

T: Grupy lokalne i domenowe.

Zadanie 1:

Zapoznaj się z zawartością witryn na temat domyślnych grup:

lokalnych <http://technet.microsoft.com/pl-pl/library/cc785098%28WS.10%29.aspx>

domenowych <http://technet.microsoft.com/pl-pl/library/cc756898%28WS.10%29.aspx>.

Grupy służą do łączenia kont użytkowników, kont komputerów i kont grup w jednostki, którymi można zarządzać. Praca z grupami zamiast z indywidualnymi użytkownikami ułatwia utrzymanie sieci i administrowanie nią.

Grupy lokalne komputera to grupy użytkowników w systemie operacyjnym, które można stosować tylko do lokalnych obiektów w systemie – grupy lokalne w systemie autonomicznym. Folder Grupy, znajdujący się w przystawce Użytkownicy i grupy lokalne w programie Microsoft Management Console (MMC), wyświetla domyślne grupy lokalne, a także grupy lokalne utworzone przez użytkownika. Domyślne grupy lokalne są automatycznie tworzone podczas instalacji serwera autonomicznego lub serwera członkowskiego z systemem Windows Server 2003. Dzięki przynależności do grupy lokalnej użytkownik ma możliwości i prawa do wykonywania różnych zadań na komputerze lokalnym.

Grupy domenowe występują tylko na kontrolerach domen i umożliwiają dostęp do zasobów sieciowych zarządzanych przez serwer.

Do grup lokalnych można dodawać konta użytkowników lokalnych, konta użytkowników domeny, konta komputerów i konta grup. Do kont grup domeny nie można jednak dodawać kont użytkowników lokalnych i kont grup lokalnych.

Zadanie 2:

Wymień grupy lokalne występujące w twoim stanowisku komputerowym w pracowni.

Grupy w usłudze Active Directory umożliwiają:

- Uproszczenie administracji przez przypisanie uprawnień do zasobu udostępnionego grupie, a nie poszczególnym użytkownikom. W ten sposób wszyscy członkowie grupy mają te same prawa dostępu do zasobu.
- Delegowanie administracji przez jednokrotne przypisanie praw użytkownika za pomocą przystawki Zasady grupy, a następnie dodanie do grupy niezbędnych członków, którzy mają mieć te same prawa, co grupa.
- Tworzenie list dystrybucyjnych poczty e-mail.

Różnice pomiędzy funkcjonowaniem grup i jednostek organizacyjnych w Active Directory:

- Przynależność do grup widoczna dla użytkowników – np. każdy użytkownik zmieniając uprawnienia do zasobów na partycjach NTFS można przeglądać użytkowników i grupy należące do danej domeny, nie można natomiast bez odpowiednich uprawnień przeglądać struktury Active Directory.
- Przynależność do wielu grup – użytkownik może należeć tylko do jednej OU, ale do wielu grup.
- Grupa jako wystawca zabezpieczeń – grupy posiadają niepowtarzalne SID i dzięki temu mogą być kojarzone we wpisach kontroli dostępu ACE. OU nie mogą być stosowane w zasadach zabezpieczeń na poziomie obiektów.
- Funkcjonalność poczty elektronicznej dla grup – grupy z obsługą poczty elektronicznej mogą posłużyć do rozsyłania wiadomości e-mail, OU niestety nie.
- Jednostki organizacyjne OU porządkują strukturę Active Directory, pozwalają wykorzystywać usługi zasady grup dla użytkowników i komputerów.

W poniższej tabeli opisano grupy domyślne znajdujące się w folderze Grupy oraz prawa użytkownika dla każdej grupy. Prawa te są przyznawane w ramach lokalnych zasad zabezpieczeń.

