Windows 2003

Ćwiczenia

Piotr Fulmański

Piotr Fulmański[1]

Wydział Matematyki i Informatyki,
Uniwersytet Łódzki
Banacha 22, 90-238, Łódź
Polska

e-mail 1: fulmanp@math.uni.lodz.pl

Data ostaniej modyfikacji: **9 lutego 2008**

Spis treści

Rozdział 1

Pozostanie bez tytułu

Niniejszy dokument stanowi moje własne **notatki** jaki sporządzam dla siebie przygotowując się do zajęć poświęconych systemowi operacyjnemu Windows Server 2003. Zdając sobie sprawę z ograniczeń własnej osoby udostępniam je z nadzieją na pomoc w uporządkowaniu prezentowanego przeze mnie materiału.

Rozdział 2

Wprowadzenie

2.1 Czym jest Windows Server 2003?

Windows Server 2003 jest serwerowym systemem operacyjnym produkcji Microsoft wprowadzonym na rynek 24 kwietnia 2003 roku jako następca Windows 2000 Server. Niektórzy nazywają go dużym pakietem Service Pack dla Windows 2000, inni zachwalają jako od dawno oczekiwaną, napisaną na nowo wersję systemu operacyjnego Windows. Można powiedzieć, że i jedni i drudzy mają po trochu rację. Z estetycznego ponktu widzenia Windows Server 2003 może być postrzegany jak graficzny interfejs użytkownika Windows XP nałożony na stary serwerowy system operacyjny Windows 2000 z kilkoma dodatkowymi narzędziami. Kiedy jednak przyjrzymy się uważnie, zobaczymy, że Windows Server 2003 jest znacznie zmodyfikowaną wersją systemu Windows 2000, z poważnymi zmianami wprowadzonymi w jądrze, dzięki którym Windows Server 2003 zapewnia większą niezawodność, odporność na błędy i skalowalność.

2.2 Rodzina systemów Windows Server 2003

Wprowadzając na rynek system Windows Server 2003 zamiast dotychczasowych wersji Server i Advanced Server udostępniono cztery odmiany systemu Windows Server 2003:

- Windows Server 2003, Web Edition,
- Windows Server 2003, Standard Edition,
- Windows Server 2003, Enterprise Edition,
- Windows Server 2003, Datacenter Edition.

2.2.1 Windows Server 2003, Web Edition

Celem umożliwienia produktom Microsoftu konkurowania z innymi rozwiązaniami na polu usług sieciowych (webowych) powstała specjalna dostosowana do tego celu wersja systemu. Funkcjonalność systemu pozwala na łatwe tworzenie usług i aplikacji sieciowych (ang. *Web pages, Web sites, Web applications, and Web services*).

Wersja Web Edition obsługuje do 2 GB RAM i dwa procesory (SMP). Umożliwia nawiązanie nielimitowanej ilości połączeń anonimowych z sieci i zdalne administrowanie systemem za pomocą Remote Desktop, ale nie udostępnia tradycyjnych usług terminalowych. Dołączona wersja Microsoft SQL Server Database Engine obsługuje do 25 różnych połączeń.

Wersja Web Edition nie nadaje się dla organizacji, chcących zainstalować tanim kosztem serwer plików, drukowania i dodatkowej infrastruktury jak DNS, DHCP czy kontroler domeny. Nie pozwala on bowiem na dostęp wielu użytkowników do plików i drukowania ani nie zawiera usług infrastruktury. Aby otrzymać funkcjonalność inną niż usługi skupione wokół WWW, trzeba wykorzystać co najmniej Windows Server 2003 Standard Edition.

2.2.2 Windows Server 2003, Standard Edition

Windows Server 2003 Standard Edition jest najbardziej powszechną wersją tego systemu operacyjnego spełniającą z powodzeniem zapotrzebowania małych i średnich organizacji. Obsługuje do czterech procesorów i maksymalnie 4GB RAM. W pełni obsługuje usługi plików i drukowania. Może pełnić także funkcję serwera WWW, poczty, obsługuje usługi terminalowe a także może spełniać rolę serwera infrastruktury.

2.2.3 Windows Server 2003, Enterprise Edition

Wersja Windows Server 2003 Enterprise Edition jest przeznaczona dla systemów serwerowych działających w średnich i dużych organizacjach. Obsługuje do ośmiu procesorów i (lub) klastrów o maksymalnie 8 węzłach oraz do 32GB RAM. Dostępna jest także 64-bitowa wersja obsługująca do 64GB RAM i ośmiu procesorów/klastrów. Dla organizacji wykorzystujących funkcjonalność Thin Client Terminal Services (usługi terminalowe dla uproszczonych klientów) systemu Windows Server 2003, która wymaga dużej ilości pamięci RAM i wielu procesorów, wersja Enterprise potrafi obsłużyć setki użytkowników w jednym serwerze.

Z dodatkowych udogodnień warto wymienić możliwość dodania pamięci RAM w trakcie pracy systemu (ang. *Hot Add Memory*), Windows System Resource Manager (WSRM), wspierający przydzielanie zasobów takich jak procesor czy pamięć na poszczególne aplikacje.

2.2.4 Windows Server 2003, Datacenter Edition

Wersja Datacenter Edition dostępna jest tylko jako wersja OEM sprzedawany wyłącznie z dedykowanymi systemami mającymi z założenia spełniać wysokie standardy wydajności, niezawodności i obsługi. Tak więc nie może po prostu kupić tej wersji systemu i samemu zbudować własnego systemu (w sensie sprzęt + system operacyjny).

System w tej wersji wspiera na platformach 32-bitowych do 32 procesorów i 64 GB RAM i na platformach 64-bitowych do 64 procesorów i 512 GB RAM.

Z dodatkowych udogodnień warto wymienić możliwość wykorzystania mechanizmów przejmowania funkcji pomiędzy systemami w klastrze w razie awarii.

Rozdział 3

Instalacja systemu i usługa Active Directory

3.1 Instalacja systemu

Instalacja systemu w najbardziej podstawowej wersji nie jest zadaniem trudnym i z wyjątkiem kilku miejsc, gdzie należy np. podać hasło dla administratora, nie wymaga większej uwagi ze strony użytkownika.

3.1.1 Opis procesu instalacji

Kiedyś będzie tutaj opis instalacji.

Po zakończeniu procesu instalacji i zalogowaniu się do systemu uruchomiona zostanie strona Manage Your Server (Zarządzanie tym serwerem), z której to możemy skonfigurować specyficzne role czy narzędzia zależnie od roli pełnionej przez system.

Wybór opcji Typical Configuration For A First Server spowoduje:

- utworzenie z serwera serwera domeny,
- zainstalowanie usługi Active Directory,
- zainstalownie usługi Domain Name Service (DNS),
- zainstalowanie usługi Dynamic Host Configuration Protocol (DHCP),
- zainstalowanie usługi Routing And Remote Access (RRAS).

Wybór opcji Custom Configuration daje nam możliwość konfiguracji następujących ról:

- **File Server.**
- **Print Server.**

- **Application Server.**
- **Mail Server.**
- **Terminal Server.**
- **Domain Controller (Active Directory).**
- **DNS Server.**
- **DHCP Server.**
- **Streaming Media Server.** Udostępnia usługi WMS (ang .*Windows Media Services*) pozwalające na przesyłanie danych multimedialnych.
- **WINS Server.** Umożliwia rozpoznawanie nazw komputerów dzięki translacji nazw NweBIOS na adresy IP.

3.2 Active Directory

3.2.1 Idea

drzewo(domena(firma.com),domena(m.firma.com))

3.2.2 LDAP – czyli katalogi

Protokół LDAP (ang. Lightweight Directory Access Protocol) służy do odpytywania i modyfikowania struktury katalogowej przez połączenie TCP/IP.

Katalog, w tym kontekście, jest zbiorem informacji zebranych i pogrupowanych w hierarchiczną strukturę. Przykładem może być katalog numerów telefonicznych złożony z nazw (czy to osób czy organizacji) posortowanych alfabetycznie wraz z odpowiadającym im numerem i ewentualnie adresem.

Katalog LDAP przyjmuje strukturę drzewiastą na wygląd której często wpływ mają położenie geograficzne zarządzanych obiektów, wewnętrzna struktura organizacji itp. Dzisiejsze instalacje LDAP preferują użycie systemu nazewniczego DNS (ang. Domain Name System) dla elementów najwyżej położonych w hierarchii. Poniżej mogą zanjdować się obiekty reprezentujące ludzi, jednostki organizacyjne, drukarki, dokumenty, grupy użytkowników, komputery i wiele innych.

Obecna wersja protokołu LDAP jest wersja 3 (LDAPv3) a jej specyfikację znaleźć można w dokumencie RFC 4510.

