

Uprawnienia NTFS w Windows 11 (wersja 24H2)

Pełna wersja instrukcji dostosowana do Windows 11 24H2.

Cel ogólny lekcji: Przygotować uczestników do zrozumienia i efektywnego zarządzania systemem plików NTFS w systemie Windows oraz zrozumienia zasad zarządzania kontami użytkowników, monitorowania dostępu do danych oraz inspekcji dostępu do folderów i plików.

Cele szczegółowe lekcji:

- Uczestnicy nauczą się tworzyć nowe konta użytkowników i dostosowywać ich typy oraz uprawnienia.
- Uczestnicy nauczą się tworzyć i modyfikować foldery, a także dostosowywać uprawnienia dostępu do nich.
- Uczestnicy zrozumieją, jak odebrać uprawnienia dostępu do folderu określonej grupie użytkowników i jak to wpływa na dostęp do danych.
- Uczestnicy nauczą się nadawać uprawnienia dostępu do konkretnych plików i zrozumieją, jak to wpływa na możliwość modyfikacji tych plików przez różnych użytkowników.
- Uczestnicy zrozumieją, jak zmieniają się uprawnienia obiektów podczas kopiowania lub przenoszenia między dyskami NTFS.
- Uczestnicy nauczą się, jak włączyć inspekcję dostępu do folderu w systemie Windows i monitorować próby dostępu.
- Uczestnicy zrozumieją, jak sprawdzić zdarzenia związane z dostępem do folderu, w tym modyfikacje zawartości i które użytkownicy były za nie odpowiedzialne.
- Uczestnicy zaprojektują strukturę katalogową zgodnie z wytycznymi, aby spełnić konkretne wymagania dotyczące zarządzania plikami i katalogami, a także dostępu do danych w firmie.

Lekcja połączy te cele w spójną całość, umożliwiając uczestnikom zrozumienie i praktyczne wykorzystanie zasad zarządzania danymi i dostępem do nich w systemie Windows 11.

Czynności wykonuj według podanej w zadaniu kolejności, jeżeli wykonasz dowolną czynność poza kolejnością pobierz nową maszynę wirtualną i wykonaj ćwiczenie od początku.

1. W folderze z materiałami znajduje się plik:

[nhdd1720.zip](#) należy go pobrać i wyodrębnić (rozpakować) w folderze Pobrane a następnie nhdd1720.vhd podłączyć jako drugi dysk do maszyny wirtualnej.

2. Z napędu optycznego lub w maszynie wirtualnej z strony z materiałami przekopiuje wskazany pliki na pulpit maszyny wirtualnej

3. Plik wskazany przez prowadzącego uruchomi jako administrator

Wykonaj polecenia, umieść notatkę w zeszycie dokumentujące wykonanie poleceń.

Każdą czynność wykonaną w zadaniach zgłoś prowadzącemu na etapie wskazanym w zadaniu. Zaloguj się do konta domyślnego z hasłem zaq1@WSX

Ćwiczenie 1.1 Folder - modyfikacja uprawnień (Windows 11 24H2)

Każdy plik i folder umieszczony na dysku NTFS jest „własnością” jednego z użytkowników. Właściciel folderu może w pełni nim zarządzać, w tym zabronić innym użytkownikom modyfikowania danych umieszczonych w tym folderze.

1. Upewnij się, że jesteś zalogowany do konta boleć bez hasła.
2. Na C:\ lokalnym dysku NTFS utwórz nowy folder o nazwie prywatne.
3. Przejdź do folderu prywatne.
4. Ustaw kursor myszki tak, aby nie wskazywał żadnego z elementów okna i naciśnij prawy przycisk myszy. Zamiast naciskać prawy przycisk myszy, możesz użyć gestu dotykowego lub skrót klawiszowy Win + X, aby otworzyć menu szybkich ustawień.
5. Z menu podręcznego wybierz opcję Nowy | Dokument tekstowy. W folderze zostanie utworzony nowy plik. Zamiast wybierać opcję Nowy | Dokument tekstowy, możesz użyć polecenia głosowego lub skrótu klawiszowego Win + N, aby utworzyć Dokument tekstowy.
6. Przejdź do obiektu Dysk lokalny C:\ jest folder o nazwie prywatne.

Jeżeli w oknie właściwości nie znajduje się zakładka Zabezpieczania: Kliknij prawym przyciskiem myszy na folderze prywatne i z podręcznego menu wybierz opcję Właściwości.

7. W oknie Właściwości: prywatne wybierz zakładkę Zabezpieczania > Edytuj.
8. Naciśnij przycisk Dodaj. W polu Wprowadź nazwę obiektów do wybrania wpisz (wklej) Użytkownicy zaawansowani i naciśnij OK.
9. Wyczyść pola Zezwalaj dla wierszy Odczyt i wykonanie oraz Wyświetlanie zawartości folderu i naciśnij przyciski Zastosuj i OK.
10. Sprawdź czy użytkownik tola nie może modyfikować danych umieszczonych w folderze C:\prywatne.
11. W zeszycie zapisz wnioski z przeprowadzonych czynności:

Każdy plik i folder na dysku NTFS ma swojego właściciela, który ma pełne uprawnienia do zarządzania nimi.

W wyniku powyższych działań zmieniliśmy uprawnienia dostępu do folderu "prywatne". Wcześniej każdy użytkownik mógł odczytywać i modyfikować zawartość tego folderu. Po zmianach użytkownik "tola" stracił prawo do modyfikowania danych w tym folderze, ale nadal może odczytywać jego zawartość. To pokazuje, jak można dokładnie kontrolować dostęp do plików i folderów na systemie plików NTFS, przydaje się to w sytuacjach, gdzie chcemy zabezpieczyć pewne dane przed nieuprawnionym dostępem.

