Temat: Konta użytkowników i grupy, konta komputerów.

Cel Ogólny lekcji: Celem ogólnym lekcji jest zrozumienie pojęć związanych z kontami użytkowników, grupami oraz kontami komputerów w systemie Windows Server oraz zdobycie wiedzy na temat ich funkcji, zastosowań i znaczenia w kontekście zarządzania dostępem do zasobów sieciowych. Uczestnicy powinni również poznać kluczowe różnice między wersjami systemów Windows Server oraz między systemami Windows 10 i Windows 11 oraz zrozumieć, jak wpływają one na zarządzanie kontami użytkowników, grupami i komputerami.

Cele szczegółowe:

Po zakończeniu lekcji uczestnicy powinni:

1. Rozumieć pojęcie konta użytkownika, jego składniki (nazwa, hasło, grupy, prawa) oraz zastosowania, takie jak logowanie, zarządzanie dostępem i uruchamianie procesów.

2. Rozumieć pojęcie identyfikatora SID (Security Identifier) i jego roli w systemie.

3. Zrozumieć rolę administratora w zarządzaniu kontami oraz rolę kont użytkowników w usługach Active Directory (AD DS).

4. Rozumieć różnicę między logowaniem lokalnym a do domeny oraz zrozumieć, jakie informacje są potrzebne do uwierzytelniania w obu przypadkach.

5. Rozumieć znaczenie grup oraz rodzaje grup (wbudowane, lokalne, domenowe, itp.) i ich zastosowanie w zarządzaniu dostępem.

6. Rozumieć zasięgi grup (domenowe lokalne, globalne, uniwersalne) oraz ich rolę w zarządzaniu dostępem.

7. Zrozumieć rolę kont komputerów w systemie, ich tworzenie i zastosowanie w zarządzaniu dostępem.

8. Rozumieć znaczenie i funkcje kont komputerów w systemie Windows Server.

9. Rozumieć, dlaczego konta komputerów są tworzone podczas dołączania komputerów do domeny lub grupy roboczej.

10. Zrozumieć, kiedy należy stosować konta użytkowników, grupy lub konta komputerów w celu skutecznego zarządzania dostępem do zasobów sieciowych.

Cele związane z różnicami wersji systemów Windows:

Uczestnicy powinni poznać:

11. Różnice między konto Administratorem w różnych wersjach systemów Windows Server oraz zdawanie sobie sprawy z ostrożności w używaniu tego konta.

12. Różnice w funkcjach konta Gościa w zależności od wersji systemów Windows Server.

13. Różnice w grupach wbudowanych w Windows Server 2016, 2019 i 2022 oraz zrozumienie ich roli.

Lekcja powinna zapewnić uczestnikom wiedzę o podstawowych pojęciach związanych z kontami użytkowników, grupami oraz kontami komputerów, ich roli i zastosowaniu w systemie Windows Server oraz umożliwić zrozumienie, jak efektywnie zarządzać dostępem do zasobów w środowisku sieciowym.

W rezultacie, uczestnicy lekcji powinni zdobyć dogłębną wiedzę na temat różnych kont użytkowników, grup i komputerów w systemach Windows Server oraz umieć zastosować tę wiedzę do efektywnego zarządzania dostępem, bezpieczeństwem i funkcjonalnością w środowisku sieciowym.

A. Podstawowe definicje

a. Konto użytkownika

jest obiektem, w którym znajdują się wszystkie informacje definiujące użytkownika w systemie Windows Server. Konto może być lokalne lub domenowe. Konta lokalne i domenowe różnią się zakresem dostępności i poziomem kontroli nad nimi. Oto główne różnice:

- Konto lokalne jest tworzone i zarządzane na pojedynczym komputerze, podczas gdy konto domenowe jest tworzone i zarządzane na domenie sieciowej.
- Konto lokalne jest zwykle używane do logowania się na jeden komputer i dostępu do zasobów i usług dostępnych na tym komputerze, podczas gdy konto domenowe jest używane do logowania się na dowolny komputer w domenie i dostępu do zasobów i usług dostępnych w domenie.
- Użytkownik ma pełną kontrolę nad swoim kontem lokalnym i zasobami, i usługami dostępnymi na jego komputerze, podczas gdy administrator sieci ma pełną kontrolę nad kontem domenowym i zasobami, i usługami dostępnymi w domenie.

