**Ćwiczenie 4: Zarządzanie dostępem do zasobów**

**Cel tematu:**

W ramach tematu zdefiniujesz dostęp do folderów i plików zarówno jako lokalny jak i sieciowy.

**W ramach tematu nauczysz się:**

* Dodawać pliki i foldery
* Przypisywać uprawnienia lokalne do folderów
* Przypisywać uprawnienia sieciowe do folderów
* Przypisywać uprawnienia lokalne do plików
* Definiować ustawienia zaawansowane
* Weryfikować uprawnienia efektywne

**Wstęp teoretyczny:**

Pliki i foldery są podstawowym zasobem dla którego konieczne jest zarządzanie dostępem. Dzięki kontom i grupom domenowym można poprzez nie przypisywać dostęp do plików i folderów na różnych komputerach należących do domeny, bez konieczności tworzenia oddzielnych kont na komputerach użytkowników.

**Dostęp może być przypisany:**

* Lokalnie – dotyczy użytkowników, którzy korzystają z folderów i plików będąc zalogowanymi na komputerze, na którym się one znajdują.
* Sieciowo - dotyczy użytkowników, którzy korzystają z folderów i plików będąc zalogowanymi na innym komputerze, niż na którym się one znajdują, i korzystając z nich poprzez sieć.

Dla plików i folderów można **przypisać uprawnienia**:

* Podstawowe, takie jak: odczyt, zapis, usuwanie, modyfikacja czy pełna kontrola
* Zaawansowane jak: przechodzenie przez folder czy uruchomienie aplikacji

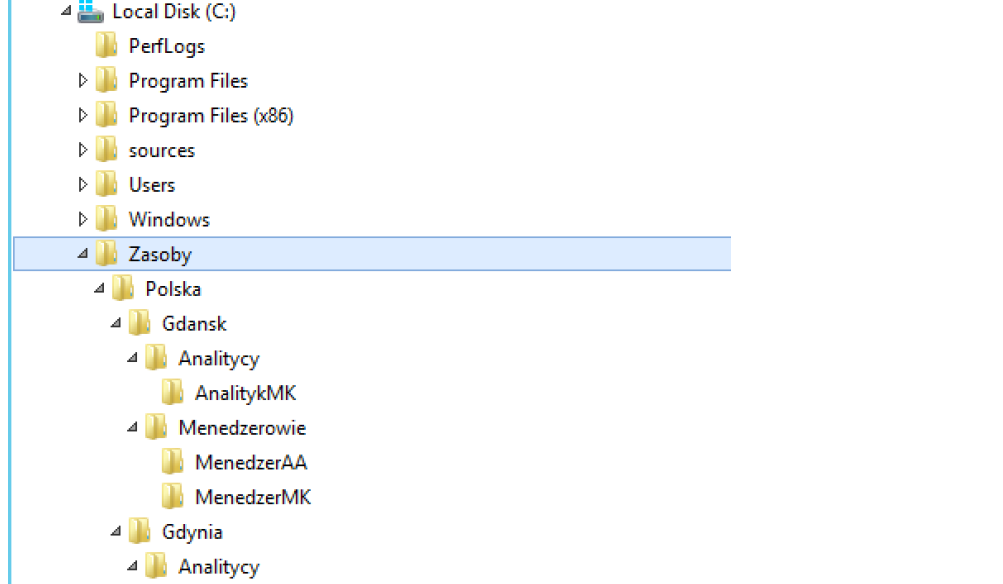
Uprawienia domyślnie są **dziedziczone**. Oznacza to, że jeśli użytkownik ma prawo odczytu plików w folderze Raporty, to również będzie miał takie prawo w jego pod-folderze Rok2018. Dziedziczenie można usunąć i w ten sposób zawężać lub poszerzać uprawnienia w folderach.

