pasja-informatyki.pl

Sieci komputerowe – Windows Server #2

Active Directory – konta, grupy, profile mobilne

Damian Stelmach

Spis treści

Active Directory to Microsoft'owa implementacja protokołu sieciowego warstwy aplikacji **LDAP** (ang. Lightweight Directory Access Protocol). Protokół LDAP stosowany jest w tak zwanych **usługach katalogowych**. Usługa katalogowa to nic innego jak **obszerna**, **hierarchiczna baz danych**, zawierająca informacje o **użytkownikach**, **grupach użytkowników**, **komputerach**, a także **zasobach sieciowych**, działających w sieciach firmowych, gdzie pracują serwery Microsoft'owe. To nic innego jak zbiór informacji o użytkownikach sieci, ich uprawnieniach do różnego rodzaju zasobów, komputerach, na jakich pracują, konfiguracji tych komputerów i tak dalej. Active Directory pozwala administratorom sieci, centralnie, z poziomu jednego komputera (odpowiednio skonfigurowanego serwera) zarządzać całym zbiorem użytkowników w sieci, określać ich uprawnienia do zasobów sieciowych, a także konfigurować komputery, na których pracują. To potężne narzędzie zdecydowania ułatwia pracę administratora w sieciach, gdzie pracują dziesiątki użytkowników i komputerów. Na całość usług związanych z Active Directory składa się aż **pięć elementów**:

1. AD **Domain Services.**
2. AD **Certificate Services.**
3. AD **Lightweight Directory Services.**
4. AD **Rights Management Services.**
5. AD **Federation Services.**

W ramach kursu zajmować się będziemy **Usługami Domenowymi Active Directory** (ang. Active Directory Domain Services).

<u>Pojęcia związane z Active Directory:</u>

- **Magazyn danych -** plik, przechowywany na dysku serwera, zawierający informacje o obiektach usługi katalogowej. Obiektem usługi katalogowej może być użytkownik, grupa, jednostka organizacyjna czy też komputer. Plik nosi nazwę NTDS.dit.
- **Kontroler domeny -** serwer, na którym zainstalowano **Active Directory**, przechowujący kopię magazyny danych. Wyróżnić możemy kontrolery typu **Global Catalog** (katalog globalny), a także kontrolery tylko do odczytu - **Read-Only Domain Controler** oraz odczytu i zapisu – **Writeable Domain Controler**.
- **Domena** – obszar sieci, któremu przydzielono określone możliwości oraz zasoby. W niej skupione są **obiekty Active Directory**, takie jak użytkownicy, grupy, jednostki organizacyjne oraz komputery działające w jej obrębie. Aby można było domenę utworzyć, wymagany jest przynajmniej **jeden kontroler**.

- **Las -** zbiór jednej lub też wielu domen. Pierwsza domena, która zostanie utworzona w lesie, będzie tak zwaną domeną główną lasu, a cały las przyjmie nazwę taką jak domena główna. Jeśli przykładowo tworzymy nową domenę w nowym lesie i nazwiemy ją ***test.local*** to **cały las przyjmie taką nazwę**.
- **Drzewo -** jedna domena, albo kilka domen pracujących pod tą samą **przestrzenią nazw DNS**.
- **Jednostka organizacyjna** – to obiekt usługi AD, pozwalający na przechowywanie użytkowników, grup użytkowników oraz komputery. Jednostkom organizacyjnym można przypisywać poszczególne **zasady grupy** oraz **delegować uprawnienia administracyjne**.

szkola.local pracownia1.szkola.local

Wymagania systemów klienckich korzystających z Active Directory:

Każdy komputer kliencki, z zainstalowanym systemem Windows (7, 8.1 oraz 10) może pracować w domenie pod dwoma warunkami:

- musi być w wersji przynajmniej **Professional** (może być w wersji **Ultimate** lub **Enterprise**), żadnej z wersji **Home** do domeny **nie podłączymy**,
- oprócz licencji na sam system, do każdego klienta należy dokupić **dodatkową licencję** pozwalającą na korzystanie z zasobów serwera. Licencja to nosi nazwę **CAL (ang. Client Access License)**. Więcej na temat licencji CAL przeczytacie na tej stronie: https://www.microsoft.com/pl-pl/Licensing/product-licensing/client-access-license.aspx

