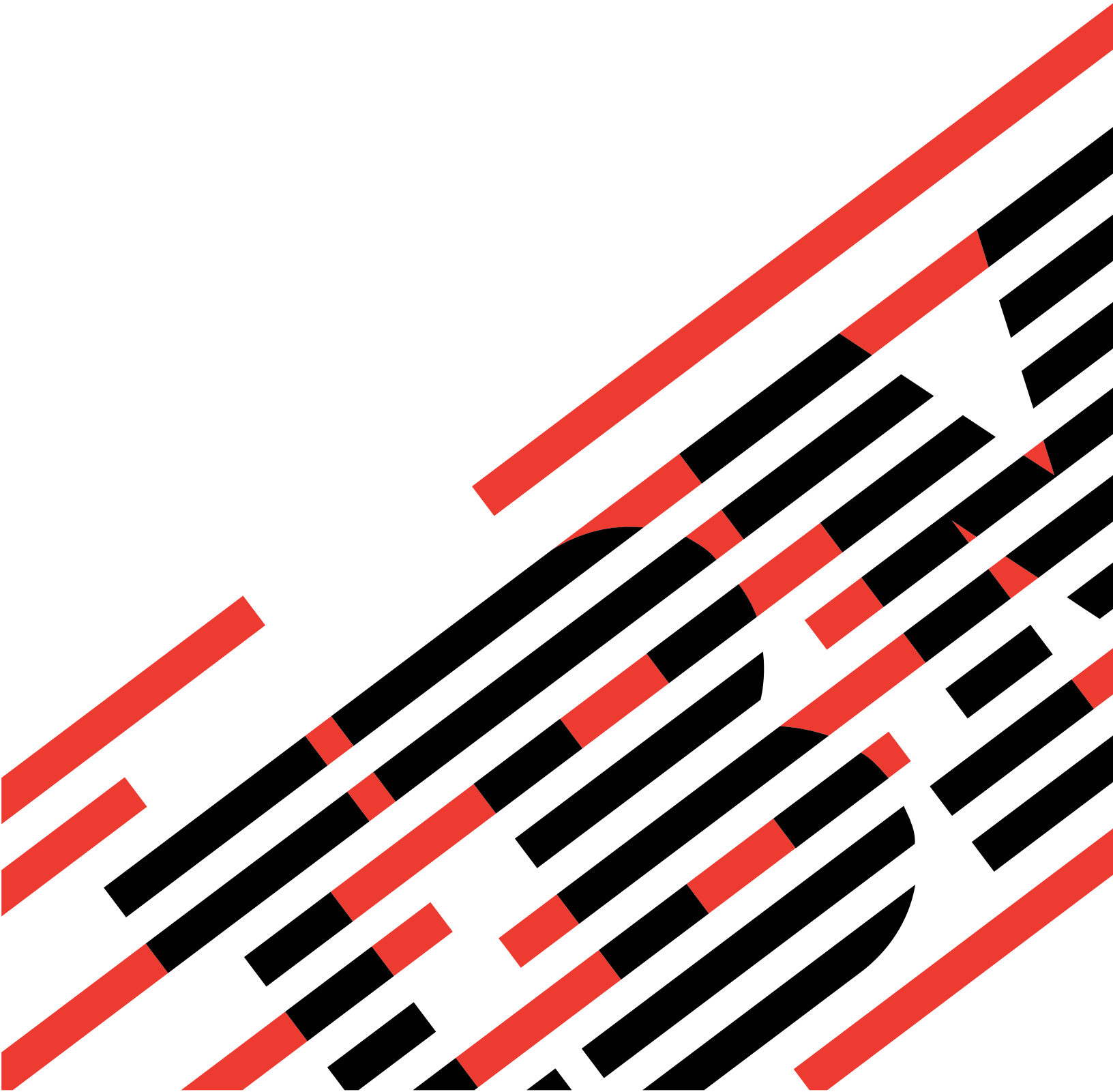
IBM

eserver

iSeries

# DNS

*Wersja 5 Wydanie 3*



IBM

@server

iSeries

# DNS

*Wersja 5 Wydanie 3*

**Uwaga**

Przed wykorzystaniem tych informacji i produktu, którego dotyczą, należy przeczytać informacje zawarte w sekcji “Uwagi”, na stronie 37.

**Wydanie piąte (sierpień 2005)**

Niniejsze wydanie dotyczy wersji 5, wydania 3, modyfikacji 0 produktu IBM Operating System/400 (numer produktu 5722-SS1) i wszystkich kolejnych wydań i modyfikacji, o ile w nowych wydaniach nie będzie stwierdzone inaczej. Wersja ta nie może być uruchamiana na wszystkich modelach komputerów z procesorem RISC, jak również na modelach CISC.

# Spis treści

# DNS

System nazw domen (Domain Name System - DNS) to rozproszony system baz danych służący do zarządzania nazwami hostów i przypisanymi im adresami protokołu Internet Protocol (IP). Dzięki zastsowaniu usług DNS użytkownicy mogą zamiast adresów IP (xxx.xxx.xxx.xxx) używać prostych nazw, jak np. ″www.jkltoys.com″. Pojedynczy serwer DNS może być odpowiedzialny za znajomość nazw hostów i adresów IP dla niewielkiej części strefy, ale serwery DNS mogą ze sobą współpracować w celu odwzorowania wszystkich nazw domen na odpowiadające im adresy IP. To dzięki współpracującym ze sobą serwerom DNS komputery mogą się ze sobą komunikować poprzez Internet.

W wersji 5 wydanie 1 (V5R1), usługi DNS są oparte na standardowej implementacji DNS, znanej pod nazwą BIND (Berkeley Internet Name Domain) w wersji 8. W poprzednich wersjach systemu OS/400(R) usługi DNS wykorzystywały program BIND w wersji 4.9.3. Aby używać serwera DNS opartego na programie BIND 8, na serwerze iSeries(TM) musi być zainstalowana opcja OS/400 33, Portable Application Solutions Environment (PASE). Jeśli na serwerze nie jest zainstalowane środowisko PASE, można w dalszym ciągu używać poprzedniej wersji serwera DNS dla OS/400, wykorzystującego program BIND 4.9.3. Jednak migracja do programu BIND 8 udostępnia ulepszone funkcjonowanie oraz zapewnia lepszą ochronę serwera DNS.

**Uwaga:** W tym dokumencie opisane są nowe funkcje związane z programem BIND 8. Jeśli na komputerze nie jest zainstalowane środowisko PASE i nie można na nim uruchomić serwera DNS wykorzystującego program BIND 8, należy zapoznać się z informacjami dotyczącymi serwera DNS wykorzystującego program BIND 4.9.3 zawartymi w dokumencie V4R5 DNS Information Center  (około 357 kB).

- W sekcji “Drukowanie tego dokumentu” na stronie 2 opisano, jak pobrać lub wydrukować dokument poświęcony usługom DNS.

**Podstawy DNS**
Wymienione niżej sekcje mają za zadanie pomóc w zrozumieniu podstaw usług DNS w systemie iSeries.

Sekcja **“Przykłady konfiguracji usług DNS” na stronie 2** zawiera schematy i objaśnienia dotyczące sposobu działania systemu DNS.

Sekcja **“Koncepcje systemu DNS” na stronie 10** opisuje obiekty i procesy wykorzystywane w funkcjonowaniu systemu DNS.

Sekcja **“Planowanie systemu DNS” na stronie 20** zawiera wskazówki pomocne podczas tworzenia planu konfiguracji usług DNS.

**Korzystanie z systemu DNS**
Poniższe sekcje zostały napisane z myślą o asystowaniu użytkownikowi podczas konfigurowania usług DNS i zarządzania nimi w systemie iSeries. W sekcjach tych opisano również, w jaki sposób wykorzystać zalety dostępnych obecnie nowych funkcji.

**“Wymagania systemu DNS” na stronie 22**
Sekcja ta przedstawia wymagania programowe, które muszą być spełnione, aby uruchomić usługi DNS na serwerze iSeries.

**“Konfigurowanie DNS” na stronie 23**
W tej sekcji opisano sposób użycia programu iSeries Navigator do skonfigurowania serwera nazw i do tłumaczenia zapytań skierowanych poza domenę.

**“Administrowanie systemem DNS” na stronie 27**
Sekcja ta zawiera informacje dotyczące weryfikowania działania systemu DNS, monitorowania jego wydajności i obsługiwania danych i plików systemu DNS.

**“Rozwiązywanie problemów z systemem DNS” na stronie 33**
W tej sekcji przedstawiono ustawienia protokołowania i debugowania konfiguracji DNS, które mogą pomóc rozwiązać problemy z serwerem DNS.

W przypadku pytań, na które nie można znaleźć odpowiedzi w Centrum informacyjnym, należy skorzystać z sekcji “Inne informacje dotyczące DNS” na stronie 35, która zawiera wykaz innych zasobów i materiałów informacyjnych.

## Drukowanie tego dokumentu

Aby przejrzeć lub pobrać wersję PDF, wybierz DNS (około 357 kB).

Aby zapisać plik PDF na stacji roboczej w celu jego dalszego wykorzystania:

1. Otwórz PDF w przeglądarce (kliknij powyższy odsyłacz).
2. W menu przeglądarki kliknij **Plik**.
3. Wybierz **Zapisz jako...**
4. Przejdź do katalogu, w którym chcesz zapisać plik PDF.
5. Kliknij **Zapisz**.

Jeśli do przeglądania lub drukowania pobranych plików potrzebny jest program Adobe Acrobat Reader, jego kopię można pobrać z serwisu WWW firmy Adobe (www.adobe.com/products/acrobat/readstep.html) .

## Przykłady konfiguracji usług DNS

DNS to rozproszony system baz danych służący do zarządzania nazwami hostów i przypisanymi im adresami protokołu IP. Poniższe przykłady mają pomóc w zrozumieniu sposobu działania systemu DNS i w wykorzystaniu go we własnej sieci. W przykładach opisano różne konfiguracje i powody, dla których zostały one wybrane. Przykłady zawierają również odsyłacze do pokrewnych koncepcji, które mogą być pomocne w zrozumieniu przedstawionych ilustracji.

**“Przykład: serwer DNS dla intranetu”**
Przedstawia prostą podsieć z serwerem DNS do użytku wewnętrznego.

**“Przykład: serwer DNS z dostępem do Internetu” na stronie 4**
Przedstawia prostą podsieć z serwerem DNS połączonym bezpośrednio z Internetem.

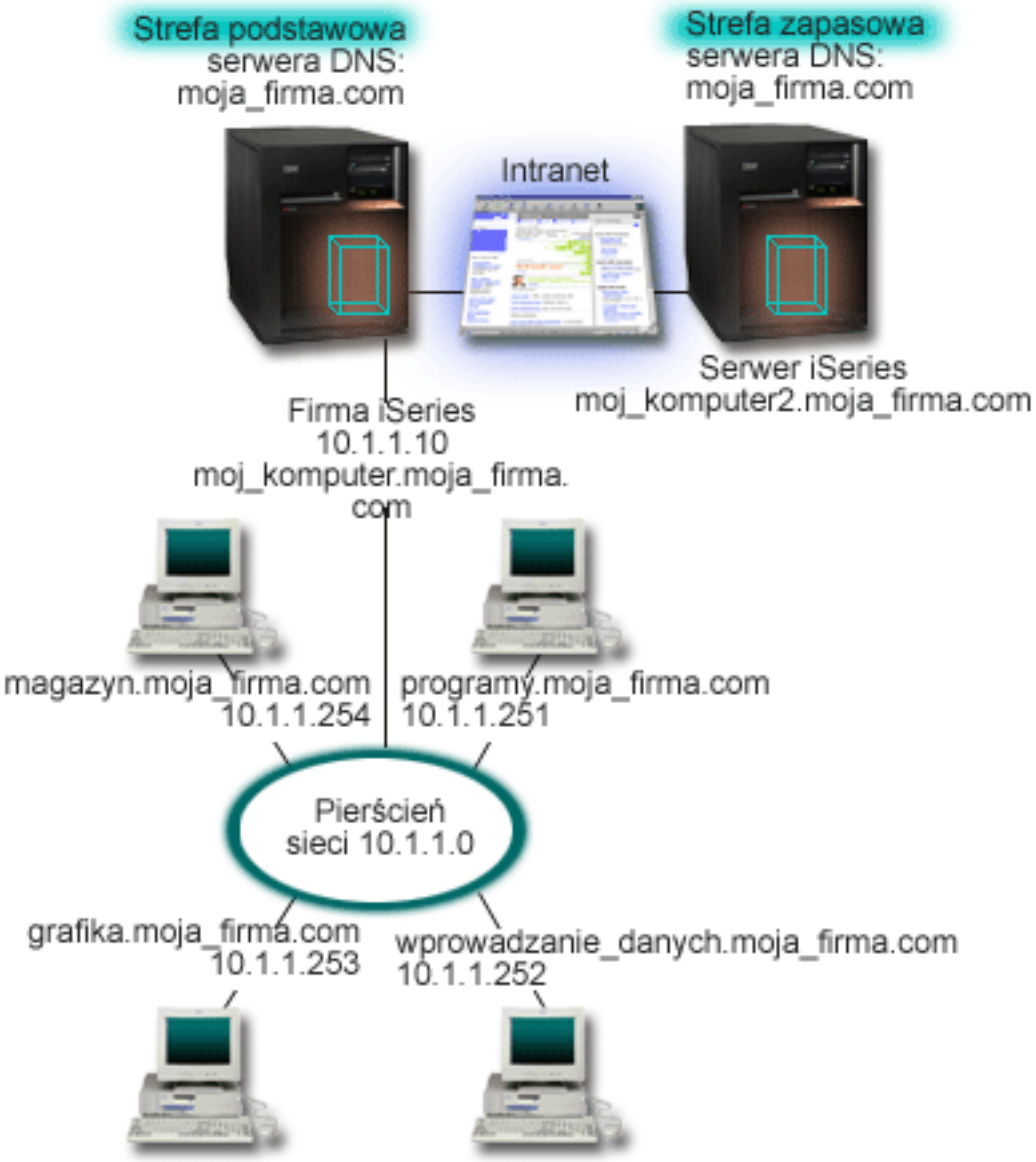
**“Przykład: serwery DNS i DHCP na tym samym serwerze iSeries(TM)” na stronie 6**
Opisuje konfigurację serwerów DNS i DHCP na tym samym serwerze. Konfigurację taką można wykorzystywać do dynamicznej aktualizacji danych strefy DNS, kiedy serwer DHCP przypisuje hostom adresy IP. W przypadku, kiedy serwer DHCP działa na innym serwerze iSeries, dodatkowe wymagania konfiguracyjne dla serwera DHCP zawiera sekcja Przykład: serwery DNS i DHCP na różnych serwerach iSeries.

**“Przykład: podział systemu DNS za firewallem” na stronie 8**
Przedstawia serwer DNS działający za firewallem, który chroni dane wewnętrzne od strony Internetu i jednocześnie udostępnia użytkownikom wewnętrznym dane w Internecie.

## Przykład: serwer DNS dla intranetu

Poniższa ilustracja przedstawia serwer DNS działający na serwerze iSeries(TM) i obsługujący sieć wewnętrzną. Ta pojedyncza instancja serwera DNS została skonfigurowana do nasłuchiwania zapytań na wszystkich adresach IP interfejsu. Przedstawiony serwer jest podstawowym serwerm nazw dla strefy ″mycompany.com″.

**Rysunek 1. Serwer DNS dla intranetu.**




Każdy host w strefie ma adres IP i nazwę domenową. Administrator musi ręcznie zdefiniować hosty w danych strefy DNS, tworząc rekordy zasobów. Rekordy odwzorowania adresów (A) odwzorowują nazwę maszyny na przypisany jej adres IP. Dzięki tym rekordom inne hosty w sieci mogą kierować do serwera DNS zapytania w celu znalezienia adresu IP przypisanego do konkretnej nazwy hosta. Rekordy wskaźników wyszukiwania odwrotnego (PTR) odwzorowują adresy IP poszczególnych maszyn na przypisane im nazwy. Te rekordy z kolei pozwalają innym hostom w sieci kierować do serwera DNS zapytania w celu znalezienia nazwy odpowiadającej adresowi IP.

Oprócz rekordów typu A i PTR, serwer DNS obsługuje wiele innych typów rekordów zasobów, które mogą być niezbędne w zależności od innych aplikacji TCP/IP uruchamianych w intranecie. Jeśli na przykład w sieci działa wewnętrzny system poczty elektronicznej, do bazy DNS należy wpisać rekordy wymienników poczty (MX), aby serwer SMTP mógł skierować do serwera DNS zapytanie o systemy, w których działają serwery poczty.

Jeśli ta mała sieć byłaby częścią dużej sieci intranetowej, konieczne byłoby zdefiniowanie wewnętrznych serwerów głównych.

