Zarządzanie użytkownikami i grupami w Windows Server

Poprzednio utworzyliśmy jedno testowe konto użytkownika w systemie Windows Server by zobaczyć, jak działa logowanie w domenie Active Directory. Jednak samo tworzenie kont nie sprowadza się do wprowadzania nazwy użytkownika oraz hasła. Użytkownicy systemu mogą bowiem mogą mieć mniej lub bardziej ograniczane prawa do wykonywania poszczególnych czynności. Niektórzy wręcz nie powinni mieć żadnych praw w tworzonym systemie sieci lokalne poza uruchamianiem określonych aplikacji – w przeciwnym wypadku mogliby, przez swoją niewiedzę bądź z pełną świadomością destabilizować działanie pozostałych maszyn, wykradać dane itp.

Dlatego administrator sieci wykorzystujący system Windows Server do centralnego zarządzania kontami użytkowników powinien odpowiednio planować jakie konta będzie tworzył, w jaki sposób będą one wykorzystywane, czy przypadkiem nie powinny być one dostępne tylko w określonym czasie, do których katalogów dany użytkownik powinien mieć dostęp itd. itp.

Domena systemu Windows daje swego rodzaju swobodę w zarządzaniu kontami. Można bowiem tworzyć konta ze względu na odpowiednie zadania (np. dla uczniów na konkretne przedmioty), za pomocą których można logować się na dowolnych komputerach w jednym i tym samym czacie. Pozwala to na odpowiednie przygotowanie pulpitów, zainstalowanych programów oraz innych części konta tak, by w razie jakiejkolwiek modyfikacji nie zachodziła potrzeba modyfikacji np. 50 kont. Dodatkowo konta te mają taką przewagę, iż w przypadku wymiany fizycznych użytkowników (wiadomo, że uczniowie zmieniają się co roku) nie trzeba było tworzyć wszystkiego od nowa (wystarczy przykładowo opróżnić jeden katalog, bez kasowania i tworzenia wszystkich kont). Niestety rozwiązanie to ma swoje wady – poszczególni użytkownicy mogą zapisywać swoje treści np. na pulpicie, przez co w następstwie będą one widoczne dla innych użytkowników.

Drugim sposobem jest tworzenie kont dla każdego użytkownika. Daje to pełną personalizację, dodatkowo pozwala na śledzenie poczynań użytkownika, umożliwia stworzenie statystyk logowania, najczęściej wykorzystywanych aplikacji, a także pozwala na dostosowanie pulpitu i przypisanych do niego właściwości według jego potrzeb. Wadą jest natomiast brak ujednolicenia aplikacji, menu start, uprawnień czy też dodatkowego oprogramowania.

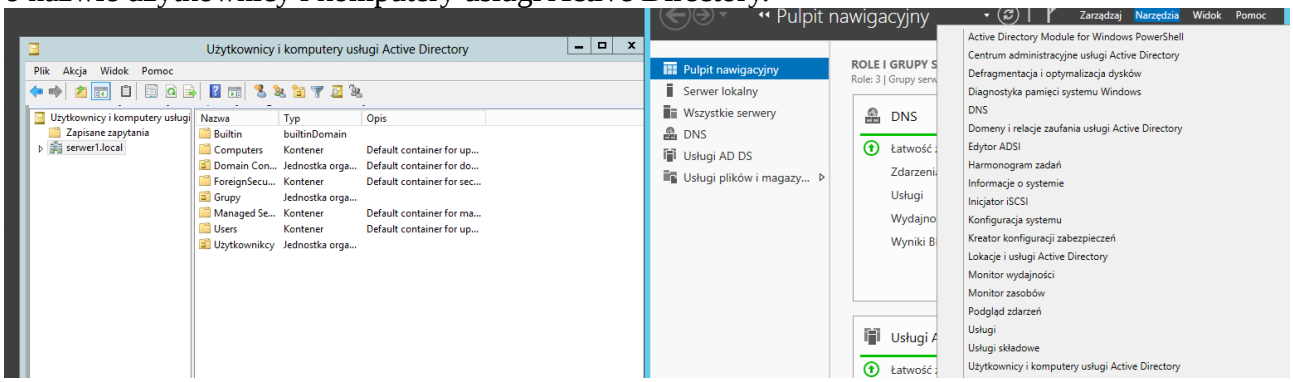
Można oba wyżej pomysły także łączyć - tworzyć np. 5 kont dla poszczególnych funkcji (np. student1, student2, student3, student4, student5), poustawiać dla nich osobne hasła, pododawać odpowiednie opcje oraz uprawnienia. Kota praktycznie trzeba będzie konfigurować raz, później będzie to jedynie np. czyszczenie zawartości folderu domowego.

Każdy administrator może wypracować swoje własne, „właściwe” rozwiązanie. Pamiętać należy jedynie o zachowaniu poufności danych, zabezpieczeniu szczególnie ważnych zasobów systemowych, a także o potencjalnej potrzebie zdobycia informacji, kto w danym momencie korzystał z danego konta.

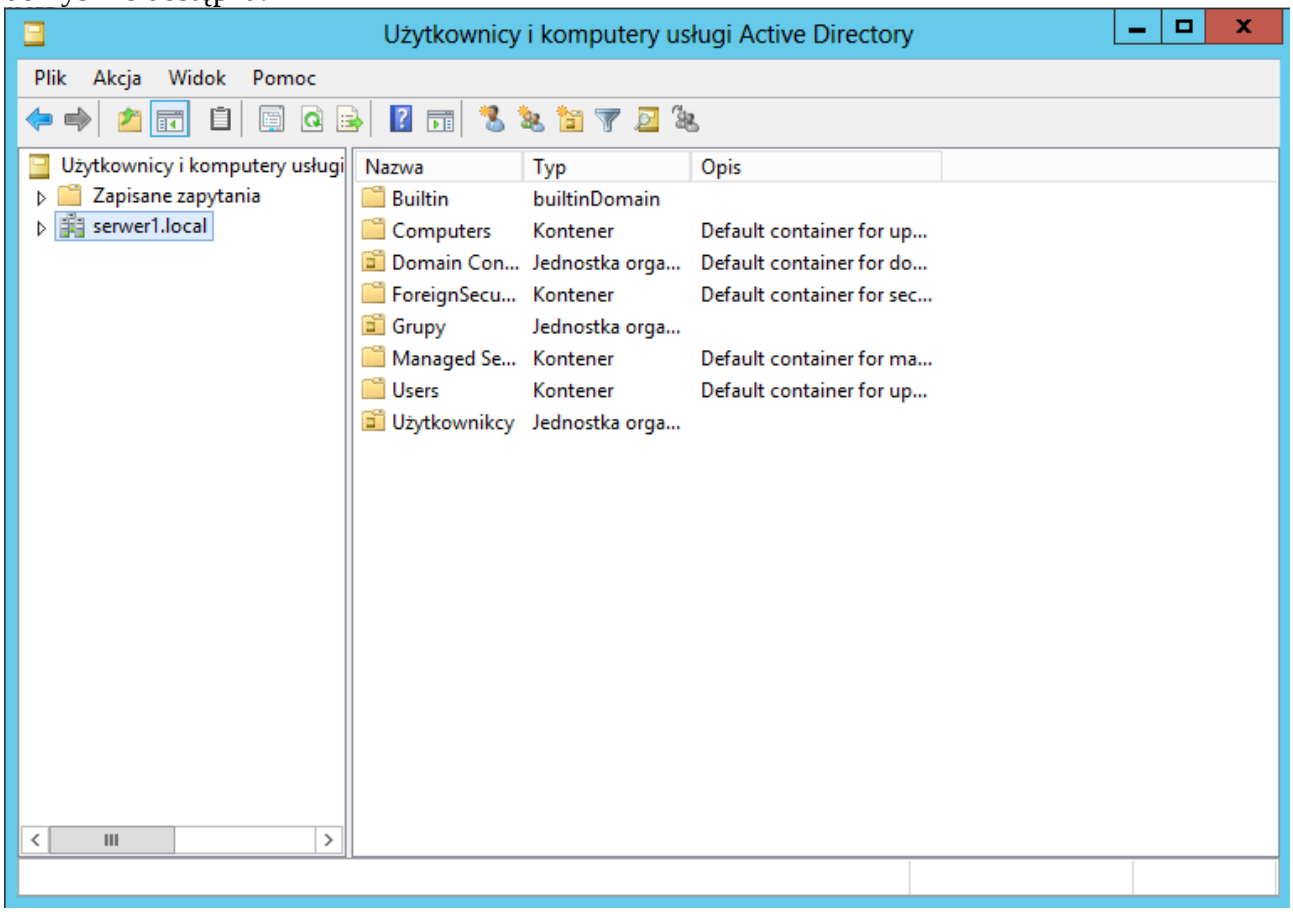
Kolejnym aspektem zarządzania użytkownikami są grupy użytkowników. Grupy stanowią swoisty zbiór poszczególnych kont. Zdarza się przecież tak, że dany serwer może mieć np. 3 administratorów. Konta te powinny być jak najbardziej osobiste (by było wiadomo, który administrator logował się do systemu i co zrobił), jednak każdy z administratorów powinien mieć nieograniczone możliwości w zarządzaniu systemem. Inna grupę mogą stanowić np. administratorzy domeny, którzy będą mogli zarządzać samą domeną, tworzyć/usuwać użytkowników bądź poszczególne zasoby do niej przypisane. W końcu sami użytkownicy mogą tworzyć pewne grupy – np. kierownicy projektów powinni mieć dostęp do katalogów z odpowiednimi materiałami, podczas gdy wykonawcy winni mieć dostęp do materiałów przesłanych przez kierowników. Przypisywanie każdemu z osobna uprawnień do poszczególnych zasobów systemowych byłoby bardzo czasochłonnym zajęciem. Jednak zamiast tego można nadać uprawnienia grupie, a wtedy wszyscy do niej należący użytkownicy (obecni oraz przyszli) automatycznie nabędą odpowiednie poświadczenia.

