dodając foldery i pliki do profilu „Użytkownik domyślny" (Default User), można skonfigurować profil standardowy i uczynić go częścią plików pulpitu, które stosuje się w całej firmie. Na przykład można dodać skróty do firmowej witryny internetowej lub aplikacji standardowych, takich jak system rejestracji czasu pracy. Dodatki do profilu Użytkownik domyślny (Default User) są dołączane do każdego nowego profilu.

W przypadku firmowych sieci komputerowych, użytkownik może nie mieć możliwości kontrolowania zawartości swojego profilu. Jest on narzucony przez administratora takiej sieci. Jeżeli jednak komputer nie jest podłączony do sieci lub też administrator sieci nie wprowadza żadnych ograniczeń, można bez ograniczeń zmieniać swój profil. Domyślnie system Windows przechowuje wszystkie informacje o profilach użytkowników w folderze o nazwie Documents and Settings (w polskiej wersji systemu Windows również), zlokalizowanym na tym samym dysku, na którym zainstalowany jest system operacyjny (profil lokalny). Każdy użytkownik ma w nim swój podkatalog, którego nazwa jest taka sama jak identyfikator użytkownika.



Rys. 20. Zawartość profilu w katalogu Documents and Settings, właściwości profilu lokalnego użytkownika



Rys. 21. Ścieżka profilu we właściwościach użytkownika

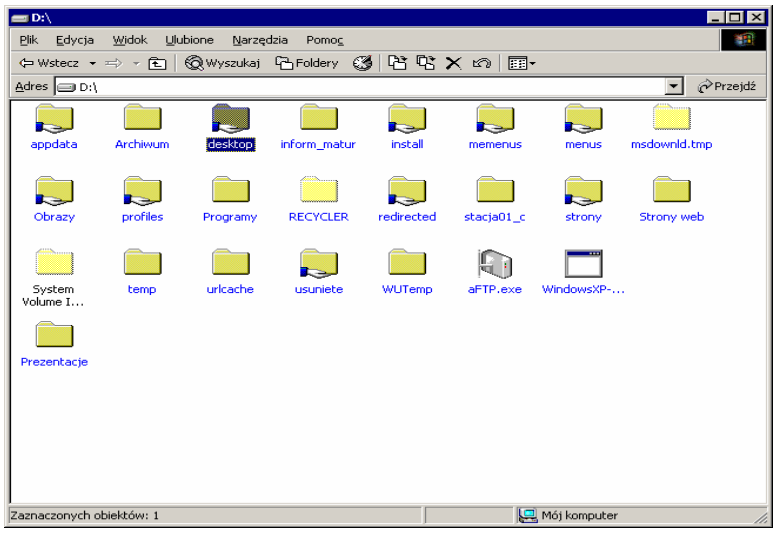
Budowa profilu

Profil użytkownika systemu Windows 2003 zawiera takie składniki klasycznego profilu Eksploratora, jak:

- Pulpit (Desktop),
- Menu startowe (Start Menu),
- znaczniki kontekstu klienta tak zwane „ciasteczka" (Cookies),
- różne otoczenia (Hoods),
- Dane aplikacji (Application Data). Folder ten zawiera pliki konfiguracyjne, właściwe dla danego użytkownika, aplikacji, które mogą wędrować razem z użytkownikiem. Na przykład w tym folderze są zapisane certyfikaty szyfrowania i pliki identyfikacyjne szyfrowania systemu plików (Encrypting File System),
- Ustawienia lokalne (Local Settings). Folder ten zawiera pliki konfiguracyjne dla aplikacji stacjonarnych, właściwe dla danego użytkownika. Na przykład ustawienia internetowe są przechowywane w tym folderze,
- Moje dokumenty (My Documents). Jest to nowa lokalizacja klasycznego folderu. W systemie Windows 2003 Server folder Moje dokumenty (My Documents) umieszczony jest w profilu użytkownika, więc może być włączony do usługi Przekierowania folderu (Folder Redirection) i profilu wędrującego (roaming profiles),
- NTUSER.DAT. Jest to gałąź użytkownika w Rejestrze i jest ładowana do Rejestru, kiedy użytkownik zaloguje się, stając się poddrzewem HKEY_Current_User,
- USRCLASS.DAT. Jest to dodatkowa gałąź użytkownika w Rejestrze zapisana w folderze \Dokumenty i ustawienia\<nazwa_użytkownika>\Ustawienia lokalne\Dane Aplikacji\Microsoft\Windows (\Documents and Setings\<username>\Local Settings\Application Data\Microsoft\Windows). Przechowuje pozycje użytkownika w Rejestrze dotyczące aplikacji stacjonarnych,
- NTUSER.INI. Jest to nowy plik w systemie Windows 2003 Server. Umieszczone w nim są ustawienia INI dla usług terminalowych (Terminal Services), pochodzące z poprzednich wersji systemu Windows. Zawiera również listę folderów wyłączonych z profilu wędrującego (roaming profiles),
- NTUSER.POL. Ten plik działa jako lokalny bufor (local cache) założeń grupowych (group policies) danego użytkownika, które są pobierane z kontrolera domeny podczas logowania się użytkownika do tej domeny,
- Szablony (Templates). W tym katalogu zapisane są szablony różnych aplikacji, takich jak AmiPro, Lotus 1–2–3 i starszych wersji Microsoft Office.

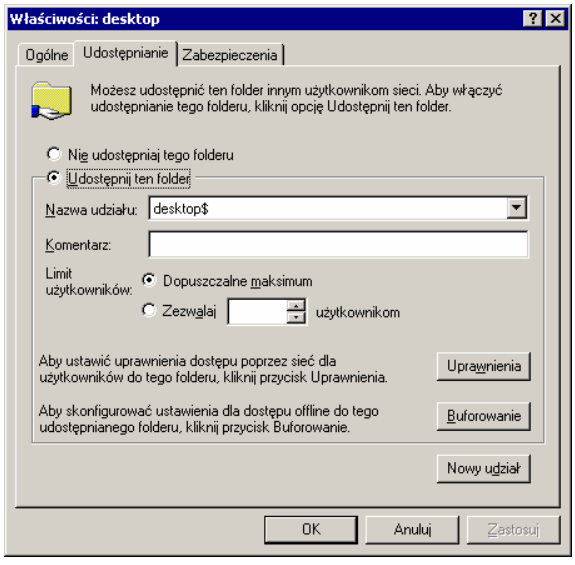
Aby utworzyć mobilny profil użytkownika należy:

- utworzyć na serwerze folder, w którym będą przechowywane profile użytkowników. Będzie to folder najwyższego poziomu zawierający wszystkie profile poszczególnych użytkowników,



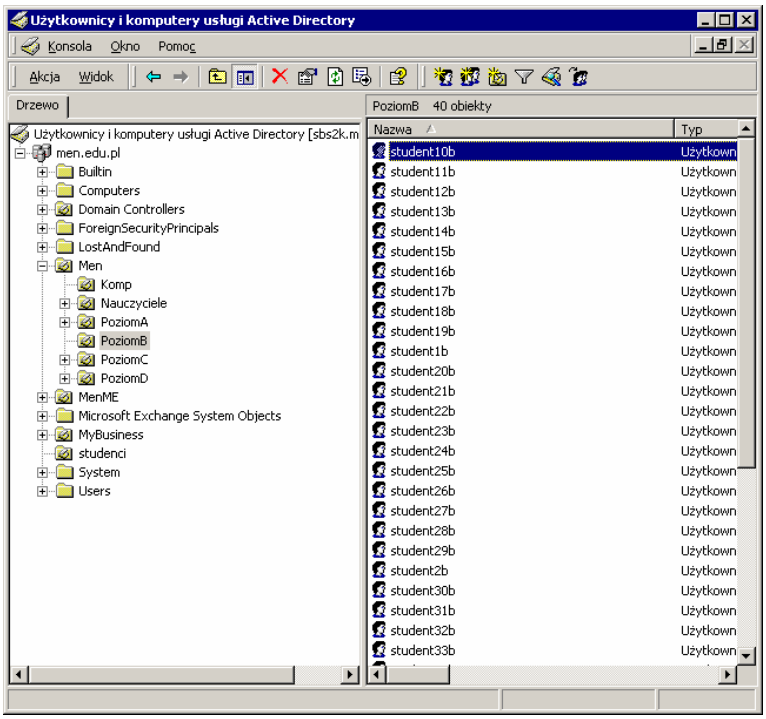
Rys. 22. Folder zawierający profile

- skonfigurować ten folder jako folder udostępniony i nadać wszystkim użytkownikom uprawnienia Pełna kontrola,



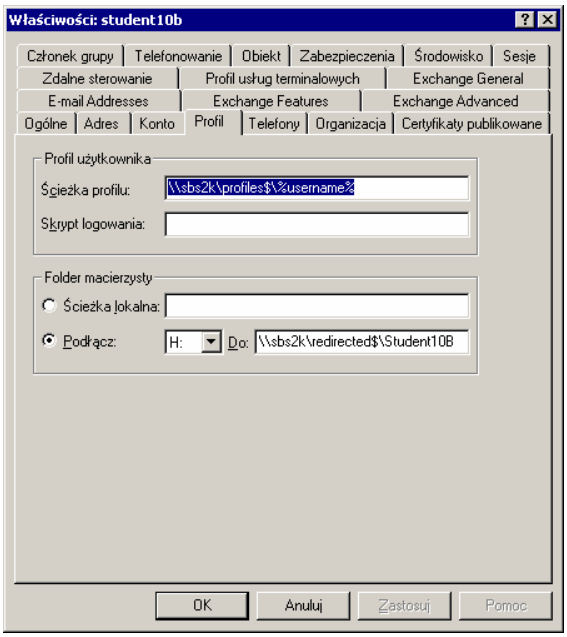
Rys. 23. Udostępnianie folderu użytkownikom

- otworzyć kontener Użytkownicy i komputery usługi Active Directory, a następnie przejść do obiektu określonego użytkownika,



Rys. 24. Active Directory – konto użytkownika

- kliknąć prawym przyciskiem myszy nazwę użytkownika, a następnie kliknąć polecenie Właściwości,
- kliknąć kartę Profil. W polu Ścieżka profilu wpisz ścieżkę do folderu udostępnionego, w którym będzie przechowywany profil użytkownika. Dla przykładowego użytkownika o nazwie sieciowej „student10b" wpisanie ścieżki \\udział_sieciowy\profile\%username% spowoduje utworzenie katalogu o nazwie „student10b" w folderze Profile na serwerze, na którym są przechowywane profile użytkowników.



Rys. 25. Ścieżka profilu we właściwościach użytkownika

Aby utworzyć obowiązkowy profil użytkownika:

- otwórz przystawkę Użytkownicy i komputery usługi Active Directory,
- w okienku szczegółów kliknij prawym przyciskiem myszy odpowiednie konto użytkownika, a następnie kliknij polecenie Właściwości,
- użytkownicy i komputery usługi Active Directory/odpowiedniadomena/odpowiedni kontener (na przykład Użytkownicy)/odpowiednie konto użytkownika,
- kliknij kartę Profil,
- w polu Ścieżka profilu wpisz ścieżkę, dodając rozszerzenie nazwy pliku .man.

Konsola GPMC – Group Policy Managment Console

Konsola GPMC została opracowana w celu uproszczenia zarządzania zasadami grupy przez udostępnienie centralnego punktu zarządzania podstawowymi aspektami zasad grupy. Konsola GPMC oferuje wszystkie funkcje niezbędne do zarządzania zasadami grupy.

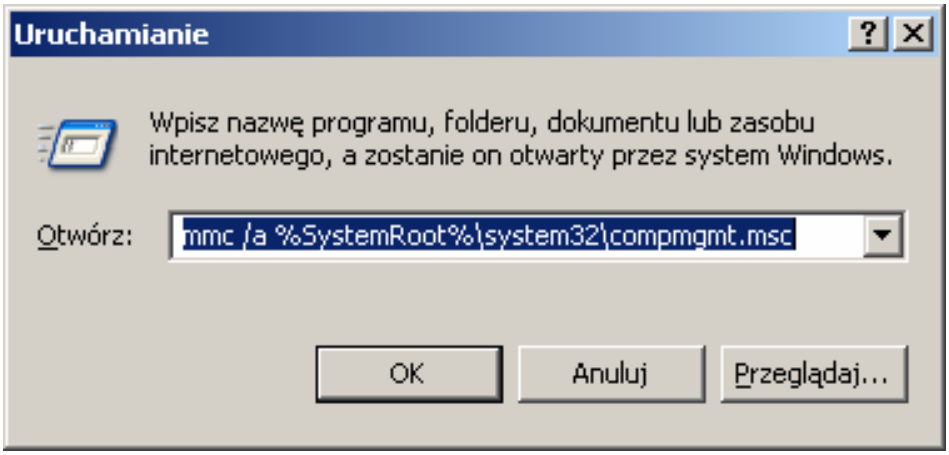
Przed opracowaniem konsoli GPMC administratorzy byli zmuszeni do korzystania z kilku narzędzi opracowanych przez firmę Microsoft, służących do zarządzania zasadami grupy. Konsola GPMC integruje aktualne funkcje związane z zasadami grupy, uwzględnione w narzędziach tego typu, w formie pojedynczej, ujednoliconej konsoli.

Konsolę GPMC należy doinstalować. Konsola jest do pobrania z witryny Microsoftu. Znaleźć ją można pod adresem http://www.microsoft.com/downloads. Po pobraniu z witryny pliku „gpmc.msi" rozpoczynamy instalację konsoli. Instalator prosi nas jedynie o przeczytanie i potwierdzenie zgody na warunki licencji.

W systemie Windows 2003 Server istnieje kilka konsol (MMC Microsoft Management Konsole) służących do administrowania systemem. Działaniem, które uprości nam dalsza pracę jest stworzenie globalnej konsoli zarządzającej, zawierającej wszystkie niezbędne przystawki. Konsole tą zbudujemy na bazie konsoli „Zarządzanie komputerem". Konsola może zawierać różne funkcje w zależności od potrzeb administratora:

- Net Framework 1.1 Configuration,
- dzienniki wydajności i alerty,
- GPMC,
- konfiguracja i analiza zabezpieczeń,
- menedżer autoryzacji,
- monitor sieci bezprzewodowej,
- pulpity zdalne,
- rozproszony system plików (DFS),
- szablony zabezpieczeń,
- trzy przystawki do zarządzania Active Direktory,
- wynikowy zestaw zasad.

