System plików NTFS

Korzystanie z systemu plików NTFS jest najlepszym sposobem przechowywania danych na partycjach dyskowych. W systemie tym istnieje rozbudowany aparat kontroli dostępu do plików i folderów oparty na przypisywaniu różnych uprawnień do tych zasobów. Możliwość kompresji danych oraz przydzielania użytkownikom tzw. kwot dyskowych (nieprzekraczalna ilość miejsca na dysku, jakie ma do dyspozycji użytkownik) pozwala na efektywne wykorzystanie przestrzeni dyskowej. Dodatkowym zabezpieczeniem danych jest możliwość szyfrowania plików przy pomocy systemu EFS (Encrypting File System)

Listy kontroli dostępu

Na partycji NTFS, z każdym plikiem i folderem przechowywana jest lista ACL (Access Control List). Zawiera ona wykaz wszystkich kont użytkowników, grup i komputerów, które mają określona prawa dostępu do pliku lub folderu, łącznie z wyszczególnieniem tych uprawnień. Aby użytkownik mógł uzyskać dostęp do pliku lub folderu, na liście ACL musi istnieć wpis, określany jako ACE (Access Control Entry), dla konkretnego użytkownika, dla grup do których należy użytkownik, lub dla komputera, z którego wykonuje operację na pliku lub folderze. Wpis ten musi zawierać zezwolenie na dostęp i określać sposób dostępu użytkownika do zasobu. W przeciwnym przypadku użytkownik nie uzyska dostępu do zasobu.

Uprawnienia NTFS

Uprawnienia NTFS do pliku (folderu) określają zakres czynności, jakie użytkownicy mogą przeprowadzić na danym pliku (folderze), bądź jego zawartości. W poniższych tabelach wyszczególnione są standardowe uprawnienia NTFS wraz z opisem operacji, na jakie dane uprawnienia zezwalają.

Uprawnienia NTFS do folderów

Read	Przeglądanie plików i podfolderów, odczyt atrybutów i uprawnień do folderu, identyfikacja właściciela folderu
	Tworzenie w folderze nowych plików i folderów, zmiana atrybutów folderu, przeglądanie uprawnień do folderu, identyfikacja właściciela folderu
List Folder Contents	Przeglądanie listy plików i podfolderów wewnątrz folderu
Read and Execute	Przemieszczanie się w drzewie katalogów w obrębie folderu i podfolderów, wszystkie czynności, na które zezwalają uprawnienia Read oraz List Folder Contents
Modify	Usunięcie folderu, wszystkie czynności, na które zezwalają uprawnienia Write oraz Read and Execute

Full Control	Zmiana uprawnień do folderu, przejęcie folderu na własność, usuwanie plików i podfolderów z folderu, wszystkie działania, na które zezwala dowolne inne uprawnienie NTFS do folderu

Uprawnienia NTFS do plików

Read	Odczyt zawartości pliku, odczyt atrybutów i uprawnień do pliku, identyfikacja właściciela pliku
Write	Modyfikacja pliku, zmiana atrybutów pliku, odczyt uprawnień do pliku, identyfikacja właściciela pliku
Read and Execute	Uruchamianie programów, wszystkie czynności, na które zezwala uprawnienie Read
Modify	Modyfikacja i usunięcie pliku, wszystkie czynności, na które zezwalają uprawnienia Write i Read and Execute
Full Control	Zmiana uprawnień do pliku, przejęcie pliku na własność, wzsystkie czynności, na które zezwala dowolne inne uprawnienie NTFS do pliku

Uwaga: Gdy partycja dyskowa formatowana jest dla systemu NTFS, do katalogu głównego automatycznie przypisywane jest uprawnienie Full Control dla grupy Everyone. A zatem grupa Everyone ma domyślne uprawnienie Full Control do wszystkich plików i folderów tworzonych w katalogu głównym. Aby zezwolić na dostęp do zasobów tylko autoryzowanym użytkownikom, należy zmienić domyślne uprawnienia do tworzonych plików i folderów.

Uprawnienia NTFS przypisywane są na karcie **Security** w oknie dialogowym **Properties** odpowiedniego pliku lub katalogu. Okno to otwiera się po kliknięciu prawym przyciskiem myszy w ikonę pliku lub folderu i wybranie opcji **Properties** z menu podręcznego. Podczas przypisywania, bądź zmiany uprawnień NTFS, można także dodać lub usunąć nowych użytkowników, grupy czy komputery do listy uprawnionych do pliku lub folderu. Wskazując użytkownika lub grupę można również zmienić przypisane im uprawnienia.