Konta lokalne są przechowywane lokalnie na komputerze, podczas gdy konta domenowe są przechowywane w katalogu Active Directory na kontrolerze domeny4.

Konto użytkownika obejmuje nazwę użytkownika wraz z hasłem, wykorzystywanym w procesie logowania, grupy, do których należy konto oraz prawa i uprawnienia, które użytkownik posiada, umożliwiające dostęp do komputera i zasobów sieciowych.

Konto użytkownika może zostać **użyte do**:

1. przeprowadzenia procesu logowania na komputerze z uwzględnieniem tożsamości konta użytkownika.
2. uruchamiania procesów i usług w określonym kontekście zabezpieczeń.

3. zarządzania dostępem użytkowników do zasobów, takich jak obiekty usługi Active Directory i ich właściwości, udostępnione foldery, pliki, katalogi i kolejki wydruku.
Wszystkie konta użytkowników identyfikowane są przez system za pomocą identyfikatora SlD (Security Identifier). Identyfikator SID jest automatycznie tworzony wraz z ustanawianiem nowych kont użytkowników (zarówno lokalnych, jaki i domenowych). Usuwając konto użytkownika, usuwa się również jego identyfikator. Utworzenie konta o tej samej nazwie co usunięty użytkownik powoduje utworzenie nowego identyfikatora SID (dla systemu będzie to inny użytkownik - inny identyfikator SID).

Jednym z głównych zadań administratora jest zarządzanie kontami użytkowników i grup.

Konta użytkowników pozwalają na logowanie się indywidualnych użytkowników do zasobów sieciowych, a konta grupowe - na zarządzanie wieloma użytkownikami jednocześnie.

Uprawnienia nadawane użytkownikom mają zapewnić bezpieczeństwo w systemie, ale jednocześnie umożliwić wykonanie zadań, dlatego należy nadawać użytkownikom tylko niezbędne uprawnienia.

b. Konta użytkowników w usługach domenowych Active Directory (AD DS, Active Directory Domain Services)

Podstawowymi składnikami systemu bezpieczeństwa w Windows Serwer są: uwierzytelnianie użytkowników oraz kontrola dostępu.

Uwierzytelnianie użytkowników składa się z:

- interaktywnego logowania - podczas logowania na lokalnym komputerze sprawdza tożsamość i nadaje lub odmawia dostępu do usługi Active Directory;
- uwierzytelniania sieciowego - uprawnienia użytkownika sprawdzane są przy każdej próbie skorzystania z zasobu sieciowego. Windows Server do uwierzytelniania sieciowego wykorzystywany jest protokół Kerberos, który zapewnia odpowiedni poziom bezpieczeństwa. Sprawdzanie uprawnień do zasobów sieciowych realizowane jest przez usługę Active Directory, dzięki czemu użytkownik może być uwierzytelniony na dowolnym kontrolerze domeny.

Podczas logowania na komputerze przyłączonym do domeny użytkownik może wybrać sposób logowania. Może zalogować się lokalnie, korzystając z konta istniejącego na komputerze - w takim przypadku będzie miał uprawnienia do korzystania tylko z komputera lokalnego. Jeżeli wskaże nazwę domeny i poprawną nazwę konta wraz z odpowiadającym mu hasłem, to zaloguje się do domeny i po uwierzytelnieniu uzyska dostęp do zasobów zdefiniowanych w Active Directory.

Podczas instalacji systemu tworzonych jest wiele kont specjalnych, wykorzystywanych w systemie.

Na zrzutach pokazano listę użytkowników domeny bezpośrednio po instalacji.

Tylko konto administratora umożliwia korzystanie z usług. Dla pozostałych użytkowników należy takie konta utworzyć. Jest to zadanie odpowiedzialne i wymaga wcześniejszego opracowania systemu nazw dla kont. Dla domeny konta domyślne znajdują się w kontenerze Users.

c. 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 dzielą się na:

1. Wbudowane

są tworzone automatycznie podczas instalacji systemu i charakteryzują się tym, że nie można ich usuwać, tworzone przez uprawnionych użytkowników (w zainstalowanym systemie).

