System i

Sieciowy system nazw domen

Wersja 6 wydanie 1

System i

Sieciowy system nazw domen

Wersja 6 wydanie 1

Uwaga

Przed skorzystaniem z tych informacji oraz z produktu, którego dotyczą, należy przeczytać informacje zawarte w sekcji “Uwagi”, na stronie 43.

Niniejsze wydanie dotyczy wersji 6, wydania 1, modyfikacji 0 systemu IBM i5/OS (numer produktu 5761-SS1) oraz wszelkich kolejnych wersji i modyfikacji tego produktu, o ile w nowych wydaniach nie określono inaczej. Wersja ta nie działa na wszystkich modelach komputerów z procesorem RISC ani na modelach z procesorem CISC.

Spis treści

System nazw domen

System nazw domen (DNS) to system rozproszonej bazy danych służący do zarządzania nazwami hostów i powiązanymi z nimi adresami IP.

Dzięki systemowi DNS użytkownicy mogą znaleźć host, używając prostych nazw, takich jak www.jkltoys.com, zamiast adresów IP, jak na przykład 192.168.12.88 (IPv4) lub 2001:D88::1 (IPv6). Pojedynczy serwer 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. Dzięki współpracującym ze sobą serwerom DNS komputery mogą komunikować się przez Internet.

W systemie IBM i5/OS wersja 6, wydanie 1 (V6R1) usługi DNS są oparte na standardowej implementacji DNS znanej jako BIND (Berkeley Internet Name Domain) w wersji 9. W poprzednich wersjach systemu i5/OS usługi DNS były oparte na programie BIND w wersji 8.2.5. Aby korzystać z serwera DNS z nową wersją BIND 9, na platformie IBM System i należy zainstalować opcję 31 (DNS) i 33 (Portable Application Solutions Environment - PASE) systemu i5/OS. Począwszy od wersji systemu i5/OS V6R1, wersje BIND 4 i 8 zostały ze względów bezpieczeństwa zastąpione wersją BIND 9. Dlatego też jest wymagana migracja serwera DNS do wersji BIND 9.

Co nowego w wersji V6R1

Poniżej opisano nowe i zmienione informacje w kolekcji tematów dotyczącej systemu DNS.

BIND 9

Wprowadzony w tym wydaniu program BIND (Berkeley Internet Name Domain) w wersji 9 oferuje kilka funkcji, które zwiększają wydajność serwera DNS. Obsługuje na przykład wyszukiwania typu nazwa/adres i adres/nazwa we wszystkich obecnie zdefiniowanych formularzach IPv6. Używa instrukcji *widok* (View), która pozwala pojedynczej instancji DNS udzielać różnych odpowiedzi na zapytania w zależności od źródła pochodzenia zapytania, takiego jak Internet lub intranet. Ponadto w zbiorach kroniki przechowuje dynamiczne aktualizacje strefy.

Poprzednie wersje BIND 4.9.3 i BIND 8.2.5 nie są już obsługiwane i należy wykonać ich migrację do wersji BIND 9.

Nowe komendy konfiguracji

Zostały dodane następujące komendy konfiguracji w celu ułatwienia zarządzania zbiorami konfiguracyjnymi DNS w systemie.

Tworzenie konfiguracji RNDC (Create RNDC Configuration - CRTRNDCCFG)
Program narzędziowy konfiguracji RNDC (RNDC Configuration Utility - CRTRNDCCFG) służy do generowania zbiorów konfiguracyjnych RNDC. Jest to wygodna alternatywa dla pisania zbioru rndc.conf i odpowiadających mu elementów sterujących oraz instrukcji kluczy w zbiorze named.conf.

Program narzędziowy konfiguracji DNS (DNS Configuration Utility - CHKDNSCFG)
Program narzędziowy konfiguracji DNS (CHKDNSCFG) sprawdza składnię zbioru konfiguracyjnego o nazwie named.conf. Komenda ta nie obsługuje jednak sprawdzania semantyki zbioru konfiguracyjnego.

Program narzędziowy strefy DNS (DNS Zone Utility - CHKDNSZNE)
Program narzędziowy strefy DNS (CHKDNSZNE) sprawdza składnię i integralność zbioru danych strefy. Sprawdzenie zbiorów danych strefy jest przydatne przed dodaniem ich do serwera DNS.

Nowe narzędzia zapytań i aktualizacji

Aby poprawić zarządzanie serwerem DNS, dodano następujące narzędzia zapytań i aktualizacji.

Narzędzie DIG

Narzędzie zapytań DIG umożliwia pobranie informacji DNS o hostach, domenach i innych serwerach DNS w oparciu o odpowiedź serwera DNS. Za pomocą tego narzędzia można także sprawdzić, czy serwer DNS działa prawidłowo, zanim system zostanie skonfigurowany do korzystania z serwera.

Uruchomienie zapytania HOST (Start HOST Query (HOST))

Komenda Uruchomienie zapytania HOST (HOST) służy do wyszukiwań DNS. Konwertuje ona nazwy domen na adresy IP (IPv4 lub IPv6) i odwrotnie.

Dynamic Update Utility (NSUPDATE)

Komenda Dynamic Update Utility (NSUPDATE) służy do wprowadzania do serwera DNS żądań dynamicznej aktualizacji DNS, jak zostało to zdefiniowane w dokumencie Request for Comments (RFC) 2136 załączonym do serwera DNS. Umożliwia to dodawanie do strefy lub usuwanie z niej rekordów zasobów podczas działania serwera DNS. Dlatego też nie jest konieczne aktualizowanie rekordów poprzez ręczną edycję zbioru strefy. Pojedyncze żądanie aktualizacji może zawierać żądania dodania lub usunięcia więcej niż jednego rekordu zasobu, ale rekordy zasobów dynamicznie dodawane lub usuwane za pomocą komendy NSUPDATE powinny znajdować się w tej samej strefie.

Remote Name Daemon Control (RNDC)

Komenda Remote Name Daemon Control (RNDC) umożliwia administratorowi systemu sterowanie działaniem serwera nazw. Odczytuje ona zbiór konfiguracyjny o nazwie *rndc.conf*, aby określić sposób kontaktowania się z serwerem nazw oraz algorytm i klucz, których powinna użyć. Jeśli zbiór rndc.conf nie zostanie znaleziony, domyślnie zostanie użyty zbiór rndc-key._KID utworzony podczas instalacji, który automatycznie zapewnia dostęp przez interfejs pętli zwrotnej.

Znajdowanie nowych lub zmienionych informacji

Aby ułatwić określenie obszarów, w których zostały wprowadzone zmiany techniczne, w Centrum informacyjnym zastosowano:

- symbol » służący do zaznaczania początku nowego lub zmienionego fragmentu;
- symbol « służący do zaznaczania końca nowego lub zmienionego fragmentu.

Nowe i zmienione informacje w plikach PDF mogą być oznaczone symbolem | na lewym marginesie.

Odsyłacze pokrewne

“Funkcje programu BIND 9” na stronie 8
Program BIND 9 jest podobny do programu BIND 8, jednak oferuje kilka funkcji, jak na przykład widoki, które poprawiają wydajność serwera DNS.

Plik PDF z informacjami na temat systemu nazw domen

Informacje zawarte w tym temacie są także dostępne w postaci pliku PDF, który można wyświetlić i wydrukować.

Aby wyświetlić albo pobrać dokument w formacie PDF, wybierz System nazw domen (wielkość pliku 255 kB).

Zapisywanie plików PDF

Aby zapisać plik PDF na stacji roboczej w celu jego wyświetlenia lub wydrukowania, wykonaj następujące czynności:

1. Kliknij prawym przyciskiem myszy odsyłacz do pliku PDF w przeglądarce.
2. Kliknij opcję zapisania pliku PDF lokalnie.
3. Przejdź do katalogu, w którym ma zostać zapisany plik PDF.
4. Kliknij opcję **Zapisz**.

Pobieranie programu Adobe Reader

Do przeglądania i drukowania plików PDF potrzebny jest program Adobe Reader. Bezpłatną kopię tego programu można pobrać z serwisu WWW firmy Adobe (www.adobe.com/products/acrobat/readstep.html) .

Odsyłacze pokrewne

"Informacje pokrewne dotyczące systemu DNS" na stronie 41
Informacje związane z kolekcją tematów dotyczących systemu nazw domen są zawarte także w dokumentacji technicznej IBM Redbooks, w serwisach WWW oraz w innych kolekcjach tematów Centrum informacyjnego. Wszystkie pliki PDF można wyświetlić lub wydrukować.

Koncepcje systemu nazw domen (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 systemowi DNS użytkownicy mogą znaleźć host, używając prostych nazw, takich jak www.jkltoys.com, zamiast adresów IP, jak na przykład 192.168.12.88 (IPv4) lub 2001:D88::1 (IPv6).

Pojedynczy serwer 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. Dzięki współpracującym ze sobą serwerom DNS komputery mogą komunikować się ze sobą przez 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 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 zawiera objaśnienia ścieżek, jakich może użyć klient do rozstrzygnięcia zapytania.

Podstawy stref

Dane DNS są podzielone na łatwe do zarządzania zestawy zwane *strefami*. Każdy z tych zestawów jest określonym typem strefy.

Strefy zawierają informacje o nazwie i adresie IP dla przynajmniej jednej części domeny DNS. Serwer, który zawiera wszystkie informacje dotyczące strefy, jest serwerem autorytatywnym dla domeny zwanym *strefą nadrzędną* (parent zone). Czasami warto przekazać uprawnienie do odpowiadania na zapytania DNS, dotyczące konkretnej poddomeny, do innego serwera DNS zwanego *strefą potomną* (child zone). 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 systemu i5/OS można zdefiniować kilka typów stref, aby ułatwić zarządzanie danymi DNS:

Strefa podstawowa
Strefa podstawowa wczytuje dane strefy bezpośrednio ze zbioru hosta. Może ona zawierać podstrefę lub strefę potomną. Może również zawierać rekordy zasobów, takie jak host, alias (CNAME), adres IPv4 (A), adres IPv6 (AAAA) lub rekordy wskaźników wyszukiwania 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
Strefa zapasowa wczytuje dane strefy z serwera głównego strefy lub innego serwera pomocniczego. Utrzymuje ona kompletną kopię danych tej strefy.

Uwaga: W innych dokumentach dotyczących programu BIND strefy zapasowe są czasami nazywane *strefami drugorzędnymi*.

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.

Pojęcia pokrewne

"Podstawy zapytań systemu nazw domen (DNS)"
Klienty DNS używają serwerów DNS do rozstrzygania zapytań. Zapytania mogą pochodzić bezpośrednio od klienta lub aplikacji działającej na kliencie.

Zadania pokrewne

"Konfigurowanie stref na serwerze nazw" na stronie 29
Po skonfigurowaniu instancji serwera DNS należy skonfigurować strefy serwera nazw.

Odsyłacze pokrewne

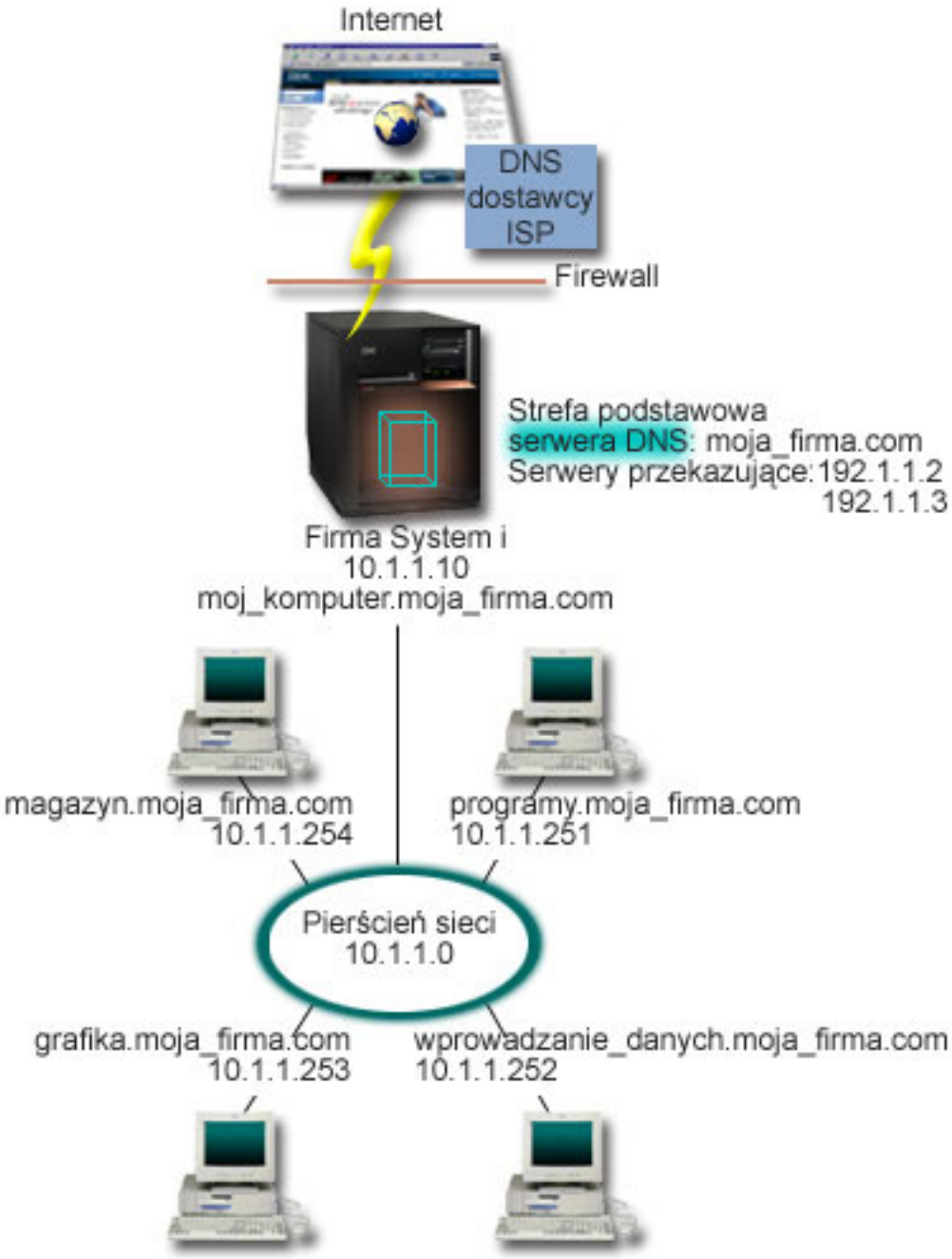
"Przykład: pojedynczy serwer systemu nazw domen dla intranetu" na stronie 14
Przykład ten przedstawia prostą podsieć z serwerem DNS do użytku wewnętrznego.