W poniższej tabeli opisane jest znaczenie elementów widocznych na karcie **Security**.

Element	Opis
Name	Lista użytkowników i (lub) grup, dla których określone są uprawnienia do zasobu. Użytkownicy i grupy nie występujące na tej liście nie mają żadnych uprawnień do zasobu.
Permission	Uprawnienia, które ma użytkownik lub grupa zaznaczona na liście **Name**

Add	Przycisk otwierający okno **Select User, Group or Computer**, z którego wybiera się użytkownika, grupę lub komputer do umieszczenia na liście **Name**
Remove	Przycisk usuwający użytkownika, grupę lub komputer z listy **Name**, co powoduje odebranie wszystkich uprawnień do zasobu
Advanced	Przycisk otwierający okno **Access Control Settings** służące do zarządzania specjalnymi uprawnieniami NTFS do zasobu

Wielokrotne uprawnienia NTFS – kumulacja uprawnień

Jeśli uprawnienia NTFS do jakiegoś zasobu przypisywane są jednocześnie użytkownikowi i grupom, do których ten użytkownik należy, wówczas ten sam użytkownik może mieć przypisanych wiele różnych uprawnień NTFS do tego samego zasobu. W takiej sytuacji efektywne uprawnienia użytkownika wynikają z następujących reguł:

1. Efektywne uprawnienia do zasobu są kumulacją uprawnień przypisanych jawnie danemu użytkownikowi, oraz grupom, do których ten użytkownik należy. Na przykład, jeśli użytkownik posiada uprawnienie Read do folderu i należy do grupy, której przypisano uprawnienie Write do tego folderu, efektywne uprawnienia są połączeniem uprawnień Read i uprawnień Write.

2. Uprawnienia NTFS do plików mają wyższy priorytet, niż uprawnienia do folderów. Jeśli użytkownik ma uprawnienie Modify do pliku, wówczas będzie mógł dokonywać w nim zmian, mimo że do folderu, w którym znajduje się plik, ma np. tylko uprawnienie Read.

3. Użytkownikowi lub grupie można zabronić dostępu do wybranego zasobu poprzez przypisanie uprawnienia **Deny**. Mimo, iż użytkownik może mieć przypisane inne uprawnienia pozwalające mu na dostęp do zasobu, zostaną one zablokowane przez uprawnienie Deny. Uprawnienie Deny jest jedynym wyjątkiem od reguły kumulowania uprawnień. W praktyce nie zaleca się stosowania tej metody ograniczania dostępu do zasobów, ponieważ znacznie prostszym sposobem jest zezwalanie na dostęp do nich wybranym użytkownikom i grupom. Preferowane jest takie projektowanie grup oraz organizowanie drzewa folderów, aby możliwe było zarządzanie dostępem do zasobów bez stosowania uprawnienia Deny.

Dziedziczenie uprawnień NTFS

Przypisanie uprawnień do folderu powoduje dziedziczenie uprawnień przez pliki i foldery w nim zawarte. Nadanie użytkownikowi określonych uprawnień do folderu jest równoważne z nadaniem tych uprawnień do wszystkich istniejących w tym folderze plików i podfolderów, jak również do nowo tworzonych plików i podfolderów.

Dziedziczenie uprawnień można zablokować, co spowoduje wyłączenie przekazywania uprawnień z folderu nadrzędnego do plików i folderów w nim zawartych. Aby wyłączyć mechanizm dziedziczenia, należy usunąć odziedziczone uprawnienia NTFS i nadać nowe uprawnienia. Folder, w którym zablokowano dziedziczenie uprawnień staje się w ten sposób

nowym folderem nadrzędnym, przekazującym uprawnienia do plików i folderów w nim zawartych.

W większości przypadków należy zezwolić na przekazywanie uprawnień z folderu nadrzędnego do plików i folderów w nim zawartych, ponieważ dziedziczenie upraszcza przypisywanie uprawnień do zasobów.

W niektórych przypadkach zablokowanie dziedziczenia może okazać się konieczne. Na przykład, umieszczenie wszystkich plików jakiegoś działu w jednym folderze, do którego każdy pracownik tego działu ma uprawnienie Write umożliwi pracownikom działu wprowadzanie zmian w plikach. Jednak jeśli kilka plików nie powinno być zmienianych, pracownicy działu powinni mieć do nich tylko uprawnienie Read. Należy zablokować propagację uprawnień dla tych dokumentów, aby uprawnienie Write nie było przez nie dziedziczone.

