Podstawy teoretyczne - konta użytkowników, komputerów i grup

Podstawowe pojęcia

Jednostka organizacyjna (OU)

Jednostka organizacyjna (OU) to szczególnie przydatny typ obiektu w katalogu, który jest zawarty w domenach. Jednostki organizacyjne są kontenerami usługi Active Directory, w których można umieszczać użytkowników, grupy, komputery i inne jednostki organizacyjne. Jednostka organizacyjna nie może zawierać obiektów z innych domen.

Jednostka organizacyjna jest najmniejszym zakresem, do jakiego można przypisywać ustawienia zasad grupy lub delegować uprawnienia administracyjne. Za pomocą jednostek organizacyjnych można tworzyć w domenie kontenery reprezentujące hierarchiczne struktury logiczne w organizacji. Dzięki temu można zarządzać konfiguracją oraz korzystać z kont i zasobów zgodnie z modelem organizacji.

Jednostki organizacyjne mogą zawierać inne jednostki organizacyjne. W razie potrzeby możliwe jest rozszerzenie hierarchii jednostek organizacyjnych w celu dopasowania jej do hierarchii organizacji wewnątrz domeny. Zastosowanie jednostek organizacyjnych ułatwia minimalizację wymaganej liczby domen w sieci.

Jednostki organizacyjne pozwalają na utworzenie modelu administracyjnego, który można skalować bez ograniczeń. Określony użytkownik może mieć uprawnienia administracyjne dla wszystkich jednostek organizacyjnych w domenie lub dla jednej jednostki organizacyjnej. Administrator jednostki organizacyjnej nie musi mieć uprawnień administracyjnych dla pozostałych jednostek organizacyjnych w domenie.

Konta użytkowników

Konta użytkowników usługi Active Directory reprezentują jednostki fizyczne, takie jak osoby. Konta użytkowników mogą także służyć jako dedykowane konta usług dla niektórych aplikacji.

Konta użytkowników są nazywane także podmiotami zabezpieczeń. Podmioty zabezpieczeń to obiekty katalogu, którym są automatycznie przypisywane identyfikatory zabezpieczeń (SID) umożliwiające uzyskanie dostępu do zasobów domeny. Główne funkcje konta użytkownika:

- Uwierzytelnianie tożsamości użytkownika.
  Konto użytkownika umożliwia logowanie się na komputerach oraz logowanie się do domen przy użyciu tożsamości, która może być uwierzytelniona przez domenę. Każdy użytkownik logujący się do sieci powinien mieć własne, unikatowe konto użytkownika oraz hasło. Aby zapewnić maksymalne zabezpieczenia, należy unikać sytuacji, w których wielu użytkowników korzysta z jednego konta.
- Udzielanie lub odmawianie dostępu do zasobów domeny.
  Po uwierzytelnieniu następuje udzielenie lub odmowa dostępu do zasobów domeny na postawie jawnych uprawnień przypisanych użytkownikowi dla tych zasobów.

Kontener **Użytkownicy**, który znajduje się w przystawce **Użytkownicy i komputery usługi Active Directory**, zawiera trzy wbudowane konta użytkowników: Administrator, Gość i Pomocnik. Te wbudowane konta użytkowników są tworzone automatycznie podczas tworzenia domeny.

Konta komputerów

Każdy **komputer** z systemem Windows NT, oraz każdy serwer z systemem Windows Server, który jest przyłączany do domeny, ma konto komputera. Podobnie jak konta użytkowników, konta komputerów umożliwiają uwierzytelnianie oraz inspekcję dostępu do sieci i zasobów domeny. Każde konto komputera musi być unikatowe.

Za pomocą przystawki **Użytkownicy i komputery usługi Active Directory** można dodawać, wyłączać, resetować, modyfikować i usuwać konta użytkowników oraz komputerów. Konto komputera można również utworzyć podczas przyłączania komputera do domeny.

Jeśli poziomem funkcjonalności domeny jest poziom systemu Windows Server 2012 lub Windows Server 2012 R2, atrybut **lastLogonTimestamp** jest używany do śledzenia godziny ostatniego logowania konta użytkownika lub komputera. Ten atrybut jest replikowany w domenie. Udostępnia on istotne informacje o historii użytkownika lub komputera.

Każde **konto komputera** tworzone w usługach domenowych w usłudze Active Directory (AD DS) ma względną nazwę wyróżniającą, nazwę komputera stosowaną w systemach starszych niż Windows 2000 (nazwę konta Menedżera kont zabezpieczeń - SAM), sufiks podstawowej domeny DNS, nazwę hosta DNS oraz główną nazwę usługi (SPN). Administrator wprowadza nazwę komputera podczas tworzenia konta danego komputera. Ta nazwa komputera jest używana jako względna nazwa wyróżniająca LDAP.