Implementacja usług katalogowych Active Directory na serwerach polega na zainstalowaniu odpowiedniej usługi. Usługa nazywa się **Usługi Domenowe Active Directory** *(Active Directory Domain Services)*. Jeśli to pierwsza nasza domena w lesie, to oprócz instalacji samej usługi, musimy jeszcze promować nasz serwer do roli kontrolera domeny. Cały proces instalacji został przeze mnie przedstawiony na zamieszczonym wideo:

- Implementacja na Windows Server 2008R2:
  https://www.youtube.com/watch?v=I1uuOiuM8v0&feature=youtu.be&t=4m17s
- Implementacja na Windows Server 2012R2:
  https://www.youtube.com/watch?v=I1uuOiuM8v0&feature=youtu.be&t=10m15s

Po instalacji i wstępnej konfiguracji usługi należy przyłączyć komputery klienckie do domeny, proces dla poszczególnych systemów również został przedstawiony na wideo:

- Dodawanie klienta do domeny z Windows 7:
  https://www.youtube.com/watch?v=I1uuOiuM8v0&feature=youtu.be&t=15m22s
- Dodawanie klienta do domeny z Windows 10
  https://www.youtube.com/watch?v=I1uuOiuM8v0&feature=youtu.be&t=16m12s

Od momentu implementacji usługi Active Directory oraz domeny, zarządzanie użytkownikami i grupami odbywa się poprzez przystawkę **Użytkownicy i komputery usługi Active Directory** (*Active Directory Users and Computers*) . To właśnie tutaj skupione są obiekty naszej domeny i tutaj będziemy nimi zarządzać.

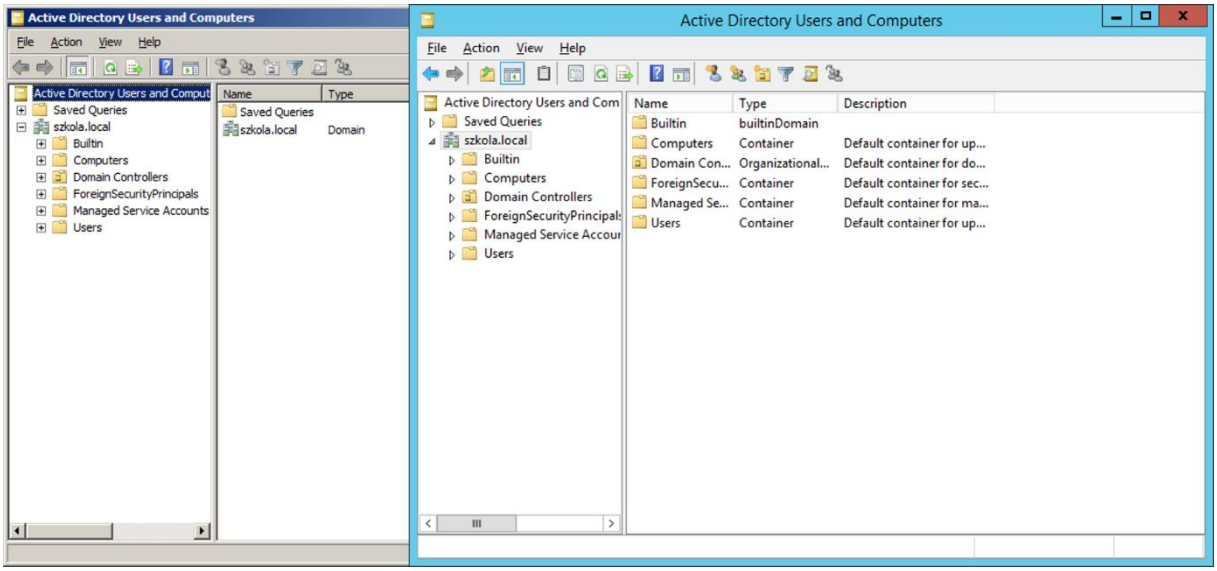
W systemie Windows Server 2008 R2 dostaniemy się do tej przystawki wybierając:

START -> ***Narzędzia Administracyjne*** (*Administrative Tools*) -> ***Użytkownicy i komputery usługi Active Directory***

W systemie Windows Server 2012 R2 dostaniemy się natomiast wybierając:

MENADŻER SERWERA -> ***Narzędzia*** (*Tools*) -> ***Użytkownicy i komputery usługi Active Directory***

Znajdują się tam obiekty domyślne, tworzone podczas instalacji samej usługi:



Wbudowane grupy zabezpieczeń (to te pełniące określone funkcje w systemie) przechowane są w kontenerze **Wbudowane** (*Builtin*). **Komputery**, które pracują w domenie, domyślnie przechowywane są w kontenerze **Komputery** (C*omputers*). Natomiast **użytkownicy** oraz **pozostałe typy grup** w systemie znajdują się w kontenerze **Użytkownicy** (U*sers*).

Na obu wersjach systemu implementacja jednostek organizacyjnych, użytkowników i grup jest dokładnie taka sama

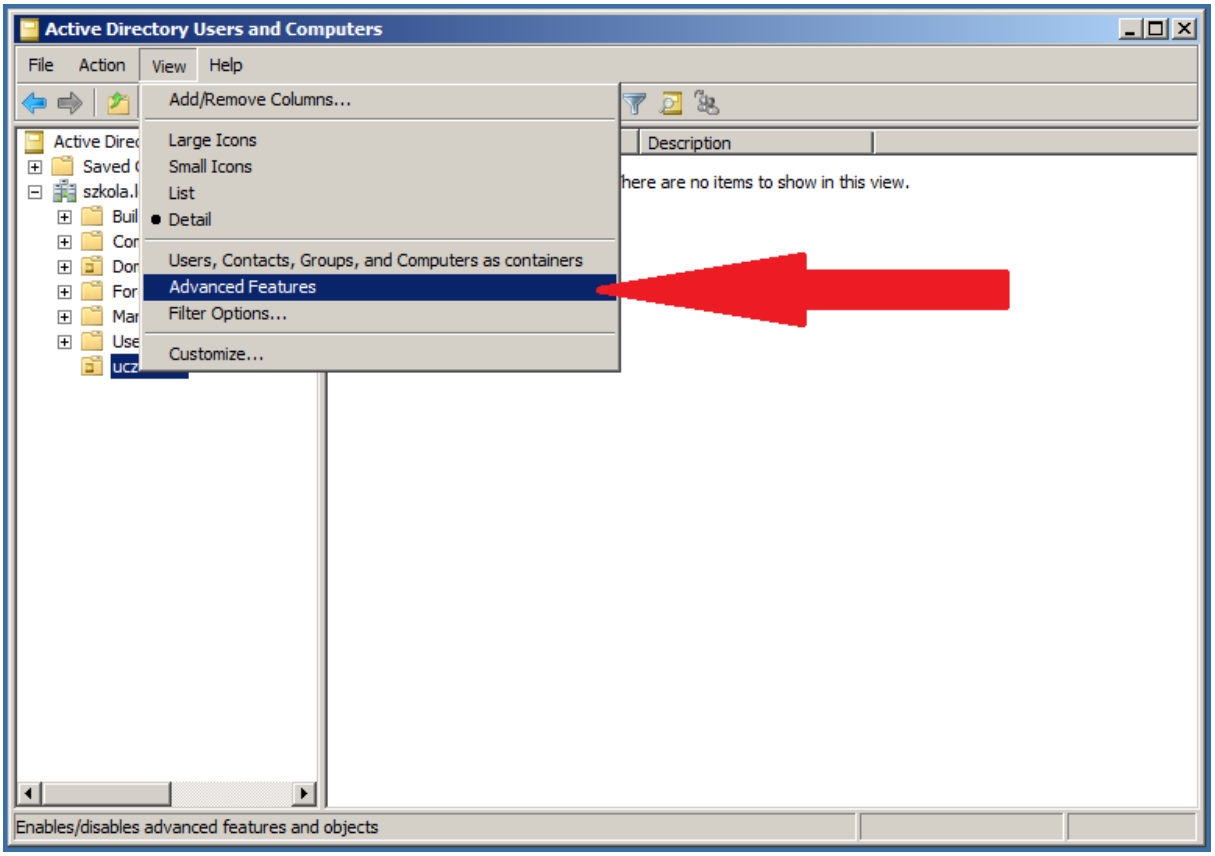
W naszej domenie podział będzie następujący: **użytkownicy, którzy w systemie pełnią rolę administratorów**, przechowywani będą w kontenerze **Użytkownicy**. Z kolei dla **użytkowników domenowych**, czyli wszystkich pozostałych użytkowników w domenie utworzymy sobie specjalne kontenery zwane **jednostkami organizacyjnymi**. Ilość jednostek organizacyjnych zależy od struktury organizacyjnej w danej firmie, przedsiębiorstwie czy szkole. Jednostki implementuje się w taki sposób, aby odzwierciedlały rzeczywistą sytuację.

