Usługa katalogowa Active Directory - Zarządzanie

Usługa katalogowa **Active Directory** (ang. **Active Directory Domain Services**) udostępnia rozproszoną bazę danych, która przechowuje i zarządza informacjami o zasobach sieci oraz danymi specyficznymi dla aplikacji potrafiących z tej bazy korzystać.

Usługa **Active Directory** przechowuje informacje o obiektach znajdujących się w sieci oraz umożliwia administratorom i użytkownikom łatwe znajdowanie tych informacji i korzystanie z nich. Usługa **Active Directory** używa magazynu danych o określonej strukturze jako podstawy dla logicznej i hierarchicznej organizacji informacji katalogowych. Ten magazyn danych, nazywany również katalogiem, zawiera informacje o obiektach usługi **Active Directory**. Do tych obiektów zazwyczaj należą zasoby udostępnione, takie jak serwery, woluminy, drukarki oraz konta użytkowników i komputerów w sieci. Usługą **Active Directory** są zintegrowane zabezpieczenia polegające na uwierzytelnianiu logowania i kontroli dostępu do obiektów w katalogu. Po jednokrotnym zalogowaniu się do sieci administratorzy mogą zarządzać danymi katalogowymi i ich organizacja w sieci, a autoryzowani użytkownicy sieci maja dostęp do zasobów znajdujących się w dowolnym miejscu sieci. Administracja oparta na zasadach ułatwia zarządzanie nawet najbardziej złożoną siecią.

Funkcje Active Directory

Usługi katalogowe pełnią następujące funkcje:

- umożliwia scentralizowane zarządzanie zasobami naszej sieci (serwery, drukarki czy udostępnione pliki) a także przypisywanie uprawnień do tychże zasobów,
- możliwość administracji nie tylko w obrębie sieci LAN ale także na roległych obszarach geograficznych na których mogą być rozproszone nasze komputery,

serwery,
- dzięki zapewnieniu hierarchicznej struktury bazy AD zyskujemy większe bezpieczeństwo przechowywania zasobów, którymi zarządzamy.

Logiczna struktura AD DS

Logiczna struktura **Active Directory** składa się z następujących elementów:

- **Obiekt** - podstawowy element struktury AD. Każdy obiekt ma klasę, która jest szablonem dla typu obiektu, w klasie są zdefiniowane grupy atrybutów i możliwe wartości jakie możemy przypisać do obiektu.
- **Jednostka organizacyjna** (**OU**) - szczególnie przydatnym typem obiektu (kontenerem) katalogu zawartym w domenie jest jednostka organizacyjna. Jednostki organizacyjne są kontenerami usługi **Active Directory**, w których można umieszczać użytkowników, grupy, komputery i inne jednostki organizacyjne, czyli umożliwiają one grupowanie obiektów o wspólnej administracji lub konfiguracji. Jednostki OU mają jednak większe możliwości niż organizowanie obiektów usługi **Active Directory**. Udostępniają ważne funkcje administracyjne - są punktem, z którego funkcje administracyjne mogą być delegowane oraz do którego odnoszone mogą być zasady grupy.
- **Domena** - to grupa komputerów połączonych w sieć, składająca się z serwera pełniącego rolę kontrolera domeny a także podstawowa jednostka funkcjonalna logicznej struktury **Active Directory**. Domeny charakteryzuje całkowicie odmienne podejście do zarządzania siecią. Ich administracja jest uproszczona przez umieszczenie w jednej bazie informacji o kontach użytkowników, zabezpieczeniach i zasobach sieci. Za jej obsługę i udostępnianie odpowiada usługa **Active Directory**. Chcąc założyć domenę, należy na jednym z serwerów Windows Server 2003 lub Windows 2008 zainstalować **Active Directory**. Od tej pory komputer ten będzie nazywany kontrolerem domeny. Baza zasobów może być replikowana na dodatkowe serwery, dzięki czemu awaria jednego z komputerów nie prowadzi do paraliżu sieci. Drzewo domen - domeny, które są zgrupowane razem w hierarchiczna strukturę. Kiedy dodajemy następną domenę do drzewa, staje się ona "domeną dzieckiem" (ang. **domain child**). Domena, do której dziecko zostało przyłączone, nazywa się domeną rodzicem (ang. **parent domain**).

Nazwa domeny dziecka jest kombinacją jej nazwy z nazwą domeny rodzica formie nazwy **Domain Name System** (**DNS**) np. opole.firma.com Oznacza to, że drzewo posiada wspólną przestrzeń nazw DNS.

Fizyczna struktura AD DS

Do elementów tworzących fizyczną strukturę AD możemy zaliczyć:

- **Kontrolery domeny** - jest to komputer w domenie, który zarządza realizacją wszystkich działań związanych z bezpieczeństwem zachodzących między użytkownikiem a domeną oraz ustala w jaki sposób użytkownicy mogą uzyskiwać dostęp, konfigurować czy korzystać z zasobów domeny, co przyczynia się do poprawienia procesu zarządzania zasobami i zabezpieczeniami. Kontroler domeny pełni rolę administratora danej domeny czy jednostki organizacyjnej w domenie np. drzewa domen, lasu. Kontroler domeny umożliwia przydzielanie uprawnień do administrowania i zarządzania obiektami w całej domenie albo w jednej lub kilku jednostkach organizacyjnych. W celu zapewnienia niezawodności działania usług czy to obsługi AD, DNS-a czy DHCP, w każdej domenie bezpiecznie jest posiadać więcej niż jeden kontroler domeny.
- **Site** - w usłudze **Active Directory** reprezentują fizyczną strukturę sieci, czyli jej topologię. Na podstawie informacji o topologii, które są przechowywane w katalogu jako obiekty typu lokacja i łącze lokacji, usługa **Active Directory** konstruuje najwydajniejszą topologię replikacji. Do określania lokacji i łączy lokacji służy przystawka **Lokacje i usługiActive Directory**. Lokacja jest zestawem dobrze połączonych podsieci. Lokacje różnią się od domen, ponieważ reprezentują fizyczną strukturę sieci, podczas gdy domeny reprezentują logiczną strukturę organizacji.
- **Partycje Active Directory** - baza danych **AD** jest podzielona na partycje katalogu. Wszystkie kontrolery domeny działające w obrębie jednego lasu posiadają dwie wspólne partycje katalogu: partycje konfiguracji i schematu. Dodatkowo partycja domeny jest współdzielona przez wszystkie kontrolery znajdujące się w domenie. Każdy kontroler domeny zawiera przeznaczoną do zapisu wzorcową kopię partycji usługi **Active Directory** dla swojej domeny, więc zmiany w partycji domeny można wprowadzić na każdym dostępnym kontrolerze domeny. W takim przypadku musi istnieć sposób powielania aktualizacji na innych kontrolerach domen po wprowadzeniu zmian na jednym kontrolerze domeny. Proces rozpowszechniania zaktualizowanych informacji na właściwe kontrolery domen nosi nazwę replikacji.
- **Partycja domeny** - znajdują się w niej repliki wszystkich obiektów w domenie (użytkownicy, grupy, komputery i jednostki organizacyjne). Na inne kontrolery domen są jednak replikowane tylko zmiany na poziomie atrybutów danego obiektu; nie są replikowane całe obiekty. Prowadzi to do znacznych oszczędności w natężeniu ruchu związanego z replikacją. Partycja domeny jest replikowana tylko pomiędzy kontrolerami domeny znajdującymi się w tej samej domenie.
- **Partycja konfiguracji** - zawiera informacje o topologii lokacji i replikacji oraz o partycji usług i katalogu. Dane te sa wspólne dla wszystkich domen w drzewie lub lesie. Dane konfiguracyjne są replikowane do wszystkich kontrolerów domen w lesie.
- **Partycja schematu** - zawiera wszystkie typy obiektów (i ich atrybuty), które mogą zostać utworzone w **Active Directory**. Dane te są wspólne dla wszystkich domen w drzewie czy lesie. Przechowywane są w niej definicje klas i atrybutów dla wszystkich istniejących oraz możliwych obiektów. Partycja schematu jest replikowana do wszystkich kontrolerów domen w lesie.
- Opcjonalna **partycja aplikacji** - przechowuje dane potrzebne do działania określonych aplikacji. Może ona zawierać dowolne obiekty z wyjątkiem podmiotów zabezpieczeń (użytkowników, grup i komputerów). Aby ograniczyć wpływ na wydajność sieci, administrator może zdefiniować zakres replikacji oraz skierować replikację do określonych kontrolerów domeny. Alternatywnie można traktować

katalog aplikacji podobnie jak pozostałe partycje, pozwalając na replikację wszystkich danych do wszystkich kontrolerów domeny. Każda aplikacja określa sposób przechowywania, kategoryzowania i użycia wykorzystywanych przez nią informacji. W przeciwieństwie do partycji domeny. Przykładem może być DNS zintegrowany z **Active Directory** - korzysta z dwóch partycji aplikacji: **ForestDNSZones** i **DomainDNSZones**.

Masters Operations

Kiedy następuje zmiana dowolnego obiektu w domenie, zmiana ta musia zostać przesłana na inne kontrolery domeny czyli następuje aktualizacja obiektu inaczej replikacja pomiędzy wszystkimi kontrolerami w domenie. **AD** stworzono specjalnie z myślą o gromadzeniu, modyfikowaniu i usuwaniu informacji w katalogu z wielu kontrolerów domen. Technika pozwalająca na to, zwana **multimaster replication (czyli z wieloma serwerami głównymi)**, pozwala na używanie więcej niż jednego autorytatywnego kontrolera domeny. Jeśli w jednym czasie na dwóch kontrolerach w domenie zostanie zmodyfikowany ten sam atrybut tego samego obiektu może wystąpić konflikt replikacji. Aby zapobiec wystąpieniu konfliktów replikacji stworzono mechanizm, który pozwala jednemu odpowiedzialnemu za przeprowadzenie zmian kontrolerowi domeny je wykonać. Mechanizm ten powoduje, że wprowadzane są tylko najnowsze zmiany. Mechanizm ten nosi nazwę **single master replication** i ma on zastosowanie do takich zmian jak dodanie nowej domeny czy do zmiany schematu.

Operacje używające **single master replication** są łączone razem w role (**operations master roles**) które odnoszą się do domeny lub lasu. **Active Directory** przechowuje informacje o kontrolerach domeny, które są odpowiedzialne za specyficzne role.

Active Directory definiuje pięć **operations master roles**, dwie związane z lasem i trzy z domeną.

Role związane z lasem:

- **Schema master** - rola, która sprawuje kontrolę nad zmianami związanymi ze schematem, który zawiera listę klas obiektów i atrybutów, które są używane do tworzenia wszystkich obiektów AD takich jak użytkownicy, komputery lub drukarki.
- **Domain naming master** - rola odpowiedzialna za dodawanie a także usuwanie domen w lesie. Kiedy jest tworzona nowa domena, tylko kontroler, który przechowuje tę rolę może dokonać odpowiednich wpisów w AD, dzięki temu mamy pewność, że nie dodamy domen o takich samych nazwach.
- Istnieje tylko jeden **schema master** i **domain namig master** w całym lesie

Role związane z domeną:

- **Primary domain controller emulator** (**PDC**) - rola która jest odpowiedzialna za zarządzanie zmianami haseł dla komputerów z systemem Windows. Dodatkowo jest odpowiedzialna za synchronizację czasu dla wszystkich kontrolerów w domenie.
- **Relative identifier master** (**RID**) - kontroler domeny, którego zadaniem jest prawidłowa obsługa nowych podmiotów zabezpieczeń (np. konto użytkownika, grupę, komputer), przypisuje do obiektu unikalny identyfikator (SID).
- **Infrastructure master** - kiedy obiekt jest przenoszony z jednej domeny do innej, rola uaktualnia obiekt odniesienia znajdujący się w domenie pierwotnej wskazujący na obiekt w nowej domenie. Obiekt odniesienia zawiera globalny unikalny identyfikator (**GUID**), nazwę wyróżniającą i **SID**.

Nazwa wyróżniająca i względna nazwa wyróżniająca

Do przeszukiwania oraz do modyfikacji obiektów zawartych w **AD** hosty używają mechanizmu **Lightweight Directory Access Protocol** (**LDAP**).

- **Nazwa wyróżniająca - LDAP** używa nazwy określającej dany obiekt w **AD** czyli jest protokołem wymiany informacji pomiędzy serwerem i klientem usług katalogowych. Serwer usług katalogowych przechowuje dane teleadresowe i identyfikacyjne dotyczące użytkowników systemu komputerowego i dostępnych zasobów, pobierane następnie przez klientów w celu określania struktury sieci lub przeprowadzenia autoryzacji użytkownika. Nazwa wyróżniająca musi być unikalna w całym lesie.
- **Względna nazwa wyróżniająca** - nazwa opisująca dany obiekt w kontenerze, niedozwolona jest sytuacja w której istnieją dwa obiekty o takiej samej nazwie.

Np. dla użytkownika *Jan Nowak* znajdującego się w jednostce organizacyjnej *Biuro* w domenie *Firma.local*, każdy z elementów logicznej struktury jest reprezentowany przez następującą nazwę wyróżniającą:

CN="Jan Nowak",OU=Biuro,DC=Firma,dc=local

- CN - nazwa ogólna (ang. common name) obiektu w kontenerze
- OU - jednostka organizacyjna (ang. organizational unit) zawierająca obiekt. Jeśli obiekt znajduje się w zagnieżdżonych jednostkach to może być więcej wartości OU.
- DC - komponent domeny (ang. domain komponent) taki jak "com", "edu" czy "local". Zawsze są przynajmniej dwa komponenty domeny, chyba, że domena jest domena podrzędną.

Do każdego obiektu w usłudze **Active Directory** można się odwołać przy użyciu różnych typów nazw opisujących lokalizację tego obiektu. Usługa **Active Directory** tworzy względną nazwę wyróżniającą i nazwę kanoniczną dla każdego obiektu na podstawie informacji podanych podczas tworzenia lub modyfikowania obiektu.

Względna nazwa wyróżniająca **LDAP** jednoznacznie identyfikuje obiekt znajdujący się w kontenerze nadrzędnym. Na przykład względną nazwą wyróżniającą **LDAP** jednostki organizacyjnej o nazwie BIURO jest OU=BIURO. Względne nazwy wyróżniające nie mogą się powtarzać w ramach jednostki organizacyjnej. Ważne jest, aby podczas tworzenia skryptów do tworzenia kwerend i zarządzania usługą **Active Directory** znać składnię względnej nazwy wyróżniającej LDAP.

W odróżnieniu od względnej nazwy wyróżniającej **LDAP**, nazwa wyróżniająca **LDAP** jest unikatowa globalnie. Na przykład nazwa wyróżniająca **LDAP** w jednostce organizacyjnej o nazwie MARKETING w domenie firma.com będzie miała postać: OU=MARKETING, DC=FIRMA, DC=COM. Względna nazwa wyróżniająca LDAP jednoznacznie identyfikuje obiekt w kontenerze nadrzędnym. Użytkownicy nigdy nie korzystają z tej nazwy, jednak administratorzy używają tej nazwy w skryptach lub w wierszu polecenia w celu dodania użytkowników do sieci. Wszystkie obiekty korzystają z tej samej konwencji nazewnictwa **LDAP**, dlatego wszystkie względne nazwy wyróżniające **LDAP** muszą być unikatowe w jednostce organizacyjnej.

