Temat: Uprawnienia NTFS do plików i folderów oraz uprawnienia do udostępnionych zasobów

Cel Ogólny lekcji: Celem tej lekcji jest zdobycie przez uczniów wiedzy na temat zarządzania przydziałami dysku oraz kontroli dostępu do plików i folderów w systemie Windows Server. Uczniowie dowiedzą się, jak skutecznie konfigurować uprawnienia NTFS oraz korzystać z narzędzia File Server Resource Manager (FSRM) w celu ograniczania przestrzeni dyskowej, klasyfikacji plików oraz monitorowania zachowań użytkowników.

Cele szczegółowe: Po zakończeniu lekcji uczniowie powinni:

1. Rozumieć znaczenie zarządzania przydziałami dysku i kontroli dostępu w środowisku Windows Server.

2. Rozpoznawać różnice między uprawnieniami NTFS a uprawnieniami udostępniania oraz znać różne poziomy uprawnień NTFS.

3. Wiedzieć, jak konfigurować uprawnienia NTFS dla plików i folderów oraz zdolni do odróżnienia uprawnień specjalnych.

4. Rozumieć, czym są przydziały dyskowe dla domeny oraz dlaczego są one ważne w zarządzaniu przestrzenią dyskową w środowisku Windows Server.

5. Rozpoznawać różnicę między przydziałami dyskowymi dla domeny a przydziałami dyskowymi dla użytkownika domeny.

6. Wiedzieć, jak włączyć przydziały dyskowe na konkretnej partycji dyskowej.

7. Umieć ustawić domyślny poziom przydziału dysku dla wszystkich użytkowników na partycji oraz definiować poziomy ostrzeżeń dla przekroczenia limitu.

8. Potrafić konfigurować indywidualne przydziały dyskowe dla poszczególnych użytkowników w obrębie domeny.

9. Zrozumieć, że konfiguracja przydziałów dyskowych wymaga regularnego monitorowania i dostosowywania w zależności od potrzeb.

10. Znajdować i eksportować wpisy przydziałów dysku do pliku tekstowego oraz potrafić interpretować te wpisy.

11. Rozumieć rolę i funkcje File Server Resource Manager (FSRM) w systemie Windows Server.

12. Zrozumieć, jak FSRM umożliwia zarządzanie limitami, klasyfikacją plików, wykonywanie działań zgodnych z klasyfikacją oraz generowanie raportów dotyczących przechowywania.

13. Umieć wykorzystać FSRM do kontrolowania dostępu, blokowania niepożądanych plików i analizy wykorzystania przestrzeni dyskowej.

14. Prześledzić korzyści wynikające z korzystania z FSRM, takie jak zaawansowane zarządzanie przydziałami, ochrona przed naruszeniami praw autorskich oraz generowanie raportów dotyczących wykorzystania pamięci masowej.

Dzięki osiągnięciu tych celów ogólnych i szczegółowych, uczniowie zdobędą wiedzę i umiejętności potrzebne do efektywnego zarządzania przestrzenią dyskową oraz kontrolowania dostępu do plików i folderów w systemie Windows Server przy użyciu uprawnień NTFS i narzędzia FSRM.

A. **Uprawnienia NTFS do plików i folderów**

Ogólne przypomnienie wiadomości z klasy pierwszej:
Podstawy dot. uprawnień NTFS do plików i folderów oraz uprawnienia do udostępnionych zasobów dotyczące systemu lokalnego (Windows 10) były w klasie pierwszej.
Poniżej przedstawiłem elementy przypomnienia rozszerzonego o kolejne zagadnienia.

Prawa użytkownika

Prawa użytkownika to zezwolenia na wykonanie operacji na całym komputerze, np. logowanie się lub zmiana czasu. Prawa użytkownika są nadawane lub odbierane przez administratorów w ustawieniach zabezpieczeń komputera.

Prawo dostępu

Prawo dostępu to uprawnienie z punktu widzenia użytkownika lub grupy. Prawo dostępu jest zapisywane w liście DACL obiektu.

Uprawnienia

Uprawnienia to zezwolenia na wykonanie operacji na obiekcie, np. pliku lub folderze.

Uprawnienia są nadawane lub odbierane przez właściciela obiektu.

NTFS

NTFS to system plików w Windows, który daje możliwość kontroli dostępu do plików i folderów.

Uprawnienia NTFS

Uprawnienia NTFS pozwalają ustalić, kto i jak może korzystać z danych plików i folderów.
Uprawnienia NTFS do plików i folderów:

1. **Pełna kontrola**: Pozwala na odczyt, zapis, wykonanie i modyfikację plików oraz zmianę uprawnień i atrybutów pliku.
2. **Zmień i zapisz**: Umożliwia modyfikowanie pliku, ale nie zmianę uprawnień.
3. **Zapisz**: Umożliwia zapisywanie zmian w pliku, ale nie modyfikację istniejącej zawartości.
4. **Odczyt i wykonanie**: Pozwala na odczyt pliku i jego wykonanie (w przypadku plików wykonywalnych).
5. **Odczyt**: Umożliwia jedynie odczyt zawartości pliku.
6. **Brak dostępu**: Wyłącza dostęp do pliku lub folderu.

Uprawnienia specjalne w systemie plików NTFS

Uprawnienia specjalne NTFS to bardziej zaawansowane ustawienia, które pozwalają na precyzyjne kontrolowanie pewnych aspektów operacji na plikach i folderach. Te uprawnienia dają większą elastyczność w definiowaniu, jakie działania mogą być wykonywane przez użytkowników i grupy.

To uprawnienia, które dają więcej możliwości do zarządzania plikami i folderami. Można nimi ustawić dokładnie, co kto może robić z danym obiektem.

Pełna lista uprawnień specjalnych NTFS z opisem to:

1. **Przechodzenie przez folder/Wykonywanie pliku** - pozwala na przechodzenie przez podfoldery i wykonywanie plików wykonywalnych.
2. **Wyświetlenie zawartości folderu/Odczyt danych** - pozwala na wyświetlanie nazw plików i podfolderów oraz odczytywanie danych z plików.
3. **Odczyt atrybutów** - pozwala na odczytywanie atrybutów plików i folderów, takich jak ukryty, tylko do odczytu, itp.
4. **Odczyt rozszerzonych atrybutów** - pozwala na odczytywanie dodatkowych metadanych plików i folderów, takich jak autor, tytuł, itp.
5. **Tworzenie plików/Zapis danych** - pozwala na tworzenie nowych plików w folderze i zapisywanie danych do istniejących plików.
6. **Tworzenie folderów/Dołączanie danych** - pozwala na tworzenie nowych podfolderów w folderze i dołączanie danych na końcu istniejących plików.
7. **Zapis atrybutów** - pozwala na zmianę atrybutów plików i folderów.

8. **Zapis rozszerzonych atrybutów** - pozwala na zmianę dodatkowych metadanych plików i folderów.
9. **Usuwanie podfolderów i plików** - pozwala na usuwanie podfolderów i plików z folderu.
10. **Usuwanie** - pozwala na usuwanie pliku lub folderu.
11. **Odczyt uprawnień** - pozwala na odczytywanie listy uprawnień dla pliku lub folderu.
12. **Zmiana uprawnień** - pozwala na zmianę listy uprawnień dla pliku lub folderu.
13. **Przejęcie własności** - pozwala na przejęcie własności pliku lub folderu.

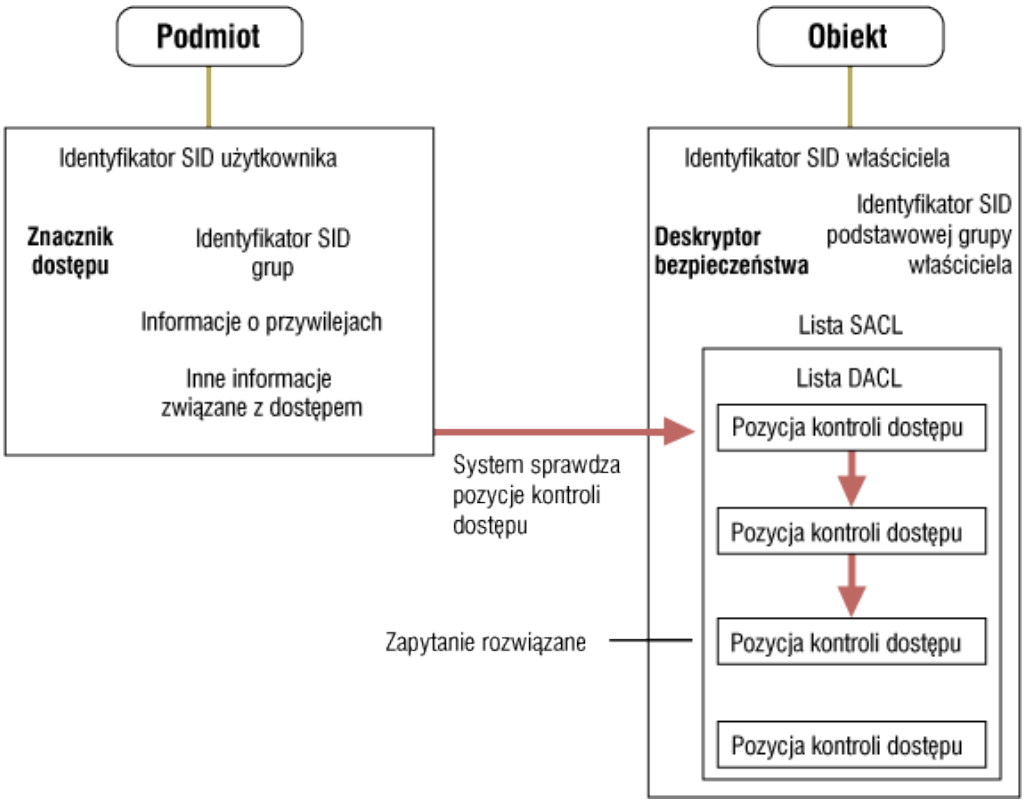
Uprawnienia specjalne pozwalają na dostosowanie kontroli dostępu do plików i folderów do bardziej zaawansowanych i specyficznych scenariuszy. Warto jednak zachować ostrożność przy ich użyciu, ponieważ niewłaściwe skonfigurowanie tych uprawnień może prowadzić do utraty dostępu do danych lub złamania zasad bezpieczeństwa.

Uprawnienia i deskryptory zabezpieczeń

Każdy obiekt w sieci ma deskryptor zabezpieczeń, który określa, kto może z nim robić co.
Deskryptor zabezpieczeń zawiera listę uprawnień dla różnych użytkowników i grup.
Uprawnienia to akcje, takie jak odczyt, zapis lub usuwanie.
Na przykład plik Temp.dat może mieć uprawnienia dla grupy Administratorzy i grupy Operatorzy kopii zapasowych.
Wpis kontroli dostępu to przypisanie uprawnień do użytkownika lub grupy.
Lista kontroli dostępu (ACL) to zbiór wpisów kontroli dostępu w deskryptorze zabezpieczeń.
Plik Temp.dat ma więc dwie listy kontroli dostępu - jedną dla grupy Administratorzy, a drugą dla grupy Operatorzy kopii zapasowych.

Deskryptory bezpieczeństwa

Deskryptor bezpieczeństwa to informacja o tym, kto jest właścicielem obiektu i kto ma do niego dostęp.
Obiekt to coś, co można zabezpieczyć, np. plik.
Deskryptor bezpieczeństwa ma listę DACL, która zawiera wpisy ACE.
Wpisy ACE określają, jakie uprawnienia mają użytkownicy i grupy do obiektu.
Gdy ktoś chce coś zrobić z obiektem, system sprawdza listę DACL i szuka wpisu ACE, który pasuje do użytkownika lub grupy. Jeśli znajdzie wpis ACE, który zezwala lub odmawia dostępu, to go stosuje.
Jeśli nie znajdzie takiego wpisu ACE, to zabrania dostępu do obiektu. Na rysunku pokazano ten proces.