Utworzenie jednostek organizacyjnych:

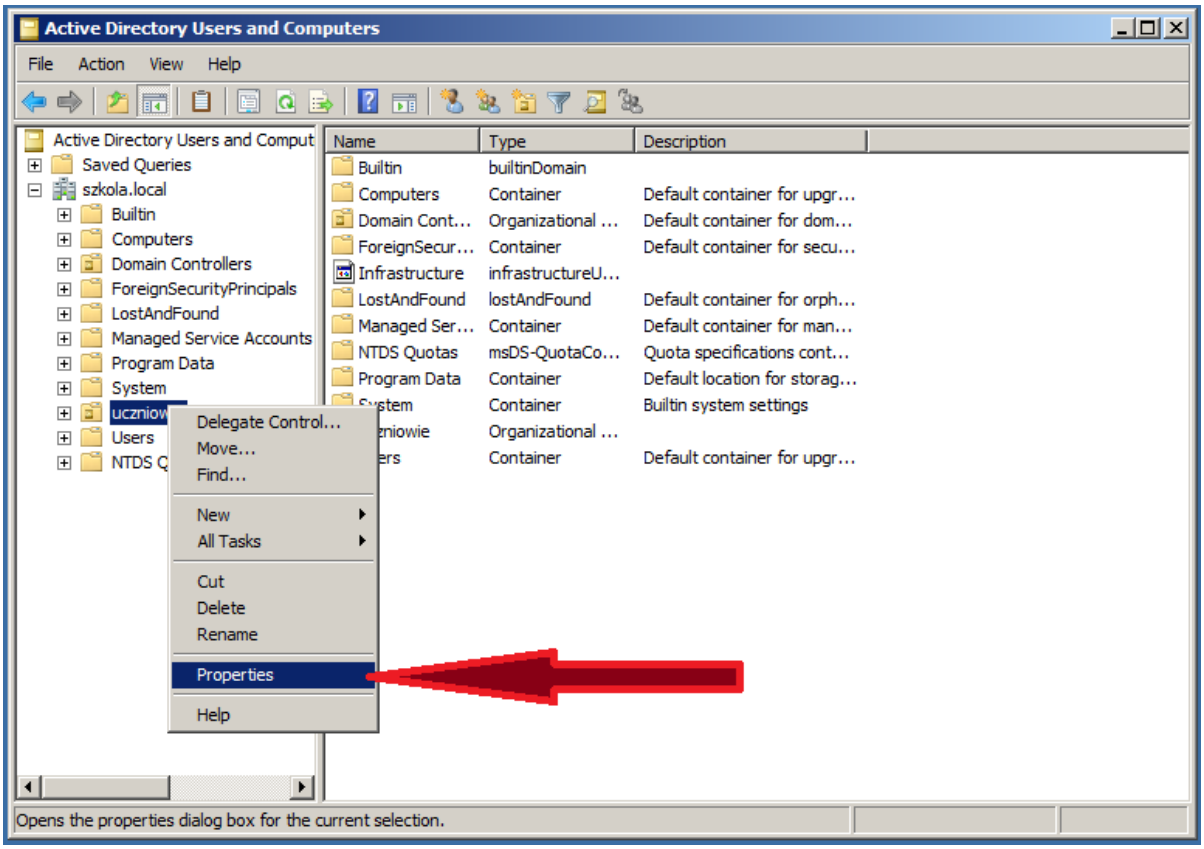
PPM klikamy w nazwę domeny -> Nowy *(New)* ***-> Jednostka Organizacyjna*** *(Organization unit)* ***-> nazwa jednostki -> OK***