Grupa	Opis	Domyślne prawa użytkownika
Administratorzy	Członkowie tej grupy mają pełną kontrolę nad	Dostęp do tego komputera z sieci; Dopasowywanie

Grupa	Opis	Domyślne prawa użytkownika
	serwerem i w razie potrzeby mogą przypisywać użytkownikom prawa użytkownika i uprawnienia kontroli dostępu. Konto Administrator jest także członkiem domyślnym. Kiedy dany serwer zostanie przyłączony do domeny, do tej grupy zostanie automatycznie dołączona grupa Administratorzy domeny. Ponieważ grupa ta ma pełną kontrolę nad serwerem, należy ostrożnie dodawać do niej użytkowników.	przydziałów pamięci dla procesu; Zezwalanie na lokalne logowanie się; Zezwalanie na logowanie się przez usługi terminalowe; Tworzenie kopii zapasowych plików i katalogów; Pomijanie sprawdzania przechodzenia; Zmienianie czasu systemowego; Tworzenie pliku stronicowania; Debugowanie programów; Wymuszanie zamknięcia systemu z systemu zdalnego; Podwyższanie priorytetu w harmonogramie; Ładowanie i zwalnianie sterowników urządzeń; Zarządzanie dziennikiem inspekcji i zabezpieczeń; Modyfikowanie wartości środowiskowych oprogramowania układowego; Wykonywanie zadań związanych z konserwacją woluminów; Profilowanie pojedynczego procesu; Profilowanie wydajności systemu; Wyjmowanie komputera ze stacji dokującej; Przywracanie plików i katalogów; Zamykanie systemu; Przejmowanie na własność plików lub innych obiektów.
Operatorzy kopii zapasowych	Członkowie tej grupy mogą tworzyć kopie zapasowe plików na serwerze i przywracać je, bez względu na uprawnienia chroniące te pliki. Dzieje się tak dlatego, że prawo tworzenia kopii zapasowych jest ważniejsze od wszystkich uprawnień do plików. Nie mogą oni zmieniać ustawień zabezpieczeń.	Dostęp do tego komputera z sieci; Zezwalanie na logowanie się lokalnie; Tworzenie kopii zapasowych plików i katalogów; Pomijanie sprawdzania przechodzenia; Przywracanie plików i katalogów; Zamykanie systemu.
Administratorzy DHCP (instalowani z usługą serwera DHCP)	Członkowie tej grupy mają dostęp administracyjny do usługi serwera DHCP (Dynamic Host Configuration Protocol). Ta grupa umożliwia przypisanie ograniczonego dostępu administracyjnego tylko do usługi serwera DHCP, bez przyznania pełnego dostępu do serwera. Członkowie tej grupy mogą administrować usługą DHCP na serwerze przy użyciu konsoli DHCP lub polecenia Netsh, ale nie mogą wykonywać innych akcji administracyjnych na serwerze.	Brak domyślnych praw użytkownika.
Użytkownicy DHCP (instalowani z usługą serwera DHCP)	Członkowie tej grupy mają dostęp tylko do odczytu do usługi serwera DHCP. Pozwala to im na przeglądanie informacji i właściwości przechowywanych na określonym serwerze DHCP. Informacje te są przydatne dla personelu obsługi, gdy musi on uzyskać raporty o stanie usługi DHCP.	Brak domyślnych praw użytkownika.
Goście	Członkowie tej grupy mają tymczasowy profil tworzony w momencie logowania, który po wylogowaniu członka jest usuwany. Konto Gość (domyślnie wyłączone) jest także domyślnym członkiem tej grupy.	Brak domyślnych praw użytkownika.
Grupa usług pomocy	Ta grupa umożliwia administratorom ustawianie praw typowych dla wszystkich aplikacji pomocy technicznej. Domyślnie jedynym członkiem grupy jest konto związane z aplikacjami pomocy technicznej firmy Microsoft, takimi jak Pomoc zdalna. Nie należy dodawać użytkowników do tej grupy.	Brak domyślnych praw użytkownika.
Operatorzy konfiguracji sieci	Członkowie tej grupy mogą zmieniać ustawienia TCP/IP oraz odnawiać i zwalniać adresy TCP/IP. Ta grupa nie ma członków domyślnych.	Brak domyślnych praw użytkownika.
Użytkownicy monitora wydajności	Członkowie tej grupy mogą monitorować liczniki wydajności na serwerze, lokalnie i z klientów zdalnych, nie będąc członkami grup Administratorzy i Użytkownicy dzienników wydajności.	Brak domyślnych praw użytkownika.

