T: Uwierzytelnianie użytkowników i komputerów.

Konta użytkowników i konta komputerów usługi Active Directory odpowiadają jednostkom fizycznym, takim jak komputer lub osoba. Konta użytkowników mogą również służyć jako specjalne konta usług dla niektórych aplikacji.

Konta użytkowników i konta komputerów (a także ich grupy) są również nazywane podmiotami zabezpieczeń. Podmioty zabezpieczeń to obiekty katalogu, którym są automatycznie przypisywane identyfikatory zabezpieczeń (SID) umożliwiające uzyskanie dostępu do zasobów domeny. Funkcje konta użytkownika lub komputera:

- Uwierzytelnianie tożsamości użytkownika lub komputera.
  Konto użytkownika umożliwia mu logowanie się do komputerów i domen przy użyciu tożsamości, która może być uwierzytelniona przez domenę. Każdy użytkownik logujący się do sieci powinien mieć własne, unikatowe konto użytkownika i hasło. Aby zapewnić maksymalne zabezpieczenia, należy unikać sytuacji, w których wielu użytkowników wspólnie korzysta z jednego konta.
- Udzielanie lub odmawianie dostępu do zasobów domeny.
  Użytkownik uwierzytelniony otrzymuje zezwolenie na dostęp do zasobów domeny lub odmowę dostępu (na podstawie jawnych uprawnień do zasobów przypisanych temu użytkownikowi).
- Administrowanie innymi podmiotami zabezpieczeń.
  Usługa Active Directory tworzy w domenie wewnętrznej obiekty typu obcy podmiot zabezpieczeń reprezentujące każdy podmiot zabezpieczeń z zaufanej domeny zewnętrznej.
- Inspekcja czynności wykonywanych przy użyciu konta użytkownika lub komputera.
  Inspekcja może ułatwiać monitorowanie zabezpieczeń kont.

Każdy komputer z systemem Windows NT, Windows 2000 lub Windows XP, albo serwer z systemem Windows Server 2003, który zostaje dołączony do domeny, otrzymuje własne konto komputera. Podobnie jak konta użytkowników, konta komputerów umożliwiają uwierzytelnianie oraz inspekcję dostępu komputera do sieci i zasobów domeny. Każde konto komputera musi być unikatowe.

Źródło: http://infojama.pl/181,artykul.aspx

Jednym z głównych zadań administratora jest zarządzanie kontami użytkowników i grup. Konta użytkowników pozwalają na logowanie się indywidualnych użytkowników do zasobów sieciowych. Natomiast konta grup tworzone są do zarządzania wieloma użytkownikami jednocześnie. Uprawnienia nadawane użytkownikom, są jednym z kluczowych elementów zabezpieczeń systemu. Powinny być możliwie najniższe, potrzebne do wykonywania ich pracy. Nie można np. dawać uprawnień wszystkim użytkownikom do serwera finansowego firmy.
Dwa główne składniki modelu zabezpieczeń w Windows Serwer 2003 to **uwierzytelnianie użytkowników** oraz **kontrola dostępu**. Uwierzytelnianie obejmuje dwie fazy: interaktywne logowanie oraz uwierzytelnianie sieciowe. Gdy użytkownik się loguje na lokalnym komputerze, uwierzytelnia go proces interaktywnego logowania, sprawdzając tożsamość i nadając mu dostęp do usługi Active Directory. Uwierzytelnianie sieciowe sprawdza uprawnienia użytkownika przy każdym odwołaniu do zasobów sieciowych. System Windows posiada dwa podstawowe protokoły uwierzytelniania sieciowego:

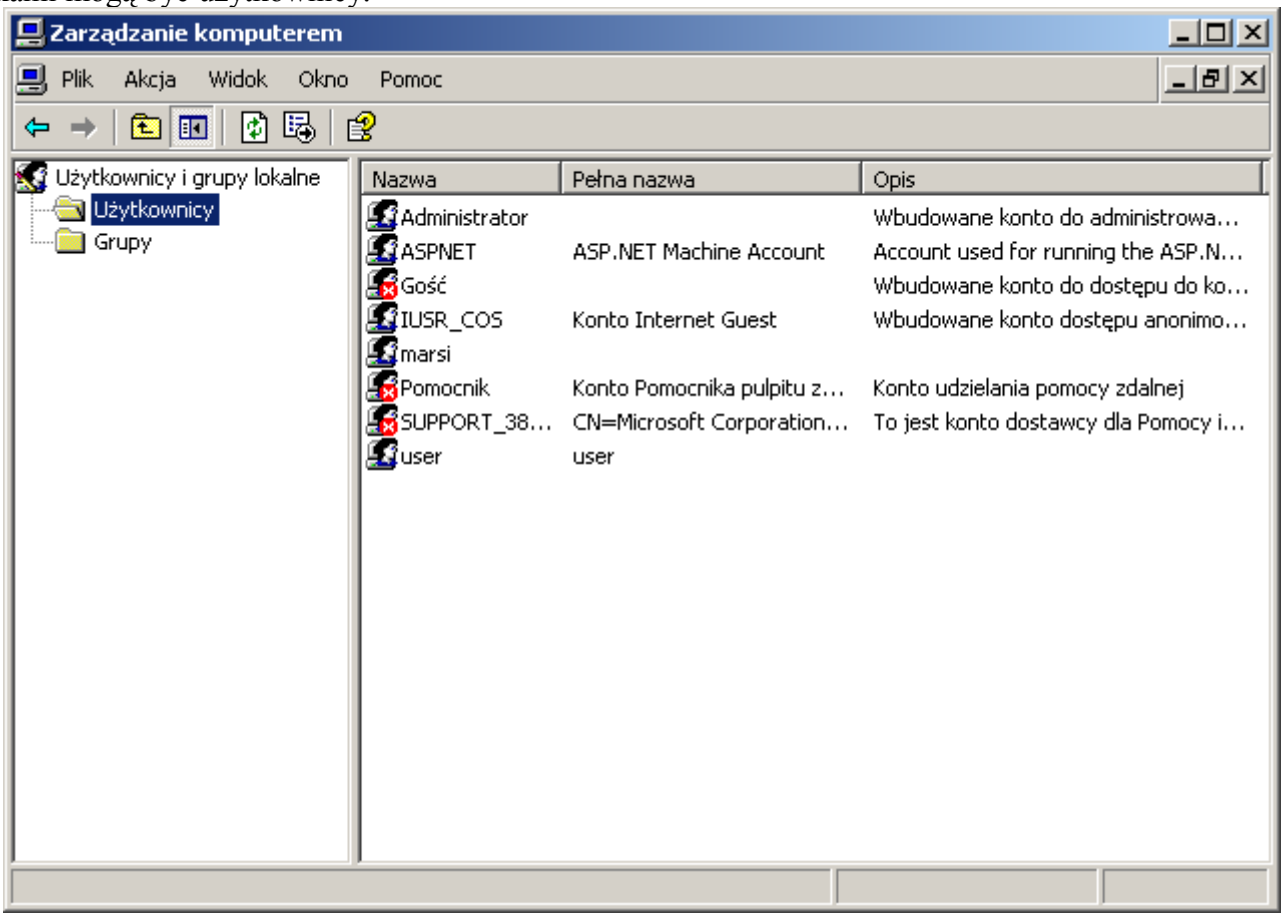
- Kerberos v5 - podstawowy mechanizm uwierzytelniania w Windows Serwer 2003, standardowy protokół internetowy do uwierzytelniania użytkowników.
- NT Lan Manager (NTLM) - protokół stosowany przy współpracy z systemami Windows NT.

