Tworzenie i zarządzanie kontami użytkowników

Aby użytkownik mógł korzystać z systemu operacyjnego, musi w nim mieć utworzone konto. Konto jest zbiorem parametrów opisujących użytkownika jak również przydzielonych mu pewnych zasobów systemowych. Podstawowe parametry konta to nazwa logowania, którą użytkownik musi podać, aby móc rozpocząć pracę w systemie, oraz hasło potrzebne do sprawdzenia tożsamości. Pozostałe parametry to m.in. pełna nazwa konta, pory dnia, w których możliwe jest logowanie, data wygaśnięcia konta.

Konta dzielą się na wbudowane – są tworzone automatycznie podczas instalacji systemu i charakteryzują się tym, że nie można ich usuwać, oraz tworzone przez uprawnionych użytkowników już w zainstalowanym systemie. Jest jeszcze jeden sposób podziału kont – na konta lokalne i konta użytkowników domenowych. Te pierwsze mogą być tworzone na osobnych komputerach nie podłączonych do sieci, na komputerach wchodzących w skład grupy roboczej lub na komputerach należących do domeny, lecz nie będących jej kontrolerami. Właściciel takiego konta ma dostęp tylko do lokalnych zasobów komputera. Konta użytkowników domenowych mogą być tworzone tylko na kontrolerach domen, natomiast ich właściciele mają dostęp do zasobów sieciowych a nie tylko lokalnych zasobów komputera, na którym dany użytkownik jest zalogowany.

Konwencje dotyczące nazw i haseł

- Nazwy logowania kont użytkowników domenowych muszą być niepowtarzalne w bazie Active Directory
- Pełne nazwy kont użytkowników domenowych muszą być niepowtarzalne w obrębie domeny, w której są tworzone konta.
- Nazwy kont użytkowników lokalnych muszą być niepowtarzalne w obrębie maszyny, na której są tworzone konta.
- Nazwy logowania mogą zawierać do 20 znaków literowych i cyfrowych z pominięciem następujących znaków o specjalnym znaczeniu: ” / \ [ ] ; ; | = , + * ? < >
- Konto administratora powinno być zawsze zabezpieczone hasłem w celu uniknięcia dostępu osób niepowołanych do tego konta
- Hasła mogą zawierać do 128 dowolnych znaków; zalecane są hasła o długości co najmniej ośmiu znaków i trudne do odgadnięcia, albo automatycznego wygenerowania

Uprawnienia użytkowników

Istnieją dwa rodzaje uprawnień, którymi mogą dysponować użytkownicy – uprawnienia do wykonywania pewnych operacji w systemie nie związanych z określonymi zasobami, oraz prawa dostępu do poszczególnych zasobów. Drugi rodzaj uprawnień jest tematem rozdziału „Udostępnianie zasobów”. Tutaj zostanie opisany pierwszy rodzaj.

Uprawnienia mogą być przyznawane poszczególnym użytkownikom lub grupom użytkowników. Zazwyczaj jednak uprawnienia nadawane są grupom i stanowią kryterium przynależności do tej bądź innej grupy. Następnie do poszczególnych grup dodawani są użytkownicy i w ten sposób nabywają oni określone uprawnienia.

Operacje, do których wykonania potrzebne są omawiane uprawnienia to m.in.:

Logowanie lokalne – możliwość logowania się na konto użytkownika lokalnego lub logowania do domeny z lokalnego komputera

Zmiana czasu systemowego – możliwość przestawienia wewnętrznego zegara w komputerze jak również zmiany strefy czasowej

Zamykanie systemu – uruchomienie procesu przygotowującego komputer do bezpiecznego wyłączenia

Dostęp do komputera z sieci – łączenie się z udostępnionymi zasobami komputera lokalnego z innego komputera w sieci

Konta użytkowników lokalnych

Konta użytkowników lokalnych są zazwyczaj używane w niewielkich sieciach (np. składających się z kilku komputerów tworzących grupę roboczą), lub na osobnych komputerach nie podłączonych do sieci. W zasadzie można utworzyć konto użytkownika lokalnego na komputerze wchodzącym w skład domeny, lecz nie będzie ono rozpoznawane przez serwer domeny i właściciel takiego konta będzie miał dostęp tylko do lokalnych zasobów danego komputera.

Jeśli użytkownik ma konto domenowe, oraz konto lokalne na jednym z komputerów domeny, to na tym komputerze może się logować albo jako użytkownik lokalny, albo domenowy. Nie jest możliwe jednoczesne logowanie do domeny i do lokalnego komputera.

Informacje o kontach lokalnych są przechowywane w bazie SAM (Security Access Management) będącej lokalną bazą kont komputera, nie są natomiast zapisywane do bazy Active Directory, której kopie znajdują się w kontrolerach domeny.