"Rekordy zasobów DNS" na stronie 9
Rekordy zasobów są używane do przechowywania danych o nazwach domenowych i adresach IP. Aby wyświetlić rekordy zasobów obsługiwane przez system operacyjny i5/OS, należy użyć tabeli wyszukiwania rekordów zasobów.

Podstawy zapytań systemu nazw domen (DNS)

Klienty DNS używają serwerów DNS do rozstrzygania zapytań. Zapytania mogą pochodzić bezpośrednio od klienta lub 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.



Rysunek 1. Pojedynczy 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. Dostępne są dwie ścieżki: *rekurencja* lub *iteracja*. Jeśli serwer DNS jest ustawiony na korzystanie z *rekurencji*, zapyta się on innych serwerów DNS lub skontaktuje się z nimi w imieniu klienta zgłaszającego żądanie, aby w pełni przetłumaczyć nazwę, a następnie odeśle odpowiedź do klienta. Ponadto serwer zgłaszający żądanie przechowuje odpowiedź w pamięci podręcznej, aby była ona dostępna następnym razem, gdy serwer znowu otrzyma to zapytanie. Jeśli serwer DNS jest ustawiony na korzystanie z *iteracji*, klient we własnym

imieniu spróbuje skontaktować się z innymi serwerami DNS, aby przetłumaczyć nazwę. W tym procesie klient używa odrębnych i dodatkowych zapytań tworzonych na podstawie odpowiedzi z serwerów.

Odsyłacze pokrewne

"Podstawy stref" na stronie 3
Dane DNS są podzielone na łatwe do zarządzania zestawy zwane *strefami*. Każdy z tych zestawów jest określonym typem strefy.

"Przykład: pojedynczy serwer systemu nazw domen z dostępem do Internetu" na stronie 16
Przykład ten przedstawia prostą podsieć z serwerem DNS połączonym bezpośrednio z Internetem.

Konfiguracja domen systemu nazw domen (DNS)

Konfiguracja domen systemu nazw domen (DNS) wymaga rejestracji nazwy domeny, która uniemożliwia innym użytkownikom korzystanie z tej nazwy domeny.

System 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 Internetowe Sieciowe Centrum Informacyjne (InterNIC).

Odsyłacze pokrewne

"Przykład: pojedynczy serwer systemu nazw domen z dostępem do Internetu" na stronie 16
Przykład ten przedstawia prostą podsieć z serwerem DNS połączonym bezpośrednio z Internetem.

Informacje pokrewne

Internetowe Sieciowe Centrum Informacyjne (Internet Network Information Center - InterNIC)

Dynamiczne aktualizacje

Serwer DNS i5/OS oparty na programie BIND 9 obsługuje dynamiczne aktualizacje. Zewnętrzne źródła, jak na przykład serwer DHCP, mogą przesyłać aktualizacje do serwera DNS. Ponadto za pomocą narzędzi klienta DNS, takich jak narzędzie Dynamic Update Utility (NSUPDATE), można wykonywać dynamiczne aktualizacje.

Protokół DHCP jest standardem TCP/IP, który korzysta z serwera centralnego do zarządzania adresami IP i innymi szczegółami konfiguracyjnymi całej sieci. Serwer DHCP odpowiada na żądania klientów i dynamicznie przypisuje im odpowiednie parametry.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.

W przeszłości wszystkie dane DNS były przechowywane w statycznych bazach danych. Wszystkie rekordy zasobów DNS musiały być tworzone i modyfikowane przez administratora. Serwery DNS oparte na programie BIND 8 lub nowszym mogą być skonfigurowane w taki sposób, aby akceptowały żądania dynamicznej aktualizacji danych strefy pochodzące z innych źródeł.

Serwer DHCP można skonfigurować w taki sposób, aby wysyłał do serwera DNS żądania aktualizacji po każdym przypisaniu hostowi nowego adresu. Ten zautomatyzowany proces pozwala zmniejszyć pracochłonność administrowania serwerem DNS w szybko rozrastających się lub zmieniających sieciach TCP/IP oraz w sieciach, w

których często zmieniają się położenia hostów. Gdy klient DHCP otrzyma adres IP, informacja o tym adresie jest natychmiast przekazywana do serwera DNS. Dzięki temu serwer DNS może prawidłowo odczytywać nazwy hostów, nawet jeśli ich adresy IP nie są stałe.

Serwer DHCP można tak skonfigurować, aby w imieniu klienta aktualizował rekordy odwzorowania adresów (A w przypadku IPv4 lub AAAA w przypadku IPv6), rekordy wskaźników wyszukiwania odwrotnego (PTR) lub oba typy rekordów. Rekordy odwzorowania adresu (A lub AAAA) odwzorowują nazwę hosta na jego adres IP. Rekordy typu PTR odwzorowują adres hosta na jego nazwę. Kiedy adres klienta ulega zmianie, serwer DHCP może automatycznie wysłać aktualizację do serwera DNS, dzięki czemu inne hosty w sieci będą mogły znaleźć klienta pod jego nowym adresem IP za pośrednictwem zapytań DNS. Dla każdego rekordu zaktualizowanego dynamicznie zapisywany jest również powiązany rekord tekstowy (TXT), który wskazuje, że rekord został zaktualizowany przez serwer DHCP.

Uwaga: Jeśli konfiguracja DHCP przewiduje aktualizowanie tylko rekordów PTR, konfiguracja serwera DNS powinna zezwalać na aktualizacje inicjowane przez klienty, aby każdy klient mógł zaktualizować odpowiadający mu rekord A, jeśli klient używa adresu IPv6, lub rekord AAAA, jeśli używa adresu IPv6. Nie wszyscy klienci serwera DHCP obsługują żądania aktualizacji własnych rekordów A lub AAAA. Dlatego przed zdecydowaniem się na tę metodę należy dokładnie zapoznać się z dokumentacją platformy klienta.

Strefy dynamiczne są zabezpieczane za pośrednictwem listy źródeł upoważnionych do zgłaszania żądań aktualizacji rekordów. 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 wprowadzeniem zmian w rekordzie serwer DNS sprawdza, czy pakiet zgłoszenia nadszedł z uprawnionego źródła.

Dynamiczne aktualizacje między serwerem DNS a DHCP mogą być wykonywane w ramach pojedynczej platformy System i, między różnymi platformami System i lub między platformą System i a systemami innego typu, które obsługują dynamiczną aktualizację.

Uwaga: Na serwerach wysyłających dynamiczne aktualizacje do serwera DNS jest wymagana funkcja API dynamicznej aktualizacji DNS (QTOBUPDT). Jest ona automatycznie instalowana z Opcją 31 produktu DNS i5/OS. Jednak w programie BIND 9 preferowaną metodą aktualizowania platformy System i jest komenda NSUPDATE.

Pojęcia pokrewne

Protokół DHCP (Dynamic Host Configuration Protocol)

Zadania pokrewne

“Konfigurowanie odbierania dynamicznych aktualizacji przez serwer DNS” na stronie 30
Serwery DNS działające pod kontrolą programu BIND 9 mogą być skonfigurowane w taki sposób, aby akceptowały żądania dynamicznej aktualizacji danych strefy pochodzące z innych źródeł. Sekcja ta zawiera instrukcje konfigurowania opcji zezwolenia na aktualizację (allow-update), tak aby serwer DNS mógł odbierać dynamiczne aktualizacje.

Konfigurowanie serwera DHCP pod kątem wysyłania dynamicznych aktualizacji DNS

Odsyłacze pokrewne

“Przykład: serwery DNS i DHCP na tym samym serwerze System i” na stronie 18
Przykład ten przedstawia serwery DNS i DHCP na tym samym serwerze System i.

“Rekordy zasobów DNS” na stronie 9
Rekordy zasobów są używane do przechowywania danych o nazwach domenowych i adresach IP. Aby wyświetlić rekordy zasobów obsługiwane przez system operacyjny i5/OS, należy użyć tabeli wyszukiwania rekordów zasobów.

QTOBUPT

“Funkcje programu BIND 9” na stronie 8
Program BIND 9 jest podobny do programu BIND 8, jednak oferuje kilka funkcji, jak na przykład widoki, które poprawiają wydajność serwera DNS.

Funkcje programu BIND 9

Program BIND 9 jest podobny do programu BIND 8, jednak oferuje kilka funkcji, jak na przykład widoki, które poprawiają wydajność serwera DNS.

Widoki na pojedynczym serwerze DNS i5/OS

Instrukcja *widok* (View) pozwala pojedynczej instancji DNS udzielać różnych odpowiedzi na zapytania w zależności od źródła pochodzenia zapytania, takiego jak Internet lub intranet.

Jednym z praktycznych zastosowań funkcji widoku jest podział konfiguracji DNS bez konieczności uruchamiania wielu serwerów DNS. Na przykład na pojedynczym serwerze DNS można zdefiniować widok odpowiadający na zapytania z sieci wewnętrznej, definiując jednocześnie inny widok odpowiadający na zapytania z sieci zewnętrznej.

Nowe komendy klienta

Następujące komendy klienta zwiększają możliwości zarządzania serwerem DNS:

Dynamic Update Utility (NSUPDATE)
Komenda Dynamic Update Utility (NSUPDATE) służy do wprowadzania do serwera DNS żądań dynamicznej aktualizacji DNS, jak zostało do zdefiniowane w dokumencie Request for Comments (RFC) 2136 załączonym do serwera DNS. Umożliwia to dodawanie do strefy lub usuwanie z niej rekordów zasobów podczas działania serwera DNS. Dlatego też nie jest konieczne aktualizowanie rekordów poprzez ręczną edycję zbioru strefy. Pojedyncze żądanie aktualizacji może zawierać żądania dodania lub usunięcia wielu rekordów zasobów, ale rekordy zasobów dynamicznie dodawane lub usuwane za pomocą komendy NSUPDATE powinny znajdować się w tej samej strefie.

Uwaga: Nie należy ręcznie edytować stref podlegających sterowaniu dynamicznemu za pomocą komendy NSUPDATE lub serwera DHCP. Ręczna edycja może spowodować konflikt z aktualizacjami dynamicznymi i utratę danych.

Uruchomienie zapytania DIG (Start DIG Query - DIG)
Produkt Domain Information Groper (DIG) jest narzędziem zapytań o wiele silniejszym od komendy Name Server Lookup (NSLOOKUP) i służy do pobierania informacji z serwera DNS lub testowania odpowiedzi z serwera DNS. Komenda NSLOOKUP jest nieaktualna i została udostępniona wyłącznie w celu zapewnienia kompatybilności ze starszymi wersjami. Za pomocą narzędzia DIG można sprawdzić, czy serwer DNS działa prawidłowo, zanim system zostanie skonfigurowany do korzystania z serwera. Narzędzie to umożliwia także pobranie informacji DNS o hostach, domenach i innych serwerach DNS.

Za pomocą komendy Uruchomienie zapytania DIG (Start DIG Query - STRDIGQRY) lub jej aliasu DIG można uruchomić narzędzie Domain Information Groper.

Uruchomienie zapytania HOST (Start HOST Query (HOST))
Komenda Uruchomienie zapytania HOST (HOST) służy do wyszukiwań DNS. Można jej używać do konwertowania nazw domen na adresy IP (IPv4 lub IPv6) i odwrotnie.

Remote Name Daemon Control (RNDC)

Produkt Remote Name Daemon Control (RNDC) to silny program narzędziowy umożliwiający administratorowi systemu sterowanie działaniem serwera nazw. Program ten odczytuje zbiór konfiguracyjny o nazwie rndc.conf, aby określić sposób kontaktowania się z serwerem nazw oraz algorytm i klucz, których serwer powinien użyć. Jeśli zbiór rndc.conf nie zostanie znaleziony, domyślnie zostanie użyty zbiór rndc-key._KID utworzony podczas instalacji, który automatycznie zapewnia dostęp przez interfejs pętli zwrotnej.

Obsługa standardu IPv6

Program BIND 9 obsługuje wyszukiwania typu nazwa/adres i adres/nazwa we wszystkich obecnie zdefiniowanych formularzach IPv6. W przypadku wyszukiwania do przodu program BIND 9 obsługuje rekordy AAAA i A6, ale

rekordy A6 są w tej chwili nieaktualne. W przypadku wyszukiwań IPv6 wstecz program obsługuje tradycyjny półbajtowy format używany w domenie ip6.arpa oraz starszej, nieaktualnej domenie ip6.int.

Pliki kroniki

Pliki kroniki służą do przechowywania dynamicznych aktualizacji strefy. Plik taki jest tworzony automatycznie po otrzymaniu od klienta pierwszej dynamicznej aktualizacji i nie przestaje istnieć. Jest to plik binarny i nie należy go edytować.

Gdy serwer jest restartowany po zamknięciu systemu lub awarii, odtwarza plik kroniki, aby wykonać aktualizacje strefy, które miały miejsce po ostatnim zrzucie strefy. Pliki kroniki służą także do przechowywania aktualizacji metody przyrostowego przesyłania strefowego (IXFR).

Serwer DNS dla systemu i5/OS został zaprojektowany ponownie, tak aby używał programu BIND 9. Aby uruchomić program BIND 9 DNS w systemie, musi on spełniać określone wymagania dotyczące oprogramowania.

Pojęcia pokrewne

"Wymagania systemu DNS" na stronie 26
Aby uruchomić system nazw domen (DNS) na platformie System i, należy mieć na uwadze wymagania dotyczące oprogramowania.

"Dynamiczne aktualizacje" na stronie 6
Serwer DNS i5/OS oparty na programie BIND 9 obsługuje dynamiczne aktualizacje. Zewnętrzne źródła, jak na przykład serwer DHCP, mogą przesyłać aktualizacje do serwera DNS. Ponadto za pomocą narzędzi klienta DNS, takich jak narzędzie Dynamic Update Utility (NSUPDATE), można wykonywać dynamiczne aktualizacje.

