13.1 Tworzenie folderów NTFS i udostępnianie folderów w domenie

Cel ogólny lekcji: Nauczenie uczniów tworzenia udostępnionych folderów w środowisku graficznym, przypisywania grupom i użytkownikom uprawnień do udostępnionych folderów, określenia skutków łączenia uprawnień NTFS z uprawnieniami do udostępnionych folderów oraz zatrzymywania udostępniania folderów.

Cele szczegółowe:

1. Uczeń będzie potrafił udostępnić folder.
2. Uczeń będzie potrafił przypisać grupom i użytkownikom uprawnienia do udostępnionego folderu.
3. Uczeń będzie potrafił podłączyć się do udostępnionego folderu.
4. Uczeń będzie potrafił określić skutki łączenia uprawnień NTFS z uprawnieniami do udostępnionych folderów.
5. Uczeń będzie potrafił zatrzymać udostępnianie folderu.

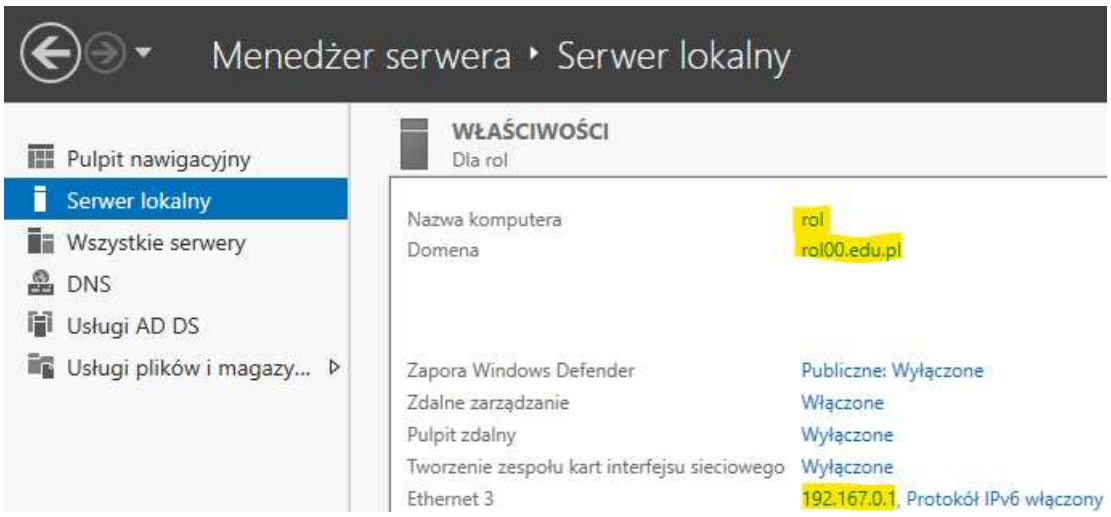
Przed przystąpieniem do ćwiczenia sprawdź i ustaw

W Menedżer funkcji Hyper-V wybierz nazwa maszynę wirtualna twojej grupy_dc2019

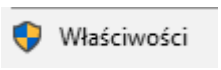
Upewnij się, że punkt kontrolny, zawiera serwer z zainstalowanym kontrolerem domeny.

Uruchom maszynę > Ctrl+Alt+Delete > Administrator > zaq1@WSX

a) system serwera są jak poniżej:



> 192.167.0.1 > 

> 

>

DHCP włączone	Nie
Adres IPv4	192.167.0.1
Maska podsieci IPv4	255.255.255.0
Brama domyślna IPv4	
Serwer DNS IPv4	192.167.0.1

b) klienta (Windows 11) w Menedżer funkcji Hyper-V wybierz nazwa maszynę wirtualna twojej grupy_11 i uruchom, jak będzie potrzebna w zadaniu

Podaj login: admin lub Administrator i hasło: zaq1@WSX

Adres ip - 192.167.0.21/24; brama 192.167.0.1; dns-192.167.0.1

W zeszycie opisz procedury tworzenie udostępnionych folderów.

Wszystkie wpisywane polecenia mają być w zeszycie z opisem co robią poszczególne elementy!

Procedura tworzenia udostępnionych folderów w środowisku graficznym.

Cele laboratorium

Po zrealizowaniu tego laboratorium uczeń będzie potrafił:

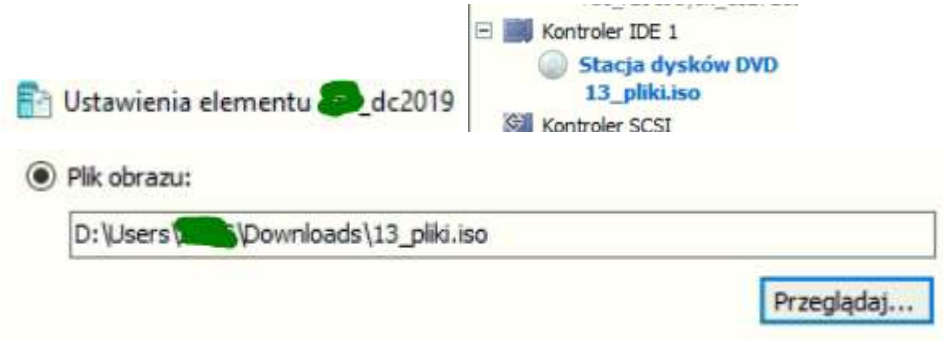
1. Udostępnić folder.
2. Przypisać grupom i użytkownikom uprawnienia do udostępnionego folderu.
3. Podłączyć się do udostępnionego folderu.
4. Określić skutki łączenia uprawnień NTFS z uprawnieniami do udostępnionego folderu.
5. Zatrzymać udostępnianie folderu. Sprawdź poprawność wykonanych zadań w GIU.

Ćwiczenie 1

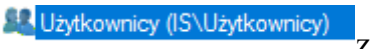
NTFS i udostępnianie folderów

1. Utworzyć konta użytkowników w tym celu

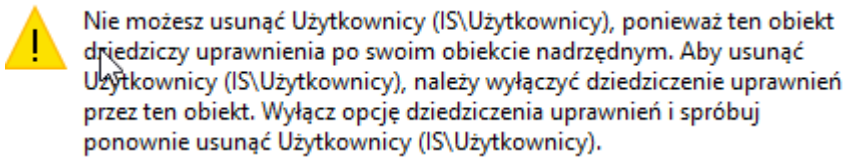
- podłącz do maszyny serwera pobrany z folderu z instrukcją plik 13_pliki.iso i otwórz w serwerze Windows zawartość napędu w Menedżer funkcji Hyper-V:



- na serwerze otwórz stacja dysków DVD (D:) plik 13.1dodajdogrupy.txt
- wybierz w notatniku Ctrl+A > Ctrl+C
- na serwerze przejdź do cmd i wybierz Ctrl+V > enter

2. Na serwerze jest na dysku C:\ folder o nazwie **GRUPY** i podfolder **DANE_GRUP**.
3. Czy możliwe jest usuniecie grupy **Użytkownicy** 

z listy uprawnionych do korzystania z foldera C:\GRUPY\DANE_GRUP? **Odpowiedz w zeszycie uzasadnij**.



4. Wyłącz dziedziczenie uprawnień do folderu C:\GRUPY. Jak wyłączyć dziedziczenie w C:\GRUPY? Instrukcja dla ucznia (GUI, krok po kroku):
   a. Kliknij PPM na folderze C:\GRUPY > Właściwości
   b. Przejdź do zakładki Zabezpieczenia
   c. Kliknij Zaawansowane
   d. W dolnej części okna kliknij przycisk: „Wyłącz dziedziczenie”
   e. System zapyta:

   ✓ „Konwertuj odziedziczone uprawnienia na jawne”

   ✓ „Usuń wszystkie uprawnienia dziedziczone z tego obiektu”

   > wybierz pierwszą opcję:

   „Konwertuj odziedziczone uprawnienia na jawne uprawnienia dla tego obiektu”

   Dlaczego? Bo wtedy uprawnienia stają się lokalne i można je usuwać pojedynczo.
5. Czy teraz jest możliwe usuniecie grupy **Użytkownicy** z listy uprawnionych do korzystania z foldera DANE_GRUP?

   Tu jest klucz: ✓ Jeśli uczeń wyłączył dziedziczenie TYLKO na C:\GRUPY

   to: C:\GRUPY\DANE_GRUP > dalej dziedziczy, więc:

   ❌ NIE można usunąć grupy **Użytkownicy**, bo wpis jest dziedziczony z GRUPY.

   > Uczeń powinien zauważyć: „W folderze DANE_GRUP nadal nie mogę usunąć grupy **Użytkownicy**.”
6. Do folderu C:\GRUPY przypisz grupie Grupa1 uprawnienia:

   uprawnienia domyślne (czyli: Odczyt, Odczyt i wykonywanie, Wyświetlanie zawartości folderu), oraz Zapis.

7. Grupie Grupa2 przypisz: Wyświetlanie zawartości folderu, Odczyt, Odczyt i wykonywanie, oraz Odmów (DENY) prawa Zapis.
8. Jakie są efektywne uprawnienia NTFS poszczególnych użytkowników?

Grupa1 – może modyfikować (może otwierać pliki, może tworzyć nowe pliki, może zapisywać zmiany, może usuwać pliki.) W skrócie: Grupa1 ma zapis i modyfikację.

Grupa2 – tylko ogląda (może wejść do folderu, może otwierać pliki, może czytać zawartość.

❌ Nie może: (zapisywać zmian, tworzyć nowych plików, usuwać plików.

Dlaczego? Bo ma ustawione Odmów (DENY) Zapis, a DENY ma pierwszeństwo przed wszystkimi innymi uprawnieniami.

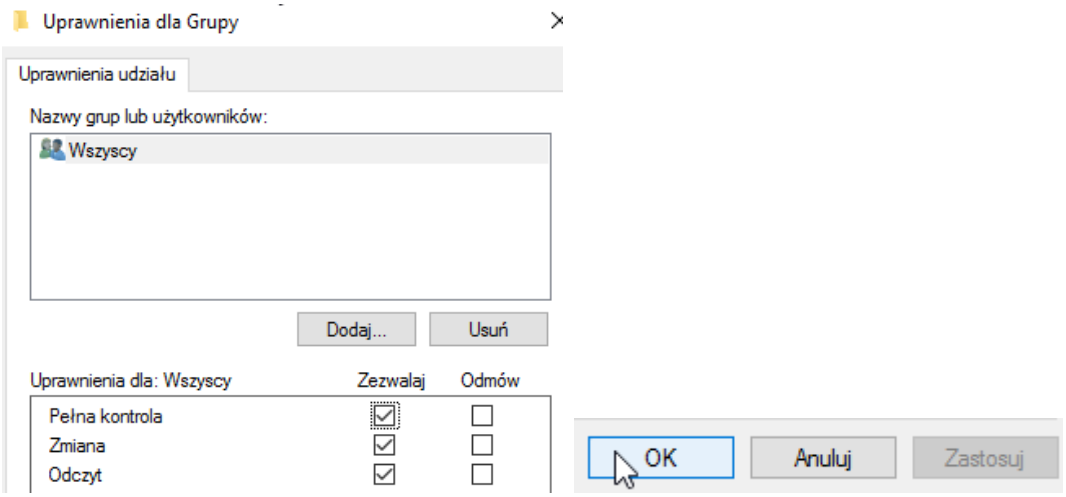
9. Zwróć szczególną uwagę na użytkownika klient3.

Z pliku konfiguracyjnego wynika, że: klient3 jest członkiem Grupa2.To oznacza, że: klient3 może: wejść do folderu C:\GRUPY, wyświetlać listę plików, czytać pliki.

klient3 NIE może: niczego zapisać, niczego stworzyć, niczego usunąć.

Powód: Należy do Grupa2, a ta grupa ma ustawione DENY Zapis, które blokuje zapis bez względu na wszystko inne.

