

Uprawnienia (permissions) nadawane są w celu ochrony dostępu do konkretnych obiektów np.: plików, folderów, folderów udostępnionych, drukarek. Najczęściej przy ich pomocy regulujemy, kto i co może z danym zasobem zrobić, np. wybrana grupa użytkowników może zapisywać dane w określonym folderze albo drukować dokumenty na wskazanej drukarce.

Uprawnienia są cechą systemu NTFS (New Technology File System).

Rodzina systemów FAT (File Allocation Table) nie posiada takich możliwości.

Uprawnienia są realizowane poprzez utrzymywanie dla każdego obiektu (folderu i plików) tak zwanej Listy Kontroli Dostępu (Access Control List - ACL), zawierającej szereg wpisów (Access Control Entries), opisujących kto i co może w odniesieniu do danego zasobu zrobić.

System operacyjny podczas logowania użytkownika generuje dla niego tzw. żeton dostępu (access token), zawierający informacje o użytkowniku, grupach, do których należy oraz nadanych mu prawach systemowych.

Podczas każdej próby uzyskania dostępu do zasobu chronionego uprawnieniami system sprawdza, czy na Liście Kontroli Dostępu znajduje się odpowiedni wpis umożliwiający albo bezpośrednio użytkownikowi, albo którejś z grup, do których należy, wykonanie wybranej akcji.

Jeśli taki wpis istnieje, to użytkownik może akcję wykonać, jeśli nie to wyświetlany jest odpowiedni komunikat systemowy informujący o braku wystarczających uprawnień.

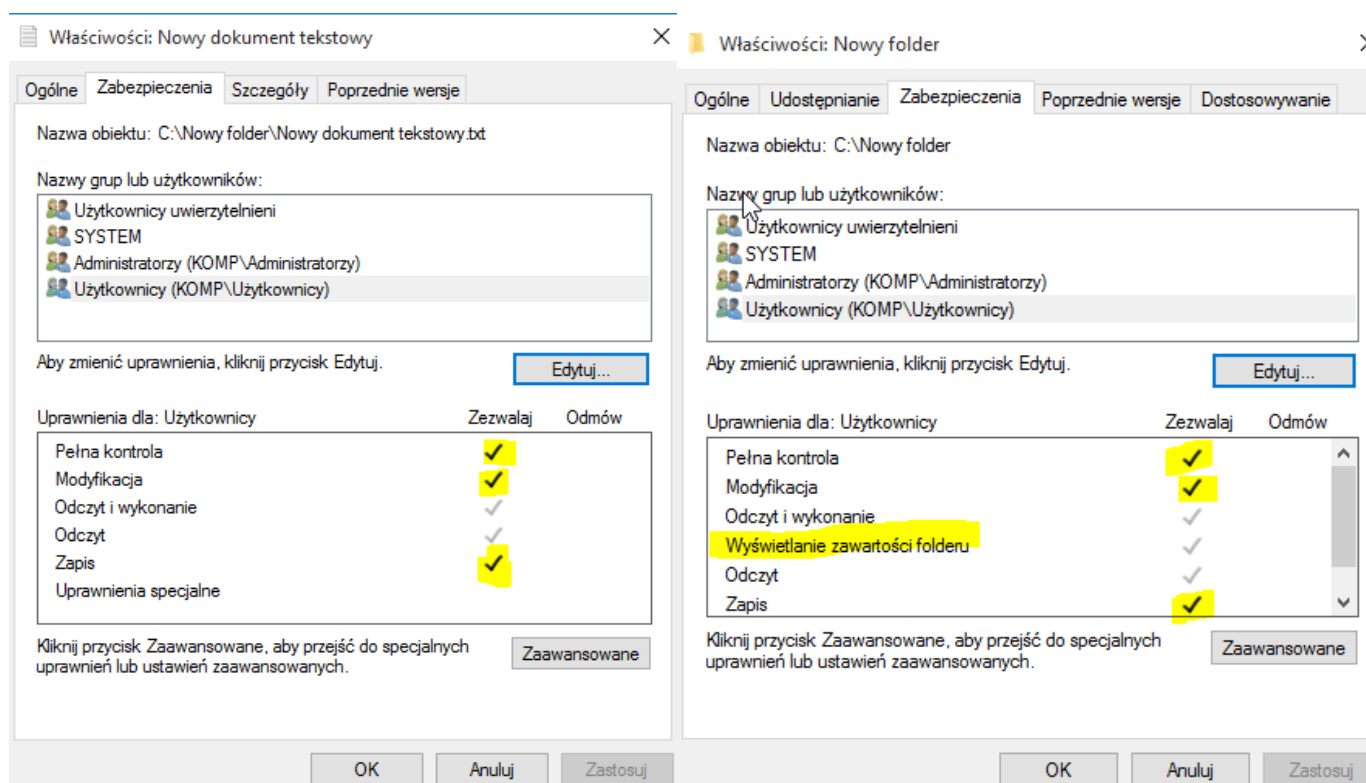
Rodzaje uprawnień:

- **Uprawnienia jawne** - dołączane bezpośrednio do obiektu lub jednostki organizacyjnej (OU), która może obejmować uprawnienia do plików i folderów (zrzut - czarne v).
- **Uprawnienia dziedziczone** - propagowane od obiektu nadrzędnego do obiektu podrzędnego (zrzut - szare v).

Uprawnienia: Zezwalaj i Odmów

Jeżeli użytkownik ma obydwa np. zezwolenie na odczyt oraz odmówienie odczytu to ważniejsze jest odmów - użytkownik nie ma prawa na czytanie pliku.

Jeżeli zezwalaj jest nadane jawnie, a odmów jest odziedziczone, to zezwalaj ma pierwszeństwo.



Pełna kontrola - umożliwia wykonywanie operacji wynikających ze wszystkich pozostałych uprawnień, a dodatkowo pozwala usuwać pliki i podkatalogi w danym folderze, zmieniać uprawnienia i przejmować pliki lub foldery na własność.

Modyfikacja - użytkownik może wykonywać wszystkie możliwe operacje oprócz dostępnych jako dodatkowe w przypadku pełnej kontroli, a więc bez usuwania plików i podkatalogów oraz bez zmiany uprawnień i przejmowania na własność.

Odczyt i wykonanie - składa się na nie możliwość wyświetlania zawartości folderu, odczytywanie danych, uprawnień, synchronizowanie, uruchamianie programów i przechodzenie przez folder. To ostatnie uprawnienie specjalne stosuje się wówczas, gdy użytkownik musi przejść przez szereg folderów nadrzędnych, aby dostać się do określonego pliku. Działanie tej funkcji zależy od ustawień zasad grup.

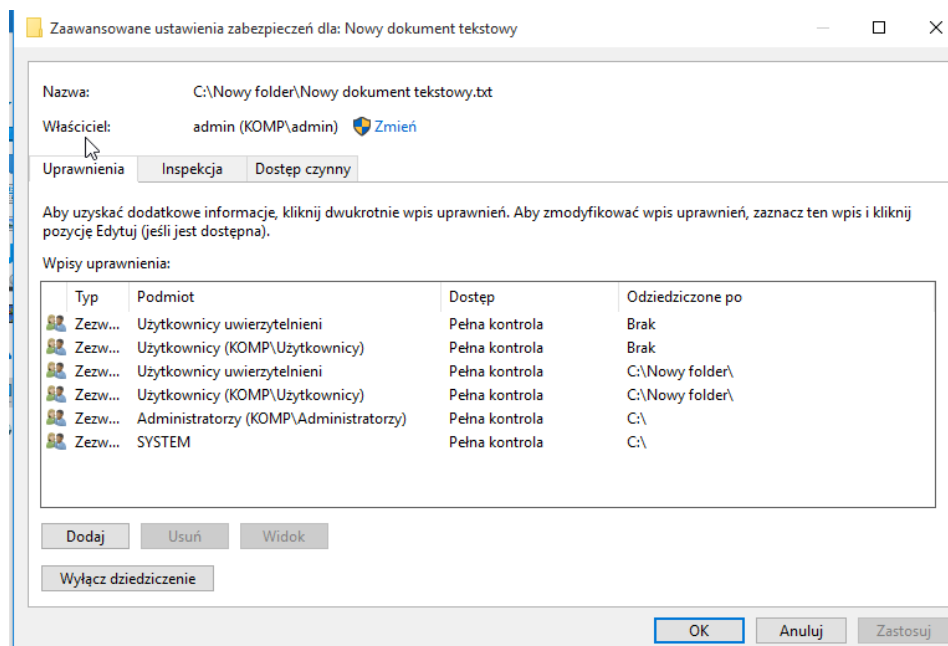
Wyświetlenie zawartości folderu - praktycznie to samo, co Odczyt i wykonanie, ale w odniesieniu do folderów. W przypadku plików nie pojawia się na liście uprawnień.