Grupy domyślne - są predefiniowanymi grupami zabezpieczeń tworzonymi automatycznie podczas instalacji domeny **Active Directory**. Grupom tym na starcie określono zestaw praw i przywilejów.

- znajdują się w:

kontenerze **Builtin** (zasięg lokalnej domeny nie może być zmieniony ani typ grupy),

kontenerze **Users** (zasięg części grup globalny a części lokalny w domenie, można zmienić ich lokalizację przenosząc do innych jednostek organizacyjnych, ale tylko w obrębie domeny).

2. Lokalne

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 zawierać tylko konta użytkowników lokalnych danego komputera.

Reguły grup lokalnych:

używa się je do nadawania uprawnień tylko do lokalnych zasobów i operacji na danym komputerze,

są umiejscowione w bazie SAM - lokalnej bazie kont komputera,
mogą do nich należeć tylko konta użytkowników lokalnych, nie mogą do nich należeć konta użytkowników domenowych,
nie może ona być elementem żadnej innej grupy,
mogą ona być tworzone tylko przez członków grupy Administratorzy (Administrators) lub Operatorzy Kont (Account Operators).

Grupy te są widoczne w oknie programu Computer Management - Zarządzanie komputerem w pod folderze Grupy folderu Użytkownicy i grupy lokalne. Przystawkę tę można również wywołać wydając polecenie lusrmgr.msc.
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.

3. Domenowe

mogą być tworzone tylko na kontrolerach domeny i zawierać konta użytkowników domenowych a nawet inne grupy domenowe.

Grupy w usługach domenowych Active Directory (AD DS, Active Directory Domain Services) to obiekty katalogu znajdujące się w obiektach kontenera będących domenami lub jednostkami organizacyjnymi. Możliwe jest także tworzenie grup.
Główne aspektami stosowania grupy:

- uproszczenie administracji dzięki zgrupowaniu kont, którym chcemy przydzielić takie same prawa np. dostęp do katalogu, podaną operację wykonujemy tylko raz, omijamy w ten sposób czynność związaną z przypisywaniem uprawnień indywidualnym użytkownikom. Takie nadanie uprawnień daje taki sam dostęp do zasobu dla wszystkich członków grupy.
- nowi członkowie dodawani do grupy, której przydzielono określone uprawnienia uzyskują takie same prawa jak grupa,
- tworzenie list dystrybucyjnych poczty elektronicznej.

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

- używa się je do nadawania praw dostępu do zasobów i operacji na dowolnym komputerze należącym do domeny.
- informacja a o nich jest w bazie Active Directory.
- 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.

Dodanie użytkownika do grupy powoduje uzyskanie przez niego:

- wszystkich praw przypisanych do grupy,
- wszystkich uprawnień, która grupa ma nadane do współdzielonych zasobów.

Grupy dzielone są ze względu na typy grup:

Grupy dystrybucyjne są używane w aplikacjach e-mail, takich jak program Microsoft Exchange, podczas wysyłania wiadomości e-mail do grupy użytkowników.
Głównym celem tego typu grupy jest gromadzenie obiektów pokrewnych, a nie udzielanie uprawnień. Grupy dystrybucyjne nie obsługują zabezpieczeń, dlatego nie mogą służyć do przypisywania uprawnień i nie są wyświetlane na poufnych listach kontroli dostępu
(ang. **Discretionary Access Control Lists**). Jeśli jest potrzebna grupa służąca do kontroli dostępu do zasobów udostępnionych, należy utworzyć grupę zabezpieczeń.

Grupy zabezpieczeń za pomocą tych grup można przypisać prawa i uprawnienia użytkownika do grup użytkowników i komputerów. Prawa służą do określania czynności, jakie członkowie grupy zabezpieczeń mogą wykonać w domenie lub lesie, a uprawnienia służą do określenia zasobów sieciowych, do których może uzyskać dostęp członek grupy.