3.2.3 Domeny, drzewa i lasy

Active Directory nie może istnieć bez przynajmniej jednej domeny (ang. *domian*) i na odwrót. Czym jest domena? Osobom znającym pojęcie domeny występujące w sieciach komputerowych można powiedzieć, że domena usługi Active Directory podobna jest do domeny sieciowej/Internetowej. A co można powiedzieć pozostałym? Najprościej chyba, to to, że domena jest pewnym sposobem logicznego wyodrębnienia pewnego fragmentu większej całości. To tak jak mówimy, że ktoś interesuje się informatyką, ale domeną jego zainteresowań są systemy operacyjne. Wiele domen tworzy strukturę logiczną nazywaną drzewem (ang. *tree*). Struktura ta nazywana jest drzewem gdyż zachowuje ona zależności pomiędzy nazwami, przez co przypomina swym wyglądem drzewo.

```
+-com               (com)
  |
  +-organizacja1    (organizacja1.com)
  | |
  | +-jednostka1    (jednostka1.organizacja1.com)
  | | |
  | | +-jednostka11 (jednostka11.jednostka1.organizacja1.com)
  | | +-jednostka12 (jednostka12.jednostka1.organizacja1.com)
  | +-jednostka2    (jednostka2.organizacja1.com)
  |   |
  |   +-jednostka21 (jednostka21.jednostka2.organizacja1.com)
  +-organizacja2    (organizacja2.com)
    |
    +-jednostka1    (jednostka1.organizacja2.com)
    +-jednostka2    (jednostka1.organizacja2.com)
      |
      +-jednostka21 (jednostka21.jednostka2.organizacja2.com)
      +-jednostka22 (jednostka22.jednostka2.organizacja2.com)
```

W sytuacji, gdy domeny nie współdzielą jednej domeny głównej (np. `com` w powyższym przykładzie), wówczas mamy wiele drzew a tym samym największą strukturę usługi Active Directory: las (ang. *forest*). Las usługi Active Directory zawiera wszystkie domeny tej usługi. Las może zawierać wiele domen w wielu drzewach lub tylko jedną domenę.

3.2.4 Obiekty i jednostki organizacyjne

Zasoby organizacji w usłudze Active Directory reprezentowane są jako obiekty lub rekordy bazy danych. Pod pojęciem zasób należy rozumieć wszystko co „należy” do danej organizacji:

- rzeczy materialnych dużego kalibru jak budynki i mieszczące się w nich pomieszczenia;
- rzeczy materialnych małego kalibru typu komputer, drukarka, stół;
- osoby związane z organizacją (np. pracujące w niej);
- logiczne związki i podział (np. podział na Dział płac i Dział kadr).

Każdy obiekt ma właściwości, które go definiują. Oczywiście zbiór właściwości różni się tak jak różnią się opisywane przez nie obiekty (np. wiadomo, że drukarka nie ma imienia, choć ma nazwę. Człowiek z kolei ma imię choć nie ma nazwy).

Ze względu na znaczne zróżnicowanie obiektów a także ich znaczną ilość opisywanym zasobom trzeba nadać jakąś strukturę usprawniającą ich zarządzanie (osobom przeciwnego zdania proponuje przegrać zawartość wszystkich katalogów w ich systemie do jednego tylko katalogu i spróbować normalnie pracować).

Wyodrębnienie czy powstanie takiej struktury możliwe jest dzięki specjalnym obiekom nazywanym jednostką organizacyjną (ang. *organizational unit*, OU). Wewnątrz domeny jednostki pełnią rolę kontenerów (pojemników) umożliwiających grupowanie „podobnych" obiektów. Podobieństwo oczywiście może być rozumiane na wiele różnych sposobów: funkcjonalne, organizacyjne, fizyczne. Poza czysto użytkową rolą jednostek organizacyjnych jaką jest wprowadzenie pewnego porządku umożliwiają one także bardziej zaawansowane zarządzanie jak na przykład przypisanie zasad bezpieczeństwa do wszystkich osób będących w danej jednostce organizacyjnej.

Active Directory jest implementacją protokołu usług katalogowych LDAP stworzoną przez Microsoft głównie celem wykorzystania w środowisku Windows. Zasadniczym celem jest dostarczenie usługi umożliwiającej scentralizowaną weryfikację i uwiarygodnianie usług dla komputerów pracujących pod kontrolą systemów Windows. Active Directory umożliwia także przydzielanie uprawnień, instalowanie oprogramownia (ang. deploy software) oraz wprowadzanie krytycznych poprawek w ramach całej organizacji. Active Directory przechowuje informacje i ustawienia związane z organizacją w centralnej bazie danych. Active Directory może zarządzać zarówno kilkoma obiektami jak i ich wieloma milionami.

Active Directory po raz pierwszy pojawiło się wraz z Windows 2000 Server a po wprowadzeniu usprawnień i modyfikacji wykorzystane zosyało w Windows Server 2003.

Active Directory wcześniej nazywane było NTDS (NT Directory Service).

3.2.5 Konfiguracja serwera

Skonfigurujemy teraz serwer jako pierwszy kontroler domeny (ang. *first domain controller*) w domenie Active Directory nazywanej `cwiczenia.com`

1. Otwórz moduł Manage Your Server (Zarządzanie tym serwerem) z grupy programów (Administrative Tools).

2. Kliknij opcję Add Or Remove A Role (Dodaj lub usuń rolę). Wyświetlone zostanie okno programu Configure Your Server Wizard (Kreator konfigurowania serwera).

3. Kliknięcie przycisku Next (Dalej) spowoduje wykrycie przez konfigurator ustawień sieci.

4. Wybierz opcję Typical Configuration For A First Server (Ustawienie typowe dla pierwszego serwera), a następnie kliknij przycisk Next (Dalej).

5. W polu przeznaczonym na nazwę domeny usługi Active Directory (Active Directory Domain Name) wpisz `cwiczenia.com`.

6. Sprawdź czy nazwa `CWICZENIA` wyświetlana jest w polu NetBIOS Domain Name, a następnie kliknij przycisk Next (Dalej).

7. Sprawdź zawartość okna Summary Of Selections (Podsumowanie ustawień); powinno w nim być:

   - Install DHCP server
   - Install Active Directory and DNS server
   - Create the followinf full domain name: cwiczenia.com

   Kliknij Next (Dalej). Program Configure Your Server Wizard (Kreator konfiguracji tego serwera) wyświetli komunikat z informacją o konieczności ponownego uruchomienia systemu i poprosi o zakończenie wszystkich działających aplikacji.

8. Kliknij Yes (Tak).

9. Po ponownym uruchomieniu komputera zaloguj się jako Administrator.

10. W oknie programu Configure Your Server Wizard (Konfigurowanie tego serwera) można będzie obserwować ostatnie etapy instalacji.

11. Kliknij Next (Dalej) a następnie Finish (Zakończ).

12. Uruchom program Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) z grupy programów Administrative Tools (Narzędzia administracyjne). Sprawdź czy w systemie jest domena o nazwie `cwiczenia.com` oraz czy w węźle Domain Controllers (Kontrolery domeny) znajduje się konto komputera dla servera WIN2003TUT.

Rozdział 4

Początki administracji

4.1 Konsola MMC

Microsoft Management Console Każda konsola MMC zawiera co najmniej jedno narzędzie nazywane przystawką. Przystawka rozbudowuje konsolę MMC dodając do niej specyficzne możliwości zarządzania i dodatkową funkcjonalność. Funkcjonalne składniki konsoli MMC znajdują się wewnątrz elementów nazywanych przystawkami. To przystawki (ang. *Snap-in*) a nie sama konsola MMC stanowią narzędzie używane w administracji. Wygląd poszczególnych konsol różni się znacznie, w zależności od przeznaczenia i funkcji dołączonych przystawek.

Występują dwa rodzaje przystawek: autonomiczne oraz rozszerzenia.

4.1.1 Tworzenie i zapisywanie konsoli

1. Kliknij menu Start, a następnie kliknij opcję Run (Uruchom).
2. W polu tekstowym Open (Otwórz) wpisz polecenie mmc i kliknij przycisk OK.
3. Wybierz z menu File (Plik) opcję Options (Opcje).
4. Sprawdź, czy w oknie rozwijanej listy Console Mode (Tryb konsoli) wybrany jest tryb Author (Autorski), a następnie kliknij przycisk OK.
5. W menu File (Plik) kliknij opcje Add/Remove Snap-In (Dodaj/Usuń przystawkę).
6. Kliknij przycisk Add (Dodaj). Wyświetlone zostanie okno Add Standalone Snap-In (Dodawanie przystawki autonomicznej).
7. Odszukaj przystawkę Event Viewer (Podgląd zdarzeń), zaznacz ją, a następnie kliknij przycisk Add (Dodaj).

8. W oknie dialogowym Select Computer (Wybierz komputer), umożliwiajacym wybór administrowanego komputera, wybierz opcje Local Computer i kliknij Finish (Zakończ).

9. W oknie dialogowym Add Standalone Snap-In kliknij przycisk Close (Zamknij), a następnie w oknie Add/Remove Snap-In kliknij przycisk OK.

10. Zapisz konsole jako MyPrivateConsole.

4.1.2 Konfiguracja przystawki do pracy zdalnej

4.1.3 Połączenie zdalne za pomocą konsoli MMC

1. Otwórz zapisaną wcześniej konsolę MyPrivateConsole.

2. W menu File kliknij opcje Add/Remove Snap-In.

3. Kliknij przycisk Add. Wyświetlone zostanie okno Add Standalone Snap-In.

4. Odszukaj przystawkę Computer Management, a następnie kliknij przycisk Add.

5. W oknie dialogowym Computer Management znajdź opcję Another Computer (Inny komputer).

6. Wpisz adres IP zdalnego komputera a następnie kliknij przycisk Finish.

7. W oknie dialogowym Add Standalone Snap-In kliknij przycisk Close, a następnie w oknie Add/Remove Snap-In kliknij przycisk OK.

8. Można teraz administrować komputerem zdalnym korzystając z odpowiednich narzędzi.

4.2 Remote Desktop for Administration

4.2.1 Konfiguracja serwera

Konfiguracja serwera umożliwiająca korzystanie z programu Remote Desktop.

1. W programie Control Panel otwórz moduł System.

2. Na zakładce Remote, włącz program Remote Desktop i zamknij okno właściwości modułu System.

3. Otwórz konsole Terminal Services Configuration (Konfiguracja usług terminalowych) znajdującą się w folderze Administrative Tools (Narzędzia administracyjne).

4. W oknie konsoli MMC – Terminal Services Configuration/Connections prawym przyciskiem myszy kliknij połączenie RDP-tcp, a następnie wybierz opcję Properties.