**Serwery zapasowe**
Serwery zapasowe pobierają dane strefy z serwera autorytatywnego. Serwery zapasowe uzyskują dane strefy poprzez przesyłanie strefowe z serwera autorytatywnego. Podczas uruchamiania, serwer zapasowy wysyła do podstawowego serwera nazw żądanie wszystkich danych dla określonej domeny. Ponadto zapasowy serwer nazw żąda zaktualizowanych danych z serwera podstawowego, gdy zostanie powiadomiony o zmianach przez podstawowy serwer nazw (jeśli używana jest funkcja NOTIFY) lub gdy na podstawie zapytań kierowanych do podstawowego serwera nazw wykryje zmianę danych.
Na powyższym rysunku serwer myiseries jest częścią intranetu. Inny serwer iSeries, myiseries2, został skonfigurowany jako zapasowy serwer DNS dla strefy mycompany.com. Serwer zapasowy pozwala zrównoważyć obciążenie serwerów, a także stanowi zabezpieczenie na wypadek awarii serwera podstawowego. Do dobrej praktyki administratora należy skonfigurowanie przynajmniej jednego serwera zapasowego dla każdej strefy.

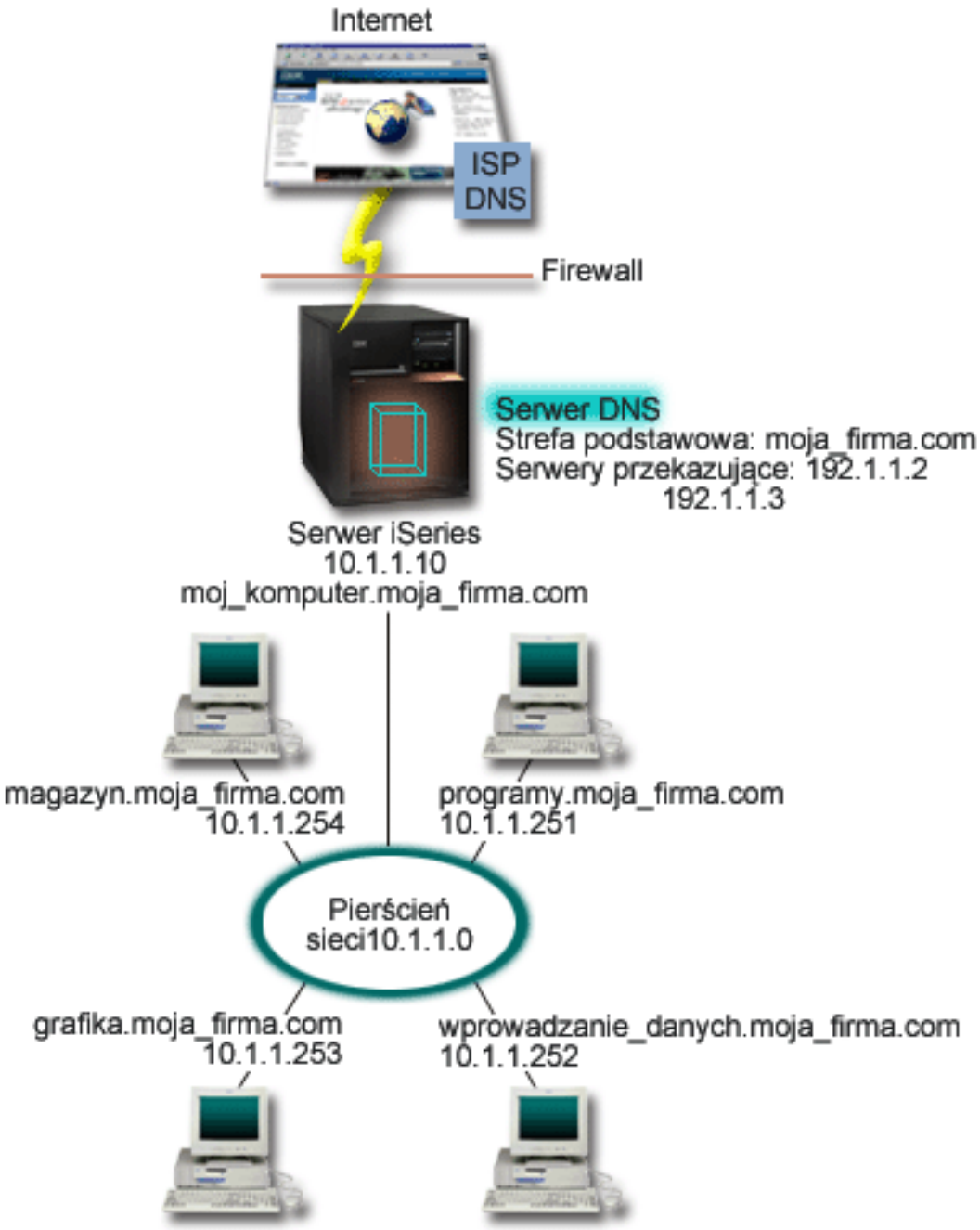
Więcej informacji dotyczących obiektów przedstawionych w tym przykładzie można znaleźć w następujących sekcjach:

- “Podstawy DNS” na stronie 11, gdzie wyjaśniono, czym jest DNS i jak działa. W sekcji tej zdefiniowano również różne typy stref, które można określić dla serwera DNS.
- “Rekordy zasobów DNS” na stronie 16, w której opisano, w jaki sposób rekordy zasobów są wykorzystywane przez system DNS.

## Przykład: serwer DNS z dostępem do Internetu

Poniższa ilustracja przedstawia ten sam przykład sieci co w sekcji “Przykład: serwer DNS dla intranetu” na stronie 2, z tym, że tutaj firma ma połączenie z Internetem. W niniejszym przykładzie firma ma dostęp do Internetu, ale firewall został tak skonfigurowany, aby zablokować ruch przychodzący z Internetu do sieci.

**Rysunek 1. Serwer DNS z dostępem do Internetu.**




W celu przetłumaczenia adresów internetowych, należy wykonać przynajmniej jedną z poniższych czynności:

**Zdefiniować Internetowe serwery główne**
Internetowe serwery główne można załadować automatycznie, ale może być konieczna aktualizacja listy. Serwery te są pomocne podczas tłumaczenia adresów spoza lokalnej strefy. Instrukcje dotyczące uzyskania danych o Internetowych serwerach głównych zawiera sekcja “Dostęp do zewnętrznych danych DNS” na stronie 27.

**Włączyć przekazywanie**
Można tak skonfigurować funkcję przekazywania, aby przekazywała zapytania o strefy spoza mycompany.com do zewnętrznych serwerów DNS, na przykład do serwerów administrowanych przez

dostawcę usług internetowych (ISP). Aby włączyć wyszukiwanie na serwerach przekazujących i głównych, należy opcji **forward** nadać wartość **first**. Spowoduje to, że serwer będzie najpierw kierował zapytanie do serwera przekazującego, a dopiero gdy ten nie będzie w stanie przetłumaczyć adresu, zapytanie zostanie skierowane do serwera głównego.

Ponadto, mogą być wymagane następujące zmiany konfiguracji:

**Przypisanie niezastrzeżonych adresów IP**
W powyższym przykładzie użyto adresów 10.x.x.x. Jednak są to adresy zastrzeżone i nie mogą być używane poza intranetem. Użyte adresy mają charakter przykładowy i w konkretnej konfiguracji mogą być inne, na przykład określone przez dostawcę usług internetowych.

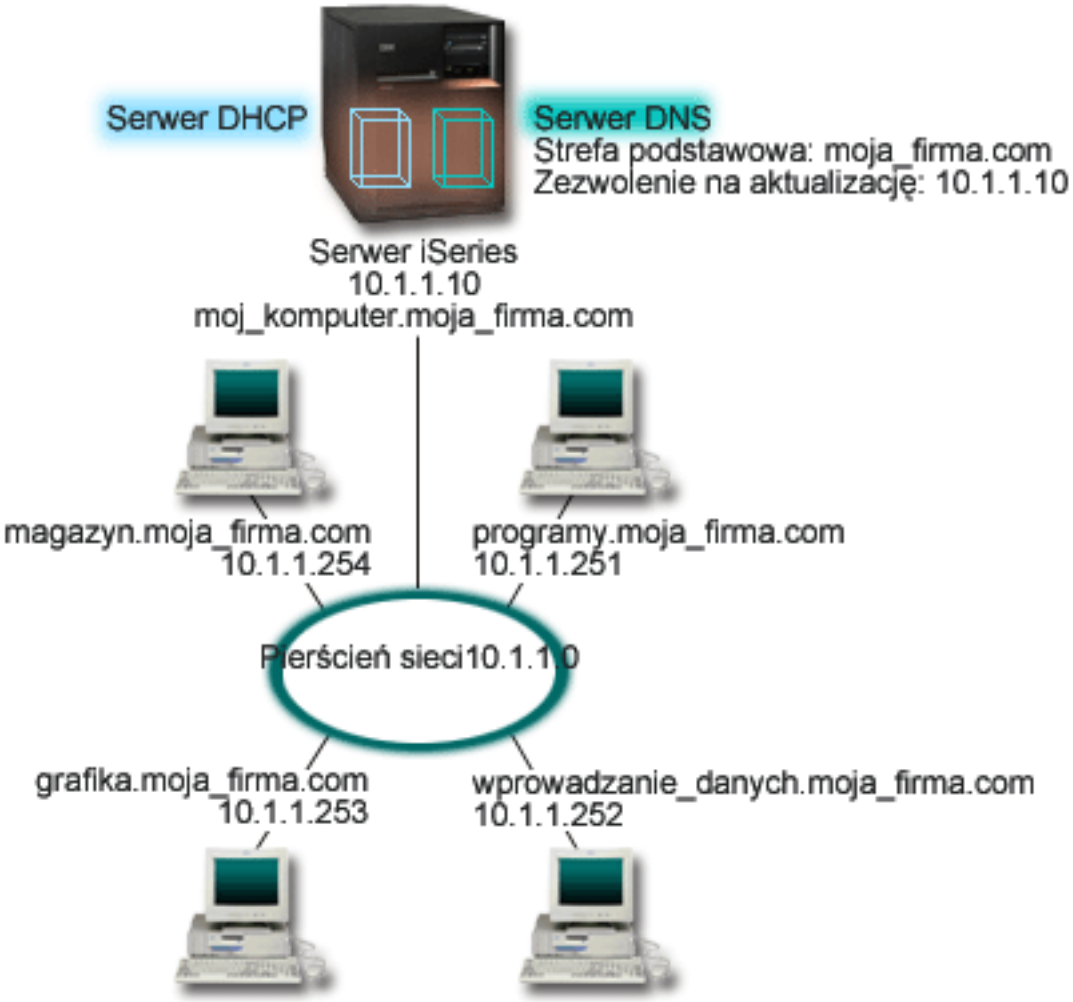
**Zarejestrowanie nazwy domeny**
Aby być widocznym w Internecie, należy “Konfigurowanie własnej domeny DNS” na stronie 14, o ile nie zostało to już zrobione.

**Uruchomienie firewalla**
Nie zaleca się bezpośredniego połączenia serwera DNS z Internetem. Należy skonfigurować firewall lub podjąć inne środki w celu zabezpieczenia serwera iSeries(TM). Więcej informacji na ten temat można znaleźć w sekcji IBM(R) Secureway: iSeries i Internet w Centrum informacyjnym.

## Przykład: serwery DNS i DHCP na tym samym serwerze iSeries(TM)

Poniższy rysunek przedstawia małą podsieć z jednym serwerem iSeries, działającym jednocześnie jako serwer DHCP i serwer DNS dla czterech klientów. Przyjmijmy, że w tym środowisku roboczym na klientach obsługujących magazyn, wprowadzanie danych i zarząd tworzone są dokumenty z grafiką pochodzącą z serwera plików graficznych. Maszyny te łączą się z serwerem plików graficznych, odwzorowując sieciowy napęd dysków na nazwę hosta.

**Rysunek 1. Serwery DNS i DHCP na tym samym serwerze iSeries.**




Poprzednie wersje serwerów DHCP i DNS były od siebie niezależne. Jeśli serwer DHCP przypisał klientowi nowy adres IP, rekordy bazy DNS musiały być aktualizowane ręcznie przez administratora. W niniejszym przykładzie zmiana adresu IP serwera plików graficznych przez serwer DHCP spowodowałaby, że rekordy DNS zawierałyby nieaktualny adres IP serwera plików, przez co klienci tego serwera nie mogliby przypisać dysku sieciowego do nazwy hosta.

Używając dostępnego w wersji V5R1 serwera DNS opartego na programie BIND 8, można skonfigurować strefę DNS tak, aby akceptowała “Aktualizacje dynamiczne” na stronie 14 rekordów DNS związane ze sporadycznymi zmianami adresów przez serwer DHCP. Kiedy na przykład serwer plików graficznych odnawia dzierżawę adresu IP z serwera DHCP i uzyskuje nowy adres IP: 10.1.1.250, powiązane rekordy DNS zostają zaktualizowane dynamicznie. Pozwala to innym klientom bez przeszkód kierować do serwera DNS zapytania dotyczące serwera plików graficznych.

Aby skonfigurować strefę DNS tak, aby akceptowała dynamiczne aktualizacje, należy wykonać następujące zadania:

**Zidentyfikować strefę dynamiczną**
Nie można ręcznie aktualizować strefy dynamicznej podczas pracy serwera. Mogłoby to spowodować kolizję z przychodzącymi aktualizacjami dynamicznymi. Aktualizacji ręcznych można dokonywać tylko po zatrzymaniu serwera. Jednak gdy serwer zostaje zatrzymany, traci się wszelkie aktualizacje dynamiczne wysyłane przez serwer DHCP. Z tego powodu może być konieczne zdefiniowanie odrębnej strefy dynamicznej, w której konieczność dokonywania aktualizacji ręcznych będzie

minimalna. Więcej informacji dotyczących konfigurowania funkcji dynamicznej aktualizacji stref zawiera sekcja “Określanie struktury domeny” na stronie 21.

**Skonfigurować opcję zezwolenia na aktualizację**
Każda strefa ze skonfigurowaną opcją zezwolenia na aktualizację jest uważana za strefę dynamiczną. Opcja zezwolenia na aktualizację jest ustawiana dla każdej strefy oddzielnie. Aby zaakceptować dynamiczne aktualizacje strefy, opcja ta musi być w tej strefie włączona. W niniejszym przykładzie strefa mycompany.com miałaby włączoną opcję zezwolenia na aktualizację, ale inne strefy zdefiniowane na serwerze mogłyby być statyczne lub dynamiczne.

**Skonfigurować wysyłanie dynamicznych aktualizacji przez serwer DHCP**
Należy autoryzować serwer DHCP do aktualizacji rekordów DNS zgodnie z rozdzielanymi adresami IP. Więcej informacji na tem temat zawiera sekcja Konfigurowanie serwera DHCP pod kątem wysyłania dynamicznych aktualizacji DNS.

**Skonfigurować preferencje dotyczące aktualizacji dla serwera zapasowego**
Aby zapewnić aktualność danych przechowywanych na serwerze zapasowym, można na serwerze DNS skonfigurować funkcję NOTIFY, która wysyła do serwerów zapasowych strefy moja_firma.com komunikaty informujące o zmianie danych strefy. Należy również skonfigurować i włączyć przyrostowe przesyłanie strefowe (IXFR), co pozwoli serwerom zapasowym śledzić aktualizację i pobierać tylko zmienione dane strefy.

W przypadku, kiedy serwery DNS i DHCP działają na różnych serwerach iSeries, istnieją jeszcze pewne dodatkowe wymagania dotyczące konfiguracji serwera DHCP. Więcej informacji na ten temat zawiera sekcja Przykład: Serwery DNS i DHCP na różnych serwerach iSeries.

## Przykład: podział systemu DNS za firewallem

Poniższa ilustracja przedstawia prostą podsieć zabezpieczoną firewallem. Dostępny w wersji V5R1 serwer DNS, wykorzystujący program BIND 8 pozwala skonfigurować wiele serwerów DNS na jednym serwerze iSeries(TM). Załóżmy, że firma ma sieć wewnętrzną z zastrzeżonymi adresami IP i część zewnętrzną sieci, która jest dostępna publicznie.

Firma chce, aby wewnętrzni klienci mogli tłumaczyć nazwy hostów zewnętrznych i wymieniać pocztę z użytkownikami z zewnątrz. Firma chce również, aby wewnętrzny program tłumaczący miał dostęp do pewnych stref wewnętrznych, które w ogóle nie są dostępne spoza sieci wewnętrznej. Dodatkowo firma nie chce, aby do sieci wewnętrznej miały dostęp zewnętrzne programy tłumaczące.

Aby osiągnąć postawiony cel, firma konfiguruje dwie instancje serwera DNS na tej samej maszynie iSeries, jedną dla intranetu i drugą dla użytkowników w domenie publicznej. Rozwiązanie takie nazywa się podziałem DNS.

**Rysunek 1. Podział systemu DNS za firewallem.**


Strefa mycompany.com została skonfigurowana jako strefa podstawowa serwera zewnętrznego DNSB. Dane tej strefy obejmują wyłącznie rekordy przewidziane jako część domeny publicznej. Dla serwera wewnętrznego DNSA strefa mycompany.com jest również strefą podstawową, ale dane strefy zdefiniowane na serwerze DNSA zawierają rekordy zasobów intranetu. Opcja przekazywania została określona jako 10.1.2.5. Wymusza to na serwerze DNSA przekazywanie zapytań, których nie umie on przetłumaczyć, do serwera DNSB.