10. Nadaj grupie „Administratorzy” pełne uprawnienia (Pełna kontrola) do folderu C:\GRUPY.
11. Pobrać do folderu C:\GRUPY plik Admin2.txt, który znajduje się w D:\.
12. Udostępnij folder **GRUPY** z uprawnieniami jak na rysunku poniżej



a. Kliknij PPM na folderze C:\GRUPY
b. Wybierz Właściwości
c. Przejdź do zakładki Udostępnianie
d. Kliknij Udostępnianie zaawansowane
e. Zaznacz Udostępnij ten folder
f. Kliknij Uprawnienia

W oknie, które widzisz na screenie:

Powinna być tylko grupa Wszyscy

Dla Wszyscy powinny być zaznaczone: Pełna kontrola, Zmiana, Odczyt

g. Kliknij Zastosuj > OK

13. Zaloguj się na kliencie (Windows 11 podłączony do domeny) kolejno do kont domenowych (przed logowaniem sugeruje zmianę haseł na zaq1@WSX i odznaczenie wymuszenia zmiany hasła przy pierwszym logowaniu) jako klient1, klient3 oraz klient5 i wykonaj na pliku Admin.txt kolejno operacje: przeglądania pliku, zmiany zawartości pliku i zapisu, usunięcia pliku. **Zanotuj w zeszycie wykonanie których operacji było możliwe?** Powtórz operacje w wierszu poleceń.

Bardziej dokładnie: W tym zadaniu sprawdzasz **efektywne uprawnienia NTFS** dla różnych użytkowników po zalogowaniu się do domeny. Masz 3 konta domenowe:

- **klient1** (Grupa1 > ma zapis)
- **klient3** (Grupa2 > tylko odczyt)
- **klient5** (Grupa2 > tylko odczyt)

Plik testowy: **Admin.txt** w folderze **C:\GRUPY**

Twoim celem jest sprawdzenie: czy możesz plik przeglądać, czy możesz zmienić jego zawartość i zapisać, czy możesz go usunąć.

Po każdej próbie wpiszesz w zeszycie: "TAK – mogłem" albo "NIE – nie miałem uprawnień".

Krok po kroku - co masz zrobić na komputerze klienckim (Windows 11)

Przed logowaniem:

1. Zaloguj się jako administrator domeny.
2. Wejdź do Active Directory Users and Computers.
3. Dla kont klient1, klient3, klient5: odznacz opcję "Wymuś zmianę hasła przy pierwszym logowaniu".

2. Zaloguj się jako kolejni użytkownicy

Zrób trzy rundy testowe - każda na innym koncie:

- najpierw **klient1**
- potem **klient3**
- potem **klient5**

Za każdym razem:

1. Zrestartuj sesję (Wyloguj).
2. Zaloguj się jako domena\klient1 (lub klient3, klient5).
3. Otwórz **Eksplorator plików**.
4. Przejdź do udziału sieciowego:

\\NAZWA_SERWERA\GRUPY

albo jeśli mapowaliście dysk:

Z:\GRUPY

Tam znajdziesz plik **Admin.txt**.

3. Wykonaj test trzech operacji na pliku Admin.txt

Dla każdego użytkownika wykonaj TE SAME trzy próby:

A) Przeglądanie pliku

- Otwórz plik **Admin.txt** dwuklikiem.
- Sprawdź, czy pokazuje się jego zawartość.

Zapisz w zeszycie: „Przeglądanie – TAK/NIE”

B) Zmiana zawartości i zapis

1. Otwórz plik.
2. Dopisz na końcu jedną linijkę, np. *test klient3*.
3. Spróbuj zapisać: **Ctrl + S**.
4. Sprawdź, czy pojawia się komunikat o braku uprawnień.

Zapisz w zeszycie: „Edycja i zapis – TAK/NIE”

C) Usunięcie pliku

1. Kliknij prawym na **Admin.txt**.
2. Wybierz **Usuń**.
3. Sprawdź, czy system pozwoli wykonać operację.

Zapisz w zeszycie: „Usunięcie pliku – TAK/NIE”

4. Powtórz te same operacje w wierszu poleceń (CMD)

1. Uruchom **CMD** (Win + R > cmd).
2. Przejdź do udziału:

cd \\NAZWA_SERWERA\GRUPY

3. Wpisz:

Przeglądanie:

type Admin.txt

Próba edycji (np. dopisanie linijki):

echo test >> Admin.txt

Próba usunięcia:

del Admin.txt

W zeszycie dopisz, która z tych operacji się udała, a która nie.

5. Jakie powinny być wyniki? (dla nauczyciela i ucznia)

Użytkownik	Grupa	Efektywne uprawnienia	Przeglądanie	Zapis/edycja	Usunięcie
klient1	Grupa1	Modyfikacja (ma zapis)	TAK	TAK	TAK
klient3	Grupa2	Tylko odczyt (DENY Write)	TAK	**NIE**	**NIE**
klient5	Grupa2	Tylko odczyt (DENY Write)	TAK	**NIE**	**NIE**

Dlaczego klient3 i klient5 nie mogą zapisać ani usunąć?

> Bo Grupa2 ma ustawiony **DENY Zapis**, który blokuje zapis nawet wtedy, gdy użytkownik miałby inne uprawnienia.

Podsumowanie dla ucznia (notatka do zeszytu)

klient1 – może wszystko robić z plikiem, bo należy do Grupa1, która ma zapis.

klient3 i klient5 – mogą tylko czytać plik; zapis i usunięcie są zablokowane przez DENY Zapis dla Grupa2.

Powtórzenie testów w CMD pomaga zrozumieć, że uprawnienia działają tak samo w GUI i w wierszu poleceń.

14. Przejrzyj i zanotuj zaawansowane prawa dostępu do zasobów plikowych:
    - pliku Admin.txt
    - folderu DANE_GRUP

Jak sprawdzić zaawansowane prawa dostępu NTFS?

W tym zadaniu masz sprawdzić, jakie **dokładne** (szczegółowe) uprawnienia NTFS ma:

- plik **Admin.txt**,
- folder **DANE_GRUP**.

To są tzw. **zaawansowane prawa dostępu** - bardziej szczegółowe niż zwykłe: Odczyt / Zapis / Modyfikacja. Tu zobaczysz wpisy typu: (Usuń), (Zapis danych), (Odczyt atrybutów), itd.

Krok po kroku - folder lub plik (instrukcja identyczna dla obu)

1. Otwórz właściwości elementu

1. Wejdź do udziału sieciowego lub lokalnego folderu, gdzie znajduje się:
    - plik **Admin.txt**,
    - folder **DANE_GRUP**.
2. Kliknij prawym przyciskiem myszy:
    - na pliku **Admin.txt**, albo

- na folderze **DANE_GRUP**.

3. Wybierz **Właściwości**.

2. Przejdź do zakładki Zabezpieczenia

1. W oknie właściwości kliknij zakładkę **Zabezpieczenia**.
2. Kliknij **Zaawansowane**.

To otwiera widok **zaawansowanych uprawnień NTFS**.

3. Sprawdź listę wpisów uprawnień. W oknie „Zaawansowane ustawienia zabezpieczeń" zobaczysz listę:

- **kto** (np. Administratorzy, Grupa1, Grupa2, SYSTEM)
- **jakie dokładnie ma prawa**
- czy wpis jest **dziedziczony**, czy **jawny**
- jaki jest **typ** wpisu (Zezwalaj / Odmów)

Uczeń powinien zwrócić uwagę na kolumny:

- **Typ** (Zezwalaj / Odmów)
- **Podmiot** (nazwa grupy lub użytkownika)
- **Uprawnienia** (lista praw szczegółowych)
- **Dziedziczone z**
- **Zastosowanie do** (tylko ten folder? podfoldery? pliki?)

4. Aby zobaczyć szczegóły konkretnej grupy

1. Kliknij dwa razy na wybranym wpisie (np. na **Grupa1**).
2. Otworzy się okno z pełną listą praw:
    - odczyt atrybutów,
    - zapis danych,
    - tworzenie plików,
    - usuwanie,
    - usuwanie podfolderów,
    - zmiana uprawnień,
    - przejmowanie na własność,
    - i wiele innych.

Co uczeń powinien zanotować w zeszycie

1. Admin.txt – kto ma jakie prawa?

Należy wypisać:

- Administratorzy – Pełna kontrola (wszystkie prawa zaznaczone)
- Grupa1 – prawo modyfikacji > w szczegółach: może zapisywać, usuwać, edytować

- Grupa2 – tylko odczyt > w szczegółach: brak praw zapisu i usuwania, DENY Write (jeśli ustawione)

Uczeń powinien dopisać:

Plik Admin.txt dziedziczy uprawnienia z folderu GRUPY, chyba że instrukcja nakazuje inaczej.

2. Folder DANE_GRUP – jakie są prawa i które są dziedziczone?

Uczeń powinien sprawdzić:

- Czy folder **DANE_GRUP** nadal dziedziczy uprawnienia z C:\GRUPY
- Czy są wpisy typu:
    - Administratorzy – pełna kontrola
    - Grupa1 – zapis / modyfikacja
    - Grupa2 – odczyt
    - SYSTEM – pełna kontrola (zwykle automatycznie)

Uczeń ma zanotować:

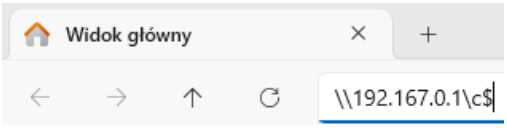
- które prawa są **dziedziczone**,
- które są **jawne**,
- oraz **dla kogo obowiązuje DENY (odmowa)**.

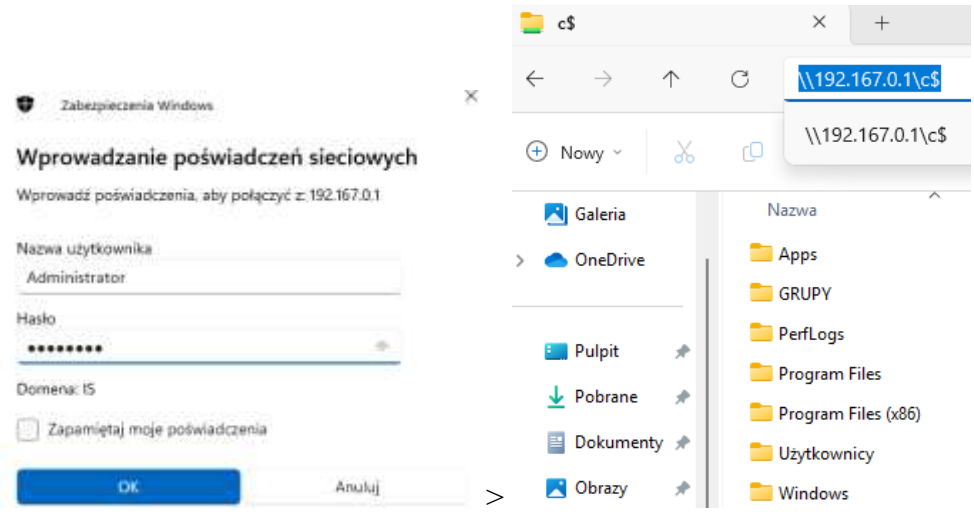
Krótka notatka do zeszytu (idealna)

Zaawansowane prawa dostępu pokazują szczegółowe uprawnienia NTFS dla plików i folderów. Sprawdziłem je dla pliku *Admin.txt* i folderu *DANE_GRUP*.

Widziałem, które prawa są dziedziczone, które są jawne oraz jakie dokładnie operacje mogą wykonywać poszczególne grupy (np. Grupa1 – zapis/modyfikacja, Grupa2 – tylko odczyt).