5. W zakładce Network Adapter zmień maksymalną liczbę połączeń na 1.

6. Na zakładce Sessions zaznacz oba pola wyboru Override User Settings i zmień ustawienia tak, aby każda rozłaczona sesja byłą zamykana po 5 minutach bez względu na przyczynę rozłaczenia bez limitu czasu sesji aktywnej.

   - End a disconnected session: 5 minut.
   - Active session limit: never.
   - Idle session limit: 5 minut.
   - When session limit is reached or connection is broken: disconnect from session.

4.2.2 Połączenie klienta z serwerem

1. Na innym komputerze otwórz program Remote Desktop Conneection znajdującego się w grupie programów Accessories, Communications, połącz się ze swoim serverem i zaloguj się do niego.

2. Pozostaw sesję bezczynną przez 5 minut - po tym czasie powinna ona zostać automatycznie odłączona.

Rozdział 5

Jednostki organizacyjne

5.1 Najważniejsze fakty

- Jednostka organizacyjna stanowi swego rodzaju logiczne pudełko, zawierające obiekty należące do jednej domeny, pogrupowane razem w celu łatwiejszego przeprowadzenia operacji administracyjnych.
- Wyróżniamy następujące modele hierarchi struktury organizacyjnej:
  - model lokalizacji,
  - model funkcji biznesowych,
  - model typów obiektów,
  - model mieszany.
- Jednostki organizacyjne zasadniczo tworzone są z trzech powodów:
  - delegowanie administracji,
  - administrowanie zasadami grup,
  - ukrycie obiektów.
- Delegacja administracji oznacza powierzenie administratorowi użytkownikowi lub grupie odpowiedzialności za zarządzanie częścią przestrzeni nazw, np. jednostką administracyjną.
- Ustawienia pozwalające na ukrycie obiektów należących do danej jednostki organizacyjnej znajdują się w oknie właściwości jednostki organizacyjnej, w zakładce Security (Zabezpieczenia).
- Jednostka organizacyjna może zostać utworzona w domenie albo w innej jednostce organizacyjnej. Dodawanie jednostek organizacyjnych do już istniejących powoduje powstawanie hierarchicznej struktury.

- Jednostki organizacyjne powinny być projektowane pod kątem ułatwienia administracji a nie potrzeb użytkowników. Użytkownicy nie korzystają ze struktury jednostek organizacyjnych.
- Jednostki organizacyjne nie są podmiotem zabezpieczeń. Nie można bowiem definiować uprawnień dostępu w zależności od przynależności użytkownika do jednostki organizacyjnej.

5.2 Tworzenie jednostek organizacyjnych

1. Otwórz konsolę Active Directory Users and Computers.
2. Kliknij prawym przyciskiem myszy na wybranej domenie lub jednostce w której ma zostać utworzona nowa jednostka.
3. Wskazać New (Nowy), a następnie kliknąć Organizational Unit (Jednostka organizacyjna).
4. W oknie dialogowym New Object – Oraganizaional Unit w polu Name (Nazwa) wpisać nazwę tworzonej jednostki organizacyjnej, a następnie kliknąć OK.

5.3 Tworzenie jednostek organizacyjnych w celu ukrycia obiektów

1. Otwórz konsolę Active Directory Users and Computers.
2. Kliknij prawym przyciskiem myszy na wybranej jednostce i z menu podręcznego wybierz Properties (Właściwości).
3. W oknie właściwości kliknąć zakładkę Security (Zabezpieczenia). Pamiętaj, że zakładka ta będzie widoczna po zaznaczeniu Advanced Features (Funkcje zaawansowane) w menu View (Widok) konsoli Użytkownicy i komputery Active Directory.
4. Usuń wszystkie istniejące uprawnienia z jednostki organizacyjnej, a następnie kliknij Advanced (Zaawansowane).
5. W oknie ustawień zaawansowanych usuń zaznaczenie z pola wyboru Allow Inheritable Permissions From The Parent To Propagate To This Object And All Child Objects (Zezwalaj na przechodzenie uprawnień podlegających dziedziczeniu z obiektu nadrzędnego do tego obiektu i wszystkich obiektów podrzędnych).
6. W oknie komunikatu kliknąć Remove (Usuń) a następnie kliknij OK.

7. Na zakładce Security (Zabezpieczenia) nadać uprawnienie Full Control (Pełna kontrola) grupom, które powinny sprawować pełną kontrolę nad jednostką organizacyjną.

8. Nadaj pozostałym grupom odpowiednie uprawnienia a następnie kliknij OK.

9. Przenieś do jednostki organizacyjnej obiekty, które mają zostać ukrte.

Rozdział 6

Konta użytkowników

6.1 Wprowadzenie

Każdy użytkownik powinien posiadać swoje konto użytkownika. Konto użytkownika jest zbiorem wszystkich informacji, służących do zdefiniowania danego użytkownika w systemie. Do tych informacji należą:

- nazwa użytkownika,
- hasło logowania,
- lista grup do których dane konto (użytkownik) należy,
- uprawnienia posiadane przez użytkownika związane z komputerami, siecią i ich zasobami.

Windows Server 2003 obsługuje trzy rodzaje kont użytkowników:

- lokalne,
- domenowe,
- wbudowane.

Konto lokalne umożliwia logowanie tylko na konkretnym komputerze (na tym, na którym konto zostało utworzone) i korzystanie tylko z jego zasobów.

Konto domenowe umożliwia logowanie się do domeny w celu uzyskania dostępu do zasobów sieciowych.

Konta wbudowane są tworzone automatycznie dla celów administracyjnych lub dostępu do zasobów sieciowych (np. Administrator, Guest (Gość)).

6.2 Profile użytkowników

Profil użytkownika jest zbiorem folderów i danych, służących do przechowywania bieżącego środowiska pulpitu, ustawień aplikacji i danych osobistych, należących do określonego użykownika. Profil użytkownika zawiera

także wszystkie połączenia sieciowe ustanawiane w momencie zalogowania, takie jak pozycje menu Start oraz napędy mapowane na serwery sieciowe. Do ustawień zawartych w profilu użytkownika należą

- wszystkie ustawienia Eksploratora Windows, które mogą być definiowane przez użytkownika;
- dokumenty przechowywane przez użytkownika (katalog Moje dokumenty);
- obrazy przechowywane przez użytkownika (katalog Moje obrazy);
- skróty do adresów Internetowych (katalog Ulubione);
- mapowane napędy sieciowe utworzone przez użytkownika;
- skróty do innych komputerów w sieci;
- skróty i inne obiekty przechowywane na pulpicie;
- ustawienia definiowane przez użytkownika dotyczące kolorów ekranu i wyświetlanego tekstu;
- dane aplikacji oraz ustawienia konfiguracyjne;
- połączenia z drukarkami sieciowymi;
- wszystkie ustawienia zdefiniowane przez użytkownika w panelu sterowania.

Zazwyczaj lokalne profile użytkowników przechowywane są w katalogu `C:\\Documents and Settings`. Mobilne profile użytkowników są przechowywane na serwerze w folderze udostępnionym.

Istnieją cztery rodzaje profili użytkownika:

- lokalny,
- mobilny (a raczej zdalny, bo: RUP remote user profile),
- obowiązkowy,
- tymczasowy.

6.3 Przygotowanie jednostek organizacyjnych

pracownicy, ochrona, administracja (patrz rozdzial 5)

6.4 Przygotowanie grup zabezpieczeń

ggz1,ggz2 (patrz rozdzial 7)

6.5 Tworzenie i zarządzanie pojedyńczymi obiektami użytkownika

1. Otwórz konsolę Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory).
2. Zaznacz jednostkę organizacyjną `Pracownicy`.
3. Kliknij menu Action (Akcja) a następnie wybierz opcje New (Nowy) i User (Użytkownik).
4. Wyświetlone zostanie okno dialogowe New Object – User.
5. Utwórz trzech użytkowników zgodnie z informacjami poniżej

Użytkownik	First Name	Last Name	User Logon Name	User Logon Name (2000)	Password
użytkownik 1	user1	User1	user1.User1	user1user1	uU12003
użytkownik 2	user2	User2	user2.User2	user2user2	uU22003
użytkownik 3	user3	User3	user3.User3	user3user3	uU32003

6. Dla obiektu użytkownika user1 User1 otwórz okno dialogowe właściwości.
7. Skonfigurcuj wybrane właściwości dla obiektu użytkownika na zakładkach General, Address, Profile, Telephones oraz Organization.
8. Zatwierdź je wciskając przycisk OK.
9. Kliknij obiekt użytkownika user2 User2, a następnie trzymajac wciśnięty przysisk `Ctrl` kliknij obiekt użytkownika user3 User3.
10. Kliknij menu Action a następnie kliknij polecenie Properties. Ukażą się tylko te właściwości które można zmieniać dla kilku obiektów jednocześnie. Jakie to są właściwości?
11. Skonfiguruj wybrane właściwości i zatwierdź je wciskając przycisk OK.
12. Sprawdz, czy faktycznie zmienione zostały właściwości wybranych użytkowników.

6.6 Tworzenie szablonu użytkownika

1. Otwórz konsolę Active Directory Users And Computers.
2. W jednostce organizacyjnej `Pracownicy` utwórz użytkownika na podstawie następujących informacji

   (a) First Name: szablon
   (b) Last name: pracownicy
   (c) User Logon Name: szablon.pracownicy
   (d) User Logon Name (Pre-Windows 2000) szablonpracownicy

3. Kliknij przycisk Next.

4. Zaznacz opcję Account Is Disabled (Konto jest wyłączone). Kliknij przycisk Next (Dalej) a później Finish (Zakończ).

5. Wyświetl właściwości obiektu `szablon pracownicy` i skonfiguruj:

   - godziny logowania od 8 do 16 we wszystkie dni tygodnia z wyjątkiem niedzieli (zakładka Account, właściwość Logon Hours),
   - wygaśnięcie konta po miesiącu (zakładka Account, właściwość Expires),
   - jako członka globalnej grupy zabezpieczeń `ggz1` (zakładka Member Of, właściwość Member Of),
   - profil na `\\WIN2003TUT\Profiles\%Username%` (zakładka Profile, właściwość Profile path).