Usługi AD DS sugerują nazwę systemu starszego niż Windows 2000 przy użyciu pierwszych 15 bajtów względnej nazwy wyróżniającej. Administrator może zmienić nazwę systemu starszego niż Windows 2000 **w dowolnym** momencie.

Nazwa DNS hosta jest określana jako pełna nazwa komputera. Jest to w pełni kwalifikowana nazwa domeny DNS (FQDN). Pełna nazwa komputera jest złączeniem nazwy komputera (pierwszych 15 bajtów nazwy konta SAM dla konta komputera, bez znaku „$”) oraz sufiksu podstawowej domeny DNS (nazwy DNS domeny, w której istnieje konto komputera).

Domyślnie sufiks podstawowej domeny DNS w nazwie FQDN komputera musi być taki sam jak nazwa domeny usługi Active Directory, w której znajduje się komputer. Aby umożliwić stosowanie różnych sufiksów podstawowej domeny DNS, administrator domeny może utworzyć ograniczoną listę dozwolonych sufiksów, tworząc atrybut **msDS-AllowedDNSSuffixes** w kontenerze obiektu domeny. Administrator domeny tworzy ten atrybut i zarządza nim za pomocą interfejsów usługi Active Directory (ADSI) lub protokołu LDAP.

Nazwa SPN jest atrybutem wielowartościowym. Zazwyczaj tworzy się ją na podstawie nazwy DNS hosta. Nazwa SPN jest używana podczas uwierzytelniania obustronnego między klientem i serwerem obsługującym określoną usługę. Klient znajduje konto komputera na podstawie nazwy SPN usługi, z którą próbuje nawiązać połączenie. Członkowie grupy Administratorzy domeny mogą modyfikować nazwę SPN.

Grupa

Grupa jest kolekcją kont użytkowników i komputerów, kontaktów i innych grup, którymi można zarządzać jako jednostką. Konta użytkowników i komputerów, które należą do określonej grupy, są nazywane elementami członkowskimi grupy.

Grupy w usługach domenowych w usłudze Active Directory (AD DS, Active Directory Domain Services) to obiekty katalogu znajdujące się w obiektach kontenera będących domenami lub jednostkami organizacyjnymi. Podczas instalacji usług AD DS jest dostępny zestaw grup domyślnych. Możliwe jest także tworzenie grup.

Grupy w usługach AD DS umożliwiają:

- Uproszczenie administracji przez przypisanie uprawnień do zasobu udostępnionego grupie, a nie poszczególnym użytkownikom. Przypisanie uprawnień do grupy powoduje udzielenie tego samego dostępu do zasobu wszystkim elementom członkowskim tej grupy.
- Delegowanie administracji przez jednokrotne przypisanie praw użytkownika grupie za pomocą zasad grupy. Można wtedy dodać do grupy członków, którzy mają mieć te same prawa co grupa.
- Tworzenie list dystrybucyjnych poczty e-mail.

Grupy różnią się zakresem i typem. Zakres grupy określa obszar domeny lub lasu, do którego grupa ma zastosowanie. Typ grupy określa, czy przy użyciu grupy można przypisać uprawnienia do zasobu udostępnionego (dotyczy grup zabezpieczeń), czy tylko utworzyć listy dystrybucyjne poczty e-mail (dotyczy grup dystrybucyjnych).

Istnieją również grupy, których członkostw nie można modyfikować ani wyświetlać. Te grupy są nazywane tożsamościami specjalnymi. Odpowiadają one różnym użytkownikom w różnym czasie, w zależności od okoliczności. Na przykład grupa Wszyscy jest tożsamością specjalną odpowiadającą wszystkim bieżącym użytkownikom sieciowym, w tym gościom i użytkownikom z innych domen.

Poniżej zawarto dodatkowe informacje dotyczące kont grup w usługach AD DS.

Opis grup domyślnych

Grupy domyślne, takie jak Administratorzy domeny, są grupami zabezpieczeń tworzonymi automatycznie podczas tworzenia domeny usługi Active Directory. Te wstępnie zdefiniowane grupy ułatwiają kontrolowanie dostępu do zasobów udostępnionych i delegowanie określonych ról administracyjnych na poziomie całej domeny.

