Laboratorium 04

Temat: zasada IGDLA – na przykładzie praw dostępu do folderów

Scenariusz

Twoim zadaniem jest przygotowanie i przetestowanie dostępu do udostępnionych folderów na serwerze **SVR1**.

Polityka firmy odnośnie zasobów IT

- Uprawnienia NTFS dla tworzonych folderów nadrzędnych powinny być określone w sposób jawny (**zablokowane dziedziczenie**).
- W firmie przyjęto następujące zasady odnośnie grup i nadawania uprawnień
  - Konta użytkowników są członkami **Grup Globalnych** związanych z pełnioną w przedsiębiorstwie funkcją (np. pracownicy działu **IT** są w Grupie Globalnej **IT**).
  - Grupy Globalne związane z działami firmy mają znajdować się we właściwych jednostkach organizacyjnych np. Grupa Globalna **IT** ma znajdować się jednostce organizacyjnej **IT**.
  - Uprawnienia do zasobów nadaje się jedynie grupom **Domenowym Lokalnym** *(Domain Local Group)*. Odstępstwem od tej zasady jest możliwość wykorzystania następujących grup domenowych/wbudowanych/lokalnych takich jak:
    Domain Users, Domain Admins, Authenticated Users, Creator Owner, Administrators
  - Chcąc przyznać użytkownikom prawa, zagnieżdża się odpowiednią grupę **Globalną** w Grupie **Domenowej Lokalnej**.
    Wyżej opisane zasady nazywają się **IGDLA** (dawniej **AGDLP**):
  - **Konwencja nazewnicza Grup Domenowych Lokalnych** jest następująca:
    DL_nazwa_zasobu_typdostepu
    Np. dla folderu DATA
    DL_data_R0 - grupa mająca dostęp ***read only***
    DL_data_M - grupa mająca dostęp ***modyfiy***
    DL_data_FC - grupa mająca dostęp ***full controll***
    DL_data_S - grupa mająca dostęp ***special***
  - grupy domenowe lokalne powinny być umieszczone w jednostce organizacyjnej o nazwie **DL_Group** zlokalizowanej w *OU=KEJAMAIN, DC=KEJA,DC=MSFT*
  - Dostęp przez sieć do udostępnionych zasobów powinien być regulowany jedynie przez prawa **NTFS**. Udostępnione zasoby powinny mieć następujące prawa udostępniania ***Authenticated Users: Full Control***. Nazwa współdzielona (*share name*) powinna być taka sama jak nazwa udostępnianego folderu. Np. Folder **d:\dane16** udostępniamy pod nazwą **dane16**.

UWAGA!: Polityka firmy odnośnie zasobów IT musi być bezwzględnie przestrzegana

Zadania do wykonania

1. Uprawnienia NTFS

   a) **Dane firmowe**: Na wolumenie dysku **C** serwera **SVR1** utwórz folder **DANE** kolejno w folderze **DANE** utwórz podfoldery**:** **raporty**, **finanse**, **regulaminy**, a w folderze raporty kolejny podfolder **tajne** (rys. 1)

Rys.1. Struktura folderów

Dodatkowo w każdym folderze utwórz plik tekstowy o nazwie ***nazwa_folderu.txt*** z dowolną treścią (będzie potrzebny do testowania). Czyli w folderze **DANE** utwórz plik ***dane.txt***, a w folderze finanse plik ***finanse.txt*** itd. Można wspomóc się powershell'em. Np.

New-Item d:\dane\dane.txt -type file -force -value "To jest zawartosc pliku dane"

   b) **Folder DANE:**

- Wszyscy użytkownicy domeny (domain users) mają prawo wejścia do folderu **DANE** i zobaczenia jakie katalogi znajdują się **bezpośrednio** w folderze DANE.
- Folder **DANE** powinien zostać udostępniony dla użytkowników domeny. Jedynie **prawa NTFS** powinny regulować dostęp do folderu **DANE** i jego podfolderów (prawa współdzielenia nie powinny ograniczać dostępu).