Do utworzenia tej konsoli użyjemy polecenia:
„mmc /a %SystemRoot%\system32\compmgmt.msc" wpisanego w linii poleceń. Polecenie to powoduje uruchomienie konsoli zarządzania komputerem w trybie edycji.



Rys. 26. Konsola uruchamiania

4.2.2. Pytania sprawdzające

Odpowiadając na pytania sprawdzisz, czy jesteś przygotowany do wykonania ćwiczeń.

1) Co oznacza skrót C2?
2) W jakim celu stworzono kryteria TCSEC?
3) Ile klas bezpieczeństwa określają kryteria TCSEC?
4) Jakie parametry decydują o bezpieczeństwie systemu?
5) Jakie warunki musi spełnić system aby był uznany za bezpieczny?
6) Co to jest Active Directory?
7) Jakie informacje przechowuje Active Directory?
8) Jakie zadania można wykonywać korzystając z Active Directory?
9) Do czego służy konsola GPMC?
10) Jaką rolę spełnia Globalna Konsola MMC?

4.2.3. Ćwiczenia

Ćwiczenie 1

Zainstaluj system Windows 2003 Server.

Sposób wykonania ćwiczenia

Aby wykonać ćwiczenie powinieneś:

1) uruchomić komputer,
2) ustawić odpowiednią kolejność bootowania w BIOS'ie,
3) umieścić płytę z wersją instalacyjną Windows 2003 Server w napędzie CD,
4) wykonać restart komputera,
5) zainstalować Windows 2003 Server na dysku komputera,
6) zainstalować potrzebne role serwera,

Wyposażenie stanowiska pracy:
- komputer,
- dysk instalacyjny Windows 2003 Server
- poradnik dla ucznia.

Ćwiczenie 2

Utwórz nową grupę użytkowników „pracownicy".

Sposób wykonania ćwiczenia

Aby wykonać ćwiczenie powinieneś:
1) uruchomić komputer z systemem Windows 2003 Server,
2) zalogować się do systemu z prawami administracyjnymi,
3) uruchomić konsolę „Użytkownicy i Komputery Usługi Active Directory",
4) wybrać z menu „Akcja" opcję „Nowy/Grupa",
5) założyć nową grupę (nadanie nazwy, określenie zakresu i typu grupy),

Wyposażenie stanowiska pracy:
- komputer z systemem Windows 2003 Server.
- poradnik dla ucznia.

Ćwiczenie 3

Stwórz 3 użytkowników o nazwach „pracownik_1", „pracownik_2", „pracownik_3".

Sposób wykonania ćwiczenia

Aby wykonać ćwiczenie powinieneś:
1) uruchomić komputer z systemem Windows 2003 Server,
2) zalogować się do systemu z prawami administratora,
3) uruchomić konsolę „Użytkownicy i Komputery usługi Active Directory",
4) wybrać z menu „Akcja" opcję „Nowy/Użytkownik",
5) wpisać dane użytkownika,
6) określić hasło i zasad używania hasła,
7) zakończyć pracę po utworzeniu użytkowników przewidzianych w ćwiczeniu.

Wyposażenie stanowiska pracy:
- komputer z systemem Windows 2003 Server,
- poradnik dla ucznia.

Ćwiczenie 4

Przydzielić użytkowników do grup.

Sposób wykonania ćwiczenia

Aby wykonać ćwiczenie powinieneś:
1) uruchomić komputer z systemem Windows 2003 Server,
2) zalogować się do systemu z prawami administracyjnymi,
3) uruchomić konsolę „Użytkownicy i Komputery usługi Active Directory",
4) wybrać z menu „Akcja" opcję „Nowy/Właściwości grupy pracownicy",

5) wybrać zakładkę „Członkowie”,
6) wyszukać w opcji „Zaawansowane/Znajdź teraz użytkowników” (pracownik_1 do 3),
7) przydzielić użytkowników „pracownik_1 do 3” do grupy „pracownicy”.

Wyposażenie stanowiska pracy:
- komputer z systemem Windows 2003 Server,
- poradnik dla ucznia.

Ćwiczenie 5

Utwórz dwie nowe grupy użytkowników „handlowcy_1” i „handlowcy_2”, utwórz nowych użytkowników „handlowiec_1” do „handlowiec_5”. Przydziel użytkowników do grup według przedstawionego klucza.

Sposób wykonania ćwiczenia

Aby wykonać ćwiczenie powinieneś:
1) uruchomić komputer z systemem Windows 2003 Server,
2) zalogować się do systemu z prawami administratora,
3) uruchomić konsolę „Użytkownicy i Komputery usługi Active Directory”,
4) wybrać z menu „Akcja” opcję „Nowy/Grupa”,
5) założyć nową grupę (nadanie nazwy, określenie zakresu i typu grupy),
6) wybrać z menu „Akcja” opcję „Właściwości i ustawienie zasad zabezpieczeń”,
7) wybrać z menu „Akcja” opcję „Nowy/Użytkownik”,
8) wpisać dane użytkownika,
9) określić hasło i zasady używania hasła,
10) wybrać z menu „Akcja” opcję „Nowy/Właściwości” kolejno dla grup użytkowników „handel_1”, „handel_2”,
11) wybrać zakładkę „Członkowie”,
12) wyszukać w opcji „Zaawansowane/Znajdź teraz użytkowników” i przydzielić ich według następującego klucza – użytkownicy „handlowiec_1 do 3” do grupy „handlowcy_1” i użytkowników „handlowiec_3 do 5” do grupy „handlowcy_2”.

Wyposażenie stanowiska pracy:
- komputer z systemem Windows 2003 Server,
- poradnik dla ucznia.

Ćwiczenie 6

Utworzyć nowy profil sprzętowy w którym będzie wyłączona kata dźwiękowa.

Sposób wykonania ćwiczenia

Aby wykonać ćwiczenie powinieneś:
1) uruchomić komputer z systemem Windows XP,
2) zalogować się do systemu z prawami administratora,
3) uruchomić konsolę „System” w panelu sterowania,
4) uruchomić konsolę „Profile sprzętowe” ,
5) skopiuj istniejący profil do nowego profilu. Nazwij profil „bezsieci",
6) wykonaj reset komputera,
7) przy logowaniu wybierz profil „bezsieci”,
8) zalogować się do systemu z prawami administratora,
9) uruchomić konsolę „System” w panelu sterowania,
10) uruchomić konsolę „Menedżer urządzeń”,

11) wybrać zakładkę „karty sieciowe”,
12) kliknąć prawym przyciskiem myszy na karcie sieciowej i wybrać opcję „właściwości”,
13) w menu „Użycie urządzenia” wybrać opcję „nie używaj tego urządzenia (wyłącz)”.

Wyposażenie stanowiska pracy:
- komputer z systemem Windows XP,
- poradnik dla ucznia.

Ćwiczenie 7

Utworzyć szablon profilu użytkownika

Sposób wykonania ćwiczenia

Aby wykonać ćwiczenie powinieneś:
1) Utworzyć konto użytkownika, które będzie używane jedynie w celu tworzenia szablonów profilu. Konto powinno być utworzone zgodnie z poniższymi informacjami:

Pole	Wpis
– Imię	Profile
– Nazwisko	Account
– Nazwa logowania użytkownika	Profile
– Nazwa logowania użytkownika (systemy starsze niż Windows 2000))	Profile

2) Wylogować się z serwera.
3) Zalogować się używając konta Profile.
4) Utworzyć niestandardowy pulpit dodając na przykład skróty do lokalnych lub sieciowych zasobów.
5) Wylogować się z konta Profile.

Wyposażenie stanowiska pracy:
- komputer z systemem Windows XP,
- Komputer z systemem Windows 2003 Server,
- poradnik dla ucznia.

Ćwiczenie 8

Zablokować w rejestrze systemu możliwość zmiany tła pulpitu i wygaszacza.

Sposób wykonania ćwiczenia

Aby wykonać ćwiczenie powinieneś:
1) uruchomić komputer z systemem Windows XP,
2) zalogować się do systemu z uprawnieniami administratora,
3) uruchomić konsolę edycji rejestru wpisując regedit w konsoli „uruchom” Menu Start”,
4) odnaleźć w rejestrze systemu ścieżkę „[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System],
5) utworzyć nową wartość “dword” o nazwie “NodispBackgroundPage”,
6) utworzyć nową wartość “dword” o nazwie “ NodispScrSavPage”,
7) zmodyfikować dane wartości na „00000001”,
8) wylosować się z systemu.

Wyposażenie stanowiska pracy:
- komputer z systemem Windows XP,
- poradnik dla ucznia.

4.2.3. Sprawdzian postępów

Czy potrafisz?

		Tak	Nie
1)	wymienić funkcje jakie musi posiadać system, aby był bezpieczny?	☐	☐
2)	wymienić działania jakie trzeba podjąć, aby system był bezpieczny?	☐	☐
3)	wymienić podstawowe kryteria jakie musi spełniać system posiadający klasę C2?	☐	☐
4)	powiedzieć jaki odpowiednik kryteriów TCSEC funkcjonuje w Europie?	☐	☐
5)	rozszyfrować skróty MAC i DAC?	☐	☐
6)	zarządzać kontem użytkownika/grupy?	☐	☐
7)	zainstalować Windows 2003 Server?	☐	☐
8)	dodać lub usunąć rolę serwera?	☐	☐
9)	udostępnić folder?	☐	☐
10)	udostępnić zasób sieciowy?	☐	☐

4.3. Prawa dostępu

4.3.1. Materiał nauczania

Prawa definiują, jakie operacje dany użytkownik (a raczej element o danym numerze SID) może wykonać na określonym obiekcie. Prawa mogą być przypisane między innymi do następujących obiektów:

- użytkowników/grup danej domeny, komputerów i innych „specjalnych" obiektów występujących w Active Directory,
- użytkowników czy grup należących do innej domeny, która jest połączona relacją zaufania z daną domeną,
- lokalnie zdefiniowanych użytkowników/grup na danym komputerze.

Należy podkreślić, że zalecane jest przypisywanie praw do grup użytkowników, a nie do poszczególnych osób. Wynika to stąd, że numer SID jest unikatowy i jeżeli na przykład Kowalski będzie miał określony numer SID, a pewne prawa będą związane bezpośrednio z Kowalskim, to po usunięciu konta użytkownika nie ma możliwości, by na przykład drugi raz utworzyć Kowalskiego z tym samym numerem SID.

Pełna lista możliwych typów uprawnień obejmuje kilkadziesiąt pozycji o określonej roli – w zależności od typu chronionego obiektu (na przykład inne będą dotyczyć pliku, a inne drukarki).

Można jednak wyodrębnić cztery główne „typy" dostępu:

- prawa do odczytu,
- prawa do modyfikacji,
- prawa do zmiany właściciela,
- prawa do usunięcia obiektu.

Definiując uprawnienia należy pamiętać, że uprawnienia „zakazujące" (ang. deny) dostępu mają priorytet nad uprawnieniami „zezwalającymi". Innymi słowy – jeżeli Kowalski należy do grupy „Sprzedawcy" i „Staż", a grupa „Sprzedawcy" ma uprawnienia zapisu do określonego folderu, ale grupa „Staż" ma jawnie te uprawnienia zabrane, to wtedy Kowalski nie ma uprawnień zapisu do danego folderu.

Własność obiektu

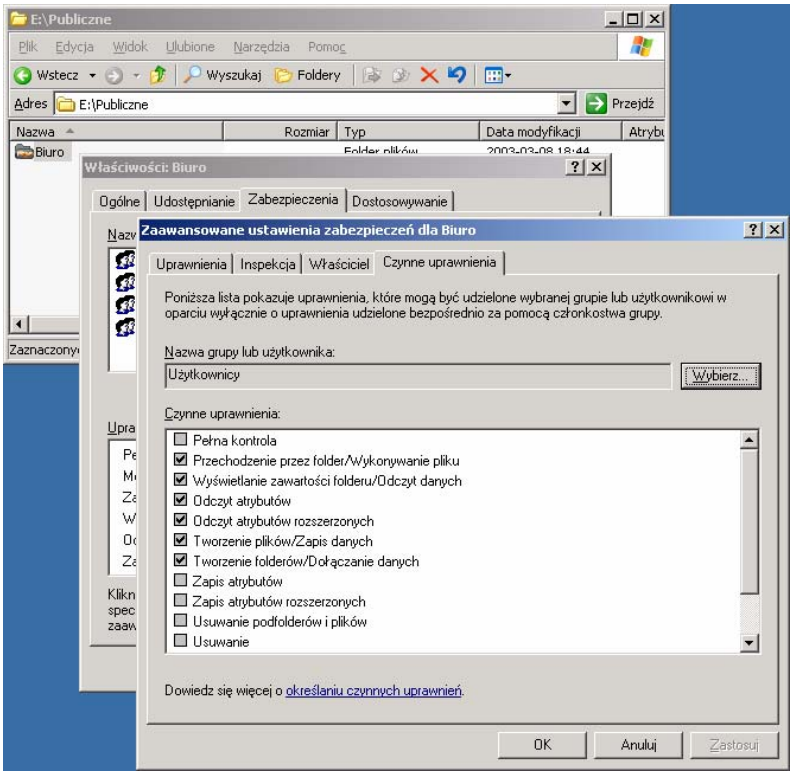
Każdy obiekt kontrolowany przez Windows 2003 Server ma swojego właściciela. Domyślnie – ten kto stworzył obiekt, jest jego właścicielem. Bez względu na uprawnienia jakie uzyskał od administratora, właściciel obiektu zawsze może zmienić ustawione uprawnienia do tego obiektu. Właściciel może zabrać sobie samemu prawa swojego obiektu. Wtedy nie ma możliwości, by na przykład odczytać dany plik, jeżeli wcześniej nie przywróci sobie tych praw.

Dziedziczenie uprawnień

Jedną z ważniejszych zalet mechanizmu DACL jest możliwość dziedziczenia uprawnień. Można określić, że np. wszystkie pliki czy podfoldery będą dziedziczyły uprawnienia z folderu nadrzędnego. Warto dodać, że w Windows 2003 Server można dokładnie określić, które uprawnienia mają być dziedziczone w obiektach „potomnych" (czyli tych, które są zawarte w danym obiekcie).