Nazwa kanoniczna jest konstruowana w ten sam sposób, co nazwa wyróżniająca LDAP, ale jest reprezentowana za pomocą innej notacji. Nazwa wyróżniająca obiektu, w której obiekt główny jest zapisywany na początku nazwy. Nazwa tego typu nie zawiera tagów atrybutów **LDAP** (takich jak: CN=, DC=). Segmenty nazwy są rozdzielane kreskami ukośnymi (/). Na przykład nazwa kanoniczna jednostki organizacyjnej o nazwie BIURO w domenie FIRMA.COM ma postać: FIRMA.COM/BIURO. Z nazw kanonicznych korzysta się podczas używania niektórych narzędzi administracyjnych np. gdy chcemy . Służy ona do przedstawiania hierarchii w narzędziach administracyjnych.

Narzędzia do zarządzania obiektami Active Directory

Do dyspozycji administratora systemu Microsoft Windows Server jest kilka narzędzi, odpowiedzialnych za tworzenie, modyfikację i usuwanie obiektó w AD:

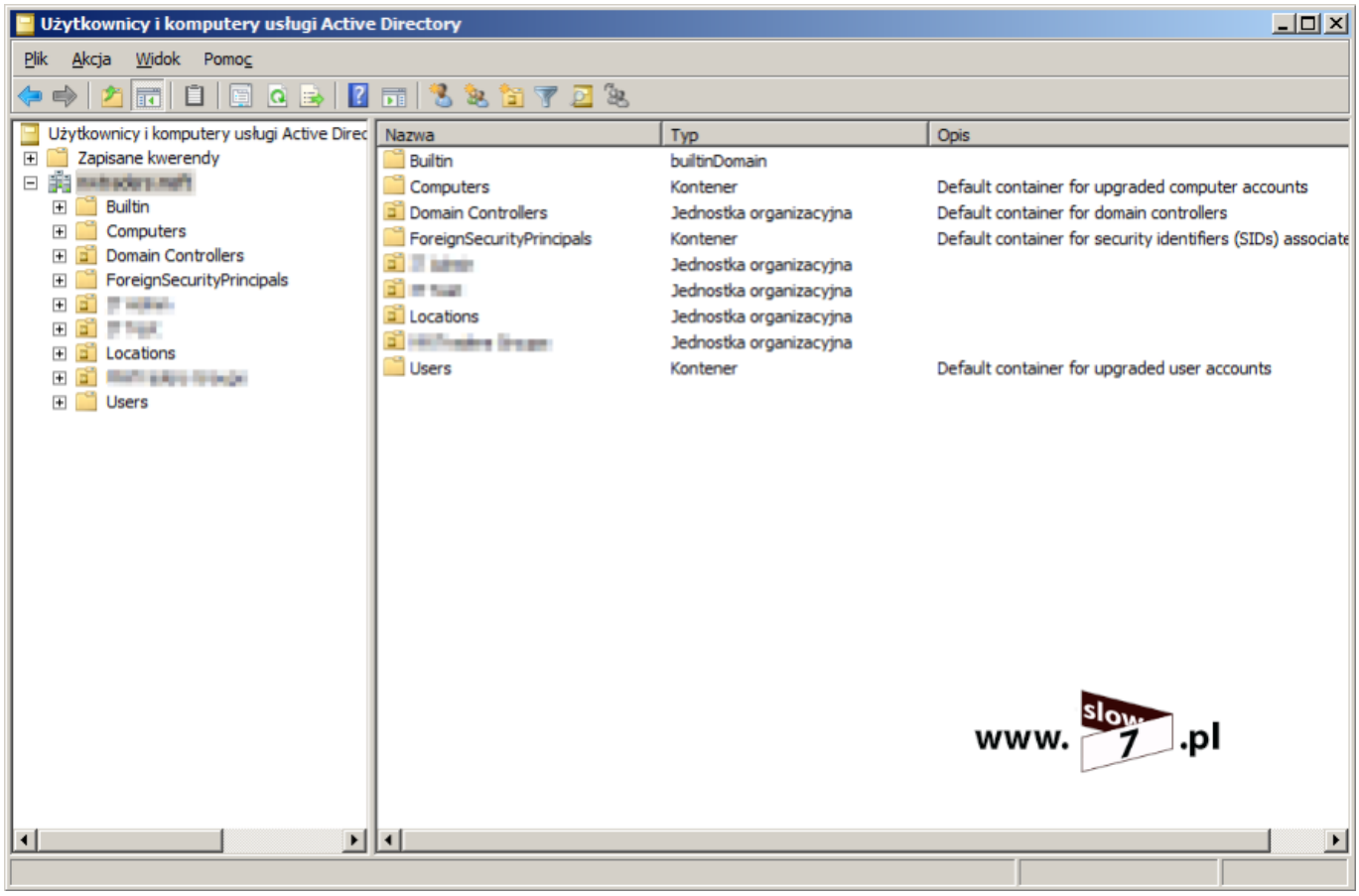
- **Active Directory Users and Computers** - Przystawka konsoli MMC, narzędzie administracyjne przeznaczone do wykonywania codziennych zadań administracyjnych usługi **Active Directory**. Do zadań tego typu należy m.in. tworzenie, usuwanie, modyfikowanie i przenoszenie obiektów oraz ustawianie uprawnień dotyczących obiektów przechowywanych w katalogu. Obiektami mogą być jednostki organizacyjne, użytkownicy, kontakty, grupy, komputery, drukarki i udostępniane pliki. Po jej uruchomieniu w **Narzędziach administracyjnych**, **Panelu sterowania**,ujrzymy drzewo

przedstawiające obiekty użytkowników i komputerów aktualnej domeny. Jeżeli chcielibyśmy pracować na innej domenie niż aktualna możemy się podłączyć do innego kontrolera klikając prawym przyciskiem mysz na wpis **Użytkownicy i komputery Active Directory** i wybierając **Podłącz do innego kontrolera domeny** lub **Podłącz do innej domeny**. W narzędziu tym, po lewej stronie występują foldery:

- **Zapisane kwerendy** - to zapisane kryteria wyszukiwania
- **Builtin** - lista wbudowanych kont użytkowników
- **Computers** - kontener dla kont komputerów
- **Domain controllers** - kontener dla kontrolerów domeny
- **ForeignSecurityPrincipals** - zawiera informacje o obiektach należących do zaufanych domen zewnętrznych
- **Users** - kontener dla kont użytkowników

Po kliknięciu w menu **Widok** na **Opcje zaawansowane**, odsłonią się następujące foldery

- **LostAndFound** - są tu obiekty osierocone, które można przywrócić
- **NTDS Quotas** - informacje o przydziałach dysku dla usługi katalogowej
- **Program Data** - informacje **Active Directory** w formacie dostępnym dla aplikacji Microsoft
- **System** - wbudowane ustawienia systemu



Rysunek 1 Okno Active Directory

- **Narzędzia wiersza poleceń usług katalogowych** - czyli zbiór narzędzi np dsadd, dsmod, dsrm, które działają w linii poleceń cmd a odpowiedzialne za tworzenie, modyfikację i usuwanie obiektów **AD**. Wygodne do użycia w skryptach.

    - **adprep** - wykonuj wstępne przygotowanie domeny Windows 2000 do zainstalowania domeny Windows Serwer 2003
    - **dsadd** - dodaje do katalogów obiekty komputerów, kontaktów, grup i użytkowników oraz jednostek organizacyjnych
    - **dsget** - wyświetla właściwości obiektu podanego w parametrze wywołania
    - **dsmod** - zmienia właściwości obiektów istniejących w katalogu
    - **dsmove** - przenosi obiekt w obrębie jednej domeny lub zmienia mu nazwę
    - **dsrm** - usuwa obiekt z katalogu
    - **dsquery** - wyszukuje obiekty różnego rodzaju według podanych kryteriów
    - **ntdsuti** - umożliwia przeglądanie informacji o lokacjach, domenach i serwerach oraz wykonywanie konserwacji bazy danych **Active Directory**.

- **Lightweight Directory Access Protocol Data Interchange Format Directory Exchange** (**Ldifde**) narzędzie wiersza poleceń, które służy do zarządzania obiektami. W pliku wejściowym są zawarte informacje o obiekcie i akcji, jakiej należy na nim wykonać. Informacje te są przechowywane, jako serie rekordów oddzielonych pustymi liniami.
- **Windows Script Host** - czyli programowe środowisko interpretacji i wykonywania skryptów w systemie Windows. Za pomocą WSH można tworzyć obiekty używając aplikacji Windows lub skryptów Windows korzystając z komponentów udostępnianych przez **Active Directory Service Interface** (**ADSI**).
- Wiele programów do konfiguracji **Active Directory** zawarte jest w narzędziach, przykładami mogą być:

    - **adsiedit.msc** - umożliwia edycję interfejsu **Active Directory** dla kontenerów domen
    - **replmon.exe** - umożliwia śledzenie przebiegu replikacji w interfejsie graficznym
    - **dsacls.exe** - pozwala zarządzać listami kontroli dostępu dla obiektów w katalogu **Active Directory**
    - **dnscmd.exe** - pozwala na zarządzanie rekordami stref serwera DNS
    - **movetree.exe** - przenosi obiekty z jednej domeny do drugiej
    - **repadmin** - pozwala na monitorowanie replikacji i zarządzanie w trybie wiersza poleceń
    - **sdcheck.exe** - sprawdza replikacje i poprawność dziedziczenia list kontroli dostępu
    - **sidwalker.exe** - ustanawia listy kontroli dostępu dla obiektów, uprzednio należących do kont, które zostały usunięte lub wydziedziczone

- **netdom.exe** - pozwala na zarządzanie relacjami zaufania i domenami z wiersza poleceń.

Jednostki organizacyjne

Jednostka organizacyjna to szczególnie przydatny typ obiektu usługi **Active Directory** znajdujący się w domenie. Przydatność jednostek organizacyjnych polega na tym, że za ich pomocą można zarządzać setkami tysięcy obiektów znajdującymi się w katalogu. Za pomocą jednostki organizacyjnej można grupować obiekty i zarządzać nimi w celu wykonania zadań administracyjnych. Jednostki organizacyjne są elementami, do których można przypisać zasady grup (**GPO**) lub delegować kontrolę administratorską. Wykorzystując je, można tworzyć kontenery w domenie reprezentujące hierarchiczną, logiczną strukturę organizacji. Zagnieżdżając jednostki organizacyjne w innych można modelować strukturę firmy minimalizując liczbę domen wymaganych w sieci.

Modele hierarchiczne jednostek organizacyjnych

Hierarchia funkcji uwzględnia wyłącznie funkcje biznesowe organizacji, bez wyróżniania lokalizacji geograficznych, działów czy oddziałów. Ten typ hierarchii można wybrać tylko wtedy, gdy funkcja IT nie jest przypisana do określonej lokalizacji ani organizacji.

Rozważając zorganizowanie struktury usługi **Active Directory** według funkcji, należy pamiętać o następujących cechach charakterystycznych takich projektów:

- Odporność na reorganizacje. Na hierarchię funkcji nie mają wpływu reorganizacje firm ani organizacji.
- Mogą być wymagane dodatkowe warstwy. Podczas korzystania z tej struktury może wystąpić konieczność utworzenia dodatkowych warstw w hierarchii jednostek organizacyjnych w celu przystosowania administracji użytkownikami, drukarkami, serwerami i udziałami sieciowymi.

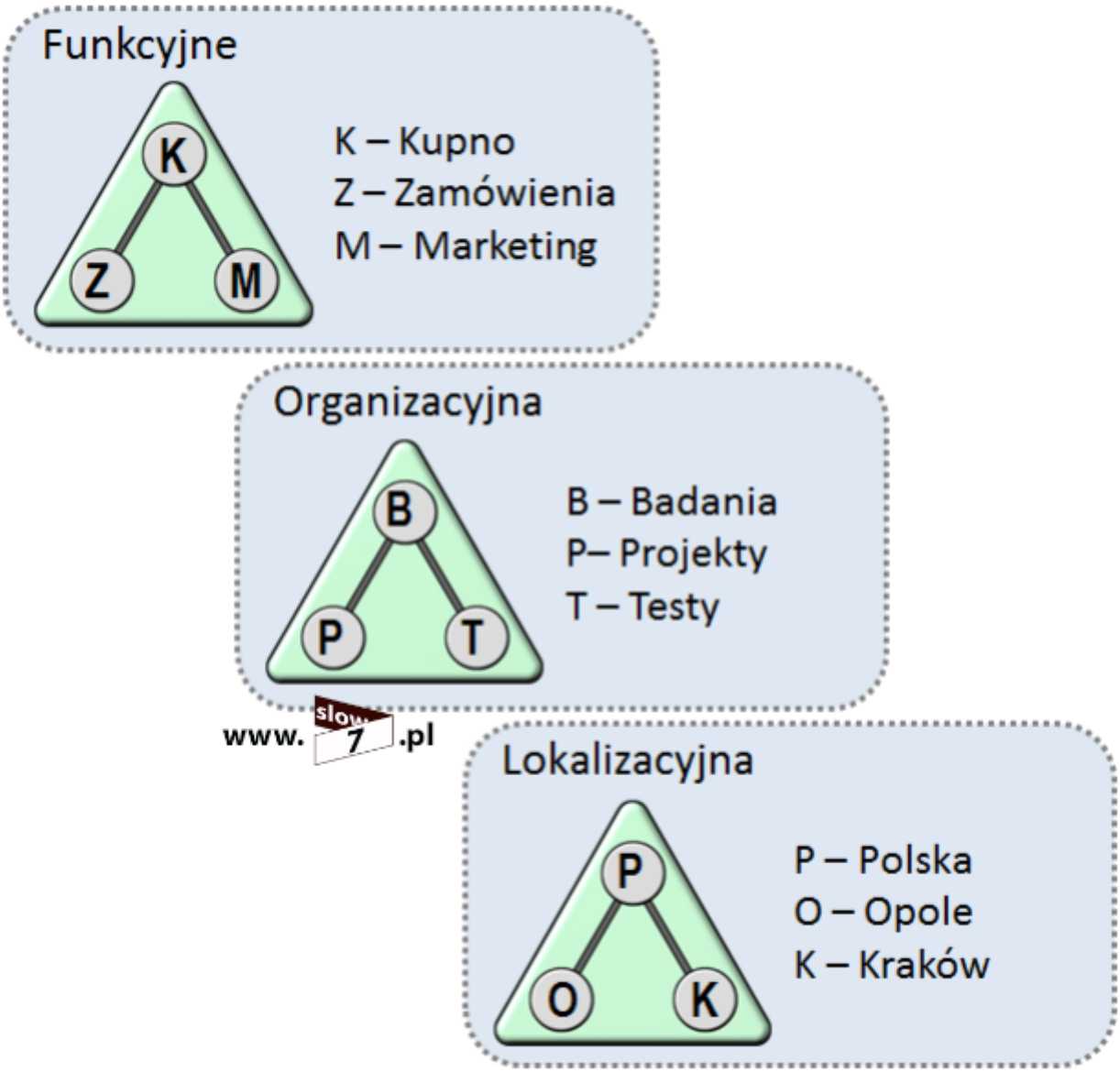
Struktura ta jest odpowiednia tylko dla małych organizacji, ponieważ wydziały w średnich lub dużych organizacjach są często bardzo zróżnicowane i nie można ich skutecznie zgrupować w jedną szerszą kategorię.