Grupa	Opis	Domyślne prawa użytkownika
Użytkownicy dzienników wydajności	Członkowie tej grupy mogą zarządzać licznikami, dziennikami i alertami wydajności na serwerze, lokalnie i z klientów zdalnych, nie będąc członkami grupy Administratorzy.	Brak domyślnych praw użytkownika.
Użytkownicy zaawansowani	Członkowie tej grupy mogą tworzyć konta użytkowników, a następnie modyfikować i usuwać utworzone przez siebie konta. Mogą tworzyć grupy lokalne, a następnie dodawać użytkowników do utworzonych przez siebie grup lokalnych i usuwać ich. Mogą również dodawać lub usuwać użytkowników w ramach grup Użytkownicy zaawansowani, Użytkownicy i Goście. Członkowie mogą tworzyć zasoby udostępnione i administrować utworzonymi przez siebie zasobami udostępnionymi. Nie mogą przejmować plików na własność, tworzyć kopii zapasowych katalogów i przywracać ich, łądować i zwalniać sterowników urządzeń ani zarządzać dziennikami zabezpieczeń i inspekcji.	Dostęp do tego komputera z sieci; Zezwalanie na logowanie się lokalne; Pomijanie sprawdzania przechodzenia; Zmienianie czasu systemowego; Profilowanie pojedynczego procesu; Wyjmowanie komputera ze stacji dokującej; Zamykanie systemu.
Operatorzy drukowania	Członkowie tej grupy mogą zarządzać drukarkami i kolejkami wydruku.	Brak domyślnych praw użytkownika.
Użytkownicy pulpitu zdalnego	Członkowie tej grupy mogą logować się zdalnie na serwer.	Zezwalanie na logowanie się przez usługi terminalowe.
Replikator	Grupa Replikator obsługuje funkcje replikacji. Jedynym członkiem grupy Replikator powinno być konto użytkownika domeny służące do logowania usługi Replikator na kontrolerze domeny. Nie należy dodawać kont prawdziwych użytkowników do tej grupy.	Brak domyślnych praw użytkownika.
Użytkownicy serwera terminali	Ta grupa zawiera wszystkich użytkowników, którzy są aktualnie zalogowani w systemie przy użyciu serwera terminali. Każdy program, który użytkownik może uruchomić w systemie Windows NT 4.0, będzie uruchomiony dla członka grupy Użytkownik serwera terminali. Domyślne uprawnienia przyznane tej grupie umożliwiają jej członkom uruchamianie większości starszych programów.	Brak domyślnych praw użytkownika.
Użytkownicy	Członkowie tej grupy mogą wykonywać typowe zadania, np. uruchamiać aplikacje, korzystać z drukarek lokalnych i sieciowych oraz blokować serwer. Użytkownicy nie mogą udostępniać katalogów ani tworzyć drukarek lokalnych. Domyślnie grupy Użytkownicy domeny, Użytkownicy uwierzytelnieni i Interakcyjni są członkami tej grupy. Dlatego każde konto użytkownika utworzone w domenie staje się członkiem tej grupy.	Dostęp do tego komputera z sieci; Zezwalanie na logowanie się lokalne; Pomijanie sprawdzania przechodzenia.
Użytkownicy WINS (instalowani z usługą WINS)	Członkowie tej grupy mają dostęp tylko do odczytu do usługi WINS (Windows Internet Name Service). Pozwala to im na przeglądanie informacji i właściwości przechowywanych na określonym serwerze WINS. Informacje te są przydatne dla personelu obsługi, gdy musi on uzyskać raporty o stanie usługi WINS.	Brak domyślnych praw użytkownika.