Wbudowane konta lokalne

W systemie Windows 2003 istnieją dwa podstawowe, wbudowane konta lokalne – „Administrator” i „Gość”. Konto „Gość” jest standardowo zablokowane, jeśli więc administrator chce umożliwić korzystanie z tego konta, powinien je odblokować. Konto „Gość” nie jest zabezpieczone hasłem.

Wbudowanych kont lokalnych nie można usunąć.

Hasło do konta „Administrator” podawane jest podczas instalacji systemu. Jeśli administrator zapomni swoje hasło, to jedynym wyjściem z sytuacji może być ponowna instalacja Windows. Administrator ma pełne prawa do wszystkich zasobów komputera. Może również tworzyć, modyfikować i usuwać konta użytkowników lokalnych (oprócz wbudowanych), oraz grupy lokalne.

Tworzenie i konfigurowanie kont użytkowników lokalnych

Do tworzenia i konfigurowania kont użytkowników lokalnych służy narzędzie „Zarządzanie komputerem lokalnym”. Aby je uruchomić, należy w podanej kolejności otworzyć:

Start -> Programy -> Narzędzia administracyjne -> Zarządzanie komputerem

Okno „Zarządzanie komputerem” podzielone jest na dwie części. Z lewej strony znajduje się lista folderów, a z prawej strony wyświetlana jest zawartość zaznaczonego aktualnie folderu.

Aby utworzyć konto lokalne, należy dotrzeć do folderu „Użytkownicy”, otwierając kolejno:

Zarządzanie Komputerem Lokalnym -> Narzędzia Systemowe -> Użytkownicy i Grupy Lokalne

następnie prawym przyciskiem myszy kliknąć folder „Użytkownicy” i z otwartej w ten sposób listy wybrać opcję „Nowy Użytkownik”. Otworzy się wówczas okno, w którym należy wypełnić pola „Nazwa Użytkownika”, „Pełna Nazwa Użytkownika” i „Opis”. W polach „Hasło” i „Potwierdź hasło” należy wpisać hasło , które ma być używane przez użytkownika do logowania, przy czym wpisywane hasło nie będzie wyświetlało się na ekranie. Potwierdzanie hasła służy zabezpieczeniu się przed nieświadomie popełnianymi błędami literowymi. System wezwie nas do ponownego dwukrotnego wpisania hasła, jeśli hasło potwierdzone nie będzie takie samo jak hasło „oryginalne”. Możemy teraz zaznaczyć opcje nakładające na hasło różne ograniczenia i zakończyć tworzenie konta wciskając przycisk „Utwórz”.

Konta użytkowników domenowych

Konta użytkowników domenowych są tworzone na kontrolerach domeny i zapewniają ich właścicielom dostęp do zasobów sieciowych, a nie tylko do lokalnych zasobów komputera, na którym dany użytkownik jest zalogowany. Informacje o tych kontach zapisywane są w bazie Active Directory i replikowane na wszystkich kontrolerach danej domeny. Użytkownik domenowy może logować się na swoje konto domenowe z dowolnego komputera domeny. Podczas logowania następuje połączenie z pierwszym dostępnym kontrolerem domeny, który sprawdza podaną przez użytkownika nazwę logowania i hasło, i jeśli są podane prawidłowo – umożliwia mu dostęp do zasobów domeny.

Wbudowane konta domenowe

W systemie Windows 2000 istnieją dwa podstawowe, wbudowane konta domenowe – „Administrator” i „Gość”. Konta te spełniają podobną rolę jak analogiczne konta lokalne, z tą jednak różnicą, że umożliwiają one dostęp do zasobów całej domeny. Administrator domeny ma pełne prawa dostępu do wszystkich zasobów domeny, może tworzyć, modyfikować i usuwać konta użytkowników domenowych, oraz grupy domenowe. Konta administratora nie można zablokować, można natomiast nadać mu inną nazwę. Wbudowanych kont domenowych nie można usuwać.

Tworzenie kont użytkowników domenowych

Do tworzenia i konfigurowania kont użytkowników domenowych służy narzędzie „Użytkownicy i Komputery Active Directory”. Aby je uruchomić, należy zalogować się na serwerze domeny i w podanej kolejności otworzyć:

Start -> Ustawienia -> Panel Sterowania -> Narzędzia Administracyjne -> Użytkownicy i Komputery Active Directory

Okno „Użytkownicy i Komputery Active Directory” podzielone jest na dwie części. Z lewej strony znajduje się rozwijana lista domen i ich zasobów, a z prawej wyświetlana jest zawartość zaznaczonego aktualnie folderu.

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” 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 cztery 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 zablokowane”.

Uwaga: Opcja „Użytkownik musi zmienić hasło przy następnym logowaniu” unieważnia opcję „Hasło nigdy nie wygasa”.

