

Rozdział 3: Bezpieczeństwo w sieci opartej na systemie Windows 2000

Spis treści

Przegląd zagadnień	1
Konta użytkowników	2
Grupy	7
Laboratorium A: Badanie kont użytkowników i grup	8
Prawa użytkownika	10
Laboratorium B: Badanie praw użytkownika	14
Uprawnienia	17
Laboratorium C: Badanie uprawnień do plików i folderów	27
Podsumowanie	31



Zastrzega się prawo wprowadzania zmian do treści niniejszego dokumentu bez uprzedniego powiadomienia. Wszystkie firmy, produkty, osoby, teksty i/lub dane opisane w przykładach są fikcyjne i jeżeli przypominają jakiegokolwiek rzeczywiste osoby, firmy lub wydarzenia, w żadnym przypadku nie było to zamierzone, o ile nie wspomniano, że jest inaczej. Odpowiedzialność za przestrzeganie wszystkich odnośnych praw autorskich ponosi użytkownik. Niniejszego dokumentu lub jego części nie wolno powielać w żadnej formie ani przekazywać za pomocą jakiegokolwiek nośników elektronicznych lub mechanicznych, z wyjątkiem przypadków, w których uzyskano na to pisemną zgodę firmy Microsoft Corporation. Jeżeli użytkownik ma dostęp do niniejszego 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 niniejszym dokumencie. Otrzymanie tego dokumentu nie oznacza udzielenia licencji na te 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. Wszystkie prawa zastrzeżone.

Microsoft, Windows, Windows NT, Active Directory, BackOffice, FrontPage, Outlook, PowerPoint i Visual Studio są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy Microsoft Corporation zarejestrowanymi w USA i/lub w innych krajach.

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

Inne produkty i nazwy firm używane w treści mogą być nazwami zastrzeżonymi przez ich właścicieli.

Project Lead: Red Johnston

Instructional Designers: Meera Krishna (NIIT (USA) Inc.), Bhaskar Sengupta (NIIT (USA) Inc.)

Instructional Design Contributors: Aneetinder Chowdhry (NIIT (USA) Inc.),

Jay Johnson (The Write Stuff), Sonia Pande (NIIT (USA) Inc.)

Lead Program Manager: Jim Cochran (Volt)

Program Manager: Jamie Mikami (Volt)

Technical Contributors: Rodney Miller, Gregory Weber (Volt)

Testing Leads: Sid Benavente, Keith Cotton

Testing Developer: Greg Stemp (S&T OnSite)

Simulation Developer: Wai Chan (Meridian Partners Ltd.)

Courseware Test Engineers: Jeff Clark, Jim Toland (ComputerPREP, Inc.)

Graphic Artist: Julie Stone (Independent Contractor)

Editing Manager: Lynette Skinner

Editor: Patricia Rytkenon (The Write Stuff)

Copy Editor: Kaarin Dolliver (S&T Consulting)

Online Program Manager: Debbi Conger

Online Publications Manager: Arlo Emerson (Aditi)

Online Support: Eric Brandt (S&T Consulting)

Multimedia Development: Kelly Renner (Entex)

Courseware Testing: Data Dimensions, Inc.

Production Support: Ed Casper (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

Symulacje oraz ćwiczenia interaktywne zostały wykonane przez firmę Macromedia Authorware

Opracowanie wersji polskiej: DC Edukacja Sp. z o.o., Al. Niepodległości 659, 81-855 Sopot
e-mail: info@edukacja.com, Internet: <http://www.edukacja.com>

Współpraca: P.S.I. Sp. z o.o., ul. Manifestu Lipcowego 9, 25-323 Kielce
e-mail: psi@edukacja.com, Internet: <http://www.interpsi.ok.pl>

Zespół tłumaczy: Artur Pucek, Sebastian Tobolski

Konsultacja: Waldemar Pierścioneck, Piotr Zejer

Uwagi dla wykładowcy

Prezentacja:
60 minut

Laboratoria:
45 minut

W rozdziale tym słuchacze dowiedzą się, w jaki sposób system Microsoft® Windows® 2000 zabezpiecza zasoby sieci przed nieuprawnionym dostępem. Rozdział ten opisuje, jak wykorzystanie kont użytkowników, haseł oraz grup zapewnia bezpieczeństwo w środowisku sieciowym oraz w jaki sposób użytkownikom i grupom nadawane są określone prawa. W rozdziale omówione zostały także uprawnienia do plików, folderów oraz drukarek.

Po zrealizowaniu tego rozdziału słuchacz będzie potrafił:

- Opisać rolę i zastosowanie różnych typów kont użytkowników.
- Opisać rolę i zastosowanie różnych typów grup.
- Określić standardowe prawa użytkowników i grup.
- Opisać uprawnienia do plików, folderów oraz udostępnionych folderów.

Materiały i sposób przygotowania

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

Wymagane materiały

Do przedstawienia tego rozdziału potrzebne będą następujące materiały:

- Plik programu Microsoft PowerPoint® o nazwie 2243A_03.ppt
- Rozdział 3, „Bezpieczeństwo w sieci opartej na systemie Windows 2000”

Sposób przygotowania

Aby przygotować się do przedstawienia tego rozdziału, należy:

- Przeczytać całość materiałów poświęconych temu rozdziałowi.
- Wykonać laboratoria.
- Przeczytać dokument *Enterprise Class Storage in Windows 2000*, znajdujący się na płycie kompaktowej Materiały dla wykładowcy.
- Przejrzeć wskazówki i zagadnienia kluczowe kolejnych sekcji i tematów.
- Przejrzeć pytania podsumowujące i podać inne odpowiedzi do dyskusji.
- Przewidzieć możliwe pytania słuchaczy i przygotować na nie odpowiedzi.

Strategia przedstawienia rozdziału

Wskazówki dotyczące prezentacji rozdziału:

- Konta użytkowników

Prezentację tej części należy zacząć od omówienia zagadnień związanych z różnymi typami kont użytkowników i ich funkcjami. Następnie należy przedstawić narzędzia, pozwalające tworzyć i modyfikować różne typy kont użytkowników.

- Grupy

W tej sekcji należy przedstawić definicję grupy oraz opisać sposób wykorzystania grup w sieciach opartych na systemie Microsoft Windows 2000. Następnie należy wyjaśnić różnicę pomiędzy grupami, które znajdują się na komputerach, będących kontrolerami domen, i grupami, które znajdują się na pozostałych komputerach.

- Prawa użytkownika

Na początku tej części należy przedstawić zagadnienia związane z prawami użytkownika. Następnie należy omówić niektóre ze standardowych praw, dostępnych w systemie Windows 2000. Rozdział należy podsumować wyjaśnieniem, dlaczego wbudowane grupy otrzymują domyślnie niektóre prawa.

- Uprawnienia

Opisując tą sekcję należy wyjaśnić, jak za pomocą przydzielania uprawnień można określić typ dostępu użytkowników do zasobów sieciowych. Następnie należy opisać obiekty, do których można przypisać uprawnienia (drukarki, pliki i foldery) oraz różne typy uprawnień, które można nadać każdemu z nich.

Informacje uzupełniające

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

Ważne Aby możliwe było wykonanie laboratoriów, zawartych w tym rozdziale, konieczne jest odpowiednie skonfigurowanie pracowni, zgodnie z uwagami znajdującymi się w sekcji Informacje uzupełniające, zamieszczonej w rozdziale Przygotowanie pracowni do kursu 2243A, *Podstawy sieci i systemu operacyjnego Microsoft Windows 2000*.

Rezultaty laboratorium

Nie ma żadnych zmian w konfiguracji komputerów słuchaczy, wpływających na powielanie lub dostosowywanie materiałów szkoleniowych.

Przegląd zagadnień

Cel slajdu

Przedstawienie tematów i celów rozdziału.

Wprowadzenie

Konta użytkowników, grupy, prawa oraz uprawnienia pozwalają zapewnić bezpieczeństwo w sieci opartej na systemie Windows 2000.

- Konta użytkowników
- Grupy
- Prawa użytkownika
- Uprawnienia

Aby zapewnić ochronę zasobów sieciowych przed nieuprawnionym dostępem, konieczne jest sprawdzanie w trakcie logowania tożsamości każdego użytkownika, uzyskującego dostęp do sieci. W tym celu każdy użytkownik musi podać odpowiednią nazwę konta oraz poprawne hasło. Nazwa konta umożliwia identyfikację poszczególnych użytkowników w domenie. Dzięki stosowaniu haseł, konta mają prywatny charakter, gdyż tylko użytkownicy, którzy znają hasło, mogą z nich korzystać. Po sprawdzeniu tożsamości użytkownika, jego dostęp do komputera w sieci zostaje uwierzytelniony.

Aby ułatwić administrowanie siecią, można podzielić użytkowników na grupy i każdej grupie nadać uprawnienia, umożliwiające uzyskiwanie dostępu do określonych zasobów sieciowych. Kontrola nad rodzajem czynności, które wykonują użytkownicy sieci, jest możliwa poprzez nadawanie im odpowiednich praw użytkownika.

Aby zapewnić jeszcze wyższy poziom bezpieczeństwa, zasoby sieciowe mogą być zabezpieczone przez uprawnienia do plików, folderów i udostępnionych folderów.