"Co nowego w wersji V6R1" na stronie 1
Poniżej opisano nowe i zmienione informacje w kolekcji tematów dotyczącej systemu DNS.

Odsyłacze pokrewne

"Przykład: dzielenie systemu DNS za zaporą firewall poprzez skonfigurowanie dwóch serwerów DNS na tej samej platformie System i" na stronie 20
Przykład ten przedstawia serwer DNS, który działa za zaporą firewall w celu zabezpieczania danych wewnętrznych ze strony Internetu i jednocześnie umożliwia wewnętrznym użytkownikom uzyskanie dostępu do danych w Internecie. Konfiguracja ta realizuje to zabezpieczenie poprzez skonfigurowanie dwóch serwerów DNS na tej samej platformie System i.

"Planowanie środków bezpieczeństwa" na stronie 25
DNS udostępnia opcje ochrony ograniczające dostęp z zewnątrz do serwera.

Rekordy zasobów DNS

Rekordy zasobów są używane do przechowywania danych o nazwach domenowych i adresach IP. Aby wyświetlić rekordy zasobów obsługiwane przez system operacyjny i5/OS, należy użyć tabeli wyszukiwania rekordów zasobów.

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.

Uwaga: Pozycje w tabeli wyszukiwania rekordów zasobów można dodawać lub usuwać w zależności od zmian wprowadzanych w dokumencie BIND. Ta tabela nie jest pełną listą wszystkich rekordów zasobów wymienionych w dokumencie BIND.

Tabela 1. Tabela wyszukiwania rekordów zasobów

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 podaje 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 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 IPv6 hosta. Rekordy AAAA są podobne do rekordów A i służą do rozstrzygania zapytań o adres IPv6 konkretnej nazwy domeny. 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.

Tabela 1. Tabela wyszukiwania rekordów zasobów (kontynuacja)

Rekord zasobu	Nazwa skrócona	Opis
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 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.

Tabela 1. Tabela wyszukiwania rekordów zasobów (kontynuacja)

Rekord zasobu	Nazwa skrócona	Opis
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.
Rekordy usług	SRV	Rekord SRV określa hosty obsługujące usługi zdefiniowane w rekordzie. Ten typ rekordu jest zdefiniowany w dokumencie RFC 2782.
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. Serwer DHCP i5/OS używa rekordów TXT do dynamicznych aktualizacji. Serwer DHCP zapisuje powiązany rekord TXT dla każdej aktualizacji rekordu PTR i A wykonywanej przez serwer DHCP. Rekordy DHCP mają prefiks AS400DHCP.

Tabela 1. Tabela wyszukiwania rekordów zasobów (kontynuacja)

Rekord zasobu	Nazwa skrócona	Opis
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.

Pojęcia pokrewne

"Poczta i rekordy wymiany poczty (MX)"
DNS obsługuje zaawansowane przekierowywanie poczty poprzez wykorzystanie rekordów MX.

Odsyłacze pokrewne

"Przykład: pojedynczy serwer systemu nazw domen dla intranetu" na stronie 14
Przykład ten przedstawia prostą podsieć z serwerem DNS do użytku wewnętrznego.

"Podstawy stref" na stronie 3
Dane DNS są podzielone na łatwe do zarządzania zestawy zwane *strefami*. Każdy z tych zestawów jest określonym typem strefy.

Poczta i rekordy wymiany poczty (MX)

DNS obsługuje zaawansowane przekierowywanie poczty poprzez wykorzystanie rekordów MX.

Rekordy MX są używane przez programy rozsyłające pocztę, takie jak protokół Simple Mail Transfer Protocol (SMTP). Tabela wyszukiwania w rekordach zasobów DNS zawiera typy rekordów poczty obsługiwane przez system DNS i5/OS.

System DNS obejmuje informacje potrzebne do wysyłania poczty elektronicznej za pomocą wymienników poczty. Jeśli w sieci używany jest system DNS, aplikacja protokołu SMTP 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 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: Uwaga: nie zaleca się stosowania znaków wieloznacznych (na przykład: *.mycompany.com) w rekordach MX dla domeny.

