Wprowadzenie

Egzamin 70-741 skupia się na funkcjach sieciowych oraz funkcjonalnościach dostępnych w systemie Windows Server 2016. Obejmuje implementację DNS, DHCP oraz IPAM, a także rozwiązania zdalne jak VPN i Direct Access. Dotyczy także rozwiązań DFS oraz pamięci podręcznej systemu Windows dla oddziałów firmy, funkcji sieci wysokiej wydajności oraz implementacji rozwiązań Software Defined Networking (SDN), takich jak Hyper-V Network Virtualization (HNV) oraz Network Controller.

Egzamin 70-741 jest adresowany do administratorów sieci, którzy chcą podwyższyć swoje umiejętności i nauczyć się nowych funkcji technik sieciowych wprowadzonych w systemie Windows Server 2016.

Książka obejmuje wszystkie tematy wchodzące w zakres egzaminu, lecz nie zawiera opisu każdego pytania egzaminacyjnego. Dostęp do zestawu pytań egzaminacyjnych, który jest regularnie rozszerzany o nowe pytania, ma tylko zespół egzaminacyjny firmy Microsoft. Książkę tę należy więc traktować jako uzupełnienie wiedzy zdobytej poprzez praktykę oraz innych materiałów szkoleniowych. Jeśli jakiś temat nie jest jasny i wymaga dodatkowych objaśnień, można skorzystać z odnośników podanych w tekście książki jako „Dodatkowe materiały" i tam znaleźć dodatkowe informacje na dany temat. Wiele cennych informacji można znaleźć również w MSDN, TechNet oraz na blogach i forach.

Układ książki

Książka jest ułożona według tematów z listy „Skills measured" (Sprawdzane umiejętności), opublikowanej na potrzeby egzaminu. Taka lista jest dostępna dla każdego egzaminu na witrynie Microsoft Learning: *https://aka.ms/examlist*. Każdy rozdział tej książki odpowiada podstawowemu tematowi z tej listy, a układ każdego rozdziału zależy od zadań technicznych w każdym obszarze tematycznym. Jeśli, przykładowo, egzamin obejmuje sześć podstawowych obszarów tematycznych, książka będzie zawierać sześć rozdziałów.

Certyfikaty firmy Microsoft

Certyfikaty firmy Microsoft wyróżniają ich posiadaczy, jako osoby mające szerokie umiejętności i doświadczenie w zakresie bieżących produktów i technologii firmy. Egzaminy wraz z odpowiadającymi im certyfikatami zostały przygotowane tak, aby ocenić biegłość w takich dziedzinach jak projektowanie i rozwój lub wdrażanie i obsługa rozwiązań produktów i technologii firmy Microsoft, zarówno lokalnie, jak i w chmurze. Uzyskanie certyfikatu daje wiele korzyści jego posiadaczom, a także pracodawcom i firmom.

Więcej informacji Wszystkie certyfikaty firmy Microsoft

Informacje dotyczące certyfikatów firmy Microsoft wraz z pełną ich listą można znaleźć pod adresem *https://www.microsoft.com/learning*.

Podziękowania

Pisanie tej książki było wysiłkiem zbiorowym, dlatego chcę tutaj podziękować mojej redaktorce, Trinie MacDonald, za jej wskazówki. Dziękuję również mojej żonie Naomi oraz córce Amelii za ich cierpliwość, gdy przez całe lato siedziałem w biurze, słuchając tych wskazówek.

– Andrew Warren

Bezpłatne e-booki z Microsoft Press

Bezpłatne e-booki przygotowane przez Microsoft Press obejmują szeroki zakres tematów. Są one dostępne w formatach PDF, EPUB oraz Mobi na Kindle. Można je pobrać ze strony:

https://aka.ms/mspressfree

Warto sprawdzać, co nowego się tam pojawiło!

Wirtualna akademia firmy Microsoft

Swoją wiedzę dotyczącą technologii firmy Microsoft można budować, korzystając z bezpłatnego szkolenia online prowadzonego przez ekspertów z akademii MVA (Microsoft Virtual Academy). MVA oferuje obszerny zestaw bibliotek wideo, wydarzeń na żywo oraz wszelką pomoc niezbędną do poznania najnowszych technologii oraz przygotowania do egzaminów. Materiały można znaleźć pod adresem:

https://www.microsoftvirtualacademy.com

Szybki dostęp do materiałów online

W całej książce pojawiają się adresy polecanych przez autora witryn internetowych, gdzie można uzyskać dodatkowe informacje. Niektóre z tych adresów (określanych jako URL) mogą być trudne do wpisania do przeglądarki. Dlatego zestawiliśmy listę adresów, do których mogą się odwołać czytelnicy papierowej wersji książki.

Listę można pobrać ze strony pod adresem *https://aka.ms/examref741/downloads*.

Adresy URL są uporządkowane według rozdziałów i nagłówków. Gdy w książce napotkacie URL, należy znaleźć odpowiedni odnośnik na liście i kliknąć go, aby przejść bezpośrednio na witrynę.

Errata, aktualizacje i wsparcie dla książki

Autorzy starali się zapewnić możliwie najlepszą dokładność informacji zawartych w książce i towarzyszącym jej materiałom. Aktualizacje do książki, dostępne są w postaci erraty, pod adresem:

https://aka.ms/examref741/errata

Każdy kto znajdzie błąd, którego nie ma na liście, proszony jest o przekazanie informacji na tej samej witrynie.

Dodatkową pomoc można uzyskać, pisząc e-mail do działu obsługi książek Microsoft Press, na adres:

mspinput@microsoft.com

Pod tymi adresami nie oferujemy wsparcia związanego ze sprzętem i oprogramowaniem oferowanym przez Microsoft. Pomoc w tym zakresie można uzyskać na witrynie *https://support.microsoft.com*.

Prosimy o kontakt

Zadowolenie czytelników stanowi priorytet dla Microsoft Press, dlatego oczekujemy na wszelkie informacje od Was. Opinie o książce proszę nadsyłać z witryny:

https://aka.ms/tellpress

Aby skrócić czas wypełniania ankiety, ograniczyliśmy się do kilku krótkich pytań. Odpowiedzi na nie zostaną przekazane bezpośrednio do redaktorów Microsoft Press. (Nie oczekujemy żadnych danych osobowych). Z góry dziękujemy za odpowiedź!

Pozostańmy w kontakcie

Bądźmy w stałym kontakcie! Mamy konto na Twitterze pod adresem: *https://twitter.com/MicrosoftPress*.

Ważne:
Jak używać tej książki podczas przygotowania do egzaminu

Egzaminy certyfikacyjne weryfikują Twoją wiedzę praktyczną i znajomość produktu. Ten podręcznik pomoże ci się przekonać, czy jesteś gotów do przystąpienia do egzaminu, sprawdzając Twoją znajomość zagadnień wchodzących w jego skład. Dzięki niemu możesz określić, które tematy znasz doskonale, a które obszary wymagają dodatkowej pracy. Aby ułatwić odświeżenie umiejętności z określonych dziedzin, dołączyliśmy też wskazówki „Szybki przegląd", kierujące do dodatkowych, zewnętrznych źródeł informacji.

Podręcznik ten nie może zastąpić doświadczenia praktycznego. Książka ta nie ma na celu uczenia nowych umiejętności, ale utrwalenie i uporządkowanie już posiadanej wiedzy.

Zalecamy, aby w trakcie przygotowań do egzaminu korzystać z wielu dostępnych materiałów szkoleniowych. Więcej informacji na temat dostępnych szkoleń można znaleźć pod adresem https://www.microsoft.com/learning. Dla wielu egzaminów dostępne są Microsoft Official Practice Tests – ich spis można znaleźć pod adresem https://aka.ms/practicetests. Dostępne są również darmowe szkolenia online i wykłady na żywo w Microsoft Virtual Academy, pod adresem https://www.microsoftvirtualacademy.com.

Książka ta została uporządkowana według listy mierzonych umiejętności (Skills measured) dla tego egzaminu. Lista taka dla każdego egzaminu jest dostępna w witrynie Microsoft Learning: https://aka.ms/examlist.

Warto odnotować, że niniejsza książka opiera się na publicznie dostępnych informacjach na temat egzaminów oraz doświadczeniach autorów. W celu zachowania pełnej poufności autorzy nie mieli dostępu do treści rzeczywistych egzaminów.

ROZDZIAŁ 1

Wdrażanie systemu nazw domen (DNS)

Do komunikacji z innymi hostami oraz usługami w sieciach, użytkownicy i komputery korzystają zazwyczaj z nazw hostów zamiast adresów sieciowych IPv4 (Internet Protocol version 4) lub IPv6 (Internet Protocol version 6). Usługa Windows Server 2016, znana jako rola DNS (Domain Name System) serwera, odwzorowuje te nazwy na adresy IPv4 lub IPv6.

Ponieważ na roli serwera DNS opiera się działanie wielu ważnych aplikacji i usług, trzeba wiedzieć, jak zainstalować i konfigurować rozpoznawanie nazw w Windows Server 2016 za pomocą tego mechanizmu. W związku z tym egzamin 70-741 Networking Windows Server 2016 obejmuje zagadnienie instalowania i konfigurowania roli serwera DNS w systemie Windows Server 2016.

Do zagadnień egzaminu 70-741 należy także wdrażanie stref i rekordów Domain Name System z użyciem roli serwera DNS. Należy zatem wiedzieć, jak tworzyć strefy DNS i zarządzać nimi, korzystając z roli serwera DNS w systemie Windows Server 2016, oraz jak w tych strefach tworzyć rekordy związane z hostem i z usługami i jak nimi zarządzać.

Zagadnienia egzaminacyjne omawiane w tym rozdziale:

Zagadnienie 1.1: Instalowanie i konfigurowanie serwerów DNS

Windows Server 2016 zapewnia rolę serwera DNS, aby dostarczyć usługi rozpoznawania nazw urządzeniom i komputerom w infrastrukturze sieci organizacji. Pierwszym etapem przy zapewnianiu rozpoznawania nazw jest wdrożenie roli serwera DNS na komputerach serwera Windows Server 2016.

Rozpoznawanie nazw

Mimo że adresowanie IP nie jest szczególnie złożone, użytkownikom łatwiej jest posługiwać się nazwami hostów np. witryn WWW, z którymi chcą się łączyć, zamiast ich adresami IPv4 lub IPv6. Gdy aplikacja, taka jak Microsoft Edge, odwołuje się do nazwy witryny, nazwa w adresie URL jest przekształcana na kryjący się pod nią adres IPv4 lub IPv6, za pomocą procesu znanego jako rozpoznawanie nazw. Komputery z systemem Windows 10 i Windows Server 2016 mogą korzystać z dwóch rodzajów nazw. Są to:

- **Nazwy hostów** Nazwa hosta, o długości do 255 znaków, zawiera tylko znaki alfanumeryczne, odstępy oraz łączniki. Nazwa hosta jest połączeniem aliasu z nazwą domeny DNS. Na przykład alias *komputer1* poprzedza nazwę domeny, Contoso.com, aby utworzyć nazwę hosta czyli pełną nazwę domenową (Fully Qualified Domain Name, FQDN), *komputer1*.contoso.com.
- **Nazwy NetBIOS** Nazwy NetBIOS, obecnie mające mniejsze znaczenia, korzystają ze struktury niehierarchicznej opartej na 16-znakowej nazwie. Szesnasty znak określa konkretną usługę uruchomioną na komputerze, którego nazwą jest 15 poprzednich znaków. A zatem, LON-SVR1[20h] to usługa serwera NetBIOS na komputerze o nazwie LON-SVR1.

Metoda, w której komputer z systemem Windows 10 lub Windows Server 2016 rozpoznaje różne nazwy opiera się na jego konfiguracji, ale zazwyczaj działa jak pokazano na rysunku 1-1.

Podane poniżej kroki to typowe etapy rozpoznawania nazw dla komputera z systemem Windows 10 lub Windows Server 2016.