Jeśli w grę wchodzi integralność firewalla lub innych środków bezpieczeństwa, można skorzystać z opcji nasłuchiwania, która pomaga zabezpieczyć dane wewnętrzne. W tym celu należy skonfigurować serwer wewnętrzny, aby obsługiwał wyłącznie te zapytania dotyczące wewnętrznej strefy mycompany.com, które pochodzą od hostów wewnętrznych. Aby to wszystko działało poprawnie, należy tak skonfigurować klientów

wewnętrznych, aby kierowali zapytania tylko do serwera DNSA. W celu zdefiniowania podziału DNS, należy wziąć pod uwagę następujące ustawienia konfiguracyjne:

**Nasłuchiwanie**
W poprzednich przykładach był tylko jeden serwer DNS na maszynie iSeries. Nasłuchiwał on na wszystkich adresach IP interfejsu. W przypadku wielu serwerów DNS na jednym serwerze iSeries, trzeba zdefiniować adresy IP interfejsów, na których każdy z tych serwerów będzie nasłuchiwał. Dwie instancje serwera DNS nie mogą nasłuchiwać na tym samym adresie. W niniejszym przykładzie, wszystkie zapytania przychodzące zza firewalla trafią pod adres 10.1.2.5. Zapytania te powinny być wysłane do serwera zewnętrznego. Dlatego skonfigurowano serwer DNSB, aby nasłuchiwał pod adresem 10.1.2.5. Serwer wewnętrzny, DNSA, został skonfigurowany tak, aby akceptował zapytania z dowolnego adresu IP interfejsu 10.1.x.x *z wyjątkiem* 10.1.2.5. Aby efektywnie wykluczyć ten adres, musi on wystąpić na liście AML (Address Match List) przed przedrostkiem dla adresów dozwolonych.

**Kolejność na liście AML (Address Match List)**
Zostanie użyty pierwszy element z listy AML, który pasuje do danego adresu. Aby na przykład dopuścić wszystkie adresy sieci 10.1.x.x, oprócz 10.1.2.5, elementy AML muszą być w następującej kolejności: (!10.1.2.5; 10.1/16). W tym przypadku adres 10.1.2.5 zostanie porównany z pierwszym elementem i natychmiast zablokowany.

Gdyby kolejność adresów była odwrotna: (10.1/16; !10.1.2.5), adres IP 10.1.2.5 zostałby przepuszczony, ponieważ serwer porównałby go z pierwszym elementem, z którym adres ten jest zgodny, i nie sprawdzałby pozostałych reguł.

## Koncepcje systemu DNS

Serwer DNS w wersji V5R1 oferuje nowe funkcje związane z programem BIND 8. Poniżej zamieszczono odsyłacze do sekcji, w których opisano, w jaki sposób działa system DNS i jak korzystać z jego nowych funkcji:

**Podstawowe funkcje DNS:**

**“Podstawy DNS” na stronie 11**
Przegląd informacji o tym, czym jest i jak działa system DNS, a także opis typów stref, jakie można zdefiniować.

**“Podstawy zapytań DNS” na stronie 12**
Objaśnienie procesu tłumaczenia zapytania przez serwer DNS w imieniu klienta.

**“Konfigurowanie własnej domeny DNS” na stronie 14**
Ogólne informacje o rejestracji domeny z odsyłaczami do innych źródeł informacji o konfigurowaniu własnej domeny.

**Nowe funkcje DNS:**

**“Aktualizacje dynamiczne” na stronie 14**
Serwer DNS w wersji V5R1, wykorzystujący program BIND 8, obsługuje aktualizacje dynamiczne. Dzięki temu zewnętrzne źródła, na przykład serwer DHCP, mogą przesyłać aktualizacje do serwera DNS.

**“Funkcje programu BIND 8” na stronie 15**
Oprócz dynamicznych aktualizacji program BIND 8 oferuje kilka nowych funkcji, które poprawiają wydajność serwera DNS.

**Informacje o rekordach zasobów:**

**“Rekordy zasobów DNS” na stronie 16**
Rekordy zasobów są używane do przechowywania danych o nazwach domenowych i adresach IP. W tej sekcji znajduje się lista rekordów zasobów obsługiwanych w wersji V5R1 z wyszukiwarką.

**“Poczta i rekordy MX” na stronie 19**
Dzięki tym rekordom system DNS obsługuje zaawansowane rozsyłanie poczty elektronicznej.

Istnieje wiele zewnętrznych źródeł bardziej szczegółowych informacji o systemie DNS. Niektóre z nich można znaleźć w sekcji “Inne informacje dotyczące DNS” na stronie 35.

## Podstawy DNS

System nazw domen (Domain Name System - DNS) to rozproszony system baz danych służący do zarządzania nazwami hostów i przypisanymi im adresami protokołu Internet Protocol (IP). Dzięki zastsowaniu usług DNS użytkownicy mogą zamiast adresów IP (xxx.xxx.xxx.xxx) używać prostych nazw, jak np. ″www.jkltoys.com″. Pojedynczy serwer DNS może być odpowiedzialny za znajomość nazw hostów i adresów IP dla niewielkiej części strefy, ale serwery DNS mogą ze sobą współpracować w celu odwzorowania wszystkich nazw domen na odpowiadające im adresy IP. To dzięki współpracującym ze sobą serwerom DNS komputery mogą się ze sobą komunikować poprzez Internet.

Dane DNS są podzielone na hierarchię domen. Poszczególne serwery znają jedynie niewielką część tych danych, na przykład pojedynczą poddomenę. Części domeny podlegające bezpośrednio danemu serwerowi są nazywane strefami. Serwer DNS dysponujący pełną informacją o hostach i danych strefy jest uważany za autorytatywny dla tej strefy. Serwer autorytatywny może obsługiwać zapytania dotyczące hostów w jego strefie, korzystając z rekordów zasobów. Proces wykonywania zapytania zależy od wielu czynników. Sekcja “Podstawy zapytań DNS” na stronie 12 zawiera objaśnienia ścieżek, jakich może użyć klient do przetłumaczenia zapytania.

### Podstawy stref

Dane DNS są podzielone na łatwe do zarządzania zestawy zwane strefami. Strefy zawierają informacje o nazwie i adresie IP dla przynajmniej jednej części domeny DNS. Serwer, który zawiera wszystkie informacje dotyczące domeny, nazywa się serwerem autorytatywnym dla tej domeny. Niekiedy wygodnie jest delegować kompetencje obsługiwania zapytań DNS dotyczących określonej poddomeny do innego serwera DNS. W takim przypadku serwer DNS dla domeny może zostać skonfigurowany tak, aby kierował zapytania dotyczące tej poddomeny do odpowiedniego serwera.

Na wypadek awarii, dane strefy są często przechowywane nie tylko na serwerze autorytatywnym, ale także na innych serwerach DNS. Te inne serwery pobierają dane z serwera autorytatywnego i są nazywane serwerami zapasowymi. Skonfigurowanie serwerów zapasowych pozwala zrównoważyć ich obciążenie, a także stanowi zabezpieczenie na wypadek awarii serwera podstawowego. Serwery zapasowe uzyskują dane strefy poprzez przesyłanie strefowe z serwera autorytatywnego. Po zainicjowaniu serwer zapasowy pobiera kompletną kopię danych strefy z serwera głównego. Ponowne pobieranie danych strefy przez serwer zapasowy z serwera podstawowego lub z innych serwerów zapasowych dla tej samej domeny odbywa się również w przypadku zmiany danych strefy.

### Typy stref DNS

Za pomocą serwera DNS iSeries (TM) można zdefiniować kilka typów stref, które będą pomocne przy zarządzaniu danymi DNS:

#### Strefa podstawowa

Zawiera dane strefy pobrane bezpośrednio z pliku na hoście. Strefa podstawowa może zawierać podstrefę lub strefę potomną. Może ona również zawierać rekordy zasobów, na przykład nazwę hosta, alias (CNAME), adres (A) lub rekordy wskaźników przypisania odwrotnego (PTR).
**Uwaga:** W innych dokumentach dotyczących programu BIND strefy podstawowe są często nazywane ″strefami nadrzędnymi″.

**Podstrefa**
Podstrefa stanowi strefę wewnątrz strefy podstawowej. Podstrefy umożliwiają organizację danych strefy w łatwe do zarządzania zestawy.

**Strefa potomna**
Strefa potomna określa podstrefę i deleguje odpowiedzialność za dane podstrefy do przynajmniej jednego innego serwera nazw.

**Alias (CNAME)**
Alias określa alternatywną nazwę domeny podstawowej.

**Host**
Obiekt hosta przypisuje rekordy A i PTR do hosta. Z hostem mogą być powiązane dodatkowe rekordy zasobów.

**Strefa zapasowa**
Zawiera dane pobrane z podstawowego serwera strefy lub z innego serwera zapasowego. Serwer zapasowy danej strefy utrzymuje kompletną kopię danych tej strefy.
**Uwaga:** W innych dokumentach dotyczących programu BIND strefy zapasowe są czasami nazywane ″strefami podrzędnymi″.

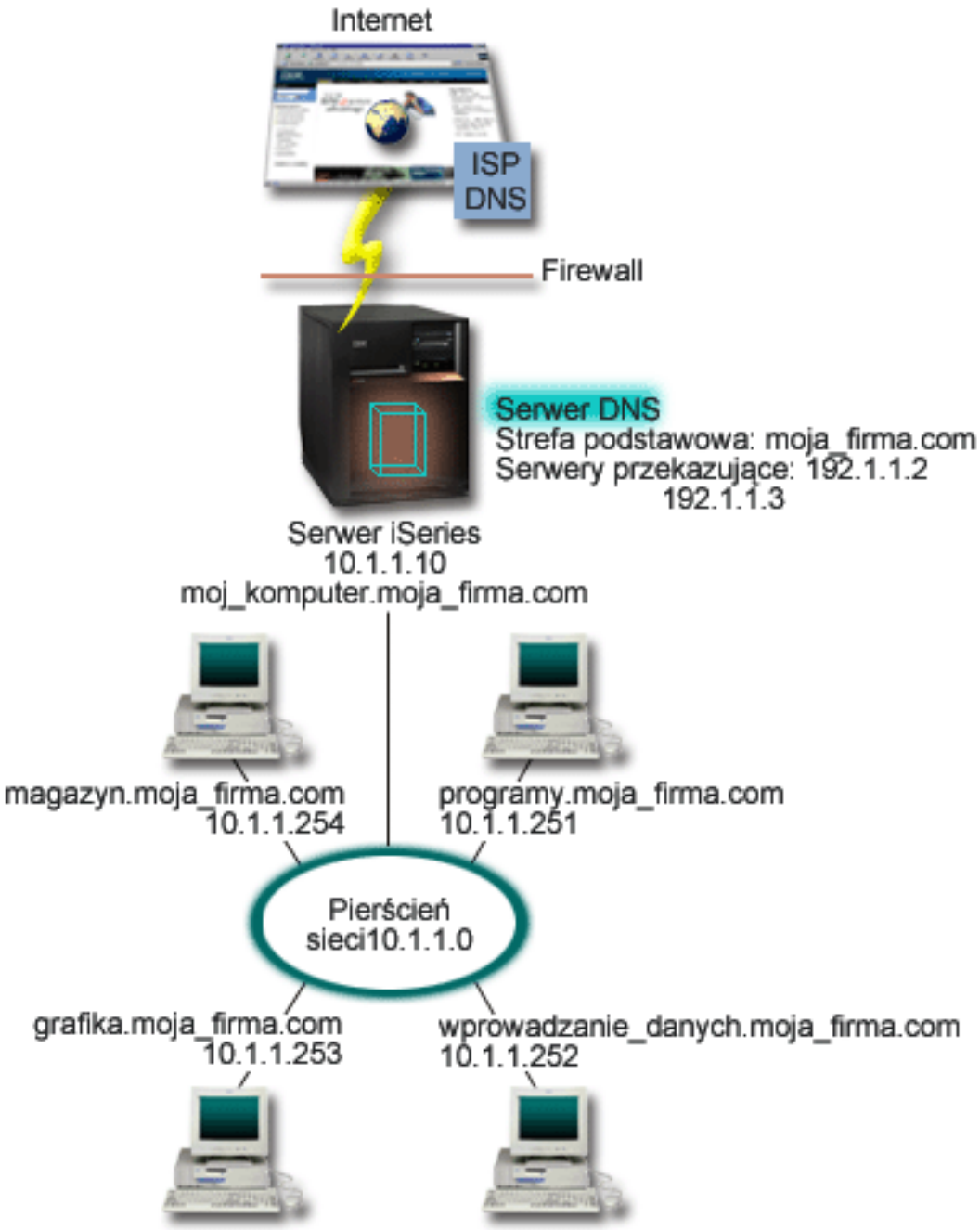
**Strefa pośrednicząca**
Strefa pośrednicząca jest podobna do strefy zapasowej, ale przekazuje ona tylko rekordy serwera nazw (NS) dla danej strefy.

**Strefa przekazująca**
Strefa przekazująca kieruje wszystkie zapytania dotyczące konkretnej strefy do innych serwerów.

## Podstawy zapytań DNS

Klienci korzystają z serwerów DNS w celu znalezienia poszukiwanych informacji. Żądanie może pochodzić bezpośrednio z klienta lub z aplikacji działającej na kliencie. Klient wysyła do serwera DNS komunikat z zapytaniem zawierającym: pełną nazwę domeny(FQDN), typ zapytania, na przykład konkretny rekord zasobów wymagany przez klienta, oraz klasę nazwy domenowej, która zwykle jest klasą internetową (IN). Poniższa ilustracja przedstawia przykładową sieć z sekcji “Przykład: serwer DNS z dostępem do Internetu” na stronie 4.

**Rysunek 1. Serwer DNS z dostępem do Internetu.**




Załóżmy, że host *wprowadzanie_danych* kieruje do serwera DNS zapytanie o ″grafika.moja_firma.com″. Na podstawie własnych danych strefy serwer DNS odpowie, podając adres IP 10.1.1.253.

Załóżmy z kolei, że host *wprowadzanie_danych* żąda adresu IP hosta o nazwie ″www.jkl.com.″. Tego hosta nie ma w danych strefy serwera DNS. Wobec tego do wyboru są dwie metody postępowania: rekurencja lub iteracja. Jeśli serwer DNS jest ustawiony do korzystania z rekurencji, skontaktuje się on z innymi serwerami DNS w imieniu żądającego klienta, aby przetłumaczyć nazwę, a następnie odeśle odpowiedź do klienta. Serwer DNS wysyłający zapytanie do innego serwera DNS zapisuje odpowiedź, aby jej użyć, kiedy następnym razem otrzyma takie samo zapytanie. Klient może również we własnym imieniu próbować kontaktować się z innymi serwerami DNS, aby przetłumaczyć nazwę. W tym procesie, zwanym iteracją, klient używa odrębnych i dodatkowych zapytań, tworzonych na podstawie odpowiedzi z serwerów.

## Konfigurowanie własnej domeny DNS

DNS umożliwia dostęp do nazw i adresów w intranecie, czyli w sieci wewnętrznej. Daje on również dostęp do tych informacji całej reszcie świata poprzez Internet. Aby skonfigurować domeny w Internecie, należy najpierw zarejestrować nazwę domeny.

W przypadku konfigurowania intranetu, rejestracja nazwy domeny używanej na potrzeby wewnętrzne nie jest wymagana. Decyzja w sprawie rejestrowania nazwy intranetowej zależy od tego, czy chce się zarezerwować tę nazwę, tak aby nikt inny nie mógł jej użyć w Internecie, niezależnie od wewnętrznego jej wykorzystania. Zarejestrowanie nazwy, która ma być używana wewnętrznie, zapewnia, że z jej wykorzystaniem na zewnątrz nie będzie żadnych problemów.

Domenę można zarejestrować poprzez bezpośredni kontakt z autoryzowanym rejestratorem nazw domen lub niekiedy za pośrednictwem dostawcy usług internetowych (ISP). Niektórzy dostawcy ISP oferują złożenie wniosku o rejestrację domeny w imieniu swoich klientów. Katalog wszystkich podmiotów rejestrujących nazwy domen, autoryzowanych przez Internet Corporation for Assigned Names and Numbers (ICANN) prowadzi centrum Internet Network Information Center (InterNIC)  .

Istnieje wiele innych źródeł informacji o rejestracji i prowadzeniu własnej domeny DNS. Dodatkową pomoc można znaleźć w sekcji “Inne informacje dotyczące DNS” na stronie 35.

## Aktualizacje dynamiczne

Protokół Dynamic Host Configuration Protocol (DHCP) jest standardem TCP/IP, który korzysta z serwera centralnego do zarządzania adresami IP i innymi szczegółami konfiguracyjnymi całej sieci. W odpowiedzi na żądania klientów serwer DHCP dynamicznie przypisuje im pewne właściwości. Protokół DHCP umożliwia centralną definicję parametrów konfiguracyjnych hostów w sieci i automatyczne konfigurowanie hostów. Jest on często używany do tymczasowego przypisywania adresów IP klientom sieci, w których jest więcej klientów niż dostępnych adresów IP.

Wcześniej, wszystkie dane DNS były przechowywane w statycznych bazach danych. Wszystkie “Rekordy zasobów DNS” na stronie 16 DNS musiały być utworzone i obsługiwane przez administratora. Obecnie serwery DNS wykorzystujące program BIND 8 można tak skonfigurować, aby akceptowały żądania dynamicznej aktualizacji danych strefy pochodzące z innych źródeł.