Odczyt - odczytywanie danych z plików, odczytywanie atrybutów i atrybutów rozszerzonych wykorzystywanych przez aplikacje oraz wyświetlanie zawartości folderów bez możliwości uruchamiania programów.

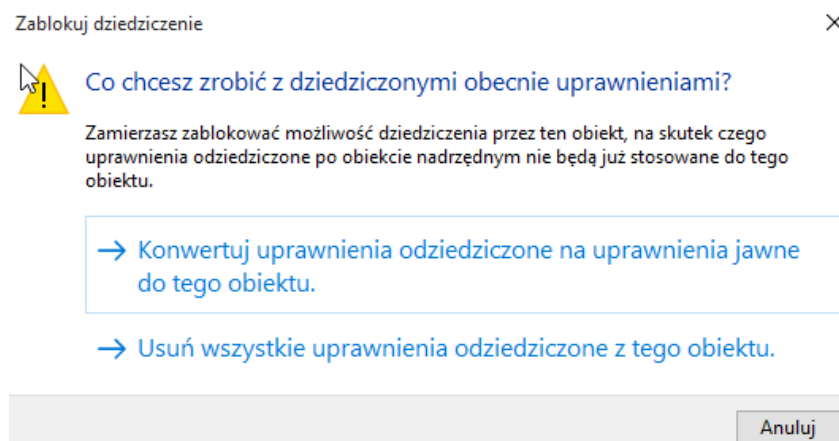
Zapis - tworzenie plików i folderów, zapis danych i modyfikacja plików, zapis atrybutów i atrybutów rozszerzonych.

