5.2 Usługi domenowe Konfigurowanie serwera DNS Pliki hosts i lmhosts WINS UNC.

Cel ogólny lekcji: Nauczenie się instalacji i konfiguracji serwera DNS oraz zrozumienie roli i zastosowania plików hosts i lmhosts, serwera WINS, ścieżki UNC.

Cele szczegółowe lekcji:

1. Zainstalowanie i skonfigurowanie serwera DNS na serwerze ROL.
2. Zrozumienie roli i zastosowania plików hosts i lmhosts.
3. Umiejętność użycia plików hosts i lmhosts oraz sposobu testowania.
4. Zrozumienie znaczenia nazwy hosta jako elementu logicznego przypisanego do urządzenia i jej roli w identyfikacji urządzenia w sieci.
5. Wykonanie konfiguracji strefy wyszukiwania do przodu w serwerze DNS.
6. Wykonanie konfiguracji strefy wyszukiwania wstecz w serwerze DNS.
7. Porównanie ilości rekordów z kontrolerem domeny AD oraz bez niego.
8. Wykonanie konfiguracji usługi przesyłania dalej nieobsłużonych zapytań (DNS forwarding).
9. Zrozumienie znaczenia serwera WINS (Windows Internet Name Service) i jego roli w sieci NetBIOS.
10. Skonfigurowanie serwera WINS w systemie Windows Server 2019.
11. Zrozumienie i użycie Universal Naming Convention (UNC) w systemach Windows.
12. Wykonanie używania ścieżki UNC w systemie Windows Server 2019.
13. Wykonanie używania ścieżki UNC w systemie Windows 11.
14. Wykonanie używania ścieżki UNC do pliku w systemie Windows 11.

Wprowadzenie do tematu

DNS odgrywa kluczową rolę w infrastrukturze Active Directory, umożliwiając identyfikację i lokalizację zasobów, takich jak kontrolery domeny i inne usługi związane z AD.

Poprawna konfiguracja DNS jest niezbędna dla prawidłowego działania usług Active Directory.
To serwer DNS przechowuje informacje o nazwach i lokalizacji zasobów w AD.

Chociaż pliki hosts i lmhosts były wykorzystywane w przeszłości jako metody rozpoznawania nazw, to w nowoczesnych sieciach zastosowanie DNS jest bardziej skuteczne i wszechstronne.

Ścieżki UNC są wykorzystywane do identyfikowania zasobów w sieci, w tym także w kontekście Active Directory. Przykłady zastosowania ścieżek UNC do zasobów AD, takich jak udziały sieciowe, mogą podkreślić ich znaczenie w infrastrukturze sieciowej zintegrowanej z AD.

Choć WINS jest nadal używany w pewnych środowiskach, to w sieciach opartych na nowszych technologiach, takich jak DNS, jego znaczenie znacznie się zmniejszyło. Można to skontrastować z rolą DNS jako dominującego mechanizmu rozpoznawania nazw w kontekście Active Directory.

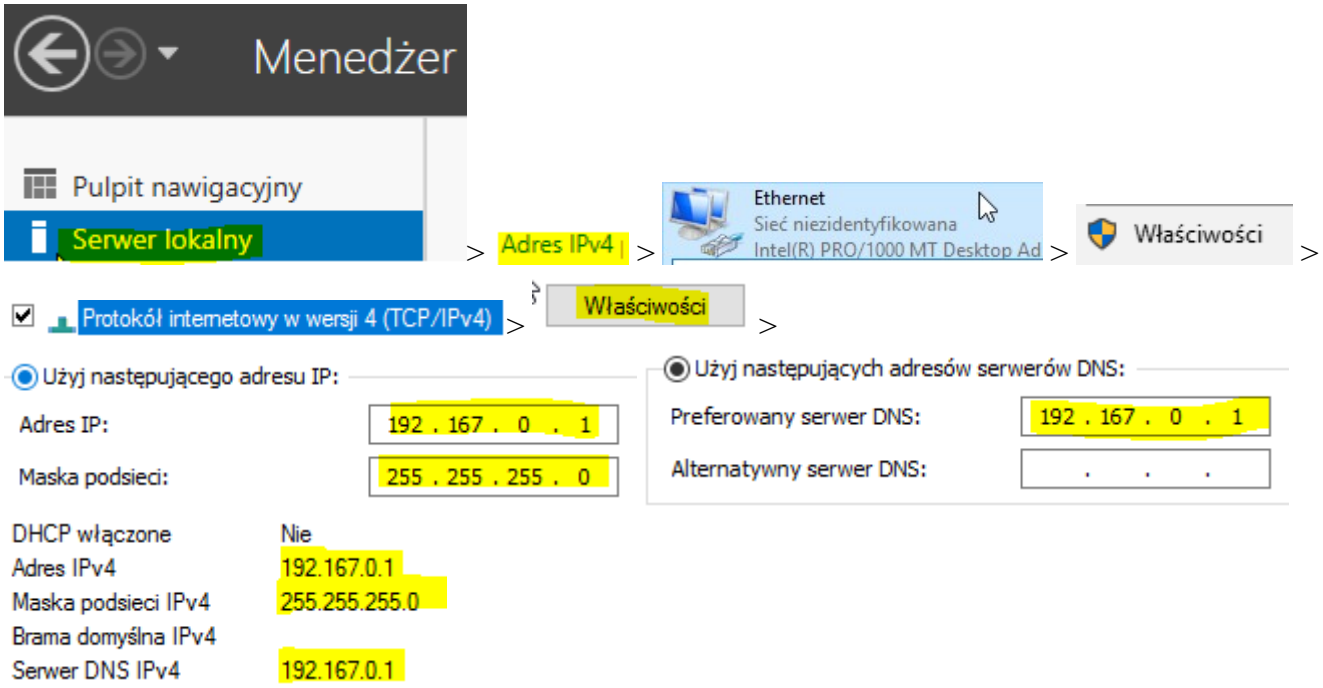
Zaczynamy ćwiczenie.

A. Usługi domenowe

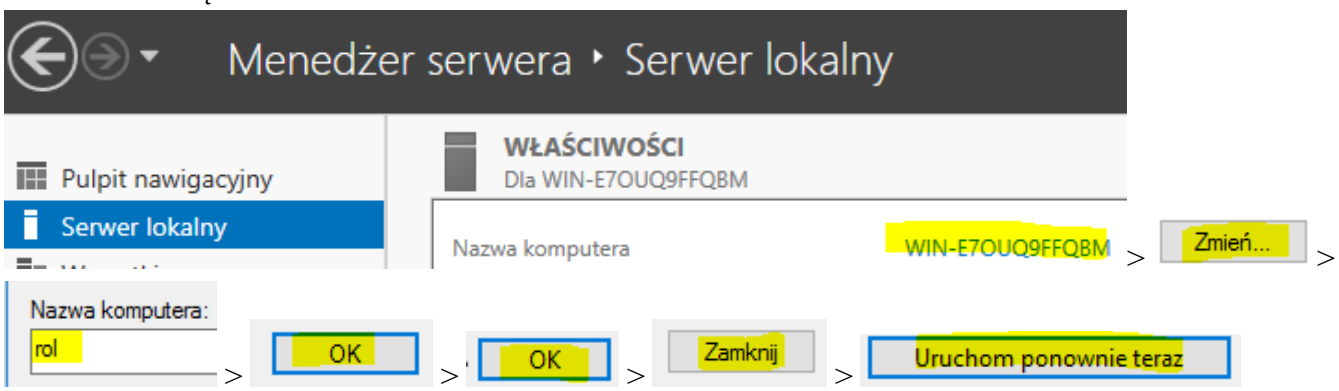
Przed przystąpieniem do ćwiczenia sprawdź i ustaw, jeśli to konieczne

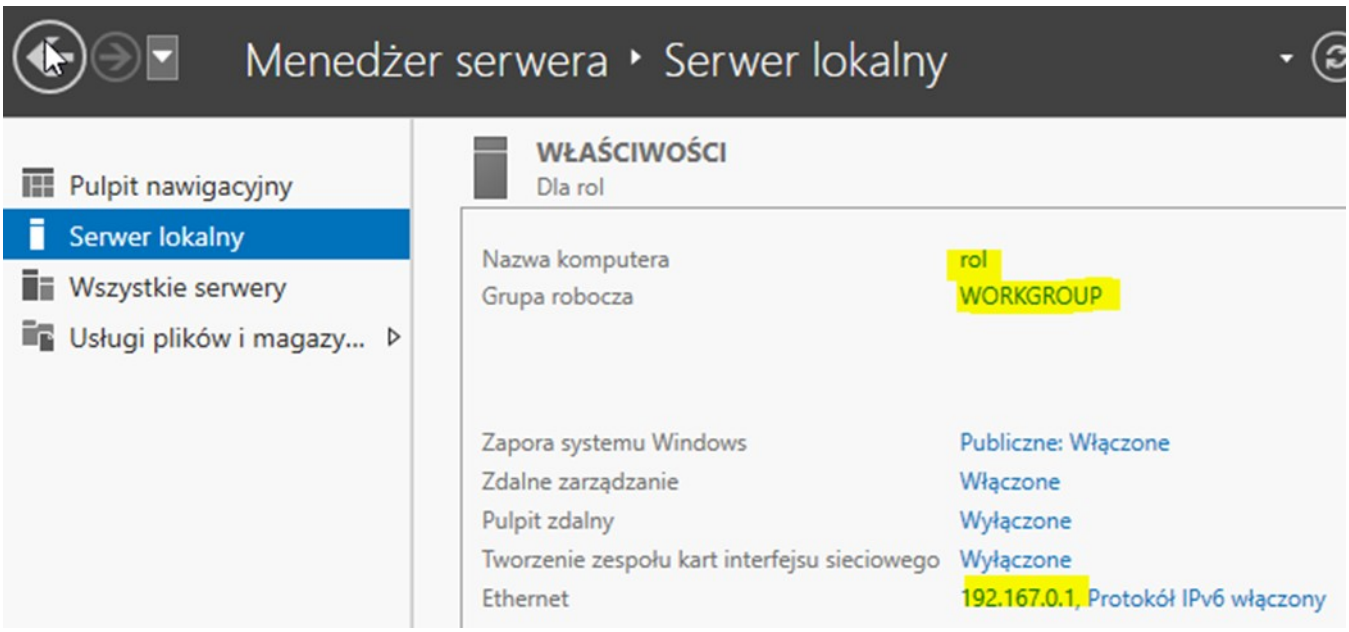
- W Menedżer funkcji Hyper-V wybierz nazwa maszynę wirtualna twojej grupy_2019
Ctrl+Delete > Administrator > zaq1@WSX