Korzystając z grup zabezpieczeń można:

- przypisywać prawa w **AD DS**. Prawa użytkownika są tylko przywilejem grup zabezpieczeń, czyli używaj ich, gdy zależy ci na określeniu praw użytkownika bądź grupy w domenie/lesie.
- przypisywać uprawnienia do zasobów. Określają one, kto ma do czego dostęp i co może wykonać, np. **Write** lub **Full Control**. Domyślne grupy zabezpieczeń mają część uprawnień do obiektów w domenie nadane automatycznie (tabele powyżej).
- używać jako listy e-mail. Wysyłając wiadomość e-mail do grupy, zostanie on wysłany do wszystkich jej członków. Z tego względu grupy zabezpieczeń mogą służyć jako grupy dystrybucyjne.

Nawet jeśli grupy zabezpieczeń mają wszystkie funkcje grup dystrybucyjnych, to grupy dystrybucyjne są nadal potrzebne, ponieważ niektóre aplikacje mogą korzystać wyłącznie z tego typu grup.

Grupy dzielone są ze względu na zasięg grup:

Zasięg grupy określa nam obszar działania danej grupy, część grup może być użyta tylko w domenie, lecz są takie, których obszar działania obejmuje cały las. Zasięg grupy ma wpływ na członków danej grupy a także ma wpływ na zagnieżdżanie (łączenie grup w grupy) samych grup.

Dostępne są grupy o trzech zasięgach: **domenowa grupa lokalna**, **globalna** i **uniwersalna**.

Domenowe grupy lokalne

Członkami mogą być inne grupy oraz konta z domen Windows Server. Grupy, ograniczają się do działania w domenie a nadawane uprawnienia ograniczają się do zasobów znajdujących się w domenie. Pomagają definiować i zarządzać dostępem do zasobów w pojedynczej domenie. Ich członkami mogą być:

- grupy o zasięgu globalnym,
- grupy o zasięgu uniwersalnym,
- konta,
- inne grupy o zasięgu domenowym lokalnym,
- kombinacja powyższych.

Można to zilustrować takim przykładem: naszym zadaniem jest dać dostęp do zasobu sieciowego kilku użytkownikom, możemy to wykonać dodając ich do listy uprawnień danego zasobu pozwalając im np. na zapis w danym katalogu. Operacja dodawania kolejnych użytkowników wymusi na nas ponowne wylistowanie uprawnień tego zasobu i dodanie nowych użytkowników do tej listy. Problematyczna również będzie operacja, w której tym samy użytkownikom będziemy chcieli dać uprawnienie do innego zasobu np. będziemy chcieli dać im możliwość drukowania. Sprowadzi się to do tego, że ponownie będzie trzeba przypisać te konta do listy uprawnień drukarki.

Wykorzystując zalety strategii grup (o strategii później) powyższe zadanie można by było zrealizować poprzez utworzenie grupy o zasięgu domenowym lokalnym i przypisując wszystkie uprawnienia do tej grupy. Następnie umieścić w niej wszystkie konta użytkowników mających prawo do tego zasobu, później dodawanie kolejnych użytkowników sprowadza się tylko do dodania ich kont do tej grupy a odpowiednie uprawnienia zostaną przypisane do użytkowników.
Jeśli chcemy dać użytkownikom prawo do korzystania z drukarki należy tylko do listy uprawnień obiektu jakim jest drukarka dodać utworzoną grupę.

Grupy o zasięgu globalnym

Są głównie używane do udostępniania klasyfikowanego członkostwa w lokalnych grupach domeny dla pojedynczych podmiotów zabezpieczeń lub dla bezpośredniego przypisania uprawnień (w szczególności dla domen o mieszanym bądź tymczasowym poziomic funkcjonalności). Są często używane do gromadzenia użytkowników lub komputerów tej samej domeny i współdzielących takie same zadania, role bądź funkcje więc do grup globalnych należą konta oraz inne grupy, lecz tylko z domeny, w której

dana grupa globalna została zdefiniowana. *Czyli można dodać do grupy globalnej utworzonej w np. domenie FiliaWarszawa konto Jan Kowalski z tej domeny, lecz już niemożliwe jest dodanie konta BeataTryla znajdującego się w domenie FiliaPoznan.* Grupy te mogą mieć nadane uprawnienia w każdej domenie w lesie.

Wskazane jest, aby grup globalnych używać do codziennego zarządzania obiektami katalogu, takimi jak konta użytkowników i komputerów. Ponieważ grupy globalne nie są replikowane poza własną domenę, można często zmieniać listę ich członków bez generowania ruchu związanego z replikacją katalogu globalnego.