Zaawansowane uprawnienia zabezpieczeń NTFS

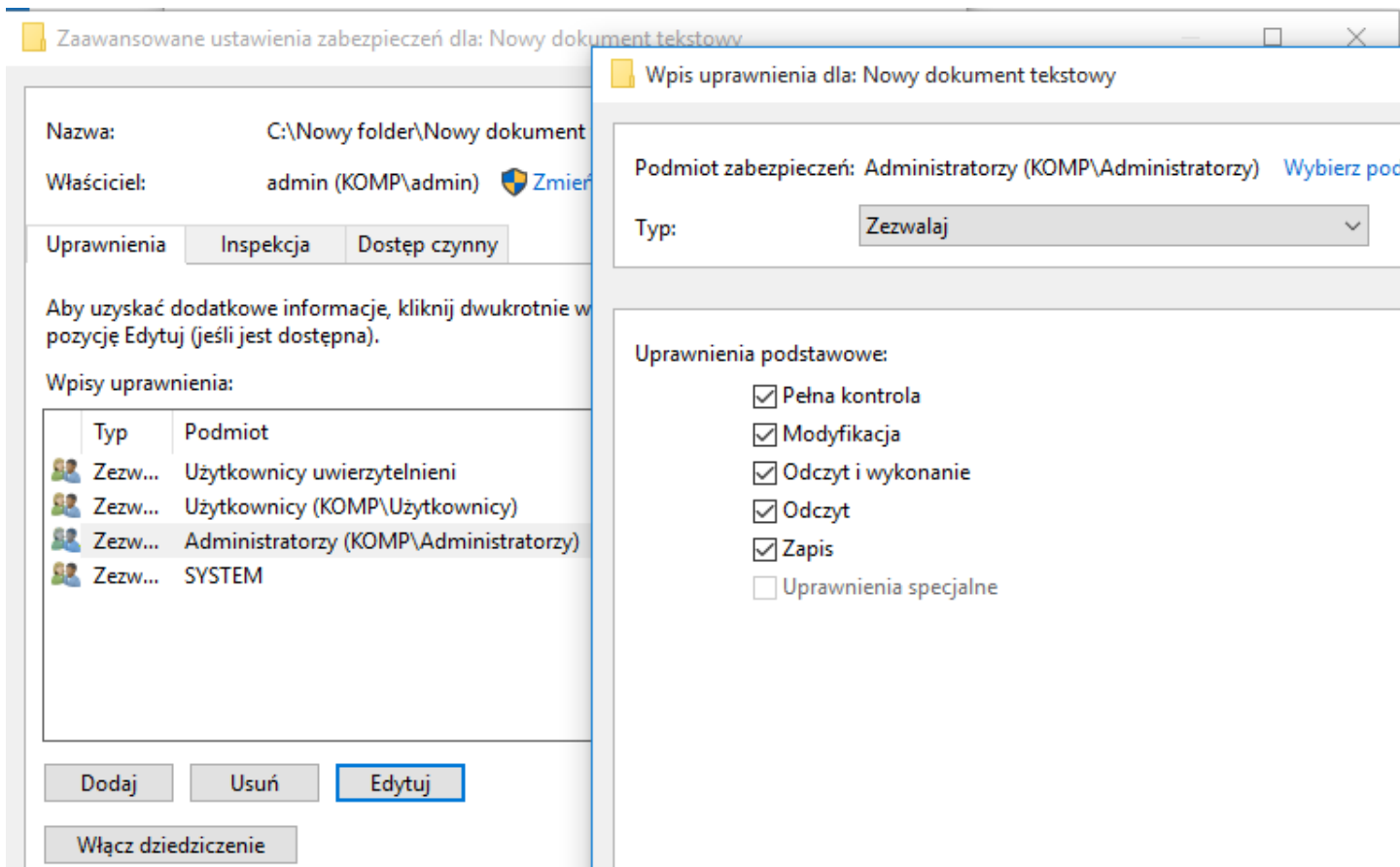
Standardowe uprawnienia NTFS zapewniają wszystkie rodzaje kontroli, wymagane do zabezpieczenia zasobów, istnieją jednak przypadki, w których uprawnienia NTFS nie zapewniają specyficznego poziomu dostępu, jaki należy przyznać użytkownikom. Aby stworzyć specyficzny poziom dostępu, należy przypisać do zasobu uprawnienia Zaawansowane. Windows 10 >



Opcja wyłączająca dziedziczenie.



Wyłączamy dziedziczenie oraz klikamy dodaj. Wybranie opcji Usuń ... spowodowałoby usunięcie wszystkich użytkowników i grup



Podmiot zabezpieczeń: Administratorzy (KOMP\Administratorzy) [Wybierz podmiot zabezpieczeń](#)

Typ:

Uprawnienia podstawowe: [Pokaż uprawnienia zaawansowane](#)

- Pełna kontrola
- Modyfikacja
- Odczyt i wykonanie
- Odczyt
- Zapis
- Uprawnienia specjalne

Uprawnienia zaawansowane: [Pokaż uprawnienia podstawowe](#)

- 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
- Usuwanie
- Odczyt uprawnień
- Zmiana uprawnień
- Przejęcie na własność

Wpisz uprawnienia dla: Nowy folder

Podmiot zabezpieczeń: admin (KOMP\admin) [Wybierz podmiot zabezpieczeń](#)

