12.6 Polityka haseł w domenie

Przed przystąpieniem do ćwiczenia sprawdź i ustaw

W Menedżer funkcji Hyper-V wybierz nazwa maszynę wirtualna twojej grupy_dc2019

Upewnij się, że punk kontrolny, zawiera serwer z zainstalowanym kontrolerem domeny.

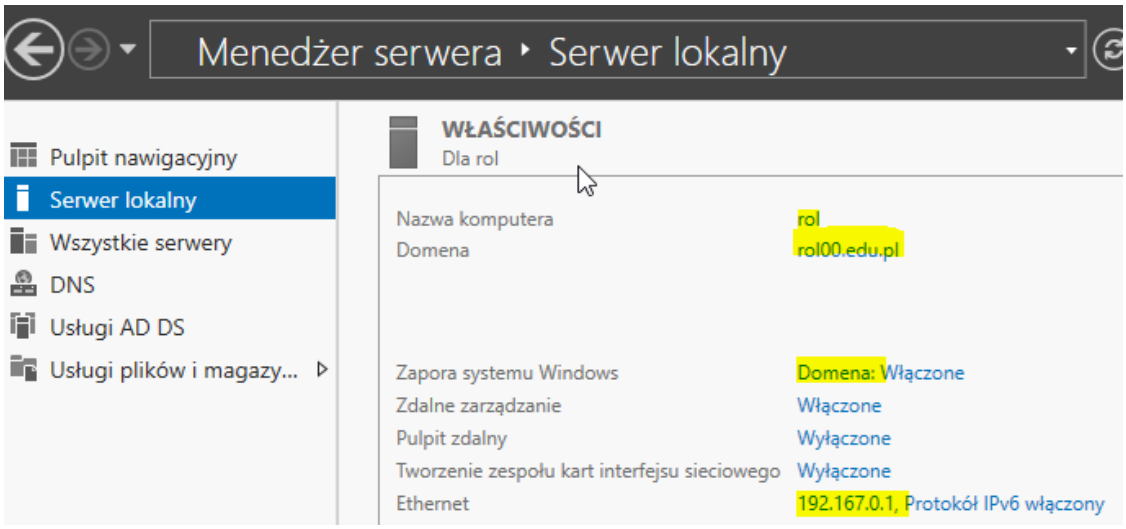
W VirtualBox wybierz nazwa maszynę wirtualna twojej grupy_dc2019

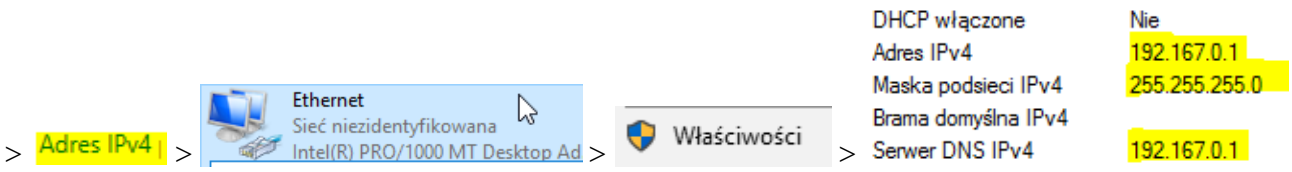
Upewnij się, że migawka, z którą pracujesz to serwer z zainstalowanym kontrolerem domeny.

Przed przystąpieniem do ćwiczenia sprawdź i ustaw, jeśli to konieczne

Uruchom maszynę > Ctrl+Delete > Administrator > zaq1@WSX

a) system serwera są jak poniżej:





W VirtualBox utwórz kolejną migawkę stanu systemu serwera z informacją o treści Migawka …

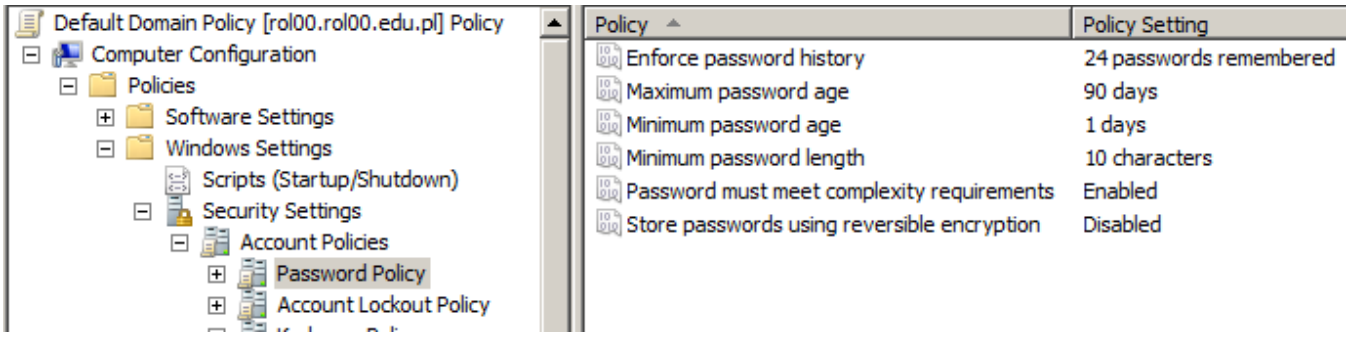
W zeszycie opisz procedury tworzenie polityki haseł w domenie.

