

Rozdział 6: Zarządzanie danymi na partycjach NTFS

Spis treści

Przegląd zagadnień	1
Wprowadzenie do uprawnień NTFS	2
Zastosowanie uprawnień NTFS w systemie Windows 2000	4
Wykorzystanie uprawnień NTFS	11
Wykorzystanie specjalnych uprawnień NTFS	15
Laboratorium A: Wykorzystanie uprawnień NTFS	19
Kompresja danych na partycjach NTFS	24
Konfiguracja przydziałów dyskowych na partycjach NTFS	29
Laboratorium B: Konfiguracja kompresji dysku i przydziałów dyskowych	33
Zabezpieczanie danych przy użyciu systemu EFS	39
Laboratorium C: Zabezpieczanie plików przy użyciu systemu EFS	44
Podsumowanie	50



Zastrzega się prawo wprowadzania zmian do treści niniejszego dokumentu bez uprzedniego powiadomienia. Wszelkie nazwy firm, nazwiska i imiona osób oraz inne dane wykorzystywane w przykładach są fikcyjne, o ile nie zaznaczono, że jest inaczej. Odpowiedzialność za przestrzeganie wszelkich praw autorskich ponosi użytkownik. Niniejszego dokumentu ani jego części nie wolno powielać w żadnej formie, ani przekazywać za pomocą jakichkolwiek nośników elektronicznych lub mechanicznych, z wyjątkiem przypadków, gdy uzyskano na to pisemną zgodę firmy Microsoft Corporation. Jeżeli użytkownik ma dostęp do tego dokumentu wyłącznie w formie elektronicznej, zezwala się na wydrukowanie jednego egzemplarza tego dokumentu.

Firma Microsoft może mieć patenty lub rozpoczęte postępowania patentowe, znaki towarowe, prawa autorskie lub inne prawa związane z własnością intelektualną, które odnoszą się do treści zawartej w tym dokumencie. Otrzymanie tego dokumentu nie oznacza udzielenia licencji na patenty, znaki towarowe, prawa autorskie lub inne prawa związane z własnością intelektualną, z wyjątkiem wyraźnie określonych przypadków zawartych w pisemnych umowach licencyjnych firmy Microsoft.

© 2000 Microsoft Corporation. Wszelkie prawa zastrzeżone.

Microsoft, Active Desktop, Active Directory, ActiveX, BackOffice, DirectX, FrontPage, JScript, MS-DOS, NetMeeting, PowerPoint, Visual Basic, Visual Studio, Windows, Windows Media, and Windows NT są zastrzeżonymi znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Microsoft Corporation zarejestrowanymi w USA i/lub w innych krajach.

Wszelkie inne nazwy firm i produktów wymienione w niniejszym dokumencie mogą być znakami towarowymi zarejestrowanymi przez ich właścicieli.

Project Lead: Rick Selby

Instructional Designers: Kelly Bowen, Victoria Fodale (ComputerPREP),
H. James Toland III (ComputerPREP), Kathryn Yusi (Independent Contractor),
Barbara Pelletier (S&T Onsite)

Lead Program Manager: Andy Ruth (Infotec Commercial Systems)

Program Manager: Chris Gehrig (Infotec Commercial Systems),
Joern Wettern (Wettern Network Solutions)

Graphic Artist: Kimberly Jackson (Independent Contractor)

Editing Manager: Lynette Skinner

Editor: Kelly Baker (The Write Stuff)

Copy Editor: Kathy Toney (S&T Consulting)

Online Program Manager: Debbi Conger

Online Publications Manager: Arlo Emerson (Aditi)

Online Support: David Myka (S&T Consulting)

Multimedia Development: Kelly Renner (Entex)

Courseware Test Engineers: Jeff Clark, H. James Toland III (ComputerPREP)

Testing Developer: Greg Stemp (S&T OnSite)

Compact Disc Testing: Data Dimensions, Inc.

Courseware Testing: Data Dimensions, Inc.

Production Support: Carolyn Emory (S&T Consulting)

Manufacturing Manager: Rick Terek (S&T OnSite)

Manufacturing Support: Laura King (S&T OnSite)

Lead Product Manager, Development Services: Bo Galford

Lead Product Manager: Gerry Lang

Group Product Manager: Robert Stewart

Simulation and interactive exercises were built with Macromedia Authorware

Opracowanie wersji polskiej: DC Edukacja Sp. z o.o. Sopot

Współpraca: P.S.I. Sp. z o.o. Kielce

Zespół tłumaczy: Przemysław Dąbkowski, Sylwester Nowicki, Marcin Sworzyński

Konsultacja: Waldemar Pierścioneek, Witold Stajura, Piotr Zejer

Uwagi dla wykładowcy

Prezentacja:
75 minut

W tej części kursu słuchacze zdobędą wiedzę oraz umiejętności niezbędne do konfigurowania uprawnień dostępu do plików na partycjach w systemie NTFS, konfigurowania przydziałów dyskowych oraz zabezpieczania danych poprzez włączanie systemu szyfrowania plików i folderów.

Laboratoria:
75 minut

Po zrealizowaniu tego rozdziału słuchacz będzie potrafił:

- Opisać uprawnienia NTFS.
- Wyjaśnić sposób stosowania uprawnień NTFS w systemie Microsoft® Windows® 2000.
- Wykorzystywać uprawnienia NTFS.
- Przypisywać specjalne uprawnienia NTFS.
- Kompresować dane na partycjach NTFS.
- Konfigurować przydziały dyskowe na partycjach NTFS.
- Zabezpieczać dane przy wykorzystaniu systemu EFS (Encrypting File System).

Materiały i sposób przygotowania

W tej sekcji opisano sposób przygotowania wykładowcy oraz materiały niezbędne do właściwej prezentacji rozdziału.

Wymagane materiały

Do przedstawienia tego rozdziału wykładowcy potrzebne będą następujące materiały:

- Prezentacja Microsoft PowerPoint®: 2152B_06.ppt.

Sposób przygotowania

Aby przygotować się do przedstawienia tego rozdziału należy:

- Przeczytać wszystkie dokumenty dotyczące rozdziału.
- Wykonać wszystkie laboratoria.

Zadania dodatkowe

W tej sekcji przedstawiono sposób przygotowania interaktywnych zajęć, takich jak zabawy czy ćwiczenia z przydzieleniem ról, mających na celu prezentację lub podsumowanie zagadnień.

Dyskusja

► Aby przygotować się do zajęć interaktywnych należy:

1. Przeczytać pytania i odpowiedzi, przeznaczone do dyskusji.
2. Przemyśleć alternatywne rozwiązania, z uwzględnieniem ich zalet i wad.

Strategia przedstawienia rozdziału

Wskazówki dotyczące prezentacji rozdziału:

- Wprowadzenie do uprawnień NTFS

W tej części rozdziału zawarto informacje dotyczące uprawnień NTFS do plików. Należy wyjaśnić, w jaki sposób wpływają one na dostęp użytkowników i grup do plików i folderów.

- Zastosowanie uprawnień NTFS w systemie Windows 2000

W tej części rozdziału zawarto informacje o przypisywaniu uprawnień NTFS w systemie Windows 2000. Należy wyjaśnić sposób działania kombinacji wielu uprawnień. Następnie, omówić dziedziczenie uprawnień oraz sposób zapobiegania dziedziczeniu. Wyjaśnić wpływ kopiowania oraz przenoszenia plików i folderów na przypisane do nich uprawnienia NTFS. Jako metodę utrwalenia tych wiadomości, wykorzystać dyskusję na temat stosowania uprawnień NTFS w systemie Windows 2000.

- Wykorzystanie uprawnień NTFS

W tej części rozdziału zawarto informacje o wykorzystaniu uprawnień NTFS w celu kontroli dostępu użytkowników i grup do plików i folderów. Przedstawić sposób przypisywania uprawnień do folderu. Zaprezentować blokowanie dziedziczenia uprawnień przez pliki zawarte w folderze. Podkreślić, że pliki i foldery domyślne dziedziczą uprawnienia NTFS folderów macierzystych. Omówić dobre nawyki i zasady stosowane przy przypisywaniu uprawnień NTFS.

- Wykorzystanie specjalnych uprawnień NTFS

W tej części rozdziału zawarto informacje na temat wykorzystania specjalnych uprawnień NTFS w celu kontroli dostępu użytkowników i grup do plików i folderów. Przedstawić różnice pomiędzy uprawnieniami standardowymi i specjalnymi oraz związki pomiędzy nimi. Krótko opisać dwa uprawnienia specjalne, przedstawione w tym rozdziale.

- Kompresja danych na partycjach NTFS

W tej części rozdziału zawarto informacje o kompresji danych, stosowanej na partycjach NTFS w celu zaoszczędzenia miejsca na dysku. Należy omówić trzy charakterystyczne cechy skompresowanych plików i folderów. Następnie pokazać sposób włączenia kompresji folderu oraz ustawienia innego koloru do jego wyświetlania. Wykorzystać animowane slajdy w celu omówienia zachowania atrybutu kompresji przy kopiowaniu i przenoszeniu plików i folderów. Omówić dobre nawyki przy wykorzystaniu kompresji.

- Konfiguracja przydziałów dyskowych na partycjach NTFS

W tej części rozdziału zawarto informacje o zarządzaniu udziałami dyskowymi (disk quotas) w celu gospodarowania miejscem składowania danych. Należy omówić charakterystykę zarządzania udziałami i sposób, w jaki można je aktywować, zarówno dla wszystkich użytkowników razem, jak i każdego z osobna.

- Zabezpieczanie danych przy użyciu systemu EFS

W sekcji tej zawarto informacje o wykorzystaniu systemu EFS do zabezpieczenia danych na partycjach NTFS. Należy omówić cel szyfrowania i deszyfrowania plików oraz folderów. Następnie pokazać sposób szyfrowania i deszyfrowania plików. Zademonstrować też procedurę odzyskiwania zaszyfrowanych plików.

Informacje uzupełniające

W sekcji tej opisano wymagania dotyczące instalacji laboratorium dla tego rozdziału oraz zmiany w konfiguracji, które zachodzą na komputerach słuchaczy w trakcie realizacji laboratorium. Informacje te będą pomocne w powieleniu lub dostosowywaniu materiałów szkoleniowych MOC (Microsoft Official Curriculum).

Ważne Aby możliwe było wykonanie laboratorium, zawartego w tym rozdziale, konieczne jest odpowiednie skonfigurowanie pracowni, zgodnie z uwagami znajdującymi się w sekcji Informacje uzupełniające, zamieszczonej w rozdziale Przygotowanie pracowni do kursu 2244A; *Wdrożenie systemów Microsoft Windows 2000 Professional i Microsoft Windows 2000 Server*.

Przygotowanie laboratorium

Do wykonania laboratorium w tym rozdziale wymagane jest, aby każdy z komputerów słuchaczy był serwerem członkowskim w domenie nwtraders.msft. Aby komputery słuchaczy spełniały te wymagania, należy ukończyć Laboratorium A “Instalacja systemu Windows 2000” z Rozdziału 1 “Instalacja lub uaktualnienie do systemu Windows 2000” kursu 2244A, *Wdrożenie systemów Microsoft Windows 2000 Professional i Microsoft Windows 2000 Server*.

Rezultaty laboratorium

Wykonanie laboratorium z tego rozdziału spowoduje następujące zmiany w konfiguracji komputerów słuchaczy:

- Uprawnienia NTFS do folderu C:\MOC\Win2152b\Labfiles\Lab06\Data zostaną zmodyfikowane w stosunku do domyślnych.
- Folder Inetpub (oraz jego zawartość) zostaną skompresowane.

Przegląd zagadnień

Cel slajdu

Przedstawienie tematów i celów rozdziału.

Wprowadzenie

W tej części kursu przedstawione zostaną zagadnienia związane z zarządzaniem danymi na partycjach NTFS.

- Wprowadzenie do uprawnień NTFS
- Zastosowanie uprawnień NTFS w Windows 2000
- Wykorzystanie uprawnień NTFS
- Wykorzystanie specjalnych uprawnień NTFS
- Kompresja danych na partycjach NTFS
- Konfiguracja przydziałów dyskowych na partycjach NTFS
- Zabezpieczanie danych przy wykorzystaniu EFS

Wykorzystanie systemu plików NTFS w Microsoft® Windows® 2000 jest najlepszym sposobem przechowywania danych na partycjach dyskowych. W systemie NTFS można przypisywać uprawnienia do plików i folderów w celu kontroli dostępu użytkowników do tych zasobów. Dzięki możliwości kompresji danych oraz przydziałom dyskowym, system NTFS umożliwia także efektywniejsze wykorzystanie miejsca na dysku. Dodatkowo, pozwala na szyfrowanie plików na dyskach fizycznych za pomocą systemu EFS (Encrypting File System). Zrozumienie zasad funkcjonowania systemu plików NTFS oraz poznanie jego właściwości, umożliwia efektywne wykorzystanie tego składnika systemu Windows 2000.

Po zrealizowaniu tego rozdziału słuchacz będzie potrafił:

- Opisać uprawnienia NTFS.
- Wyjaśnić sposób stosowania uprawnień NTFS w systemie Microsoft® Windows® 2000.
- Wykorzystywać uprawnienia NTFS.
- Przypisywać specjalne uprawnienia NTFS.
- Kompresować dane na partycjach NTFS.
- Konfigurować przydziały dyskowe na partycjach NTFS.
- Zabezpieczać dane przy wykorzystaniu systemu EFS (Encrypting File System).

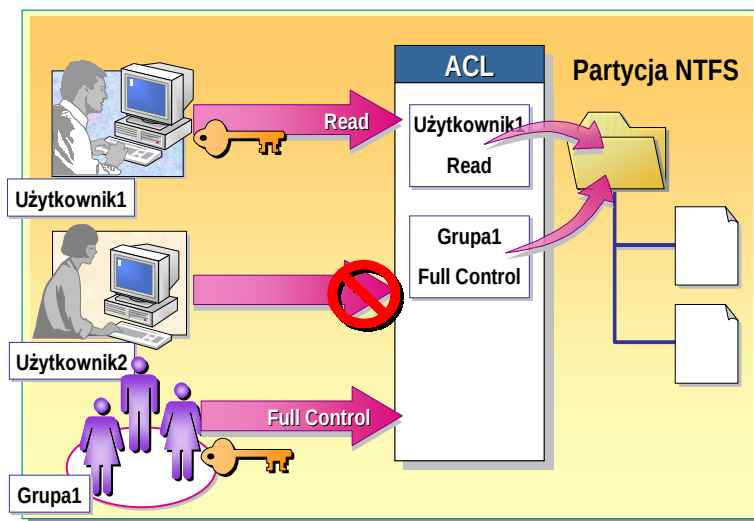
Wprowadzenie do uprawnień NTFS

Cel slajdu

Wprowadzenie do uprawnień NTFS.

Wprowadzenie

Aby kontrolować dostęp użytkowników do folderów i pojedynczych plików, należy wykorzystać uprawnienia NTFS.



Zagadnienie kluczowe

Uprawnienia NTFS są dostępne tylko na partycjach NTFS.

Nie można z nich korzystać na partycjach w systemach FAT i FAT32.