Typ: Zezwalaj

Dotyczy: Ten folder, podfoldery i pliki

Uprawnienia podstawowe

- Pełna kontrola
- Modyfikacja
- Odczyt i wykonanie
- Wyświetlanie zawartości folderu
- Odczyt
- Zapis
- Uprawnienia specjalne

Zastosuj te uprawnienia jedynie do obiektów i/lub kontenerów znajdujących się wewnątrz tego kontenera

W poniższej tabeli przedstawiono listę ograniczeń dostępu dla każdego zestawu specjalnych uprawnień NTFS.

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

Lista uprawnień specjalnych zapewniające dodatkowe poziomy dostępu do wykonania działań, na które NTFS może zezwolić lub ich zabronić.

Uprawnienia	Opis
Przechodzenie poprzez folder/Wykonanie pliku	Uprawnienie Przechodzenie poprzez folder zezwala lub zabrania na dostęp do pliku w sytuacji, gdy użytkownik ten nie posiada odpowiednich uprawnień do zawierającego ten plik katalogu, ale posiada je w stosunku do samego pliku. Prawo to można stosować tylko do folderów. Uprawnienie to ma zastosowanie tylko w stosunku do tych użytkowników i grup, którym poprzez zasady grup nie przyznano prawa Pomijanie sprawdzania przebiegu . (domyślnie grupa Wszyscy otrzymuje prawo Pomijanie sprawdzania przebiegu). Ustawienie dla folderu uprawnienia Przechodzenie poprzez folder nie powoduje automatycznego ustawienia Wykonanie pliku . Uprawnienie Wykonanie pliku przyznaje lub odmawia użytkownikowi prawa do uruchamiania plików zawierających programy. Prawo to stosuje się jedynie do plików.
Odczyt atrybutów	Zezwala lub odmawia przeglądania atrybutów pliku lub folderu takich jak Tylko do odczytu lub Ukryty
Odczyt atrybutów rozszerzonych	Zezwala bądź odmawia przeglądania rozszerzonych atrybutów pliku bądź folderu. Niektóre rozszerzone atrybuty definiują same aplikacje we właściwy dla siebie sposób. Należą do nich również dwa atrybuty NTFS - kompresji i szyfrowania.
Tworzenie plików/Zapis danych	Zezwala bądź odmawia prawa do tworzenia plików wewnątrz folderu. Zapis danych zezwala bądź odmawia prawa do dokonywania zmian w plikach i nadpisywania ich bieżącej zawartości. Prawo to stosuje się jedynie do plików.
Tworzenie folderów/Dołączanie danych	Zezwala bądź odmawia prawa tworzenia podkatalogów wewnątrz folderu. Dołączanie danych zezwala bądź odmawia do dopisywania danych na końcu istniejącego pliku, lecz nie do zmiany, usuwania lub nadpisywania istniejących już w nim danych.
Zapis atrybutów	Zezwala bądź odmawia prawa do zmieniania atrybutów pliku lub folderu takich jak Tylko do odczytu , Ukryty .

Zapis rozszerzonych atrybutów	Zezwala bądź odmawia prawa do zmieniania rozszerzonych atrybutów pliku lub folderu.
Usuwanie podfolderów i plików	Zezwala bądź odmawia prawa do usuwania znajdujących się wewnątrz folderu plików zabezpieczeń podkatalogów, nawet jeżeli użytkownik nie posiada uprawnienia Usuwanie do usuwanego pliku lub podkatalogu.
Usuwanie	Zezwala bądź odmawia prawa do usuwania plików i katalogów. Jeżeli użytkownik nie posiada uprawnienia Usuwanie do pliku lub katalogu, ciągle może je usunąć o ile posiada uprawnienie Usuwanie podfolderów i plików w stosunku do folderu nadrzędnego.
Odczyt uprawnień	Zezwala bądź odmawia prawa do odczytywania uprawnień zastosowanych do pliku lub folderu, takich jak Pełna kontrola, Zapis, Odczyt .
Zmiana uprawnień	Zezwala bądź odmawia prawa do zmieniania uprawnień zastosowanych do pliku lub folderu takich jak Pełna kontrola, Zapis, Odczyt .
Przejęcie na własność	Zezwala bądź odmawia prawa do przejęcia pliku lub folderu na własność. Właściciel pliku lub folderu może zawsze zmienić jego uprawnienia, niezależnie od tego, jakie zastosowano uprawnienia w celu jego ochrony.
Synchronizacja	Zezwala bądź odmawia prawa do tego, aby różne wątki mogły oczekiwać na zwolnienie uchwytu do pliku zabezpieczeń w ten sposób synchronizować się z innymi, sygnalizującymi to wątkami. Ten rodzaj uprawnienia ma zastosowanie jedynie dla programów wielowątkowych i wieloprocessorowych.