Można skonfigurować serwer DHCP, aby wysyłał żądania aktualizacji do serwera DNS za każdym razem, gdy przypisze hostowi nowy adres. Ten zautomatyzowany proces redukuje administracyjną obsługę serwera DNS w szybko rozrastających się lub zmieniających sieciach TCP/IP oraz w sieciach, w których hosty często zmieniają miejsce. Kiedy klient serwera DHCP uzyskuje od niego adres IP, dane te są natychmiast wysyłane do serwera DNS. Metoda ta pozwala serwerowi DNS poprawnie tłumaczyć nazwy hostów, nawet wtedy, gdy ich adresy IP się zmienią.

Serwer DHCP może w imieniu klienta aktualizować rekordy odwzorowania (A) i rekordy wyszukiwania odwrotnego. Rekordy typu A odwzorowują nazwę hosta na jego adres IP. Rekordy typu PTR odwzorowują adres hosta na jego nazwę. Kiedy zmienia się adres klienta, serwer DHCP może automatycznie wysłać aktualizację do serwera DNS, tak aby inne hosty w sieci mogły poprzez zapytanie DNS znaleźć tego klienta pod nowym adresem IP. Dla każdego rekordu zaktualizowanego dynamicznie zapisywany jest również powiązany rekord tekstowy (TXT), który wskazuje, że rekord został zaktualizowany przez serwer DHCP.
**Uwaga:** Jeśli skonfiguruje się serwer DHCP, tak aby aktualizował tylko rekordy PTR, należy również skonfigurować serwer DNS, aby zezwolił klientom na aktualizację swoich rekordów A. Jednak nie wszyscy klienci serwera DHCP obsługują żądania aktualizacji własnych rekordów A. Przed użyciem tej metody, należy więc zapoznać się z dokumentacją używanej platformy klienta.

Strefy dynamiczne zabezpiecza się tworząc listę autoryzowanych źródeł, które mogą wysyłać aktualizacje. Źródła takie można zdefiniować posługując się indywidualnymi adresami IP, całą podsiecią, pakietami podpisanymi za pomocą współużytkowanego klucza tajnego (tak zwanymi podpisami transakcyjnymi -

TSIG) lub dowolną kombinacją tych metod. Przed aktualizacją rekordów zasobów serwer DNS sprawdza, czy przychodzące pakiety żądań pochodzą z autoryzowanych źródeł.

Dynamiczne aktualizacje mogą się odbywać pomiędzy serwerami DNS i DHCP działającymi na tym samym serwerze iSeries (TM), na różnych serwerach iSeries lub na serwerze iSeries i na innych maszynach obsługujących dynamiczne aktualizacje. Więcej informacji dotyczących konfigurowania dynamicznych aktualizacji na serwerze iSeries można znaleźć w następujących sekcjach:

- "Konfigurowanie odbierania dynamicznych aktualizacji przez serwer DNS" na stronie 25
- Konfigurowanie wysyłania dynamicznych aktualizacji przez serwer DHCP
- Na serwerach wysyłających dynamiczne aktualizacje do serwera DNS wymagana jest funkcja API dynamicznej aktualizacji QTOBUPT. Jest ona instalowana automatycznie wraz z opcją 31 systemu OS/400 (R).

## Funkcje programu BIND 8

W wersji V5R1 serwer DNS został przeprojektowany i używa programu BIND 8. Jeśli w systemie nie został zainstalowany program PASE, można w dalszym ciągu używać poprzedniej wersji serwera DNS dla OS/400 (R) wykorzystującego program BIND 4.9.3. W sekcji "Wymagania systemu DNS" na stronie 22 opisano wymagania dotyczące uruchamiania DNS na serwerze iSeries (TM) z użyciem programu BIND 8. Nowy serwer DNS pozwala wykorzystać zalety następujących funkcji:

**Wiele serwerów DNS działających na pojedynczym serwerze iSeries**
W poprzednich wersjach można było skonfigurować tylko jeden serwer DNS. Obecnie można skonfigurować wiele serwerów DNS lub instancji. Funkcja ta umożliwia logiczne rozdzielenie danych między serwerami. Tworząc wiele instancji, należy w sposób jawny zdefiniować dla każdej z nich adresy IP interfejsu nasłuchującego. Dwie instancje serwera DNS nie mogą nasłuchiwać na tym samym interfejsie.

Przykładem praktycznego zastosowania wielu serwerów jest podział systemu DNS, w którym jeden serwer jest autorytatywny dla sieci wewnętrznej, a drugi obsługuje zapytania zewnętrzne. Więcej informacji o podziale systemu DNS zawiera przykład znajdujący się w sekcji "Przykład: podział systemu DNS za firewallem" na stronie 8.

**Przekazywanie warunkowe**
Funkcja przekazywania warunkowego pozwala skonfigurować serwer DNS z uwzględnieniem preferencji dotyczących przekazywania zapytań. Można skonfigurować serwer tak, aby przekazywał wszystkie zapytania, na które nie umie udzielić odpowiedzi. Możliwe jest skonfigurowanie przekazywania na poziomie globalnym, ale z wyjątkami dla domen, dla których tłumaczenie nazw ma się odbywać w toku normalnej procedury iteracyjnej. Alternatywnie można skonfigurować normalną procedurę iteracyjną na poziomie globalnym, a następnie wymusić przekazywanie dla niektórych domen.

**Bezpieczne aktualizacje dynamiczne**
Serwer DHCP lub inne autoryzowane źródło może wysłać dynamiczne aktualizacje rekordów zasobów, korzystając z podpisów transakcyjnych (TSIG) i/lub uwierzytelniania adresu IP. Eliminuje to konieczność ręcznej aktualizacji danych strefy, zapewniając jednocześnie, że do aktualizacji używane są wyłącznie dane z autoryzowanych źródeł.

Więcej informacji o aktualizacjach dynamicznych zawiera sekcja "Aktualizacje dynamiczne" na stronie 14. Informacje o autoryzacji aktualizacji ze źródeł zewnętrznych można znaleźć w sekcji "Planowanie ochrony" na stronie 21.

**Opcja NOTIFY**
Kiedy opcja NOTIFY jest włączona, podczas każdej aktualizacji danych strefy na serwerze podstawowym aktywowana jest funkcja DNS NOTIFY. Dzięki niej serwer podstawowy wysyła do wszystkich znanych serwerów zapasowych komunikat z informacją o zmianie danych. W odpowiedzi na ten komunikat serwery zapasowe mogą wystąpić z żądaniem przesłania strefowego zaktualizowanych danych strefy. Dzięki temu zapasowe dane strefy są aktualizowane na bieżąco, co zwiększa przydatność serwerów zapasowych.

**Przesyłanie strefowe (IXFR i AXFR)**
W przeszłości, kiedy serwery potrzebowały odświeżyć dane strefy, musiały pobierać cały zestaw tych danych w procesie całkowitego przesyłania strefowego (AXFR). Program BIND 8 obsługuje nową metodę przesyłania strefowego: przyrostowe przesyłanie strefowe (IXFR). Przesyłanie IXFR umożliwia serwerom pobranie tylko zmienionych danych, zamiast wszystkich danych strefy.

Kiedy metoda ta jest włączona na serwerze podstawowym, zmienionym danym zostają przypisane flagi, wskazujące wystąpienie zmiany. Kiedy serwer zapasowy zażąda aktualizacji danych strefy w trybie IXFR, serwer podstawowy prześle tylko nowe dane. Przesyłanie IXFR jest szczególnie użyteczne w strefach aktualizowanych dynamicznie i redukuje ruch w sieci, gdyż wysyłane są mniejsze ilości danych.
**Uwaga:** Aby korzystać z tej funkcji, przesyłanie IXFR musi być włączone na serwerze podstawowym i zapasowym.

## Rekordy zasobów DNS

Baza danych strefy DNS składa się z kolekcji rekordów zasobów. Każdy rekord zasobu zawiera informację o konkretnym obiekcie. Na przykład rekordy odwzorowania adresów (A) odwzorowują nazwę hosta na adres IP, a rekordy wyszukiwania odwrotnego (PTR) odwzorowują adres IP na nazwę hosta. Serwer używa tych rekordów do odpowiadania na zapytania dotyczące hostów w jego strefie. Aby uzyskać więcej informacji, należy skorzystać z tabeli zawierającej rekordy zasobów DNS.

| Rekord zasobu | Nazwa skrócona | Opis |
|---|---|---|
| Rekord odwzorowania adresów (A) | A | Rekord A określa adres IP danego hosta. Rekordy A używane są podczas rozwiązywania zapytań o adres IP domeny o podanej nazwie. Ten typ rekordu jest zdefiniowany w dokumencie RFC 1035. |
| Rekord bazy danych systemu plików Andrew (AFSDB) | AFSDB | Rekord AFSDB określa adres AFS lub DCE obiektu. Rekordy AFSDB, podobnie jak rekordy A, są wykorzystywane podczas odwzorowywania nazwy domeny na jej adres AFSDB oraz podczas odwzorowywania nazwy domeny komórki na uwierzytelnione serwery nazw tej komórki. Ten typ rekordu jest zdefiniowany w dokumencie RFC 1183. |
| Rekord nazwy kanonicznej (CNAME) | CNAME | Rekord CNAME określa bieżącą nazwę domeny obiektu. Jeśli serwer DNS wysyła zapytanie o nazwę-alias i znajduje rekord CNAME wskazujący na nazwę kanoniczną, wysyła zapytanie o kanoniczną nazwę domeny. Ten typ rekordu jest zdefiniowany w dokumencie RFC 1035. |
| Rekord informacji o hoście (HINFO) | HINFO | Rekord HINFO określa ogólne informacje o hoście. Nazwy standardowych procesów i nazwy systemów operacyjnych są zdefiniowane w dokumencie Assigned Numbers RFC 1700. Jednak nie jest wymagane używanie numerów standardowych. Ten typ rekordu jest zdefiniowany w dokumencie RFC 1035. |

| Rekord zasobu | Nazwa skrócona | Opis |
|---|---|---|
| Rekord ISDN | ISDN | Rekord ISDN określa adres obiektu. Odwzorowuje nazwę hosta na adres ISDN. Rekordy te są używane tylko w sieciach ISDN. Ten typ rekordu jest zdefiniowany w dokumencie RFC 1183. |
| Rekord odwzorowania adresów IP wersja 6 (AAAA) | AAAA | Rekord AAAA określa 128-bitowy adres hosta. Rekordy AAAA służą, podobnie jak rekordy A, do odwzorowywania nazwy hosta na jego adres IP. Należy ich używać do obsługi adresów IP w wersji 6, które nie są zgodne ze standardowym formatem rekordu A. Ten typ rekordu jest zdefiniowany w dokumencie RFC 1886. |
| Rekord położenia (LOC) | LOC | Rekord LOC określa fizyczne położenie elementów sieci. Rekordy te mogą być wykorzystywane przez aplikacje do szacowania wydajności sieci oraz do odwzorowywania sieci fizycznej. Ten typ rekordu jest zdefiniowany w dokumencie RFC 1876. |
| Rekord wymiany poczty (MX) | MX | Rekord MX definiuje host wymiany poczty dla poczty wysyłanej do tej domeny. Rekordy tego typu są wykorzystywane przez protokół SMTP (Simple Mail Transfer Protocol) podczas znajdowania hostów obsługujących przesyłanie poczty w tej domenie oraz podczas ustalania preferowanych wartości dla hostów wymiany poczty. Dla każdego hosta wymiany poczty muszą być zdefiniowane odpowiadające mu rekordy odwzorowania adresów (A) w poprawnej strefie. Ten typ rekordu jest zdefiniowany w dokumencie RFC 1035. |
| Rekord grupy poczty (MG) | MG | Rekord MG określa nazwę domeny grupy poczty. Ten typ rekordu jest zdefiniowany w dokumencie RFC 1035. |
| Rekord skrzynki pocztowej (MB) | MB | Rekord MB określa nazwę domeny hosta, który zawiera skrzynkę pocztową dla tego obiektu. Poczta wysłana do tej domeny zostanie skierowana do hosta podanego w rekordzie MB. Ten typ rekordu jest zdefiniowany w dokumencie RFC 1035. |

| Rekord zasobu | Nazwa skrócona | Opis |
|---|---|---|
| Rekord informacji o skrzynce pocztowej (MINFO) | MINFO | Rekord MINFO określa skrzynkę pocztową, do której mają być wysyłane komunikaty i komunikaty o błędach dotyczące danego obiektu. Rekord MINFO zwykle jest używany dla list skrzynek pocztowych, a nie dla pojedynczych skrzynek. Ten typ rekordu jest zdefiniowany w dokumencie RFC 1035. |
| Rekord zmiany nazwy skrzynki pocztowej (MR) | MR | Rekord MR określa nową nazwę domeny dla skrzynki pocztowej. Rekordu tego typu można używać jako pozycji przekazywania dla użytkownika, który został przeniesiony do innej skrzynki pocztowej. Ten typ rekordu jest zdefiniowany w dokumencie RFC 1035. |
| Rekord serwera nazw (NS) | NS | Rekord NS określa autorytatywny serwer nazw dla danego hosta. Ten typ rekordu jest zdefiniowany w dokumencie RFC 1035. |
| Rekord NSAP (Network Service Access Protocol) | NSAP | Rekord NSAP określa adres zasobu NSAP. Rekordy NASP są wykorzystywane do odwzorowywania nazw domen na adresy NSAP. Ten typ rekordu jest zdefiniowany w dokumencie RFC 1706. |
| Rekord klucza publicznego (KEY) | KEY | Rekord KEY określa klucz publiczny skojarzony z nazwą serwera DNS. Klucz może być przeznaczony dla strefy, użytkownika lub dla hosta. Ten typ rekordu jest zdefiniowany w dokumencie RFC 2065. |
| Rekord osoby odpowiedzialnej (RP) | RP | Rekord RP zawiera adres poczty elektronicznej i opis osoby odpowiedzialnej za strefę lub host. Ten typ rekordu jest zdefiniowany w dokumencie RFC 1183. |
| Rekord wskaźnika wyszukiwania wstecz (PTR) | PTR | Rekord PTR określa nazwę domeny hosta, dla którego jest definiowany rekord PTR. Rekordy PTR umożliwiają wyszukanie nazwy hosta, jeśli jest znany jego adres IP. Ten typ rekordu jest zdefiniowany w dokumencie RFC 1035. |
| Rekord przekierowania (RT) | RT | Rekord RT określa nazwę domeny hosta, która może działać jako domena przekazująca pakiety IP dla tego hosta. Ten typ rekordu jest zdefiniowany w dokumencie RFC 1183. |

| Rekord zasobu | Nazwa skrócona | Opis |
|---|---|---|
| Rekord uruchamiania uprawnień (SOA) | SOA | Rekord SOA określa, że dany serwer jest autorytatywny dla tej strefy. Serwer autorytatywny jest najlepszym źródłem danych w strefie. Rekord SOA zawiera ogólne informacje o strefie i przeładowuje zasady dla serwerów zapasowych. Dla każdej strefy może istnieć tylko jeden rekord SOA. Ten typ rekordu jest zdefiniowany w dokumencie RFC 1035. |
| Rekord z tekstem (TXT) | TXT | Rekord TXT zawiera łańcuchy tekstowe o maksymalnej długości 255, które są skojarzone z nazwą domeny. Rekordy TXT mogą być wykorzystywane łącznie z rekordami osób odpowiedzialnych (RP) i mogą zawierać informacje o osobach odpowiedzialnych za strefy. Ten typ rekordu jest zdefiniowany w dokumencie RFC 1035.<br>Rekordy TXT są wykorzystywane przez protokół DHCP dla iSeries podczas aktualizacji dynamicznych. Serwer DHCP zapisuje skojarzony rekord TXT dla każdej aktualizacji rekordu PTR i A wykonywanej przez serwer DHCP. Rekordy DHCP mają prefiks **AS400DHCP:**. |
| Rekord ogólnie znanych usług (WKS) | WKS | Rekord WKS określa ogólnie znane usługi obsługiwane przez dany obiekt. Najczęściej rekordy WKS wskazują, czy dany adres obsługuje protokół TCP, UDP czy obydwa protokoły. Ten typ rekordu jest zdefiniowany w dokumencie RFC 1035. |
| Rekord odwzorowania adresu X.400 (PX) | PX | Rekord PX jest wskaźnikiem do informacji dotyczących odwzorowania X.400/RFC 822. Ten typ rekordu jest zdefiniowany w dokumencie RFC 1664. |
| Rekord odwzorowania adresu X25 (X25) | X25 | Rekord X25 określa adres zasobu X25. Odwzorowuje nazwę hosta na adres PSDN. Rekordy te są używane tylko w sieciach X25. Ten typ rekordu jest zdefiniowany w dokumencie RFC 1183. |

## Poczta i rekordy MX

Rekordy MX są używane przez programy rozsyłające pocztę, takie jak protokół Simple Mail Transfer Protocol (SMTP). Więcej informacji o typach rekordów dotyczących poczty, obsługiwanych przez serwer DNS w systemie iSeries(TM) można znaleźć w tabeli znajdującej się w sekcji Rekordy zasobów DNS.