Hierarchia organizacji uwzględnia działy i oddziały organizacji. Jeśli struktura usługi **Active Directory** odzwierciedla strukturę organizacyjną, delegowanie praw administracyjnych może być trudne, ponieważ obiektów w usłudze **Active Directory**, takich jak drukarki i udziały plików, nie można grupować w sposób ułatwiający delegację praw administracyjnych. Ponieważ struktura usługi **Active Directory** jest niewidoczna dla użytkowników, należy przystosować ją do potrzeb administratora, a nie użytkownika.

Hierarchia uwzględniająca lokalizacje i organizacje oraz wszelkie inne kombinacje typów struktur noszą nazwę hierarchii mieszanej. Hierarchia mieszana spełnia wymagania organizacji, łącząc w sobie zalety kilku typów struktur.

Ten typ hierarchii ma następujące cechy charakterystyczne:

- Przystosowanie do dodatkowego zwiększenia liczby lokalizacji, działów lub oddziałów.
- Wyraźne rozróżnienie zarządzania działem od zarządzania wydziałem.
- Potrzeba współpracy między administratorami w celu wykonania zadań administracyjnych w sytuacji, gdy znajdują się oni w tej samej lokalizacji, ale w różnych działach lub oddziałach.



Rysunek 2 Modele hierarchiczne jednostek organizacyjnych

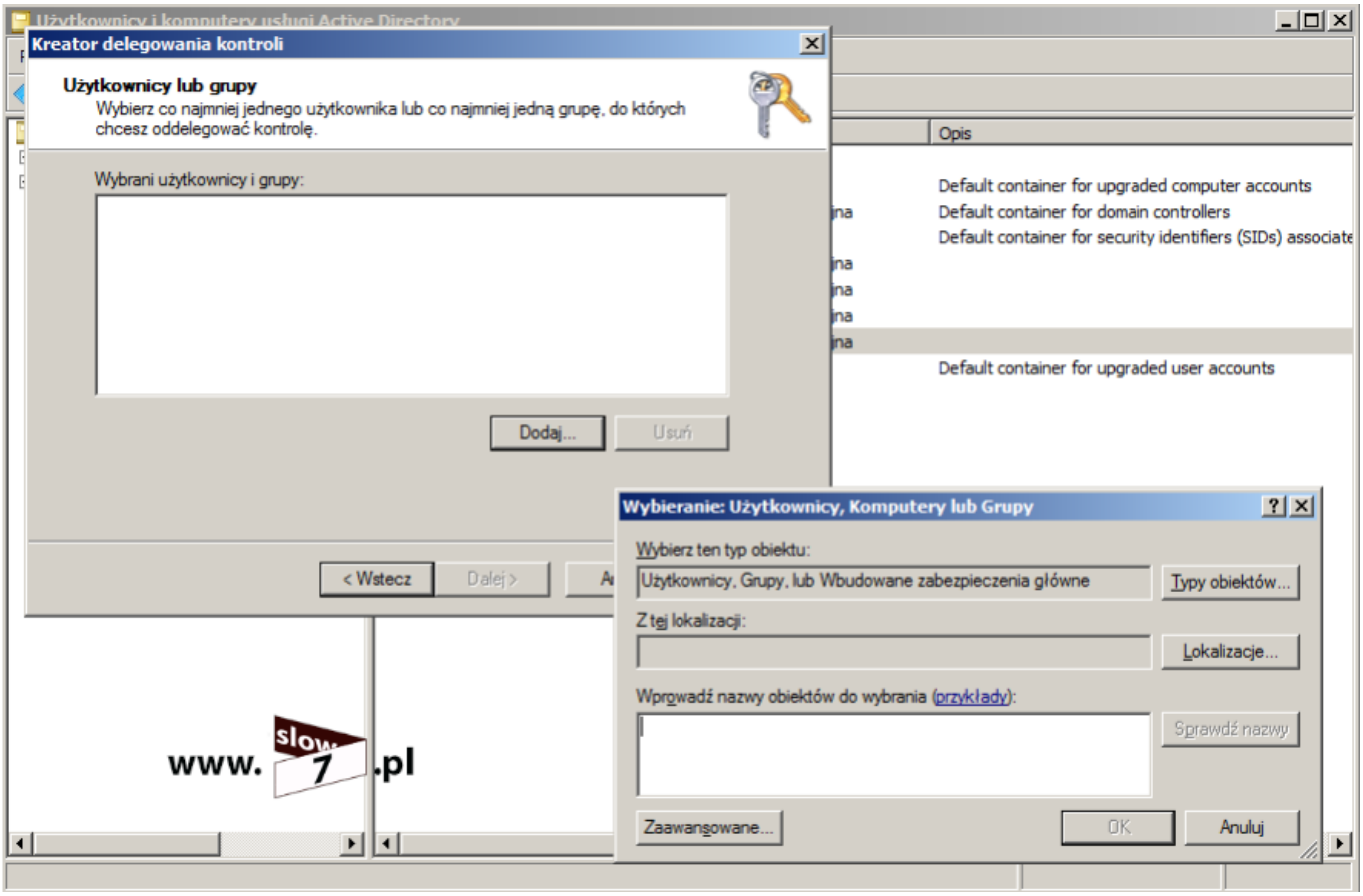
Delegowanie kontroli do jednostek organizacyjnych

Można delegować prawa administracyjne do poszczególnych atrybutów w pojedynczych obiektach usługi **Active Directory**, ale w tym celu zwykle używa się jednostek organizacyjnych. Użytkownik może mieć prawa administracyjne do wszystkich jednostek organizacyjnych w domenie lub do jednej jednostki organizacyjnej. Dzięki takiemu zabiegowi ograniczamy grupę osób mających uprawnienia do całej struktury **AD** ale dając im w zamian możliwość zarządzania tylko jej pewną częścią lub wybranymi funkcjami.

Kontrolę administracyjną można delegować na trzy sposoby:

- przyznanie uprawnień do zarządzania całym kontenerem, co połączone jest z prawem modyfikacji wszystkimi obiektami znajdującymi się wewnątrz kontenera.
- przyznanie uprawnień do zarządzania czyli możliwość tworzenia, modyfikowania i usuwania obiektów, którymi mogą być użytkownicy, komputery czy grupy.
- przyznanie uprawnień do modyfikacji atrybutów wybranego obiektu, np. zmiana hasła użytkowników

Kontrolę można przekazać korzystając z kreatora delegowanie kontroli **Delegation of Control Wizard** dostępnego w konsoli **Active Directory Users and Computers**. W celu wywołania kreatora, należy wybrać z menu kontekstowego wybranej jednostki organizacyjnej polecenie **Delegate Control** a następnie wskazać użytkownika lub grupę, dla której wykonujemy akcję, wybrać z listy zadanie, jakie pozwolimy wykonywać i określić, czy będzie to dotyczyło wszystkich obiektów w jednostce czy tylko wybranych. Jeżeli chcemy nadać dodatkowe, specjalne uprawnienia niedostępne w kreatorze bądź zweryfikować nadane uprawnienia należy czynność tą wykonać bezpośrednio na obiekcie. Dlatego w tym celu klikamy w menu **Active Directory Users and Computers** przycisk **View** i wybieramy **Advanced Features.** Należy pamiętać, że chcąc skorzystać z delegowania kontroli administracyjnej należy być członkiem grupy **Account Operators**, **Domain Admins**, lub **Enterprise Admins**



Rysunek 3 Delegowanie kontroli

Tworzenie, modyfikacja i usuwanie OU z wiersza poleceń.

Tworzenie OU z wiersza poleceń polega na uruchomieniu polecenia:

dsadd ou *nazwa_wyróżniająca_jednostki_organizacyjnej* [**-desc** *opis*] [{**-s** *serwer* | **-d** *domena*}][**-u** *nazwa_użytkownika*] [**-p** {*hasło* | *}] [**-q**] [{**-uc** | **-uco** | **-uci**}]

Parametry

nazwa_wyróżniająca_jednostki_organizacyjnej

Wymagana. Określa nazwę wyróżniającą jednostki organizacyjnej, którą należy dodać. Jeżeli pominięto nazwę wyróżniającą, nazwa zostanie pobrana z wejścia standardowego (stdin).

-desc *opis*

Określa opis jednostki organizacyjnej, którą należy dodać.

{-s *serwer* | -d *domena*}

Ustanawia połączenie z określonym serwerem zdalnym lub z domeną. Domyślnie komputer jest łączony z kontrolerem domeny w domenie logowania.

-u *nazwa_użytkownika*

Określa nazwę użytkownika używaną do logowania na serwerze zdalnym. Domyślnie używana jest nazwa zalogowanego użytkownika. Nazwę użytkownika można określić przy użyciu jednego z następujących formatów:

- nazwa_użytkownika (na przykład Linda)
- domena\nazwa_użytkownika (na przykład widgets\Linda)
- nazwa_główna_użytkownika (UPN) (na przykład Linda(at)widgets.microsoft.com)

-p {*hasło* | *}

Określa, że do logowania na serwerze zdalnym należy używać hasła lub znaku *. Jeżeli zostanie wpisany znak *, zostanie wyświetlony monit o podanie hasła.

-q

Pomija wszystkie dane wyjściowe przekazywane do wyjścia standardowego (tryb cichy).

{-uc | -uco | -uci}

Określa, że dane wyjściowe lub wejściowe są formatowane zgodnie ze standardem Unicode. Następująca tabela zawiera listę i opisy poszczególnych formatów.

-uc Określa format Unicode dla danych wejściowych pobieranych z potoku lub danych wyjściowych przekazywanych do potoku (|).

-uco Określa format Unicode dla danych wyjściowych przekazywanych do potoku (|) lub pliku.

-uci Określa format Unicode dla danych wejściowych pobieranych z potoku (|) lub pliku.

/?

Powoduje wyświetlenie Pomocy w wierszu polecenia.

Spostrzeżenia

- Jeżeli w wierszu polecenia nie określono obiektu docelowego, obiekt docelowy jest pobierany z wejścia standardowego (stdin). Dane stdin mogą być pobierane z klawiatury, przekierowanego pliku lub jako dane wyjściowe innego polecenia przekazywane w potoku. Aby oznaczyć koniec danych stdin z klawiatury lub w przekierowanym pliku, należy użyć znaku końca pliku (CTRL+Z).
- Jeżeli podana wartość zawiera spacje, tekst należy ująć w cudzysłowy (na przykład "OU=Kontrolery domen, DC=Microsoft,DC=Com").
- To polecenie obsługuje tylko najczęściej używane atrybuty klas obiektów.

Modyfikacja OU z wiersza poleceń polega na uruchomieniu polecenia:

dsmod ou *nazwa_wyróżniająca_jednostki_organizacyjnej* [**-desc** *opis*] [{**-s** *serwer* |**-d** *domena*}] [**-u** *nazwa_użytkownika*] [**-p** {*hasło* | *}][**-c**] [**-q**] [{**-uc** | **-uco** | **-uci** }]

Przykład

Aby zmienić opis kilku jednostek organizacyjnych jednocześnie, należy wpisać:

dsmod ou "OU=Kontrolery domen,DC=Microsoft,DC=Com" "OU=Zasoby,DC=Microsoft,DC=Com" "OU=Rozwiązywanie problemów,DC=Microsoft,DC=Com" -desc "To jest test jednostki organizacyjnej"

Usuwanie OU z wiersza poleceń polega na uruchomieniu polecenia dsrm

dsrm *nazwa_wyróżniająca_obiektu ...* [**-subtree** [**-exclude**]] [**-noprompt**] [{**-s** *serwer* | **-d** *domena*}] [**-u** *nazwa_użytkownika*] [**-p** {*hasło* | *}][**-c**][**-q**][{**-uc** | **-uco** | **-uci**}]

Parametry

nazwa_wyróżniająca_obiektu ...

Wymagany. Określa nazwy wyróżniające obiektów, które należy usunąć. Jeżeli żadna wartość nie zostanie wprowadzona w wierszu polecenia, wartość zostanie uzyskana za pośrednictwem wejścia standardowego.

-subtree [-exclude]

Określa, że zarówno dany obiekt, jak i wszystkie obiekty w poddrzewie poniżej danego obiektu powinny być usunięte. Parametr **-exclude** może być określony tylko razem z parametrem **-subtree** w celu wskazania, że obiekt podstawowy określony przez parametr *nazwa_wyróżniająca_obiektu* nie powinien być usuwany podczas usuwania poddrzewa znajdującego się poniżej tego obiektu. Domyślnie tylko określony obiekt podstawowy jest usuwany.

-noprompt

Ustawia opcjonalny tryb cichy, w którym nie są wyświetlane monity o potwierdzenie usunięcia każdego obiektu. Domyślnie wyświetlane są monity o potwierdzenie każdej operacji usunięcia obiektu.

{-s*serwer*| -d*domena*}

Ustanawia połączenie z określonym serwerem zdalnym lub z domeną. Domyślnie komputer jest łączony z kontrolerem domeny w domenie logowania.

-u *nazwa_użytkownika*

Określa nazwę użytkownika używaną do logowania na serwerze zdalnym. Domyślnie w parametrze **-u** jest stosowana nazwa użytkownika, która została użyta do zalogowania danego użytkownika. Nazwę użytkownika można określić przy użyciu jednego z następujących formatów:

-p {*hasło* | *}

Określa, że należy używać hasła lub znaku * do logowania na serwerze zdalnym. Jeżeli zostanie wpisany znak *, zostanie wyświetlony monit o podanie hasła.

-c

Zgłasza błędy, ale kontynuuje przetwarzanie następnego obiektu na liście argumentów, gdy jest określonych wiele obiektów docelowych (tryb działania ciągłego). Bez tej opcji wykonywanie polecenia jest przerywane po napotkaniu pierwszego błędu.

-q

Pomija wszystkie dane wyjściowe przekazywane do wyjścia standardowego (tryb cichy).

{-uc | -uco | -uci}

Określa, że dane wyjściowe lub wejściowe są formatowane zgodnie ze standardem Unicode.