1. Zarządzanie użytkownikami.

Poznane na poprzednich zajęciach narzędzie (Centrum Administracyjne usługi Active Directory) niestety ma sporo ograniczeń – nie pozwana przykładowo na dodawanie urządzeń w usłudze domen, dodawaniu własnych kontenerów, udostępnionych zasobów itp. Poza tym dla administratorów znających narzędzia w poprzedniej wersji systemu może być po prostu niewygodne. Dlatego lepszym rozwiązaniem będzie znane z poprzednich wersji systemu narzędzie o nazwie użytkownicy i komputery usługi Active Directory.

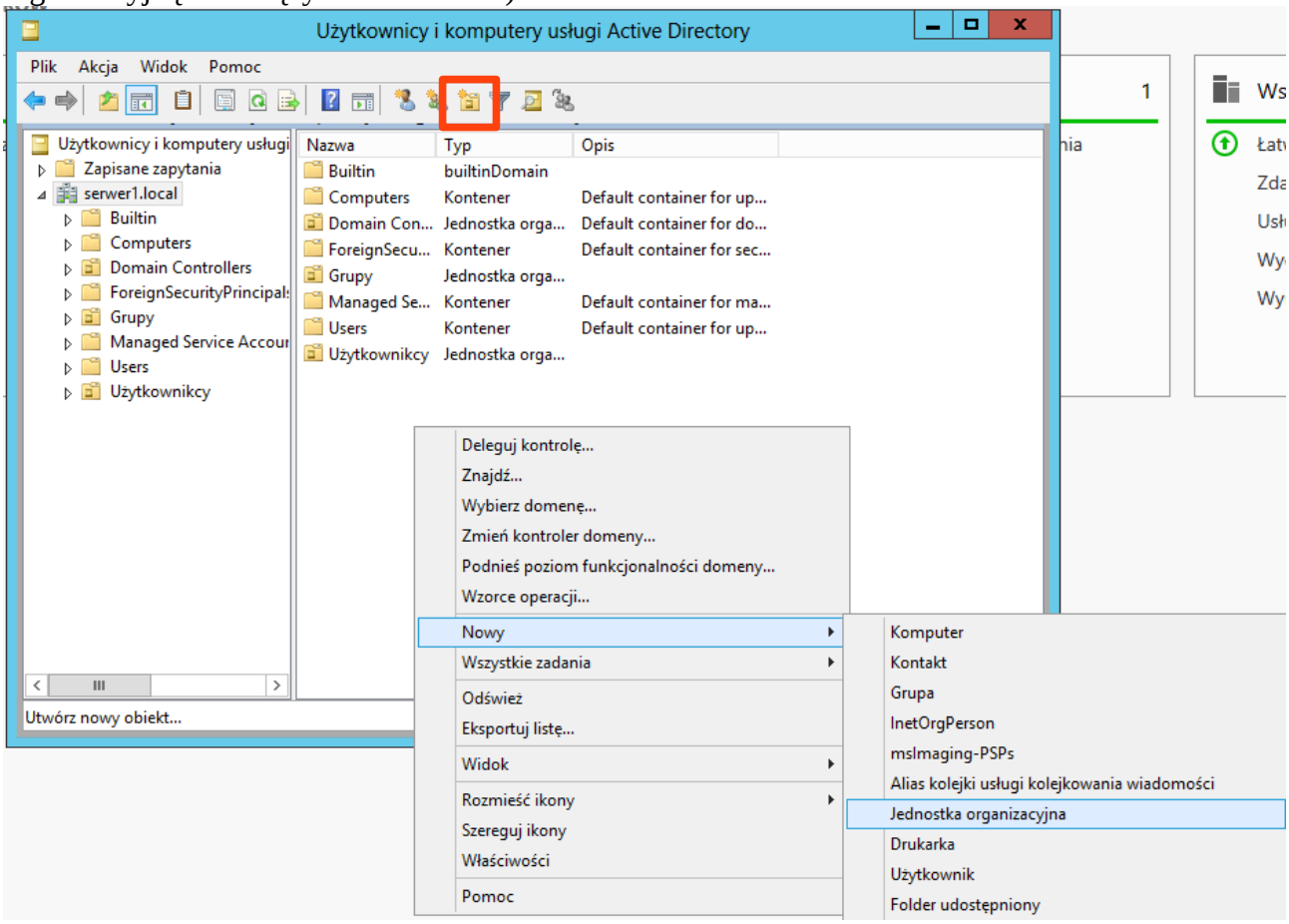


Narzędzie pozwala na zarządzanie zarówno lokalnie ustanowioną domeną jak i wszystkimi domenami dostępnymi w lesie. Nas interesuje wcześniej utworzona lokalna domena, która jest domyślnie dostępna:



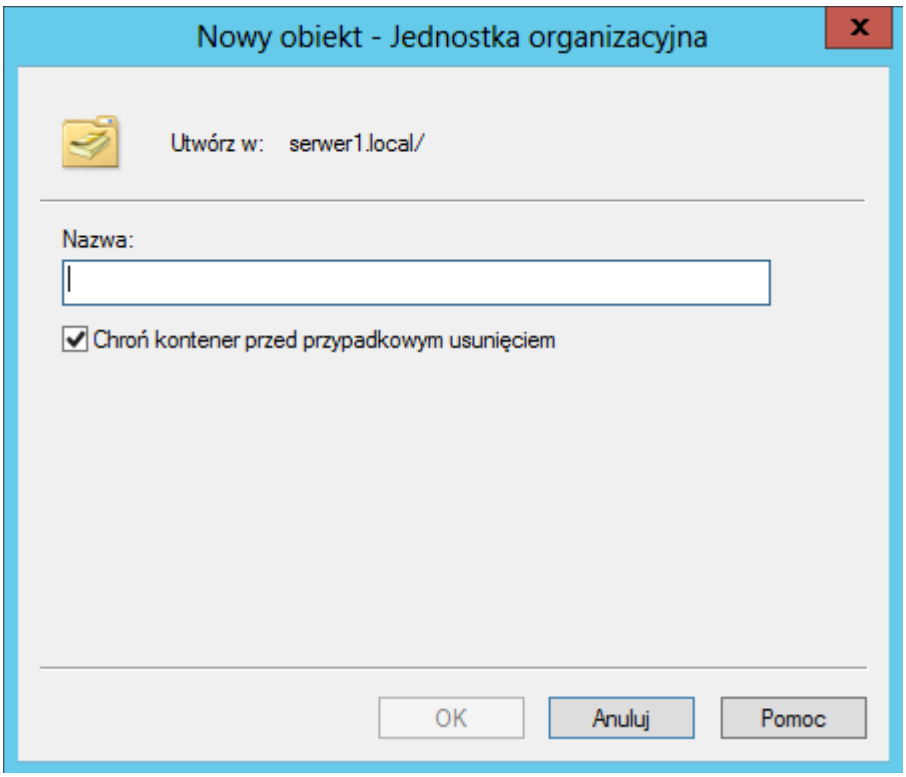
Administrator może z tego miejsca zarządzać zarówno kontenerami, jednostkami organizacyjnymi jak i ich zawartością – komputerami podłączonymi do domeny, grupami, użytkownikami. Domyślnie wszyscy użytkownicy oraz grupy użytkowników znajdują się w kontenerze Użytkownicy (Users). Kontenery (CN) stanowią logiczną, wbudowaną – mają za zadanie domyślnie grupować w hierarchii pewne elementy i stosować dla nich pewne domyślne ustawienia. Niestety tych ustawień nie da się zmienić indywidualnie – są domyślnie stosowane dla wszystkich elementów w kontenerze.