6. Zatwierdź zmiany klikając przycisk OK.

6.7 Tworzenie użytkownika w oparciu o szablon

1. Kliknij na obiekcie `szablon pracownicy` a następnie z menu Action (Akcja) wybierz polecenie Copy (Kopiuj).

2. Utwórz nowe konto użytkownika zgodnie z następującymi informacjami:

   - First Name: user4
   - Last name: User4
   - User Logon Name: user4.User4
   - User Logon Name (Pre-Windows 2000): user4user4
   - Account is Disabled: usuń zaznaczenie
   - Password: uU42003

3. Kliknij przycisk Next (Dalej) a następnie Finish (Zakończ).

4. Wyświetl właściwości obiektu user4 User4 i sprawdź jakie z właściwości skonfigurowanych dla szblonu, zostały do niego zastosowane.

6.8 Tworzenie użytkowników przy pomocy polecenia CSVDE

1. Otwórz dowolny program do edycji tekstu pozwalający na zapisanie danych jako zwykły plik tekstowy (np. Notatnik, może być MS Word, ale pamiętaj zapisać plik jako zwykły (nieformatowany) plik tekstowy).

2. Wpisz następujący tekst: DN,objectClass,sAMAccountName,sn,givenName
ĆN=Agnieszka J, OU=Pracownicy, DC=, DC=",user,agnieszka.j,J,Agnieszka
ĆN=Aneta J, OU=Pracownicy, DC=, DC=",user,aneta.j,J,Aneta

3. Zapisz plik jako `C:\newuser.csv`.

4. Otwórz okno wiersza poleceń i wpisz następujące polecenie
`csvde -i -f c:\newuser.csv`

5. Uruchom konsole Active Directory Users and Computers i sprawdź, czy zostały utworzone odpowiednie obiekty.

6.9 Inne narzędzia wiersza poleceń

Programy narzędziowe wiersza poleceń, ułatwiające zarządzanie usługą Active Directory

- DSADD
- DSGET
- DSMOD
- DSMOVE
- DSRM
- DSQUERY

Odszukaj opis tych programów w systemie pomocy (Help and Support Center (Centrum pomocy i obsługi technicznej)). Do czego one służą? Jak je używać? Wypróbuj ich działanie.

6.10 Tworzenie szablonu profilu mobilnego

1. Prace wstępne zmierzające do umożliwienia logowania się użytkownikom bezpośrednio w kontrolerze domeny. Możliwość taką daje np. grupa Print Operators.

   (a) Otwórz konsolę Active Directory Users And Computers.
   (b) W oknie drzewa przystawki zaznacz kontener Builtin.
   (c) Otwórz menu właściwości grupy Print Operators (Operatorzy drukowania).
   (d) Za pomocą zakładki Members (Członkowie) dodaj grupę Domain Users do grupy Print Operators.

2. Stworzymy teraz ogólniedostępny katalog z profilami.
   (a) Utwórz katalog `C:\profiles`.
   (b) Kliknij prawym przysickiem myszy na katalogu `C:\profiles` i wybierz opcję Sharing and Security (Udostępnianie i zabezpieczenia).
   (c) Kliknij zakładkę Sharing (Udostępnianie).
   (d) Udostępnij katalog używając domyślnej nazwy `profiles`.
   (e) Kliknij przycisk Permissions (Uprawnienia).
   (f) Zaznacz pole wyboru zezwalające na pełną kontrolę: Full Control.
   (g) Kliknij przycisk OK.

3. Przechodzimy teraz do właściwego trworzenia szablonu profilu mobilnego.
   (a) W tym celu utwórz konto użytkownika, które będzie używane jedynie w celu tworzenia szablonów profilu, zgodnie z poniższymi informacjami:
      - First Name: szblon
      - Last name: profil
      - User Logon Name: profile
      - User Logon Name (Pre-Windows 2000): profile
      - Password: uSP2003
   (b) Wyloguj się i zaloguj się ponownie jako użytkownik `profile`.
   (c) Utwórz niestandardowy wygląd pulpitu (zmień tło, dodaj skróty itp.).
   (d) Wyloguj się z konta `profile`.

6.11 Mobilny profil użytkownika

1. Zaloguj się jako `administrator`.
2. Otwórz właściwości modułu System z programu Control Panel (Panel sterowania).

3. Kliknij zakładkę Advanced.
4. W sekcji User Profiles (Profile użytkownika) kliknij przycisk Settings, co spowoduje otwarcie okna dialogowego Copy To (Kopiuj do).
5. Wybierz profil konta użytkownika `profile`.
6. Kliknij przycisk Copy To (Kopiuj do).
7. W ramce Copy Profile To (Kopiowanie profilu do) wpisz `\\nazwa_servera\profiles\user2`.
8. W ramce Permitted To Use kliknij przycisk Change.
9. Wpisz user2 i kliknij przycisk OK.
10. W oknie dialogowym Copy To kliknij przycisk OK.
11. Po skopiowaniu profilu kliknij jeszcze dwa razy przycisk OK aby zamknąć okna User Profiles i System Properties.
12. Sprawdź czy w katalogu `C:\profiles` utworzony został katalog `user2`.
13. Otwórz przystawkę Active Directory Users And Computers i w oknie drzewa przystawki zaznacz jednostkę organizacyjną Pracownicy.
14. Otwórz właściwości obiektu użytkownika `user2 User2`.
15. Kliknij zakładkę Profile.
16. W polu Profile Path wpisz `\\nazwa_servera\profiles\%username%`.
17. Kliknij przycisk Aply (zmienna `%username%` powinna zostać zmieniona na `user2`.
18. Kliknij przycisk OK.
19. Zaloguj się jako `user2`. Powinny pojawić się zmiany wprowadzone dla konta `profile`.

6.12 Mobilny profil dla grupy

1. Po zalogowaniu się jako administrator, kliknij dwukrotnie ikonę System w programie Control Panel.
2. Kliknij zakładkę Advanced.
3. W ramce User Profiles kliknij przycisk Settings.

4. Zaznacz profil konta użytkownika `user2`.
5. Kliknij przycisk Copy To.
6. W ramce Copy Profile To wpisz `\\nazwa_servera\profiles\all`.
7. W ramce Permitted To Use kliknij przycisk Change.
8. Wpisz Users i kliknij przycisk OK.
9. W oknie dialogowym Copy To kliknij przycisk OK.
10. Po skopiowaniu profilu kliknij jeszcze dwa razy przycisk OK aby zamknąć okna User Profiles i System Properties.
11. Sprawdź czy w katalogu `C:\profiles` utworzony został katalog `all`.
12. W programie Control Panel otwórz moduł Folder Options i na zakładce View, w ramce Advanced Settings sprawdź, czy zaznaczona jest opcja Show Hidden Files And Folders.
13. Otwórz katalog `C:\profiles\all` i zmień nazwę pliku `Ntuser.dat` na `Ntuser.man`. Zmiana ta powoduje, że profil staje się profilem obowiązkowym.
14. Otwórz przystawkę Active Directory Users And Computers i w oknie drzewa przystawki zaznacz jednostkę organizacyjną Pracownicy.
15. Otwórz właściwości obiektu użytkownika Hanna L.
16. Kliknij zakładkę Profile.
17. W polu Profile Path wpisz `\\nazwa_servera\profiles\all`.
18. Kliknij przycisk OK.
19. Zaloguj się jako hannal. Spróbuj wprowadzić zmiany do profilu, przez modyfikację wyglądu pulpitu. Wyloguj się i zaloguj się ponownie – zmiany nie powinny być widoczne.

6.13 Uwierzytelnianie

1. Konfiguracja zasad uwierzytelniania i inspekcji.
   (a) Otwórz konsole Active Directory Users And Computers.
   (b) Zaznacz węzeł domeny i z menu Action wybierz polecenie Properties.

(c) Na zakładce Group Policy zaznacz domyślną zasadę domeny (Default Domain Policy) i kliknij przycisk Edit.

(d) Przez węzły Computer Configuration, Window Settings, Security Settings i Account Policies przejdź do Account Lockout Policy.

(e) Kliknij dwukrotnie zasadę Account Lockout Duration.

(f) Zaznacz pole wyboru Define This Policy Settings.

(g) Wpisz 0 jako określenie czasu trwania blokady i kliknij przycisk Apply. Możliwe wartości do wpisania mieszczą się w przedziale 0-99999 minut; 0 oznacza, że konto musi zostać odblokowane przez administratora.

(h) Dwukrotnie kliknij przycisk OK.

(i) Sprawdź, czy wartość parametru zasady Account Lockout Duration wynosi 0, Account Lockout Threshold ma wartość 5[1] , Reset Account Lockout Counter After ma wartość 30[2].

(j) Zamknij okno Group Policy Object Editor.

(k) Kliknij przycisk OK aby zamknąć okno dialogowe Properties.

(l) Po rozwinięciu węzał domeny zaznacz kontroler Domain Controllers.

(m) W menu Action wybierz polecenie Properties.

(n) Na zakładce Group Policy zaznacz zasadę Default Domain Controllers Policy i kliknij przycisk Edit.

(o) Przez węzły Computer Configuration, Window Settings, Security Settings i Local Policies przejdź do Audit Policy (Zasada inspekcji).

(p) Kliknij dwukrotnie zasadę Audit Account Logon Events.