15. Zaloguj się na kliencie do domenowego konta **klient3**: rol00\klient3 lub klient3@rol00.edu.pl
16. Na kliencie (Windows 11) przejdź na dysk serwera
    a. Zaloguj się na komputerze klienckim (Windows 11).
    b. Otwórz Eksplorator plików (ikonka folderu na pasku zadań lub skrót Win + E).
    c. W pasku adresu na górze wpisz:





17. Z komputera klienckiego utwórz z poziomu dysku serwera plik C:\GRUPY\klient3.txt

a. Utwórz nowy plik klient3.txt

Będąc w folderze GRUPY, kliknij PPM > Nowy > Dokument tekstowy

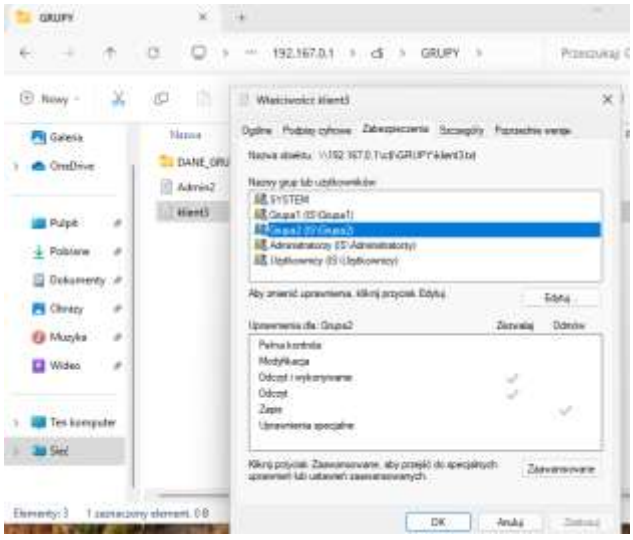
Zmień nazwę na: klient3.txt

b. Sprawdź uprawnienia pliku

1. Kliknij prawym przyciskiem myszy na **klient3.txt**
2. Wybierz **Właściwości**
3. Przejdź do zakładki **Zabezpieczenia**

Zobaczysz tam grupy i ich uprawnienia - zwykle:

- Administratorzy
- SYSTEM
- Grupa1
- Grupa2



Te wpisy NIE pojawiły się przypadkowo - zostały **odziedziczone**.

4. Zobacz szczegóły (zaawansowane prawa)

1. Kliknij **Zaawansowane**
2. Zwróć uwagę na kolumny:
    - **Typ** (Zezwalaj / Odmów)
    - **Podmiot** (kto ma uprawnienia)
    - **Dziedziczone z**
    - **Uprawnienia**

Uczniowie powinni zobaczyć, że przy pliku **klient3.txt** jest napis:

Dziedziczone z > C:\GRUPY

To jest najważniejsza część zadania.

c. Dlaczego plik ma właśnie takie uprawnienia? - wyjaśnienie dla ucznia

Po utworzeniu nowego pliku, Windows nie tworzy uprawnień od zera.

Zamiast tego: Nowy plik dziedziczy uprawnienia ze swojego folderu nadrzędnego.

Czyli: Jeśli folder C:\GRUPY ma dla Grupa1 > Modyfikacja,

dla Grupa2 > Tylko odczyt + DENY Write,

dla Administratorów > Pełna kontrola,

to dokładnie te same uprawnienia dostanie nowo utworzony plik klient3.txt.

Plik nie „wie", kto go stworzył - po prostu bierze prawa z folderu.

i przejrzyj jego prawa dostępu.

Zanotuj w zeszycie, dlaczego są takie prawa?

Notatka, którą uczeń powinien wpisać do zeszytu

Plik klient3.txt ma takie uprawnienia, ponieważ dziedziczy je z folderu C:\GRUPY.

Folder GRUPY miał wcześniej ustawione uprawnienia dla Administratorów, Grupa1 i Grupa2, dlatego te same wpisy pojawiły się w nowym pliku.

Dziedziczenie NTFS oznacza, że wszystkie nowe pliki i foldery automatycznie przejmują uprawnienia od folderu nadrzędnego.

Efekt, który uczeń powinien zauważyć

Grupa1 > może otworzyć i zapisać klient3.txt

Grupa2 > tylko odczyt (nie zapisze, bo DENY)

Administratorzy > wszystko

SYSTEM > wszystko (Windowsowe konto systemowe)

18. Zmień dziedziczenie praw dostępu do katalogu na dysku serwera C:\GRUPY tak aby uprawnienia dla tego katalogu dotyczyły tylko tego folderu.

W tym zadaniu masz sprawić, aby folder C:\GRUPY nie przekazywał swoich uprawnień dalej do podfolderów, takich jak DANE_GRUP.

Czyli:

> uprawnienia mają działać tylko na folder GRUPY,

> nie mają automatycznie przechodzić na podfoldery ani pliki.

To nazywamy wyłączeniem dziedziczenia w dół.

Krok po kroku - instrukcja dla ucznia

1. Otwórz właściwości folderu GRUPY
    1. Przejdź na serwer lub otwórz udział sieciowy z serwera:\\NAZWA_SERWERA\GRUPY
    2. Kliknij prawym przyciskiem **GRUPY**
    3. Wybierz **Właściwości**

2. Przejdź do ustawień zabezpieczeń
    1. Kliknij zakładkę **Zabezpieczenia**
    2. Kliknij **Zaawansowane**

Otworzy się okno „Zaawansowane ustawienia zabezpieczeń".

3. Wyłącz dziedziczenie
    1. Kliknij przycisk **Wyłącz dziedziczenie**
    2. Pojawią się dwie opcje:

✓ Konwertuj odziedziczone uprawnienia na jawne uprawnienia

✓ Usuń wszystkie uprawnienia dziedziczone z tego obiektu

Wybierz pierwszą opcję, czyli: „Konwertuj odziedziczone uprawnienia na jawne"

Dlaczego? Bo chcemy dalej widzieć wszystkie uprawnienia, ale **bez ich przekazywania dalej**.

4. Zatrzymaj przekazywanie uprawnień na podfoldery

Teraz musisz ustawić, aby wpisy w folderze GRUPY:

- obowiązywały **TYLKO** dla tego folderu,
- nie obowiązywały dla plików i podfolderów.

Jak to zrobić?

1. Na liście uprawnień kliknij dwa razy każdy wpis (np. Grupa1, Grupa2, Administratorzy).
2. W oknie „Wpis uprawnień" znajdziesz pole **„Dotyczy:"**
3. Zmień je na: Tylko ten folder
4. Kliknij **OK**.
5. Zrób to samo dla wszystkich wpisów.

Po tej zmianie:

- folder **C:\GRUPY** ma swoje własne uprawnienia,
- ale **DANE_GRUP** NIE dostaje automatycznie tych samych praw.

Co uczeń powinien zauważyć?

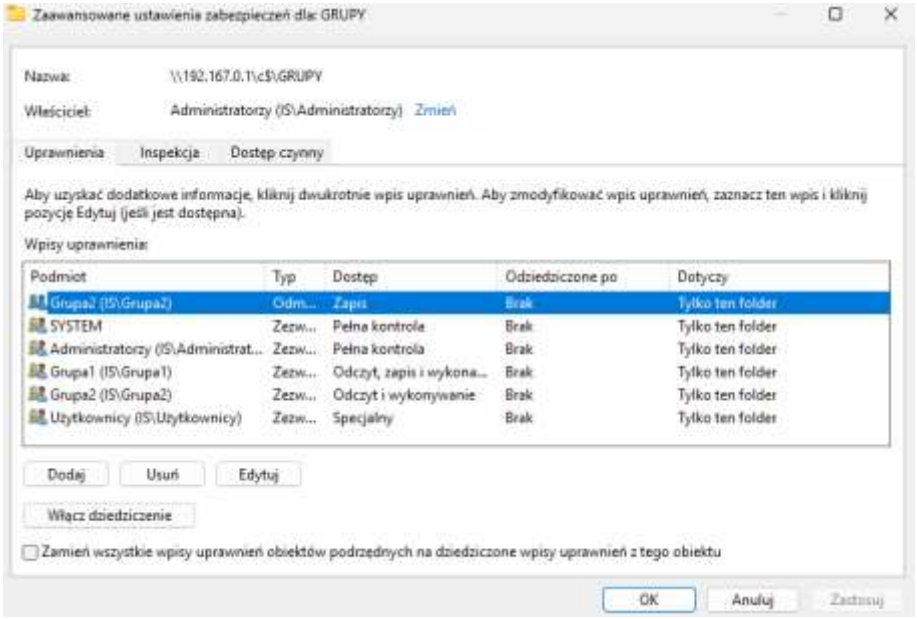
Po wykonaniu zadania:

- folder **C:\GRUPY** ma uprawnienia ustawione ręcznie,
- **podfolder DANE_GRUP ma swoje uprawnienia niezależne**,
- dziedziczenie jest wyłączone, czyli **nic nie jest przekazywane w dół**.

Notatka do zeszytu

Wyłączyłem dziedziczenie w folderze **C:\GRUPY** i ustawiłem, aby jego uprawnienia obowiązywały **tylko w tym folderze**.

Dzięki temu podfoldery (np. DANE_GRUP) nie przejmują jego praw i mogą mieć własne, oddzielne uprawnienia.



19. Z komputera klienckiego będąc zalogowany jako **klient3** spróbuj utworzyć na dysku serwera plik \\192.168.0.1\c$\GRUPY\DANE_GRUP\klient31.txt.

Zapisz w zeszycie czy udało się utworzyć plik? Sprawdzić prawa dostępu do C:\GRUPY i zanotuj je w zeszycie.

Odpowiedź zadanie 19: Nie, pliku nie udało się utworzyć.

Folder DANE_GRUP nie posiada prawa Zapis, a uprawnienia z C:\GRUPY nie są już dziedziczone.

Prawa dostępu do folderu C:\GRUPY:

Administratorzy – pełna kontrola

Grupa1 – modyfikacja

Grupa2 – odczyt + DENY Zapis

SYSTEM – pełna kontrola

Uprawnienia dotyczą tylko tego folderu („Tylko ten folder”), bo dziedziczenie zostało wyłączone.

Dlaczego klient3 nie może utworzyć pliku?

✓ klient3 należy do Grupa2

A Grupa2 ma ustawione w NTFS:

Odczyt

Wyświetlanie zawartości

Wykonywanie

DENY ZAPIS

To oznacza:

❌ brak prawa tworzenia plików

❌ brak prawa zapisu

❌ brak prawa modyfikacji

dodatkowo - po zadaniu 18 - folder C:\GRUPY przestał przekazywać uprawnienia do DANE_GRUP

Czyli:

Grupa2 ma DENY Zapis w C:\GRUPY

DANE_GRUP nie dziedziczy już niczego od C:\GRUPY

DANE_GRUP nie ma prawa Zapis ustawionego samodzielnie

Dlatego klient3:

❌ nie może stworzyć żadnego pliku w DANE_GRUP.

Co powinna zawierać odpowiedź ucznia w zeszycie?

„Jestem zalogowany jako klient3. Próba utworzenia pliku klient31.txt > NIEUDANA.

Folder DANE_GRUP nie ma prawa Zapis, a użytkownik klient3 należy do Grupa2, która ma DENY Zapis.”

Ćwiczenie 2

Udostępnianie folderów z zainstalowaną aplikacją.

Użytkownicy w twojej sieci muszą mieć dostępu do aplikacji na serwerze, którym administrujesz.

1. Na serwerze na dysku C: jest folder o nazwie **Apps.**
2. Zainstaluj z dysku D:\ pliku tcmd1156x64.exe aplikacje total comander w folderze o nazwie C:**Apps** z domyślnymi ustawieniami
3. Przypisz uprawnienia NTFS do aplikacji, znajdujących się wewnątrz folderu dla grup użytkowników serwera. tak, aby:

✓ Grupa Administratorzy (tylko sprawdź)

Pełna kontrola - mogą zmieniać pliki, aktualizować program, naprawiać błędy.

✓ Grupa1

Odczyt i wykonanie - mogą korzystać z programu, ale nie mogą go modyfikować.

✓ Grupa2 (jeśli wymaga tego ćwiczenie)

Tylko Odczyt - mogą program uruchamiać, ale nie mogą niczego w nim zmieniać.

Pozostaw wyświetlanie.

4. Udostępnij folder **Apps** jako **Apps$**

1. Kliknij PPM na folderze C:\Apps

Otwórz Eksplorator plików

Przejdź do C:\Apps

Kliknij prawym przyciskiem myszy

Wybierz Właściwości

2. Wejdź do zakładki „Udostępnianie”

Kliknij zakładkę Udostępnianie

Kliknij Udostępnianie zaawansowane

Zaznacz pole: Udostępnij ten folder

3. Ustaw nazwę udziału na „Apps$” (jeśli nie jest ustawiona)

W polu Nazwa udziału wpisz:

Apps$

To sprawi, że zasób jest udostępniony, ale niewidoczny na liście udziałów (trzeba wpisać go ręcznie, np. \\rol00\Apps$).