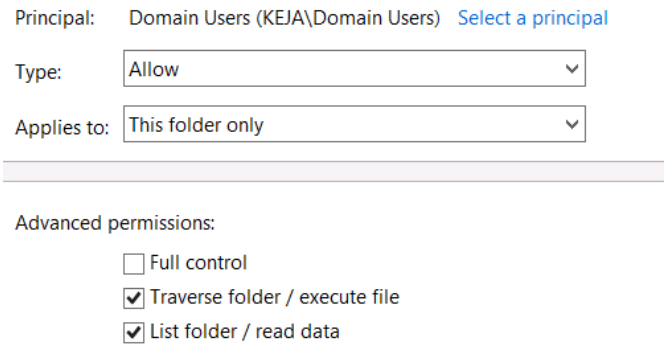
   c) **Pozostałe foldery:**

- Do folderu **finanse** dostęp '*read only*' powinni mieć pracownicy działu **HR**,
  dostęp '*modify*' powinni mieć pracownicy działu **Sales**
- Do folderu **raporty** dostęp *'read only'* powinni mieć pracownicy działu **Sales, HR, IT**
- Do folderu **tajne** dostęp ''*read only*' powinni mieć jedynie pracownicy działu **Sales**.
- Do folderu **regulaminy** dostęp '*read only'* powinni mieć pracownicy działu **IT**
  dostęp '*full control'* powinni mieć pracownicy działu **Sales** i **HR**

   d) Zaloguj się na **CL1** na konto użytkownik działu **Sales** i zmapuj folder **DANE** z serwera **SVR1** (np. net use r: \\svr1\dane) i przetestuj czy masz odpowiedni dostęp do folderów, możesz próbować edytować pliki, tworzyć nowe itp.
   Powtórz tę czynność z pracownikiem działu **HR** (ola) i działu **IT** (ewa)

Wskazówki do punktu 1

Blokujemy dziedziczenie praw na folderze DANE, Dla grupy Administrators nadajemy prawo Full Control, a dla grupy Domain Users nadajemy prawa szczegółowe jak na rysunku 2.

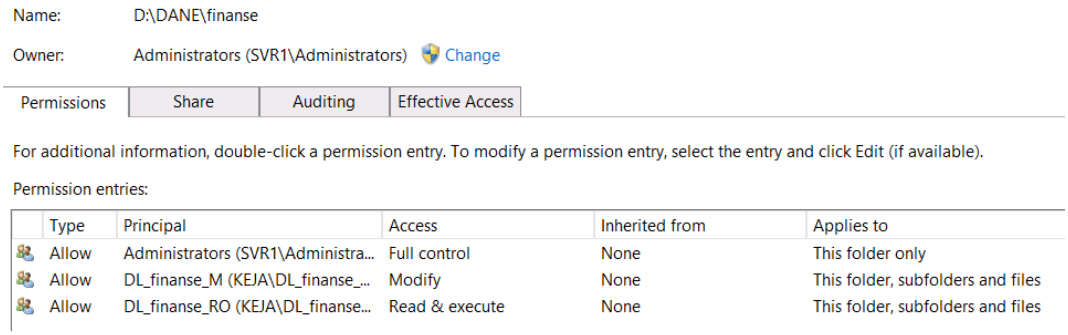


Rys. 2. Prawa NTFS dla Domain Users

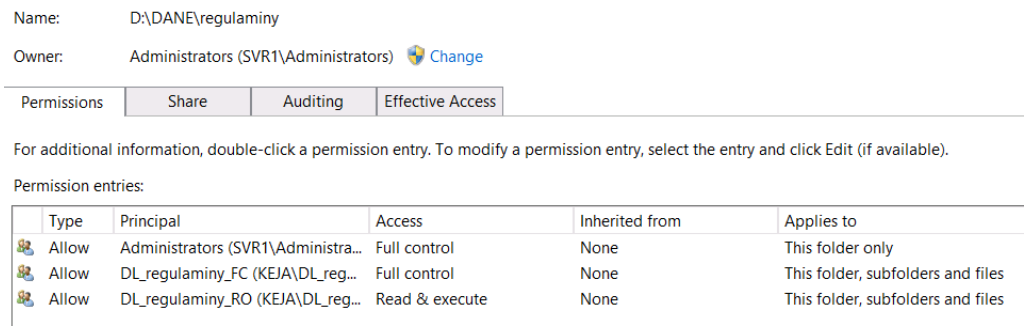
Tworzymy następujące Grupy Domenowe Lokalne, zgodnie z konwencją nazewniczą. Grupy domenowe lokalne powinny być umieszczone w jednostce organizacyjnej o nazwie **DL_Group** zlokalizowanej w *OU=KEJAMAIN, DC=KEJA,DC=MSFT*