- system serwera są jak poniżej:



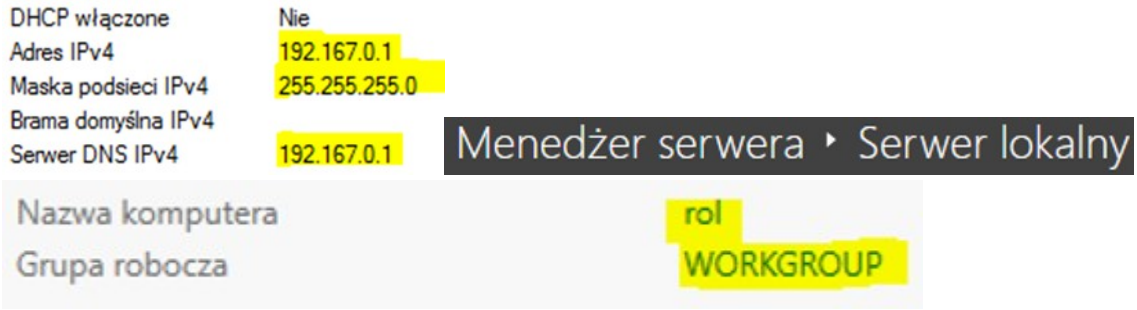
- Ustaw nazwę serwera





Przed przystąpieniem do ćwiczenia sprawdź, czy

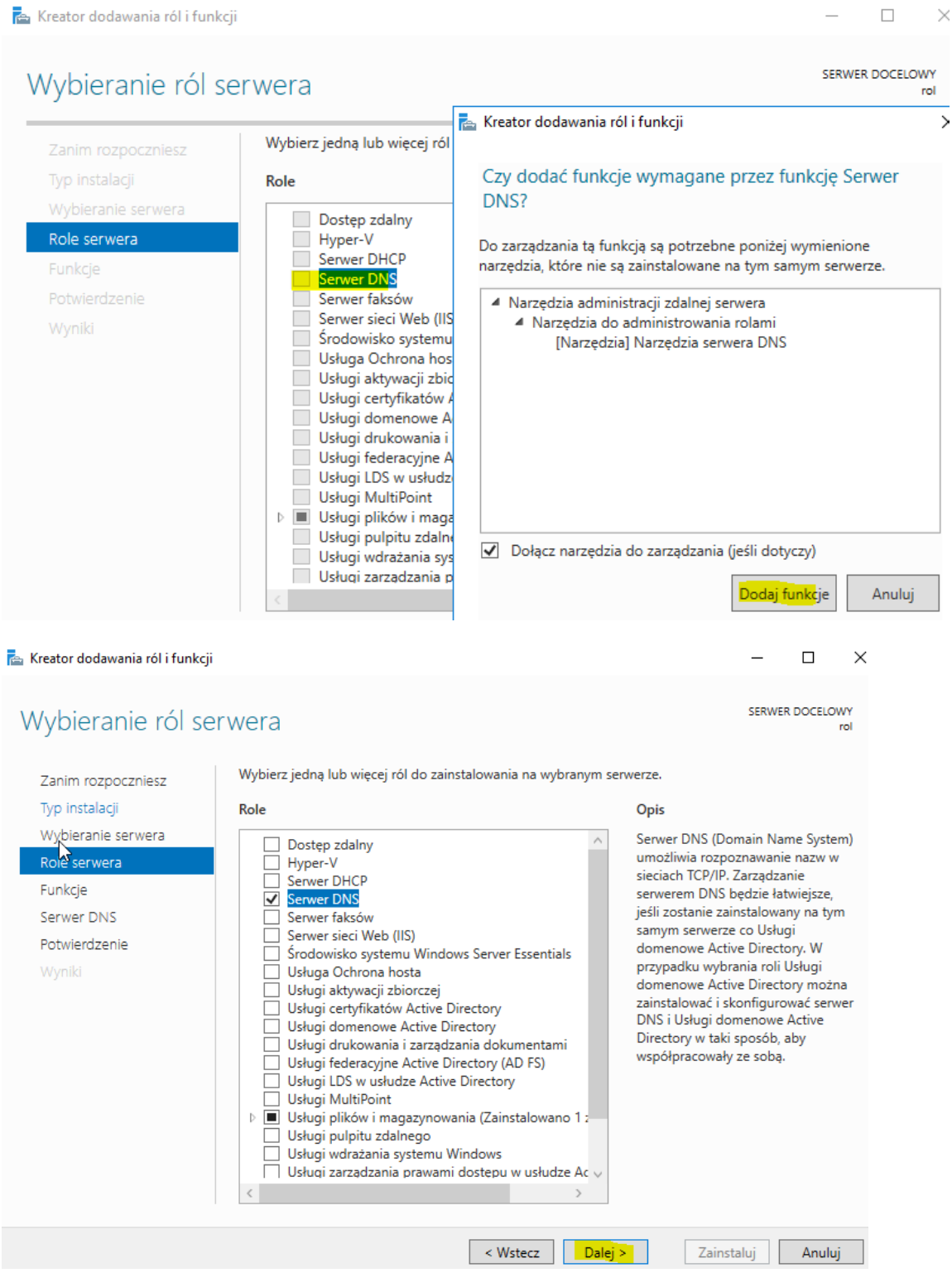
a) system serwera jest ustawiony jak poniżej:



W zeszycie opisz procedurę instalacji i konfiguracji serwera DNS (szczególnie Opis i do zapamiętania).

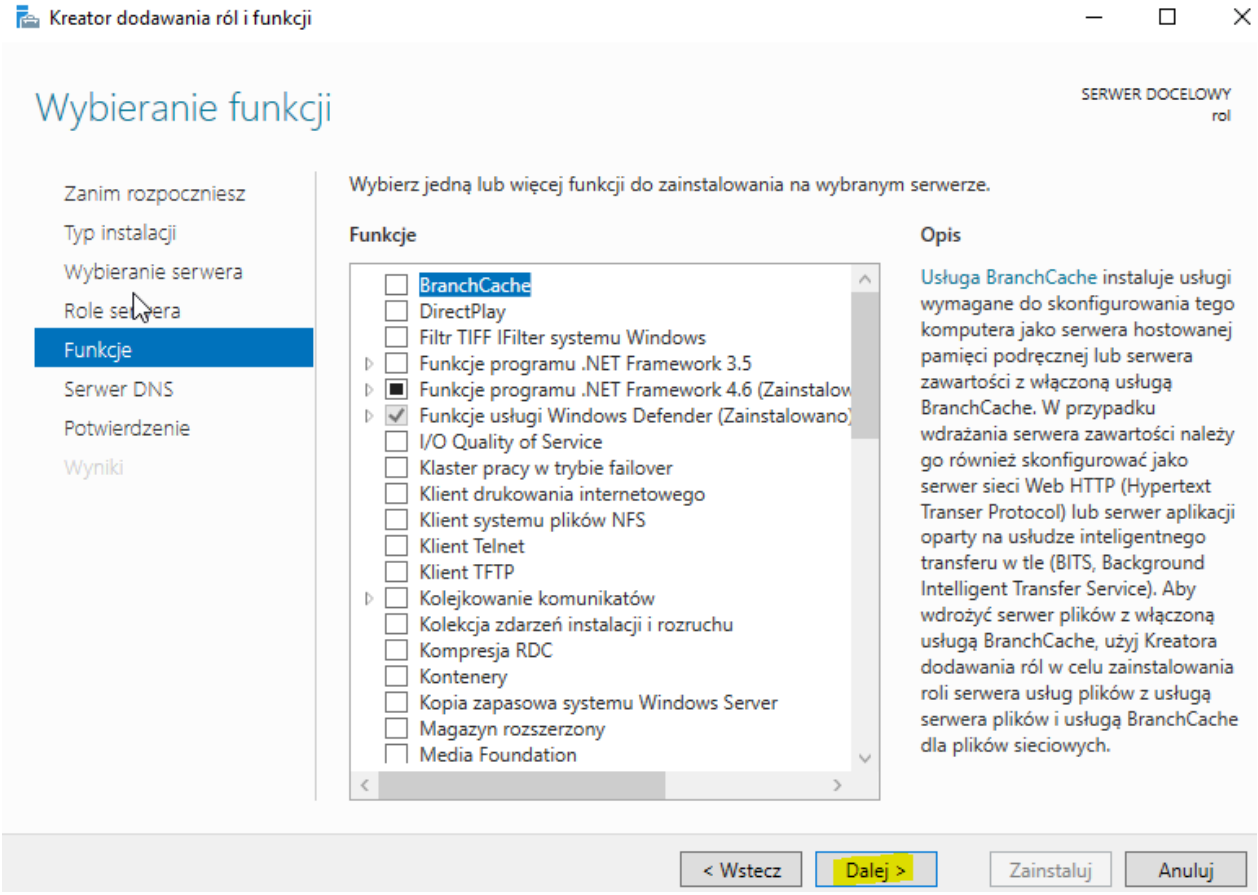
1. Dodanie roli serwera DNS na serwerze ROL
   1. Zaloguj się za pomocą konta Administrator (hasło: zaq1@WSX).
   2. W konsoli Menedżera serwera kliknij link Dodaj role i funkcje.
   3. Na stronie Przed rozpoczęciem Kreatora dodawania ról i funkcji kliknij przycisk Dalej.
   4. Na stronie Wybierz typ instalacji kliknij przycisk Dalej.
   5. Na stronie Wybierz serwer docelowy upewnij się, że wybrano ROL, a następnie kliknij przycisk Dalej.
   6. Na stronie *Wybieranie ról serwera* zaznacz pole wyboru Serwer DNS.
   7. W oknie dialogowym *Kreator dodawania ról i funkcji* kliknij opcję Dodaj funkcje.
   8. Zostanie zwrócona strona *Wybieranie ról serwera*, jak pokazano poniżej, kliknij Dalej.
   9. Na stronie *Wybieranie funkcji* kliknij przycisk Dalej.
   10. Na stronie *Serwer DNS* kliknij przycisk Dalej.
   11. Na stronie *Potwierdzenie opcji instalacji* kliknij przycisk Instaluj.
   12. Rozpocznie się proces instalacji. Kliknij Zamknij, gdy instalacja się powiedzie.