5. Skonfiguruj uprawnienia do **Apps$** tak, aby wszyscy użytkownicy mogli uzyskać dostęp do folderu poprzez sieć.

a. Kliknij przycisk „Uprawnienia”

Tutaj ustawiamy share permissions (uprawnienia do udostępnienia).

Usuń wpisy, jeśli są zbędne

Jeśli jest coś innego niż Wszyscy, usuń to.

Dodaj wpis: „Wszyscy”

Kliknij Dodaj…

Wpisz:

Wszyscy

Kliknij OK

b. Nadaj grupie „Wszyscy” pełny dostęp przez sieć

Zaznacz trzy pola:

✓ Pełna kontrola

✓ Zmiana

✓ Odczyt

Dzięki temu:

> Każdy użytkownik domenowy lub lokalny może wejść do Apps$ i zobaczyć zawartość

> OGRANICZENIA będą wynikały z NTFS, a nie z udostępniania (to jest cel ćwiczenia)

Dlaczego tak ustawiamy?

Uprawnienia udostępniania (share) mówią: „Czy użytkownik może wejść przez sieć do folderu?”

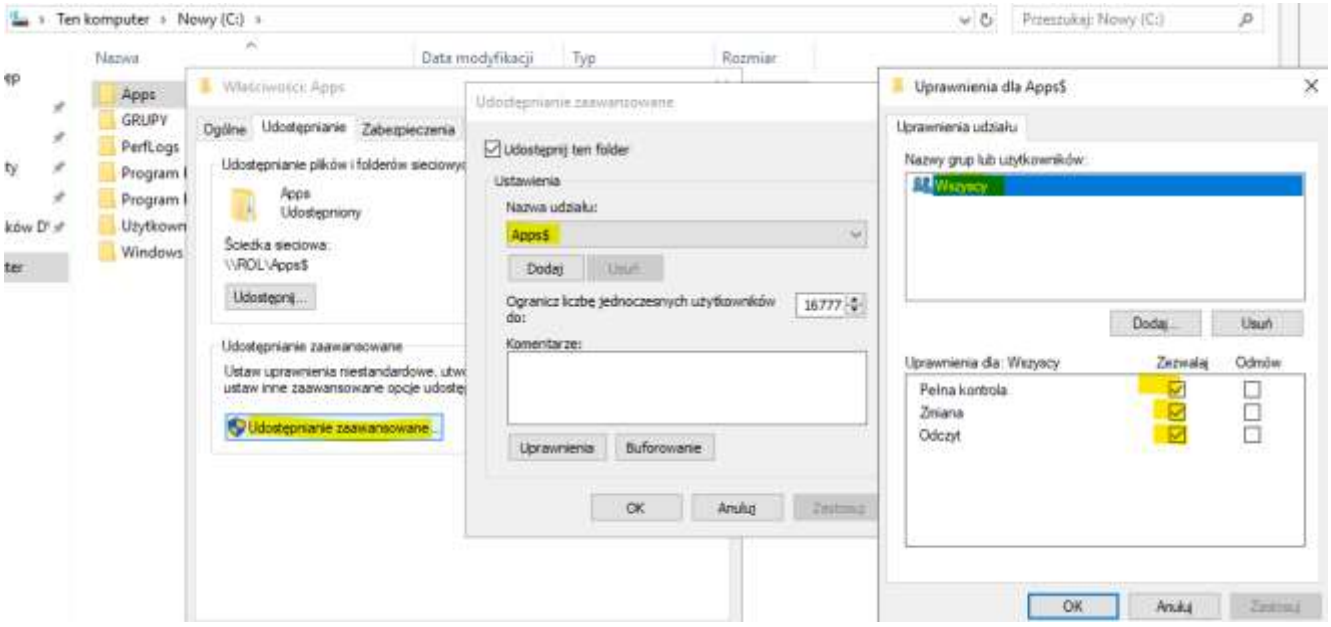
Skoro zadanie mówi, że wszyscy użytkownicy mają mieć dostęp, to:

> w udostępnianiu Apps$ dajemy Wszyscy – pełne prawa,

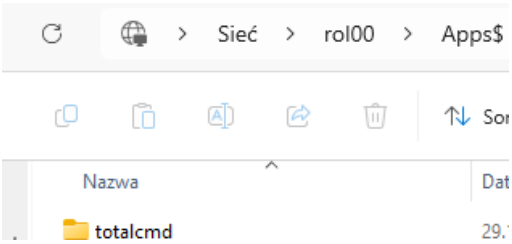
> a dopiero NTFS w środku folderu reguluje, co wolno komu zrobić.

To normalna praktyka w administracji Windows: Share = szeroko, NTFS = dokładnie.

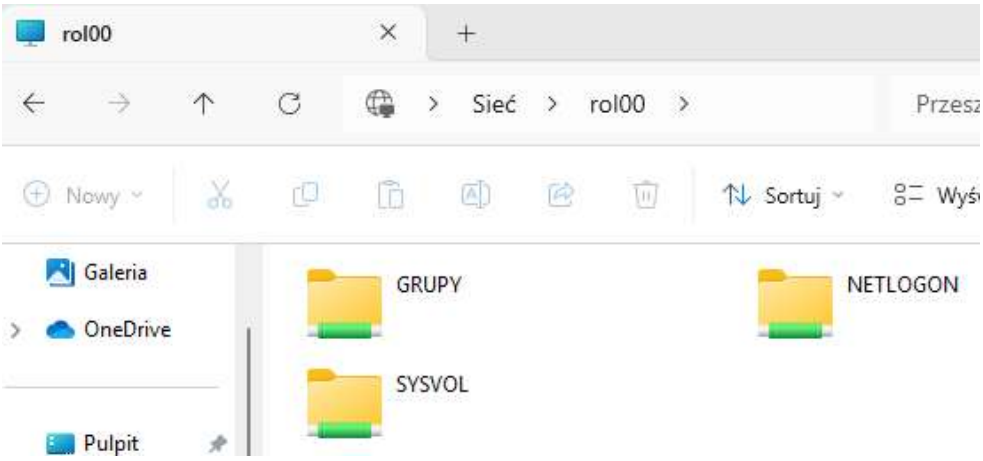
Cel: W tym ćwiczeniu, utworzysz udostępnienia na swoim serwerze, aby użytkownicy mogli mieć dostęp do folderu **Apps$** poprzez sieć.



a) Sprawdź na kliencie z kont użytkowników domenowych (klient3) i zapisz jako wycinek i w zeszycie zapisz czy na serwerze jest dostęp do ukrytego zasobu Apps$



b) Sprawdź na kliencie z kont użytkowników domenowych (klient3) i zapisz jako wycinek w zeszycie zapisz czy na serwerze ukryty zasób Apps$ jest widoczny (oczekiwane, aby zasób nie był widoczny).



Ćwiczenie 3

Przypisywanie uprawnień do udostępnionego folderu.

Scenariusz

Udostępniłeś folder, który zawiera aplikacje używane przez wszystkich pracowników firmy, dając możliwość użytkownikom podłączenia się do niego poprzez sieć.

Mimo, że skonfigurowałeś uprawnienia NTFS, założenia bezpieczeństwa w firmie nakazują usunięcie domyślnych uprawnień i zastąpienie ich uprawnieniami wymienionymi w założeniach organizacji.

Aby skonfigurować uprawnienia do udostępnionego folderu, należy określić aktualne uprawniania, a następnie przypisać uprawnienia grupom w domenie, zgodnie z wymogami firmy.

Cel

W tym ćwiczeniu zmodyfikujesz domyślne uprawnienia do folderu Apps tak, aby umożliwić dostęp tylko określonym grupom użytkowników. Oczekiwany efekt końcowy:

- klient1 ma możliwość korzystania z programu w Apps
- klient3 ma ograniczony dostęp zgodnie z NTFS
- każdy użytkownik może wejść na \\serwer\Apps$ (share)
- ale NTFS decyduje, co w środku wolno

Uprawnienia udostępniania (share) określają, kto MOŻE wejść przez sieć do folderu.

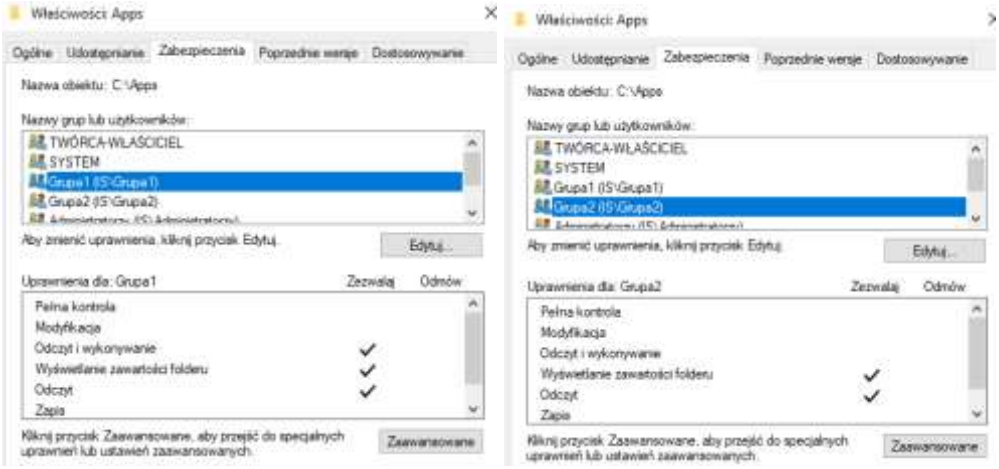
Uprawnienia NTFS decydują, co można zrobić w środku.

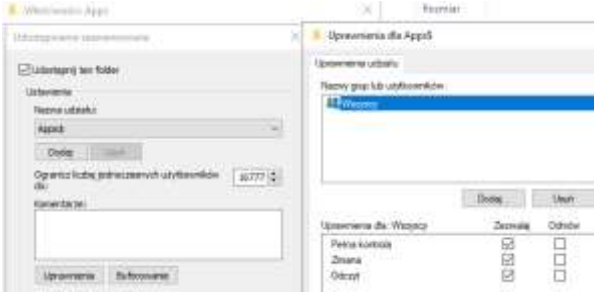
W tym ćwiczeniu celowo ustawiamy share szeroko, a NTFS precyzyjnie.

W tym ćwiczeniu logujemy się jako klient1 i klient3, aby porównać różnice.

