Różnice pomiędzy kontami lokalnymi a domenowymi. Profile mobilne.

Jednym z podstawowych zadań usługi katalogowej jest zarządzanie kontami użytkowników w obrębie danej domeny. Każdy komputer (stacja robocza) podłączony do domeny uzyskuje możliwość korzystania z opcji logowania na konta, które „fizycznie" znajdują się właśnie na serwerze domeny. Dla systemu należącego do domeny korzystanie z tej opcji staje się domyślne. Oczywiście nie pozbawia to użytkownika końcowego z możliwości wykorzystywania kont lokalnych – aby zalogować się na konto nie utworzone w usłudze katalogowej trzeba nazwę użytkownika poprzedzić znakami kropki oraz backslasha (np. .\<nazwa_użytkownika>), ewentualnie nazwą komputera (np. LAB1\<nazwa_użytkownika>).

Logując się poprzez konto domenowe użytkownik otrzymuje konto przygotowane przez administratora – wszystkie ikony na pulpicie mogą być odpowiednio przygotowane, układ Menu Start (ekranu startowego w Windows 8/8.1), Dokumenty użytkownika oraz wszelkie ograniczenia związane z konfiguracją i używaniem komputera (logowanie w określonych godzinach, blokowanie określonych czynności systemowych, blokowanie dostępu do konfiguracji składników systemowych, konfiguracja aktualizacji oprogramowania i wiele, wiele innych ustawień). Dodatkowo administrator może zabronić zmiany tychże ustawień – nawet gdyby użytkownik zmienił np. układ ikon na pulpicie czy w ekranie startowym/Menu Start, to i tak po przelogowaniu wszystkie ustawienia będą zmienione na pierwotne.

W związku z tym dla każdego administratora sieci, który posiada serwer z zainstalowanym Windows Server, niemal koniecznością jest dodanie roli Active Directory. Po instalacji roli każdy z systemów klienckich musi być włączony do domeny (poprzednie zajęcia). Administrator powinien zablokować konta lokalne użytkowników (jeżeli takie istnieją) pozostawiając sobie tylko konto administracyjne zabezpieczone odpowiednim hasłem (chociaż i je można wyłączyć; AD daje możliwość zdalnego zarządzania użytkownikami poszczególnych komputerów). Dzięki temu, niezależenie od tego gdzie dany użytkownik naszej sieci zasiądzie do pracy, zawsze dostanie odpowiednie narzędzia i układ ikon.

UWAGA! Należy pamiętać, że Active Directory nie zapewnia nam jednolitego oprogramowania. Każde oprogramowanie (np. pakiet Office) MUSI być niezależnie instalowany na każdym komputerze z osobna. Wyjątek stanowi oprogramowanie, które nie wymaga integracji z rejestrem systemowym (tzw. aplikacje zdalne).

Wszystkie dane użytkownika, jeżeli nie posiada on zablokowanego profilu przed zapisem, będą gromadzone na aktualnie wykorzystywanym komputerze. Jeżeli użytkownik będzie logował się na innym komputerze to, w przypadku pierwszego uruchomienia profilu, katalog domowy zostanie pobrany z serwera (a tym samym wszystkie ustawienia ekranu startowego , pulpitu oraz pozostałe). Dodatkowo co logowanie na innej maszynie użytkownik będzie posiadał inne ustawienia (jeżeli na danej stacji roboczej je zmieni). Dla takiego użytkownika sytuacja ta może być bardzo niekomfortowa i wprowadzać w pewnym stopniu spore nieuporządkowanie (fragmentację profilu).

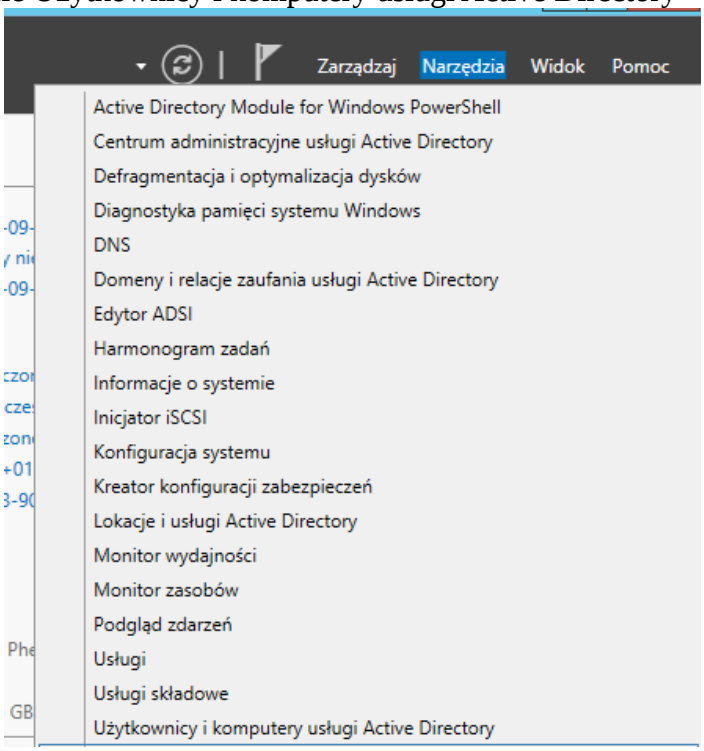
Pewnym rozwiązaniem jest wymuszenie korzystania z mapowanego dysku. Wszystkie dokumenty, dane i inne informacje użytkownik powinien gromadzić w zmapowanym, udostępnionym na serwerze katalogu. Ponieważ dysk automatycznie przypina się do okna Komputer (jest widziany jako fizyczny napęd) użytkownik będzie miał zawsze dostęp do swoich danych niezależnie od komputera, z którego korzysta (będzie miał dostęp nawet w przypadku, gdy w danym dniu będzie korzystał z własnego komputera, np. laptopa).