Przykład: rekord MX dla hosta

W poniższym przykładzie system, zgodnie z preferencjami, dostarczy 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
```

Odsyłacze pokrewne

“Rekordy zasobów DNS” na stronie 9
Rekordy zasobów są używane do przechowywania danych o nazwach domenowych i adresach IP. Aby wyświetlić rekordy zasobów obsługiwane przez system operacyjny i5/OS, należy użyć tabeli wyszukiwania rekordów zasobów.

Przykłady: system nazw domen

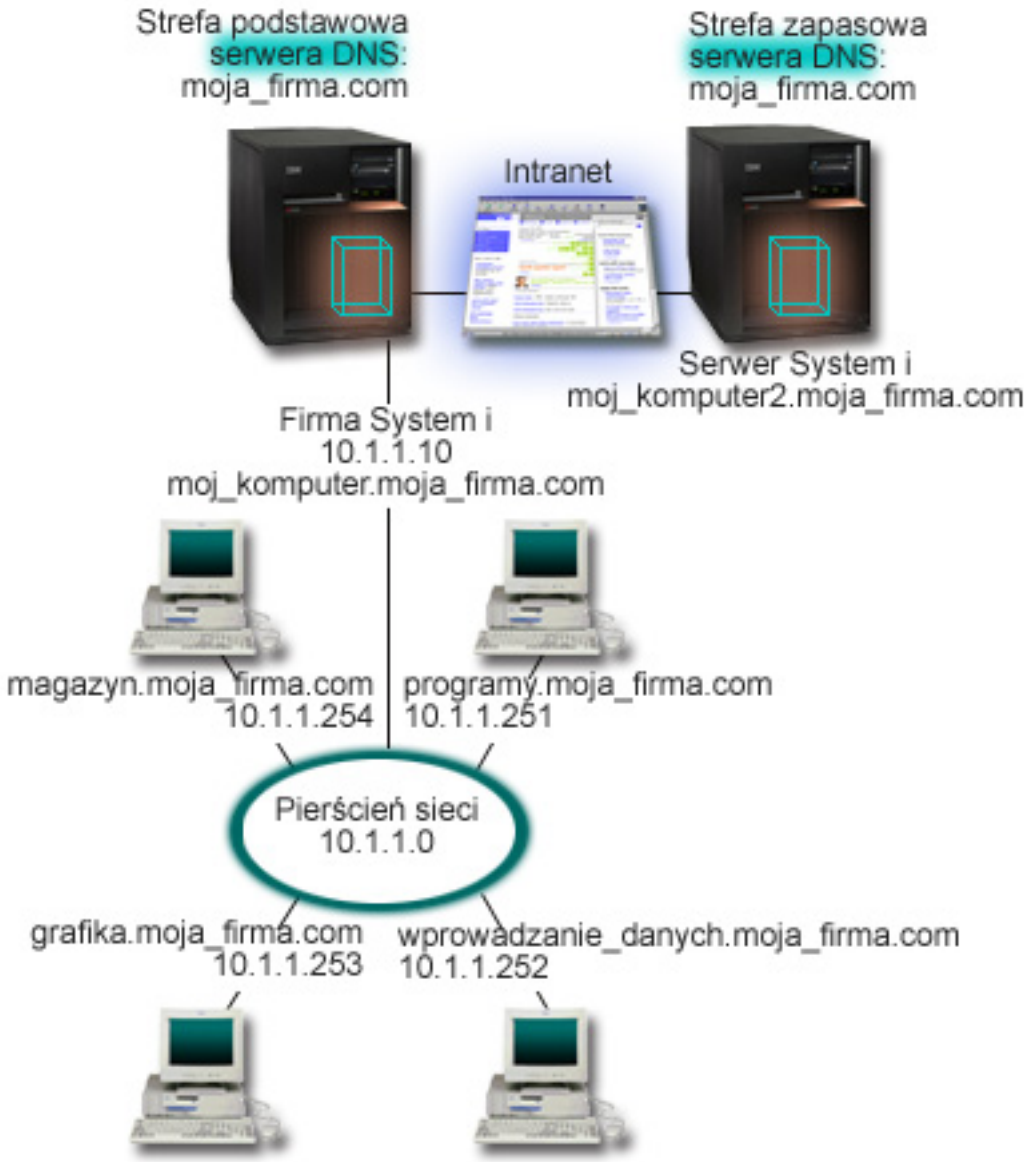
Przykłady te mogą okazać się pomocne w zrozumieniu działania systemu nazw domen (DNS) w sieci użytkownika.

DNS to system rozproszonej bazy 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: pojedynczy serwer systemu nazw domen dla intranetu

Przykład ten przedstawia prostą podsieć z serwerem DNS do użytku wewnętrznego.

Poniższy rysunek przedstawia serwer DNS dla sieci wewnętrznej działający na platformie System i. Ta pojedyncza instancja serwera DNS została skonfigurowana do nasłuchiwania zapytań na wszystkich adresach IP interfejsu. Przedstawiony system jest podstawowym serwerem nazw dla strefy moja_firma.com.



Rysunek 2. Pojedynczy serwer DNS z dostępem do 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 w przypadku IPv4 lub AAAA w przypadku IPv6) 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, AAAA i PTR serwer DNS obsługuje wiele innych typów rekordów zasobów, które mogą być niezbędne w zależności od innych aplikacji TCP/IP działających 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 rysunku powyżej serwer mój_systemi jest częścią intranetu. Inny system, mój_systemi2, został skonfigurowany jako zapasowy serwer DNS dla strefy moja_firma.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.

Odsyłacze pokrewne

“Rekordy zasobów DNS” na stronie 9
Rekordy zasobów są używane do przechowywania danych o nazwach domenowych i adresach IP. Aby wyświetlić rekordy zasobów obsługiwane przez system operacyjny i5/OS, należy użyć tabeli wyszukiwania rekordów zasobów.

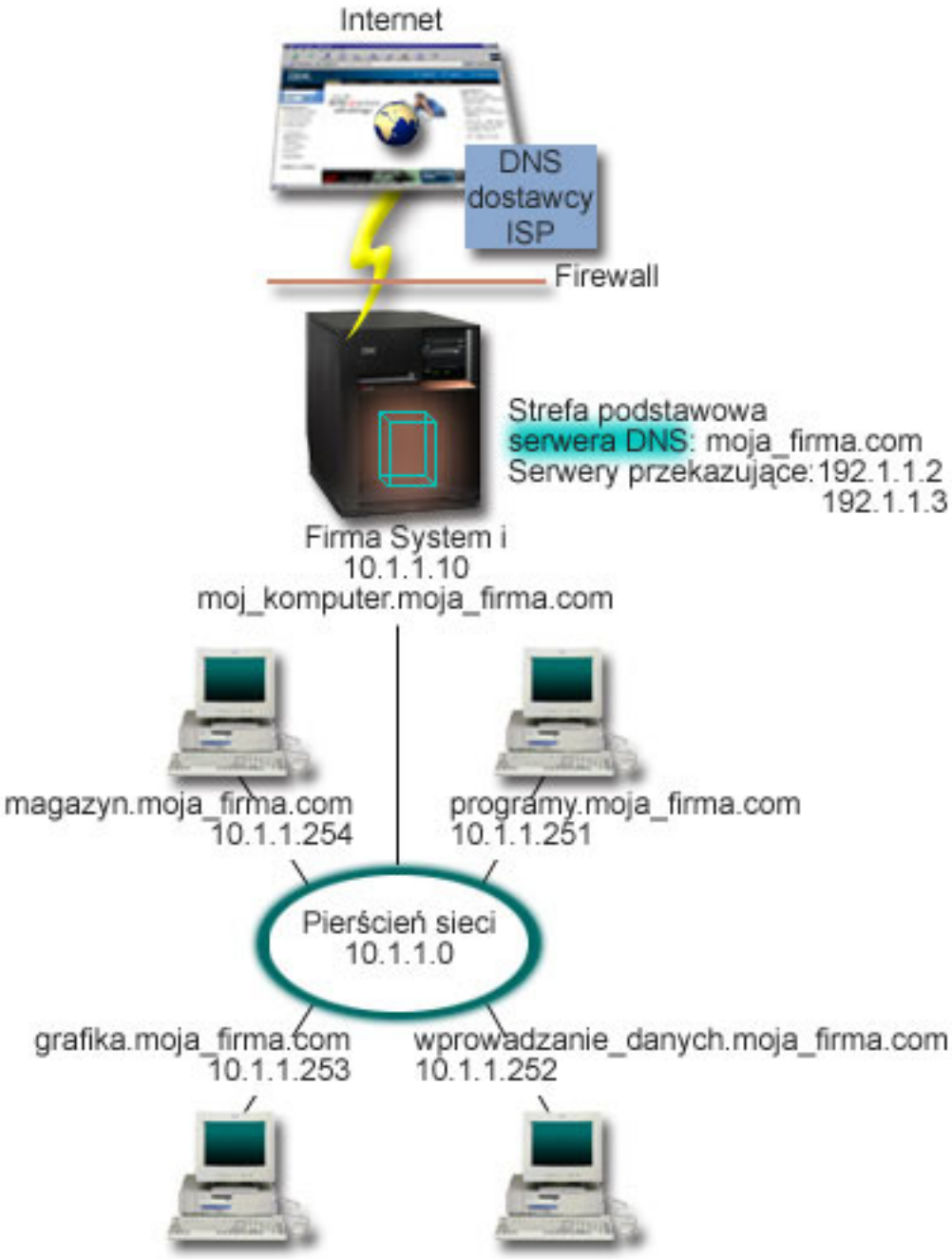
“Podstawy stref” na stronie 3
Dane DNS są podzielone na łatwe do zarządzania zestawy zwane *strefami*. Każdy z tych zestawów jest określonym typem strefy.

“Przykład: pojedynczy serwer systemu nazw domen z dostępem do Internetu”
Przykład ten przedstawia prostą podsieć z serwerem DNS połączonym bezpośrednio z Internetem.

Przykład: pojedynczy serwer systemu nazw domen z dostępem do Internetu

Przykład ten przedstawia prostą podsieć z serwerem DNS połączonym bezpośrednio z Internetem.

Poniższy rysunek przedstawia ten sam przykład sieci, co w sekcji Serwer DNS dla intranetu, ale w tym przypadku 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 3. Pojedynczy 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 informacji o Internetowych serwerach głównych zawiera sekcja Dostęp do zewnętrznych danych systemu nazw domen.
- 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 zarejestrować nazwę domeny, o ile nie zostało to już zrobione.
- Uruchomienie firewalla

  Nie zaleca się korzystania z bezpośredniego połączenia serwera DNS z Internetem. Należy skonfigurować zaporę firewall lub podjąć inne środki ostrożności w celu zabezpieczenia platformy System i.

Pojęcia pokrewne

“Konfiguracja domen systemu nazw domen (DNS)” na stronie 6
Konfiguracja domen systemu nazw domen (DNS) wymaga rejestracji nazwy domeny, która uniemożliwia innym użytkownikom korzystanie z tej nazwy domeny.

Serwery System i - bezpieczeństwo internetowe

“Podstawy zapytań systemu nazw domen (DNS)” na stronie 4
Klienty DNS używają serwerów DNS do rozstrzygania zapytań. Zapytania mogą pochodzić bezpośrednio od klienta lub aplikacji działającej na kliencie.

Odsyłacze pokrewne

“Przykład: pojedynczy serwer systemu nazw domen dla intranetu” na stronie 14
Przykład ten przedstawia prostą podsieć z serwerem DNS do użytku wewnętrznego.

Przykład: serwery DNS i DHCP na tym samym serwerze System i

Przykład ten przedstawia serwery DNS i DHCP na tym samym serwerze System i.

Konfigurację taką można wykorzystywać do dynamicznej aktualizacji danych strefy DNS, kiedy serwer DHCP przypisuje hostom adresy IP.

Poniższy rysunek przedstawia małą podsieć z jedną platformą System i, która działa jednocześnie jako serwer DHCP i serwer DNS dla czterech klientów. W przykładowej sieci klienty w magazynie, stacje wprowadzania danych oraz komputery dyrekcji służą do tworzenia dokumentów zawierających grafiki pobierane z serwera plików graficznych. Maszyny te łączą się z serwerem plików graficznych, odwzorowując sieciowy napęd dysków na nazwę hosta.

Rysunek 4. Serwery DNS i DHCP na tej samej platformie System i

Poprzednie wersje serwerów DHCP i DNS działały niezależnie od siebie. Jeśli serwer DHCP przypisał klientowi nowy adres IP, administrator musiał samodzielnie zmodyfikować odpowiednie rekordy DNS. 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 systemie i5/OS serwera DNS opartego na programie BIND 9, można skonfigurować strefę DNS, tak aby akceptowała dynamiczne aktualizacje rekordów DNS wraz ze sporadycznymi zmianami adresów przez serwer DHCP. Na przykład rekordy DNS serwera plików zostaną dynamicznie zaktualizowane po tym, jak serwer ten odnowi dzierżawę i otrzyma nowy adres IP 10.1.1.250. Dzięki temu pozostałe komputery będą mogły dalej bez przeszkód odwoływać się do serwera plików graficznych poprzez nazwy hostów interpretowane prawidłowo przez serwer DNS.

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

- Zidentyfikowanie strefy dynamicznej

  Nie można ręcznie aktualizować strefy dynamicznej podczas pracy serwera. Może to bowiem 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.

- Konfigurowanie opcji 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.
- Konfigurowanie wysyłania dynamicznych aktualizacji przez serwer DHCP

  Należy autoryzować serwer DHCP do aktualizacji rekordów DNS zgodnie z rozdzielanymi adresami IP.
- Konfigurowanie preferencji dotyczących aktualizacji dla serwera pomocniczego

  Aby zapewnić aktualność danych przechowywanych na serwerze pomocniczym, można na serwerze DNS skonfigurować funkcję NOTIFY, która wysyła do serwerów pomocniczych strefy moja_firma.com komunikaty informujące o zmianie danych strefy. Należy również skonfigurować i włączyć przyrostowe przesyłanie strefowe (IXFR), co pozwoli serwerom pomocniczym 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.

Pojęcia pokrewne

“Dynamiczne aktualizacje” na stronie 6
Serwer DNS i5/OS oparty na programie BIND 9 obsługuje dynamiczne aktualizacje. Zewnętrzne źródła, jak na przykład serwer DHCP, mogą przesyłać aktualizacje do serwera DNS. Ponadto za pomocą narzędzi klienta DNS, takich jak narzędzie Dynamic Update Utility (NSUPDATE), można wykonywać dynamiczne aktualizacje.

Zadania pokrewne

Konfigurowanie serwera DHCP pod kątem wysyłania dynamicznych aktualizacji DNS

Odsyłacze pokrewne

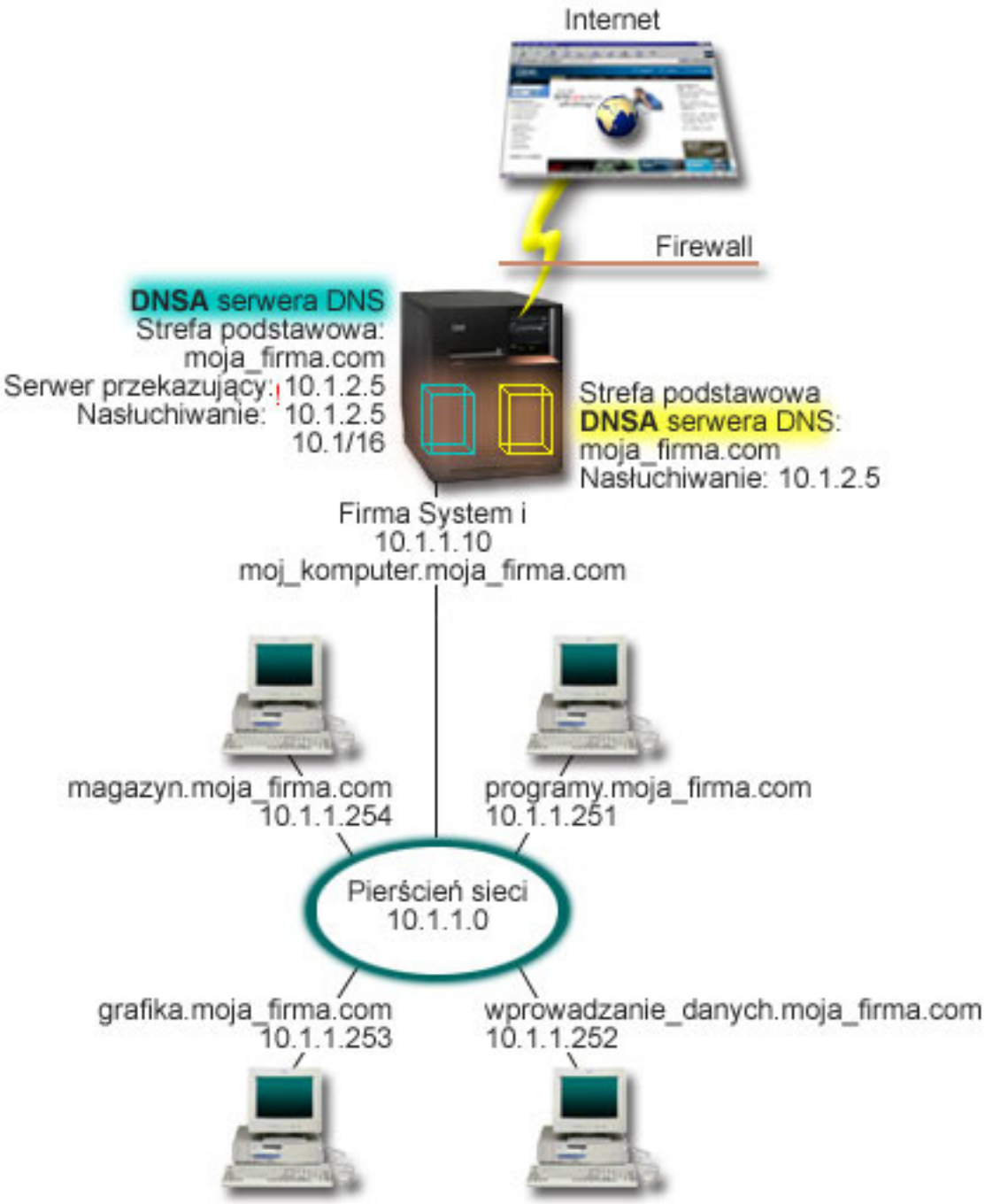
Przykład: serwery DNS i DHCP na różnych platformach System i

Przykład: dzielenie systemu DNS za zaporą firewall poprzez skonfigurowanie dwóch serwerów DNS na tej samej platformie System i

Przykład ten przedstawia serwer DNS, który działa za zaporą firewall w celu zabezpieczania danych wewnętrznych ze strony Internetu i jednocześnie umożliwia wewnętrznym użytkownikom uzyskanie dostępu do danych w Internecie. Konfiguracja ta realizuje to zabezpieczenie poprzez skonfigurowanie dwóch serwerów DNS na tej samej platformie System i.

Poniższy rysunek przedstawia prostą podsieć zabezpieczoną przez zaporę firewall. Załóżmy, że firma posiada 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.

System DNS i5/OS oparty na programie BIND 9 umożliwia zrealizowanie tych zadań na dwa sposoby. Pierwszy sposób polega na skonfigurowaniu przez firmę dwóch instancji serwera DNS na tej samej platformie System i, jednej dla intranetu i drugiej dla użytkowników w domenie publicznej, co opisano w poniższym przykładzie. Inny sposób polega na użyciu funkcji widoku udostępnionej w programie BIND 9, którą opisano w przykładzie dotyczącym dzielenia systemu DNS za zaporą firewall za pomocą widoku.



Rysunek 5. Dzielenie systemu DNS za zaporą firewall poprzez skonfigurowanie dwóch serwerów DNS na tej samej platformie System i

Serwer zewnętrzny DNSB został skonfigurowany ze strefą podstawową moja_firma.com. Dane tej strefy obejmują wyłącznie rekordy przewidziane jako część domeny publicznej. Serwer wewnętrzny DNSA jest skonfigurowany ze strefą podstawową moja_firma.com, ale dane strefy zdefiniowane na serwerze DNSA zawierają rekordy zasobów intranetu. Opcja przekazywania została zdefiniowana 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. Aby dokonać podziału systemu DNS, należy wziąć pod uwagę następujące ustawienia konfiguracyjne:

- Nasłuchiwanie

  W innych przykładach dotyczących systemu DNS tylko jeden serwer DNS znajduje się na platformie System i. Nasłuchuje on na wszystkich adresach IP interfejsu. W przypadku wielu serwerów DNS na platformie System i 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 tym przypadku wszystkie zapytania przychodzące z zapory firewall będą wysyłane 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 znajdować się na liście AML przed przedrostkiem adresu dołączonego do listy.

- Kolejność elementów na liście AML

  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 zostanie natychmiast zablokowany.

  Jeśli elementy byłyby wpisane na listę w odwrotnej kolejności, tj. (10.1/16; !10.1.2.5), adresowi IP 10.1.2.5 zostałby przyznany dostęp, ponieważ serwer porównałby go z pierwszym elementem, który jest z nim zgodny, i pominąłby sprawdzanie pozostałych reguł.

Odsyłacze pokrewne

“Funkcje programu BIND 9” na stronie 8
Program BIND 9 jest podobny do programu BIND 8, jednak oferuje kilka funkcji, jak na przykład widoki, które poprawiają wydajność serwera DNS.

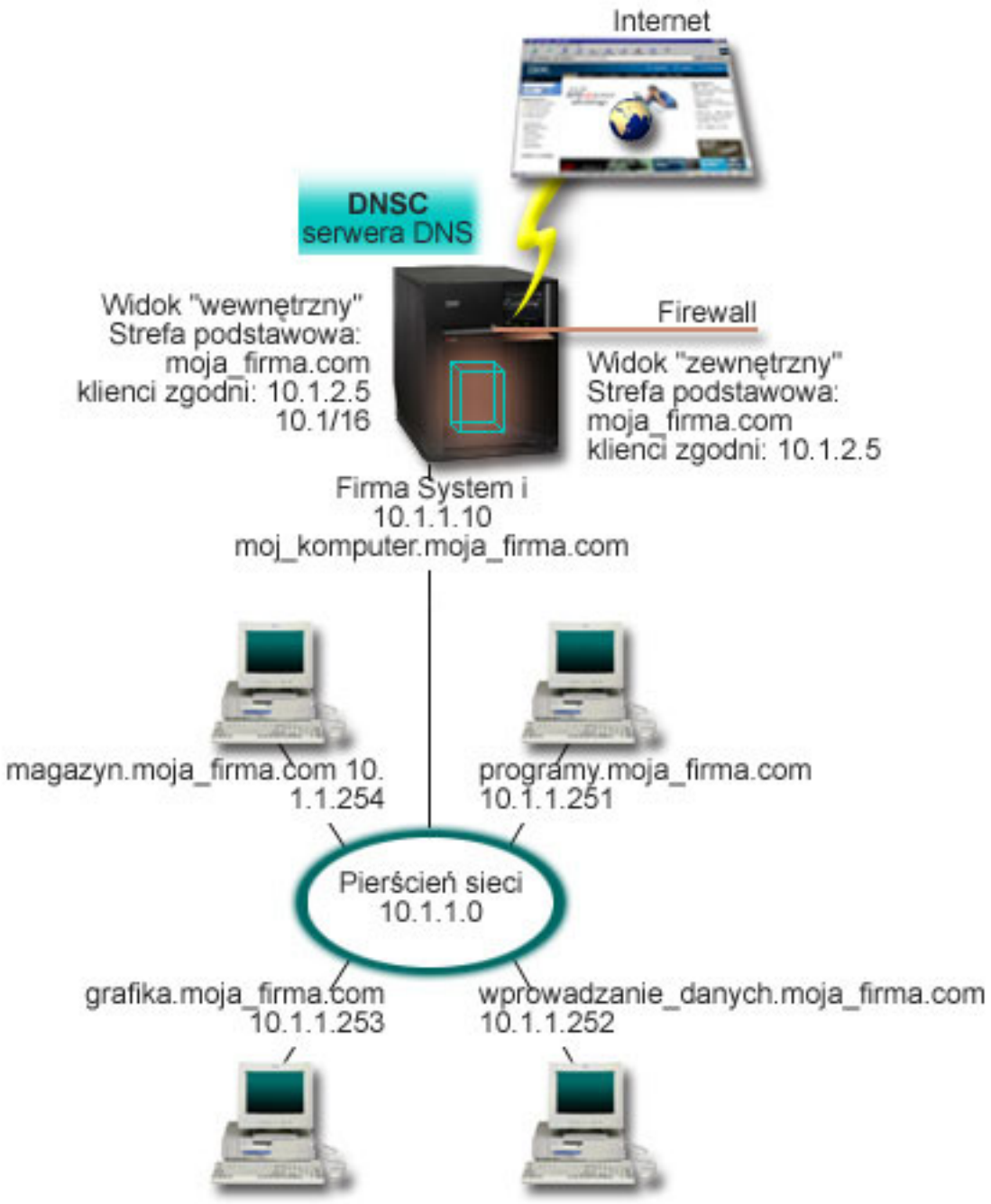
“Przykład: dzielenie systemu DNS za zaporą firewall za pomocą widoku”
Przykład ten przedstawia serwer DNS, który działa za zaporą firewall w celu zabezpieczania danych wewnętrznych ze strony Internetu i jednocześnie umożliwia wewnętrznym użytkownikom uzyskanie dostępu do danych w Internecie za pomocą funkcji *widok* (View) programu BIND 9.

Przykład: dzielenie systemu DNS za zaporą firewall za pomocą widoku

Przykład ten przedstawia serwer DNS, który działa za zaporą firewall w celu zabezpieczania danych wewnętrznych ze strony Internetu i jednocześnie umożliwia wewnętrznym użytkownikom uzyskanie dostępu do danych w Internecie za pomocą funkcji *widok* (View) programu BIND 9.

Poniższy rysunek przedstawia prostą podsieć zabezpieczoną przez zaporę firewall. Załóżmy, że firma posiada 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 spoza sieci. Firma chce również, aby jej wewnętrzne programy tłumaczące miały dostęp do pewnych stref wewnętrznych, które nie są dostępne spoza sieci wewnętrznej. Firma jednak nie chce, aby do sieci wewnętrznej miały dostęp zewnętrzne programy tłumaczące.

System DNS i5/OS oparty na programie BIND 9 umożliwia zrealizowanie tych zadań na dwa sposoby. W tym przykładzie opisano konfigurację serwera DNS z dwoma różnymi widokami nasłuchującymi różnych zapytań, jednym dla intranetu i drugim dla użytkowników w domenie publicznej. Inny sposób polega na skonfigurowaniu dwóch instancji serwera DNS na tej samej platformie System i, co opisano w przykładzie dotyczącym dzielenia systemu DNS za zaporą firewall za pomocą dwóch serwerów DNS.



Rysunek 6. Dzielenie systemu DNS za zaporą firewall za pomocą widoku

Serwer DNS, DNSC, definiuje dwa widoki zwane *zewnętrznym* (external) i *wewnętrznym* (internal). Widok *zewnętrzny* jest skonfigurowany ze strefą podstawową moja_firma.com zawierającą wyłącznie rekordy zasobów, które mają być częścią domeny publicznej, podczas gdy widok *wewnętrzny* jest skonfigurowany ze strefą podstawową moja_firma.com zawierającą rekordy zasobów intranetowych.

Jeśli w grę wchodzi integralność zapory firewall lub inne zagrożenia, można skorzystać z podinstrukcji łączenia zgodnych klientów, która pomaga zabezpieczyć dane wewnętrzne. W tym celu można skonfigurować widok wewnętrzny, aby obsługiwał wyłącznie zapytania dotyczące wewnętrznej strefy moja_firma.com, które pochodzą od hostów wewnętrznych. W celu zdefiniowania podziału DNS, należy wziąć pod uwagę następujące ustawienia konfiguracyjne:

- Łączenie zgodnych klientów

  Łączenie zgodnych klientów w instrukcji widoku używa jako argumentu listy AML. Wartości konfiguracji zdefiniowane w odpowiednim widoku są widoczne tylko dla adresów IP, z których wysłano zapytanie, jeśli są zgodne z adresem na liście AML. Jeśli adres IP, z którego wysłano zapytanie, jest zgodny z wieloma pozycjami zgodnych klientów w różnych instrukcjach widoku, jest używana pierwsza instrukcja widoku. W tym przypadku wszystkie zapytania przychodzące z zapory firewall zostaną wysłane pod adres 10.1.2.5. Zapytania te powinny zostać obsłużone przez dane strefy w widoku zewnętrznym. Dlatego też adres 10.1.2.5 został skonfigurowany tak, aby był zgodnym klientem widoku zewnętrznego. Widok wewnętrzny 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 znajdować się na liście AML przed przedrostkiem adresu dołączonego do listy.

- Kolejność elementów na liście AML

  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 zostanie natychmiast zablokowany.

  Jeśli elementy byłyby wpisane na listę w odwrotnej kolejności, tj. (10.1/16; !10.1.2.5), adresowi IP 10.1.2.5 zostałby przyznany dostęp, ponieważ serwer porównałby go z pierwszym elementem, który jest z nim zgodny, i nie pominąłby sprawdzania pozostałych reguł.

Odsyłacze pokrewne

"Przykład: dzielenie systemu DNS za zaporą firewall poprzez skonfigurowanie dwóch serwerów DNS na tej samej platformie System i" na stronie 20
Przykład ten przedstawia serwer DNS, który działa za zaporą firewall w celu zabezpieczania danych wewnętrznych ze strony Internetu i jednocześnie umożliwia wewnętrznym użytkownikom uzyskanie dostępu do danych w Internecie. Konfiguracja ta realizuje to zabezpieczenie poprzez skonfigurowanie dwóch serwerów DNS na tej samej platformie System i.

Planowanie systemu nazw domen

System DNS można skonfigurować na wiele sposobów. Jednak wcześniej należy zaplanować, jak powinien on działać w danej sieci. Należy ocenić takie tematy, jak struktura sieci, wydajność i bezpieczeństwo.

Określanie uprawnień systemu nazw domen

Istnieją szczególne wymagania autoryzacyjne dotyczące administratora DNS. Należy również uwzględnić wpływ autoryzacji na ochronę.

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

Aby administrator mógł skonfigurować i zarządzać systemem DNS, jest wymagany minimalny poziom uprawnień. 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 autoryzowania użytkowników można użyć programu System i Navigator. Więcej informacji zawiera temat Nadawanie uprawnień administratorowi DNS w pomocy elektronicznej dla systemu DNS.

Uwaga: Jeśli profil administratora nie ma pełnych uprawnień, należy mu przydzielić określone uprawnienia do wszystkich katalogów i powiązanych plików konfiguracyjnych DNS.

Odsyłacze pokrewne

"Obsługa plików konfiguracyjnych systemu nazw domen" na stronie 34
System DNS i5/OS może być używany do tworzenia instancji serwera DNS i zarządzania nią na platformie System i. Pliki konfiguracyjne DNS są zarządzane przez program System i Navigator. Nie można ich edytować ręcznie. Do tworzenia, zmiany lub usuwania plików konfiguracyjnych DNS należy zawsze używać programu System i Navigator.

Określanie struktury domeny

Konfigurując domenę po raz pierwszy, przed utworzeniem stref należy przewidzieć obciążenie i obsługę 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 firewallami. 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 i5/OS udostępnia interfejs graficzny do konfigurowania systemów. W niektórych przypadkach używane w tym interfejsie terminy i koncepcje różnią się od używanych w innych źródłach. Korzystając z innych źródeł informacji podczas planowania konfiguracji systemu DNS, warto pamiętać o następujących pozycjach:

- Wszystkie strefy i obiekty zdefiniowane na platformie System i 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, takie jak rekordy typu A lub AAAA. Strefy wyszukiwania wstecz to strefy używane do odwzorowywania adresów IP na nazwy domen według rekordów typu PTR.
- System DNS i5/OS odnosi się do *stref podstawowych* i *stref dodatkowych*.
- Interfejs korzysta z *podstref*, określanych w innych źródłach jako *poddomeny*. Strefa potomna jest podstrefą, do której delegowano odpowiedzialność przynajmniej jednego serwera nazw.

Planowanie środków bezpieczeństwa

DNS udostępnia opcje ochrony ograniczające dostęp z zewnątrz do serwera.

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 (lista kontroli dostępu - access control list). Dzięki temu, zawsze, gdy trzeba będzie użyć tej listy, można wywołać ACL i cała lista zostanie załadowana.

Kolejność elementów na liście AML

Zostanie użyty pierwszy element z listy AML, który pasuje do danego adresu. 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 zablokowany.

Jeśli elementy byłyby wpisane na listę w odwrotnej kolejności, tj. (10.1.1/24; !10.1.1.5), adresowi IP 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.

Ochrona serwera DNS jest kwestią podstawową. Oprócz przedstawionych w tym temacie uwag dotyczących bezpieczeństwa, bezpieczeństwo serwera DNS i serwera System i zostało omówione w różnych źródłach, w tym również w kolekcji tematów dotyczącej platformy System i i Internetu. Zagadnienia dotyczące bezpieczeństwa systemu DNS opisano również w książce *DNS and BIND*.

Pojęcia pokrewne

Serwery System i - bezpieczeństwo internetowe

Odsyłacze pokrewne

“Funkcje programu BIND 9” na stronie 8
Program BIND 9 jest podobny do programu BIND 8, jednak oferuje kilka funkcji, jak na przykład widoki, które poprawiają wydajność serwera DNS.

Wymagania systemu DNS

Aby uruchomić system nazw domen (DNS) na platformie System i, należy mieć na uwadze wymagania dotyczące oprogramowania.

Funkcja DNS, Opcja 31 nie może być automatycznie zainstalowana wraz z systemem operacyjnym. Należy ją oddzielnie wybrać do instalacji. Serwer DNS dołączony do systemu i5/OS opiera się na standardowej implementacji DNS znanej jako BIND 9. W poprzedniej wersji systemu OS/400 dostępne były usługi DNS oparte na programie BIND 8.2.5. Są one nadal dostępne w systemie i5/OS.

Po zainstalowaniu serwera DNS należy skonfigurować ten serwer i wykonać jego migrację z wersji BIND 4 lub 8 do wersji BIND 9. Należy także zainstalować środowisko PASE i5/OS, czyli Opcję 33 systemu i5/OS. Po zainstalowaniu środowiska PASE i5/OS program System i Navigator automatycznie skonfiguruje bieżącą implementację programu BIND.

Aby skonfigurować wysyłanie aktualizacji do danego serwera DNS przez serwer DHCP znajdujący się na innej platformie, należy również na serwerze DHCP zainstalować Opcję 31. Interfejsy programistyczne instalowane z Opcją 31 są niezbędne podczas wykonywania dynamicznych aktualizacji przez serwer DHCP.

Pojęcia pokrewne

i5/OS PASE

| “Konfigurowanie systemu nazw domen”
| Za pomocą programu System i Navigator można skonfigurować serwery nazw i rozstrzygnąć zapytania skierowane poza domenę.

| **Odsyłacze pokrewne**

| “Funkcje programu BIND 9” na stronie 8
| Program BIND 9 jest podobny do programu BIND 8, jednak oferuje kilka funkcji, jak na przykład widoki, które poprawiają wydajność serwera DNS.

Określanie, czy system nazw domen jest zainstalowany

Aby określić, czy system nazw domen (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 następnej strony **5761SS1 System nazw domen** (5761SS1 Domain Name System) (Opcja 31). Jeśli system DNS został pomyślnie zainstalowany, status instalacji będzie oznaczony wartością *COMPATIBLE, jak pokazano poniżej:

```
Progr.lic. Status instalacji    Opis
5761SS1    *COMPATIBLE          Domain Name System
```

4. Naciśnij klawisz F3, aby zamknąć ekran.

Instalowanie systemu nazw domen

Aby zainstalować system nazw domen (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 System nazw domen i naciśnij klawisz Enter.
4. Ponownie naciśnij klawisz Enter, aby potwierdzić instalację.

Konfigurowanie systemu nazw domen

Za pomocą programu System i Navigator można skonfigurować serwery nazw i rozstrzygnąć zapytania skierowane poza domenę.

Przed przystąpieniem do konfigurowania systemu DNS należy zapoznać się z sekcją Wymagania systemu DNS oraz zainstalować niezbędne komponenty DNS.

Pojęcia pokrewne

“Wymagania systemu DNS” na stronie 26
Aby uruchomić system nazw domen (DNS) na platformie System i, należy mieć na uwadze wymagania dotyczące oprogramowania.

Dostęp do systemu nazw domen w programie System i Navigator

Poniższe instrukcje wprowadzają do interfejsu konfigurowania serwera DNS w programie System i Navigator.

Za pomocą środowiska PASE i5/OS można skonfigurować serwery DNS działające w oparciu o program BIND 9.

Konfigurując serwer DNS po raz pierwszy, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń ***system*** → **Sieć** → **Serwery** → **DNS** (*system* > Network > Servers > DNS).
2. Prawym przyciskiem myszy kliknij **DNS** i wybierz **Nowa konfiguracja**.

Pojęcia pokrewne

Podstawowe informacje o programie System i Navigator

Konfigurowanie serwerów nazw

System DNS umożliwia utworzenie wielu instancji serwera nazw. W sekcji tej przedstawiono instrukcje dotyczące konfigurowania serwera nazw.

Serwer DNS i5/OS działający w oparciu o program BIND 9 obsługuje wiele instancji serwera nazw. Zadania opisane w poniższych sekcjach przedstawiają proces tworzenia pojedynczej instancji serwera nazw, w tym określenie jej właściwości i stref.

Aby utworzyć wiele instancji, należy powtarzać te procedury, dopóki wszystkie instancje nie zostaną utworzone. Różne instancje serwera nazw mogą mieć różne właściwości, na przykład poziomy debugowania i wartości autostartu. Podczas tworzenia nowej instancji tworzone są odrębne pliki konfiguracyjne.

Odsyłacze pokrewne

"Obsługa plików konfiguracyjnych systemu nazw domen" na stronie 34
System DNS i5/OS może być używany do tworzenia instancji serwera DNS i zarządzania nią na platformie System i. Pliki konfiguracyjne DNS są zarządzane przez program System i Navigator. Nie można ich edytować ręcznie. Do tworzenia, zmiany lub usuwania plików konfiguracyjnych DNS należy zawsze używać programu System i Navigator.

Tworzenie instancji serwera nazw

Kreator konfiguracji nowego systemu nazw domen (DNS) przeprowadzi użytkownika przez proces defniowania instancji serwera DNS.

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

1. W programie System i Navigator rozwiń ***system*** **→ Sieć → Serwery → DNS** (*system* > Network > Servers > DNS).
2. W lewym panelu kliknij prawym przyciskiem myszy pozycję **DNS** i wybierz opcję **Nowy serwer nazw** (New Name Server).
3. Aby zakończyć proces konfigurowania, postępuj zgodnie z instrukcjami kreatora.

Kreator wymaga podania następujących danych wejściowych:

Nazwa serwera DNS:
Określ nazwę dla serwera DNS. Może ona składać się z maksymalnie pięciu znaków i musi zaczynać się od znaku alfabetu (A-Z). 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.

Adres IP nasłuchiwania:
Dwie instancje serwera DNS nie mogą nasłuchiwać na tym samym adresie IP. Ustawieniem domyślnym jest nasłuchiwanie wszystkich adresów IP. W przypadku tworzenia dodatkowych instancji serwera żaden z nich nie może być skonfigurowany tak, aby nasłuchiwał wszystkich adresów IP. W przeciwnym razie nie będą one mogły być uruchomione jednocześnie. 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 można załadować tylko wtedy, gdy serwer DNS ma dostęp do Internetu i będzie mógł 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.

Edytowanie 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 programie System i Navigator rozwiń ***system*** → **Sieć** → **Serwery** → **DNS** (*system* > Network > Servers > DNS).
2. W prawym panelu okna kliknij prawym klawiszem myszy ***serwer DNS*** i wybierz **Konfiguracja**.
3. W oknie Konfiguracja DNS (DNS Configuration) kliknij prawym przyciskiem myszy pozycję **Serwer DNS** (DNS Server) i wybierz opcję **Właściwości** (Properties).
4. Edytuj odpowiednie właściwości według potrzeb.

Konfigurowanie stref na serwerze nazw

Po skonfigurowaniu instancji serwera DNS należy skonfigurować strefy serwera nazw.

Aby skonfigurować strefy na serwerze, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń ***system*** → **Sieć** → **Serwery** → **DNS** (*system* > Network > Servers > DNS).
2. W prawym panelu okna kliknij prawym klawiszem myszy ***serwer DNS*** i wybierz **Konfiguracja**.
3. W oknie Konfiguracja DNS (DNS Configuration) wybierz typ strefy, którą chcesz utworzyć, klikając prawym przyciskiem myszy folder **Strefa wyszukiwania do przodu** (Forward Lookup Zone) lub **Strefa wyszukiwania wstecz** (Reverse Lookup Zone).
4. Aby zakończyć proces tworzenia, postępuj zgodnie z instrukcjami kreatora.

Pojęcia pokrewne

"Dostęp do zewnętrznych danych systemu nazw domen" na stronie 31
Po utworzeniu danych strefy DNS serwer będzie w stanie tłumaczyć zapytania dotyczące tej strefy.

Zadania pokrewne

"Konfigurowanie odbierania dynamicznych aktualizacji przez serwer DNS" na stronie 30
Serwery DNS działające pod kontrolą programu BIND 9 mogą być skonfigurowane w taki sposób, aby akceptowały żądania dynamicznej aktualizacji danych strefy pochodzące z innych źródeł. Sekcja ta zawiera instrukcje konfigurowania opcji zezwolenia na aktualizację (allow-update), tak aby serwer DNS mógł odbierać dynamiczne aktualizacje.

"Importowanie plików systemu nazw domen" na stronie 30
Do systemu DNS można zaimportować istniejące pliki danych strefy. Przedstawione procedury tworzenia nowych stref na podstawie istniejących plików konfiguracyjnych sprzyjają oszczędzaniu na czasie.

Odsyłacze pokrewne

"Podstawy stref" na stronie 3
Dane DNS są podzielone na łatwe do zarządzania zestawy zwane *strefami*. Każdy z tych zestawów jest określonym typem strefy.

Konfigurowanie widoków na serwerze nazw

Jedną z opcji oferowanych przez program BIND 9 jest instrukcja *widok* (View), która pozwala pojedynczej instancji systemu nazw domen udzielać różnych odpowiedzi na zapytanie w zależności od źródła pochodzenia zapytania, takiego jak Internet lub intranet. Jednym z praktycznych zastosowań opcji Widok jest podział konfiguracji DNS bez potrzeby uruchamiania wielu serwerów DNS.

Aby skonfigurować widoki na serwerze, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń ***system*** → **Sieć** → **Serwery** → **DNS** (*system* > Network > Servers > DNS).
2. W prawym panelu okna kliknij prawym klawiszem myszy ***serwer DNS*** i wybierz **Konfiguracja**.

3. W oknie Konfiguracja DNS (DNS Configuration) kliknij prawym przyciskiem myszy pozycję **Widoki** (Views) i wybierz opcję **Nowy widok** (New View).
4. Aby zakończyć proces tworzenia, postępuj zgodnie z instrukcjami kreatora.

Konfigurowanie odbierania dynamicznych aktualizacji przez serwer DNS

Serwery DNS działające pod kontrolą programu BIND 9 mogą być skonfigurowane w taki sposób, aby akceptowały żądania dynamicznej aktualizacji danych strefy pochodzące z innych źródeł. Sekcja ta zawiera instrukcje konfigurowania opcji zezwolenia na aktualizację (allow-update), tak aby serwer DNS mógł odbierać dynamiczne aktualizacje.

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 strefy dynamicznej i zrestartować go po zakończeniu aktualizacji. Zatrzymanie serwera wymusza aktualizację bazy danych strefy wraz ze wszystkimi aktualizacjami dynamicznymi dokonanymi od czasu pierwszego załadowania przez serwer danych strefy z bazy danych strefy. Jeśli serwer nie zostanie zatrzymany, wszystkie ręczne aktualizacje bazy danych strefy zostaną utracone, ponieważ zostaną nadpisane przez działający serwer. 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 programie System i Navigator rozwiń ***system*** **→ Sieć → Serwery → DNS** (*system* > Network > Servers > 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 listy zgodności adresów, wybierz typ pozycji listy i kliknij **Dodaj** (Add). Możesz dodać adres IP, przedrostek IP, listę ACL (Access Control List) lub klucz.
8. Po zakończeniu aktualizacji listy zgodności adresów kliknij przycisk **OK**, aby zamknąć stronę Opcje.

Zadania pokrewne

"Konfigurowanie stref na serwerze nazw" na stronie 29
Po skonfigurowaniu instancji serwera DNS należy skonfigurować strefy serwera nazw.

Konfigurowanie serwera DHCP pod kątem wysyłania dynamicznych aktualizacji DNS

Importowanie plików systemu nazw domen

Do systemu DNS można zaimportować istniejące pliki danych strefy. Przedstawione procedury tworzenia nowych stref na podstawie istniejących plików konfiguracyjnych sprzyjają oszczędzaniu na czasie.

Strefę podstawową można utworzyć, importując plik danych strefy, który jest poprawnym plikiem konfiguracyjnym strefy według zasad składni BIND. Plik powinien znajdować się w katalogu zintegrowanego systemu plików. Podczas importowania serwer DNS sprawdzi, czy jest to poprawny plik danych strefy i dołączy go do pliku named.conf dla określonej instancji serwera.

Aby zaimportować plik strefy, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń ***system*** **→ Sieć → Serwery → DNS** (*system* > Network > Servers > DNS).
2. W prawym panelu dwukrotnie kliknij instancję serwera DNS, do której chcesz zaimportować strefę.

3. W lewym panelu okna Konfiguracja DNS (DNS Configuration) kliknij prawym przyciskiem myszy **Serwer DNS** (DNS Server) i wybierz **Strefa importująca** (Import Zone).
4. Wykonuj instrukcje kreatora, aby zaimportować strefę podstawową.

Zadania pokrewne

"Konfigurowanie stref na serwerze nazw" na stronie 29
Po skonfigurowaniu instancji serwera DNS należy skonfigurować strefy serwera nazw.

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.

Uwagi:

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

Dostęp do zewnętrznych danych systemu nazw domen

Po utworzeniu danych strefy DNS serwer będzie w stanie tłumaczyć zapytania dotyczące tej strefy.

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 programu System i 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 dostarczona z programem System i Navigator. Lista jest aktualna na dzień wprowadzenia bieżącej wersji programu System i Navigator. Można sprawdzić aktualność domyślnej listy, porównując ją z listą w serwisie InterNIC. Należy aktualizować konfiguracyjną listę serwerów głównych, aby odpowiadała stanowi bieżącemu.

Pobieranie adresów 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. Zaloguj się anonimowo przez protokół FTP na serwer InterNIC: FTP.INTERNIC.NET lub RS.INTERNIC.NET
2. Pobierz ten plik: /domain/named.root
3. Zapisz plik w katalogu o następującej ścieżce: /QOpenSys/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.

Zadania pokrewne

"Konfigurowanie stref na serwerze nazw" na stronie 29
Po skonfigurowaniu instancji serwera DNS należy skonfigurować strefy serwera nazw.

Zarządzenie systemem nazw domen

Zarządzenie serwerem DNS obejmuje sprawdzanie działania funkcji DNS, monitorowanie wydajności oraz obsługiwanie danych i plików systemu DNS.

Funkcja sprawdzania systemu nazw domen działa

Narzędzie DIG może pomóc w pobraniu informacji z serwera DNS i umożliwia testowanie odpowiedzi tego serwera. Za pomocą narzędzia DIG można sprawdzić, czy serwer DNS działa prawidłowo.

Można zażądać nazwy hosta powiązanej z adresem IP pętli zwrotnej (127.0.0.1). Serwer powinien zwrócić nazwę hosta lokalnego (localhost). Można również wysłać zapytania dotyczące specyficznych nazw zdefiniowanych w instancji serwera, która ma zostać sprawdzona. Pozwoli to potwierdzić, że testowana instancja serwera działa prawidłowo.

Aby sprawdzić działanie funkcji DNS za pomocą narzędzia DIG, wykonaj następujące czynności:

1. W wierszu komend wpisz DIG HOSTNAME('127.0.0.1') REVERSE(*YES).

   Powinny zostać wyświetlone następujące informacje (w tym również nazwa hosta pętli zwrotnej):