Aby zablokować dziedziczenie uprawnień dla określonego folderu, należy kliknąć ikonę folderu prawym przyciskiem myszy, z menu podręcznego wybrać opcję **Properties** i w oknie właściwości folderu otworzyć kartę **Security**. Na dole karty znajduje się pole **Allow inheritable permissions from parent to propagate to this object**, z którego należy usunąć zaznaczenie. Spowoduje to wyświetlenie okna **Security**, w którym widoczne będą przyciski **Copy** i **Remove**. Wciśnięcie **Copy** spowoduje skopiowanie uprawnień z folderu nadrzędnego i zablokuje dziedziczenie uprawnień przez pliki i podfoldery. Natomiast wciśnięcie **Remove** spowoduje usunięcie odziedziczonych uprawnień i pozostawienie tylko tych, które nadano przez operację przypisania. Oczywiście, dziedziczenie uprawnień też zostanie zablokowane.

Kopiowanie plików i folderów

W wyniku kopiowania plików lub folderów do innego folderu lub na inną partycję dyskową, uprawnienia do zasobów docelowych mogą ulec zmianom. Zmiany te podlegają następującym regułom:

1. Przy kopiowaniu pliku lub folderu w obrębie tej samej partycji NTFS, kopia zasobu dziedziczy uprawnienia od folderu docelowego.

2. Przy kopiowaniu pliku lub folderu na inną partycję NTFS, kopia zasobu dziedziczy uprawnienia od folderu docelowego.

3. Przy kopiowaniu pliku lub folderu na inną partycję nie będącą partycją NTFS (na przykład FAT), kopia zasobu traci wszelkie uprawnienia NTFS, ponieważ inne systemy plików nie przechowują, a co za tym idzie, nie wykorzystują informacji o uprawnieniach NTFS.

Uwaga: Aby móc kopiować pliki lub foldery w obrębie jednej partycji NTFS lub pomiędzy partycjami NTFS, użytkownik musi mieć uprawnienie Read do folderu źródłowego i uprawnienie Write do folderu docelowego.

Przenoszenie plików i folderów

W wyniku przenoszenia plików lub folderów do innego folderu lub na inną partycję dyskową, uprawnienia do zasobów docelowych mogą ulec zmianom. Zmiany te podlegają następującym regułom:

1. Przy przenoszeniu pliku lub folderu w obrębie tej samej partycji NTFS, uprawnienia do zasobu docelowego są zachowywane i pozostają takie same jak do zasobu źródłowego.

2. Przy przenoszeniu pliku lub folderu na inną partycję NTFS następuje przejmowanie uprawnień od folderu docelowego. Operacja przenoszenia jest więc równoważna skopiowaniu zasobu do nowej lokalizacji, a następnie usunięciu oryginału z poprzedniego miejsca.

3. Przy przenoszeniu pliku lub folderu na inną partycję nie będącą partycją NTFS (na przykład FAT), wszelkie uprawnienia NTFS ulegają usunięciu, ponieważ inne systemy plików nie przechowują, a co za tym idzie, nie wykorzystują informacji o uprawnieniach NTFS.

Uwaga: Aby móc przenosić pliki lub foldery w obrębie jednej partycji NTFS lub pomiędzy partycjami NTFS, użytkownik musi mieć uprawnienie Modify do folderu źródłowego i uprawnienie Write do folderu docelowego. Uprawnienie Modify jest niezbędne, ponieważ podczas przenoszenia zawartość folderu źródłowego ulega zmianie.

Kilka przykładów

Zakładamy, że na partycji NTFS istnieje folder **Folder1** zawierający plik **Plik1** i folder **Folder2**. Folder **Folder2** zawiera z kolei plik **Plik2**. Utworzone jest też konto użytkownika **User1**, który należy jednocześnie do grup **Users** i **Sales**.

Przykład 1

Grupa **Users** ma uprawnienie **Write**, a grupa **Sales** - uprawnienie **Read** do folderu **Folder1**. Użytkownik **User1** ma efektywne uprawnienia **Read** i **Write** do folderu **Folder1**, ponieważ uprawnienia **Read** i **Write** kumulują się z racji przynależności użytkownika do dwóch grup.