System DNS obejmuje informacje potrzebne do wysyłania poczty elektronicznej za pomocą wymienników poczty. Jeśli w sieci używany jest system DNS, aplikacja protokołu SMTP (Simple Mail Transfer Protocol) nie

wysyła poczty adresowanej do hosta TEST.IBM.COM poprzez nawiązanie połączenia TCP z tym hostem. Aplikacja SMTP najpierw kieruje zapytanie do serwera DNS, aby dowiedzieć się, na którym hoście działa serwer dostarczający pocztę.

**Dostarczanie poczty pod określony adres**
Serwery DNS korzystają z rekordów zasobów nazywanych rekordami wymiennika poczty (MX). Rekordy MX odwzorowują nazwę domeny lub nazwę hosta na wartość preferencji i nazwę hosta. Rekordy MX są najczęściej używane do wskazania hosta, używanego do przetwarzania poczty z innego hosta. Rekordy te są również używane do wskazania innego hosta, do którego należy próbować dostarczyć pocztę, jeśli z pierwszym hostem nie można się połączyć. Innymi słowy, rekordy te pozwalają, aby poczta adresowana do określonego hosta była dostarczana do innego hosta.

Dla tej samej domeny lub nazwy hosta może istnieć wiele rekordów zasobów MX. W takiej sytuacji kolejność, w jakiej hosty te będą użyte do dostarczenia poczty, określa wartość preferencji (czyli priorytet). Najniższa wartość preferencji odpowiada rekordowi, który zostanie użyty jako pierwszy. Kiedy najbardziej preferowany host jest niedostępny, aplikacja wysyłająca pocztę próbuje skontaktować się z kolejnym, mniej preferowanym hostem MX. Wartość preferencji określa administrator domeny lub autor rekordu MX.

W przypadku zapytania o nazwę, która znajduje się w domenie obsługiwanej przez serwer DNS, ale której nie przypisano rekordów MX, serwer może zwrócić pustą listę rekordów zasobów MX. W takiej sytuacji aplikacja wysyłająca pocztę może próbować nawiązać bezpośrednie połączenie z hostem docelowym.
**Uwaga:** Nie zaleca się stosowania znaków zastępczych (na przykład: *.mycompany.com) w nazwach domeny występujących w rekordach MX.

**Przykład: rekord MX dla hosta**
W poniższym przykładzie system powinien zgodnie z preferencjami dostarczyć pocztę adresowaną do fsc5.test.ibm.com bezpośrednio do tego hosta. Jeśli host będzie niedostępny, system może dostarczyć pocztę do hosta psfred.test.ibm.com lub do mvs.test.ibm.com (jeśli psfred.test.ibm.com również nie będzie dostępny). A oto przykład odpowiednich rekordów MX:

```
fsc5.test.ibm.com   IN MX 0 fsc5.test.ibm.com
                    IN MX 2 psfred.test.ibm.com
                    IN MX 4 mvs.test.ibm.com
```

## Planowanie systemu DNS

System DNS można skonfigurować na wiele sposobów. Jednak wcześniej należy zaplanować, jak powinien on działać w danej sieci. Przed wdrożeniem systemu DNS należy rozważyć strukturę sieci, jej wydajność i system ochrony. Podczas planowania działania systemu DNS, należy wziąć pod uwagę następujące zagadnienia:

**“Określanie uprawnień DNS”**
Istnieją szczególne wymagania autoryzacyjne dotyczące administratora DNS. Należy również uwzględnić wpływ autoryzacji na ochronę. W sekcji opisano te wymagania.

**“Określanie struktury domeny” na stronie 21**
Konfigurując domenę po raz pierwszy, przed utworzeniem stref należy przewidzieć obciążenie i obsługę domeny.

**“Planowanie ochrony” na stronie 21**
DNS udostępnia opcje ochrony ograniczające dostęp z zewnątrz do serwera. W sekcji opisano te opcje i sposób kontroli dostępu.

## Określanie uprawnień DNS

Po skonfigurowaniu systemu DNS należy zdefiniować ochronę w celu zabezpieczenia konfiguracji. Należy określić, którzy użytkownicy są uprawnieni do dokonywania zmian w konfiguracji.

Minimalny wymagany poziom uprawnień powinien umożliwić administratorowi serwera iSeries(TM) skonfigurowanie systemu DNS i administrowanie nim. Przydzielenie praw dostępu do wszystkich obiektów pozwoli administratorowi na realizację zadań związanych z zarządzaniem systemem DNS. Zaleca się, aby użytkownicy konfigurujący DNS mieli uprawnienia szefa ochrony z dostępem do wszystkich obiektów (*ALLOBJ). Do nadania użytkownikom odpowiednich uprawnień można użyć programu iSeries Navigator. Więcej informacji na ten temat można znaleźć w sekcji **Granting authority to the DNS administrator**, w elektronicznej pomocy dla systemu DNS.

**Uwaga:** Jeśli profil administratora nie ma pełnych uprawnień, należy mu przydzielić określone uprawnienia do wszystkich “Obsługa plików konfiguracyjnych DNS” na stronie 30.

## Określanie struktury domeny

Ważne jest określenie sposobu podziału domeny lub poddomen na strefy, tak aby jak najlepiej obsłużyć żądania z sieci, dostęp do Internetu i sposób negocjacji z firewalami. Czynniki te mogą być złożone i muszą być brane pod uwagę w odniesieniu do konkretnej sytuacji. Szczegółowe wytyczne można znaleźć w autorytatywnych źródłach, na przykład w książce O'Reilly DNS and BIND.

Po skonfigurowaniu strefy DNS jako strefy dynamicznej nie można ręcznie zmieniać danych strefy podczas działania serwera. Może to bowiem spowodować kolizję z przychodzącymi aktualizacjami dynamicznymi. Jeśli trzeba dokonać ręcznych aktualizacji, należy zatrzymać serwer, dokonać zmian, a następnie restartować serwer. Jednak dynamiczne aktualizacje wysłane do zatrzymanego serwera DNS nie zostaną nigdy dokonane. Z tego powodu może być uzasadnione odrębne skonfigurowanie strefy dynamicznej i statycznej. Można to zrobić tworząc całkowicie odrębne strefy lub definiując nową poddomenę, na przykład dynamic.mycompany.com, dla klientów, którzy będą obsługiwani dynamicznie.

System DNS na serwerze iSeries(TM) udostępnia graficzny interfejs do konfigurowania serwerów. W niektórych przypadkach używane w tym interfejsie terminy i koncepcje różnią się od używanych w innych źródłach. Korzystając z innych źródeł informacji podczas konfigurowania systemu DNS, warto uwzględnić następujące wskazówki:

- Wszystkie strefy i obiekty zdefiniowane na serwerze znajdują się w folderach **Strefy wyszukiwania do przodu (Forward Lookup Zones)** i **Strefy wyszukiwania wstecz (Reverse Lookup Zones)**. Strefy wyszukiwania do przodu to strefy używane do odwzorowywania nazw domen na adresy IP według rekordów typu A. Strefy wyszukiwania wstecz to strefy używane do odwzorowywania adresów IP na nazwy domen według rekordów typu PTR.
- System DNS na serwerze iSeries korzysta ze **stref podstawowych** i **stref zapasowych**. W innych dokumentach dotyczących programu BIND strefy te są niekiedy nazywane, odpowiednio, strefami nadrzędnymi i strefami podrzędnymi.
- Interfejs korzysta z **podstref**, określanych w innych źródłach jako poddomeny. Strefa potomna jest podstrefą, do której delegowano odpowiedzialność przynajmniej jednego serwera nazw.

## Planowanie ochrony

Ochrona serwera DNS jest kwestią podstawową. Oprócz przedstawionych poniżej uwag dotyczących ochrony, ochrona serwera DNS i serwera iSeries(TM) została omówiona w różnych źródłach, w tym również w sekcji IBM(R) Secureway: iSeries i Internet w Centrum informacyjnym. Zagadnienia dotyczące ochrony systemu DNS opisano również w książce “Inne informacje dotyczące DNS” na stronie 35.

**Listy zgodności adresów (Address Match Lists - AML)**
Serwer DNS używa list AML w celu umożliwienia lub zablokowania dostępu jednostek zewnętrznych do pewnych funkcji DNS. Listy te mogą zawierać określone adresy IP, podsieci (używające przedrostka IP) lub określać użycie kluczy TSIG. Na liście AML można zdefiniować jednostki, którym zostanie przyznany dostęp i jednostki, które nie będą miały prawa dostępu. Aby wielokrotnie używać listy AML, można ją zapisać jako listę ACL (Access Control List). Dzięki temu, zawsze, gdy trzeba będzie użyć tej listy, można po prostu wywołać ACL i cała lista zostanie załadowana.

**Kolejność elementów na liście AML**
Decydujące znaczenie dla danego adresu ma pierwszy zgodny z nim element znaleziony na liście AML. Aby na przykład zezwolić na wszystkie adresy sieci 10.1.1.x, oprócz 10.1.1.5, elementy listy zgodności muszą być wpisane w następującej kolejności (!10.1.1.5; 10.1.1/24). W takim przypadku adres 10.1.1.5 zostanie porównany z pierwszym elementem i natychmiast odrzucony.

Jeśli elementy byłyby wpisane na listę w odwrotnej kolejności, to jest (10.1.1/24; !10.1.1.5), adresowi 10.1.1.5 zostałby przyznany dostęp, ponieważ serwer porównałby go z pierwszym elementem. który jest z nim zgodny, i pominąłby sprawdzanie pozostałych reguł.

**Opcje kontroli dostępu**
DNS umożliwia ustawienie ograniczeń dotyczących tego, kto może wysyłać aktualizacje dynamiczne do serwera, wysyłać zapytania i żądać przesyłania strefowego. Do ograniczenia dostępu do serwera można użyć listy kontroli dostępu z następującymi opcjami:

**Zezwolenie na aktualizację (allow-update)**
Aby serwer DNS akceptował dynamiczne aktualizacje z dowolnych źródeł zewnętrznych, należy włączyć tę opcję.

**Zezwolenie na zapytania (allow-query)**
Określa hosty, które mogą wysyłać zapytania do serwera. Jeśli nie zostaną podane, domyślnie obsługiwane będą zapytania ze wszystkich hostów.

**Zezwolenie na przesyłanie (allow-transfer)**
Określa hosty, które mogą odbierać przesyłanie strefowe z serwera. Jeśli nie zostaną podane, domyślnie realizowane będą żądania przesyłania ze wszystkich hostów.

**Zezwolenie na rekurencję (allow-recursion)**
Określa hosty, które mogą wysyłać zapytania rekurencyjne przez ten serwer. Jeśli nie zostaną podane, domyślnie obsługiwane będą zapytania rekurencyjne ze wszystkich hostów.

**Odrzucenie (blackhole)**
Określa listę adresów, których zapytania nie będą akceptowane przez serwer, i które nie będą używane do tłumaczenia zapytań. Serwer nie będzie odpowiadał na zapytania przychodzące spod tych adresów.

## Wymagania systemu DNS

Opcja DNS (Opcja 31) nie jest instalowana automatycznie z podstawowym systemem operacyjnym. Należy ją oddzielnie wybrać do instalacji. Nowy serwer DNS dołączony do wersji V5R1 wykorzystuje standardową implementację DNS, znaną jako BIND 8. W poprzedniej wersji systemu OS/400(R) dostępne były usługi DNS wykorzystujące program BIND 4.9.3. Są one w dalszym ciągu dostępne w wersji V5R1.

Po zainstalowaniu usługi DNS są domyślnie skonfigurowane do korzystania z serwera opartego na programie BIND 4.9.3, dostępnego w poprzednich wersjach. Aby uruchomić serwery DNS korzystające z programu BIND 8, należy zainstalować środowisko Portable Application Solutions Environment (PASE). Środowisko PASE jest dostępne jako SS1 Opcja 33. Po zainstalowaniu środowiska PASE program iSeries Navigator automatycznie skonfiguruje odpowiednią implementację programu BIND.

Brak zainstalowanego środowiska PASE uniemożliwia skorzystanie z nowych funkcji programu BIND 8. Będzie to taki sam serwer, jaki był dostępny w poprzednich wersjach systemu. Dokumentacja dotycząca programu BIND 4.9.3 znajduje się w dokumencie V4R5 DNS Information Center (około 357 kB).

Aby skonfigurować wysyłanie do danego serwera DNS przez serwer DHCP na innym serwerze iSeries, należy również na serwerze iSeries z serwerem DHCP zainstalować Opcję 31. Serwer DHCP używa bowiem interfejsów programowych Opcji 31 do wykonywania dynamicznych aktualizacji.

Aby określić, czy serwer DNS jest zainstalowany, wykonaj następujące czynności:

1. W wierszu komend wpisz **GO LICPGM** i naciśnij klawisz **Enter**.
2. Wpisz **10** (Wyświetlanie zainstalowanych programów licencjonowanych) i naciśnij klawisz **Enter**.
3. Przejdź do strony **5722SS1 OS/400 - System nazw domen** (SS1 Opcja 31).
   Jeśli serwer DNS został zainstalowany pomyślnie, w polu **Status instalacji** będzie wartość ***compatible**, jak pokazano poniżej:

```
Progr.lic. Status instalacji    Opis
5722SS1    *COMPATIBLE          OS/400 - System nazw domen
```

4. Naciśnij klawisz **F3**, aby zamknąć ekran.

Aby zainstalować serwer DNS, wykonaj następujące czynności:

1. W wierszu komend wpisz **GO LICPGM** i naciśnij klawisz **Enter**.
2. Wpisz **11** (Instalowanie programów licencjonowanych) i naciśnij klawisz **Enter**.
3. Wpisz **1** (Instalacja) w polu **Opcja** obok OS/400 - System nazw domen i naciśnij klawisz **Enter**.
4. Ponownie naciśnij klawisz **Enter**, aby potwierdzić instalację.

## Konfigurowanie DNS

Przed przystąpieniem do konfigurowania systemu DNS należy zapoznać się z sekcją Wymagania systemu DNS oraz zainstalować niezbędne komponenty DNS. W poniższych sekcjach przedstawiono wskazówki dotyczące konfigurowania serwera DNS:

**“Dostęp do DNS przez iSeries Navigator”**
Instrukcje dotyczące dostępu do konfiguracji systemu za pomocą programu iSeries Navigator.

**“Konfigurowanie serwerów nazw” na stronie 24**
System DNS umożliwia utworzenie wielu instancji serwera nazw. W sekcji tej przedstawiono instrukcje dotyczące konfigurowania serwera nazw.

**“Konfigurowanie odbierania dynamicznych aktualizacji przez serwer DNS” na stronie 25**
Serwery DNS wykorzystujące program BIND 8 można skonfigurować tak, aby akceptowały przychodzące z innych źródeł żądania dynamicznych aktualizacji danych strefy. Sekcja ta zawiera instrukcje konfigurowania opcji zezwolenia na aktualizację (allow-update), tak aby serwer DNS mógł odbierać dynamiczne aktualizacje.

**“Importowanie plików DNS” na stronie 26**
Do systemu DNS można zaimportować istniejące pliki danych strefy. Przedstawione procedury tworzenia nowych stref na podstawie istniejących plików konfiguracyjnych sprzyjają oszczędzaniu na czasie.

**“Dostęp do zewnętrznych danych DNS” na stronie 27**
Po utworzeniu danych strefy DNS serwer będzie w stanie tłumaczyć zapytania dotyczące tej strefy. W sekcji opisano sposób konfiguracji serwera DNS, umożliwiający mu tłumaczenie zapytań spoza lokalnej domeny.

## Dostęp do DNS przez iSeries Navigator

Poniższe instrukcje stanowią przewodnik po interfejsie umożliwiającym konfigurowanie DNS w programie iSeries Navigator.Jeśli w systemie zainstalowane jest środowisko PASE, można skonfigurować serwery DNS wykorzystujące program BIND 8. Jeśli środowisko PASE nie jest wykorzystywane, można w dalszym

ciągu używać serwera DNS wykorzystującego program BIND 4.9.3, który był dostępny w poprzednich wersjach systemu. Informacje dotyczące serwera DNS wykorzystującego program BIND 4.9.3 znajdują się w dokumencie V4R5 DNS Information Center  (około 62 strony).

Konfigurując serwer DNS po raz pierwszy, wykonaj następujące czynności:

1. W **iSeries Navigator** rozwiń **serwer iSeries** —> **Sieć** —> **Serwery** —> **DNS**.
2. Prawym przyciskiem myszy kliknij **DNS** i wybierz **Nowa konfiguracja**.

Jeśli w systemie działa serwer DNS skonfigurowany w wersji wcześniejszej niż V5R1, wykonaj następujące czynności:

1. W **iSeries Navigator** rozwiń **serwer iSeries** —> **Sieć** —> **Serwery** —> **DNS**.
2. W prawym panelu dwukrotnie kliknij serwer DNS, aby otworzyć okno **Konfiguracja DNS**.
3. Jeśli w systemie zainstalowane jest środowisko PASE, dostępna będzie opcja migracji istniejącej konfiguracji do implementacji BIND 8. Jednak po przejściu do wersji BIND 8 nie będzie można powrócić do wersji BIND 4.9.3. Jeśli nie jesteś pewien, wybierz **Nie**. Jeśli chcesz dokonać migracji, wybierz **Tak**.
4. Aby w dowolnej chwili przeprowadzić migrację serwra DNS do wersji BIND 8, kliknij prawym przyciskiem myszy **DNS** w lewym panelu okna i wybierz **Migruj do wersji 8**.