W przypadku, gdy użytkownik loguje się do domeny interaktywny proces logowania przydziela uprawnienie w usłudze Active Directory, dzięki czemu otrzymuje on dostęp do zasobów sieciowych. Co za tym idzie użytkownik może zostać uwierzytelniony automatycznie na każdym komputerze w domenie.
Wszystko co zawarte jest w katalogu Active Directory (np. grupy, udostępniane zasoby, użytkownicy), zdefiniowane jest w sposób obiektowy. Dzięki temu, administrator może kontrolować dostęp do tych obiektów poprzez deskryptory zabezpieczeń. Dodatkowo możliwe jest zdefiniowanie właścicieli tych obiektów, zdarzeń których wystąpienie powinno podlegać inspekcji, określenie drobiazgowych praw przyznawanych użytkownikom oraz wybranie użytkowników i grup, które mają prawo dostępu do obiektu. Obiekty Active

Directory mogą dziedziczyć uprawnienia po swoich obiektach nadrzędnych. Jeśli tworzymy wpisy kontroli dostępu musimy pamiętać o dwóch rzeczach:

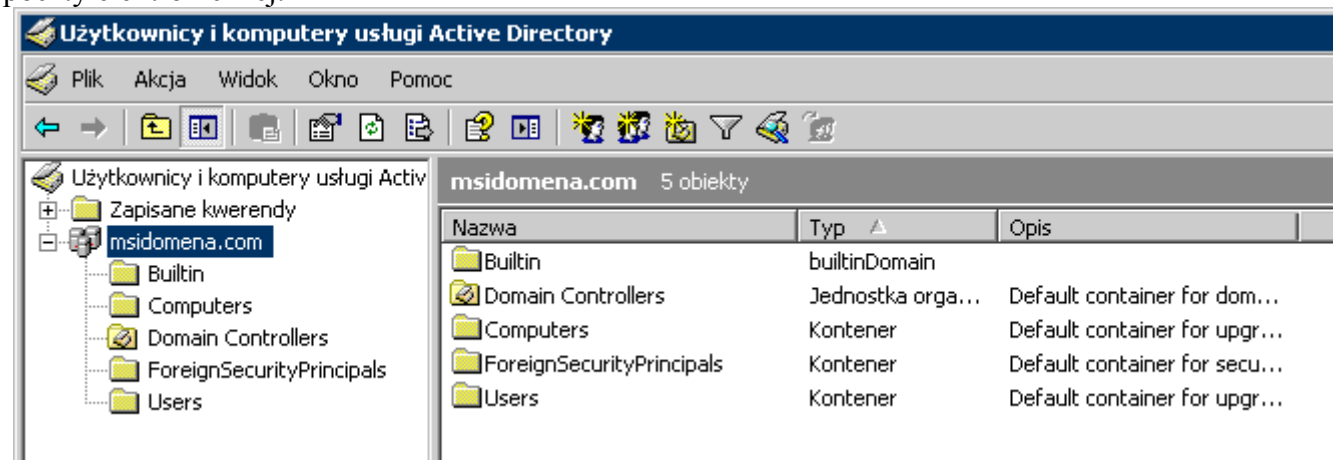
- Dziedziczenie wpisów jest domyślnie włączone i wykonywane natychmiastowo po zapisaniu wpisu.
- Każdy wpis zawiera informacje czy podlega dziedziczeniu, czy też przydzielany jest tylko dla konkretnego obiektu.

W Windows Serwer 2003 rozróżniamy dwa rodzaje kont: **konta użytkowników** i **konta grup**, których członkami mogą być użytkownicy.