Wielu grupom domyślnym jest automatycznie przypisywany zestaw praw użytkownika, które upoważniają członków grupy do wykonywania w domenie określonych czynności, takich jak logowanie się do systemu lokalnego czy wykonywanie kopii zapasowych plików i folderów. Na przykład członek grupy Operatorzy kopii zapasowych ma prawo do wykonywania kopii zapasowych w przypadku wszystkich kontrolerów domeny w domenie.

Po dodaniu do grupy użytkownik otrzymuje następujące prawa:

- Wszystkie prawa użytkownika, które są przypisane do grupy
- Wszystkie uprawnienia do zasobów udostępnionych, które są przypisane do grupy

Grupy domyślne znajdują się w kontenerach **Wbudowane** (**Builtin**) i **Użytkownicy** (**Users**). Grupy domyślne w kontenerze **Wbudowane** mają zakres grupy **Lokalna domenowa**. Nie można zmieniać zakresu i typu tych grup. Kontener **Użytkownicy** zawiera grupy o zakresie globalnym i grupy o zakresie lokalnym w domenie. Grupy zawarte w tych kontenerach można przenosić do innych grup lub jednostek organizacyjnych, ale nie do innych domen.

Opis zakresu grupy

Grupy różnią się zakresem określającym obszar drzewa domen lub lasu, do którego grupa ma zastosowanie. Istnieją trzy zakresy grupy: lokalny w domenie, globalny oraz uniwersalny.

Opis grup lokalnych w domenie

Elementami członkowskimi grup lokalnych w domenie mogą być inne grupy i konta z domen systemów Windows Server. Elementom członkowskim tych grup można przypisywać uprawnienia tylko w danej domenie.

Grupy o zakresie lokalnym w domenie ułatwiają określanie dostępu do zasobów pojedynczej domeny i zarządzanie nim. Te grupy mogą zawierać jako elementy członkowskie:

- grupy o zakresie globalnym;
- grupy o zakresie uniwersalnym;
- konta;

- inne grupy o zakresie lokalnym w domenie;
- dowolną kombinację powyższych kont i grup.

Na przykład aby udostępnić pięciu użytkownikom określoną drukarkę, wszystkie pięć kont tych użytkowników można umieścić na liście uprawnień do drukarki. Aby jednak tym pięciu użytkownikom udzielić później dostęp do nowej drukarki, należy ponownie umieścić ich konta na liście uprawnień do nowej drukarki.

Niewielkim nakładem pracy to rutynowe zadanie administracyjne można uprościć, tworząc grupę o zakresie lokalnym w domenie i przypisując tej grupie uprawnienia dostępu do drukarki. Można umieścić pięć kont użytkowników w grupie o zakresie globalnym, a następnie dodać tę grupę do grupy o zakresie lokalnym w domenie. Aby tym pięciu użytkownikom udzielić dostępu do nowej drukarki, wystarczy przypisać grupie o zakresie lokalnym w domenie uprawnienia dostępu do nowej drukarki. Wszystkie elementy członkowskie grupy o zakresie globalnym automatycznie uzyskają dostęp do nowej drukarki.

Opis grup globalnych

Elementami członkowskimi grup globalnych mogą być inne grupy i konta tylko z domeny, w której grupa jest zdefiniowana. Elementom członkowskim tych grup można przypisać uprawnienia w dowolnej domenie w lesie.

Grupy o zakresie globalnym służą do zarządzania obiektami katalogu, które wymagają codziennej obsługi, takimi jak konta użytkowników i komputerów. Grupy o zakresie globalnym nie są replikowane poza własną domeną, więc konta należące do grupy o zakresie globalnym mogą często zmieniać się, nie generując ruchu sieciowego replikacji do wykazu globalnego.

Mimo że prawa i uprawnienia dotyczą tylko domeny, w której je przypisano, stosując grupy o zakresie globalnym w jednolity sposób w odpowiednich domenach, można skonsolidować odwołania do kont o podobnych celach. Upraszcza to i usprawnia zarządzanie grupami w różnych domenach. Na przykład w przypadku sieci z dwiema domenami, Europa i StanyZjednoczone, jeśli w domenie StanyZjednoczone istnieje grupa o zakresie globalnym o nazwie KsięgowośćKG, w domenie Europa również powinna znajdować się grupa o nazwie KsięgowośćKG (chyba że w domenie Europa nie ma funkcji księgowości).

Ważne

Zdecydowanie zaleca się, aby przy określaniu uprawnień do obiektów katalogu domeny replikowanych w wykazie globalnym używać grup globalnych lub grup uniwersalnych, a nie grup lokalnych w domenie.

Opis grup uniwersalnych

Elementami członkowskimi grup uniwersalnych mogą być grupy i konta z dowolnego drzewa domen lub lasu. Elementom członkowskim tych grup można przypisać uprawnienia w dowolnej domenie w drzewie domen lub lesie.