## Konfigurowanie serwerów nazw

Serwer DNS (TM) w systemie iSeries wykorzystujący program BIND 8 obsługuje wiele instancji serwera nazw. Zadania opisane w poniższych sekcjach przedstawiają proces tworzenia pojedynczej instancji serwera nazw, w tym określenie jej właściwości i stref.

1. “Tworzenie instancji serwera nazw”
   Aby zdefiniować instancję serwera DNS, należy posłużyć się kreatorem **Nowa konfiguracja DNS**.
2. “Edycja właściwości serwera DNS” na stronie 25
   W sekcji opisano definiowanie globalnych właściwości nowej instancji serwera.
3. “Konfigurowanie stref na serwerze nazw” na stronie 25
   Sekcja przedstawia proces tworzenia stref i danych stref, którymi będzie posługiwał się serwer DNS.

Aby utworzyć wiele instancji, należy odpowiednią liczbę razy powtórzyć procedurę opisaną w powyższych sekcjach. Różne instancje serwera nazw mogą mieć różne właściwości, na przykład poziomy debugowania i wartości autostartu. Podczas tworzenia nowej instancji tworzone są odrębne pliki konfiguracyjne. Więcej informacji o plikach konfiguracyjnych zawiera sekcja Obsługa plików konfiguracyjnych DNS.

### Tworzenie instancji serwera nazw

Aby uruchomić kreator **Nowa konfiguracja DNS**, wykonaj następujące czynności:

1. W **iSeries Navigator** rozwiń **serwer iSeries(TM)** —> **Sieć** —> **Serwery** —> **DNS**.
2. W lewym panelu okna kliknij prawym klawiszem myszy **DNS** i wybierz **Nowy serwer nazw...**
3. Kreator przeprowadzi Cię przez proces konfiguracyjny.

Kreator wymaga podania następujących danych wejściowych:

**Nazwa serwera DNS:** Wpisz nazwę dla serwera DNS. Może ona składać się z maksymalnie pięciu znaków i musi zaczynać się od litery. W przypadku tworzenia wielu serwerów, każdy z nich musi mieć unikalną nazwę. W innych obszarach systemu nazwa ta będzie używana jako nazwa ″instancji″ serwera DNS.

**Adresy IP nasłuchiwania:** Dwa serwery DNS nie mogą nasłuchiwać pod tym samym adresem. Ustawieniem domyślnym jest nasłuchiwanie pod WSZYSTKIMI adresami IP. W przypadku tworzenia wielu serwerów żaden z nich nie może nasłuchiwać pod WSZYSTKIMI adresami. Należy określić adresy IP dla każdego serwera.

**Serwery główne:** Można załadować listę domyślnych Internetowych serwerów głównych lub podać własne serwery główne, na przykład wewnętrzne serwery główne dla intranetu.
**Uwaga:** Listę domyślnych Internetowych serwerów głównych powinno się załadować tylko wtedy, gdy serwer DNS ma działać w Internecie i w pełni tłumaczyć nazwy internetowe.

**Uruchamianie serwera:** Można określić, czy serwer ma być automatycznie uruchamiany podczas uruchamiania protokołów TCP/IP. W przypadku działania wielu instancji serwerów DNS, każda z nich może być uruchamiana i zatrzymywana niezależnie od innych.

**Kolejne czynności:** “Edycja właściwości serwera DNS”.

### Edycja właściwości serwera DNS

Po utworzeniu serwera nazw można zmienić jego właściwości, na przykład opcję zezwolenia na aktualizację (allow-update) i poziomy debugowania. Opcje te będą odnosiły się tylko do wybranej instancji serwera. Aby zmienić właściwości serwera DNS, wykonaj następujące czynności:

1. W **iSeries Navigator** rozwiń **serwer iSeries(TM)** —> **Sieć** —> **Serwery** —> **DNS**.
2. W prawym panelu okna kliknij prawym klawiszem myszy **serwer DNS** i wybierz **Konfiguracja**.
3. Prawym klawiszem myszy kliknij **Serwer DNS** i wybierz **Właściwości**.

**Kolejne czynności:** “Konfigurowanie stref na serwerze nazw”.

### Konfigurowanie stref na serwerze nazw

Po utworzeniu serwera nazw należy powrócić do głównego okna programu **iSeries Navigator**. Utworzony serwer będzie wyświetlony w prawym panelu okna. Aby skonfigurować strefy na tym serwerze, należy kliknąć jego nazwę prawym klawiszem myszy i wybrać **Konfiguracja**. Zostanie wyświetlone okno **Konfiguracja DNS**.

Wszystkie strefy konfiguruje się za pomocą kreatorów. Klikając prawym klawiszem myszy folder **Strefy wyszukiwania do przodu** lub **Strefy wyszukiwania wstecz**, należy utworzyć odpowiednią strefę. Zostaną wyświetlone opcje dla danego typu strefy. Należy wybrać odpowiedni typ strefy, aby uruchomić kreatora.

Opis typów obiektów, jakie można utworzyć w systemie DNS w wersji V5R1 zawiera sekcja “Podstawy DNS” na stronie 11.

Po skonfigurowaniu stref użyteczne mogą być informacje dotyczące konfiguracji, znajdujące się w następujących sekcjach:

“Konfigurowanie odbierania dynamicznych aktualizacji przez serwer DNS”
Dynamiczne aktualizacje umożliwiają autoryzowanym źródłom wysyłanie rekordów zasobów w celu aktualizacji danych strefy. Może to zmniejszyć konieczność ręcznego dokonywania zmian danych strefy.

“Importowanie plików DNS” na stronie 26
Jeśli dane strefy istnieją już dla innego serwera DNS, można je wykorzystać dla nowego serwera.

“Dostęp do zewnętrznych danych DNS” na stronie 27
Serwer DNS można skonfigurować tak, aby tłumaczył zapytania dotyczące adresów spoza podległej mu strefy. W tym celu można przekazywać zapytania do innych serwerów autorytatywnych lub wykorzystać serwery główne do pomocy w przetłumaczeniu zapytania.

## Konfigurowanie odbierania dynamicznych aktualizacji przez serwer DNS

Tworząc strefy dynamiczne, należy wziąć pod uwagę strukturę sieci. Jeśli niektóre części domeny w dalszym ciągu wymagają ręcznej aktualizacji, można wziąć pod uwagę skonfigurowanie odrębnych stref statycznej i dynamicznej. Jeśli trzeba dokonać ręcznej aktualizacji strefy dynamicznej, należy zatrzymać

serwer i restartować go po dokonaniu zmian. Zatrzymanie serwera wymusza synchronizację wszystkich aktualizacji dynamicznych, dokonanych od czasu załadowania przez serwer danych strefy z bazy danych. Jeśli serwer nie zostanie zatrzymany, wszystkie dynamiczne aktualizacje przetworzone od czasu jego uruchomienia zostaną utracone. Jednak zatrzymanie serwera w celu ręcznej aktualizacji oznacza utratę aktualizacji dynamicznych wysłanych w czasie, kiedy serwer nie działa.

System DNS wskazuje, że strefa jest dynamiczna, kiedy obiekty są zdefiniowane w instrukcji zezwolenia na aktualizację. Aby skonfigurować opcję zezwolenia na aktualizację (allow-update), wykonaj następujące czynności:

1. W **iSeries Navigator** rozwiń **serwer iSeries** —> **Sieć** —> **Serwery** —> **DNS**.
2. W prawym panelu okna kliknij prawym klawiszem myszy **serwer DNS** i wybierz **Konfiguracja**.
3. W oknie **Konfiguracja DNS** rozwiń **Strefy wyszukiwania do przodu** lub **Strefy wyszukiwania wstecz**.
4. Prawym klawiszem myszy kliknij strefę podstawową, którą chcesz zmienić, i wybierz **Właściwości**.
5. Na stronie **Właściwości strefy podstawowej** kliknij zakładkę **Opcje**.
6. Na stronie **Opcje** rozwiń **Kontrola dostępu** —> **Zezwolenie na aktualizację**.
7. Do sprawdzenia autoryzowanych aktualizacji system DNS używa listy zgodności adresów. Aby dodać obiekt do tej listy, wybierz typ elementu listy i kliknij **Dodaj...** Możesz dodać adres IP, przedrostek IP, listę ACL (Access Control List) lub klucz.
8. Po zakończeniu aktualizacji listy zgodności adresów kliknij **OK**, aby zamknąć stronę **Opcje**.

Konfigurując serwer DNS do odbierania dynamicznych aktualizacji z serwera DHCP na serwerze iSeries, należy zapoznać się z sekcją Konfigurowanie wysyłania dynamicznych aktualizacji przez serwer DHCP.

## Importowanie plików DNS

Strefę podstawową można utworzyć importując plik danych strefy lub dokonując konwersji istniejących tabel hostów. Opis procedury tworzenia danych strefy na podstawie tabeli hostów znajduje się w sekcji

*Przekształcanie tabel hostów* w dokumencie V4R5 DNS Information Center  (około 357 kB).

Można zaimportować dowolny poprawny plik konfiguracyjny strefy zgodny ze składnią programu BIND. Plik ten powinien znajdować się w katalogu IFS. Podczas importu serwer DNS sprawdzi, czy jest to poprawny plik danych strefy i dołączy go do pliku NAMED.CONF dla danej instancji serwera.

Aby zaimportować plik strefy, wykonaj następujące czynności:

1. W **iSeries Navigator** rozwiń **serwer iSeries(TM)** —> **Sieć** —> **Serwery** —> **DNS**.
2. W prawym panelu dwukrotnie kliknij instancję serwera DNS, do której chcesz zaimportować strefę.
3. W lewym panelu kliknij prawym klawiszem myszy **Serwer DNS** i wybierz **Strefa importująca**.
4. Wykonuj instrukcje kreatora, aby zaimportować strefę podstawową.

**Sprawdzanie rekordów**

Funkcja importu danych domeny odczytuje i sprawdza każdy rekord z importowanego pliku. Po zakończeniu jej działania wszystkie błędne rekordy mogą być sprawdzone indywidualnie na stronie właściwości **Inne rekordy** zaimportowanej strefy.

- **Uwaga:**
- Import dużej domeny podstawowej może zająć kilka minut.
- Funkcja importu danych domeny nie obsługuje dyrektywy $include. Podczas procedury sprawdzania, rekordy które zawierają dyrektywę $include, są identyfikowane jako błędne.

## Dostęp do zewnętrznych danych DNS

Serwery główne mają podstawowe znaczenie dla serwerów DNS podłączonych bezpośrednio do Internetu lub do dużych sieci intranetowych. Serwery DNS muszą korzystać z serwerów głównych podczas odpowiadania na zapytania o hosty inne niż wymienione w plikach ich własnych domen.

Aby zdobyć pożądane informacje, serwery DNS muszą wiedzieć, gdzie ich szukać. W Internecie, pierwszym miejscem przeszukiwanym przez serwery DNS są serwery główne. Serwery główne kierują serwery DNS do kolejnych serwerów w hierarchii do czasu, aż zostanie znaleziona odpowiedź, lub zostanie stwierdzone, że odpowiedzi nie ma.

Domyślna lista serwerów głównych w programie **iSeries(TM) Navigator.**
Z Internetowych serwerów głównych należy korzystać tylko wtedy, kiedy ma się połączenie z Internetem i chce się tłumaczyć nazwy hostów internetowych, które nie mogą być przetłumaczone przez lokalny serwer DNS. Domyślna lista Internetowych serwerów głównych jest dostępna w programie Operations Navigator. Lista jest aktualna na dzień wprowadzenia bieżącej wersji programu iSeries Navigator. Można sprawdzić aktualność domyślnej listy, porównując ją z listą w serwisie InterNIC. Należy aktualizować konfiguracyjną listę serwerów głównych, aby odpowiadała stanowi bieżącemu.

**Skąd wziąć adresy Internetowych serwerów głównych**
Adresy serwerów głównych najwyższego poziomu zmieniają się od czasu do czasu, a aktualizacja tych zmian jest obowiązkiem każdego administratora serwera DNS. Bieżącą listę adresów Internetowych serwerów głównych publikuje organizacja InterNIC. Aby uzyskać bieżącą listę Internetowych serwerów głównych, wykonaj następujące czynności:

1. połącz się poprzez anonimowe FTP z serwerem InterNIC: FTP.RS.INTERNIC.NET,
2. pobierz ten plik: /domain/named.root,
3. zapisz plik w katalogu o poniższej ścieżce: Integrated File System/Root/QIBM/ProdData/OS400/DNS/ROOT.FILE.

Serwer DNS znajdujący się za firewallem nie może mieć określonych serwerów głównych. W takim przypadku serwer DNS może tłumaczyć zapytania tylko na podstawie wpisów istniejących w jego własnych plikach bazy danych domeny podstawowej lub na podstawie zawartości jego pamięci podręcznej. Serwer taki może przekazywać zapytania skierowane poza domenę do serwera DNS firewalla. Wówczas serwer DNS firewalla będzie działał jako serwer przekazujący.

**Intranetowe serwery główne**
Jeśli dany serwer DNS jest częścią dużej sieci intranetowej, mogą w niej działać wewnętrzne serwery główne. Jeśli lokalny serwer DNS nie będzie miał dostępu do Internetu, nie trzeba ładować domyślnych Internetowych serwerów głównych. Należy jednak wpisać wewnętrzne serwery główne, aby lokalny serwer DNS mógł tłumaczyć wewnętrzne adresy spoza podległej mu domeny.

## Administrowanie systemem DNS

Po skonfigurowaniu serwera DNS przydatne mogą okazać się informacje przedstawione w następujących sekcjach:

**“Sprawdzanie działania DNS za pomocą komendy NSLookup” na stronie 28**
Komenda NSLookup pozwala sprawdzić, jak działa serwer DNS.

**“Zarządzanie kluczami ochrony” na stronie 28**
Klucze ochrony pozwalają ograniczyć dostęp do lokalnych danych DNS.

**“Statystyki serwera DNS” na stronie 29**
Zrzut bazy danych i narzędzia statystyczne mogą pomóc w ocenie wydajności serwera i w zarządzaniu nią.

**“Obsługa plików konfiguracyjnych DNS” na stronie 30**
W sekcji opisano pliki używane przez serwer DNS oraz przedstawiono wskazówki dotyczące ich archiwizowania i obsługi.

**“Zaawansowane funkcje DNS” na stronie 32**
W tej sekcji pokazano, w jaki sposób doświadczeni administratorzy mogą korzystać z funkcji zaawansowanych.

## Sprawdzanie działania DNS za pomocą komendy NSLookup

Komenda NSLookup (Name Server Lookup) służy do wysyłania zapytań o adresy IP do serwera DNS. Pozwala to sprawdzić, czy serwer odpowiada na zapytania. Można zażądać nazwy hosta powiązanej z adresem IP pętli zwrotnej (127.0.0.1). Serwer powinien zwrócić nazwę hosta lokalnego (localhost). Należy również wysłać zapytania dotyczące określonych nazw zdefiniowanych w sprawdzanej instancji serwera. Pozwoli to stwierdzić, że dana instancja serwera działa prawidłowo.

Aby sprawdzić działanie serwera DNS za pomocą komendy NSLookup, wykonaj następujące czynności:

1. W wierszu komend wpisz NSLOOKUP DMNNAMSVR(n.n.n.n), gdzie n.n.n.n jest adresem skonfigurowanym jako adres nasłuchiwania testowanej instancji.
2. W wierszu komend wpisz NSLOOKUP i naciśnij klawisz **Enter**. Uruchomi to sesję zapytania komendy NSLookup.
3. Wpisz server, a następnie nazwę lokalnego serwera i naciśnij klawisz **Enter**. Na przykład: server myiseries.mycompany.com.
   Zostaną wyświetlone następujące informacje:

   ```
   Server:  myiseries.mycompany.com
   Address: n.n.n.n
   ```

   Gdzie n.n.n.n będzie adresem IP danego serwera DNS.
4. W wierszu komend wpisz 127.0.0.1 i naciśnij klawisz **Enter**.
   Powinny zostać wyświetlone następujące informacje (w tym również nazwa hosta pętli zwrotnej):

   ```
    > 127.0.0.1
   Server:  myiseries.mycompany.com
   Address: n.n.n.n

   Name:    localhost
   Address:  127.0.0.1
   ```

   Serwer DNS odpowie prawidłowo, jeśli zwróci nazwę hosta pętli zwrotnej: **localhost**.
5. Aby zakończyć sesję terminalu komendy NSLOOKUP, wpisz exit i naciśnij klawisz **Enter**.

**Uwaga:** Aby uzyskać pomoc dotyczącą komendy NSLookup, należy wpisać ? i nacisnąć klawisz **Enter**.

## Zarządzanie kluczami ochrony

Istnieją dwa typy kluczy związanych z DNS. Każdy z nich pełni inną rolę w ochronie konfiguracji serwera DNS. Poniżej opisano ich związek z serwerem DNS.

### Klucze DNS

Klucz DNS jest kluczem zdefiniowanym dla programu BIND. Jest on używany przez serwer DNS jako element procesu weryfikacji przychodzącej aktualizacji. Klucz ten można skonfigurować i przypisać mu nazwę. Następnie, chcąc zabezpieczyć obiekt DNS, na przykład strefę dynamiczną, można wpisać klucz na listę AML (Address Match List).