1. Ustal, czy nazwa hosta, będąca przedmiotem zapytania, jest taka sama jak nazwa hosta lokalnego.
2. Znajdź w pamięci podręcznej programu rozpoznawania nazw DNS podaną z zapytaniu nazwę hosta. Pamięć ta jest aktualizowana po udanym rozpoznaniu nazwy. Ponadto do tej pamięci podręcznej jest dodawana zawartość lokalnego pliku Hosts.
3. Wyślij zapytanie do serwera DNS o żądaną nazwę hosta.

Rysunek 1-1 Typowe etapy rozpoznawania nazw na komputerze z systemem Windows Server

Dodatkowe materiały **Rozpoznawanie nazw IPv4**

Szczegółowe informacje dotyczące rozpoznawania nazw IPv4 można znaleźć w witrynie Microsoft TechNet *https://technet.microsoft.com/library/dd379505(v=ws.10).aspx*.

Usługa rozpoznawania nazw w systemie Windows Server 2016 to oczywiście więcej niż tylko zwykłe odwzorowanie podanej nazwy na adres IP. Rola serwera DNS jest również wykorzystywana w celu lokalizacji usług w infrastrukturze sieciowej. Na przykład podczas rozruchu komputera użytkownik musi zalogować się do domeny Active Directory Domain Services (AD DS) i być może otworzyć Microsoft Office Outlook. To oznacza, że komputer klienta musi zlokalizować serwer, który dostarcza usługi uwierzytelniania w lokalnej lokalizacji AD DS, a ponadto znaleźć odpowiedni serwer skrzynek pocztowych Microsoft Exchange użytkownika. Te procesy wymagają DNS.

Określanie wymagań dla instalacji DNS

Przed rozpoczęciem instalacji roli serwera DNS trzeba sprawdzić, czy nasz serwer spełnia wymagania instalacyjne dla tej roli.

Wymagania instalacji roli serwera DNS są następujące:

- **Bezpieczeństwo** Należy zalogować się na serwerze jako członek lokalnej grupy Administrators (Administratorzy).
- **Konfiguracja IP** Server musi mieć statycznie przypisaną konfigurację IPv4 i/lub IPv6. To zapewnia komputerom klienta możliwość zlokalizowania roli serwera DNS przy użyciu jego adresu IP.

Poza tymi wymaganiami dotyczącymi serwera, trzeba być również przygotowanym na na pytania związane z infrastrukturą sieciową swojej organizacji. Te pytania dotyczą

naszej obecności w Internecie oraz zarejestrowanych nazw domen, które mają być wykorzystywane jako publiczne. Mimo że nazw tych domen nie trzeba definiować podczas instalacji roli DNS, należy podać te informacje w czasie jej konfiguracji.

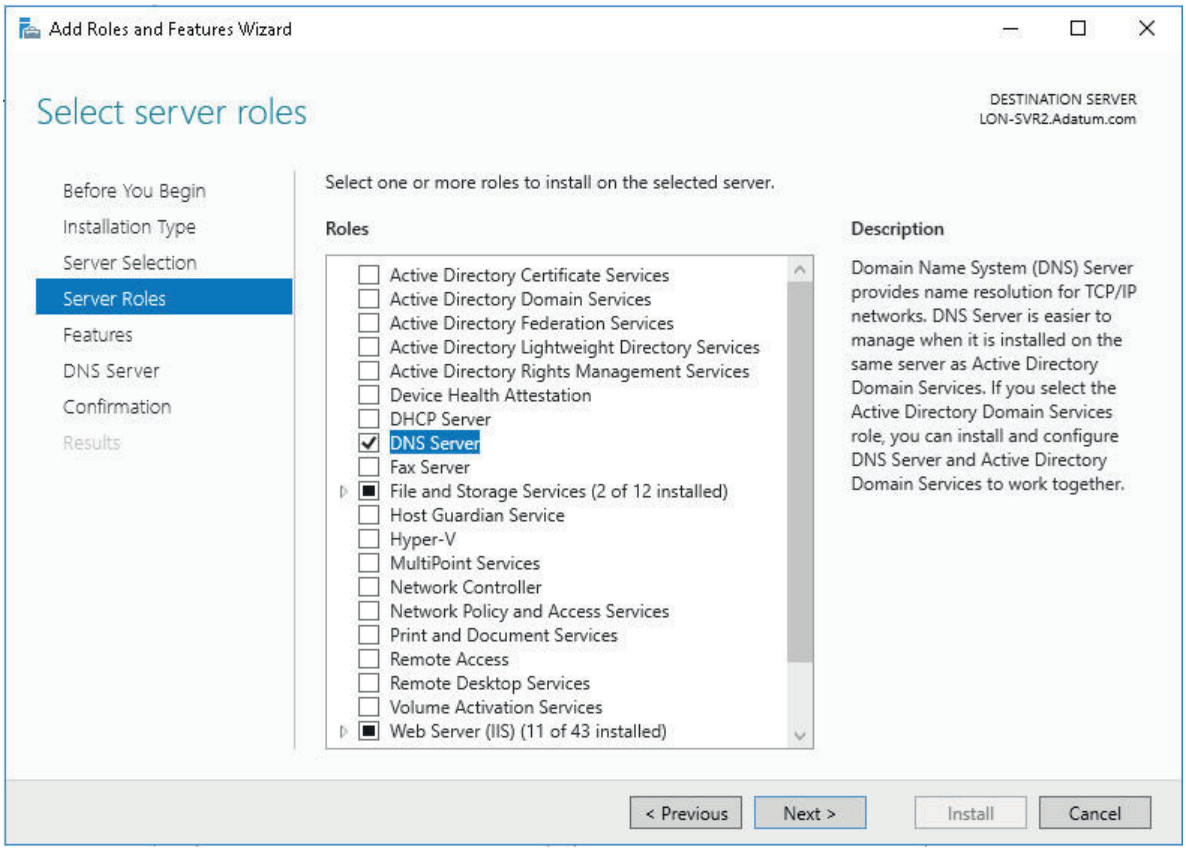
Instalowanie roli serwera DNS

Rolę serwera DNS można zainstalować za pomocą konsoli Server Manager (Menedżer serwera) lub korzystając z Windows PowerShell.

Instalowanie DNS za pomocą konsoli Server Manager

Aby zainstalować rolę serwera DNS za pomocą Server Managera, należy wykonać następujące kroki:

1. Zaloguj się na docelowym serwerze jako lokalny administrator.
2. Otwórz Server Manager.
3. Kliknij Manage (Zarządzaj), a następnie kliknij Add Roles And Features (Dodaj role i funkcje).
4. W kreatorze Add Roles And Features (Kreator dodawania ról i funkcji), na stronie Before You Begin (Zanim rozpoczniesz) kliknij Next (Dalej).
5. Na stronie Select Installation Type (Wybieranie typu instalacji) kliknij Role-Based Installation (Instalacja oparta na rolach) lub Feature-Based Installation (Instalacja oparta na funkcjach), a następnie kliknij Next.
6. Na stronie Select Destination Server (Wybieranie serwera docelowego) wybierz serwer z listy Server Pool (Pula serwerów), a następnie kliknij Next.
7. Na liście Roles (Role), na stronie Select Server Roles (Wybieranie ról serwera) wybierz DNS Server (Serwer DNS) – patrz rysunek 1-2.
8. W wyskakującym oknie dialogowym Add Roles And Features Wizard kliknij Add Features (Dodaj funkcje), a następnie kliknij Next.
9. Na stronie Select features (Wybieranie funkcji) kliknij Next.
10. Na stronie DNS Server kliknij Next.
11. Na stronie Confirm Installation Selections (Potwierdzenie wybranych opcji instalacji) kliknij Install (Instaluj). Po zakończeniu instalacji kliknij Close (Zamknj).



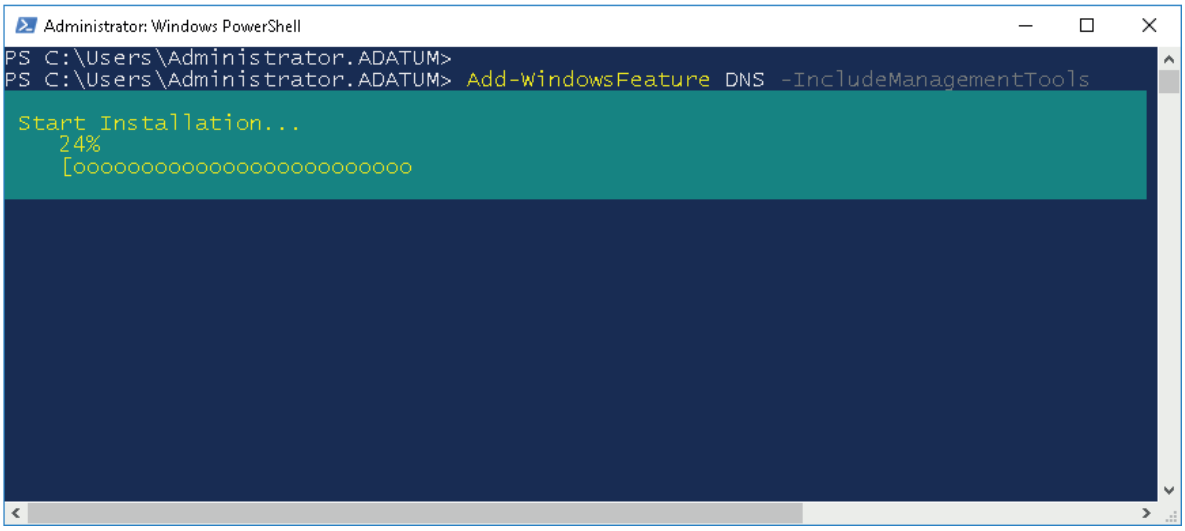
Rysunek 1-2 Instalowanie roli DNS Server za pomocą Server Managera

Instalowanie DNS za pomocą Windows PowerShell

Mimo że korzystanie z Server Managera do instalowania ról i funkcji serwera jest proste, lecz nie zawsze jest to najszybsza metoda. Aby zainstalować rolę serwera DNS i wszystkie narzędzia związane z zarządzaniem za pomocą Windows PowerShell, należy wykonać następujące kroki:

1. Zaloguj się na docelowym serwerze jako lokalny administrator.
2. Otwórz Windows PowerShell z pełnymi uprawnieniami.
3. W zgłoszeniu Windows PowerShell (patrz rysunek 1-3) wpisz następujące polecenie i naciśnij Enter:

```
Add-WindowsFeature DNS -IncludeManagementTools
```



Rysunek 1-3 Instalowanie serwera DNS za pomocą Windows PowerShell

Określenie scenariuszy wdrożeń DNS obsługiwanych przez Nano Server

Nano Server to nowa opcja wdrażania Windows Server 2016. Jest ona podobna do Windows Server Core, ma jednak dużo mniejsze wymagania sprzętowe. Nano Server ma bardzo ograniczone lokalne możliwości logowania oraz lokalne funkcje administracyjne i obsługuje tylko 64-bitowe aplikacje, agenty oraz narzędzia.

W kilku sytuacjach trzeba wziąć pod uwagę Nano Server zamiast innych opcji wdrażania Windows Server. Na przykład Nano Server zapewnia dobrą platformę dla serwera WWW z uruchomionymi usługami IIS (Internet Information Services). Nano Server pasuje także doskonale do działania roli serwera DNS.

Dodatkowe materiały **Rozpoczęcie pracy w systemie Nano Server**

Szczegółowy opis pracy z systemem Nano Server można znaleźć w witrynie Microsoft TechNet, pod adresem *https://technet.microsoft.com/windows-server-docs/compute/nano-server/getting-started-with-nano-server*.

Aby zainstalować rolę serwera DNS w systemie Nano Server, można zastosować jedną z dwóch następujących strategii.

- **Instalacja roli serwera DNS jako część wdrożenia Nano Servera** Gdy wdrażamy Nano Server za pomocą cmdleta New-NanoServerImage, można użyć parametru -Packages Microsoft-NanoServer-DNS-Package w celu zainstalowania roli serwera DNS.
- **Dodanie roli po wdrożeniu** Po wdrożeniu Nano Servera można dodać rolę serwera DNS, korzystając z Server Manager lub Windows PowerShell. Ponieważ

jednak Nano Server jest bezobsługową platformą serwera z bardzo małymi możliwościami lokalnego zarządzania, serwerem trzeba zarządzać zdalnie.