Założenia bezpieczeństwa w firmie:

- użytkownicy mogą uruchamiać programy, ale nie mogą ich modyfikować,
- administratorzy zarządzają aplikacjami i mają pełną kontrolę,
- Apps$ musi być dostępny dla wszystkich przez sieć,
- NTFS ogranicza działania użytkowników (tylko odczyt i wykonywanie),
- brak możliwości zapisu chroni aplikację przed uszkodzeniem,
- folder C:\Apps ma świadomie skonfigurowane uprawnienia.
- Firma wymaga następującej konfiguracji NTFS dla folderu C:\Apps:
    - Administratorzy – pełna kontrola
    - Grupa1 – odczyt i wykonanie (Read & Execute)
    - Grupa2 – tylko odczyt
    - Nie powinno być grupy Wszyscy (Everyone) w NTFS
    - Udostępnienie Apps$ ma dawać dostęp przez sieć wszystkim użytkownikom
    - Ograniczenia mają wynikać z NTFS, nie z udostępniania





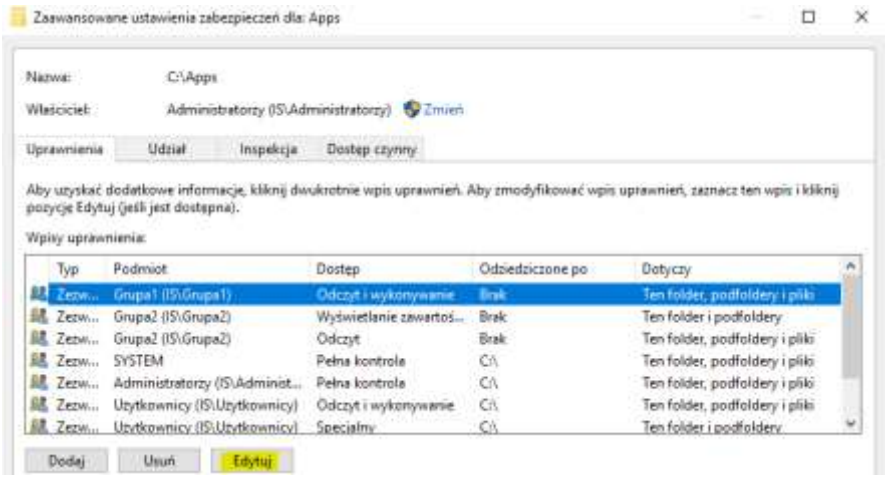
1. Sprawdź i zapisz jako wycinek listę efektywnych uprawni NTFS użytkownika **klient1** i **klient3** do C:\Apps. Do jakiej grupy należy konto **klient3**, jaki uprawnienia ma ta grupa do C:\Apps.
    1. Zaloguj się na komputerze klienckim jako użytkownik **klient1**.
    2. Otwórz Eksplorator plików Przejdź do lokalizacji: \\ROL\c$
    3. Sprawdź efektywne uprawnienia użytkownika **klient1**:
        - Kliknij prawym przyciskiem na folder **Apps**
        - Wybierz **Właściwości**
        - Przejdź do zakładki **Zabezpieczenia**
        - Kliknij **Zaawansowane**
        - Kliknij przycisk **Dostęp czynny (Effective Access)**
        - Kliknij **Wybierz użytkownika** → wpisz: klient1
        - Zatwierdź i odczytaj listę uprawnień.
        - **Zapisz jako wycinek ekranu** wynik efektywnych uprawnień klient1.
    4. Wyloguj się i zaloguj jako użytkownik klient3.
    5. **Powtórz te same czynności** dla użytkownika klient3:
        - Właściwości folderu **Apps**
        - Zabezpieczenia → Zaawansowane
        - Dostęp czynny
        - Dodaj użytkownika: klient3
        - Odczytaj uprawnienia i **zapisz wycinek ekranu**.
    6. Ustal, do jakiej grupy należy użytkownik klient3:
        - Na serwerze uruchom **Active Directory Users and Computers**
        - Odszukaj konto **klient3**
        - Otwórz właściwości konta
        - Przejdź do zakładki **Członek grup (Member Of)**
        - Zanotuj, do jakich grup należy klient3 (najważniejsze: **Grupa2**).
    7. **Na podstawie członkostwa w grupie odpowiedz w zeszycie:**
        - Jakie uprawnienia ma grupa, do której należy klient3, do folderu **C:\Apps**?
        - Jakie to daje efektywne uprawnienia dla użytkownika klient3?

Oczekiwany zapis w zeszycie ucznia

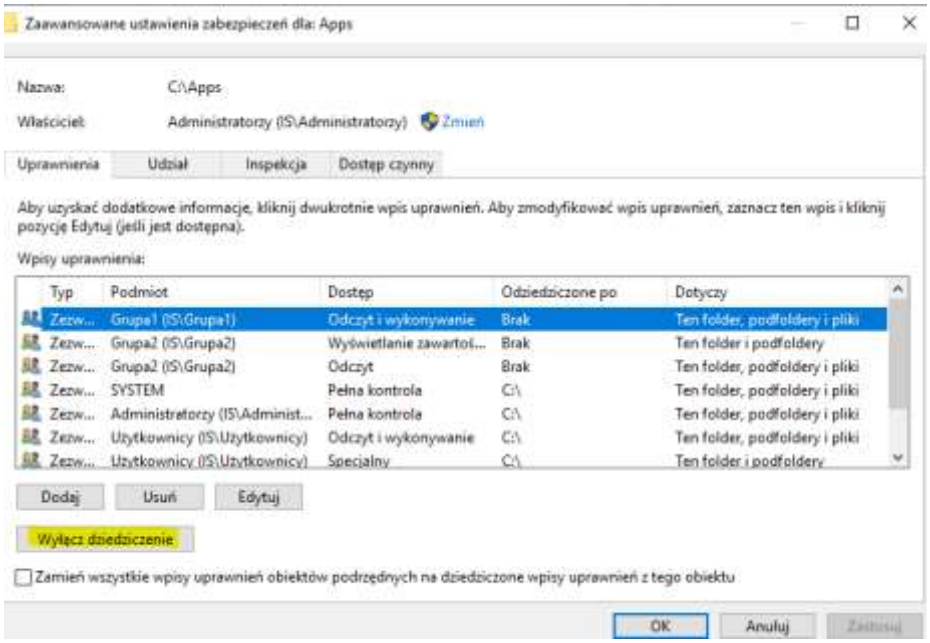
(krótka forma do przepisania – nie musisz kopiować)

- **klient1** – członek *Grupa1*, efektywne uprawnienia: *Odczyt i wykonywanie*
- **klient3** – członek *Grupa2*, efektywne uprawnienia: *Tylko odczyt*
- Uprawnienia wynikają z NTFS folderu **C:\Apps**

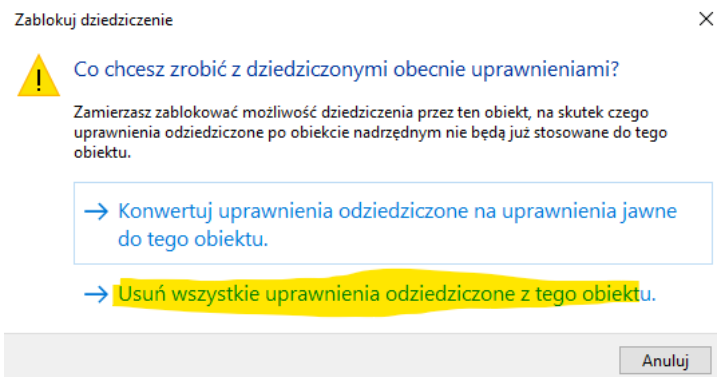
Edytuj zawansowane uprawnienia



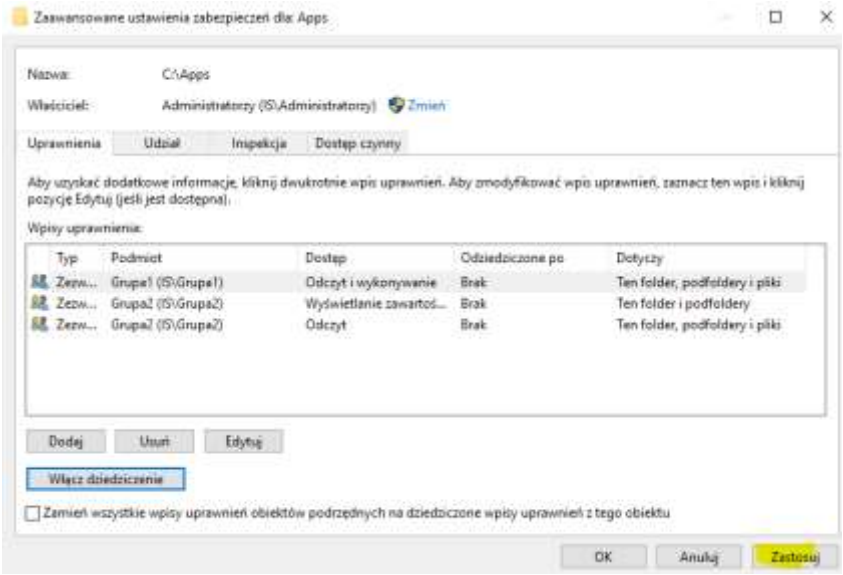
Wyłącz dziedziczenie



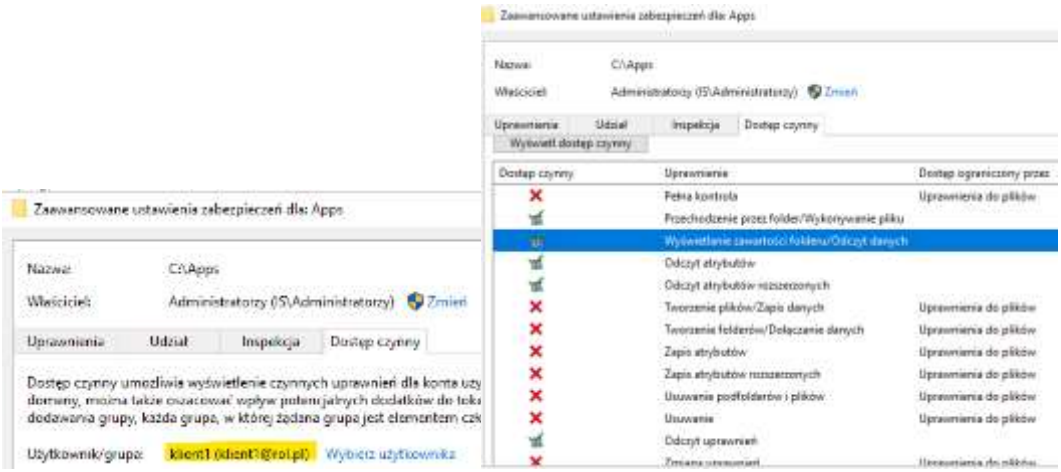
Usuń niepotrzebne wpisy



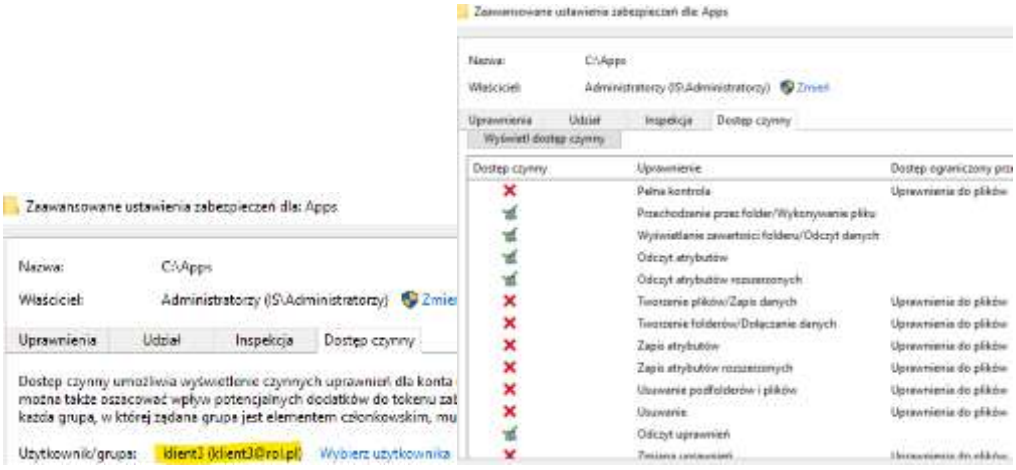
Efekt:



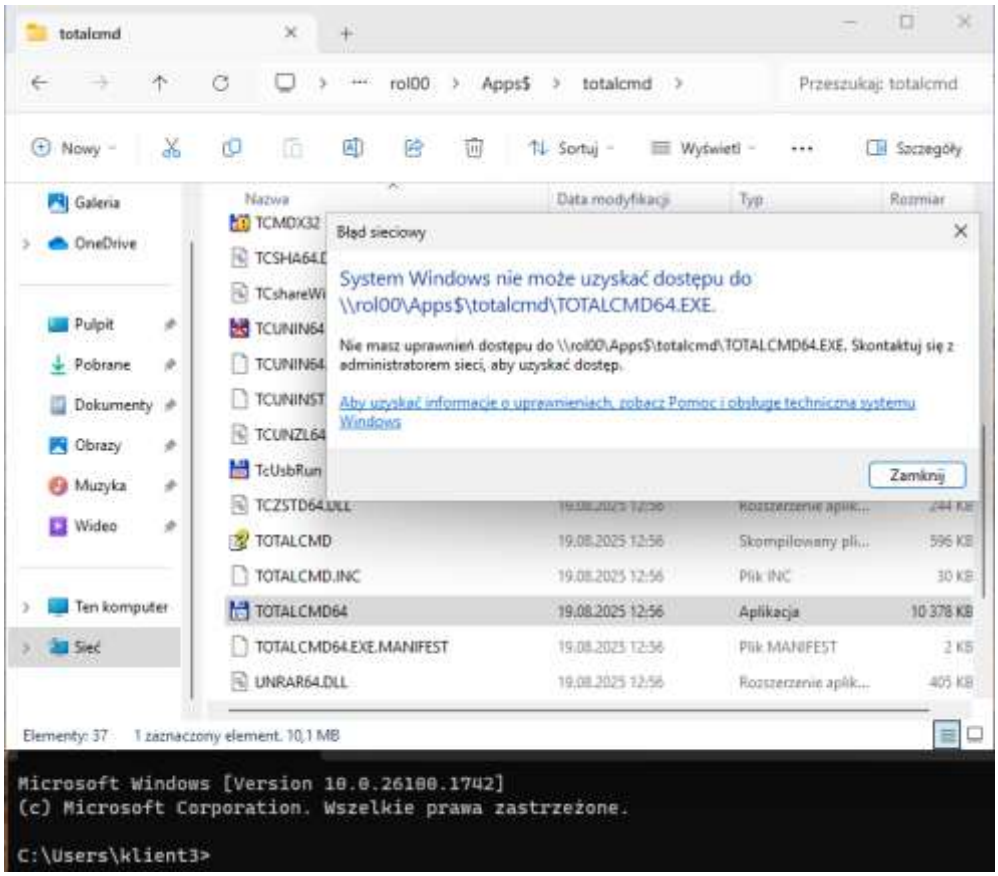
Wyświetl efektywne uprawnienia klient1



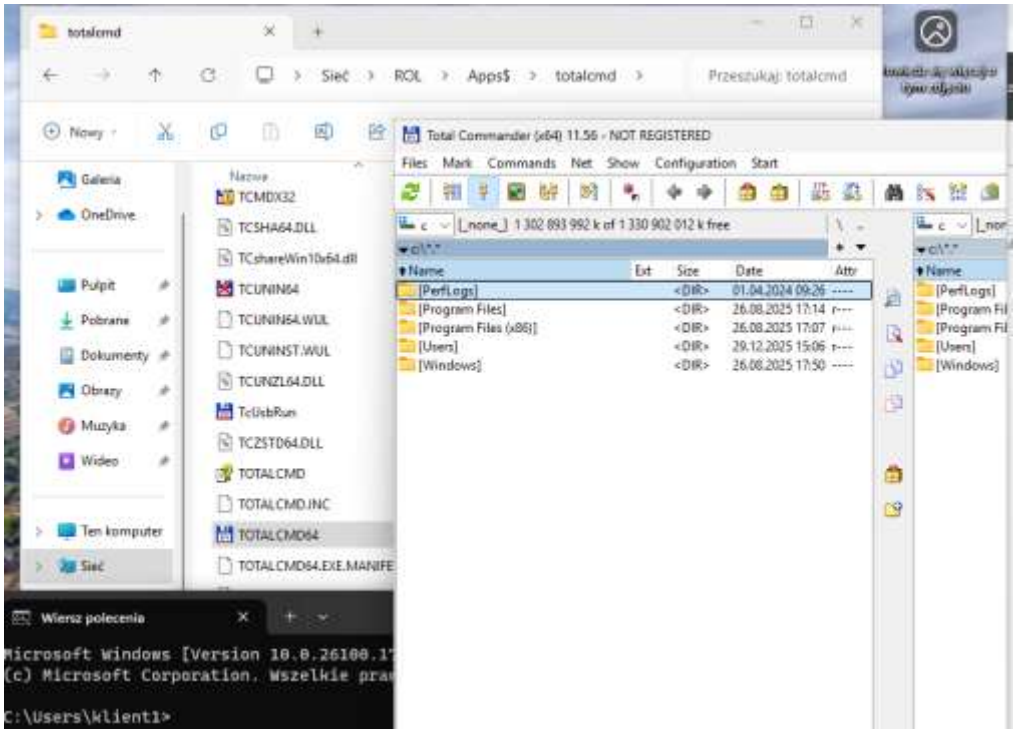
Wyświetl efektywne uprawnienia klient3



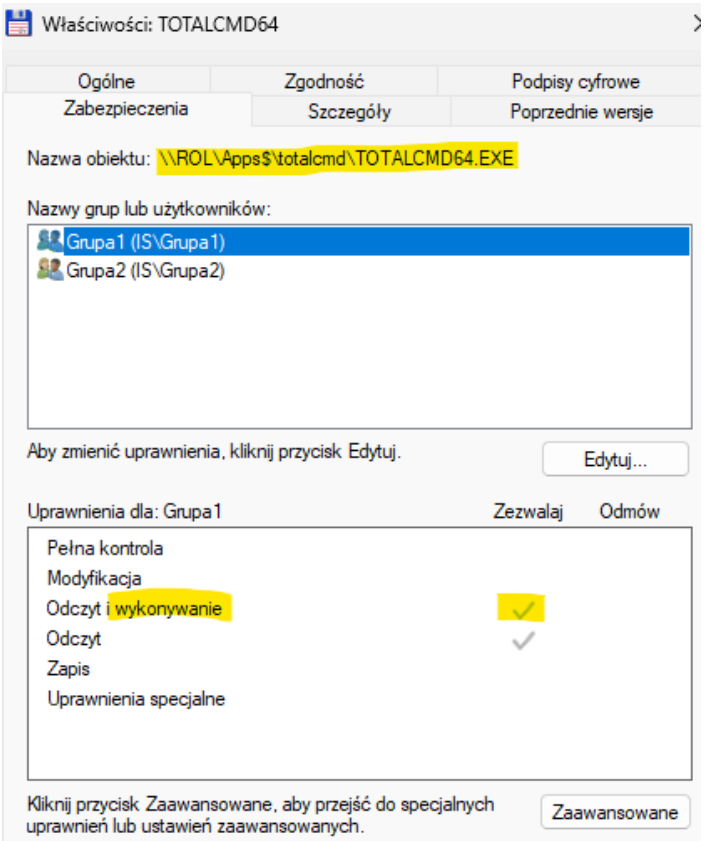
2. Na kliencie zalogowany do klient3 sprawdź dostęp do zasobu serwera i zapisz efekt.



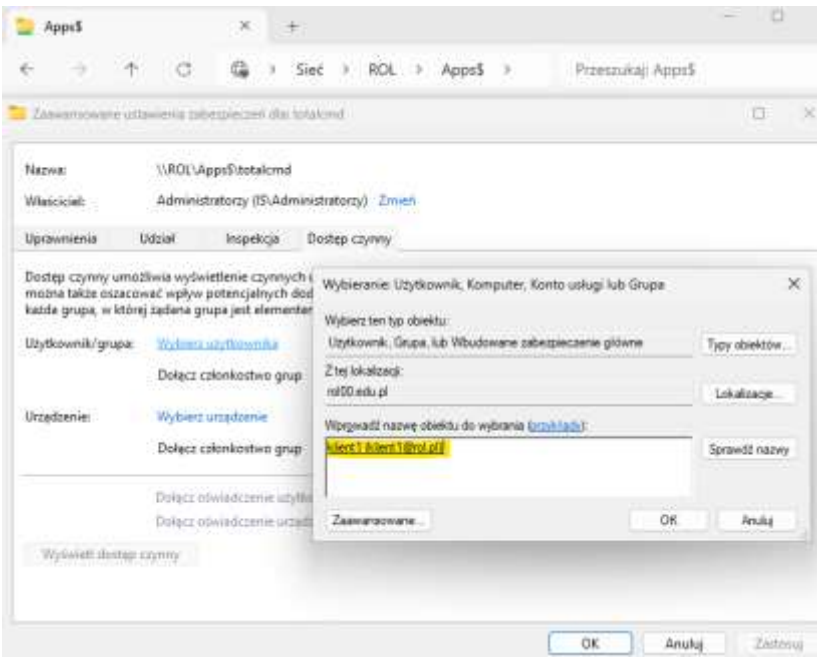
3. Na kliencie zalogowany do klient1 sprawdź dostęp do zasobu serwera i zapisz efekt.



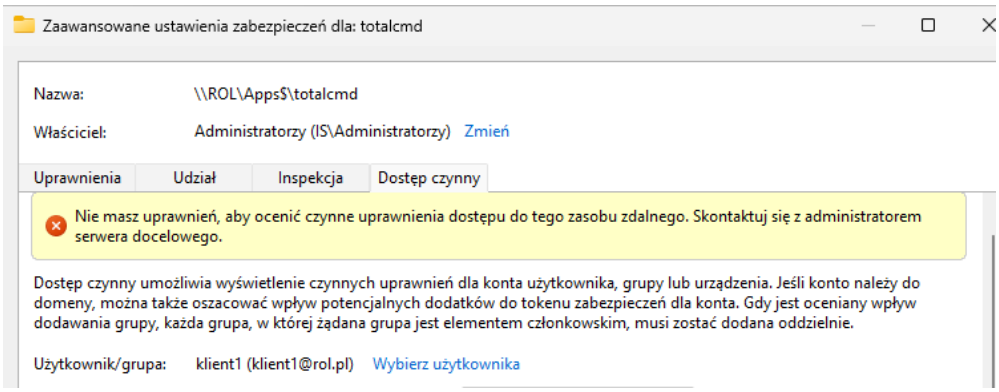
4. Zalogowany do klient1 sprawdź uprawnienia NTFS do zasobu serwera i zapisz jako wycinek.



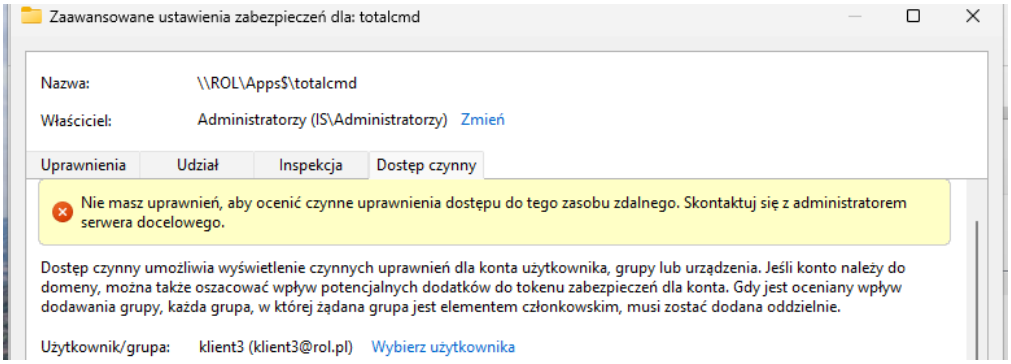
5. Zalogowany do klient1 sprawdź czynne uprawnienia NTFS dla użytkownika klient1 i klient3 do C:\Apps\totalcmd i zapisz jako wycinek.