Zarządzanie kontami użytkowników domenowych

Z każdym nowo tworzonym kontem domenowym związane są parametry domyślne, podzielone na kilka grup. Parametrów tych nie konfiguruje się podczas zakładania konta, można natomiast je modyfikować, kiedy konto już istnieje w systemie. Aby dokonać modyfikacji parametrów konta, należy w podanej kolejności otworzyć

Start -> Ustawienia -> Panel Sterowania -> Narzędzia Administracyjne -> Użytkownicy i Komputery Active Directory,

w drzewie zasobów właściwej domeny zaznaczyć folder „Użytkownicy”, następnie w panelu szczegółów prawym przyciskiem myszy kliknąć wybrane konto. Z otwartej w ten sposób listy należy wybrać „Właściwości”, co spowoduje otwarcie okna z właściwościami konta. W oknie tym widnieje szereg zakładek, które pozwalają otwierać karty z poszczególnymi grupami parametrów. Jeśli, na przykład, klikniemy zakładkę „Konto”, a na otwartej w ten sposób karcie przycisk „Godziny logowania”, to będziemy mogli określić pory dnia, w których dany użytkownik będzie mógł logować się do domeny. Poza określonymi godzinami użytkownik ten nie będzie miał dostępu do domeny.

Administrator ma również możliwość wyznaczenia komputerów, z których użytkownicy mogą logować się do domeny. Standardowo użytkownicy mogą logować się do domeny z każdego komputera należącego do tej domeny. Jeśli jednak administrator utworzy dla danego użytkownika listę komputerów, z których może on się logować do domeny, to użytkownik ten nie będzie mógł się logować do domeny z żadnego komputera spoza tej listy. W celu utworzenia takiej listy na karcie „Konto” należy wcisnąć przycisk „Logowanie na”.

Otworzy się wówczas okno zawierające pole do wpisania nazwy komputera i przycisk „Dodaj”. Wpisanie nazwy komputera i wciśnięcie „Dodaj” powoduje umieszczenie komputera na liście. Przycisk „OK” służy do zakończenia edycji listy.

Uwaga: nie można w ten sposób ograniczyć dostępu administratora do domeny.

Aby uprościć czynność zakładania kont domenowych wielu użytkownikom, możemy skorzystać z możliwości kopiowania kont. Zakładamy w ten sposób nowe konto domenowe, które jest „kopią” już istniejącego konta, tzn. ma w większości takie same parametry, z wyjątkiem praw dostępu i niektórych parametrów takich jak np. adres czy telefony.

Uwaga: Przy kopiowaniu konta prawa dostępu nie są kopiowane z konta źródłowego na konto docelowe.

Aby utworzyć kopię istniejącego konta domenowego, należy otworzyć „Użytkownicy i Komputery Active Directory”, w drzewie zasobów we właściwej domenie rozwinąć folder „Użytkownicy”, następnie prawym klawiszem myszy kliknąć wybrane konto. Z otwartej w ten sposób listy opcji wybieramy „Kopiuj”, w oknie dialogowym „Kopiuj Obiekt – Użytkownik” wpisujemy nazwę logowania nowego użytkownika, wciskamy przycisk „Dalej” i wpisujemy dwukrotnie hasło, oraz zaznaczamy znane już opcje. Całą operację kończymy wciskając przycisk „Zakończ”.

Często stosowanym przez administratorów zabiegiem jest tworzenie tzw. szablonów kont. Szablon jest po prostu zwykłym kontem domenowym, tyle tylko, że z zaznaczoną opcją „Konto zablokowane”. Chodzi o to, aby nikt nie wykorzystał konta szablonowego w celu uzyskania dostępu do systemu. Korzystając z szablonów i możliwości kopiowania kont można znacznie przyspieszyć proces zakładania kont w sieci obsługującej dużą organizację. W tym celu należy podzielić użytkowników na grupy, w obrębie których parametry większości użytkowników niewiele się różnią, dla każdej takiej grupy utworzyć szablon i tworzyć z niego konta przy pomocy operacji kopiowania.

Profile użytkowników - konfigurowanie środowiska pracy

W systemie Windows 2003 środowisko pracy użytkownika determinowane jest przede wszystkim przez tzw. profil. Mianem profilu określa się wszystkie ustawienia, które użytkownik może skonfigurować, jak np. ikony wyświetlane na pulpicie, rozmieszczenie ikon na pulpicie, tapeta będąca tłem pulpitu, ustawienia myszy, itd. Podstawowym profilem jest tzw. profil lokalny, fizycznie będący katalogiem tworzonym wtedy, kiedy użytkownik po raz pierwszy loguje się na danym komputerze. W tym katalogu, w postaci różnych plików, zapisywane są wszystkie ustawienia właściwe dla użytkownika. Katalog z profilem ma nazwę taką samą jak użytkownik i znajduje się w katalogu „C:\Dokumenty i ustawienia” na komputerze lokalnym. Kiedy użytkownik zamyka sesję, katalog ten jest aktualizowany. W ten sposób każdy użytkownik zachowuje osobiste ustawienia na komputerze, na którym pracował. Istnieją cztery typy profili:

- Profil domyślny - służy jako szablon dla profili użytkowników logujących się po raz pierwszy na danej maszynie. Każdy nowo tworzony profil jest jego kopią

- Profil lokalny - jest tworzony wtedy, kiedy użytkownik po raz pierwszy loguje się na danym komputerze i na tym komputerze jest przechowywany. Jeśli użytkownik otwiera

sesję z profilem lokalnym, to w tym profilu zapisywane są wszystkie zmiany w ustawieniach poczynione w trakcie sesji. Zmiany te są więc związane tylko z tym komputerem, na którym sesja była otwarta. Krótko mówiąc – profil lokalny istnieje zawsze na każdym komputerze, z którego użytkownik logował się do domeny.

- Profil globalny (użytkownika wędrującego) - profil ten jest właściwy tylko dla użytkowników domenowych. Położenie katalogu zawierającego profil globalny jest określane podczas konfigurowania opcji użytkownika. Musi to być udostępniony w sieci katalog bazowy dla profilu znajdujący się np. na dysku kontrolera domeny, albo na innym komputerze. Profil ten jest tworzony przy pierwszym logowaniu użytkownika i uaktywniany za każdym razem, kiedy użytkownik loguje się do domeny na dowolnym komputerze w sieci. Jeśli użytkownik otwiera sesję z profilem globalnym, to w tym profilu zapisywane są wszystkie zmiany w ustawieniach poczynione w trakcie sesji. Zmiany te nie są więc związane z komputerem, na którym sesja była otwarta.

- Profil stały (bez możliwości modyfikacji przez użytkownika) - jest to profil stosowany w celu przypisania użytkownikowi określonych, niezmiennych ustawień sesji. Zarówno profil lokalny jak i globalny może być profilem stałym. Profil stały nie daje użytkownikowi możliwości zapisania zmian ustawień dokonanych w trakcie sesji. Jeśli użytkownik pracuje z profilem stałym, to zmiany ustawień są aktualne tylko do końca sesji i giną po jej zakończeniu. Każda nowa sesja jest więc otwierana z takimi samymi ustawieniami.

W celu utworzenia profilu globalnego dla wybranego użytkownika korzystamy z narzędzia „Użytkownicy i komputery Active Directory”. W wyświetlanym drzewie zasobów we właściwej domenie rozwijamy folder „Użytkownicy” i prawym klawiszem myszy klikamy wybrane konto. Z otwartej w ten sposób listy wybieramy opcję „Właściwości”, co spowoduje otwarcie okna z właściwościami konta. W oknie tym otwieramy kartę „Profil”, gdzie w polu „Ścieżka” wpisujemy ścieżkę do profilu globalnego. Ścieżka ta powinna mieć następującą postać:

\\nazwa_serwera\profiles\nazwa_logowania_uzytkownika

przy czym folder o nazwie „profiles” powinien być wcześniej utworzony na serwerze, na którym ma być przechowywany profil globalny, a użytkownik powinien mieć do tego folderu prawo „Zmieniaj”. W tym celu można np. nadać prawo „Zmieniaj” grupie „Domain Users”. Nazwa „profiles” jest przykładowa, można tu użyć dowolnej innej nazwy. Zamiast nazwy logowania użytkownika można wpisać %username%, gdzie „username” jest zmienną środowiskową przechowującą tę nazwę.

Uwaga: Plik z profilem globalnym ma nazwę Ntuser.dat i jest plikiem ukrytym. Zawiera on tę część rejestru, w której zapisane są ustawienia sesji użytkownika. Aby Eksplorator Windows wyświetlał nazwę tego pliku, należy włączyć opcję wyświetlania plików ukrytych.

W celu zmiany zwykłego profilu globalnego na stały profil globalny należy zmienić nazwę pliku Ntuser.dat na Ntuser.man. Zmianę taką może przeprowadzić tylko administrator. Jeśli administrator chce nadać użytkownikowi określone ustawienia, zanim zmieni mu profil na stały, musi zalogować się jako ten użytkownik, odpowiednio skonfigurować ustawienia,

wylogować się, następnie zalogować jako administrator i plik Ntuser.dat przemianować na Ntuser.man.

Foldery osobiste – miejsce na własne pliki użytkowników

Przy zakładaniu konta użytkownika można utworzyć specjalny folder, w którym użytkownik będzie przechowywał swoje pliki i który po zalogowaniu stanie się automatycznie folderem bieżącym użytkownika. Folder taki jest nazywany folderem domowym i może znajdować się na serwerze sieciowym lub na komputerze, na którym użytkownik ma konto lokalne. Do najważniejszych czynników, które powinny być brane pod uwagę przy wyborze miejsca dla katalogu domowego, należą:

- Częstość, z jaką będą wykonywane kopie zapasowe folderów domowych użytkowników. Jeśli foldery te znajdują się na jednym, centralnym serwerze, wówczas łatwiej jest je archiwizować, niż wtedy, kiedy są rozproszone na wielu komputerach.