Przykład 2

Grupa **Users** ma uprawnienie **Read** do folderu **Folder1**, a grupa **Sales** - uprawnienie **Write** do folderu **Folder2**. Użytkownik **User1** ma efektywne uprawnienia **Read** i **Write** do pliku **Plik2**, ponieważ należy do grupy **Users** mającej uprawnienie **Read** do folderu **Folder1**, oraz do grupy **Sales** mającej uprawnienie **Write** do folderu **Folder2**. Plik **Plik2** dziedziczy uprawnienia zarówno od folderu **Folder1** jak i folderu **Folder2**.

Przykład 3

Grupa **Users** ma uprawnienie **Modify** do folderu **Folder1**. Należy spowodować, aby jedynym uprawnieniem do pliku **Plik2** było uprawnienie **Read** dla grupy **Sales**. W tym celu należy wyłączyć dziedziczenie w folderze **Folder2** lub pliku **Plik2** i usunąć z folderu **Folder2** lub

pliku **Plik2** uprawnienia odziedziczone od folderu **Folder1**. Następnie należy przypisać grupie **Sales** uprawnienie **Read** do folderu **Folder2** lub pliku **Plik2**.

Specjalne uprawnienia NTFS

Specjalne uprawnienia NTFS zapewniają większe pole manewru przy wyznaczaniu zakresu kontroli, jaką daje się użytkownikowi przypisując mu uprawnienia do zasobu. Istnieje 13 specjalnych uprawnień NTFS, które można zestawiać w różne kombinacje, dopasowując w ten sposób kontrolę użytkowników systemu nad zasobami do specyficznych wymagań danej organizacji.

Standardowe uprawnienia NTFS są również kombinacjami uprawnień specjalnych. Na przykład, standardowe uprawnienie Read składa się ze specjalnych uprawnień **Read Data**, **Read Attributes**, **Read Permissions** i **Read Extended Attributes**.

Dwa z uprawnień specjalnych są szczególnie użyteczne przy zarządzaniu dostępem do plików i folderów:

- **Change Permissions**. Uprawnienie to daje użytkownikowi możliwość zmiany uprawnień do pliku lub folderu bez konieczności nadawania mu uprawnienia **Full Control**. Dzięki temu, użytkownik nie będzie miał możliwości modyfikacji, ani usunięcia pliku lub folderu, ale będzie mógł nadawać do nich uprawnienia.

Uwaga: Jeśli użytkownik utworzy nowy plik lub folder, to nikt oprócz niego, nawet administrator, nie ma do tego zasobu uprawnienia Change Permissions. Aby zezwolić innym użytkownikom, w tym administratorom, na zmianę uprawnień, właściciel zasobu musi przypisać tym użytkownikom uprawnienia Change Permissions.

- **Take Ownership**. Uprawnienie to daje użytkownikowi możliwość stania się właścicielem pliku lub folderu. Właściciel lub użytkownik z uprawnieniem **Full Control** zasobu może nadać uprawnienie **Take Ownership** dowolnemu innemu użytkownikowi lub grupie, co pozwoli im na przejęcie pliku lub folderu na własność. Członek lokalnej grupy **Administrators** może przejąć na własność dowolny plik lub folder, niezależnie od posiadanych do niego uprawnień. Jeśli administrator przejmie zasób na własność, jego właścicielem staje się lokalne grupa **Administrators**, a wówczas dowolny użytkownik z tej grupy ma możliwość zmiany uprawnień do zasobu, łącznie z przypisaniem komukolwiek uprawnienia **Take Ownership**. Na przykład, administrator może przejąć na własność pliki pracownika odchodzącego z firmy, a następnie zezwolić na ich przejęcie przez innego pracownika, przejmującego obowiązki odchodzącego, przyznając mu uprawnienie **Take Ownership**.

Uwaga: Aby stać się właścicielem pliku lub folderu, użytkownik z uprawnieniem Take Ownership musi z tego uprawnienia w sposób bezpośredni skorzystać. Nie można przenieść własności zasobu na innego użytkownika. Właściciel, członek grupy Administrators, lub ktokolwiek z uprawnieniem Full Control może nadać uprawnienie Take Ownership innemu użytkownikowi, ale tylko sam użytkownik może przejąć zasób na własność.

Aby przypisać użytkownikowi lub grupie uprawnienia specjalne do pliku lub folderu, należy kliknąć w odpowiednią ikonę prawym przyciskiem myszy, z menu podręcznego wybrać opcję

Properties, następnie w oknie z właściwościami zasobu otworzyć kartę **Security** i wcisnąć przycisk **Advanced**. W wyniku tych czynności otworzy się okno dialogowe **Access Control Settings**, w którym na karcie **Permissions** należy wskazać użytkownika lub grupę, dla której chcemy ustawić uprawnienia specjalne NTFS i wcisnąć przycisk **View/Edit**. Otworzy się wówczas okno dialogowe **Permissions Entry for...**, w którym można konfigurować zakres kontroli nad zasobem przy pomocy 13 uprawnień specjalnych. Elementy okna **Permissions Entry for...** są opisane w poniższej tabeli.