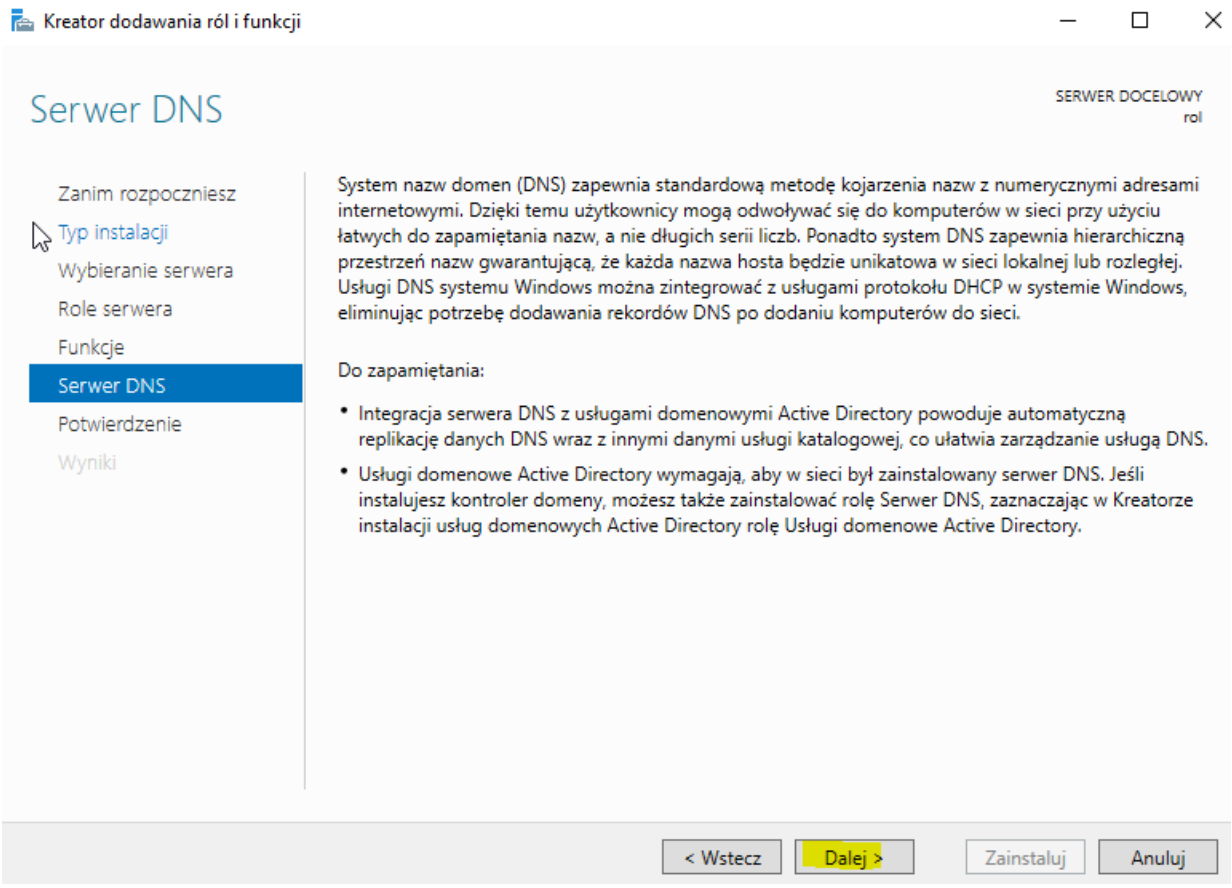
Podobnie jak w AD DS, DNS w Windows Server 2019 jest rolą dodawaną przez Server Manager, jak pokazano na rysunku 5.23:

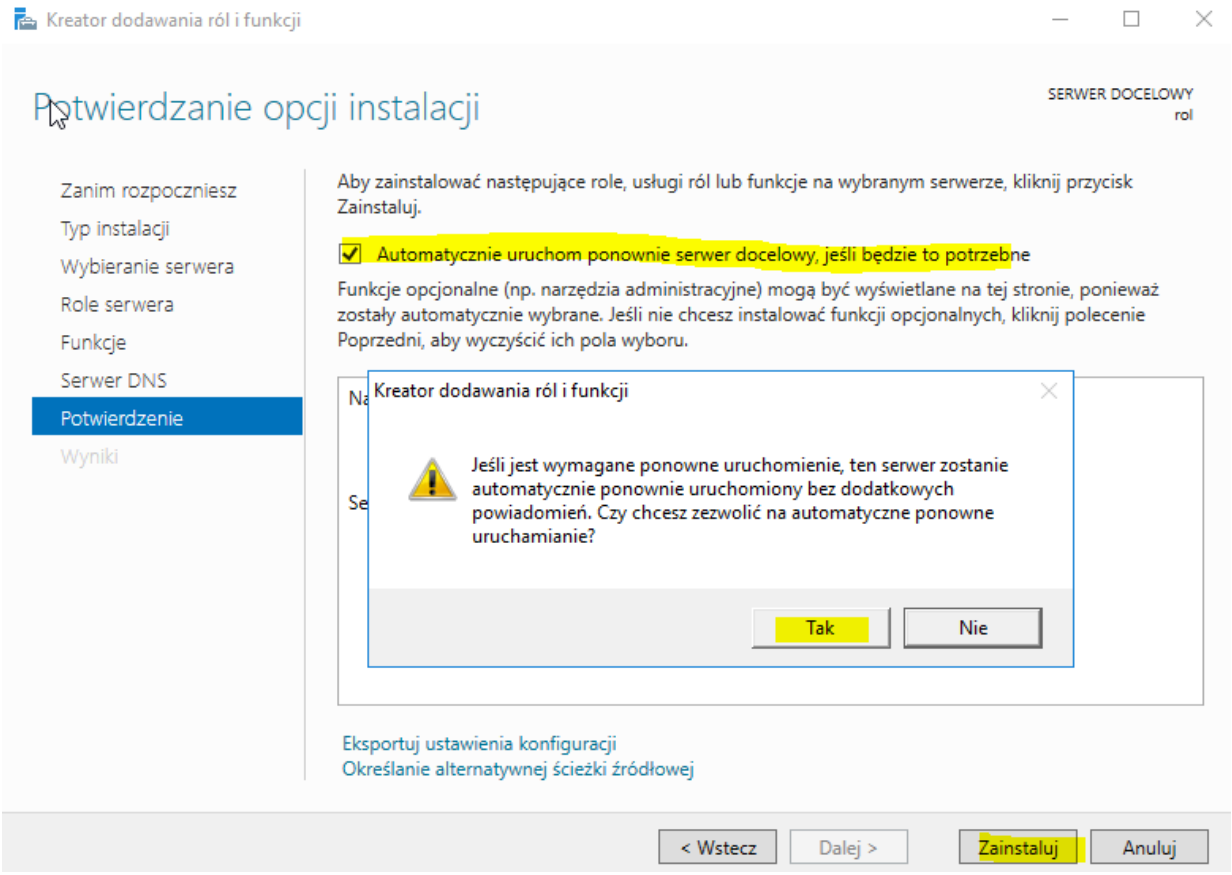


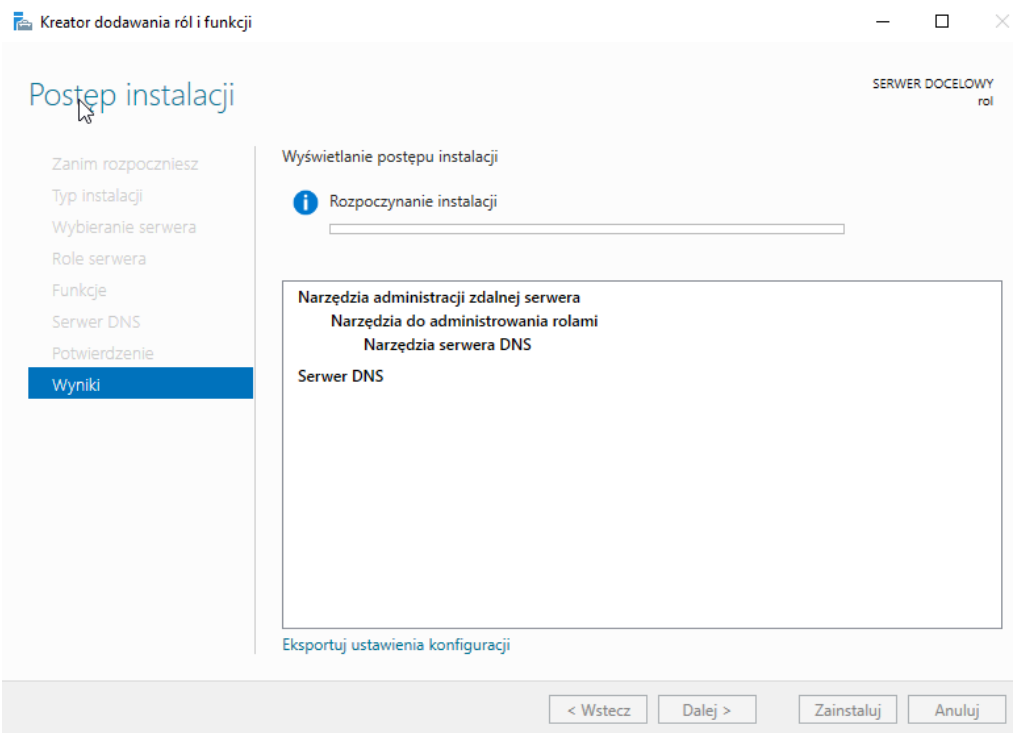
RYSUNEK 5.23. Dodanie roli DNS w systemie Windows Server 2019