W systemie Windows 2000, uprawnienia NTFS są dostępne tylko na partycjach NTFS. Aby zabezpieczyć pliki i foldery na takich dyskach, należy przypisać uprawnienia NTFS każdemu użytkownikowi lub grupie, potrzebującym dostępu do zasobów. Każdy z użytkowników musi mieć jawnie przypisane uprawnienia do zasobów. Jeśli żadne uprawnienia nie zostaną użytkownikowi przypisane, nie będzie on mógł korzystać z pliku czy folderu. Uprawnienia NTFS działają zawsze, gdy użytkownik uzyskuje dostęp do pliku lub folderu lokalnie oraz przez sieć.

Lista kontroli dostępu

W systemie NTFS, z każdym plikiem i folderem na partycji NTFS, przechowywana jest lista ACL (Access Control List). Zawiera ona wykaz wszystkich kont użytkowników, grup i komputerów, które mają zdefiniowane prawo dostępu do pliku lub folderu, łącznie z rodzajem przypisanych 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, bądź dla komputera, z którego wykonuje operację. Wpis ten musi zawierać zezwolenie na dostęp i określać sposób dostępu użytkownika do zasobu. W przeciwnym wypadku użytkownik nie będzie miał dostępu do zasobu.

Uprawnienia NTFS

Uprawnienia NTFS wykorzystywane są w celu wskazania komputerów, użytkowników i grup, które mają prawo dostępu do plików lub folderów. Przy pomocy uprawnień NTFS określa się również zakres czynności, jakie użytkownicy mogą wykonać w odniesieniu do zawartości tych zasobów.

Uprawnienia NTFS do folderów

Uprawnienia do folderów przypisywane są w celu kontrolowania dostępu do tych folderów oraz plików i folderów w nich zawartych. W poniższej tabeli zawarto opis standardowych uprawnień NTFS do folderów oraz rodzaju dostępu, jaki każde z nich zapewnia.

Wyjaśnij, że Read-only, Hidden, Archive i System to atrybuty plików i folderów, a nie uprawnienia do nich.

Uprawnienie NTFS do folderu	Zezwala użytkownikowi na
Read	Przeglądanie plików i folderów, podgląd atrybutów i uprawnień do folderu oraz identyfikację właściciela.
Write	Tworzenie w folderze nowych plików i folderów, zmianę atrybutów folderu, podgląd uprawnień do folderu oraz identyfikację właściciela.
List Folder Contents	Przeglądanie listy plików i folderów wewnątrz folderu.
Read & Execute	Przechodzenie w drzewie katalogów wewnątrz folderu oraz wszystkie czynności, na które zezwalają uprawnienia Read oraz List Folder Contents.
Modify	Usunięcie folderu oraz wszystkie działania, na które zezwalają uprawnienia Write oraz Read & Execute.
Full Control	Zmianę uprawnień, przejęcie folderu na własność, usuwanie plików i folderów zawartych w folderze oraz wszystkie działania, na które zezwala dowolne inne uprawnienie NTFS do folderów.

Uprawnienia NTFS do plików

Uprawnienia do plików stosowane są w celu kontrolowania dostępu do plików. W poniższej tabeli zawarto opis standardowych uprawnień NTFS do plików oraz rodzaju dostępu, jaki poszczególne z nich zapewniają

Uprawnienie NTFS do pliku	Zezwala użytkownikowi na
Read	Odczyt zawartości pliku, atrybutów i uprawnień do folderu oraz identyfikację właściciela.
Write	Nadpisanie pliku, zmianę atrybutów pliku, podgląd uprawnień do pliku i identyfikację właściciela.
Read & Execute	Uruchamianie programów oraz wszystkie czynności, na które zezwala uprawnienie Read.
Modify	Modyfikację i usunięcie pliku oraz wszystkie czynności, na które zezwalają uprawnienia Write i Read & Execute.
Full Control	Zmianę uprawnień, przejęcie pliku na własność oraz wszystkie czynności, na które zezwala dowolne inne uprawnienie.

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

◆ Zastosowanie uprawnień NTFS w systemie Windows 2000

Cel slajdu

Prezentacja zastosowania uprawnień NTFS w systemie Windows 2000.

Wprowadzenie

Ze stosowaniem uprawnień NTFS do plików i folderów związane są ściśle określone zasady.

- Wielokrotne uprawnienia NTFS
- Dziedziczenie uprawnień NTFS
- Kopiowanie i przenoszenie plików i folderów
- Dyskusja: Stosowanie uprawnień NTFS

Gdy użytkownikowi bądź grupie przypisywane jest uprawnienie NTFS do folderu, takie samo uprawnienie jest domyślnie definiowane dla wszystkich plików i folderów zawartych wewnątrz tego folderu. Poznanie zasad dziedziczenia uprawnień do folderu macierzystego przez pliki i foldery w nim zawarte, umożliwia wykorzystanie tej właściwości systemu NTFS do propagacji uprawnień do innych plików i folderów.

Jeśli uprawnienia NTFS do plików lub folderów są przypisywane jednocześnie użytkownikom i grupom, do których ci użytkownicy należą, wówczas jeden użytkownik może mieć przypisanych wiele różnych uprawnień NTFS do tych samych zasobów. W takiej sytuacji, o efektywnych uprawnieniach użytkownika do zasobu decydują ściśle określone reguły i priorytety. Na ostateczne uprawnienia NTFS do zasobów wpływają także operacje kopiowania i przenoszenia plików oraz folderów.

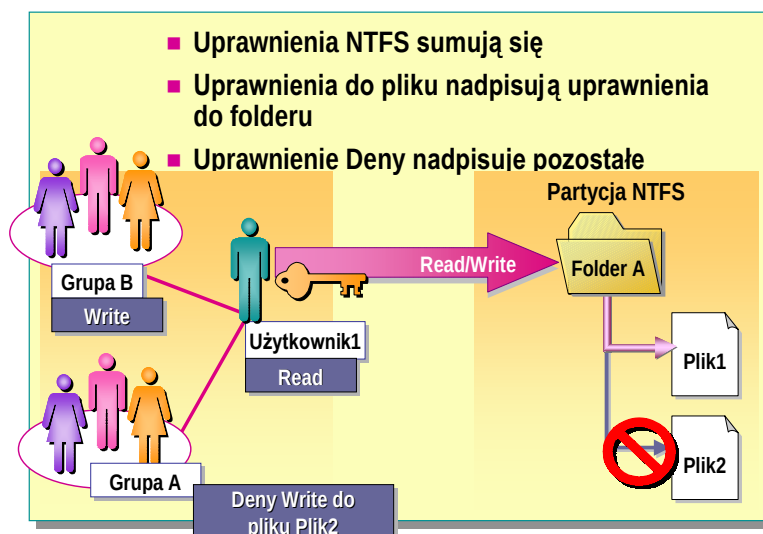
Wielokrotne uprawnienia NTFS

Cel slajdu

Prezentacja łączenia uprawnień NTFS.

Wprowadzenie

Bardzo ważne jest poznanie sposobu, w jaki powstaje wynikowe uprawnienie NTFS do zasobu.



Wskazówka

Zaprezentuj:

- sposób łączenia uprawnień NTFS
- priorytet uprawnień do plików nad uprawnieniami do folderu
- nadpisywanie innych uprawnień przez uprawnienie Deny.

Objasnij sytuację przedstawioną na slajdzie.

Jeśli uprawnienia NTFS do plików lub folderów są przypisywane jednocześnie użytkownikom i grupom, do których ci użytkownicy należą, wówczas jeden użytkownik ma przypisanych wiele różnych uprawnień NTFS do tych samych zasobów. Istnieją ściśle określone zasady, wiążące kombinacje uprawnień NTFS, pozwalające określić uprawnienie efektywne.

Uprawnienia kumulują się

Efektywne uprawnienie do zasobu jest kombinacją uprawnień przypisanych użytkownikowi, zarówno jawnie jak i poprzez przynależność do grup. Na przykład, jeśli użytkownik posiada uprawnienie Read do folderu i jest członkiem grupy, której przypisano uprawnienie Write do tego samego folderu, efektywne uprawnienie użytkownika powstanie przez połączenie uprawnień Read oraz Write.

Uprawnienia do pliku nadpisują uprawnienia do folderu

Uprawnienia NTFS do plików mają wyższy priorytet niż uprawnienia do folderów. Jeśli użytkownik ma uprawnienie Change do pliku, będzie mógł dokonać w nim zmian, mimo że do folderu, w którym znajduje się plik, przypisano mu tylko uprawnienie Read.

Wyjaśnij różnicę pomiędzy uprawnieniem Deny a brakiem uprawnień.

Uprawnienie Deny nadpisuje pozostałe uprawnienia

Można zabronić użytkownikowi lub grupie dostępu do wybranego pliku czy folderu poprzez przypisanie uprawnienia Deny. Mimo, iż użytkownik może mieć zdefiniowane inne uprawnienia, pozwalające mu na dostęp do zasobu, uprawnienie Deny zablokuje wszystkie inne uprawnienia. Uprawnienie Deny jest jedynym wyjątkiem od zasady kumulowania uprawnień. Należy jednak unikać stosowania w praktyce odmowy dostępu, ponieważ znacznie prostszym sposobem na zarządzanie danymi jest zezwalanie na dostęp do nich wybranym użytkownikom i grupom. Preferowane jest takie projektowanie grup oraz organizowanie drzewa folderów, aby możliwe było zarządzanie zasobami tylko poprzez zezwalanie na dostęp, bez konieczności wykorzystywania uprawnienia Deny.

Uwaga W systemie Windows 2000 istnieje różnica pomiędzy brakiem zdefiniowanego uprawnienia, a uprawnieniem Deny dodanym do listy ACL pliku lub folderu. Oznacza to, że administrator ma do wyboru nie przypisywać użytkownikowi uprawnienia do zasobu bądź zakazać do niego dostępu.

Dziedziczenie uprawnień NTFS

Cel slajdu

Prezentacja mechanizmu dziedziczenia uprawnień NTFS oraz sposobu jego blokowania.

Wprowadzenie

Uprawnienia NTFS są dziedziczone z folderu, w którym tworzone są pliki lub foldery.



Wskazówka

Pokaż, w jaki sposób uprawnienia NTFS są dziedziczone oraz jak można dziedziczenie zablokować.

Przypisz uprawnienie do przykładowego folderu i w ten sposób pokaż słuchaczom, jak uprawnienia są propagowane do plików i folderów. Następnie zaprezentuj, w jaki sposób można zablokować dziedziczenie uprawnień z folderu nadrzędnego.

Objasnij sytuację, którą ilustruje slajd.

Domyślnie, uprawnienia przypisane do folderu nadrzędnego są propagowane i dziedziczone przez zawarte w nim foldery i pliki. Jeśli jednak istnieje potrzeba przypisania do plików i folderów innych uprawnień, niż do folderu nadrzędnego, dziedziczenie można zablokować.

Dziedziczenie uprawnień

Przypisanie uprawnień do folderu nadrzędnego powoduje dziedziczenie uprawnień przez pliki i foldery w nim zawarte. Przypisanie przez użytkownika uprawnień NTFS do folderu jest równoważne z przypisaniem takich samych uprawnień do wszystkich już istniejących w nim, jak i nowo tworzonych, plików i folderów.

Blokowanie dziedziczenia uprawnień

Dziedziczenie uprawnień można zablokować, co powoduje wyłączenie przekazywania uprawnień z folderu nadrzędnego do plików i folderów w nim zawartych. Aby wyłączyć mechanizm dziedziczenia uprawnień, należy usunąć odziedziczone uprawnienia NTFS i pozostawić tylko te przypisane bezpośrednio na poziomie zasobu..

Folder, dla którego zablokowano dziedziczenie uprawnień stanie się tym samym nowym folderem nadrzędnym. Pliki i foldery w nim zawarte będą dziedziczyły uprawnienia do tego folderu macierzystego.

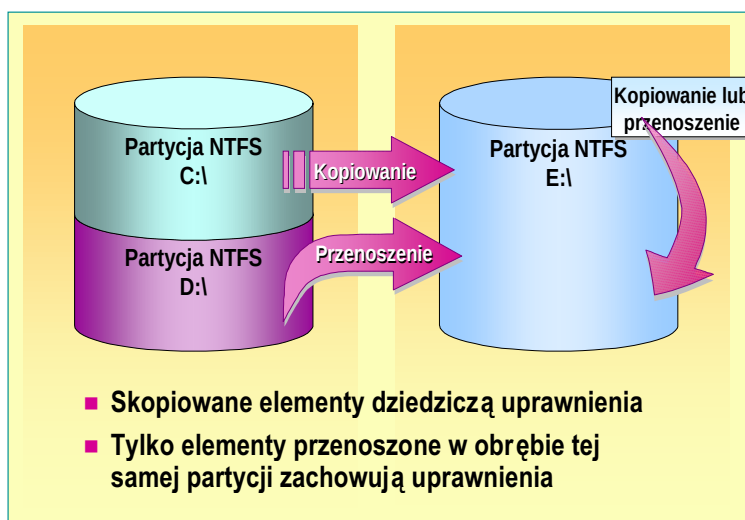
Kopiowanie i przenoszenie plików i folderów

Cel slajdu

Prezentacja wpływu operacji przenoszenia i kopiowania plików na uprawnienia NTFS.

Wprowadzenie

Kopiowanie i przenoszenie plików pomiędzy lub na partycjach NTFS może mieć wpływ na uprawnienia do tych zasobów.



Zagadnienie kluczowe

Kopiowanie pliku w systemie Windows 2000, w obrębie jednej lub pomiędzy partycjami NTFS, traktowanie jest jak tworzenie nowego pliku. W tej sytuacji nowy plik dziedziczy uprawnienia do folderu docelowego.

Aby użytkownik mógł skopiować plik lub folder, musi mieć uprawnienie Write do folderu docelowego.

Podczas kopiowania lub przenoszenia pliku albo folderu, uprawnienia NTFS mogą ulec zmianie, w zależności od tego, gdzie dany zasób został umieszczony. Ważne jest, aby móc przewidzieć zmiany uprawnień, jakie mogą powstać w czasie wykonywania tych operacji.

Kopiowanie plików i folderów

Podczas kopiowania pliku lub folderu do innego folderu lub na inną partycję dyskową, uprawnienia do nich mogą ulec zmianie. Kopiowanie pliku lub folderu może spowodować następujące efekty:

- Podczas kopiowania pliku lub folderu w obrębie tej samej partycji NTFS, jego kopia dziedziczy uprawnienia do folderu docelowego.
- Podczas kopiowania pliku lub folderu pomiędzy partycjami NTFS jego kopia dziedziczy uprawnienia do folderu docelowego.
- Podczas kopiowania pliku lub folderu na partycję inną niż NTFS (na przykład FAT) jego kopia traci wszelkie uprawnienia NTFS, ponieważ inne systemy plików nie przechowują informacji o uprawnieniach NTFS.

Aby skopiować 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.

Zagadnienie kluczowe

Aby użytkownik mógł przenieść plik lub folder, musi mieć uprawnienie Write do folderu docelowego i uprawnienie Modify do folderu źródłowego.