Istnieje także jeszcze jedno, znacznie wygodniejsze rozwiązanie – profil mobilny. Profile mobilne otrzymują na serwerze odrębne katalogi składowane w jednym, nadrzędnym katalogu zbiorczym (trzeba go utworzyć; trzeba także zadbać o jego odpowiednią widoczność dla domeny oraz uprawnienia użytkownika). Od tego momentu niezależnie gdzie użytkownik się zaloguje (serwer, maszyna z Windows XP/7/8.1) zawsze będzie miał dostęp do wszystkich ustawień oraz

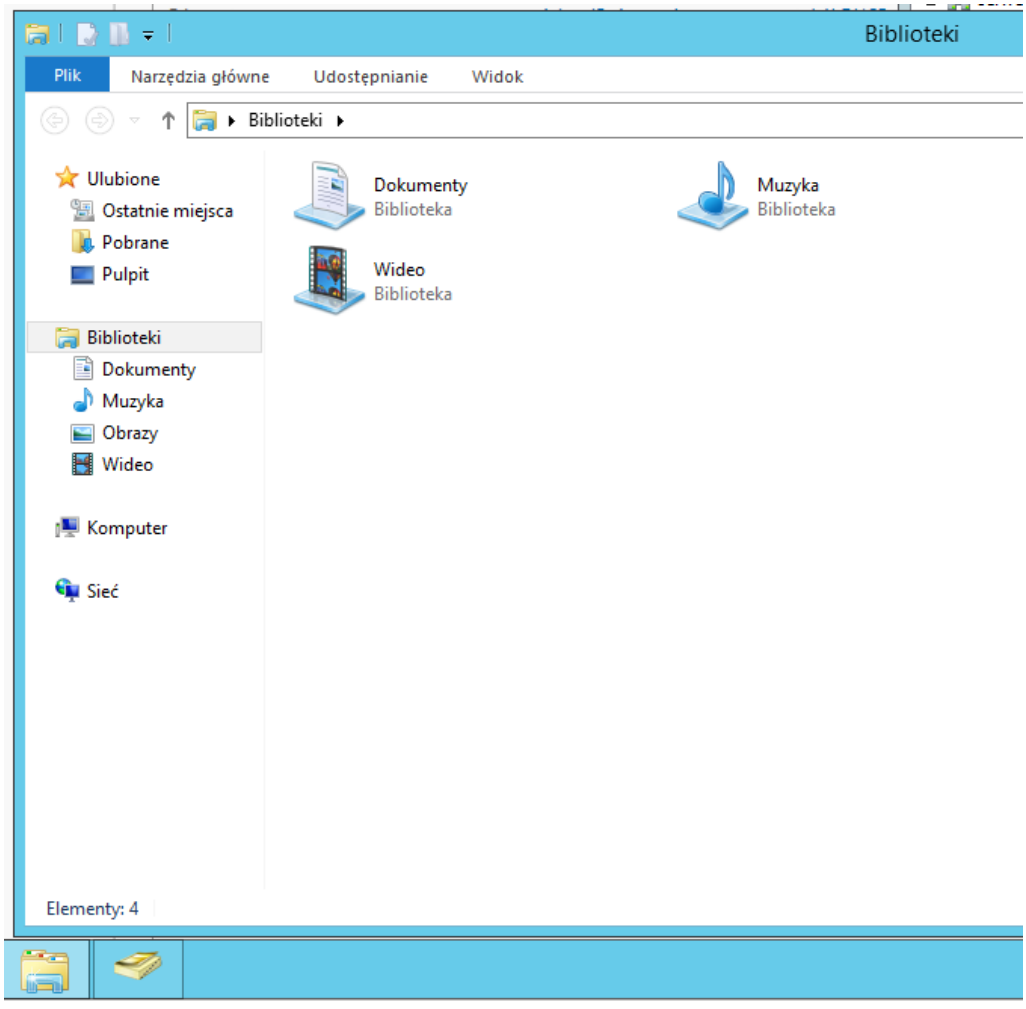
katalogów wraz z zapisanymi plikami w obrębie konta (katalog Użytkownika w systemie Windows).

TWORZENIE KONTA MOBILNEGO:

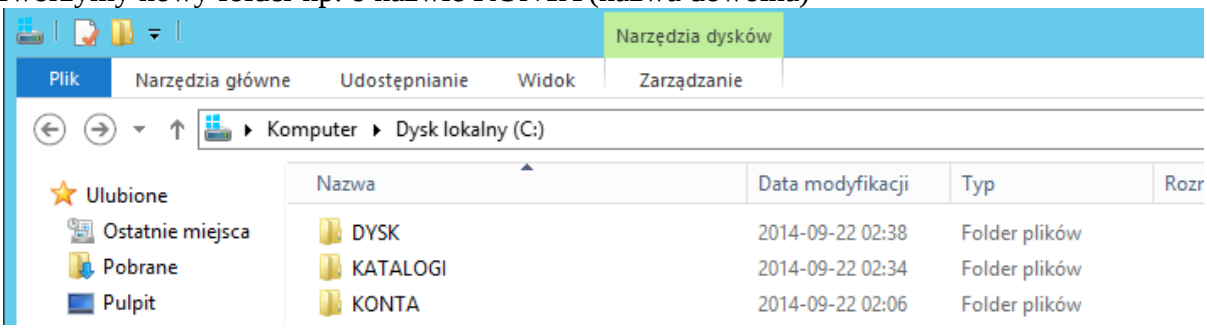
1. Otwieramy narzędzie Użytkownicy i komputery usługi Active Directory