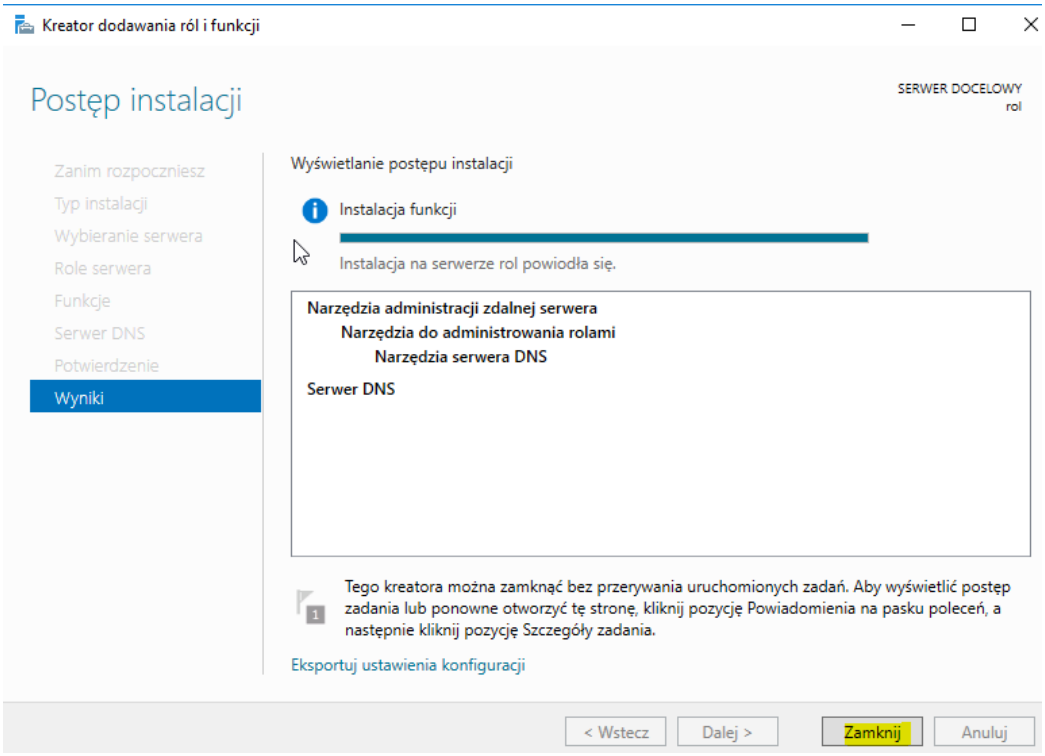
Pamiętaj, że dodając rolę DNS, dodaj ją jako osobną rolę (patrz Rysunek 5.23):


Kreator dodawania ról i funkcji
Wybieranie funkcji
SERWER DOCELOWY
rol
Zanim rozpoczniesz
Typ instalacji
Wybieranie serwera
Role serwera
Funkcje
Serwer DNS
Potwierdzenie
Wyniki
Wybierz jedną lub więcej funkcji do zainstalowania na wybranym serwerze.
Funkcje
BranchCache
DirectPlay
Filtr TIFF IFilter systemu Windows
Funkcje programu .NET Framework 3.5
Funkcje programu .NET Framework 4.6 (Zainstalow
Funkcje usługi Windows Defender (Zainstalowano)
I/O Quality of Service
Klaster pracy w trybie failover
Klient drukowania internetowego
Klient systemu plików NFS
Klient Telnet
Klient TFTP
Kolejkowanie komunikatów
Kolekcja zdarzeń instalacji i rozruchu
Kompresja RDC
Kontenery
Kopia zapasowa systemu Windows Server
Magazyn rozszerzony
Media Foundation
Opis
Usługa BranchCache instaluje usługi wymagane do skonfigurowania tego komputera jako serwera hostowanej pamięci podręcznej lub serwera zawartości z włączoną usługą BranchCache. W przypadku wdrażania serwera zawartości należy go również skonfigurować jako serwer sieci Web HTTP (Hypertext Transer Protocol) lub serwer aplikacji oparty na usłudze inteligentnego transferu w tle (BITS, Background Intelligent Transfer Service). Aby wdrożyć serwer plików z włączoną usługą BranchCache, użyj Kreatora dodawania ról w celu zainstalowania roli serwera usług plików z usługą serwera plików i usługą BranchCache dla plików sieciowych.
< Wstecz
Dalej >
Zainstaluj
Anuluj


Kreator dodawania ról i funkcji
Serwer DNS
SERWER DOCELOWY
rol
Zanim rozpoczniesz
Typ instalacji
Wybieranie serwera
Role serwera
Funkcje
Serwer DNS
Potwierdzenie
Wyniki
System nazw domen (DNS) zapewnia standardową metodę kojarzenia nazw z numerycznymi adresami internetowymi. Dzięki temu użytkownicy mogą odwoływać się do komputerów w sieci przy użyciu łatwych do zapamiętania nazw, a nie długich serii liczb. Ponadto system DNS zapewnia hierarchiczną przestrzeń nazw gwarantującą, że każda nazwa hosta będzie unikatowa w sieci lokalnej lub rozległej. Usługi DNS systemu Windows można zintegrować z usługami protokołu DHCP w systemie Windows, eliminując potrzebę dodawania rekordów DNS po dodaniu komputerów do sieci.
Do zapamiętania:
• Integracja serwera DNS z usługami domenowymi Active Directory powoduje automatyczną replikację danych DNS wraz z innymi danymi usługi katalogowej, co ułatwia zarządzanie usługą DNS.
• Usługi domenowe Active Directory wymagają, aby w sieci był zainstalowany serwer DNS. Jeśli instalujesz kontroler domeny, możesz także zainstalować rolę Serwer DNS, zaznaczając w Kreatorze instalacji usług domenowych Active Directory rolę Usługi domenowe Active Directory.
< Wstecz
Dalej >
Zainstaluj
Anuluj


Kreator dodawania ról i funkcji
Potwierdzanie opcji instalacji
SERWER DOCELOWY
rol
Zanim rozpoczniesz
Typ instalacji
Wybieranie serwera
Role serwera
Funkcje
Serwer DNS
Potwierdzenie
Wyniki
Aby zainstalować następujące role, usługi ról lub funkcje na wybranym serwerze, kliknij przycisk Zainstaluj.
Automatycznie uruchom ponownie serwer docelowy, jeśli będzie to potrzebne
Funkcje opcjonalne (np. narzędzia administracyjne) mogą być wyświetlane na tej stronie, ponieważ zostały automatycznie wybrane. Jeśli nie chcesz instalować funkcji opcjonalnych, kliknij polecenie Poprzedni, aby wyczyścić ich pola wyboru.
Kreator dodawania ról i funkcji
Jeśli jest wymagane ponowne uruchomienie, ten serwer zostanie automatycznie ponownie uruchomiony bez dodatkowych powiadomień. Czy chcesz zezwolić na automatyczne ponowne uruchamianie?
Tak
Nie
Eksportuj ustawienia konfiguracji
Określanie alternatywnej ścieżki źródłowej
< Wstecz
Dalej >
Zainstaluj
Anuluj

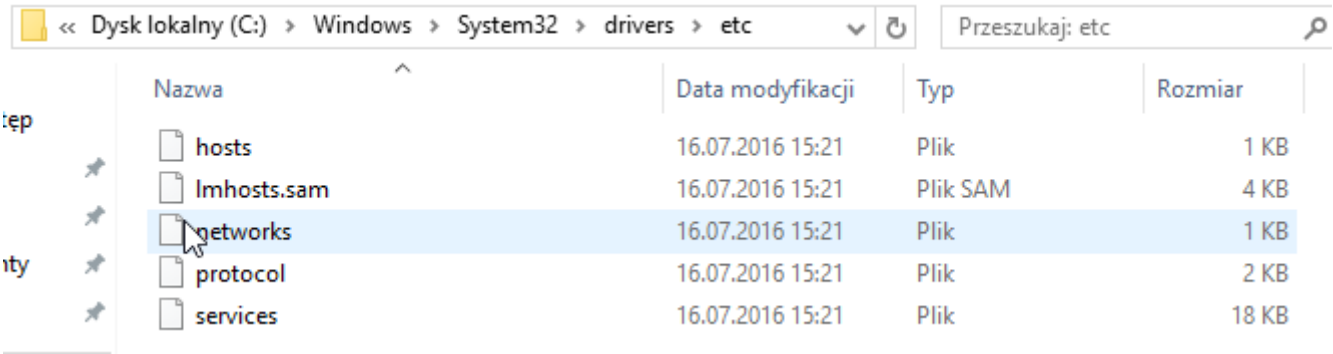

Kreator dodawania ról i funkcji
Postęp instalacji
SERWER DOCELOWY
rol
Zanim rozpoczniesz
Typ instalacji
Wybieranie serwera
Role serwera
Funkcje
Serwer DNS
Potwierdzenie
Wyniki
Wyświetlanie postępu instalacji
Rozpoczynanie instalacji
Narzędzia administracji zdalnej serwera
Narzędzia do administrowania rolami
Narzędzia serwera DNS
Serwer DNS
Eksportuj ustawienia konfiguracji
< Wstecz
Dalej >
Zainstaluj
Anuluj