(zgłoszenie) 1

Alternatywa PowerShell: `icacls C:\prywatne /grant 'Użytkownicy zaawansowani':(R)`

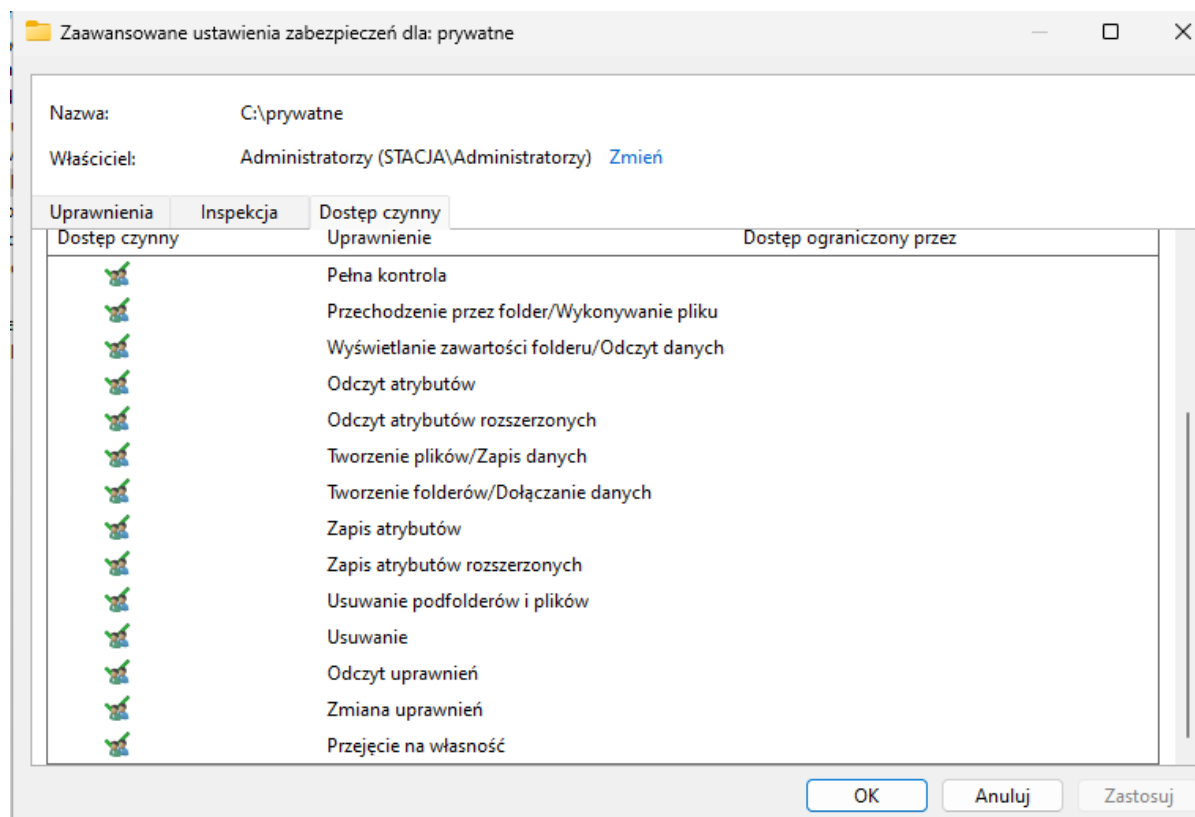
Ćwiczenie 1.2. Odebranie uprawnień do folderu danej grupie użytkowników (Windows 11 24H2)

Ponieważ użytkownik może być członkiem więcej niż jednej grupy odznaczenie opcji **Zezwalaj** dla niektórych tylko grup, w których znajduje się konto użytkownika nie powoduje odebrania mu praw do pliku lub folderu.

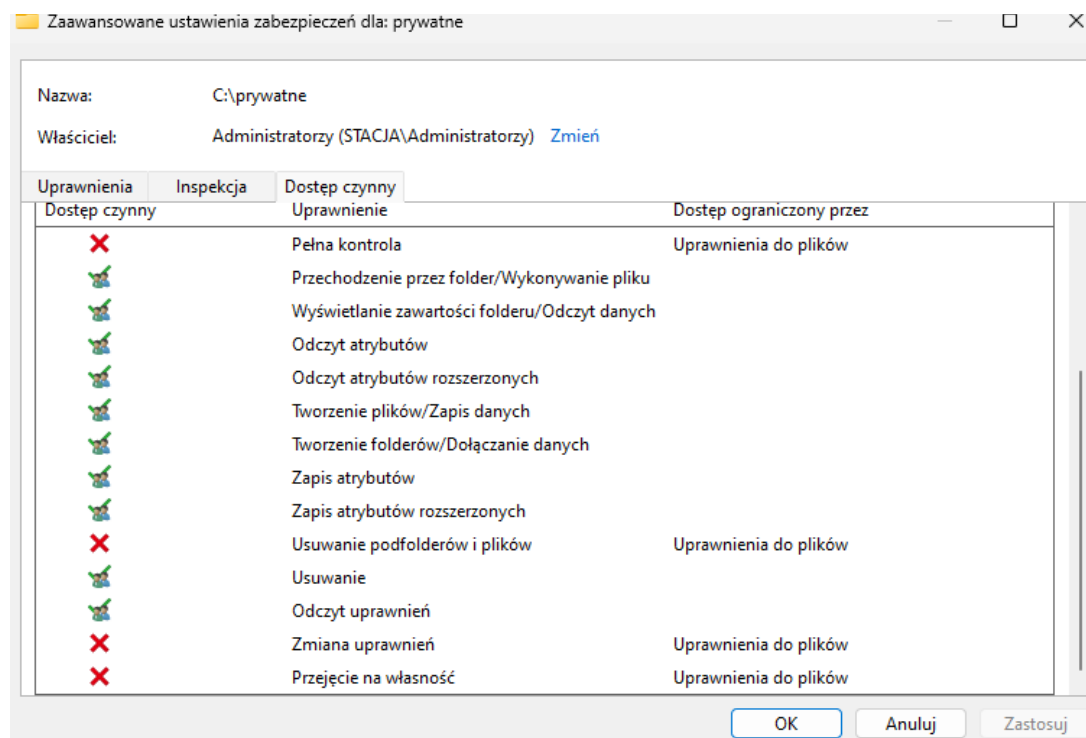
Dla kont użytkowników bolelek, lolek, tola sprawdź który z użytkowników nadal ma dostęp do folderu prywatne i zapisz to w zeszycie.