- Ilość miejsca na dyskach centralnego serwera. W systemie Windows 2003 istnieje mechanizm zabezpieczający przed „nieograniczonym apetytem" użytkowników na przestrzeń dyskową – tzw. mechanizm kwot, pozwalający na limitowanie przestrzeni dyskowej wykorzystywanej przez użytkownika.

- Ilość miejsca na dyskach komputerów, na których użytkownicy mają swoje konta lokalne.

- Natężenie ruchu w sieci. Umiejscowienie folderów domowych użytkowników na centralnym serwerze może spowodować znaczne zwiększenie ruchu w sieci.

W celu założenia folderu domowego należy otworzyć okno z właściwościami konta użytkownika, w oknie tym otworzyć kartę „Profil" i w polu „Folder Domowy" wpisać ścieżkę do wybranego folderu. Zazwyczaj ścieżka ta ma następującą postać:

\\nazwa_serwera\home\nazwa_logowania_użytkownika

gdzie „home" jest folderem bazowym dla folderów domowych użytkowników. Nazwa „home" jest przykładowa, można tu użyć dowolnej innej nazwy. Zamiast nazwy logowania użytkownika można wpisać %username%, gdzie „username" jest zmienną środowiskową przechowującą tę nazwę. Użytkownik powinien mieć prawo „Zmieniaj" do swojego folderu domowego.

Skrypty logowania

Skrypt logowania jest to program, który wykonuje się automatycznie po zalogowaniu użytkownika na koncie lokalnym lub domenowym. Aby taki program mógł się wykonać, należy przede wszystkim utworzyć plik z programem (może to być na przykład plik wsadowy zawierający polecenia systemu DOS), a następnie odpowiednio skonfigurować konto użytkownika. W celu wykonania tej drugiej czynności należy otworzyć okno z właściwościami konta użytkownika, w oknie tym otworzyć kartę „Profil" i w polu „Skrypt logowania" wpisać nazwę pliku z programem (standardowo – %username%.bat). Ważne jest, że nie można tu podać bezwzględnej ścieżki dostępu, a tylko nazwę pliku ze skryptem logowania.

Uwaga: W przypadku konta lokalnego skrypt logowania zostanie umieszczony na komputerze lokalnym, w folderze

<Główny folder systemowy>\system32\repl\import\scripts,

przy czym folder repl\import\scripts należy utworzyć ręcznie (nie jest on tworzony automatycznie podczas instalacji) i udostępnić pod nazwą NETLOGON

W przypadku konta domenowego skrypt logowania zostanie umieszczony na kontrolerze domeny w katalogu

<Główny folder systemowy>\SYSVOL\sysvol\<nazwa domeny>\scripts

udostępnionym jako NETLOGON. Katalog ten jest tworzony i udostępniany automatycznie, więc nie należy go tworzyć i udostępniać ręcznie. Ścieżka do głównego folderu systemowego przechowywana jest w zmiennej o nazwie systemroot.

Polecenie net user

Użytkowników, zarówno lokalnych jak i domenowych można tworzyć, usuwać lub modyfikować przy pomocy komendy „net user" wydawanej z wiersza poleceń. Komenda „net user" należy do grupy „net", pełną listę komend z tej grupy dostajemy wydając polecenie „net help". Oto przykłady komendy „net user" wraz z podstawowymi opcjami:

net user jacek password xyz123 /add /domain

Powyższa komenda tworzy konto użytkownika domenowego z nazwą logowania jacek i hasłem xyz123. Konto jest tworzone w bieżącej domenie, czyli tej, do której zalogowany jest użytkownik wydający polecenie „net user". Bez przełącznika „/domain" powstałoby konto użytkownika lokalnego. Przełączniki „/homedir", „/profilepath" i „/scriptpath" służą do określania katalogu domowego, katalogu z profilem i nazwy skryptu logowania użytkownika. Bardziej szczegółowy opis komendy „net user" uzyskujemy wydając polecenie „net help user"

Tworzenie i zarządzanie grupami

W najprostszej postaci grupa jest zbiorem kont użytkowników. Grup używa się po to, aby ułatwić zarządzanie dostępem do współdzielonych w sieci zasobów takich jak foldery, pliki, czy drukarki. Nadanie grupie określonych praw dostępu powoduje nadanie tych praw wszystkim użytkownikom należącym do danej grupy. Jeden użytkownik może równocześnie należeć do wielu grup. Oprócz kont użytkowników do grup mogą należeć komputery, oraz – w określonych przypadkach – również inne grupy.