W celu indywidualnego grupowania poszczególnych elementów służą jednostki organizacyjne (OU). Można do nich przenosić dowolne elementy. Pozwalają też na tworzenie w ramach swojej struktury kolejnych jednostek organizacyjnych (w kontenerach nie można zagnieżdżać kolejnych kontenerów ani też jednostek organizacyjnych).
Należy pamiętać, że poszczególne elementy (foldery udostępnione, serwery, komputery i inne) można dowolnie przenosić zarówno pomiędzy kontenerami jak i jednostkami organizacyjnymi. Skutkuje to nałożeniem/zdjęciem odpowiednich zasad grup (Group Policy Object – GPO), jednak nie wpływa w żaden sposób na właściwości samych elementów.
Przykładowo utworzenie jednostki organizacyjnej, w której zgrupujemy użytkowników domeny, osiągalne jest na dwa sposoby:
a) po wybraniu nazwy serwera z listy serwerów (lewa strona), można kliknąć prawym przyciskiem myszy w polu po prawej stronie (ukazującym wszystkie jednostki organizacyjne, kontenery oraz elementy AD). Z menu kontekstowego należy wybrać Nowy->Jednostka organizacyjna.
b) po wybraniu nazwy serwera, w pasku narzędziowym (pod menu okna) należy wybrać ikonę folderu z gwiazdką (po najechaniu myszy wyświetli się podpowiedź „Utwórz nową jednostkę organizacyjną w bieżącym kontenerze”)

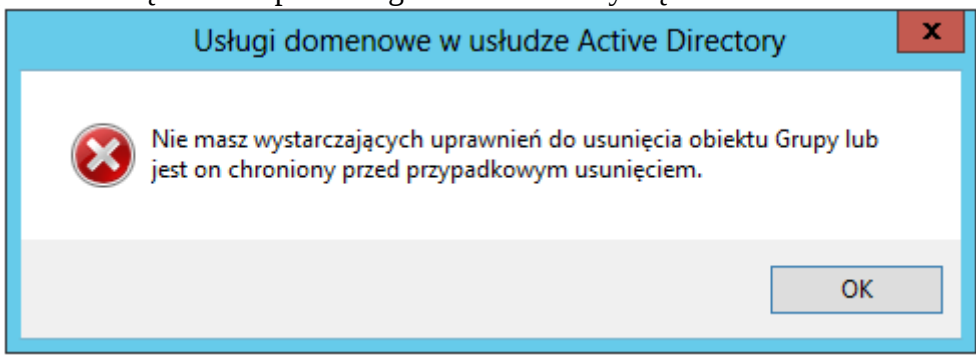


INFORMACJA: Kontenerów w zasadzie nie można tworzyć. Jeżeli jednak byłyby one nam niezbędne to trzeba użyć innego narzędzia o nazwie Edytor ADSI.

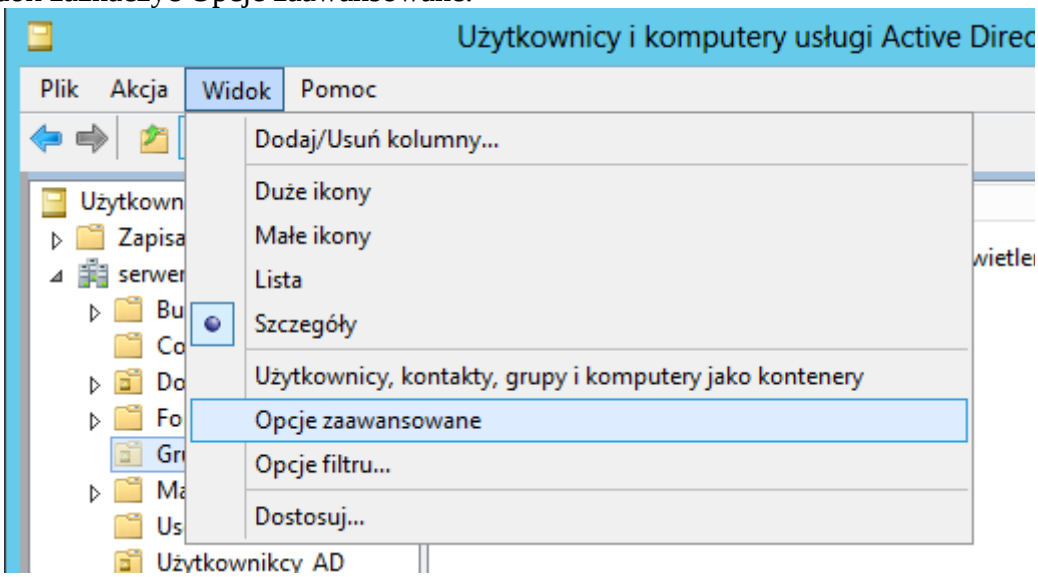
Jakkolwiek nie uruchomimy dodawania jednostki organizacyjnej, pojawi się okno, w którym, należy podać jej nazwę. Nazwa musi być unikatowa w skali całego AD. Narzędzie od razu sugeruje zaznaczenie pola „Chroń kontener przed przypadkowym usunięciem” - usunięcie tak zabezpieczonego obiektu będzie możliwe tylko wtedy, gdy odznaczymy to pole w jego właściwościach.



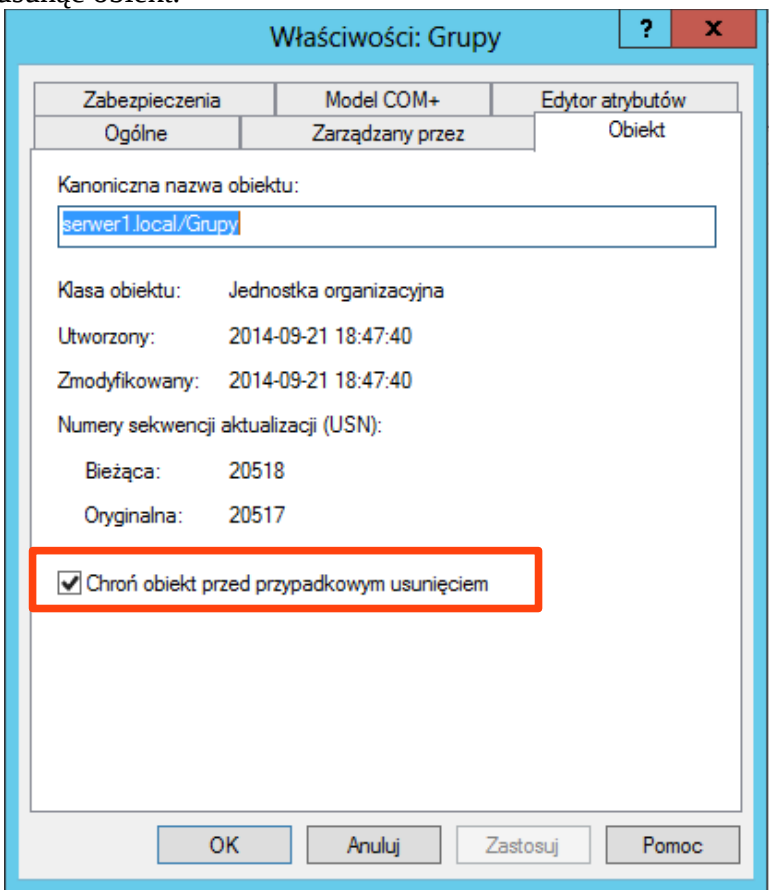
Późniejsza próba usunięcia zabezpieczonego obiektu kończy się takim komunikatem:



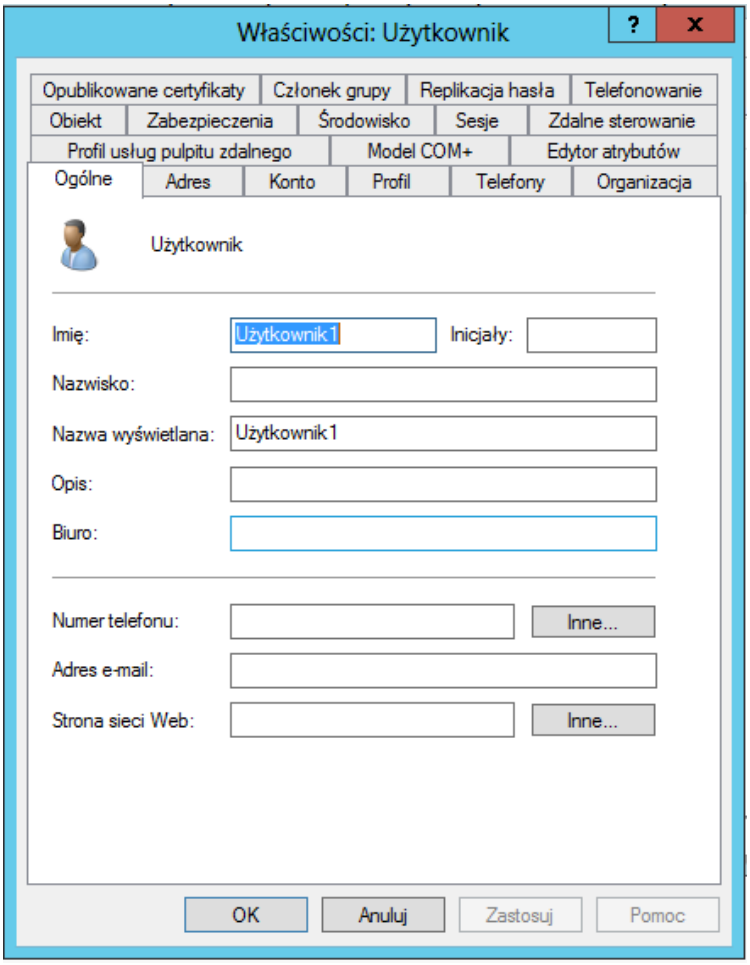
INFORMACJA: Jeżeli z jakichś powodów zechcemy usunąć zabezpieczone elementy to, jak już zostało wspomniane, trzeba zdjąć nałożone zabezpieczenie przed usunięciem (jeżeli zostało nałożone). Niestety w podstawowym widoku narzędzie nie da nam możliwości zmiany stanu tego pola – po wybraniu właściwości danego obiektu jest ono ukryte. W celu zmiany tego stanu należy w menu Widok zaznaczyć Opcje zaawansowane.