Przenoszenie plików i folderów

W czasie przenoszenia pliku lub folderu uprawnienia do niego mogą ulec zmianie, w zależności od uprawnień do folderu docelowego. Przenoszenie pliku lub folderu może spowodować następujące efekty:

- Gdy plik lub folder jest przenoszony w obrębie tej samej partycji NTFS, uprawnienia są zachowywane.
- Gdy plik jest przenoszony pomiędzy partycjami NTFS, następuje dziedziczenie uprawnień folderu docelowego. Tego typu operacja jest równoważna kopiowaniu pliku lub folderu do nowej lokalizacji, a następnie usunięciu oryginału z poprzedniego miejsca.
- Gdy plik lub folder jest przenoszony na partycję inną niż NTFS, wszelkie uprawnienia NTFS ulegają usunięciu, ponieważ inne systemy plików nie przechowują informacji o uprawnieniach NTFS.

Aby przenieść pliki lub foldery w obrębie jednej lub pomiędzy partycjami NTFS, użytkownik musi mieć uprawnienie Modify do folderu źródłowego i uprawnienie Write do folderu docelowego. Uprawnienie Modify jest niezbędne do wykonania tej operacji, ponieważ w systemie Windows 2000, w czasie przenoszenia pliku lub folderu, po skopiowaniu go do nowej lokalizacji jest on usuwany z lokalizacji źródłowej.

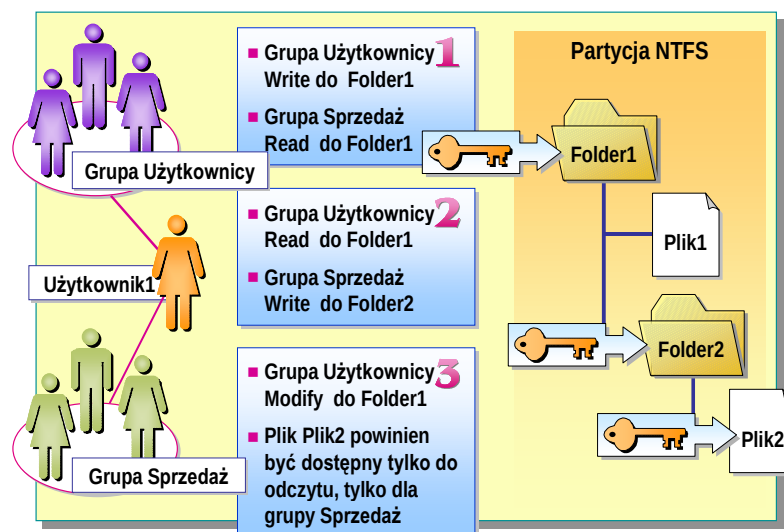
Dyskusja: Stosowanie uprawnień NTFS

Cel slajdu

Przypomnienie słuchaczom, w jaki sposób w systemie Windows 2000 stosowane są uprawnienia NTFS do plików i folderów.

Wprowadzenie

Przeanalizujemy kilka przykładów zastosowania uprawnień NTFS do plików i folderów.



Użytkownik1 jest członkiem grup Użytkownicy i Sprzedaż.

1. Grupa Użytkownicy ma uprawnienie Write, a grupa Sprzedaż uprawnienie Read do folderu Folder1. Jakie efektywne uprawnienie do folderu Folder1 ma Użytkownik1?

Użytkownik1 ma uprawnienia Write i Read do folderu Folder1, ponieważ jest członkiem grupy Użytkownicy, która ma uprawnienie Write i grupy Sprzedaż, która ma uprawnienie Read.

2. Grupa Użytkownicy ma uprawnienie Read do folderu Folder1. Grupa Sprzedaż ma uprawnienie Write do folderu Folder2. Jakie efektywne uprawnienie ma Użytkownik1 do pliku Plik2?

Użytkownik1 ma uprawnienia Read i Write do pliku Plik2 ponieważ jest członkiem grupy Użytkownicy, która ma uprawnienie Read do folderu Folder1 i grupy Sprzedaż, która ma uprawnienie Write do folderu Folder2. Plik Plik2 dziedziczy uprawnienia zarówno z folderu Folder2 jak i folderu Folder1.

3. Grupa Użytkownicy ma uprawnienie Modify do folderu Folder1. Plik Plik2 powinien być dostępny tylko do odczytu i tylko dla grupy Sprzedaż. Jakiego kroku należy przedsięwziąć, aby spowodować, że jedynym uprawnieniem do pliku Plik2 jest uprawnienie Read dla grupy Sprzedaż?

Należy wyłączyć dziedziczenie uprawnień dla folderu Folder2 lub pliku Plik2, usunąć uprawnienia dla folderu Folder2 lub pliku Plik2, które były dziedziczone z folderu Folder1. Ostatnim krokiem jest przypisanie grupie Sprzedaż uprawnienia Read do folderu Folder2 lub pliku Plik2.

◆ Wykorzystanie uprawnień NTFS

Cel slajdu

Przedstawienie zagadnień związanych z wykorzystaniem uprawnień NTFS.

Wprowadzenie

Dostępem do folderów i plików zarządzają ich właściciele i administratorzy.

- Przypisywanie uprawnień NTFS
- Konfiguracja dziedziczenia uprawnień
- Dobre przyzwyczajenia przy przypisywaniu uprawnień NTFS

Administratorzy, użytkownicy z uprawnieniem Full Control oraz właściciele mogą przypisywać uprawnienia do plików i folderów innym użytkownikom. Przy przypisywaniu uprawnień NTFS oraz zarządzaniu dziedziczeniem, należy korzystać z dobrych rad, pomocnych w efektywnym zarządzaniu dostępem do zasobów. Zawsze należy przypisywać uprawnienia dostosowane do potrzeb użytkowników i grup.

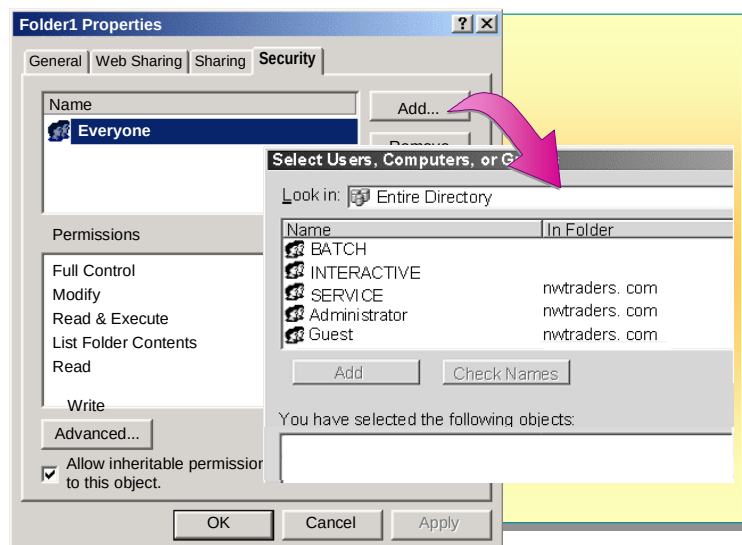
Przypisywanie uprawnień NTFS

Cel slajdu

Prezentacja sposobu przypisywania uprawnień NTFS.

Wprowadzenie

Domyślnie, w systemie Windows 2000, przy tworzeniu pliku, folderu lub formatowaniu partycji NTFS, grupie Everyone przypisywane jest uprawnienie Full Control.



Wskazówka

Zaprezentuj przypisywanie uprawnień NTFS do folderu, a następnie blokowanie dziedziczenia uprawnień przez pliki zawarte w tym folderze. Następnie przypisz nowe uprawnienia do pliku, dla którego zablokowano dziedziczenie uprawnień.

Uprawnienia NTFS przypisywane są w oknie dialogowym **Properties** odpowiedniego folderu lub pliku. Podczas przypisywania, bądź zmiany uprawnień NTFS, można także usunąć lub dodać nowych użytkowników, grupy czy komputery do listy uprawnionych do pliku lub folderu. Wskazując użytkownika lub grupę można również zmienić przypisane im uprawnienia..

Na karcie **Security**, w oknie dialogowym **Properties** pliku lub folderu można konfigurować opcje opisane w poniższej tabeli.

Opcja	Opis
Name	Wskazanie konta użytkownika lub grupy, dla których należy zmienić uprawnienia bądź usunąć konto z listy.
Permissions	Zezwolenie na uprawnienie, po zaznaczeniu opcji Allow . Zablokowanie uprawnienia, po zaznaczeniu opcji Deny .
Add	Otwarcie okna Select User, Groups, or Computers , w którym należy wybrać konta użytkowników lub grup, które zostaną dodane do listy Name .
Remove	Usunięcie wybranego konta użytkownika lub grupy, wraz z przypisanymi uprawnieniami do pliku lub folderu.

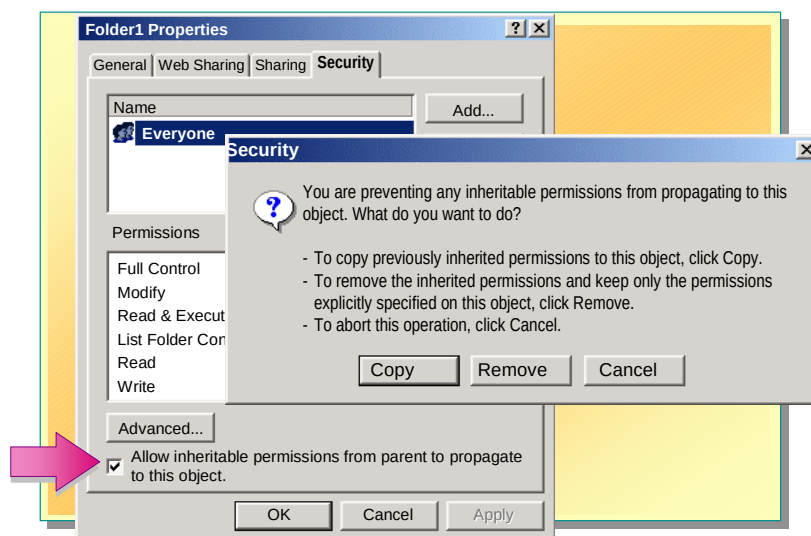
Konfiguracja dziedziczenia uprawnień

Cel slajdu

Prezentacja sposobu kontroli dziedziczenia uprawnień.

Wprowadzenie

Domyślnie, uprawnienia do folderu są dziedziczone przez wszystkie pliki i foldery w nim zawarte.



W większości przypadków, w systemie Windows 2000 należy zezwolić na propagowanie uprawnień do folderu nadrzędnego do folderów i plików w nim zawartych. Dziedziczenie upraszcza przypisywanie uprawnień do zasobów.

W niektórych przypadkach, może być konieczne zablokowanie dziedziczenia uprawnień. Na przykład, może istnieć potrzeba umieszczenia wszystkich plików działu sprzedaży w jednym folderze, do którego każdy z pracowników tego działu będzie miał uprawnienie Write. Jednak kilka dokumentów zawartych w folderze nie powinno być zmienianych, co oznacza, że użytkownicy powinni mieć do nich tylko uprawnienie Read. Należy zablokować propagację uprawnień dla tych dokumentów tak, aby uprawnienie Write nie było dziedziczone.

Gdy zaznaczona jest pole opcji **Allow inheritable permissions from parent to propagate to this object**, jak jest to widoczne na karcie **Security** okna **Properties**, foldery i pliki dziedziczą uprawnienia do folderu nadrzędnego.

Aby zapobiec dziedziczeniu przez pliki i foldery uprawnień do folderu nadrzędnego, należy wyczyścić pole opcji **Allow inheritable permissions from parent to propagate to this object**, a następnie wybrać jedną z dwóch możliwości, opisanych w poniższej tabeli.

Opcja	Opis
Copy	Powoduje skopiowanie, dotychczas dziedziczonych, uprawnień do folderu nadrzędnego do pliku lub folderu, a następnie blokuje dziedziczenie uprawnień.
Remove	Powoduje usunięcie z plików lub folderów odziedziczonych uprawnień do folderu nadrzędnego i pozostawienie tylko uprawnień przypisanych bezpośrednio do pliku lub folderu.

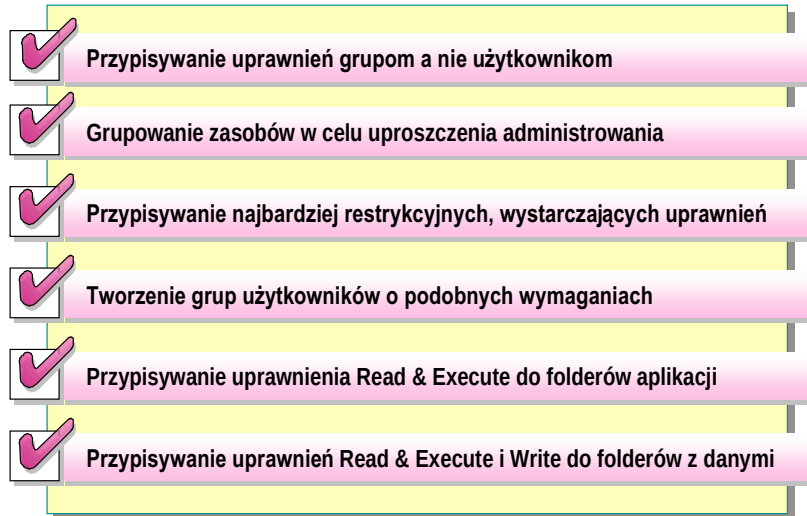
Dobre rady przy przypisywaniu uprawnień NTFS

Cel slajdu

Zapoznanie z dobrymi przyzwyczajeniami przy przypisywaniu uprawnień NTFS.

Wprowadzenie

Przy przypisywaniu uprawnień NTFS warto wziąć pod uwagę następujące wskazówki.



Przy przypisywaniu uprawnień NTFS, warto wziąć pod uwagę następujące dobre rady:

- Należy przypisywać uprawnienia grupom, a nie użytkownikom. Łatwiej jest zarządzać grupami, niż indywidualnymi użytkownikami. Takie postępowanie powoduje skrócenie listy ACL, co zwiększa wydajność systemu.
- Dla uproszczenia administrowania należy tworzyć oddzielne foldery do przechowywania plików aplikacji, danych udostępnianych wielu użytkownikom oraz foldery domowe, aby użytkownicy mogli przechowywać w nich pliki osobiste. Foldery domowe oraz foldery z danymi warto umieścić w jednym miejscu, na osobnych partycjach.
- Przypisać użytkownikom najbardziej restrykcyjne, wymagane przez nich uprawnienia. Jeśli użytkownik musi jedynie odczytać zawartość pliku, należy przypisać mu, bądź grupie, do której należy, tylko uprawnienie Read.
- Tworzyć grupy na podstawie wymogów dostępu do zasobów, a następnie grupom tym przypisywać odpowiednie uprawnienia.
- Przypisać grupom Users i Administrators uprawnienie Read & Execute do folderu z aplikacjami. Zapewni to ochronę danych i plików aplikacji przed przypadkowym skasowaniem lub uszkodzeniem przez użytkowników i wirusy.
- Przypisać grupie Users uprawnienie Read & Execute oraz Write i grupie Owner uprawnienie Full Control do folderu z danymi. Pozwoli to użytkownikom na odczyt i zmiany w dokumentach stworzonych przez innych użytkowników oraz odczyt, zmiany i usuwanie plików, które sami utworzyli.

Uwaga Z uprawnienia Deny należy korzystać tylko wtedy, gdy ważne jest zakazanie użytkownikowi lub grupie dostępu do zasobu.

◆ Wykorzystanie specjalnych uprawnień NTFS

Cel slajdu

Prezentacja zagadnień związanych z przypisywaniem specjalnych uprawnień NTFS.