Grupy dzielą się na wbudowane – są tworzone automatycznie podczas instalacji systemu i charakteryzują się tym, że nie można ich usuwać, oraz tworzone przez uprawnionych użytkowników już w zainstalowanym systemie. Jest jeszcze jeden sposób podziału grup – na grupy lokalne i grupy domenowe. Te pierwsze mogą być tworzone na osobnych komputerach nie podłączonych do sieci, komputerach wchodzących w skład grupy roboczej, lub komputerach należących do domeny, lecz nie będącej jej kontrolerami. Mogą one zawierać tylko konta użytkowników lokalnych danego komputera. Grupy domenowe mogą być tworzone tylko na kontrolerach domeny i zawierać konta użytkowników domenowych a nawet inne grupy domenowe.

Chociaż prawa dostępu do zasobów można nadawać pojedynczym użytkownikom, to najczęściej stosowana metoda nadawania praw dostępu polega na utworzeniu grupy, nadaniu jej określonych uprawnień, a następnie przypisaniu do tej grupy kont użytkowników.

Uwaga: jeśli użytkownik jest dołączany do grupy w tym czasie, kiedy jest zalogowany, to uzyska on prawa dostępu właściwe tej grupie dopiero po wylogowaniu i powtórnym zalogowaniu.

Grupy lokalne na maszynach nie będących kontrolerami domeny

Jeśli grupy tworzone są na osobnych maszynach nie podłączonych do sieci, maszynach należących do grupy roboczej, albo należących do domeny, lecz nie będących jej kontrolerami, wówczas nazywane są grupami lokalnymi i stosują się do nich następujące reguły:

- grup lokalnych używa się do nadawania uprawnień tylko do lokalnych zasobów i operacji na danym komputerze
- grupy lokalne są umiejscowione w bazie SAM – lokalnej bazie kont komputera
- do grupy lokalnej mogą należeć tylko konta użytkowników lokalnych, nie mogą do niej należeć konta użytkowników domenowych
- grupa lokalna nie może być elementem żadnej innej grupy
- grupy lokalne mogą być tworzone tylko przez członków grupy Administratorzy (Administrators) lub Operatorzy Kont (Account Operators)

Grupy lokalne dzielą się na zwykłe (tworzone po instalacji systemu) i wbudowane.

Grupy wbudowane mają z góry określony zestaw uprawnień i nie można ich usuwać. Można natomiast dodawać i usuwać z nich użytkowników.

Wbudowane grupy lokalne

Grupy te są widoczne w oknie programu „Computer Management” w pod-folderze „Grupy” folderu „Użytkownicy i grupy lokalne”. Istnieje kilka wbudowanych grupy lokalnych, niektóre z nich to: Administratorzy (Administrators), Użytkownicy (Users), Użytkownicy o Rozszerzonych Uprawnieniach (Power Users), Operatorzy Kopii Zapasowych (Backup Operators), Operatorzy drukarek (Print Operators). Użytkownicy z tych grup mają przydzielone standardowe uprawnienia, opisane poniżej.

Członkowie grupy Administratorzy mają pełne prawa do wszystkich zasobów i operacji na lokalnym komputerze.

Członkowie grupy Użytkownicy mogą uruchamiać aplikacje, używać lokalnych i sieciowych drukarek, zamykać i blokować system, nie mogą natomiast zarządzać użytkownikami i grupami, udostępniać folderów, ani dodawać drukarek lokalnych.

Członkowie grupy Użytkownicy o Rozszerzonych Uprawnieniach mogą wykonywać pewne zadania administracyjne, jak np. tworzenie kont użytkowników i grup lokalnych, modyfikowanie i usuwanie utworzonych przez siebie kont i grup, udostępnianie zasobów. Nie mogą natomiast modyfikować grup Administratorzy i Operatorzy Kopii Zapasowych, oraz tworzyć kopii zapasowych folderów i odtwarzać folderów z kopii zapasowych.

Członkowie grupy Operatorzy Kopii Zapasowych mogą wykonywać kopie zapasowe folderów i odtwarzać foldery z tych kopii, niezależnie od praw dostępu do folderów i umieszczonych w nich plików. Mogą również logować się do lokalnych komputerów i zamykać system na tych komputerów, ale nie mogą zmieniać ustawień mających związek z bezpieczeństwem.

Wbudowanych grup lokalnych nie można usuwać – próba usunięcia takiej grupy powoduje wypisanie komunikatu o błędzie.

Strategia A L P

Jest to najbardziej efektywna metoda nadawania określonych uprawnień do zasobów lub operacji na lokalnej maszynie wielu użytkownikom jednocześnie. Nazwa metody jest skrótem utworzonym z pierwszych liter angielskich słów „Account”, „Local” i „Permissions”. Polega na dodaniu kont użytkowników lokalnych (Accounts) do grupy lokalnej (Local) , a następnie nadaniu tej grupie określonych uprawnień (Permissions).