Rolę do Nano Servera można dodać, stosując następujące metody:

- W konsoli Server Manager korzystamy z opcji Add Other Servers To Manage (Dodaj inne serwery do zarządzania), aby dodać Nano Server jako serwer zarządzalny. Następnie dodajemy do tego serwera rolę DNS Server, stosując procedurę przedstawioną wcześniej w tym rozdziale (patrz „Instalowanie DNS za pomocą konsoli Server Manager").
- Tworzymy zdalną sesję Windows PowerShell za pomocą Nano Servera, korzystając z cmdletu Enter-PSSession. Następnie można użyć cmdletów Windows PowerShell, aby zainstalować rolę serwera DNS, jak opisano wcześniej w tym rozdziale. Na przykład w celu dodania roli DNS do Nano Servera ze zdalnej sesji Windows PowerShell, korzystamy z następującego polecenia:

```
Enable-WindowsOptionalFeature -Online -FeatureName DNS-Server-Full-Role
```

WSKAZÓWKA EGZAMINACYJNA

DNS zintegrowany z Active Directory nie jest obsługiwany przez Nano Server, co oznacza, że na takim serwerze można zaimplementować tylko DNS oparty na plikach.

DODATKOWE MATERIAŁY **Włączanie i używanie zdalnych poleceń w Windows PowerShell**

Więcej szczegółów na temat korzystania ze zdalnych usług w Windows PowerShell można znaleźć w witrynie Microsoft TechNet, pod adresem *https://technet.microsoft.com/magazine/ff700227.aspx*.

Konfigurowanie usług przesyłania dalej, wskazówek dotyczących serwerów głównych, rekurencji oraz delegowania

Po zainstalowaniu roli serwera DNS na serwerze systemu Windows Server 2016 należy ją skonfigurować. Konfiguracja ta obejmuje usługi przesyłania dalej, wskazówki dotyczące serwerów, rekurencję oraz delegowanie.

Konfigurowanie usług przesyłania dalej

Usługi przesyłania dalej umożliwiają zdefiniowanie, co dzieje się z zapytaniem DNS, gdy serwer DNS, do którego kierujemy zapytanie, nie jest w stanie podać adresu. Na przykład można skonfigurować i wykorzystać przekazywanie DNS, aby sterować

przepływem zapytań DNS w całej organizacji tak, aby do obsługi internetowych zapytań DNS można używać tylko określonych serwerów DNS.

Za pomocą usług przesyłania dalej w DNS, można:

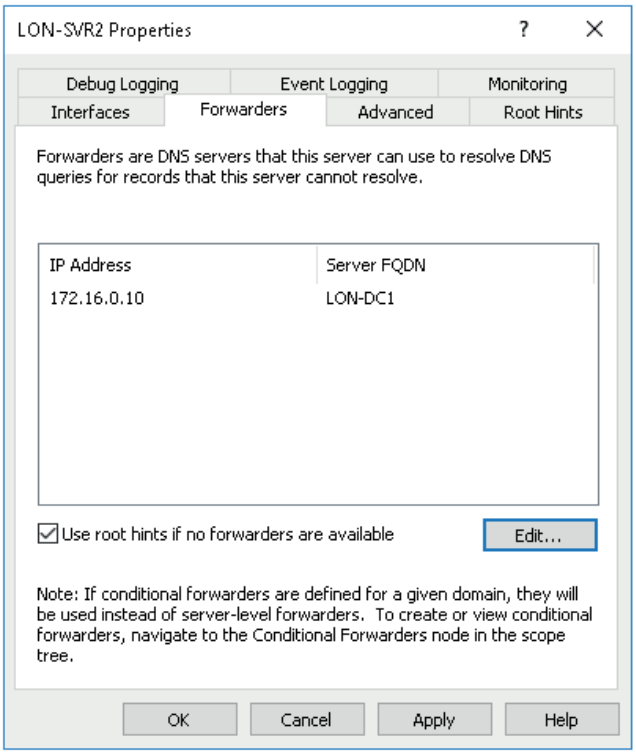
- Skonfigurować serwer DNS tak, aby odpowiadał tylko na te zapytania, które może zrealizować przez odwołanie do przechowywanych lokalnie informacji o strefie. Wszystkie inne zapytania muszą być przekazywane przez zapytywany serwer do innego serwera DNS.
- Zdefiniować działanie przesyłania dla określonych domen DNS, konfigurując przekazywanie warunkowe DNS. W tym scenariuszu, jeśli zapytanie DNS zawiera określoną nazwę domeny, na przykład Contoso.com, jest ono przesyłane do konkretnego serwera DNS.

Aby skonfigurować przesyłanie dalej, należy wykonać następujące kroki:

1. W konsoli Server Manager (Menedżer serwerów) kliknij Tools (Narzędzia), a następnie kliknij DNS.
2. W konsoli DNS Manager (Menedżer DNS) kliknij prawym przyciskiem myszy serwer DNS w okienku nawigacji, a następnie kliknij Properties (Właściwości).
3. W oknie dialogowym Server Properties (Właściwości serwera), na karcie Forwarders (Usługi przesyłania dalej) kliknij Edit (Edytuj).
4. Na liście IP Address (Adres IP), znajdującej się w oknie dialogowym Edit Forwarders (Edytuj usługi przesyłania dalej), wprowadź adres IP serwera, do którego chcesz przesyłać wszystkie zapytania DNS, a następnie kliknij OK. Można tutaj skonfigurować kilka serwerów DNS; zapytania do tych serwerów są wysyłane w kolejności zgodnej z preferencjami. Można również ustawić czas oczekiwania (w sekundach), po upłynięciu którego wygasa.
5. W oknie dialogowym Server Properties, na karcie Forwarders można przeglądać i edytować listę usług przesyłania dalej DNS, jak pokazano na rysunku 1-4. Można również określić, co będzie się działo, jeśli z żadną z usług przesyłania dalej DNS nie będzie się mógł połączyć. W takim przypadku domyślnie są stosowane wskazówki dotyczące serwerów głównych. Wskazówki te są omówione w następnym punkcie. Kliknij OK, aby zakończyć konfigurację.

WSKAZÓWKA EGZAMINACYJNA

Przesyłanie dalej można również skonfigurować, korzystając z cmdletu Windows PowerShell, Add-DnsServerForwarder.



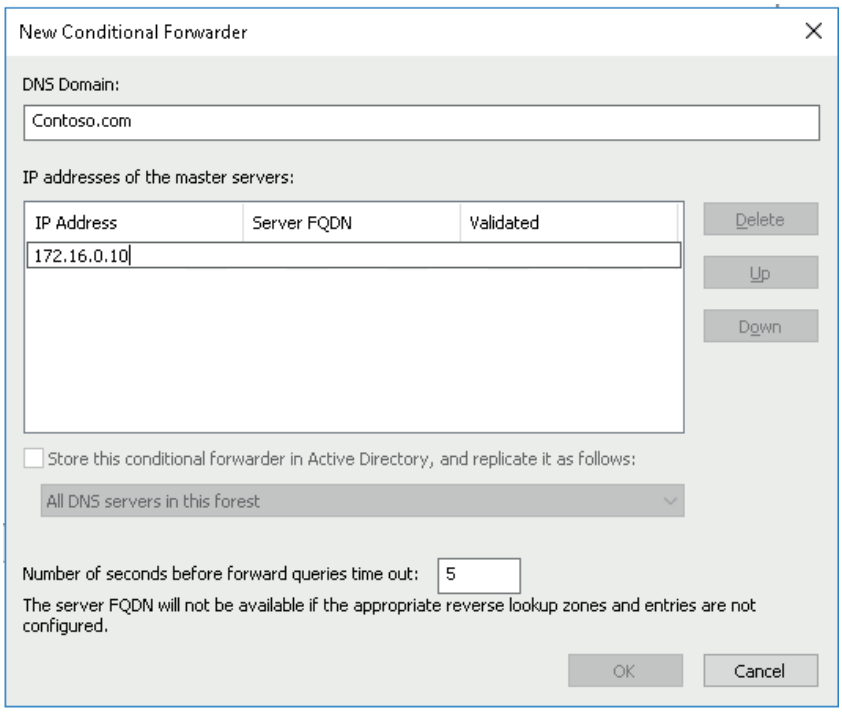
Rysunek 1-4 Konfigurowanie usługi przesyłania dalej DNS

Aby włączyć i skonfigurować warunkowe przesyłanie dalej, należy wykonać następujące kroki:

1. W okienku nawigacji DNS Managera kliknij prawym przyciskiem węzeł Conditional Forwarders (Usługi warunkowego przesyłania dalej), a następnie kliknij New Conditional Forwarder (Nowa usługa warunkowego przesyłania dalej).
2. W oknie dialogowym New Conditional Forwarder, w polu DNS Domain (Domena DNS), wpisz nazwę domeny, dla której chcesz utworzyć usługę warunkowego przesyłania dalej (patrz rysunek 1-5). Następnie, na liście adresów IP serwerów głównych, wprowadź adres IP serwera usługi przesyłania dalej dla tej domeny; naciśnij Enter.
3. Opcjonalnie określ wartość Number of Seconds Before Forward Queries Time Out (Liczba sekund przed upłynięciem limitu czasu przesyłania kwerend dalej). Wartość domyślna to 5 sekund.
4. Kliknij OK.

WSKAZÓWKA EGZAMINACYJNA

Do konfiguracji usługi warunkowego przesyłania dalej można również użyć cmdletu Windows PowerShell, Add-DnsServerConditionalForwarderZone.



Rysunek 1-5 Konfigurowanie usługi warunkowego przesyłania dalej DNS

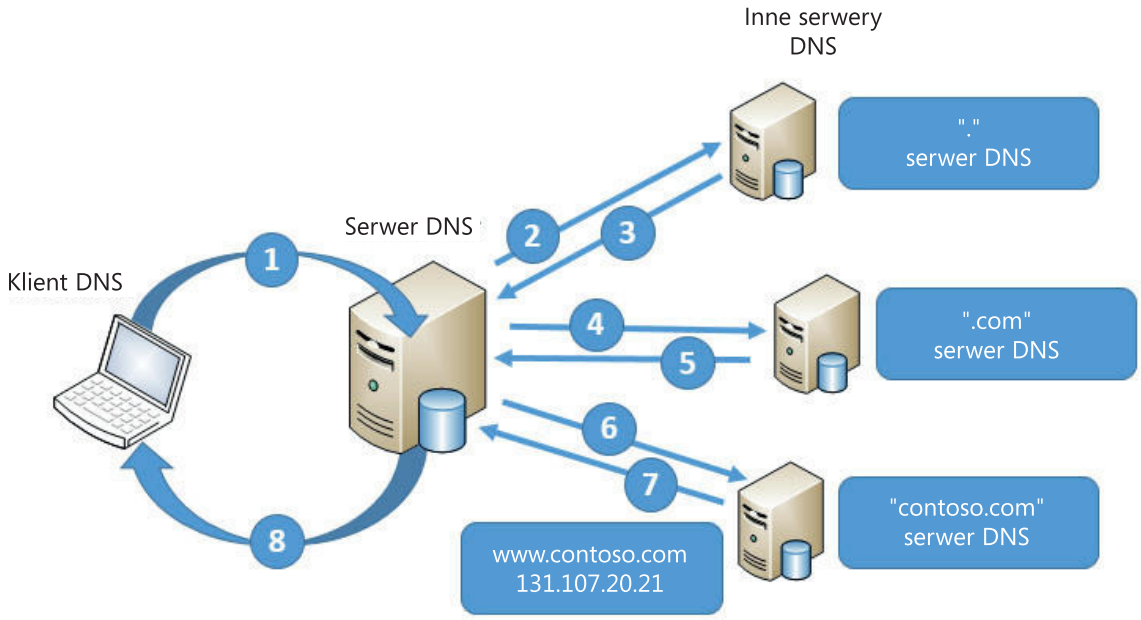
Konfiguracja wskazówek dotyczących serwerów głównych

Jeśli nie określimy usługi przekazywania dalej DNS, to w sytuacji, gdy serwer DNS, do którego wysłano zapytanie DNS, nie może na nie odpowiedzieć, korzysta ze wskazówek dotyczących serwerów głównych, aby ustalić, jak znaleźć adres. Zanim przyjrzymy się wskazówkom dotyczącym serwerów głównych, trzeba zrozumieć, jak obsługiwane jest internetowe zapytanie DNS.