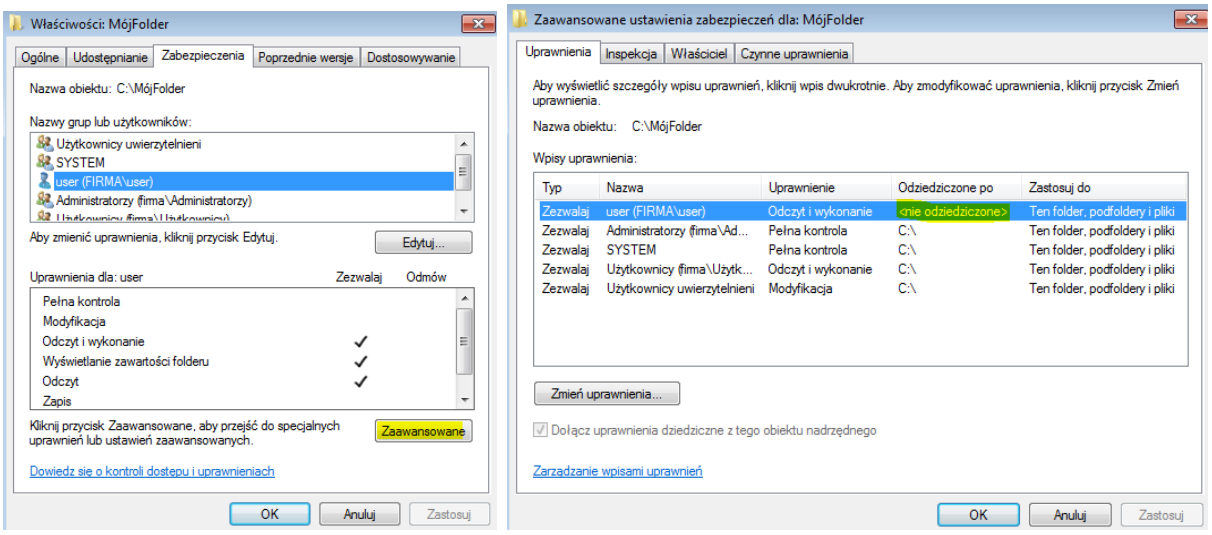


Uprawnienia jawne a dziedziczone

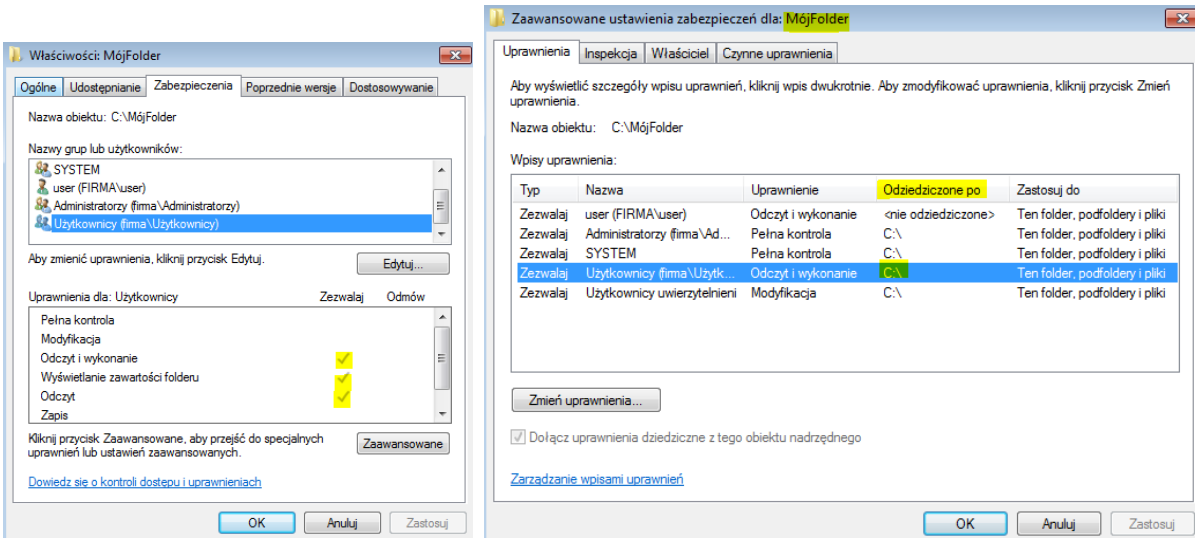
Uprawnienia to zasady, które określają, co można zrobić z plikami i folderami.

Uprawnienia mogą być jawne lub dziedziczone.

Jawne uprawnienia to te, które są ustawione ręcznie lub automatycznie przy tworzeniu pliku lub folderu.



Dziedziczone uprawnienia to te, które są kopiowane z folderu nadrzędnego do folderów i plików podrzędnych.



Dzięki dziedziczeniu uprawnienia można łatwiej zarządzać i utrzymywać spójność. Na przykład, jeśli utworzysz folder MójFolder z uprawnieniem everyone:read, to wszystkie podfoldery i pliki w nim będą miały to samo uprawnienie. Wtedy folder MójFolder ma uprawnienie jawne, a podfoldery i pliki mają uprawnienia dziedziczone.

Uprawnienia do plików i folderów

Uprawnienia to zasady, które określają, co można zrobić z plikami i folderami. Uprawnienia mogą być specjalne lub standardowe.

- Specjalne uprawnienia to szczegółowe uprawnienia, które można dostosować do konkretnych potrzeb.
- Standardowe uprawnienia to uproszczone uprawnienia, które obejmują kilka specjalnych uprawnień.

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

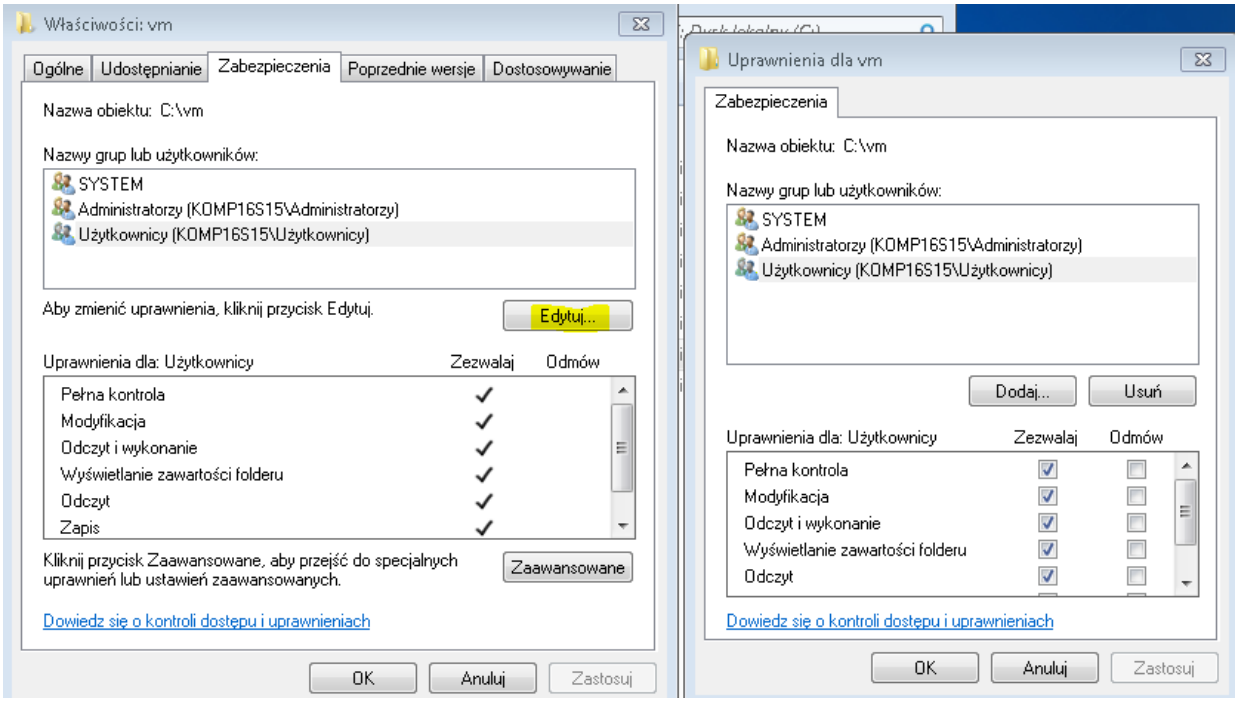
Zmiana uprawnień	X					
Przejęcie na własność	X					
Synchronizowanie	X	x	X	x	X	X

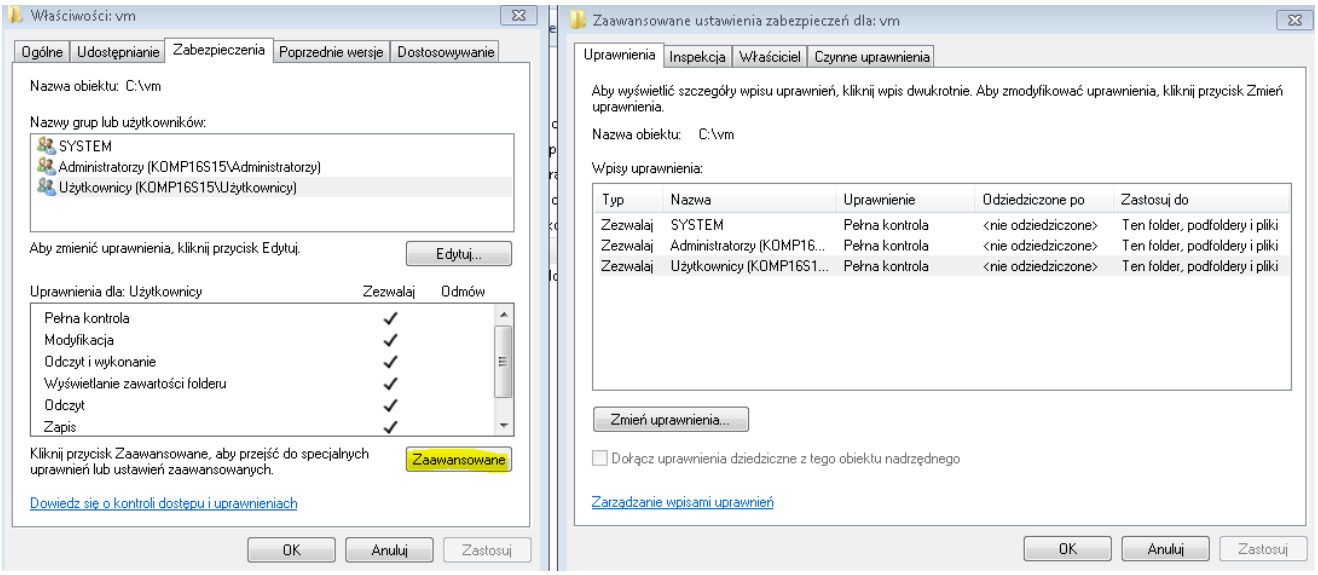
Uprawnienia można też podzielić na uprawnienia udziału i uprawnienia NTFS.

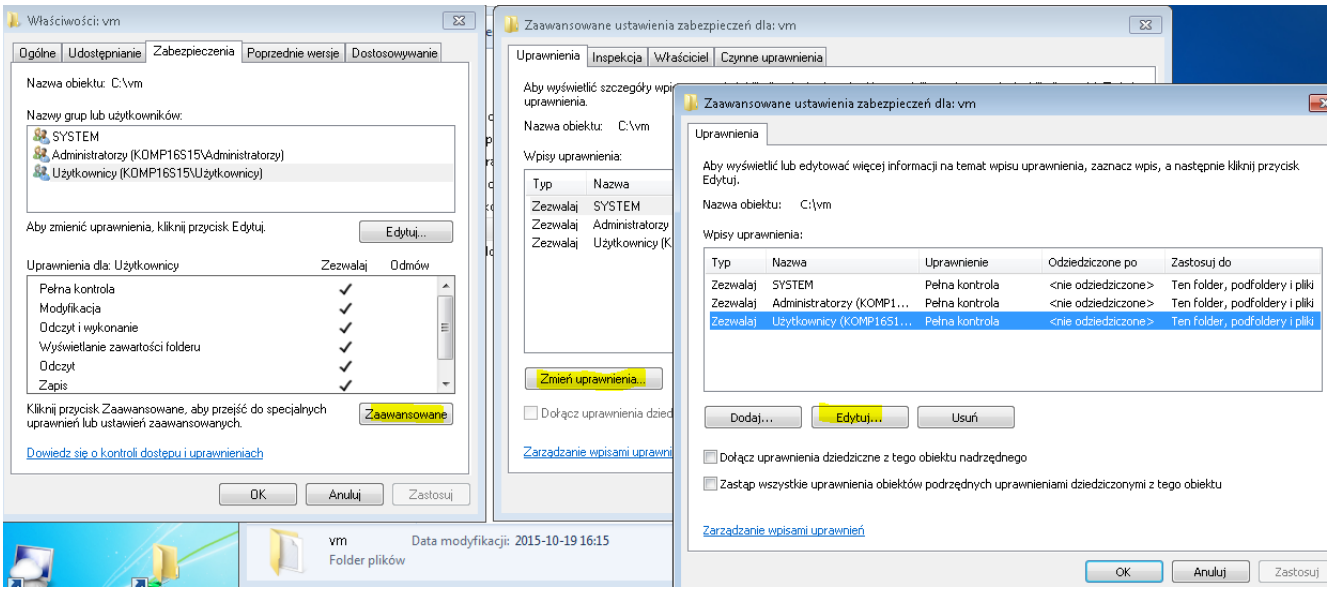
- Uprawnienia NTFS to te, które dotyczą dostępu do plików i folderów na dysku.
- Uprawnienia udziału to te, które dotyczą dostępu do folderów przez sieć.