(q) Zaznacz opcję Define These Policy Settings, a dalej Success i Failure i kliknij przycisk OK.

(r) Dwukrotnie kliknij zasadę Audit Logon Events.

(s) Zaznacz opcję Define These Policy Settings, a dalej Success i Failure i kliknij przycisk OK.

(t) Dwukrotnie kliknij zasadę Acount Management.

(u) Zaznacz opcję Define These Policy Settings, a dalej Success i kliknij przycisk OK.

(v) Zamknij okno Group Policy Object Editor.

[1]Możliwe wartości mieszczą się w przedziale 0-999 i określają liczbę nieprawidłowych prób logowania, po przekroczeniu której konto zostanie zablokowane.

[2]Możliwe wartości mieszczą się w przedziale 1-99999 minut i określają czas jaki musi upłynąć od próby nieudanego logowania, zanim licznik zostanie wyzerowany. Wartość ta musi być różna lub mniejsza niż wartość określająca czas trwania blokady.

(w) Kliknij przycisk OK zamykając okno dialogowe Properties.

2. Generowanie zdarzeń i ich analiza

   (a) Spróbuj zalogować się jako zwykły użytkownik, podając nieprawidłowe hasło i/lub login.

   (b) Zaloguj się prawidłowo jako zwykły użytkownik.

   (c) Wyloguj się.

   (d) Zaloguj się jako administrator.

   (e) Zresetu hasło dla użytkownika hannal podając jego nową wartość jako newuHL2003.

   (f) W grupie programów Administrative Tools otwórz konsolę Computer Management.

   (g) Rozwiń węzły Event Viewer i wybierz dziennik Security.

   (h) Przejrzyj ostatnio wygenerowane zdarzenia. Powinny znaleźć się tam informacje o nieprawidłowym i prawidłowym logowaniu oraz zmianie hasła.

Rozdział 7

Grupy

Grupa jest zbiorem kont użytkowników służącym do uproszczenia administracji. Przypisanie praw i uprawnień do grupy eliminuje konieczność skonfigurowania uprawnień dla każdego konta użytkownika oddzielnie. Użytkownik może należeć do kilku grup.

Wyróżniamy następujące grupy

- grupy zabezpieczeń,
- grupy dystrybucyjne.

Grupa dystrybucyjna jest wykorzystywana przez aplikacje do funkcji nie związanych z zabezpieczeniami, np. do przesłania wiadomości do określonej grupy użytkowników.

Grupy zabezpieczeń służą do przypisywania uprawnień dostępu do zasobu. Grupa zabezpieczeń może być traktowana jako grupa dystrybucyjna.

Biorąc pod uwagę zakres działania grupy wyróżniamy

- grupę globalną,
  - członkowie mogą pochodzić tylko z domeny, w której grupa została utworzona,
  - może zostać uprawniona do dostępu do dowolnej domeny należącej do drzewa lub lasu.

  Najczęściej używane są do pogrupowania użytkowników potrzebujących jednakowych uprawnień dostępu do zasobów sieciowych.
- domenową grupę lokalną,
  - członkowie mogą pochodzić z dowolnej domeny
  - ma dostęp tylko do tych zasobów, które należą do domeny, w której utworzono grupę

Najczęściej używane są do przypisywania uprawnień do określonych zasobów.

- grupę uniwersalną.
  - członkowie mogą pochodzić z dowolnej domeny w lesie
  - może zostać uprawniona do dostępu do dowolnej domeny należącej do drzewa lub lasu
  - dostępna jest tylko w domenach, w których poziom funkcjonalny ustawiony jest na poziom rodzimy Windows 2000 lub poziom Windows Server 2003.

  Najczęściej używane są do przypisywania uprawnień do podobnych zasobów należących do różnych domen.

Możliwe są następujące zmiany zakresu:

- Grupa globalna może zostać grupą uniwersalną pod warunkiem, że nie jest członkiem innej grupy o zakresie globalnym.
- Domenowa grupa lokalna może zostać grupą uniwersalną pod warunkiem, że nie zawiera innej domenowej grupy lokalnej.
- Grupa uniwersalna może zostać grupą globalną pod warunkiem, że nie zawiera innej grupy uniwersalnej.
- Grupa uniwersalna może zostać domenową grupą lokalną.

Windows Server 2003 zawiera cztery kategorie grup domyślnych:

- grupy należące do katalogu Builtin (Wbudowane) (przypisywanie domyślnych zbiorów uprawnień użykownikom odpowiedzialnym za wykonywanie konkretnych zadań administracyjnych) (porównaj [3], s. 401),
- grupy należące do katalogu Users (Użytkownicy) (przypisywanie domyślnych zbiorów uprawnień użykownikom odpowiedzialnym za wykonywanie konkretnych zadań administracyjnych) (porównaj [3], s. 403),
- grupy tożsamości specjalnej (można przypisywać uprawnienia ale nie można wyświetlić ani modyfikować listy członków takiej grupy; przynależność do tyh grup uzależniona jest od trybu dostępu a nie od konkretnej osoby),
- domyślne grupy lokalne, katalog Grous (służą do upoważnienia użytkowników do wykonania zadań administracyjnych na jednym komputerze).

7.1 Tworzenie grupy zabezpieczeń

1. Otwórz konsolę Active Directory Users and Computers.
2. Kliknij prawym przyciskiem myszy na odpowiedniej domenie lub jednostce organizacyjnej.
3. Z menu podręcznego wybierz Nowy (New), a następnie kliknij Group (Grupa).
4. W oknie dialogowym w polu tekstowym Group Name (Nazwa Grupy) wpisz nazwę grupy (drugie pole tekstowe, Group Name – Pre-Windows 2000, zostanie uzupełnione automatycznie).
5. Zaznaczyć odpowiednie opcje w polach Group Scope (Zakres grupy) oraz Group Type (Typ grupy).
6. Kliknij OK.

7.2 Dodawanie członków do grup

1. Otwórz konsolę Active Directory Users and Computers.
2. Wybierz domenę lub jednostkę w której znajduje się docelowa (to znaczy ta do której chcesz dodać użytkownika) grupa.
3. Kliknij prawym przyciskiem myszy na grupie a następnie kliknij Properties (Właściwości).
4. W oknie właściwości grupy kliknij zakładkę Members (Członkowie), a następnie kliknij Add (Dodaj).
5. W oknie Select Users, Contacts, Computers, or Groups kliknij Advanced (Zaawansowane).
6. W rozszerzonym oknie dialogowym kliknij Find Now (Znajdź teraz). Na wyświetlonej na dole liście zaznaczyć jeden lub więcej obiektów (użytkownik, grupa, komputer).
7. Kliknij OK a potem jeszcze dwa razy OK.

7.3 Zmiana zakresu grupy

1. Otwórz konsolę Active Directory Users and Computers.
2. Wybierz domenę lub jednostkę w której znajduje się docelowa grupa.

3. Kliknij prawym przyciskiem myszy na grupie a następnie kliknij Properties (Właściwości).

4. Na zakładce General (Ogólne) okna właściwości grupy zaznaczyć odpowiedni zakres grupy.

5. Kliknij OK.

7.4 Wyszukiwanie tych grup z domeny do których należy określony użytkownik

1. Wpisz
   `dsget user UserDN -memberof [-expand]`
   Przełącznik `-memberof` powoduje wyświetlenie tych grup do których użytkownik należy bezpośrednio. Przełącznik `-expand` powoduje rekurencyjne przeszukiwanie przez co otrzymamy pełną listę wszystkich grup, do których należy dany użytkownik domeny.

Rozdział 8

Pliki i foldery

8.1 Foldery udostępnione

8.1.1 Udostępnianie udziałów

Najbardziej uniwersalną metodą pozwalającą zarządzać folderami udostępnionymi (nazywanymi też udziałami) jest użycie przystawki Shared Folder. Można z niej korzystać zarówno w przypadku systemu lokalnego jak i zdalnego. Zauważmy tutaj, że Windows Explorera, dającego nam możliwość zarządzania udostępnianiem folderów (po kliknięciu prawym przyciskiem myszy na nazwie folderu należy wybrać Sharing and Security (Udostępnianie i zabezpieczenia), a następnie opcję Share This Folder (Udostępnij ten folder), możemy użyć jedynie dla systemu lokalnego.

Przystawkę Shared Folders uruchomić można jako

- element pewnej niestandardowej konsoli MMC,
- jako część konsoli Copmuter Management,
- jako część konsoli File Server Management.

W węźle Shares (Udziały) przystawki Shares Folders wyświetlana jest lista wszystkich udziałów danego komputera. Kliknięcie na ten węzeł i wybranie z menu kontekstowego lub z menu Action polecenia New Share pozwala utworzyć nowy udział. Węzeł Sessions umożliwia monitorowanie liczby użytkowników przyłączonych do konkretnego serwera, natomiast węzeł Open Files wyświetla listę wszystkich otwartych i zablokowanych plików, pozwalając je zamknąć jeśli zajdzie taka potrzeba.

Dla każdego udziału w oknie jego właściwości dostępne są następujące zakładki:

General

Publish

Share Permissions

Security

8.1.2 Uprawnienia udziałów

Lista uprawnień udziału nie jest tak rozbudowana jak lista uprawnień NTFS. Składają się na nią następujące uprawnienia

- Read
- Change
- Full Control

Najważniejsze fakty

- Uprawnienia udziału mogą być zezwolone (Allow) lub odmówione (Deny).
- Efektywny zestaw uprawnień jest **sumą** uprawnień Allow przydzielonych bezpośrednio użytkownikowi i grupom do których należy.

```
User is member of Group1    Allow: Read
     is member of Group2    Allow: Change

Effective rights for User:         Change
```

- Odmowa uprawnień (Deny) unieważnia uprawnienia Allow.

```
User is member of Group1    Allow: Read
     is member of Group2    Deny:  Full Control

Effective rights for User:         nie można odczytać plików
                                   i folderów
```

- Uprawnienia udziału określają **maksymalne** uprawnienia efektywne dla wszystkich plików i folderów umieszczonych poniżej foldera udostępnionego. Uprawnienia te można zawęzić stosując uprawnienia NTFS, ale nie można ich rozszerzyć.
- Różne askpety uprawnień udziałów ([1], s. 181).