1. Zaloguj się do konta bolelek.
2. Kliknij prawym przyciskiem myszy na folderze prywatne i z menu podręcznego wybierz opcję **Właściwości > Zabezpieczanie**.
3. W polu Nazwy grupy lub użytkownika zaznacz **Użytkownicy zaawansowani > Edytuj**. Tytuł dolnego okna zostanie zmieniony na **Uprawnienia dla Użytkownicy zaawansowani**.
4. Zaznacz pole **Odmów** dla wiersza **Modyfikacja**. Ponieważ pozostałe uprawnienia (z wyjątkiem uprawnienia **Pełna kontrola**) zależą od uprawnienia do modyfikacji, system automatycznie potwierdzi odebranie tych uprawnień.
5. Naciśnij przycisk **Zastosuj**. Zostanie wyświetlony komunikat ostrzegający przed konsekwencjami jawnego odbierania uprawnień. Naciśnij przycisk **TAK > potwierdź OK**.
6. Sprawdź czy użytkownik

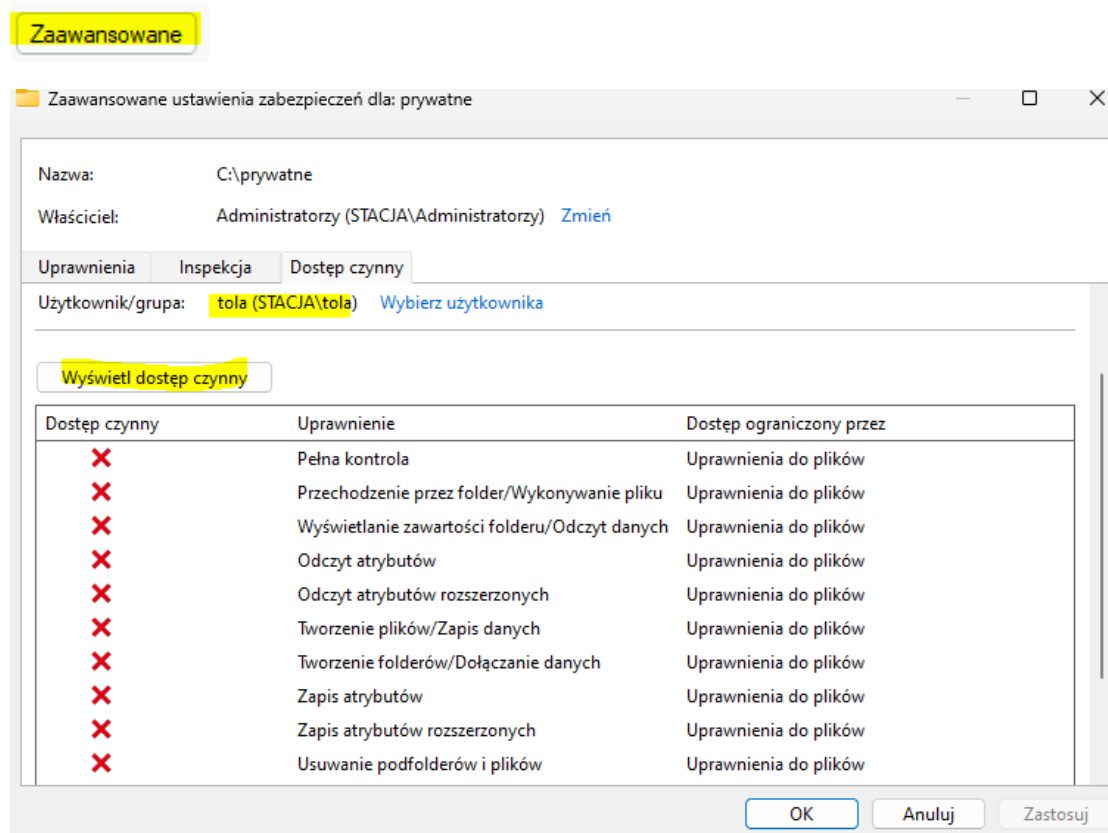
bolelek będzie miał uprawnienia jak poniżej



lolek będzie miał uprawnienia jak poniżej



tola nie będzie mógł modyfikować danych umieszczonych w tym folderze.



7. W zeszycie zapisz wnioski z wyżej wymienionych czynności.

Z zadania wynika, że masz trzy konta użytkowników: bolelek, lolek i tola. Zakładam, że bolelek należy do grupy Administratorzy, lolek należy do grupy Użytkownicy, a tola do grupy Użytkownicy zaawansowani. Jeśli tak jest, to po wykonaniu kroków 1-5 z twojego zadania wynika, że

- a. bolelek będzie miał dostęp jak powyżej, ponieważ nie należy on do grupy Użytkownicy zaawansowani.
- b. lolek będzie miał dostęp jak powyżej, ponieważ nie należy on do grupy Użytkownicy zaawansowani.
- c. tola zostanie pozbawiona dostępu do folderu "prywatne" zgodnie z zasadą nadawania uprawnień.