Po zrealizowaniu tego rozdziału słuchacz będzie potrafił:

- Opisać rolę i zastosowanie różnych typów kont użytkowników.
- Opisać rolę i zastosowanie różnych typów grup.
- Określić standardowe prawa użytkowników i prawa poszczególnych wbudowanych grup.
- Opisać uprawnienia do plików, folderów oraz udostępnionych folderów.

◆ Konta użytkowników

Cel slajdu

Przedstawienie pojęć lokalnego konta użytkownika oraz domenowego konta użytkownika.

Wprowadzenie

W sieciach opartych na systemie Windows 2000 dostępne są dwa typy kont użytkowników: lokalne konta użytkowników oraz domenowe konta użytkowników.

- **Lokalne konta użytkowników**
- **Domenowe konta użytkowników**

Dzięki kontom użytkowników, poszczególni użytkownicy mogą uzyskiwać dostęp do zasobów sieci. Konto użytkownika stanowi unikalny zbiór cech, rozpoznawany przez sieć. Dla każdej osoby, która regularnie korzysta z sieci, administrator tworzy konto użytkownika. Także administrator przypisuje każdemu kontu użytkownika nazwę i hasło, a później zajmuje się ich obsługą. W systemie Microsoft® Windows® 2000 dostępne są dwa typy kont użytkowników: lokalne konta użytkowników oraz domenowe konta użytkowników.

W przypadku lokalnego konta użytkownika, konto tworzone jest w lokalnej bazie danych systemu bezpieczeństwa, co daje użytkownikowi możliwość logowania się do określonego komputera i korzystania ze zgromadzonych na nim zasobów. Sytuacja taka ma zazwyczaj miejsce w przypadku grup roboczych. Jeśli komputer jest członkiem grupy roboczej, to wszystkie konta są przechowywane lokalnie na tym komputerze. Użytkownik posiadający takie konto ma dostęp tylko do zasobów, znajdujących się na tym komputerze.

Jeśli użytkownik posiada domenowe konto użytkownika, to może on zalogować się do domeny i korzystać z zasobów sieci. Użytkownik posiadający domenowe konto użytkownika ma dostęp do wszystkich zasobów domeny.

W sytuacji, gdy istnieje domena, użytkownik może posiadać zarówno domenowe konto użytkownika, jak i konto na lokalnym komputerze. Możliwość utworzenia tych kont, zwanych kontami ręcznie tworzonymi, ma administrator. Konta użytkowników mogą być przechowywane w jednym z dwóch miejsc: albo w lokalnej bazie danych systemu bezpieczeństwa (pod warunkiem, że komputer nie jest kontrolerem domeny), albo w bazie danych usługi MS Active Directory™.

Oprócz kont ręcznie utworzonych, w systemie Windows 2000 dostępne są także dwa domyślne, wbudowane konta użytkowników. Za pomocą tych kont można wykonywać zadania administracyjne oraz uzyskiwać tymczasowy dostęp do zasobów sieci. Wbudowane konta użytkowników są dostępne zarówno w przypadku komputerów lokalnych jak i domen.

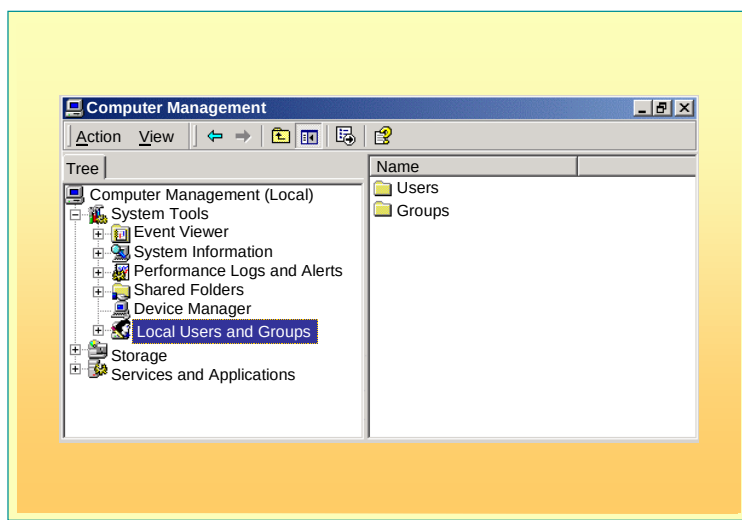
Lokalne konta użytkowników

Cel slajdu

Opisanie zastosowania lokalnych kont użytkowników.

Wprowadzenie

Osoba posiadająca lokalne konto użytkownika ma dostęp tylko do zasobów, znajdujących się na określonym komputerze.



Aby użytkownik mógł uzyskać dostęp do zasobów zgromadzonych na danym komputerze, musi posiadać na nim lokalne konto użytkownika. Dostępne są dwa rodzaje lokalnych kont użytkowników: konta ręcznie tworzone oraz konta wbudowane. W czasie tworzenia lokalnego konta użytkownika, informacja o nim zapisywana jest tylko w lokalnej bazie danych systemu bezpieczeństwa danego komputera.

Wskazówka

Przypomnij słuchaczom, że grupa robocza i domena różnią się od siebie oraz że do administrowania nimi używa się innych narzędzi.

Ręcznie tworzone lokalne konta użytkowników

Ręcznie tworzone lokalne konta użytkowników są to konta tworzone przez administratora, pozwalające użytkownikom uzyskiwać dostęp tylko do tych komputerów, na których zostały one utworzone. Lokalne konta użytkowników mogą zostać utworzone na serwerach oraz na komputerach pracujących w systemie Microsoft Windows 2000 Professional, pod warunkiem, że nie są one kontrolerami domen. Lokalne konta użytkowników są zazwyczaj stosowane tylko w przypadku niezależnych komputerów lub w niewielkich środowiskach sieciowych, takich jak na przykład grupy robocze. Użytkownik może posiadać jednocześnie konto na lokalnym komputerze oraz konto w domenie, jednak w danym czasie może korzystać tylko z jednego z nich. O tym, które konto będzie w danej chwili wykorzystywane, decyduje użytkownik w czasie logowania.

Wbudowane (lokalne) konta użytkowników

Oprócz ręcznie tworzonych kont w systemie Windows 2000 dostępne są także dwa wbudowane konta użytkownika: do wykonywania zadań administracyjnych oraz do uzyskiwania tymczasowego dostępu do lokalnego komputera. W trakcie instalacji systemu Windows 2000 automatycznie tworzone są dwa wbudowane konta użytkowników—konto Administrator oraz konto Guest.

Konto Administrator

Administratorzy, korzystając z wbudowanego konta użytkownika Administrator, mogą po zainstalowaniu systemu Windows 2000 utworzyć dla siebie konto dedykowane. Wbudowane konto Administrator nie może zostać usunięte, ani wyłączone, dzięki czemu administrator może zawsze uzyskać dostęp do dowolnego komputera. Wykorzystanie tego konta wymaga znajomości hasła, które zostało podane w trakcie instalacji systemu.

Konto Guest

Użytkownicy, którzy nie mają konta użytkownika na danym komputerze, mogą się na nim logować, korzystając z konta Guest. Taką samą możliwość mają także użytkownicy, których konta zostały wyłączone. Ponieważ konto Guest domyślnie jest wyłączone, aby można było się na nie logować, musi zostać ono włączone przez administratora. Podczas logowania się na to konto nie trzeba podawać hasła.

Narzędzie Local Users and Groups

W systemie Windows 2000 dostępne jest narzędzie Local Users and Groups, które pozwala administratorom zarządzać kontami użytkowników na lokalnym komputerze. Narzędzie to dostępne jest na wszystkich komputerach pracujących w systemie Windows 2000 Professional oraz na serwerach pracujących w systemie Microsoft Windows 2000 Server. Za pomocą narzędzia Local Users and Groups można wykonywać następujące zadania:

- Tworzyć nowe lub usuwać istniejące konta użytkowników
- Modyfikować konta użytkowników, zmieniając ich nazwy lub informacje dotyczące kont, takie jak hasła lub ich opisy
- Usuwać hasła kont użytkowników
- Wyłączać lub włączać konta użytkowników

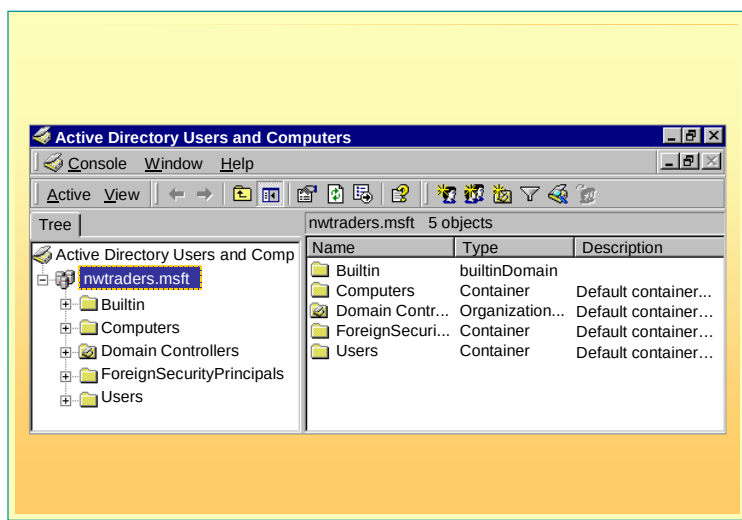
Domenowe konta użytkowników

Cel slajdu

Opisanie zastosowania domenowych kont użytkowników.