Zadanie 1

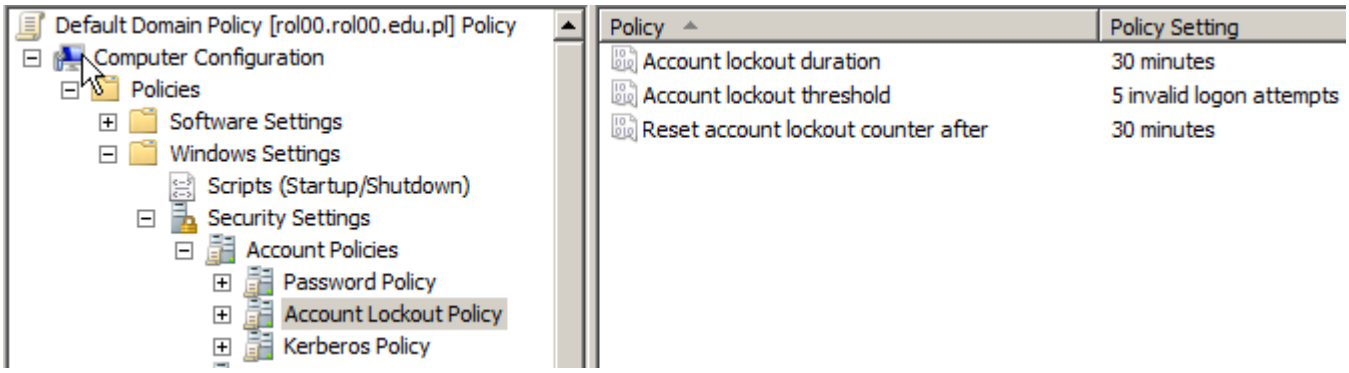
Konfigurowanie domenowych zasad haseł i blokady konta

W tym zadaniu zmodyfikujemy obiekt zasad grupy Default Domain Policy, aby zaimplementować zasady haseł i blokady konta dla użytkowników w domenie rol00.edu.pl.

1. Zaloguj się jako Administrator na komputerze rol00.
2. Otwórz konsolę Group Policy Management (Zarządzanie zasadami grupy) z foldera Administrative Tools (Narzędzia administracyjne).
3. Rozwiń węzły Forest (Las), Domains (Domeny) i rol00.edu.pl.
4. Kliknij prawym przyciskiem myszy obiekt Default Domain Policy w domenie rol00.edu.pl i wybierz Edit (Edytuj).
   Może pojawić się komunikat przypominający, że zmieniamy ustawienia obiektu zasad grupy.
5. Kliknij OK.
   Pojawi się konsola Group Policy Management Editor (Edytor zarządzania zasadami grupy).
6. Rozwiń folder Computer Configuration\Policies\Windows Settings\Security Scttings\ Account Policies (Konfiguracja komputera\Zasady\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zasady konta), a następnie zaznacz węzeł Password Policy (Zasady haseł).
7. Podwójnie kliknij następujące ustawienia zasad w okienku szczegółów konsoli i skonfiguruj podane ustawienia:
   - Maximum Password Age (Maksymalny okres ważności hasła): 90 dni
   - Minimum Password Length (Minimalna długość hasla): 10 znaków



8. Zaznacz węzeł Account Lockout Policy (Zasady blokady konta) w drzewie konsoli.
9. Podwójnie kliknij ustawienie zasady Account Lockout Thresholcl (Próg blokady konta) i skonfiguruj ją na 5 nieudanych prób logowania. Następnie kliknij OK.
10. Pojawi się okno Suggested Value Changes (Sugerowana zmiany wartości). Kliknij OK.
    Wartości zasad Account Lockout Duration (Czas trwania blokady konta) i Reset Account Lockout Counter After (Wyzeruj licznik blokady konta po) zostaną automatycznie ustawione na 30 minut.