Przykłady

Aby usunąć jednostkę organizacyjną o nazwie "Marketing" i wszystkie obiekty należące do danej jednostki organizacyjnej, należy wpisać:

dsrm -subtree -noprompt -c OU=Marketing,DC=Microsoft,DC=Com

Aby usunąć wszystkie obiekty należące do jednostki organizacyjnej o nazwie "Marketing", ale pozostawić jednostkę organizacyjną bez zmian, należy wpisać:

dsrm -subtree -exclude -noprompt -c "OU=Marketing,DC=Microsoft,DC=Com"

Download Media File

Przykład tworzenia jednostek organizacyjnych

Konto użytkownika

Konta użytkowników w **Active Directory** przypisujemy osobą, którym chcemy dać możliwość korzystania z naszej domeny czyli mogą to być np. pracownicy jakiejś danej firmy. Inną możliwością jest również przypisanie konta użytkownika pozwalające na uruchomienie zdefiniowanej przez nas aplikacji. Konto użytkownika zawiera unikalne dane, które pozwalają na jego uwierzytelnienie oraz umożliwiają użytkownikowi dostęp do zasobów (zalogowanie się do domeny lub korzystanie z komputera lokalnego). Konto użytkownika powinno być zdefiniowane dla każdej osoby, korzystającej regularnie z sieci lub z komputera. Dzięki posiadaniu konta, użytkownik może zalogować się do komputera lub do domeny. Dane, wykorzystane w procesie logowania, służą do kontroli dostępu do zasobów. Konto użytkownika jest również podmiotem zabezpieczeń, dzieje się tak ponieważ do konta jest przypisany identyfikator zabezpieczeń (**SID**), wymagany do udostępnienia zasobów sieciowych danej domeny. Jedne z głównych zastosowań kont użytkowników to :

- sprawdzenie tożsamości użytkownika - czyli proces logowania się przy użyciu danego konta użytkownika.
- pozwolenie na dostęp do zasobów sieciowych - po procesie sprawdzenia tożsamości, następuje proces kontroli nadanych uprawnień i określenie czy dany użytkownik ma prawo do korzystania z zasobu czy też dostęp do niego jest zabroniony.

Istnieją trzy typy kont użytkownika:

a. **Lokalne konto użytkownika**. Konto to pozwala na zalogowanie się do określonego komputera i uzyskanie dostępu do zasobów tego komputera. Użytkownik może mieć dostęp do zasobów innego komputera, jeśli posiada na nim oddzielne konto. Konta użytkowników przechowywane są w bazie **SAM** (**Security Accounts Manager**) na komputerze lokalnym.
b. **Domenowe konto użytkownika**. Pozwala na zalogowanie się do domeny i uzyskanie dostępu do zasobów sieciowych. Konta takie można tworzyć w sieci Microsoft Windows. Użytkownik może uzyskać dostęp do zasobów sieci z dowolnego komputera, posługując się wyłącznie swoją, pojedynczą nazwą użytkownika i hasłem. Konta takie są przechowywane w bazie usługi **Active Directory** na kontrolerze domeny.
c. **Wbudowane konta użytkownika**. Pozwalają na wykonywanie zadań administratorskich lub uzyskanie tymczasowego dostępu do zasobów. Istnieją trzy wbudowane konta, znajdujące się w kontenerze **Users,** w przystawce **Active Directory Users and Computers,** których usunięcie nie jest możliwe (aczkolwiek możliwe jest ich wyłączenie):

- **Administrator** - konto posiadające pełną kontrolę w domenie, nie może być skasowane ale jest możliwość wyłączenia go oraz zmiany domyślnej nazwy. Uwierzytelnienie za pomocą konta **Administrator** mamy możliwość wpływania na wszystkie obiekty istniejące w naszej domenie a w szczególności możemy definiować prawa użytkownikom i kontrolować ich uprawnienia dostępu do zasobów. Nie trzeba chyba tłumaczyć, że konto to powinno być chronione silnym hasłem i że wskazane jest by używać tego konta tylko do zadań wymagających uprawnień administratora. Konto **Administrator** jest domyślnie członkiem wbudowanych grup w **AD**: **Administrators**, **Domain Admins (Administratorzy domeny)**, **Enterprise Admins (Administratorzy przedsiębiorstwa)**, **Group Policy Creator Owners (Twórcy właściciele zasad grupy)**, i **Schema Admins (Administratorzy schematu)**.
- **Guest (Gość)** używane podobnie jak w przypadku logowania lokalnego przez

osoby, które nie posiadają własnego konta z tą różnicą, że tu odbywa się wszystko w domenie. Konto **Gość** nie wymaga hasła. Prawa i uprawnienia dla konta **Gość** można ustawiać w taki sam sposób, jak dla dowolnego innego konta użytkownika. Domyślnie konto **Gość** jest członkiem grupy wbudowanej **Guests (Goście)** i grupy globalnej **Domain Guests(Goście domeny**). Domyślnie konto **Gość** jest wyłączone i nie zaleca się włączania go.

- **HelpAssistant (Pomocnik)** (instalowane z sesją **Remote Assistence**). Główne konto do zestawienia sesji **Remote Assistance**, tworzone automatycznie w momencie, gdy zażądamy takiej sesji. Ma ograniczony dostęp do komputera. Konto **HelpAssistance** jest zarządzane przez usługę **Remote Desktop Help session Manager**. Jest kasowane automatycznie jeśli nie ma oczekujących żądań **Remote Assistance**

Konta wbudowane są często wykorzystywane do nieuprawnionego zalogowania się do domeny. Dlatego by ograniczyć prawdopodobieństwo nieautoryzowanego dostępu można zmienić im prawa i uprawnienia, dobrą praktyką jest ich wyłączenie lub zmiana ich nazwy. Zmieniając nazwę konta zachowywujemy ich **SID**, czyli zachowane są wszelkie własności tego konta takie jak opis, hasło, przynależność do grup, profil i wszystkie przypisane prawa i uprawnienia. Aby uzyskać korzyści zabezpieczeń autentykacji i autoryzacji użytkownika, należy stworzyć indywidualne konta dla wszystkich użytkowników korzystających z sieci. Tak utworzone konta użytkowników można łączyć w grupy i dopiero grupą dodawać poszczególne uprawnienia. Kolejną linią obrony naszej domeny jest wymuszenie stosowania silnych haseł (domyślnie włączone) oraz stosowanie limitu możliwych prób logowań. Odpowiednio skomplikowane hasło redukuje możliwość jego odgadnięcia lub pomyślnego ataku słownikowego. Zasady blokowania hasła ograniczają atakującemu możliwość powtarzanie kolejnych nieudanych prób logowania.

Każde konto użytkownika w **Active Directory** posiada kilka opcji określających jak przebiegnie logowanie i autentykacja w sieci. Poniżej znajdują się ustawienia związane z konfiguracją hasła i specyficznymi informacjami związanymi z bezpieczeństwem kont użytkowników. Administrator systemów może zarządzać opcjami haseł kont użytkowników. Te opcje można konfigurować podczas tworzenia konta użytkownika lub w oknie dialogowym **Właściwości konta użytkownika**.

User must change password at next logon (**Użytkownik musi zmienić hasło przy następnym logowaniu).** Ta opcja jest używana wówczas, gdy nowy użytkownik loguje się do systemu po raz pierwszy lub w przypadku resetowania zapomnianych haseł przez administratora na żądanie użytkowników.

User cannot change password (Użytkownik nie może zmienić hasła). Z tej opcji należy korzystać wówczas, gdy konieczne jest kontrolowanie zmian hasła konta użytkownika. Opcja używana, kiedy administrator zarządza jakimś kontem np. kontem gościa lub tymczasowym.

Password never expires (Hasło nigdy nie wygasa). Korzystając z tej opcji, można zapobiegać wygaśnięciu hasła. Aby zapewnić najlepszą ochronę, należy zrezygnować z korzystania z tej opcji.. Ustawienie rekomendowane dla kont używanych przez usługi posiadających mocne hasło

Store password using reversible encryption (Zapisz hasła, korzystając z szyfrowania

odwracalnego) Umożliwia zalogowanie się do sieci Windows użytkownikom komputerów Apple.

Account is disabled (Konto jest wyłączone). Korzystając z tej opcji, można zapobiegać logowaniu użytkowników przy użyciu danego konta. Nie zezwala na zalogowanie się przy użyciu tego konta. Używane dla kont będących szablonami lub dla użytkowników, którzy nie będą dłuższy czas korzystać z niego.

Smart Card is required for interactive logon (Logowanie interakcyjne wymaga karty inteligentnej) - Wymaga, aby w przypadku interakcyjnego logowania się do sieci użytkownik używał karty inteligentnej. W przypadku wybrania tej opcji automatycznie jest generowane losowe i złożone hasło dla konto użytkownika, a ponadto zostaje ustawiona opcja Hasło nigdy nie wygasa.

Konto jest zaufane w kwestii delegowania - Umożliwia usłudze uruchamianej przy użyciu tego konta wykonywanie operacji w imieniu innych kont użytkowników w sieci. Usługa uruchomiona przy użyciu konta użytkownika (nazywanego kontem usługi), które jest zaufane w kwestii delegowania, może przyjąć tożsamość klienta, aby uzyskać dostęp do zasobów na komputerze, na którym jest uruchomiona, lub na innych komputerach.

Account is sensitive and cannot be delegated (Konto jest poufne i nie może być delegowane) - Daje kontrolę nad kontem użytkownika, na przykład kontem gościa lub kontem tymczasowym. Tej opcji można użyć, jeśli konto nie powinno być delegowane przez inne konto.

Use Kerberos DES encryption types for this account (Użyj typów szyfrowania DES dla tego konta) - Zapewnia obsługę szyfrowania DES.

Do not require Kerperos preauthentication (Nie jest wymagane wstępne uwierzytelnienie protokołu Kerberos) - Zapewnia obsługę alternatywnych implementacji protokołu Kerberos. Kontrolery domeny z systemem Windows 2000 lub Windows Server 2003 mogą korzystać z innych mechanizmów synchronizowania czasu. Wstępne uwierzytelnianie jest dodatkowym zabezpieczeniem, więc włączając tę opcję, należy zachować ostrożność.

Przed tworzeniem kont użytkowników należy przyjąć dla nich konwencję nazewniczą. Ustala ona sposób identyfikacji kont w domenie. Powinna ona uwzględniać konta użytkowników o takich samych nazwiskach oraz konta tymczasowe.

Konwencja nazewnictwa

Z kontami użytkowników domeny skojarzone są cztery typy nazw. W usłudze Active Directory dla każdego konta użytkownika określona jest nazwa logowania użytkownika, nazwa logowania użytkownika dla systemów starszych niż Windows 2000 (nazwa konta Menedżera kont zabezpieczeń), nazwa główna logowania użytkownika oraz względna nazwa wyróżniająca LDAP (Lightweight Directory Access Protocol).

Nazwę logowania użytkownika - Używa się w procesie logowania do domeny, składa się maks. z 20 znaków. Przykład: jankow. Użytkownicy korzystają z tej nazwy tylko podczas procesu logowania. Użytkownik wprowadza nazwę logowania użytkownika, hasło i nazwę domeny w oddzielnych polach na ekranie logowania. Nazwa może zawierać kombinację znaków specjalnych i alfanumerycznych, z wyjątkiem następujących znaków: " / \ [ ] : ; | = , + * ? <>.

Nazwy domen usługi Active Directory są zazwyczaj pełnymi nazwami DNS domeny. Jednak ze względu na zachowanie zgodności z poprzednimi wersjami każda domena ma również nazwę dla systemów starszych niż Windows 2000 (używaną przez komputery z systemem operacyjnym starszym niż Windows 2000). Nazwy domeny dla systemu starszego niż Windows 2000 można używać do logowania się w domenie systemu Windows Server z komputerów z systemem operacyjnym starszym niż Windows 2000, używając formatu NazwaDomeny\NazwaUżytkownika. Nazwa logowania systemu starszego niż Windows 2000 musi być unikatowa w domenie. Użytkownicy mogą korzystać z tej nazwy logowania w poleceniu Uruchom jako lub na pomocniczym ekranie logowania.

Przykład: firma.com\jankow

Użytkownicy mogą również logować się do komputerów za pomocą nazwy głównej użytkownika (UPN) skojarzonej z kontem użytkownika. Administrator wprowadza nazwę logowania użytkownika i wybiera sufiks UPN podczas tworzenia konta użytkownika. Nazwa UPN składa się z nazwy logowania użytkownika i sufiksu UPN połączonych znakiem @. Nie należy dodawać znaku @ do nazwy logowania użytkownika ani do sufiksu UPN. Usługa Active Directory dodaje go automatycznie podczas tworzenia nazwy UPN. Nazwa UPN zawierająca więcej niż jeden znak @ jest nieprawidłowa. Nazwa UPN musi być unikatowa w lesie. W domenach systemu Windows NT 4.0 i systemów starszych można było używać kropki (.) na końcu nazwy logowania użytkownika, o ile nazwa ta nie składała się wyłącznie z kropek. W domenach systemu Windows Server 2003 nie można używać kropki ani wielu kropek na końcu nazwy logowania użytkownika. Druga część nazwy UPN, sufiks UPN, identyfikuje domenę, do której należy konto użytkownika. Ten sufiks UPN może być nazwą DNS dowolnej domeny w lesie lub alternatywną nazwą utworzoną przez administratora i używaną tylko do logowania. W usłudze Active Directory domyślny sufiks UPN jest nazwą DNS domeny, w której utworzono konto użytkownika. Przykładowa nazwa UPN użytkownika w takiej domenie mogłaby być następująca: opole.polska.firma.com Nazwa logowania użytkownika w tej domenie miałaby format: użytkownik(at)opole.polska.firma.com. Utworzenie sufiksu UPN "firma" umożliwiłoby temu samemu użytkownikowi logowanie się przy użyciu dużo prostszej nazwy logowania - użytkownik(at)firma.

Każde konto komputera utworzone w usłudze Active Directory ma względną nazwę wyróżniającą. Ta

nazwa komputera jest używana jako względna nazwa wyróżniająca LDAP (Lightweight Directory Access Protocol). Nazwa DNS dla hosta jest nazywana pełną nazwą komputera i jest w pełni kwalifikowaną nazwą domeny (FQDN) DNS. Pełna nazwa komputera jest złączeniem nazwy komputera (pierwsze 15 bajtów nazwy konta Menedżera kont zabezpieczeń (SAM) konta komputera bez znaku $) i podstawowego sufiksu DNS (nazwa DNS domeny, do której należy konto komputera). Jest ona wyświetlana na karcie Nazwa komputera w aplecie Właściwości systemu w Panelu sterowania. Domyślnie podstawowy sufiks DNS nazwy FQDN komputera jest taki sam, jak nazwa domeny usługi Active Directory, do której należy komputer. Np. serwer001.firma.com

Konwencja nazewnictwa określa sposób identyfikowania kont użytkowników w domenie. Spójna konwencja nazewnictwa ułatwia zapamiętanie nazw logowania użytkowników i lokalizowanie ich na listach. Dobrym rozwiązaniem jest przestrzeganie konwencji nazewnictwa używanej już w istniejącej sieci obsługującej dużą liczbę użytkowników.