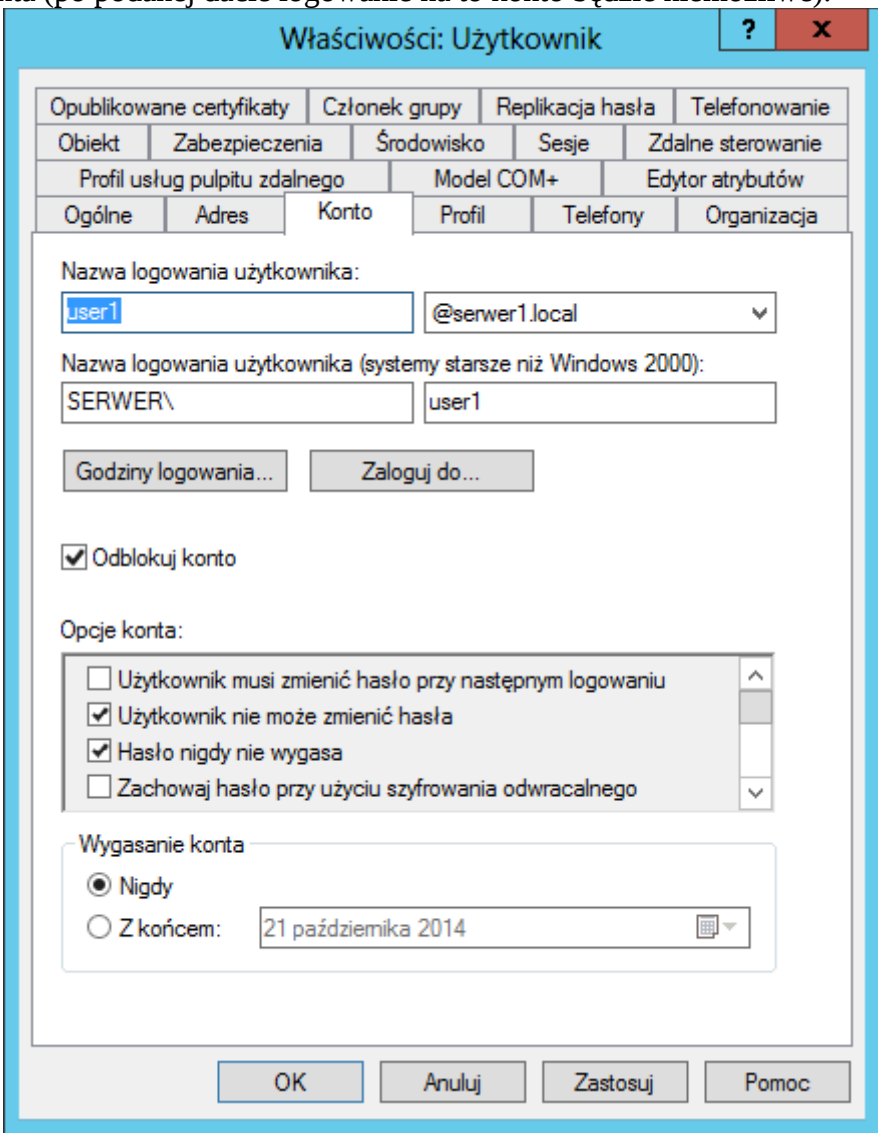
Od tego momentu we właściwościach elementów będzie widoczne pole z ochroną, które można będzie odznaczyć i usunąć obiekt.



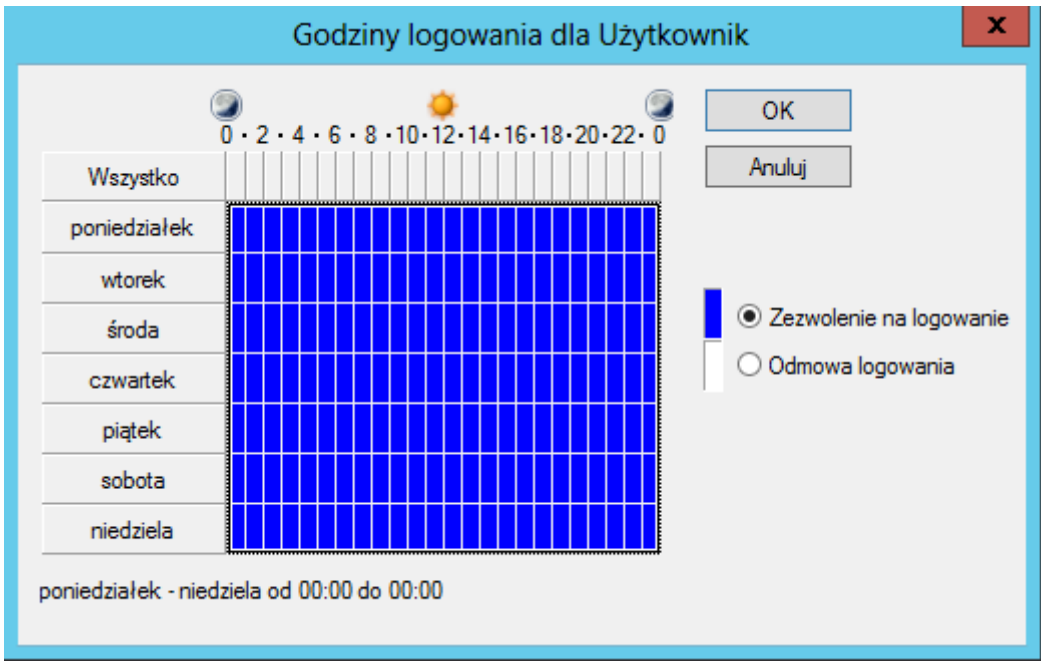
Wróćmy teraz do samych użytkowników. Wybierzmy użytkownika, którego wcześniej tworzyliśmy (poprzednie materiały).
Okno każdego użytkownika w usłudze wygląda następująco:



Poszczególne zakładki pozwalają na:
a) Ogólne – są to ogólne dane informacyjne o danym użytkowniku systemu. Stanowią one swoisty terminarz informacyjny użytkownika – telefon kontaktowy, adres e-mail, strona WWW, zajmowane stanowisko w firmie itd. Wszystkie pola, poza Nazwa wyświetlana, są opcjonalne
b) Adres – ciąg dalszy danych o użytkowniku, opcjonalne
c) Konto – informacje właściwe o użytkowniku systemu. Tutaj zapisana jest nazwa logowania, blokowanie/odblokowanie konta, dodatkowe opcje jak zmiana loginu przy zalogowaniu (każdorazowa zmiana hasła przez użytkownika będzie zerować to pole), blokada hasła (to my ustalamy użytkownikowi hasło), wygaśnięcie hasła (użytkownik będzie musiał co jakiś czas zmienić hasło), włączenie/wyłączenie konta i wiele innych. Dodatkowo można ustalić czas wygaśnięcia konta (po podanej dacie logowanie na to konto będzie niemożliwe).



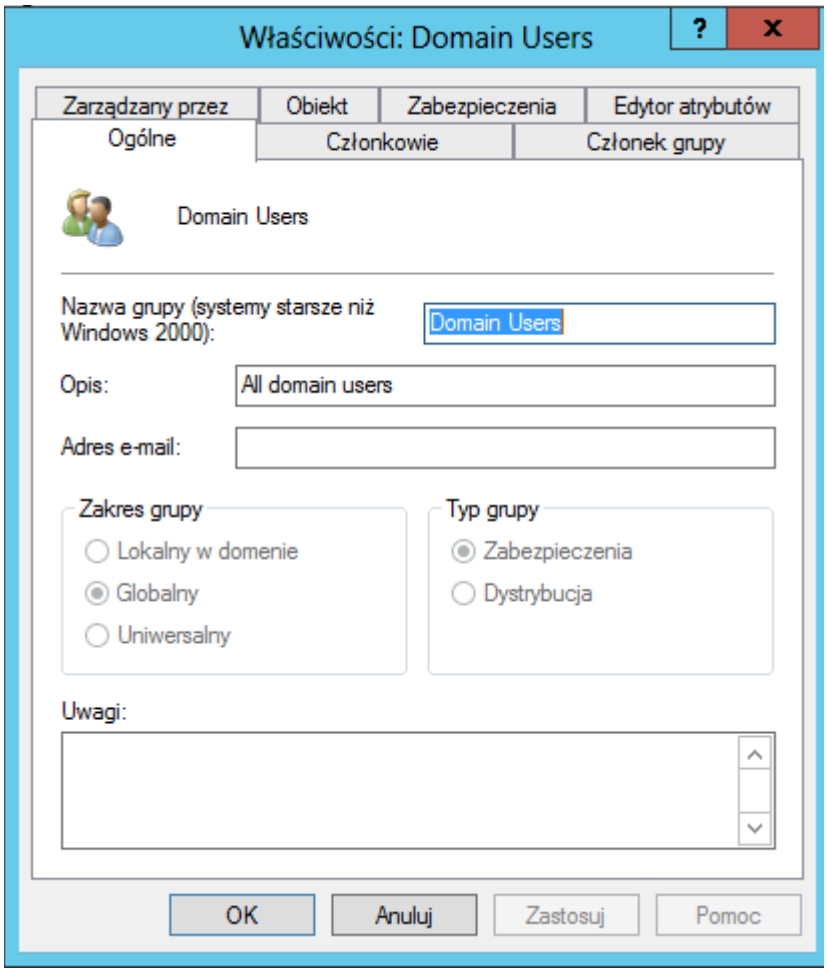
Przycisk „Godziny logowania...” pozwala na graficzne zarządzanie czasem, w którym użytkownik będzie w stanie się logować do systemu.