Wprowadzenie

Standardowe uprawnienia NTFS umożliwiają, w większości przypadków, pełną kontrolę dostępu do zasobów, jednak w celu spełnienia szczególnych wymagań, należy wykorzystać specjalne uprawnienia NTFS.

- Wprowadzenie do specjalnych uprawnień NTFS
- Przypisywanie specjalnych uprawnień NTFS

Zwykle, standardowe uprawnienia NTFS wystarczają do zapewnienia wymaganego poziomu kontroli dostępu do zasobów. Mogą jednak zdarzyć się sytuacje, w których nie będzie można określić specyficznego poziomu dostępu do zasobów, jakiego wymagają użytkownicy. W takim przypadku należy wykorzystać specjalne uprawnienia NTFS.

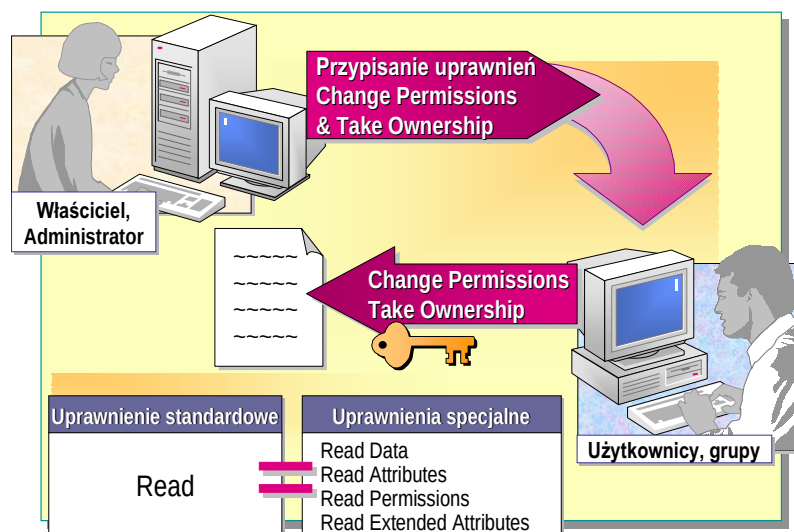
Wprowadzenie do specjalnych uprawnień NTFS

Cel slajdu

Prezentacja specjalnych uprawnień NTFS.

Wprowadzenie

Specjalne uprawnienia NTFS zapewniają większą swobodę kontroli poziomu dostępu przy przypisywaniu uprawnień dostępu do zasobów.



Specjalne uprawnienia NTFS zapewniają większą swobodę określania poziomu kontroli przy przypisywaniu uprawnień do zasobów. Kombinacjami 13 specjalnych uprawnień są także uprawnienia standardowe NTFS. 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 dla pliku lub folderu.
- *Take Ownership*. Uprawnienie to daje użytkownikowi możliwość stania się właścicielem pliku lub folderu.

Uprawnienie Change Permissions

Istnieje możliwość zezwolenia innemu administratorowi lub użytkownikowi na przypisywanie lub zmianę uprawnień dla pliku lub folderu, bez przypisywania uprawnienia Full Control. Dzięki temu, użytkownik ten nie będzie miał możliwości zapisu, ani usunięcia pliku lub folderu, ale będzie mógł przypisywać do nich uprawnienia.

Aby zezwolić administratorom na zmianę uprawnień, należy przypisać grupie Administrators uprawnienie Change Permissions do pliku lub folderu.

Uprawnienie Take Ownership

Można pozwolić innemu użytkownikowi lub grupie użytkowników przejąć plik lub folder na własność. Administrator ma prawo stać się właścicielem dowolnego zasobu.

Przy przejmowaniu na własność pliku lub folderu stosowane są następujące zasady:

- Właściciel lub użytkownik z uprawnieniem Full Control może przypisać innemu użytkownikowi lub grupie użytkowników standardowe uprawnienie Full Control lub uprawnienie specjalne Take Ownership. Pozwoli to użytkownikowi lub członkowi grupy na przejęcie pliku na własność.
- Członek 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 grupa Administrators, a dowolny członek tej grupy ma możliwość zmiany uprawnień do tego zasobu, łącznie z przypisaniem dowolnemu użytkownikowi uprawnienia Take Ownership.

Na przykład, administrator może przejąć na własność pliki pracownika opuszczającego firmę, a następnie zezwolić na ich przejęcie przez innego pracownika, przejmującego obowiązki odchodzącego, przypisując mu uprawnienie Take Ownership.

Uwaga Aby stać się właścicielem pliku lub folderu, użytkownik lub członek grupy z uprawnieniem Take Ownership musi z tego uprawnienia jawnie skorzystać. Nie można zdecydować, że inny użytkownik staje się właścicielem pliku lub folderu. Właściciel pliku, członek grupy Administrators lub ktokolwiek z uprawnieniem Full Control może przypisać uprawnienie Take Ownership innemu użytkownikowi, aby ten mógł jawnie przejąć plik na własność.

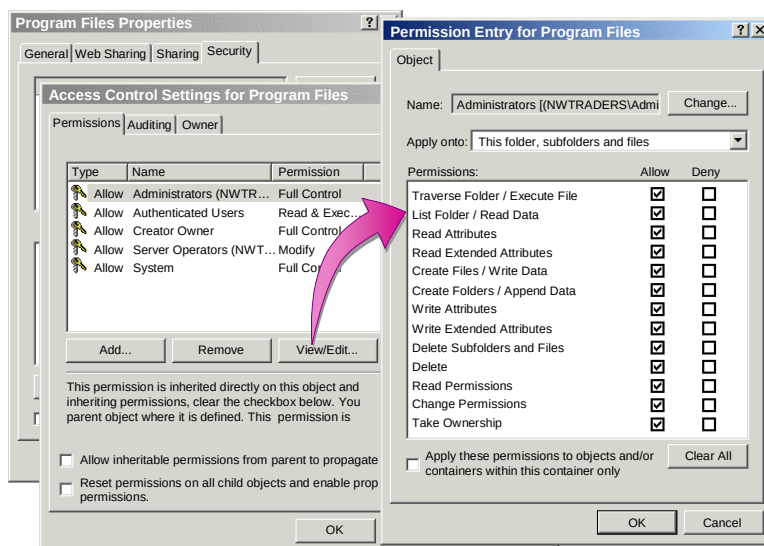
Przypisywanie specjalnych uprawnień NTFS

Cel slajdu

Przedstawienie interfejsu do przypisywania uprawnień NTFS.

Wprowadzenie

W celu zmiany uprawnień do plików i folderów lub przypisania uprawnienia do przejęcia tych obiektów na własność, można wykorzystać specjalne uprawnienia NTFS.



Aby przypisać użytkownikowi lub grupie specjalne uprawnienia NTFS należy:

1. W oknie dialogowym **Properties** pliku lub folderu, na karcie **Security** wybrać przycisk **Advanced**.
2. W oknie dialogowym **Access Control Settings**, na karcie **Permissions** wskazać użytkownika lub grupę, dla której ma nastąpić zmiana uprawnień specjalnych NTFS i wybrać przycisk **View/Edit**.
3. W oknie dialogowym **Permissions Entry** skonfigurować opcje opisane w poniższej tabeli.

Opcja	Opis
Name	Wskazuje użytkownika lub grupę. Aby wskazać innego użytkownika lub grupę, należy wybrać przycisk Change .
Apply onto	Wskazuje hierarchię folderów w drzewie katalogów, które będą dziedziczyły specjalne uprawnienia NTFS. Domyślnym ustawieniem jest opcja This folder, subfolders and files .
Permissions	Wyświetla specjalne uprawnienia NTFS. Aby przypisać uprawnienia Change Permissions lub Take Ownership , należy zaznaczyć pole opcji Allow przy odpowiednim uprawnieniu.
Apply these permissions to objects and/or containers within this container only	Określa, czy foldery i pliki zawarte w folderze będą dziedziczyły przypisane specjalne uprawnienia NTFS. Zaznaczenie tego pola opcji spowoduje propagację uprawnień. Usunięcie zaznaczenia zablokuje dziedziczenie.
Clear All	Wybranie tego przycisku powoduje usunięcie wszystkich przypisanych uprawnień.

Laboratorium A: Wykorzystanie uprawnień NTFS

Cel slajdu

Wprowadzenie do laboratorium.

Wprowadzenie

W tym laboratorium, uprawnienia NTFS zostaną wykorzystane do kontroli dostępu do plików i folderów.



Wyjaśnij cele laboratorium.

Cele laboratorium

Po zrealizowaniu tego laboratorium słuchacz będzie potrafił:

- Przypisywać uprawnienia NTFS do plików i folderów użytkownikom i grupom.
- Sprawdzić uprawnienia NTFS do plików i folderów.
- Wyjaśnić, co stanie się z uprawnieniami NTFS przy kopiowaniu oraz przenoszeniu plików i folderów na partycje NTFS i sformatowane w innych systemach plików.

Wymagania wstępne

Przed rozpoczęciem tego laboratorium należy:

- Zdobyć wiedzę na temat kont użytkowników i grup w systemie Windows 2000.
- Zdobyć wiedzę na temat różnic pomiędzy grupą roboczą a domeną.

Przygotowanie laboratorium

Do wykonania tego laboratorium niezbędny jest komputer pracujący w systemie Windows 2000 Advanced Server, skonfigurowany jako serwer członkowski w domenie nwtraders.msft.

Przewidywany czas ukończenia laboratorium: 30 minut

Ćwiczenie 1

Przypisywanie uprawnień NTFS

Scenariusz

Zasady bezpieczeństwa przedsiębiorstwa wymagają usunięcia domyślnych uprawnień NTFS do zasobów plikowych i przypisania uprawnień zgodnych z wymaganiami użytkowników i grup użytkowników w firmie. Przygotowujesz serwer do przechowywania plików i folderów, do których użytkownicy będą musieli mieć dostęp poprzez sieć. Utworzyłeś strukturę folderów, a teraz przypiszesz odpowiednie uprawnienia. W folderze z danymi użytkownicy będą zapisywali efekty swojej pracy. Użytkownicy powinni mieć możliwość zapisywania i modyfikacji swoich własnych dokumentów, ale nie powinni modyfikować plików innych osób. Chcesz także być pewien, że tylko autoryzowani użytkownicy będą mieli dostęp do folderów.

Cel

W tym ćwiczeniu usuniesz domyślne uprawnienia NTFS do folderu Data i przypiszesz uprawnienia wymagane w ćwiczeniu. Następnie przetestujesz przypisane uprawnienia.

Zadania	Szczegółowe kroki
1. Zaloguj się do domeny nwtraders jako Adminx (gdzie x jest numerem Twojego stanowiska) z hasłem domain i usuń domyślne uprawnienia do folderu Data, blokując dziedziczenie uprawnień.	a. Zaloguj się wykorzystując następujące informacje: Username: Adminx (gdzie x jest numerem Twojego stanowiska) Password: domain Log on to: nwtraders b. Korzystając z programu Windows Explorer, przejdź do folderu C:\MOC\Win2152b\Labfiles\Lab06 i otwórz okno dialogowe Properties folderu Data. c. W oknie dialogowym Data Properties , na karcie Security przyjrzyj się uprawnieniom do folderu Data.
? Jakie są uprawnienia do folderu Data? Dlaczego pola opcji są szare? Grupa Everyone ma uprawnienie Full Control. Pola opcji są szare, ponieważ uprawnienia te są dziedziczone z folderu nadrzędnego.	
1. (ciąg dalszy)	d. Na liście Name wskaż grupę Everyone , a następnie wybierz przycisk Remove .  Zostanie wyświetlona informacja wskazująca, że nie można usunąć grupy Everyone, ponieważ uprawnienia są dziedziczone z folderu nadrzędnego. e. Wybierz przycisk OK , aby zamknąć okno komunikatu. f. Wyczyść pole opcji Allow inheritable permissions from parent to propagate to this object , aby zablokować dziedziczenie uprawnień.  Zostanie wyświetlony komunikat o możliwości skopiowania uprawnień aktualnie dziedziczonych lub usunięcia wszystkich uprawnień do tego folderu, z wyjątkiem jawnie przypisanych.

Zadania	Szczegółowe kroki
1. <i>(ciąg dalszy)</i>	g. W oknie dialogowym Security wybierz przycisk Remove .
2. Przypisz uprawnienia do folderu Data grupie Users.	a. W oknie dialogowym Data Properties wybierz przycisk Add . b. W oknie dialogowym Select Users, Computers, or Groups upewnij się, że w polu Look in widnieje nazwa domeny nwtraders.msft . c. Na liście Name wskaż grupę Domain Users , następnie wybierz kolejno przyciski Add i OK .
? Jakie są aktualne uprawnienia do folderu? Grupa Domain Users ma uprawnienia Read & Execute, List Folder Contents i Read. Są to domyślne uprawnienia, przypisywane w systemie Windows 2000 podczas dodawania nowej grupy lub użytkownika do listy uprawnionych do zasobu.	
2. <i>(ciąg dalszy)</i>	d. W oknie dialogowym Data Properties upewnij się, że wybrana jest grupa Domain Users i przypisz jej uprawnienie Write.
? W jaki sposób zapewnisz użytkownikom możliwość modyfikacji jedynie tych plików, które sami utworzyli? Należy przypisać uprawnienie Full Control grupie Creator Owner. W ten sposób do dowolnego, utworzonego przez siebie pliku użytkownik będzie miał uprawnienie Full Control.	
3. Przypisz grupie Creator Owner uprawnienie Full Control do folderu Data.	a. W oknie dialogowym Data Properties wybierz przycisk Add . b. W oknie dialogowym Select Users, Groups, or Computers upewnij się, że w polu Look in widnieje nazwa domeny nwtraders.msft . c. Na liście Name wskaż grupę Creator Owner , następnie wybierz przycisk Add , a później przycisk OK . d. W oknie Data Properties upewnij się, że wybrana jest grupa Creator Owner i przypisz jej uprawnienie Full Control.
4. Przypisz lokalnej grupie Administrators uprawnienie Full Control do folderu Data i utwórz plik Admin.txt.	a. W oknie dialogowym Data Properties wybierz przycisk Add . b. W oknie Select Users, Groups, or Computers wybierz z listy Look in nazwę Server (gdzie Server jest nazwą Twojego komputera). c. Na liście Name wskaż grupę Administrators , następnie przycisk Add , a później przycisk OK . d. W oknie Data Properties upewnij się, że wybrana jest grupa Administrators i przypisz jej uprawnienie Full Control. e. Wybierz przycisk OK , aby zamknąć okno dialogowe Data Properties .