Wprowadzenie

Osoba posiadająca domenowe konto użytkownika może uzyskiwać dostęp do zasobów, znajdujących się w domenie.

**Wskazówka**

Przypomnij słuchaczom zagadnienia dotyczące domen, pytając ich, czym jest domena i jakie są jej cechy.

Lokalne konto użytkownika pozwala jedynie na logowanie się na lokalnych komputerach i uzyskiwanie dostępu do lokalnych zasobów. Tymczasem w środowisku sieciowym bardzo często zachodzi konieczność uzyskania dostępu do zasobów, które znajdują się gdzieś w sieci. Aby uzyskać dostęp do tych zasobów, konieczne jest zastosowanie domenowego konta użytkownika. W czasie tworzenia domenowego konta użytkownika, informacja o nim zapisywana jest w bazie danych usługi Active Directory, dzięki czemu można z niego korzystać z dowolnego miejsca, znajdującego się w obrębie domeny. Rozwiązanie to bardzo różni się od sposobu przyjętego w grupach roboczych, gdzie informacja o koncie użytkownika zapisywana jest tylko na lokalnym komputerze.

Ręcznie utworzone domenowe konta użytkowników

Ręcznie utworzone domenowe konta użytkowników są to konta tworzone przez administratora, umożliwiające użytkownikom logowanie się do domeny i uzyskiwanie dostępu do zasobów znajdujących się w dowolnym miejscu w sieci. Domenowe konta użytkowników mogą zostać utworzone na kontrolerze domeny. Kontroler domeny przesyła informacje o nowym koncie użytkownika do wszystkich pozostałych kontrolerów danej domeny. W czasie procesu logowania, użytkownik podaje swoją nazwę i hasło oraz określa, w której domenie znajduje się jego konto. Pierwszy dostępny kontroler domeny weryfikuje konto użytkownika, korzystając z informacji podanych przez użytkownika.

Wbudowane (domenowe) konta użytkowników

Oprócz domenowych kont użytkowników, które mogą zostać utworzone przez administratorów, w systemie Windows 2000 dostępne są także dwa wbudowane domenowe konta użytkowników—konto Administrator oraz konto Guest. Wbudowane domenowe konta użytkowników pełnią podobną funkcję, co wbudowane konta użytkowników, tworzone na lokalnych komputerach w grupach roboczych. Główna różnica polega na tym, że za pomocą tych kont można uzyskiwać dostęp do całej domeny.

Konto Administrator

Wbudowane konto Administrator pozwala zarządzać wszystkimi komputerami i zmieniać konfigurację domeny. Administrator, korzystając z tego konta, może tworzyć i modyfikować konta użytkowników i grup, zarządzać systemem bezpieczeństwa, administrować drukarkami oraz przypisywać uprawnienia kontom użytkowników. Można zmienić nazwę tego konta, ale nie można go usunąć.

Konto Guest

Za pomocą wbudowanego konta Guest użytkownicy, którzy rzadko korzystają z sieci, mogą uzyskać dostęp do zasobów sieciowych. Na przykład w środowisku, w którym kwestia bezpieczeństwa nie jest bardzo istotna, pracownicy mogą za pomocą konta Guest uzyskiwać na krótki czas dostęp do zasobów. Domyślnie konto to jest wyłączone.

Konsola Active Directory Users and Computers

W systemie Windows 2000 dostępna jest konsola Active Directory Users and Computers, za pomocą której administratorzy mogą zarządzać kontami użytkowników, znajdującymi się w bazie danych usługi Active Directory.

Konsola ta jest instalowana na komputerach, które zostały skonfigurowane do pracy jako kontroler domeny. Aby móc skorzystać z konsoli Active Directory Users and Computers, należy zalogować się do domeny systemu Windows 2000 (a nie na lokalny komputer) i posiadać odpowiednie uprawnienia do wykonywania pewnych operacji.

Za pomocą konsoli Active Directory Users and Computers można wykonywać w domenie następujące zadania:

- Dodawać lub usuwać konta użytkowników
- Włączać i wyłączać konta użytkowników
- Odnajdywać i przenosić konta użytkowników
- Zmieniać nazwy kont użytkowników
- Usuwać hasła użytkowników

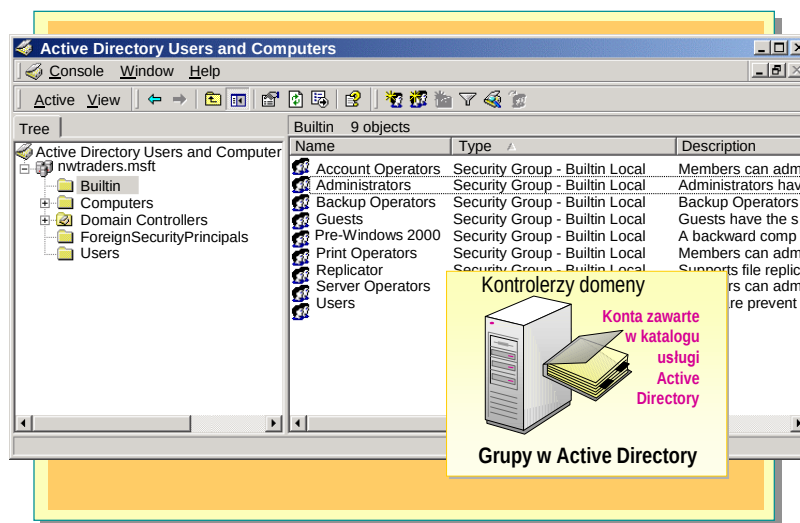
Grupy

Cel slajdu

Przedstawienie zastosowania grup w administrowaniu siecią opartą na systemie Windows 2000.

Wprowadzenie

Aby uprościć administrowanie kontami użytkowników, można te konta podzielić na grupy.



Grupa jest to zbiór kont użytkowników. Wszystkim członkom danej grupy można jednocześnie przypisać określone uprawnienia dostępu, co zwalnia z konieczności przydzielania uprawnień poszczególnym użytkownikom. Po udzieleniu grupie uprawnień dostępu, wystarczy po prostu dodać do niej odpowiednich użytkowników. Można przy tym posłużyć się domyślnymi, czyli wbudowanymi, grupami, dostępnymi w systemie Windows 2000, albo też utworzyć nowe grupy, spełniające wymogi danej organizacji.

Grupa może istnieć na lokalnym komputerze, na komputerach znajdujących się w jednej domenie, albo na komputerach znajdujących się w różnych domenach.

Grupy na lokalnym komputerze

Na komputerach lokalnych (komputerach, które nie są kontrolerami domeny), można tworzyć tylko lokalne grupy, o których informacje zapisywane są w lokalnej bazie danych systemu bezpieczeństwa. Grupy utworzone na komputerach, które nie są kontrolerami domen, zapewniają bezpieczeństwo i umożliwiają uzyskiwanie dostępu tylko do lokalnego komputera. Na przykład, aby dany użytkownik uzyskał uprawnienia administratora na lokalnym komputerze, jego konto musi zostać na tym komputerze dodane do grupy Administrators za pomocą narzędzia Local Users and Groups.

Grupy na kontrolerze domeny

Informacje na temat grup tworzonych na kontrolerze domeny są gromadzone w bazie danych usługi Active Directory. Grupa utworzona na kontrolerze domeny może zawierać konta użytkowników z jednej domeny lub konta użytkowników z wielu domen. Na przykład, aby nadać użytkownikowi uprawnienia administratora, należy dodać jego konto do grupy Administrators, istniejącej na kontrolerze domeny, za pomocą konsoli Active Directory Users and Computers.

Laboratorium A: Badanie kont użytkowników i grup

Cel slajdu

Omówienie laboratorium.

Wprowadzenie

Realizacja tego laboratorium polega na określaniu głównych właściwości kont użytkowników i grup.



Cele laboratorium

Po zrealizowaniu tego laboratorium słuchacz będzie potrafił:

- Określić główne właściwości kont użytkowników i grup.

Wymagania wstępne

Przed rozpoczęciem tego laboratorium należy:

- Nauczyć się logować i wylogowywać z systemu Microsoft Windows 2000.

Przewidywany czas ukończenia laboratorium: 15 minut

Ćwiczenie 1

Badanie domenowych kont użytkowników i grup

Scenariusz

Powierzone zostało Tobie zadanie nadzorowania jednostek organizacyjnych Sales oraz Managers. Na początku musisz dowiedzieć się, jakie obiekty znajdują się w tych jednostkach. Ich zawartość możesz obejrzeć za pomocą konsoli Active Directory Users and Computers.

Cel

W tym ćwiczeniu sprawdzisz różne jednostki organizacyjne, znajdujące się w domenie oraz zapiszesz wybrane informacje na ich temat.