Przycisk „Zaloguj do...” pozwala określić, na których maszynach w sieci edytowany użytkownik będzie mógł się logować (domyślnie dowolna stacja robocza podłączona do domeny/serwer).
d) Profil – pozwala na określanie ścieżki profilu dla użytkownika (szczególnie ważne przy profilach mobilnych; określa się go wg adresacji otoczenia sieciowego, np. \\<Nazwa_serwera>\<katalog_domowy). Ponadto pozwala na wybranie pliku logowania dla użytkownika – gdy użytkownik będzie się logował to ten właśnie skrypt będzie się wykonywał (można dzięki temu np. podpiąć dodatkowe dyski sieciowe, ustawić odpowiednie uprawnienia do katalogów i wiele innych opcji).
Pole „Folder macierzysty” pozwala na podpięcie dodatkowego folderu sieciowego do użytku właściciela konta (podawany w notacji otoczenia sieciowego bądź poprzez ścieżkę bezwzględną na serwerze).
e) Telefony – pozwala wpisać więcej numerów telefonu do danego użytkownika (stacjonarne, komórkowe, IP)
f) Organizacja – pozwala na określenie dokładnej roli w firmie. Ponadto pole Menedżer pozwala na określenie, którzy z użytkowników systemu jest podwładnym edytowanego pracownika.
g) Edytor atrybutów – wyświetla wszystkie atrybuty obiektu usługi katalogowej. Niektóre z tych atrybutów można edytować (np. badPasswordTime – czas, jaki musi upłynąć pomiędzy błędnie podanym hasłem a próbą ponownego wpisywania), inne są tylko do odczytu (np. distinguishedName – jednoznaczna nazwa katalogowa obiektu wraz z lokalizacją).
h) Model COM+ - pozwala określić system interfejs łączący dany element usługi katalogowej z inną aplikacją firmy Microsoft (np. relację pomiędzy AD a bazą MS SQL Server). W podstawowej wersji żaden model COM+ nie jest dostępny.
i) Profil usług pulpitu zdalnego – pozwala na określanie uprawnień do logowania się użytkownika do pulpitów zdalnych na tym serwerze. Umożliwia zmianę profilu użytkownika jeżeli loguje się przy pomocy RDP (także folderu domowego).
j) Zdalne sterowanie – pozwala określić poziom ingerencji, jaki może mieć administrator nad połączeniami zdalnym edytowanego użytkownika. Przykładowo może tylko przyglądać się co robi wskazany użytkownik lub może ingerować w to co aktualnie robi.
k) Sesje – pozwala szczegółowo określić czas życia sesji zdalnej użytkownika, limit aktywnych sesji (wielokrotne łączenie się w ramach jednego loginu) oraz czas bezczynności, po którym nastąpi zamknięcie sesji zdalnej
l) Środowisko – pozwala na uruchamianie określonego programu użytkownikowi, który zalogował się do systemu (np. księgowemu możemy od razu uruchomić jego program do księgowości. Dodatkowo określamy z których zasobów lokalnych będzie mógł korzystać użytkownik (możemy np. wyłączyć mu dostęp do drukarek bądź do dysków w stacji roboczej).

m) Zabezpieczenia – pozwala określić uprawnienia użytkownika względem poszczególnych grup użytkowników systemu – jak domyślnie mają się zachowywać obiekty względem niego gdy przynależą do którejś z grup. Zabezpieczenia te przypisuje się tak samo jak w przypadku systemu Windows Vista/7/8/8.1
n) Obiekt – zakładka wyświetla (i pozwala zmienić) nazwę kanoniczną obiektu (użytkownika) oraz (w przypadku opcji zaawansowanych) zezwala na zabezpieczenie/odbezpieczenie przed przypadkowym usunięciem.
o) Telefonowanie – pozwala określić metody łączenia się z siecią telefoniczną (szczególnie z siecią cyfrową).
p) Replikacja hasła – pozwala określić, na których serwerach będą przechowywane konta i hasła użytkowników z bieżącego serwera (dostępne tylko w przypadku posiadania kilku serwerów w obrębie użytkowanej domeny)
r) Członek grupy – umożliwia zarządzanie członkostwem w grupach danego użytkownika. Użytkownik może być członkiem więcej niż jednej grupy (przykładowo może być członkiem grupy administratorów polityki zabezpieczeń oraz protokołu RDP lecz nie będzie miał możliwości zmian ustawień AD czy samego serwera bo nie będzie członkiem grupy Administratorzy).
s) Opublikowane certyfikaty – pozwala na przypisanie użytkownikowi dostępnych w systemie certyfikatów. Certyfikaty mogą posłużyć np. w celu weryfikacji poczty elektronicznej bądź pozwolić na autoryzowane zmiany w systemie (np. jako administrator).

Właściwości grup nie są już tak rozbudowane. Po wybraniu dowolnej grupy wyświetli się takie oto okno:

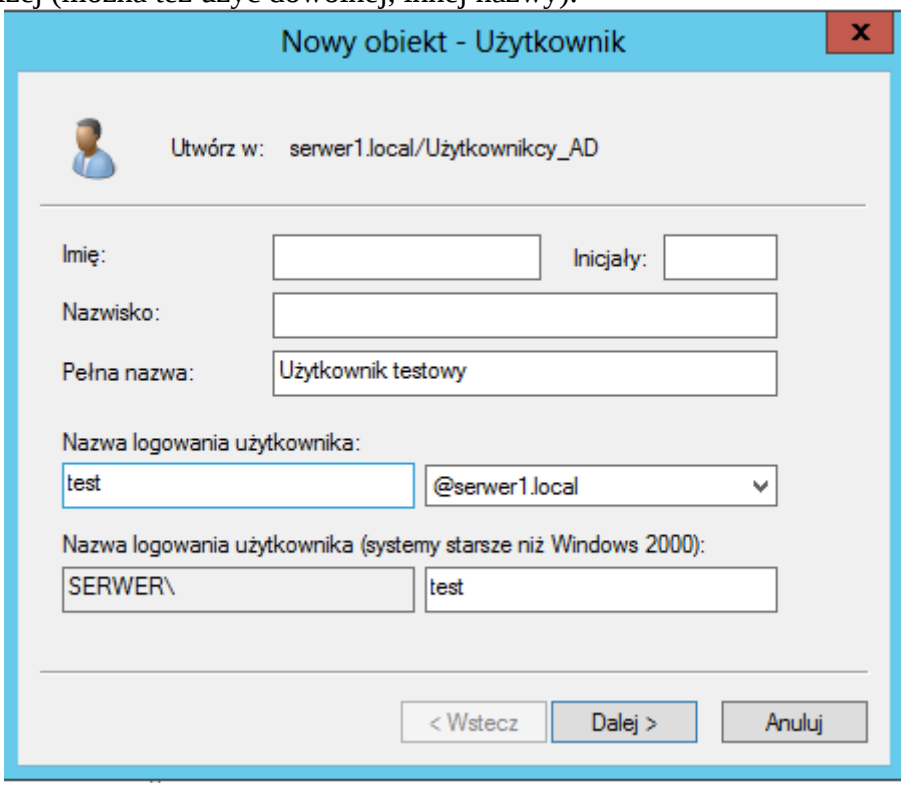


a) Ogólne – umożliwia zmianę nazwy grupy oraz jej opis. Jeżeli zostanie dodany adres e-mail będzie on automatycznie przypisany do każdego członka grupy (na niego będzie mógł wysyłać pocztę administrator, a wszyscy członkowie grupy powinni mieć do niego dostęp). Grupy