Definiując uprawnienia należy pamiętać o **zasadach**:

* Uprawnienia kumulują się – jeśli użytkownik ma do folderu uprawnienie odczytu, a grupa do której należy, ma do folderu uprawnienia zapisu, użytkownik ma prawo odczytu i zapisu.
* Wykluczenia mają wyższy priorytet – jeśli użytkownik należy do 5 grup, która mają pełne uprawnienia do folderu, i do 1, która ma zabroniony odczyt, użytkownik nie będzie miał prawa odczytu plików (ale zapis tak skoro nie został on mu odebrany).
* Uprawnienia sieciowe są przypisywane jako najbardziej restrykcyjna wersja – jeśli użytkownik do folderu ma dostęp lokalny ustawiony jako odczyt, a sieciowy jako pełna kontrola, będzie miał wyłącznie uprawnienia odczytu (część wspólna) – użytkownik nigdy przez sieć nie może mieć większych uprawnień niż lokalnie.

**Zadanie 1:** Dodaj konto użytkownika o nazwie menedzerAA do jednostki organizacyjnej Gdansk. Dodaj to konto do grupy menedzerowieGdansk. Jakich innych grup automatycznie to konto stało się członkiem? Dodaj konto użytkownika o nazwie partnerTwojeInicjały do kontenera Users.

Na partycji C wirtualnej maszyny serwera utwórz katalog o nazwie Zasoby a w nim podkatalogi o strukturze zgodnej z rysunkiem poniżej, pamiętając że wybrane foldery powinny mieć przyrostek Twoich inicjałów a nie MK.



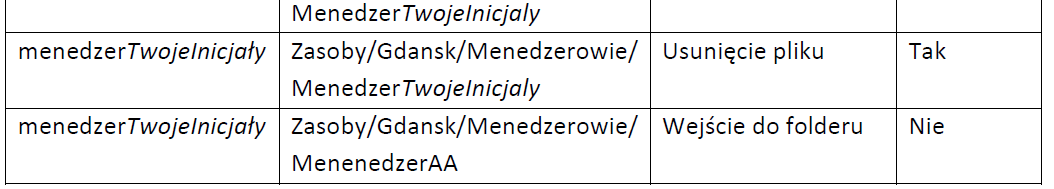
Przypisz uprawnienia zgodnie z tabelą poniżej:

|  |  |
| --- | --- |
| **Folder** | **Uprawnienia (wyłącznie poniższe)** |
| Zasoby | **Wszyscy użytkownicy uwierzytelnieni** (czyt. posiadający konto w domenie) – odczyt i wyświetlenie zawartości  **Administratorzy** – pełen dostęp (również do wszystkich podfolderów) |
| Polska | Grupa **pracownicyPolska** – odczyt i wyświetlenie zawartości |
| Gdańsk | Grupa **pracownicyGdansk** – odczyt i wyświetlenie zawartości |
| Analitycy | Grupa **analitycyGdansk** – odczyt i wyświetlenie zawartości |
| AnalitykTwojeInicjały | Konto **analitykTwojeInicjały** – pełen dostęp |
| Menedzerowie | Grupa **menedzerowieGdansk** – odczyt i wyświetlenie zawartości |
| MenedzerTwojeInicjały | Konto **menedzerTwojeInicjały** – pełen dostęp |
| MenedzerAA | Konto **menedzerAA** – pełen dostęp |
| Gdynia | Grupa **pracownicyGdynia** – odczyt i wyświetlenie zawartości |
| Analitycy | Grupa **analitycyGdynia** – odczyt i wyświetlenie zawartości |
| andrzejNowak | Konto **andrzejNowak** – pełen dostęp |
| Menedzerowie | Grupa **menedzerowieGdynia** – odczyt i wyświetlenie zawartości |
| janKowalski | Konto **janKowalski** – pełen dostęp |

W folderze **Zasoby** i w każdym z folderów utwórz plik o nazwie **dokument.txt**, w którym wpisz nazwę folderu, w którym się on znajduje.

Utwórz w kontenerze **Users** konto o nazwie **partnerTwojeInicjały**.