Zadania	Szczegółowe kroki
4. <i>(ciąg dalszy)</i>	f. W folderze C:\MOC\Win2152b\Labfiles\Lab06\Data utwórz plik tekstowy Admin.txt. Będzie on wykorzystywany do testowania uprawnień. g. Zamknij wszystkie otwarte okna i wyloguj się.
5. Zaloguj się do domeny nwtraders jako Studentx (gdzie x jest numerem Twojego stanowiska) z hasłem domain i sprawdź uprawnienia przypisane do folderu Data.	a. Zaloguj się, wykorzystując następujące informacje: Username: Studentx (gdzie x jest numerem Twojego stanowiska) Password: domain Log on from: nwtraders b. Korzystając z programu Windows Eksplorator przejdź do folderu C:\MOC\Win2152b\Labfiles\Lab06\Data. c. W folderze Data spróbuj utworzyć plik tekstowy Student.txt.
? Czy udało Ci utworzyć plik? Dlaczego tak lub nie? Udało się, ponieważ grupa Users ma przypisane do folderu Data uprawnienie Write.	
5. <i>(ciąg dalszy)</i>	d. Spróbuj wykonać na utworzonym pliku następujące operacje, notując, które udało się przeprowadzić. • Otwórz plik • Zmień zawartość pliku • Zapisz plik • Usuń plik
? Czy operacje udało się przeprowadzić? Tak. Wszystkie zadania można było wykonać, ponieważ grupie Creator Owner przypisano do folderu Data uprawnienie NTFS Full Control.	
5. <i>(ciąg dalszy)</i>	e. Spróbuj wykonać na pliku Admin.txt następujące operacje, notując, które udało się przeprowadzić. • Otwórz plik • Zmień zawartość pliku • Zapisz plik • Usuń plik

(ciąg dalszy)

Zadania	Szczegółowe kroki
? Czy operacje udało się przeprowadzić ? Częściowo. Operacje zakończone sukcesem to otwarcie, modyfikacja i zapisanie pliku, ale nie udało się usunąć pliku. Przyczyną jest to, że użytkownik był zalogowany jako członek grupy Domain Users, która jest członkiem grupy Users. Grupie Users przypisano do folderu Data uprawnienia Read & Execute, List Folder Contents, Read oraz Write. Pliki tworzone w folderze Data dziedziczą uprawnienia przypisane do folderu nadrzędnego. Dlatego Studentx może tylko odczytywać i modyfikować plik utworzony przez administratora.	
5. (ciąg dalszy)	f. Zamknij wszystkie otwarte okna i wyloguj się.

◆ Kompresja danych na partycjach NTFS

Cel slajdu

Prezentacja zagadnień związanych z zarządzaniem kompresją danych na partycjach NTFS.

Wprowadzenie

Kompresja danych ma na celu zmniejszenie ilości miejsca na dysku, zajętego przez pliki i foldery.

- Wprowadzenie do kompresji plików i folderów
- Kompresowanie plików i folderów
- Kopiowanie i przenoszenie skompresowanych plików i folderów
- Dobre rady przy kompresowaniu danych

Kompresja danych w systemie plików NTFS pozwala na oszczędzenie miejsca zajmowanego przez pliki i foldery. Skompresowane dane zajmują mniej miejsca na dysku, pozwalając tym samym na przechowywanie większej ich ilości. Stan plików i folderów, skompresowany lub nie, można zmieniać ustawiając odpowiednio atrybut kompresji. Przy kopiowaniu i przenoszeniu pliki i foldery mogą zachowywać ustawienia, jak i dziedziczyć atrybut kompresji folderu docelowego. W trakcie zarządzania kompresją danych, warto korzystać z dobrych rad dotyczących kompresji.

Wprowadzenie do kompresji plików i folderów

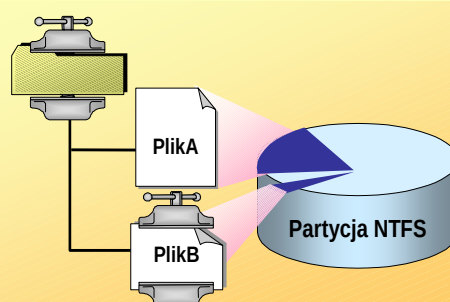
Cel slajdu

Prezentacja koncepcji kompresji plików i folderów.

Wprowadzenie

Skompresowane pliki i foldery zajmują mniej miejsca na partycjach NTFS.

- Przydział miejsca na dysku
- Wyróżnianie elementów skompresowanych
- Dostęp aplikacji do plików skompresowanych



Zagadnienie kluczowe

W czasie kopiowania i przenoszenia skompresowanych plików i folderów, ilość miejsca, zajmowanego przez nie na partycjach NTFS, jest obliczana na podstawie ich rzeczywistego rozmiaru.

Każdy plik i folder, umieszczony na partycji NTFS, ma określony stan atrybutu kompresji; *compressed* lub *uncompressed*. Atrybut kompresji określony dla folderu nie musi być taki sam, jak dla plików i folderów w nim zawartych. Na przykład, folder może być skompresowany, ale wszystkie pliki w nim zawarte mogą nie być skompresowane. Należy także zauważyć, że nie skompresowany folder może zawierać skompresowane pliki.

Podczas korzystania z kompresji plików i folderów warto rozważyć poniższe kwestie:

■ Przydział miejsca na dysku

Na partycjach NTFS, miejsce na dysku przydzielane jest na podstawie rzeczywistej wielkości pliku. Podczas kopiowania skompresowanego pliku na partycję, na której nie ma odpowiedniej ilości miejsca do zapisu pliku nie skompresowanego, wyświetlony zostanie komunikat o błędzie, informujący, że na dysku nie ma wystarczającej ilości miejsca do skopiowania pliku.

■ Wyróżnianie elementów skompresowanych

Użytkownik może zmienić kolor, w jakim wyświetlane są nazwy skompresowanych plików i folderów, aby łatwiej odróżnić je od pozostałych.

■ Dostęp aplikacji do skompresowanych plików

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

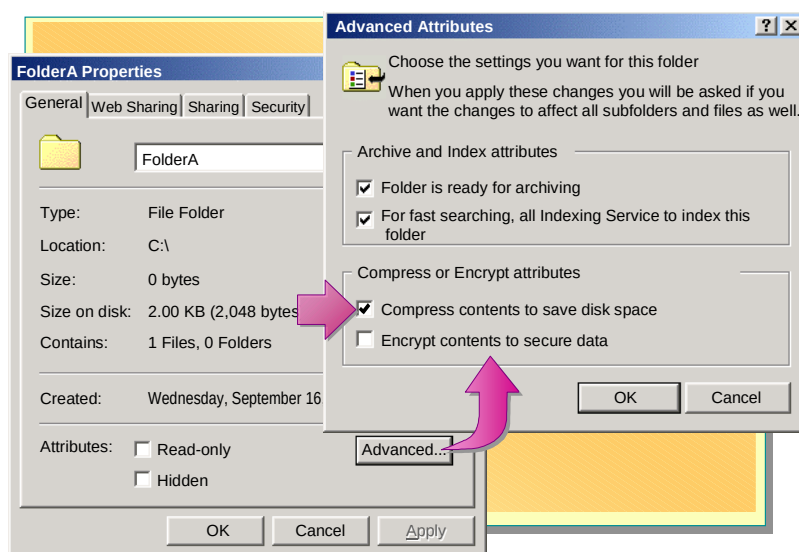
Kompresowanie plików i folderów

Cel slajdu

Przedstawienie sposobu kompresowania plików i folderów.

Wprowadzenie

Stan kompresji plików i folderów oraz kolor wyświetlania nazw obiektów skompresowanych można określić wykorzystując program Windows Explorer.



Wskazówka

Pokaż słuchaczom, w jaki sposób można przypisać folderowi atrybut kompresji.

Zaprezentuj, w jaki sposób można zmienić kolor wyświetlania nazw skompresowanych plików i folderów.

Stan kompresji plików i folderów oraz kolor wyświetlania nazw obiektów skompresowanych można określić wykorzystując program Windows Explorer.

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

Przypisywanie atrybutu kompresji

Aby ustawić atrybut kompresji folderu lub pliku, należy w oknie dialogowym **Advanced attributes** zaznaczyć pole opcji **Compress contents to save disk space**.

Po włączeniu kompresji folderu zostanie wyświetlone okno dialogowe **Confirm Attribute Changes**, w którym można 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 zostaną w nim utworzone.
Apply changes to this folder, subfolders and files	Powoduje skompresowanie wybranego folderu oraz wszystkich plików i folderów w nim zawartych (istniejących i nowo tworzonych)

Zmiana koloru wyświetlania

Do wyświetlania nazw skompresowanych plików i folderów można wybrać inny kolor. W oknie programu Windows Explorer, z menu **Tools** należy wybrać polecenie **Folder Options**. Następnie, na karcie **View**, wybrać opcję **Display compressed files and folders with alternate color**.

Kopiowanie i przenoszenie skompresowanych plików i folderów

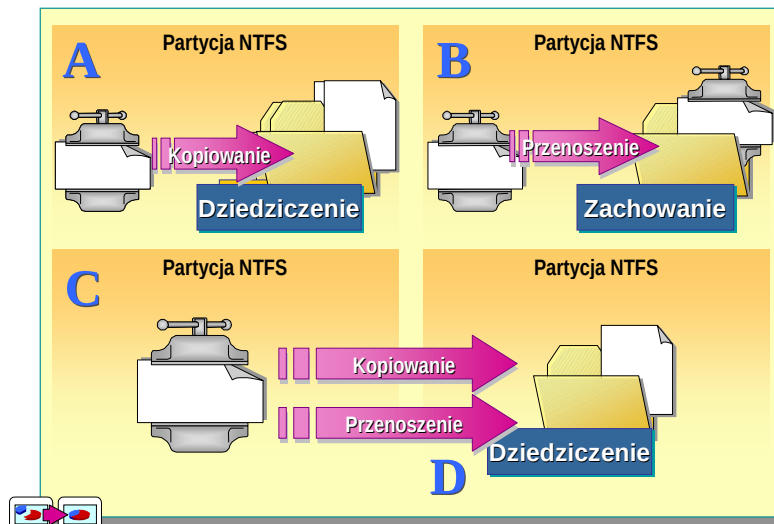
Cel slajdu

Prezentacja zasad przypisywania atrybutu kompresji plikom kopiowanym, bądź przenoszonym, na partycjach NTFS.

Wprowadzenie

Kilka reguł pozwala określić, czy stan kompresji plików i folderów zostanie zachowany podczas kopiowania lub przenoszenia zasobów plikowych w obrębie i pomiędzy partycjami NTFS oraz innych systemów plików.

plików.



Wskazówka

Slajd przygotowany dla tego zagadnienia jest animowany. Rozpocznij od wyjaśnienia, w jaki sposób pliki dziedziczą atrybut kompresji folderu docelowego.

Zagadnienie kluczowe

Przeniesienie pliku lub folderu z jednej partycji NTFS na inną jest równoważne ze skopiowaniem, a następnie usunięciem obiektu źródłowego.

Kompresja NTFS nie jest dostępna na partycjach innych niż NTFS. Pliki kopiowane lub przenoszone na partycje sformatowane w innych systemach plików, są przez system Windows 2000 automatycznie dekompresowane.

Poniżej opisano sposób, w jaki, w systemie Windows 2000, zmienia się atrybut kompresji pliku lub folderu podczas kopiowania lub przenoszenia obiektów pomiędzy i na partycji NTFS oraz w innym systemie plików:

- Gdy folder lub plik jest kopiowany w obrębie partycji NTFS, dziedziczy atrybut kompresji folderu docelowego, jak pokazano w części A slajdu. Na przykład, przy kopiowaniu skompresowanego pliku do nie skompresowanego folderu, plik zostanie automatycznie zdekompresowany.
- Gdy folder bądź plik jest przenoszony w obrębie partycji NTFS, zachowuje swój atrybut kompresji, jak pokazano w części B slajdu. Na przykład, po przeniesieniu skompresowanego pliku do nie skompresowanego folderu, plik pozostanie skompresowany.
- Gdy folder lub plik jest kopiowany pomiędzy partycjami NTFS, dziedziczy atrybut kompresji folderu docelowego, tak, jak zostało to pokazane w części C slajdu.
- Gdy folder lub plik jest przenoszony pomiędzy partycjami NTFS, dziedziczy atrybut kompresji folderu docelowego, jak pokazano w części D slajdu. W systemie Windows 2000, przeniesienie pliku pomiędzy partycjami jest równoważne ze skopiowaniem, a następnie usunięciem go z folderu źródłowego.

Ważne W systemie Windows 2000 kompresja jest możliwa tylko na partycjach NTFS. Gdy plik lub folder jest przenoszony lub kopiowany na inną partycję, następuje automatyczna dekompresja pliku lub folderu w miejscu docelowym.

Uwaga Operacja kopiowania pliku skompresowanego w Windows 2000 jest trójstopniowa: najpierw plik jest zdekompresowany, następnie kopiowany, a na końcu kompresowany ponownie. Może to zmniejszyć wydajność systemu.

Dobre rady przy kompresowaniu danych

Cel slajdu

Prezentacja dobrych przyzwyczajeń przy zarządzaniu kompresją NTFS.

Wprowadzenie

Przed rozpoczęciem korzystania z kompresji, warto zapoznać się z prezentowaną listą.



Określenie typu kompresowanych plików



Nie kompresowanie plików już skompresowanych



Wykorzystanie innego koloru do prezentacji skompresowanych plików i folderów



Kompresowanie danych rzadko zmieniających się

Warto rozważyć przedstawione poniżej wskazówki, dotyczące zarządzania kompresją plików na partycjach NTFS:

- Niektóre pliki można skompresować bardziej niż inne, dlatego typy plików do kompresji należy starannie wybierać, biorąc pod uwagę oczekiwany efekt. Na przykład, mapy bitowe Windows zawierają więcej danych nadmiarowych niż wykonywalne pliki aplikacji, dlatego ten typ plików jest lepiej kompresowany. Wielkość pliku mapy bitowej po kompresji często jest mniejsza niż 50 procent oryginalnego rozmiaru, podczas gdy wielkość programu dochodzi do 75 procent wielkości pierwotnej.
- Nie należy kompresować plików już skompresowanych. W systemie Windows 2000 zostanie podjęta próba jeszcze większej kompresji, co spowoduje stratę czasu, a nie spowoduje zwolnienia dodatkowego miejsca na dysku.
- Aby łatwiej odnaleźć skompresowane dane, warto wykorzystać inny kolor do wyświetlania nazw takich plików i folderów.
- Nie należy kompresować danych często używanych, a raczej dane archiwalne. Częsta kompresja i dekompresja plików powoduje obniżenie wydajności systemu. Wybór do kompresji plików rzadko używanych zmniejsza czas tracony przez system na kompresję i dekompresję danych.

◆ Konfiguracja przydziałów dyskowych na partycjach NTFS

Cel slajdu

Prezentacja zagadnień związanych z konfiguracją przydziałów dyskowych na partycjach NTFS.

Wprowadzenie

Przydziały dyskowe wykorzystywane są do zarządzania rosnącymi wymaganiami składowania danych.

- Wykorzystanie przydziałów dyskowych
- Konfigurowanie przydziałów dyskowych

Przydziały dyskowe wykorzystywane są do zarządzania miejscem do magazynowania danych w środowiskach rozproszonych. Pozwala to na przydzielenie poszczególnym użytkownikom miejsca na dysku, stosownie do posiadanych przez nich plików i folderów. Przydziały dyskowe umożliwiają także kontrolę przestrzeni dyskowej, wykorzystywanej przez użytkowników do składowania swoich danych. Zrozumienie istoty funkcjonowania przydziałów dyskowych pozwoli na efektywne wykorzystanie tej możliwości systemu w swojej sieci.

Wykorzystanie przydziałów dyskowych

Cel slajdu

Identyfikacja typów przydziałów dyskowych.

Wprowadzenie

Przydziały dyskowe pozwalają na kontrolę ilości miejsca zajętego na dyskach. Można określić próg ostrzegawczy, którego przekroczenie spowoduje wpis do dziennika zdarzeń, jeśli użytkownicy będą zbliżali się do wyznaczonych limitów przestrzeni dyskowej.