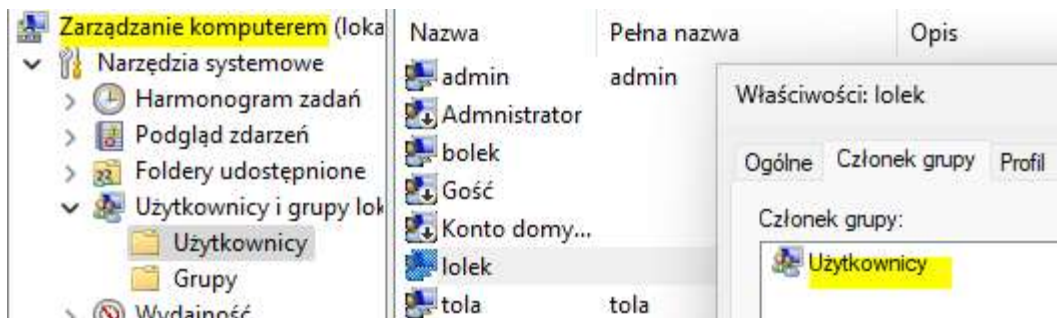
(zgłoszenie) 2

Ćwiczenie 1.3. Nadawanie uprawnień do danego pliku (Windows 11 24H2)

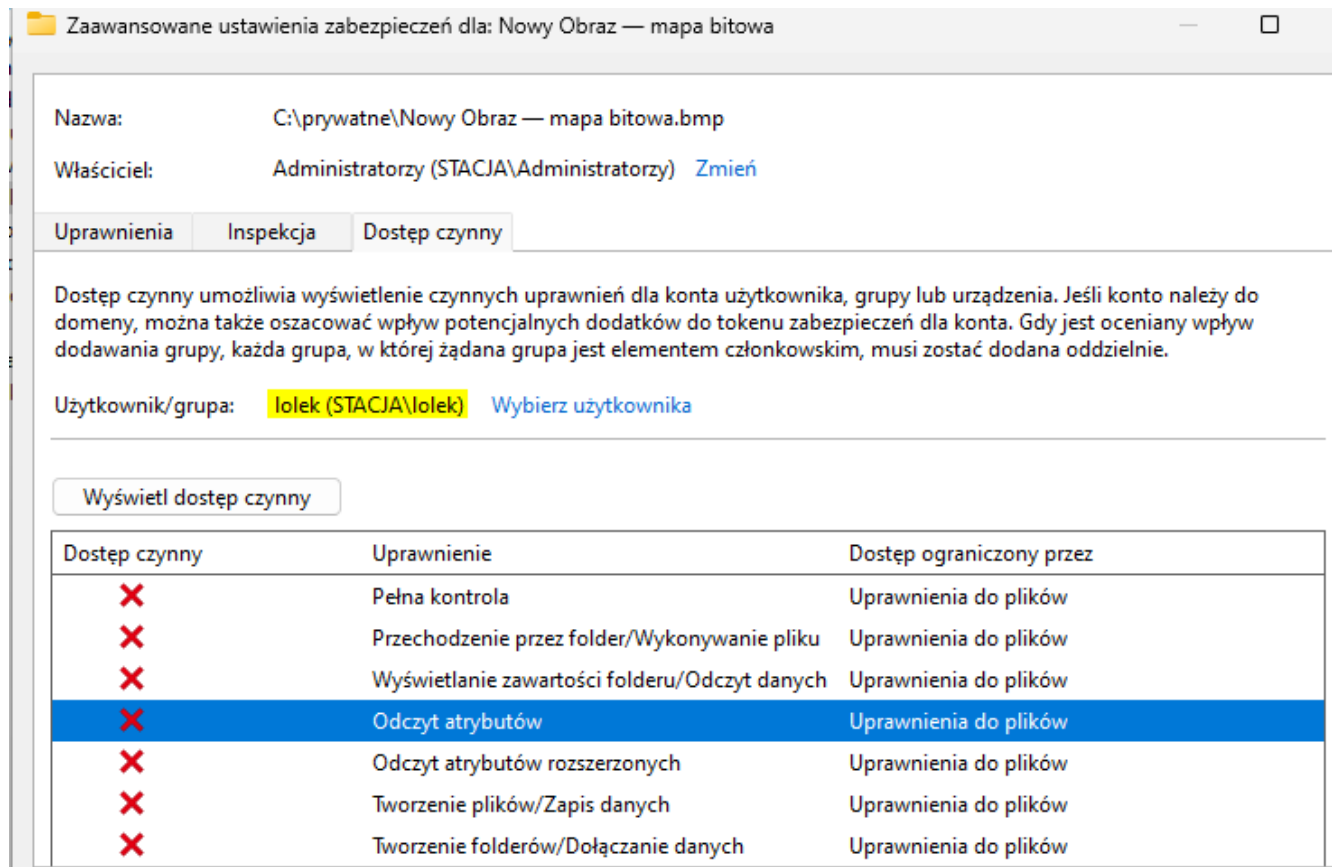
1. Przejdź do folderu prywatne.
2. Ustaw kursor myszki tak, aby nie wskazywał żadnego z elementów okna i naciśnij prawy przycisk myszy.
3. Z menu podręcznego wybierz opcję Nowy | Obraz - mapa bitowa. W folderze zostanie utworzony nowy plik.
4. Kliknij prawym przyciskiem myszy na ikonie nowego pliku i z podręcznego menu wybierz opcję Właściwości.
5. W polu Właściwości: Nowy obraz – mapa bitowa wybierz opcję Zabezpieczenia.
6. Naciśnij przycisk Edytuj > Dodaj. W polu Wprowadź nazwę obiektów do wybrania wpisz lub sprawdź nazwę konta lolek.