8.1.3 Ćwiczenia

Udostępnianie foldera

1. Utwórz folder `C:\shareddocs`.
2. Uruchom konsolę File Server Management (Zarządzanie serwerem plików).
3. Z menu Action lub z menu podręcznego wybierz Add A Shared Folder.
4. W wyświetlonym oknie Share A Folder Wizard naciśnij przycisk Next.
5. Jako ścieżkę wpisz `C:\shareddocs` i naciśnij przycisk Next.
6. Zaakceptuj domyślną nazwę udziału i naciśnij przycisk Next.
7. Na zakładce Permissions zaznacz opcję Use Custom Share And Folder Permissions a następnie kliknij przycisk Customize (Dostosuj).
8. Wybierz Allow Full Control, a następnie kliknij przycisk OK.
9. Kliknij przycisk Finish a następnie Close.

Kontrolowanie połączeń

1. W menu Start wybierz polecenie Run, a następnie wpisz `\\nazwa_serwera\shareddocs`. W ten sposób utworzone zostanie połączenie sieciowe do wskazanego foldera.
2. Teraz w konsoli File Server Management klikając na węzeł:
   - Sessions możemy zobaczyć siebie na liście osób obsługujących sesję,
   - Open Files możemy zobaczyć kto i jaki plik otworzył,
   - Open Files możemy zamknąc otwarty plik.

8.2 Uprawnienia systemu plików

Uprawnienia systemu plików mogą być konfigurowane tylko na dowolnym wolumenie NTFS.

Po kliknięciu na zasobie prawym przyciskiem myszy wybieramy Properties lub Sharing and Security a następnie zakładkę Security.

Obecnie edytor ACL pozwala na przyznawanie uprawnień w oparciu o trzy różne okna.

- Pierwsze okno dialogowe (dostępne na przykład na zakładce Security okna Properties) pozwala na ogólny przegląd ustawień zabezpieczeń i uprawnień zasobu.

- Drugie kono, Advanced Security Settings for... (dostępne na przykład po kliknięciu przycisku Advanced w poprzednim oknie) zawiera listę wpisów kontroli dostępu przypisanych do pliku lub foldera.
- Trzecie okno, Permission Entry For... zawiera listę szczegółowych, pojedynczych uprawnień i stanowi pewnego rodzaju kompromis pomiędzy listą uprawnień użytkownika z pierwszego okna a listą wpisów uprawnień z okna drugiego.

Najważniejsze fakty

- Nowe podmioty zabezpieczeń (komputery, typ logowania – Interactive, Network, Terminal Server User).
- Szablony uprawnień oraz uprawnienia specjalne.

8.2.1 Mechanizm dziedziczenia uprawnień

Dziedziczenie uprawnień oznacza, że uprawnienia zastosowane do foldera będą się również stosowały do plików i folderów znajdujących się poniżej danego foldera. Dowolne zmiany nadrzędnej listy ACL będą miały wpływ na zawartość całego foldera.

Uprawnienia dziedziczone nie mogą być usuwane z listy ACL. Dziedziczone uprawnienie można unieważnić przez:

- przydzielenie uprawnienia bezpośredniego,
- zablokowanie dziedziczenia i utworzenie całej bezpośredniej listy ACL.

Aby unieważnić dziedziczone uprawnienia poprzez ich zastąpienie uprawnieniami bezpośrednimi, wystarczy po prostu zaznaczyć pole wyboru odpowiedniego uprawnienia.

Aby unieważnić wszystkie dziedziczone uprawnienia, należy dla zasobu otworzyć okno dialogowe Advanced Security Settings i usunąć zaznaczenie opcji Allow Inheritable Permissions From The Parent To Propagate to This Object... W ten sposób zablokowane zostanie dziedziczenie wszystkich uprawnień pochodzących z obiektu nadrzędnego. Następnie trzeba skonfigurować dostęp do zasobu poprzez przydzielenie odpowiednich uprawnień bezpośrednich.

Przywracanie dziedziczenia z punktu widzenia obiektu podrzędnego polega na zaznaczeniu opcji Allow Inheritable Permissions from... Cytując [1]:„Uprawnienia dziedziczone po obiekcie nadrzędnym nie mają wpływu na zasób. Pozostają wszystkie uprawnienia bezpośrednie przydzielone do zasobu. Wynikowa lista ACL jest połączeniem uprawnień bezpośrednich, które mogą być usuwane oraz odziedziczonych uprawnień.”. Wydaje się, że sens tego sprzecznego zdania jest następujacy. Otórz uprawnienia dziedziczone po obiekcie nadrzędnym nie mają wpływu na zasób w tym sensie, że

nie modyfikują fizycznie jego listy ACL. Natomiast mają wpływ w tym sensie, że WYNIKOWA lista ACL jest połączeniem uprawnień bezpośrednich, które mogą być usuwane oraz odziedziczonych uprawnień.

8.2.2 Uprawnienia efektywne

Uprawnienia efektywne są wynikiem wpływu uprawnień pochodzących z różnych źródeł.

Uprawnienia efektywne podlegają następującym regułom:

- Uprawnienia plików unieważniają uprawnienia folderów lub inaczej: znaczenie ma jedynie lista ACL danego zsobu.
- Uprawnienia zezwalające sumują się.
- Odmowa uprawnień ma pierwszeństwo w stosunku do zezwoleń.
- Uprawnienia bezpośrednie mają pierwszeństwo nad uprawnieniami dziedziczonymi.

Sprawdzenie uprawnień efektywnych, z dość dobrym przybliżeniem, umożliwia zakładka Effective Permissions z okna dialogowego Advanced Security Settings.

8.2.3 Właściciel i własność zasobu

W systemie Windows Server 2003 określony został specjalny podmiot zabezpieczeń nazwany Creator Owner (twórca właściciel) oraz wpis w deskryptorze zabezpieczeń zasobu, który definiuje właściciela obiektu.

Każdy użytkownik tworzący plik lub folder staje się twórcą i początkowym (pierwszym) właścicielem tego zasobu. Własność można zmieniać. Właściciel obiektu moze w dowolnym momencie modyfikować listę ACL obiektu. Użytkownik posiadający uprawnienie Take Ownership (Przejmij na własność) może stać się właścicielem obiektu. Administatorzy mogą stać się właścicielami dowolnego obiektu. Konta grup Administrators, Backup Operators i wszystkich tych, którym przydzielone zostało prawo Restore Files And Directories mogą zmienić właściciela pliku.

8.2.4 Ćwiczenia

Chwilowo brak :/ Proszę najzwyczajniej „pobawić się” systemem zabezpieczeń.

8.3 Inspekcja dostępu systemu plików

Inspekcja dostępu do systemu plików wskazana jest ze względu na

- pozyskanie wiadomości o stopniu wykorzystania zasobów,
- ewentualnych nieproawidłowościach w sposobie zabezpieczenia.

Konfigurowanie inspekcji odbywa się według następujących etapów:

1. Konfiguracja ustawień inspekcji dla pliku lub foldera.
2. Włączenie zasad inspekcji.
3. Kontrolowanie zdarzeń zarejestrowanych w dzienniku zabezpieczeń.

8.3.1 Konfiguracja ustawień inspekcji

Konfiguracja ustawień inspekcji odbywa się w oknie Advanced Security Settings for ... na zakładce Auditing (Inspekcja). Naciśnięcie przycisku Add powoduje otworzenie okna Auditing Entry, w którym to możemy wybrać te uprawnienia, które chcemy monitorować. Można rejestrować udane (Successful), nieudane (Failed) lub obie próby dostępu do zasobu przy użyciu uprawnienia przypisanego do obiektu. Uprawnienia inspekcji, podobnie jak zwykłe uprawnienia, podlegają zasadom dziedziczenia. Dziedziczenie to jest stosowane do obiektów, które zezwalają na dziedziczenie. Skonfigurowanie ustawień inspekcji nie włacza jeszcze inspekcji. Inspekcję włącza się za pośrednictwem zasady.

8.3.2 Włączenie zasad inspekcji

Zasada inspekcji może zostać włączona na serwerze autonomicznym za pomocą konsoli Local Security Policy (Lokalna zasada zabezpieczeń), a na kontrolerze domeny z pomocą konsoli Domain Controller Security Policy (Zasada zabezpieczeń kontrolera domeny). Następnie nalezy wybrać węzeł Local Policies (Zasady lokalne) a w nim węzeł Audit Policy (Zasada inspekcji) i dwukrotnie kliknąć zasadę Audit Object Access (Przeprowadź inspekcję dostępu do obiektu). Należy zaznaczyć opcję Define These Policy Settings (Definiuj następujące ustawienia zasad), a następnie zaznaczyć, czy włączona będzie inspekcja dla „sukcesu", „niepowodzenia" czy obu tych zdarzeń. Zauważmy w tym miejscu, że rejestrowane zdarzenia są **częścią wspólną** wpisów inspekcji dotyczących określonego foldera lub pliku oraz ustawień zasady inspekcji.

8.3.3 Analiza dziennika zabezpieczeń

Wyniki inspekcji można przeglądać za pomocą programu Event Viewer (Podgląd zdarzeń), w którym należy wybrać dziennik Security (Zabezpieczenia).