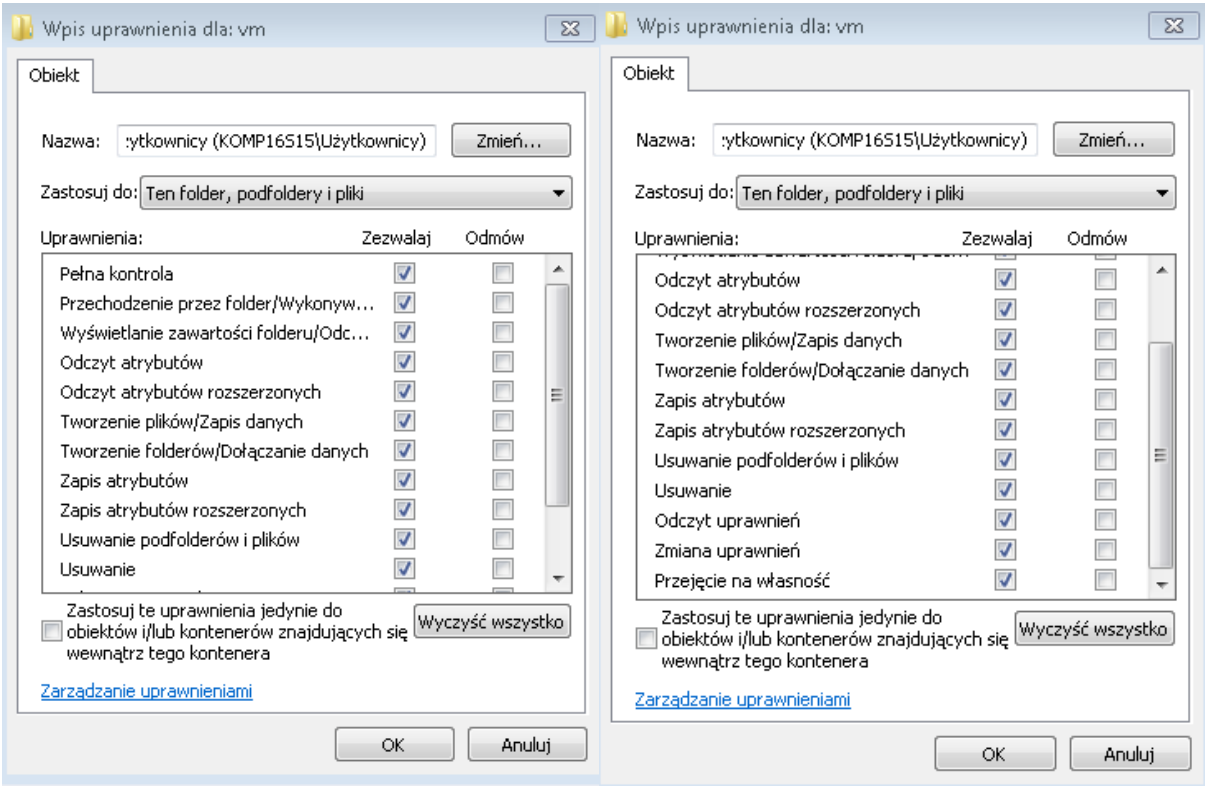
Ważne jest, żeby wiedzieć, że:

- Jeśli ktoś ma pełną kontrolę nad folderem, to może usuwać wszystkie pliki w nim, nawet jeśli mają one inne uprawnienia.
- Uprawnienie Wyświetlanie zawartości folderu dotyczy tylko folderów, a nie plików. Uprawnienie Odczyt i wykonanie dotyczą zarówno folderów, jak i plików.
- W tej wersji systemu Windows Server 2016, 2019, 2022 grupa Wszyscy nie obejmuje użytkowników anonimowych.




Właściwości: vm
Ogólne
Udostępnianie
Zabezpieczenia
Poprzednie wersje
Dostosowywanie
Nazwa obiektu: C:\vm
Nazwy grup lub użytkowników:
SYSTEM
Administratorzy (KOMP16S15\Administratorzy)
Użytkownicy (KOMP16S15\Użytkownicy)
Aby zmienić uprawnienia, kliknij przycisk Edytuj.
Edytuj...
Uprawnienia dla: Użytkownicy
Zezwalaj
Odmów
Pełna kontrola
Modyfikacja
Odczyt i wykonanie
Wyświetlanie zawartości folderu
Odczyt
Zapis
Kliknij przycisk Zaawansowane, aby przejść do specjalnych uprawnień lub ustawień zaawansowanych.
Zaawansowane
Dowiedz się o kontroli dostępu i uprawnieniach
OK
Anuluj
Zastosuj
Zaawansowane ustawienia zabezpieczeń dla: vm
Uprawnienia
Inspekcja
Właściciel
Czynne uprawnienia
Aby wyświetlić szczegóły wpisu uprawnień, kliknij wpis dwukrotnie. Aby zmodyfikować uprawnienia, kliknij przycisk Zmień uprawnienia.
Nazwa obiektu: C:\vm
Wpisy uprawnienia:
Typ
Nazwa
Uprawnienie
Odziedziczone po
Zastosuj do
Zezwalaj SYSTEM Pełna kontrola <nie odziedziczone> Ten folder, podfoldery i pliki
Zezwalaj Administratorzy (KOMP16... Pełna kontrola <nie odziedziczone> Ten folder, podfoldery i pliki
Zezwalaj Użytkownicy (KOMP16S1... Pełna kontrola <nie odziedziczone> Ten folder, podfoldery i pliki
Zmień uprawnienia...
Dołącz uprawnienia dziedziczne z tego obiektu nadrzędnego
Zarządzanie wpisami uprawnień
OK
Anuluj
Zastosuj


Właściwości: vm
Zaawansowane ustawienia zabezpieczeń dla: vm
Zaawansowane ustawienia zabezpieczeń dla: vm
Uprawnienia
Aby wyświetlić lub edytować więcej informacji na temat wpisu uprawnienia, zaznacz wpis, a następnie kliknij przycisk Edytuj.
Nazwa obiektu: C:\vm
Wpisy uprawnienia:
Typ
Nazwa
Uprawnienie
Odziedziczone po
Zastosuj do
Zezwalaj SYSTEM Pełna kontrola <nie odziedziczone> Ten folder, podfoldery i pliki
Zezwalaj Administratorzy (KOMP1... Pełna kontrola <nie odziedziczone> Ten folder, podfoldery i pliki
Zezwalaj Użytkownicy (KOMP16S1... Pełna kontrola <nie odziedziczone> Ten folder, podfoldery i pliki
Dodaj...
Edytuj...
Usuń
Dołącz uprawnienia dziedziczne z tego obiektu nadrzędnego
Zastąp wszystkie uprawnienia obiektów podrzędnych uprawnieniami dziedziczonymi z tego obiektu
Zarządzanie wpisami uprawnień
OK
Anuluj
Zastosuj
vm
Data modyfikacji: 2015-10-19 16:15
Folder plików



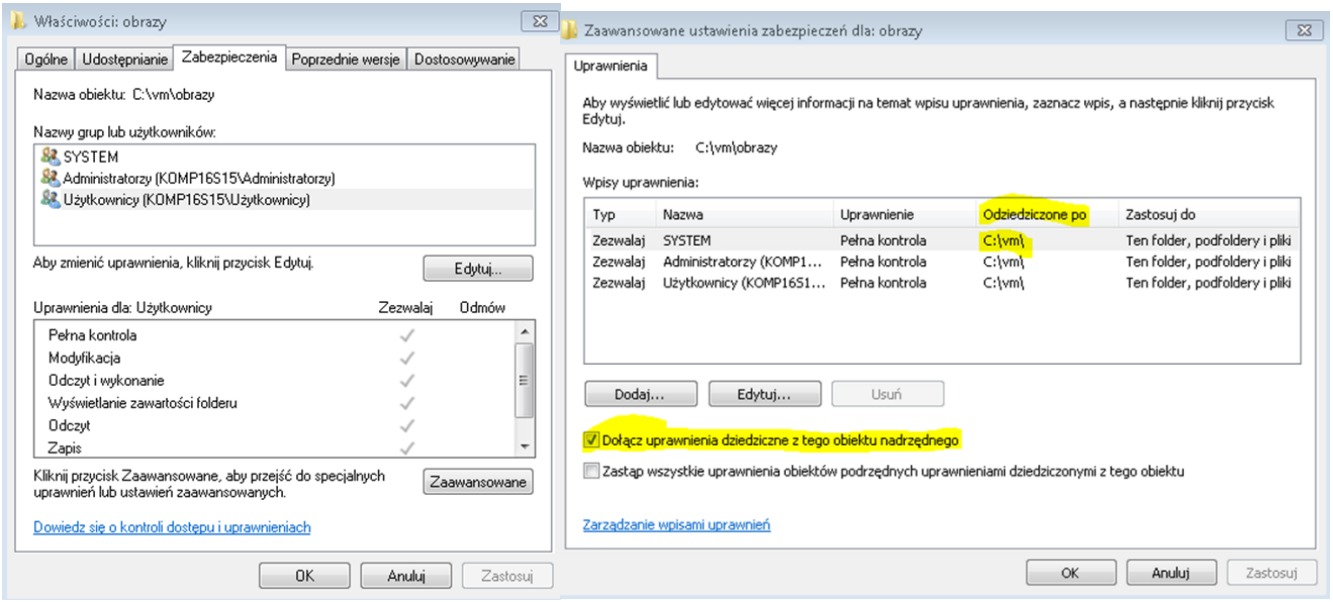
Uprawnienia dziedziczone

Uprawnienia dziedziczone to uprawnienia, które obiekt otrzymuje z folderu nadrzędnego. Ułatwiają one zarządzanie uprawnieniami i zapewniają spójność uprawnień w folderach i plikach. Możesz zmienić uprawnienia dziedziczone na trzy sposoby:

1. Zmień uprawnienia w folderze nadrzędnym - obiekt podrzędny dostosuje się do nich.
2. Zaznacz uprawnienie Zezwalaj, aby nadpisać uprawnienie Odmów.
3. Odznacz pole Dołącz uprawnienia dziedziczone z tego obiektu nadrzędnego. Wtedy możesz ustawić własne uprawnienia dla obiektu, ale nie będzie on dziedziczył uprawnień z folderu nadrzędnego.

Pamiętaj, że uprawnienia jawne mają wyższy priorytet niż uprawnienia dziedziczone. Jeśli widzisz zacienione pole Uprawnienia specjalne, to znaczy, że zostało ono zaznaczone.

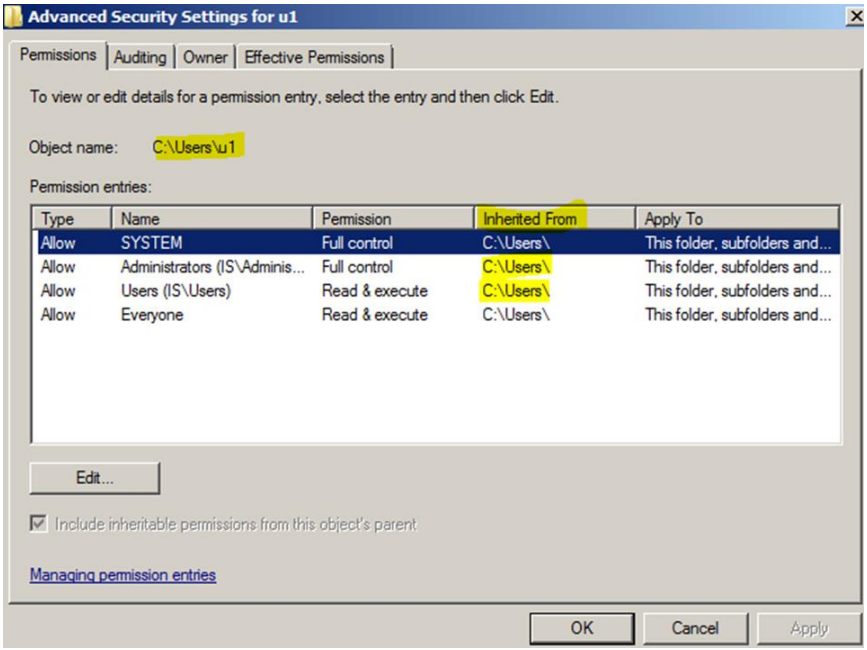
Na karcie Uprawnienia strony Zaawansowane ustawienia zabezpieczeń dla <folder> możesz zobaczyć, jakie uprawnienia są nadane dla folderów i podfolderów. Możesz też zmienić te uprawnienia w polu Zastosuj do na stronie Wpis uprawnienia dla <folder>. Kolumna Odziedziczone po pokazuje, skąd pochodzą uprawnienia.



Dziedziczenie dla obiektów usługi Active Directory

Jeśli używasz opcji Zastosuj do, aby ustawić dziedziczenie uprawnień dla obiektów Active Directory, pamiętaj, że uprawnienia te będą dotyczyć nie tylko wybranych obiektów podrzędnych, ale też wszystkich innych obiektów podrzędnych. Te inne obiekty będą miały te same uprawnienia, ale nie będą ich wymuszały. Jeśli takich obiektów będzie dużo, to może to spowolnić sieć.

Aby uniknąć tego problemu, najlepiej nadać wszystkim obiektom podrzędnym takie same listy uprawnień (ACL). Wtedy Windows będzie przechowywał tylko jedną kopię tych list w Active Directory i nie będzie marnował miejsca ani czasu na powtarzanie tych samych danych. To poprawi wydajność sieci.