Ponieważ to konto należy do pewnej grupy, automatycznie ma nadane, takie same jak grupa, uprawnienia do wszystkich obiektów znajdujących się w katalogu prywatne. Zaznacz opcję Odmów dla wiersza Pełna kontrola.

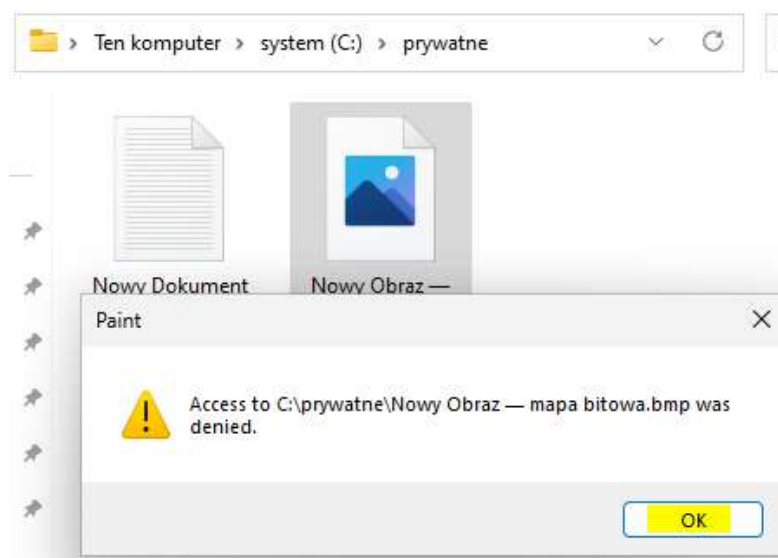
7. Naciśnij przycisk Zastosuj i OK.
8. W zeszycie opowiedz na pytania.
 - a. Do jakich grup należy konto lolek?



- b. Jakie uprawnienia użytkownika konta lolek do pliku Nowy obraz – mapa bitowa zostały odebrane?



- c. Sprawdź czy po zalogowaniu do konta lolek w katalogu poufne jest niemożliwa modyfikacja pliku Nowy obraz – mapa bitowa?



(zgłoszenie) 3

Kopiowanie plików i folderów

Ponieważ każdy obiekt (taki jak plik lub folder) „dziedziczy” uprawnienia od folderu nadrzędnego, to podczas kopiowania i przenoszenia obiektów uprawnienia te mogą ulec zmianie.

Ćwiczenia 1.4. Zmiana właściwości kopiowanych obiektów

Kopiowane lub przenoszone pomiędzy dyskami NTFS obiekty otrzymują uprawnienia nadrzędnego obiektu docelowego. Jedynym wyjątkiem od tej zasady jest przenoszenie obiektów w ramach pojedynczej partycji - wtedy obiekt zachowuje wszystkie swoje uprawnienia. Aby sprawdzić prawdziwość powyższej reguły:

1. Zaloguj się ponownie do konta bolelek.
2. Otwórz folder prywatne.
3. Wyświetl i zapamiętaj uprawnienia poszczególnych grup i użytkowników do pliku Nowy obraz – mapa bitowa. Zapisz w zeszycie. (wykonaj zrzut ekranu)

Zaawansowane ustawienia zabezpieczeń dla: Nowy Obraz — mapa bitowa

Nazwa: C:\prywatne\Nowy Obraz — mapa bitowa.bmp
Właściciel: Administratorzy (STACJA\Administratorzy) [Zmień](#)

Uprawnienia Inspekcja Dostęp czynny

Dostęp czynny umożliwia wyświetlenie czynnych uprawnień dla konta użytkownika, grupy lub urządzenia. Jeśli domeny, można także oszacować wpływ potencjalnych dodatków do tokenu zabezpieczeń dla konta. Gdy jest dodawana grupa, każda grupa, w której żądana grupa jest elementem członkowskim, musi zostać dodana od

Użytkownik/grupa: **Użytkownicy uwierzytelnieni** [Wybierz użytkownika](#)

[Wyświetl dostęp czynny](#)

Dostęp czynny	Uprawnienie	Dostęp ograniczony przez:
	Pełna kontrola	Uprawnienia do plików
	Przechodzenie przez folder/Wykonywanie pliku	

Zaawansowane ustawienia zabezpieczeń dla: Nowy Obraz — mapa bitowa

Nazwa: C:\prywatne\Nowy Obraz — mapa bitowa.bmp
Właściciel: Administratorzy (STACJA\Administratorzy) [Zmień](#)

Uprawnienia Inspekcja Dostęp czynny

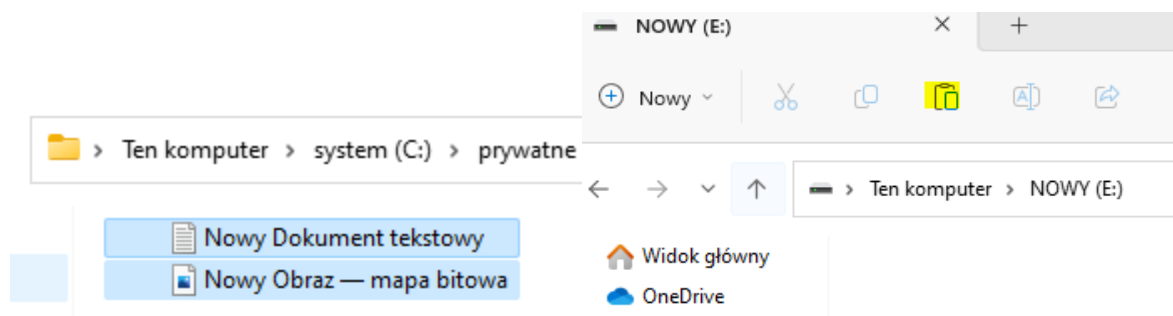
Dostęp czynny umożliwia wyświetlenie czynnych uprawnień dla konta użytkownika, grupy lub urządzenia. Jeśli domeny, można także oszacować wpływ potencjalnych dodatków do tokenu zabezpieczeń dla konta. Gdy jest dodawana grupa, każda grupa, w której żądana grupa jest elementem członkowskim, musi zostać dodana od