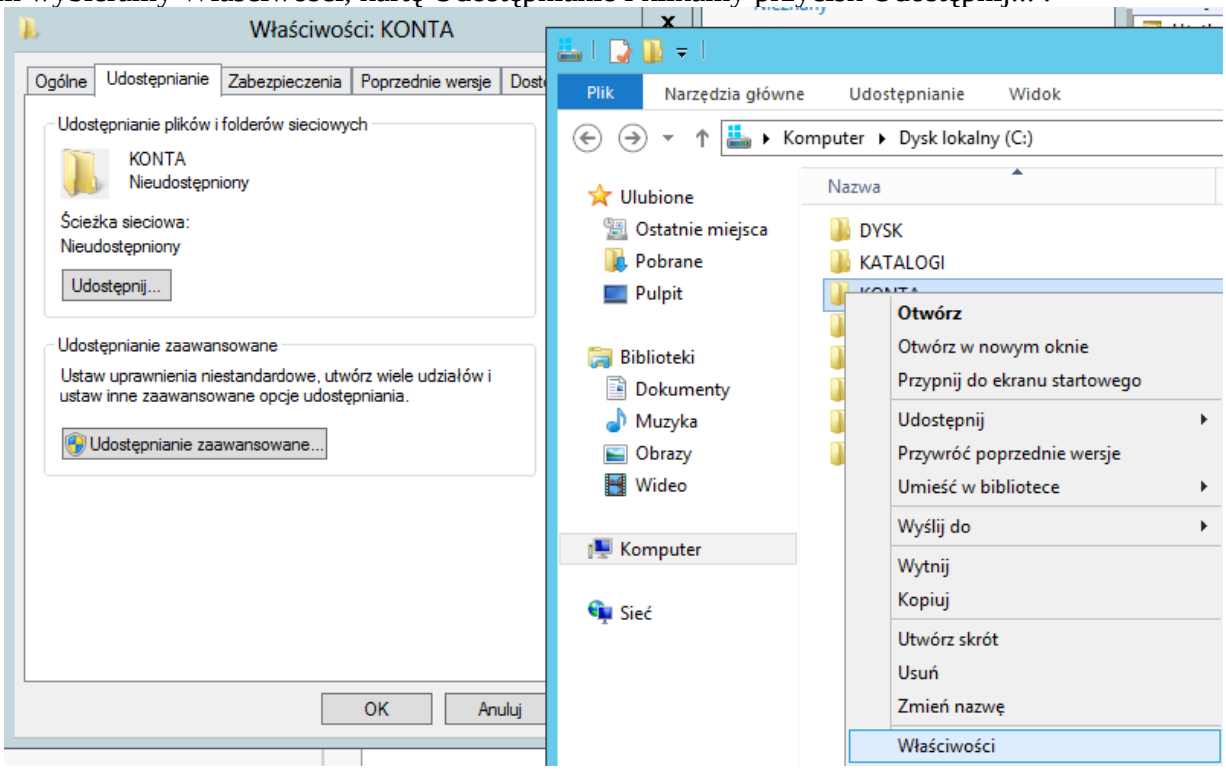
2. Otwieramy Eksplorator plików



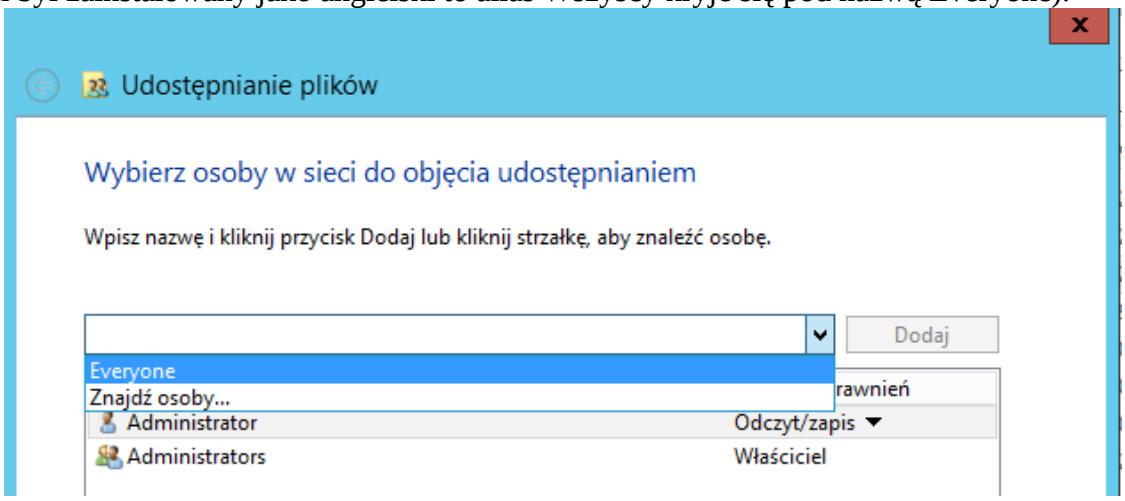
3. Tworzymy nowy folder np. o nazwie KONTA (nazwa dowolna)



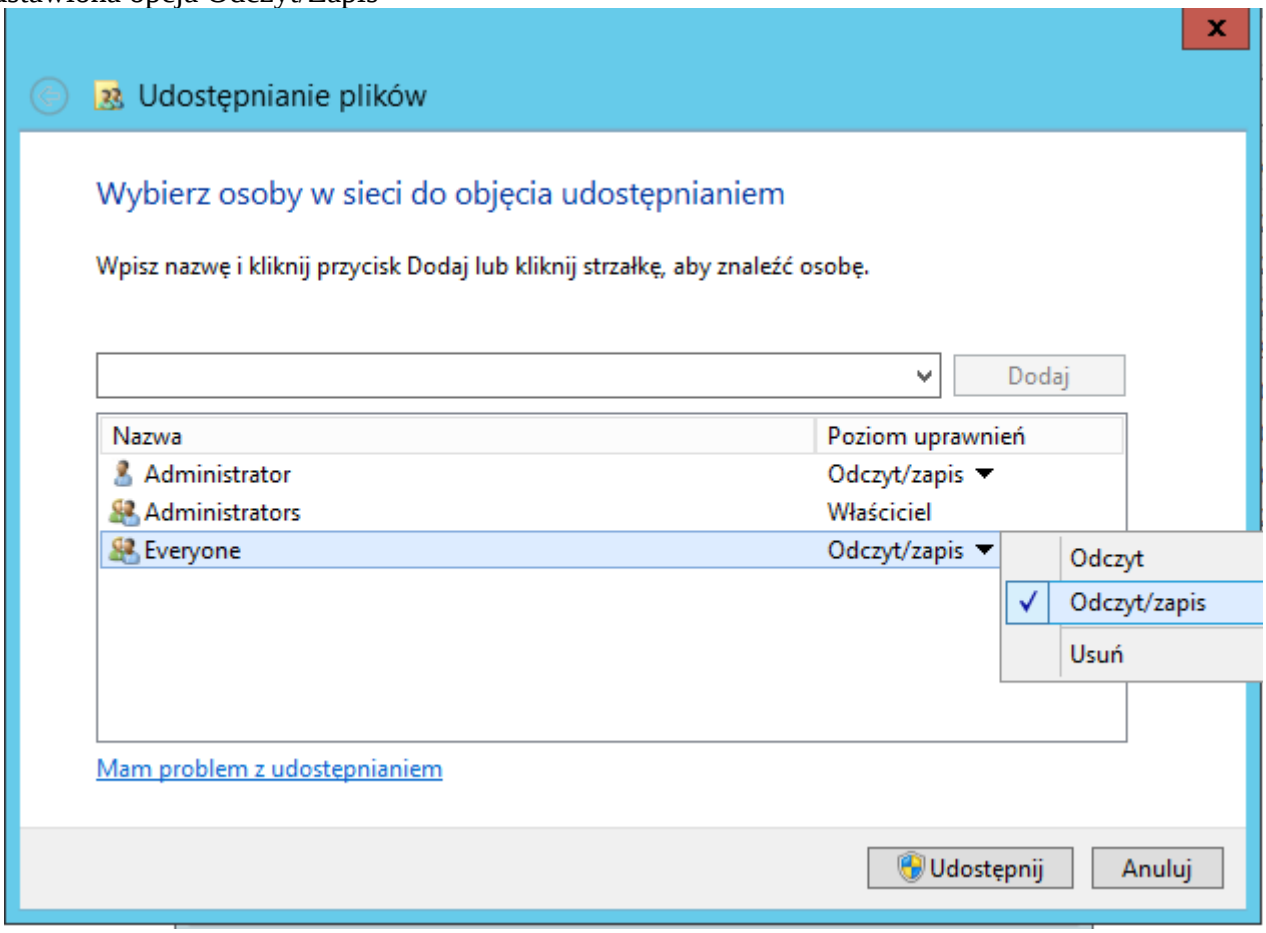
4. Teraz musimy ustawić odpowiednie opcje udostępniania dla tego folderu. Generalnie musi być dostępny dla wszystkich użytkowników z pełnymi prawami zapisu/odczytu (dopiero foldery domowe poszczególnych użytkowników będą miały spersonalizowane ustawienia). W związku z tym wybieramy Właściwości, kartę Udostępnianie i klikamy przycisk Udostępnij... .