Po kolei przeloguj się na serwerze na konta i wykonaj operacje zgodnie z tabelą poniżej notując co było możliwe do wykonania a co nie. Wartości w tablicy wskazują jaki powinien być efekt zgodnie z zadaniem – w przypadku innych rezultatów sprawdź i zmodyfikuj uprawnienia.

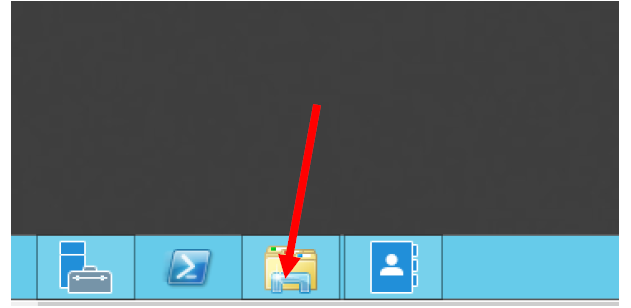
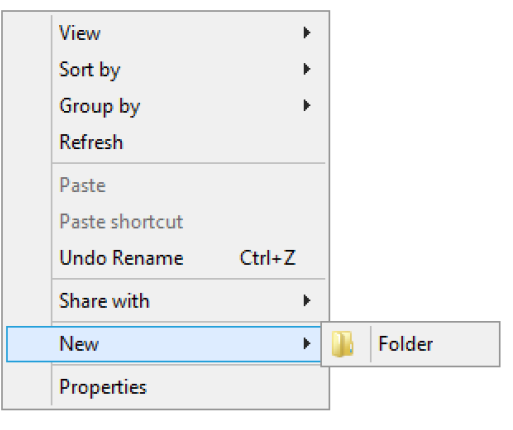
 

Do folderu **Zasoby** przypisz grupę wbudowaną Wszystkich (**Everyone**) zabierając jej uprawnienie **Full Control**. *Kto ma prawo teraz wejść do folderu i co wykonać?* Jeśli nie wiesz, sprawdź to empirycznie.

**Sposób wykonania:**

* Zarządzanie folderami i plikami – Eksplorator windows (**File explorer)**
* Zmiana uprawnień do pliku lub folderu - operacja Właściwości (**Properties**) -> zakładka Uprawnienia (**Security**)