Domyślnie, ustawiona jest opcja zabezpieczająca przed przypadkowym usunięciem jednostki. Jeśli podczas tworzenia jednostki opcje zostawiliście aktywną, a z jakichś powodów chcielibyście usunąć daną jednostkę, można to zrobić tak:

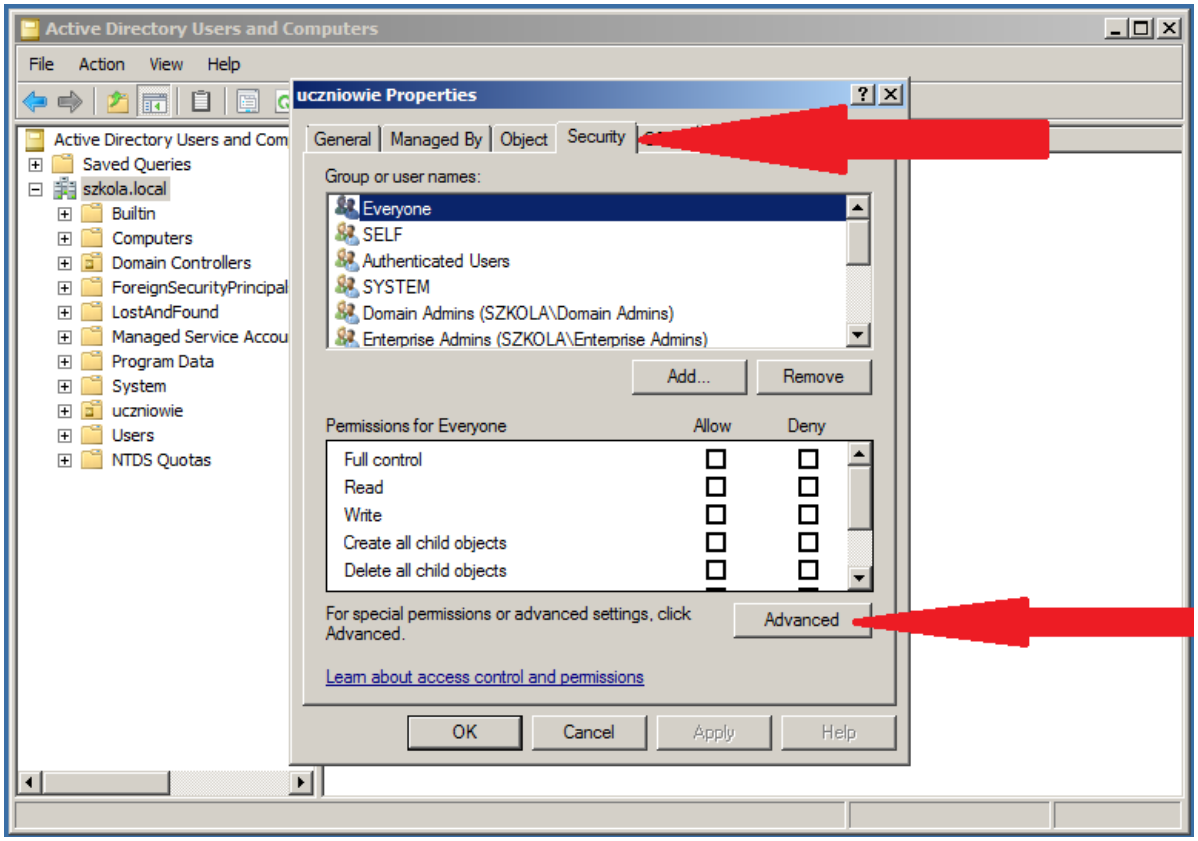
Widok *(View)* ***-> Funkcje zaawansowane*** *(Advanced Features)*



