

Ćwiczenie 1: Zapoznanie się ze środowiskiem wirtualnym, tworzenie nowego lasu, domeny.

Zestaw laboratoryjny

Zestaw laboratoryjny

Virtual BOX - HotKey : Prawy control

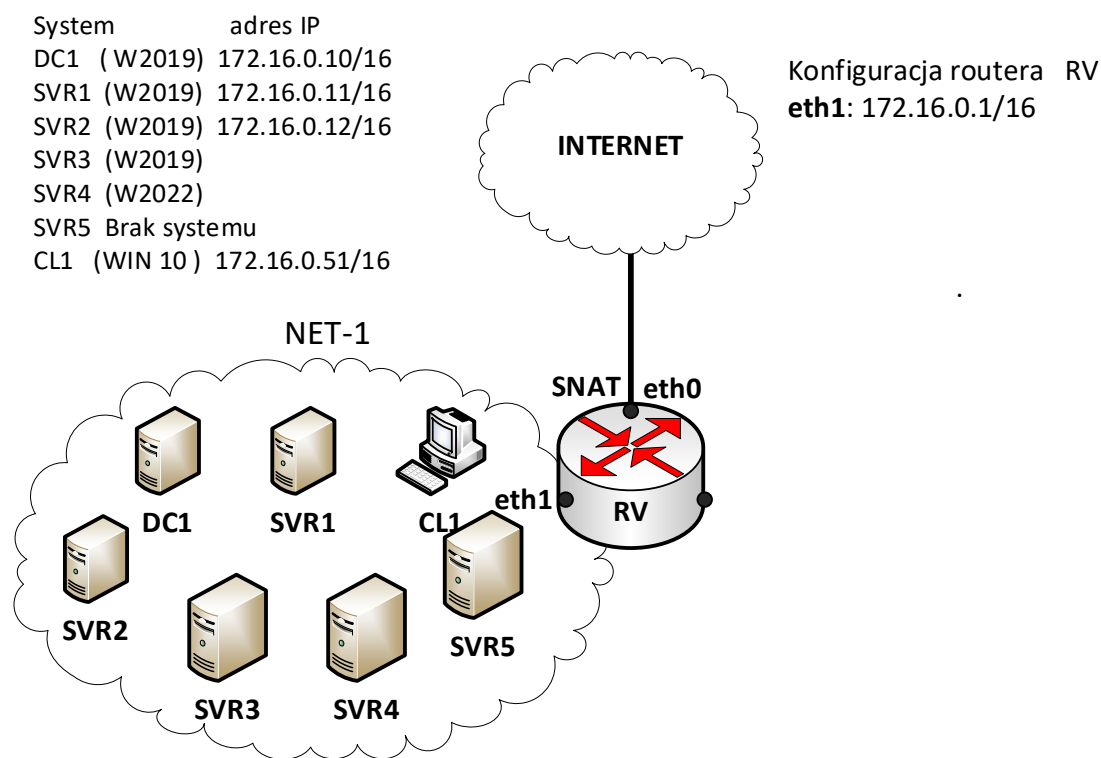
Ctrl-Alt-Del -> HotKye Del

FullScreen -> HotKye F

FullScreen -> HotKye F

AutoSkalowanie -> HotKye Y

Na poniższym schemacie (rys. 1) przedstawiony został zestaw laboratoryjny na którym będą wykonywane ćwiczenia.



Rys. 1. Schemat wirtualnej sieci laboratoryjnej

DC1 : Windows Server 2019, kontroler domeny

Adresacja IP 172.16.0.10/16 , Brama domyślna 172.16.0.1, DNS 127.0.0.1

SVR1: Windows Server 2019, członek domeny

Adresacja IP 172.16.0.11/16 , Brama domyślna 172.16.0.1, DNS 172.16.0.10

SVR2: Windows Server 2019, członek domeny

Adresacja IP 172.16.0.12/16 , Brama domyślna 172.16.0.1, DNS 172.16.0.10

CL1: Windows 10 lub 11 (minimum profesjonal) – Komputer kliencki w domenie.
Adresacja IP 172.16.0.50/16 , Brama domyślna 172.16.0.1

SVR3: System Windows Server 2019 – zainstalowany , bez wstępnej konfiguracji

SVR4: Zainstalowany system Windows Server 2022

UWAGI dotyczące haseł i użytkowników

Hasło domenowe: **Pa55w.rd (administrator)**

Hasło lokalne: **Pa\$\$w0rd (administrator)**

- a) Zaloguj się jako użytkownik **administrator@keja.msft** z hasłem **Pa55w.rd**, patrz rys.1
HASŁA:



Rys. 1. Ekran logowania

W zestawie laboratoryjnym używane są następujące hasła

- logowanie do kont domenowych **Pa55w.rd**
- logowanie do kont lokalnych **Pa\$\$w0rd**

UWAGA !! Domena ma nazwę **keja.msft** , zalogować się do niej można w następujący sposób **nazwa_uzytkownika@keja.msft** lub **keja\nazwa_uzytkownika**.