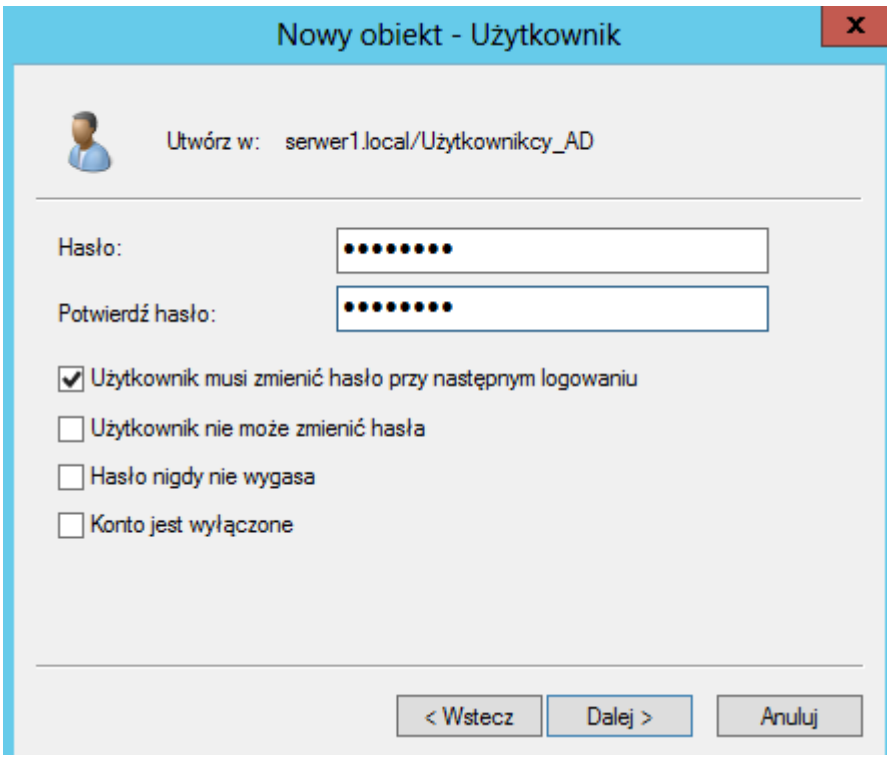
wbudowane nie pozwalają na zmiany w zakresie grupy oraz typu grupy (grupy tworzone przez administratora mają takie możliwości)
b) Członkowie – pozwala dodawać lub usuwać użytkowników przypisanych do tej grupy
c) Członek grupy – każda grupa może być członkiem jednej/kilku pozostałych grup
d) Edytor atrybutów – jak w przypadku konta użytkownika
e) Zabezpieczenia – jak w przypadku konta użytkownika
f) Obiekt – jak w przypadku konta użytkownika
g) Zarządzany przez – można wybrać tzw. moderatora grupy. Będzie on sprawował nad nią pieczę. Dodatkowo można takiej osobie zezwolić na modyfikację członkostwa tejże grupy

1. Tworzenie konta użytkownika w domenie Active Directory
Celem ćwiczenia będzie utworzenie konta użytkownika, który będzie mógł logować się w określone dni. Dodatkowo podczas startu systemu wykona się skrypt podłączający do jego konta zmapowany dysk do wymiany danych (dostępny poprzez Eksplorator Windows). W tym celu utworzymy nowe konto z loginem test.

W pierwszej kolejności stwórzmy jednostkę organizacyjną, do której będą dołączane tworzone przez nas konta i grupy (przykładowa nazwa – Użytkownicy_AD). Następnie, będąc w utworzonej jednostce, utwórzmy nowego użytkownika. Pojawi się okno, które można wypełnić jak na zrzucie poniżej (można też użyć dowolnej, innej nazwy).



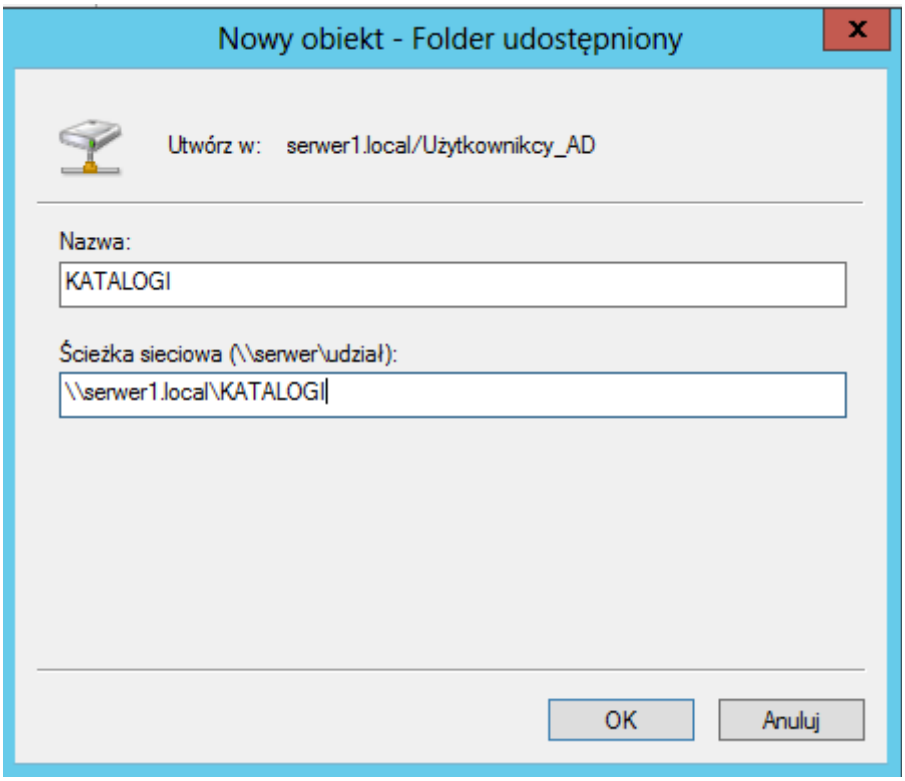
W następnym kroku musimy podać hasło. Domyślna polityka zabezpieczeń nakazuje podanie hasła z minimum 8 znakami,w którym znajdzie się co najmniej jedna mała litera, jedna duża, jedna cyfra oraz jeden znak specjalny. Dodatkowo ustalmy, że użytkownik musi zmienić hasło przy pierwszym logowaniu. Przykład hasła: Qwerty1@



Na koniec potwierdzamy (klikamy przycisk Zakończ – ostatni, trzeci etap).
Teraz ustalmy, że użytkownik nie może logować się w określonym dniu tygodnia oraz godzinach tak, by przy próbie zalogowania na to konto otrzymać stosowany komunikat. Proszę pamiętać, że w oknie wyboru dni i godzin logowania można zaznaczać kilka godzin/kilka dni poprzez zaznaczanie myszą określonego obszaru (zmiana grupowa).

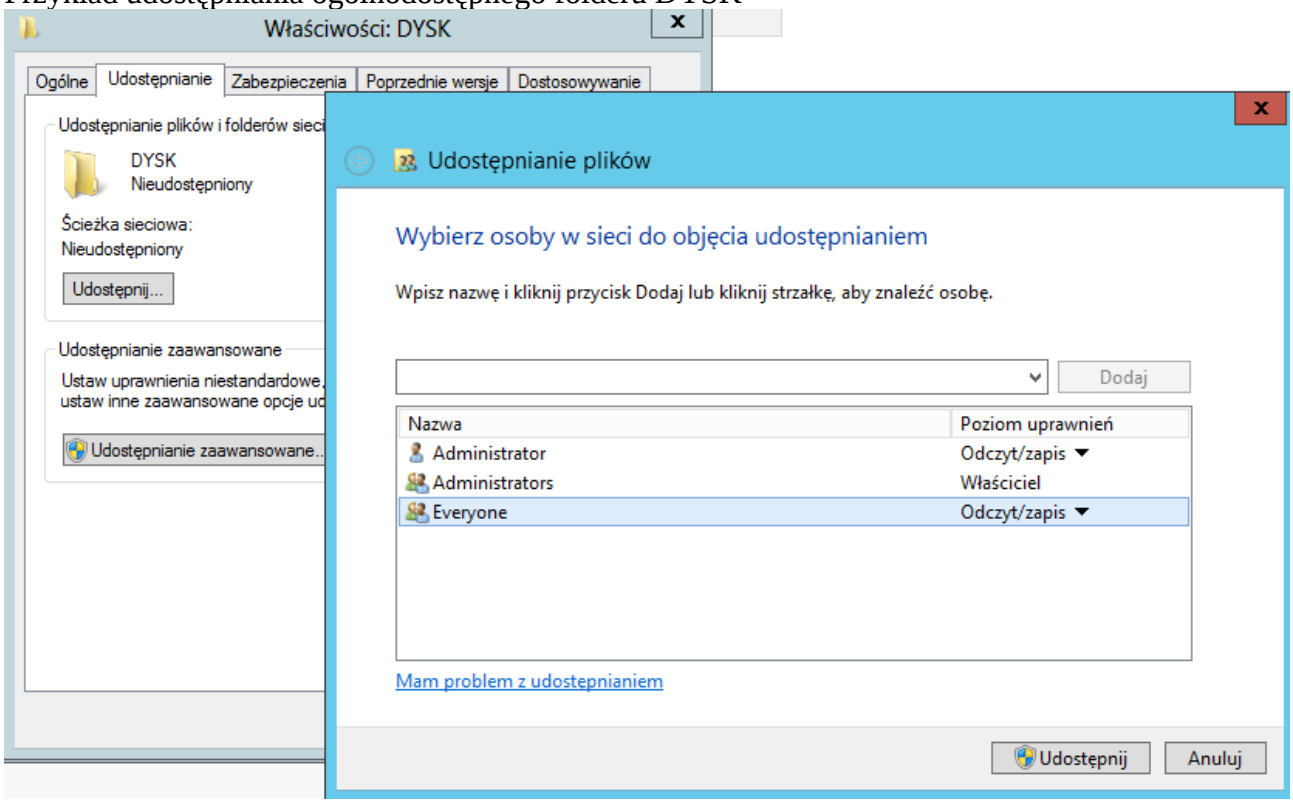
Teraz czas na dodanie zasobów sieciowych dostępnych w ramach AD. Na dysku C proszę utworzyć dwa katalogi: DYSK oraz KATALOGI. Pierwszy z nich będzie służył jako globalna wymiana danych pomiędzy użytkownikami (każdy będzie miał do niego dostęp). Drugi z katalogów będzie zawierał podkatalogi. W zależności od użytkownika będzie on podłączany lecz tylko administrator będzie mógł edytować jego zawartość. Natomiast wybrany użytkownik będzie mógł jedynie przeglądać jego zawartość (bez możliwości modyfikacji jego zawartości).