Element	Opis
Name	Użytkownik lub grupa, której przypisywane są uprawnienia
Apply onto	Hierarchiczna podstruktura folderów w drzewie katalogów, które będą dziedziczyły skonfigurowane w panelu **Permissions** uprawnienia. Domyślnie wyświetla się **This folder, subfolders and files**
Permissions	Panel służący do konfiguracji specyficznych uprawnień do zasobu przy pomocy uprawnień specjalnych. Aby dodać określone uprawnienie specjalne, należy zaznaczyć odpowiadające mu pole w kolumnie **Allow**
Apply these permissions to objects and/or containers within this container only	
Clear All	Przycisk służący do szybkiego usunięcia wszystkich przypisanych uprawnień

Kompresja danych na partycjach NTFS

Każdy plik i folder, znajdujący się na partycji NTFS, ma tzw. atrybut kompresji. Stan tego atrybutu może przyjmować jedną z dwóch wartości – **compressed** lub **uncompressed**. Atrybut kompresji dla folderu nie musi być taki sam jak dla plików i folderów w nim zawartych. Na przykład, folder może być skompresowany, ale niektóre pliki w nim zawarte mogą nie być skompresowane. Jest również możliwa sytuacja taka, że nie skompresowany folder zawiera skompresowane pliki.

Na partycjach NTFS, miejsce na dysku przydzielane jest na podstawie rozmiaru nie skompresowanego pliku. Dlatego podczas kopiowania skompresowanego pliku na partycję, na której nie ma wystarczającej ilości miejsca dla pliku nie skompresowanego, zostanie wyświetlony komunikat o błędzie i plik nie będzie skopiowany.

Istnieje możliwość wyświetlania ikon skompresowanych plików i folderów w innym kolorze. W tym celu należy otworzyć program **Windows Explorer**, z menu **Tools** wybrać **Folder Options**, otworzyć kartę **View** i zaznaczyć opcję **Display compressed files and folders with alternate color**.

Wszystkie aplikacje Windows lub MS-DOS mogą odczytywać i zapisywać skompresowane pliki, bez wcześniejszej ich dekompresji lub kompresji za pomocą innego programu. Gdy aplikacja lub polecenie systemu operacyjnego wymaga dostępu do skompresowanego pliku, wówczas plik jest dekompresowany automatycznie. Po zamknięciu lub zapisaniu pliku następuje jego automatyczna kompresja.

Aby ustawić atrybut kompresji folderu lub pliku, należy kliknąć ikonę zasobu prawym przyciskiem myszy, z menu podręcznego wybrać **Properties**, w oknie właściwości zasobu otworzyć kartę **General** i kliknąć przycisk **Advanced**. Otworzy się wówczas okno **Advanced Attributes**, w którym należy zaznaczyć pole **Compress contents to save disk space**. Po zaznaczeniu tego pola zostanie wyświetlone kolejne okno - **Confirm Attribute Changes**, w którym należy wybrać jedną z dwóch dodatkowych opcji, opisanych w poniższej tabeli:

Opcja	Opis
Apply changes to this folder only	Powoduje skompresowanie tylko wybranego folderu, oraz plików i folderów, które będą dopiero tworzone. Nie powoduje kompresji już istniejących w folderze plików i podfolderów
Apply changes to this folder, subfolders and files	Powoduje skompresowanie wybranego folderu, oraz wszystkich plików i folderów w nim zawartych, zarówno już istniejących jak i nowo tworzonych

Uwaga: Nie można skompresować pliku ani folderu, jeśli zostały one zaszyfrowane. Gdy zaznaczone jest pole „Encrypt contents to secure data", wówczas nie ma możliwości włączenia kompresji takiego pliku lub folderu.

Kopiowanie i przenoszenie skompresowanych plików i folderów

W wyniku kopiowania albo przenoszenia pliku lub folderu do innego folderu, czy też na inną partycję dyskową**,** atrybut kompresji pliku lub folderu docelowego może ulec zmianie. Zmiana atrybutu kompresji podlega następującym regułom:

1. Gdy plik lub folder jest kopiowany w obrębie tej samej partycji NTFS, albo na inną partycję NTFS, wówczas przejmuje atrybut kompresji od folderu docelowego. Na przykład, przy kopiowaniu skompresowanego pliku do nie skompresowanego folderu, następuje automatyczna dekompresja pliku.