5. W nowo otwartym oknie będziemy widzieć aktualnie uprawnione osoby i grupy, które będą mieć automatycznie przydzielone odpowiednie prawa. Ponieważ jednak nam zależy, by każdy użytkownik systemu mógł korzystać z tego katalogu możemy ustawić opcję Wszyscy (ponieważ system był zainstalowany jako angielski to alias Wszyscy kryje się pod nazwą Everyone).

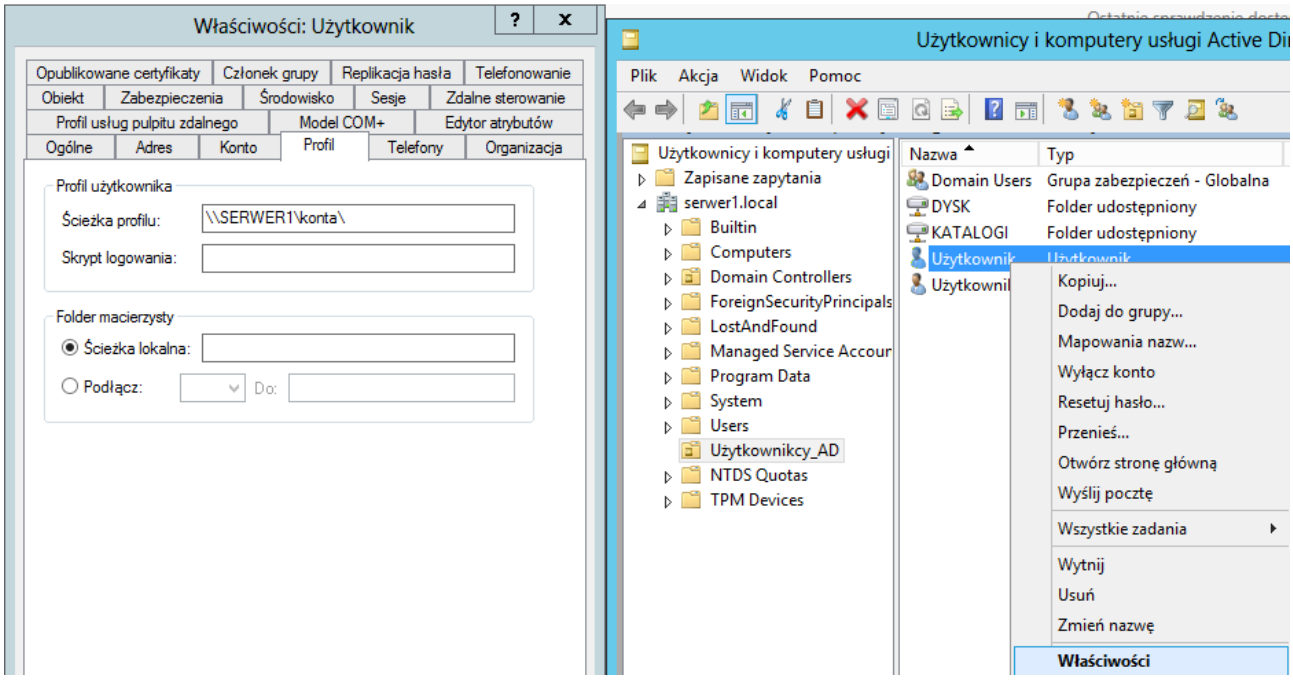


6. Teraz trzeba zadbać o odpowiedni poziom uprawnień. Przy „użytkowniku” Everyone musi być ustawiona opcja Odczyt/Zapis

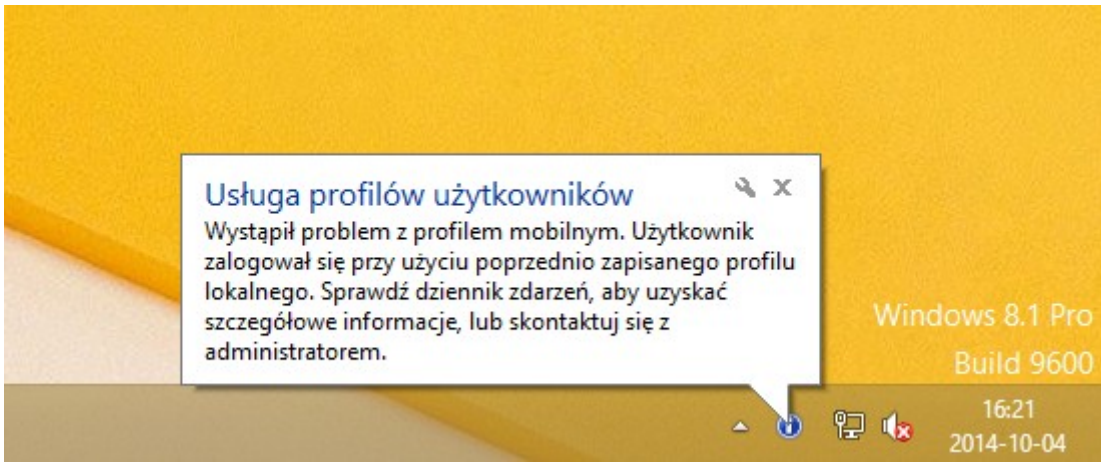


7. Teraz można kliknąć Udostępnij. System nada uprawnienia oraz zadba o widoczność nowego zasobu w otoczeniu sieciowym.
8. Kolejnym elementem będzie nadanie wskazanemu użytkownikowi ścieżki do składowania informacji profilowych. W tym celu w narzędziu Użytkownicy i komputery usługi Active Directory wybieramy kontener z utworzonymi poprzednio użytkownikami. Wybieramy prawym przyciskiem myszy konto jednego z tych użytkowników i klikamy Właściwości. Na zakładce Profil w grupie Profil użytkownika trzeba zmienić wartość pola Ścieżka profilu. W opisywanym przypadku będzie to