Konta grup nie umożliwiają zalogowania się w systemie, służą jedynie do prostszego administrowania wieloma użytkownikami jednocześnie. Jeżeli użytkownik jest członkiem grupy, która ma prawo do korzystania z jakiegoś zasobu, to prawo to przechodzi na niego. Nazwę grupy bardzo często podaje się stosując schemat domena\grupa. Jest to spowodowane tym, że w różnych domenach mogą istnieć grupy o tej samej nazwie. W systemie Windows Serwer 2003 rozróżniane są trzy rodzaje grup:

- **Grupy lokalne** - odnoszące się tylko do komputera na którym były zdefiniowane. Tworzy się je korzystając z narzędzia **Lokalni użytkownicy i grupy**.
- **Grupy zabezpieczeń** - mają przydzielone identyfikatory zabezpieczeń (SID), tworzy się je w domenach przy użyciu narzędzia **Użytkownicy i komputery Active Directory**.
- **Grupy dystrybucji** - nie posiadają identyfikatorów zabezpieczeń, tworzy się je jak poprzednio przy użyciu przystawki **Użytkownicy i komputery Active Directory**, wykorzystywane są, jako listy dystrybucyjne poczty elektronicznej.



Grupy można także podzielić ze względu na obszar ich ważności:

- **Lokalne domenowe** - uprawnienia mogą być przydzielane tylko w granicach jednej domeny, członkami mogą być użytkownicy, komputery oraz grupy z tej domeny. Powinny być używane do określenia zasobów do drukarek sieciowych i udostępnionych folderów.
- **Wbudowane grupy lokalne** - tak jak poprzednie grupy, posiadają uprawnienia domeny lokalnej, główną różnicą jest to, że nie można ich tworzyć ani usuwać, a jedynie modyfikować im uprawnienia.
- **Globalne** - umożliwiają przydzielenie uprawnień do obiektów w dowolnej domenie z lasu lub drzewa domen. Do tej grupy mogą należeć jedynie konta z domeny, w której są zdefiniowane. Grupy te można uczynić członkami domenowych grup lokalnych w celu przydzielenia użytkownikom uprawnień do zasobów.
- **Uniwersalne** - wymagają działania Active Directory na poziomie funkcjonalności Windows 2000 lub Windows Server 2003, podobnie jak poprzednie grupy umożliwiają przydzielenie uprawnień w obrębie drzewa lub lasu domen. Do grup tych mogą należeć konta użytkowników, grupy globalne oraz inne grupy uniwersalne. Członkowie grup uniwersalnych nie powinni być często zmieniani, ponieważ każda zmiana wymaga replikacji do wszystkich wykazów globalnych w drzewie lub lesie domen. Członkami tych grupy powinny być raczej inne grupy. Jeżeli organizacja posiada jedną domenę, nie ma potrzeby korzystania z grup uniwersalnych.