2. Gdy folder lub plik jest przenoszony w obrębie tej samej partycji NTFS, wówczas zachowuje swój atrybut kompresji. Na przykład, po przeniesieniu skompresowanego pliku do nie skompresowanego folderu, plik pozostanie skompresowany.

3. Gdy folder lub plik jest przenoszony na inną partycję NTFS, wówczas przejmuje atrybut kompresji od folderu docelowego. Przeniesienie pliku na inna partycję NTFS jest równoważne ze skopiowaniem, a następnie usunięciem z folderu źródłowego.

Uwaga: W systemie Windows Server 2003 kompresja jest możliwa tylko na partycjach NTFS. Gdy plik lub folder jest przenoszony lub kopiowany na partycję innego typu, następuje automatyczna dekompresja pliku lub folderu w lokalizacji docelowej.

Uwaga: W systemie Windows Server 2003 kopiowanie skompresowanego pliku lub folderu jest operacją trójetapową: najpierw plik jest dekompresowany, następnie kopiowany, a na końcu kompresowany ponownie. Może to mieć ujemny wpływ na wydajność systemu.

Wskazówki dotyczące kompresji danych dyskowych

Stopień kompresji pliku, czyli ilość miejsca zajęta przez plik skompresowany w stosunku do ilości miejsca zajmowanego przez plik nie skompresowany, zależy w sposób istotny od typu pliku. Na przykład, dla map bitowych stopień kompresji jest często mniejszy od 50%, natomiast stopień kompresji dla aplikacji często dochodzi do 75%. Z tego względu, pliki do kompresji należy wybierać pod względem typu, aby osiągnąć jak najlepszy efekt.

Nie można kompresować plików, które już raz zostały skompresowane. System Windows Server 2003 podejmie co prawda próbę ponownej kompresji pliku, ale spowoduje to tylko stratę czasu, bez uzyskania dodatkowego miejsca na dysku.

Aby łatwiejsze było odnajdywanie skompresowanych danych, należy korzystać z możliwości oznaczania innym kolorem skompresowanych plików i folderów.

Nie należy kompresować zasobów często używanych, a raczej dane archiwalne. Każda operacja kompresji i dekompresji zajmuje stosunkowo dużo czasu, co w konsekwencji może spowodować spadek wydajności systemu.

Kwoty dyskowe na partycjach NTFS

Kwoty dyskowe pozwalają na przydzielanie poszczególnym użytkownikom określonej ilości miejsca na dysku, co pozwala na kontrolę zajmowania przestrzeni dyskowej przez pliki i foldery tworzone przez użytkowników. Każdemu użytkownikowi może być przydzielony określony limit, w ramach którego użytkownik ten może wykorzystywać przestrzeń dyskową na danej partycji NTFS. Nie jest istotne, w którym folderze znajdują się pliki i foldery użytkownika, limit dotyczy całej partycji, a nie wybranych folderów.

Kwoty dyskowe są przydzielane niezależnie dla każdej partycji NTFS, nawet jeśli partycje znajdują się na jednym dysku fizycznym. Oznacza to, ilość dostępnego miejsca w jednej partycji NTFS jest niezależna od ilości dostępnego miejsca w innej partycji NTFS.

Wykorzystanie przestrzeni dyskowej oparte jest na prawie własności do plików i folderów. Gdy użytkownik tworzy na partycji NTFS nowy plik lub folder, kopiuje plik lub folder na partycję NTFS, oraz przejmuje na własność plik lub folder znajdujący się na partycji NTFS, wówczas miejsce zajmowane przez ten plik lub folder obciąża limit przyznany użytkownikowi.

Przy obciążaniu limitu nie jest brany pod uwagę atrybut kompresji pliku lub folderu. Nawet jeśli plik lub folder jest skompresowany, to i tak limit jest obciążany rozmiarem nie skompresowanego pliku lub folderu.

Istnieje możliwość ostrzegania użytkownika o wyczerpywaniu się jego limitu. W tym celu należy ustawić tzw. poziom ostrzegania, co spowoduje, że po przekroczeniu określonego progu procentowego użytkownik będzie ostrzegany o wyczerpywaniu się jego limitu, a oprócz tego informacja o tym zdarzeniu zostanie zapisana do dziennika zdarzeń systemowych (w przypadku ustawienia odpowiedniej opcji). Po wyczerpaniu się limitu użytkownikowi zostanie zablokowany dostęp do dysku, chyba że administrator zezwoli mu na przekroczenie limitu i kontynuowanie pracy.

