Laboratorium 02-03 – Uzupełnienie Teoretyczne

Uzupełnienie teoretyczne - Obiekty AD, Prawa dodawania kont komputerów itp..

Obiekty w Active Directory (AD)

to podstawowe elementy, którymi zarządza AD. Każdy obiekt reprezentuje zasób w sieci, taki jak użytkownik, komputer, serwer, drukarka czy grupa. Obiekty są przechowywane w bazie danych AD i organizowane w strukturze hierarchicznej.

1. **Konta użytkowników**: Umożliwiają użytkownikom logowanie się do domeny i korzystanie z zasobów sieciowych. Każde konto użytkownika zawiera atrybuty takie jak imię, nazwisko, hasło i członkostwo w grupach.
2. **Konta komputerów**: Reprezentują komputery podłączone do domeny. Konta te są niezbędne do uwierzytelniania komputerów i stosowania polityk grupowych.
3. **Grupy**: Obiekty, które umożliwiają zarządzanie uprawnieniami i dostępem. Mogą być używane do przydzielania uprawnień do zasobów (np. plików, folderów) większej liczbie użytkowników lub komputerów.
4. **Jednostki organizacyjne (OU)**: Logiczne kontenery, które organizują obiekty w AD. Umożliwiają delegowanie uprawnień administracyjnych i stosowanie polityk grupowych (GPO) dla wybranych grup obiektów.
5. **Obiekty polityk grupowych (GPO)**: Zbiory reguł konfiguracji systemu, które mogą być stosowane do użytkowników i komputerów w domenie w celu zarządzania środowiskiem systemowym i bezpieczeństwem.

Obiekty AD są kluczowe dla centralnego zarządzania siecią i kontrolowania dostępu do zasobów w domenie.

Konta użytkowników w Active Directory (AD) są kluczowe dla uwierzytelniania i zarządzania dostępem do zasobów w domenie. Każde konto użytkownika reprezentuje indywidualnego użytkownika i posiada zestaw właściwości, które określają jego tożsamość oraz uprawnienia.

Najważniejsze właściwości konta użytkownika:

1. **sAMAccountName (Security Account Manager Name)**: Krótsza nazwa logowania (do 20 znaków), która musi być **unikalna** w obrębie domeny. Używana przy logowaniu w starszych systemach (np. Windows NT).
2. **UserPrincipalName (UPN)**: Pełna nazwa logowania, w formacie przypominającym adres e-mail (np. user@domain.com). Jest unikalna w całej lesie AD i wykorzystywana w nowszych systemach Windows oraz aplikacjach zgodnych z AD.
3. **DistinguishedName (DN)**: Unikalny identyfikator konta w hierarchii Active Directory. Zawiera pełną ścieżkę do obiektu, np. CN=JanKowalski,OU=Users,DC=domain,DC=com.
4. **ObjectGUID**: Globalnie unikalny identyfikator (GUID) przypisywany każdemu obiektowi w AD, w tym kontom użytkowników. **ObjectGUID** jest zawsze unikalny w całej strukturze AD i nigdy się nie zmienia.

5. **CN (Common Name)**: Nazwa obiektu, która identyfikuje konto w strukturze AD. **CN** musi być unikalne w obrębie jednostki organizacyjnej (OU), w której znajduje się konto.
6. **Hasło**: Każde konto użytkownika musi mieć przypisane hasło, które spełnia zasady polityki haseł w domenie (np. minimalna długość, złożoność).
7. **Członkostwo w grupach**: Określa, do jakich grup bezpieczeństwa i dystrybucji należy użytkownik, co wpływa na jego uprawnienia i dostęp do zasobów w domenie.

unikalne:

- **sAMAccountName**: Musi być unikalny w obrębie domeny.
- **UserPrincipalName (UPN)**: Musi być unikalny w całym lesie AD.
- **ObjectGUID**: Globalnie unikalny w całej strukturze AD.
- **DistinguishedName (DN)**: Musi być unikalny w obrębie struktury AD.

Dodawanie kont komputerów

Standardowo prawo do dodawania komputerów do domeny w Active Directory mają:

1. **Członkowie grupy "Domain Admins":**
    - Ta grupa ma pełne uprawnienia administracyjne w domenie, w tym prawo dodawania dowolnej liczby komputerów do domeny.
2. **Członkowie grupy "Account Operators":**
    - Mogą zarządzać kontami użytkowników, grup oraz komputerów w domenie, w tym dodawać komputery do domeny.
3. **Zwykli użytkownicy:**
    - Domyślnie, każdy zwykły użytkownik ma prawo do dodania **do 10 komputerów** do domeny. Limit ten jest skonfigurowany w Active Directory i może być zmieniony.

ms-DS-MachineAccountQuota

to atrybut na poziomie domeny, który definiuje, ilu komputerom użytkownik bez uprawnień administracyjnych może utworzyć konto komputerowe w domenie.

- **Domyślna wartość** tego klucza to **10**, co oznacza, że standardowy użytkownik może dodać do 10 komputerów do domeny.

Sprawdzenie wartości za pomocą PowerShell:

Aby sprawdzić bieżącą wartość **ms-DS-MachineAccountQuota**, możesz użyć następującego polecenia

Get-ADObject (Get-ADDomain).DistinguishedName -Property ms-DS-MachineAccountQuota

Różnice między dodawaniem a usuwaniem komputera z domeny

Akcja	Kto ma prawo?	Komentarz
Dodanie do domeny	Domain Admins, Account Operators, zwykli użytkownicy (do limitu 10)	Prawa można modyfikować przez ms-DS-MachineAccountQuota lub delegację w AD.
Usunięcie z domeny	Administratorzy lokalni, Domain Admins	Ograniczenie wymaga modyfikacji uprawnień lokalnych oraz zarządzania grupą Administratorzy.