Łańcuch uprawnień

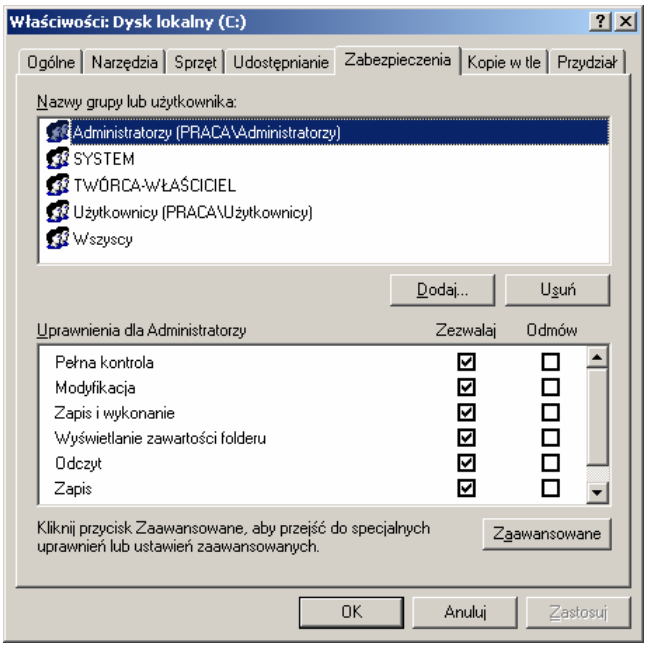
W skomplikowanych przypadkach trudno od razu określić, jakie uprawnienia ma konkretna grupa czy użytkownik. Wynika to stąd, że w Windows 2003 Server prawa można ustalać na dowolnym poziomie drzewa katalogu – użytkownik może należeć do wielu grup, grupy mogą być zagnieżdżone i tym podobne. Tak więc przy skomplikowanej strukturze administrator musi poświęcić wiele uwagi, aby prawidłowo określić prawa dostępu. W Windows 2003 Server pomoże mu w tym dodatkowa zakładka w oknie zaawansowanego ustawiania uprawnień. Można w niej wybrać określoną grupę czy wręcz danego użytkownika i podejrzeć „obowiązujące" uprawnienia dla danej grupy.



Rys. 27. Konsola ustalania praw grupy

Uprawnienia definiują, jakie operacje dany użytkownik może wykonać na określonym obiekcie.

Po kliknięciu prawym przyciskiem na dowolnym dysku, z systemem plików NTFS lub folderze czy pliku przechowanym na dysku NTFS, z menu będzie dostępna zakładka Zabezpieczenia. Po jej wybraniu w górnej części okna zobaczymy listę grup i użytkowników, w dolnej – listę uprawnień nadanych lub odebranych danej grupie lub użytkownikowi.



Rys. 28. Konsola przydzielania praw do obiektu

W rzeczywistości na liście uprawnień znajdują się grupy uprawnień mające ułatwić zarządzanie dostępem do danych. Nadanie każdego z uprawnień wymienionych na liście spowoduje umożliwienie wybranemu użytkownikowi lub grupie użytkowników wykonania pewnych operacji. Pełna lista uprawnień specjalnych składających się na poszczególne uprawnienia znajduje się poniżej.

Tab. 2. Lista uprawnień i odpowiadających im praw do wykona określonych czynności

Uprawnienia specjalne	Pełna kontrola	Modyfikacja	Odczyt i wykonanie	Wyświetlanie zawartości folderu (tylko foldery)	Odczyt	Zapis
Przechodzenie przez folder /Wykonywanie pliku	X	X	X	X		
Wyświetlanie zawartości folderu/Odczyt danych	X	X	X	X	X	
Odczyt atrybutów	X	X	X	X	X	
Odczyt atrybutów rozszerzonych	X	X	X	X	X	
Tworzenie plików/Zapis danych	X	X				X
Tworzenie folderów /Dołączanie danych	X	X				X
Zapis atrybutów	X	X				X
Zapis atrybutów rozszerzonych	X	X				X
Usuwanie podfolderów i plików	X					
Usuwanie	X	X				
Odczyt uprawnień	X	X	X	X	X	X
Zmiana uprawnień	X					
Przejęcie na własność	X					
Synchronizowanie	X	X	X	X	X	X

Uprawnienia się kumulują. Jeżeli ten sam użytkownik jest członkiem trzech grup, z których jedna ma nadane uprawnienia do odczytu pliku, druga – do zapisu, a trzecia nie ma nadanych żadnych uprawnień, wynikowymi uprawnieniami użytkownika będą uprawnienia do odczytu i zapisu pliku.

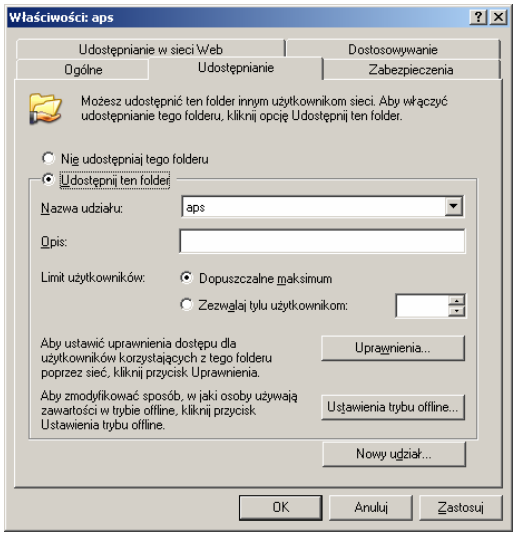
Kopiowanie plików i folderów

Aby skopiować plik lub folder, musimy posiadać co najmniej uprawnienia odczytu do obiektu źródłowego i zapisu do folderu docelowego.

Wszystkie obiekty zarówno pliki, jak foldery, „dziedziczą" uprawnienia od folderu nadrzędnego (lub dysku w przypadku folderów głównych), to podczas kopiowania i przenoszenia obiektów uprawnienia te mogą ulec zmianie. Po skopiowaniu pliku z folderu „X", do którego jedynie my mieliśmy uprawnienia do odczytu do folderu „Y", do którego wszyscy mają pełny dostęp, wszyscy użytkownicy będą mogli odczytywać, modyfikować a nawet skasować nasz plik.

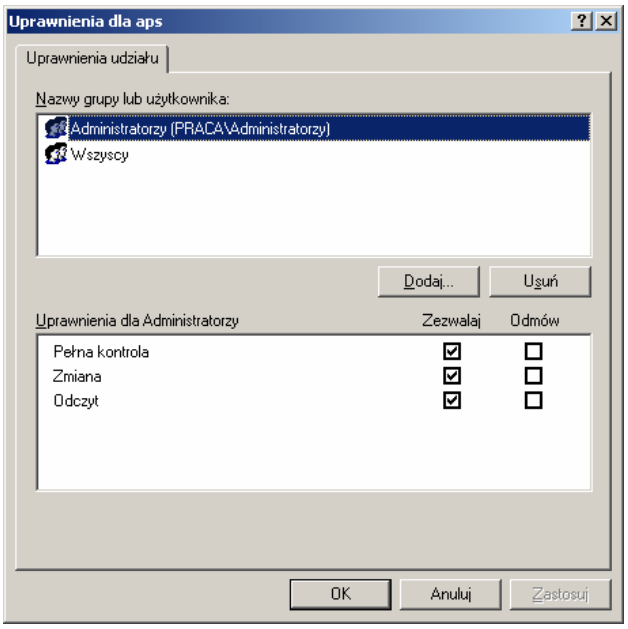
Kopiowane lub przenoszone pliki i foldery dziedziczą uprawnienia folderu lub dysku docelowego. Jedynym wyjątkiem jest przeniesienie obiektów w obrębie tego samego dysku logicznego. W takim przypadku przeniesiony obiekt zachowa początkowe uprawnienia użytkownika.

Jeżeli chcemy ustawiać uprawnienia na poziomie udziału sieciowego, należy wejść na zakładkę Udostępnianie,



Rys. 29. Konsola udostępniania zasobów (Foldery, dyski)

a następnie wybrać Uprawnienia.



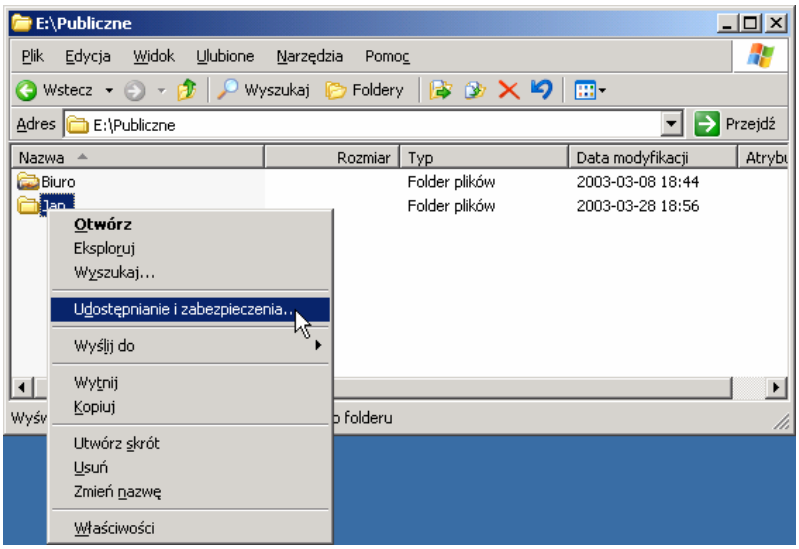
Rys. 30. Konsola wyboru uprawnień do zasobu

Należy podkreślić różnicę pomiędzy ustanawianiem uprawnień na poziomie udziału sieciowego, a uprawnień przypisywanych poszczególnym obiektom. Zakres uprawnień „dla udziału" jest uboższy – można określić, że dany użytkownik/grupa ma albo pełną kontrolę, uprawnienia do odczytu lub też uprawnienia do zmiany. Przy użyciu mechanizmów NTFS można ustawić znacznie dokładniejsze uprawnienia. Uprawnienia ustawione na poziomie udziału sieciowego, nie mają znaczenia, jeżeli użytkownik zaloguje się lokalnie.

Jeżeli równocześnie ustanawiamy uprawnienia na poziomie udziału sieciowego oraz na poziomie NTFS, to aby dana grupa miała możliwość skorzystania z określonego udziału sieciowego, musi mieć uprawnienia zarówno do udziału jak i do zasobów w NTFS.

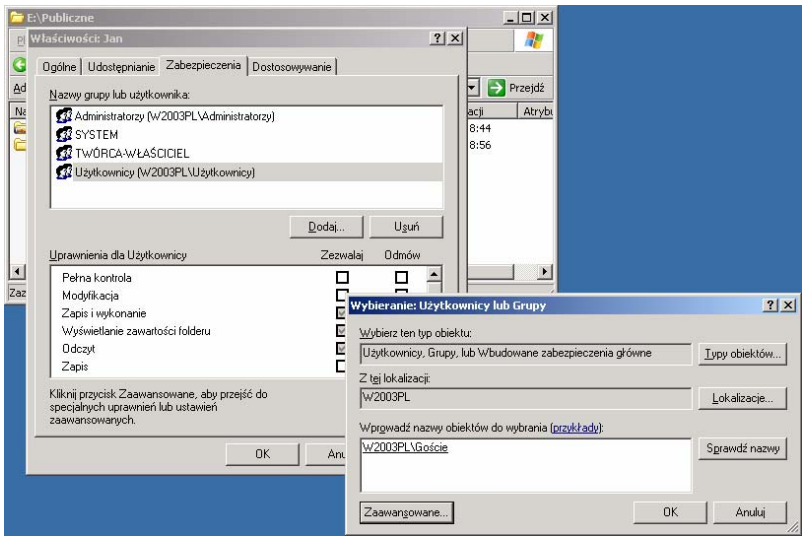
W Windows 2003 wszystkie operacje związane z uprawnieniami można także wykonywać z poziomu linii poleceń. Polecenie cacls pozwala wyświetlać albo zmieniać listę uprawnień dostępu dla wybranych plików/katalogów.

Aby dodać lub sprawdzić jakie uprawnienia są przypisane do określonego pliku, można skorzystać na przykład z interfejsu eksploratora Windows. W tym celu wystarczy kliknąć prawym przyciskiem myszy na odpowiednim obiekcie (pliku, folderze) i z menu wybrać opcję „Udostępnianie i zabezpieczenia".



Rys. 31. Kontrola uprawnień do zasobu – Udostępnianie i zabezpieczenia

Dalszy sposób postępowania zależy od tego, co się chce osiągnąć. Jeżeli uprawnienia do plików ustawiane są na poziomie partycji NTFS, wtedy należy przełączyć się na zakładkę Zabezpieczenia po czym można dodać nowego użytkownika (lepiej – grupę) i przypisać mu określone uprawnienia.



Rys. 32. Podgląd i dodawanie uprawnionych użytkowników do zasobu

Polisy

W Active Directory w Windows 2003 Server dostępne są tak zwane grupowe polisy (Group Policy), czyli zestaw zasad i uprawnień obowiązujących użytkowników i komputery dołączone do danej domeny. Polisy grupowe w odróżnieniu od polis lokalnych mogą być ustawiane na dowolnym poziomie hierarchii w katalogu. W Windows 2003 Server istnieje ponad 160 ustawień obejmujących różne aspekty działania systemu i uprawnień użytkownika. Wśród nowych cech, warto wymienić możliwość ustawiania położenia folderu „Moje dokumenty" czy – mechanizm pozwalający określić „dozwolony do uruchamiania" zestaw oprogramowania.

Polisa jest zbiorem zasad określających uprawnienia komputera pełniącego określoną rolę w domenie czy też uprawnienia użytkownika. Określane są tu zasady postępowania z hasłami

(minimalna długość, po jakim czasie hasło musi zostać zmienione), w jakich warunkach konto jest blokowane.

Polisy mogą obowiązywać na lokalnym komputerze jak i na komputerach wykorzystujących usługę katalogową.

Wraz z instalacją Windows 2003 Server, instalowane są wzorcowe „zestawy" polis, które określają standardowe zabezpieczenia w zależności od tego, jaką rolę ma pełnić dany serwer czy stacja robocza. Także administrator może opracowywać nowe wzorce, a następnie dystrybuować je w sieci, tak by w obrębie sieci obowiązywała wspólna polityka bezpieczeństwa.

Główne narzędzia do konfiguracji bezpieczeństwa stanowią tzw. pakiet do zarządzania i konfiguracji bezpieczeństwa (ang. Security Confguration Manager). Mogą one służyć do automatyzacji wielu zadań związanych z bezpieczeństwem.