OBSŁUGA INTERNETOWEGO ZAPYTANIA DNS

Aplikacja kliencka, taka jak Microsoft Edge, chce odwzorować nazwę (jak www.contoso.com) na odpowiedni adres IPv4. Aplikację tę określamy jako klienta DNS. Procedurę stosowaną do rozpoznania tej nazwy opisano poniżej i pokazano na rysunku 1-6.

1. Klient DNS wysyła do swojego skonfigurowanego serwera DNS prośbę dotyczącą potrzebnego rekordu (na przykład www.contoso.com), za pomocą zapytania rekurencyjnego.
   - Serwer DNS, do którego kierowane jest zapytanie, sprawdza, czy jest autorytatywny dla żądanego rekordu. Jeśli jest, zwraca potrzebne informacje.
   - Jeśli nie jest autorytywny, serwer DNS sprawdza swoją lokalną pamięć podręczną, aby ustalić, czy rekord był ostatnio wyszukiwany. Jeśli rekord znajduje się w pamięci podręcznej, jest zwracany klientowi, który go zażądał.



Rysunek 1-6 Działanie internetowego zapytania DNS

Wskazówka egzaminacyjna

Gdy serwer DNS otrzymuje zapytanie rekurencyjne, albo zwraca żądany wynik, albo błąd; w żadnym przypadku nie odsyła klienta DNS do innego serwera.

2. Jeśli rekordu nie ma w pamięci podręcznej, wtedy serwer DNS wysyła szereg zapytań iteracyjnych do innych serwerów DNS, pytając o żądany rekord. Zaczyna ten proces od serwera głównego.

Wskazówka egzaminacyjna

Gdy serwer DNS otrzyma zapytanie iteracyjne, zwraca żądany wynik lub odsyła do innego serwera, który może być autorytatywny dla żądanego rekordu.

3. Rekord jest zwracany, jeśli serwer główny jest autorytatywny dla żądanego rekordu. W przeciwnym przypadku serwer główny zwraca adres IP serwera DNS autorytatywnego dla domeny kolejnego, niższego poziomu, w tym przypadku .com.
4. Początkowy serwer DNS wysyła żądanie do określonego serwera DNS .com za pomocą kolejnego zapytania iteracyjnego.
5. Serwer DNS .com nie jest autorytatywny, więc zwraca adres IP serwera DNS Contoso.com.
6. Początkowy serwer DNS wysyła żądanie do serwera DNS Contoso.com, korzystając z kolejnego zapytania iteracyjnego.

7. Serwer Contoso.com DNS jest autorytatywny, więc zawraca żądaną informację – w tym przypadku adres IPv4 dla www.contoso.com.
8. Początkowy serwer DNS buforuje rekord i zwraca żądaną informację klientowi DNS.

JAK SĄ WYKORZYSTYWANE WSKAZÓWKI DOTYCZĄCE SERWERÓW GŁÓWNYCH

Jak wynika z poprzednich wyjaśnień i diagramu, jeśli serwer DNS nie jest autorytatywny i nie utrzymuje pamięci podręcznej dla domeny DNS, wysyła żądanie do serwera głównego, aby rozpocząć proces ustalania, który serwer jest autorytatywny dla żądanego rekordu. Jednak bez adresu IP głównego serwera nazw ten proces nie może się rozpocząć.

Wskazówki dotyczące serwerów głównych są wykorzystywane przez serwery DNS, aby umożliwić im przeszukiwanie hierarchii DNS w Internecie, zaczynając od serwera głównego. Serwery DNS firmy Microsoft są wstępnie skonfigurowane z odpowiednimi rekordami wskazówek. Listę serwerów we wskazówkach można jednak zmodyfikować, korzystając z konsoli DNS Manager lub z Windows PowerShell.

WSKAZÓWKA EGZAMINACYJNA

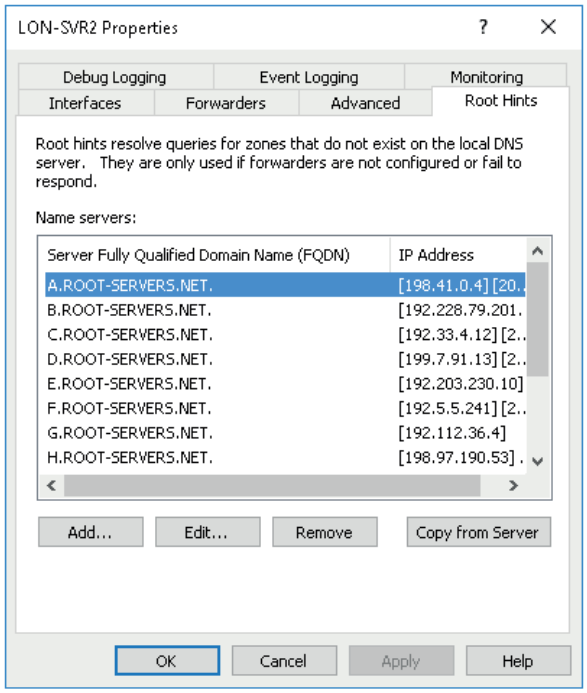
Usługa DNS Server implementuje wskazówki dotyczące serwerów głównych, korzystając z pliku, CACHE.DNS, przechowywanego w folderze %systemroot%\System32\dns na serwerze.

Można wziąć rozważyć edycję informacji wskazówek dotyczących serwerów głównych, jeśli chcemy skonfigurować przepływ ruchu zapytań DNS w naszej sieci wewnętrznej. Jest to także przydatne między naszą siecią wewnętrzną a siecią graniczną, która znajduje się między naszą siecią wewnętrzną a Internetem.

EDYCJA WSKAZÓWEK DOTYCZĄCYCH SERWERÓW GŁÓWNYCH

Aby zmodyfikować wskazówki dotyczące serwerów głównych za pomocą DNS Managera, należy wykonać następujące kroki:

1. W konsoli Server Manager kliknij Tools, a następnie kliknij DNS.
2. W konsoli DNS Manager znajdź odpowiedni serwer DNS. Kliknij prawym przyciskiem serwer, a następnie kliknij Properties.
3. W oknie dialogowym Properties kliknij kartę Root Hints, jak pokazano na rysunku 1-7.
4. Możesz następnie dodać nowe rekordy lub edytować albo usunąć dowolne istniejące rekordy. Możesz również kliknąć Copy From Server (Kopiuj z serwera), aby zaimportować wskazówki dotyczące serwerów głównych z innego serwera DNS będącego online. Po zakończeniu edycji wskazówek kliknij OK.



Rysunek 1-7 Konfigurowanie wskazówek dotyczących serwerów głównych

Do modyfikacji informacji zawartych we wskazówkach dotyczących serwerów głównych można również używać Windows PowerShell. Do zarządzania tymi wskazówkami służą następujące cmdlety:

- **Add-DnsServerRootHint** Umożliwia dodawanie nowych rekordów wskazówek dotyczących serwerów głównych.
- **Remove-DnsServerRootHint** Umożliwia usuwanie rekordów wskazówek.
- **Set-DnsServerRootHint** Umożliwia edycję nowych rekordów wskazówek. Można również korzystać z cmdletu Get-DnsServerRootHint, aby wyszukać rekord, który chcemy poddać edycji.
- **Import-DnsServerRootHint** Umożliwia kopiowanie informacji wskazówek dotyczących serwerów głównych z innego serwera DNS będącego online.

Na przykład, aby uaktualnić wartość wskazówek przypisanych do H.Root-servers.adatum.com, korzystamy z dwóch poniższych poleceń Windows PowerShell:

```
$hint = (Get-DnsServerRootHint | Where-Object
 {$_.NameServer.RecordData.NameServer -eq "H.Root-Servers.Adatum.com."} )

$hint.IPAddress[0].RecordData.Ipv4address = "10.24.60.254"
```

Pierwsze polecenie pobiera wskazówkę H.Root-servers.adatum.com i przypisuje ją zmiennej `$hint`. Cmdlet Get-DnsServerRootHint pobiera listę wszystkich wskazówek dotyczących serwerów głównych, a cmdlet Where-Object filtruje wyniki, aby otrzymać tylko wskazówki dla H.Root-servers.adatum.com.

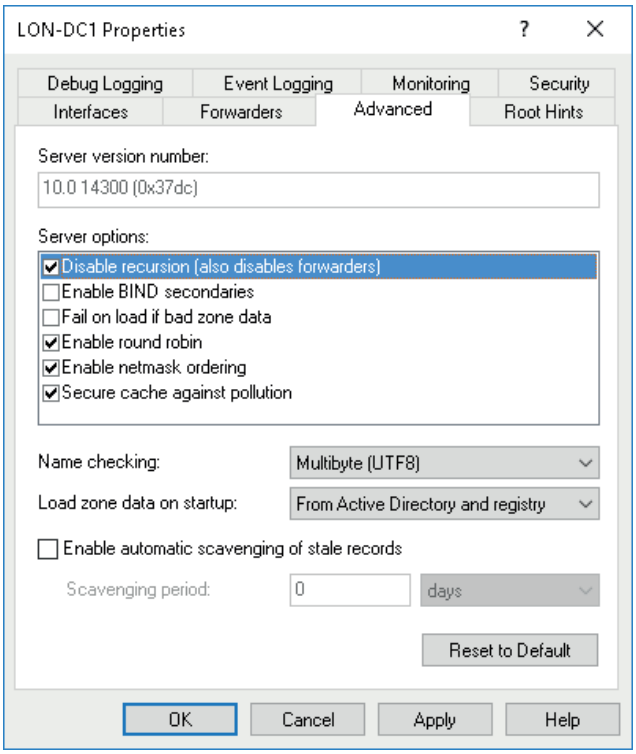
Konfigurowanie rekurencji

Rekurencja to nazwa procesu rozpoznawania nazwy, w którym serwer DNS, do którego wysłano żądanie, kieruje zapytanie do innych serwerów DNS, aby uzyskać odpowiedź na zapytanie DNS w imieniu żądającego klienta. Serwer, do którego skierowano prośbę, zwraca wtedy odpowiedź do klienta DNS. Domyślnie wszystkie serwery DNS wykonują zapytania rekurencyjne w imieniu swoich klientów DNS i innych serwerów DNS, które przesłały do nich zapytania klienta DNS.

Ponieważ jednak rekurencja może być wykorzystana przez atakujących jako metoda wykonania próby ataku odmowy usług na waszych serwerach DNS, należy rozważyć wyłączenie rekurencji na dowolnym serwerze DNS w naszej sieci, która nie jest przeznaczona do otrzymywania zapytań rekurencyjnych.

Aby wyłączyć rekurencję, należy wykonać następujące kroki:

1. W konsoli Server Manager kliknij Tools, a następnie DNS.
2. W konsoli DNS Manager kliknij prawym przyciskiem myszy odpowiedni serwer, a następnie kliknij Properties.
3. Kliknij zakładkę Advanced (Zaawansowane), a następnie, na liście Server options (Opcje serwera), zaznacz pole wyboru Disable Recursion (Also Disables Forwarders) (Wyłącz rekurencję (także wyłącza usługi przesyłania dalej)), jak pokazano na rysunku 1-8, a następnie kliknij OK.



Rysunek 1-8 Wyłączanie rekurencji

ZAKRESY REKURENCJI

Wprawdzie wyłączenie rekurencji może się wydawać właściwe, jest jednak kilka serwerów, które muszą wykonywać rekurencję dla swoich klientów i innych serwerów DNS. Są one jednak narażone na szkodliwe ataki sieciowe. Windows Server 2016 obsługuje funkcję określaną jako zakresy rekurencji (ang. *recursion scopes)*, która pozwala kontrolować działanie zapytania rekurencyjnego. W tym celu trzeba użyć DNS Server Policies (Zasady serwera DNS).