Kopiowanie i przenoszenie folderów z uprawnieniami NTFS

Uprawnienia zabezpieczeń mogą ulec zmianie w wyniku operacji kopiowania lub przenoszenia.

Jeżeli plik lub folder jest kopiowany w obrębie tego samego woluminu NTFS, dziedziczy uprawnienia nowej lokalizacji.

Jeżeli plik lub folder jest przenoszony w obrębie tego samego woluminu NTFS, jego uprawnienia się nie zmieniają.

Jeżeli plik lub folder jest kopiowany bądź przenoszony na inny wolumin NTFS, dziedziczy uprawnienia nowej lokalizacji.



Jeżeli pliki lub foldery zostaną przeniesione na wolumin FAT, utracą one posiadane uprawnienia NTFS, ponieważ woluminy typu FAT nie obsługują uprawnień NTFS.

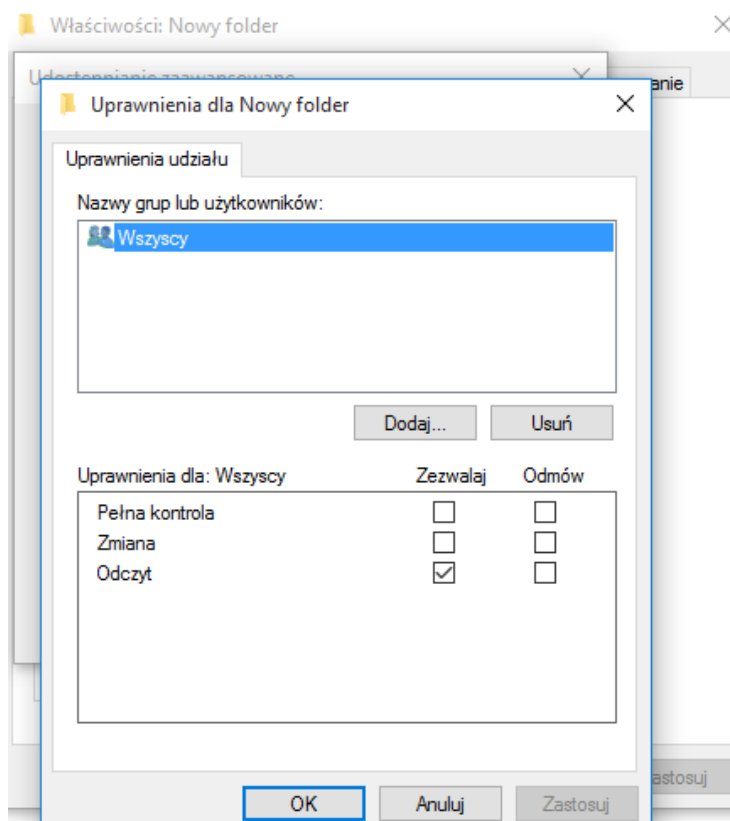
Operacja	Ten sam wolumin NTFS	Inny wolumin NTFS
Kopiowanie	Dziedziczy uprawnienia NTFS folderu docelowego	Dziedziczy uprawnienia NTFS folderu docelowego
Przenoszenie	Zachowuje uprawnienia folderu źródłowego	Dziedziczy uprawnienia NTFS folderu docelowego