2. Zrozumienie plików hosts i lmhosts

Pliki hosts i lmhosts są używane do rozpoznawania nazw i są przechowywane w katalogu C:\Windows\system32\drivers\etc, jak pokazano na rysunku 5.25. Pliki hosta zawierają mapowanie adresów IP na nazwy hostów i służą do rozpoznawania nazw DNS. W przeciwieństwie do hostów plik hosts menedżera LAN (lmhosts) zawiera mapowanie adresów IP na nazwy komputerów i jest używany do rozpoznawania nazw NetBIOS. W obu plikach wpisy są wstawiane ręcznie, a każdy wpis powinien znajdować się w osobnym wierszu. Tabela 1 przedstawia przykłady wstawiania wpisów hosts i lmhosts:

Wpis HOSTS:	Adres IP Nazwa hosta FQDN #Komentarz
Wpis LMHOSTS:	Adres IP Nazwa hosta FQDN Rozszerzenie <tag> #Comment



Rysunek 5.2.1 Pliki HOSTS i LMHOSTS w systemie Windows Server 2019

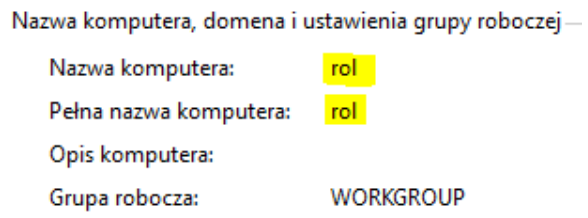
2.1 Użyj zgodnie z powyższą informacją (wyjaśnieniem) pliku

a) hosts - w zeszycie zapisz do czego użyjesz pliku i sposób testowania,

b) lmhosts - w zeszycie zapisz do czego użyjesz pliku i sposób testowania.

3. Zrozumienie nazwy hosta

Nazwa hosta to element logiczny przypisany do urządzenia (patrz rysunek 5.2.2). Jest unikalny i służy do identyfikacji urządzenia w sieci komputerowej. Często nazywa się to również nazwą domeny:



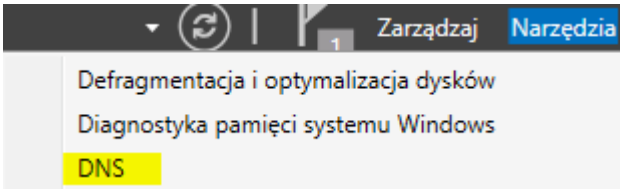
Rysunek 5.2.2. Przypisywanie nazwy hosta w systemie Windows Server 2019

4. Zrozumienie stref DNS

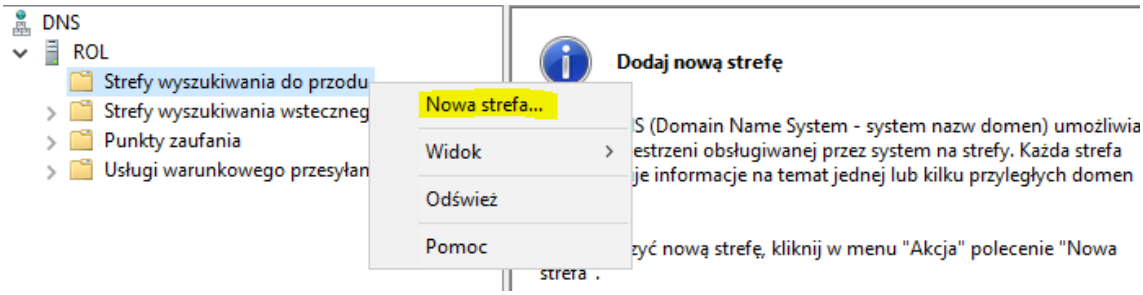
4.1 Wykonaj konfigurację strefę wyszukiwania do przodu

Aby skonfigurować strefę przekierowania w przód (forwarding zone) w systemie Windows Server 2019, postępuj zgodnie z poniższymi krokami:

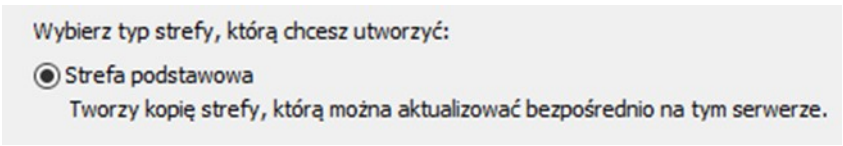
1. Otwórz "Konsolę zarządzania DNS" (DNS Manager) na serwerze Windows Server 2019.



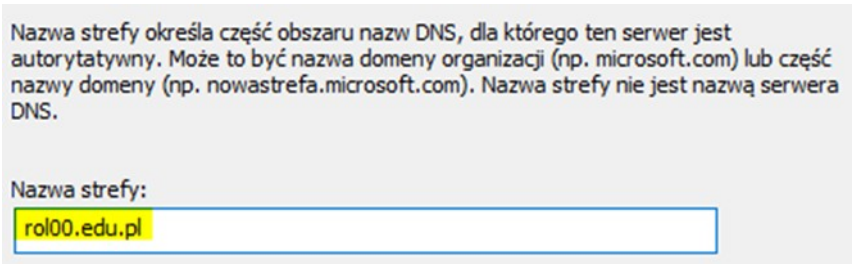
2. Rozwiń drzewko "Nazwa serwera" i kliknij prawym przyciskiem myszy na "Strefy wyszukiwania do przodu" (Forward Lookup Zones). Wybierz opcję "Nowa strefa ..." (New Forward Lookup Zone).



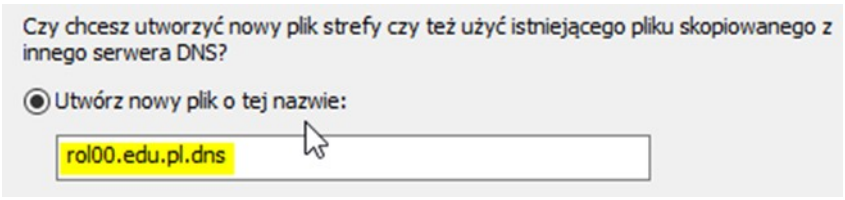
3. W oknie kreatora, kliknij "Dalej" (Next) i wybierz opcję "Strefa podstawowa" (Forward). Kliknij ponownie "Dalej" (Next).



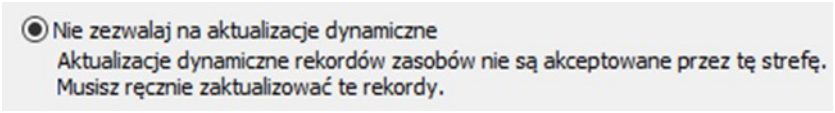
4. Wprowadź nazwę domeny, dla której chcesz skonfigurować strefę przekierowania. Na przykład, jeśli chcesz skonfigurować przekierowanie dla domeny "rol00.edu.pl", wprowadź "rol00.edu.pl". Kliknij "Dalej" (Next).



5. Wybierz opcję "Utwórz nowy plik o tej nazwie" i kliknij "Dalej" (Next).

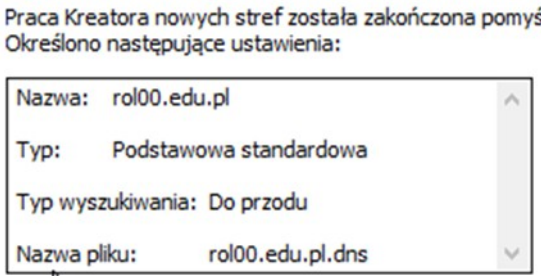


6. Określ, że ta strefa DNS akceptuje dynamiczne aktualizacje zabezpieczone lub niezabezpieczone albo nie akceptuje dynamicznych aktualizacji. Ustaw jak poniżej Kliknij "Dalej" (Next).



Patrz teoria DNS (dynamiczne aktualizacje)

7. Na ekranie podsumowania, sprawdź swoje ustawienia i kliknij "Zakończ" (Finish), aby utworzyć strefę przekierowania.



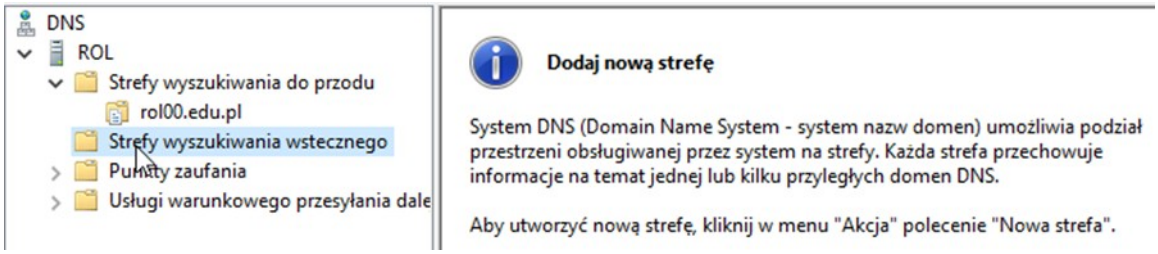
Po utworzeniu strefy przekierowania, serwer DNS będzie przekierowywał zapytania dla podanej domeny do określonych serwerów DNS.