Uwzględnij następujące wskazówki dotyczące tworzenia konwencji nazewnictwa:

1. W przypadku dużej liczby użytkowników konwencja nazewnictwa, dotycząca nazw logowania użytkowników, powinna uwzględniać zduplikowane nazwiska pracowników. Metoda wykonania tego zadania polega na wykorzystaniu imienia oraz inicjału reprezentującego nazwisko, a następnie dodawaniu kolejnych liter z nazwiska w celu uwzględnienia zduplikowanych nazwisk. Na przykład w przypadku dwóch użytkowników o nazwisku Jan Kowalski, można utworzyć nazwy logowania Jank i Janko.
2. W niektórych organizacjach użytecznym rozwiązaniem jest identyfikowanie pracowników tymczasowych przy użyciu ich kont użytkowników. W tym celu można dodać prefiks do nazwy logowania użytkownika, taki jak T i łącznik. Przykład: T-Jank.
3. Nazwy logowania użytkowników w przypadku kont użytkowników domeny muszą być unikatowe w usłudze Active Directory. Pełne nazwy kont użytkowników domeny muszą być unikatowe w domenie, w której jest tworzone konto użytkownika.

Hasła

- Słabe hasło:

- W ogóle nie jest hasłem.

- Zawiera nazwę użytkownika, imię, nazwisko lub nazwę firmy.

- Zawiera cały wyraz słownikowy. Na przykład **hasło** jest słabym hasłem.

- Silne hasło:

- Ma co najmniej siedem znaków długości.

- Nie zawiera nazwy użytkownika, imienia, nazwiska ani nazwy firmy.

- Nie zawiera całego wyrazu słownikowego.

- Różni się znacznie od poprzednich haseł. Hasła tworzone na zasadzie wyliczanki (Hasło1,

Hasło2, Hasło3...) nie są silne.

- Zawiera znaki z każdej z czterech następujących grup:

  Wielkie litery: A, B, C...

  Małe litery: a, b, c...

  Cyfry: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9

  Symbole występujące na klawiaturze (wszystkie znaki na klawiaturze niezdefiniowane jako litery lub cyfry): **` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /**

- Hasło może spełniać większość kryteriów dotyczących silnego hasła i pozostać dość słabym hasłem np.:

- Hasło **Dzis3maja!** jest stosunkowo słabym hasłem, choć spełnia większość kryteriów silnego hasła, a także wymogi złożoności opisane w zasadach haseł.

- Hasło **D!z+i|s3Ma?j** jest silnym hasłem, ponieważ wyraz słownikowy przeplata się z symbolami, liczbami i innymi literami.

- Można tworzyć hasła z wykorzystaniem znaków z rozszerzonego zestawu ASCII np.: **kU?!?0o** i **Wfc$0k#?g.5ard**.
- Można skonfigurować ustawienia zasady haseł tak, aby wymagane były hasła o określonej złożoności.

Download Media File

Wyłączenie wymagań co do złożoności hasła

Download Media File

Próg logowania

Żądanie zmian haseł należy używać przy tworzeniu nowych kont użytkowników domeny poprzez zaznaczenie pola wyboru w celu wymagania zmiany hasła przez użytkownika w przypadku logowania użytkownika do domeny po raz pierwszy. Zmiana hasła jest też stosowana przy resetowaniu haseł. Korzystając z tej opcji, administrator może resetować hasło, które uległo wygaśnięciu lub zostało zapomniane przez użytkownika.

Natomiast ograniczanie zmian haseł stosujemy przy tworzeniu kont usług lokalnych lub kont usług domeny. Dla kont usług zazwyczaj określanych jest wiele zależności. Konieczne może więc być ograniczenie zmian haseł i zezwolenie na zmianę haseł tylko administratorowi odpowiedzialnemu za

aplikacje zależne od konta usługi. Ograniczenie stosowane też jest przy tworzeniu nowych kont lokalnych, które nie będą używane do lokalnego logowania.

Profile użytkownika

W systemie Windows Serwer środowisko pracy użytkownika określane jest przez profil użytkownika. Profil ten ustawiamy na **Karcie Profil**, która jest zawarta we właściwościach użytkownika, pełni jedną z ważniejszych funkcji przy konfigurowaniu konta. Znajduje się na niej miejsce na ustawienia obejmujące profile, katalogi domowe oraz skrypty logowania. W profilu użytkownika zawarte są wszystkie ustawienia, które użytkownik może zdefiniować w środowisku systemu Windows. Uwzględnia preferencje związane ze sprzętem (mysz, klawiatura), pulpitem, menu Start i Programy itp. Profile są tworzone w czasie pierwszego logowania użytkownika do stacji roboczej (domyślnie jest to folder C:/Documents and Settings/Nazwa użytkownika). Domyślnie są tam również przechowywane. Dzięki temu użytkownicy po modyfikacji swoich preferencji, takich jak np. przystosowanie myszy dla leworęcznych, mogą z nich korzystać po każdorazowym zalogowaniu do komputera. Jeśli ktoś zmieni miejsce pracy, w nowym systemie będzie musiał ustawiać swoje parametry od początku. W Windows Server 2003, podobnie jak w Windows NT i 2000, można skonfigurować profile mobilne. Dzięki ich zastosowaniu zmiana komputera nie zmusza użytkownika do rekonfiguracji systemu. Opcja ta jest możliwa, ponieważ profile nie są przechowywane lokalnie, lecz na serwerze. Podczas logowania do sieci profil jest pobierany z serwera, a podczas wylogowywania jest na nim zapisywany.

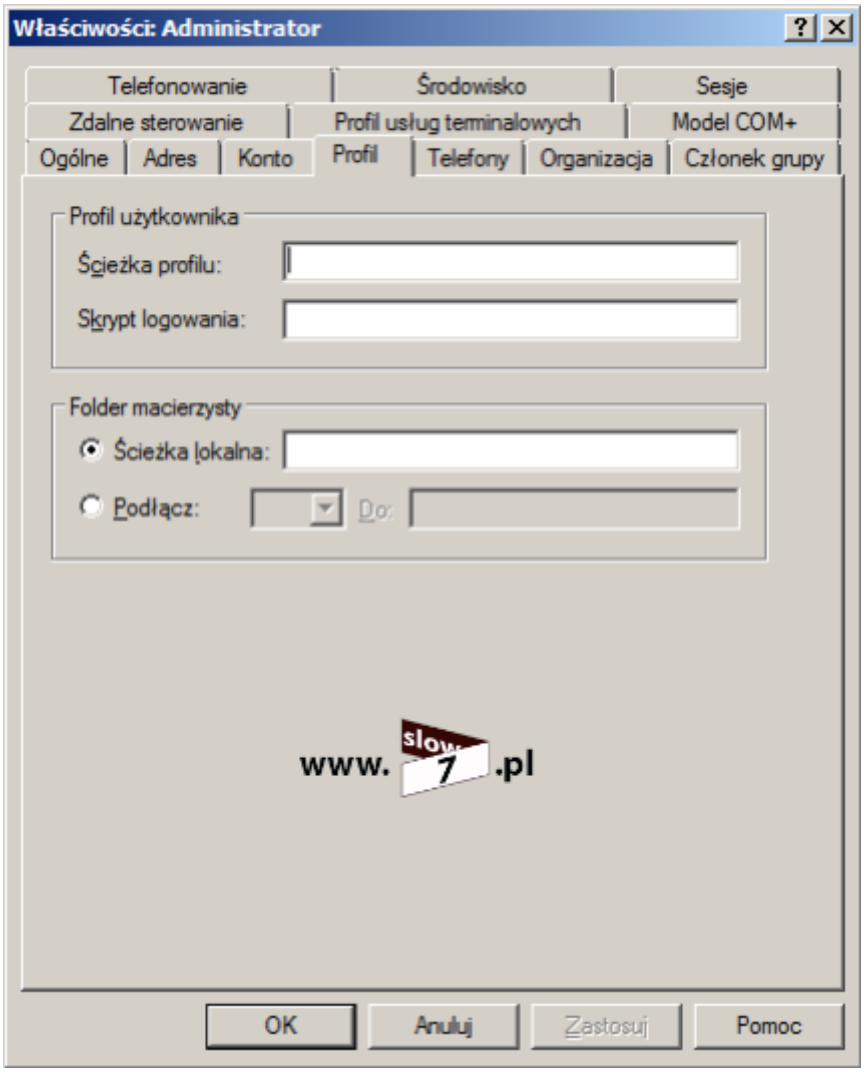
Wyróżniane są następujące profile użytkownika:

a) **Domyślny profil użytkownika**. Służy jako podstawowy profil dla wszystkich użytkowników. Każdy profil jest początkowo kopią domyślnego profilu przechowywanego na komputerze pracującym z systemem Windows.

b) **Lokalny profil użytkownika**. Tworzony jest w chwili pierwszego logowania do komputera i przechowywany jest lokalnie. Wszystkie zmiany dokonane w tym profilu są zapisywane na komputerze, na którym zostały wykonane. Na jednym komputerze może istnieć wiele profili lokalnych obsługujących wielu użytkowników.

c) **Mobilny profil użytkownika**. Tworzony jest przez administratora i przechowywany na serwerze. Profil ten jest dostępny z dowolnego komputera, do którego loguje się użytkownik. Wszelkie zmiany w profilu zapisywane są na serwerze w chwili wylogowywania.

d) **Obowiązkowy profil użytkownika**. Tworzony jest przez administratora. Zdefiniowane są w nim określone ustawienia użytkownika lub użytkowników. Może to być profil lokalny lub wędrujący. Profil obowiązkowy nie pozwala na zapisanie żadnych zmian dokonanych przez użytkowników. Użytkownicy mogą zmieniać ustawienia profilu po zalogowaniu się, ale podczas wylogowywania się żadne zmiany nie zostaną zapisane.



Rysunek 4 Karta Profil

Na **karcie Profil** znajduje się pole służące do wpisywania, skąd system ma pobierać profil użytkownika. W ścieżce do profilu należy podać lokalizację folderu z profilem. Ścieżkę wprowadzamy zgodnie ze składnią UNC (Universal Naming Convention). Obejmuje ona nazwę serwera oraz nazwę udostępnienia, zapisane w formie \\nazwa_serwera\nazwa_udostępnienia. Na końcu ścieżki powinniśmy wprowadzić nazwę logowania użytkownika lub zmienną %UserName%. Wpisanie zmiennej jest przydatne, jeśli ustawiamy parametry profili wielu użytkowników i nie możemy jawnie podać ich nazwy. %UserName% zostanie automatycznie zamienione na nazwę konta. Po wpisaniu ścieżki i naciśnięciu przycisku OK system skonfiguruje również odpowiednie uprawnienia do folderów każdego z użytkowników. Jest to możliwe pod warunkiem, że partycja, na której przechowywane są profile, wykorzystuje system plików NTFS.

Jak przekształcić domyślny profil użytkownika w sieciowy domyślny profil użytkownika w systemach Windows 7 i Windows Server 2008 R2

1. Zaloguj się do komputera, na którym znajduje się dostosowany domyślny profil użytkownika, używając konta z uprawnieniami administracyjnymi.

2. Za pomocą polecenia **Uruchom** nawiąż połączenie z folderem udostępnionym NETLOGON kontrolera domeny. Ścieżka może być na przykład podobna do następującej: \\<*nazwa_serwera*>\NETLOGON
3. W folderze udostępnionym NETLOGON utwórz nowy folder i nadaj mu nazwę **Użytkownik domyślny**
4. Kliknij przycisk **Uruchom** w menu Start, kliknij prawym przyciskiem myszy polecenie **Komputer**, kliknij polecenie **Właściwości**, a następnie kliknij pozycję **Zaawansowane ustawienia systemu**.
5. W obszarze **Profile użytkownika** kliknij pozycję **Ustawienia**. Okno dialogowe **Profile użytkownika** zawiera listę profilów przechowywanych na komputerze.
6. Zaznacz pozycję **Profil domyślny**, a następnie kliknij pozycję **Kopiuj do**.
7. W polu tekstowym **Kopiuj profil do** wpisz ścieżkę sieciową folderu domyślnego profilu użytkownika systemu Windows 7, który utworzono zgodnie z opisem w kroku 3. Można na przykład wpisać następującą ścieżkę: \\<*nazwa_serwera*>\NETLOGON\Użytkownik domyślny
8. W obszarze **Pozwolenie na używanie** kliknij pozycję **Zmień**, wpisz nazwę Wszyscy, a następnie kliknij przycisk **OK**.
9. Kliknij przycisk **OK**, aby rozpocząć kopiowanie profilu.
10. Po zakończeniu procesu kopiowania wyloguj się z komputera.

Jak przekształcić domyślny profil użytkownika w obowiązkowy profil użytkownika w systemach Windows 7 i Windows Server 2008 R2

Domyślny lokalny profil użytkownika można skonfigurować tak, aby stał się profilem obowiązkowym. Dzięki temu wszyscy użytkownicy będą mogli korzystać z jednego centralnego profilu. Aby to zrobić, należy przygotować lokalizację profilu obowiązkowego, skopiować do niej lokalny domyślny profil użytkownika, a następnie skonfigurować lokalizację profilu użytkownika w taki sposób, aby wskazywała profil obowiązkowy.

Krok 1. Przygotowywanie lokalizacji profilu obowiązkowego

a. Na centralnym serwerze plików utwórz nowy folder lub wybierz istniejący folder używany do przechowywania profilów użytkowników mobilnych. Możesz na przykład użyć następującej nazwy folderu: \Profile

b. W przypadku tworzenia nowego folderu udostępnij ten folder, używając nazwy odpowiedniej dla danej organizacji.

> **Uwaga** Uprawnienia udziału, które dotyczą folderów udostępnionych zawierających profile użytkowników mobilnych, muszą uwzględniać uprawnienie Pełna kontrola dla grupy **Użytkownicy uwierzytelnieni**. Uprawnienia udziału, które dotyczą folderów służących do przechowywania obowiązkowych profilów użytkowników, powinny uwzględniać uprawnienie Odczyt dla grupy **Użytkownicy uwierzytelnieni** oraz uprawnienie Pełna kontrola dla grupy **Administratorzy**.

c. Utwórz nowy folder w folderze, który został utworzony lub wybrany w kroku 1a. Nazwa tego

nowego folderu powinna rozpoczynać się od nazwy logowania dla konta użytkownika, jeśli dany obowiązkowy profil użytkownika dotyczy określonego użytkownika. Jeśli obowiązkowy profil użytkownika jest przeznaczony dla wielu użytkowników, nadaj mu odpowiednią nazwę. W tym przykładzie domena zawiera profil obowiązkowy, a nazwa folderu zaczyna się od wyrazu "obowiązkowy": \Profile\obowiązkowy

d. Na końcu nazwy dodaj ciąg .wersja2. W przykładzie podanym w kroku 1c użyto nazwy folderu "obowiązkowy". Dlatego ostateczna nazwa folderu dla danego użytkownika będzie miała postać "obowiązkowy.wersja2": \Profile\obowiązkowy.wersja2

Krok 2. Kopiowanie domyślnego profilu użytkownika do lokalizacji profilu obowiązkowego

a. Zaloguj się do komputera, na którym znajduje się dostosowany lokalny domyślny profil użytkownika, używając konta z uprawnieniami administracyjnymi.

b. Kliknij przycisk **Uruchom** w menu Start, kliknij prawym przyciskiem myszy polecenie **Komputer**, kliknij polecenie **Właściwości**, a następnie kliknij pozycję **Zaawansowane ustawienia systemu**.

c. W obszarze **Profile użytkownika** kliknij pozycję **Ustawienia**. Zostanie wyświetlone okno dialogowe **Profile użytkownika** z listą profilów przechowywanych na komputerze.

d. Zaznacz pozycję **Profil domyślny**, a następnie kliknij pozycję **Kopiuj do**.

e. W polu tekstowym **Kopiuj profil do** wpisz ścieżkę sieciową domyślnego folderu użytkownika systemu Windows 7, który utworzono zgodnie z opisem w sekcji "Krok 1. Przygotowywanie lokalizacji profilu obowiązkowego". Możesz na przykład wpisać następującą ścieżkę:

\\<*nazwa_serwera*>\Profile\obowiązkowy.wersja2

f. W obszarze **Pozwolenie na używanie** kliknij pozycję **Zmień**, wpisz nazwę Wszyscy, a następnie kliknij przycisk **OK**.

g. Kliknij przycisk **OK**, aby rozpocząć kopiowanie profilu.

h. Po zakończeniu procesu kopiowania wyloguj się z komputera.

i. Na centralnym serwerze plików zlokalizuj folder utworzony zgodnie z opisem w sekcji "Krok 1. Przygotowywanie lokalizacji profilu obowiązkowego".

j. Kliknij pozycję **Organizuj**, a następnie kliknij pozycję **Opcje folderów**.

k. Kliknij kartę **Widok**, zaznacz pole wyboru **Pokaż ukryte pliki i foldery**, wyczyść pole wyboru **Ukryj rozszerzenia znanych typów plików**, wyczyść pole wyboru **Ukryj chronione pliki systemu operacyjnego**, kliknij przycisk **Tak**, aby zamknąć okno z ostrzeżeniem, a następnie kliknij przycisk **OK**, aby zastosować zmiany i zamknąć okno dialogowe.

l. Zlokalizuj i kliknij prawym przyciskiem myszy plik NTUSER.DAT, kliknij polecenie **Zmień nazwę**, zmień nazwę pliku na NTUSER.MAN, a następnie naciśnij klawisz ENTER.