Udostępniając zasób możesz każdemu użytkownikowi lub grupie przydzielić uprawnienia:

Pełna kontrola - Jak sama nazwa wskazuje użytkownik z takimi prawami posiada pełną swobodę działania, może tworzyć nowe pliki, odczytywać, modyfikować, zapisywać i usuwać już istniejące oraz zmieniać uprawnienia i przejmować na własność. Nadawaj te uprawnienie ze szczególną ostrożnością.

Zmiana - Użytkownik posiada te same uprawnienia co Pełna kontrola poza prawem do zmiany uprawnień i przejmowania na własność, czyli może tworzyć nowe pliki, odczytywać, modyfikować, zapisywać i usuwać już istniejące.

Odczyt - Użytkownik posiada prawo do odczytywania plików (w tym ich uruchamiania), nie może tworzyć nowych plików i usuwać ani modyfikować już istniejących.



Efektywne uprawnienia

to suma uprawnień użytkownika i wszystkich grup, do których należy.

Przykład: Jeśli użytkownik ma prawo odczytu do folderu, a grupa, do której należy ma prawo do zapisu to znaczy, że użytkownik ma obydwa prawa.

Pamiętaj:

1. Uprawnienia NTFS są sumowane
2. Odmów ważniejszy niż pozwól. Odmowa usuwa pozwolenie.
3. Uprawnienia do pliku w folderze są ważniejsze niż do samego folderu.

Przykładowo:, jeśli masz uprawnien folderu, możesz uzyskać dostęp do pliku wpisując pełną ścieżkę.

Połączone uprawnienia

Po wprowadzeniu różnorodnych uprawnień, określenie jaka ich kombinacja dotyczy konkretnego użytkownika może stać się skomplikowane.

Jeżeli folder ma uprawnienia udziału i uprawnienia zabezpieczeń, jak wpływa to na dostęp użytkowników do zasobów?

Pamiętaj:

1. Jeżeli użytkownik jest związany z wieloma uprawnieniami udziału, są one łączone i przypisywany jest najwyższy poziom dostępu.
2. Jeżeli użytkownik jest związany z wieloma uprawnieniami zabezpieczeń, są one łączone i przypisywany jest najwyższy poziom dostępu.
3. Jeżeli użytkownik jest związany z uprawnieniami udziału i uprawnieniami zabezpieczeń zasobu, są one łączone i przypisywane są uprawnienia bardziej restrykcyjne.

Przykłady:

1. Użytkownik na poziomie NTFS ma uprawnienie „Odczyt” a na poziomie folderu udostępnionego „Pełna kontrola”. Wynikowym uprawnieniem jest zatem „Pełna kontrola”.
2. Użytkownik na poziomie NTFS ma uprawnienie „Modyfikacja” a na poziomie folderu udostępnionego „Odczyt”. Wynikowym uprawnieniem jest zatem „Odczyt”.
3. Użytkownik na poziomie NTFS ma uprawnienie „Odczyt” oraz „Pełna kontrola” a na poziomie folderu udostępnionego „Modyfikacja”. Wynikowym uprawnieniem jest zatem „Modyfikacja” (mniej restrykcyjnym uprawnieniem NTFS jest „Pełna kontrola” – nie „Odczyt”, natomiast folder udostępniony ma uprawnienie „Modyfikacja” dlatego uprawnieniem wynikowym jest „Modyfikacja” – uprawnienie bardziej restrykcyjne).

Odpowiedz na pytania

- 1) Wymień uprawnienia do plików i folderów na dyskach NTFS.
- 2) Na czym polega dziedziczenie i sumowanie uprawnień NTFS?
- 3) Wymień uprawnienia specjalne NTFS.
- 4) Co oznacza pojęcie czynne uprawnienia?
- 5) Czym są uprawnienia jawne i dziedziczone.