```
;; opcje globalne: printcmd
;; Przyszła odpowiedź:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id:865
;; flagi: qr aa rd ra; ZAPYTANIE: 1, ODPOWIEDŹ: 1, UPRAWNIENIA: 1, DODATKOWE:1

;; SEKCJA PYTANIA:
;1.0.0.127.in-addr.arpa.          IN   PTR

;; SEKCJA ODPOWIEDZI:
1.0.0.127.in-addr.arpa.  86400   IN    PTR  localhost.

;; SEKCJA UPRAWNIEŃ:
0.0.127.in-addr.arpa.   86400   IN    NS   ISA2LP05.RCHLAND.IBM.COM.

;; SEKCJA DODATKOWA:
ISA2LP05.RCHLAND.IBM.COM. 38694   IN    A   9.5.176.194

;; Czas zapytania: 552 ms
;; SERWER: 9.5.176.194#53(9.5.176.194)
;; DATA: Thu May 31 21:38:12 2007
;; Wielkość odebranego komunikatu: 117
```

   Serwer DNS odpowie prawidłowo, jeśli zwróci nazwę hosta pętli zwrotnej: **localhost**.

2. Naciśnij klawisz Enter, aby wyjść z sesji.

Uwaga: Aby uzyskać pomoc podczas korzystania z narzędzia DIG, wpisz ?DIG i naciśnij klawisz Enter.

Zarządzanie kluczami blokady

Klucze blokady pozwalają ograniczyć dostęp do danych DNS.

Istnieją dwa typy kluczy związanych z DNS. Są to klucze DNS i klucze dynamicznej aktualizacji. Każdy z nich pełni inną rolę w zabezpieczaniu konfiguracji serwera DNS. Poniżej opisano ich związek z serwerem DNS.

Zarządzanie kluczami systemu nazw domen

Klucze DNS są kluczami definiowanymi dla BIND i są używane 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 programie System i Navigator rozwiń ***system*** → **Sieć** → **Serwery** → **DNS** (*system* > Network > Servers > DNS).
2. W prawym panelu kliknij prawym przyciskiem myszy instancję serwera DNS, którą chcesz zarządzać, i wybierz opcję **Konfiguracja** (Configuration).
3. W oknie Konfiguracja DNS (DNS Configuration) wybierz opcje **Zbiór** → **Zarządzanie kluczami** (File > Manage Keys).

W oknie Zarządzanie kluczami (Manage Keys) można wykonać odpowiednie zadania związane z zarządzaniem.

Zarządzanie kluczami 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 tej samej platformie System i. Jeśli serwer DHCP działa na innej platformie System i, należy rozesłać te same zbiory kluczy aktualizacji dynamicznej do każdej zdalnej platformy System i, dla której zbiory te są niezbędne do wysłania aktualizacji dynamicznych do serwerów autorytatywnych. Zbiory te można rozesłać za pomocą FTP, poczty elektronicznej itp.

Aby zarządzać kluczami aktualizacji dynamicznej, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń ***system*** → **Sieć** → **Serwery** → **DNS** (*system* > Network > Servers > DNS).
2. Kliknij prawym przyciskiem myszy pozycję **DNS** i wybierz opcję **Zarządzanie kluczami aktualizacji dynamicznej** (Manage Dynamic Update Keys)

Następnie w oknie Zarządzania kluczami aktualizacji dynamicznej można wykonać odpowiednie zadania związane z zarządzaniem.

Dostęp do statystyk serwera DNS

Zrzut bazy danych i narzędzia statystyczne mogą pomóc w ocenie wydajności serwera i w zarządzaniu nią.

System nazw domen (DNS) udostępnia kilka narzędzi diagnostycznych. Można ich używać do monitorowania wydajności lokalnego serwera.

Odsyłacze pokrewne

"Obsługa plików konfiguracyjnych systemu nazw domen" na stronie 34
System DNS i5/OS może być używany do tworzenia instancji serwera DNS i zarządzania nią na platformie System i. Pliki konfiguracyjne DNS są zarządzane przez program System i Navigator. Nie można ich edytować ręcznie. Do tworzenia, zmiany lub usuwania plików konfiguracyjnych DNS należy zawsze używać programu System i Navigator.

Dostęp do statystyk serwera

Statystyki serwera zawierają podsumowanie liczby zapytań i odpowiedzi odebranych przez serwer od czasu ostatniego restartu lub przeładowania bazy danych.

System DNS umożliwia przeglądanie statystyk dla każdej instancji serwera. 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 programie System i Navigator rozwiń ***system*** **→ Sieć → Serwery → DNS** (*system* > Network > Servers > DNS).
2. W prawym panelu okna kliknij prawym klawiszem myszy ***serwer DNS*** i wybierz **Konfiguracja**.
3. W oknie Konfiguracja DNS (DNS configuration) wybierz **Widok → Statystyki serwera** (View > Server Statistics).

Aby wyświetlić informacje dotyczące statystyk serwera, które znajdują się w pliku named.stats, można użyć komendy Remote Name Daemon Control (RNDC). Odpowiednia komenda jest następująca.