Uwaga Do tej pory można było kopiować profile za pośrednictwem apletu System w Panelu sterowania. Obecnie nie ma możliwości kopiowania do profilu domyślnego, ponieważ mogło to powodować dodawanie danych uniemożliwiających korzystanie z profilu.

Krok 3. Przygotowywanie konta użytkownika

a. Jako administrator domeny otwórz konsolę administracyjną Użytkownicy i komputery usługi **Active Directory** na komputerze z systemem Windows Server 2008 R2 lub Windows Server 2008.

b. Kliknij prawym przyciskiem myszy konto użytkownika, do którego zastosować obowiązkowy profil użytkownika, a następnie kliknij polecenie **Właściwości**.

c. Kliknij kartę **Profil**, a następnie w polu tekstowym ścieżki profilu wpisz ścieżkę sieciową utworzoną zgodnie z opisem w sekcji "Krok 1. Przygotowywanie lokalizacji profilu obowiązkowego". Nie dodawaj jednak ciągu ".wersja2" na końcu. W tym przykładzie ścieżka powinna mieć następującą postać: \\<*nazwa_serwera*>\Profile\obowiązkowy

d. Kliknij przycisk **OK**, a następnie zamknij konsolę administracyjną Użytkownicy i komputery usługi **Active Directory**.

Od tej chwili użytkownik będzie mógł korzystać z dostosowanego profilu obowiązkowego.

Zawartość **karty Profil** nie ogranicza się do ustawień związanych z profilami użytkowników. W tym miejscu możemy skonfigurować jeszcze dwie istotne właściwości konta: **skrypt logowania** i **ścieżka do folderu domowego użytkownika**.

Konfiguracja skryptu na karcie profilu użytkownika to pozostałość po systemie Windows NT. Możemy określić lokalizację skryptów przetwarzanych podczas logowania do domeny. Obecnie bardziej elastyczne rozwiązanie oferują Zasady grupy, które pozwalają na skonfigurowanie skryptów logowania, wylogowania użytkownika oraz startu i zamykania systemu operacyjnego. Nie oznacza to, że opcja **Skrypt logowania** jest całkowicie zbędna. Należy ją stosować wtedy, gdy klientami sieciowymi są komputery ze starszymi systemami operacyjnymi, takimi jak Windows 98 lub NT Workstation, oraz gdy przypisanie **Zasad grupy** nie spełnia wymagań administratora. Konfiguracja jest bardzo prosta, wystarczy napisać odpowiedni skrypt, następnie na **karcie Profil** umieścić jego nazwę, np. Logon.bat. W przeciwieństwie do profilu nie podajemy ścieżki, a jedynie nazwę. Skrypt należy zapisać w folderze katalog_główny_systemu\SYSVOL\sysvol\nazwa_domeny\scripts. Jako parametr katalog_główny_systemu z reguły podajemy Windows, a jako nazwę domeny - jej DNS-ową nazwę, np. firma.com. W nazwie katalogu głównego tkwi pewnego rodzaju pułapka, na którą warto zwrócić uwagę. Poprzednie systemy serwerowe, takie jak Windows NT i 2000, domyślnie instalowały się w folderze WINNT, a nie w Windows. Administratorzy przenoszący skrypty ze starszych wersji powinni zwracać uwagę na tę zmianę.

Przykładowy skrypt, który utworzy użytkownika o nazwie "tester", oraz ustawi: komentarz, ustawienia wygasania hasła, folder macierzysty i ścieżkę profilu: mógłby mieć postać:

```
NET USER tester /add /comment:"Przykładowe konto użytkownika"

/expires:never

/homedir:\\zippy\%username%$

/profilepath:\\zippy\profile
```

Jedną z opcji konfiguracji serwera plików jest konfiguracja **folderów macierzystych użytkowników**. Ich głównym zadaniem jest przechowywanie plików klientów sieci. Standardowo dane zapisywane są w folderze Moje dokumenty na komputerach lokalnych. Zaletą takiego rozwiązania jest szybkość zapisu, niezależność i brak obciążenia sieci. Najpoważniejszą wadę stanowi trudność wykonywania kopii zapasowych. Najczęściej stacje robocze nie są wyposażone w sprzęt do sporządzania kopii zapasowych, a jeśli nawet są, to użytkownicy często zaniedbują regularną archiwizację swoich danych. Centralne składowanie dokumentów osobistych umożliwia proste rozwiązanie tego problemu. Za sporządzanie kopii odpowiada administrator, a ponieważ powinien przeprowadzać również archiwizację systemu i aplikacji, jest to tylko dodatkowa partia danych. Zalecane jest również połączenie konfiguracji folderów domowych z narzuceniem Przydziałów dyskowych. Ograniczymy w ten sposób przestrzeń zajmowaną przez użytkowników.

Karta Profil pozwala na określenie położenia folderów macierzystych. Do wyboru mamy ścieżkę lokalną albo podłączenie do udostępnienia sieciowego. Ścieżka lokalna powinna zawierać informacje o lokalizacji folderu na stacji roboczej, np. d:\pliki. Konfiguracja lokalizacji sieciowej wymaga założenia i udostępnienia odpowiedniego katalogu na serwerze. Tak jak w przypadku profili mobilnych, zalecane jest założenie folderu na innej partycji niż systemowa. Przykładowa konfiguracja może wyglądać następująco. Otwieramy Eksplorator Windows. Na danej partycji zaznaczamy katalog, który będzie służył za folder składowania plików i następnie wybieramy menu Plik | Właściwości | Udostępnianie i przenosimy znacznik z Nie udostępniaj tego folderu na Udostępnij ten folder. Klikamy przycisk Uprawnienia. W oknie Uprawnienia, usuwamy grupę Wszyscy i klikając Dodaj, przypisujemy grupie Użytkownicy domeny uprawnienia Zmiana i Odczyt. Dwukrotne naciśnięcie przycisku OK zamyka otwarte okna. Na koniec przechodzimy do narzędzia Użytkownicy i komputery usługi **Active Directory** i wyszukujemy użytkownika, któremu chcemy przypisać folder macierzysty. Otwieramy właściwości użytkownika, wybieramy **kartę Profil** i klikamy Podłącz. Z listy oznaczeń dyskowych wybieramy odpowiadającą nam literę, a w pole Do wprowadzamy ciąg znaków \\nazwa_komputera\udostępniony_katalog\%UserName%. Kliknięcie OK kończy konfigurację folderów macierzystych.

Aby przypisać folder macierzysty z wiersza polecenia można użyć polecenia **net user**. Na przykład wpisz w wierszu polecenia następujące polecenie, a następnie naciśnij klawisz ENTER:

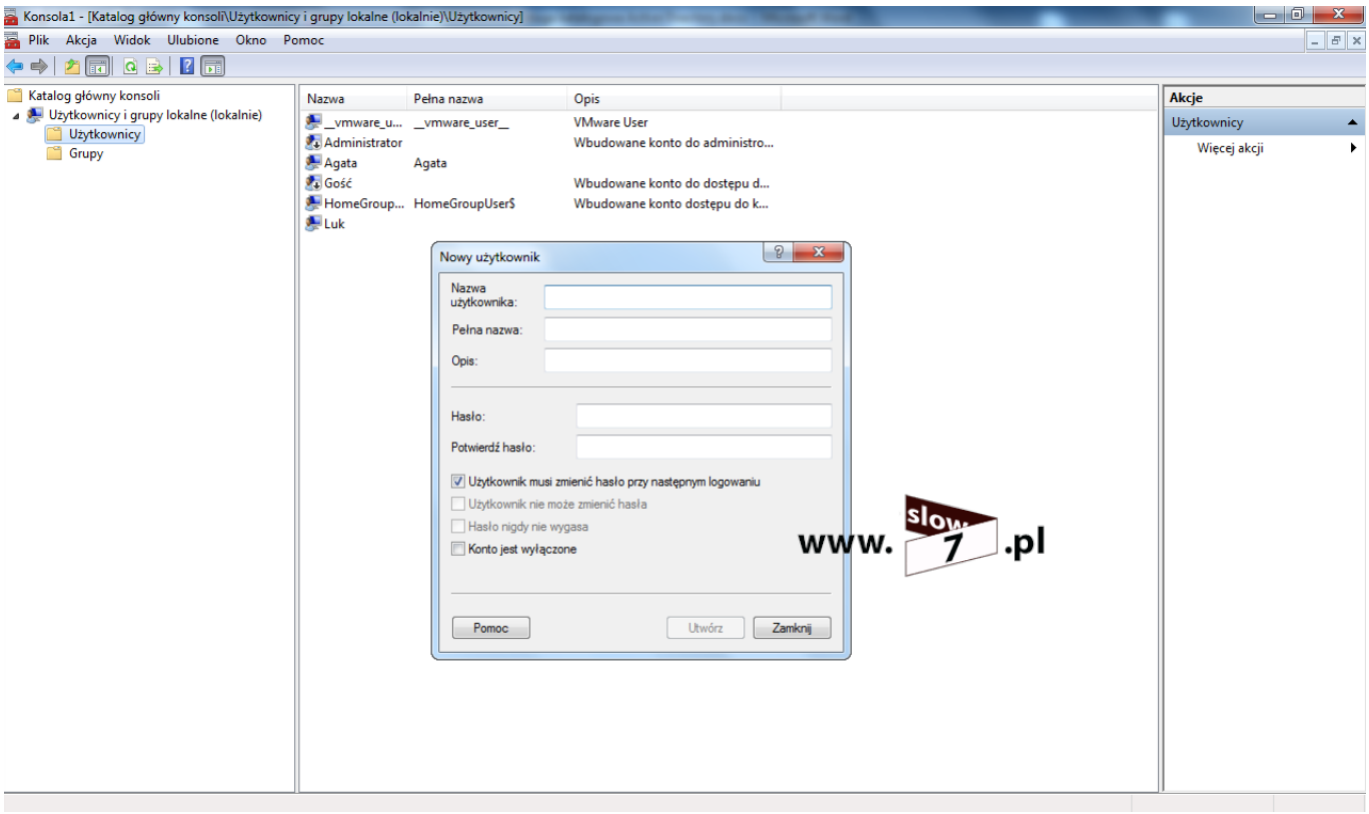
```
net user tester /homedir:\\server\tester$
```

To polecenie przypisuje ukryty udostępniony folder tester$ na serwerze użytkownikowi Tester.

Podobnie jak skrypty tę metodę używamy raczej dla systemów starszych chociaż nic nie stoi na przeszkodzie by stosować ją również dla nowych systemów. Innym rozwiązanie przypisującym foldery macierzyste jest skorzystanie z **Zasad grup** i wykorzystanie **Przekierowania folderów**.

Tworzenie konta lokalnego

Konta lokalne są tworzone na lokalnym komputerze i przechowywane w bazie **SAM** (**Security Accounts Manager**). Mogą być wykorzystywane tylko do logowania na komputerze, na którym zostały stworzone i wykorzystane do nadania praw w systemie i uprawnień do zasobów lokalnych. Konto lokalne tworzymy przy wykorzystaniu przystawki **Local Users and Groups - Użytkownicy i grupy lokalne**, która jest również częścią konsoli **MMC**. Wybierając w kontenerze **Users** polecenie **New User** wypełniamy formularza podając nazwę konta, opis, hasło oraz wypełniając związane z nim opcje.



Rysunek 5 Tworzenie konta lokalnego

Tworzenie konta domenowego

Konto użytkownika domenowego możemy stworzyć przy pomocy przystawki **Active Directory Users and Computers** - **Użytkownicy i Komputery Active Directory** lub przy użyciu narzędzi wiersza poleceń.

Aby utworzyć konto domenowe, należy najpierw otworzyć folder główny - **Użytkownicy i**

Komputery Active Directory, a potem folder właściwej domeny. Następnie prawym przyciskiem myszy kliknąć folder **Użytkownicy** bądź inną dowolną wcześniej utworzoną jednostkę organizacyjną i na otwartej w ten sposób liście wskazać opcje **Nowy**, a potem **Użytkownik**. Otworzy się wówczas okno **Nowy Obiekt** - **Użytkownik**, w którym należy wypełnić pola: "Imię", "Nazwisko", "Inicjały" (opcjonalnie), "Pełna nazwa", "Nazwa logowania" (będzie używana przez użytkownika podczas logowania do domeny), "Nazwa logowania (w systemie starszym niż Windows 2000). Po wypełnieniu

pól wciskamy przycisk **Next**, co spowoduje wyświetlenie okna, w którym nadajemy i konfigurujemy hasło użytkownika. Hasło wpisujemy dwukrotnie w pola "Hasło" i "Potwierdź hasło", przy czym działa tu mechanizm taki sam jak przy nadawaniu hasła użytkownikowi lokalnemu. Następnie w zależności od potrzeb zaznaczamy lub pozostawiamy niezaznaczone następujące opcje nakładające na hasło dodatkowe restrykcje: "Użytkownik musi zmienić hasło przy następnym logowaniu", "Użytkownik nie może zmieniać hasła", "Hasło nigdy nie wygasa" i "Konto jest wyłączone". Opcja "Użytkownik musi zmienić hasło przy następnym logowaniu" unieważnia opcje "Hasło nigdy nie wygasa". Nazwy logowania użytkowników dla kont domenowych muszą być unikalne w usłudze **Active Directory**. Pełne nazwy domenowych kont użytkowników muszą być unikalne w kontenerze, w którym są tworzone.