Sposób określania czynnych uprawnień

Na karcie Czynne uprawnienia strony właściwości Zaawansowane ustawienia zabezpieczeń możesz zobaczyć, jakie uprawnienia ma wybrana grupa lub użytkownik tylko dlatego, że należy do tej grupy. Czynne uprawnienia zależą od:

• Grup globalnych, do których należy użytkownik

• Grup lokalnych, do których należy użytkownik

• Uprawnień lokalnych, które ma użytkownik

• Przywilejów lokalnych, które ma użytkownik

• Grup uniwersalnych, do których należy użytkownik

Czynne uprawnienia nie zależą od:

• Niektórych specjalnych identyfikatorów zabezpieczeń (SID), takich jak Logowanie anonimowe, Interakcyjny czy System

• Uprawnień udostępniania, które mogą blokować dostęp do udziałów nawet jeśli uprawnienia NTFS na to pozwalają.

Czynniki nieużywane w przypadku obiektów, do których dostęp jest uzyskiwany zdalnie

Jeśli chcesz uzyskać dostęp do obiektu na innym komputerze, to nie będą się liczyć:

• Grupy lokalne, do których należysz na tym innym komputerze

• Przywileje lokalne, które masz na tym innym komputerze

• Uprawnienia udostępniania, które dotyczą tego obiektu

Czynne uprawnienia zależą tylko od tego, jakie grupy, przywileje i uprawnienia masz na swoim komputerze. Nie widać tego, co masz na komputerze zdalnym.

Pobieranie czynnych uprawnień

Aby zobaczyć, do jakich grup należysz, musisz mieć uprawnienie do odczytu tych informacji. Jeśli jesteś użytkownikiem lub grupą w domenie, musisz mieć uprawnienie do odczytu informacji o grupach w domenie. Uwaga Karta Czynne uprawnienia może pokazywać nieprawdziwe uprawnienia do zasobów w domenie, jeśli spełniony jest jeden z tych warunków:

• Uruchamiasz narzędzia administracyjne z innego komputera niż ten, na którym jest zasób.

• Używasz konta użytkownika z innej domeny niż ta, w której jest zasób.

Aby tego uniknąć, sprawdzaj czynne uprawnienia tylko na tym komputerze, na którym jest zasób i używaj konta użytkownika z tej samej domeny co zasób.

Oto kilka domyślnych uprawnień w domenie:

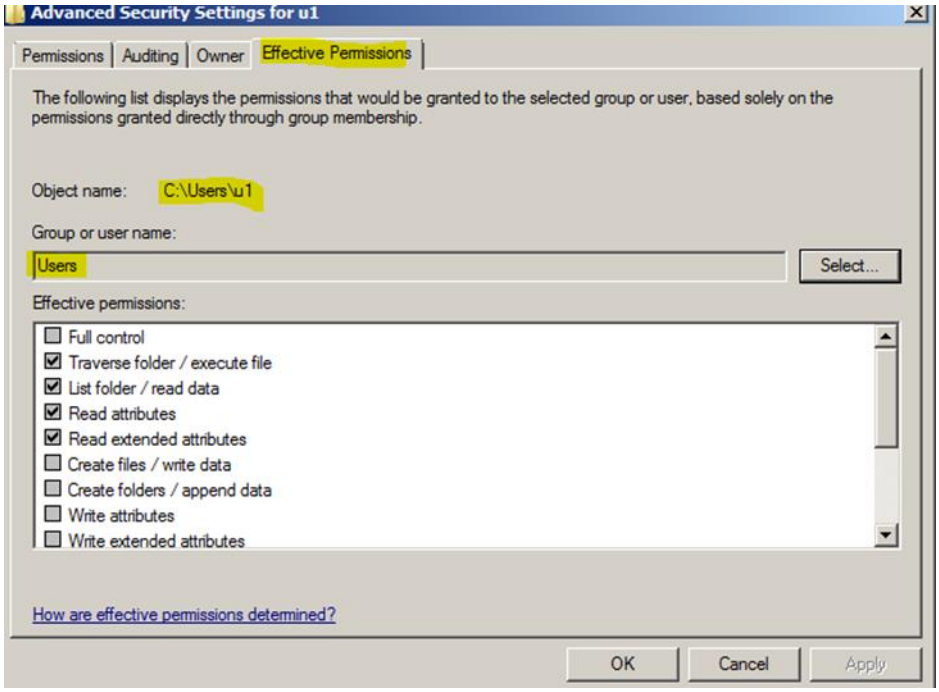
• Administratorzy domeny mogą zobaczyć, do jakich grup należą wszyscy użytkownicy i grupy.

• Administratorzy lokalni na komputerach niepodłączonych do domeny nie mogą zobaczyć, do jakich grup należą użytkownicy domeny.

Narzędzie czynne uprawnienia

Narzędzie czynne uprawnienia pokazuje, jakie uprawnienia do obiektu ma użytkownik lub grupa. Liczy to na podstawie grup, do których należy użytkownik lub grupa i uprawnień odziedziczonych. Sprawdza wszystkie grupy domenowe i lokalne, w których jest użytkownik lub grupa.
Grupa Wszyscy jest zawsze brana pod uwagę, chyba że użytkownik lub grupa jest w grupie Logowanie anonimowe.
Uwaga Narzędzie Czynne uprawnienia nie pokazuje dokładnych uprawnień użytkownika. Uprawnienia mogą się zmieniać w zależności od tego, jak się loguje (sposób logowania) użytkownik. Narzędzie nie wie, jak się loguje, jeśli nie jest zalogowany. Dlatego narzędzie pokazuje tylko uprawnienia wybrane przez użytkownika lub grupę, a nie te, które ma po zalogowaniu.

Na przykład, jeśli użytkownik łączy się z tym komputerem przez udostępniony folder, to jest zalogowany jako sieć. Uprawnienia można dawać lub zabierać sieciom z numerem SID (identyfikatorem zabezpieczeń, Security ID), który ma podłączony użytkownik.
Wtedy użytkownik może mieć inne uprawnienia, gdy jest zalogowany na komputerze, a inne, gdy jest zalogowany przez sieć.



Określanie, gdzie stosować uprawnienia

Można ustawić szczegółowe uprawnienia do plików i folderów w oknie Wpis uprawnienia dla <nazwa obiektu>. Można tam wybrać, które obiekty zależne będą dostawać te same uprawnienia.
Aby otworzyć to okno, w interfejsie kontroli dostępu kliknij Zaawansowane. Na karcie Uprawnienia kliknij Edytuj. W oknie Wpis uprawnienia dla <nazwa obiektu> na karcie Obiekt w polu Zastosuj dla są miejsca, gdzie można dać uprawnienia. To zależy od tego, czy zaznaczono pole Zastosuj te uprawnienia jedynie dla obiektów i/lub kontenerów znajdujących się wewnątrz tego kontenera.

Uwaga W Active Directory nie tylko obiekty z pola Zastosuj dla dostają wpisy kontroli dostępu, ale wszystkie obiekty podrzędne dostają ich kopię. Obiekty podrzędne bez pola Zastosuj dla nie będą używać wpisu kontroli dostępu, którego kopię dostaną, ale jeśli jest dużo takich obiektów, to może spowolnić sieć

To pole wyboru jest domyślnie puste. W tabelach poniżej są szczegóły o tym, jak dziedziczyć uprawnienia:

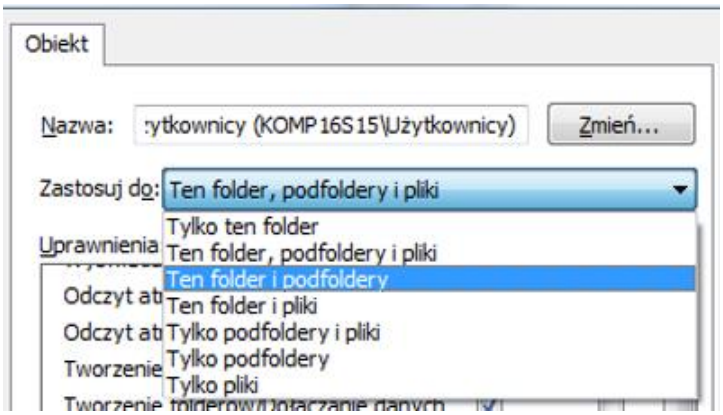
- Kiedy pole wyboru Zastosuj te uprawnienia jedynie dla obiektów i/lub kontenerów znajdujących się wewnątrz tego kontenera jest wyczyszczone

Zastosuj dla	**Stosuje uprawnienia do bieżącego folderu**	**Stosuje uprawnienia do podfolderów w bieżącym folderze**	**Stosuje uprawnienia do plików w bieżącym folderze**	**Stosuje uprawnienia do wszystkich kolejnych podfolderów**	**Stosuje uprawnienia do plików we wszystkich kolejnych podfolderach**

Tylko ten folder	x				
Ten folder, podfoldery i pliki	x	x	X	x	x
Ten folder i podfoldery	x	x		x	
Ten folder i pliki	x		X		x
Tylko podfoldery i pliki		x	X	x	x
Tylko podfoldery		x		x	
Tylko pliki			X		x

- Kiedy pole Zastosuj te uprawnienia jedynie dla obiektów i/lub kontenerów znajdujących się wewnątrz tego kontenera jest zaznaczone

Zastosuj dla	**Stosuje uprawnienia do bieżącego folderu**	**Stosuje uprawnienia do podfolderów w bieżącym folderze**	**Stosuje uprawnienia do plików w bieżącym folderze**	**Stosuje uprawnienia do wszystkich kolejnych podfolderów**	**Stosuje uprawnienia do plików we wszystkich kolejnych podfolderach**
Tylko ten folder	**x**				
Ten folder, podfoldery i pliki	**x**	**x**	**X**		
Ten folder i podfoldery	**x**	**x**			
Ten folder i pliki	**x**		**X**		
Tylko podfoldery i pliki		**x**	**X**		
Tylko podfoldery		**x**			
Tylko pliki			**X**		



Ustawianie, wyświetlanie, zmienianie lub usuwanie uprawnień do plików i folderów

Windows daje domyślne uprawnienia do nowych plików i folderów. Do tej procedury trzeba mieć uprawnienie Modyfikacja. Więcej informacji jest w sekcji „Uwagi dodatkowe". Aby ustawić, oglądać, zmieniać lub usuwać uprawnienia do plików i folderów

1. Kliknij prawym przyciskiem plik lub folder, kliknij Właściwości, a potem kartę Zabezpieczenia.
2. Kliknij Edytuj, aby otworzyć okno Uprawnienia dla <obiekt>.
3. Zrób jedno z tego:
   - Aby dodać grupę lub użytkownika, których nie ma w polu Nazwy grupy lub użytkownika, kliknij Dodaj. Wpisz nazwę grupy lub użytkownika i kliknij OK.
   - Aby zmienić lub usunąć uprawnienia grupy lub użytkownika, kliknij nazwę grupy lub użytkownika.
4. Zrób jedno z tego:
   - Aby dać lub zabrać uprawnienia, w polu Uprawnienia dla <użytkownik lub grupa> zaznacz Zezwalaj lub Odmów.
   - Aby usunąć grupę lub użytkownika z pola Nazwy grupy lub użytkownika, kliknij Usuń.

Uwagi dodatkowe

- Może być potrzebne podniesienie uprawnień użytkownika przez Kontrolę dostępu użytkownika.
- Aby otworzyć Eksploratora Windows, kliknij Start, Wszystkie programy, Akcesoria i Eksplorator Windows.
- Uprawnienia do plików i folderów można ustawiać tylko na dyskach NTFS.
- Aby zmienić uprawnienia, trzeba być właścicielem lub mieć uprawnienia od właściciela.
- Grupy lub użytkownicy z Pełną kontrolą nad folderem mogą usuwać pliki i podfoldery w nim, nawet jeśli mają inne uprawnienia.

- Jeśli pola wyboru w Uprawnienia dla <użytkownik lub grupa> są zacieniowane lub przycisk Usuń jest niedostępny, to znaczy, że plik lub folder ma uprawnienia z folderu wyżej.
- Dodani użytkownicy lub grupy mają domyślnie uprawnienia Odczyt i wykonanie, Wyświetlanie zawartości folderu i Odczyt.