Efekt dla klient1:



Efekt dla klient3:



Ćwiczenie 4

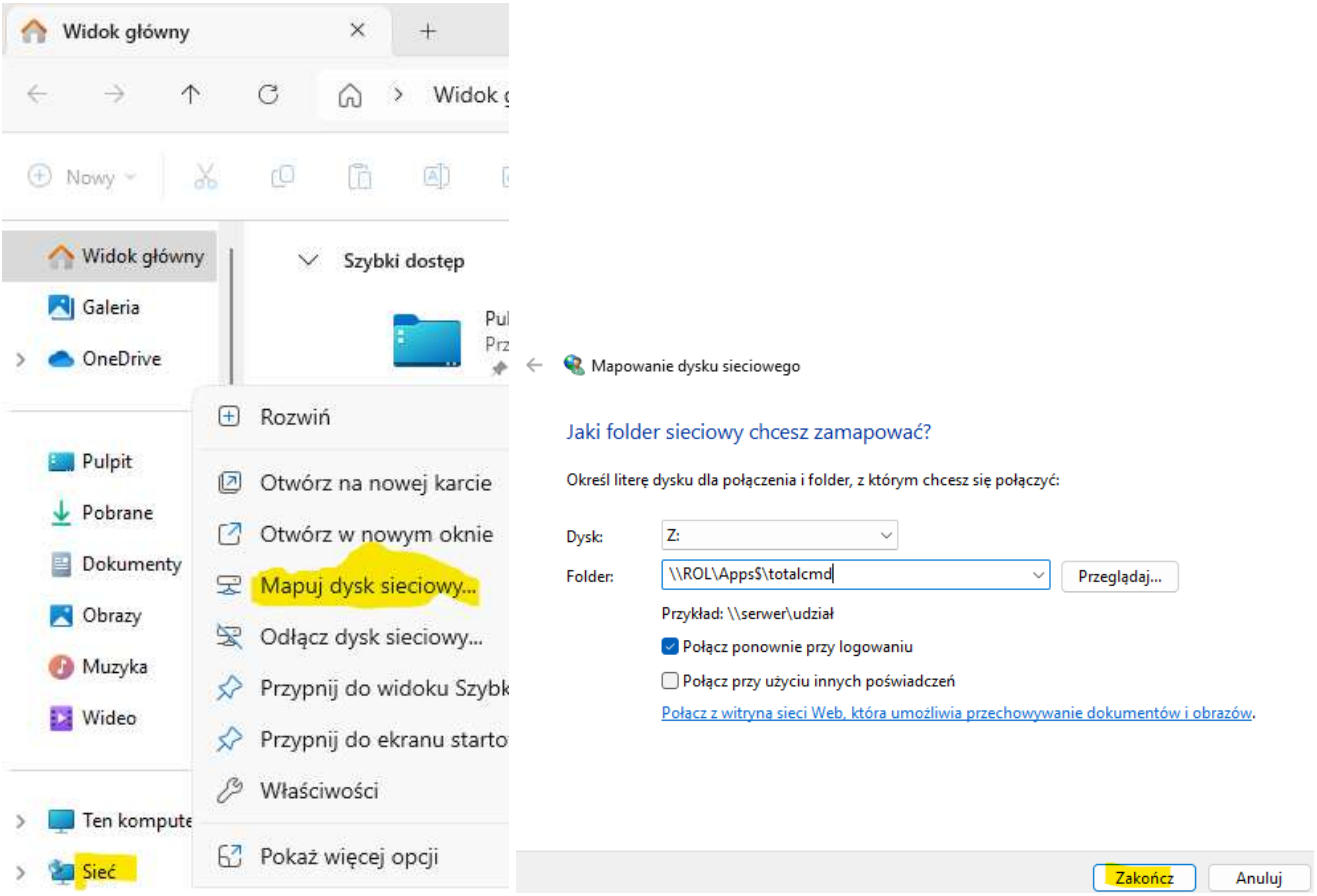
Otwieranie folderu udostępnionego na innym komputerze

Scenariusz

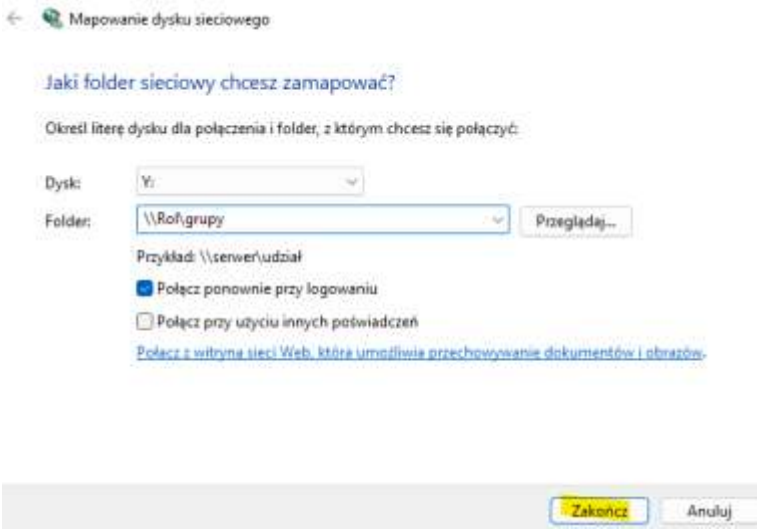
Zainstalowałeś aplikacje, w celu ograniczenia dostępu do aplikacji przypisałeś uprawnienia NTFS wybranym grupom użytkowników. Następnie udostępniłeś folder z aplikacjami tak, aby użytkownicy mogli z nich korzystać poprzez sieć. Teraz chcesz się upewnić, że będą oni mogli podłączyć się do folderu z aplikacjami z różnych komputerów, korzystając z różnych metod otwierania udostępnionych folderów.

Cel

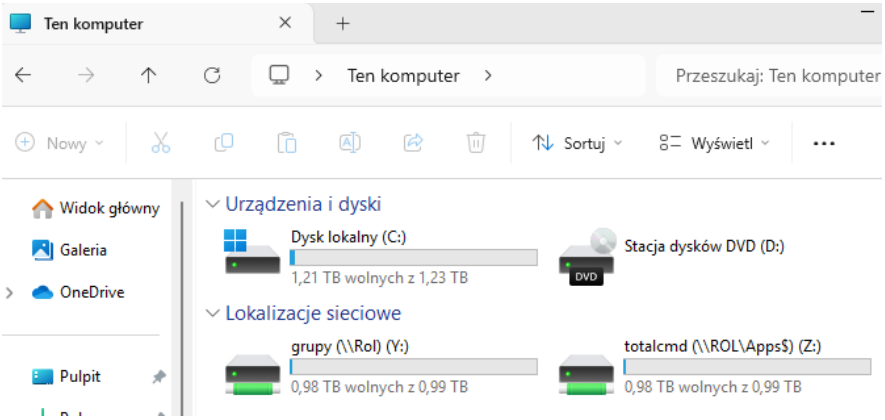
1. W tym ćwiczeniu, zalogujesz się jako użytkownik, który posiada ograniczone uprawnienia do utworzonych we wcześniejszych ćwiczeniach udostępnień.
2. Chcesz sprawdzić, czy dostęp ten jest ograniczony zgodnie z twoimi oczekiwaniami.
3. Na kliencie jesteś zalogowany do klient1, zmapuj dysk sieciowy jako dysk Z:



4. Na kliencie jesteś zalogowany do klient1, zmapuj dysk sieciowy jako dysk Y:

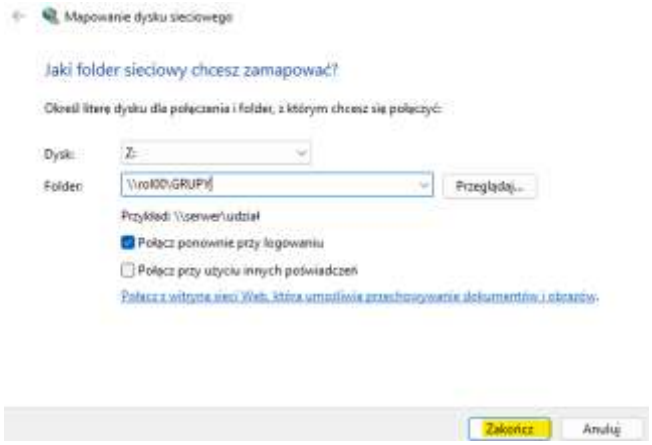


5. Na kliencie jesteś zalogowany do klient1, wyświetl lokalizacje sieciowe (zamapowane zasoby serwera)

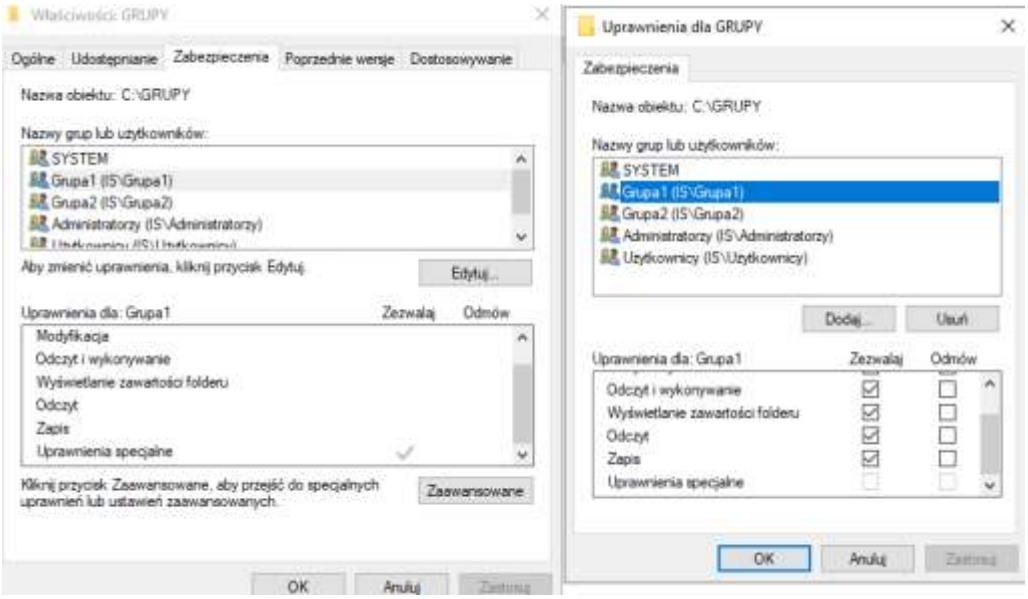


zgłoszenie 1

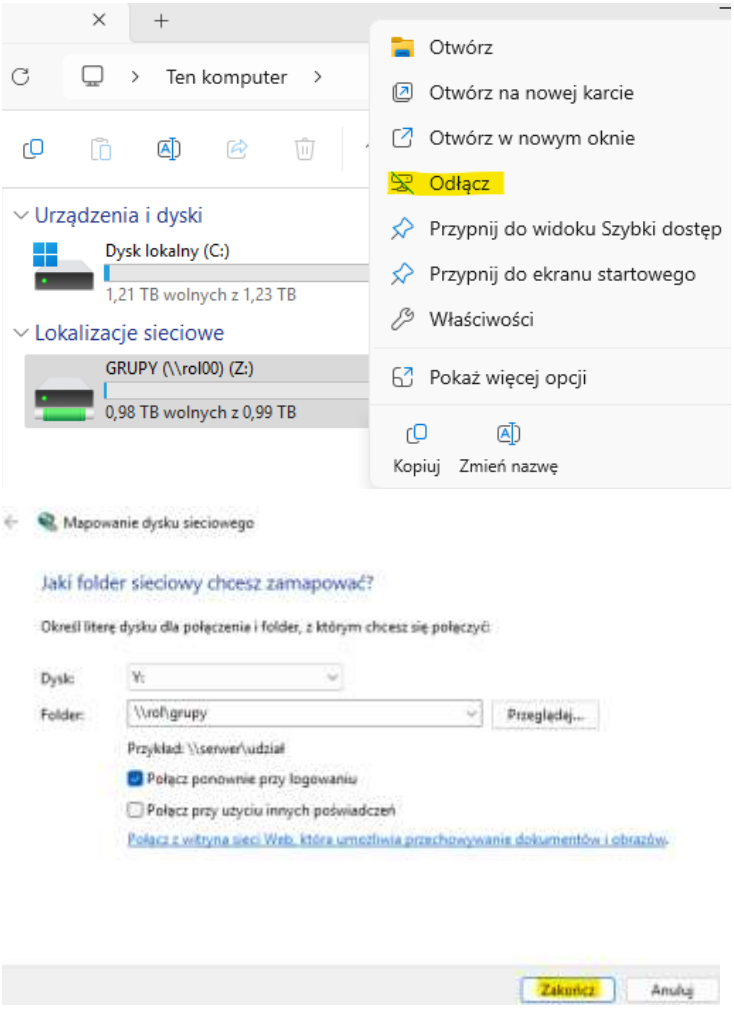
6. Zaloguj się do użytkownika klient3, spróbuj zmapować dysk sieciowy i zapisz efekt.