\\SERWER1\konta\user1



UWAGA! Jeżeli wskażemy na katalog, w którym już inny użytkownik składuje swoje dane (nadał swoje prawa i zabezpieczenia) to serwer nie będzie w stanie utworzyć profilu mobilnego - ze względów bezpieczeństwa system nie dopuści do skopiowania do niego/zamiany w nim informacji poufnych (katalog użytkownika mobilnego posiada ochronę danych – nikt poza samym użytkownikiem oraz wewnętrznym systemowym kontem SYSTEM nie ma do niego dostępu ani praw). Po zalogowaniu użytkownika system klienta, ponieważ nie będzie mógł nałożyć odpowiednich praw na katalog, nie zapisze informacji na serwerze, a sam użytkownik dostanie stosowny komunikat:



Podobny efekt otrzymamy gdy nie udostępnimy folderów kont w sieci/domenie.

Jeżeli wszystko wykonamy według powyższej instrukcji to wraz z pierwszym zalogowaniem po zmianie system utworzy w przygotowanym folderze katalog użytkownika mobilnego. Od tego momentu za każdym razem kiedy użytkownik będzie się wylogowywał stan jego konta zostanie zapisany na serwerze. Z kolei przy logowaniu w dowolnej części sieci stan jego konta będzie pobierany do maszyny docelowej/zamieniany na aktualny. Jeżeli stan będzie taki sam to po prostu nic nie zostanie dodane/skasowane/zmodyfikowane (nawet modyfikacja jednego znaku w pliku tekstowym powoduje podmianę danego pliku na nowy).

INFORMACJA Trzeba pamiętać, że usługa nie nadpisuje danych w czasie rzeczywistym! Wszystko

jest aktualizowane jedynie w trakcie logowania oraz wylogowywania użytkownika z systemu.

UŻYTKOWANIE PROFILU MOBILNEGO

Niestety profil mobilny może stać się „przekleństwem” dla sieci lokalnej oraz dla samego użytkownika. Trzeba bowiem pamiętać, że nawet w tej chwili sieci w dużych firmach bazują na rozwiązaniach z przepustowością do 100 Mbit/s. Jeżeli użytkownik pobierze w trakcie korzystania z sieci duży plik (np. plik obrazu serwera SQL – ok 2 GB) i wyloguje się to trzeba pamiętać, że synchronizacja do serwera potrwa ok. 200 sekund pod warunkiem, że synchronizacji dokonuje tylko jeden użytkownik. Jeżeli większa ilość użytkowników próbowałaby tego dokonać to czas ten może się drastycznie wydłużyć (najczęściej serwer także posiada jedną kartę sieciową; w jego wypadku prędkość karty dzieli się pomiędzy wszystkich użytkowników).

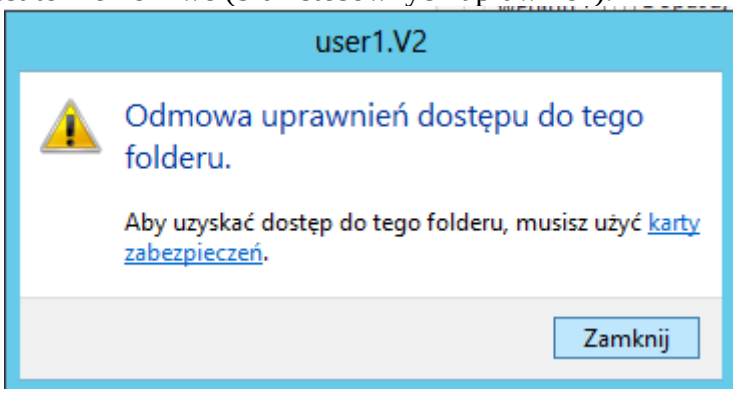
Rozwiązaniem tego problemu jest odpowiednia konfiguracja profilu użytkownika, np. przesunięcie niektórych folderów do innych katalogów lokalnych (w tym wypadku wystarczy odpowiednio skonfigurować przeglądarkę internetową). Użytkownik może jednak obejść takie zabezpieczenie i zapisać swój pobierany plik na pulpicie.

Oznacza to więc, że lepiej zrezygnować z profili mobilnych? Niekoniecznie. Można bowiem wymusić na serwerze by przekazywał samą konfigurację stanowiska pomiędzy poszczególnymi komputerami, a zapisane pliki i foldery automatycznie usuwał przy wylogowaniu z systemu.