Aby włączyć przydziały dyskowe, należy otworzyć program **My Computer** lub **Windows Explorer**, kliknąć prawym przyciskiem myszy w ikonę dysku, z menu podręcznego wybrać opcję **Properties** i w oknie właściwości dysku otworzyć kartę **Quota**. Na karcie tej można konfigurować limitowanie przestrzeni dyskowej przy pomocy różnych opcji opisanych w poniższej tabeli:

Opcja	Opis
Enable quota management	Zaznaczenie tej opcji włącza mechanizm kwot
Deny disk space to users exceeding quota limit	Zaznaczenie tej opcji powoduje, że po przekroczeniu przez użytkownika limitu miejsca na dysku, wyświetlany jest komunikat **Out of disk space**, oraz następuje zablokowanie możliwości zapisu na dysk
Do not limit disk usage	Zaznaczenie tej opcji powoduje przyznanie nowym użytkownikom nieograniczonego limitu
Limit disk space to	Zaznaczenie tej opcji powoduje ustawienie limitu dla nowych użytkowników na wartość określoną w polu znajdującym się po prawej stronie
Set warning level to	Pole służące do określenia ilości miejsca zajmowanego przez dane użytkownika, po przekroczeniu której użytkownik otrzymuje komunikat ostrzegawczy o wyczerpywaniu się miejsca w ramach przyznanego limitu
Select the quota logging options for this volume	Są to opcje, których zaznaczenie powoduje, że fakt przekroczenia przez użytkownika przyznanego mu limitu i (lub) przekroczenia poziomu ostrzegania będzie zapisany w dzienniku zdarzeń systemowych
Quota Entries	Przycisk otwierający okno **Quota Entries for...**, w którym można dodać nowy przydział dyskowy albo obejrzeć lub usunąć istniejący przydział

Kwoty dyskowe mogą być określane zbiorczo dla wszystkich użytkowników, bądź indywidualnie dla wybranych użytkowników. Aby określić kwoty dla wszystkich użytkowników, w polach **Limit disk space to**, oraz **Set warninig level to** należy wpisać wymagane wartości limitu przestrzeni dyskowej i poziomu ostrzegawczeg, oraz zaznaczyć pole opcji **Deny disk space to users exceeding quota limit** i wcisnąć **OK**. System Windows server 2003 będzie monitorował wykorzystanie przestrzeni dyskowej i w przypadku próby przekroczenia limitu, nastąpi odmowa utworzenia nowego pliku lub folderu.

Aby określić indywidualną kwotę dla wybranego użytkownika, w oknie właściwości dysku należy wcisnąć przycisk **Quota Entries**, i w otwartym w ten sposób oknie **Quota Entries for...** utworzyć nowy wpis określający limit dla wskazanego użytkownika. Wpis taki tworzy się przez wybranie z menu **Quota** opcji **New Quota Entry**, wskazanie użytkownika na liście i określenie limitu ilości miejsca i poziomu ostrzegawczego.

Szyfrowanie danych przy użyciu EFS

System szyfrowania plików EFS (Encrypting file system) umożliwia szyfrowanie danych, od poziomu pliku wzwyż, na partycjach NTFS. Technika szyfrowania EFS opiera się na metodzie klucza publicznego, jest integralną usługą systemową i pozwala na deszyfrowanie plików przez tego użytkownika, który je zaszyfrował, lub wyznaczonego agenta odzyskiwania EFS. Agent odzyskiwania jest potrzebny wówczas, gdy użytkownik, który zaszyfrował plik utraci swój klucz, albo klucz ten jest niedostępny z innych powodów. Domyślnym agentem odzyskiwania jest administrator.

Oto kluczowe cechy systemu EFS:

- Operacje szyfrowania i deszyfrowania są przeprowadzane w tle w sposób niewidoczny dla użytkowników i aplikacji korzystających z tych plików.

- System EFS umożliwia dostęp do pliku tylko autoryzowanemu użytkownikowi. Przed otwarciem pliku jest on automatycznie deszyfrowany i szyfrowany ponownie przed zamknięciem i zapisaniem na dysk. Administrator, lub ogólnie – wyznaczony agent odzyskiwania, może przywrócić do postaci jawnej plik zaszyfrowany przez dowolnego użytkownika. Umożliwia to dostęp do zaszyfrowanego pliku, gdy użytkownik jest w danej chwili nieobecny lub utraci swój klucz prywatny.