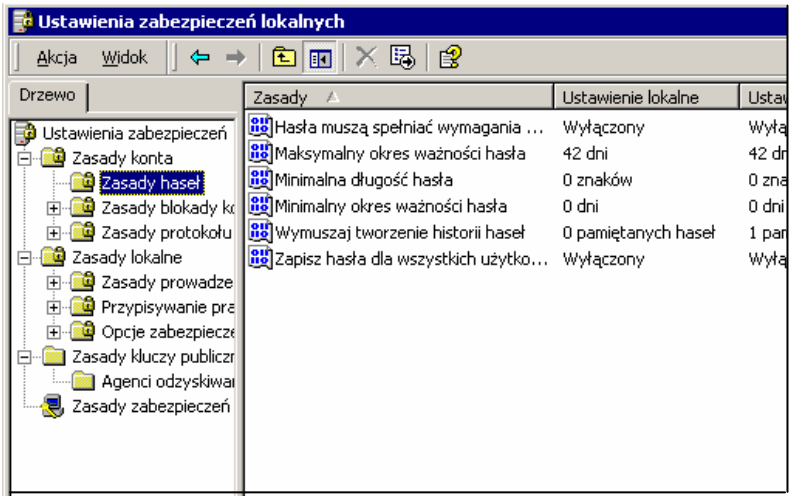
Używając ustawień zabezpieczeń (czy to lokalnych, czy też na poziomie katalogu) można:

- ograniczyć uruchamianie nieznanych programów (w tym wirusów),
- określić, jakiego typu komponenty ActiveX mogą być ściągane i uruchamiane na komputerze,
- wymóc, by można było uruchamiać tylko skrypty podpisane cyfrowo.

Można wskazać określony katalog, z którego można (lub nie) uruchamiać programy. Mogą to być udziały sieciowe lub dyski lokalne.

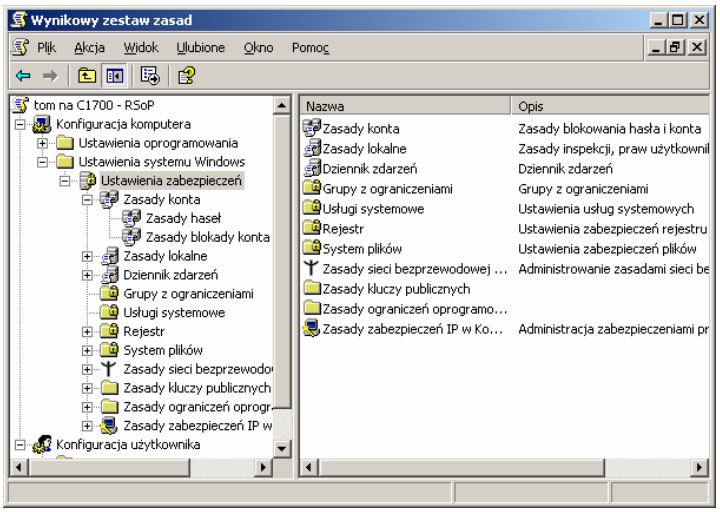
Można także wskazać konkretny plik EXE czy DLL. Wtedy, Windows 2003 Server policzy klucz mieszający (ang. hash), który identyfikuje na przykład plik EXE czy DLL. Następnie przy użyciu tego klucza badane jest czy uruchamiany program pasuje do wzorca i w zależności od uprawnień dana aplikacja jest uruchamiana lub też nie.

Można również wskazać dowolny certyfikat używany do podpisywania kodu (lub skryptów), po czym określić, że na przykład tylko elementy podpisane danym kluczem będą mogły być uruchamiane na konkretnym serwerze (czy stacji roboczej).



Rys. 33. Ustawienia zabezpieczeń lokalnych

Bardzo wygodnym mechanizmem jest tak zwany „wynikowy" zestaw uprawnień (polis) – czyli RSoP (Resultant Set of Policy). W Windows 2003 Server administrator może przetestować jak naprawdę będą wyglądać polisy ustawione na danym komputerze, czy też, jakie będzie miał uprawnienia dany użytkownik. Można również sprawdzić co się stanie jeśli dane ustawienie ulegnie zmianie.



Rys. 34. Wynikowy zestaw zasad

Prawa przypisywane do poszczególnych obiektów istniejących w Windows są tak naprawdę wynikiem złożenia wielu różnych ustawień – na przykład dany użytkownik może należeć do wielu różnych grup bezpieczeństwa.

Nowe możliwości wprowadzono także w mechanizmach automatycznego instalowania aplikacji. Na przykład użytkownik może przypisać, że w ramach danej polisy, każdy użytkownik ma mieć zainstalowany określone oprogramowanie. W momencie, gdy użytkownik, któremu przypisano taki zbiór zasad zaloguje się do sieci, system sprawdzi czy ma odpowiednie oprogramowanie. Jeżeli nie – zostanie ono zainstalowane.

Skrypty logowania

Skrypty logowania to grupy poleceń uruchamiane w czasie logowania się użytkownika na komputerze. Administratorzy projektują skrypty logowania, aby zautomatyzować konfigurację środowiska użytkownika.

Skrypty logowania, wylogowania, uruchamiania i zamykania systemu – skrypty, które komputer ma uruchomić przy uruchomieniu i wyłączeniu oraz podczas logowania i wylogowania użytkownika. Pozwalają one na łatwe zaimplementowanie funkcji, przypisanych do określonych użytkowników, grup lub komputerów. Na przykład, skrypt logowania może podłączyć określony udział plików lub wydruku, skrypt wylogowania może służyć do usunięcia zmiennych środowiskowych, uruchomienia procesu lub powiadomienia systemu o wyjściu. Windows 2003 Server do opracowania skryptów udostępnia narzędzie skryptowe WSH – Windows Scripting Host (Visual Basic, JavaScript i tak dalej), jak również interfejsy WMI i ADSI.

Do zadań wykonywanych przez skrypty logowania należą:

- mapowanie dysków sieciowych,
- instalowanie i ustawianie domyślnej drukarki użytkownika,
- zbieranie informacji o systemie komputera,
- aktualizowanie sygnatur wirusów,
- aktualizowanie oprogramowania.

Pliki skryptów to pliki tekstowe zawierające polecenia skryptów. Systemy operacyjne z rodziny Windows Server 2003 obsługują następujące typy skryptów:

- polecenia plików wsadowych są zapisywane w plikach tekstowych w rozszerzeniem .bat lub .cmd. Pliki wsadowe automatyzują proste serie zadań, które w przeciwnym razie zostałyby uruchomione z wiersza polecenia. Skrypty napisane z użyciem poleceń plików wsadowych są uruchamiane przez powłokę poleceń,

– polecenia języka Visual Basic Scripting Edition (VBScript) są zapisywane w plikach tekstowych z rozszerzeniem nazwy vbs, a polecenia języka JScript są zapisywane w plikach z rozszerzeniem nazwy js. Języki VBScript i JScript umożliwiają administratorowi tworzenie wyrafinowanych skryptów. Host skryptów systemu Windows może uruchamiać te skrypty z pulpitu komputera oraz z wiersza polecenia.

Po utworzeniu skryptu logowania można przypisać go co najmniej jednemu użytkownikowi lokalnemu, lokacji, domenie lub jednostce organizacyjnej.

Tab. 3. Interpretacja różnych formatów tekstu

Format	**Znaczenie**
Kursywa	Informacje, które musi podać użytkownik
Pogrubienie	Elementy, które użytkownik musi wpisać dokładnie tak jak pokazano
W nawiasie okrągłym (...)	Parametry, które mogą się kilka razy powtórzyć w wierszu polecenia
W nawiasie kwadratowym ([])	Elementy opcjonalne
W nawiasie klamrowym ({}); opcje oddzielone znakiem potoku (|). Przykład: {even|odd}	Zestaw opcji, z których użytkownik musi wybrać tylko jedną
czcionka courier	Kod lub wynik działania programu

Tab. 4. Znaki specjalne do przekazywania poleceń

Znak	**Składnia**	**Definicja**
& [**...**]	*polecenie1* **&** *polecenie2*	Służy do oddzielania wielu poleceń w pojedynczym wierszu polecenia. Program cmd.exe wykonuje pierwsze polecenie, a następnie drugie polecenie
&& [**...**]	*polecenie1* **&&***polecenie2*	Służy do wykonywania polecenia następującego po symbolu **&&** tylko wtedy, gdy poprzedzające symbol polecenie wykonano pomyślnie. Program cmd.exe wykonuje pierwsze polecenie, a następnie wykonuje drugie polecenie, jeśli pierwsze polecenie zostało wykonane pomyślnie
|| [**...**]	*polecenie1* **||** *polecenie2*	Służy do wykonywania polecenia następującego po symbolu || tylko wtedy, gdy nie powiedzie się wykonywanie polecenia poprzedzającego symbol ||. Program cmd.exe wykonuje pierwsze polecenie, a następnie wykonuje drugie polecenie, jeśli pierwsze polecenie nie zostało wykonane pomyślnie (zgłoszony był kod błędu większy od zera)
( ) [**...**]	**(***polecenie1* **&** *polecenie2***)**	Służy do grupowania lub zagnieżdżania wielu poleceń
; lub **,**	*polecenie1 parametr1***;** *parametr2*	Służy do oddzielania parametrów poleceń

Tab. 5. Lista systemowych i lokalnych zmiennych środowiskowych serwerowego systemu operacyjnego Windows

Zmienna	Typ	Opis
%ALLUSERSPROFILE%	Lokalna	Zwraca lokalizację profilu wszystkich użytkowników
%APPDATA%	Lokalna	Zwraca lokalizację, w której aplikacje domyślnie przechowują dane
%CD%	Lokalna	Zwraca ciąg bieżącego katalogu
%CMDCMDLINE%	Lokalna	Zwraca dokładny wiersz polecenia użyty do uruchomienia bieżącego wystąpienia programu Cmd.exe
%CMDEXTVERSION%	Systemowa	Zwraca numer wersji bieżących rozszerzeń procesora poleceń
%COMPUTERNAME%	Systemowa	Zwraca nazwę komputera
%COMSPEC%	Systemowa	Zwraca dokładną ścieżkę do pliku wykonywalnego powłoki poleceń
%DATE%	Systemowa	Zwraca bieżącą datę. Korzysta z tego samego formatu co polecenie **date /t**. Generowana przez program cmd.exe. Aby uzyskać więcej informacji o poleceniu **date**, zobacz
%ERRORLEVEL%	Systemowa	Zwraca kod błędu ostatnio używanego polecenia. Wartość różna od zera zazwyczaj oznacza błąd
%HOMEDRIVE%	Systemowa	Zwraca literę dysku lokalnej stacji roboczej połączoną z katalogiem macierzystym użytkownika. Jest ustawiana na podstawie wartości katalogu macierzystego. Katalog macierzysty użytkownika jest określany w przystawce Użytkownicy i grupy lokalne
%HOMEPATH%	Systemowa	Zwraca pełną ścieżkę katalogu macierzystego użytkownika. Jest ustawiana na podstawie wartości katalogu macierzystego. Katalog macierzysty użytkownika jest określany w przystawce Użytkownicy i grupy lokalne

Zmienna	Typ	Opis
%HOMESHARE%	Systemowa	Zwraca ścieżkę sieciową udostępnionego katalogu macierzystego użytkownika. Jest ustawiana na podstawie wartości katalogu macierzystego. Katalog macierzysty użytkownika jest określany w przystawce Użytkownicy i grupy lokalne
%LOGONSERVER%	Lokalna	Zwraca nazwę kontrolera domeny weryfikującego bieżącą sesję logowania
%NUMBER_OF_PROCESSORS%	Systemowa	Określa liczbę procesorów zainstalowanych w komputerze
%OS%	Systemowa	Zwraca nazwę systemu operacyjnego. W systemie Windows 2000 nazwa systemu operacyjnego jest wyświetlana jako Windows NT
%PATH%	Systemowa	Określa ścieżkę wyszukiwania plików wykonywalnych
%PATHEXT%	Systemowa	Zwraca listę rozszerzeń nazw plików rozpoznawanych jako wykonywalne przez system operacyjny
%PROCESSOR_ARCHITECTURE%	Systemowa	Zwraca architekturę mikroukładu procesora. Wartości: x86 lub IA64 (procesor Itanium)
%PROCESSOR_IDENTFIER%	Systemowa	Zwraca opis procesora
%PROCESSOR_LEVEL%	Systemowa	Zwraca numer modelu procesora zainstalowanego w komputerze
%PROCESSOR_REVISION%	Systemowa	Zwraca numer wersji procesora
%PROMPT%	Lokalna	Zwraca ustawienia wiersza polecenia bieżącego interpretera. Jest generowana przez program Cmd.exe
%RANDOM%	Systemowa	Zwraca losowy numer dziesiętny z zakresu od 0 do 32 767. Jest generowana przez program Cmd.exe
%SYSTEMDRIVE%	Systemowa	Zwraca dysk zawierający katalog główny systemu operacyjnego Windows Server (to znaczy główny katalog systemowy)
%SYSTEMROOT%	Systemowa	Zwraca lokalizację katalogu głównego systemu operacyjnego Windows Server

Zmienna	Typ	Opis
%TEMP% i %TMP%	Systemowa i użytkownika	Zwraca domyślne katalogi tymczasowe używane przez aplikacje dostępne dla użytkowników, którzy są aktualnie zalogowani. Niektóre aplikacje wymagają katalogu TEMP, a inne katalogu TMP
%TIME%	Systemowa	Zwraca bieżącą godzinę. Korzysta z tego samego formatu co polecenie **time /t**. Jest generowana przez program Cmd.exe
%USERDOMAIN%	Lokalna	Zwraca nazwę domeny zawierającej konto użytkownika
%USERNAME%	Lokalna	Zwraca nazwę aktualnie zalogowanego użytkownika
%USERPROFILE%	Lokalna	Zwraca lokalizację profilu bieżącego użytkownika
%WINDIR%	Systemowa	Zwraca lokalizację katalogu systemu operacyjnego

Przykładowy skrypt logowania widnieje poniżej

```
Const ENGINEERING_GROUP     = "cn=engineering" Const FINANCE_GROUP        = "cn=finance"
Const HUMAN_RESOURCES_GROUP = "cn=human resources"
Set wshNetwork = CreateObject("WScript.Network") wshNetwork.MapNetworkDrive "h:",
"\\FileServer\Users\" & wshNetwork.UserName
Set ADSysInfo = CreateObject("ADSystemInfo") Set CurrentUser = GetObject("LDAP://" &
ADSysInfo.UserName) strGroups = LCase(Join(CurrentUser.MemberOf))
If InStr(strGroups, ENGINEERING_GROUP) Then
wshNetwork.MapNetworkDrive "g:", "\\FileServer\Engineering\"
wshNetwork.AddWindowsPrinterConnection "\\PrintServer\EngLaser"
wshNetwork.AddWindowsPrinterConnection "\\PrintServer\Plotter" wshNetWork.SetDefaultPrinter
"\\PrintServer\EngLaser"
ElseIf InStr(strGroups, FINANCE_GROUP) Then
wshNetwork.MapNetworkDrive "g:", "\\FileServer\Finance\" wshNetwork.AddWindowsPrinterConnection
"\\PrintServer\FinLaser" wshNetWork.SetDefaultPrinter "\\PrintServer\FinLaser"
ElseIf InStr(strGroups, HUMAN_RESOURCES_GROUP) Then
wshNetwork.MapNetworkDrive "g:", "\\FileServer\Human Resources\"
wshNetwork.AddWindowsPrinterConnection "\\PrintServer\HrLaser" wshNetWork.SetDefaultPrinter
"\\PrintServer\HrLaser"

End If
```