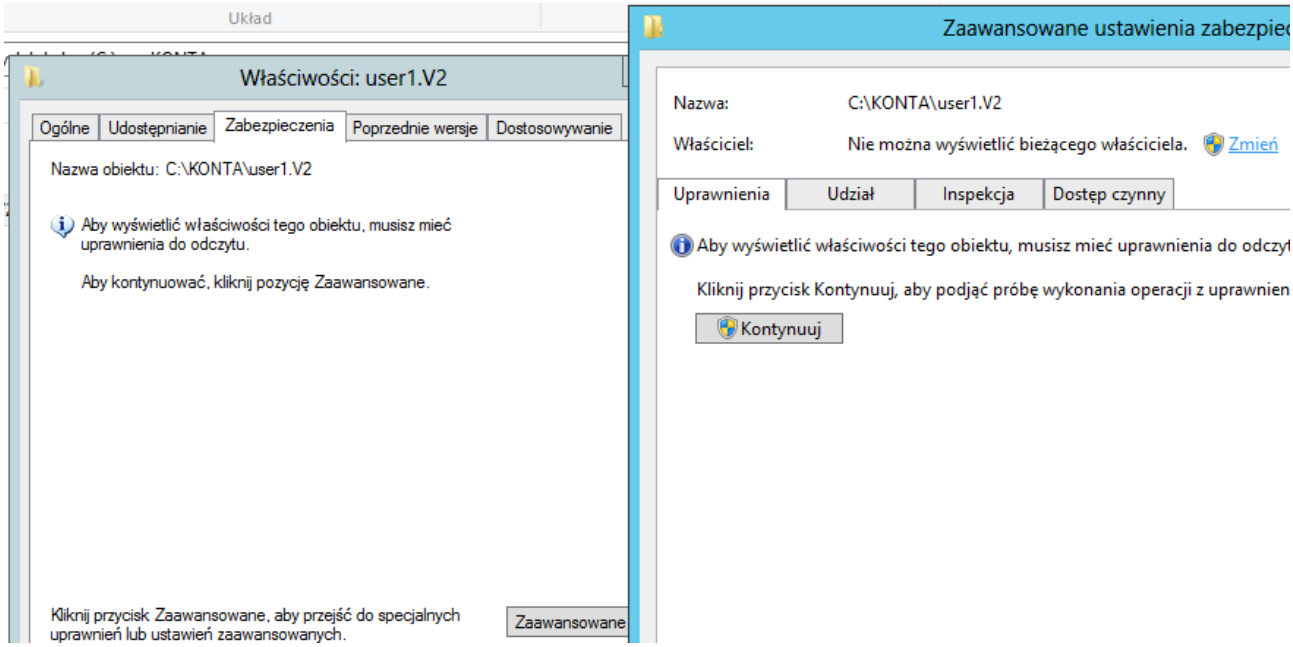
1. Należy przygotować nasz profil. Logujemy się na konto użytkownika na dowolnym systemie w sieci. Konfigurujemy jego wygląd, ustawienia pulpitu, aplikacji itd.

2. Wylogowujemy się. Profil zostanie zapisany na serwerze.

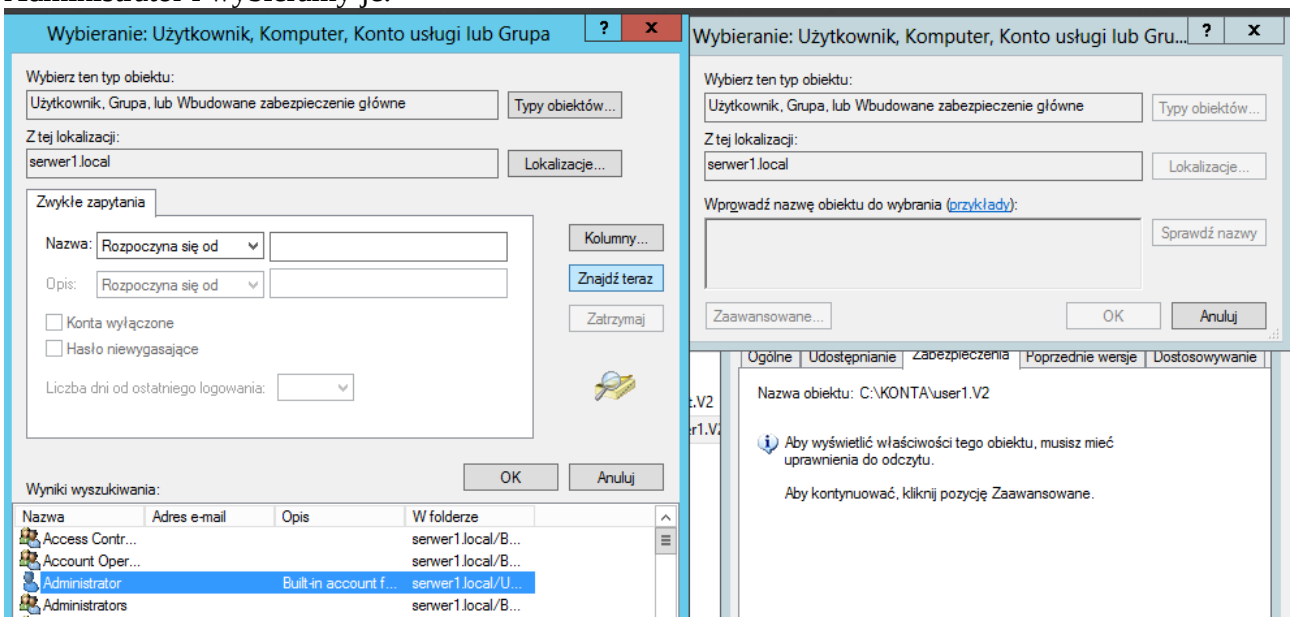
3. Teraz trzeba uzyskać dostęp do folderu konta użytkownika po stronie serwera. Nie jest to możliwe bez pewnych modyfikacji – gdy będziemy próbowali przejrzeć zawartość katalogu system poinformuje nas, iż jest to niemożliwe (brak stosownych uprawnień).



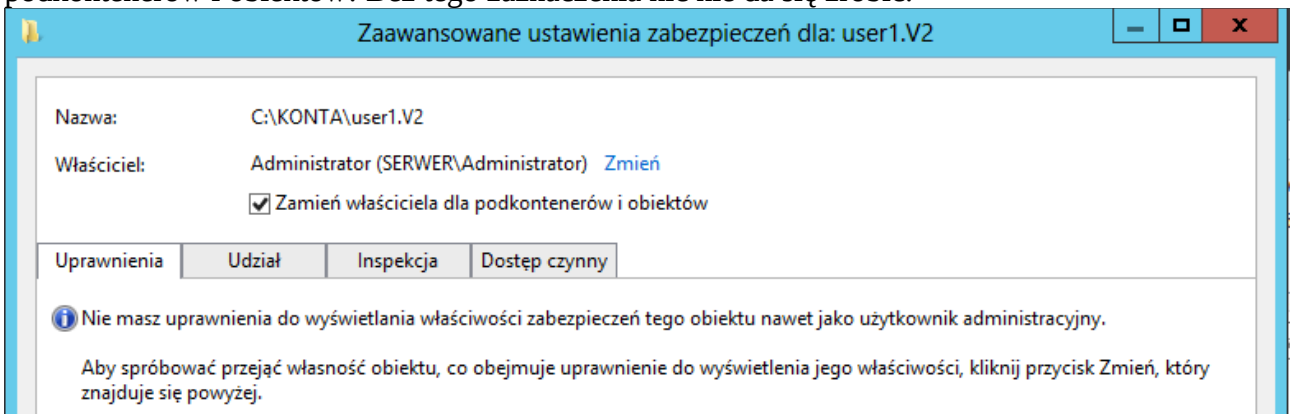
4. Po pierwsze należy uzyskać dostęp do zabezpieczeń. W tym celu klikamy prawym przyciskiem myszy na folderze domowym i wybieramy Właściwości. W otwartym oknie wybieramy zakładkę Zabezpieczenia i klikamy przycisk Zaawansowane. W nowo otwartym oknie klikamy zmianę właściciela folderu (opcja Zmień – podświetlone na zrzucie)



5. W nowym oknie (po prawej) klikamy przycisk Zaawansowane... . Otworzy się nowe okno, w którym trzeba kliknąć Znajdź teraz. W tym momencie zostaną wyszukane konta wszystkich dostępnych użytkowników oraz wszystkie grupy obecne w systemie. Odnajdujemy konto Administrator i wybieramy je.