Aby zarządzać kluczami DNS, wykonaj następujące czynności:

1. W **iSeries Navigator** rozwiń **serwer iSeries(TM)** —> **Sieć** —> **Serwery** —> **DNS**.

2. W prawym panelu okna kliknij prawym klawiszem myszy instancję serwera DNS, którą chcesz otworzyć, i wybierz **Konfiguracja**.
3. W oknie **Konfiguracja DNS** wybierz **Plik** > **Zarządzaj kluczami...**

**Klucze aktualizacji dynamicznej**
Klucze aktualizacji dynamicznej są używane do ochrony aktualizacji dynamicznych dokonywanych przez serwer DHCP. Klucze te muszą być obecne, gdy serwery DNS i DHCP działają na tym samym serwerze iSeries. Jeśli serwer DHCP działa na innym serwerze iSeries, w celu dopuszczenia bezpiecznych aktualizacji dynamicznych należy utworzyć taki sam klucz aktualizacji dynamicznej na każdym serwerze iSeries.

Aby zarządzać kluczami aktualizacji dynamicznej, wykonaj następujące czynności:

1. W **iSeries Navigator** rozwiń **serwer iSeries** —> **Sieć** —> **Serwery** —> **DNS**.
2. Kliknij prawym klawiszem myszy **DNS** i wybierz **Zarządzaj dynamicznym aktualizowaniem kluczy...**

## Statystyki serwera DNS

System DNS udostępnia kilka narzędzi diagnostycznych. Można ich używać do monitorowania wydajności lokalnego serwera.

**Statystyki serwera**
System DNS umożliwia przeglądanie statystyk dla każdej instancji serwera. Statystyki te zawierają podsumowanie liczby zapytań i odpowiedzi odebranych przez serwer od czasu ostatniego restartu lub przeładowania bazy danych. Nowe informacje są w sposób ciągły dopisywane do tego pliku, aż do jego usunięcia. Informacje te mogą być przydatne do oceny natężenia ruchu odbieranego przez serwer oraz do rozwiązywania problemów. Więcej informacji o statystykach serwera można znaleźć w temacie pomocy elektronicznej dla systemu DNS **Podstawy statystyk serwera DNS**.

Aby obejrzeć statystyki serwera, wykonaj następujące czynności:

1. W **iSeries Navigator** rozwiń **serwer iSeries(TM)** —> **Sieć** —> **Serwery** —> **DNS**.
2. W prawym panelu okna kliknij prawym klawiszem myszy **serwer DNS** i wybierz **Konfiguracja**.
3. W oknie **Konfiguracja DNS** wybierz **Widok** —> **Statystyki serwera**.

**Baza danych aktywnego serwera**
System DNS umożliwia przeglądanie zrzutu danych autorytatywnych, danych z pamięci podręcznej i wskazówek dla poszczególnych instancji serwera. Zrzut obejmuje informacje ze wszystkich podstawowych i zapasowych stref serwera (stref wyszukiwania do przodu i wstecz), a także informacje uzyskane przez serwer na podstawie zapytań. Baza danych zawiera informacje o strefie i o hoście, w tym niektóre właściwości strefy, jak na przykład informację o początku uprawnień (SOA), oraz właściwości hosta, na przykład informacje o wymienniku poczty (MX). Informacje te mogą być przydatne podczas rozwiązywania problemów.

Zrzut bazy danych aktywnego serwera można przeglądać za pomocą programu Operations Navigator. Gdyby trzeba było zeskładować kopię plików, plik zrzutu bazy danych o nazwie NAMED_DUMP.DB znajduje się na lokalnym serwerze iSeries w katalogu **Integrated File System**/**Root**/**QIBM**/**UserData**/**OS400**/**DNS**/**<instancja serwera>**, gdzie ″<instancja serwera>″ jest nazwą instancji serwera DNS. Więcej informacji o bazie danych aktywnego serwera można znaleźć w temacie pomocy elektronicznej dla systemu DNS **Podstawy operacji zrzutu bazy danych serwera DNS**.

Aby obejrzeć zrzut bazy danych aktywnego serwera, wykonaj następujące czynności:

1. W **iSeries Navigator** rozwiń **serwer iSeries** —> **Sieć** —> **Serwery** —> **DNS**.
2. W prawym panelu okna kliknij prawym klawiszem myszy **serwer DNS** i wybierz **Konfiguracja**.
3. W oknie **Konfiguracja DNS** wybierz **Widok** —> **Aktywna baza danych serwera**.

## Obsługa plików konfiguracyjnych DNS

Implementacja DNS w systemie OS/400(R) umożliwia tworzenie instancji serwera DNS na lokalnym serwerze iSeries(TM) i zarządzanie nimi. Pliki konfiguracyjne systemu DNS są zarządzane za pomocą programu iSeries Navigator. Plików tych nie wolno zmieniać ręcznie. Do tworzenia, zmiany lub usuwania plików konfiguracyjnych DNS należy zawsze używać programu iSeries Navigator. Pliki te są przechowywane w katalogach zintegrowanego systemu plików o ścieżkach podanych poniżej.

**Uwaga:** Poniższa struktura plików odnosi się do serwera DNS wykorzystującego program BIND 8. Jeśli używany jest serwer DNS korzystający z programu BIND 4.9.3, należy zapoznać się z sekcją *Składowanie plików konfiguracyjnych DNS i obsługa plików protokołu* w dokumencie V4R5 DNS Information Center (około 62 strony).

Pliki w poniższej tabeli są wymienione według przedstawionej hierarchii ścieżek. Pliki oznaczone ikoną kopii zapasowej powinny być zarchiwizowane w celu zabezpieczenia danych. Pliki oznaczone ikoną usuwania powinny być okresowo usuwane.

| Nazwa | | Opis |
|---|---|---|
| **QIBM/UserData/OS400/DNS/** | | Katalog początkowy systemu DNS. |
| ATTRIBUTES | | System DNS korzysta z tego pliku do określenia używanej wersji programu BIND. |
| **QIBM/UserData/OS400/DNS/<*nazwa_instancji*>/** | | Katalog początkowy instancji serwera DNS. |
| ATTRIBUTES | | Atrybuty konfiguracyjne używane przez serwer DNS w systemie iSeries. |
| NAMED.CONF | | Ten plik zawiera dane konfiguracyjne. Jest on używany do poinformowania serwera, gdzie znajdują się pliki stref, które strefy mogą być dynamicznie aktualizowane, gdzie znajdują się serwery przekazujące oraz inne ustawienia opcji. |
| BOOT.AS400BIND4 | | Plik konfiguracji i reguł serwera BIND 4.9.3, który zostanie poddany konwersji na plik NAMED.CONF programu BIND 8 dla tej instancji. Plik ten jest tworzony podczas migracji z programu BIND 4.9.3 do programu BIND 8. Jest on kopią zapasową na potrzeby migracji i może zostać usunięty, jeśli serwer BIND 8 działa prawidłowo. |
| NAMED.CA | | Lista serwerów głównych dla tej instancji serwera. |
| NAMED_DUMP.DB | | Zrzut danych serwera utworzony dla “Statystyki serwera DNS” na stronie 29. |
| NAMED.STATS | | “Statystyki serwera DNS” na stronie 29. |

| Nazwa | | Opis |
|---|---|---|
| NAMED.PID | | Przechowuje adres IP działającego serwera. Plik ten jest tworzony podczas każdego uruchomienia serwera DNS. Jest on używany przez funkcje bazy danych, statystyk i aktualizacji serwera. Pliku tego nie wolno usuwać ani zmieniać. |
| QUERYLOG |  | Protokół serwera DNS z odebranymi zapytaniami. Plik jest tworzony, kiedy serwer DNS ma włączone protokołowanie. Wówczas jednak ten plik staje się duży i powinien być okresowo usuwany. |
| *<nazwa-strefy-a>*.DB |  | Plik strefy dla konkretnej domeny, która ma być obsługiwana przez ten serwer. Zawiera wszystkie rekordy zasobów dla tej strefy. |
| *<nazwa-strefy-b>*.DB |  | Plik strefy dla konkretnej domeny, która ma być obsługiwana przez ten serwer. Zawiera wszystkie rekordy zasobów dla tej strefy. Każda strefa ma osobny plik .DB. |
| *.ixfr.* |  | Pliki przyrostowego przesyłania strefowego (IXFR). Pliki te są używane przez serwery zapasowe do ładowania tylko tych danych, które zmieniły się od czasu ostatniego przesyłania strefowego. W miarę kolejnych aktualizacji liczba plików IXFR będzie rosła. Należy okresowo usuwać starsze pliki IXFR. Pozostawienie plików utworzonych w ciągu ostatniego dnia lub dwóch w dalszym ciągu pozwoli większości serwerów zapasowych przeprowadzić przesyłanie IXFR. Jeśli wszystkie pliki IFXR zostaną usunięte, serwery zapasowe zażądają pełnego przesyłania (AFXR). |
| TMP | | Katalog używany przez instancję serwera do tworzenia tymczasowych plików roboczych. |
| **QIBM/UserData/OS400/DNS/TMP** | | Katalog tymczasowy używany przez program QTOBH2N do tworzenia plików pośrednich zrzuconych z tabeli hostów, w celu późniejszego zaimportowania za pomocą programu iSeries Navigator. |
| **QIBM/UserData/OS400/DNS/_DYN/** | | Katalog, w którym przechowywane są pliki wymagane podczas aktualizacji dynamicznych. |
| *<nazwa-id_klucza-x>*._KID |  | Plik zawierający instrukcję klucza BIND 8 dla id_klucza o nazwie *<nazwa_id_klucza_x>*. |

| Nazwa | | Opis |
|---|---|---|
| <*nazwa-id_klucza-x*>._DUK.<*nazwa-strefy-a*> |  | Klucz aktualizacji dynamicznej wymagany do zainicjowania żądania aktualizacji dynamicznej do strefy <*nazwa-strefy-a*> za pomocą klucza <*nazwa-id_klucza-x*>. |
| <*nazwa-id_klucza-y*>._KID |  | Plik zawierający instrukcję klucza BIND 8 dla id_klucza o nazwie <*nazwa_id_klucza_y*>. |
| <*nazwa-id_klucza-y*>._DUK.<*nazwa-strefy-a*> |  | Klucz aktualizacji dynamicznej wymagany do zainicjowania aktualizacji dynamicznej do strefy <*nazwa_strefy_a*> za pomocą klucza <*nazwa_id_klucza_y*>. |
| <*nazwa-id_klucza-y*>._DUK.<*nazwa-strefy-b*> |  | Klucz aktualizacji dynamicznej wymagany do zainicjowania żądania aktualizacji dynamicznej do strefy <*nazwa_strefy_b*> za pomocą klucza <*nazwa_id_klucza_y*>. |

## Zaawansowane funkcje DNS

Funkcje DNS w programie iSeries Navigator udostępniają interfejs do konfigurowania serwera DNS i zarządzania nim. Poniższe zadania są skróconymi instrukcjami dla administratorów, którzy znają graficzny interfejs serwera iSeries. Przedstawiają one metody szybkiej zmiany statusu serwera i atrybutów dla wielu instancji jednocześnie.

### Zmiana atrybutów DNS

Interfejs DNS nie pozwala na jednoczesną zmianę wartości autostartu i poziomów debugowania dla wszystkich instancji serwera. Do zmiany tych ustawień dla poszczególnych instancji serwera DNS lub dla wszystkich instancji jednocześnie można użyć interfejsu znakowego. Aby skorzystać z komendy CHGDNSA, wykonaj następujące czynności:

1. W wierszu komend wpisz CHGDNSA i naciśnij klawisz **F4**.
2. Na stronie Zmiana atrybutów serwera DNS (Change DNS Server Attributes - CHGDNSA) wpisz nazwę pojedynczej instancji serwera lub *ALL i naciśnij klawisz **Enter**.

   Zostaną wyświetlone dostępne opcje atrybutów serwera:
   Autostart serwera. . . . . *SAME *YES, *NO, *SAME
   Poziom debugowania . . . . . *SAME 0-11, *SAME, *DFT
3. **Autostart** Aby wybrany serwer DNS uruchamiał się automatycznie podczas startu TCP/IP, wpisz *YES. Jeśli nie chcesz, aby serwer uruchamiał się automatycznie podczas startu TCP/IP, wpisz *NO. Aby pozostawić bieżące ustawienia atrybutu, należy wpisać *SAME.

   **Poziom debugowania** Aby zmienić poziom debugowania używany przez wybrany serwer DNS, należy wpisać wartość z zakresu od 0 do 11. Wpisanie *DFT spowoduje, że poziom debugowania zostanie odziedziczony z wartości uruchomieniowej serwera. Aby pozostawić bieżące ustawienia atrybutu, należy wpisać *SAME.

   Po ustawieniu wszystkich preferencji naciśnij klawisz **Enter**, aby ustawić wartości atrybutów DNS.

### Uruchamianie lub zatrzymywanie serwerów DNS

Interfejs DNS nie pozwala na jednoczesne uruchomienie lub zatrzymanie wielu instancji serwera. Do zmiany tych ustawień dla wszystkich instancji jednocześnie można użyć interfejsu znakowego. Aby za pomocą interfejsu znakowego uruchomić wszystkie instancje serwera DNS jednocześnie, należy w wierszu komend wpisać STRTCPSVR SERVER(*DNS) DNSSVR(*ALL). Aby zatrzymać wszystkie serwery DNS jednocześnie, należy w wierszu komend wpisać ENDTCPSVR SERVER(*DNS) DNSSVR(*ALL).

### Zmiana wartości debugowania

Interfejs DNS w programie iSeries Navigator nie pozwala na zmianę poziomu debugowania podczas pracy

serwera. Czynność tę można jednak wykonać za pomocą interfejsu znakowego. Funkcja ta może być przydatna dla administratorów dużych stref, którzy nie chcą dużych ilości danych debugowania, generowanych, kiedy serwer jest uruchamiany po raz pierwszy i ładuje wszystkie dane stref. Aby zmienić poziom debugowania za pomocą interfejsu znakowego, wykonaj następujące czynności, wpisując w miejsce <instancja> nazwę instancji serwera:

1. W wierszu komend wpisz ADDLIBLE QDNS i naciśnij klawisz **Enter**.
2. Zmień poziom debugowania:
   - Aby włączyć debugowanie lub zwiększyć poziom debugowania o jeden, wpisz CALL QTOBDRVS ('BUMP' '<instancja>') i naciśnik klawisz **Enter**.
   - Aby wyłączyć debugowanie, wpisz CALL QTOBDRVS ('OFF' '<instancja>') i naciśnik klawisz **Enter**.

## Rozwiązywanie problemów z systemem DNS

System DNS działa podobnie, jak inne funkcje i aplikacje TCP/IP. Podobnie jak aplikacje SMTP lub FTP, zadania DNS działają w podsystemie QSYSWRK i w ramach profilu użytkownika QTCP generują protokoły zadań z informacjami dotyczącymi zadań DNS. Jeśli zadanie DNS zostaje zakończone, można użyć protokołu zadania do określenia przyczyny. Jeśli serwer DNS nie zwraca oczekiwanych odpowiedzi, protokoły zadań mogą zawierać informacje pomocne w analizie problemu.

Konfiguracja systemu DNS składa się z kilku plików z kilkoma różnymi typami rekordów w każdym z nich. Problemy z serwerem DNS są najczęściej spowodowane przez nieprawidłowe wpisy do jego plików konfiguracyjnych. W przypadku wystąpienia problemu, należy sprawdzić, czy pliki te zawierają odpowiednie wpisy.

**"Protokołowanie serwera DNS" na stronie 34**
W systemie DNS dostępnych jest wiele opcji protokołowania, których ustawienia można dostosować, próbując znaleźć źródło problemu. Protokołowanie zapewnia elastyczność, oferując liczne możliwości dobrania parametrów protokołowania, takich jak poziomy istotności, kategorie komunikatów i pliki wyjściowe, które mogą pomóc w znalezieniu przyczyny problemu.

**"Ustawienia debugowania DNS" na stronie 35**
W systemie DNS dostępnych jest 12 poziomów debugowania. Zwykle protokołowanie jest łatwiejszą metodą rozwiązywania problemów, ale niekiedy konieczne może być użycie debugowania. W normalnych warunkach debugowanie jest wyłączone (wartość = 0).

**"Inne informacje dotyczące DNS" na stronie 35**
Ogólne informacje o rozwiązywaniu problemów z systemem DNS są dostępne w wielu źródłach. W szczególności, godna polecenia jest książka wydawnictwa O'Reilly DNS and BIND, a katalog zasobów DNS zawiera odsyłacze do grup dyskusyjnych dla administratorów serwerów DNS.

**Identyfikowanie zadań**
Przeszukując protokół zadania w celu sprawdzenia działania serwera DNS (na przykład za pomocą komendy WRKACTJOB), należy wziąć pod uwagę następujące wskazówki dotyczące nazewnictwa:

- Jeśli używany jest program BIND 4.9.3, zadanie serwera będzie nazywać się QTOBDNS. Więcej informacji o debugowaniu serwera DNS 4.9.3 można znaleźć w sekcji *Rozwiązywanie poblemów dotyczących serwerów DNS* w dokumencie V4R5 DNS Information Center  (około 357 kB).
- W przypadku serwera wykorzystującego program BIND 8, każda działająca instancja serwera będzie miała odrębne zadanie. Nazwa każdego zadania to pięć stałych znaków (QTOBD) z następującą po nich nazwą instancji. Jeśli na przykład w systemie działają dwie instancje, INST1 i INST2, ich zadania będą nazywać się QTOBDINST1 i QTOBDINST2.