Tworzenie kont użytkowników za pomocą wiersza poleceń.

Tworzenie kont za pomocą wiersza poleceń jest bardzo szybkim sposobem gdy musimy za jednym zamachem utworzyć wiele kont. Ktoś by pomyślał patrząc na poniższą składnię polecenia **dsadd user** - odpowiedzialnego za dodanie nowego użytkownika, jak to możliwe przecież zanim ja to wpiszę a jeszcze pewnie po drodze się pomylę, to ja dziękuję wolę sobie wyklikać. Tylko pytanie jest takie po co klikać cały dzień zakładając konta dla np. 500 użytkowników na coś co można zrobić w 5 minut. Dobrze czytasz to nie jest pomyłka 500 kont w 5 minut? Już śpieszę się i wyjaśniam. Trzeba zaprząc do pracy starego poczciwego Excela i za pomocą odpowiednich formuł ułożyć składnię polecenia **dsadd user.** Żeby nie być gołosłownym przykładowy plik z ułożoną formułką. A po głowie krążą mi słowa moich uczniów PROSZĘ PANA A PO CO MI SIĘ UCZYĆ TEGO EXCELA? ANO NP PO TO.

dsadd user *nazwa_wyróżniająca_użytkownika* [**-samid** *nazwa_SAM*] [**-upn** *nazwa_główna_użytkownika*] [**-fn** *imię*] [**-mi** *inicjał*] [**-ln** *nazwisko*] [**-display** *nazwa_wyświetlana*] [**-empid** *identyfikator_pracownika*] [**-pwd** {*hasło* | *}] [**-desc** *opis*] [**-memberof** *grupa ...*] [**-office** *biuro*] [**-tel** *numer_telefonu*] [**-email** *adres_e-mail*] [**-hometel** *numer_telefonu_domowego*] [**-pager** *numer_pagera*] [**-mobile** *numer_telefonu_komórkowego*] [**-fax** *numer_faksu*] [**-iptel** *numer_telefonu_IP*] [**-webpg** *strona_sieci_Web*] [**-title** *tytuł*] [**-dept** *dział*] [**-company** *firma*] [**-mgr** *nazwa_wyróżniająca_menedżera*] **[-hmdir** *katalog_macierzysty*] [**-hmdrv** *litera_dysku***:**][**-profile** *ścieżka_profilu*] [**-loscr** *ścieżka_skryptu*] [**-mustchpwd** {**yes** | **no**}] [**-canchpwd** {**yes** | **no**}] [**-reversiblepwd** {**yes** | **no**}] [**-pwdneverexpires** {**yes** | **no**}] [**-acctexpires** *liczba_dni*] [**-disabled** {**yes** | **no**}] [{**-s** *serwer* | **-d** *domena*}] [**-u** *nazwa_użytkownika*] [**-p** {*hasło* | *}] [**-q**] [{**-uc** | **-uco** | **-uci**}]

Parametry

nazwa_wyróżniająca_użytkownika

Wymagana. Określa nazwę wyróżniającą użytkownika, który należy dodać. Jeżeli pominięto nazwę wyróżniającą, nazwa zostanie pobrana z wejścia standardowego (stdin).

-samid *nazwa_SAM*

Określa, że należy użyć nazwy SAM jako unikatowej nazwy konta SAM dla tego użytkownika (na przykład Linda). Jeśli ta nazwa nie zostanie podana, polecenie dsadd spróbuje utworzyć nazwę konta SAM, używając pierwszych 20 znaków wartości nazwy pospolitej parametru *nazwa_wyróżniająca_użytkownika*.

-upn *nazwa_główna_użytkownika*

Określa nazwę główną użytkownika, którego należy dodać (na przykład Linda(at)widgets.microsoft.com).

-fn *imię*

Określa imię użytkownika, którego należy dodać.

-mi *inicjał*

Określa inicjał drugiego imienia użytkownika, którego należy dodać.

-ln *nazwisko*

Określa nazwisko użytkownika, którego należy dodać.

-display *nazwa_wyświetlana*

Określa nazwę wyświetlaną użytkownika, którego należy dodać.

-empid *identyfikator_pracownika*

Określa identyfikator pracownika użytkownika, którego należy dodać.

-pwd {*hasło* | *}

Określa hasło dla użytkownika, które należy ustawić na wartość parametru *hasło* lub *. Jeżeli hasło jest ustawione na wartość *, wyświetlany jest monit o podanie hasła użytkownika.

-desc *opis*

Określa opis użytkownika, którego należy dodać.

-memberof *nazwa_wyróżniająca_grupy ...*

Określa nazwy wyróżniające grup, których członkiem powinien być dany użytkownik.

-office *biuro*

Określa lokalizację biura użytkownika, którego należy dodać.

-tel *numer_telefonu*

Określa numer telefonu użytkownika, którego należy dodać.

-email *adres_e-mail*

Określa adres e-mail użytkownika, którego należy dodać.

-hometel *numer_telefonu_domowego*

Określa numer telefonu domowego użytkownika, którego należy dodać.

-pager *numer_pagera*

Określa numer pagera użytkownika, którego należy dodać.

-mobile *numer_telefonu_komórkowego*

Określa numer telefonu komórkowego użytkownika, którego należy dodać.

-fax *numer_faksu*

Określa numer faksu użytkownika, którego należy dodać.

-iptel *numer_telefonu_IP*

Określa numer telefonu IP użytkownika, którego należy dodać.

-webpg *strona_sieci_Web*

Określa adres URL strony sieci Web użytkownika, którego należy dodać.

-title *tytuł*

Określa tytuł użytkownika, którego należy dodać.

-dept *dział*

Określa dział użytkownika, którego należy dodać.

-company *firma*

Określa informacje dotyczące firmy użytkownika, którego należy dodać.

-mgr *nazwa_wyróżniająca_menedżera*

Określa nazwę wyróżniającą menedżera użytkownika, którego należy dodać.

-hmdir *katalog_macierzysty*

Określa lokalizację katalogu macierzystego użytkownika, którego należy dodać. Jeżeli parametr *katalog_macierzysty* jest podany jako ścieżka UNC, należy określić literę dysku, który należy zmapować na tę ścieżkę przy użyciu parametru **-hmdrv**.

-hmdrv *litera_dysku* :

Określa literę dysku katalogu macierzystego (na przykład E:) użytkownika, którego należy dodać.

-profile *ścieżka_profilu*

Określa ścieżkę profilu użytkownika, którego należy dodać.

-loscr *ścieżka_skryptu*

Określa ścieżkę skryptu logowania użytkownika, którego należy dodać.

-mustchpwd {yes | no}

Określa, czy podczas kolejnego logowania użytkownicy będą musieli zmieniać hasło (**yes**), czy nie (**no**). Domyślnie użytkownik nie musi zmieniać hasła (**no**).

-canchpwd {yes | no}

Określa, czy użytkownicy w ogóle mają możliwość zmiany haseł (**yes**), czy też nie (**no**). Domyślnie użytkownik może zmienić hasło (**yes**). Wartość tego parametru musi być równa **yes**, jeżeli wartość parametru **-mustchpwd** jest równa **yes**.

-reversiblepwd {yes | no}

Określa, czy hasło użytkownika powinno być przechowywane przy użyciu odwracalnego szyfrowania (**yes**), czy nie (**no**). Domyślnie użytkownik nie może używać odwracalnego szyfrowania (**no**).

-pwdneverexpires {yes | no}

Określa, że hasło użytkownika nigdy nie wygasa (**yes**) lub wygasa (**no**). Domyślnie hasło użytkownika wygasa (**no**).

-acctexpires *liczba_dni*

Określa liczbę dni, począwszy od bieżącego dnia, po upływie których konto użytkownika wygaśnie. Wartość 0 powoduje ustawienie daty wygaśnięcia na koniec bieżącego dnia. Wartość dodatnia powoduje ustawienie daty wygaśnięcia w przyszłości. Wartość ujemna powoduje ustawienie daty wygaśnięcia w przeszłości. W przypadku wartości **never** konto nigdy nie wygasa. Na przykład wartość **0** wskazuje, że konto wygaśnie na koniec dnia. Wartość **-5** wskazuje, że konto wygasło już 5 dni temu i powoduje ustawienie daty wygaśnięcia w przeszłości. Wartość **5** oznacza, że konto wygaśnie za 5 dni.

-disabled {yes | no}

Określa, czy logowanie przy użyciu danego konta komputera jest wyłączone (**yes**) czy włączone (**no**). Na przykład polecenie **dsadd user CN=Mietek,CN=Users,DC=Widgets,DC=Microsoft,DC=Com pwd- hasło1 -disabled no** tworzy konto użytkownika Mietek w stanie włączonym. Domyślnie logowanie przy użyciu tego konta użytkownika jest wyłączone (**yes**). Na przykład polecenie **dsadd user CN=Natalia,CN=Users,DC=Widgets,DC=Microsoft,DC=Com** tworzy konto użytkownika Natalia w stanie wyłączonym.

{-s *serwer* | -d *domena*}

Ustanawia połączenie z określonym serwerem zdalnym lub z domeną. Domyślnie komputer jest łączony z kontrolerem domeny w domenie logowania.

-u *nazwa_użytkownika*

Określa nazwę użytkownika używaną do logowania na serwerze zdalnym. Domyślnie w parametrze **-u** jest stosowana nazwa użytkownika, która została użyta do zalogowania danego użytkownika. Nazwę użytkownika można określić przy użyciu jednego z następujących formatów:

- nazwa_użytkownika (na przykład Linda)
- domena\nazwa_użytkownika (na przykład widgets\Linda)
- nazwa_główna_użytkownika (UPN) (na przykład Linda(at)widgets.microsoft.com)

-p {*hasło* | *}

Określa, że do logowania na serwerze zdalnym należy używać hasła lub znaku *. Jeżeli zostanie wpisany znak *, zostanie wyświetlony monit o podanie hasła.

-q Pomija wszystkie dane wyjściowe przekazywane do wyjścia standardowego (tryb cichy).

{-uc | -uco | -uci}

Określa, że dane wyjściowe lub wejściowe są formatowane zgodnie ze standardem Unicode. Następująca tabela zawiera listę i opisy poszczególnych formatów.

Z kontami użytkowników jest związanych wiele atrybutów. Odpowiednio pogrupowane są dostępne na różnych zakładkach okna właściwości użytkownika. Mogą być używane przez użytkowników jako źródło informacji o innych użytkownikach (dane teleadresowe) oraz przez administratorów do definiowania zasad i środowiska pracy osób logujących się na te konta.

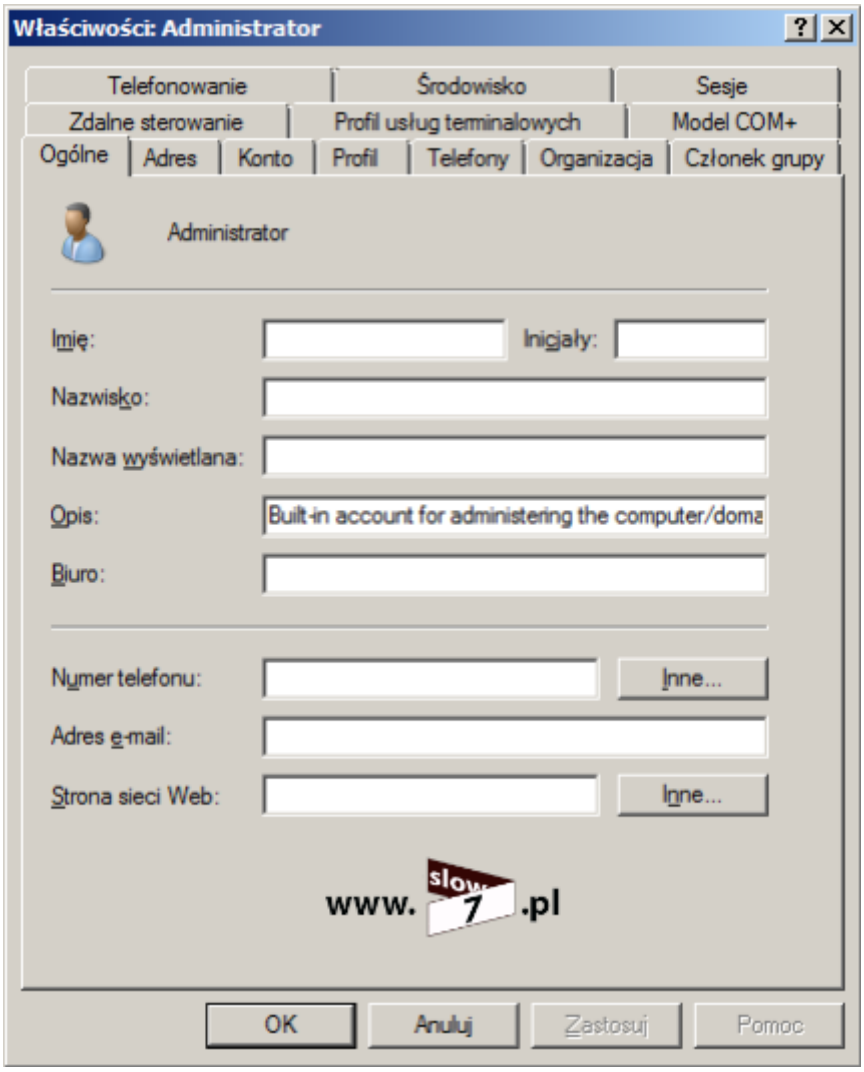
Okno właściwości obiektu użytkownika

Najczęściej używane opcje we właściwościach konta użytkownika:

- **General (Ogólne)** - imię, nazwisko, inicjały, opis, biuro, telefony oraz adresy e-mail i strony domowej użytkownika,
- **Address (Adres)** - ulica, skrytka pocztowa, miasto, województwo, kod pocztowy oraz kraj,
- **Account (Konto)** - nazwy logowania, godziny w których możliwe jest logowanie oraz komputery, z których może przebiegać proces logowania, opcje dotyczące

konta i data jego wygaśnięcia,

- **Profile (Profil)** - ścieżką wskazująca miejsce przechowywania profilu, skrypt logowania, ścieżka do folderu domowego, mapowanie dysku sieciowego,
- **Telephone (Telefony)** - numery telefonu domowego, pagera, komórkowego, faksu oraz telefonu IP,
- **Organization (Organizacja)** - stanowisko pracy, dział, firma, menedżer oraz podwładni,
- **Member Of(Członek grupy)** - nazwy grupy ,do których należy określony użytkownik,
- **Dial-in (Telefonowanie)** - uprawnienia usługi dostęp zdalny, w tym opcje oddzwaniania, adres IP i routing,
- **Environment (Środowisko)** - opcje związane z połączeniem terminalowym np. uruchamiany program, mapowanie dysków, drukarek,
- **Session (Sesje)** - sposób zachowania sesji terminalowych w przypadku bezczynności i rozłączonych połączeń,
- **Remote Control(Zdalne sterowanie)** - opcje związane z dostępem zdalnym danego użytkownika,
- **Terminal Services Profile (Profil usług terminalowych)** - profil użytkownika korzystającego z sesji terminalowej.