Powyższy przykładowy skrypt logowania zawiera polecenia języka VBScript, które za pomocą interfejsu ADSI (Active Directory Service Interfaces) wykonują trzy typowe zadania uzależnione od członkostwa grup użytkownika:

- mapuje dysk H: do katalogu macierzystego użytkownika, wywołując metodę MapNetworkDrive obiektu Network modelu WSH z właściwością UserName tego obiektu,
- za pomocą obiektu IADsADSystemInfo interfejsu ADSI uzyskuje nazwę wyróżniającą bieżącego użytkownika, która z kolei służy do łączenia się z obiektem odpowiadającym temu użytkownikowi w usłudze Active Directory. Po nawiązaniu połączenia za pomocą

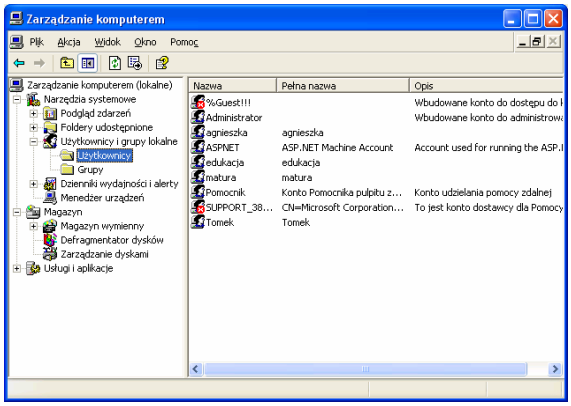
atrybutu memberOf użytkownika pobierana jest lista grup, których użytkownik jest członkiem. Wielowartościowa lista nazw grup jest złączana w jeden ciąg znaków za pomocą funkcji Join języka VBScript, aby łatwiej było wyszukiwać docelowe nazwy grup,

– jeśli bieżący użytkownik jest członkiem jednej z trzech grup zdefiniowanych na początku skryptu, wówczas skrypt mapuje literę G: na dysk udostępniony grupy i ustawia domyślną drukarkę użytkownika jako drukarkę grupy.

Aby uruchomić skrypt logowania, należy przypisać go użytkownikowi lub grupie.

Aby przypisać skrypt logowania użytkownikowi lub grupie:

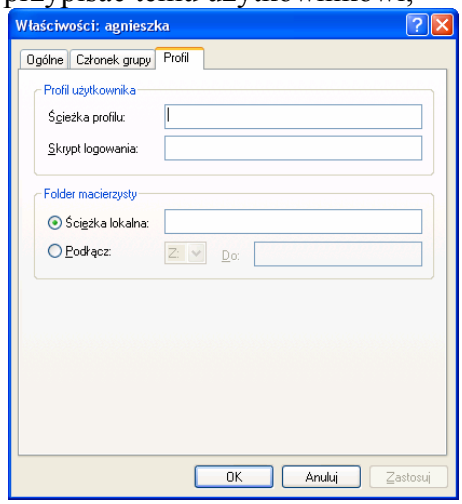
– otwórz konsolę Zarządzanie komputerem,



Rys. 35. Konsola zarządzania komputerem

– w drzewie konsoli kliknij węzeł użytkownicy, kliknij dwukrotnie użytkownika, do którego chcesz przypisać skrypt logowania,

– kliknij kartę profil, w polu skrypt logowania wprowadź ścieżkę i nazwę skryptu logowania, który chcesz przypisać temu użytkownikowi,

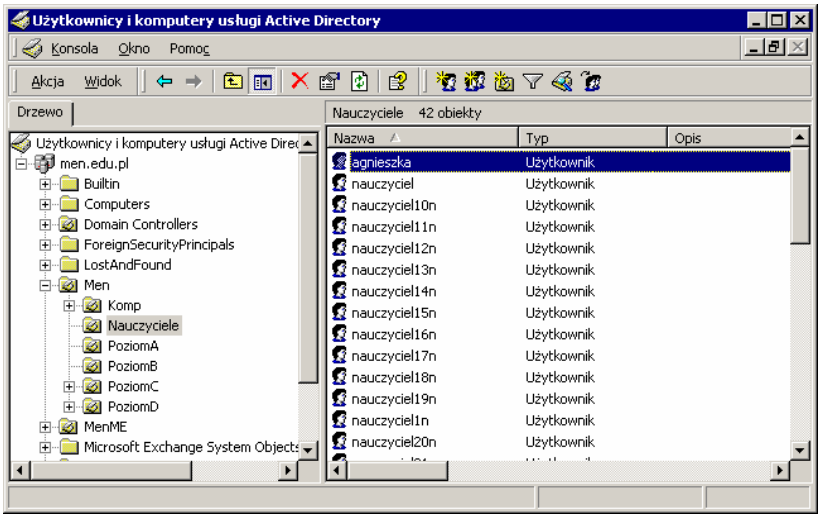


Rys. 36. Konsola właściwości użytkownika, zakładka „Profil”

– kliknij przycisk ok.

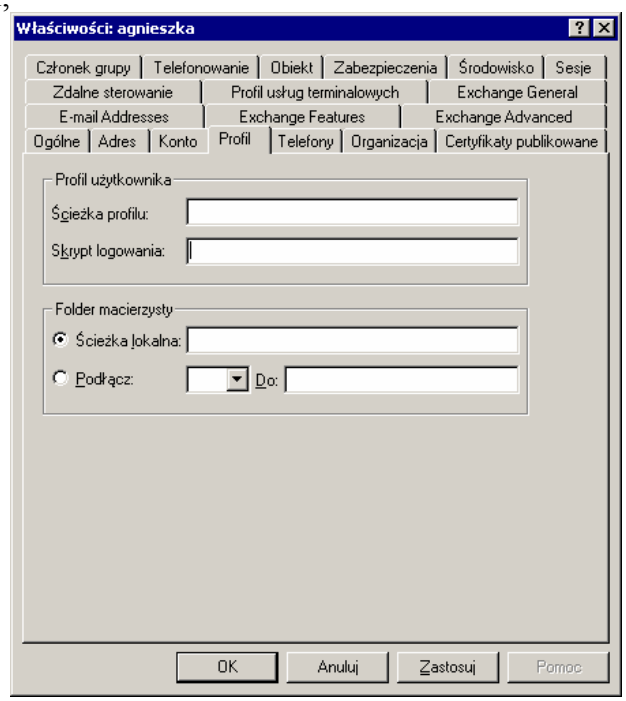
Aby przypisać skrypt logowania użytkownikowi w usłudze Active Directory:

- otwórz przystawkę użytkownicy i komputery usługi Active Directory,
- w drzewie konsoli odnaleźć użytkownika, któremu chcemy przypisać skrypt logowania,



Rys. 37. Konsola „Użytkownicy i komputery usługi Active Directory"

- kliknij dwukrotnie użytkownika, któremu chcesz przypisać skrypt logowania,
- kliknij kartę profil,

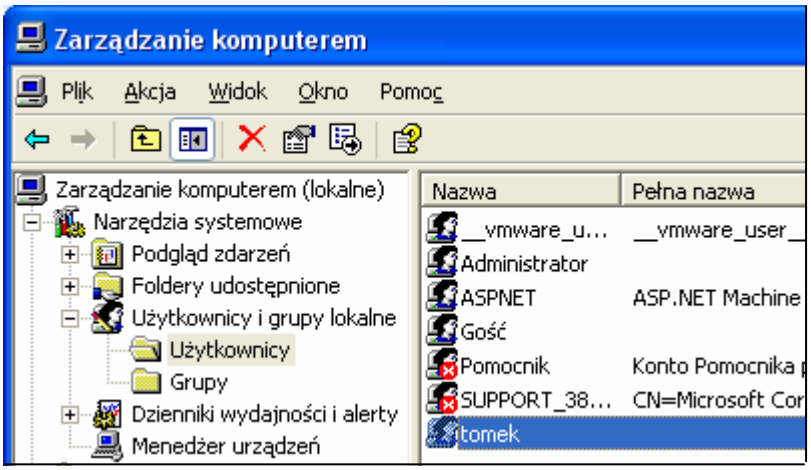


Rys. 38. Konsola „Właściwości użytkownika" zakładka „Profil"

- w polu skrypt logowania wpisz ścieżkę i nazwę skryptu logowania, który chcesz przypisać temu użytkownikowi, a następnie kliknij przycisk ok.,

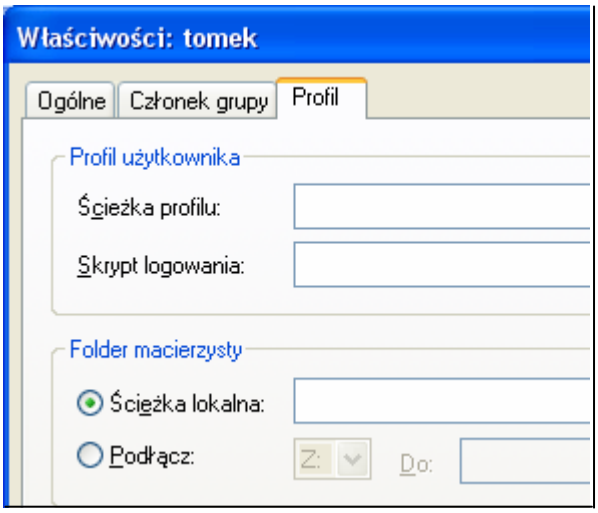
Aby przypisać skrypt logowania kontu użytkownika lokalnego:

- otwórz przystawkę Zarządzanie komputerem,
- w drzewie konsoli kliknij węzeł Użytkownicy/zarządzanie komputerem/narzędzia systemowe/użytkownicy i grupy lokalne/użytkownicy,



Rys. 39. Konsola „Zarządzanie komputerem”

– kliknij prawym przyciskiem myszy żądane konto użytkownika, a następnie kliknij polecenie właściwości,
– na karcie profil w polu skrypt logowania wpisz nazwę pliku i ścieżkę względną do skryptu,



Rys. 40. Konsola „Właściwości” zakładka ”Profil”

4.4.2. Pytania sprawdzające

Odpowiadając na pytania sprawdzisz, czy jesteś przygotowany do wykonania ćwiczeń.

1) Co definiują prawa dostępu?
2) Podaj główne typy dostępu.
3) Na czym polega dziedziczenie uprawnień?
4) Z czego wynika łańcuch uprawnień?
5) Na czym polega kumulacja uprawnień?
6) Co to jest polisa?
7) W ramach jakiego narzędzia działają polisy?
8) Co można ustalić przy pomocy polis?
9) Co to jest profil użytkownika?
10) Jaka jest budowa profilu?

4.4.3. Ćwiczenia

Ćwiczenie 1

Ustal dla nowej jednostki organizacyjnej maksymalny czas trwania hasła na 5 dni.

Sposób wykonania ćwiczenia

Aby wykonać ćwiczenie powinieneś:

1) uruchomić komputer z systemem Windows 2003 Server,
2) zalogować się do systemu z prawami administratora,
3) uruchomić konsolę „Użytkownicy i Komputery usługi Active Directory”,
4) utworzyć nową jednostkę organizacyjną „studenci”,
5) uruchomić z menu „Właściwości dla nowej jednostki”,
6) wprowadzić opis i przejść do zasad grupy,
7) dodać nowy obiekt zasad grup,
8) przejść do edycji zasad,
9) w konfiguracji komputera wybrać „Ustawienia systemu Windows/Ustawienia zabezpieczeń/Zasady haseł/Maksymalny okres ważności hasła” i ustawić tą wartość na 5 dni.

Wyposażenie stanowiska pracy:

- komputer z systemem Windows 2003 Server,
- poradnik dla ucznia.

Ćwiczenie 2

Udostępnij na dysku sieciowym (dysku serwera) folder „faktury”.

Sposób wykonania ćwiczenia

Aby wykonać ćwiczenie powinieneś:

1) uruchomić komputer z systemem Windows 2003 Server,
2) zalogować się do systemu z prawami administracyjnymi,
3) na dysku C: serwera założyć folder o nazwie „Faktury”,
4) w folderze „faktury” założyć trzy pliki tekstowe: faktury_1, faktury_2, faktury_3,
5) wybrać z menu „Plik/Udostępnianie”,
6) udostępnić w sieci folder „faktury” z następującymi uprawnieniami:

handlowiec_1	ZMIANA
handlowiec_2	BRAK DOSTĘPU
handlowiec_3	ODCZYT
handlowcy_1	ODCZYT
handlowcy_2	PEŁNA KONTROLA

Wyposażenie stanowiska pracy:

- komputer z systemem Windows 2003 Server,
- poradnik dla ucznia.

Ćwiczenie 3

Nadaj grupom i użytkownikom uprawnienia NTFS do plików i folderów.

Sposób wykonania ćwiczenia

Aby wykonać ćwiczenie powinieneś:
1) uruchomić komputer z systemem Windows Server,
2) zalogować się do systemu z prawami administracyjnymi,
3) wybrać z menu „Plik/Właściwości”,
4) nadać grupom i użytkownikom następujące uprawnienia NTFS do folderu „faktury” i plików tekstowych:

	handlowiec_1	handlowiec_2	handlowiec_3	handlowcy_1	handlowcy_2
faktury	Brak dostępu	Pełna kontrola	Zmiana	Odczyt	List
faktury_1	Odczyt	Brak dostępu	Pełna kontrola	Brak dostępu	Odczyt
faktury_2	Pełna kontrola	Zmiana	No Access	Odczyt	Pełna kontrola
faktury_3	Change	Odczyt	Zmiana	Pełna kontrola	Zmiana

Wyposażenie stanowiska pracy:
- komputer z systemem Windows 2003 Server,
- poradnik dla ucznia.

Ćwiczenie 4

Dodaj folder udostępniony przy pomocy konsoli zarządzania serwerem.