- System EFS ma wbudowany system odzyskiwania danych. W systemie zabezpieczeń Windows Server 2003 wymuszana jest konfiguracja kluczy odzyskiwania. Szyfrowanie plików jest możliwe tylko wtedy, kiedy na komputerze lokalnym istnieje co najmniej jeden klucz odzyskiwania. System EFS automatycznie generuje klucze odzyskiwania i umieszcza je w rejestrze systemu, gdy nie jest możliwe połączenie z kontrolerem domeny.

    - Szyfrowanie i kompresja wykluczają się nawzajem. Nie można zaszyfrować skompresowanego pliku lub folderu, jak również nie można poddać kompresji zaszyfrowanego pliku lub folderu.

Aby zaszyfrować plik lub folder znajdujący się na partycji NTFS, należy otworzyć okno z właściwościami obiektu, na karcie **General** wcisnąć **Advanced** i zaznaczyc pole opcji **Encrypt contents to secure data**.

Po zaszyfrowaniu folderu, tworzone i zapisywane w nim pliki i podfoldery będą automatycznie szyfrowane. Podczas przenoszenia pliku z folderu nie zaszyfrowanego do folderu zaszyfrowanego plik jest automatycznie szyfrowany. Do szyfrowania zawartości plików używane są szybkie klucze symetryczne przechowywane w polach DDF (Data Decryption Field) oraz DRF (Data Recovery Field), znajdujących się w nagłówku pliku. Pliki szyfrowane są blokami, przy czym do każdego bloku stosuje się inny klucz.

Podczas otwierania zaszyfrowanego pliku, system EFS automatycznie wykrywa szyfrowanie i wyszukuje certyfikat użytkownika, oraz powiązany z nim klucz prywatny. Klucz ten jest wykorzystywany do deszyfrowania pola DDF i odblokowania listy kluczy szyfrujących

Zaszyfrowany plik może odczytać tylko właściciel klucza prywatnego lub agent odzyskiwania EFS. Nawet, jeśli administrator przypisze innemu użytkownikowi uprawnienie

Take Ownership do pliku i użytkownik ten przejmie plik na własność, to nie będzie go mógł odczytać, dopóki nie będzie miał dostępu do klucza prywatnego, lub nie stanie się agentem odzyskiwania EFS.

Jeśli jest niedostępny prywatny klucz użytkownika, który zaszyfrował plik, wówczas plik może odszyfrować agent odzyskiwania EFS. Wykorzystuje on do tego swój klucz prywatny, który zastosowany do pola DRF, odblokowuje listę kluczy szyfrujących zawartość pliku. Jeśli agent odzyskiwania pracuje na innym komputerze, wówczas plik należy przesłać do niego. Agent odzyskiwania może również przesłać swój klucz prywatny do innego komputera, ale nie jest to zalecane ze względów bezpieczeństwa. Istnieje po prostu możliwość przechwycenia klucza w czasie jego transmisji.

Aby odzyskać zaszyfrowany plik lub folder będąc agentem odzyskiwania EFS, należy otworzyć okno z właściwościami obiektu, następnie na karcie **General** wcisnąć przycisk **Advanced** i usunąć zaznaczenie z pola opcji **Encrypt contents to secure data**.

NTFS – podsumowanie

Oto w skrócie te własności systemu NTFS, których nie ma system FAT lub FAT32

- Zabezpieczenie dostępu do plików i folderów w oparciu o rozbudowany system uprawnień – 13 podstawowych uprawnień, z których można komponować uprawnienia złożone (prawa dostępu do plików i folderów w systemach FAT i FAT32 określają atrybuty)
- Tworzenie kwot dyskowych, czyli ograniczania rozmiaru przestrzeni dyskowej dostępnej dla użytkownika
- Kompresja i szyfrowanie plików i folderów
- Możliwość rozszerzania wolumenów sformatowanych w systemie NTFS
- Możliwość montowania partycji lub wolumenów sformatowanych w dowolnym systemie plików do pustych folderów na partycjach lub wolumenach NTFS
- Możliwość śledzenia prób dostępu (audyt) do plików i folderów
- Wielkość pliku jest ograniczona tylko rozmiarem partycji lub wolumenu
- Możliwość używania długich nazw plików i folderów – do 255 znaków