Grupy o zakresie uniwersalnym służą do konsolidowania grup, które obejmują kilka domen. W tym celu należy dodać konta do grup o zakresie globalnym i zagnieździć te grupy w grupach o zakresie uniwersalnym. W przypadku takiej strategii wszelkie zmiany członkostwa w grupach o zakresie globalnym nie mają wpływu na grupy o zakresie uniwersalnym.

Na przykład w przypadku sieci z dwiema domenami, Europa i StanyZjednoczone oraz z grupą o zakresie globalnym o nazwie KsięgowośćKG w każdej domenie można utworzyć grupę o zakresie uniwersalnym o nazwie UKsięgowość, której elementami członkowskimi są dwie grupy: KsięgowośćKG,

StanyZjednoczone\KsięgowośćKG i Europa\KsięgowośćKG. Grupy UKsięgowość można używać w dowolnym miejscu w przedsiębiorstwie. Żadne zmiany członkostwa poszczególnych grup KsięgowośćKG nie spowodują replikacji grupy UKsięgowość.

Nie należy zbyt często zmieniać członkostwa w grupie o zakresie uniwersalnym. Wszelkie zmiany członkostwa grupy tego typu spowodują replikację całego członkostwa grupy w każdym wykazie globalnym w lesie.

Opis typów grupy

W usługach AD DS istnieją dwa typy grup: grupy dystrybucyjne i grupy zabezpieczeń. Grup dystrybucyjnych można używać do tworzenia list dystrybucyjnych poczty e-mail, a grup zabezpieczeń - do przypisywania uprawnień do zasobów udostępnionych.

Grup dystrybucyjnych można używać tylko z aplikacjami poczty e-mail (takimi jak program Microsoft Exchange Server 2007) do wysyłania poczty e-mail do grup użytkowników. Grupy dystrybucyjne nie obsługują włączonych zabezpieczeń, nie są więc wyświetlane na poufnych listach 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 rozwagą, stanowią wydajną metodę udzielania dostępu do zasobów w sieci. Za pomocą grup zabezpieczeń można wykonywać następujące czynności:

- Przypisywanie praw użytkownika grupom zabezpieczeń w usługach AD DS
  Grupie zabezpieczeń przypisuje się prawa użytkownika, aby określić, jakie czynności mogą wykonywać członkowie tej grupy w zakresie domeny (lub lasu). Prawa użytkownika są automatycznie przypisywane niektórym grupom zabezpieczeń podczas instalowania usług AD DS, aby ułatwić administratorom określenie roli administracyjnej poszczególnych osób w domenie. Na przykład użytkownik dodany do grupy Operatorzy kopii zapasowych w usłudze Active Directory ma możliwość wykonywania kopii zapasowych oraz przywracania plików i katalogów na każdym kontrolerze domeny w domenie.

- Przypisywanie grupom zabezpieczeń uprawnień do zasobów
  Uprawnienia różnią się od praw użytkownika. Uprawnienia decydują o tym, kto może uzyskiwać dostęp do zasobu udostępnionego, i na jakim poziomie (na przykład Pełna kontrola). Grup zabezpieczeń można używać do zarządzania dostępem oraz uprawnieniami do zasobu udostępnionego. Niektóre uprawnienia ustawione dla obiektów domeny są automatycznie przypisywane, aby określić różne poziomy dostępu do domyślnych grup zabezpieczeń, takich jak grupa Operatorzy kont lub grupa Administratorzy domeny.

Podobnie jak grupy dystrybucyjne, grupy zabezpieczeń mogą być używane jako adresaci poczty e-mail. Wysłanie wiadomości e-mail do grupy powoduje wysłanie wiadomości do wszystkich członków tej grupy.

Tożsamości specjalne

Oprócz grup, które znajdują się w kontenerach Użytkownicy i Wbudowane, serwery z systemem Windows Server zawierają kilka tożsamości specjalnych. Dla wygody te tożsamości są zazwyczaj nazywane grupami. Te grupy specjalne nie mają określonych członkostw, które można zmodyfikować. Jednak mogą odpowiadać różnym użytkownikom w różnym czasie, w zależności od okoliczności. Następujące grupy odpowiadają tożsamościom specjalnym:

- Logowanie anonimowe
  Ta grupa odpowiada użytkownikom oraz usługom, które uzyskują dostęp do komputera oraz jego

zasobów za pośrednictwem sieci, bez używania nazwy konta, hasła lub nazwy domeny. Na komputerach z systemem Windows NT lub starszym grupa Logowanie anonimowe jest domyślnie elementem członkowskim grupy Wszyscy. Na komputerach z systemem Windows Server grupa Logowanie anonimowe domyślnie nie jest elementem członkowskim grupy Wszyscy.