Tworzenie grup lokalnych

Aby utworzyć grupę lokalną, należy otworzyć w podanej kolejności:

Start -> Ustawienia -> Panel Sterowania -> Narzędzia Administracyjne -> Computer Management -> Użytkownicy i Grupy Lokalne,

następnie prawym przyciskiem myszy kliknąć folder „Grupy” i z otwartej w ten sposób listy wybrać opcję „Nowa Grupa”. Otworzy się wówczas okno, w którym należy wypełnić pola „Nazwa Grupy”, „Opis” i „Członkowie”.

Grupy domenowe

Grupy tworzone na **kontrolerach domeny** nazywane są grupami domenowymi i stosują się do nich następujące reguły:

- Grup domenowych używa się do nadawania praw dostępu do zasobów i operacji na dowolnym komputerze należącym do domeny
- Informacja o grupach domenowych umiejscowiona jest w bazie Active Directory
- Grupy domenowe dzielone są ze względu na typ – grupy bezpieczeństwa i grupy dystrybucyjne, oraz ze względu na zakres – lokalne grupy domenowe, globalne grupy domenowe i uniwersalne grupy domenowe
- Zasoby, do których nadawane są prawa grupom domenowym, nie muszą znajdować się na kontrolerze domeny, lecz mogą być umiejscowione na dowolnym komputerze należącym do tej domeny
- Oprócz wymienionych wyżej rodzajów grup domenowych istnieją jeszcze tak zwane grupy specjalne. Do grup tych użytkownicy nie są przypisywani przez administratora lub innego uprawnionego użytkownika, lecz należą do nich domyślnie, lub stają się ich członkami poprzez wykonywanie określonych operacji. Np. z chwilą poprawnego zalogowania do domeny, użytkownik staje się członkiem grupy specjalnej „Uwierzytelnieni użytkownicy” (Authenticated Users). Przykłady innych grup specjalnych to „Everyone” i „Domain Users”. Grupy specjalne nie są widoczne w oknie programu „Active Directory Users and Computers”. Można im nadawać uprawnienia do zasobów, nie można natomiast zmieniać ani odczytywać przynależności użytkowników do grup specjalnych.

Wbudowane i predefiniowane grupy domenowe

Wbudowane grupy domenowe są widoczne w folderze „Builtin” w oknie programu „Active Directory Users and Computers”. Należą one do kategorii tzw. lokalnych grup domenowych, omawianych w dalszym ciągu.

Istnieje kilkanaście wbudowanych grup domenowych. Niektóre z nich mają takie same uprawnienia jak odpowiednie wbudowane grupy lokalne. Należą do nich m.in.: Administratorzy, Użytkownicy, Operatorzy Kont i Operatorzy Kopii Zapasowych. Nie istnieje natomiast wbudowana grupa domenowa Użytkownicy o Rozszerzonych Uprawnieniach (Power Users).

Grupy predefiniowane są widoczne w folderze „Users” w oknie programu „Active Directory Users and Computers”. Należą one do kategorii tzw. globalnych grup domenowych, omawianych w dalszym ciągu.

Wbudowanych i predefiniowanych grup domenowych nie można usuwać, próba usunięcia kończy się komunikatem o błędzie.

Grupy zabezpieczeniowe i dystrybucyjne

Grupy zabezpieczeniowe są tworzone, najogólniej mówiąc, do celów związanych z bezpieczeństwem w sieci, takich jak np. nadawanie praw dostępu do chronionych zasobów przechowywanych na komputerach wchodzących w skład domeny.

Grupy dystrybucyjne są tworzone w celu umożliwienia operacji nie wykorzystujących mechanizmów bezpieczeństwa, jak np. wysłanie wiadomości pocztowej do wszystkich

użytkowników umieszczonych na liście dystrybucyjnej. Grupom dystrybucyjnym nie można nadawać praw dostępu. Są potrzebne, gdyż niektóre aplikacje nie mogą korzystać z grup zabezpieczeniowych, a tylko z grup dystrybucyjnych.

Grupy lokalne, globalne i uniwersalne

Grup domenowych globalnych używa się do łączenia użytkowników o podobnych lub takich samych wymaganiach odnośnie dostępu do zasobów i operacji na komputerach w określonej domenie. Elementami grupy globalnej mogą być użytkownicy domenowi lub inne grupy globalne, ale tylko z tej samej domeny, do której należy dana grupa globalna.

Grup domenowych lokalnych używa się do nadawania uprawnień do zasobów i operacji na komputerach wchodzących w skład domeny, do której należy dana grupa lokalna. Grupa taka jest widoczna tylko na tym komputerze, na którym została utworzona, oraz na kontrolerze domeny. Można jej nadawać uprawnienia tylko do lokalnych zasobów komputera – stąd nazwa. Lokalne grupy domenowe nie mogą należeć do innych grup, natomiast grupy globalne z dowolnej domeny, użytkownicy z dowolnej domeny, oraz grupy uniwersalne mogą należeć do domenowej grupy lokalnej.