Sposób wykonania ćwiczenia

Aby wykonać ćwiczenie powinieneś:
1) uruchomić komputer z systemem Windows 2003 Server,
2) zalogować się do systemu z prawami administratora,
3) utworzyć na dysku C folder „udostępnianie”,
4) uruchomić konsolę „Zarządzanie Komputerem”,
5) wybrać „Narzędzia systemowe/Foldery udostępnione/Udziały”,
6) wybrać z menu „Akcja/Nowy/Udział pliku”,
7) udostępnić folder „udostępnianie”,
8) dostosować uprawnienia podobnie jak w ćwiczeniu z folderem „faktury”.

Wyposażenie stanowiska pracy:
- komputer z systemem Windows 2003 Server,
- poradnik dla ucznia.

Ćwiczenie 5

Skonfiguruj zasady inspekcji domeny.

Sposób wykonania ćwiczenia

Aby wykonać ćwiczenie powinieneś:
1) otworzyć konsolę „Użytkownicy” i komputery usługi Active Directory,
2) zaznaczyć węzeł domeny,
3) wybrać z menu „Akcja” polecenie „Właściwości”,
4) na zakładce „Zasada grupy” zaznaczyć domyślną zasadę domeny (Default Domain Policy),
5) kliknąć „Edit”,

6) wybrać kolejno opcje – „Konfiguracja komputera, Ustawienia systemu Windows, Ustawienia zabezpieczeń, Zasady kont, Zasada blokady konta”,
7) dwukrotnie kliknąć zasadę „Czas trwania blokady konta”,
8) zaznaczyć pole „Definiuj następujące ustawienia zasad”,
9) wpisać 0 jako określenie czasu trwania blokady i kliknąć przycisk „Zastosuj”,
10) kliknąć przycisk OK, aby potwierdzić ustawienia,
11) kliknąć przycisk OK, aby zamknąć okno dialogowe zasady,
12) sprawdzić, czy wartość parametru zasady Czas trwania blokady konta wynosi zero, czy próg ma wartość 5, a licznik zasady ustawiony został na 30 minut,
13) zamknąć konsolę „Edytor” obiektów zasady grupy,
14) zamknąć okno dialogowe „Właściwości domeny”.

Wyposażenie stanowiska pracy:
- komputer z systemem Windows 2003 Server,
- poradnik dla ucznia.

Ćwiczenie 6

Utwórz nową domenę.

Sposób wykonania ćwiczenia

Aby wykonać ćwiczenie powinieneś:
1) otworzyć konsolę „Użytkownicy i komputery usługi Active direktory”,
2) kliknąć prawym przyciskiem myszy na opcji „Domain controlers” (Kontrolery domeny),
3) wybrać opcję „Nowy komputer”,
4) wpisać nazwę komputera nowego kontrolera domeny,
5) zaznaczyć pole „Przypisz to konto komputera jako zapasowy kontroler domeny”,
6) potwierdź klikając dalej w kolejnych oknach,

Wyposażenie stanowiska pracy:
- komputer z systemem Windows 2003 Server,
- poradnik dla ucznia.

Ćwiczenie 7

Zainstaluj serwer DHCP.

Sposób wykonania ćwiczenia

Aby wykonać ćwiczenie powinieneś:
1) uruchomić Panel sterowania,
2) wybrać opcję Dodaj lub usuń programy,
3) wybrać opcję Dodaj/Usuń składniki systemu Windows,
4) wybrać opcję Usługi sieciowe,
5) kliknąć przycisk Szczegóły,
6) wybrać w składnik „usługi sieciowe”,
7) wybrać „Protokół dynamicznej konfiguracji hosta (DHCP)”,
8) kliknąć przycisk OK.,
9) po wyświetleniu monitu wpisz pełną ścieżkę do plików dystrybucyjnych systemu Windows Server 2003 i kliknij przycisk Kontynuuj.

Wyposażenie stanowiska pracy:
- komputer z systemem Windows 2003 Server,
- poradnik dla ucznia.

4.3.4. Sprawdzian postępów

Czy potrafisz?

		Tak	Nie
1)	powiedzieć co definiują uprawnienia w Windows NT?	☐	☐
2)	wymienić główne typy praw?	☐	☐
3)	wyjaśnić na czym polega dziedziczenie i łańcuch uprawnień?	☐	☐
4)	ustawić uprawnienia użytkownika/grupy?	☐	☐
5)	przypisać użytkowników do grupy?	☐	☐
6)	określić korzyści wynikające ze stosowania polis?	☐	☐
7)	zdefiniować pojęcie polisy?	☐	☐
8)	skonfigurować polisy dla użytkowników/grup?	☐	☐
9)	ustawić ścieżkę dojścia do profilu?	☐	☐
10)	zmienić folder macierzysty użytkownika?	☐	☐

4.4. Drukowanie

4.4.1. Materiał nauczania

W systemach z rodziny Windows 2003 Server wprowadzono wiele udoskonaleń infrastruktury systemu drukowania.

Istnieje kilka sposobów drukowania:

- drukowanie na lokalnym urządzeniu drukującym (print device). Urządzenie drukujące jest połączone z komputerem Windows 2003 Server poprzez port równoległy, port szeregowy, port USB lub port podczerwieni,
- drukowanie na sieciowym urządzeniu drukującym (network print server device). Urządzenie drukujące posiada interfejs sieciowy, który rozpoznaje bezpośrednio sieciowe polecenia drukowania,
- drukowanie na serwerach Windows. Serwer systemu Windows 2003 lub serwer poprzednich wersji Windows, które mają drukarkę (urządzenie logiczne) skonfigurowaną jako zasób udostępniony (shared resource). Udostępniona drukarka przyjmuje zadania drukowania (print jobs) z innych komputerów, pobierając je z bufora wydruku i przesyłając (despools) do podłączonego lokalnie urządzenia drukującego lub sieciowego urządzenia drukującego.

Drukowanie na sieciowym urządzeniu drukującym

Często firmy, zamiast podłączania drukarek do komputerów lokalnych decyduje się na zakup urządzenia, które posiadając interfejs umożliwiający podłączenie do Sieci, jest niezależne od komputerów.

Drukowanie na urządzeniu sieciowym wymaga korzystania z protokołów komunikacyjnych i języka poleceń zrozumiałych dla urządzenia.

Właściwie wszystkie sieciowe urządzenia drukujące obsługują główne protokoły komunikacyjne: TCP/IP, IPX/SPX, AppleTalk/EtherTalk i DLC/LLC. W systemie Windows 2003 Server można korzystać z wszystkich wyżej wymienionych protokołów, chociaż tylko TCP/IP jest ładowany domyślnie.

Większość sieciowych urządzeń drukujących do obsługi drukowania z systemu UNIX wykorzystuje Line Printer Daemon (LPD), a do obsługi systemu NetWare (główna baza danych serwera NetWare (bindery) i usługi NDS) funkcję NCP. Większość ma zaprogramowaną obsługę komputerów Macintosh do drukowania w standardzie Postscript, które nie wymaga specjalnych znaków sterujących i ma własny sterownik dla drukarki danego producenta.

W systemie Windows 2003 Server sieciowe urządzenie drukujące traktowane jest tak, jak gdyby to była drukarka podłączona lokalnie. Zamiast drukowania do portu LPT lub COM, system drukuje do portu LPR lub portu HP. Porty te i związane z nimi protokoły transportowe (transport protocols) muszą najpierw zostać zainstalowane. Częścią tej instalacji jest sterownik monitora portu (port monitor driver), taki jak LPRMON i HPMON.

System Windows 2003 Server oferuje efektywną komunikację z urządzeniami. Posiada obsługę ponad 3800 sterowników drukarek.

Publikowanie drukarek w usłudze katalogowej Active Directory ułatwia użytkownikom znajdowanie drukarek i nawiązywanie połączeń z drukarkami, zgodnie z przyjętymi kryteriami, takimi jak lokalizacja, możliwość sporządzania wydruków kolorowych czy szybkość druku.

Uprawnienia do drukarki

Uprawnienia do drukarki mogą być przypisywane użytkownikom, grupom lub użytkownikom i grupom jednocześnie. Wyróżniamy następujące rodzaje uprawnień:

Domyślnie wszyscy użytkownicy mają uprawnienie Print

Tab. 6. Uprawnienia do drukarki

Możliwości	No Access	Print	Manage Documents	Full Control
Drukowanie dokumentów		X	X	X
Wstrzymywanie, wznawianie, ponowne uruchamianie i anulowanie wydruku własnych dokumentów		X	X	X
Podłączanie się do drukarki		X	X	X
Kontrolowanie ustawień zadań drukowania dla wszystkich dokumentów			X	X
Wstrzymywanie, ponowne uruchamianie i usuwanie wydruku wszystkich dokumentów			X	X
Udostępnianie drukarki				X
Zmiana właściwości drukarki				X
Usuwanie drukarek				X
Zmiana uprawnień do drukarki				X

4.4.2. Pytania sprawdzające

Odpowiadając na pytania sprawdzisz, czy jesteś przygotowany do wykonania ćwiczeń.
1. Jakie możliwości drukowania daje Windows 2003 Server?
2. Jakie prawa do drukowania można przypisać użytkownikom?
3. Jakich protokołów używa się do drukowania na urządzeniu sieciowym?
4. Czy można udostępnić drukarkę na Windows 2003 Server?
5. Czy można publikować drukarki w Active Directory?

4.4.3. Ćwiczenia

Ćwiczenie 1

Zainstaluj drukarkę na serwerze.

Sposób wykonania ćwiczenia

Aby wykonać ćwiczenie powinieneś:
1) uruchomić komputer z systemem Windows 2003 Serwer,
2) uruchomić w menu „Start" opcję „Ustawienia\drukarki i faksy",
3) wybrać opcję „Dodaj drukarkę",
4) zainstalować drukarkę na serwerze,
5) wykonać wydruk próbny.

Wyposażenie stanowiska pracy:
- komputer z systemem Windows 2003 Server,
- drukarka podłączana do portu LPT lub USB,
- poradnik dla ucznia.

Ćwiczenie 2

Udostępnij drukarkę innym użytkownikom.

Sposób wykonania ćwiczenia

Aby wykonać ćwiczenie powinieneś:
1) uruchomić komputer z systemem Windows 2003 Server,
2) zalogować się z uprawnieniami administracyjnymi,
3) uruchomić w menu „Start" opcję „Ustawienia\drukarki i faksy",
4) wybrać z menu „Plik" opcję „Udostępnianie",
5) udostępnić drukarkę pod nazwą udziału „drukarka_1".

Wyposażenie stanowiska pracy:
- komputer z systemem Windows 2003 Server,
- drukarka podłączana do portu LPT lub USB,
- poradnik dla ucznia,

Ćwiczenie 3

Zainstaluj udostępnioną drukarkę na stacji roboczej.

Sposób wykonania ćwiczenia

Aby wykonać ćwiczenie powinieneś:
1) uruchomić stację roboczą z uprawnieniami administracyjnymi,
2) uruchomić w menu „Start" opcję „Ustawienia\drukarki i faksy",
3) wybrać opcję „Dodaj drukarkę",
4) odnaleźć w sieci udostępnioną drukarkę,
5) zainstalować drukarkę na stacji roboczej.

Wyposażenie stanowiska pracy:
- komputer z systemem Windows Server z udostępnioną drukarką,
- stacja robocza z możliwością logowania w domenie,
- nośniki ze sterownikami do drukarki,
- poradnik dla ucznia.

4.4.3. Sprawdzian postępów

Czy potrafisz?

		Tak	Nie
1)	zainstalować drukarkę na serwerze?	☐	☐
2)	udostępnić drukarkę innym użytkownikom?	☐	☐
3)	zainstalować drukarkę na stacji roboczej?	☐	☐
4)	zainstalować w sieci drukarkę sieciową?	☐	☐
5)	zainstalować drukarkę sieciową na stacji roboczej?	☐	☐

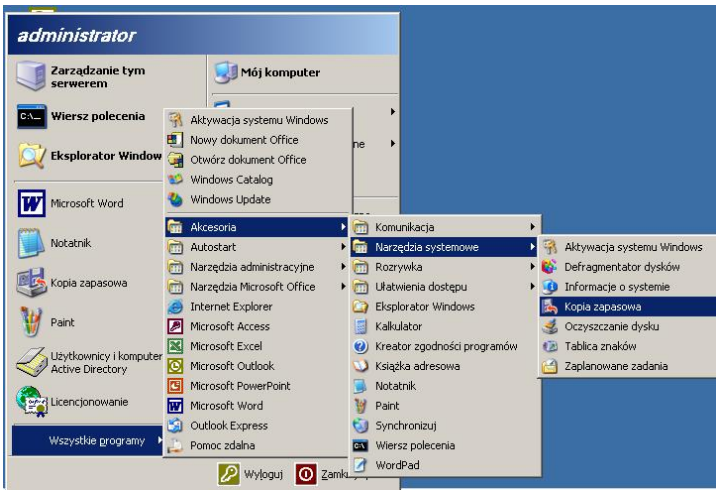
4.5. Archiwizacja danych

4.5.1. Materiał nauczania

Archiwizację danych znajdujących się na serwerze możemy wykonać przy pomocy wbudowanego narzędzia do tworzenia kopii zapasowych.

Systematyczne tworzenie kopii zapasowych lokalnych dysków twardych stanowi zabezpieczenie przed utratą danych w przypadku zdarzeń losowych jak, awarii napędów, błędów kontrolerów dyskowych, zaników zasilania, wirusów. Dobrze zaplanowane kopie zapasowe, powodują, że odzyskiwanie danych jest łatwiejsze i pochłania mniej czasu. Kopie zapasowe pozwalają również na odzyskiwanie danych skasowanych przez użytkowników.

Do tworzenia kopii zapasowych służy program „Kopia Zapasowa", dostępny poprzez menu Start/Programy/Akcesoria/Narzędzia systemowe/Kopia zapasowa.



Rys. 41. Uruchamianie kreatora kopii zapasowej

Programu można używać do tworzenia kilku różnych typów kopii zapasowych.

Kopia normalna polega na skopiowaniu wszystkich wybranych plików i oznaczeniu każdego z nich jako zarchiwizowanego. Kopie normalne są najłatwiejsze w użyciu podczas odzyskiwania plików, ponieważ wymagają jedynie posiadania najświeższego pliku. Wykonywanie kopii normalnych zajmuje najwięcej czasu, ponieważ kopiowany jest każdy plik, niezależnie od tego czy został zmieniony od czasu tworzenia ostatniej kopii zapasowej, czy nie.