8.3.4 Ćwiczenia

Konfiguracja ustawień inspekcji

- Otwórz okno dialogowe Advanced Security Settings dla wybranego foldera (np. `C:\myauditttest`).
- Wybierz zakładkę Auditing.
- Dodaj wpis inspekcji, pozwalający np. na śledzenie wybranej grupy i określ monitorowanie wybranych zdarzeń (proponuje wbierać zdarzenia łatwowywoływalne, np. usuwanie ubiektu).

Włączenie zasad inspekcji

- Otwórz konsolę Domain Controller Security Policy (Zasada zabezpieczeń kontrolera domeny) znajdującą się w folderze Administrative Tools (Narzędzia administracyjne).
- Rozwiń węzeł Local Policies (Zasady lokalne) i wybierz Audit Policy (Zasadę inspekcji).
- Dwukrotnie kliknij zasadę Audit Object Access (Przeprowadź inspekcję dostępu do obiektu).
- Zaznacz pole wyboru Define These Policy Settings (Definiuj następujące ustawienia zasad).
- Włącz inspekcję dla wpisów związanych zarówno z powodzeniem, jak i niepowodzeniem wykonywanych operacji.
- Kliknij przycisk OK a następnie zamknij konsolę.
- W celu odświeżenia zasad inspekcji, otwórz okno wiersza poleceń i wpisz polecenie gpupdate.

Analiza dziennika zabezpieczeń

- W monitorowanym folderze wykonaj akcje związane z monitorowanymi zdarzeniami (np. usuń jakieś pliki).
- Uruchom program Event Viewer znajdujący się w foldrze Administrative Tools.
- Wybierz dziennik Security.
- Przyjrzyj się zarejestrowanym zdarzeniom, spróbuj jakoś zawęzić otrzymane wyniki, np. używając polecenia Filter a menu View.

Rozdział 9

IIS jako alternatywna metoda współdzielenia plików

Niniejszy rozdział jest krótkim wprowadzeniem do usługi IIS (Internet Information Services)[1]. IIS potraktujemy tutaj jedynie jako rozszerzenie możliwości współdzielenia plików omawianych w poprzednim rozdziale.

Zanim przejdziemy do omawiania użytecznych z naszego punktu widzenia możiwości usługi IIS, omówimy pojęcie katalogu wirtualnego.

9.1 IIS a uprawnienia

Zabezpieczenia plików udostępnianych za pomocą usługi IIS rozpatrywać można na następujacych poziomach:

- uwierzytelnianie,
- uprawnienia NTFS,
- uprawnienia IIS.

Uwierzytelnianie to proces weryfikacji tożsamości w oparciu o nazwę użytkownika i jego hasło. Według ustawień domyślnych, wszystkie żadania kierowane do programu IIS obsługuje bezosobowy użytkownik `IUSR\_nazwakomputera`.

Na zakładce Directory Security, dostępne są następujące opcje związane z uwierzytelnianiem sieci Web lub FTP:

Uwierzytelnianie anonimowe (także FTP)

[1] Wyznawcom ideologii „Linux is the best, Linux forever" proponuję wizytę na stronie `http://news.netcraft.com`; wbrew obiegowym opiniom, serwery Microsoftu obsługują sporą część runku (prawie 40% w 2007 roku) i mają się one (wydajnościowo) całkiem nieźle.

Uwierzytelnianie podstawowe (także FTP)

Zaawansowane uwierzytelnianie szyfrowane

Zintegrowane uwierzytelnianie systemu Windows

Certyfikat uwierzytelnienia

Uwierzytelnienie usługi Passport w sieci .NET

Uprawnienia NTFS – stosują się wszystkie zasady z rozdziału 8. Uprawnienia IIS.

- Read
- Write
- Script Source Access
- Directory browsing
- Execute
  - None
  - Scripts only
  - Scripts and Executables

9.2 Ćwiczenia

9.2.1 Instalowanie IIS

Jako, że domyślnie usługi IIS nie są instalowane, należy je oddzielnie zainstalować.

1. Otwórz moduł Add Or Remove Programs z programu Control Panel i kliknij Add/Remove Windows Components.
2. Po zaznaczeniu opcji Application Server kliknij przycisk Details.
3. Po zaznaczeniu opcji Internet Information Sevices (IIS) kliknij przycisk Details.
4. Sprawdź czy zaznaczone są następujące (wymagane do zainstalowania IIS) opcje:
   - Common Files, usługi File Transfer Protocol (FTP),
   - World Wide Web Service,
   - Internet Information Services Manager.
5. Zakończ instalacje.

9.2.2 Tworzenie witryny sieci Web

1. Utwórz katalog domowy dla witryny, np. `C:\www_default` i umieść tam jakiś dokument htm.
2. Z grupy programów Administrative Tools wybierz przystawkę Internet Information Services (IIS) Manager.
3. Klikając prawym przyciskiem myszy na węźle Default Web Site wybierz polecenie Stop.
4. Klikając prawym przyciskiem myszy na węźle Web Sites wybierz polecenie New Web Site.
5. Nadaj witrynie nazwę `mywww1` i określ ścieżkę jako `C:\www_default`.

9.2.3 Tworzenie chronionego katalogu wirtualnego

1. Utwórz katalog domowy dla witryny, np. `C:\www\users\ali` i umieść tam jakiś dokument htm.
2. Po kliknięciu prawym przyciskiem myszy na witrynie `mywww1` wybierz polecenie New Virtual Directory.
3. W polu Alias wpisz `ali`.
4. W polu Path wpisz `C:\www\users\ali`.
5. Otwórz okno właściwości dla katalogu wirtualnego `www`.
6. Kliknij zakładkę Directory Security.
7. W ramce Authentication and Access Control kliknij przycisk Edit.
8. Usuń zaznaczenie opcji umożliwiającej dostęp anonimowy i dwukrotnie kliknij przycisk OK.
9. Otwórz przeglądarkę i wpisz nazwę:
   - `http://nazwa_servera/nazwa_domeny` – powinna zostać wyświetlona strona z katalogu `C:\www_default`;
   - `http://nazwa_servera/nazwa_domeny/ali` – użytkownik zostanie poproszony o poświadczenie tożsamości a po poprawnym zalogowaniu powinna zostać wyświetlona strona z katalogu `C:\www\users\ali`.
10. Zmień uprawnienia NTFS związane z dokumentem z katalogu `C:\www\users\ali`. Czy teraz dostęp jest możliwy? Zawsze?

Rozdział 10

Kopie bezpieczeństwa

W niniejszym rozdziale poruszone zostaną zagadnienia związane z planowaniem i wykonywaniem kopii zapasowych. Programem narzędziowym tworzenia kopii zapasowych jest Backup Utility (ntbackup.exe) znajdujący się w grupie System Tools w grupie programów Accessories.

10.1 Tworzenie kopii zapasowych

10.1.1 Strategie tworzenia kopii zapasowych

Normalna kopia zapasowa

Przyrostowa kopia zapasowa

Różnicowa kopia zapasowa

Kopia

Codzienna kopia zapasowa

My Info: Powiedzieć o: Wybieranie plików → Save Selections.

Przed przystąpieniem do testowania różnych zadań kopii zapasowych należy przygotować odpowiednie dane testowe. Utwórz np. w katalogu `C:\test\doc` cztery pliki o nazwach `file1.txt`, `file2.txt`, `file3.txt` oraz `file4.txt`. Po utworzeniu struktury katalogowo-plikowej, otwórz program Windows Explorer i wybierz widok, w którym wyświetlone będą atrybuty plików. Wszytstkie pliki powinny mieć atrybut `A`.

10.1.2 Normalna kopia zapasowa

1. Po uruchomieniu programu Backup Utility usuń zaznaczone pole wyboru Always Start In Wizard Mode i kliknij na odnośnik Advanced Mode.

2. Wybierz zakładkę Backup.
3. Rozpoczynając od My Computer rozwiń kolejne węzły aż dojdziesz do uprzednio utworzonego folderu `doc`.
4. W menu Job wybierz polecenie Save Selections.
5. Dokonany wybór plików zapisz jako `docnormback.bks`.
6. W polu Backup Media Or Filename wpisz `C:\docnormback.bkf`.
7. Kliknij przycisk Start Backup a następnie Advanced.
8. Z listy rozwijalnej Backup Type wybierz Normal i naciśnij przycisk OK.
9. Zaznacz opcję Replace The Data On The Media With This Backup, a następnie kliknij przycisk Start Backup.
10. Po zakończeniu pocesu tworzenia kopi sprawdź atrybuty archiwizowanych plików – powinien zniknąć atrybut `A`.

10.1.3 Przyrostowa kopia zapasowa

1. Uruchom program Backup Utility.
2. Wybierz zakładkę Backup.
3. W menu Job wybierz polecenie Load Selections i wskaż docnormback.bks.
4. W polu Backup Media Or Filename wpisz `C:\docincback.bkf`.
5. Kliknij przycisk Start Backup a następnie Advanced.
6. Z listy rozwijalnej Backup Type wybierz Incremental i naciśnij przycisk OK.
7. Po zakończeniu pocesu tworzenia kopi sprawdź atrybuty archiwizowanych plików – powinien zniknąć atrybut `A`.

10.1.4 Różnicowa kopia zapasowa

1. Zmodyfikuj jeden z wcześniej utworzonych plików. Sprawdź atrybuty wszystkich plików – tylko ten jedne powinien mieć atrybut `A`.
2. Uruchom program Backup Utility.
3. Wybierz zakładkę Backup.

4. W menu Job wybierz polecenie Load Selections i wskaż docnormback.bks.
5. W polu Backup Media Or Filename wpisz `C:\docdiffback.bkf`.
6. Kliknij przycisk Start Backup a następnie Advanced.
7. Z listy rozwijalnej Backup Type wybierz Differential i naciśnij przycisk OK.
8. Po zakończeniu pocesu tworzenia kopi sprawdź atrybuty archiwizowanych plików – atrybut `A` powinien wciąż być widoczny.