Zadania	Szczegółowe kroki
1. Uruchom konsolę Active Directory Users and Computers, a następnie określ, jakie obiekty wchodziły w skład jednostki organizacyjnej Managers.	a. Zaloguj się do systemu Windows 2000 jako Administrator, wpisując hasło password . b. W menu Start wskaż pozycję Programs , następnie wskaż pozycję Administrative Tools i kliknij ikonę Active Directory Users and Computers . c. Zmaksymalizuj konsolę Active Directory Users and Computers. d. Kliknij pozycję Managers , znajdującą się w drzewie konsoli.
? Sprawdź, jakie obiekty znajdują się w okienku szczegółów konsoli Active Directory Users and Computers. Za jakie konta użytkowników oraz grupy jesteś odpowiedzialny? Jesteś odpowiedzialny za konta użytkowników Jae Pak i Kim Yoshida oraz za grupę Managers.	
2. Określ, jakie konta wchodziły w skład jednostki organizacyjnej Sales.	a. Kliknij pozycję Sales , znajdującą się w drzewie konsoli.
? Sprawdź, jakie obiekty znajdują się w okienku szczegółów konsoli Active Directory Users and Computers. Za jakie konta użytkowników oraz grupy jesteś odpowiedzialny? Jesteś odpowiedzialny za konta użytkowników Anne Paper i Don Hall oraz za grupę Sales.	
3. Zamknij wszystkie okna i wyloguj się z systemu Windows 2000	a. Zamknij wszystkie okna i wyloguj się z systemu Windows 2000.

◆ Prawa użytkownika

Cel slajdu

Przedstawienie pojęć związanych z prawami użytkownika oraz prawami przypisanymi do wbudowanych grup.

Wprowadzenie

Prawa stosowane są raczej w odniesieniu do całego systemu, niż do poszczególnych zasobów i wpływają na całość operacji wykonywanych na komputerze lub w domenie.

- Standardowe prawa u użytkownika
- Prawa przypisane do wbudowanych grup

Prawa stosowane są raczej w odniesieniu do całego systemu, niż do poszczególnych zasobów i wpływają na całość operacji wykonywanych na komputerze lub w domenie. Wszyscy użytkownicy, uzyskujący dostęp do zasobów sieciowych, powinni mieć na komputerach, z których korzystają, pewne standardowe prawa, jak na przykład prawo do logowania się lokalnie, czy do zmiany czasu systemowego. Administratorzy mogą nadać określone standardowe prawa grupie użytkowników lub poszczególnym użytkownikom. Oprócz tego sam system Windows 2000 nadaje domyślnie pewne prawa wbudowanym grupom. Prawa użytkownika określają czynności, które użytkownicy mogą wykonywać na określonym komputerze lub w domenie.

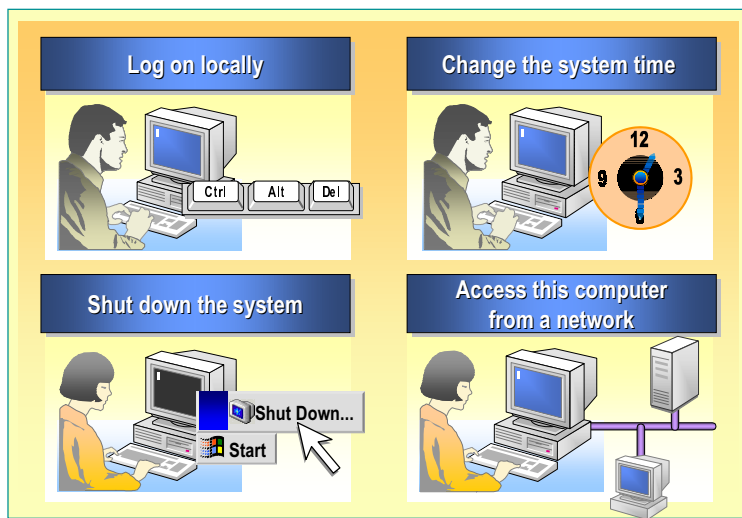
Standardowe prawa użytkownika

Cel slajdu

Określenie standardowych praw użytkownika.

Wprowadzenie

Prawa umożliwiają użytkownikom wykonywanie określonych czynności w systemie.



Prawa umożliwiają użytkownikowi, który zalogował się na komputerze lub w sieci, wykonywanie w systemie określonych czynności. Jeśli użytkownik nie posiada praw zezwalających mu na wykonywanie określonej czynności, każda próba jej realizacji zostanie zablokowana.

Chociaż prawa użytkownika mogą być nadawane zarówno grupom, jak i indywidualnym użytkownikom, to jednak przyznawanie praw w odparciu o grupy znacznie ułatwia wykonywanie wszystkich zadań administracyjnych. Dzieje się tak, ponieważ użytkownik, który loguje się jako członek grupy, automatycznie otrzymuje wszystkie prawa, które zostały przypisane grupie. System Windows 2000 pozwala administratorowi przypisywać prawa użytkownikom oraz grupom użytkowników. Standardowe prawa użytkownika to: Log on locally (prawo do logowania się lokalnie), Change the system time (prawo do zmiany czasu systemowego), Shut down the system (prawo do zamykania systemu) oraz Access this computer from a network (prawo do uzyskiwania dostępu do komputera z sieci).

- Log on locally

Użytkownik posiadający to prawo może logować się na lokalny komputer lub do domeny przez lokalny komputer.

- Change the system time

Użytkownik posiadający to prawo może zmieniać ustawienia wewnętrznego zegara komputera.

- Shut down the system

Użytkownik posiadający to prawo może zakończyć pracę lokalnego komputera.

- Access this computer from a network

Użytkownik posiadający to prawo może uzyskiwać dostęp do komputera, pracującego w systemie Windows 2000, z dowolnego innego komputera, znajdującego się w sieci.

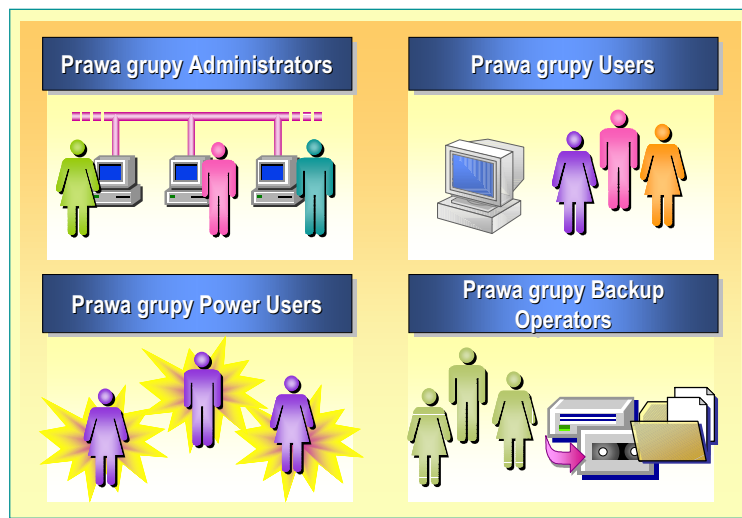
Prawa przypisane do wbudowanych grup

Cel slajdu

Określenie praw wbudowanych grup.

Wprowadzenie

Wbudowanym grupom są domyślnie przyznawane pewne prawa.



System Windows 2000 domyślnie przyznaje pewne prawa wbudowanym grupom, takim jak Administrators, Users, Power Users oraz Backup Operators.

Grupa Administrators

Wbudowana grupa Administrators jest dostępna zarówno na komputerach, które są jak i tych, które nie są kontrolerami domeny. Członkowie grupy Administrators posiadają pełną kontrolę nad komputerem lub domeną. Grupa Administrators jest jedyną wbudowaną grupą, której nadawane są automatycznie wszystkie prawa, dostępne w systemie.

Grupa Users

Wbudowana grupa Users jest dostępna zarówno na komputerach, które są jak i tych, które nie są kontrolerami domeny. Członkowie grupy Users mogą wykonywać tylko te zadania, do których przyznane zostały im odpowiednie prawa, jak na przykład uruchamianie aplikacji, korzystanie z lokalnych i sieciowych drukarek oraz zamykanie i blokowanie stacji roboczych. Członkowie grupy Users mogą tworzyć i modyfikować lokalne grupy, ale nie mogą udostępniać folderów ani lokalnych drukarek.

Grupa Power Users

Wbudowana grupa Power Users jest dostępna tylko na komputerach, które nie są kontrolerami domeny. Członkowie grupy Power Users mogą wykonywać różnego rodzaju zadania administracyjne, ale nie mają wszystkich praw, które pozwoliłyby im przejąć całkowitą kontrolę nad systemem. Prawa grupy Power Users obejmują:

- Tworzenie kont użytkowników i grup na lokalnym komputerze.
- Modyfikowanie i usuwanie kont, które wcześniej sami utworzyli.
- Udostępnianie zasobów.

Członkowie grupy Power Users nie mają jednak prawa do:

- Zmieniania ustawień grupy Administrators oraz Backup Operators.
- Tworzenia kopii zapasowych oraz przywracania folderów.

Grupa Backup Operators

Wbudowana grupa Backup Operators jest dostępna zarówno na komputerach, które są jak i tych, które nie są kontrolerami domeny. Członkowie grupy Backup Operators mogą tworzyć kopie zapasowe i przywracać pliki na komputerze, niezależnie od uprawnień, które chronią te pliki. Członkowie grupy Backup Operators mogą także logować się na komputerze oraz zakończyć jego pracę, ale nie mogą zmieniać ustawień systemu bezpieczeństwa.