- **Przeliczenia zasobów, oparte się na własności plików i folderów**
- **Ignorowanie kompresji przy przeliczaniu zasobów**
- **Wolne miejsce dla aplikacji, oparte na limicie przydziału dyskowego**
- **Śledzenie przydziałów dyskowych niezależnie dla każdej partycji NTFS**

W systemie Windows 2000, przydziały dyskowe pozwalają na kontrolowanie ilości miejsca na dysku dla każdego użytkownika i partycji dyskowej. Wielkość zajętego obszaru dysku można kontrolować niezależnie od tego, w którym z folderów znajdują się pliki użytkownika. Poniżej opisano charakterystyczne cechy przydziałów dyskowych w systemie Windows 2000:

- Wykorzystanie przestrzeni dyskowej oparte jest na prawie własności do plików i folderów. Gdy użytkownik kopiuje lub zapisuje nowy plik na partycji NTFS lub przejmuje plik na własność, miejsce, które ten plik zajmuje obciąża przydział dyskowy użytkownika.
- Przydział dyskowy nie uwzględnia kompresji plików. Limit użytkownika jest obciążany wielkością plików nieskompresowanych, niezależnie od tego, ile miejsca pliki zajmują faktycznie na dysku. Jedną z przyczyn jest różny współczynnik kompresji dla plików zawierających różne typy danych.
- Ilość wolnego miejsca, dostępna dla aplikacji, bazuje na limicie przydziału dyskowego. Gdy przydziały dyskowe zostaną włączone, aplikacja potrafi wykryć i wykorzystać tyle miejsca na dysku, ile użytkownikowi pozostaje do osiągnięcia limitu.
- W systemie Windows 2000, przydziały dyskowe kontrolowane są niezależnie dla każdej partycji NTFS, nawet, jeśli partycje są zlokalizowane na jednym dysku fizycznym.

Ważne W systemie Windows 2000, przydziały dyskowe można wykorzystać tylko na partycjach NTFS.

Aby w pełni kontrolować dostępny dla użytkowników obszar na dysku, należy ustawić poziom ostrzeżeń dla przydziałów dyskowych, co pozwoli na zapis do dzienników zdarzeń systemowych informacji o tym, że użytkownik niedługo osiągnie swój limit. Można także zablokować użytkownikowi dostęp do dysku po osiągnięciu limitu miejsca lub zezwolić na przekroczenie limitu i kontynuację pracy.

Konfiguracja przydziałów dyskowych

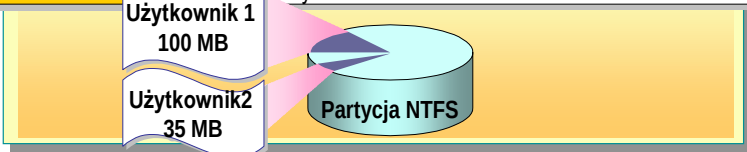
Cel slajdu

Prezentacja opcji, konfigurowanych przy zarządzaniu przydziałami dyskowymi.

Wprowadzenie

Istnieje możliwość włączenia przydziałów dyskowych w celu wymuszenia limitów miejsca na dysku dla wszystkich użytkowników jednocześnie lub dla każdego z osobna.

Option	Description
Enable quota management	Włączenie zarządzania przydziałami dyskowymi
Deny disk space to users exceeding quota limit	Odmowa miejsca na dysku użytkownikom przekraczającym limit przydziału
Do not limit disk usage	Brak ograniczania użycia dysku
Limit disk space to	Ograniczenie miejsca na dysku do wprowadzonej wartości
Set warning level to	Ustanowienie poziomu ostrzeżeń do wprowadzonej wartości
Quota Entries	Wprowadzanie, usuwanie, właściwości wpisów przydziału



Wskazówka

Pokaż, w jaki sposób włączyć przydziały dyskowe najpierw dla wszystkich użytkowników, a następnie dla jednego użytkownika.

Przydziały dyskowe można skonfigurować tak, aby wymusić ograniczenia przestrzeni dyskowej i generować ostrzeżenia, zarówno dla wszystkich użytkowników jednocześnie, jak i dla każdego z osobna.

Włączanie przydziałów dyskowych

Aby włączyć przydziały dyskowe, należy w oknie dialogowym **Properties** dla dysku, na karcie **Quota** skonfigurować opcje opisane w poniższej tabeli.

Opcja	Opis
Enable quota management	Zaznaczenie pola opcji umożliwia zarządzanie przydziałami dla tego dysku.
Deny disk space to users exceeding quota limit	Zaznaczenie pola opcji powoduje, po przekroczeniu przez użytkownika limitu miejsca na dysku, wyświetlanie komunikatu Out of disk space oraz zablokowanie możliwości zapisu.
Do not limit disk usage	Należy włączyć tę opcję wtedy, gdy nie istnieje potrzeba limitowania użytkownikom miejsca na dysku.
Limit disk space to	Umożliwia określenie ilości miejsca na dysku, dostępnego dla użytkowników.
Set warning level to	Umożliwia określenie ilości miejsca na dysku, którego przekroczenie spowoduje umieszczenie w dzienniku zdarzeń systemu Windows 2000 wpisu o zbliżaniu się użytkownika do ustalonego dla niego limitu.
Quota Entries	Wybranie tego przycisku umożliwia dodanie nowego, usunięcie istniejącego lub podgląd właściwości przydziału dyskowego.

Przydziały dyskowe dla wszystkich użytkowników

Aby określić limity wykorzystania dysku dla wszystkich użytkowników należy:

1. W polach **Limit disk space to** oraz **Set warning level to** wprowadzić wymagane wartości limitu zasobów dyskowych oraz poziomu ostrzegawczego.
2. Zaznaczyć pole opcji **Deny disk space to users exceeding quota limit**.
W systemie Windows 2000 będzie następowało monitorowanie wykorzystania zasobów dysku, a w przypadku próby przekroczenia przypisanego limitu, nastąpi odmowa utworzenia nowego pliku lub folderu.

Przydziały dyskowe dla indywidualnych użytkowników

Aby określić przydział dyskowy dla indywidualnego użytkownika, należy:

1. W oknie dialogowym **Properties** dla dysku, na karcie **Quota** wybrać przycisk **Quota Entries**.
2. W oknie dialogowym **Quota Entries for** utworzyć nowy wpis, wybierając z menu **Quota** polecenie **New Quota Entry** i wskazując wybranego użytkownika.

Następnie, należy ustalić limit miejsca na dysku i poziom ostrzegawczy.

Laboratorium B: Konfiguracja kompresji dysku i przydziałów dyskowych

Cel slajdu

Omówienie laboratorium.

Wprowadzenie

W tym laboratorium będą konfigurowane przydziały dyskowe i kompresja danych.



Wyjaśnij cele laboratorium.

Cele laboratorium

Po zrealizowaniu tego laboratorium słuchacz będzie potrafił:

- Konfigurować partycję NTFS do kompresji danych.
- Konfigurować przydziały dyskowe dla użytkowników.

Wymagania wstępne

Przed rozpoczęciem tego laboratorium należy:

- Posiadać wiedzę o systemie plików NTFS.
- Posiadać wiedzę na temat różnic pomiędzy grupą roboczą i domeną.
- Posiadać wiedzę o przydziałach dyskowych w systemie plików NTFS.

Przygotowanie laboratorium

Do wykonania tego laboratorium niezbędny jest komputer pracujący w systemie Windows 2000 Advanced Server, skonfigurowany jako serwer członkowski w domenie.

Przewidywany czas ukończenia laboratorium: 30 minut

Ćwiczenie 1

Konfiguracja kompresji NTFS

Scenariusz

Aby umożliwić maksymalne wykorzystanie zasobów dyskowych w sieci, kierownik działu IT postanowił włączyć kompresję folderów z danymi, na dyskach NTFS wszystkich serwerów członkowskich. Twoim zadaniem jest włącznie kompresji wybranych folderów na dyskach swojego serwera.

Cel

W tym ćwiczeniu włączysz kompresję danych i przyjrzyś się jej efektom, na przykładzie folderu Inetpub oraz wszystkich folderów w nim zawartych.

Zadania	Szczegółowe kroki
1. Zaloguj się do domeny nwtraders jako Adminx (gdzie x jest numerem Twojego stanowiska) z hasłem domain i skonfiguruj program Windows Explorer do wyświetlania nazw skompresowanych plików i folderów w innym kolorze.	a. Zaloguj się wykorzystując następujące informacje: User name: Adminx (gdzie x jest numerem Twojego stanowiska) Password: domain Log on to: nwtraders b. W oknie programu Windows Explorer, z menu Tools wybierz polecenie Folder Options. c. W oknie Folder Options, na karcie View zaznacz pole opcji Display compressed files and folders with alternate color, a następnie wybierz przycisk OK.
2. Skompresuj folder Inetpub i całą jego zawartość.	a. W oknie Windows Explorer rozwiń pozycję Local Disk (C:) , a następnie z menu podręcznego folderu Inetpub wybierz polecenie Properties .
 Jakie są wartości parametrów Size i Size on disk dla folderu Inetpub? Odpowiedzi mogą się różnić.	
2. (ciąg dalszy)	b. W oknie dialogowym Inetpub Properties wybierz przycisk Advanced. c. W oknie dialogowym Advanced Attributes, w sekcji Compress or Encrypt attributes zaznacz pole opcji Compress contents to save disk space, a następnie wybierz przycisk OK. d. Wybierz przycisk OK, aby zamknąć okno Inetpub Properties. e. W oknie Confirm Attribute Changes zaznacz pole opcji Apply changes to this folder, subfolders and files i wybierz przycisk OK.  W drzewie katalogów, w programie Windows Explorer, nazwa folderu Inetpub będzie wyróżniona innym kolorem. f. Otwórz okno dialogowe Properties dla folderu Inetpub.

(ciąg dalszy)

Zadania	Szczegółowe kroki
? Jakie są wartości parametrów Size i Size on disk dla folderu Inetpub? Jak dużo miejsca na dysku zostało zaoszczędzone po zastosowaniu kompresji? (Podpowiedź: porównaj wartości zapisane we wcześniejszej części ćwiczenia, zanim kompresja została włączona, z uzyskanymi po kompresji.) Odpowiedzi mogą się różnić.	
2. (ciąg dalszy)	g. Wybierz przycisk OK, aby zamknąć okno dialogowe Inetpub Properties.

Ćwiczenie 2

Określanie przydziałów dyskowych

Scenariusz

Użytkownicy przechowują pliki na serwerze sieciowym, ale wielu z nich nie potrafi prawidłowo zarządzać zasobami dyskowymi. Dlatego, serwer ciągle pracuje przy braku wolnego miejsca na dysku. Kierownicy Twojego departamentu IT postanowili ograniczyć użytkownikom miejsce dostępne na dyskach serwera. Twoim zadaniem jest włączenie przydziałów dyskowych na serwerze oraz ograniczenie do 10 MB miejsca dostępnego dla każdego z użytkowników. Gdy użytkownicy wykorzystają 60 procent przydzielonego im limitu, mają być informowani, że ich dane zajmują już większość dostępnego dla nich miejsca na dysku.

Cel

W tym ćwiczeniu włączysz przydziały dyskowe na partycji C: i utworzysz konsolę MMC, zawierającą przystawkę Local User Manager. Następnie wykorzystasz utworzoną konsolę do odblokowania konta gościa, któremu przypiszesz limit dyskowy.

Zadania	Szczegółowe kroki
1. Skonfiguruj domyślne ustawienia przydziałów dyskowych dla dysku C:, wykorzystując podane wielkości: Disk Space Limit: 10 MB Disk Space Warning: 6 MB	a. W programie Windows Explorer otwórz okno dialogowe Properties dysku Local Disk (C:). b. W oknie dialogowym Local Disk (C:) Properties, na karcie Quota zaznacz pola opcji Enable quota management oraz Deny disk space to users exceeding quota limit. c. Upewnij się, że w sekcji Select the default quota limit for new users on this volume wybrana jest opcja Limit disk space to. d. W polu Limit disk space to wpisz wartość 10, a następnie zmień jednostkę na MB. e. W polu Set warning level to wpisz wartość 6, a następnie zmień jednostkę na MB. f. Wybierz przycisk Apply.  Zostanie wyświetlona informacja o ponownym przeglądaniu wolumenu, jeśli włączone zostały przydziały dyskowe. g. Wybierz przycisk OK, a następnie przycisk Quota Entries. h. Z menu Quota wybierz polecenie New Quota Entry. i. W oknie Select Users, w polu Look in wybierz Server (gdzie Server jest nazwą Twojego komputera). j. Na liście Name zaznacz użytkownika QuotaUser, wybierz przycisk Add, a następnie przycisk OK, aby zamknąć okno Select Users.  Zostanie wyświetlone okno Add New Quota Entry. Zauważ, że wyświetlane są wartości, określone wcześniej dla dysku C. k. Wybierz przycisk OK, aby zamknąć okno Add New Quota Entry. l. Zamknij okno dialogowe Quota Entries for Local Disk (C:). m. Wybierz przycisk OK, aby zamknąć okno Local Disk (C:) Properties. n. Zamknij wszystkie otwarte okna i wyloguj się.

Ćwiczenie 3

Sprawdzanie i usuwanie przydziałów dyskowych

Scenariusz

Włączyłeś zarządzanie przydziałami dyskowymi na serwerze i chcesz sprawdzić, czy efekty są zgodne z oczekiwaniami. W tym celu, określisz przydział dyskowy i poziom ostrzegawczy dla konta QuotaUser. Następnie, zalogujesz się jako ten użytkownik i sprawdzisz poprawność konfiguracji i działania przydziałów dyskowych, kopiując nieco danych na partycję, dla której zdefiniowane zostały ograniczenia.

Cel

W tym ćwiczeniu przetestujesz, a następnie usuniesz przydziały dyskowe dla konta QuotaUser.

Zadania	Szczegółowe kroki
1. Zaloguj się do komputera <i>Server</i> (gdzie <i>Server</i> jest nazwą Twojego komputera) z hasłem password i przetestuj przydziały dyskowe dla konta QuotaUser, sprawdzając ilość wolnego miejsca na dysku C. Skopiuj folder Program Files do folderu My Documents.	a. Zaloguj się, wykorzystując następujące informacje: User name: QuotaUser Password: password Log on to: <i>Server</i> (gdzie <i>Server</i> jest nazwą Twojego komputera) b. W oknie programu Windows Explorer zaznacz Local Disk (C:).
? Jak dużo wolnego miejsca jest na dysku? Dlaczego? Mniej niż 10 MB. Wskazuje to na poprawne działanie przydziałów dyskowych.	
1. <i>(ciąg dalszy)</i>	c. Wyświetl zawartość dysku Local Disk (C:) i z menu podręcznego folderu Program Files wybierz polecenie Properties.
? Czy będąc zalogowany jako użytkownik QuotaUser, będziesz mógł skopiować całą zawartość folderu Program Files, jeśli jest włączone zarządzanie przydziałami dyskowymi? Nie. Miejsce wymagane do skopiowania folderu Program Files przekracza narzucony użytkownikowi QuotaUser limit miejsca na dysku.	