Użytkownik/grupa: Użytkownicy zaawansowani **(STACJA\Użytkownicy zaawansowani)** [Wybierz użytkow](#)

[Wyświetl dostęp czynny](#)

Dostęp czynny	Uprawnienie	Dostęp ograniczony przez:
	Pełna kontrola	Uprawnienia do plików

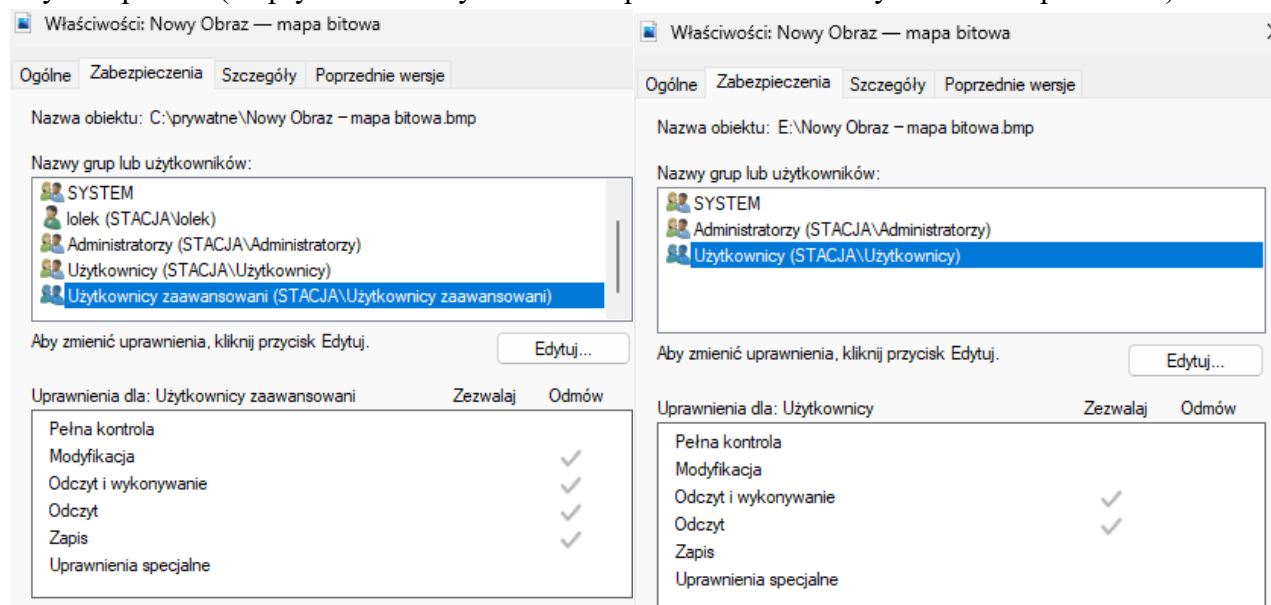
4. Skopiuj plik do głównego katalogu na E:\ (inny dysk NTFS).



Ctrl+C > lub Ctrl+V

5. Wyświetl uprawnienia do pliku Nowy obraz – mapa bitowa. (wykonaj zrzut ekranu)

6. Zapisz w zeszycie zabezpieczenia i wykonaj zrzut ekranu, na którym będą okna Zabezpieczenia obydwu plików (C:\prywatne\Nowy obraz – mapa bitowa i E:\Nowy obraz – mapa bitowa)



7. Na liście, którego pliku nie ma grupy Użytkownicy zaawansowani i użytkownika konta lolek

8. W zeszycie wyjaśnij, dlaczego na liście wskazanego pliku nie ma grupy Użytkownicy zaawansowani i użytkownika konta lolek.

a. Na liście uprawnień na nowym dysku mogą brakować grupy "Użytkownicy zaawansowani" i użytkownika "lolek", ponieważ w systemie plików NTFS obiekty zachowują uprawnienia nadrzędnego obiektu docelowego. W tym przypadku, "Nowy obraz – mapa bitowa" został skopiowany na inny dysk i te uprawnienia dostosowały się do nowego dysku.

b. Jeśli grupa "Użytkownicy zaawansowani" lub użytkownik "lolek" nie posiadał uprawnień na nowym dysku, to po skopiowaniu pliku, mogą nie mieć dostępu do nowej lokalizacji.

c. Warto zaznaczyć, że w przypadku przenoszenia obiektu w obrębie tej samej partycji, obiekt zachowuje swoje uprawnienia. Jednak w przypadku przeniesienia między partycjami lub dyskami, uprawnienia te zostaną dostosowane do miejsca docelowego.

To ćwiczenie pokazuje, że podczas kopiowania obiektów między dyskami NTFS, ważne jest zrozumienie, jakie uprawnienia obowiązują w miejscu docelowym. Grupy lub użytkownicy, którzy nie mieli uprawnień w nowym miejscu docelowym, mogą nie mieć dostępu do skopiowanych obiektów.