Na przykład można mieć jeden serwer DNS umożliwiający wykonywanie zapytań rekurencyjnych dla klientów wewnętrznych w domenie Adatum.com, który jednak nie powinien akceptować żadnych zapytań rekurencyjnych od komputerów z Internetu. Aby skonfigurować takie działanie, otwieramy Windows PowerShell i wykonujemy dwa poniższe polecenia:

```
Set-DnsServerRekurencjaScope -Name . -EnableRekurencja $False

Add-DnsServerRekurencjaScope -Name "InternalAdatumClients"
 -EnableRekurencja $True
```

Pierwsze polecenie dezaktywuje rekurencję dla domyślnego zakresu, czyli w rezultacie ją wyłącza. Domyślny zakres obejmuje rekurencję na poziomie serwera i ustawienia przesyłania dalej, które zostały już omówione w tym rozdziale (patrz „Konfigurowanie usług przesyłania dalej, wskazówek dotyczących serwerów głównych, rekurencji oraz delegowania).

Drugie polecenie tworzy nowy zakres rekurencji o nazwie InternalAdatumClients. Rekurencja zostaje włączona dla klientów z tego zakresu. Następnie trzeba zdefiniować, które klienty należą do tego zakresu rekurencji. W tym celu korzystamy z następującego polecenia Windows PowerShell:

```
Add-DnsServerQueryResolutionPolicy -Name "RekurencjaControlPolicy"
 -Action ALLOW -ApplyOnRekurencja -RekurencjaScope "InternalAdatumClients"
 -ServerInterfaceIP  "EQ,10.24.60.254"
```

W tym przykładzie żądania klienta otrzymane na interfejsie serwera DNS z adresem IP 10.24.60.254 są oceniane jako należące do InternalAdatumClients, a rekurencja zostaje włączona. Dla żądań klientów otrzymanych na innych interfejsach serwera rekurencja pozostaje wyłączona.

Dodatkowe materiały **Cmdlet Add-Dns ServerQueryResolutionPolicy**

Więcej informacji na temat wykorzystania Windows PowerShell do konfiguracji zakresów rekurencji można znaleźć w witrynie TechNet, pod adresem *https://technet.microsoft.com/library/mt126273.aspx*.

Konfigurowanie delegowania

To zagadnienie jest ujęte w kolejnym podrozdziale, „Zagadnienie 1.2: Tworzenie i konfigurowanie stref i rekordów DNS”, w punkcie „Konfigurowanie delegowania”.

Konfigurowanie zaawansowanych ustawień DNS

Dzięki konfigurowaniu przesyłania dalej, rekurencji oraz wskazówkom dotyczącym serwerów głównych możemy sterować podstawowymi zasadami przetwarzania zapytań DNS w naszej organizacji. Po skonfigurowaniu tych ustawień można przejść do włączenia i konfiguracji ustawień bardziej zaawansowanych.

Konfigurowanie DNSSEC

DNSSEC jest ustawieniem zabezpieczeń dla DNS, które pozwala na cyfrowe podpisywanie wszystkich rekordów DNS w strefie DNS, aby klienty DNS mogły zweryfikować tożsamość serwera DNS. DNSSEC pomaga w uzyskaniu pewności, że klient DNS kontaktuje się z prawdziwym serwerem DNS.

Uwaga Strefy DNS

Tworzenie stref DNS i zarządzanie nimi opisano w punkcie „Tworzenie stref DNS”.

Gdy klient wysyła zapytanie do serwera DNS, który został skonfigurowany z opcją DNSSEC, serwer DNS zwraca wynik wraz z podpisem cyfrowym. Aby sprawdzić, czy podpis jest ważny, klient DNS otrzymuje klucz publiczny z pary kluczy publiczny/prywatny powiązanej z tym podpisem z *kotwicy zaufania*. Aby to działało, trzeba skonfigurować swoich klientów DNS z kotwicą zaufania dla oznaczonej strefy DNS.

KOTWICE ZAUFANIA

Implementacja DNSSEC wymaga utworzenia strefy TrustAnchors (Kotwice zaufania). Ta strefa służy do przechowywania kluczy publicznych związanych z konkretnymi strefami DNS. Trzeba utworzyć kotwicę zaufania z zabezpieczanej strefy na każdym serwerze DNS, który przechowuje tę strefę.

TABLICA ZASAD ROZPOZNAWANIA NAZW

Ponadto trzeba utworzyć, skonfigurować i rozdystrybuować tablicę zasad rozpoznawania nazw, NRPT (Name Resolution Policy Table). Reguła DNSSEC w NRPT jest wykorzystywana przez klienty w celu zdefiniowania sposobu działania klienta DNS oraz jest używana przez DNSSEC do poinstruowana klienta, aby wymagał potwierdzenia poprzez zastosowanie podpisu.

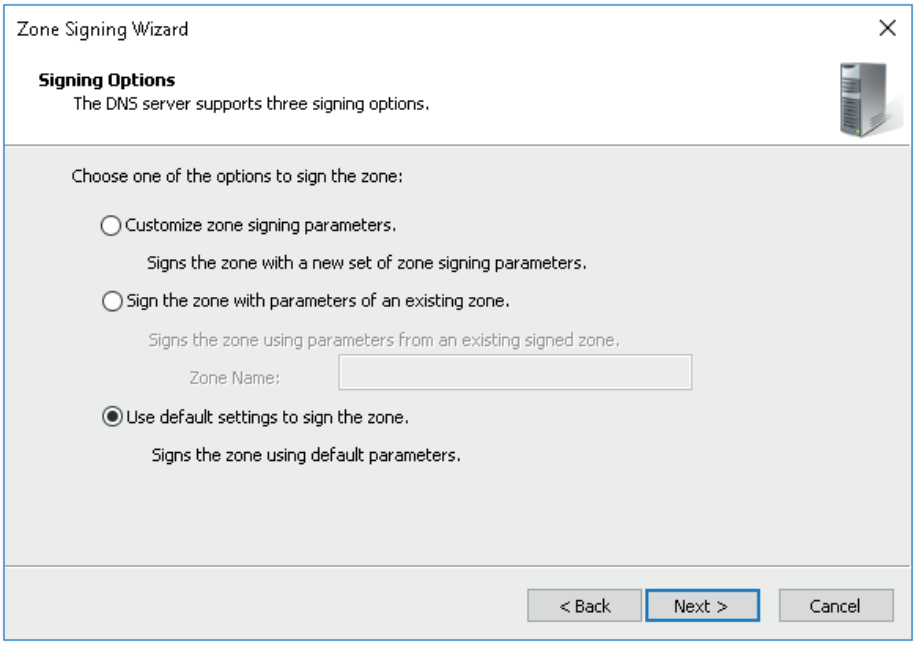
WSKAZÓWKA EGZAMINACYJNA

Do dystrybucji NRPT w środowiskach Active Directory Domain Services (AD DS) zazwyczaj stosuje się obiekty grup zasad, GPO (Group Policy Objects).

IMPLEMENTACJA DNSSEC

Po zainstalowaniu systemu Windows Server 2016 i wdrożeniu roli serwera DNS na serwerze, aby zaimplementować DNSSEC, należy wykonać następujące kroki:

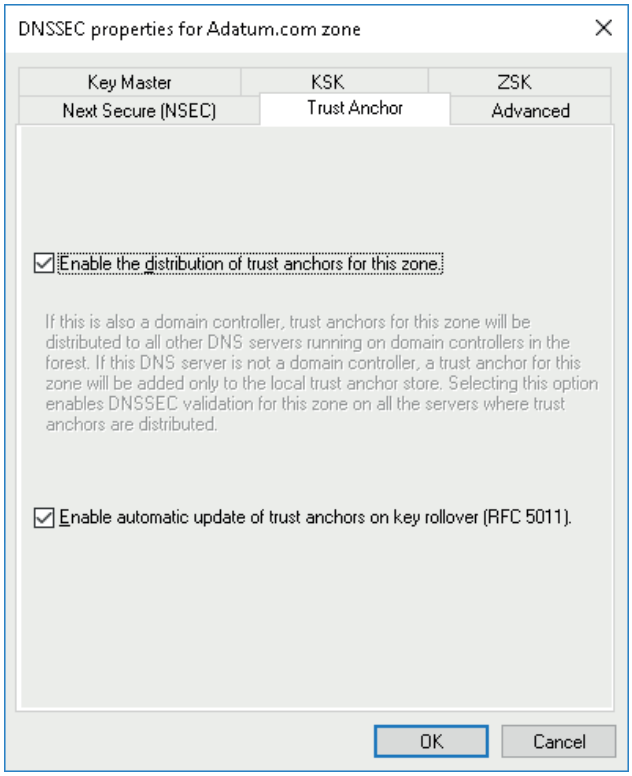
1. Uruchom kreator DNSSEC Configuration Wizard z konsoli DNS Manager, aby podpisać strefę DNS. W konsoli DNS Manager kliknij prawym przyciskiem pożądaną strefę, wskaż DNSSEC, a następnie kliknij Sign The Zone (Podpisz strefę). Po podpisaniu strefy można wybrać jedną z trzech opcji, jak to pokazano na rysunku 1-9.



RYSUNEK 1-9 Podpisywanie strefy DNS

- **Customize Zone Signing Parameters (Dostosuj parametry podpisywania strefy)** Umożliwia konfigurację wszystkich wartości dla kluczy KSK (Key Signing Key) oraz ZSK (Zone Signing Key).
- **Sign The Zone With Parameters Of An Existing Zone (Podpisz strefę przy użyciu parametrów istniejącej strefy)** Umożliwia wykorzystanie tych samych wartości i opcji jak w istniejącej podpisanej strefie.
- **Use Default Settings To Sign The Zone (Użyj ustawień domyślnych do podpisania strefy)** Podpisuje strefę, wykorzystując wartości domyślne.

2. Skonfiguruj punkty dystrybucji kotwic zaufania. Z tej możliwości można skorzystać po wybraniu opcji Customize Zone Signing Parameters. W innym przypadku, po podpisaniu strefy, należy wykonać następujące kroki w celu skonfigurowania punktów dystrybucji kotwic zaufania:
   A. W konsoli DNS Manager kliknij prawym przyciskiem myszy pożądaną strefę, wskaż DNSSEC, a następnie kliknij Properties.
   B. W oknie dialogowym DNSSEC Properties For Selected Zone, na karcie Trust Anchor (Kotwica zaufania) zaznacz okno wyboru Enable The Distribution Of Trust Anchors For This Zone (Włącz dystrybucję kotwic zaufania dla tej strefy) i kliknij OK, co pokazano na rysunku 1-10. Gdy pojawi się zgłoszenie kliknij Yes, a następnie OK.
   C. Sprawdź, czy węzeł Trust Points istnieje i zawiera odpowiednie rekordy DNS KEY (DNSKEY). W tym celu, w konsoli DNS Manager, rozwiń węzeł Server, a następnie rozwiń Trust Points. Zawiera on węzły podrzędne naszych stref DNS, w których znajdują się dwa rekordy DNS KEY (DNSKEY).