## Protokołowanie serwera DNS

Program BIND 8 oferuje kilka nowych opcji protokołowania. Można obecnie określić typy protokołowanych komunikatów, miejsca do których zostały wysłane, i poziom istotności dla każdego typu komunikatu. W ogólności wszystkie domyślne ustawienia protokołowania powinny być dopasowane i przed ich zmianą warto skorzystać z innych “Inne informacje dotyczące DNS” na stronie 35 informacji o programie BIND 8.

**Kanały protokołowania**

Serwer DNS może protokołować komunikaty do różnych kanałów wyjściowych. Kanały te określają, dokąd wysyłane są komunikaty. Można wybrać następujące typy kanałów:

- **Kanały zbiorów**
  Komunikaty protokołowane do kanałów zbiorów są wysyłane do zbioru. Domyślne kanały zbiorów to as400_debug i as400_QPRINT. Komunikaty debugowania są domyślnie protokołowane do kanału as400_debug, który jest zbiorem NAMED.RUN. W zbiorze tym można jednak protokołować inne kategorie komunikatów. Kategorie komunikatów protokołowanych w kanale as400_QPRINT są wysyłane do zbioru buforowego QPRINT z profilem użytkownika QTCP. Oprócz domyślnych kanałów zbiorów, można również tworzyć własne.
- **Kanały Syslog**
  Komunikaty protokołowane w tym kanale są wysyłane do protokołu zadania serwera. Domyślnym kanałem syslog jest as400_joblog. Komunikaty kierowane do tego kanału są wysyłane do protokołu zadania instancji serwera DNS.
- **Kanały null**
  Wszystkie komunikaty protokołowane do kanału null zostaną usunięte. Domyślnym kanałem null jest as400_null. Aby określone kategorie komunikatów nie pojawiały się w żadnym pliku protokołu, można je kierować do kanału null.

**Kategorie komunikatów**

Komunikaty są zgrupowane w kategorie. Można określić, jakie kategorie powinny być protokołowane w każdym kanale. Istnieje wiele kategorii, w tym:

- config: przetwarzanie pliku konfiguracyjnego,
- db: operacje bazy danych,
- queries: krótkie komunikaty dla każdego zapytania odebranego przez serwer,
- lame-servers: wykrycie nieprawidłowych delegacji,
- update: aktualizacje dynamiczne,
- xfer-in: przesyłania strefowe odbierane przez serwer,
- xfer-out: przesyłania strefowe wysyłane przez serwer.

Pliki protokołów mogą znacznie zwiększać swoją objętość, więc należy je okresowo usuwać. Podczas zatrzymania, a następnie uruchomienia serwera DNS zawartość wszystkich plików protokołu serwera DNS jest usuwana.

**Poziom ważności komunikatu**

Kanały umożliwiają filtrowanie komunikatów według ich poziomu ważności. Dla każdego kanału można określić poziom ważności, począwszy od którego komunikaty będą protokołowane. Dostępne są następujące poziomy ważności komunikatów:

- Krytyczne,
- Błąd,
- Ostrzeżenie,
- Uwaga,
- Informacja,
- Debugowanie (należy podać poziom debugowania z zakresu 0-11),
- Dynamiczne (odziedziczone na podstawie początkowego poziomu ważności serwera).

Wszystkie komunikaty o poziomie ważności nie niższym od wybranego, są protokołowane. Jeśli na przykład zostanie wybrany poziom Ostrzeżenie, w kanale zostaną zaprotokołowane komunikaty z poziomem Ostrzeżenie, Błąd i Krytyczny. Jeśli zostanie wybrany poziom Debugowanie, można określić wartość od 0 do 11, dla której komunikaty debugowania będą protokołowane.

**Zmiana ustawień protokołowania**
Aby uzyskać dostęp do opcji protokołowania, wykonaj następujące czynności:

1. W **iSeries Navigator** rozwiń **serwer iSeries(TM)** —> **Sieć** —> **Serwery** —> **DNS**.
2. W prawym panelu okna kliknij prawym klawiszem myszy **serwer DNS** i wybierz **Konfiguracja**.
3. W oknie **Konfiguracja DNS** kliknij prawym klawiszem myszy **Serwer DNS** i wybierz **Właściwości**.
4. W oknie **Właściwości serwera** wybierz zakładkę **Kanały**, aby utworzyć nowe kanały zbioru lub właściwości kanału, takie jak poziom ważności komunikatów protokołowanych w każdym kanale.
5. W oknie **Właściwości serwera** wybierz zakładkę **Protokołowanie**, aby określić, jakie kategorie komunikatów mają być protokołowane w każdym kanale.

**Wskazówka do rozwiązywania problemów**
Domyślny poziom ważności komunikatu dla kanału as400_joblog to Błąd. Ustawienie to ma na celu wyeliminowanie komunikatów ostrzegawczych i informacyjnych, które w przeciwnym razie byłyby protokołowane. Jeśli pojawiają się problemy, a protokół zadania nie wskazuje ich źródeł, można zmienić poziom ważności komunikatu. Postępując według powyższej procedury należy wyświetlić stronę Kanały i zmienić poziom ważności dla kanału as400_joblog na Ostrzeżenie, Uwaga lub Informacja, tak aby można było zobaczyć więcej zaprotokołowanych danych. Po rozwiązaniu problemu, należy przywrócić poziom ważności Błąd, aby zredukować liczbę komunikatów w protokole zadania.

## Ustawienia debugowania DNS

Funkcje debugowania DNS dostarczają informacji, które mogą pomóc w określeniu i rozwiązaniu problemów z serwerem DNS. Zaleca się jednak, aby do rozwiązywania problemów użyć najpierw protokołowania.

Poprawne poziomy debugowania należą do zakresu od 1 do 11. W określeniu wartości debugowania odpowiedniej do zdiagnozowania problemu z serwerem DNS może pomóc przedstawiciel serwisu IBM. Wartości większe od zera powodują zapisywanie informacj debugowania w pliku NAMED.RUN na serwerze iSeries w katalogu **Integrated File System**/**Root**/**QIBM**/**UserData**/**OS400**/**DNS**/**<instancja serwera>**, gdzie ″<instancja serwera>″ jest nazwą instancji serwera DNS. Kiedy poziom debugowania ma wartość większą od 0 i serwer DNS działa, plik NAMED.RUN stale zwiększa swoją objętość. Zaleca się usuwanie go od czasu do czasu, aby nie zabierał zbyt wiele miejsca na dysku. Można również skorzystać ze strony **Właściwości serwera** - **Kanały**, aby określić maksymalną wielkość i liczbę wersji pliku NAMED.RUN.

Aby zmienić wartość debugowania dla instancji serwera DNS, wykonaj następujące czynności:

1. W **iSeries Navigator** rozwiń **serwer iSeries** —> **Sieć** —> **Serwery** —> **DNS**.
2. W prawym panelu okna kliknij prawym klawiszem myszy **serwer DNS** i wybierz **Konfiguracja**.
3. W oknie **Konfiguracja DNS** kliknij prawym klawiszem myszy serwer DNS i wybierz **Właściwości**.
4. Na stronie **Właściwości serwera - Ogólne** podaj początkowy poziom debugowania serwera.
5. Jeśli serwer działa, zatrzymaj go i restartuj.
   **Uwaga:** Zmiany poziomu debugowania nie odniosą skutku, jeśli serwer działa. Ustawiony poziom debugowania zostanie zastosowany podczas następnego pełnego restartu serwera. Aby zmienić poziom debugowania podczas pracy serwera, należy skorzystać z instrukcji opisanych w sekcji “Zaawansowane funkcje DNS” na stronie 32

## Inne informacje dotyczące DNS

Istnieje wiele źródeł informacji dotyczących systemu DNS i programu BIND 8. Poniższa lista to tylko niewielka część dostępnych zasobów:

- DNS and BIND, wydanie trzecie. Paul Albitz i Cricket Liu. Wydane przez O'Reilly and Associates,Inc. Sebastopol, California, 1998. ISBN: 1-56592-512-2. To jedno z najbardziej kompetentnych źródeł dotyczących systemu DNS.
- Serwis WWW Internet Software Consortium zawiera aktualności, odsyłacze i inne zasoby dotyczące programu BIND.
- W serwisie InterNIC Publikowany jest katalog wszystkich podmiotów rejestrujących nazwy domen autoryzowanych przez Internet Corporation for Assigned Names and Numbers (ICANN).
- Serwis DNS Resources Directory zawiera materiały pomocnicze dotyczące DNS oraz odsyłacze do wielu innych zasobów poświęconych DNS, w tym do grup dyskusyjnych. W serwisie znajduje się również wykaz dokumentów RFC dotyczących DNS .

**Podręczniki i dokumentacja techniczna IBM(TM)**

- AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support

  Dokumentacja techniczna zawiera opis obsługi serwerów systemu nazw domen (DNS) i protokołu DHCP (Dynamic Host Configuration Protocol) w systemie OS/400(R). Informacje i przykłady zawarte w tej dokumentacji pomagają zainstalować, dostosować i skonfigurować obsługę DNS i DHCP, a także rozwiązywać ewentualne problemy.
  **Uwaga:** Ta dokumentacja techniczna nie zawiera opisu funkcji programu BIND 8 dostępnych w wersji V5R1. Mimo to jest ona dobrym źródłem informacji o ogólnych koncepcjach DNS.

# Dodatek. Uwagi

Niniejsza publikacja została przygotowana z myślą o produktach i usługach oferowanych w Stanach Zjednoczonych.

IBM może nie oferować w innych krajach produktów, usług lub opcji omawianych w tej publikacji. Informacje o produktach i usługach dostępnych w danym kraju można uzyskać od lokalnego przedstawiciela IBM. Jakakolwiek wzmianka na temat produktu, programu lub usługi firmy IBM nie oznacza, że tylko ten produkt, program lub ta usługa mogą być używane. Wykorzystany może być dowolny, funkcjonalnie równoważny, produkt, program lub usługa, o ile nie łamie to praw autorskich firmy IBM. Odpowiedzialność za sprawdzenie działania produktu, programu lub usługi nie pochodzących od firmy IBM spoczywa jednak na użytkowniku.

IBM może posiadać patenty lub złożone wnioski patentowe na towary i usługi, o których mowa w niniejszej publikacji. Przedstawienie tej publikacji nie daje żadnych uprawnień licencyjnych do tychże patentów. Zapytania dotyczące licencji można wysłać na piśmie pod adresem:

```
IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY  10594-1785
U.S.A.
```

Zapytania w sprawie licencji na informacje dotyczące zestawów znaków dwubajtowych (DBCS) należy kierować do lokalnych działów własności intelektualnej IBM (IBM Intellectual Property Department) lub zgłaszać na piśmie pod adresem:

```
IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan
```

**Poniższy akapit nie obowiązuje w Wielkiej Brytanii, a także w innych krajach, w których jego treść pozostaje w sprzeczności z lokalnymi przepisami prawa:** FIRMA INTERNATIONAL BUSINESS MACHINES CORPORATION DOSTARCZA TĘ PUBLIKACJĘ W TAKIM STANIE, W JAKIM SIĘ OBECNIE ZNAJDUJE, ″AS IS″, BEZ JAKICHKOLWIEK GWARANCJI (W TYM TAKŻE RĘKOJMI), WYRAŹNYCH LUB DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ ORAZ PRZYDATNOŚCI DO OKREŚLONEGO CELU LUB GWARANCJI, ŻE PUBLIKACJA TA NIE NARUSZA PRAW OSÓB TRZECICH. Niektóre państwa nie zezwalają na nieudzielanie gwarancji przy określonych transakcjach, zatem informacje te nie dotyczą każdego.

Informacje zawarte w tej publikacji mogą zawierać techniczne nieścisłości lub błędy typograficzne. Okresowo informacje te ulegają zmianom; zmiany te zostaną uwzględnione w następnych wydaniach tej publikacji. Firma IBM może wprowadzić ulepszenia lub zmiany w produktach lub programach opisanych w tej publikacji w dowolnej chwili bez wcześniejszego ostrzeżenia.

Jakiekolwiek wzmianki na temat stron internetowych nie należących do firmy IBM zostały podane jedynie dla wygody użytkownika i nie oznaczają, że firma IBM w jakikolwiek sposób firmuje te strony. Materiały zawarte na tych stronach nie wchodzą w skład dokumentacji opisanego produktu firmy IBM i można ich używać jedynie na własną odpowiedzialność.

Firma IBM może używać lub rozpowszechniać dowolne informacje dostarczone przez użytkownika bez żadnych zobowiązań z tego tytułu.

Informacje na temat możliwości stosowania tego programu, takie jak: (i) wymiana informacji między niezależnie tworzonymi programami a innymi programami (włącznie z tym programem) czy (ii) wspólne używanie wymienianych informacji, można uzyskać pod adresem:

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Informacje takie mogą być udostępnione na odpowiednich warunkach, w niektórych przypadkach za opłatą.

Licencjonowany program opisany w tej publikacji i wszystkie inne licencjonowane materiały dostępne dla tego programu są dostarczane przez firmę IBM na warunkach określonych w Umowie IBM z Klientem, Międzynarodowej Umowie Licencyjnej IBM na Program lub w innych podobnych umowach zawartych między firmą IBM a użytkownikami.

Jeżeli niniejsza publikacja jest przeglądana w postaci elektronicznej, mogą nie pojawiać się zdjęcia i kolorowe ilustracje.

## Znaki towarowe

Następujące nazwy są znakami towarowymi firmy International Business Machines Corporation w Stanach Zjednoczonych i/lub innych krajach:
Application System/400
AS/400
e (logo)
IBM
iSeries
Operating System/400
OS/400
400

Lotus, Freelance i WordPro Notes są znakami towarowymi firm International Business Machines Corporation i Lotus Development Corporation w Stanach Zjednoczonych i/lub w innych krajach.

C-bus jest znakiem towarowym firmy Corollary, Inc. w Stanach Zjednoczonych i/lub w innych krajach.

ActionMedia, LANDesk, MMX, Pentium i ProShare są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Intel Corporation w Stanach Zjednoczonych i/lub w innych krajach.

Microsoft, Windows, Windows NT i logo Windows są znakami towarowymi Microsoft Corporation w Stanach Zjednoczonych i/lub w innych krajach.

SET i logo SET Logo są znakami towarowymi, będącymi własnością firmy SET Secure Electronic Transaction LLC.

Java i wszystkie znaki towarowe związane z językiem Java są znakami towarowymi Sun Microsystems, Inc. w Stanach Zjednoczonych i/lub w innych krajach.

UNIX jest zastrzeżonym znakiem towarowym Open Group w Stanach Zjednoczonych i w innych krajach.

Nazwy innych firm, produktów i usług mogą być znakami towarowymi lub znakami usług innych podmiotów gospodarczych.

## Warunki pobierania i drukowania publikacji

Używanie publikacji, która zostanie pobrana, podlega następującym warunkom, na które zgadza się użytkownik.

**Użytek osobisty:** publikacje te wolno powielać do niekomercyjnego osobistego użytku pod warunkiem, że zostaną zachowane wzmianki o prawach autorskich. Publikacji tych ani ich fragmentów nie wolno rozpowszechniać, wyświetlać lub wykorzystywać do własnych opracowań bez wyraźnej zgody IBM.

**Użytek komercyjny:** publikacje te wolno powielać, rozpowszechniać i wyświetlać jedynie wewnątrz firmy pod warunkiem, że zostaną zachowane wzmianki o prawach autorskich. Publikacji tych ani ich fragmentów nie wolno rozpowszechniać, wyświetlać lub wykorzystywać do własnych opracowań na zewnątrz firmy bez wyraźnej zgody IBM.

Poza uprawnieniami wyraźnie określonymi w tym zezwoleniu, użytkownik nie nabywa żadnych licencji oraz praw, zarówno wyraźnych jaki i domniemanych, do publikacji lub dowolnych informacji, danych, oprogramowania lub innych zawartych w nich własności intelektualnych.

IBM rezerwuje sobie w dowolnej chwili i według własnego uznania, prawa do wycofania niniejszych uprawnień do używania publikacji jeżeli uzna, że używanie publikacji przynosi szkodę interesom firmy IBM lub, zdaniem IBM, powyższa instrukcja nie jest właściwie przestrzegana.

Nie wolno pobierać, eksportować lub ponownie eksportować tych informacji, za wyjątkiem sytuacji, gdy zostanie zapewnione przestrzeganie wszystkich regulacji prawnych, włączając w to prawa eksportowe USA. IBM NIE DAJE ŻADNYCH GWARANCJI CO DO ZAWARTOŚCI TYCH PUBLIKACJI. PUBLIKACJE SĄ DOSTARCZANE ″TAKIE JAKIE SĄ″ BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI, WYRAŹNYCH LUB DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ ORAZ PRZYDATNOŚCI DO OKREŚLONEGO CELU.

IBM posiada prawa autorskie do wszystkich materiałów.

Poprzez fakt pobrania lub wydrukowania publikacji zawartych na tej stronie użytkownik potwierdza, że zgadza się na powyższe warunki.