Gdy dyski zostaną już utworzone należy udostępnić je oraz dodać w odpowiednie miejsce w strukturze AD (najlepiej w jednostce organizacyjnej z kontami użytkowników).
Przykład dodania zaosbu do AD:



Proszę zauważyć, że w ścieżce sieciowej podana została nazwa domenowa serwera. Można też podać adres IP (najpewniejsza metoda) jednak w przypadku jego zmiany każdy zasób trzeba będzie ręcznie edytować i zmieniać go. W tym przypadku nie trzeba niczego zmieniać!

Przykład udostępniania ogólnodostępnego folderu DYSK



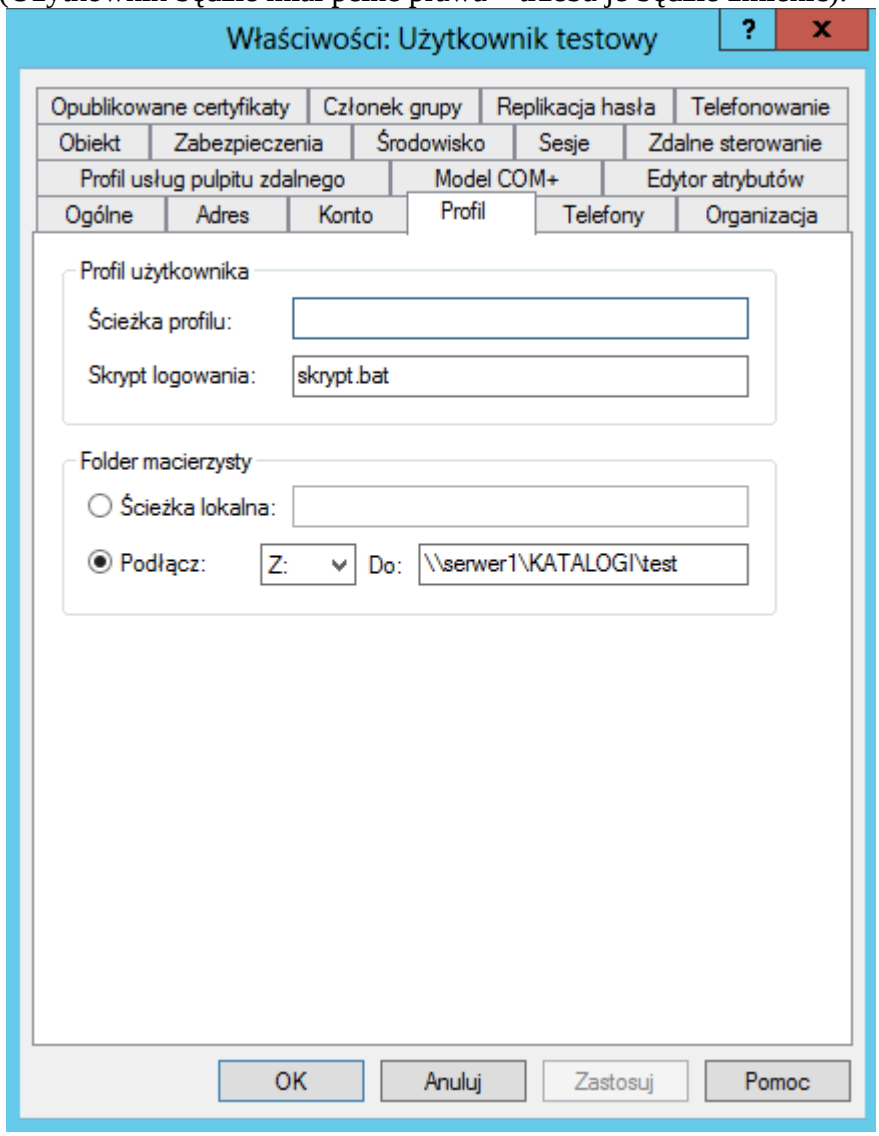
Przykład udostępniania ogólnodostępnego folderu KATALOGI (wszyscy mają mieć prawo tylko do odczytu!):

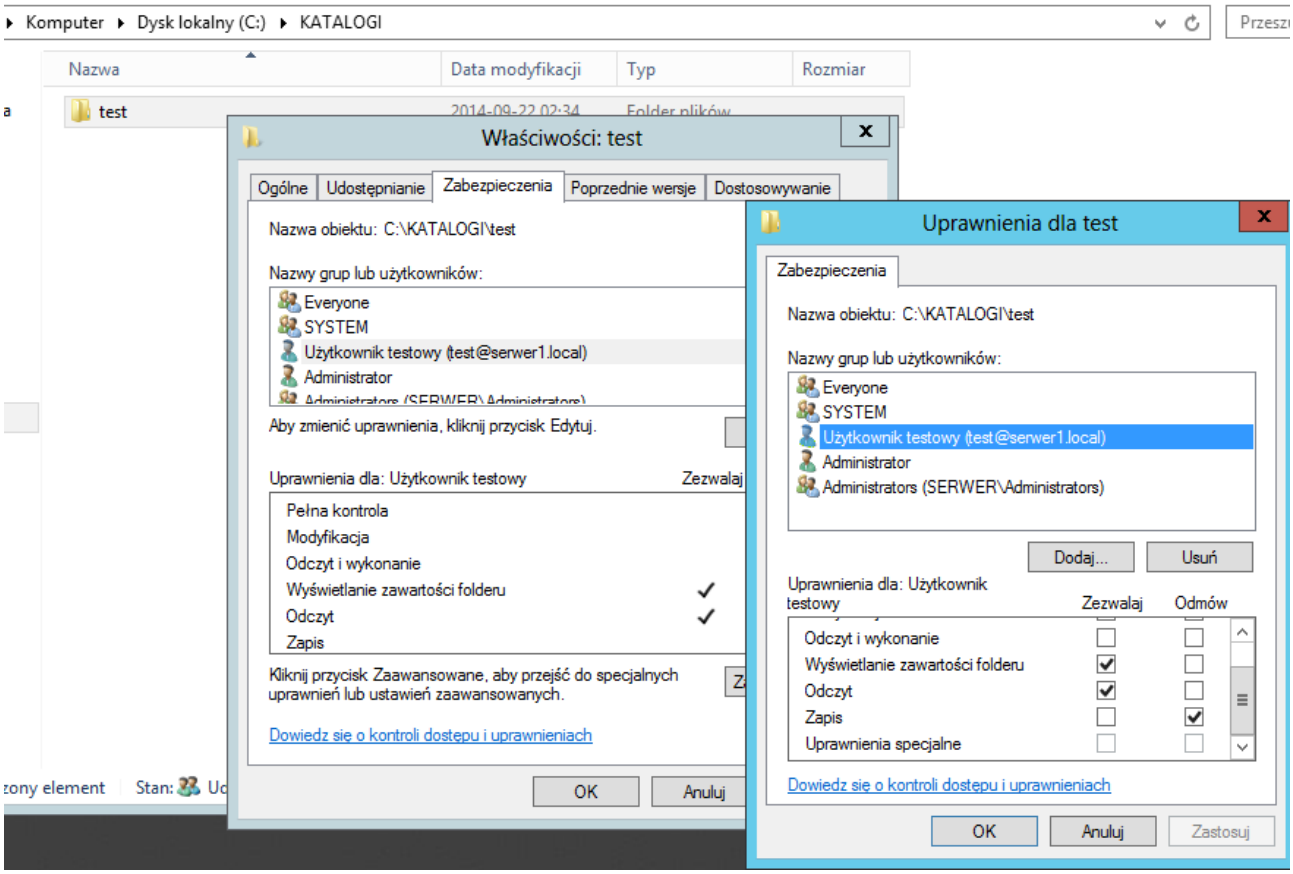
Kolejnym zadaniem jest dodanie skryptu wykonującego się przy logowaniu użytkownika. Posłużymy się tutaj starymi plikami bat (chociaż Windows 2012 pozwala także na użytkownie skryptów PowerShell).