**Szczegółowy tutorial:**

1. Dodaj konta użytkowników i grup zgodnie z treścią zadania (szczegółowy opis procedury – ćwiczenie 3, zadanie 2 i 5)
2. Na maszynie serwera otwórz okno File explorer w lewej dolnej części pulpitu. 
3. W oknie **File explorer** kliknij prawym przyciskiem myszki i wybierz operację New -> Folder. 
4. Jako nazwę folderu podaj Zasoby.
5. Analogicznie dodaj pozostałe foldery zgodnie z treścią zadania.
6. Wejdź do folderu Zasoby i dodaj w nim plik tekstowy o nazwie zasoby.txt w którym wpisz tekst zasoby. Analogiczne czynności zgodnie z treścią zadania wykonaj dla pozostałych folderów.
7. Wejdź we właściwości (operacja Properties) folderu Zasoby.
8. Przejdź na zakładkę Security. Zgodnie z treścią dostęp: Wszyscy użytkownicy uwierzytelnieni (czyt. posiadający konto w domenie) – odczyt; Administratorzy – pełen dostęp.
9. Kliknij na przycisk Edit i postaraj się usunąć występujące tam grupy. Przeczytaj komunikat – dlaczego nie jest to możliwe?
10. Kliknij na przycisk Cancel.
11. Kliknij na przycisk Advanced -> przycisk Disable inheritance. W ten sposób usuniesz dziedziczenie uprawnień z folderu nadrzędnego, co pozwoli na ich zmianę.
12. Przeczytaj komunikat w oknie dialogowym i wybierz opcję Remove iherited… Spowoduje to usunięcie odziedziczonych wpisów – ta opcja jest korzystna jeśli chcesz znacząco zmienić uprawnienia. Jeśli chciałbyś dokonać głownie ich modyfikacji to opcja Convert inherited… usunęła by dziedziczenie (czyli de facto blokadę zmian) pozostawiając aktualne uprawnienia.
13. Kliknij OK -> Yes.
14. Ponownie kliknij na przycisk Edit. Lista wpisów jest pusta.
15. Kliknij na przycisk Add.
16. Wpisz Administrator i kliknij na Check names. Pasuje więcej wpisów, więc z listy wybierz Administrators (udostępnisz folder wszystkim członkom grupy administratorów, a nie wyłącznie administratorowi głównemu czyli kontu Administrator).
17. Kliknij OK - > OK.
18. Zgodnie z treścią zadania zaznacz na liście uprawnień Full control.
19. Kliknij na przycisk Add.
20. Wpisz auth i kliknij na Check names. Pojawi się Authenticated users.
21. Kliknij OK - > OK.
22. Zgodnie z treścią zadania zaznacz Read oraz List folder contents.
23. Kliknij OK - > OK.  
    Zdefiniowałeś odpowiednie uprawnienia dla folderu Zasoby.
24. Przeloguj się na konto partnerTwojeInicjały. Wykonaj czynności na folderze Zasoby zgodnie z tabelą zadania. Wykonaj czynności wskazane w tej samej tabeli dla pozostałych kont.
25. Przeloguj się na konto administratora.
26. Wejdź we właściwości folderu Zasoby.
27. Na zakładce Security przypisz grupę wbudowaną Wszystkich (Everyone) zabierając jej uprawnienie Full Control (kolumna Deny).
28. Czy możesz wejść do tego folderu? Czy będą mogli wejść do niego inni użytkownicy? – jeśli tego nie wiesz sprawdź empirycznie.
29. Usuń grupę Everyone z listy uprawnień.

**Zadanie 2:** Udostępnij folder **Zasoby** pod nazwą **Materialy** z uprawnieniami udostępnienia (przez sieć) jako odczytu (**read**) dla wszystkich użytkowników uwierzytelnionych (**Authenticated users**). Połącz się z folderem przez sieć z maszyny klienta jako **menedzer*TwojeInicjały***. *Jakie uprawnienia są lokalne, a jakie zdalne dla konta* ***menedzerTwojeInicjały****? Jakie będą uprawnienia przy dostępie sieciowym jak zmienisz uprawnienia do folderu dla grupy* ***Authenticated users*** *z odczytu na zmianę (****change****)?*

Dodaj we wpisach udostępnienia folderu sieciowego **Materiały** grupę **analitycyGdansk** zabierając uprawnienie odczytu (**Read** jako **Deny**). Połącz się z folderem przez sieć z maszyny klienta jako **analityk*TwojeInicjały***. *Czy jest to możliwe?*

Sprawdź listę udostępnionych zasobów na serwerze. Następnie ustaw, aby folder udostępniony **Materialy** był **ukryty** przy przeglądaniu udostępnionych zasobów. *Jakie będą uprawnienia przy dostępie jak zmienisz dostęp do folderu z odczytu na zmianę (change)?*