Kopia przyrostowa polega na kopiowaniu jedynie tych plików, które zostały utworzone lub zmienione od czasu utworzenia ostatniej kopii przyrostowej lub normalnej oraz na oznaczeniu ich jako zarchiwizowanych. Pozwala to na skrócenie czasu potrzebnego do tworzenia kopii zapasowej. Przed utworzeniem pierwszej kopii przyrostowej, powinno się utworzyć normalną kopię systemu. Jeżeli korzysta się z kombinacji kopii normalnych oraz przyrostowych, to do odtworzenia danych trzeba koniecznie posiadać, w chronologicznym porządku, ostatnio utworzoną kopię normalną oraz wszystkie kolejne kopie przyrostowe.

Kopia różnicowa polega na kopiowaniu jedynie tych plików, które zostały utworzone lub zmienione od czasu utworzenia ostatniej kopii normalnej lub przyrostowej. Pozwala to skrócić czas konieczny do jej utworzenia. Podczas wykonywania kopii różnicowej kopiowane pliki nie są oznaczane jako zarchiwizowane. Przed utworzeniem pierwszej kopii różnicowej zalecane jest wykonanie pełnej kopii normalnej. Jeżeli korzysta się z kombinacji kopii

normalnych oraz różnicowych, to do odtworzenia danych trzeba koniecznie posiadać ostatnią kopię normalną oraz ostatnią kopię różnicową.

Kopia – wszystkie wybrane pliki są kopiowane, ale nie są oznaczane jako zarchiwizowane. Jest to działanie przydatne, gdy chce się zabezpieczyć dane pomiędzy poszczególnymi operacjami tworzenia kopii normalnych i przyrostowych bez zmiany listy archiwizowanych przez nie plików.

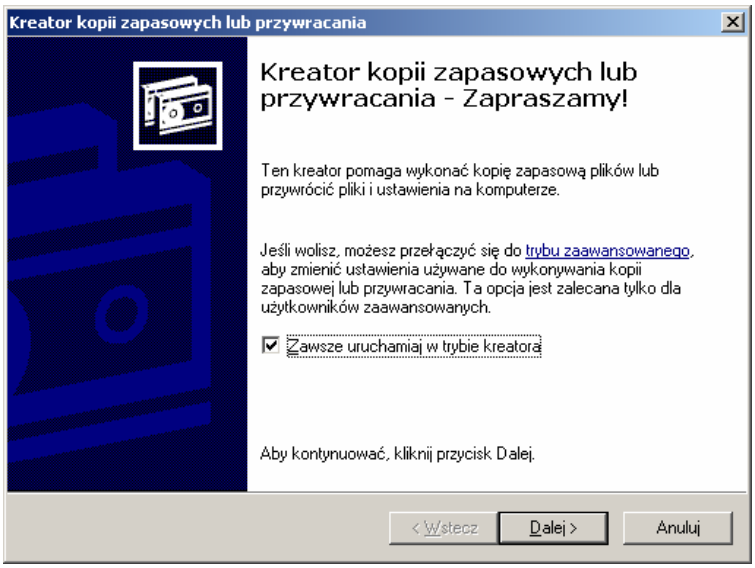
Codzienna kopia zapasowa uwzględnia wszystkie pliki spośród wybranych, które zostały zmodyfikowane w dniu jej wykonywania. Nie są one zaznaczane jako zarchiwizowane.

Pewne rodzaje kopii zapasowych korzystają ze znacznika, zwanego atrybutem archiwizacji. Umożliwia on śledzenie, kiedy dany plik został ostatnio uwzględniony w kopii zapasowej. Jeżeli plik zostanie zmieniony, to system Windows 2003 Server automatycznie oznacza go jako wymagający ponownej archiwizacji. Pliki i katalogi, które zostały przeniesione, nie są w ten sposób oznaczane. Program Kopia zapasowa umożliwia archiwizację wszystkich plików lub jedynie tych, które posiadają ten znacznik ustawiony, a także określenie czy po zarchiwizowaniu mają być one odpowiednio oznaczane.

Tworzenie kopii należy zaplanować na moment, gdy wszystkie aplikacje są zamknięte oraz nikt nie korzysta z udziałów sieciowych w komputerze, w którym tworzona jest kopia zapasowa. Pliki, które są otworzone i używane podczas operacji tworzenia kopii zapasowej, z reguły nie są zarchiwizowane.

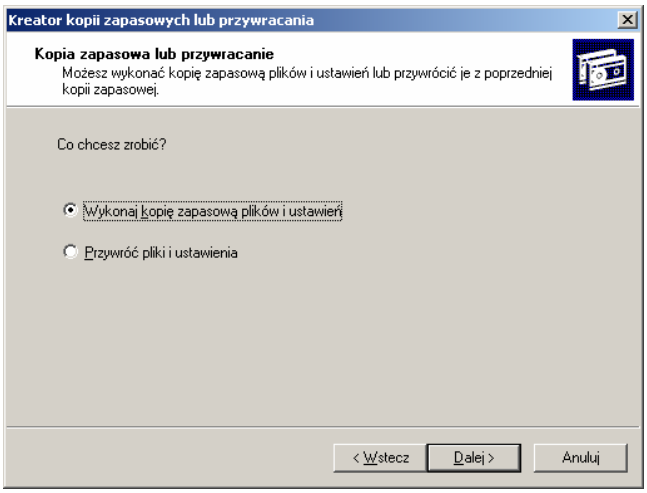
Wykonywanie kopii zapasowych

Uruchamiamy program kopia zapasowa. Po uruchomieniu pojawiają się kolejne okna kreatora.



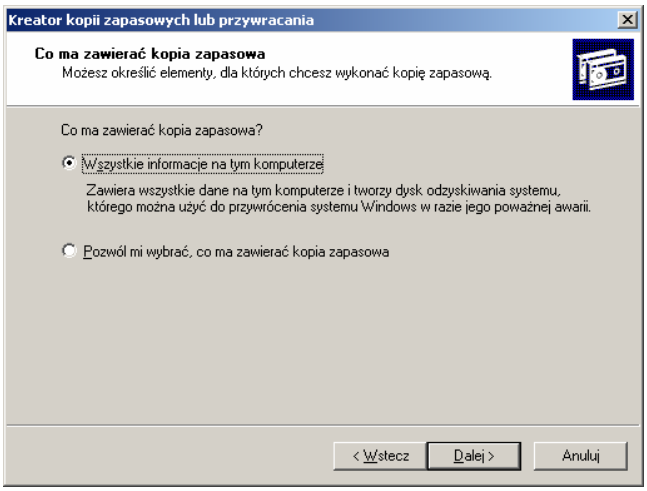
Rys. 42. Kreator kopii zapasowej

Na następnym ekranie mamy dwa rodzaje zadań do wykonania: Wykonaj kopię zapasową – tutaj tworzymy kopie zapasowe; Przywróć pliki i ustawienia – służy do odtwarzania danych z kopii zapasowej.



Rys. 43. Konsola wyboru Wykonaj/Przywróć

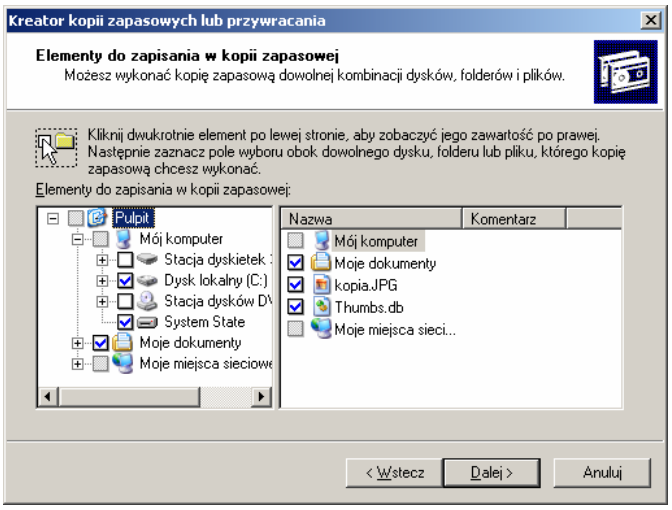
Kolejne okno pozwala nam wybrać elementy kopii zapasowej, to jest czy chcemy zrobić kopię wszystkich informacji na dysku lub tylko wybranych.



Rys. 44. Konsola wyboru zawartości kopii

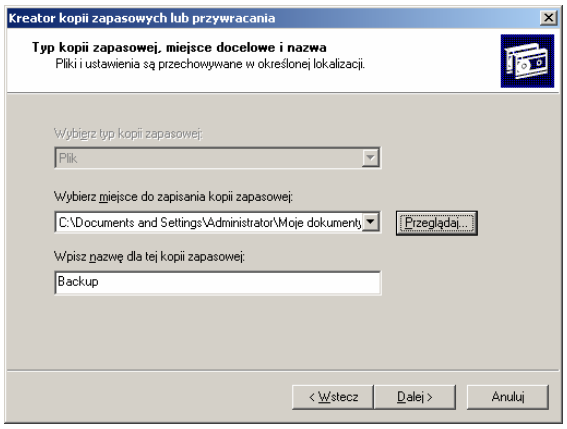
Powyższe ustawienia pozwalają na:

- wykonanie kopii wszystkich danych znajdujących się na komputerze – zazwyczaj opcja ta nie będzie używana – potrzeba odpowiednio dużego nośnika oraz czasu i zwykle nie potrzeba robić kopii, na przykład plików systemowych, aplikacji,
- wykonanie kopii zapasowej użytkowników – będzie można wskazać foldery, z których będzie zrobiona kopia, zarówno lokalne, jak i sieciowe – najczęściej będziemy robić kopię zapasową folderu „Redirected”, w którym przechowywane są dane użytkowników.



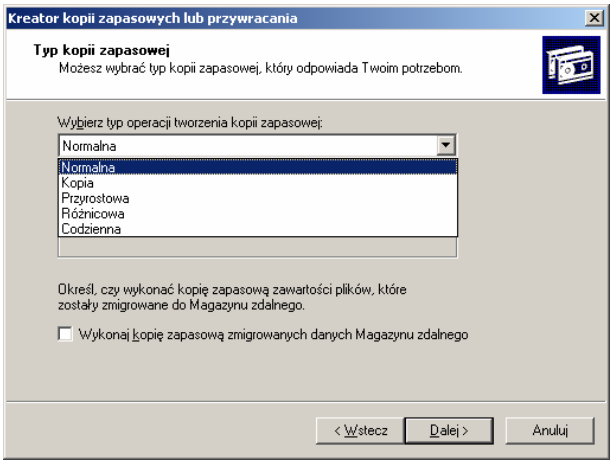
Rys. 45. Zaawansowana konsola wyboru zawartości kopii

Po kliknięciu na opcję „Dalej” ukazuje się kolejne okno wyboru miejsca zapisu kopii oraz jej nazwy.



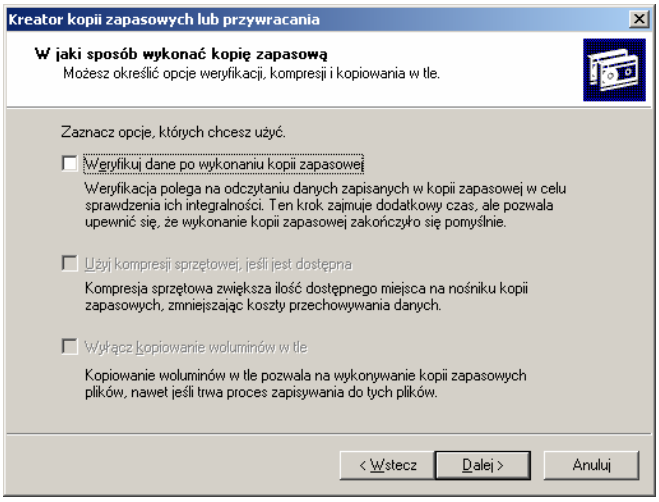
Rys. 46. Wybór miejsca tworzenia i nazwy kopii

W kolejnym kroku kreator daje nam możliwość wybrania opcji zaawansowanych, w których możemy określić rodzaj kopii,



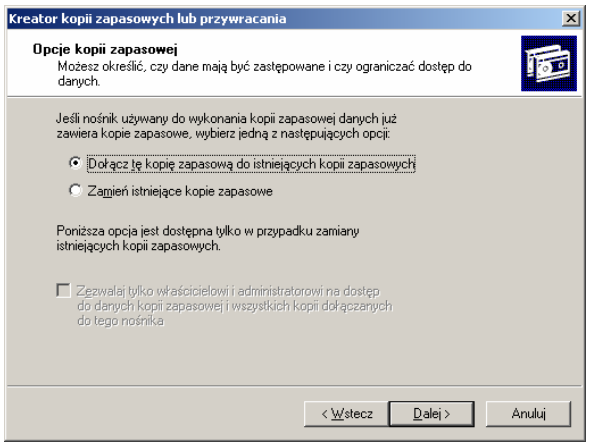
Rys. 47. Wybór rodzaju kopii

weryfikację i kompresję,



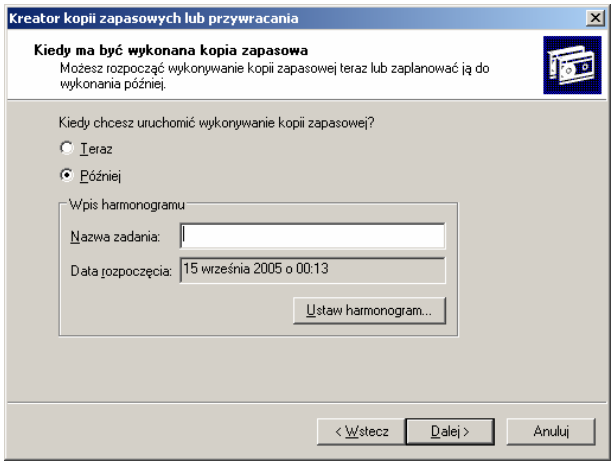
Rys. 48. Weryfikacja i kompresja kopii

sposób zapisu (zastąpienie poprzedniej lub utworzenie nowej kopii),



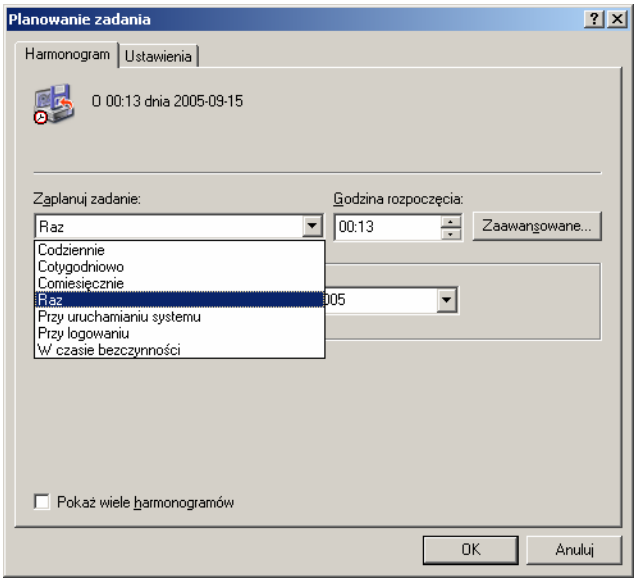
Rys. 49. Sposób zapisu kopii

termin wykonania kopii



Rys. 50. Wybór terminu wykonania kopii

oraz terminarz wykonywania kopii zapasowej.