Laboratorium B: Badanie praw użytkownika

Cel slajdu

Omówienie laboratorium.

Wprowadzenie

Realizacja tego laboratorium polega na zbadaniu różnych praw użytkownika.



Cele laboratorium

Po zrealizowaniu tego laboratorium słuchacz będzie potrafił:

- Opisać, jaki wpływ mają prawa użytkownika na konto użytkownika.

Wymagania wstępne

Przed rozpoczęciem tego laboratorium należy:

- Nauczyć się logować i wylogowywać z systemu Microsoft Windows 2000.

Przewidywany czas ukończenia laboratorium: 15 minut

Ćwiczenie 1

Sprawdzenie praw użytkownika

Scenariusz

Inny administrator stworzył kilka kont użytkowników w Twojej domenie. Chcesz sprawdzić, jaki jest efekt przypisania określonych praw użytkownika do tych kont.

Cel

W tym ćwiczeniu zalogujesz się dwukrotnie, za każdym razem na inne konto użytkownika, i sprawdzisz, czy użytkownikom tym zostały nadane określone prawa.

Zadania	Szczegółowe kroki
1. Zaloguj się jako Kimyo, podając hasło password. Spróbuj dokonać zmiany czasu systemowego.	a. Zaloguj się na komputerze, podając następujące dane: Username: kimyo Password: password Domain: <i>nazwa_domeny</i> (gdzie zmienna <i>nazwa_domeny</i> określa domenę, do której chcesz się zalogować). b. W menu Start wskaż pozycję Settings, a następnie kliknij ikonę Control Panel. c. W Panelu sterowania kliknij dwukrotnie ikonę Date/Time.
 Jaka informacja jest wyświetlana, gdy próbujesz zmienić czas systemowy? Dlaczego tak się dzieje? Wyświetlana jest informacja: „You do not have the proper privilege level to change the system time”. Dzieje się tak, ponieważ użytkownik Kimyo nie posiada prawa do zmiany czasu systemowego.	
2. Spróbuj uruchomić program Add/Remove Hardware.	a. W oknie Control Panel kliknij dwukrotnie ikonę Add/Remove Hardware.
 Czy użytkownikowi Kimyo nadane zostało prawo, pozwalające dodawać nowy sprzęt za pomocą kreatora Add/Remove Hardware? Dlaczego istotne może okazać się ograniczenie tego prawa? Nie. Ograniczenie tego prawa uniemożliwia nieuprawnionym użytkownikom dokonywanie zmian, które w znaczny sposób mogłyby wpłynąć na system operacyjny i jego wydajność.	

(ciąg dalszy)

Zadania	Szczegółowe kroki
3. Spróbuj zalogować się jako użytkownik Donha.	a. Wyloguj się. b. Zaloguj się na komputerze, podając następujące dane: Username: donha Password: password Domain: <i>nazwa_domeny.nwtraders.msft</i> (gdzie zmienna <i>nazwa_domeny</i> określa domenę, do której chcesz się zalogować).
 Czy możesz zalogować się na komputerze jako Donha? Dlaczego jest to lub nie jest możliwe? Nie. Donha nie posiada praw do interaktywnego logowania się. _____ _____ _____ _____	
4. Zamknij okno komunikatu.	a. Wybierz przycisk OK , aby zamknąć okno komunikatu.

◆ Uprawnienia

Cel slajdu

Przedstawienie zastosowania uprawnień w sieci.

Wprowadzenie

Za pomocą uprawnień można kontrolować, którzy użytkownicy mają dostęp do zasobów sieciowych.

- Przedstawienie zagadnień związanych z uprawnieniami
- Uprawnienia do plików w systemie NTFS
- Uprawnienia do folderów w systemie NTFS
- Uprawnienia do udostępnionych folderów
- Uprawnienia do drukarek

Dzięki przypisaniu odpowiednich uprawnień można kontrolować, którzy użytkownicy mają dostęp do zasobów, udostępnionych na komputerze pracującym w systemie Windows 2000. Uprawnienia określają typ dostępu, który jest przypisany do użytkownika lub grupy dla określonego zasobu. Na przykład osoby pracujące w dziale kadr danej organizacji, powinny mieć zapewnioną możliwość modyfikowania dokumentów opisujących działalność tego działu. Aby pracownicy działu kadr mieli zapewnioną taką możliwość, administrator powinien nadać im odpowiednie uprawnienia.

Przypisywanie uprawnień do określonych plików i folderów w systemie Windows 2000 jest możliwe dzięki systemowi plików NTFS. Administrator może także przypisywać użytkownikom uprawnienia, zezwalające na dostęp do udostępnionych folderów oraz drukarek sieciowych.

Przedstawienie zagadnień związanych z uprawnieniami

Cel slajdu

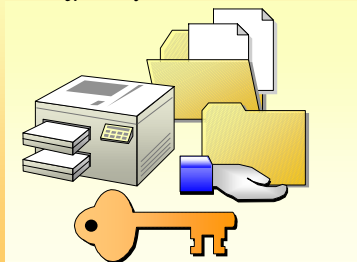
Opisanie uprawnień do obiektów.

Wprowadzenie

Uprawnienia pozwalają kontrolować, kto ma dostęp do określonych obiektów, znajdujących się w sieci oraz określać, jaki typ dostępu jest dozwolony. Uprawnienia umożliwiające dostęp do obiektów mogą być nadawane zarówno użytkownikom jak i grupom.

■ Uprawnienia do obiektów

- Uprawnienia nadawane są do obiektów
- Obiekt jest to niezależny element, taki jak plik, folder, udostępniony folder lub drukarka



Uprawnienia określają typ dostępu, jaki posiada użytkownik lub grupa do określonego obiektu. Typ uprawnień, który może zostać przypisany użytkownikowi, zależy od typu obiektu.

Uprawnienia do obiektów

Obiekt jest to niezależny element, taki jak plik, folder, udostępniony folder lub drukarka. Uprawnienia, które są przypisywane użytkownikom do określonych obiektów, nazywane są uprawnieniami do obiektów.

Uprawnienia do obiektów można przypisywać w bazie danych usługi Active Directory lub na lokalnym komputerze. Aby uprościć proces przypisywania uprawnień, najlepiej nadawać je grupom, a nie poszczególnym użytkownikom. Taki sposób wykorzystania grup ułatwia zadania, wiążące się z zarządzaniem uprawnieniami do obiektów.

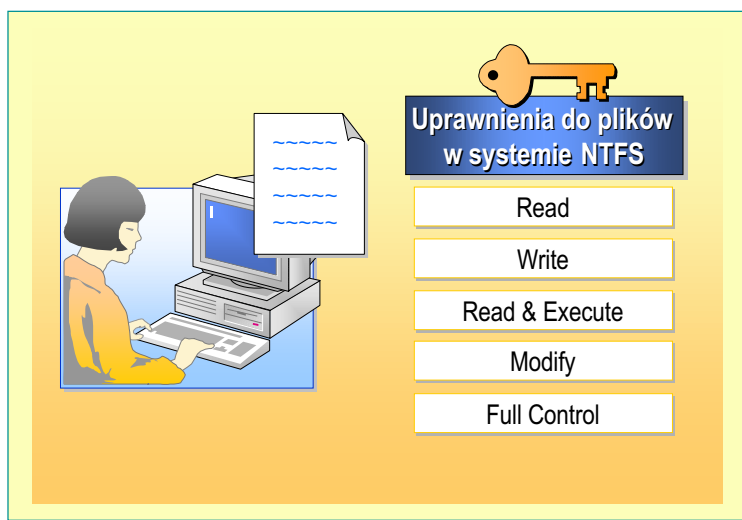
Uprawnienia do plików w systemie NTFS

Cel slajdu

Opisanie uprawnień do plików w systemie NTFS.

Wprowadzenie

Za pomocą uprawnień do plików w systemie NTFS można kontrolować, którzy użytkownicy będą mieli dostęp do określonych plików, znajdujących się na partycji NTFS.



Wskazówka

Pokaż słuchaczom, w jaki sposób można przeglądać uprawnienia do plików w systemie NTFS. Na tym etapie kursu nie powinienś podawać jeszcze szczegółów dotyczących zmiany uprawnień.

Uprawnienia do plików w systemie NTFS umożliwiają kontrolę dostępu do poszczególnych plików, pozwalając wybrać użytkowników, którzy mogą uzyskiwać dostęp i określać typ dostępu.

Uwaga Więcej informacji na temat systemu plików NTFS znajduje się w dokumencie *File and Print Services Technical Overview*, do którego dostęp można uzyskać poprzez łącze **Dodatkowe dokumenty**, znajdujące się na stronie sieci Web na płycie kompaktowej Materiały dla słuchacza.

Zamieszczona poniżej tabela przedstawia listę standardowych uprawnień do plików w systemie NTFS wraz z opisem typu dostępu, na które zezwala każde z nich. Uprawnienia zostały przedstawione w kolejności od najbardziej do najmniej restrykcyjnego.