DL_raporty_RO
DL_finanse_RO, DL_finanse_M
DL_regulaminy_RO, DL_regulaminy_FC
DL_tajne_RO

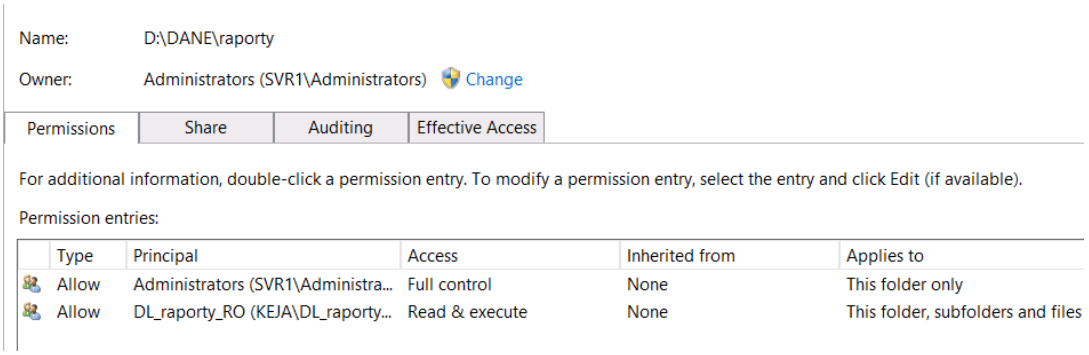
Konfigurujemy odpowiednie uprawnienia na folderach dla grup domenowych lokalnych. W przypadku folderu TAJNE blokujemy dziedziczenie i ustawiamy prawa w sposób bezpośredni. (rys 3,4,5,6)



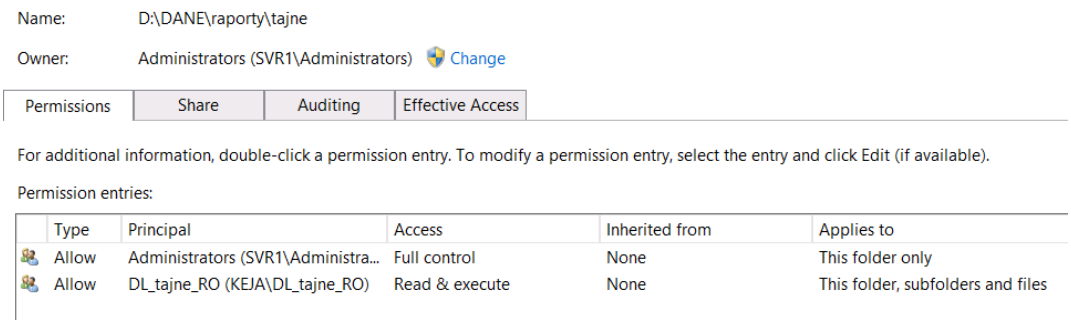
Rys.3. Prawa do folderu finanse



Rys.4. Prawa do folderu regulaminy

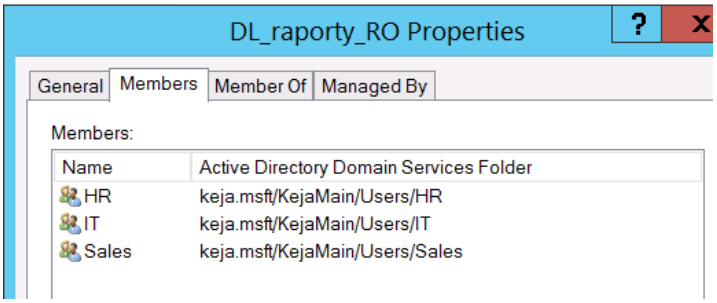


Rys.5. Prawa do folderu raporty



Rys.6. Prawa do folderu tajne

Następnie zagnieżdżamy odpowiedni grupy globalne we właściwych grupach domenowych lokalnych, przykład na rys. 7.



Rys.7. Zagnieżdżanie grup