Rysunek 1-10 Włączanie dystrybucji zaufanych kotwic

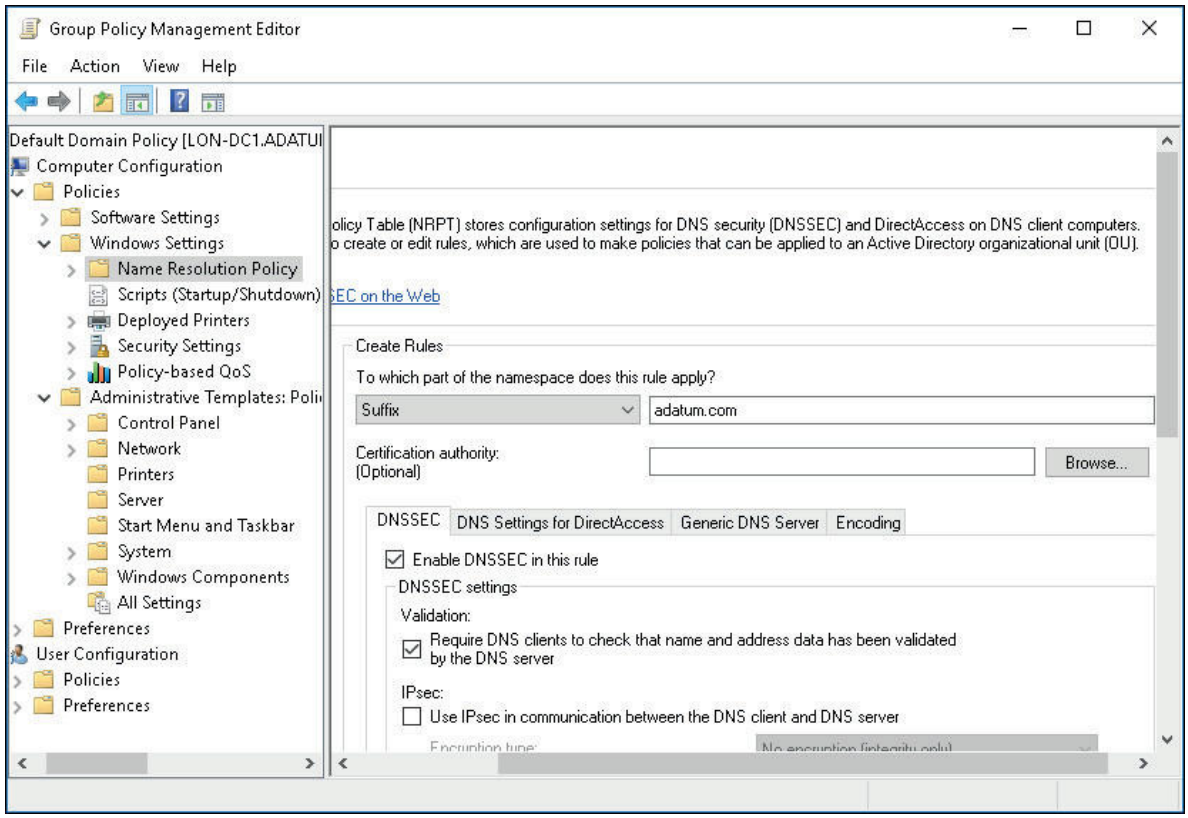
3. Skonfiguruj NRPT na komputerach klienckich. Należy rozprowadzić NRPT do wszystkich komputerów klienckich, aby wiedziały, że mają żądać potwierdzenia za pomocą DNSSEC. Najłatwiejszą metodą osiągnięcia tego jest użycie dystrybucji GPO:

A. Otwórz Group Policy Management (Zarządzanie zasadami grupy) i znajdź Default Domain Policy (Domyślne zasady domeny).

B. Otwórz zasadę do edycji i przejdź do Computer Configuration / Policies / Windows Settings / Name Resolution Policy, jak to pokazano na rysunku 1-11.

C. W części Create Rules (Utwórz reguły) wpisz w polu testowym Suffix (Sufiks) nazwę swojej domeny (na przykład Adatum.com); w ten sposób reguła zostanie zastosowana do sufiksu tego obszaru nazw.

D. Zaznacz pola wyboru Enable DNSSEC in this Rule (Włącz zabezpieczenia DNSSEC w tej regule) oraz Require DNS Clients To Check That The Name And Address Data Has Been Validated By The DNS Server (Wymagaj od klientów DNS sprawdzenia, czy dane nazwy i adresu zostały zweryfikowane przez serwer DNS), a następnie kliknij Create (Utwórz).



Rysunek 1-11 Tworzenie GPO NRPT

Dodatkowe materiały krok po kroku: Pokaz DNSSEC w laboratorium testowym

Więcej informacji na temat wdrażania DNSSEC można znaleźć w witrynie Microsoft TechNet, pod adresem *https://technet.microsoft.com/library/hh831411(v=ws.11).aspx*.

Konfiguracja puli gniazd DNS

Pulę gniazd DNS można wykorzystać, aby włączyć możliwość używania przez serwer DNS losowego portu źródłowego przy wydawaniu zapytań DNS. Jeśli uaktywnimy pulę gniazd DNS, po uruchomieniu usługi DNS serwer DNS wybiera port źródłowy z puli dostępnych gniazd. To oznacza, że serwer DNS unika używania dobrze znanych portów. To może pomóc w zabezpieczeniu serwera DNS, ponieważ atakujący musi odgadnąć zarówno port źródłowy zapytania DNS, jak i losowy ID transakcji, aby z powodzeniem przeprowadzić atak.

Do skonfigurowania rozmiaru puli gniazd DNS można wykorzystać narzędzie wiersza poleceń, DNSCMD.exe.

W tym celu z wiersza polecenia z podwyższonym poziomem uprawnień uruchomiamy polecenie dnscmd /Config /SocketPoolSize <wartość> , a następnie restartujemy serwer DNS. Rozmiar puli gniazd można skonfigurować na wartość od 0 do 10 000. Rozmiarem domyślnym jest 2 500.

Konfigurowanie blokowania pamięci podręcznej

Gdy klient DNS kieruje zapytanie do rekurencyjnego serwera DNS, serwer zapisuje wynik w pamięci podręcznej, aby mógł szybciej odpowiedzieć na zapytania innych klientów DNS, dotyczące tych samych informacji. Czas przechowywania rekordu w pamięci podręcznej jest określona przez jego wartość czasu życia (Time To Live, TTL).

W czasie TTL rekord można nadpisać, jeśli dostępne są nowsze dane. To jednak stanowi potencjalne zagrożenie bezpieczeństwa. Atakujący może być w stanie zastąpić rekord w pamięci podręcznej informacjami, które mogłyby przekierować na stronę zawierającą niebezpieczną zawartość.

Aby zmniejszyć to ryzyko, można w systemie Windows Server 2016 zastosować blokowanie pamięci podręcznej, aby określić, kiedy informacje w pamięci podręcznej usługi rozpoznawania DNS mogą zostać nadpisane. Po uaktywnieniu blokowania pamięci podręcznej serwer DNS nie pozwala na aktualizacje przechowywanych rekordów przed upłynięciem czasu TTL.

Aby skonfigurować blokowanie pamięci podręcznej na swoim serwerze DNS, uruchamiamy w Windows PowerShell polecenie Set-DnsServerCache –LockingPercent <wartość>. Wpisywana <wartość> jest procentem czasu życia (TTL). Dla przykładu, jeśli wpiszemy 75, wtedy serwer DNS nie pozwoli na aktualizację przechowywanego rekordu, dopóki nie upłynie 75 procent jego czasu życia.

WSKAZÓWKA EGZAMINACYJNA

Domyślną wartością procentu przy blokowaniu pamięci podręcznej jest 100, co oznacza, że przechowywane rekordy nie mogą być nadpisane przed upływem całkowitego czasu życia (TTL).

Włączanie ograniczania częstości odpowiedzi

Inną funkcją zabezpieczeń, z której można korzystać w systemie Windows Server 2016, jest ograniczanie częstości odpowiedzi, co jest obroną przed atakami odmowy usług DNS. Popularnym atakiem odmowy usług DNS jest oszukiwanie serwerów DNS, aby wysyłały duże ilości ruchu DNS do określonych serwerów DNS, przeciążając w ten sposób docelowe serwery.

Gdy serwer DNS ze skonfigurowanym ograniczeniem częstości odpowiedzi rozpozna potencjalnie złośliwe zapytania, ignoruje je zamiast je propagować. Serwer DNS może rozpoznać takie zagrożenia, ponieważ wiele jednakowych zapytań z tego samego źródła w krótkim okresie czasu wzbudza podejrzenie.

Domyślnie ograniczanie częstości odpowiedzi jest wyłączone. Aby go włączyć, uruchamiamy w Windows PowerShell polecenie, Set-DnsServerResponseRateLimiting. To uaktywnia ograniczanie częstości odpowiedzi z użyciem domyślnych wartości. Można również podać parametry polecenia, aby dostosować ograniczanie częstości odpowiedzi.

Dodatkowe materiały Set-DnsServerResponseRateLimiting

Więcej informacji na temat konfigurowania ograniczania częstości odpowiedzi DNS można znaleźć w witrynie Microsoft TechNet, pod adresem *https://technet.microsoft.com/library/mt422603.aspx*.

Konfigurowanie uwierzytelniania nazwanych jednostek opartego na DNS

Windows Server 2016 obsługuje nową funkcję uwierzytelniania nazwanych jednostek opartego na DNS – DNS-Based Authentication of Named Entities (DANE). Ta funkcja działa w oparciu o Transport Layer Security Authentication (TLSA) i może pomóc ograniczyć ataki pośrednika w naszej sieci.

Działanie DANE polega na informowaniu klientów DNS żądających rekordów z naszej domeny, przez który CA (Certification Authority) powinny być wydawane certyfikaty cyfrowe powiązane z tymi rekordami. Przypuśćmy na przykład, że klient DNS wysyła zapytanie o adres IPv4 powiązany z rekordem https://www.adatum.com. Serwer DNS dostarcza adres IPv4 oraz powiązane z nim informacje. Jednak serwer dostarcza również informacje, iż certyfikat użyty do uwierzytelniania tożsamości serwera www.adatum.com został dostarczony przez określony urząd certyfikacji (CA).

Administrowanie DNS

Trzeba koniecznie wiedzieć, jak administrować serwerami DNS. Do interaktywnego administrowania serwerami DNS w swojej organizacji można używać takich narzędzi jak Windows PowerShell i konsola DNS Manager. Jednak w środowiskach dużych

przedsiębiorstw dobre administrowanie taką krytyczną usługą może być trudne. W takich sytuacjach można rozważyć wdrożenie zasad DNS, przekazanie administracji DNS zespołowi specjalistów oraz wykorzystywanie dzienników DNS jako wskaźnika potencjalnych problemów z DNS.

Implementowanie zasad DNS

DNS Policy (Zasady DMS) to nowa funkcja w systemie Windows Server 2016, która pozwala sterować sposobem funkcjonowania serwera DNS w określonych warunkach. Na przykład widzieliśmy już, jak zaimplementować zakresy rekurencji, aby sterować rekurencją DNS na podstawie określonych czynników; jest to przykład działania zasady DNS.

Można utworzyć jedną lub więcej zasad DNS zgodnie z potrzebami organizacji. Do typowych powodów wdrażania zadań DNS należą:

- **Wysoka dostępność aplikacji** Serwer DNS przekierowuje klienty do punktów końcowych dla aplikacji, na przykład na podstawie czynników wysokiej dostępności w klastrze typu failover.
- **Zarządzanie ruchem** Serwer DNS przekierowuje klienty do najbliższego serwera lub centrum danych.
- **Podział DNS** Serwer DNS odpowiada klientom na podstawie tego, czy klient jest zewnętrzny czy wewnętrzny w intranecie naszej organizacji.
- **Filtrowanie** Serwer DNS blokuje zapytania DNS, jeśli pochodzą ze złośliwych hostów.
- **Techniki śledcze** Serwer DNS przekierowuje złośliwe klienty DNS do pułapki zamiast do hosta, do którego próbują dotrzeć.
- **Przekierowanie oparte na godzinach** Serwer DNS przekierowuje klienty do serwerów lub centrów danych na podstawie wskazanych godzin.

Aby implementować zasady DNS, trzeba korzystać z poleceń Windows PowerShell. Najpierw trzeba jednak sklasyfikować grupy rekordów w strefie DNS, klienty DNS w określonej sieci lub inne charakterystyki, które pomogą zidentyfikować klienty DNS. Do scharakteryzowania swoich klientów DNS można używać następujących obiektów DNS:

- **Podsieć klienta** Podsieć IPv4 lub IPv6 zawierająca klienty DNS.
- **Zakres rekurencji** Niepowtarzalna instancja grupy ustawień, które sterują rekurencją serwera DNS.
- **Zakresy obszarów** Zawiera własny zestaw rekordów zasobów DNS. Rekord może istnieć w kilku zakresach, a każdy ma inny adres IP zależnie od zakresu. Strefy DNS mogą mieć kilka zakresów dla stref.