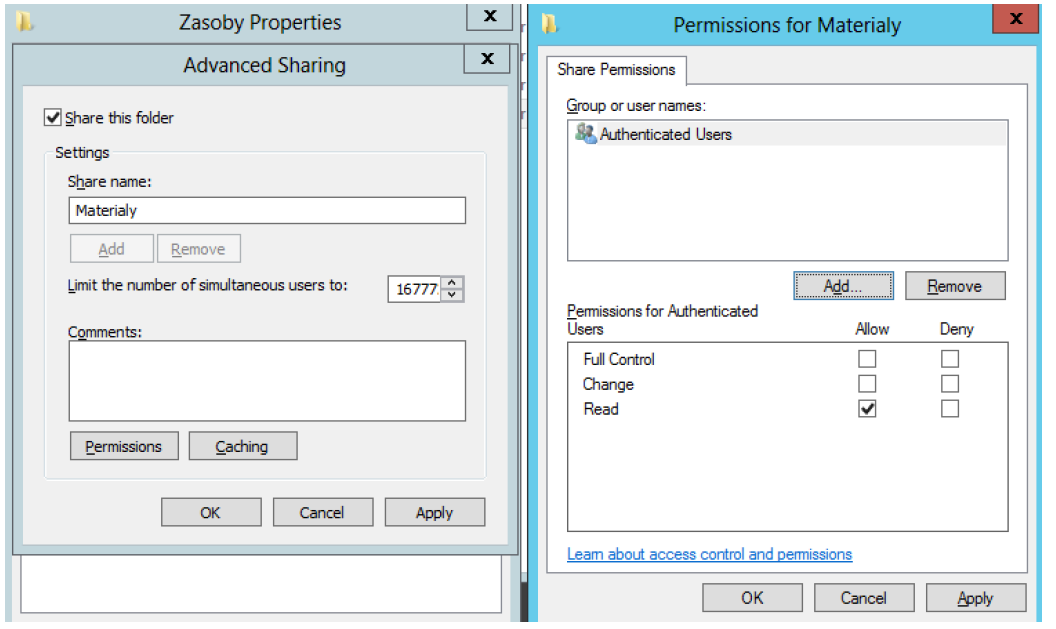
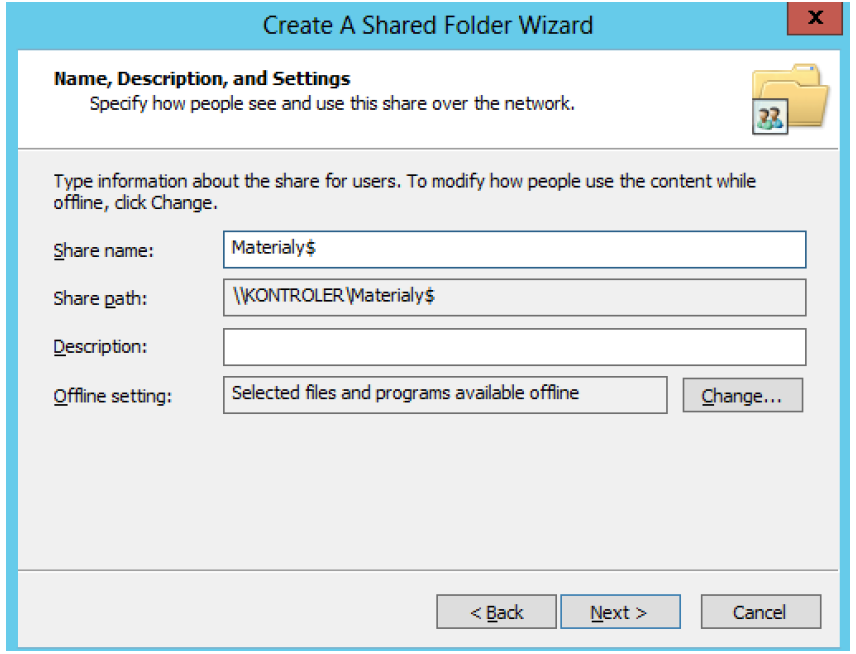
Zdefiniuj dostęp do folderu udostępnionego **Materialy** jako dysku sieciowego **X**.

*Jak uważasz co należy zrobić aby dostęp do folderu był możliwy dla użytkowników, którzy nie są zalogowani do domeny?* Jeśli nie wiesz spróbuj empirycznie tak skonfigurować folder **Zasoby** (wymagane zmiany w ustawieniach uprawnień lokalnych i sieciowych).