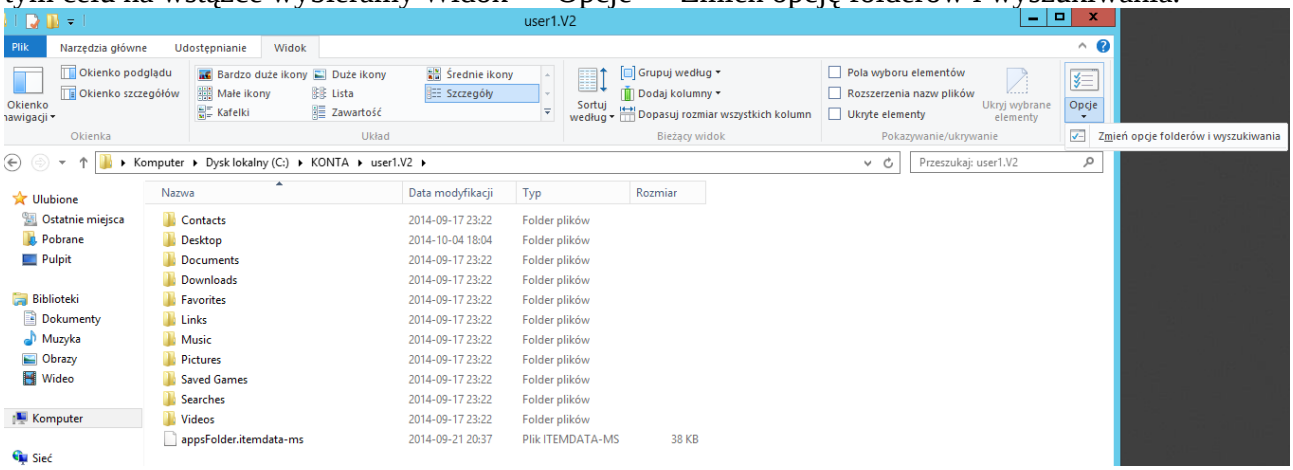


6. Przed zamknięciem okna bardzo ważne jest by zaznaczyć opcję Zamień właściciela dla podkontenerów i obiektów! Bez tego zaznaczenia nic nie da się zrobić.

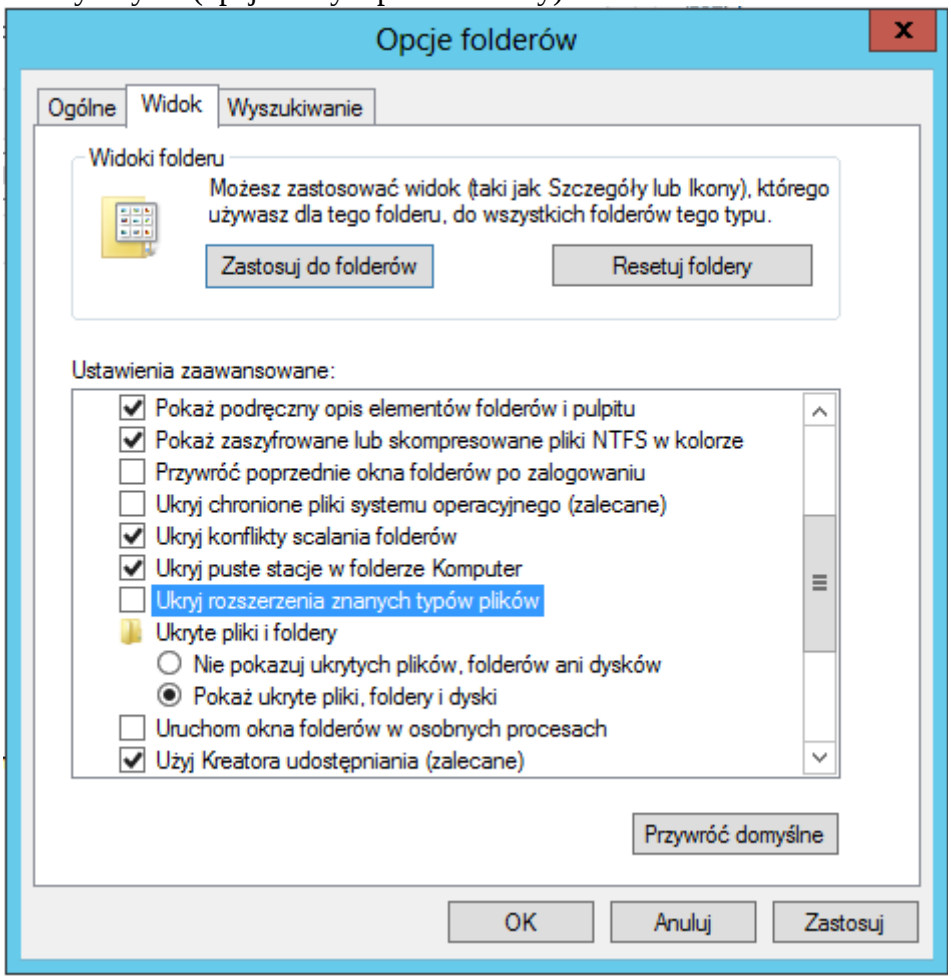


7. Teraz zamykamy wszystkie okna i komunikaty (wraz z komunikatem o nadaniu nam pełnych

uprawnień do odczytu – tak samo ważne!). Niestety nadal nie mamy dostępu do interesującego nas pliku (NTUSER.DAT). Plik jest niewidoczny (ukryty) oraz oznaczony jako systemowy (dodatkowe ukrycie). Ponadto by zmienić jego rozszerzenie musimy wyłączyć ukrywanie rozszerzeń plików. W tym celu na wstążce wybieramy Widok → Opcje → Zmień opcję folderów i wyszukiwania.