Aby wdrożyć zasady DNS, trzeba najpierw zdefiniować jeden lub więcej powyższych obiektów, aby sklasyfikować swoje klienty i zakresy DNS.

1. Na przykład, aby utworzyć podsieć dla klientów DNS w Nowym Jorku, korzystamy z następującego polecenia:

   ```
   Add-DnsServerClientSubnet -Name "NYCSubnet" -IPv4Subnet "172.16.0.0/24"
   ```

2. Na podstawie adresów podsieci IPv4 lub IPv6 trzeba utworzyć wiele obiektów podsieci klientów.
3. Następnie, korzystając z poniższego polecenia, utwórz zakres obszaru DNS dla klientów DNS z Nowego Jorku:

   ```
   Add-DnsServerZoneScope -ZoneName "Adatum.com" -Name "NYCZoneScope"
   ```

4. Znów trzeba utworzyć wiele zakresów stref według własnych wymagań.
5. Dalej, aby utworzyć rekord z określonym adresem IP dla klientów w zakresie strefy New York City, uruchom następujące polecenie:

   ```
   Add-DnsServerResourceRecord -ZoneName "Adatum.com" -A -Name "www"
   -IPv4Address "172.16.0.41" -ZoneScope "NYCZoneScope"
   ```

6. Na koniec utwórz zasadę, która instruuje serwer DNS, aby odpowiadał na podstawie wcześniej zdefiniowanych czynników:

   ```
   Add-DnsServerQueryResolutionPolicy -Name "NYCPolicy" -Action ALLOW
   -ClientSubnet "eq,NYCSubnet" -ZoneScope "NYCZoneScope,1" -ZoneName
   "Adatum.com"
   ```

Teraz, jeśli klient w podsieci New York prosi serwer DNS o adres IPv4 hosta www.adatum.com host, serwer DNS odpowiada adresem IP 172.16.0.41. Jeśli tworzymy inne podsieci i zakresy stref dla innych lokalizacji, możemy nakazać serwerowi DNS, aby odpowiadał przy użyciu innego adresu IP w przypadku zapytań klientów z innych lokalizacji.

Dodatkowe materiały Przegląd zasad DNS

Więcej informacji na temat konfigurowania zasad DNS można znaleźć w witrynie Microsoft TechNet, pod adresem *https://technet.microsoft.com/windows-server-docs/networking/dns/deploy/dns-policies-overview*.

Konfigurowanie delegowanego administrowania

Następujące grupy mają w organizacji możliwości administrowania serwerami DNS:

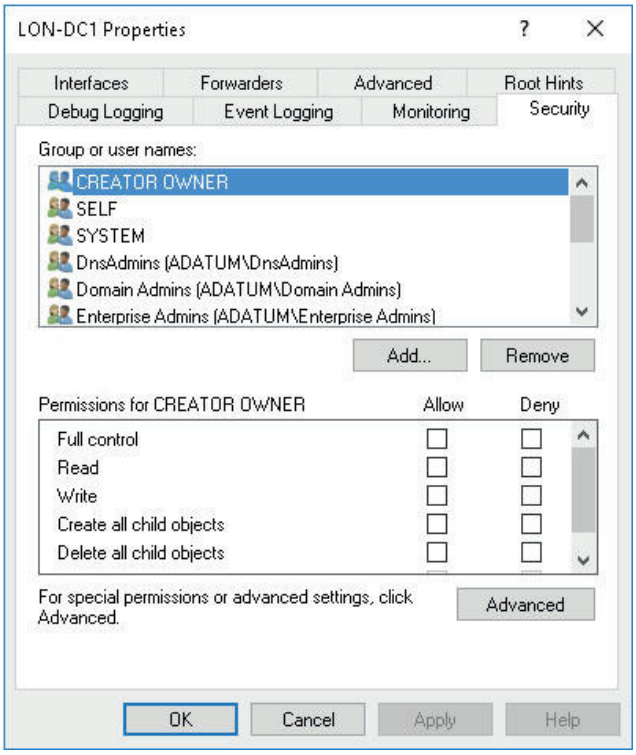
- **Domain Admins (Administratorzy domeny)** Mają pełne uprawnienia do zarządzania wszystkimi aspektami serwerów DNS w ich domenie głównej.

- **Enterprise Admins (Administratorzy przedsiębiorstwa)** Mają pełne uprawnienia do zarządzania wszystkimi aspektami serwerów DNS w każdej domenie w naszym lesie AD DS.
- **DnsAdmins (Administratorzy DNS)** Mogą przeglądać i modyfikować wszystkie dane i ustawienia DNS oraz konfiguracje serwera DNS w ich domenie głównej.

W sieci małej lub średniej wielkości, na ogół akceptuje się używanie wartości domyślnych. Jednak w środowiskach dużych sieci korzystne może być przekazanie administracji związanej z zarządzaniem DNS innym zespołom.

Po podjęciu decyzji o przekazaniu administracji serwerem DNS innemu użytkownikowi lub grupie można dodać tego użytkownika lub grupę do grupy DnsAdmins dla danej domeny w lesie. Do modyfikacji członkostwa w tej grupie można użyć Active Directory Users and Computers lub cmdletu Windows PowerShell, Add-ADGroupMember.

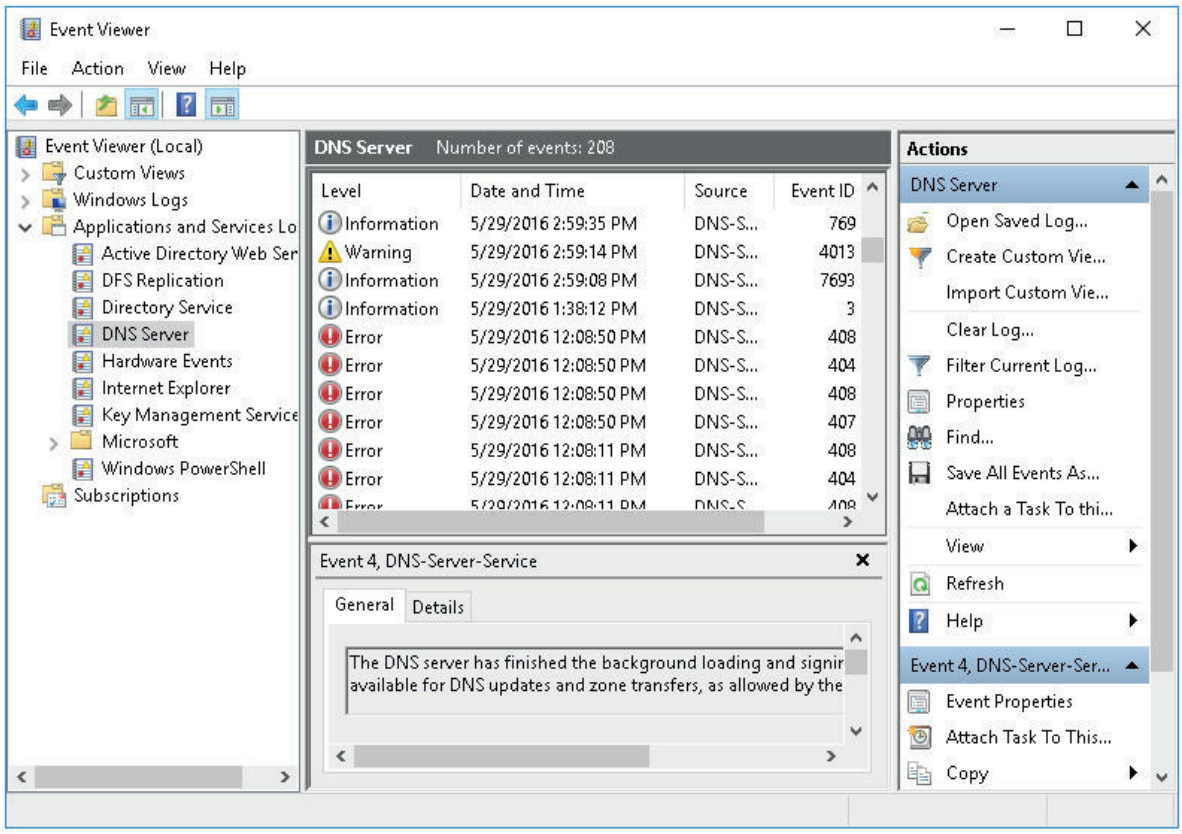
Aby skonfigurować uprawienia administracyjne DNS, klikamy prawym przyciskiem myszy odpowiedni serwer DNS lub obszar DNS w konsoli DNS Manager, a następnie klikamy **Properties**. W oknie dialogowym Server Properties lub w oknie Zone Properties (Właściwości strefy), na karcie Security (Zabezpieczenia), można przeglądać i modyfikować uprawnienia dla serwera lub strefy, jak pokazano na rysunku 1-12.



Rysunek 1-12 Delegowanie administracji DNS

Konfigurowanie rejestrowania DNS

Uaktywnianie rejestrowania może być bardzo przydatne do proaktywnego monitorowania, szczególnie gdy analizujemy słabą wydajność lub błędne i nieoczekiwane działanie usługi. Domyślnie DNS rejestruje zdarzenia w dzienniku serwera DNS, który można przeglądać za pomocą konsoli Event Viewer (Podgląd zdarzeń). Dziennik serwera DNS znajduje się w węźle Application and Services Logs (Dzienniki aplikacji i usług), jak to pokazano na rysunku 1-13.



Rysunek 1-13 Przeglądanie dziennika zdarzeń serwera DNS

Dziennik zawiera typowe zdarzenia związane z DNS, takie jak rozpoczęcie i zakończenie usługi, zdarzenia podpisywania stref, zmiany konfiguracji oraz typowe ostrzeżenia i błędy.

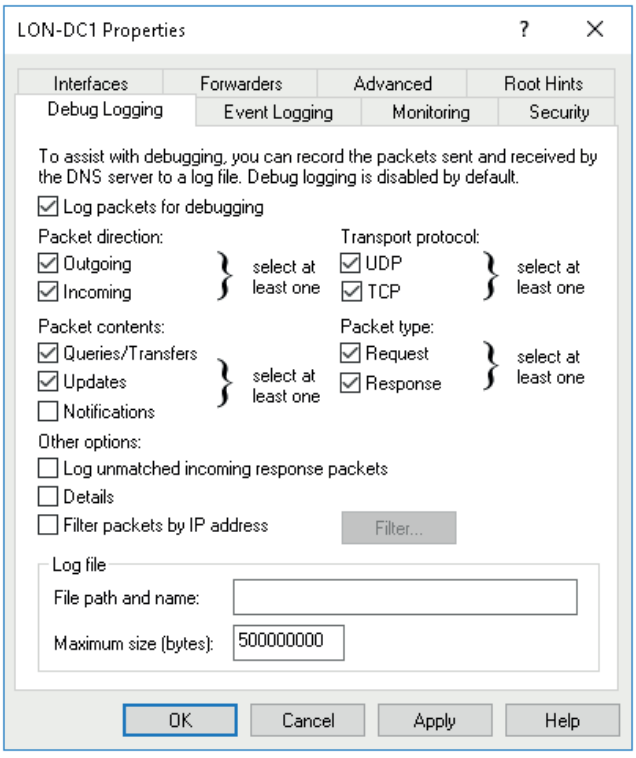
Można również włączyć bardziej szczegółowe rejestrowanie za pomocą rejestrowania *debugowania*. Należy jednak zachować ostrożność przy włączaniu rejestrowania *debugowania*, ponieważ może to nałożyć na serwer DNS obciążenie, które będzie mieć wpływ na dostarczanie usługi. Rejestrowania *debugowania* dostarcza następujące dodatkowe informacje szczegółowe:

- Kierunek pakietu (Outgoing lub Incoming – wychodzący lub wchodzący)
- Zawartość pakietu (Queries/Transfers, Updates lub Notifications – zapytania/transfery, aktualizacje lub powiadomienia)

- Protokół transportowy (UDP lubTCP)
- Typ pakietu (Request lub Response – żądanie lub odpowiedź)
- Filtrowanie pakietów według adresu IP
- Nazwa i lokalizacja pliku dziennika, domyślnie to katalog %systemroot%\System32\DNS
- Maksymalny limit rozmiaru pliku dziennika

Aby włączyć rejestrowanie debugowania, należy z konsoli DNS Manager wykonać następujące kroki:

1. Kliknij prawym przyciskiem myszy odpowiedni serwer DNS, a następnie kliknij Properties.
2. W oknie dialogowym Server Properties kliknij zakładkę Debug Logging (Rejestrowanie debugowania), jak to pokazano na rysunku 1-14, zaznacz pole wyboru Log Packets For Debugging (Rejestruj pakiety do debugowania) wybierz zdarzenia, dla których serwer DNS ma zapisywać wyniki debugowania, a następnie kliknij OK.