Uprawnienie do pliku w systemie NTFS	Pozwala użytkownikowi
Read	Odczytywać plik i przeglądać informacje dotyczące jego atrybutów, właściciela oraz uprawnień.
Write	Zastępować plik, zmieniać jego atrybuty oraz przeglądać informacje dotyczące jego właściciela oraz uprawnień.
Read & Execute	Uruchamiać aplikacje i wykonywać wszystkie czynności, które są dozwolone dla uprawnienia typu Read.
Modify	Modyfikować i usuwać plik oraz wykonywać wszystkie czynności, które są dozwolone dla uprawnień typu Write oraz Read & Execute.
Full Control	Zmieniać uprawnienia, przejmować na własność oraz wykonywać wszystkie czynności, które są dozwolone dla wszystkich pozostałych uprawnień do plików w systemie NTFS.

Przeglądanie uprawnień do plików

Administrator może przypisywać uprawnienia do pliku za pomocą karty **Security** okna dialogowego **Properties** danego pliku. Za pomocą tej karty można także sprawdzić aktualne ustawienia uprawnień do pliku.

Aby uzyskać dostęp do karty Security, należy:

1. W oknie Windows Explorer kliknąć prawym przyciskiem myszy wybrany plik.
2. Z podręcznego menu wybrać pozycję **Properties**.
3. W oknie dialogowym **Properties** wybrać kartę **Security**.

Karta **Security** składa się z dwóch sekcji—Name oraz Permissions. W sekcji Name wyświetlana jest lista użytkowników oraz grup, które posiadają uprawnienia do danego pliku. W sekcji Permissions wyświetlana jest lista uprawnień, które zostały przyznane lub zablokowane danemu użytkownikowi lub grupie.

Zazwyczaj zaznacza się uprawnienia, które mają zostać nadane. Czasami jednak łatwiej jest wybrać uprawnienia, które mają zostać zablokowane. Sytuacja taka może mieć miejsce, gdy generalnie wszyscy użytkownicy mają mieć dostęp do pliku, za wyjątkiem na przykład użytkowników, którzy uzyskują dostęp do zasobu poprzez konto Guest. W tym celu należy zablokować uprawnienia dla konta Guest.

Uprawnienia do folderów w systemie NTFS

Cel slajdu

Opisanie uprawnień do folderów w systemie NTFS.

Wprowadzenie

Za pomocą uprawnień do folderów w systemie NTFS można kontrolować, którzy użytkownicy będą mieli dostęp do określonych folderów, znajdujących się na partycji NTFS.



Wskazówka

Pokaż słuchaczom, w jaki sposób można przeglądać uprawnienia do folderów w systemie NTFS. Omawiając typy uprawnień, nie powinieneś przedstawiać sposobu ich ustawiania.

Uprawnienia do folderów w systemie NTFS umożliwiają kontrolę dostępu do poszczególnych folderów oraz znajdujących się w nich plików i podfolderów. Jeśli zablokowane zostanie uprawnienie do pliku, znajdującego się w folderze, dla którego dane uprawnienie jest dozwolone, to atrybut Deny uprawnienia do pliku będzie miał pierwszeństwo nad atrybutem Allow uprawnienia do folderu.

Zamieszczona poniżej tabela przedstawia listę standardowych uprawnień do folderów w systemie NTFS wraz z opisem typu dostępu, na które zezwala każde z nich. Uprawnienia zostały przedstawione w kolejności od najbardziej do najmniej restrykcyjnego.

Uprawnienie do folderu w systemie NTFS	Pozwala użytkownikowi
Read	Przeglądać pliki i podfoldery danego folderu oraz informacje dotyczące jego właściciela, uprawnień oraz atrybutów, takich jak atrybuty Read-Only, Hidden, Archive, oraz System.
Write	Tworzyć nowe pliki i podfoldery w danym folderze, zmieniać atrybuty folderu oraz przeglądać informacje dotyczące jego właściciela i uprawnień.
List Folder Contents	Przeglądać nazwy plików i podfolderów.
Read & Execute	Przemieszczać się między folderami, w celu odnalezienia innych plików oraz wykonywać wszystkie czynności, które są dozwolone dla uprawnień Read oraz List Folder Contents.
Modify	Usunąć folder oraz wykonywać wszystkie czynności, dozwolone dla uprawnień Write i Read & Execute.
Full Control	Zmieniać uprawnienia, przejmować na własność, usuwać pliki i foldery oraz wykonywać wszystkie czynności, które są dozwolone dla pozostałych uprawnień do folderów w systemie NTFS.

Przeglądanie uprawnień do folderów

Administrator może przypisywać uprawnienia do folderu za pomocą karty **Security** okna dialogowego **Properties** danego folderu. Za pomocą tej karty można także sprawdzić aktualne ustawienia uprawnień do folderów.

Aby uzyskać dostęp do karty Security, należy:

1. W oknie Windows Explorer kliknąć prawym przyciskiem myszy wybrany plik.
2. Z podręcznego menu wybrać pozycję **Properties**.
3. W oknie dialogowym **Properties** wybrać kartę **Security**.

Karta **Security** składa się z dwóch sekcji—Name oraz Permissions. W sekcji Name wyświetlana jest lista użytkowników oraz grup, które posiadają uprawnienia do danego folderu. W sekcji Permissions wyświetlana jest lista uprawnień, które zostały przyznane lub zablokowane danemu użytkownikowi lub grupie.

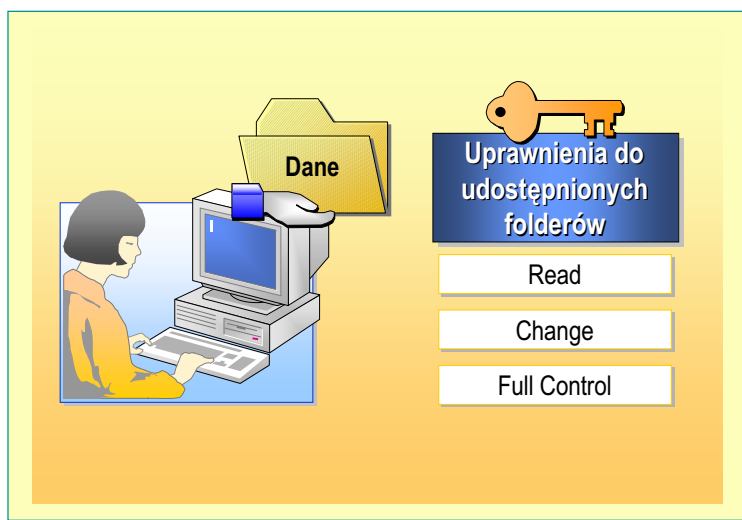
Uprawnienia do udostępnionych folderów

Cel slajdu

Opisanie uprawnień do udostępnionych folderów.

Wprowadzenie

Przyznając uprawnienia do udostępnionych folderów można umożliwić dostęp do zasobów sieciowych.

**Wskazówka**

Pokaż słuchaczom, w jaki sposób można przeglądać uprawnienia do udostępnionych folderów. Omawiając udostępnione foldery, nie powinieneś przedstawiać sposobu ustawiania uprawnień do nich.

Aby umożliwić wielu użytkownikom dostęp do tego samego zasobu, takiego jak folder, należy go udostępnić. Udostępnianie folderu jest to proces, na skutek którego dany folder staje się dostępny poprzez sieć dla wielu użytkowników w tym samym czasie. Po udostępnieniu folderu, użytkownicy mają dostęp do wszystkich plików i podfolderów znajdujących się w udostępnionym folderze, po warunkiem, że przyznane zostały im odpowiednie uprawnienia.

Udostępniać można tylko foldery, a nie pojedyncze pliki. Jeśli wielu użytkowników ma mieć zapewnioną możliwość dostępu do określonego pliku, należy umieścić ten plik w osobnym folderze, a następnie udostępnić cały folder.

Udostępnione foldery

Udostępnione foldery są zazwyczaj umieszczane na serwerze plików, jednak teoretycznie można umieścić je na każdym komputerze, znajdującym się w sieci. Pliki mogą być umieszczane w określonych udostępnionych folderach ze względu na ich kategorię lub funkcję. Na przykład, wszystkie pliki danych mogą zostać umieszczone w jednym folderze, a udostępnione pliki aplikacji w innym.

Poniżej przedstawione zostały niektóre właściwości udostępnionych folderów:

- Udostępnione foldery są wyróżniane w programie Microsoft Windows Explorer za pomocą ikony przedstawiającej rękę trzymającą folder.
- Uprawnienia można przypisywać tylko do całej zawartości folderu, a nie do pojedynczych plików lub podfolderów udostępnionego folderu
- Domyślnie, po udostępnieniu folderu, grupie Everyone przypisywane jest uprawnienie Full Control.

- Kiedy użytkownik zostaje dodany do listy osób posiadających uprawnienia do danego folderu, otrzymuje on domyślnie uprawnienie Read.
- Jeśli udostępniony folder zostanie skopiowany, oryginalny folder pozostanie udostępniony, ale jego kopia nie będzie udostępniana. Jeśli udostępniony folder zostaje przeniesiony w inne miejsce, przestaje on być udostępniany.

Stopień dostępu do udostępnionego folderu można kontrolować za pomocą uprawnień. Zamieszczona poniżej tabela przedstawia listę uprawnień do udostępnionych folderów wraz z opisem typu zadań, na wykonywanie których zezwala każde z nich.