Grupy globalne:

- Istnieją we wszystkich domenach i lasach o mieszanym, tymczasowym bądź macierzystym poziomie funkcjonalności.
- Mogą mieć członków, którzy znajdujących się w tej samej domenie.
- Mogą być członkiem lokalnej grupy komputera lub domeny.
- Mogą mieć uprawnienia w dowolnej domenie (wliczając w to zaufane domeny innych lasów i domeny systemów wcześniejszych niż Windows 2003).
- Mogą zawierać inne grupy globalne (oprócz poziomu funkcjonalności domeny Windows 2000 mieszany).

Grupa o zasięgu uniwersalnym

Do nich mogą należeć inne grupy oraz konta z dowolnej domeny w lesie oraz grupom tym można przypisać uprawnienia w każdej domenie w lesie. W praktyce grup o zasięgu uniwersalnym używa się tam, gdzie występuje potrzeba połączenia grup z różnych domen. Najczęściej strategia łączenia grup przebiega w ten sposób, że w pierwszej kolejności są tworzone grupy zasięgu globalnym a te z kolei są zagnieżdżane w grupach uniwersalnych. Zaletą tej strategii jest to, że zmiana, która jest dokonywana w grupie globalnej nie ma wpływu na grupę uniwersalną.

Grupy uniwersalne są stosowane w praktyce dla dużych lasów domen dzięki temu, że grupy uniwersalne z całego lasu mogą być przechowywane na specjalnych serwerach przechowując tak zwane wykazy globalne (Global Catalog). Ma to na celu skrócenie zdarzeń logowania i dostępu do zasobów w sytuacji, gdy nasza organizacja ma infrastrukturę AD połączoną łączami WAN w kilku miastach lub państwach.

Grupy uniwersalne mogą być pomocne przy przedstawianiu i konsolidacji grup, które obejmują kilka domen oraz przy wykonywaniu wspólnych zadań w obrębie przedsiębiorstwa.

Przydatną wskazówką może być wyznaczenie rzadko zmieniających się grup używanych w dużym zakresie jako grup uniwersalnych.

Grupy specjalne

- użytkownicy nie są przypisywani przez administratora lub innego uprawnionego użytkownika, lecz należą do nich domyślnie, lub stają się ich członkami poprzez wykonywanie określonych operacji. 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.

Przykłady grup specjalnych to:

- **Anonymous Logon (Logowanie anonimowe)** - grupa ta dotyczy użytkowników, którzy korzystają z zasobów sieci z pominięciem procesu uwierzytelnienia, czyli bez użycia nazwy konta, hasła i nazwy domeny.
- **Everyone (Wszyscy)** - grupa reprezentuje wszystkich bieżących użytkowników sieci, włączając w to gości i użytkowników z innych domen. Zawsze, kiedy użytkownik loguje się do sieci jest automatycznie dodawany do tej grupy.
- **Network (Sieć)** - grupa reprezentuje użytkowników, którzy uzyskują dostęp do zasobu poprzez sieć w przeciwieństwie do użytkowników, którzy korzystają z tego zasobu po uprzednim lokalnym zalogowaniu się do komputera, na którym jest udostępniony dany zasób. Kiedy użytkownik uzyskuje dostęp do zasobu w sieci jest automatycznie dodawany do tej grupy.
- **Interactive (Interakcyjni)** - reprezentuje użytkowników zalogowanych lokalnie i uzyskujących dostęp do zasobu na tym komputerze. Zawsze, gdy użytkownik uzyskuje dostęp do zasobu na komputerze, na którym się lokalnie zalogował, jest automatycznie dodawany do tej grupy Interactive.
- **Authenticated Users (Użytkownicy uwierzytelnieni) -** zawiera wszystkich użytkowników, którzy zostali uwierzytelnieni w sieci za pomocą ważnego konta użytkownika. Podczas przydzielania uprawnień, grupę **Authenticated Users** można używać zamiast grupy Everyone, dzięki czemu zabroniony zostanie anonimowy dostęp do zasobów.
- **Creator Owner (Twórca właściciel)** - Grupa **Creator Owner** dotyczy użytkowników, którzy utworzyli lub są właścicielami zasobu. Przykładowo, jeśli użytkownik utworzył zasób, ale administrator stał się właścicielem tego zasobu, to administrator stanie się członkiem grupy **Creator Owner**.
- **Dialup -** Grupa **Dialup** zawiera użytkowników, którzy połączyli się z siecią za pomocą łącza telefonicznego.