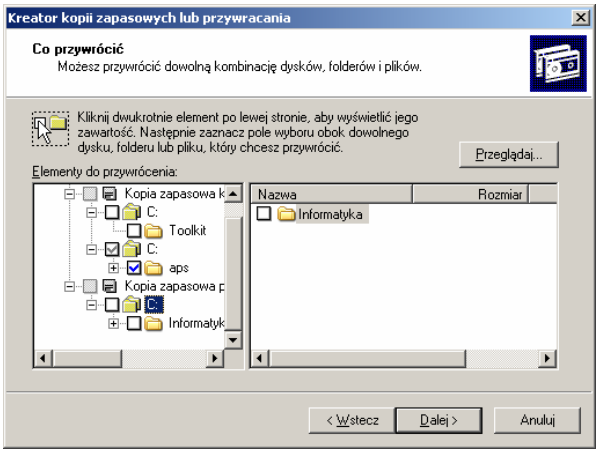
Rys. 51. Terminarz wykonywania kopii zasobu

Na koniec system weryfikuje nasze uprawnienia do tworzenia kopii.

Odtwarzanie kopii zapasowej

Odtwarzanie kopii zapasowej zaczynamy dokładnie jak tworzenie wybierając w menu Start\progarmy\Akcesoria\Narzędzia systemowe\Kopia zapasowa. W pierwszym oknie kreatora kopii zapasowych\przywracania klikamy na przycisk dalej. W następnym oknie wybieramy opcję „Przywróć pliki i ustawienia".

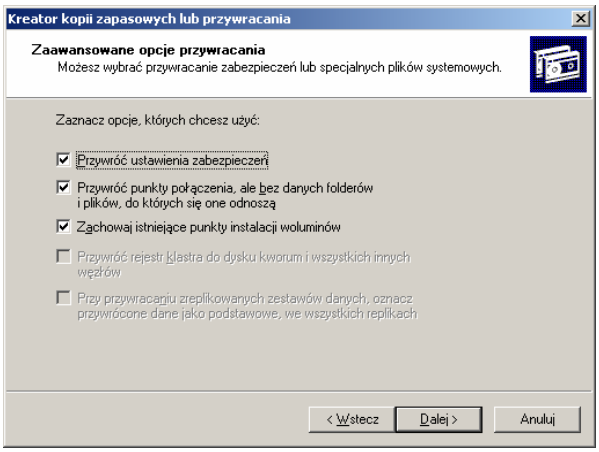
Następnie mamy okno pozwalające na wybór kopi, którą chcemy odtworzyć.



Rys. 52. Wybór kopii do odtworzenia

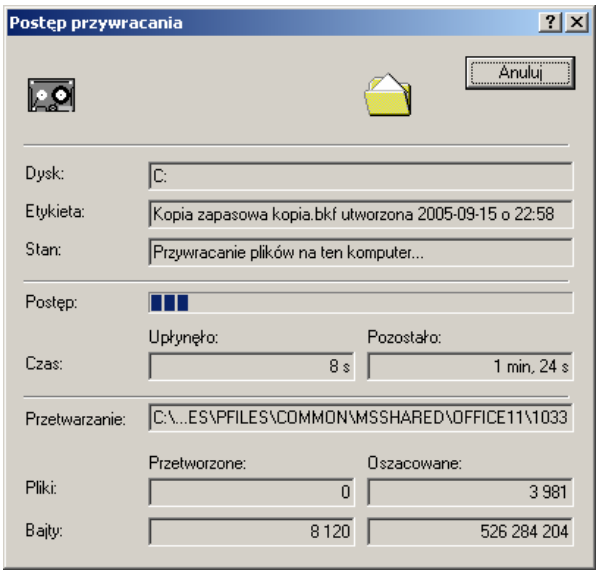
Wybranie opcji „Dalej" powoduje przejście do okna kończącego proces odtwarzania. W oknie tym mamy jeszcze przycisk „zaawansowane", gdzie podobnie jak przy tworzeniu kopii możemy ustalić dodatkowe parametry odtwarzania – lokalizację przywracania, wybór opcji nadpisania bądź zachowania istniejących plików.

Kolejne okno pozwala wybrać opcje przywracania zabezpieczeń.



Rys. 53. Przywracanie zabezpieczeń

Potwierdzenie wyboru powoduje przejście do okna kończącego, a następnie rozpoczęcie odtwarzania zgodnie z wybranymi opcjami.



Rys. 54. Postęp procesu przywracania

4.5.2. Pytania sprawdzające

Odpowiadając na pytania, sprawdzisz, czy jesteś przygotowany do wykonania ćwiczeń.

1. W jakim celu wykonuje się archiwizację danych?
2. Jak nazywa się narzędzie systemowe pozwalające na archiwizację danych?
3. Jakiego rodzaju kopie możemy wykonywać?
4. Kiedy powinno się robić kopię zapasową ?
5. Jakim narzędziem systemowym odtwarzamy kopię zapasową?

4.5.3. Ćwiczenia

Ćwiczenie 1

Zrób kopię zapasową folderu „Documents and Settings”.

Sposób wykonania ćwiczenia

Aby wykonać ćwiczenie powinieneś:
1) uruchomić komputer z systemem Windows 2003 Server,
2) wybrać w menu „Start\progarmy\Akcesoria\Narzędzia systemowe\Kopia zapasowa”,
3) wybrać opcję „Wykonaj kopię zapasową plików i ustawień”,
4) wybrać do archiwizacji folder „Document and Settings”,
5) wykonać kopię zapasową.

Wyposażenie stanowiska pracy:
- komputer z systemem Windows 2003 Server,
- poradnik dla ucznia.

Ćwiczenie 2

Ustal harmonogram wykonywania kopii zapasowej folderu „aplikacje” (należy utworzyć taki folder i skopiować do niego pliki o wielkości około 10 MB).

Sposób wykonania ćwiczenia

Aby wykonać ćwiczenie powinieneś:
1) uruchomić komputer z systemem Windows 2003 Server,
2) utworzyć folder „Aplikacje”,
3) skopiować do folderu „Aplikacje” pliki o wielkości około 10 MB,
4) wybrać w menu „Start\progarmy\Akcesoria\Narzędzia systemowe\Kopia zapasowa”,
5) wybrać opcję „Wykonaj kopię zapasową plików i ustawień”,
6) wybrać do archiwizacji folder „Aplikacje”,
7) ustalić harmonogram wykonywania kopii zapasowej tak, aby tworzenie zaczęło się po upływie około 5 min po zakończeniu pracy z kreatorem,
8) zaobserwować rozpoczęcie tworzenia kopii.

Wyposażenie stanowiska pracy:
- komputer z systemem Windows 2003 Server,
- poradnik dla ucznia.

Ćwiczenie 3

Odtwórz kopie zapasowa folderu „Documents and Settings”.

Sposób wykonania ćwiczenia

Aby wykonać ćwiczenie powinieneś:
1) uruchomić komputer z systemem Windows 2003 Server,
2) wybrać w menu Start\progarmy\Akcesoria\Narzędzia systemowe\Kopia zapasowa”,
3) wybrać opcję Przywróć pliki i ustawienia,
4) wybrać do odtworzenia kopie folderu „Documents and Settings”,
5) odtworzyć z kopi folder „Documents and Settings”.

Wyposażenie stanowiska pracy:
- komputer z systemem Windows 2003 Server,
- poradnik dla ucznia.

Ćwiczenie 4

Zarejestruj dane o wydajności systemu

Sposób wykonania ćwiczenia

Aby wykonać ćwiczenie powinieneś:
1) zalogować się z uprawnieniami administratora na serwerze
2) uruchomić konsolę „Wydajność”,
3) wybrać opcję „Dzienniki wydajności i alerty”,
4) zaznaczyć opcję „Dzienniki liczników”,
5) wybrać w szczegółach opcję „Ustawienia nowego dziennika”,
6) utworzyć plik dziennika o nazwie „wydajność” i dodać do niego obiekty „Dysk logiczny”, „Dysk fizyczny” oraz „Kolejki robocze serwera”,
7) wybierz okresu próbkowania równy 8 sekund,
8) kliknij przycisk OK,
9) wykonać pewne czynności na komputerze,
10) przerwać rejestrowanie danych po ok. 1 minucie (w programie Dzienniki wydajności i alerty),
11) wyświetlić w Monitorze systemu dane dziennika i otworzyć plik dziennika utworzonego podczas testu.

Wyposażenie stanowiska pracy:
- komputer z systemem Windows 2003 Server,
- poradnik dla ucznia.

4.5.4. Sprawdzian postępów

Czy potrafisz?

		Tak	Nie
1)	wykonać kopię zapasową dowolnego folderu?	☐	☐
2)	wykonać kopię zapasową całego dysku?	☐	☐
3)	ustalić harmonogram wykonywania kopii zapasowej?	☐	☐
4)	odtworzyć dowolny folder z kopii zapasowej?	☐	☐

5. SPRAWDZIAN OSIĄGNIĘĆ

INSTRUKCJA DLA UCZNIA

1. Przeczytaj uważnie instrukcję.
2. Podpisz imieniem i nazwiskiem kartę odpowiedzi.
3. Zapoznaj się z zestawem zadań testowych.
4. Udzielaj odpowiedzi tylko na załączonej karcie odpowiedzi.
5. Zestaw zadań testowych składa się z zadań wielokrotnego wyboru.
6. Zadania typu wielokrotnego wyboru mają 4 wersje odpowiedzi, z których tylko jedna jest prawidłowa. Prawidłową odpowiedź należy zakreślić we właściwym miejscu na karcie odpowiedzi.
7. W przypadku pomyłki błędną odpowiedź należy zakreślić kółkiem i ponownie zakreślić odpowiedź prawidłową.
8. Jeżeli udzielenie odpowiedzi na jakieś pytanie sprawia Ci trudność, to opuść je i przejdź do zadania następnego. Do zadań bez odpowiedzi możesz wrócić później.

Powodzenia !

ZESTAW ZADAŃ TESTOWYCH

1. Technologia NT to:
   a) technologia budowy maszyn,
   b) system operacyjny,
   c) system operacyjny z funkcjami zabezpieczeń,
   d) system plików.

2. Ile istnieje wersji systemu NT:
   a) 2,
   b) 6,
   c) 4,
   d) 3.

3. System plików określa:
   a) sposób organizacji zapisu plików na dysku,
   b) sposób zapisu katalogów,
   c) rodzaj uporządkowania danych w pliku,
   d) miejsce zapisu dokumentów.

4. FAT to:
   a) rejestr użytkowników,
   b) system alokacji plików,
   c) nazwa systemu operacyjnego,
   d) sposób zapisu danych na CD.

5. NTFS został użyty po raz pierwszy w:
   a) Windows 98,
   b) Windows nt,
   c) Windows me,
   d) Windows 2000.

6. Maksymalny rozmiar woluminu w systemie FAT 32 jest ograniczony do:
   a) powyżej 32 GB,
   b) 2 GB,
   c) 6 GB,
   d) 32 GB.

7. C2 to:
   a) zestaw poleceń systemowych,
   b) konsola administracyjna,
   c) klasa poziomu zabezpieczeń systemu,
   d) poprzednik c3.

8. Orange Book opublikowano w:
   a) Wielkiej Brytanii,
   b) Kanadzie,
   c) Australi,
   d) USA.

9. TCSEC dotyczy:
   a) kryteriów zabezpieczeń,
   b) systemu plików,
   c) pliku alokacji,
   d) administracji kontami.

10. TCSEC definiuje:
   a) 3 klasy,
   b) 5 klas,
   c) 7 klas,
   d) 9 klas.

11. Bezpieczeństwo systemu zależy od:
   a) systemu,
   b) systemu i sposobu zarządzania,
   c) systemu i Active Directory,
   d) Active Directory i konsol.

12. Podstawowym systemem plików Windows XP jest:
   a) FAT32,
   b) FAT16,
   c) NTFS,
   d) TCSEC.

13. Skróty MAC i DAC dotyczą
   a) nazw konsol administracyjnych,
   b) kodowania,
   c) konsole Active Directory,
   d) rozszerzenia uprawnień użytkownika.

14. Jednostki alokacji w NTFS są:
   a) większe niż w FAT 32,
   b) mniejsze niż w FAT 32,
   c) takie same jak w FAT 32,
   d) takie jak w fat16.

15. MFT to:
   a) indeks plików systemowych,
   b) jednostka alokacji plików,
   c) sposób odczytu danych,
   d) rozszerzenie aplikacji Active Directory.

KARTA ODPOWIEDZI

Imię i nazwisko .....

Zakreśl poprawną odpowiedź.

Nr zadania	Odpowiedź				Punkty
1	a	b	c	d	
2	a	b	c	d	
3	a	b	c	d	
4	a	b	c	d	
5	a	b	c	d	
6	a	b	c	d	
7	a	b	c	d	
8	a	b	c	d	
9	a	b	c	d	
10	a	b	c	d	
11	a	b	c	d	
12	a	b	c	d	
13	a	b	c	d	
14	a	b	c	d	
15	a	b	c	d	
				RAZEM	

6. LITERATURA

1. Morimoto R., Noel M., Droubi O., Gardinier K., Neal N.: Windows Server 2003. Księga eksperta, tłum. Jarczyk A., Miszkiel T., Pilch P., Helion 02/2004
2. Rampling B.: Windows Server 2003. Bezpieczeństwo. Biblia, tłum. Koronkiewicz P., Helion 11/2003
3. Ruest N., Ruest D.: Windows Server 2003. Podręcznik administratora, tłum.: Jarczyk A. Helion 03/2004
4. Simpson A.: Windows XP PL Biblia, tłum. Gołębiewski M., Pilch P., Słodownik K., Helion 02/2003
5. Źródła internetowe.