Uprawnienie do udostępnionego folderu	Pozwala użytkownikowi
Read	Przeglądać nazwy folderów i plików, dane zgromadzone w plikach i ich atrybuty, uruchamiać pliki aplikacji oraz przemieszczać się w obrębie udostępnionego folderu.
Change	Tworzyć foldery, dodawać pliki do folderów, zmieniać dane w plikach, dodawać dane do plików, zmieniać atrybuty plików, usuwać foldery i pliki oraz wykonywać wszystkie czynności, które są dozwolone dla uprawnienia Read.
Full Control	Zmieniać uprawnienia do plików, przejmować pliki na własność oraz wykonywać wszystkie czynności, które są dozwolone dla uprawnienia Change.

Uwaga Uprawnienia do udostępnionych folderów mogą zostać przyznane lub zablokowane danemu użytkownikowi. Aby zablokować jakikolwiek dostęp do udostępnionego folderu, należy zablokować uprawnienie Full Control.

Sprawdzanie uprawnień do udostępnionych folderów

Po utworzeniu udostępnionego folderu, administrator może przypisywać uprawnienia do niego użytkownikom i grupom za pomocą okna dialogowego **Properties** danego folderu. Za pomocą tej karty można także sprawdzić aktualne ustawienia uprawnień do udostępnionych folderów.

Aby sprawdzić uprawnienia przypisane dla użytkowników lub grup do udostępnionego folderu, należy:

1. W oknie Windows Explorer kliknąć prawym przyciskiem myszy wybrany plik.
2. Z podręcznego menu wybrać pozycję **Properties**.
3. Na karcie **Sharing** okna dialogowego **Properties** wybrać przycisk **Permissions**.
4. Wybrać konto użytkownika lub grupę, której uprawnienia mają zostać sprawdzone.

Uprawnienia do drukarek

Cel slajdu

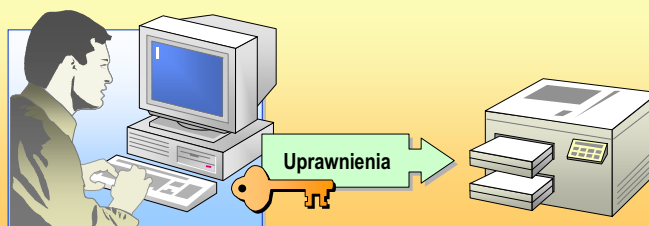
Opisanie trzech poziomów uprawnień do drukarek.

Wprowadzenie

Uprawnienia do drukarek można ustawić na jednym z trzech poziomów.

■ Trzy poziomy uprawnień do drukarek

- Print
- Manage Documents
- Manage Printers

**Wskazówka**

Przedstaw słuchaczom interfejs użytkownika, umożliwiający ustawienie uprawnień do drukarek.

Oprócz możliwości przypisywania uprawnień do udostępnionych folderów, administrator może także przypisywać uprawnienia do drukarek. Uprawnienia te są przypisywane użytkownikom, którzy nie są administratorami. Uprawnienia do drukarek pozwalają ustalić, jaki typ działań związanych z drukowaniem mogą wykonywać użytkownicy oraz pozwalają ograniczyć dostęp do wybranych drukarek z powodów związanych z bezpieczeństwem.

Poziomy uprawnień do drukarek

W systemie Windows 2000 uprawnienia do drukarek mogą zostać ustawione na jednym z trzech poziomów—Print, Manage Documents oraz Manage Printers.

Uprawnienie Print

Uprawnienie Print pozwala łączyć się z drukarką. Pozwala ono także drukować lub przerwać drukowanie własnych dokumentów.

Uprawnienie Manage Documents

Uprawnienie Manage Documents pozwala łączyć się z drukarką. Pozwala ono także zatrzymać, wznowić, rozpocząć od początku oraz przerwać wydruk wszystkich dokumentów.

Uprawnienie Manage Printers

Uprawnienie Manage Printers pozwala wykonywać wszystkie czynności, które są dozwolone dla uprawnień Print oraz Manage Documents. Dodatkowo uprawnienie to pozwala udostępniać drukarkę, zmieniać jej właściwości, usunąć ją oraz zmienić jej uprawnienia.

Sprawdzanie uprawnień do drukarek

Uprawnienia do drukarek mogą zostać przypisane indywidualnym użytkownikom lub grupom. Domyślnie system Windows 2000 przypisuje wbudowanej grupie Everyone uprawnienie Print dla każdej drukarki, umożliwiając w ten sposób wszystkim użytkownikom przesyłanie dokumentów na wszystkie drukarki. Administrator może jednak zmienić te uprawnienia, jeśli pewnym użytkownikom lub grupom należy uniemożliwić dostęp do danej drukarki. Na przykład, administrator może użytkownikom z działu marketingu ograniczyć dostęp do kolorowej drukarki. W takim przypadku domyślne uprawnienie, przyznawane grupie Everyone, powinno zostać usunięte, a następnie uprawnienie to należy nadać poszczególnym grupom, wyłączając grupę Marketing.

Aby sprawdzić ustawienia uprawnień do drukarek, należy:

1. W menu **Start** wskazać pozycję **Search**, a następnie kliknąć pozycję **For Printers**, co spowoduje wyświetlenie okna dialogowe **Find Printers**.
2. Na karcie **Printers** w polu **Name** wpisać nazwę drukarki, a następnie wybrać przycisk **Find Now**.
3. Kliknąć prawym przyciskiem myszy nazwę drukarki, a następnie z podręcznego menu wybrać pozycję **Properties**.
4. W oknie dialogowym **Properties** wybrać kartę **Security**. Za pomocą tej karty można sprawdzić ustawienia uprawnień do drukarki dla użytkowników i grup.

Laboratorium C: Badanie uprawnień do plików i folderów

Cel slajdu

Omówienie laboratorium.

Wprowadzenie

Realizacja tego laboratorium polega na zbadaniu uprawnień do plików i folderów.



Cele laboratorium

Po zrealizowaniu tego laboratorium słuchacz będzie potrafił:

- Opisać funkcję uprawnień do plików i folderów.

Wymagania wstępne

Przed rozpoczęciem tego laboratorium należy:

- Nauczyć się logować i wylogowywać z systemu Microsoft Windows 2000.

Przewidywany czas ukończenia laboratorium: 15 minut

Ćwiczenie 1

Badanie uprawnień do plików i folderów

Scenariusz

Chcesz sprawdzić, czy możesz tworzyć pliki w różnych folderach.

Cel

W tym ćwiczeniu zajmiesz się badaniem uprawnień do plików i folderów oraz sprawdzisz, jaki wpływ mają te uprawnienia na wykonywane codziennie zadania. Aby określić, do której grupy należą występujący w tym ćwiczeniu użytkownicy, możesz posłużyć się zamieszczoną poniżej tabelką.

Grupa	Użytkownicy w grupie
Sales	Don Hall Anne Paper
Managers	Jae Pak Kim Yoshida

Zadania	Szczegółowe kroki
1. Zaloguj się jako Kimyo, podając hasło password . W folderze C:\MOC\WIN2243A\labfiles\lab03\managers utwórz plik tekstowy o nazwie Meeting.txt.	a. Zaloguj się na komputerze, podając następujące dane: Username: kimyo Password: password Domain: <i>nazwa_domeny.nwtraders.msft</i> (gdzie zmienna <i>nazwa_domeny</i> określa domenę, do której chcesz się zalogować). b. Korzystając z programu Windows Explorer wyświetl zawartość folderu C:\moc\win2243a\labfiles\lab03\managers. c. Kliknij prawym przyciskiem myszy w dowolnym miejscu okna Managers , z podręcznego menu wybierz pozycję New , a następnie kliknij pozycję Text Document . d. Wpisz nazwę meeting , po czym naciśnij klawisz ENTER.
 Aby utworzyć plik w folderze Managers, musisz posiadać odpowiednie uprawnienia. Jakie uprawnienia powinien posiadać użytkownikowi Kimyo dla folderu Managers, aby mógł on utworzyć w nim plik? Uprawnienia Read oraz Write. 	
2. Sprawdź uprawnienia dla folderu C:\MOC\WIN2243A\labfiles\lab03\managers.	a. Korzystając z programu Windows Explorer wyświetl zawartość folderu C:\MOC\WIN2243A\labfiles\lab03. b. Kliknij prawym przyciskiem myszy folder Managers , a następnie z podręcznego menu wybierz pozycję Properties . c. Wybierz kartę Security .