Rysunek 6 Właściwości konta użytkownika

Przy tworzeniu kont można skorzystać z pewnego uproszczenia, które polega na stworzeniu sobie szablonu czyli konta w którym są już zdefiniowane pewne często powtarzające się atrybuty konta. By stworzyć sobie nowe konto na podstawie szablonu należy kliknąć na koncie prawym przyciskiem myszy wybrać polecenie **Copy (Kopiuj)**. W oknie **Copy Object - User (Kopiuj obiekt - Użytkownik)** należy wypełnić indywidualne atrybuty związane z kontem. Część atrybutów z szablonu konta zostanie przekopiowanych do nowego konta. Są to:

- dla karty **Address (Adres)** - wszystkie wartości atrybutów z wyjątkiem **Street (Ulica)**
- dla karty **Account (Konto)** - wszystkie wartości atrybutów z wyjątkiem **User logon name (Nazwa logowania użytkownika)**
- dla karty **Profile (Profil)** - wszystkie wartości atrybutów a dodatkowo pola **Profile path (Ścieżka profilu)** i **Home folder (Folder macierzysty)** zostaną zmienione tak by odpowiadały nazwie logowania użytkownika
- dla karty **Organization (Organizacja)** - wszystkie wartości atrybutów
- dla karty **Member Of (Członek grupy)** - wszystkie wartości atrybutów

Nietrudno się domyślić, że szablony kont będą używane tam gdzie wymagania dla poszczególnych kont użytkownika są takie same lub nieznacznie się różnią - np. jeden dział danej firmy. Należy mieć na uwadze by nazwa szablonu odróżniała się od innych kont i by konto szablonu było wyłączone (konta nieużywane do logowania zawsze powinny być wyłączone)

By ograniczyć zbyt dużą ilość nieudanych logowań a tym samym zablokować konto użytkownika z którego następuje próba uwierzytelnienia możemy zdefiniować próg logowania. Próg blokady konta ustawiamy w konfiguracji zabezpieczeń usługi **Active Directory**. Do zablokowania konta może dojść również w sytuacji w której sam użytkownik je blokuje nie pamiętając hasła i sprawdzając kolejne kombinacje a także gdy pozostając zalogowanym na jednym komputerze następuje zmiana hasła na innym. O fakcie zablokowania konta jesteśmy informowani przy próbie logowania a poprawne logowanie nastąpi wtedy gdy administrator odblokuje konto, lub upłynie czas, po którym zostaje automatycznie zdjęta blokada konta.

Download Media File

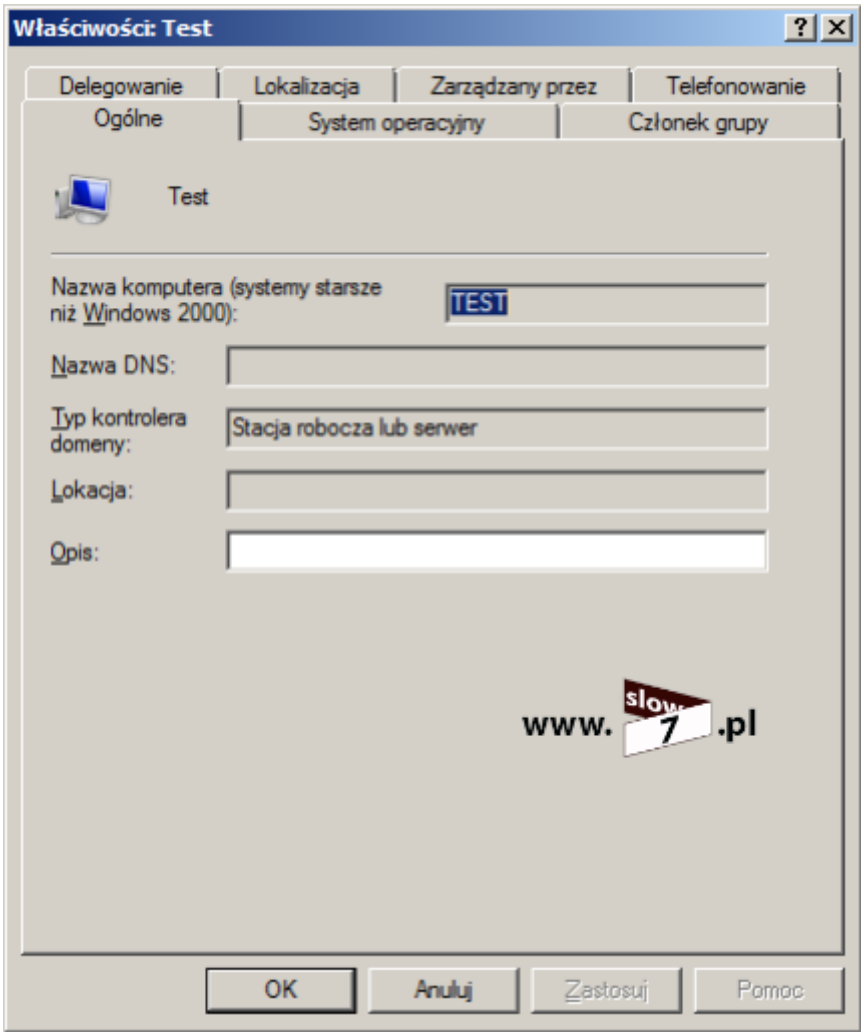
Tworzenie i modyfikacja konta użytkownika

Konto komputera

Podobnie jak użytkownik również każdy komputer z rodziny Windows należący do domeny posiada swoje odrębne konto w domenie. Komputery wykonują kluczowe zadania, takie jak uwierzytelnianie logowania użytkowników, rozpowszechnianie adresów protokołu IP (Internet Protocol), obsługa

integralności usługi **Active Directory** i wymuszanie zasad zabezpieczeń. Aby uzyskać pełny dostęp do tych zasobów sieciowych, komputery muszą korzystać z prawidłowych kont w usłudze **Active Directory**. Dwie podstawowe funkcje konta komputera są związane z zabezpieczeniami i zarządzaniem.

Użytkownicy mogą korzystać z wszystkich funkcji usługi **Active Directory** pod warunkiem, że konto komputera zostanie utworzone w usłudze **Active Directory**. Komputer, dla którego utworzono konto, może szyfrować ruch sieciowy protokołu IP przy użyciu procesów zaawansowanego uwierzytelniania takich jak uwierzytelnianie Kerberos i zabezpieczenia protokołu IP (IPSec). Konto komputera jest również niezbędne do kontrolowania sposobu stosowania i rejestrowania inspekcji.



Rysunek 7 Właściwości konto komputera

Konta komputerów ułatwiają administratorowi systemów zarządzanie strukturą sieci. Korzystając z kont komputerów, administrator systemów zarządza funkcjami środowiska pulpitu, automatyzuje rozmieszczanie oprogramowania przy użyciu usługi **Active Directory** oraz prowadzi spis sprzętu i oprogramowania przy użyciu programu Microsoft Systems Management Server (SMS). Konta komputerów w domenie są również używane do kontrolowania dostępu do zasobów.

Konto komputera może być stworzone na dwa sposoby:

- przyłączenie komputera przez użytkownika mającego takie uprawnienia. Konto komputera po przyłączeniu go do domeny zostanie umieszczone w wbudowanej jednostce organizacyjnej **Computers**, tak utworzone konto można oczywiście przenieść do dowolnej innej jednostki organizacyjnej,
- sytuacja odwrotna w której to najpierw jest tworzone konto komputera w danym kontenerze a następnie nazywany i przyłączany jest dany komputer.

Konto komputera podobnie jak konto użytkownika tworzymy przy pomocy przystawki **Active Directory Users and Computers** lub przy użyciu narzędzi wiersza poleceń. Wybieramy interesującą nas jednostkę organizacyjną i z menu kontekstowego wybieramy polecenie **New** a następnie **Computer**. W oknie **New Object** - **Computer** należy podać nazwę komputera (nazwa używana przez systemy starsze niż Windows 2000 zostanie uzupełniona automatycznie). Jeśli na komputerze, który będzie używał tworzonego konta, jest zainstalowany system starszy niż Windows 2000, zaznacz pole wyboru **Przypisz to konto komputera jako komputer z systemem starszym niż Windows 2000**. Spowoduje to utworzenie hasła komputera bazującego na jego nazwie. Jeśli komputer, który będzie używał tworzonego konta, jest zapasowym kontrolerem domeny systemu Windows NT, zaznacz pole wyboru **Przypisz to konto komputera jako zapasowy kontroler domeny**.

Aby dodać pojedynczy komputer do katalogu należy wydać polecenie:

dsadd computer *nazwa_wyróżniająca_komputera* [**-samid** *nazwa_SAM*] [**-desc** *opis*] [**-loc***lokalizacja*] [**-memberof** *nazwa_wyróżniająca_grupy ...*] [{**-s** *serwer* | **-d** *domena*}] [**-u***nazwa_użytkownika*] **[-p** {*hasło* | *}] [**-q**] [{**-uc** | **-uco** | **-uci**}]

Parametry

nazwa_wyróżniająca_komputera

Wymagana. Określa nazwę wyróżniającą komputera, który należy dodać. Jeżeli pominięto nazwę wyróżniającą, nazwa zostanie pobrana z wejścia standardowego (stdin).

-samid *nazwa_SAM*

Określa, że należy użyć nazwy SAM jako unikatowej nazwy konta SAM dla tego komputera (na przykład TESTPC2$). Jeżeli ten parametr nie jest określony, nazwa konta SAM jest ustalana na postawie wartości atrybutu nazwy pospolitej używanego w parametrze *nazwa_wyróżniająca_komputera*.

-desc *opis*

Określa opis komputera, który należy dodać.

-loc *lokalizacja*

Określa lokalizację komputera, który należy dodać.

-memberof *nazwa_wyróżniająca_grupy ...*

Określa grupy, do których dany komputer powinien należeć.

{-s *serwer* | -d *domena*}

Ustanawia połączenie komputera z określonym serwerem lub domeną. Domyślnie komputer jest łączony z kontrolerem domeny w domenie logowania.

-u *nazwa_użytkownika*

Określa nazwę użytkownika używaną do logowania na serwerze zdalnym. Domyślnie w parametrze **-u** jest stosowana nazwa użytkownika, która została użyta do zalogowania danego użytkownika.

-p {*hasło* | *}

Określa, że do logowania na serwerze zdalnym należy używać hasła lub znaku *. Jeżeli zostanie wpisany znak *, zostanie wyświetlony monit o podanie hasła.

-q Pomija wszystkie dane wyjściowe przekazywane do wyjścia standardowego (tryb cichy).

{-uc | -uco | -uci}

Określa, że dane wyjściowe lub wejściowe są formatowane zgodnie ze standardem Unicode. Następująca tabela zawiera listę i opisy poszczególnych formatów.

Download Media File

Tworzenie i modyfikacja konta komputera

Warto zapamiętać:

a) W celu zapewnienia wyższego stopnia bezpieczeństwa, należy zmienić nazwę wbudowanego konta administratora. Nazwę należy zdefiniować tak, aby nie kojarzyła się z kontem administratora. Dzięki temu dostęp do tego konta przez nieuprawnionych użytkowników zostanie znacznie utrudniony.

b) Utworzyć konto dla siebie i zdefiniować dla niego uprawnienia administratorskie. Konta tego należy używać jedynie do wykonywaniu zadań administratorskich.

c) W celu zapewnienia bezpieczeństwa nie zezwalaj by kilku użytkowników korzystało z jednego konta

d) Innym rozwiązaniem jest generowanie losowych haseł dla wszystkich użytkowników. Hasła te powinny składać sie z kombinacji znaków i cyfr. Tworzenie takich haseł zwiększa poziom bezpieczeństwa w sieci, często jednak użytkownicy, jeżeli maja trudności z zapamiętaniem

haseł, zapisują je na przechowywanych obok komputera kartkach.

e) Nowy użytkownik o takiej samej nazwie jak poprzednio skasowany nie otrzymuje automatycznie uprawnień i przynależności do grup jakie posiadało skasowane konto ponieważ identyfikator zabezpieczeń (**SID**) dla każdego konta jest unikalny. Jeśli chcesz zduplikować skasowane konto musisz odtworzyć wszystkie uprawnienia i członkostwo w grupach ręcznie.

f) Utworzyć konto, które będzie wykorzystywane do wykonywania codziennych zadań. Na konto, posiadające uprawnienia administratora należy się logować tylko w przypadku, gdy są do wykonania jakieś zadania administratorskie.

g) Komputery z systemami Windows 95 i Windows 98 nie posiadają zaawansowanych funkcji zabezpieczeń, dlatego nie można stworzyć dla nich kont komputerów.

h) W sieciach o niskim poziomie bezpieczeństwa można odblokować konto Gość. Należy jednak koniecznie zdefiniować dla tego konta hasło. Konto to domyślnie jest zablokowane.

i) Można zawsze wymagać od nowego użytkownika, aby zmieniał hasło przy pierwszym logowaniu. Dzięki temu administrator może być pewien, ze hasła są unikalne i znane tylko użytkownikom. Metoda ma te wadę, że użytkownicy często wybierają hasła trywialne do odgadnięcia, co ułatwia włamanie metoda zgadywania hasła.

j) Jeśli konto Administratora jest wyłączone, może być nadal używane w celu dostania się do kontrolera domeny w trybie bezpiecznego uruchamiania (ang. **Safe Mode**)

k) Należy bezwzględnie zabezpieczać każde konto hasłem, nawet, jeżeli użytkownik będzie musiał zmienić to hasło przy pierwszym logowaniu.

l) Lokalnych kont użytkowników nie można tworzyć na kontrolerach domeny.

m) Warto określić datę wygaśnięcia konta w przypadku, gdy będzie ono wykorzystywane tylko przez pewien określony czas (np. konta pracowników tymczasowych).

BIBLIOGRAFIA

http://infojama.pl/175,artykul.aspx

http://rbanasi.kis.p.lodz.pl/sso/ad2.pdf

http://technet.microsoft.com/pl-pl/library/cc770319%28WS.10%29.aspx

http://support.microsoft.com/kb/310997/pl

http://technet.microsoft.com/pl-pl/library/cc770970.aspx

http://www.kraszewscy.net/Podstawy_LDAP

http://www.pcworld.pl/artykuly/40698_3_1/Administarcja.dla.leniuchow.html#sub57662

http://tech-blog.it/2009/02/delegowanie-uprawnien-administracyjnych-dla-jednostki-organizacyjnej-ou/

http://technet.microsoft.com/pl-pl/library/default%28en-us%29.aspx

http://www.wstt.edu.pl/pliki/materialy/aswnt/wyklad/wyk1-2.pdf

http://www.pcworld.pl/artykuly/42393/Administracja.od.podstaw.html#top

http://support.microsoft.com/kb/973289/pl

http://support.microsoft.com/kb/816313/pl

http://infojama.pl/177,artykul.aspx