Wyświetlanie czynnych uprawnień do plików i folderów

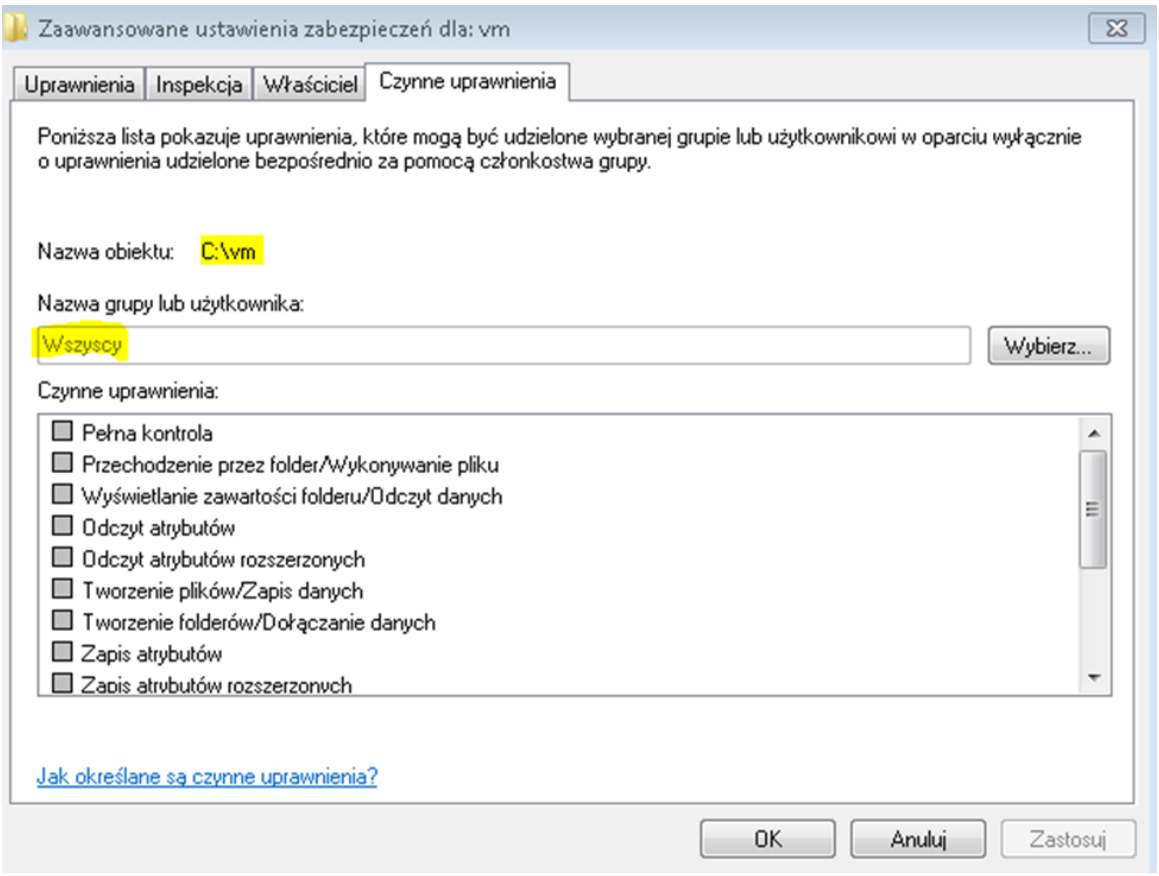
Windows daje domyślne uprawnienia do nowych plików i folderów. Twórca obiektu też może dać mu uprawnienia. Do oglądania czynnych uprawnień trzeba mieć uprawnienie Odczyt. Więcej informacji jest w sekcji „Uwagi dodatkowe". Aby oglądać czynne uprawnienia do plików i folderów

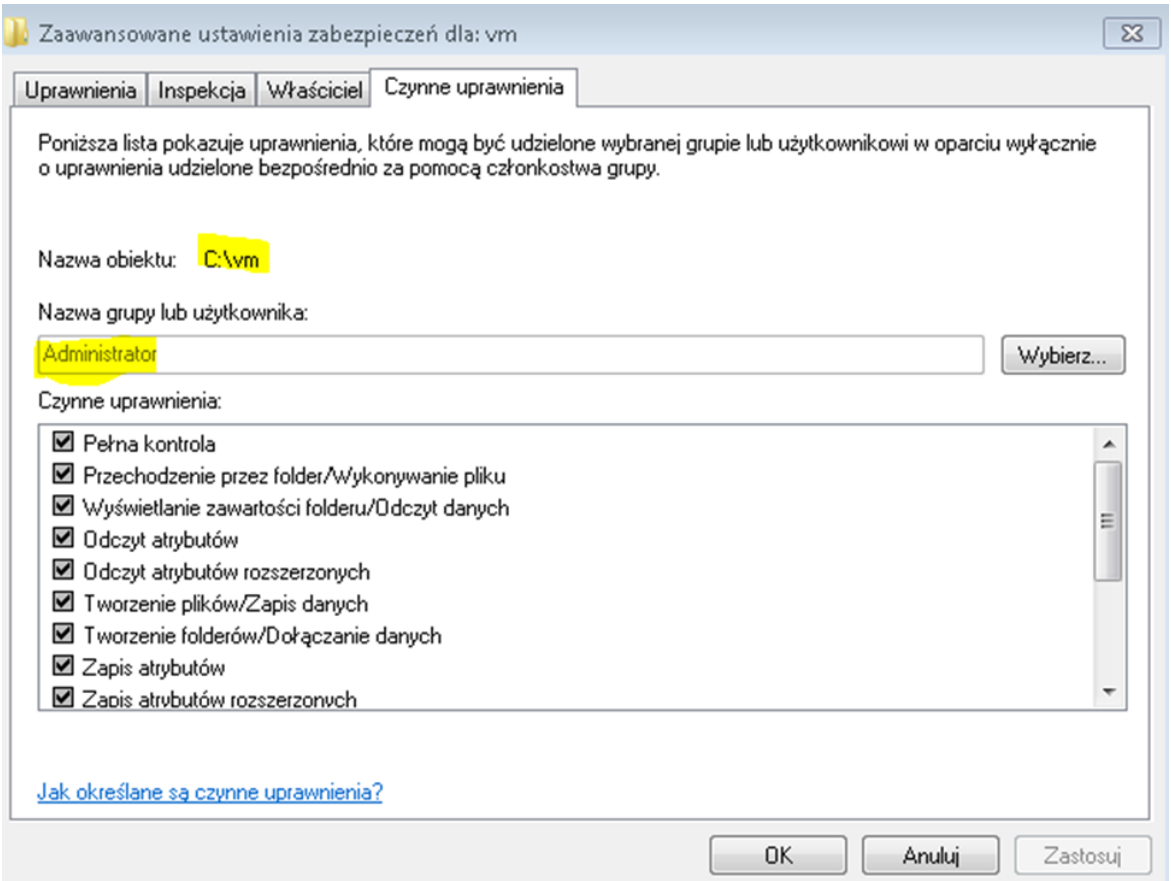
1. Otwórz Eksploratora Windows i znajdź plik lub folder, dla którego chcesz oglądać czynne uprawnienia.
2. Kliknij prawym przyciskiem plik lub folder, kliknij Właściwości, a potem kartę Zabezpieczenia.
3. Kliknij Zaawansowane, kliknij kartę Czynne uprawnienia i kliknij Wybierz.
4. W polu Wprowadź nazwę obiektu do wybrania wpisz nazwę użytkownika lub grupy i kliknij OK.

Zaznaczone pola wyboru pokazują czynne uprawnienia użytkownika lub grupy do tego pliku albo folderu.

Uwagi dodatkowe:

- Aby otworzyć Eksploratora Windows, kliknij Start, Wszystkie programy, Akcesoria i Eksplorator Windows.
- Jeśli grupa Wszyscy, Użytkownicy uwierzytelnieni lub Użytkownicy lokalni ma uprawnienia do obiektu, to czynne prawa będą je zawierać, chyba że użytkownik lub grupa jest anonimowy. W tej wersji Windows grupa Wszyscy nie ma użytkowników anonimowych.
- Karta Czynne uprawnienia pokazuje informacje obliczone z wpisów uprawnień. Informacje są tylko do odczytu i nie można zmieniać uprawnień użytkownika przez pola wyboru uprawnień.
- Uprawnienia można ustawiać tylko na dyskach NTFS.
- Uprawnienia udziału nie liczą się do czynnych uprawnień. Uprawnienia udziału mogą blokować dostęp do folderów udostępnianych, nawet jeśli uprawnienia NTFS na to pozwalają.


Zaawansowane ustawienia zabezpieczeń dla: vm
Uprawnienia
Inspekcja
Właściciel
Czynne uprawnienia
Poniższa lista pokazuje uprawnienia, które mogą być udzielone wybranej grupie lub użytkownikowi w oparciu wyłącznie o uprawnienia udzielone bezpośrednio za pomocą członkostwa grupy.
Nazwa obiektu: C:\vm
Nazwa grupy lub użytkownika:
Wszyscy
Wybierz...
Czynne uprawnienia:
Pełna kontrola
Przechodzenie przez folder/Wykonywanie pliku
Wyświetlanie zawartości folderu/Odczyt danych
Odczyt atrybutów
Odczyt atrybutów rozszerzonych
Tworzenie plików/Zapis danych
Tworzenie folderów/Dołączanie danych
Zapis atrybutów
Zapis atrybutów rozszerzonych
Jak określane są czynne uprawnienia?
OK
Anuluj
Zastosuj


Zaawansowane ustawienia zabezpieczeń dla: vm
Uprawnienia
Inspekcja
Właściciel
Czynne uprawnienia
Poniższa lista pokazuje uprawnienia, które mogą być udzielone wybranej grupie lub użytkownikowi w oparciu wyłącznie o uprawnienia udzielone bezpośrednio za pomocą członkostwa grupy.
Nazwa obiektu: C:\vm
Nazwa grupy lub użytkownika:
Administrator
Wybierz...
Czynne uprawnienia:
Pełna kontrola
Przechodzenie przez folder/Wykonywanie pliku
Wyświetlanie zawartości folderu/Odczyt danych
Odczyt atrybutów
Odczyt atrybutów rozszerzonych
Tworzenie plików/Zapis danych
Tworzenie folderów/Dołączanie danych
Zapis atrybutów
Zapis atrybutów rozszerzonych
Jak określane są czynne uprawnienia?
OK
Anuluj
Zastosuj

Ustawianie, wyświetlanie, zmienianie lub usuwanie uprawnień specjalnych

Obiekty mają uprawnienia, które mogą ograniczać dostęp do nich. Te uprawnienia specjalne można zmieniać dla obiektów. Aby to zrobić, użytkownik musi być właścicielem obiektu lub mieć uprawnienie od właściciela. Więcej informacji jest w sekcji „Uwagi dodatkowe". Aby ustawić, oglądać, zmienić lub usunąć uprawnienia specjalne

1. Kliknij prawym przyciskiem obiekt, dla którego chcesz ustawić uprawnienia specjalne, kliknij Właściwości i kartę Zabezpieczenia.

2. Kliknij Zaawansowane i Zmiana uprawnień.

3. Na karcie Uprawnienia zrób jedną z tych czynności:

- Ustaw uprawnienia specjalne dla nowej grupy lub użytkownika
  Kliknij Dodaj. W polu Wprowadź nazwę obiektu do wybrania wpisz nazwę użytkownika lub grupy i kliknij OK.
- Oglądaj lub zmień uprawnienia specjalne dla grupy lub użytkownika.
  Kliknij nazwę grupy lub użytkownika i Edytuj.
- Usuń grupę lub użytkownika i ich uprawnienia specjalne.
  Kliknij nazwę grupy lub użytkownika i Usuń. Jeśli Usuń jest niedostępny, wyczyść pole Dołącz uprawnienia dziedziczne z tego obiektu nadrzędnego i kliknij Usuń.

Przestroga

Jeśli zaznaczysz pole Zastąp wszystkie uprawnienia obiektów podrzędnych uprawnieniami dziedziczonymi z tego obiektu, to uprawnienia podfolderów i plików będą takie same jak tego obiektu nadrzędnego.

4. W polu Uprawnienia zaznacz lub wyczyść pole Zezwalaj lub Odmów.

5. W polu Zastosuj dla zaznacz foldery lub podfoldery, do których chcesz dać te uprawnienia.

6. Jeśli nie chcesz, żeby podfoldery i pliki dziedziczyły te uprawnienia, wyczyść pole Zastosuj te uprawnienia jedynie dla obiektów i/lub kontenerów znajdujących się wewnątrz tego kontenera.

7. Kliknij OK i w oknie Zaawansowane ustawienia zabezpieczeń dla <NazwaObiektu> kliknij OK.

Uwagi dodatkowe

• Grupy lub użytkownicy z uprawnieniem Pełna kontrola do folderu mogą usuwać pliki i podfoldery w tym folderze bez względu na ich uprawnienia.

• Wykonanie tych czynności może wymagać podniesienia uprawnień użytkownika przez Kontrolę dostępu użytkownika.

• Aby otworzyć Eksploratora Windows, kliknij Start, Wszystkie programy, Akcesoria i Eksplorator Windows.

• Grupa Wszyscy nie ma już uprawnienia Logowanie anonimowe.

• Jeśli wyczyścisz pole Dołącz uprawnienia dziedziczne z tego obiektu nadrzędnego, to plik lub folder nie będzie dziedziczyć uprawnień po obiekcie nadrzędnym.

• Uprawnienia można ustawiać tylko na dyskach z systemem plików NTFS.

• Jeśli pola wyboru w Uprawnienia są zacieniowane, to uprawnienia są dziedziczone po folderze nadrzędnym.

B. Uprawnienia do udostępnionych zasobów

Uprawnienia do udostępnionych zasobów na serwerach Windows (2016, 2019, 2022) obejmują zarówno uprawnienia NTFS, jak i dodatkowe uprawnienia dotyczące udostępniania zasobów w sieci:

1. **Pełna kontrola**: Odpowiada pełnym uprawnieniom NTFS, umożliwiając kontrolę dostępu do plików i folderów oraz zmianę uprawnień udostępniania.

2. **Zmień i zapisz**: Podobne do uprawnień NTFS, pozwala na modyfikację zasobów, ale nie zmianę uprawnień udostępniania.

3. **Zapisz**: Umożliwia zapisywanie zmian w udostępnionych zasobach, ale nie zmianę uprawnień udostępniania.