(ciąg dalszy)

Zadania	Szczegółowe kroki
? Przyjrzyj się pozycjom znajdującym się na karcie Security. Czy są to pozycje dotyczące użytkowników czy też grup? Na jakiej podstawie można to stwierdzić? Pozycje dotyczą grup, co można stwierdzić na podstawie ich ikon.	
? Która z grup posiada uprawnienia typu Full Control? Czy użytkownik Kimyo jest członkiem tej grupy? Grupa Managers, której użytkownik Kimyo jest członkiem. Można to stwierdzić na podstawie tabeli, która została zamieszczona na początku tego ćwiczenia.	
2. (ciąg dalszy)	d. Wybierz przycisk Cancel, aby zamknąć okno Managers Properties.
3. Spróbuj utworzyć plik Meetings1.txt w folderze C:\MOC\WIN2243A\labfiles\lab03\sales.	a. Korzystając z programu Windows Explorer wyświetl zawartość folderu C:\MOC\WIN2243A\labfiles\lab03\sales. b. Kliknij prawym przyciskiem myszy w dowolnym miejscu okna Sales, z podręcznego menu wybierz pozycję New, a następnie kliknij pozycję Text Document.
? Czy użytkownik Kimyo może utworzyć plik w tym folderze? Jakie uprawnienia powinien posiadać użytkownikowi Kimyo dla folderu Sales, aby mógł on utworzyć w nim plik? Nie. Użytkownik Kimyo musiałby mieć przynajmniej uprawnienie Write, aby utworzyć plik w tym folderze.	
3. (ciąg dalszy)	c. Wybierz przycisk OK, aby zamknąć okno komunikatu Sales.
4. Sprawdź uprawnienia dla folderu C:\MOC\WIN2243A\labfiles\lab03\sales.	a. Korzystając z programu Windows Explorer wyświetl zawartość folderu C:\MOC\WIN2243A\labfiles\lab03. b. Kliknij prawym przyciskiem myszy folder Sales, a następnie z podręcznego menu wybierz pozycję Properties. c. Wybierz kartę Security. d. Kliknij pozycję Managers, znajdującą się na liście Name.

(ciąg dalszy)

Zadania	Szczegółowe kroki
? Jakie uprawnienia posiada grupa Managers dla folderu Sales? Uprawnienia Read & Execute, List Folder Contents oraz Read.	
? Jakie uprawnienia posiada grupa Sales dla folderu Sales? Uprawnienie Full Control.	
4. (ciąg dalszy)	e. Wybierz przycisk Cancel, aby zamknąć okno dialogowe Sales Properties. f. Zamknij wszystkie okna i wyloguj się.

Podsumowanie

Cel slajdu

Podsumowanie celów rozdziału poprzez przypomnienie zagadnień kluczowych.

Wprowadzenie

Pytania podsumowujące dotyczą głównych tematów omówionych w rozdziale.

- Konta użytkowników
- Grupy
- Prawa użytkownika
- Uprawnienia

1. Dział marketingu zatrudnił dwóch nowych pracowników. Administrator sieci musi utworzyć dla nich konta użytkowników tak, aby mogli oni korzystać z zasobów sieci, takich jak udostępnione foldery lub drukarki. Jakiego typu konto użytkownika powinni otrzymać nowi pracownicy?
 - a. Domenowe konto użytkownika.
 - b. Lokalne konto użytkownika.
 - c. Wbudowane konto Administrator.
 - d. Wbudowane konto Guest.

Poprawną odpowiedzią jest odpowiedź A. Dzięki domenowym kontom użytkowników, nowi pracownicy będą mogli uzyskiwać dostęp do zasobów w sieci. Gdyby otrzymali tylko konto na lokalnym komputerze, mogliby korzystać tylko z zasobów zgromadzonych na tym komputerze.

2. Administrator sieci zainstalował na komputerze system Windows 2000 Server. Za pomocą jakiego konta może uzyskać on dostęp do komputera, zanim utworzy dla siebie konto?
 - a. Domenowe konto użytkownika.
 - b. Lokalnego konta użytkownika.
 - c. Wbudowanego konta Administrator.
 - d. Wbudowanego konta Guest.

Poprawną odpowiedzią jest odpowiedź C. Po zainstalowaniu systemu dostępne są tylko dwa wbudowane konta—konto Administrator oraz konto Guest. Z tych dwóch kont, tylko konto Administrator ma odpowiednie prawa, umożliwiające zalogowanie się i zarządzanie komputerem.

3. Do grupy administratorów sieci dołączył nowy praktykant. Administrator sieci chce, aby praktykant był w stanie wykonywać wszystkie podstawowe zadania administracyjne w domenie, takie jak tworzenie i modyfikowanie kont użytkowników i grup użytkowników oraz udostępnianie zasobów. Nie chce on jednak, aby praktykant miał pełną kontrolę nad systemem. Praktykant nie powinien być w stanie zmieniać ustawień grupy Administrators oraz Backup Operators, ani zarządzać plikami dziennika systemu zabezpieczeń. W jaki sposób administrator może to osiągnąć? Zaznacz wszystkie poprawne odpowiedzi.
- a. Nadając odpowiednie prawa bezpośrednio praktykantowi.
 - b. Dodając praktykanta do wbudowanej grupy Power Users.
 - c. Dodając praktykanta do wbudowanej grupy Administrators.
 - d. Tworząc nową grupę i dodając do niej praktykanta, a następnie nadając tej grupie odpowiednie prawa.

Poprawne są odpowiedzi A oraz D. Administrator może nadać odpowiednie prawa bezpośrednio praktykantowi, lecz jeśli utworzona zostanie grupa, z przydzielonymi do niej odpowiednimi użytkownikami, a następnie nadane jej zostaną jednorazowo odpowiednie prawa, łatwiej będzie taką grupą później administrować. Grupa Power Users dostępna jest tylko na komputerach, które nie są kontrolerami domeny i w związku z tym nie daje żadnych praw w domenie, a tylko na lokalnym komputerze. Jeśli administrator doda praktykanta do grupy Administrators, to otrzyma on pełną kontrolę nad domeną.

4. W Twojej organizacji ma się odbyć coroczna inspekcja. W związku z tym kierownik działu finansów chce, aby określone, uprawnieni użytkownicy z jego działu mogli przeglądać arkusze bilansu finansowego organizacji. Dokumenty te znajdują się w folderze Bilans. Który z opisanych poniżej sposobów przydzielania uprawnień użytkownikom z działu finansów jest najlepszy?
- a. Przypisanie wszystkim użytkownikom z działu finansów uprawnień do tego folderu.
 - b. Przypisanie grupie Finanse, w skład której wchodzi wszyscy użytkownicy z działu finansów, uprawnień do tego folderu.
 - c. Przypisanie uprawnień poszczególnym użytkownikom z działu finansów.
 - d. Utworzenie grupy uprawnionych użytkowników. Grupie tej powinny zostać przypisane odpowiednie uprawnienia do tego folderu.

Poprawną odpowiedzią jest odpowiedź D. Ponieważ tylko niektórzy użytkownicy z działu finansów powinni mieć dostęp do tych informacji, administrator powinien utworzyć grupę, zawierającą tylko użytkowników, którym potrzebny jest dostęp i nadać im uprawnienia do tego folderu.

5. Użytkownicy w dziale produkcji bardzo często korzystają z informacji o produktach, znajdujących się w folderze, umieszczonym na serwerze. Folder ten zawiera także kilka aplikacji, z których użytkownicy czasami korzystają. Użytkownicy nie powinni jednak mieć możliwości modyfikowania plików, znajdujących się w tym folderze. Jakie uprawnienia powinny zostać przypisane temu folderowi?
- a. Read.
 - b. Read & Execute.
 - c. List Folder Contents.
 - d. Read & Write.

Poprawną odpowiedzią jest odpowiedź B. Chociaż każdy z podanych typów uprawnień umożliwia przeglądanie informacji, tylko uprawnienia Read & Execute pozwalają uruchamiać aplikacje, znajdujące się w danym folderze, uniemożliwiając jednocześnie dokonywanie jakichkolwiek zmian.

6. Administrator sieci chce, abyś zajął się administrowaniem kolorową drukarką, która została przyznana działowi sprzedaży. Jakie uprawnienia powinny zostać Tobie nadane, abyś mógł zarządzać wszystkimi drukowanymi dokumentami, jak również udostępniać drukarkę i zmieniać jej właściwości?
- a. Print.
 - b. Full Control.
 - c. Manage Documents.
 - d. Manage Printer.

Poprawną odpowiedzią jest odpowiedź D. Uprawnienie Manage Printer pozwala użytkownikowi wykonywać wszystkie wymagane czynności. Uprawnienie Print pozwala użytkownikowi tylko drukować dokumenty. Uprawnienie Manage Documents pozwala tylko wpływać na dokumenty, które znajdują się aktualnie w kolejce do druku. Uprawnienie Full Control nie jest dostępne dla drukarek.

7. Administrator sieci działu inżynierii chce ograniczyć wykorzystanie drukarki, która została zakupiona tylko dla tego działu. Co należy zrobić, aby tylko pracownicy z grupy Inżynierowie mogli korzystać z drukarki?
- a. Nadać uprawnienie Print wszystkim użytkownikom z działu inżynierii.
 - b. Nadać uprawnienie Print grupie Inżynierowie, zachowując domyślne uprawnienie grupy Everyone.
 - c. Usunąć domyślne uprawnienie Print grupy Everyone i przypisać je tylko grupie Inżynierowie.
 - d. Usunąć domyślne uprawnienie Print grupy Inżynierowie i przypisać je tylko grupie Everyone.

Poprawną odpowiedzią jest odpowiedź C. Domyślnie grupie Everyone nadawane jest uprawnienie Print. Administrator musi najpierw usunąć uprawnienie grupy Everyone i nadać je tylko tej grupie, która ma uzyskiwać dostęp do drukarki, czyli w tym przypadku grupie Inżynierowie.