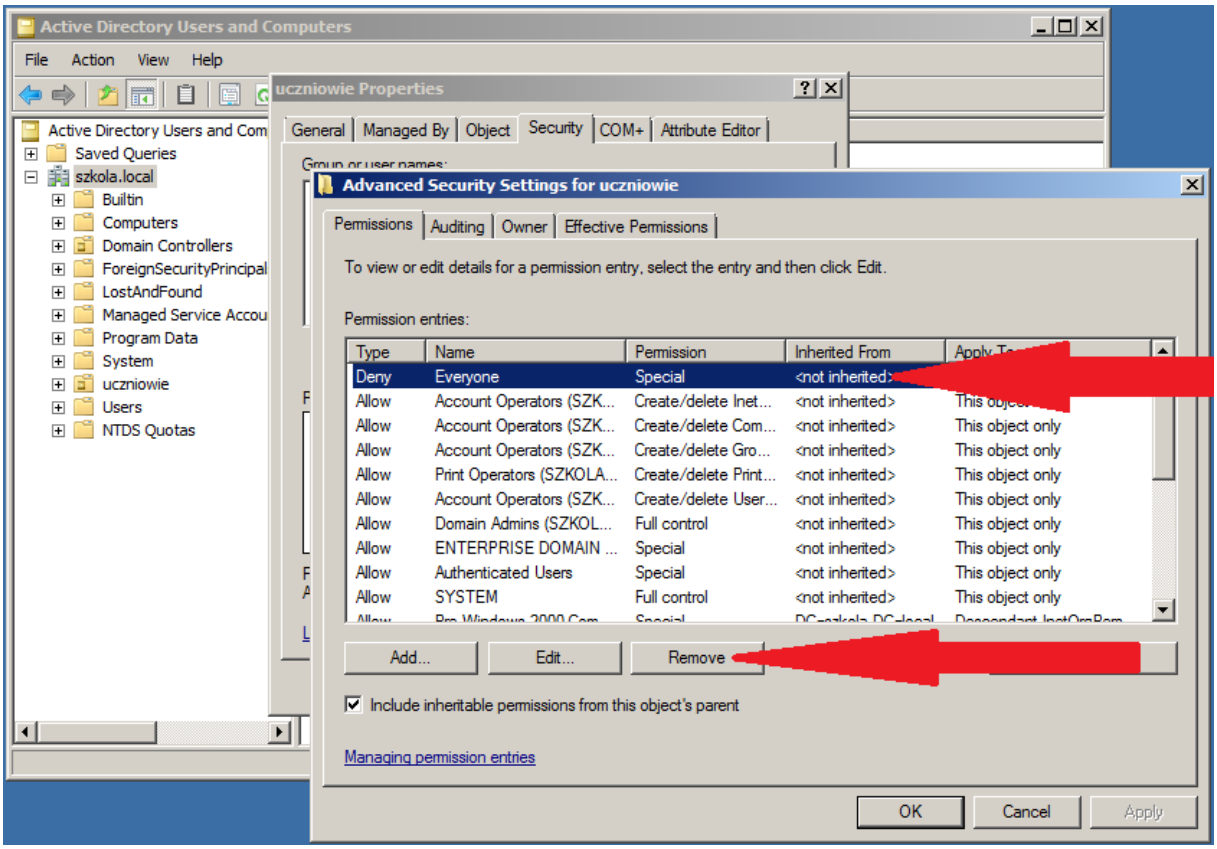
Klikamy PPM w jednostkę, którą chcemy usunąć -> Właściwości *(Properties)*



Zakładka Zabezpieczenia *(Security)* ***-> Zaawansowane*** *(Advenced)*



Zaznaczamy Wszyscy *(Everyone)* ***-> Usuń*** *(Remove)*



Teraz można już usunąć daną jednostkę klikając ***PPM -> Usuń***. Czynność tą wykonujemy **dla wszystkich jednostek**, które chcemy usunąć.

W nowo utworoznej jednostce organizazcyjnej możliwe jest tworzenie **grup użytkowników**, samych **uzytkowników**, a także obiektów komputerów.