10.2 Odtwarzanie danych

Odtwarzanie danych odbywa się przy pomocy opcji dostępnych na zakładce Restore And Manage Media programu Backup Utility.

Podczas odtwarzania do wyboru są trzy lokalizacje w których odtworzone zostaną dane:

Original location Lokalizacja oryginalna

Alternate location Lokalizacja alternatywna

Single folder Pojedynczy folder

Opcje przywracania

Do Not Replace The File On My Computer

Replace The File On Disk Only If The File On Disk Is Older

Always Replace The File On My Computer

10.2.1 Przywracanie danych: ćwiczenie

1. Otwórz program Backup Utility.
2. Kliknij zakładkę Restore And Manage Media.
3. Kliknij znak „plus” aby rozwinąć pliki.
4. Kliknij znak „plus” aby rozwinąć plik docnormback.bkf i wybierz pliki do odtworzenia.
5. Z listy rozwijanej Restore Files To wybierz opcje Alternte location.
6. W polu Alternate location wpisz alternatywną lokalizacje odtwarzanych plików, np. `C:\testtest`.

7. Kliknij przycisk Start Restore.
8. W oknie dialogowym Confirm Restore kliknij przycisk OK.
9. Po zakończeniu zadania kliknij przycisk Report i sprawdź dziennik operacji przywracania (raport dostępny jest także w menu Tools → Report).

10.2.2 Harmonogram

Dla zadanie tworzenia kopii zapasowych można określić harmonogram co pozwoli na regularne i zautomatyzowane ich tworzenie np. w okresie małego obiążenia systemu.

1. Uruchom program Backup Utility i kliknij zakładkę Backup.
2. Z menu Job wybierz polecenie Load selection i wybierz uprzednio przygotowany zestwa, np. zestaw docnormback.bks.
3. W polu Backup Media Or File Name wpisz: `C:\Backup-Everyday.bkf`.
4. Naciśnij przycisk Start Backup.
5. Naciśnij przycisk Advanced i wybierz typ kopii zapasowej: Incremental. Naciśnij przycisk OK.
6. Naciśnij przycisk Schedule.
7. W oknie Set Account Information, wpisz swoje hasło i naciśnij przycisk OK.
8. Nazwij zadanie Daily Incremental Backup.
9. Kliknij przycisk Properties. Skonfiguruj zadanie tak, aby było uruchamiane codziennie. Określ czas o kilka minut późniejszy niż bieżąca godzina, tak aby możliwe było zaobserwowanie działanie zadania.
10. Zakończ konfigurowanie harmonogramu. Program poprosi o ponowne wprowadzenie hasła.
11. Zamknij program Backup Utility.
12. W programie Windows Explorer otwórz napęd C i poczekaj taki czas aby zadanie zostało uruchomione. Po tym czasie zadanie kopii zapasowej powinno zostać wyświetlone.
13. Otwórz program Backup Utility, w menu Tools wybierz polecenie Report i obejrzyj dziennik ostatniego zadania kopii zapasowej, aby potwierdzić status zadania. Jeśli żaden plik nie został zmodyfikowany, to podczas wykonywania kopii zapasowej, żaden plik nie został skopiowany.

14. W przypadku nieprawidłowej pracy zadania należy otworzyć program Event Viewer znajdujący się w folderze Administrative Tools i w celu rozpoznania przyczyny awarii przeanalizować dziennik aplikacji.

Rozdział 11

Zarządzanie pamięcią dyskową

11.1 Podstawowa terminologia

11.2 Ćwiczenia

11.2.1 Tworzenie nowej partycji

1. Otwórz przystawkę Disk Management z konsoli Computer Management.
2. W dolnej ramce okna kliknij prawym przyciskiem myszy na nieprzydzielonej przestrzeni dyskowej wybranego dysku i wybierz polecenie New Partition. Uruchomiony zostanie program New Partition Wizard.
3. Utwórz partycję podstawową o wybranej pojemności (np, 100 MB). Zaakceptuj domyślne oznaczenie (przy pomocy litery) dysku. Oznacz wolumin wybraną etykietą, np. `data_vol`. Wykonaj szybkie formatowanie stosując system plików NTFS. Po zakończeniu formatowania status partycji powinien zmienić się na Healthy.

11.2.2 Konwertowanie dysku podstawowego na dysk dynamiczny

1. Otwórz przystawkę Disk Management z konsoli Computer Management.
2. Kliknij prawym przyciskiem myszy na oknie statusu wybranego dysku i wybierz polecenie Convert To Dynamic Disk. Uruchomiony zostanie program Convert To Dynamic Disk.
3. Postępuj zgodnie z instrukcjami programu aż do zakończenia procedury.

4. Jeśli przekształcany dysk jest dyskiem systemowym, konieczne będzie ponowne uruchomienie systemu.

11.2.3 Użycie programu DiskPart

1. W oknie wiersza poleceń wpisz diskpart i naciśnij `Enter`.
2. Wpisz polecenie `list disk` i naciśnij Enter. Wyświetlona zostanie lista wszystkich dysków serwera. W szczególności powinien być widoczny dysk 0.
3. Wpisz polecenie `create volume simple size=250 disk=0` i naciśnij Enter.
4. Wpisz polecenie `list volume` i naciśnij Enter. Gwiazdka znajdująca się przed nazwą woluminu wskazuje na wybrany wolumin.
5. Wpisz polecenie `assign letter z` i naciśnij Enter.
6. Wpisz polecenie `list volume` i naciśnij Enter aby sprawdzić czy do wybranego woluminu przypisana została litera `Z`.
7. Wpisz polecenie `extend size=250 disk=0` i naciśnij Enter.
8. Wpisz polecenie `list volume` i naciśnij Enter. Pojemność wybranego woluminu powinna wynosić teraz 500 MB.
9. Wpisz polecenie `exit` i naciśnij Enter.
10. Wpisz polecenie `format z:/fs:NTFS /v:Extended_Volume /q` i naciśnij Enter.
11. Potwierdz wszystkie pytania wciskając przycisk Y i ewentualnie Enter.

Lista wszystkich poleceń dostępna jest po wprowadzeniu znaku zapytania.

11.2.4 Rozszerzanie woluminu

1. Otwórz przystawkę Disk Management z konsoli Computer Management.
2. Po kliknięciu prawym przyciskiem myszy na Extended_Volume wybierz polecenie Delete Volume.
3. Potwierdź operację klikając przycisk Yes.
4. Po kliknięciu prawym przyciskiem myszy na Data_Volume wybierz polecenie Extend Volume. Uruchomiony zostanie program Extend Volume Wizard.

5. Naciśnie przycisk Next.
6. Ustaw wielkość woluminu na 500 MB.
7. Naciśnie przycisk Next.
8. Naciśnij przycisk Finish.

11.2.5 Tworzenie nowej partycji

1. Po kliknięciu prawym przyciskiem myszy na Data_Volume wybierz polecenie Change Drive Letter And Paths.
2. Zmień literę dysku na np. `Y`.
3. Po kliknięciu prawym przyciskiem myszy na Data_Volume (Y:) wybierz polecenie Open.
4. Utwórz folder o nazwie `docs`.
5. Na dysku Disk 0 kliknij prawym przyciskiem myszy na nieprzydzieloną przestrzeń dyskową i wybierz polecenie New Volume.
6. Utwórz wolumn prosty wykorzystujac całą pozostałą na dysku przestrzeń. Zamiast przypisywać literę dysku, zainstaluj wolumin w ścieżce `Y:\docs`. Sformatuj wolumin stosując system plików NTFS i utwórz etykietę `docs_space`.
7. Sprawdź teraz dostępną przestrzeń na dysku `Y`.

11.2.6 Konfigurowanie przydziału dysku

1. Otwórz przystawkę Disk Management z konsoli Computer Management.
2. Po kliknięciu prawym przyciskiem myszy na wolumenie `docs_space` wybierz polecenie Open.
3. Kliknij zakładkę Quota.
4. Kliknij pole wyboru Enable Quota Management.
5. Zaznacz pole wyboru Deny Disk Space To Users Exceeding Quota Limit.
6. Zaznacz opcję Limit Disk Space To. Określ limit ważniości na mało wielkość, np. 5 MB, a poziom ostrzeżeń na jego połowę.
7. Zaznacz oba pola dotyczące opcji protokołowania.

8. Kliknij przycisk Apply.
9. Naciskając przycisk OK, zaakceptuj okno dialogowe Disk Quota.
10. W oknie dialogowym Properties woluminu `docs_space`, na zakładce Quota kliknij przycisk Quota Entries.
11. W menu Quota kliknij polecenie New Quota Entry.
12. Kliknij przycisk Advanced, a następnie Find Now. Wyświetlona zostanie lista wszystkich użytkowników domeny.
13. Wybierz jednego lub więcej użytkowników, kliknij przycisk OK i jeszcze raz OK.
14. Zmień wpisy określajace limit ważności, np na wielkość 20 MB, a poziom ostrzeżeń na 15 MB.
15. Przetestuj ustalone limity i ograniczenia.

Spis rysunków

Bibliografia

[1] Dan Holme, Orin Thomas, *Zarządzanie i obsługa rodowiska Microsoft Windows Serwer 2003*, Microsoft Press.

[2] Rand Morimoto, Michael Noel, Omar Droubi, Kenton Gardinier, Noel Neal, *Windows Server 2003. Księga eksperta*, Helion.

[3] Jill Spealman, Kurt Hudson, Melissa Craft, *Planowanie, wdrażanie i obsługa infrastruktury Active Directory Windows Server 2003*, Microsoft Press.