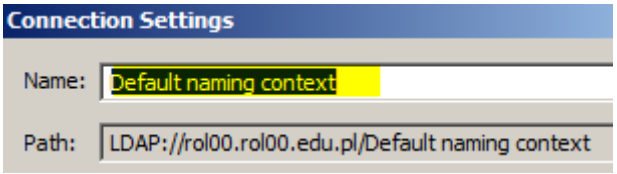
11. Zamknij okno konsoli Group Policy Management Editor (Edytor zarządzania zasadami grupy).

Zadanie 2

Tworzenie obiektu ustawień haseł

W tym zadaniu utworzysz obiekt PSO, który zastosuje restrykcyjne, szczegółowe zasady haseł wobec użytkowników w grupie Domain Admins (Administratorzy domeny). Zanim przejdziesz do tego zadania, potwierdź, że grupa Domain Admins (Administratorzy domeny) znajduje się w kontenerze Users. Jeżeli nie, to przenieś ją do kontenera Users.

1. Otwórz ADSI Edit (Edytor ADSI) z foldera Administrative Tools (Narzędzia administracyjne).
2. Kliknij prawym przyciskiem myszy folder ADSI Edit (Edytor ADSI) i wybierz opcję Connect To (Połącz z).



3. W polu Name (Nazwa) pozostaw domyślną wartość. Kliknij OK.
4. Rozwiń Default naming context [rol00.rol00.edu.pl] i zaznacz DC=rol00,DC=edu,DC=pl.
5. Rozwiń węzeł DC=rol00,DC=edu,DC=pl i zaznacz CN=System.
6. Rozwiń węzeł CN=System i zaznacz CN= Password Settings Container.

Wszystkie obiekty PSO są tworzone w kontenerze Password Settings Container (PSC).

7. Kliknij prawym przyciskiem myszy kontener PSC, wybierz New (Nowy), a następnie wybierz Object (Obiekt). CN=Password Settings Container > pk > New > Object...

Pojawi się okno dialogowe Create Object (Tworzenie obiektu). Prosi ono o podanie typu obiektu do utworzenia, jest tylko jeden wybór: msDS-PasswordSettings – techniczna nazwa dla klasy obiektu PSO.

8. Kliknij Next (Dalej).

Następnie zostaniemy poproszeni o podanie wartości dla każdego atrybutu PSO.

Te atrybuty są podobne do tych, które można znaleźć w obiekcie zasad grupy, który badaliśmy w zadaniu 1.

9. Skonfiguruj każdy atrybut zgodnie z następującą listą, Kliknij Next (Dalej) po każdym atrybucie. (Wpisujemy wartości kolejnych obiektów zaznaczone na żółto.)

- Common-Name: Obiekt PSO dla administratorów domeny, jest to przyjazna nazwa obiektu PSO.
- msDS-PasswordSettingsPrecedence: 1. Ten obiekt PSO ma najwyższe możliwe pierwszeństwo, ponieważ jego wartość jest najbliższa 1.
- msDS-PasswordReversihleEncryptionEnabled: False. Hasło nie będzie przechowywane przy użyciu szyfrowania odwracalnego.
- msDS-PasswordHistoryLength: 30. Użytkownik nie może ponownie wykorzystać żadnego 2 ostatnich 30 haseł.
- msDS-PasswordComplexityEnabled: True. Wymuszone są reguły skomplikowania hasła.
- msDS-MinimumPasswordLength: 15. Hasła muszą mieć długość co najmniej 15 znaków.
- msDS-MinirnumPasswordAge: 1:00:00:00. Użytkownik nie może zmienić swojego hasła w ciągu jednego dnia od poprzedniej zmiany Format ma postać d:gg:mm:ss (dni, godziny, minuty. sekundy).
- MaximumPasswordAge: 45:00:00:00. Hasło musi być zmieniane co 45 dni.
- msDS-LockoutThreshold: 5. Pięć nieprawidłowych logowań w czasie określanym przez atrybut MSDN-LockoutObservationWindow spowoduje zablokowanie konta.
- msDS-LockoutObservationWindow: 0:01:00:00. Pięć nieprawidłowych logowań (określone w poprzednim atrybucie) w ciągu jednej godziny spowoduje zablokowanie konta.
- msDS-LockoutDuration: 1:00:00:00. Zablokowane konto pozostanie zablokowane przez jeden dzień albo dopóki ktoś go ręcznie nie odblokuje. Wartość zero sprawi, że konto pozostanie zablokowane, dopóki administrator go nie odblokuje.