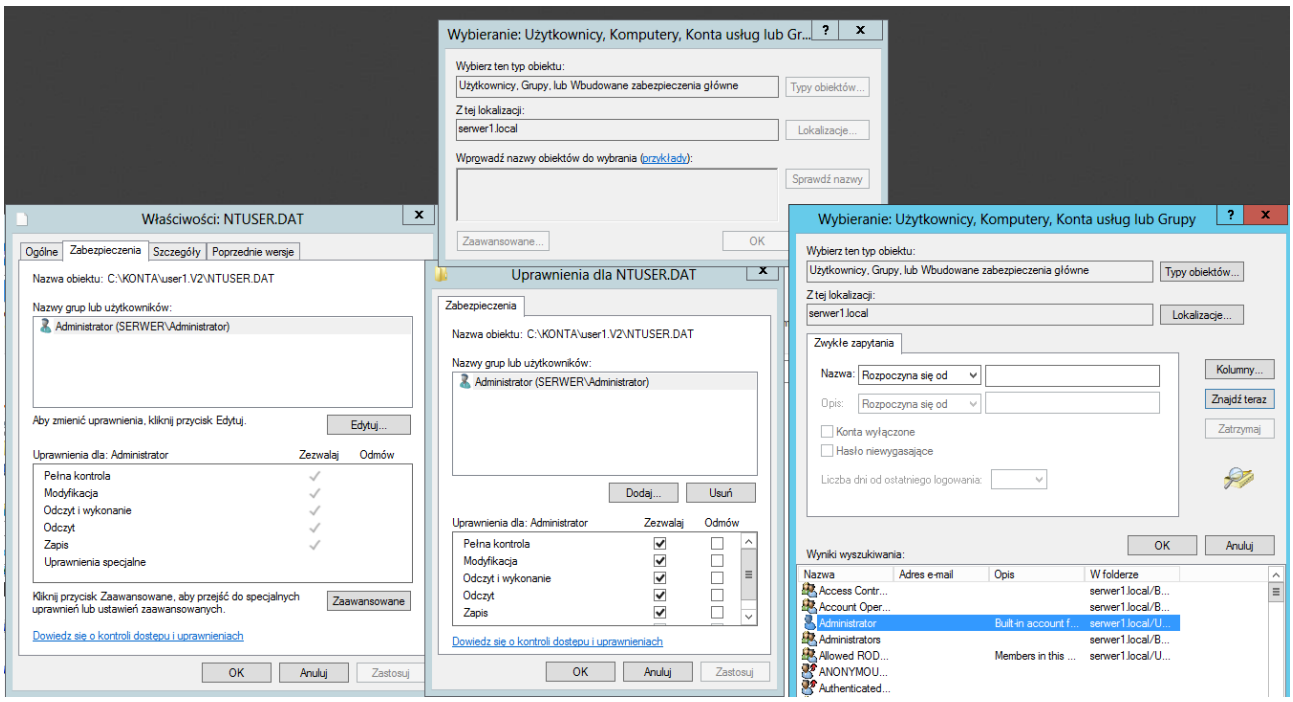


W nowym oknie wybieramy zakładkę Widok i odznaczamy Ukryj chronione pliku systemu operacyjnego, Ukryj rozszerzenia znanych typów plików oraz wybieramy zaznaczamy Pokaż ukryte pliki, foldery i dyski (opcja Ukryte pliki i foldery)



Teraz plik NTUSER.DAT powinien być już widoczny.

8. Prawdopodobnie plik będzie dodatkowo chroniony przez jakimikolwiek zmianami. Dlatego też trzeba zmienić jego ustawienia – dodać nasze konto administracyjne jako użytkownika uprzywilejowanego do zmian. Otwieramy właściwości pliku i dokonujemy zmian takich jak na poniższym zrzucie (Administrator ma mieć pełne prawa modyfikacji).



9. Teraz zmieniamy nazwę pliku z NTUSER.DAT na NTUSER.MAN (mandatory – obligatoryjny, ustalony). Od tego momentu system będzie wiedział, że nie wolno modyfikować mu zawartości tego pliku ani jakiejkolwiek zawartości profilu tego użytkownika. Po zmianie trzeba na powrót ustawić wszystkie zabezpieczenia jakie były poprzednio. Beza tego system nie skorzysta z z tego folderu przy uruchamianiu profilu naszego użytkownika! Poniżej zmiany jakich trzeba dokonać:
a) dla pliku NTUSER.MAN
- dodajemy użytkownika – właściciela profilu (pełne prawa)
- dodajemy konto SYSTEM (pełne prawa)
- kasujemy konto Administrator (jeżeli system powie, że to niemożliwe to można pominąć ten krok)
b) dla folderu z profilem
- zmieniamy właściciela na użytkownika, dla którego konfigurowaliśmy profil 9zaznaczamy zmianę dla podfolderów)
- dodajemy konto SYSTEM i nadajemy mu pełne uprawnienia (oraz dla całej zawartości)
- dodajemy naszego użytkownika i nadajemy mu pełne prawa (oraz dla całej zawartości)
- usuwamy naszego administratora
- zaznaczamy by system uczynił to dla wszystkich podfolderów
- klikamy Zastosuj
10. Logujemy się na konto użytkownika np. w systemie Windows 8.1. Jeżeli w katalogu Użytkownicy\<nasz_uzytkownik> znajduje się plik NTUSER.MAN to znaczy, że operacja przebiegła pomyślnie. Można spróbować dodać na pulpit np. folder, wylogować się i zalogować ponownie. Folder powinien zniknąć.
INFORMACJA: Użytkownik korzystający z tak zmienionego konta nie będzie mógł sam zmienić rozszerzenia pliku NTUSER.MAN. System będzie informował go iż plik ten jest aktualnie w użyciu i nie można na nim dokonywać jakichkolwiek zmian (proszę pamiętać, że to ten plik przechowuje m.in. zawartość naszego rejestru systemu Windows).

Zadania:
1. Proszę spróbować zalogować się do swojej domeny na komputerze innej osoby w sali. Proszę za pomocą tamtego systemu pobrać jakiś plik (do 100 MB) i zapisać go na pulpicie. Następnie proszę zalogować się na swoje konto z powrotem u siebie i sprawdzić czy plik się pojawi.
2. Proszę zmienić ustawienia profilu na mobilny. Proszę powtórzyć etapy z punktu 1 i zobaczyć czy profil spełnia swoje zadanie.