- **Domain Users - Użytkownicy domeny** - Grupa ta zawiera wszystkich domenowych użytkowników. Domyślnie, każde konto użytkownika tworzone w domenie staje się członkiem tej grupy automatycznie. Może być użyta do reprezentowania wszystkich użytkowników w domenie

d. Konto komputera (Computer account):

- jest tworzone dla każdego komputera dołączającego do domeny lub grupy roboczej. Umożliwia to zarządzanie komputerem z poziomu kontrolera domeny oraz dostęp do zasobów udostępnionych w sieci.
- identyfikuje komputer w domenie,
- umożliwia uwierzytelnianie oraz inspekcję dostępu komputera do sieci i zasobów domeny,
- jest wymagane w przypadku każdego komputera.

Konta komputerów w domenie są tworzone w tzw. "Kontenerze komputerów". Kontener ten jest specjalnym miejscem w kontrolerze domeny, w którym przechowywane są informacje o komputerach dołączających do domeny. To właśnie tam znajdują się rekordy dotyczące komputerów, takie jak nazwa komputera, identyfikator SID (Security Identifier), informacje o kontach komputerowych itp.

Kiedy tworzysz nowe konto komputera i dołączasz je do domeny, informacje o tym koncie są przechowywane w kontenerze komputerów w kontrolerze domeny. Dzięki temu konto komputera staje się częścią domeny i może korzystać z usług i zasobów dostępnych w tej domenie.

B. Różnice między wersjami systemów Windows

Windows Server 2016

- Zaawansowane narzędzia zarządzania użytkownikami i grupami w konsoli Zarządzania komputerem.
- Wsparcie dla zaawansowanych strategii uwierzytelniania i zabezpieczeń.

Windows Server 2019

- Ulepszona integracja z chmurą i usługami Office 365.
- Wprowadzenie kont zarządzanych z poziomu Azure AD.

Windows Server 2022

- Wydajność i skalowalność zoptymalizowana dla chmur hybrydowych.
- Wsparcie dla kontenerów i nowoczesnych aplikacji.

Windows 10 i Windows 11

- Ulepszona integracja z kontami Microsoft oraz usługami online.
- Wprowadzenie funkcji związanych z prywatnością i bezpieczeństwem.

C. Windows Server 2016, 2019 i 2022

a. Konta domyślne w Windows Server 2016, 2019 i 2022

1. **Administrator:** Jest utworzone podczas instalacji systemu i ma pełne uprawnienia do zarządzania serwerem.

2. **Gość (Guest):** Ma ograniczone uprawnienia, a jego domyślne konto jest zazwyczaj wyłączone z powodów bezpieczeństwa.

3. **Administrator lokalny (Administrator):** To jest lokalne konto administratora na serwerze. W wersjach nowszych niż Windows Server 2016, konto to ma wyłączone dziedziczenie ustawień.

4. **Konto wsparcia (Support_388945a0):** Jest dostępne tylko w niektórych wersjach i pełni funkcje wsparcia technicznego.

5. **Konto sieciowe (Network service) i Konto lokalne (Local service):** Służące do uruchamiania usług z ograniczonymi uprawnieniami.

6. **Konto systemowe (System):** Jest używane przez system do uruchamiania procesów systemowych.

7. **Konto Default Account:** Jest używane do obsługi nowo zainstalowanych aplikacji w kontenerach.

Pamiętaj, że te konta mogą różnić się w zależności od konkretnego systemu i wersji systemu. Warto zawsze dokładnie przestudiować dokumentację dostawcy lub oficjalne źródła, aby uzyskać najnowsze i dokładne informacje dotyczące dostępnych kont domyślnych.

b. Grupy domyślne w Windows Server 2016, 2019 i 2022

1. **Administratorzy (Administrators):** To jest grupa posiadająca pełne uprawnienia do zarządzania serwerem. Administratorzy mają pełne prawa do wszystkich zasobów i operacji na lokalnym komputerze. Administratorzy mogą tworzyć, usuwać oraz modyfikować konta wszystkich użytkowników i grup, nadawać uprawnienia do wszystkich zasobów komputera. Inne prawa, jakie posiadają to:

- instalacja systemu operacyjnego oraz jego komponentów uwzględniając sterowniki, urządzenia sprzętowe, usługi systemowe itd.