4. **Odczyt i wykonanie**: Pozwala na odczyt plików i wykonanie programów z udostępnionych zasobów.

5. **Odczyt**: Umożliwia jedynie odczyt zawartości udostępnionych plików i folderów.

6. **Brak dostępu**: Wyłącza dostęp do udostępnionych zasobów.

7. **Uprawnienia specjalne**: W przypadku udostępniania zasobów można także określić specjalne uprawnienia, takie jak umożliwienie lub zabronienie tworzenia plików i folderów, usuwania ich czy zmiany atrybutów.

W serwerach Windows 2016, 2019 i 2022, proces zarządzania uprawnieniami do udostępnionych zasobów jest zbliżony, choć mogą występować pewne różnice w interfejsie użytkownika lub dodatkowych funkcjach w nowszych wersjach systemu.

Ważne jest, aby odpowiednio skonfigurować zarówno uprawnienia NTFS, jak i uprawnienia do udostępniania, aby zapewnić właściwą kontrolę dostępu do plików i folderów na serwerze Windows oraz w sieci.

Ustawianie uprawnień do zasobu udostępnionego

Zasobem udostępnionym jest zasób sieciowy, np. folder, plik, drukarka lub nazwane potoki. Może to być też zasób na serwerze dla użytkowników sieciowych. Gdy udostępniasz zasób, używasz uprawnień udziału zamiast uprawnień NTFS.

Ważne Uprawnienia udziału dotyczą tylko użytkowników przez sieć. Nie dotyczą użytkowników lokalnych, np. na serwerze terminali. Aby ograniczyć dostęp do obiektów użytkownikom lokalnym, ustaw odpowiednie uprawnienia NTFS na karcie Zabezpieczenia we Właściwościach obiektu.

Możesz ustawić uprawnienia do zasobu udostępnionego na dwa sposoby, w zależności od typu zasobu.

Ustawianie uprawnień do pliku lub folderu przez Kreator udostępniania plików

1. Prawym przyciskiem myszy kliknij plik lub folder i kliknij Udostępnij.
2. Wykonaj kroki Kreatora udostępniania plików, aby wybrać użytkowników i grupy, którym udostępniasz plik lub folder, i ustawić ich uprawnienia.

Aby ustawić uprawnienia do zasobu przez Eksploratora Windows

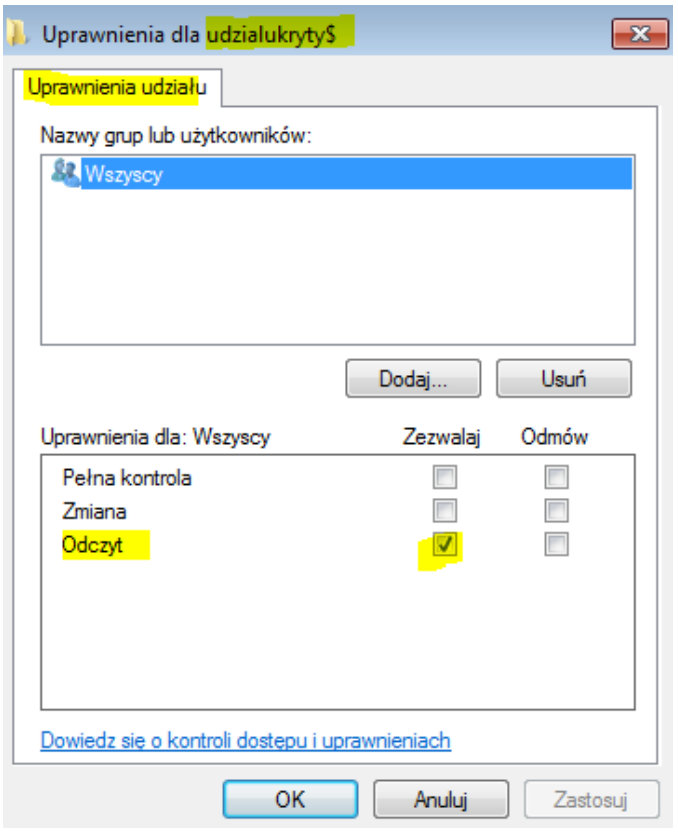
3. Otwórz Eksploratora Windows.
4. Prawym przyciskiem myszy kliknij obiekt i kliknij Udostępnij lub Właściwości.
5. Kliknij kartę Udostępnianie i przycisk Udostępnianie zaawansowane, aby ustawić uprawnienia.

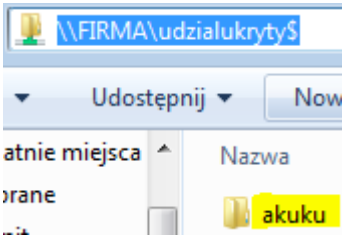
Uwagi dodatkowe

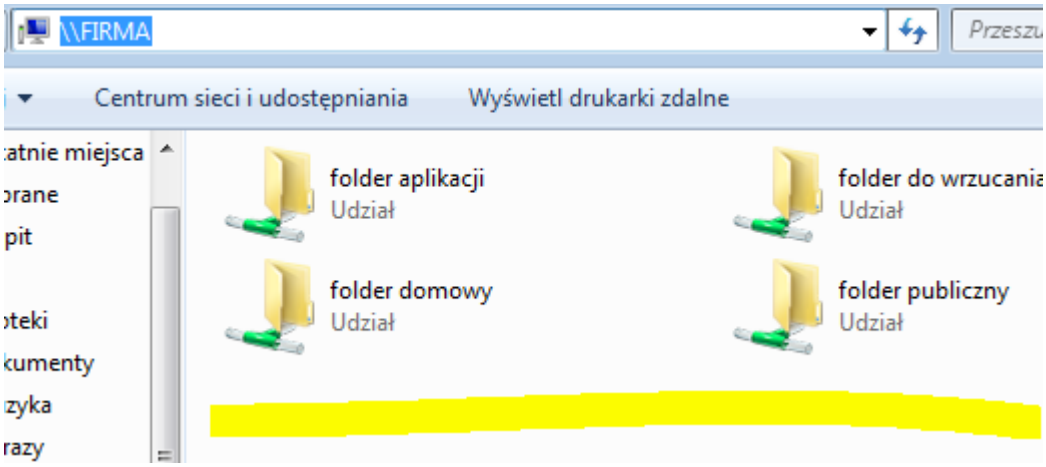
- Aby otworzyć Eksploratora Windows, kliknij Start, Wszystkie programy, Akcesoria i Eksplorator Windows.
- Kreator udostępniania plików pozwala zarządzać zasobami udostępnionymi na komputerach lokalnych i zdalnych. Eksplorator Windows i wiersz polecenia pozwalają zarządzać zasobami udostępnionymi tylko na komputerze lokalnym.
- Jeśli zasób udostępniony ma uprawnienia zarówno udziału, jak i systemu plików, obowiązuje uprawnienie bardziej restrykcyjne.

• Łatwiej jest przypisać uprawnienia do grup i dodać do nich użytkowników niż przypisywać te same uprawnienia wielu użytkownikom.

• Jeśli zmienisz uprawnienia do specjalnych zasobów udostępnionych, np. ADMIN$, możesz przywrócić ustawienia domyślne, zatrzymując i uruchamiając usługi serwera i ponownie uruchamiając komputer. To nie dotyczy zasobów udostępnionych utworzonych przez użytkowników, których nazwa udziału kończy się znakiem $ i są niewidoczne dla użytkowników sieci.







Uprawnienia udziału i uprawnienia NTFS na serwerze plików

Dostęp do folderu na serwerze plików zależy od dwóch rodzajów uprawnień: uprawnień udziału do folderu i uprawnień NTFS do folderu (i plików). Uprawnienia udziału są używane do zarządzania komputerami z systemem plików FAT32 lub innymi niż NTFS.

Uprawnienia udziału i NTFS nie wpływają na siebie. Ostateczne uprawnienia dostępu do folderu udostępnionego są określone przez połączenie uprawnień udziału i NTFS. Obowiązuje uprawnienie bardziej restrykcyjne.

W tabeli poniżej przedstawiono przykładowe uprawnienia, które administrator może dać grupie Użytkownicy do różnych typów folderów udostępnionych. Można też dać uprawnienie udziału Pełna kontrola dla grupy Wszyscy i ograniczać dostęp tylko przez uprawnienia NTFS.

Typ folderu	Uprawnienia udziału	Uprawnienia NTFS
Folder publiczny. Folder, do którego mają dostęp wszyscy.	Udziel uprawnienia Zmiana grupie Użytkownicy.	Udziel uprawnienia Modyfikacja grupie Użytkownicy.
Folder do wrzucania. Folder, w którym użytkownicy mogą zapisywać zrzut raportów poufnych lub zadania domowe, które może odczytać tylko menedżer grupy lub instruktor.	Udziel uprawnienia Zmiana grupie Użytkownicy. Udziel uprawnienia Pełna kontrola menedżerowi grupy.	Udziel uprawnienia Zapis grupie użytkowników, dla której zastosowano opcję **Tylko ten folder** (ta opcja jest dostępna na stronie **Zaawansowane**). Jeśli każdy użytkownik musi mieć określone uprawnienia do zrzuconych przez siebie plików, można utworzyć wpis uprawnienia dla dobrze znanego identyfikatora zabezpieczeń (SID, Security Identifier) twórcy-właściciela i zastosować dla niego opcję **Tylko podfoldery i pliki**. Można na przykład udzielić uprawnienia Odczyt i zapis do folderu do wrzucania identyfikatorowi SID twórcy-właściciela i zastosować to uprawnienie dla wszystkich podfolderów i plików. Dzięki temu użytkownik, który zrzucił lub utworzył plik (twórca-właściciel), może odczytywać zawartość pliku i zapisywać w nim dane. Twórca-właściciel może uzyskać dostęp do pliku za pomocą polecenia **Uruchom** z podaniem ścieżki *\\NazwaSerwera\FolderDoWrzucania\NazwaPliku*. Udziel uprawnienia Pełna kontrola menedżerowi grupy.
Folder aplikacji. Folder zawierający aplikacje, które można uruchamiać za pośrednictwem sieci.	Udziel uprawnienia Odczyt grupie Użytkownicy.	Udziel uprawnień Odczyt, Odczyt i wykonanie oraz Wyświetlanie zawartości folderu grupie Użytkownicy.
Folder domowy. Folder danego użytkownika. Tylko użytkownik ma dostęp do folderu.	Udziel uprawnienia Pełna kontrola do odpowiedniego folderu każdemu użytkownikowi.	Udziel uprawnienia Pełna kontrola do odpowiedniego folderu każdemu użytkownikowi.

Uwagi dodatkowe

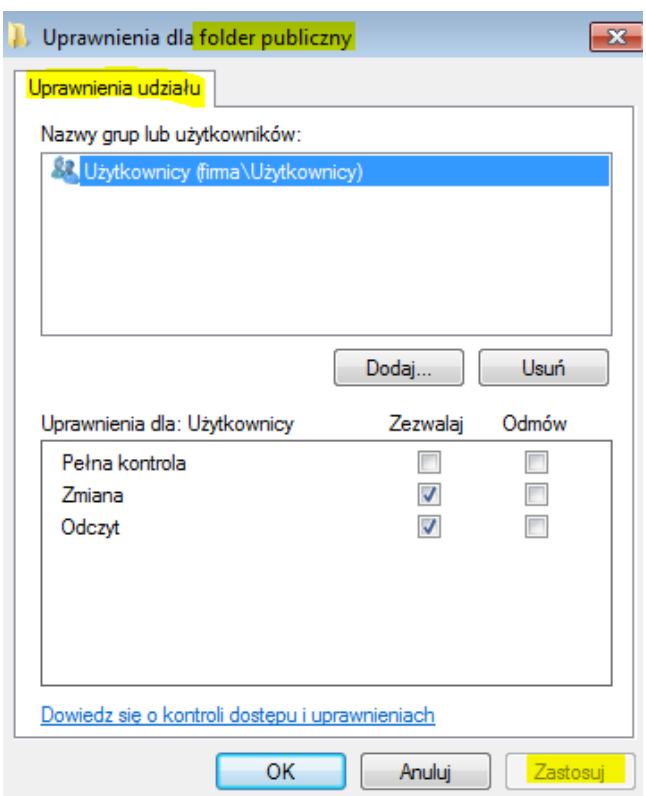
• Użytkownik z uprawnieniem NTFS Pełna kontrola do folderu może stać się właścicielem folderu, jeśli nie ma innych ograniczeń. Uprawnienia Pełna kontrola należy dawać ostrożnie.