**Sposób wykonania:**

* Zarządzanie folderami i plikami – Eksplorator windows (File explorer)
* Udostępnienie folderu - operacja Właściwości (Properties) -> zakładka Udostępnianie (Sharing)
* Dostęp poprzez sieć do katalogu - \\serwer\zasób, np. \\kontroler.wsb.pl\materialy
* Lista udostępnionych zasobów – konsola Computer Management \ sekcja Shared Folders
* Ukrycie folderu – na końcu nazwy należy dodać $
* Definiowanie dysku sieciowego – Eksplorator Windows (File explorer) \ menu Narzędzia (Tools) \ operacja Mapuj dysk sieciowy (Map Network Drive …)

**Szczegółowy tutorial:**

1. Uruchom obie maszyny wirtualne jeśli nie są one uruchomione.
2. Na serwerze wejdź we właściwości folderu Zasoby i przejdź na zakładkę Sharing.
3. Kliknij na przycisk Advanced sharing…
4. Zaznacz pole Share this folder.
5. W pole tekstowe Share name wpisz Materialy.
6. Kliknij na przycisk Permissions.
7. Usuń grupę Everone i dodaj grupę Authenticated users z uprawnieniem Read. 
8. Kliknij OK -> OK.
9. Na komputerze klienta zaloguj się jako menedzerTwojeInicjały.
10. Wejdź do folderu sieciowego poprzez przycisk Start -> Uruchom … -> wpisz \\kontroler.zsl.pl\materialy (tzw. Ścieżka UNC – Universal Naming Convention) i naciśnij Enter.
11. Wejdź do folderu Polska\Gdansk\Menedzerowie\menedzerTwojeInicjały. Czy jest to możliwe? Odczytaj plik w dokument.txt. Czy jest to możliwe? Dodaj nowy dokument. Czy jest to możliwe i czy można było zrobić to lokalnie?
12. Ponownie na serwerze wejdź we właściwości folderu Zasoby i przejdź na zakładkę Sharing.
13. Kliknij na przycisk Advanced sharing…
14. Kliknij na przycisk Permissions.
15. Dla grupy Authenticated users zaznacz jeszcze uprawnienie Change.
16. Na komputerze klienta będąc dalej zalogowanym jako menedzerTwojeInicjały wejdź ponownie do folderu sieciowego [\\kontroler.zsl.pl\materialy](file:///\\kontroler.zsl.pl\materialy).
17. Wejdź do folderu Polska\Gdansk\Menedzerowie\menedzerTwojeInicjały. Dodaj nowy dokument. Czy teraz jest to możliwe?
18. Na serwerze wejdź do katalogu Zasoby\Polska\Gdansk\Menedzerowie\menedzerTwojeInicjały i usuń jego zawartość.
19. Powróć do maszyny klienta. Co stało się z zawartością wyświetlanego folderu?
20. Ponownie na serwerze wejdź we właściwości folderu Zasoby i przejdź na zakładkę Sharing.
21. Kliknij na przycisk Advanced sharing…
22. Kliknij na przycisk Permissions.
23. Dodaj grupę analitycyTwojeInicjały i zaznacz uprawnienie jako Deny.
24. Na komputerze klienta zaloguj się jako analityjTwojeInicjały.
25. Wejdź do folderu sieciowego poprzez przycisk Start -> Uruchom … -> wpisz \\kontroler.zsl.pl\materialy i naciśnij Enter. Czy jest to możliwe i czy można wejść do tego folderu lokalnie?
26. Na komputerze klienta zaloguj się jako menedzerTwojeInicjały.
27. Wejdź do folderu sieciowego poprzez przycisk Start -> Uruchom … -> wpisz \\kontroler.zsl.pl i naciśnij Enter. W ten sposób wyświetliłeś wszystkie katalogi udostępnione na serwerze.
28. Wejdź do folderu Polska\Gdansk\Menedzerowie\menedzerTwojeInicjały. Czy jest to możliwe? Odczytaj plik dokument.txt. Czy jest to możliwe? Dodaj nowy dokument. Czy jest to możliwe i czy można było zrobić to lokalnie?
29. Powróć do maszyny serwera.
30. Naciśnij Windows + Q i wpisz Computer. Z listy wybierz Computer manager.
31. Wejdź do sekcji Share folders -> Shares  
    W tym miejscy widać wszystkie udostępnione udziały, również te ukryte. Oznacza to, że podając na końcu adres C$ można zobaczyć zawartość całej partycji C.
32. Na komputerze klienta zaloguj się jako menedzerTwojeInicjały.
33. Wejdź do folderu sieciowego poprzez przycisk Start -> Uruchom … -> wpisz \\kontroler.zsl.pl\C$ i naciśnij Enter. Na szczęście foldery ukryte mają ustawione uprawnienie dostępu przez sieć tylko dla administratorów.
34. Po pojawieniu się okna podaj login (zsl\administrator) i hasło (zaq1@WSX) administratora domeny. W ten sposób wyświetliłeś wszystkie katalogi partycji C. Jeśli się to nie uda przeloguj się na kliencie na administratora.
35. Na serwerze w konsoli Computer manager wejdź do sekcji Share folders -> Shares.
36. Wejdź we właściowości folderu Materialy. Spróbuj zmienić nazwę – niestety nie jest to możliwe.
37. Usuń udostępnienie poprzez operację Stop sharing.
38. Wybierz klikając prawym przyciskiem myszy operację Start shaing.
39. Kliknij next.
40. Wskaż jako ścieżkę folder C:\Zasoby i przejdź dalej.
41. W share name wpisz Materialy$. 
42. Wybierz Administrator have full access; other users have read only access.
43. Finish -> Finish.
44. Na komputerze klienta zaloguj się jako menedzerTwojeInicjały.
45. Wejdź do folderu sieciowego poprzez przycisk Start -> Uruchom … -> wpisz \\kontroler.zsl.pl\ i naciśnij Enter. Czy zasób Materiały jest widoczny?
46. Zmień adres na \\kontroler.zsl.pl\materialy$ i naciśnij Enter. Czy teraz zasób Materiały jest widoczny?
47. Na komputerze klienta w Eksplorator Windows (File explorer) \ menu Narzędzia (Tools) \ wybierz operację Mapuj dysk sieciowy (Map Network Drive …)
48. Jako dysk wskaż X, a folder [\\kontroler.zsl.pl\matarialy$](file:///\\kontroler.zsl.pl\matarialy$).
49. Sprawdź w eksploratorze plików, że dysk sieciowy się pojawił.
50. Ustaw, aby folder sieciowy Materialy był dostępny dla wszystkich bez konieczności posiadania konta w domenie (zastosuj grupę Everyone). Sprawdź to logując się do klienta po koncie lokalnym (login: admin; hasło:QwertX), zmieniając pole Zaloguj do na Klient (ten komputer).