```
RNDC RNDCCMD('stats')
```

Dostęp do bazy danych aktywnego serwera

Baza danych aktywnego serwera 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), pomocne przy rozwiązywaniu problemów.

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.

Zrzut bazy danych aktywnego serwera można wyświetlić za pomocą programu System i Navigator. Jeśli konieczne będzie zeskładowanie kopii zbiorów, zbiór zrzutu bazy danych o nazwie named_dump.db znajduje się w katalogu systemu i5/OS o ścieżce: /QIBM/UserData/OS400/DNS/<instancja serwera>/, gdzie <*instancja serwera*> jest nazwą instancji serwera DNS. Więcej informacji o bazie danych aktywnego serwera można znaleźć w następującym temacie pomocy elektronicznej dla serwera DNS: Podstawy operacji zrzutu bazy danych serwera DNS.

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

1. W programie System i Navigator rozwiń ***system*** **→ Sieć → Serwery → DNS** (*system* > Network > Servers > DNS).
2. W prawym panelu okna kliknij prawym klawiszem myszy ***serwer DNS*** i wybierz **Konfiguracja**.
3. W oknie Konfiguracja DNS (DNS configuration) wybierz pozycje **Widok → Baza danych aktywnego serwera** (View > Active Server Database).

Aby wyświetlić informacje o bazie danych aktywnego serwera znajdujące się w zbiorze named_dump.db, można użyć komendy Remote Name Daemon Control (RNDC). Odpowiednia komenda jest następująca.