(zgłoszenie) 4

Inspekcja dostępu do danych

Alternatywa PowerShell: AuditPol /set /subcategory:'File System' /success:enable /failure:enable

Ćwiczenie 1.5 Monitorowanie dostępu do katalogu (Windows 11 24H2)

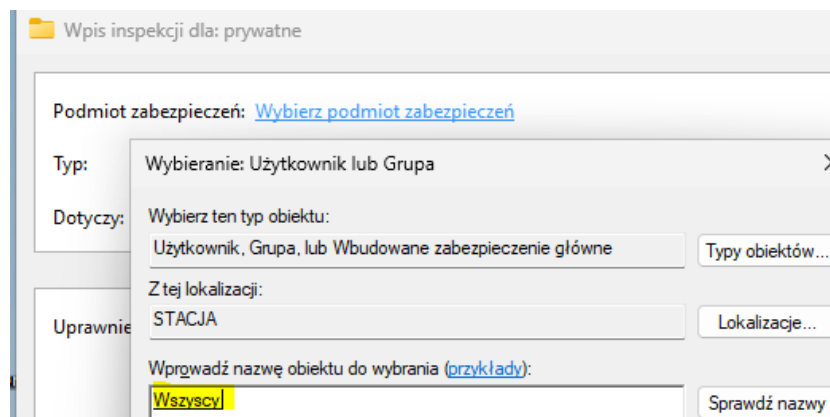
Alternatywa PowerShell: AuditPol /set /subcategory:'File System' /success:enable /failure:enable

Celem ćwiczenia jest włączenie inspekcji dostępu do folderu prywatne.

1. Upewnij się, że jesteś zalogowany do konta boleć.
2. Uruchom przycisk Flaga + R | secpol.msc.
3. Rozwiń folder Zasady lokalne i wybierz opcję Zasady inspekcji.
4. Dwukrotnie kliknij zasadę Przeprowadź inspekcję dostępu do obiektów.
5. Zaznacz opcje Sukces oraz Niepowodzenie.
6. Naciśnij klawisz OK i zamknij okno konsoli Zasady zabezpieczeń lokalnych.
7. Kliknij prawym przyciskiem myszki na folderze prywatne i z menu podręcznego Właściwości:prywatne wybierz opcję Zabezpieczanie.
8. Wybierz opcje Zaawansowane | Inspekcja.

Alternatywa PowerShell: AuditPol /set /subcategory:'File System' /success:enable /failure:enable

9. Kliknij przycisk > Dodaj.
10. W polu Wprowadź nazwę obiektów do wybrania wpisz Wszyscy. Sprawdź poprawność nazwy i naciśnij OK.



11. Zostanie wyświetlone okno Wpis inspekcji dla prywatne. Zaznacz opcję Powodzenie i Niepowodzenie dla wiersza Pełna kontrola.

Uprawnienia podstawowe:

- ☒ Pełna kontrola
- ☒ Modyfikacja
- ☒ Odczyt i wykonywanie
- ☒ Wyświetlanie zawartości folderu
- ☒ Odczyt
- ☒ Zapis
- ☐ Uprawnienia specjalne

12. Naciśnij klawisz OK. Zostanie zamknięte okno Zaawansowane ustawianie zabezpieczeń dla prywatne.

13. Naciśnij przycisk OK.

W praktyce nie stosuje się tak dokładnej modyfikacji obiektu. Monitorowanie dla każdego użytkownika zarówno udanych, jak i nieudanych prób dostępu w krótkim czasie skończyłoby się zapelnieniem Dziennika zabezpieczenia.

14. W zeszycie wyjaśnij jaka modyfikacja zawartości folderu prywatne zostanie odnotowana w Dzienniku zabezpieczenia.

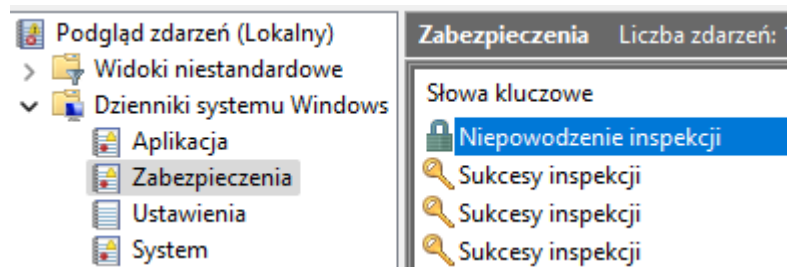
(zgłoszenie) 5

Alternatywa PowerShell: AuditPol /set /subcategory:'File System' /success:enable /failure:enable