- b) Poświęć kilka minut na przejrzanie opcji i zapoznanie się z Server Managerem.

2) Sprawdzenie konfiguracji IP maszyn wirtualnych i komunikacji IP.

Wstęp Teoretyczny:

Przed rozpoczęciem pracy z domeną, ważne jest, aby każda maszyna miała poprawnie skonfigurowane parametry sieciowe. Sprawdzanie konfiguracji IP oraz komunikacji między maszynami wirtualnymi pozwala upewnić się, że systemy są poprawnie połączone i mogą się komunikować z kontrolerem domeny (DC).

Parametry sieciowe – Kluczowe elementy:

- **Adres IP (IP Address):** Unikalny identyfikator komputera w sieci.
- **Maska podsieci (Subnet Mask):** Definiuje zakres adresów IP, które mogą się ze sobą komunikować bez konieczności użycia routera.
- **Brama domyślna (Default Gateway):** Urządzenie, które umożliwia komunikację z urządzeniami poza lokalną siecią.

- **DNS (Domain Name System):** Serwer, który tłumaczy nazwy domenowe na adresy IP, umożliwiając komunikację między systemami na podstawie nazw.

PowerShell to potężne narzędzie, które umożliwia administratorom zarządzanie konfiguracją systemu, w tym sieciami i połączeniami w domenę. W tym ćwiczeniu użyjemy następujących komend:

- **Get-NetIPConfiguration:** Wyświetla konfigurację sieciową systemu, w tym adres IP, maskę podsieci, bramę domyślną i serwer DNS.
- **Test-ComputerSecureChannel:** Testuje połączenie komputera z kontrolerem domeny, sprawdzając poprawność i bezpieczeństwo kanału komunikacyjnego między systemem a domeną.

Wykonaj zadania:

Uruchom **SVR1**

Zweryfikuj

- konfigurację IP (Adres IP, Maska, Brama Domyślną, Server DNS)
- zainstalowany system operacyjny

W tym celu uruchom w PowerShell w trybie administratora i wykonaj polecenie

```
Get-NetIPConfiguration
Test-ComputerSecureChannel
```

Polecenie to testuje kanał komunikacyjny pomiędzy danym systemem a kontrolerem domeny (DC1). Powtórz powyższą czynność na pozostałych systemach domenowych.

Zamknij system SVR1, Powtórz punkt 2 dla SVR2 i CL1.

Po zakończeniu punktu 2 powinieneś mieć jedynie uruchomiony system **DC1**

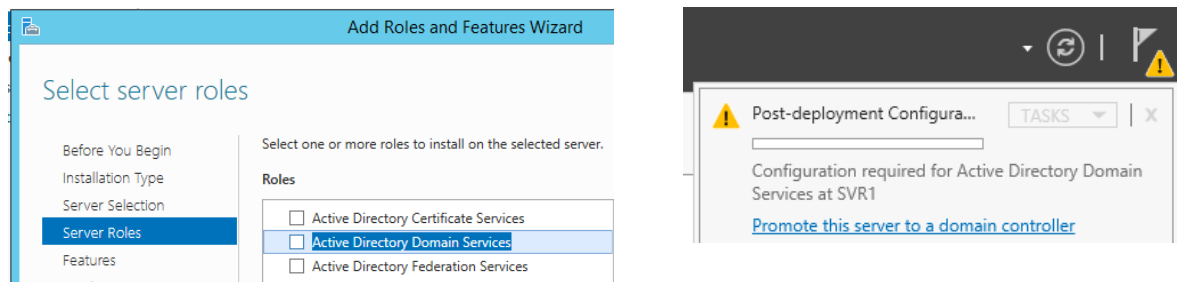
Zadanie 2: Utworzenie nowej domeny (lasu), Dodanie komputera do domeny

Firma w której jesteś zatrudniony postanowiła zaimplementować system Windows Server 2019 oraz usługę katalogową Active Directory. Przygotowany został serwer **SVR3**. Zadanie, które otrzymałeś polegają na:

- Wstępnej konfiguracja systemu oraz zainstalowaniu wskazanych funkcjonalności,
- przekształceniu systemu **SVR3** w kontroler domeny,
- przeniesienie komputera klienckiego **CL1** z domeny keja.msft do nowopowstałej domeny.

1. Włącz wirtualne maszynę **SVR3** i **dokonaj** wstępnej konfiguracja systemu.
 - a. Zaloguj się do systemu **SVR3**
 - b. Zmień nazwę komputera na swoje **NEWDC**
 - c. Wdróż następującą konfigurację **IP**: 172.16.0.13/16, brama domyślna 172.16.0.1, DNS 127.0.0.1

2. Zainstaluj rolę Active Directory Domain Services (rys. 2a), po zainstalowaniu wykonaj czynności poinstalacyjne (rys 2b) , promując serwer na nowy kontroler domeny w nowym lesie.