Różnice między lokalnymi a globalnymi grupami domenowymi zostaną zilustrowane przy omawianiu tzw. strategii A G DL P.

Grup domenowych uniwersalnych używa się do nadawania uprawnień do zasobów i operacji na komputerach z dowolnej domeny. Elementami grupy uniwersalnej mogą być dowolne grupy lub konta użytkowników, niekoniecznie z tej samej domeny, w której utworzona została grupa uniwersalna. Sama grupa uniwersalna może być elementem dowolnej innej grupy uniwersalnej albo lokalnej. Nie może natomiast być elementem żadnej globalnej grupy domenowej.

Strategia A G DL P

Jest to najbardziej efektywna metoda nadawania określonych uprawnień do zasobów i operacji na maszynach należących do określonej domeny. Nazwa metody jest skrótem utworzonym z pierwszych liter angielskich słów „Account”, „Global”, „Domain Local” i „Permissions”. Polega na dodaniu kont użytkowników domenowych (Accounts) do grup globalnych (Global), umieszczeniu tych grup w domenowej grupie lokalnej (Domain Local), a następnie nadaniu tej grupie określonych uprawnień (Permissions).

Tworzenie grup domenowych

Aby utworzyć grupę domenową, należy zalogować się na kontrolerze domeny i w podanej kolejności otworzyć:

Start -> Ustawienia -> Panel Sterowania -> Narzędzia Administracyjne -> Użytkownicy i Komputery Active Directory,

następnie rozwinąć listę zasobów domeny, prawym przyciskiem myszy kliknąć folder „Użytkownicy” i na otwartej w ten sposób liście wskazać opcje „Nowy”, a potem „Grupa”. Otworzy się wówczas okno „Nowy Obiekt – Grupa”, w którym należy wypełnić pola „Nazwa

Grupy” i „Nazwa Grupy (Pre-Windows 2000)”, oraz wybrać typ i zakres tworzonej grupy domenowej.

Usuwanie grup domenowych

Usunięcie grupy powoduje tylko usunięcie uprawnień dla obiektów należących do grupy, nie powoduje natomiast usunięcia kont ani grup będących elementami usuwanej grupy. Każda grupa ma swój niepowtarzalny identyfikator – SID (Security Identifier). Identyfikator ten nigdy nie będzie użyty ponownie, nawet jeśli zostanie utworzona grupa o takiej samej nazwie jak nazwa usuniętej grupy.

Aby usunąć grupę, należy w pierwszym rzędzie zalogować się na kontrolerze domeny i uruchomić narzędzie „Użytkownicy i Komputery Active Directory”. Następnie trzeba rozwinąć listę zasobów domeny, kliknąć folder zawierający tę grupę i prawym przyciskiem myszy kliknąć nazwę grupy. Z otwartej w ten sposób listy wybrać opcję „Usuń”, co spowoduje usunięcie grupy.

Uwaga: nie można usunąć lokalnej grupy wbudowanej ani globalnej predefiniowanej.

Dodawanie elementów do grupy domenowej

W celu dodania elementu do grupy domenowej logujemy się na kontrolerze domeny i uruchamiamy narzędzie „Użytkownicy i Komputery Active Directory”. Następnie w drzewie zasobów domeny zaznaczamy folder „Użytkownicy”, w panelu szczegółów klikamy dwukrotnie wybraną grupę, w oknie jej właściwości otwieramy kartę „Członkowie” i wciskamy przycisk „Dodaj”. Otwiera się wtedy okno „Wybierz użytkowników, kontakty,...”, w którym wciskamy „Zaawansowane”, następnie przycisk „Szukaj”. Z otwartej w ten sposób listy wybieramy konto lub grupę, którą chcemy dodać i wciskamy przycisk „Dodaj”. Wciskamy przycisk „OK”, co spowoduje zamknięcie okna „Wybierz użytkowników, kontakty,...”, kolejne wciśnięcie „OK” spowoduje zamknięcie okna „Właściwości grupy”. Wybrane konto lub grupa zostanie dodana do grupy domenowej.

Polecenie net group

Służy do dodawania, usuwania lub modyfikacji grup lokalnych lub globalnych grup domenowych. Oto przykłady komendy „net group”:

net group NEWUSERS – wypisuje listę użytkowników lokalnej grupy NEWUSERS

net group SALES /domain – wypisuje listę użytkowników domenowej grupy SALES

net group MANAGERS /add /domain – tworzy domenową grupę MANAGERS w bazie Active Directory

Przełącznik “/delete” służy do usuwania wskazanej grupy.