4.2 Wykonaj konfigurację strefy wyszukiwania wstecz.

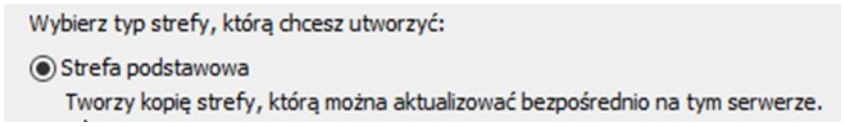
Aby skonfigurować strefę wyszukiwania wstecz (reverse lookup zone) w systemie Windows Server 2019, wykonaj następujące kroki:

1. Otwórz "Konsolę zarządzania DNS" (DNS Manager) na serwerze Windows Server 2019.

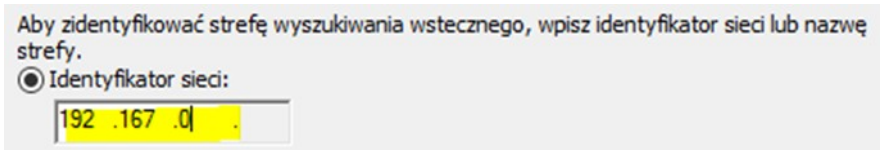
2. Rozwiń drzewko "Nazwa serwera" i kliknij prawym przyciskiem myszy na "Strefy wyszukiwania wstecz" (Reverse Lookup Zones). Wybierz opcję "Nowa strefa ..." (New Reverse Lookup Zone).



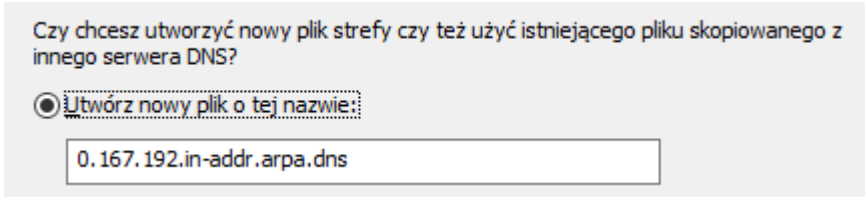
3. W oknie kreatora, wybierz opcję "Strefa podstawowa" kliknij "Dalej" (Next) i wybierz opcję "Strefa wyszukiwania wstecznego" "Dalej" (Next).



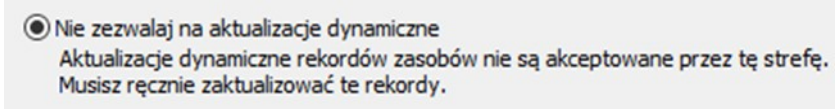
4. W oknie kreatora, wybierz Identyfikator sieci dla którego chcesz skonfigurować strefę wyszukiwania wstecz. Wybierz "192.167.0". Kliknij "Dalej" (Next).



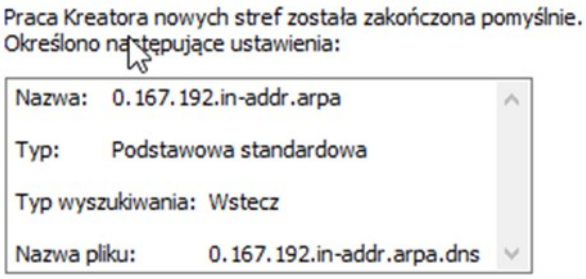
5. Wybierz opcję "Utwórz nowy plik o tej nazwie" i kliknij "Dalej" (Next).



6. Określ, że ta strefa DNS akceptuje dynamiczne aktualizacje zabezpieczone lub niezabezpieczone albo nie akceptuje dynamicznych aktualizacji. Ustaw jak poniżej Kliknij "Dalej" (Next).



7. Na ekranie podsumowania, sprawdź swoje ustawienia i kliknij "Zakończ" (Finish), aby utworzyć strefę wyszukiwania wstecz.



Po utworzeniu strefy wyszukiwania wstecz, będziesz mógł przeprowadzać odwrotne wyszukiwanie DNS, czyli odnaleźć nazwę komputera na podstawie znanego adresu IP.

Ważne jest, aby pamiętać, że strefa wyszukiwania wstecz wymaga prawidłowej konfiguracji strefy strefy przekierowania (forward lookup zone) oraz rekordów PTR (Pointer) dla odpowiednich adresów IP. Upewnij się, że rekordy PTR są poprawnie utworzone dla maszyn w sieci i że strefy wyszukiwania wstecz i przekierowania są skonfigurowane zgodnie z wymaganiami sieci.

4.3 Porównaj obecną ilość rekordów w ćwiczeniu 5.2 z ilością rekordów z kontrolerem domeny AD którą uzyskałeś wykonując dokumentację w ćwiczeniu 5.1. Za co odpowiadają poszczególne wpisy, których nie ma teraz? Poszczególne wpisy, które można porównać, to na przykład:

a. Rekordy NS (Name Server): W ćwiczeniu 5.1, rekordy NS wskazywały na kontroler domeny AD jako serwer DNS. W ćwiczeniu 5.2, te rekordy będą wskazywać na nowo skonfigurowany serwer DNS.
b. Rekordy A (Host Address): W ćwiczeniu 5.1, rekordy A mogły wskazywać na adres IP kontrolera domeny. W ćwiczeniu 5.2, rekordy A będą wskazywać na adres IP serwera DNS.
c. Rekordy PTR (Pointer): W ćwiczeniu 5.1, rekordy PTR byłyby tworzone dla odwrotnego przypisywania nazw do adresów IP kontrolera domeny. W ćwiczeniu 5.2, jeśli konfigurujesz również strefę przekierowania wstecz, to rekordy PTR byłyby tworzone dla nowego serwera DNS.
d. Inne rekordy związane z usługami AD: W ćwiczeniu 5.1 mogłyby istnieć różne rekordy SRV (Service) wskazujące na usługi AD, takie jak LDAP, Kerberos itp. W ćwiczeniu 5.2 te rekordy byłyby obecne tylko wtedy, jeśli nadal masz skonfigurowane usługi AD na swoim serwerze.

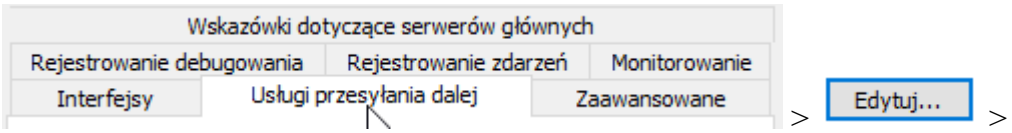
W związku z tym, porównanie ilości i rodzaju rekordów między tymi dwoma ćwiczeniami pozwoli na zrozumienie różnic w konfiguracji DNS w kontekście serwera AD i niezależnego serwera DNS.

4.4 Wykonaj konfigurację usług przesyłania dalej nieobsłużonych zapytań.

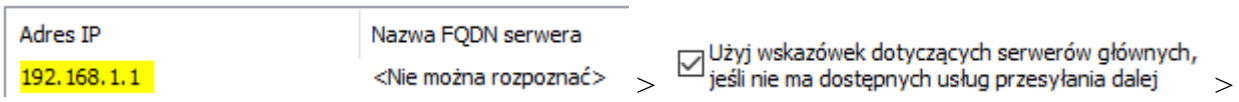
Aby skonfigurować usługę przesyłania dalej nieobsłużonych zapytań (DNS forwarding) w systemie Windows Server 2019, wykonaj następujące kroki:

1. Otwórz "Konsolę zarządzania DNS" (DNS Manager) na serwerze Windows Server 2019.
2. Rozwiń drzewko "Nazwa serwera" i kliknij prawym przyciskiem myszy na serwerze DNS. Wybierz opcję "Właściwości" (Properties).

3. W oknie "Właściwości serwera DNS", przejdź do zakładki "Usługi przesyłania dalej" (Forwarders).



4. Zaznacz opcję "Edytuj" (Enable forwarders).
5. W polu "Adres IP" (IP Address) wprowadź adresy IP serwerów DNS, do których chcesz przekierować zapytania DNS. Możesz wprowadzić jeden lub więcej adresów IP, oddzielając je przecinkami. Upewnij się, że podane serwery DNS są poprawnie skonfigurowane i dostępne w sieci.



6. Opcjonalnie, jeśli chcesz, aby serwer DNS przesyłał zapytania dalej, jeśli nie jest w stanie odnaleźć rekordów lokalnie, zaznacz opcję "Przesyłaj zapytania, jeśli nie odnaleziono rekordów lokalnie" (Forward queries for unresolved names).
7. Kliknij „Zastosuj” i "OK", aby zapisać wprowadzone zmiany.

Po skonfigurowaniu przekierowania, serwer DNS będzie przesyłał zapytania, których rekordy nie zostały odnalezione lokalnie, do określonych serwerów DNS.

8. Upewnij się, że podane adresy IP serwerów DNS są poprawne i dostępne w sieci.
9. Po skonfigurowaniu usługi przesyłania dalej nieobsłużonych zapytań, przetestuj, czy zapytania są prawidłowo przekierowywane do określonych serwerów DNS.