Wymienione atrybuty są wymagane. Po kliknięciu Next (Dalej) na stronie atrybutu msDS-LockoutDuration można skonfigurować atrybuty opcjonalne (pomiń).

10. Kliknij przycisk More Attributes (Więcej atrybutów).
11. W polu Edit Attributes (Edytuj atrybut) wpisz CN=DomainAdmins,CN=Users,DC=rol00,DC=edu,DC=pl (jest domyślnie) i kliknij OK.

Kliknij Finish (Zakoncz).

Zadanie 3

Ustalanie wynikowego obiektu PSO dla użytkownika

W tym zadaniu zidentyfikuj obiekt PSO, który określa zasady hasła i blokady konta dla wybranego użytkownika.

1. Otwórzy przystawkę Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory).
2. Kliknij menu View (Widok) i upewnić się. że zaznaczona jest opcja Advanced Features (Opcje zaawansowane).
3. Rozwiń domenę rol00.edu.pl i kliknij kontener Users w drzewie konsoli.
4. Kliknij prawym przyciskiem myszy konto Administrator i wybierz Properties (Właściwości).
5. Kliknij kartę Attribute Editor (Edytor atrybutów).
6. Kliknij przycisk Filter (Filtruj) i upewnić się, że zaznaczona jest opcja Constructed (Złożone).
   Atrybut, który znajdziemy w następnym kroku jest atrybutem złożonym, co oznacza, że wynikowy obiekt PSO nie jest zakodowanym trwale atrybutem użytkownika, a raczej jest obliczany w czasie rzeczywistym na podstawie badania obiektów PSO przyłączonych do użytkownika.
7. Na liście Attributes (Atrybuty) znajdź msDS-ResultantPSO.
8. Ustal obiekt PSO wpływający na użytkownika.
   Obiekt PSO dla administratorów domeny, który utworzyłeś/łaś w zadaniu 2 „Tworzenie obiektu ustawień haseł" jest wynikowym obiektem PSO dla konta Administrator.

Poproś nauczyciela, pokaż efekt wykonania zadania.

Zadanie 4

Usuwanie obiektu PSO

W tym zadaniu usuniemy obiekt PSO utworzony w zadaniu 2, tak aby jego ustawienia nie wpływały na nas w późniejszych zadaniach.

1. Powtórz kroki 1-6 zadania 2, aby zaznaczyć węzeł Password Settings Containen w programie ADSI Edit (Edytor ADSI).
2. W okienku szczegółów konsoli zaznaczyć CN=Obiekt PSO dla administratorów domeny.
3. Naciśnij Delete.

4. Kliknij Yes (Tak).

Notatka: Zapisz w zeszycie podsumowanie lekcji

Ustawienia zasad haseł określają, kiedy hasło może lub musi być zmienione i jakie są wymagania odnośnie nowego hasła.

Ustawienia blokady konta powodują zablokowanie konta użytkownika przez Active Directory, jeśli wystąpi określona liczba nieprawidłowych logowań w określonym odstępie czasu.
Blokada pomaga zapobiegać ciągłym próbom logowania się na koncie użytkownika przez intruza, które ma na celu odgadnięcie hasła użytkownika.

Domena może mieć tylko jeden zestaw zasad haseł i blokady konta wpływający na wszystkich użytkowników w domenie. Te zasady są definiowane przy użyciu zasad grupy.
Można modyfikować domyślne ustawienia w obiekcie zasad grupy Default Domain Policy, aby konfigurować zasady dla swojej organizacji.

System Windows Server 2008 udostępnia opcję określania różnych zasad haseł i blokady konta dla globalnych grup zabezpieczeń i użytkowników w domenie. Szczegółowe zasady haseł są wdrażane nie przy użyciu zasad grupy, ale za pomocą obiektów ustawień haseł.

Jeśli więcej niż jeden obiekt PSO ma zastosowanie wobec użytkownika lub grup, do których użytkownik należy, to pojedynczy obiekt PSO zwany wynikowym obiektem PSO określa zasady haseł i blokady konta obowiązujące dla tego użytkownika. Wybrany zostanie obiekt PSO z najwyższym pierwszeństwem (wartością pierwszeństwa bliższa 1). Jeśli jeden lub kilka obiektów PSO jest przyłączonych bezpośrednio do użytkownika, a nie pośrednio do grup, to obiekty PSO przyłączone do grup nie będą brane pod uwagę przy określaniu wynikowego obiektu PSO, a przeważy obiekt PSO przyłączony do użytkownika i mający najwyższe pierwszeństwo.