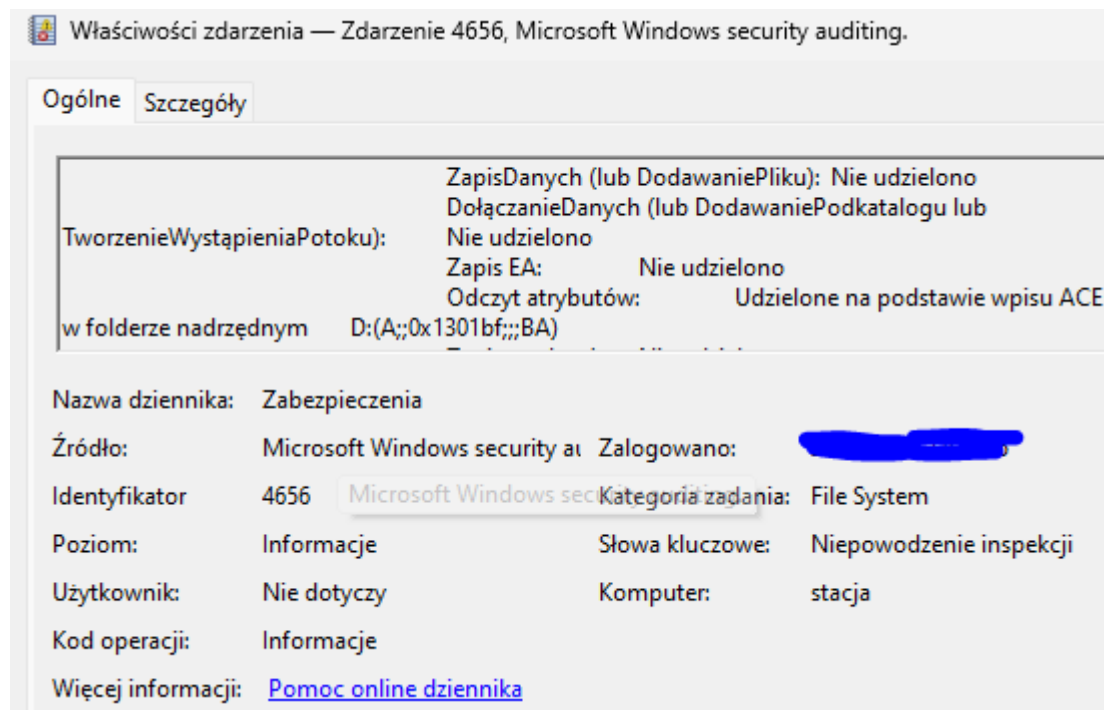
Ćwiczenie 1.6 Przeglądanie Dziennika zabezpieczenia (Windows 11 24H2)

Aby sprawdzić kto modyfikował zawartość folderu prywatne:

1. Upewnij się, że jesteś zalogowany do konta boleek.
2. Uruchom przycisk Flaga + R | eventvwr.msc | Podgląd zdarzeń.
3. Wybierz Dziennik Zabezpieczenia. W oknie po prawej stronie zostanie wyświetlona lista zarejestrowanych zdarzeń.



4. Aby poznać więcej szczegółów o konkretnym zdarzeniu kliknij na nim dwukrotnie lewym przyciskiem myszki.
5. W zeszycie wyjaśnij szczegóły konkretnego zdarzenia dotyczącego modyfikacji zawartości folderu prywatne które zostanie odnotowane w podglądzie zdarzeń dziennika Zabezpieczenia.



(zgłoszenie) 6

Zadania do samodzielnego wykonania

Ćwiczenie 1.7 Zaprojektuj w zeszycie, a następnie stwórz w systemie Windows strukturę katalogową w katalogu E:\1720 spełniającą następujące wytyczne (Windows 11 24H2)

1. boleć pracuje w marketingu i zwykle zapisuje pliki w katalogu marketing.
2. lolek pracuje w finansach i zwykle zapisuje pliki w katalogu finanse.
3. Użytkownicy boleć i lolek nie mogą zapisywać plików i katalogów poza katalogami: marketing, finanse.
4. Użytkownicy boleć i lolek nie mogą zmieniać nazw i usuwać plików i katalogów poza katalogami: marketing, finanse.
5. Użytkownicy boleć i lolek mogą pracować na wspólnych plikach w katalogach: marketing, finanse.
6. W katalogach marketing i finanse znajdują się podkatalogi sekret, które zawierają pliki dostępne tylko dla (odpowiednio) marketingu i finansów.

7. Zapisz w zeszycie następujące wnioski na podstawie tych wytycznych:

- a. Katalog "marketing" i "finanse" zostały utworzone, aby odpowiednio oddzielić pliki i katalogi dla działów marketingu i finansów.
- b. W każdym z tych katalogów znajduje się podkatalog o nazwie "wspolne_pliki".
To miejsce, w którym użytkownicy boleek i lolek mogą współpracować, ponieważ mogą tam zapisywać i zmieniać pliki.
- c. Ograniczenie dotyczące zapisywania i zmiany nazw plików oraz katalogów poza katalogami "marketing" i "finanse" może być zaimplementowane, ustawiając odpowiednie uprawnienia na poziomie dysku NTFS. Użytkownicy boleek i lolek będą mieli dostęp tylko do swojego odpowiedniego działu i do katalogu "wspolne_pliki", co zapewni zgodność z tym ograniczeniem.
- d. W katalogach "marketing" i "finanse" znajdują się podkatalogi "sekret", w których można przechowywać pliki, do których dostęp mają tylko pracownicy z odpowiednich działów. Ograniczenia dostępu do tych plików można również zaimplementować za pomocą odpowiednich uprawnień NTFS.
- e. Wszystkie te zasady struktury katalogowej pomagają zorganizować i kontrolować dostęp do plików i katalogów w zgodzie z potrzebami i polityką firmy.

Wniosek z tych zadań to zrozumienie, jak skonfigurować strukturę katalogową i uprawnienia NTFS, aby spełnić określone wymagania dotyczące zarządzania plikami i katalogami w systemie Windows. Umożliwia to efektywne zarządzanie danymi i dostępem do nich na poziomie użytkownika.

(zgłoszenie) 7

Przywróć pierwszą migawkę.

Podsumowanie:

Po wykonaniu wszystkich czynności z powyższej instrukcji przeczytaj ponownie z zrozumieniem cel ogólny i cele szczegółowe, które znajdują się na pierwszej stronie instrukcji. Jeżeli one zostały niezrealizowane to powtarzaj wykonanie tej instrukcji w szkole lub/i w domu do momentu zrealizowania.

Podsumowanie: Dokument zawiera pełną instrukcję zaktualizowaną dla Windows 11 24H2, wszystkie ćwiczenia, różnice w interfejsie oraz alternatywne polecenia PowerShell.