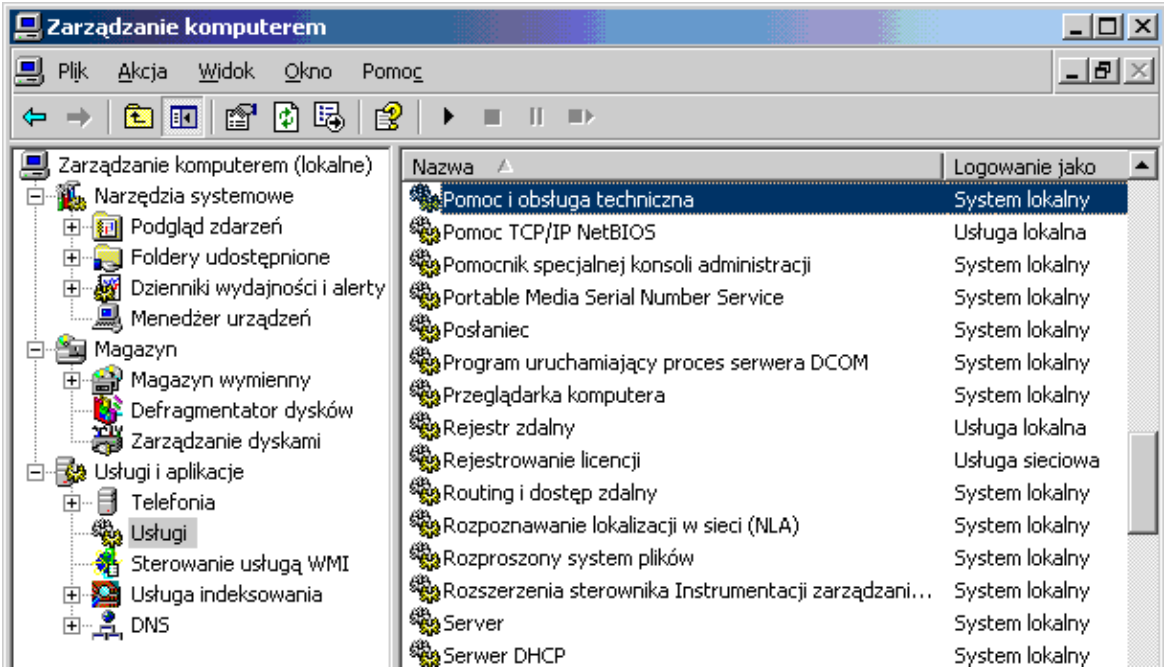
Podczas przydzielania członków do grup musimy pamiętać, że nie wszystkie działania dostępne są we wszystkich zakresach. Konta użytkowników dzielą się na lokalne i domenowe zdefiniowane w usłudze Active Directory. Konta użytkowników mogą posiadać hasła oraz certyfikaty publiczne, które w celu identyfikacji użytkownika wykorzystują kombinację klucza publicznego i prywatnego. Podczas logowania użytkownika do systemu Windows Server 2003 tworzony jest żeton zabezpieczeń, który zawiera identyfikator użytkownika oraz identyfikatory zabezpieczeń wszystkich grup, do których należy użytkownik. Wynika z tego, że wielkość żetonu zależy od ilości grup, do których użytkownik należy. Żeton ten przesyłany jest do każdego komputera, do którego użytkownik chce się zalogować.

W systemie Windows Serwer 2003 stworzone są wbudowane konta logowania, które służą do realizacji szczególnych zadań, są to:

-**System lokalny** (LocalSystem) - służy do uruchamiania procesów systemowych i obsługi zadań systemowych. Z tego konta korzysta większość usług niewymagających dodatkowych uprawnień. Konto posiada uprawnienie **Zaloguj jako usługę**.

-**Usługa lokalna** (LocalService) - używane w przypadku usług wymagających dodatkowych uprawnień - **Zmień czas systemowy**, **Generuj zdarzenie inspekcji w systemie** oraz **Zaloguj jako usługę**. Z konta tego korzystają takie usługi jak np. Rejestr zdalny, Pomoc TCP/IP Net BIOS, Alertowanie i WebClient.

-**Usługa sieciowa** (NetworkService) - służy do uruchamiania usług, które wymagają dodatkowych praw dostępu do sieci. Usługi uruchomione przy użyciu tego konta posiadają uprawnienia **Zaloguj jako usługę**, z przywilejem **Zmień czas systemowy** i **Generuj zdarzenie inspekcji zabezpieczeń**. Usługi, które korzystają z tego konta to np. Lokalizator usługi zdalnego wywołania procedur (RPC), Klient DNS, Klient DHCP, Koordynator transakcji rozproszonych.



Powyższe konta nie mogą zostać usunięte. Możliwe, że przy instalowaniu dodatkowych rozszerzeń pojawią się jeszcze inne konta domyślne, jednak będą one mogły zostać usunięte. Jeżeli na serwerze zostaną zainstalowane Internetowe usługi informacyjne, pojawią się nowe konta między innymi: IUSR_nazwakomputera (wykorzystywane przez anonimowy dostęp do IIS) oraz IWAM_nazwakomputera (do uruchamiania aplikacji wywołanych przez IIS).