Rysunek 1-14 Konfigurowanie rejestrowania debugowania DNS

Wdrażanie dostrajania wydajności DNS

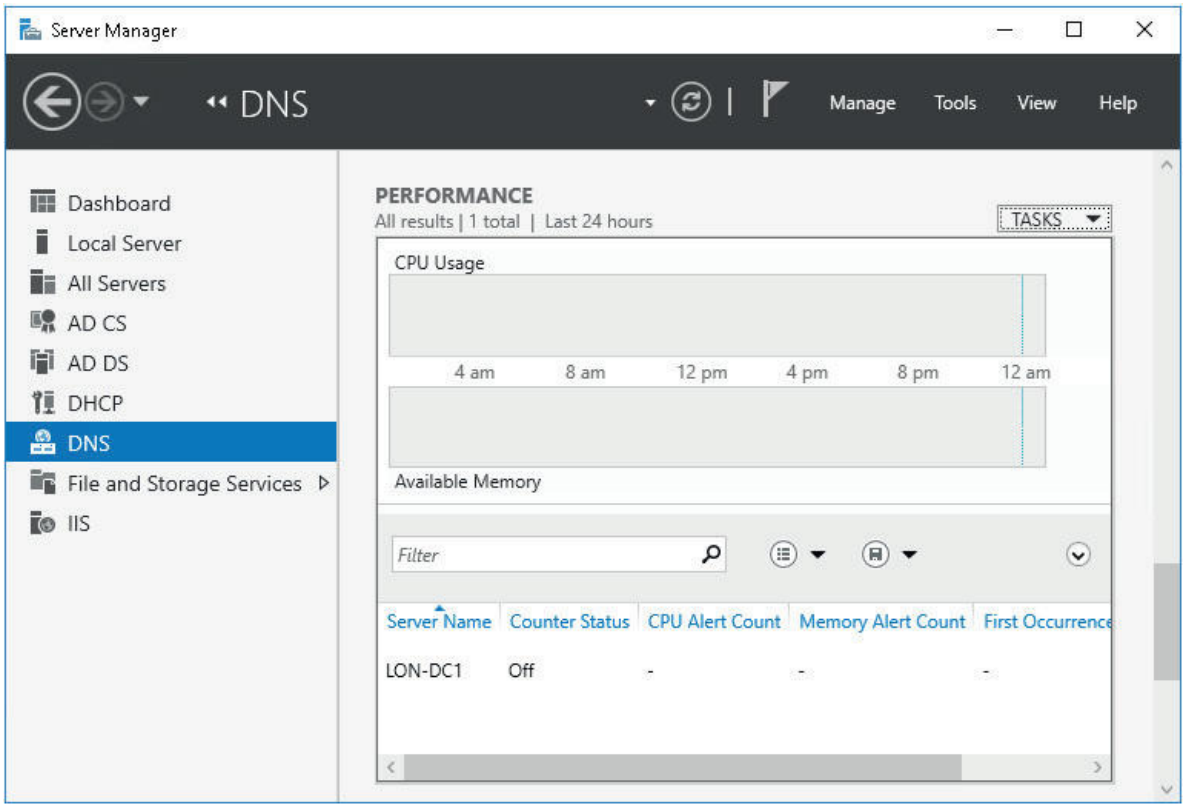
Na rolę serwera DNS, tak jak na inne role i usługi, może mieć wpływ słaba wydajność naszego serwera. Słaba wydajność jest często spowodowana brakiem zasobów serwera: pamięci, procesora, niewystarczającą przepływność dysku i przepustowość sieci. Do zmierzenia, czy w naszym serwerze te zasoby są wystarczające oraz ustalenia, które z nich powodują wąskie gardło, można użyć narzędzi ogólnych, takich jak Performance Monitor (Monitor wydajności).

Gdy jeden lub większa liczba tych zasobów jest niewystarczająca, tworzy się wąskie gardło wydajności. Rozwiązaniem jest określenie, który zasób tworzy wąskie gardło i optymalizacja tego zasobu, często poprzez dodanie większej jego ilości. Alternatywą jest dystrybucja obciążenia poprzez dodanie dodatkowych serwerów DNS.

DODATKOWE MATERIAŁY **Performance Monitor w systemie Windows**

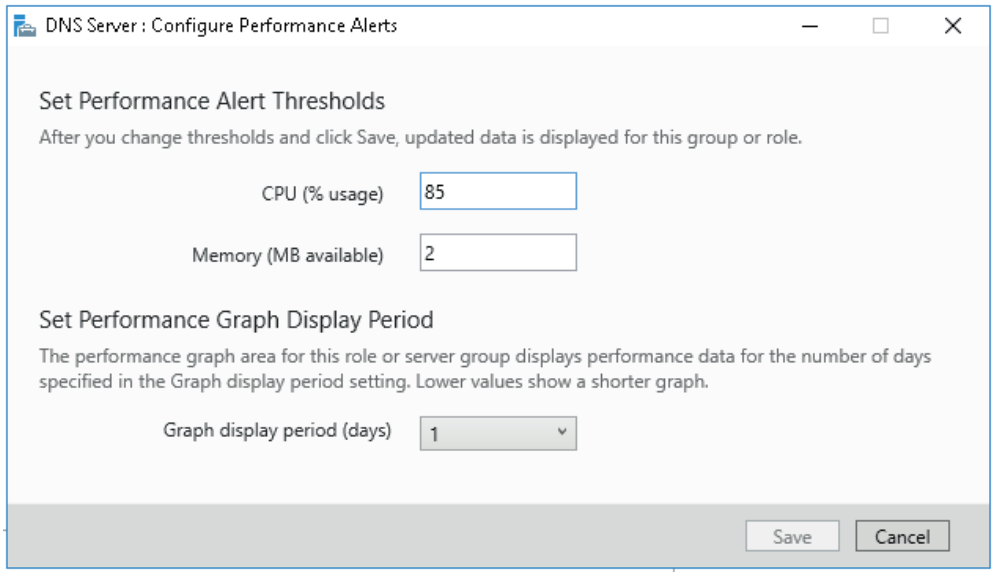
Więcej informacji na temat używania przystawki Performance Monitor (Monitor wydajności) można znaleźć w witrynie Microsoft TechNet, pod adresem *https://technet.microsoft.com/library/cc749249(v=ws.11).aspx*.

Dwoma najważniejszymi zasobami roli serwera DNS są procesor oraz pamięć. Karta DNS w konsoli Server Manager zawiera okienko Performance, którego można używać do monitorowania tych dwóch krytycznych zasobów, jak pokazano na rysunku 1-15.



RYSUNEK 1-15 Monitorowanie wydajności DNS

Aby rozpocząć monitorowanie tych zasobów, klikamy **Tasks** (Zadania), a następnie **Configure Performance Alerts** (Konfiguruj alerty wydajności). W oknie dialogowym DNS Server: Configure Performance Alerts można skonfigurować progi dla alertów zarówno dla procesora (użycie w procentach), jak i pamięci (liczba dostępnych MB), jak to pokazano na rysunku 1-16. Klikamy **Save** (Zapisz), gdy będziemy gotowi.



Rysunek 1-16 Konfigurowanie alertów wydajności DNS

Poza tymi podstawowymi charakterystykami wydajności serwera, można tak skonfigurować serwer DNS, aby pomagał optymalizować czas odpowiedzi DNS. Na przykład pozwolenie na wykonywanie rekurencji przez serwer DNS pociąga za sobą nałożenie na niego dodatkowego obciążenia, gdy nie można dostarczyć autorytatywnej odpowiedzi na zapytanie klienta. Wyłączając rekurencję, można zredukować obciążenie na danym serwerze DNS, ale kosztem niemożności jej użycia. Podobnie, usunięcie wskazówek dotyczących serwerów głównych chroni serwer przed zapytaniami klientów związanymi z internetowym drzewem DNS, co redukuje obciążenie.

Wiele z podejmowanych decyzji, związanych z wydajnością, ma wpływ na sposób funkcjonowania rozpoznawania nazw w naszej organizacji. To oznacza, że trzeba starannie rozważyć ten wpływ. Planując optymalizację DNS, należy utworzyć standardowy serwer DNS, a następnie monitorować jego wydajność dla typowego obciążenia zapytaniami. W tym celu można użyć takich narzędzi jak standardowe narzędzie *dnsperf* i określić optymalną liczbę zapytań na sekundę dla standardowego serwera.

Dodatkowe materiały **Wydajność rozpoznawania nazw autorytatywnego serwera Windows DNS**

Poniżej podano link do artykułu na blogu TechNet, który zawiera procedurę testową do optymalizacji serwerów Microsoft DNS: *https://blogs.technet.microsoft.com/networking/2015/08/13/name-resolution-performance-of-authoritative-windows-dns-server-2012-r2/*.

Wdrażanie globalnych ustawień DNS oraz konfigurowanie ustawień globalnych za pomocą Windows PowerShell

W tym rozdziale poznaliśmy już wiele zadań związanych z wdrażaniem i konfiguracją na serwerach DNS, które można wykonać za pomocą Windows PowerShell. W części „Zagadnienie 1.2: Tworzenie i konfigurowanie stref i rekordów DNS", analizujemy więcej cmdletów Windows PowerShell dla roli serwera DNS.

Dodatkowe materiały Cmdlety serwera DNS

Pełną listę cmdletów Windows PowerShell dla serwera DNS można przejrzeć w witrynie Microsoft TechNet, pod adresem h*ttps://technet.microsoft.com/library/jj649850.aspx*.

Zagadnienie 1.2: Tworzenie i konfigurowanie stref i rekordów DNS

Wprawdzie system nazw domen DNS opiera się na koncepcji domen i poddomen, informacje o tych domenach i poddomenach oraz o relacjach między nimi przechowujemy w strefach DNS. Strefę DNS można traktować jako jedną lub więcej domen i poddomen z naszej infrastruktury DNS.

Na przykład domeny Adatum.com i sales.adatum.com mogą być razem przechowywane w strefie DNS o nazwie Adatum.com, lub też sales.adatum.com może być przechowywane w wyznaczonej strefie o nazwie sales.adatum.com, podczas gdy domena nadrzędna, Adatum.com, jest przechowywana w swojej własnej strefie.

Strefę można przechowywać w plikach na serwerze DNS lub w bazie danych AD DS (Active Directory Domain Services). Ważne jest posiadanie wiedzy, jak i kiedy tworzyć strefy podstawową i pomocniczą, strefy delegowane, strefy zintegrowane z usługami AD DS oraz strefy skrótowe (ang. stub zones).

Korzystanie ze stref DNS

Strefy są wykorzystywane przez serwery DNS do odpowiadania na zapytania klientów DNS. Zazwyczaj zapytania klientów wymagają wyszukiwania do przodu, a nazwa hosta musi być odwzorowana na odpowiedni adres IPv4 (Internet Protocol Version 4) lub IPv6 (Internet Protocol Version 6). Zapytania z wyszukiwaniem do przodu są rozwiązywane poprzez odwołanie do stref wyszukiwania do przodu *(ang. forward lookup zones)*.

Strefy wyszukiwania do przodu zawierają różnorodne rodzaje rekordów DNS (omówione w następnym punkcie) i obejmują:

- Rekordy hosta (A)