Tworzymy na serwerze nowy plik tekstowy, w którym wpisujemy następującą frazę:

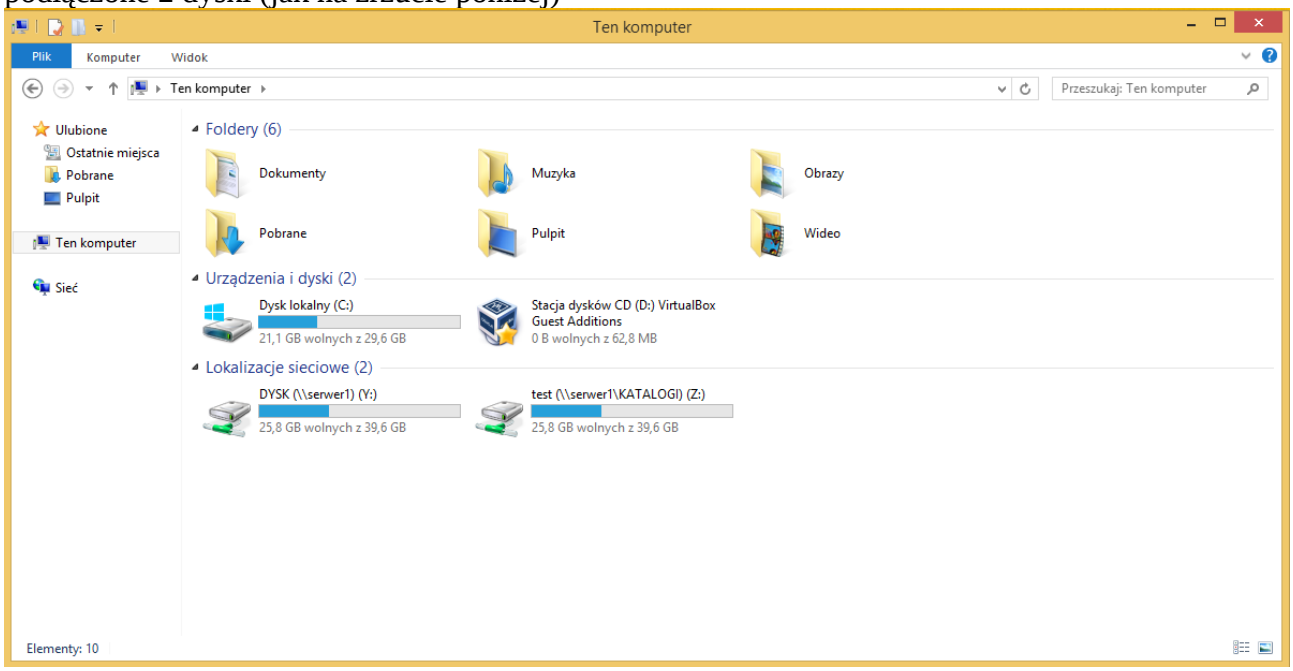
net use Y: \\serwer1\DYSK

Plik zapisujemy pod nazwą skrypt.bat w katalogu C:\Windows\SYSVOL\sysvol\swerwer1.local\scripts (jeżeli lokalizacja katalogu przy tworzeniu AD została zmieniona to trzeba właśnie ją podać!).
Teraz trzeba podać, że chcemy podany skrypt uruchamiać przy logowaniu się użytkownika. W tym celu podajemy go w zakładce Profil->Skrypt logowania (wystarczy wpisać jego nazwę)
Dodatkowo wskażmy domenie, że chcemy dołączyć sieciowy dysk pod litera Z:, który kryje się pod ścieżką \\serwer1\KATALOGI\test
Proszę zauważyć, że katalog test sam doda się do folderu KATALOGI z odpowiednimi uprawnieniami (Użytkownik będzie miał pełne prawa – trzeba je będzie zmienić).





Po zalogowaniu (proszę pamiętać o zdjęciu zakazu logowania!) użytkownik test powinien mieć podłączone 2 dyski (jak na zrzucie poniżej)



Na dysku DYSK powinien mieć pełna prawa zapisu/odczytu, w katalogu test powinien móc przeglądać zawartość lecz nie powinien mieć pozwolenia na tworzenie folderów i plików.

WAŻNE! Bez zainstalowanej roli Active Directory system Windows 2012 Server niczym nie różni się od systemu „klienckiego”, jakim jest Windows 7, 8 czy 8.1. Tak jak w tych systemach, tak i w edycji serwerowej do zarządzania kontami użytkownika służy Panel sterowania (narzędzie lusrmgr lub Zarządzanie komputerem->Użytkownicy i grupy lokalne). Stale istnieje również dodawania użytkowników poprzez polecenie net user lub poprzez odpowiednie funkcje PowerShell:

a) Przykład polecenia powłoki cmd

NET USER test „Qwerty1@” /ADD

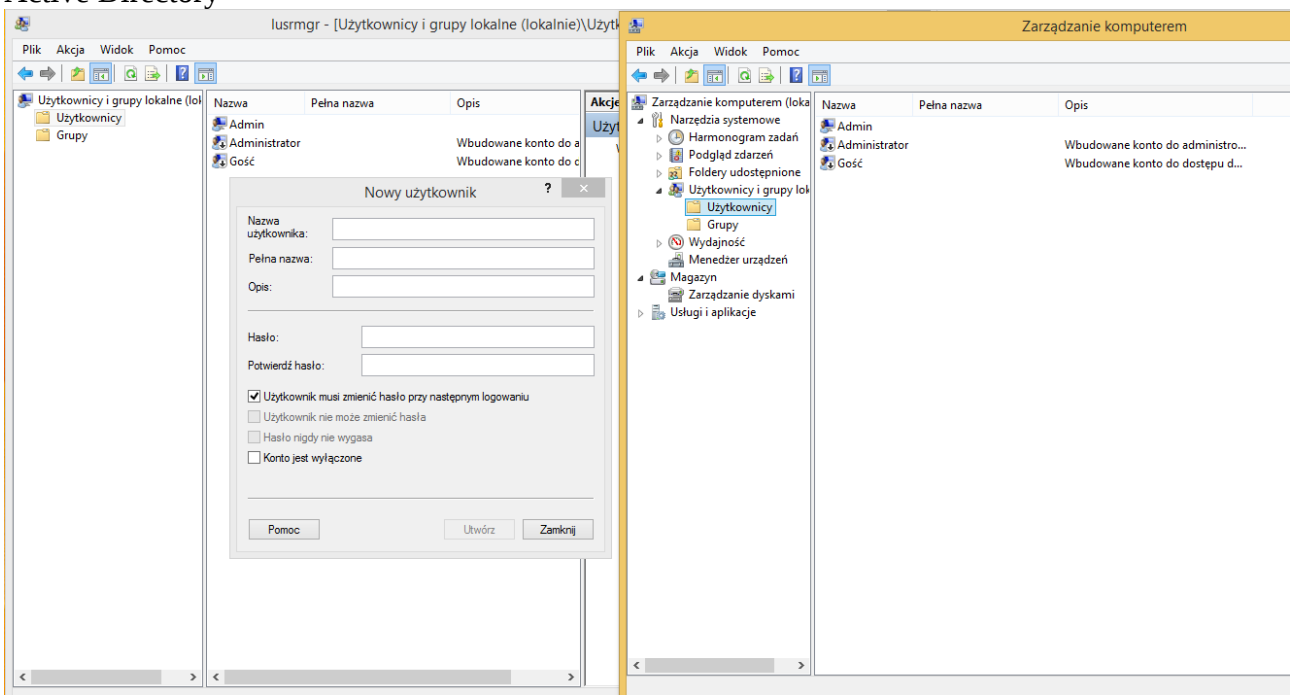
NET LOCALGROUP „gupa” „test” /ADD

b) Przykład polecenia PowerShell

Install-User -Username "test" -Description "Użytkownik testowy" -FullName "Użytkownik testowy" -Password "Qwerty1@" Add-GroupMember -Name 'Domain Users' -Member 'test'

Proszę pamiętać, że w konsoli PowerShell nadal działają polecenia powłoki cmd!

Narzędzie do zarządzania użytkownikami i grupami w Windows 8.1/Windows 2012 Server bez roli Active Directory



Polecenia do wykonania:
1. Proszę utworzyć kolejne konto użytkownika.
2. Proszę utworzyć grupę o nazwie 'lokalna' .
3. Proszę dodać nowy udostępniony folder o nazwie 'LOKLANY'.
4. Proszę udostępnić go jedynie dla grupy 'lokalna' (pełne prawa odczyt/zapis).
5. Proszę dodać do tej grupy dwóch z trzech utworzonych użytkowników.
6. Proszę logować się na odpowiednich użytkowników i sprawdzać możliwości modyfikacji folderu.