Oprócz wbudowanych kont logowania, na serwerze podczas instalacji tworzone są wbudowane konta użytkowników: **Administrator**, **ASPNET**, **Gość** oraz **Pomocnik**. Posiadają one prawa dostępu w całej domenie i są odrębne od kont lokalnych. Mają swoje odpowiedniki w katalogu Active Directory. Konto **Administrator** posiada nieograniczony dostęp do usług systemowych, plików czy katalogów. Nie może zostać usunięte ani wyłączone. W katalogu Active Directory posiada ono dostęp do zasobów całej domeny. Konto to, jest krytyczne z punktu widzenie bezpieczeństwa systemu. Ze względu na popularną nazwę może stać się celem ataku nieautoryzowanego dostępu do systemu. Powinno ono posiadać bezpieczne hasło złożone z małych i wielkich liter, znaków specjalnych oraz cyfr. Dobrą praktyką jest zmiana nazwy tego konta na mniej oczywistą a następnie utworzenie konta o nazwie Administrator nieposiadającego żadnych praw. Możliwe jest ograniczenie dostępu Administratorowi do plików czy folderów, jednak zawsze będzie on mógł przywrócić sobie prawa dostępu. W środowisku domenowym konto Administrator wykorzystywane jest głównie do konfiguracji systemu po pierwszej jego instalacji. Później prawdopodobnie nie będzie już wykorzystywane. W przypadku systemów będących częścią grup roboczych konto to będzie wykorzystywane do realizacji zadań administracyjnych. Konto **ASPNET** posiada domyślnie takie same prawa jak zwykli użytkownicy, należy do grupy **Użytkownicy domeny**, służy do uruchamiania procesów ASP.NET przez system .NET Framework. Konto **Gość** stworzone zostało do jednorazowego dostępu do systemu. Posiada mocno ograniczone prawa dostępu. Może stać się źródłem problemów zabezpieczeń w systemie, dlatego w domyślnej konfiguracji systemu jest wyłączone. Należy do grupy **Goście**, **Użytkownicy domniemani** oraz **Wszyscy** - która posiada dostęp do plików i katalogów. Podobnie jak w przypadku konta Administrator, dobrze jest zmienić mu nazwę na mniej oczywistą. Konto **Pomocnik** wykorzystywane jest przez usługę **Pomoc i obsługa techniczna**, nie posiada prawa do logowania lokalnego (z wyjątkiem logowania jako proces wsadowy), oraz prawa do logowania zdalnego. Należy do grup **Użytkownicy domeny** oraz **Użytkownicy pomocy**.

Każde konto użytkownika posiada pewne możliwości, które możemy określić. Najczęściej przyznaje się użytkownikowi te możliwości poprzez włączenie go do pewnych grup. W systemie Windows Server 2003 istnieją cztery kategorie potencjalnych zdolności:

- Przywileje - są to rodzaje uprawnień pozwalające na wykonywanie pewnych zadań np. możliwość wykonania zamknięcia systemu.
- Prawa logowania - np. uprawnienie do logowania lokalnego, są to typy uprawnień przyznające możliwości logowania do systemu.
- Uprawnienia wbudowane - to rodzaje uprawnień przypisywane grupom i zawierające ich możliwości np. prawo do tworzenia innych kont.

- Prawa dostępu - definiują operacje, jakie mogą być wykonywane na zasobach sieciowych np. prawo do tworzenia plików w katalogu.

Zanim zaczniemy budować system uprawnień oparty na grupach, powinniśmy zapoznać się z zasadami ich tworzenia. Niewłaściwe stosowanie np. zakresów grup może doprowadzić do tego, że nakładające się zakresy będą trudne w konfiguracji praw dostępu dla użytkowników. Niezbędna jest też często wiedza o domyślnych ustawieniach kont czy grup. Dobrze nadane prawa mogą przyczynić się do zmniejszenia liczby nadużyć przez użytkowników systemu, a tym samym do zwiększenia jego bezpieczeństwa.