- instalacja pakietów Service Pack oraz łat hot fix.
- naprawa systemu operacyjnego.
- przejmowanie własności obiektów.

2. **Użytkownicy (Users):** Grupa ta zawiera domyślnie wszystkich zwykłych użytkowników serwera. Użytkownicy mogą uruchamiać aplikacje, używać lokalnych i sieciowych drukarek, zamykać i blokować system, nie mogą natomiast zarządzać użytkownikami i grupami, udostępniać folderów, dodawać drukarek lokalnych.

3. **Goście (Guests):** Grupa Gości posiada ograniczone uprawnienia i jest zwykle wyłączona dla bezpieczeństwa.

4. **Operatorzy kopii zapasowych (Backup Operators):** Członkowie tej grupy mogą:

- wykonywać operacje kopii zapasowych na serwerze,
- wykonywać kopie zapasowe folderów i odtwarzać foldery z tych kopii, niezależnie od praw dostępu do folderów i umieszczonych w nich plików, logować się do lokalnych komputerów i zamykać system, nie mogą zmieniać ustawień mających związek z bezpieczeństwem,
- tworzyć i odtwarzać kopie zapasowe niezależnie od posiadanych uprawnień do plików i folderów. Grupa ta powinna zawierać wyłącznie konta osób odpowiedzialnych za wykonywanie kopii zapasowych.

5. **Użytkownicy zdalnego pulpitu (Remote Desktop Users):**

- Grupa ta pozwala użytkownikom zdalnego pulpitu na logowanie się na serwerze.

6. **Zarządzanie dostępem do pamięci masowej (Storage Replica Administrators):**

- Grupa ta ma uprawnienia do zarządzania funkcją replikacji pamięci masowej.

7. **Kreatorzy właścicieli serwera (Server Operators):**

- Członkowie tej grupy mają uprawnienia do zarządzania serwerem, ale nie mogą zmieniać ustawień bezpieczeństwa.

8. **Zarządzanie replikacją DFS (DFS Management):**

- Ta grupa pozwala na zarządzanie replikacją w systemie plików rozproszonych (DFS).

9. **Zarządzanie drukowaniem (Print Operators):**

- Grupa ta ma uprawnienia do zarządzania drukarkami na serwerze.

10. **Zarządzanie katalogami sieciowymi (Network Configuration Operators):**

- Członkowie tej grupy mogą zarządzać konfiguracją sieciową.

Pamiętaj, że to tylko wybrane grupy i ich funkcje. Systemy Windows Server oferują wiele innych domyślnych grup, a także pozwalają na tworzenie niestandardowych grup w celu dostosowania zarządzania dostępem do zasobów. Wbudowanych grup lokalnych nie można usuwać - próba usunięcia takiej grupy powoduje wypisanie komunikatu o błędzie.

D. Windows Server 2016, 2019 i 2022 kontrolera domeny

a. Konta domyślne w Windows Server 2016, 2019 i 2022 kontrolera domeny

Po zainstalowaniu kontrolera domeny w systemach Windows Server 2016, 2019 i 2022, pojawiają się pewne domyślne konta użytkowników i grupy, które są istotne dla funkcjonowania i zarządzania kontrolerem domeny oraz środowiskiem Active Directory. Oto niektóre z tych kont i grup:

b. Domyślne konta użytkowników:

1. **Administrator:**

- To konto administratora domeny, które jest tworzone podczas instalacji kontrolera domeny.
- Ma pełne uprawnienia do zarządzania systemem i wszystkimi zasobami.
- Posiada pełne uprawnienia do zarządzania domeną i kontrolerem domeny.
- Powinno być używane ostrożnie, ponieważ nadmierna eksploatacja może stanowić ryzyko dla bezpieczeństwa.
- Konto domyślne na każdym serwerze i umożliwia pełen dostęp do wszystkich funkcji i ustawień.