Zadania	Szczegółowe kroki
1. (ciąg dalszy)	d. Wybierz przycisk OK, aby zamknąć okno Program Files Properties. e. Z menu podręcznego folderu Program Files wybierz polecenie Copy. f. Z menu podręcznego folderu My Documents wybierz polecenie Paste.  Zostanie wyświetlony komunikat wskazujący, że proces kopiowania rozpoczął się. Po chwili zostanie wyświetlony komunikat Error Copying File or Folder z informacją, że nie ma wystarczającej ilości wolnej przestrzeni na dysku i propozycją usunięcia jednego lub kilku plików, aby zwiększyć ilość wolnego miejsca.
 Dlaczego został wyświetlony taki komunikat o błędzie? Ponieważ na skutek ustawienia limitu dyskowego, nie ma wystarczającej ilości wolnego miejsca na dysku, aby kontynuować kopiowanie plików.	
1. (ciąg dalszy)	g. Wybierz przycisk OK, aby zamknąć okno komunikatu Error Copying File or Folder. h. Zamknij okno programu Windows Explorer i wyloguj się.
2. Zaloguj się do domeny nwtraders jako Adminx (gdzie x jest numerem Twojego stanowiska) z hasłem domain i wyłącz przydziały dyskowe dla dysku C.	a. Zaloguj się, wykorzystując następujące informacje: User name: Adminx (gdzie x jest numerem Twojego stanowiska) Password: domain Log on to: nwtraders b. W programie Windows Explorer, z menu podręcznego dysku Local Disk (C:) wybierz polecenie Properties. c. Na karcie Quota usuń znacznik z pola opcji Enable quota management.  Zauważ, że ustawienia limitów dla dysku C są niedostępne. d. Wybierz przycisk Apply.  Zostanie wyświetlony komunikat Disk Quota, ostrzegający, że wyłączenie zarządzania przydziałami dyskowymi spowoduje ponowne przeglądanie wolumenu, gdy zostaną one powtórnie włączone. e. Wybierz przycisk OK, aby zamknąć okno komunikatu Disk Quota. f. Wybierz przycisk OK, aby zamknąć okno dialogowe Local Disk (C:) Properties. g. Zamknij wszystkie otwarte okna i wyloguj się.

◆ Zabezpieczanie danych przy użyciu EFS

Cel slajdu

Prezentacja zagadnień związanych z odzyskiwaniem zaszyfrowanych plików.

Wprowadzenie

System EFS, będący składnikiem systemu plików NTFS w Windows 2000, umożliwia zabezpieczanie plików i folderów, oparte na wykorzystaniu kluczy publicznych.

- Wprowadzenie do technologii EFS
- Szyfrowanie folderów lub plików
- Deszyfrowanie folderów lub plików
- Odzyskiwanie zaszyfrowanego folderu lub pliku

System szyfrowania plików EFS (Encrypting File System) umożliwia szyfrowanie danych, na poziomie plików, na partycjach NTFS. Technologia szyfrowania EFS oparta jest na wykorzystaniu klucza publicznego, działa jako integralna usługa systemowa i pozwala na odzyskiwanie plików przez wyznaczonego agenta odzyskiwania EFS.

System EFS jest łatwy w zarządzaniu, ponieważ w razie konieczności uzyskania dostępu do ważnych, zaszyfrowanych przez użytkownika, danych, gdy jego klucz jest niedostępny, agent odzyskiwania EFS (domyślnie administrator) może odszyfrować plik.

Poznanie korzyści, jakie oferuje system EFS, pomoże w efektywnym wykorzystaniu tej technologii w sieci przedsiębiorstwa.

Wprowadzenie do technologii EFS

Cel slajdu

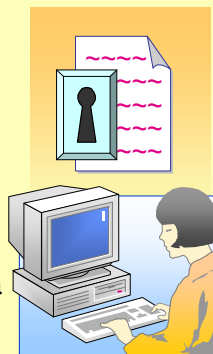
Prezentacja charakterystycznych cech systemu EFS.

Wprowadzenie

System EFS umożliwia użytkownikowi przechowywanie danych na dysku w postaci zaszyfrowanej.

Charakterystyczne cechy systemu EFS:

- Przeprowadzanie operacji w tle
- Dostęp tylko dla autoryzowanych użytkowników
- Wbudowana możliwość odzyskiwania zaszyfrowanych danych
- Istnienie przynajmniej jednego agenta odzyskiwania



Przedyskutuj ze słuchaczami cel stosowania systemu EFS oraz proces szyfrowania i deszyfrowania plików i folderów.

System EFS umożliwia użytkownikowi przechowywanie na dysku danych zaszyfrowanych. Po zaszyfrowaniu pliku, będzie on przechowywany w takim stanie, dopóki pozostanie na dysku. Użytkownicy mogą wykorzystywać system EFS do szyfrowania plików, w celu zachowania poufności danych.

Kluczowe cechy systemu EFS:

- Operacje szyfrowania i deszyfrowania przeprowadzane są w tle i są niewidoczne dla użytkowników oraz aplikacji.
- System EFS umożliwia dostęp do zaszyfrowanego pliku tylko autoryzowanemu użytkownikowi. Podczas używania pliku jest on automatycznie deszyfrowany i szyfrowany ponownie podczas zapisu na dysk. Administrator może odzyskać plik zaszyfrowany przez dowolnego użytkownika. Umożliwia to dostęp do zaszyfrowanego przez użytkownika pliku, gdy użytkownik jest nieobecny lub zgubi swój klucz prywatny.
- System EFS ma wbudowany system odzyskiwania danych. W systemie zabezpieczeń Windows 2000 Server wymuszana jest konfiguracja kluczy odzyskiwania. Z szyfrowania plików można skorzystać tylko wtedy, gdy na komputerze lokalnym istnieje przynajmniej jeden klucz odzyskiwania. System EFS automatycznie generuje klucze odzyskiwania i umieszcza je w rejestrze systemu, gdy nie jest możliwy dostęp do domeny.
- Wymagany jest przynajmniej jeden agent odzyskiwania EFS. Można wyznaczyć dowolną liczbę agentów do zarządzania programem odzyskiwania EFS. Każdy agent wymaga posiadania certyfikatu EFS Recovery Agent.

Uwaga Szyfrowanie i kompresja danych nawzajem się wykluczają. Dlatego można wybrać albo szyfrowanie, albo kompresję pliku, a nie obydwie technologie jednocześnie.

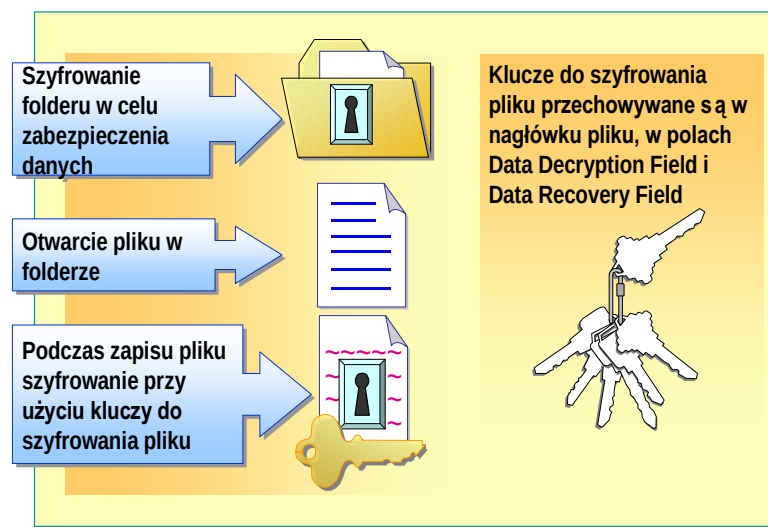
Szyfrowanie folderów lub plików

Cel slajdu

Prezentacja sposobu szyfrowania plików i folderów na partycjach NTFS.

Wprowadzenie

Plik jest szyfrowany przy użyciu kluczy szyfrowania.



Aby zaszyfrować pliki i foldery, na partycji NTFS należy utworzyć obiekt, a następnie zaszyfrować go, wykorzystując okno dialogowe **Properties** dla tego obiektu. Na karcie **General**, należy wybrać przycisk **Advanced** i zaznaczyć pole opcji **Encrypt contents to secure data**.

Po zaszyfrowaniu folderu, pliki w nim zapisywane będą automatycznie szyfrowane z użyciem kluczy szyfrowania plików. Do szyfrowania plików używane są szybkie klucze symetryczne, zaprojektowane do powszechnego szyfrowania danych. W systemie Windows 2000 pliki szyfrowane są blokami, przy wykorzystaniu innego klucza do szyfrowania każdego bloku. Klucze szyfrujące są przechowywane w polach DDF (Data Decryption Field) oraz DRF (Data Recovery Field), znajdujących się w nagłówku pliku.

Wszystkie pliki i foldery tworzone w zaszyfrowanym folderze są również automatycznie szyfrowane. Każdy plik ma unikalny klucz szyfrujący, zapewniający bezpieczną zmianę nazwy pliku. W czasie przenoszenia pliku z folderu zaszyfrowanego do folderu nie szyfrowanego na tej samej partycji, plik pozostaje zaszyfrowany.

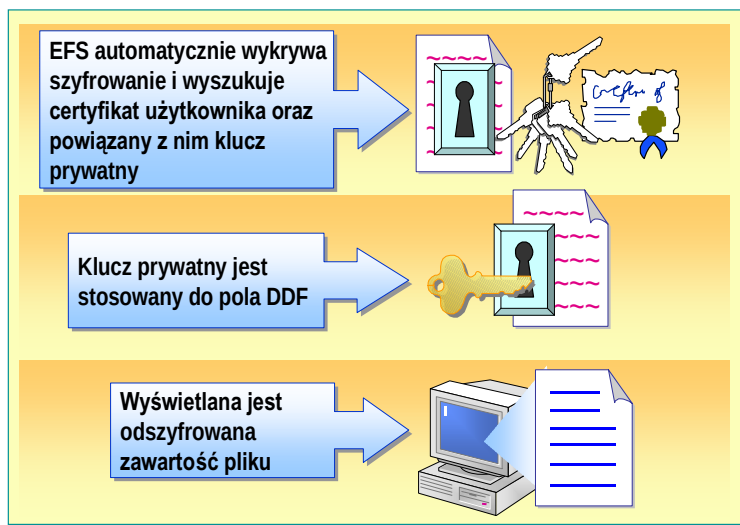
Deszyfrowanie folderów lub plików

Cel slajdu

Prezentacja metody deszyfrowania plików i folderów na partycjach NTFS.

Wprowadzenie

Folder lub plik na partycji NTFS można odszyfrować używając swojego klucza prywatnego.



Podczas otwierania zaszyfrowanego pliku, system EFS automatycznie wykrywa szyfrowanie i wyszukuje certyfikat użytkownika oraz powiązany z nim klucz prywatny. System EFS wykorzystuje ten klucz do deszyfrowania pola DDF i odblokowania listy kluczy szyfrujących, co pozwala na jawne wyświetlenie zawartości pliku.

Dostęp do zaszyfrowanego pliku jest zakazany wszystkim użytkownikom, poza właścicielem klucza prywatnego. Tylko właściciel klucza lub agent odzyskiwania EFS może odszyfrować plik. Twierdzenie to jest prawdziwe także wtedy, gdy administrator przypisze innemu użytkownikowi uprawnienie Take Ownership do tego pliku. Nawet, jeśli użytkownik stanie się właścicielem zaszyfrowanego pliku nie będzie mógł go odczytać, dopóki nie będzie posiadał klucza prywatnego lub nie stanie się agentem odzyskiwania EFS.

Uwaga Zaszyfrowanego pliku nie można udostępniać innym użytkownikom.

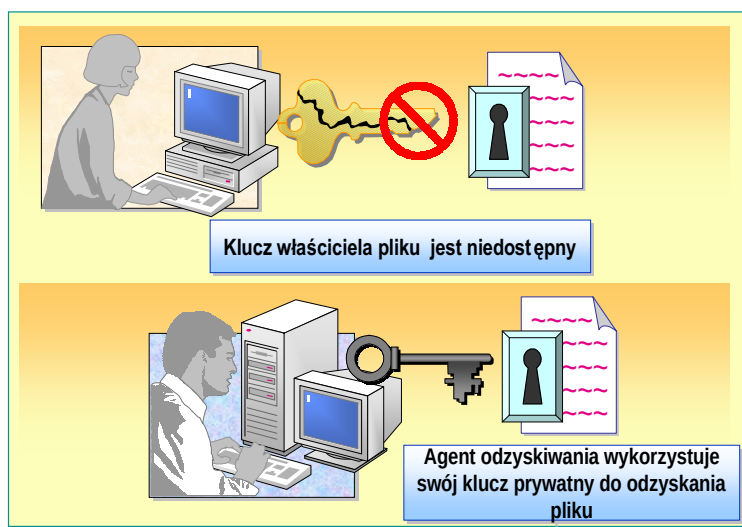
Odzyskiwanie zaszyfrowanego folderu lub pliku

Cel slajdu

Prezentacja procesu odzyskiwania zaszyfrowanych plików.

Wprowadzenie

W przypadku, gdy właściciel zgubi swój klucz prywatny, agent odzyskiwania EFS może odtworzyć zawartość zaszyfrowanego pliku.



Jeśli klucz prywatny właściciela pliku jest niedostępny, agent odzyskiwania może otworzyć zaszyfrowany plik, wykorzystując swój klucz prywatny, który, zastosowany do pola DRF, odblokowuje listę kluczy szyfrujących pliku. Jeśli agent odzyskiwania wykorzystuje inny komputer w sieci, plik należy przesłać do niego. Agent odzyskiwania może przesłać swój klucz prywatny do innego komputera, ale nie jest to polecane ze względów bezpieczeństwa.

Dobrym zwyczajem jest okresowa zmiana agentów. Jeśli jednak agent ulegnie zmianie, dostęp do zaszyfrowanych plików nie będzie możliwy. Dlatego, dobrze jest przechowywać certyfikaty odzyskiwania i klucze prywatne, dopóki wszystkie zaszyfrowane pliki nie zostaną uaktualnione.

Aby odzyskać zaszyfrowany plik będąc agentem odzyskiwania EFS, należy:

1. Wykorzystując program Windows Backup lub inne narzędzie do archiwizacji, odtworzyć zaszyfrowaną kopię pliku lub folderu użytkownika na komputerze, gdzie jest umieszczony certyfikat odzyskiwania.
2. W programie Windows Explorer otworzyć okno **Properties** dla zaszyfrowanego pliku lub folderu. Na karcie **General** wybrać przycisk **Advanced**.
3. Wyczyścić pole opcji **Encrypt contents to secure data**.
4. Utworzyć kopię odszyfrowanego pliku lub folderu i przekazać ją użytkownikowi.

Laboratorium C: Zabezpieczanie plików przy użyciu EFS

Cel slajdu

Omówienie laboratorium

Wprowadzenie

W tym laboratorium pliki będą zabezpieczane przy użyciu systemu EFS.



Cele laboratorium

Po zrealizowaniu tego laboratorium słuchacz będzie potrafił:

- Eksportować certyfikat agenta odzyskiwania.
- Szyfrować plik przy użyciu systemu EFS.
- Importować certyfikat agenta odzyskiwania.
- Odzyskiwać zaszyfrowane pliki.