Rys. 2a i 2b. Instalowanie Active Directory i promocja kontrolera domeny

Nazwa domeny powinna być następująca **kejasail.msft**

3. Dodaj komputer kliencki **CL1** do nowoutworzonej domeny (w pierwszej kolejności przenieś go do grupy roboczej (o dowolnej nazwie) gdyż aktualnie jest członkiem domeny **keja.msft** a następnie zmień konfigurację IP) i dodaj do nowoutworzonej domeny.
4. Opcjonalnie, jeśli wystarczy masz czasu to do nowej domeny możesz dodać komputer **SVR4**

Po zakończonym ćwiczeniu **przywróć maszynę do stanu INIT** (sprzed wykonania ćwiczeń)

Uzupełnienie wiedzy, Lokacje w Active Directory

Lokacje (ang. **Sites**) to elementy infrastruktury Active Directory (AD), które odzwierciedlają fizyczną strukturę sieci organizacji. Używane są do optymalizacji replikacji danych między kontrolerami domeny oraz zarządzania przepływem ruchu sieciowego, szczególnie w środowiskach rozproszonych geograficznie.

1. Cel lokacji:

Lokacje w AD zostały zaprojektowane, aby zoptymalizować komunikację między kontrolerami domeny oraz minimalizować opóźnienia i przeciążenia w replikacji. Lokacje grupują **kontrolery domeny** znajdujące się w tej samej fizycznej lokalizacji sieciowej (np. w jednym centrum danych lub biurze), co pozwala na efektywniejsze zarządzanie replikacją między nimi.

2. Lokacje a fizyczna struktura sieci:

- **Logika vs fizyka:** W przeciwieństwie do domen, które są logicznymi strukturami AD, lokacje odzwierciedlają rzeczywistą fizyczną lokalizację sieci (taką jak oddział firmy czy centrum danych).
- **Podział sieci:** Lokacje są zazwyczaj używane w sieciach rozproszonych, gdzie różne oddziały organizacji mogą być połączone wolniejszymi łączami WAN. Lokacje pomagają w minimalizowaniu ruchu replikacyjnego przez takie łącza.

3. Replikacja danych w AD:

Replikacja między kontrolerami domeny w ramach jednej **lokacji** odbywa się w sposób **automatyczny i szybki**, bez większych ograniczeń. Natomiast replikacja między **lokacjami** jest zoptymalizowana tak, aby ograniczać przepustowość łącza – odbywa się rzadziej i zgodnie z ustalonymi harmonogramami.

- **Intra-Site Replication:** Replikacja między kontrolerami domeny w obrębie tej samej lokacji. Jest to szybki proces realizowany przy użyciu protokołu RPC (Remote Procedure Call).
- **Inter-Site Replication:** Replikacja między kontrolerami domeny w różnych lokacjach. Zwykle korzysta z protokołu SMTP lub RPC, jednak może być dostosowana do pracy przy mniejszych przepustowościach łącza.

4. Elementy lokacji w AD:

- **Subnety:** Lokacje są powiązane z subnetami (podsieciami IP), co pozwala na przypisywanie komputerów i serwerów do odpowiednich lokacji na podstawie ich adresów IP.
- **Bridgehead Servers:** Kontroler domeny w lokacji, który odpowiada za wymianę danych replikacyjnych między lokacjami. To kluczowe serwery, które minimalizują ruch replikacyjny przez łącza WAN.

5. Przykłady zastosowania lokacji:

- **Rozproszone biura:** Organizacja posiadająca biura w różnych miastach lub krajach może skonfigurować osobne lokacje dla każdego oddziału. Dzięki temu replikacja między nimi będzie zoptymalizowana i nie będzie przeciążać wolniejszych łączy między lokalizacjami.
- **Optymalizacja logowania użytkowników:** Lokacje zapewniają, że użytkownicy uwierzytelniają się na najbliższym kontrolerze domeny, co przyspiesza logowanie i dostęp do zasobów.

6. Korzyści z używania lokacji:

- **Optymalizacja replikacji:** Lokacje redukują nadmiarowy ruch sieciowy i minimalizują wykorzystanie przepustowości łącza w przypadku replikacji między geograficznie oddalonymi lokalizacjami.
- **Lepsze zarządzanie zasobami:** Lokacje pozwalają na przypisywanie zasobów sieciowych w zależności od fizycznej lokalizacji, co ułatwia zarządzanie użytkownikami i komputerami.

- **Zwiększenie wydajności:** Zwiększenie efektywności operacji logowania i dostępu do zasobów poprzez kierowanie użytkowników do najbliższego kontrolera domeny.

Podsumowanie:

Lokacje w Active Directory to elementy odzwierciedlające fizyczną strukturę sieci organizacji. Ich głównym celem jest optymalizacja replikacji między kontrolerami domeny, szczególnie w środowiskach rozproszonych geograficznie. Lokacje umożliwiają także lepsze zarządzanie ruchem sieciowym oraz poprawiają wydajność logowania użytkowników, co jest kluczowe dla dużych organizacji działających w wielu lokalizacjach.