```
RNDC RNDCCMD('dumpdb -all')
```

Obsługa plików konfiguracyjnych systemu nazw domen

System DNS i5/OS może być używany do tworzenia instancji serwera DNS i zarządzania nią na platformie System i. Pliki konfiguracyjne DNS są zarządzane przez program System i Navigator. Nie można ich edytować ręcznie. Do tworzenia, zmiany lub usuwania plików konfiguracyjnych DNS należy zawsze używać programu System i Navigator.

Pliki te są przechowywane w katalogach zintegrowanego systemu zbiorów o ścieżkach podanych poniżej.

Uwaga: Poniższa struktura pliku dotyczy serwera DNS działającego z programem BIND 9.

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	Ikona	Opis
/QIBM/UserData/OS400/DNS/		Katalog początkowy systemu DNS.
/QIBM/UserData/OS400/DNS/ <*instance-n*>/		Katalog początkowy instancji serwera DNS.
ATTRIBUTES		System DNS korzysta z tego pliku do określenia używanej wersji programu BIND.
BOOT.AS400BIND4		Plik strategii i konfiguracji serwera BIND 4.9.3, który zostanie przekonwertowany na plik o nazwie named.conf serwera BIND 8 dla tej instancji. Plik ten jest tworzony podczas migracji serwera BIND 4.9.3 do BIND 9. Jest on kopią zapasową na potrzeby migracji i może zostać usunięty, jeśli serwer BIND 9 działa prawidłowo.
named.ca		Lista serwerów głównych dla tej instancji serwera.
named.conf		Ten plik zawiera dane konfiguracyjne. Informuje on serwer o konkretnych strefach, którymi serwer zarządza, oraz o tym, gdzie znajdują się pliki stref, które strefy mogą być dynamicznie aktualizowane, gdzie znajdują się serwery przekazujące, jak również o innych ustawieniach opcji.
named_dump.db		Zrzut danych serwera utworzony dla bazy danych aktywnego serwera.
named.memstats		Statystyki pamięci serwera (jeśli zostały skonfigurowane w pliku named.conf).
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.
named.random		Plik entropii generowany przez serwer.
named.recursing		Rekurencyjne zapytania serwerów (jeśli są żądane przez program System i Navigator).
named.run		Domyślny protokół debugowania (jeśli jest żądany). Może przybierać nazwę named.run.0, named.run.1, itd.
named.stats		Statystyki serwera.
<*primary-zone-n*>.db		Jest to plik strefy podstawowej dla konkretnej domeny na tym serwerze. Plik zawiera wszystkie rekordy zasobów dla tej strefy. Każda strefa ma osobny plik .db.

Nazwa	Ikona	Opis
<*primary-zone-n*>.jnl		Plik kroniki zawierający aktualizacje dynamiczne dla strefy. Jest tworzony podczas odbierania pierwszej aktualizacji dynamicznej. Gdy serwer jest restartowany po zamknięciu systemu lub awarii, odtwarza plik kroniki, aby wykonać aktualizacje strefy, które miały miejsce po ostatnim zrzucie strefy. Plik ten jest także używany do przyrostowego przesyłania strefowego (IXFR). Te pliki protokołu nie przestają istnieć. Jest to plik binarny i nie należy go edytować.
db.<*secondary-zone-n*>		Kopia pliku strefy dla konkretnej domeny na tym serwerze. Zawiera wszystkie rekordy zasobów dla tej strefy. Podczas uruchamiania plik ten służy do początkowego ładowania serwera pomocniczego, jeśli serwer główny jest niedostępny. Każda strefa ma osobny plik .db.
/QIBM/UserData/OS400/DNS/_DYN/		Katalog, w którym przechowywane są pliki wymagane podczas aktualizacji dynamicznych.
<*key_id-n*>._KEY		.Symlink do klucza DNSSEC z kluczem <*key_id-n*>. Zawsze wskazuje na ostatnio utworzony klucz K<*key_id-n*>.+*aaa*+*nnnnn*.key.
<*key_id-x*>._DUK. <*zone-a*>		Klucz aktualizacji dynamicznej wymagany do zainicjowania żądania aktualizacji dynamicznej do strefy <*zone-a*> za pomocą klucza <*key_id-x*>.
<*key_id-x*>._KID		Plik zawierający instrukcję klucza dla id_klucza o nazwie <*key_id-x*>
<*key_id-y*>._DUK. <*zone-a*>		Klucz aktualizacji dynamicznej wymagany do zainicjowania żądania aktualizacji dynamicznej do strefy <*zone-a*> za pomocą klucza <*key_id-y*>.
<*key_id-y*>._DUK. <*zone-b*>		Klucz aktualizacji dynamicznej wymagany do zainicjowania żądania aktualizacji dynamicznej do strefy <*zone-b*> za pomocą klucza <*key_id-y*>.
<*key_id-y*>._KID		Plik zawierający instrukcję klucza dla id_klucza o nazwie <*key_id-y*>
rndc-confgen.random.*nnnnnn*		Pliki entropii dla różnych komend, które ich wymagają. Część *nnnnn* określa numer zadania, które utworzyło zbiór. Pozostają one tylko wtedy, gdy komenda jest z jakiegoś powodu anulowana i nie zostanie wykonana procedura czyszcząca.

Pojęcia pokrewne

“Określanie uprawnień systemu nazw domen” na stronie 24
Istnieją szczególne wymagania autoryzacyjne dotyczące administratora DNS. Należy również uwzględnić wpływ autoryzacji na ochronę.

"Dostęp do statystyk serwera DNS" na stronie 33
Zrzut bazy danych i narzędzia statystyczne mogą pomóc w ocenie wydajności serwera i w zarządzaniu nią.

Zadania pokrewne

"Konfigurowanie serwerów nazw" na stronie 28
System DNS umożliwia utworzenie wielu instancji serwera nazw. W sekcji tej przedstawiono instrukcje dotyczące konfigurowania serwera nazw.

Zaawansowane funkcje systemu nazw domen

Temat ten zawiera informacje na temat zaawansowanych funkcji DNS, pozwalających doświadczonym administratorom na łatwiejsze zarządzanie serwerem DNS.

System DNS w programie System i Navigator udostępnia interfejs z zaawansowanymi funkcjami służącymi do konfigurowania serwera DNS i zarządzania nim. Następujące zadania są skrótami dla administratorów, którzy znają graficzny interfejs systemu i5/OS. Przedstawiają one metody szybkiej zmiany statusu serwera i atrybutów dla wielu instancji jednocześnie.

Zadania pokrewne

"Zmiana ustawień debugowania systemu DNS" na stronie 40
Funkcje debugowania DNS dostarczają informacji, które mogą pomóc w określeniu i rozwiązaniu problemów z serwerem DNS.

Uruchamianie lub zatrzymywanie serwerów DNS

Jeśli system nazw domen w interfejsie System i Navigator nie pozwala na jednoczesne uruchomienie lub zatrzymanie wielu instancji serwera, można zmienić te ustawienia dla wielu instancji jednocześnie za pomocą 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

Zmiana poziomu debugowania może okazać się użyteczna dla administratorów dużych stref, którzy nie chcą dużych ilości danych debugowania zbieranych, gdy serwer uruchamia się po raz pierwszy i ładuje wszystkie dane strefy.

System DNS w interfejsie programu System i Navigator nie pozwala na zmianę poziomu debugowania podczas pracy serwera. Poziom debugowania można jednak zmienić podczas pracy serwera za pomocą interfejsu znakowego. Aby zmienić poziom debugowania za pomocą interfejsu znakowego, wykonaj następujące czynności, zastępując wartość *nnnnn* w komendzie nazwą 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 RNDC RNDCCMD('trace') i naciśnij klawisz Enter.
   - Aby wyłączyć debugowanie, wpisz RNDC RNDCCMD('notrace') i naciśnij klawisz Enter.

Rozwiązywanie problemów dotyczących systemu nazw domen

Ustawienia protokołowania i debugowania systemu DNS mogą pomóc rozwiązać problemy z serwerem 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.

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:

- W przypadku serwerów wykorzystujących program BIND 9 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 komunikatów serwera systemu nazw domen

W systemie nazw domen (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.

Program BIND 9 oferuje kilka opcji protokołowania. Można obecnie określić typy protokołowanych komunikatów, miejsca, do których zostały wysłane, jak również poziom istotności dla każdego typu komunikatu. Zasadniczo domyślne ustawienia protokołowania są odpowiednie, ale przed ich zmianą jest zalecane odniesienie się do innych źródeł dokumentacji programu BIND 9 w celu uzyskania informacji o protokołowaniu.

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 i5os_debug i i5os_QPRINT. Komunikaty debugowania są domyślnie protokołowane w kanale i5os_debug, który jest zbiorem named.run, do którego można również wysyłać inne kategorie komunikatów. Kategorie komunikatów protokołowanych w kanale i5os_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 i5os_joblog. Protokołowane komunikaty kierowane do tego kanału są wysyłane do protokołu zadania instancji serwera DNS.

- **Kanały null**

  Wszystkie komunikaty protokołowane w kanale null są usuwane. Domyślnym kanałem null jest i5os_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. Kategorie są następujące:

client Przetwarzanie żądań klienta.

config Analizowanie i przetwarzanie zbioru konfiguracyjnego.

database
Komunikaty dotyczące baz danych używanych wewnętrznie przez serwer DNS do składowania danych o strefie i pamięci podręcznej.

default Definicje opcji protokołowania dla tych kategorii, w których nie zdefiniowano konkretnej konfiguracji.

delegation-only
Tylko delegacja. Protokołuje zapytania, które zostały wymuszone na elemencie NXDOMAIN jako wynik strefy typu ″tylko delegacja″ lub elementu typu ″tylko delegacja″ we wskazówce lub deklaracji wyznacznika strefy.

dispatch
Rozsyłanie pakietów przychodzących do modułów serwera, gdzie mają zostać przetworzone.

dnssec Przetwarzanie protokołów DNS Security Extensions (DNSSEC) i Transaction Signature (TSIG).

general
Kategoria ogólna dla elementów, których nie sklasyfikowano w innych kategoriach.

lame-servers
Serwery niepoprawne, które są błędnymi konfiguracjami serwerów zdalnych wykrytymi przez program BIND 9 podczas próby wysłania do nich zapytania w czasie rozstrzygania.

network
Działania w sieci.

notify Protokół NOTIFY.

resolver
Rozstrzyganie DNS, np. wyszukiwania rekurencyjne, wykonywane w imieniu klientów przez buforujący serwer nazw.

security
Zatwierdzanie i odrzucanie żądań.

xfer-in Transfery strefowe otrzymywane przez serwer.

xfer-out
Transfery strefowe wysyłane przez serwer.

unmatched
Nazwane komunikaty, który klasy nie można określić lub dla których nie istnieje odpowiedni widok. W kategorii Client jest również protokołowane jednowierszowe podsumowanie. Najlepiej wysłać tę kategorię do pliku lub standardowego wyjścia błędów. Kategoria ta jest domyślnie wysyłana do kanału null.

update Aktualizacje dynamiczne.

update-security
Zatwierdzanie i odrzucanie żądań aktualizacji. Zapytania określają miejsce ich protokołowania. Określenie zapytań kategorii podczas uruchamiania włącza protokołowanie zapytań, o ile nie określono opcji querylog.

Pozycja protokołu zapytania informuje o adresie IP i numerze portu klienta, a także nazwie, klasie i typie zapytania. Informuje także o tym, czy ustawiono flagę Recursion Desired (+ jeśli ją ustawiono, - jeśli nie), czy użyto EDNS (E) lub czy zapytanie zostało podpisane (S).

Pliki protokołów mogą znacznie zwiększać swoją objętość, więc można je okresowo usuwać. Kiedy serwer DNS jest zatrzymywany lub uruchamiany, cała zawartość pliku protokołu 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 programie System i Navigator rozwiń ***system*** → **Sieć** → **Serwery** → **DNS** (*system* > Network > Servers > 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 dotycząca rozwiązywania problemów z poziomem istotności

Domyślny poziom istotności komunikatu dla kanału i5os_joblog to Błąd (Error). 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 źródła, może być potrzebna zmiana poziomu istotności. Należy wykonać powyższą procedurę, aby uzyskać dostęp do strony Kanały (Channels) i zmienić poziom istotności dla kanału i5os_joblog na Ostrzeżenie (Warning), Uwaga (Note) lub Informacja (Info), tak aby można było zobaczyć więcej protokołowanych danych. Po rozwiązaniu problemu należy przywrócić poziom istotności na Błąd (Error), aby zmniejszyć liczbę komunikatów w protokole zadania.

Zmiana ustawień debugowania systemu DNS

Funkcje debugowania DNS dostarczają informacji, które mogą pomóc w określeniu i rozwiązaniu problemów z serwerem DNS.

W systemie DNS dostępnych jest 12 poziomów debugowania. Protokołowanie jest zazwyczaj łatwiejszą metodą rozwiązywania problemów, ale niekiedy konieczne może być użycie debugowania. W normalnych warunkach debugowanie jest wyłączone (wartość = 0). 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 wynoszące 1 lub więcej powodują zapisywanie informacji debugowania w pliku named.run w katalogu systemu i5/OS o podanej ścieżce: /QIBM/UserData/OS400/DNS/<*instancja serwera*>, gdzie <*instancja serwera*> jest nazwą instancji serwera DNS. Plik named.run zwiększa swoją objętość tak długo, jak poziom debugowania jest ustawiony na jeden lub więcej, a serwer DNS nadal działa. Można również skorzystać ze strony Właściwości serwera - Kanały (Server Properties - Channels), aby określić maksymalną wielkość i liczbę wersji pliku named.run.

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

1. W programie System i Navigator rozwiń ***system*** → **Sieć** → **Serwery** → **DNS** (*system* > Network > Servers > 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.

Pojęcia pokrewne

"Zaawansowane funkcje systemu nazw domen" na stronie 37
Temat ten zawiera informacje na temat zaawansowanych funkcji DNS, pozwalających doświadczonym administratorom na łatwiejsze zarządzanie serwerem DNS.

Informacje pokrewne dotyczące systemu DNS

Informacje związane z kolekcją tematów dotyczących systemu nazw domen są zawarte także w dokumentacji technicznej IBM Redbooks, w serwisach WWW oraz w innych kolekcjach tematów Centrum informacyjnego. Wszystkie pliki PDF można wyświetlić lub wydrukować.

IBM Redbooks (Dokumentacja techniczna)

AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support (około 5181 kB)

Ta dokumentacja techniczna Redbooks zawiera informacje na temat obsługi serwerów DNS (Domain Name System) i DHCP (Dynamic Host Configuration Protocol) wchodzących w skład systemu i5/OS. Przykłady zawarte w tej dokumentacji pomagają zainstalować, dostosować i skonfigurować obsługę DNS i DHCP, a także rozwiązywać problemy.

Serwisy WWW

- *DNS and BIND*, wydanie piąte. Paul Albitz i Cricket Liu. Wydane przez O'Reilly and Associates,Inc. Sebastopol, California, 2006. ISBN: 0-59610-057-4.
- The BIND Administrator Reference Manual (wersja PDF) z serwisu WWW Internet System Consortium (ISC) .
- Serwis WWW Internet Software Consortium zawiera wiadomości, odsyłacze i inne zasoby dotyczące programu BIND.
- W serwisie InterNIC jest publikowany katalog wszystkich podmiotów rejestrujących nazwy domen autoryzowanych przez Internet Corporation for Assigned Names and Numbers (ICANN).
- Serwis DNS Resources Directory zawiera materiały referencyjne 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 .

Odsyłacze pokrewne

"Plik PDF z informacjami na temat systemu nazw domen" na stronie 2
Informacje zawarte w tym temacie są także dostępne w postaci pliku PDF, który można wyświetlić i wydrukować.

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. Odwołanie do produktu, programu lub usługi IBM nie oznacza, że można użyć wyłącznie tego produktu, programu lub usługi. Zamiast nich można zastosować ich odpowiednik funkcjonalny pod warunkiem, że nie narusza to praw własności intelektualnej IBM. Jednakże cała odpowiedzialność za ocenę przydatności i sprawdzenie działania produktu, programu lub usługi pochodzących od producenta innego niż IBM spoczywa na użytkowniku.

IBM może posiadać patenty lub złożone wnioski patentowe na towary i usługi, o których mowa w niniejszej publikacji. Przedstawienie niniejszej publikacji nie daje żadnych uprawnień licencyjnych do tychże patentów. Pisemne zapytania w sprawie licencji można przesyłać na adres:

IBM
Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
USA

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
Tokio 106-0032, Japonia

Poniższy akapit nie obowiązuje w Wielkiej Brytanii, a także w innych krajach, w których jego treść pozostaje w sprzeczności z przepisami prawa miejscowego: INTERNATIONAL BUSINESS MACHINES CORPORATION DOSTARCZA TĘ PUBLIKACJĘ W STANIE, W JAKIM SIĘ ZNAJDUJE “AS IS” BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI (W TYM TAKŻE RĘKOJMI), WYRAŹNYCH LUB DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CELU ORAZ GWARANCJI, ŻE PUBLIKACJA NIE NARUSZA PRAW STRON TRZECICH. Ustawodawstwa niektórych krajów nie dopuszczają zastrzeżeń dotyczących gwarancji wyraźnych lub domniemanych w odniesieniu do pewnych transakcji; w takiej sytuacji powyższe zdanie nie ma zastosowania.

Informacje zawarte w niniejszej publikacji mogą zawierać nieścisłości techniczne lub błędy drukarskie. Informacje te są okresowo aktualizowane, a zmiany te zostaną uwzględnione w kolejnych wydaniach tej publikacji. IBM zastrzega sobie prawo do wprowadzania ulepszeń i/lub zmian w produktach i/lub programach opisanych w tej publikacji w dowolnym czasie, bez wcześniejszego powiadomienia.

Wszelkie wzmianki w tej publikacji na temat stron internetowych innych firm zostały wprowadzone wyłącznie dla wygody użytkowników i w żadnym wypadku nie stanowią zachęty do ich odwiedzania. Materiały dostępne na tych stronach nie są częścią materiałów opracowanych dla tego produktu IBM, a użytkownik korzysta z nich na własną odpowiedzialność.

IBM ma prawo do używania i rozpowszechniania informacji przysłanych przez użytkownika w dowolny sposób, jaki uzna za właściwy, bez żadnych zobowiązań wobec ich autora.

Licencjobiorcy tego programu, którzy chcieliby uzyskać informacje na temat programu w celu: (i) wdrożenia wymiany informacji między niezależnie utworzonymi programami i innymi programami (łącznie z tym opisywanym) oraz (ii) wspólnego wykorzystywania wymienianych informacji, powinni skontaktować się z:

IBM
Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
USA

Informacje takie mogą być udostępnione, o ile spełnione zostaną odpowiednie warunki, w tym, w niektórych przypadkach, uiszczenie odpowiedniej opłaty.

Licencjonowany program opisany w niniejszym dokumencie oraz wszystkie inne licencjonowane materiały dostępne dla tego programu są dostarczane przez IBM na warunkach określonych w Umowie IBM z Klientem, Międzynarodowej Umowie Licencyjnej IBM na Program, Umowie Licencyjnej IBM na Kod Maszynowy lub w innych podobnych umowach zawartych między IBM i użytkownikami.

Wszelkie dane dotyczące wydajności zostały zebrane w kontrolowanym środowisku. W związku z tym rezultaty uzyskane w innych środowiskach operacyjnych mogą się znacząco różnić. Niektóre pomiary mogły być dokonywane na systemach będących w fazie rozwoju i nie ma gwarancji, że pomiary te wykonane na ogólnie dostępnych systemach dadzą takie same wyniki. Niektóre z pomiarów mogły być estymowane przez ekstrapolację. Rzeczywiste wyniki mogą być inne. Użytkownicy powinni we własnym zakresie sprawdzić odpowiednie dane dla ich środowiska.

Informacje dotyczące produktów firm innych niż IBM pochodzą od dostawców tych produktów, z opublikowanych przez nich zapowiedzi lub innych powszechnie dostępnych źródeł. Firma IBM nie testowała tych produktów i nie może potwierdzić dokładności pomiarów wydajności, kompatybilności ani żadnych innych danych związanych z tymi produktami. Pytania dotyczące możliwości produktów firm innych niż IBM należy kierować do dostawców tych produktów.

Wszelkie stwierdzenia dotyczące przyszłych kierunków rozwoju i zamierzeń IBM mogą zostać zmienione lub wycofane bez powiadomienia.

Publikacja ta zawiera przykładowe dane i raporty używane w codziennych operacjach działalności gospodarczej. W celu kompleksowego ich zilustrowania, podane przykłady zawierają nazwiska osób prywatnych, nazwy przedsiębiorstw oraz nazwy produktów. Wszystkie te nazwy/nazwiska są fikcyjne i jakiekolwiek podobieństwo do istniejących nazw/nazwisk i adresów jest całkowicie przypadkowe.

LICENCJA W ZAKRESIE PRAW AUTORSKICH:

Niniejsza publikacja zawiera przykładowe aplikacje w kodzie źródłowym, ilustrujące techniki programowania w różnych systemach operacyjnych. Użytkownik może kopiować, modyfikować i dystrybuować te programy przykładowe w dowolnej formie bez uiszczania opłat na rzecz IBM, w celu projektowania, używania, sprzedaży lub dystrybucji aplikacji zgodnych z aplikacyjnym interfejsem programowym dla tego systemu operacyjnego, dla którego napisane zostały programy przykładowe. Programy przykładowe nie zostały gruntownie przetestowane. IBM nie może zatem gwarantować lub sugerować niezawodności, użyteczności i funkcjonalności tych programów.

Każda kopia programu przykładowego lub jakikolwiek jego fragment, jak też jakiekolwiek prace pochodne muszą zawierać następujące uwagi dotyczące praw autorskich:

© (nazwa przedsiębiorstwa użytkownika, rok). Fragmenty tego kodu pochodzą z programów przykładowych IBM Corp. © Copyright IBM Corp. (wpisać rok lub lata). Wszelkie prawa zastrzeżone.

W przypadku przeglądania niniejszych informacji w formie elektronicznej, zdjęcia i kolorowe ilustracje mogą nie być wyświetlane.

Informacje dotyczące interfejsu programistycznego

Niniejsza publikacja System nazw domen (DNS) opisuje planowane interfejsy programistyczne, pozwalające na pisanie programów umożliwiających korzystanie z usług systemu IBM i5/OS.

Znaki towarowe

Następujące nazwy są znakami towarowymi International Business Machines Corporation w Stanach Zjednoczonych i/lub w innych krajach:

AS/400
i5/OS
IBM
IBM (logo)
OS/400
Redbooks
System i

Adobe, logo Adobe, PostScript oraz logo PostScript są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Adobe Systems Incorporated w Stanach Zjednoczonych i/lub w innych krajach.

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

Warunki

Zezwolenie na korzystanie z tych publikacji jest przyznawane na poniższych warunkach.

Użytek osobisty: Użytkownik ma prawo kopiować te publikacje do własnego, niekomercyjnego użytku pod warunkiem zachowania wszelkich uwag dotyczących praw własności. Użytkownik nie ma prawa dystrybuować ani wyświetlać tych publikacji czy ich części, ani też wykonywać na ich podstawie prac pochodnych bez wyraźnej zgody IBM.

Użytek służbowy: Użytkownik ma prawo kopiować te publikacje, dystrybuować je i wyświetlać wyłącznie w ramach przedsiębiorstwa Użytkownika pod warunkiem zachowania wszelkich uwag dotyczących praw własności. Użytkownik nie ma prawa wykonywać na podstawie tych publikacji ani ich fragmentów prac pochodnych, kopiować ich, dystrybuować ani wyświetlać poza przedsiębiorstwem Użytkownika bez wyraźnej zgody IBM.

Z wyjątkiem zezwoleń wyraźnie udzielonych w niniejszym dokumencie, nie udziela się jakichkolwiek innych zezwoleń, licencji ani praw, wyraźnych czy domniemanych, odnoszących się do tych publikacji czy jakichkolwiek informacji, danych, oprogramowania lub innej własności intelektualnej, o których mowa w niniejszym dokumencie.

IBM zastrzega sobie prawo do anulowania zezwolenia przyznanego w niniejszym dokumencie w każdej sytuacji, gdy, według uznania IBM, korzystanie z tych publikacji jest szkodliwe dla IBM lub jeśli IBM uzna, że warunki niniejszego dokumentu nie są przestrzegane.

Użytkownik ma prawo pobierać, eksportować lub reeksportować niniejsze informacje pod warunkiem zachowania bezwzględnej i pełnej zgodności z obowiązującym prawem i przepisami, w tym ze wszelkimi prawami i przepisami eksportowymi Stanów Zjednoczonych.

IBM NIE UDZIELA JAKICHKOLWIEK GWARANCJI, W TYM TAKŻE RĘKOJMI, DOTYCZĄCYCH TREŚCI TYCH PUBLIKACJI. PUBLIKACJE TE SĄ DOSTARCZANE W STANIE, W JAKIM SIĘ ZNAJDUJĄ (″AS IS″) BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI, W TYM TAKŻE RĘKOJMI, WYRAŹNYCH CZY DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CELU ORAZ NIENARUSZANIA PRAW STRON TRZECICH.

Drukowane w USA