Wymagania wstępne

Przed rozpoczęciem tego laboratorium należy:

- Posiadać wiedzę na temat zabezpieczania plików technologią EFS w systemie Windows 2000.
- Posiadać wiedzę na temat certyfikatów i roli agenta odzyskiwania w procesie szyfrowania i deszyfrowania plików.

Przygotowanie laboratorium

Do wykonania tego laboratorium niezbędne są:

- Komputer pracujący w systemie Windows 2000 Server, skonfigurowany jako serwer członkowski w domenie nwtraders.msft.
- Konto użytkownika EfsUser na komputerze słuchacza.
- Folder C:\MOC\Win2152b\Labfiles\Lab06\Efs, zawierający plik Confidential.txt.
- Czysta, sformatowana dyskietka.

Przewidywany czas ukończenia laboratorium: 15 minut

Ćwiczenie 1

Zabezpieczanie certyfikatu agenta odzyskiwania

Scenariusz

Zasady bezpieczeństwa w Twojej firmie wymagają zastosowania systemu EFS do zabezpieczania danych, przechowywanych na serwerze wolnostojącym. Wymagane jest również usunięcie certyfikatu agenta odzyskiwania ze wszystkich serwerów wolnostojących i umieszczenia ich w bezpiecznym miejscu.

Cel

W tym ćwiczeniu przekształcisz swój komputer w serwer wolnostojący i wyeksportujesz certyfikat agenta odzyskiwania.

Zadania	Szczegółowe kroki
1. Zaloguj się do domeny nwtraders.msft jako Adminx (gdzie x jest numerem Twojego stanowiska) z hasłem domain i skonfiguruj swój komputer jako serwer wolnostojący.	- Zaloguj się, wykorzystując następujące informacje: User name: Adminx (gdzie x jest numerem Twojego stanowiska) Password: domain Log on to: nwtraders - W oknie Control Panel uruchom program System. - W oknie System Properties, na karcie Network Identification wybierz przycisk Properties. - W sekcji Member of wybierz opcję Workgroup, w polu Workgroup wpisz Workgroup i wybierz przycisk OK. - W oknie komunikatu Network Identification wybierz dwa razy przycisk OK. - Wybierz przycisk OK, aby zamknąć okno System Properties. - Zamknij okno Control Panel. - W oknie System Settings Change wybierz przycisk Yes, aby ponownie uruchomić komputer.
2. Zaloguj się jako Administrator z hasłem password i wyeksportuj na dyskietkę certyfikat szyfrowania plików dla konta Administrator.	- Zaloguj się do swojego serwera, wykorzystując informacje: User name: Administrator Password: password - Z menu Start wybierz polecenie Run. - W oknie Open wpisz mmc i wybierz przycisk OK. - W oknie Console1 z menu Console wybierz Add/Remove Snap-in. - W oknie Add/Remove Snap-in wybierz przycisk Add. - W oknie Add Standalone Snap-in zaznacz Certificates i wybierz przycisk Add. - W oknie Certificates snap-in upewnij się, że zaznaczona jest opcja My user account i wybierz przycisk Finish. - Wybierz przycisk Close, aby zamknąć okno Add Standalone Snap-in, a następnie przycisk OK, aby zamknąć okno Add/Remove Snap-in.  W oknie drzewa konsoli pojawi się <i>Certificates - Current User</i>.

Zadania	Szczegółowe kroki
2. <i>(ciąg dalszy)</i>	i. Z menu Console wybierz polecenie Save As. j. W oknie Save As, w polu Save in upewnij się, że wyświetlany jest folder Administrative Tools. k. W polu File name wpisz Certificates i wybierz przycisk Save. l. W oknie drzewa konsoli rozwiń Certificates - Current User, następnie Personal i wybierz Certificates. m. Pracując w oknie szczegółów, w menu podręcznym dla Administrator rozwiń menu All Tasks i wybierz polecenie Export. n. Na karcie Welcome to the Certificate Export Wizard wybierz przycisk Next. o. Na karcie Export Private Key upewnij się, że wybrana jest opcja Yes, export the private key i wybierz przycisk Next. p. Na karcie Export File Format wybierz opcję Delete the private key if the export is successful, a następnie przycisk Next. q. Na karcie Password, w polach Password oraz Confirm password wpisz password i wybierz przycisk Next. r. Na karcie File to Export, w polu File name wpisz a:\certificate s. Włóż dyskietkę do napędu A i wybierz przycisk Next. t. Na karcie Completing the Certificate Export Wizard wybierz przycisk Finish. u. W oknie komunikatu Certificate Export Wizard wybierz przycisk OK. v. Usuń dyskietkę z napędu. w. Zamknij okno Certificates, zapisz ustawienia konsoli i wyloguj się.

Ćwiczenie 2

Szyfrowanie pliku przy wykorzystaniu systemu EFS (Encrypting File System)

Scenariusz

Założenia bezpieczeństwa Twojej firmy wymagają od Ciebie szyfrowania poufnych plików, abyś tylko Ty miał do nich dostęp.

Cel

W tym ćwiczeniu zaszyfrujesz plik wykorzystując system EFS.

Zadania	Szczegółowe kroki
1. Zaloguj się jako EfsUser z hasłem password i zaszyfruj plik Confidential.txt, znajdujący się w folderze C:\MOC\Win2152b\Labfiles\Lab06\Efs.	a. Zaloguj się, wykorzystując następujące informacje: User name: EfsUser Password: password b. Wykorzystując program Windows Explorer, przejdź do folderu C:\MOC\Win2152b\Labfiles\Lab06\Efs, upewnij się, że masz możliwość odczytu zawartości pliku Confidential.txt i zamknij program Notepad. c. Otwórz okno dialogowe Properties dla pliku Confidential.txt. d. Na karcie General wybierz przycisk Advanced . e. W oknie dialogowym Advanced Attributes zaznacz pole opcji Encrypt contents to secure data i wybierz przycisk OK . f. Wybierz przycisk OK , aby zamknąć okno Confidential Properties . g. W oknie dialogowym Encryption Warning wybierz opcję Encrypt the file only , a następnie przycisk OK . h. Upewnij się, że ciągle masz możliwość odczytu zawartości pliku Confidential.txt i zamknij program Notepad. i. Zamknij okno programu Windows Explorer i wyloguj się.

Ćwiczenie 3

Odzyskiwanie zaszyfrowanego pliku przy użyciu certyfikatu agenta odzyskiwania

Scenariusz

Użytkownik opuścił firmę i jego konto zostało usunięte. Po usunięciu konta użytkownika okazało się, że zaszyfrował on plik, zawierający ważne dane firmowe. Twój przełożony potrzebuje dostępu do tych danych.

Cel

W tym ćwiczeniu importujesz certyfikat agenta odzyskiwania i odzyskasz zaszyfrowany plik, który zawiera dane potrzebne Twojemu przełożonemu.

Zadania	Szczegółowe kroki
1. Zaloguj się jako Administrator z hasłem password i podejmij próbę otwarcia pliku Confidential z folderu C:\MOC\Win2152b\Labfiles\Lab06\Efs.	a. Zaloguj się wykorzystując następujące informacje: User name: Administrator Password: password b. W programie Windows Explorer przejdź do folderu C:\MOC\Win2152b\Labfiles\Lab06\Efs i spróbuj odczytać zawartość pliku Confidential.txt.
? Czy możesz odczytać zawartość pliku Confidential? Dlaczego tak lub nie? Nie. Nie możesz odczytać zawartości pliku, ponieważ inny użytkownik zaszyfrował plik.	
1. (ciąg dalszy)	c. Wybierz przycisk OK , zamknij program Notepad i zminimalizuj okno programu Windows Explorer.
2. Importuj certyfikat agenta odzyskiwania i odszyfruj plik Confidential z folderu C:\MOC\Win2152b\Labfiles\Lab06\Efs.	a. Włóż do napędu dyskietkę, zawierającą certyfikat. b. Z menu Administrative Tools otwórz konsolę Certificates. c. W oknie drzewa konsoli rozwiń Certificates - Current User , jeśli to będzie konieczne, w menu podłącznym kontenera Personal wskaż All Tasks i wybierz polecenie Import . d. W oknie kreatora Welcome to the Certificate Import Wizard wybierz przycisk Next . e. W oknie File to Import , w polu File name wpisz a:\certificate.pfx i wybierz przycisk Next . f. W oknie Password , w polu Password wpisz password i wybierz przycisk Next . g. W oknie Certificate Store wybierz przycisk Next , a następnie w oknie Completing the Certificate Import Wizard wybierz przycisk Finish .

Zadania	Szczegółowe kroki
2. <i>(ciąg dalszy)</i>	h. W oknie komunikatu Certificate Import Wizard wybierz przycisk OK i zamknij konsolę Certificates, zapisując ustawienia konsoli, jeśli to będzie konieczne. i. Przywróć okno programu Windows Explorer i spróbuj odczytać zawartość pliku Confidential.txt.
 Czy możesz odczytać zawartość pliku Confidential? Dlaczego tak lub nie? Tak. Możesz odczytać zawartość pliku, ponieważ wykorzystujesz certyfikat agenta odzyskiwania.	
2. <i>(ciąg dalszy)</i>	j. Zamknij program Notepad i otwórz okno Properties dla pliku Confidential.txt. k. Na karcie General wybierz przycisk Advanced. l. W oknie dialogowym Advanced Attributes wyczyść pole opcji Encrypt contents to secure data i wybierz przycisk OK. m. Wybierz przycisk OK, aby zamknąć okno Confidential Properties i zamknij okno programu Windows Explorer.
3. Dołącz się do domeny nwtraders.msft.	a. W oknie Control Panel wybierz ikonę System. b. Na karcie Network Identification wybierz przycisk Properties. c. W sekcji Member of wybierz opcję Domain, w polu Domain wpisz nwtraders.msft i wybierz przycisk OK. d. W oknie Domain Username and Password, w polu Name wpisz Adminx (gdzie x jest numerem Twojego stanowiska). e. W polu Password wpisz domain i wybierz przycisk OK. f. W oknie komunikatu Network Identification dwa razy wybierz przycisk OK. g. Wybierz przycisk OK, aby zamknąć okno dialogowe System Properties, a następnie zamknij okno Control Panel. h. Usuń dyskietkę z napędu. i. W oknie System Settings Change wybierz przycisk Yes, aby ponownie uruchomić komputer.

Podsumowanie

Cel slajdu

Podsumowanie celów rozdziału poprzez przypomnienie zagadnień kluczowych.

Wprowadzenie

Pytania podsumowujące dotyczą głównych tematów omówionych w rozdziale.

- Wprowadzenie do uprawnień NTFS
- Zastosowanie uprawnień NTFS w Windows 2000
- Wykorzystanie uprawnień NTFS
- Wykorzystanie specjalnych uprawnień NTFS
- Kompresja danych na partycjach NTFS
- Konfiguracja przydziałów dyskowych na partycjach NTFS
- Zabezpieczanie danych przy wykorzystaniu EFS

-
1. Kierownik działu sprzedaży awansował ostatnio na stanowisko Wiceprezesa do spraw sprzedaży, a regionalny kierownik działu sprzedaży przeszedł na jego miejsce. Nowy kierownik działu sprzedaży powinien stać się właścicielem plików, zawierających miesięczne raporty sprzedaży. W jaki sposób przypisać specjalne uprawnienia NTFS, aby umożliwić nowemu kierownikowi przejęcie na własność plików działu sprzedaży?

Dotychczasowy właściciel plików powinien przypisać nowemu kierownikowi działu sprzedaży uprawnienie NTFS Take Ownership. Pozwoli to nowemu kierownikowi na przejęcie istniejących plików na własność.

2. Z komputera korzysta wiele osób. W jaki sposób umożliwić autoryzowanym użytkownikom tego komputera dostęp tylko do swoich plików z danymi?

Należy dokonać konwersji dysku do systemu plików NTFS, utworzyć folder dla każdego z użytkowników, a następnie skonfigurować tak uprawnienia NTFS, aby użytkownicy jako jedyni mieli dostęp do swoich folderów.

3. Użytkownik JDRoland jest członkiem grup Engineers, ENGManagers i Users. Uprawnienia NTFS do folderu Drawings są następujące:
JDRoland – Nie zdefiniowane
Engineers – Full Control
ENGManagers – Read
Users – Nie zdefiniowane
Jakie uprawnienie ma użytkownik JDRoland do folderu Drawings?
Dlaczego?

Full Control. Mimo, że konto użytkownika nie ma przypisanych żadnych uprawnień, jest jednak członkiem grupy Engineers. Ponieważ uprawnienia NTFS kumulują się, użytkownik JDRoland ma do folderu Drawings uprawnienie Full Control.

4. Podczas konfigurowania uprawnień NTFS do folderu użytkownik zauważył, że część uprawnień jest zaznaczona, ale pola opcji są szare i nie można ich wyczyścić. Dlaczego tak się dzieje i w jaki sposób można pola opcji zmienić?

Szare pola opcji wskazują, że dziedziczone są uprawnienia folderu nadrzędnego. Aby zmienić te uprawnienia, należy najpierw wyczyścić pole opcji Allow inheritable permissions from the parent to propagate to this object, co pozwoli na usunięcie uprawnień dziedzicznych i bezpośrednie przypisanie tylko tych wymaganych.

5. Włączono kompresję NTFS dla folderu Archive, w którym przechowywane są dzienniki zdarzeń i archiwalne dane. Raz w tygodniu użytkownik przenosił pliki do folderu Archive. Po pewnym czasie zauważył, że nie wszystkie pliki są skompresowane. Co może być tego powodem?

Część plików była przenoszona z tej samej partycji, na której znajduje się folder Archive, a część z innych partycji. Gdy pliki przenoszone są w obrębie tej samej partycji, zachowują swoje atrybuty. Gdy przenosi się je z innych partycji, dziedziczone są atrybuty folderu docelowego.

6. Do przechowywania i kontrolowania dokumentów korporacyjnych w Firmie wykorzystywana jest jedna, centralna lokalizacja. Każdy z użytkowników ma przydzieloną pewną ilość miejsca, a wydziały, w których użytkownicy pracują, są obciążane rachunkami za wykorzystane miejsce. W przeszłości strategia przydzielania zasobów dyskowych polegała na tworzeniu na dyskach serwera partycji dla każdego z użytkowników. Powodowało to problemy, gdy wielkość przydzielonego miejsca musiała ulec zmianie. Centrum przechowywania danych planuje uaktualnienie wszystkich serwerów do systemu Windows 2000. Która cecha Windows 2000 ułatwi kontrolę przydzielanego użytkownikom miejsca na dyskach?

W systemie Windows 2000 obsługiwane jest zarządzanie przydziałami dyskowymi, co umożliwia administratorowi dynamiczną zmianę limitu dyskowego.

7. Użytkownik udostępnia swój komputer innym osobom. Próbował odczytać zawartość pliku na dysku lokalnym komputera i otrzymał komunikat **Access denied**. Po sprawdzeniu uprawnień NTFS okazało się, że ma do tego pliku uprawnienie Full Control. Co jest powodem wyświetlania komunikatu o braku dostępu do pliku i w jaki sposób użytkownik może ten dostęp uzyskać?

Plik jest zaszyfrowany przy wykorzystaniu systemu EFS. Tylko osoba, która plik zaszyfrowała może go odszyfrować. Jeśli użytkownik potrzebuje dostępu do tego pliku, musi zwrócić się do agent odzyskiwania lub osoby, która zastosowała szyfrowanie, aby plik odszyfrować.