Aby przetestować, czy zapytania są prawidłowo przekierowywane do określonych serwerów DNS po skonfigurowaniu usługi przesyłania dalej nieobsłużonych zapytań (DNS forwarding), możesz wykonać następujące kroki:

a) **Otwórz "Konsolę zarządzania DNS" (DNS Manager) na serwerze Windows Server 2019:** Otwórz menu Start, wpisz "Konsola zarządzania DNS" lub "DNS Manager", i wybierz odpowiednią opcję.

b) **Znajdź swoją strefę przekierowania:** W lewym panelu, rozwiń drzewko "Nazwa serwera", a następnie "Strefy wyszukiwania do przodu" (Forward Lookup Zones). Tam powinna być strefa przekierowania, którą skonfigurowałeś wcześniej.

c) **Wyślij zapytanie DNS:** Możesz użyć polecenia wiersza poleceń lub narzędzia "cmd" (wiersza poleceń) do wysłania zapytania DNS i sprawdzenia, czy jest ono przekierowywane poprawnie. Wpisz następujące polecenie:

nslookup nazwa_domeny serwer_dns

Gdzie "nazwa_domeny" to domena, dla której chcesz przetestować przekierowanie, a "serwer_dns" to adres IP jednego z serwerów DNS, które skonfigurowałeś jako przekierowanie.

Na przykład:

nslookup example.com 8.8.8.8

To polecenie wyśle zapytanie DNS dla domeny "example.com" na serwer DNS o adresie IP "8.8.8.8" (który jest serwerem DNS Google).

d) **Sprawdź wynik:** Otrzymasz odpowiedź od serwera DNS. Jeśli otrzymasz odpowiedź zawierającą informacje o rozwiązaniu nazwy domeny, to znaczy, że przekierowanie działa poprawnie i zapytanie zostało przekierowane do określonego serwera DNS.

e) **Sprawdź dzienniki DNS:** Jeśli masz włączoną opcję rejestracji zdarzeń w serwerze DNS, możesz również sprawdzić dzienniki, aby upewnić się, że zapytania były przekierowywane. W Konsoli zarządzania DNS, kliknij prawym przyciskiem myszy na swoim serwerze DNS, wybierz "Właściwości", a następnie przejdź do zakładki "Dzienniki". Tam znajdziesz informacje o zapytaniach i przekierowaniach.

Pamiętaj, że zapytania DNS mogą być buforowane, dlatego wynik może być inne w przypadku kolejnych prób. Dlatego warto kilka razy przetestować, aby upewnić się, że przekierowanie działa zgodnie z oczekiwaniami.

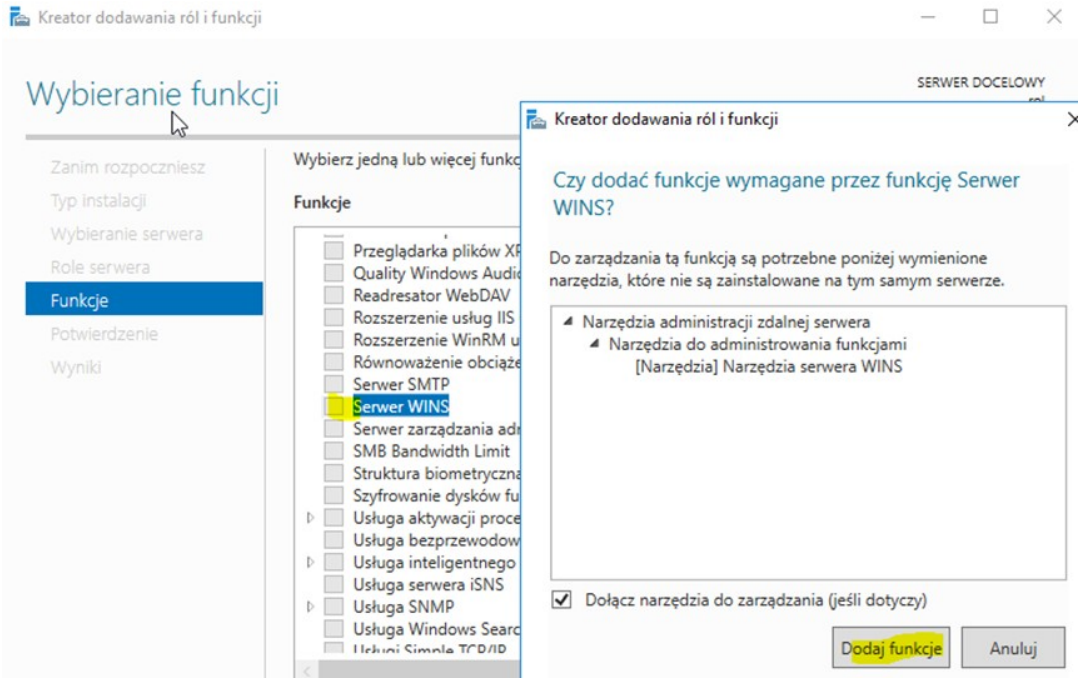
Pozostałe czynności testowe w serwerze DNS należy wykonywać w ćw5.1 w ćwiczeniu ćw5.2 nie wykonuj ich.

5. Zrozumienie WINS i wyjaśnij w zeszycie jego znaczenie.

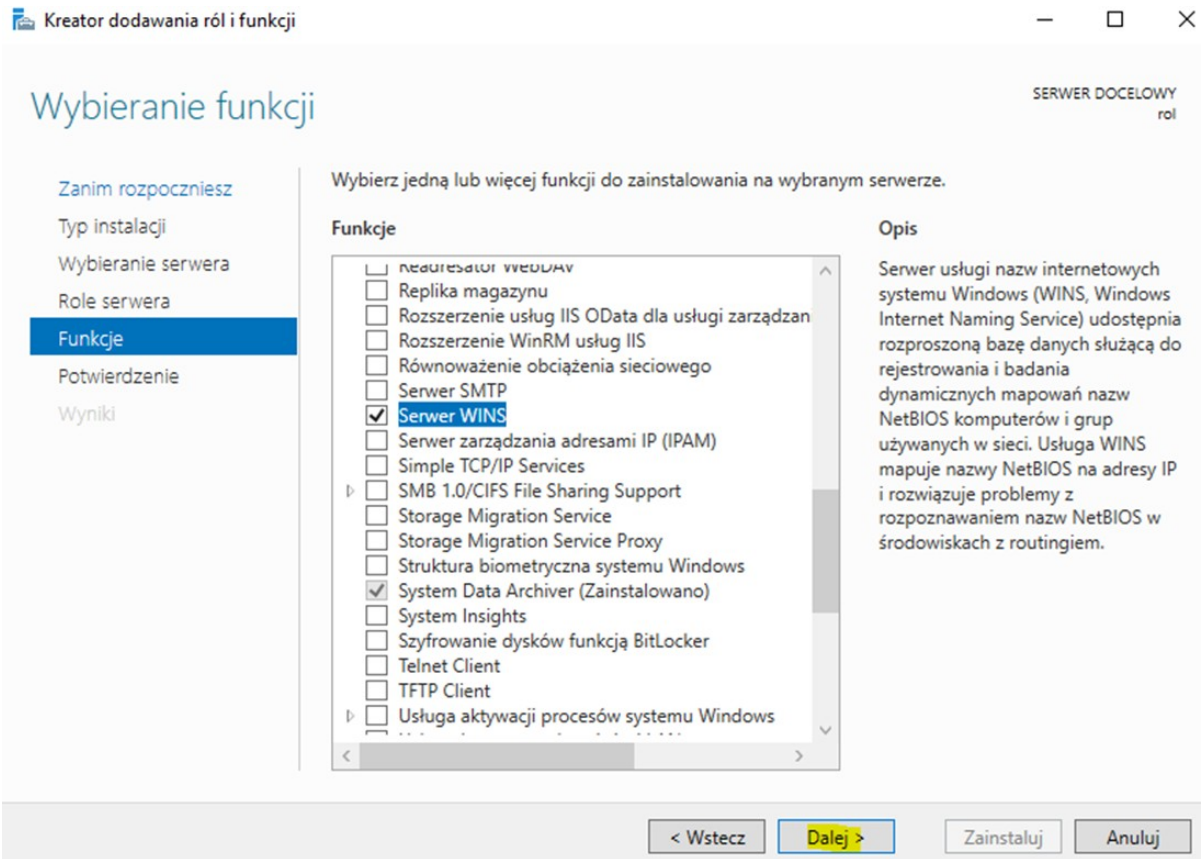
5.1 Wykonaj konfigurowanie funkcji WINS w systemie Windows Server 2019