7. Przydziel uprawnienia na serwerze i zmapuj dysk sieciowy i zapisz efekt.



8. Wyloguj i zaloguj się do użytkownika klient3, spróbuj zmapować dysk sieciowy i zapisz efekt.



9. W cmd wpisz polecenie net share

Porównaj wynik net share z widocznością udziałów w Eksploratorze plików.

10. Na serwerze w cmd wpisz polecenie net share

Porównaj wynik net share z widocznością udziałów w Eksploratorze plików.

11. Porównaj wynik net share z komputera klienckiego i serwera. Wyjaśnij różnice.

zgłoszenie 2

Ćwiczenie 5

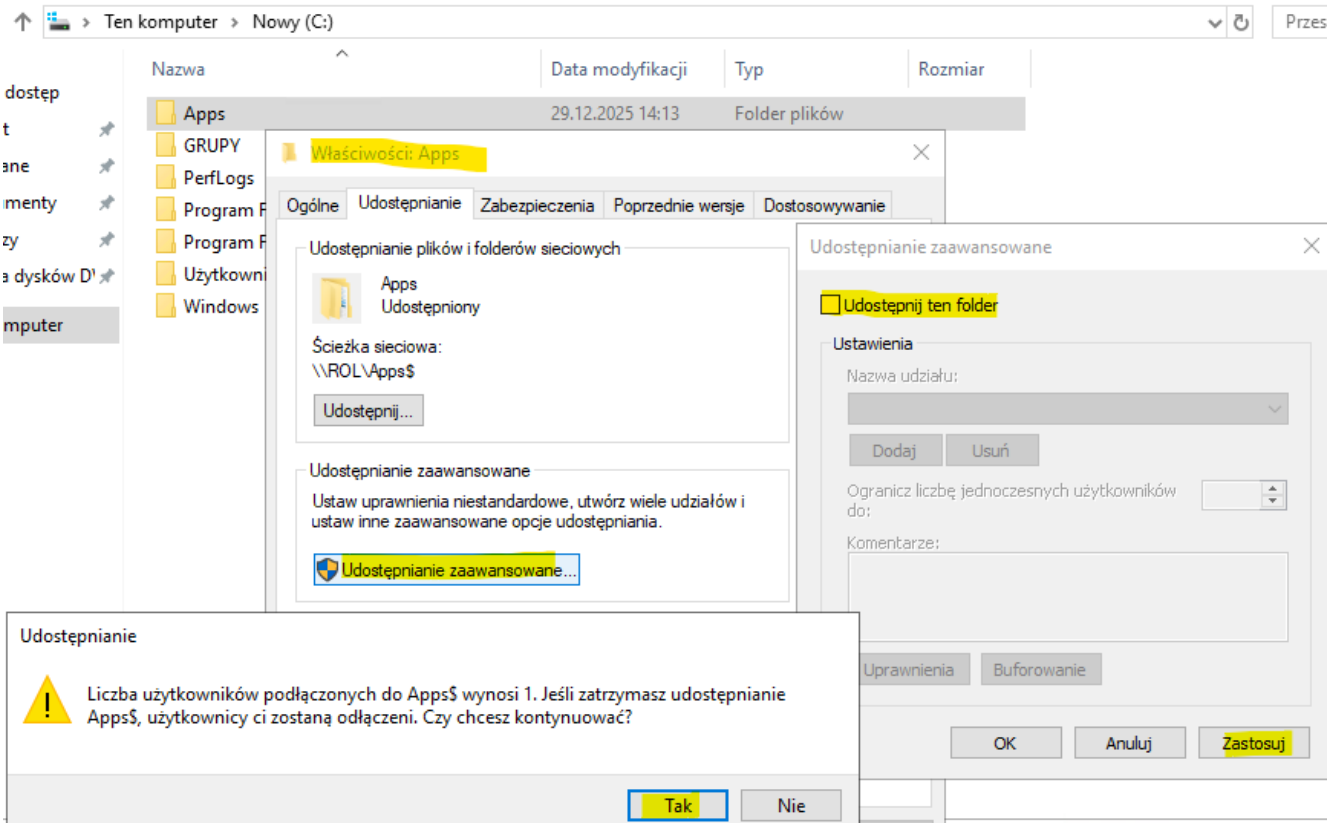
Usuwanie udostępnionego folderu

Scenariusz

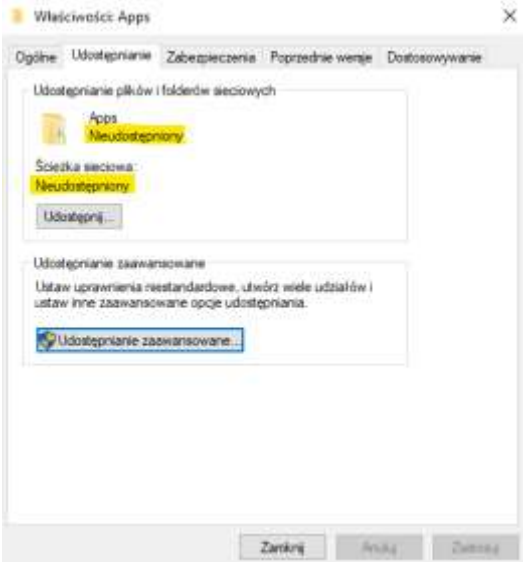
Musisz dokonać wielu istotnych zmian w folderze z aplikacjami i chcesz uniemożliwić użytkownikom dostęp do plików w podczas tych czynności. Dlatego, zatrzymasz udostępnianie folderu, aby uniemożliwić użytkownikom podłączanie się do niego.

Cel

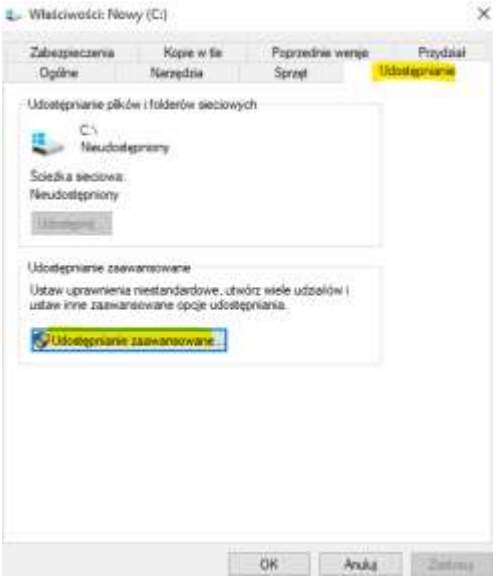
1. W tym ćwiczeniu zatrzymaj udostępnianie folderu **Apps** na swoim serwerze i zapisz.



2. Zweryfikuj wykonane zadania poprzez GUI i zapisz efekt. C:\Apps PPM > Właściwości > Udostępnianie



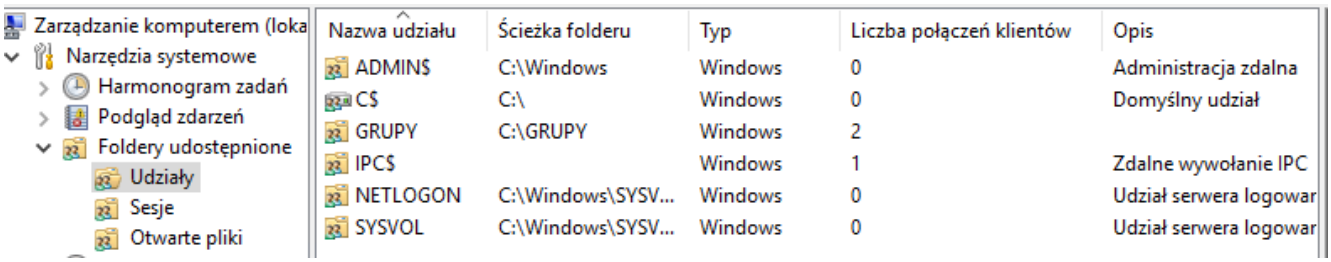
3. Zweryfikuj wykonane zadania poprzez GUI i zapisz efekt. C:\ > PPM > Właściwości > Udostępnianie



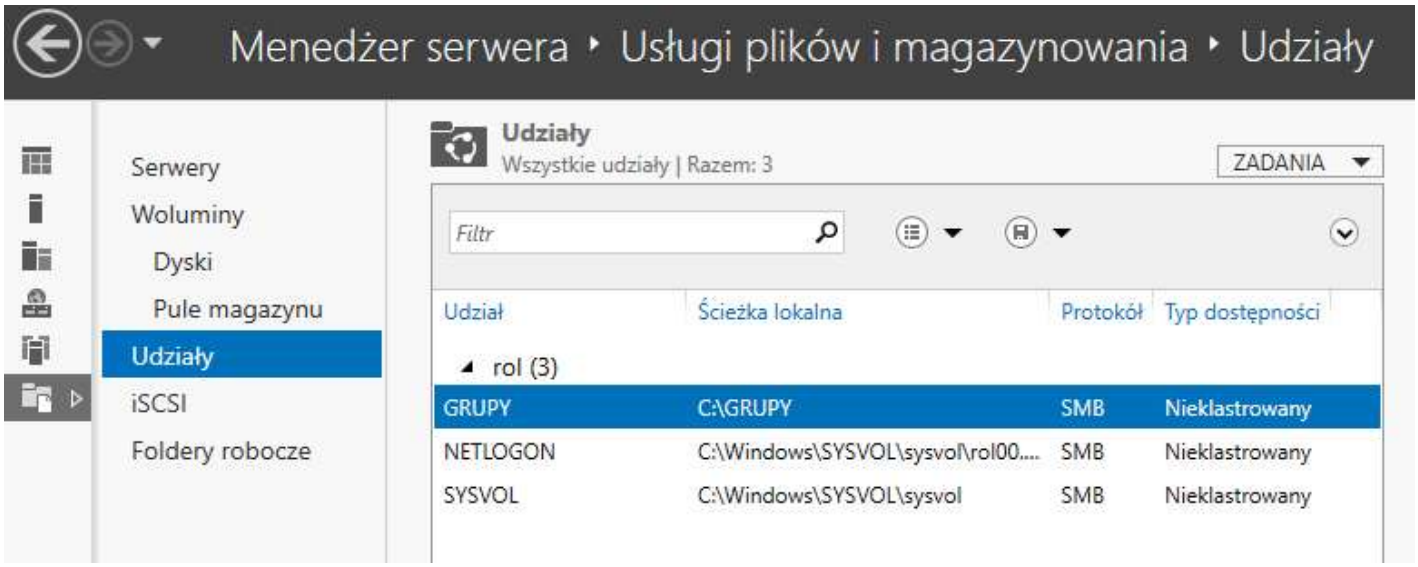
4. Na serwerze wyświetli listę wszystkich udziałów serwera, w tym Apps$, GRUPY, NETLOGON i SYSVOL w cmd

```
C:\Users\Administrator>net share

Udział       Zasób                           Uwaga

-------------------------------------------------------------------------------
Apps$        C:\Apps
C$           C:\                             Domyślny udział
IPC$                                         Zdalne wywołanie IPC
ADMIN$       C:\Windows                      Administracja zdalna
GRUPY        C:\GRUPY
NETLOGON     C:\Windows\SYSVOL\sysvol\rol00.edu.pl\SCRIPTS
                                             Udział serwera logowania
SYSVOL       C:\Windows\SYSVOL\sysvol        Udział serwera logowania
Polecenie zostało wykonane pomyślnie.
```

5. Na serwerze wyświetli listę wszystkich udziałów serwera, w tym Apps$, GRUPY, NETLOGON i SYSVOL w zarządzaniu komputerem



6. Na serwerze wyświetli listę wszystkich udziałów serwera, w tym Apps$, GRUPY, NETLOGON i SYSVOL w menedżerze serwera



7. W zeszycie opisz procedury konfiguracji udostępniania folderu.

zgłoszenie 3

Przywróć pierwszy punkt kontrolny

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 wykonie tej instrukcji w szkole lub/i w domu do momentu zrealizowania.