

T: Funkcjonowanie grup użytkowników w systemach Windows.

Wskazówki dotyczące procesu tworzenia grupy użytkowników:

- Przegląd pojęć dotyczących grup.

Grupa jest kolekcją kont użytkowników i komputerów, kontaktów i innych grup, którymi można zarządzać jako jednostką. Konta użytkowników i komputerów należące do określonej grupy są nazywane członkami grupy. Grupy upraszczają administrację, umożliwiając przypisanie wspólnego zestawu uprawnień i praw wielu kontom jednocześnie, zamiast każdemu kontu pojedynczo. Uprawnienia definiują typ dostępu udzielanego użytkownikom lub grupom do obiektu lub właściwości obiektu. Grupy mogą być oparte na katalogu lub lokalne dla określonego komputera. Grupy w usłudze Active Directory to obiekty typu katalog znajdujące się w obiektach typu kontener, będących domenami lub jednostkami organizacyjnymi. Podczas instalacji usługi Active Directory są tworzone grupy domyślne. Ponadto jest dostępna opcja tworzenia grup.
- Określenie, jakiego typu grupa ma być utworzona (grupa zabezpieczeń lub grupa dystrybucyjna).

W usłudze Active Directory istnieją dwa typy grup: grupy dystrybucyjne i grupy zabezpieczeń. Grupy dystrybucyjne mogą być używane tylko z aplikacjami poczty e-mail (np. Exchange) do wysyłania poczty e-mail do grup użytkowników. Grupy dystrybucyjne nie obsługują zabezpieczeń, co oznacza, że nie są wyświetlane na listach arbitralnej kontroli dostępu (DACL, discretionary access control list). Jeśli jest potrzebna grupa służąca do kontroli dostępu do zasobów udostępnionych, należy utworzyć grupę zabezpieczeń. Grupy zabezpieczeń, jeśli są używane z rozważą, stanowią wydajny sposób udzielania dostępu do zasobów w sieci. Za pomocą grup zabezpieczeń można wykonywać następujące operacje:

 - Przypisywanie praw użytkownika grupom zabezpieczeń w usłudze Active Directory. Prawa użytkownika są przypisywane grupie zabezpieczeń w celu ustalenia czynności, jakie członkowie danej grupy mogą wykonać w zakresie domeny (lub lasu). Prawa użytkownika są automatycznie przypisywane niektórym grupom zabezpieczeń podczas instalowania usługi Active Directory, aby ułatwić administratorom określenie roli administracyjnej poszczególnych osób w domenie. Za pomocą przystawki Zasady grupy można przypisać grupom zabezpieczeń prawa użytkownika, aby ułatwić delegowanie określonych zadań. Przypisując delegowane zadania, należy zachować dużą ostrożność, ponieważ niedoświadczony użytkownik mający zbyt wiele praw w grupie zabezpieczeń stanowi zagrożenie dla bezpieczeństwa sieci.
 - Przypisywanie grupom zabezpieczeń uprawnień do zasobów. Uprawnień nie należy mylić z prawami użytkownika. Uprawnienia są przypisywane grupom zabezpieczeń dla określonego zasobu udostępnionego. Uprawnienia decydują o tym, kto może uzyskiwać dostęp do zasobu i na jakim poziomie (na przykład Pełna kontrola). Niektóre uprawnienia ustawione dla obiektów domeny są przypisywane automatycznie, aby określić różne poziomy dostępu grup domyślnych, takich jak Operatorzy kont czy Administratorzy domeny. Grupy zabezpieczeń są wymieniane na listach DACL, które określają uprawnienia do zasobów i obiektów. Administratorzy powinni przypisywać uprawnienia do zasobów (udziałów plików, drukarek itd.) grupom zabezpieczeń, a nie pojedynczym użytkownikom. Przypisując uprawnienia grupie, nie trzeba wielokrotnie powtarzać tej samej procedury dla każdego użytkownika. Każde konto dodane do grupy otrzymuje prawa przypisane tej grupie w usłudze Active Directory i uprawnienia tej grupy do określonych zasobów. Podobnie jak grupy dystrybucyjne, grupy zabezpieczeń mogą być używane jako adresaci poczty e-mail. Wysłanie wiadomości e-mail do grupy powoduje wysłanie tej wiadomości do wszystkich członków danej grupy.
- Określenie zakresu grupy (uniwersalny, globalny lub lokalny w domenie).

Wszystkie grupy, zarówno grupy zabezpieczeń, jak i grupy dystrybucyjne, mają zakres, który identyfikuje obszar w drzewie domen lub lesie, do którego dana grupa ma zastosowanie. Granica, zasięg, czy też zakres grupy określany jest także przez ustawienie poziomu funkcjonalności domeny, w której znajduje się grupa. Istnieją trzy zakresy grupy: uniwersalny, globalny oraz lokalny w domenie.

Grupy o zakresie lokalnym w domenie ułatwiają określanie dostępu do zasobów pojedynczej domeny i zarządzanie nim.

Grup o zakresie globalnym należy używać do zarządzania obiektami katalogowymi, które wymagają codziennej obsługi, takimi jak konta użytkowników i komputerów. Grupy o zakresie globalnym nie są replikowane poza ich własną domeną, więc konta należące do grupy o zakresie globalnym można często zmieniać, nie generując ruchu związanego z replikacją do wykazu globalnego.

Grup o zakresie uniwersalnym należy używać do konsolidowania grup, które obejmują kilka domen. Aby to zrobić, należy dodać konta do grup o zakresie globalnym, a następnie zagnieździć te grupy w

grupach o zakresie uniwersalnym. W przypadku takiej strategii wszelkie zmiany członkostwa grup o zakresie globalnym nie mają wpływu na grupy o zakresie uniwersalnym.

- Użycie odpowiedniego narzędzia administracyjnego do utworzenia grupy:

Aby utworzyć grupę lokalną na stacji roboczej lub serwerze członkowskim, należy użyć narzędzia Użytkownicy i grupy lokalne w przystawce Zarządzanie komputerem.

Aby utworzyć grupę w domenie systemu Windows Server 2003, należy użyć przystawki Użytkownicy i komputery usługi Active Directory.