- Wszyscy
  Ta grupa odpowiada wszystkim bieżącym użytkownikom sieci, w tym gościom i użytkownikom z innych domen. Ilekroć użytkownik loguje się do sieci, jest automatycznie dodawany do grupy Wszyscy.

- Sieć
  Ta grupa odpowiada użytkownikom, którzy w danej chwili korzystają z jakiegoś zasobu w sieci, w odróżnieniu od użytkowników, którzy uzyskują dostęp do zasobu, logując się lokalnie na komputerze, na którym znajduje się ten zasób. Ilekroć użytkownik uzyskuje dostęp do zasobu za pośrednictwem sieci, jest automatycznie dodawany do grupy Sieć.

- Interaktywna
  Ta grupa odpowiada wszystkim użytkownikom, którzy są w danej chwili zalogowani na określonym komputerze i korzystają z danego zasobu znajdującego się na tym komputerze, w odróżnieniu od użytkowników korzystających z tego zasobu za pośrednictwem sieci. Ilekroć użytkownik uzyskuje dostęp do danego zasobu na komputerze, na którym jest w danej chwili zalogowany, jest automatycznie dodawany do grupy Interaktywna.

Mimo że tożsamościom specjalnym można przypisywać prawa i uprawnienia do zasobów, ich członkostw nie można modyfikować ani wyświetlać. Zakresy grup nie mają zastosowania do tożsamości specjalnych. Użytkownicy są automatycznie przypisywani do tych tożsamości specjalnych, ilekroć logują się lub uzyskują dostęp do jakiegoś zasobu.

Opis możliwych lokalizacji tworzenia grup

W usługach AD DS grupy są tworzone w domenach. Do tworzenia grup służy przystawka Użytkownicy i komputery usługi Active Directory. Mając odpowiednie uprawnienia, użytkownik może tworzyć grupy w domenie katalogu głównego lasu lub w dowolnej innej domenie w lesie albo w jednostce organizacyjnej.

Grupy różnią się domenami, w której są utworzone oraz zakresem. Zakres grupy określa:

- Domenę, z której można dodawać elementy członkowskie.
- Domenę, której dotyczą prawa i uprawnienia przypisane grupie.

Domenę lub jednostkę organizacyjną, w której ma zostać utworzona grupa, należy wybrać zgodnie z wymaganiami administracyjnymi grupy. Na przykład jeśli katalog zawiera wiele jednostek organizacyjnych, z których każda ma innego administratora, należy utworzyć grupy o zakresie globalnym w tych jednostkach organizacyjnych, tak aby administratorzy mogli zarządzać członkostwami grup użytkowników w poszczególnych jednostkach organizacyjnych. Jeśli grupy są wymagane do kontrolowania dostępu poza jednostką organizacyjną, grupy zawarte w jednostce organizacyjnej można zagnieździć w grupach o zakresie uniwersalnym (lub w innych grupach o zakresie globalnym), których można użyć w innym miejscu w lesie.

Jeśli poziomem funkcjonalności domeny jest poziom systemu Windows 2000 lokalny lub wyższy, domena zawiera hierarchię jednostek organizacyjnych, a administracja jest oddelegowana do administratorów poszczególnych jednostek, zagnieżdżenie grup o zakresie globalnym może być bardziej wydajnym rozwiązaniem. Na przykład jeśli jednostka organizacyjna JO1 zawiera jednostki organizacyjne JO2 i JO3, grupa o zakresie globalnym w jednostce organizacyjnej JO1 może zawierać jako elementy członkowskie grupy o zakresie globalnym z jednostek organizacyjnych JO2 i JO3. W jednostce organizacyjnej JO1 administrator

może dodawać lub usuwać elementy członkowskie grup z jednostki organizacyjnej JO1, a administratorzy jednostek JO2 i JO3 mogą dodawać lub usuwać elementy członkowskie grup z ich własnych jednostek organizacyjnych, nie mając uprawnień administracyjnych do grupy o zakresie globalnym w jednostce organizacyjnej JO1.

Uwaga

Grupy można przenosić wewnątrz domeny. Jednak między domenami można przenosić tylko grupy o zakresie uniwersalnym.

Prawa i uprawnienia udzielone grupie o zakresie uniwersalnym zostaną utracone po przeniesieniu tej grupy do innej domeny.

Konieczne jest wtedy przypisanie nowych praw i uprawnień.