**Zadanie 3:** Użytkownik **menedzerTwojeInicjały** zgłosił, że nie może utworzyć pliku w katalogu **Zasoby/Gdansk/Menedzerowie** w związku z tym, że nie chcesz analizować wszystkich wpisów aby ustalić jakie rzeczywiście ma on uprawnienia do tego folderu sprawdź uprawnienia efektywne (czynne).

**Sposób wykonania:**

* Sprawdzanie uprawnień czynnych - właściwości folderu -> zakładka **Security** -> ustawienia zaawansowane (przycisk **Advanced**) \ zakładka **Effective Permissions** -> wskazanie grupy/konta, dla którego sprawdzane są uprawnienia efektywne -> przycisk **Select**

**Szczegółowy tutorial:**

1. Na maszynie serwera wejdź do właściwości folderu **Zasoby/Gdansk/Menedzerowie**.
2. Przejdź na zakładkę **Security** i kliknij na przycisk **Advanced**.
3. Przejdź na zakładkę **Effective permissions**.
4. Kliknij w odnośnik **Select a user**, wskaż konto **menedzerTwojeInicjały** i zatwierdź wybór.
5. Kliknij na przycisk View effective access i sprawdź uprawnienia. Czy zgodnie z wynikami użytkownik powinien móc tworzyć nowe pliki? Jeśli nie to co trzeba wykonać, aby przyznać mu stosowny dostęp.