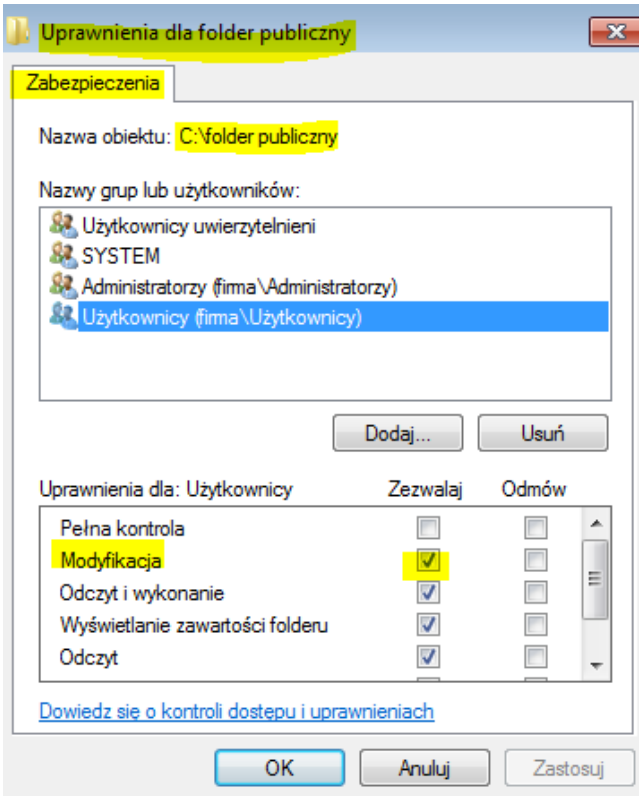
• Jeśli chcesz zarządzać dostępem do folderu tylko przez uprawnienia NTFS, daj grupie Wszyscy uprawnienie udziału Pełna kontrola.

• Uprawnienia NTFS dotyczą dostępu lokalnego i zdalnego. Uprawnienia NTFS działają niezależnie od protokołu. Uprawnienia udziału dotyczą tylko udziałów sieciowych. Uprawnienia udziału nie ograniczają dostępu lokalnego użytkowników komputera ani użytkowników serwera terminali, na którym są ustawione uprawnienia udziału. Dlatego uprawnienia udziału nie zapewniają poufności wielu użytkownikom tego samego komputera lub serwera terminali.

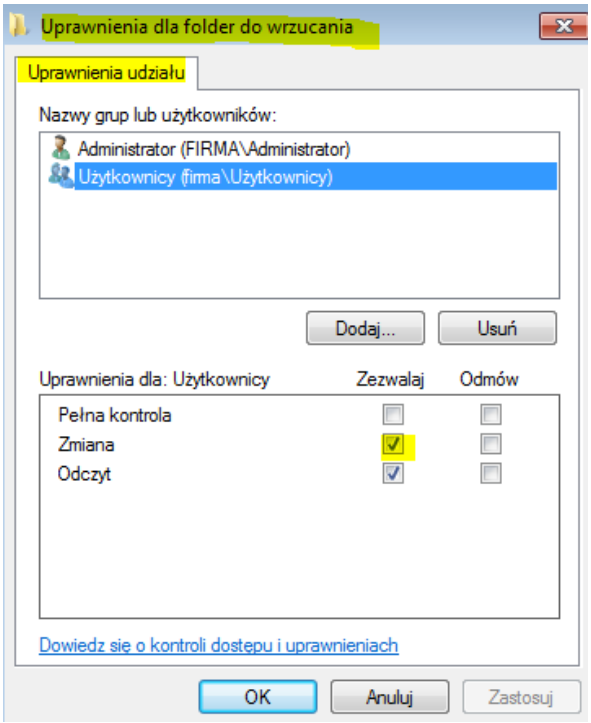
• Domyślnie grupa Wszyscy nie zawiera grupy użytkowników anonimowych, więc uprawnienia dane grupie Wszyscy nie dotyczą tej grupy.

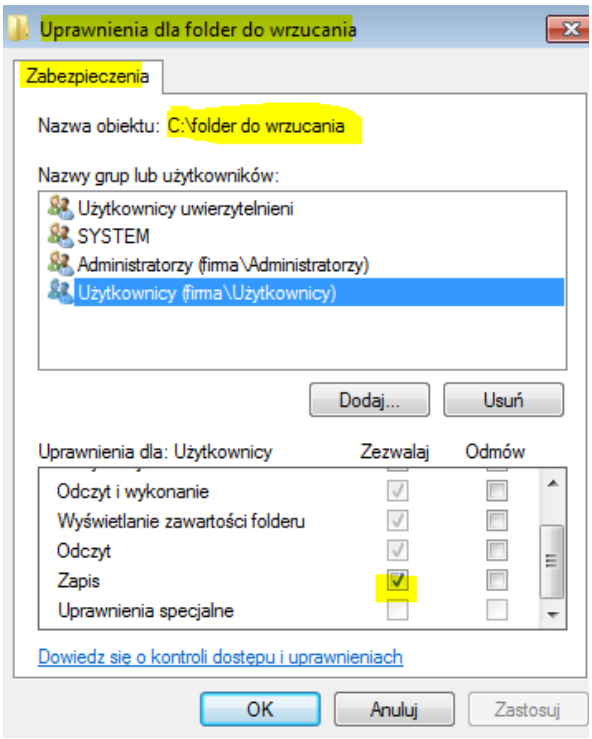
Folder publiczny.

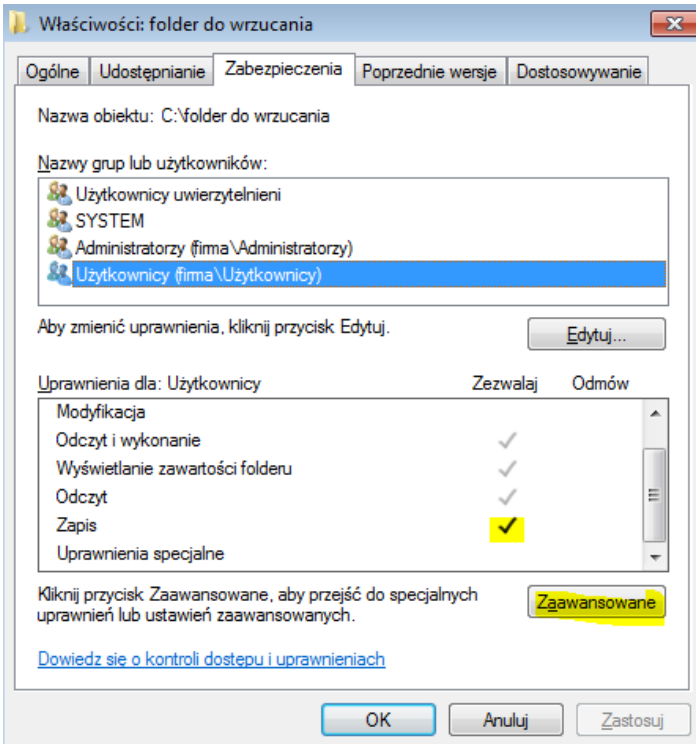


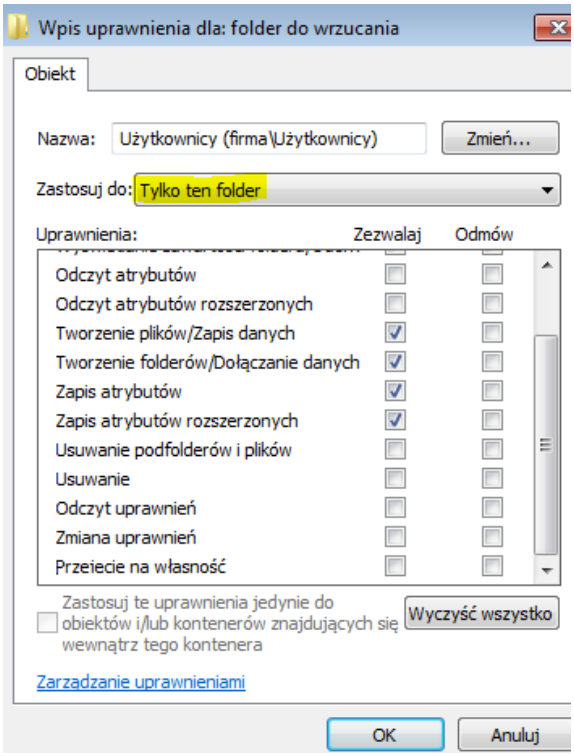


Folder do wrzucania.

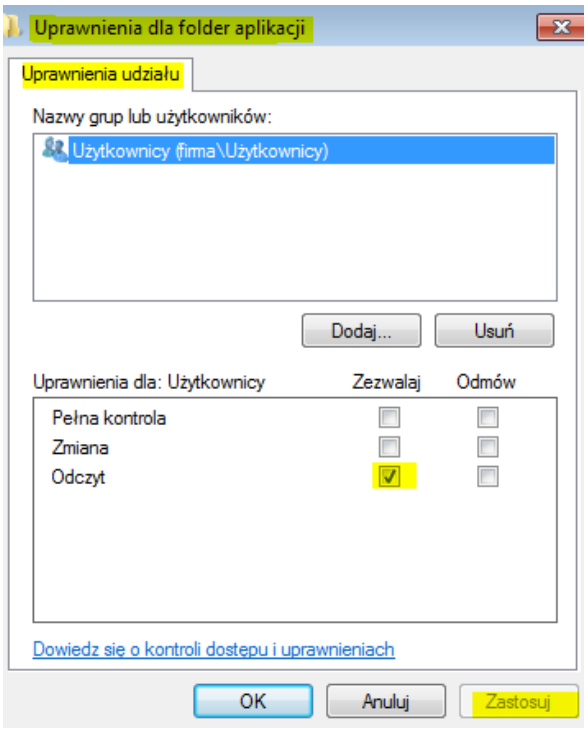




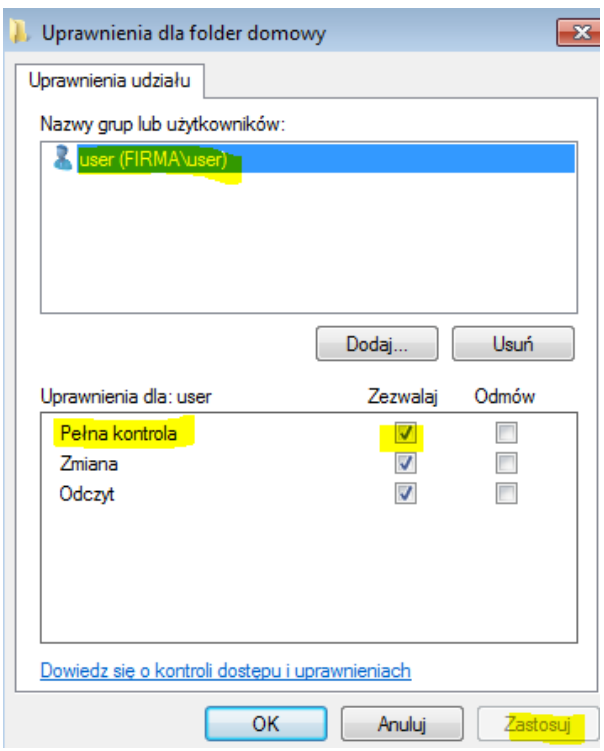


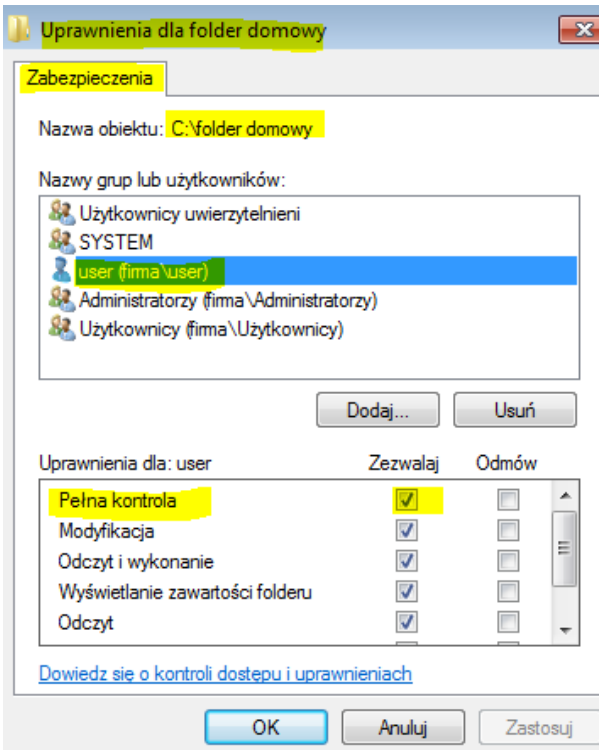


Folder aplikacji.



Folder domowy.





Niektóre z najlepszych praktyk dotyczących uprawnień specjalnych NTFS to:

- Zawsze używać uprawnień NTFS do zabezpieczania plików i folderów, nawet jeśli są one udostępnione w sieci.
- Zastosować zasadę najmniejszych przywilejów, czyli nadawać użytkownikom i grupom tylko te uprawnienia, które są im niezbędne do wykonywania swoich zadań.
- Unikać nadawania uprawnień specjalnych na poziomie plików, ponieważ może to spowodować problemy z dziedziczeniem i zarządzaniem uprawnieniami.
- Używać grup do nadawania uprawnień specjalnych, a nie poszczególnych użytkowników, ponieważ ułatwia to zarządzanie i zmiany uprawnień.

C. Przydziały dyskowe dla domeny:

Przydziały dyskowe dla domeny dotyczą ogólnych limitów, które można zastosować na poziomie partycji lub woluminu dostępnego dla wszystkich użytkowników w ramach tej domeny.