2. **Gość (Guest):**

- Konto ma ograniczone uprawnienia dostęp do systemu i zasobów, zazwyczaj jest wyłączone dla celów bezpieczeństwa.
- Nie ma dostępu do danych użytkownika ani funkcji zarządzania.

c. Domyślne Grupy:

1. **Administratorzy (Administrators):**

- Grupa ta zawiera użytkowników, którzy posiadają pełne uprawnienia do zarządzania kontrolerem domeny i domeną.

2. **Użytkownicy domyślni (Domain Users):**

- Grupa ta zawiera wszystkich użytkowników, którzy zostaną dodani do domeny.

3. **Komputery (Computers):**

- Grupa ta zawiera konta komputerów, które dołączyły do domeny.

4. **Kreatorzy właścicieli głównych (Enterprise Admins):**

- Grupa ta posiada najwyższe uprawnienia w całej strukturze Active Directory. Uprawnienia te dotyczą całego las.

5. **Kreatorzy właścicieli domen (Domain Admins):**

- Grupa ta ma pełne uprawnienia w ramach jednej konkretnej domeny w strukturze Active Directory.

6. **Domyślni kontrolerzy domeny (Domain Controllers):**

- Grupa ta zawiera wszystkie kontrolery domeny w danej domenie.

7. **Kreatorzy właścicieli schematu (Schema Admins):**

- Grupa ta ma uprawnienia do zarządzania schematem Active Directory.

8. **Użytkownicy dostępu zdalnego (Remote Desktop Users):**

- Grupa ta pozwala użytkownikom na dostęp zdalny do serwera.

9. **Serwer DNS (DNSAdmins):**

- Grupa ta ma uprawnienia do zarządzania usługą DNS na kontrolerze domeny.

10. **Kreatorzy własnych grup (Group Policy Creator Owners):**

- Grupa ta ma uprawnienia do tworzenia i zarządzania obiektami zasad grupy.

To tylko wybrane przykładowe konta użytkowników i grupy, które pojawiają się po instalacji kontrolera domeny w systemach Windows Server 2016, 2019 i 2022. Dokładne konta i grupy mogą się różnić w zależności od konfiguracji środowiska i wersji systemu.

E. Inne konta w systemach Windows:

1. **Konto usług (Service Account)**:

- Konta usług są wykorzystywane do uruchamiania usług i aplikacji. Zapewniają one bezpieczny sposób uruchamiania tych procesów, zwykle z ograniczonymi uprawnieniami. W odróżnieniu od kont użytkowników, konta serwisowe nie są przeznaczone do logowania się interaktywnie, ale do automatycznego wykonywania określonych zadań.

2. **Konto usługi zarządzania kluczami (Key distribution center service account)**:

- Jest odpowiedzialne za obsługę procesów uwierzytelniania w usługach Kerberos oraz zarządzania kluczami szyfrującymi. Kluczowe dla bezpieczeństwa infrastruktury uwierzytelniania w środowiskach Windows.

3. **Konto zadania harmonogramu (Scheduled task account)**:

- Konta te są używane do uruchamiania zadań zaplanowanych w harmonogramie, takich jak automatyczne skrypty, kopie zapasowe czy inne procedury. Te konta mogą mieć ograniczone uprawnienia w celu minimalizacji ryzyka.

Każde z tych kont ma swoje specyficzne przeznaczenie i wpływ na zarządzanie i bezpieczeństwo systemu Windows Server. Ważne jest, aby stosować zasady bezpieczeństwa i najlepsze praktyki w zarządzaniu kontami w celu minimalizacji ryzyka i utrzymania bezpieczeństwa infrastruktury IT.

Zrzuty domyślnych kont z Windows Server.

Podsumowanie

Zarządzanie kontami użytkowników, grup oraz kontami komputerów jest niezwykle istotne dla utrzymania bezpieczeństwa i organizacji w systemach Windows. W zależności od wersji systemu operacyjnego, dostępne narzędzia i funkcje mogą się różnić, a także mogą być dodawane nowe rozwiązania, aby sprostać rosnącym wymaganiom w dziedzinie zarządzania tożsamością i dostępem.