Domyślne kontenery

redircmp i **redirusr** to narzędzia w Active Directory, które pozwalają administratorom zmieniać domyślne lokalizacje (OU) dla nowo tworzonych kont komputerów i użytkowników. Domyślnie, nowe konta komputerów trafiają do kontenera **CN=Computers**, a nowe konta użytkowników do **CN=Users**. Te narzędzia pozwalają przekierować te obiekty do wybranych jednostek organizacyjnych (OU), co ułatwia zarządzanie i stosowanie polityk grupowych (GPO).

Przykład zastosowania:

- **redircmp**: Używane do przekierowania nowych kont komputerów do innej OU.

  redircmp "OU=NewComputers,DC=domain,DC=com"

- **redirusr**: Używane do przekierowania nowych kont użytkowników do innej OU.

  redirusr "OU=NewUsers,DC=domain,DC=com"

redircmp i **redirusr** ma sens w środowiskach Active Directory, zwłaszcza gdy organizacja stosuje **polityki grupowe (GPO)** lub chce lepiej zorganizować zasoby AD. Umożliwiają one:

1. **Lepszą organizację**: Obiekty trafiają bezpośrednio do odpowiednich OU, co ułatwia ich zarządzanie.
2. **Automatyczne przypisanie polityk GPO**: Używanie odpowiednich OU sprawia, że nowo utworzone konta są automatycznie objęte politykami, co eliminuje konieczność ręcznego przenoszenia obiektów.

W dużych i rozbudowanych środowiskach, gdzie porządek i automatyzacja są kluczowe, stosowanie tych narzędzi jest zalecane.

Prestage konta komputera (ang. **pre-staging computer account**) to proces ręcznego tworzenia konta komputera w Active Directory (AD) przed faktycznym dołączeniem komputera do domeny. Jest to technika stosowana głównie w sytuacjach, gdzie konieczna jest większa kontrola nad procesem dołączania komputerów do domeny, szczególnie w środowiskach o podwyższonym poziomie bezpieczeństwa.

Korzyści z pre-stagingu konta komputera:

1. **Zwiększona kontrola**: Administratorzy mogą z góry utworzyć konto komputera w odpowiedniej jednostce organizacyjnej (OU), zapewniając, że komputer będzie zarządzany zgodnie z politykami przypisanymi do tej OU.
2. **Bezpieczeństwo**: Pre-stage umożliwia ograniczenie, kto może dołączyć komputer do domeny. Komputer może zostać dołączony do domeny tylko, jeśli jego konto zostało wcześniej utworzone przez administratora, co zapobiega nieautoryzowanemu dołączaniu urządzeń.
3. **Automatyczne przypisywanie polityk**: Dzięki pre-stagingowi komputer jest od razu przypisany do odpowiedniej OU, co oznacza, że po dołączeniu do domeny natychmiast zaczynają na niego działać polityki grupowe (GPO) przypisane do tej jednostki organizacyjnej.

Jak działa proces pre-staging konta komputera:

1. **Ręczne tworzenie konta komputera**: Administrator w narzędziu **Active Directory Users and Computers** ręcznie tworzy konto komputera w odpowiedniej jednostce organizacyjnej (OU), gdzie komputer będzie zarządzany. Tworzone są podstawowe atrybuty konta, takie jak nazwa komputera, ale bez połączenia z fizycznym urządzeniem.
2. **Dołączenie komputera do domeny**: Kiedy fizyczny komputer jest dołączany do domeny, proces weryfikuje, czy istnieje już zarejestrowane konto komputera w AD. Jeśli takie konto istnieje (przez pre-staging), system skojarzy nowy komputer z tym kontem.
3. **Przypisywanie uprawnień**: Administratorzy mogą również przypisać prawa do dołączenia komputera do domeny wybranym użytkownikom lub grupom. Jeśli użytkownik próbuje dodać komputer do domeny, ale nie ma przypisanych praw, proces zostanie zablokowany.

Scenariusze, w których pre-staging jest przydatny:

- **Środowiska o wysokim poziomie bezpieczeństwa**: W firmach z restrykcyjnymi zasadami bezpieczeństwa, gdzie nie każdy użytkownik może dodawać komputery do domeny.
- **Przygotowanie maszyn przed masowym wdrożeniem**: W środowiskach, gdzie przed masowym wdrożeniem komputerów, administratorzy chcą upewnić się, że wszystkie komputery trafią do odpowiednich jednostek organizacyjnych (OU) i będą objęte odpowiednimi politykami grupowymi.
- **Ograniczenie nieautoryzowanego dodawania komputerów do domeny**: Pre-stage ogranicza możliwość, aby standardowy użytkownik przypadkowo (lub celowo) dodał nieznany komputer do domeny, co mogłoby zagrozić bezpieczeństwu sieci.

Podsumowanie:

Prestage konta komputera to praktyka stosowana przez administratorów Active Directory w celu zwiększenia kontroli nad procesem dołączania komputerów do domeny. Dzięki pre-stagingowi możliwe jest przypisanie komputerów do odpowiednich jednostek organizacyjnych z góry oraz kontrola, kto ma uprawnienia do dołączania komputerów do domeny, co poprawia bezpieczeństwo i organizację infrastruktury sieciowej.