Umożliwia to kontrolowanie ogólnej ilości miejsca, które grupa użytkowników może wykorzystać na konkretnej partycji dyskowej.

a) Przydziały dyskowe dla użytkownika domeny:

Przydziały dyskowe dla użytkownika domeny pozwalają na indywidualne zarządzanie dostępną przestrzenią dyskową dla każdego użytkownika w obrębie danej domeny.

To oznacza, że można przypisać różne limity przestrzeni dyskowej dla różnych użytkowników, zapewniając równocześnie, że żaden użytkownik nie zajmie nadmiernie dużo miejsca.

b) Konfigurowania przydziałów dyskowych dla domeny, użytkownika domeny i eksportu wpisów przydziałów dysku do pliku:

Ogólne kroki konfigurowania przydziałów dyskowych dla domeny, użytkownika domeny i eksportu wpisów przydziałów dysku do pliku:

1. Włącz przydziały dyskowe na partycji dysku, na której chcesz je zastosować. Możesz to zrobić poprzez wykonanie następujących czynności:
    - Otwórz Eksplorator plików i przejdź do okna Ten komputer.
    - Kliknij prawym przyciskiem myszy na partycji dysku, na której chcesz włączyć przydziały dyskowe, i wybierz Właściwości z menu kontekstowego.

- W oknie Właściwości partycji kliknij zakładkę Przydziały dyskowe.
- Zaznacz pole wyboru Włącz przydziały dyskowe i kliknij przycisk Zastosuj lub OK.

2. Ustaw poziom domyślny przydziału dysku dla wszystkich użytkowników na partycji.
Możesz to zrobić poprzez wykonanie następujących czynności:

- W oknie Właściwości partycji kliknij przycisk Konfiguruj.
- W oknie Konfiguracja przydziałów dyskowych wpisz wartość w polu Ogranicz miejsce dyskowe do i wybierz jednostkę (KB, MB, GB lub TB) z listy rozwijanej. To jest maksymalna ilość miejsca na dysku, którą każdy użytkownik może zajmować na partycji.
- Wpisz wartość w polu Ustaw poziom ostrzeżenia do i wybierz jednostkę (KB, MB, GB lub TB) z listy rozwijanej. To jest ilość miejsca na dysku, po której osiągnięciu użytkownik otrzyma ostrzeżenie o przekroczeniu limitu.
- Kliknij przycisk Zastosuj lub OK.

3. Ustaw indywidualne przydziały dyskowych dla poszczególnych użytkowników domeny.
Możesz to zrobić poprzez wykonanie następujących czynności:

- W oknie Właściwości partycji kliknij przycisk Przydziały. Zobaczysz listę użytkowników i ich aktualne przydziały dyskowe na partycji.
- Aby dodać nowego użytkownika do listy, kliknij przycisk Nowy. W oknie Nowy wpis przydziału dysku wpisz nazwę użytkownika lub kliknij przycisk Znajdź, aby wyszukać użytkownika domeny. Następnie wpisz wartość w polu Ogranicz miejsce dyskowe do i wybierz jednostkę z listy rozwijanej. Możesz także wpisać wartość w polu Ustaw poziom ostrzeżenia do i wybierz jednostkę z listy rozwijanej. Kliknij przycisk OK, aby dodać użytkownika do listy.
- Aby edytować istniejącego użytkownika na liście, kliknij dwukrotnie na jego nazwę lub kliknij prawym przyciskiem myszy i wybierz Właściwości. W oknie Właściwości wpisu przydziału dysku zmień wartości w polach Ogranicz miejsce dyskowe do i Ustaw poziom ostrzeżenia do według potrzeb. Kliknij przycisk OK, aby zapisać zmiany.

4. Kroki eksportowania wpisów przydziałów dysku do pliku tekstowego:

- Otwórz Eksplorator plików i przejdź do okna Ten komputer.
- Kliknij prawym przyciskiem myszy na partycji dysku, z której chcesz wyeksportować wpisy przydziałów dysku, i wybierz Właściwości z menu kontekstowego.

- W oknie Właściwości partycji kliknij zakładkę Przydziały dyskowe.
- W oknie Przydziały dyskowych kliknij przycisk Przydziały. Zobaczysz listę użytkowników i ich aktualne przydziały dyskowe na partycji.
- Kliknij menu Narzędzia i wybierz opcję Eksportuj do pliku tekstowego. Zostanie otwarte okno dialogowe Eksportuj do pliku tekstowego.
- W polu Nazwa pliku wpisz nazwę pliku tekstowego, do którego chcesz wyeksportować wpisy przydziałów dysku. Możesz także kliknąć przycisk Przeglądaj, aby wybrać lokalizację zapisu pliku.
- W polu Separator wpisz znak, który chcesz użyć do oddzielania wartości w pliku tekstowym. Domyślnie jest to przecinek (,).
- Zaznacz lub odznacz pole wyboru Dołącz nagłówki kolumn, w zależności od tego, czy chcesz dodać nazwy kolumn do pliku tekstowego.
- Kliknij przycisk OK, aby rozpocząć eksportowanie wpisów przydziałów dysku do pliku tekstowego. Po zakończeniu procesu zostanie wyświetlone okno dialogowe Potwierdzenie eksportu.
- Kliknij przycisk OK, aby zamknąć okno dialogowe Potwierdzenie eksportu. Możesz teraz otworzyć plik tekstowy w dowolnym edytorze tekstu lub programie arkusza kalkulacyjnego.

Ważne uwagi:

- Przydziały dyskowe są przydatne, aby kontrolować wykorzystanie przestrzeni dyskowej, ale należy pamiętać, że mogą wymagać regularnego monitorowania i dostosowywania w miarę potrzeb.
- Dobre praktyki obejmują respektowanie potrzeb użytkowników i dostarczanie odpowiednich limitów, aby zapewnić, że żaden użytkownik nie będzie ograniczony nadmiernie.
- W środowiskach bardziej zaawansowanych, można także wykorzystać tzw. "pule dyskowe", które pozwalają na dynamiczne przydzielanie przestrzeni w miarę potrzeb.

Pamiętaj, że konfiguracja przydziałów dyskowych może różnić się w zależności od wersji systemu Windows Server oraz konkretnych wymagań i preferencji Twojej organizacji.

D. Zarządzanie przydziałami dysku w systemie Windows serwer

Zarządzanie przydziałem dysku to funkcja, która pozwala ograniczyć ilość miejsca na dysku, którą użytkownicy mogą wykorzystać na serwerze plików. Jeśli użytkownik przekroczy swój limit, nie może

zapisywać więcej plików na serwerze. Windows Server obsługują zarządzanie przydziałem dysku za pomocą File Server Resource Manager (FSRM), który jest rolą serwera w systemie Windows.

FSRM umożliwia nie tylko ustawianie limitów dla woluminów i folderów, ale także klasyfikowanie plików według ich zawartości i typu. Możesz też użyć FSRM do blokowania niepożądanych typów plików na serwerze plików.

1. Co to jest FSRM w systemie Windows Server?

FSRM to funkcja systemu Windows Server, która pomaga zarządzać danymi na serwerach plików. Działa w systemach Windows Server 2016, 2019 i 2022. Możesz ustawić limity dyskowe, blokować niepożądane pliki i sprawdzać użycie dysku. FSRM jest dostępny od systemu Windows Server 2003 R3. Jeśli chcesz przenieść dane na nowy serwer, możesz użyć usługi migracji pamięci masowej. Ta usługa działa ze wszystkimi serwerami od Windows Server 2003 do Server 2019 i kopiuję pliki do chmury lub Azure. Nie kopiuję jednak aplikacji, więc musisz je zainstalować ponownie.

2. Funkcje FSRM

FSRM ma pięć głównych funkcji, które są dostępne w systemach Windows Server 2016, 2019 i 20221. Są to:

1. Zarządzanie limitami: pozwala na ograniczanie rozmiaru folderów lub woluminów.
Możesz też tworzyć szablony limitów i stosować je do nowych folderów i woluminów.
2. Struktura klasyfikacji plików: pozwala na automatyczne lub ręczne klasyfikowanie plików według ich właściwości, takich jak data modyfikacji, lokalizacja lub typ pliku. Możesz też używać tej funkcji do zabezpieczania plików za pomocą dynamicznej kontroli dostępu lub szyfrowania.
3. Zadania związane z zarządzaniem plikami: pozwala na wykonywanie akcji lub polityk na plikach w zależności od ich klasyfikacji, takich jak przenoszenie, kopiowanie, usuwanie lub wysyłanie powiadomień.
4. Raporty dotyczące przechowywania: pozwala na monitorowanie użycia dysku, trendów klasyfikacji i nieautoryzowanych plików. Możesz generować raporty na żądanie lub według harmonogramu.
5. Konfiguracja pamięci masowej: pozwala na zarządzanie ustawieniami FSRM, takimi jak adres e-mail administratora, opcje raportowania i lokalizacja plików.

Uwaga: FSRM obsługuje tylko woluminy w formacie NTFS. Nie obsługuje elastycznych typów woluminów.
Jak pokażemy później, możesz konfigurować i zarządzać tymi funkcjami, które są dostarczane

z Menedżerem zasobów serwera plików, za pomocą aplikacji FSRM lub narzędzia Windows PowerShell.

6. Co możesz zrobić z FSRM

Możesz użyć FSRM do wykonania:

- Użyj dynamicznej kontroli dostępu do ograniczania dostępu do folderów i plików według ich klasyfikacji.
- Użyj zadania zarządzania plikami do usuwania plików, które nie były modyfikowane przez określony czas.
- Użyj szablonu limitu do ustawienia limitu 200 MB dla każdego użytkownika i wysłania powiadomienia, gdy wykorzystanie przestrzeni dyskowej przekroczy 180 MB.
- Użyj raportu dotyczącego przechowywania do sprawdzenia najczęściej otwieranych plików w ciągu ostatnich dwóch dni i zaplanuj go na niedzielę.
- Użyj zadania zarządzania plikami do blokowania lub usuwania plików muzycznych z osobistych folderów udostępnionych.
- Użyj reguły klasyfikacji plików do oznaczania plików z więcej niż dziesięcioma typami informacji jako posiadających informacje umożliwiające identyfikację.

7. Korzyści z FSRM

1. Obsługuje zaawansowane funkcje zarządzania przydziałami

Możesz użyć FSRM do zarządzania przydziałami na woluminach, folderach i plikach:

- FSRM ma konsolę do zarządzania przydziałami i powiadomieniami.
- FSRM pozwala na różne limity dla różnych ścieżek na tym samym woluminie.
- FSRM używa szablonów przydziału, które można łatwo zmieniać.
- FSRM obsługuje miękkie i twarde limity.

2. Reguluje zawartość serwera

Możesz użyć FSRM do filtrowania plików na serwerze i zapobiegania naruszeniom praw autorskich:

- FSRM pozwala na blokowanie lub monitorowanie plików o określonych rozszerzeniach na woluminach, folderach lub plikach.
- FSRM używa grup plików do definiowania typów plików do filtrowania.
- FSRM wysyła powiadomienia lub błędy, gdy użytkownik próbuje zapisać zablokowany plik.
- FSRM pomaga w ochronie danych i zgodności z prawem.

- FSRM pozwala na zezwalanie lub blokowanie plików wideo

3. Generuje raporty wykorzystania pamięci masowej

FSRM to usługa w Windows Server, która pozwala zarządzać i klasyfikować dane na serwerach plików. FSRM działa na Windows Server 2016, 2019 i 2022. FSRM może generować raporty o danych, takie jak:

- Lokalizacja, duplikaty i typy plików
- Data ostatniej modyfikacji i dostępu
- Właściwości plików i folderów
- Wykorzystanie limitu

FSRM pomaga efektywnie zarządzać zasobami pamięci masowej.

4. Łatwo lokalizuje pliki

FSRM pozwala wyszukiwać pliki według różnych kryteriów, takich jak:

- Właściwości plików
- Data modyfikacji, nazwa lub utworzenia
- Lokalizacja lub typ pliku
- FSRM ułatwia znalezienie plików na serwerze.

Źródła:

https://technet.microsoft.com/pl-pl/library/cc770962.aspx

http://old.zs.sztum.pl/naucz/1ti-so/17_uprawnienia_ntfs_i_listy_kontroli_dostepu_acl.pdf

https://soisk.info/index.php/Uprawnienia_NTFS_do_folder%C3%B3w_i_plik%C3%B3w

https://www.jakubkulikowski.pl/2021/04/14/uprawnienia-ntfs-w-systemach-windows/

https://admx.help/?Category=Windows_10_2016&Policy=Microsoft.Policies.DiskQuota::DQ_Limit&Language=pl-pl

https://www.centrumxp.pl/Zarzadzamy-przydzialami-dysku

https://pl.telusuri.info/articles/windows-server-2008/upravlenie-diskovimi-kvotami-v-windows-server-2008.html

https://learn.microsoft.com/en-us/windows-server/storage/fsrm/fsrm-overview

https://learn.microsoft.com/en-us/windows-server/storage/fsrm/quota-management

https://learn.microsoft.com/en-us/windows-server/storage/fsrm/classification-management

https://learn.microsoft.com/en-us/windows-server/storage/fsrm/file-screening-management

https://learn.microsoft.com/en-us/windows-server/storage/fsrm/checklist-apply-quota-to-volume-or-folder