Tworzenie grup:

PPM w nazwę jednostki organizacyjnej (lub też w samej jednostce) -> Nowy *(New)* ***-> Grupa*** *(Group)* ***-> nazwa grupy -> określamy zakres*** *(scope)* ***oraz typ*** *(type)* ***grupy -> OK.***

W systemach Windows Server mamy dostępne 3 zakresy grup:

- **Lokalne w domenie** (ang. Domain local) – grupy, do których można dodać użytkowników z każdej domeny w lesie. Stosowane są do nadawania uprawnień do katalogów.
- **Globalne** (ang. Global) – grupy, do których można dodać użytkowników z tylko jednej domeny w lesie. Stosowane są do nadawania uprawnień do katalogów, a także do definiowania ról w systemie.
- **Uniwersalne** (ang. Universal) – grupy, do których można dodać użytkowników z każdej domeny w lesie. Stosowane są do nadawania uprawnień do katalogów, a także do definiowania ról w systemie.

A także 2 typy grup:

- **Zabezpieczeń** (ang. Security) – grupy pozwalające na nadawanie uprawnień do zasobów.
- **Dystrybucyjne** (ang. Distribution) – grupy stosowane do tworzenia list dystrybucyjnych poczty elektronicznej.

Tworzenie użytkowników:

PPM w nazwę jednostki organizacyjnej (lub też w samej jednostce) -> Nowy *(new)* ***-> Użytkownik*** *(User)* ***-> Wprowadzamy imię, nazwisko, login -> Wprowadzamy hasło (dwukrotnie) -> OK.***

Domyślnie hasło, które nadawane jest dla użytkownika **musi** zawierać co najmniej 7 znaków i spełniać wymagania co do złożoności (mała, wielka litera, cyfra, znak specjalny). Pozostawienie tej opcji bez zmian jest bezpiecznym rozwiązaniem ponieważ niweluje ryzyko stosowania łatwych do odgadnięcia haseł przez użytkowników. Jeśli natomiast ktoś chciałby to zmienić może to zrobić postępując, tak jak w tym fragmencie wideo:

https://www.youtube.com/watch?v=I1uuOiuM8v0&feature=youtu.be&t=22m51s

Dodawanie użytkowników do grupy:

PPM w nazwę użytkownika -> Dodaj do grupy *(Add to group)* ***-> wprowadzamy nazwę grupy -> OK***

Zadanie do samodzielnego rozwiązania | 2017

1. Utwórz nowy **las** oraz **domenę** o nazwie ***firma.com***
2. Ustaw długość haseł dla użytkowników w domenie na min. **4 znaki** oraz **wyłącz złożoność** tych haseł.
3. Podłącz do domeny **2 komputery klienckie** i nadaj im odpowiednio nazwy: **STACJA1** oraz **STACJA2**.
4. Utwórz i skonfiguruj konta użytkowników pracujących w domenie wg podanych założeń:
   4.1. Utwórz **jednostkę organizacyjną** o nazwie ***workers***, a w niej:
      4.1.1. Utwórz konto ***Maria Skłodowska*** z loginem ***ksiegowy*** oraz hasłem ***B456***
      4.1.2. Utwórz konto ***Zofia Antonina*** z loginem ***kadrowy*** oraz hasłem ***C789***
   4.2. Konta ***księgowy*** oraz ***kadrowy*** skonfiguruj tak, aby możliwe było logowanie **od poniedziałku do piątku** w godzinach **od 8:00 do 16:00**, tylko na komputerze **STACJA1.**
   4.3. Utwórz **jednostkę organizacyjną** o nazwie ***owners***, a w niej:
      4.3.1. Utwórz konto ***Adam Słodowy*** z loginem ***wlasciciel*** oraz hasłem ***A123***
5. Na serwerze w katalogu głównym dysku C, załóż folder **dane**, udostępnij go w sieci pod nazwą **dane** i zabezpiecz wg założeń:
   5.1. konta ***wlasiciel*** oraz ***księgowy*** mają mieć pełne prawa dostępu,
   5.2. konto ***kadrowy*** ma mieć prawo tylko do odczytu.
6. Na serwerze w katalogu głównym **dysku C** załóż folder **profil**, udostępnij go w sieci pod nazwą **profil** i zabezpiecz wg założeń:
   6.1. konto ***wlasiciel*** ma prawa do **odczytu i zapisu**.
7. Dla użytkownika ***kadrowy***, ustaw **automatyczne mapowanie udostępnionego folderu pod literę X**.
8. Dla użytkownika ***wlasciciel*** skonfiguruj **profil mobilny**.