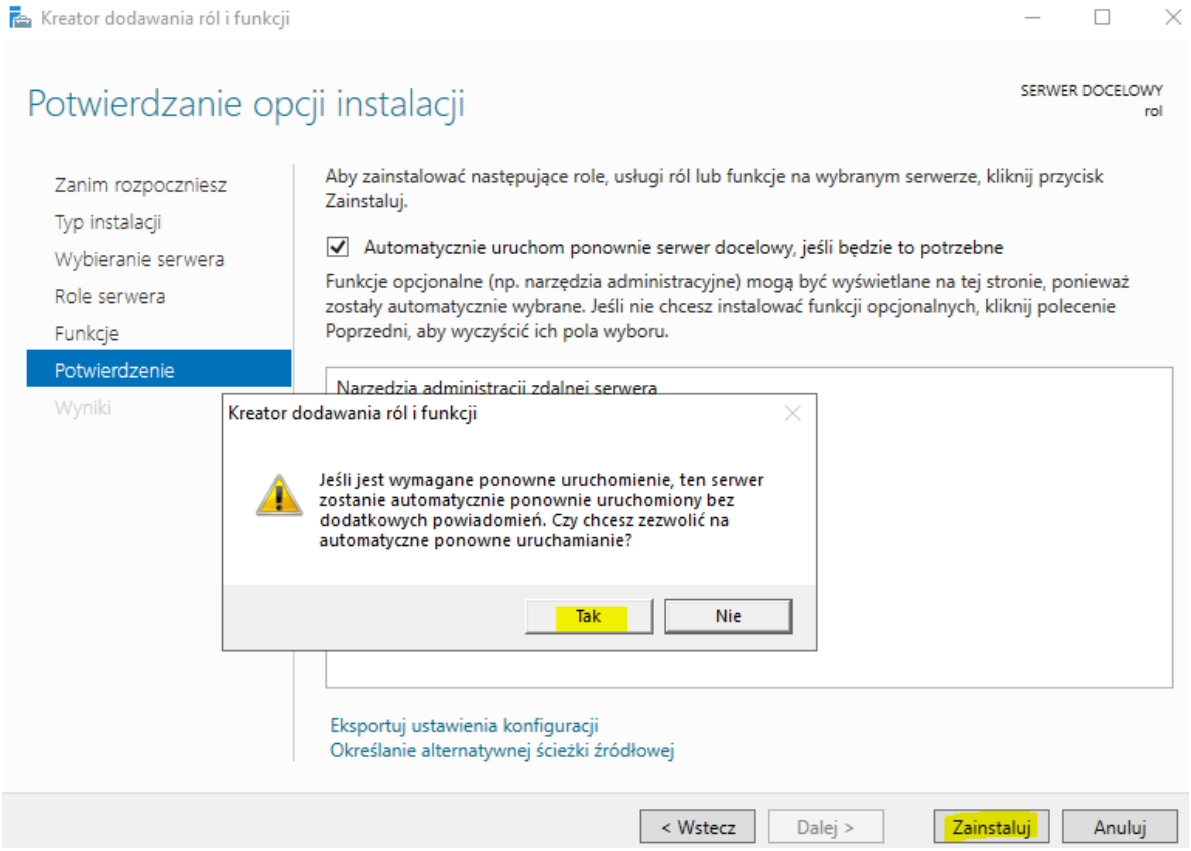
Aby skonfigurować funkcję WINS (Windows Internet Name Service) w systemie Windows Server 2019, wykonaj następujące kroki:

1. Otwórz "Zarządzanie serwerem" (Server Manager) na serwerze Windows Server 2019.
2. Kliknij na "Dodaj role i funkcje" (Add Roles and Features) w obszarze "Dashboard".
3. Przejdź przez kroki kreatora, akceptując domyślne opcje, aż do ekranu "Wybór funkcji" (Select features).

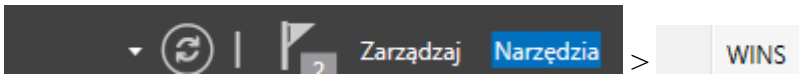


4. Rozwiń "Serwer DNS" (DNS Server) i zaznacz opcję "Usługa WINS" (WINS Server).
5. Kliknij "Dalej" (Next) i dokończ instalację, postępując zgodnie z instrukcjami kreatora.





6. Po zakończeniu instalacji, otwórz "Konsolę zarządzania WINS" (WINS Management Console) poprzez menu "Start" -> "Menedżer serwera" -> "WINS".



7. W "Konsoli zarządzania WINS", kliknij prawym przyciskiem myszy na serwer WINS i wybierz opcję.
8. W oknie konfiguracji WINS, możesz dostosować ustawienia WINS według potrzeb, takie jak zakresy IP, zezwolenia replikacji, partnerskie serwery WINS itp. Wykonaj odpowiednie zmiany zgodnie z Twoimi wymaganiami.
9. Kliknij "OK", aby zapisać wprowadzone zmiany.

Po skonfigurowaniu funkcji WINS, serwer Windows Server 2019 będzie działał jako serwer WINS, umożliwiając rozwiązywanie nazw NetBIOS na adresy IP i umożliwiając replikację danych WINS między serwerami WINS.

Upewnij się, że korzystasz z funkcji WINS zgodnie z wymaganiami Twojej sieci i systemu. WINS jest starszym rozwiązaniem i często jest stosowane w starszych środowiskach sieciowych. W przypadku nowszych systemów i aplikacji, zaleca się stosowanie usługi DNS.

Przedstaw efekty wykonanych czynności w serwerze WINS.

Wyjaśnij w zeszycie znaczenie funkcji WINS.

6. Zrozumienie UNC (Universal Naming Convention)

UNC składa się z dwóch głównych elementów:

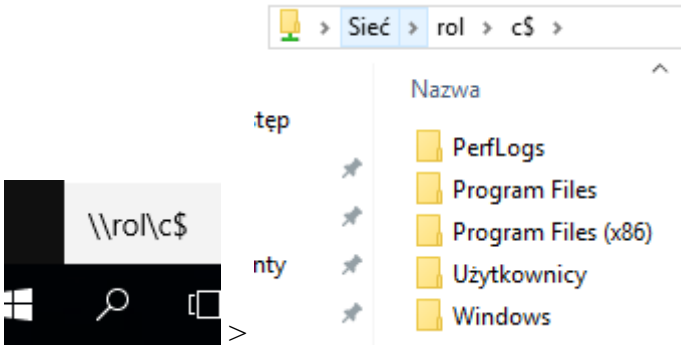
1. Nazwa serwera: Jest to nazwa lub adres IP komputera, na którym znajduje się udostępniony zasób.
   Na przykład: \\nazwa_serwera lub \\192.168.0.100.
2. Ścieżka do zasobu: To ścieżka, która wskazuje konkretny zasób na serwerze.
   Może to być nazwa udostępnionego folderu, pliku lub drukarki.
   Na przykład: \\nazwa_serwera\udostepny_folder lub \\192.168.0.100\udostepny_folder.

UNC jest standardem służącym do identyfikacji udziału w sieci komputerowej. Jego format (patrz rysunek 5.2.3) wykorzystuje podwójne ukośniki odwrotne, aby poprzedzić nazwę serwera, na przykład \ \nazwa_serwera\folder.

Przykłady pełnych UNC:

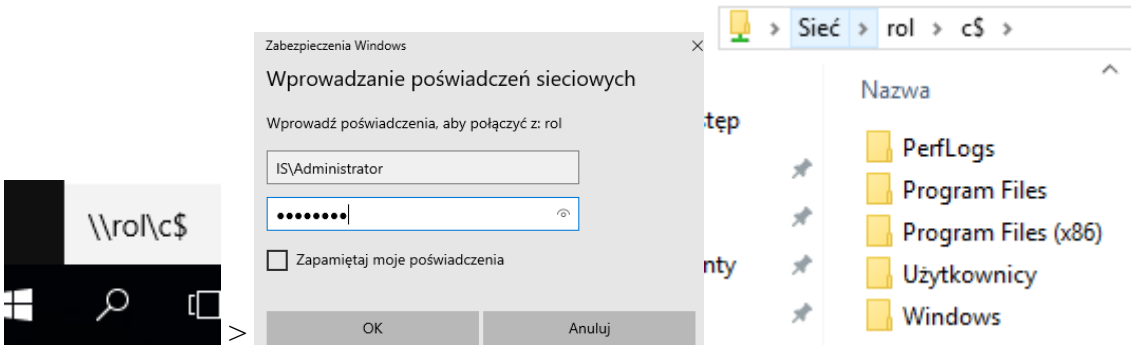
1. Dostęp do udostępnionego folderu: \\serwer\udostepny_folder
2. Dostęp do udostępnionego ukrytego folderu: \\serwer\udostepny_folder$
3. Dostęp do pliku w udostępnionym folderze: \\serwer\udostepny_folder\nazwa_pliku.txt
4. Dostęp do drukarki sieciowej: \\serwer\nazwa_drukarki

6.1 Użyj ścieżki UNC w systemie Windows Server 2019 i wyjaśnij w zeszycie jej znaczenie. Co oznacza \ \rol\c$



Rysunek 5.2.3. Ścieżka UNC do zasobu w systemie Windows Server 2019

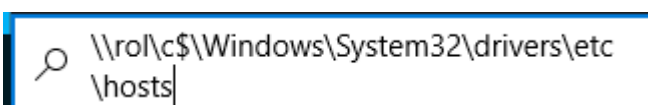
6.2 Użyj ścieżki UNC w systemie Windows 11 i wyjaśnij w zeszycie jej znaczenie.



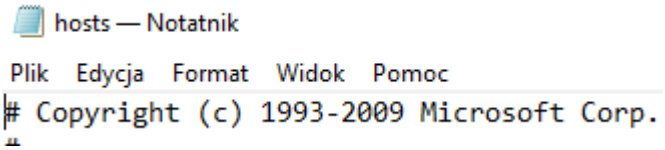
Rysunek 5.2.4. Ścieżka UNC do zasobu w systemie Windows 11

6.3 Użyj ścieżki UNC w systemie Windows 11 i wyjaśnij w zeszycie jej znaczenie.

\\rol\c$\Windows\System32\drivers\etc\hosts



> > OK. >



Rysunek 5.30. Ścieżka UNC do pliku w systemie Windows 11

7. Podaj wnioski dotyczące zagadnień, które wystąpiły podczas powyższego ćwiczenia zwróć uwagę na to, jakie konkretne umiejętności i wiedzę jaką zdobyłeś, którą będziesz mógł zastosować w praktyce, zarówno podczas konfiguracji serwera DNS, jak i zrozumienia jego znaczenia w kontekście usługi Active Directory.

Podsumowanie:

Po wykonaniu wszystkich czynności z powyższej instrukcji przeczytaj ponownie z zrozumieniem cel ogólny i cele szczegółowe, które znajdują się na pierwszej stronie instrukcji. Jeżeli one zostały niezrealizowane to powtarzaj wykonie tej instrukcji w szkole lub/i w domu do momentu zrealizowania.