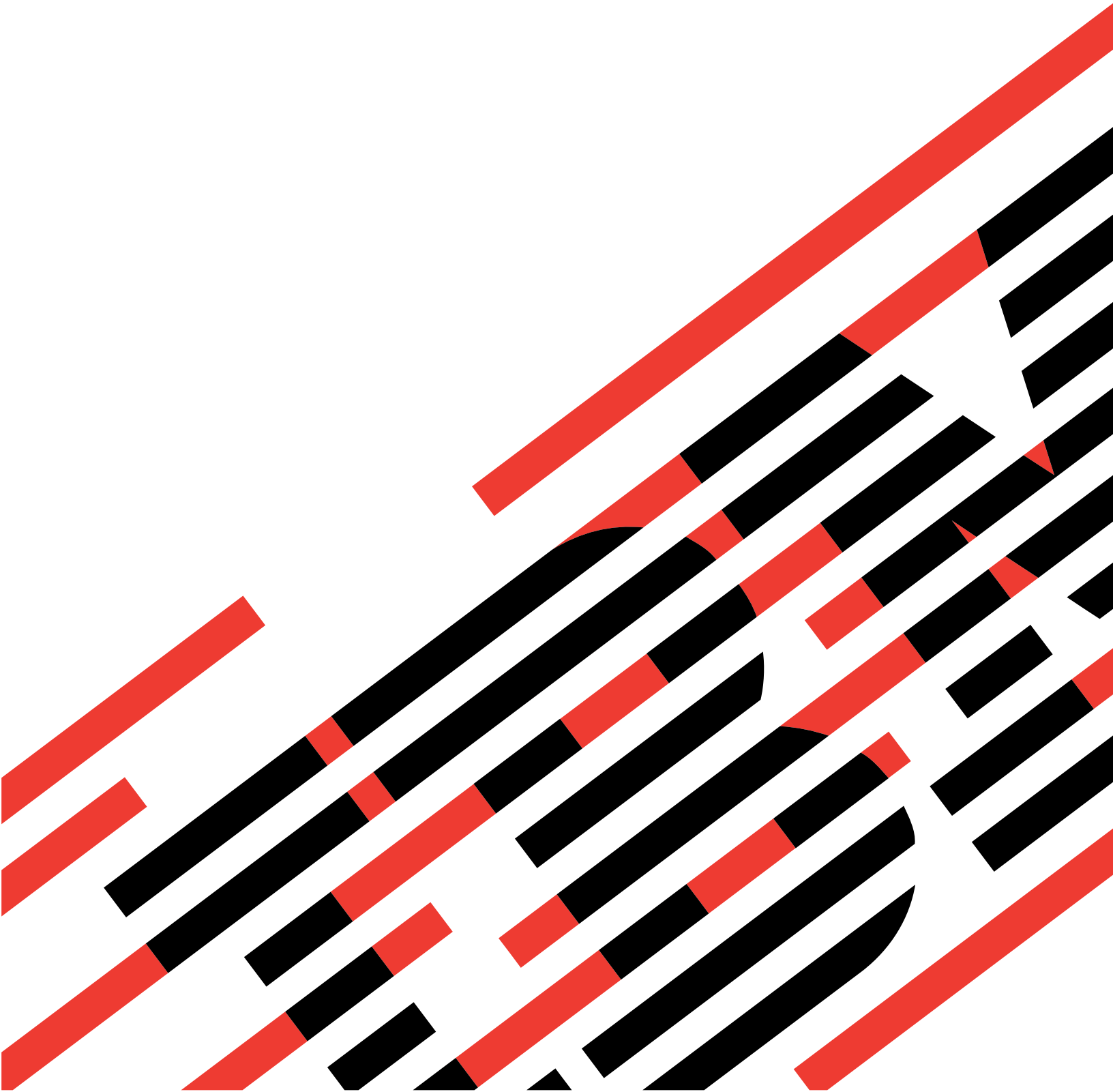
IBM

eserver

iSeries

DNS

Verzia 5 Vydanie 3



IBM

@server

iSeries

DNS

Verzia 5 Vydanie 3

Poznámka

Skôr ako použijete tieto informácie a produkt, ktorý podporujú, určite si prečítajte informácie v časti “Poznámky”, na strane 35.

Piate vydanie (August 2005)

Toto vydanie sa týka verzie 5, vydania 3, modifikácie 0 IBM Operating System/400 (číslo produktu 5722-SS1) a všetkých ďalších vydaní a modifikácií, pokiaľ nové vydania neurčujú inak. Táto verzia sa nespúšťa na modeloch RISC (reduced instruction set computer) ani na modeloch CISC.

Obsah

DNS

DNS (Domain Name System) je distribuovaný databázový systém určený na riadenie hostiteľských názvov a k nim priradených adries internetového protokolu (IP). Použitie DNS znamená, že užívatelia môžu na lokalizáciu hostiteľa používať jednoduché názvy ako napríklad ″www.jkltoys.com″ a nemusia používať IP adresu (xxx.xxx.xxx.xxx). Jeden server môže zodpovedať len za poznanie hostiteľských názvov a IP adries pre malú podskupinu zóny, ale servery DNS môžu fungovať spolu a mapovať všetky názvy domény do ich IP adries. Spolupracujúce servery DNS umožňujú počítačom komunikovať cez internet.

Pre verziu 5 vydanie 1 (V5R1) sú služby DNS založené na zavedení priemyselného štandardu DNS známeho ako BIND (Berkeley Internet Name Domain) verzie 8. Predchádzajúce služby DNS OS/400(R) boli založené na BIND verzie 4.9.3. Ak chcete používať nový server DNS založený na BIND 8, na vašom serveri iSeries(TM) musí byť nainštalovaný OS/400, voľba 33 PASE (Portable Application Solutions Environment). Ak nemáte nainštalovaný PASE, môžete ešte stále spúšťať ten istý server DNS založený na BIND 4.9.3, dostupný v predchádzajúcich vydaniach. Avšak migrácia na BIND 8 poskytuje pre váš server DNS zlepšenú funkciu a väčšiu bezpečnosť.

Poznámka: Táto téma sa zaoberá novými vlastnosťami založenými na BIND 8. Ak nepoužívate PASE na spustenie DNS založeného na BIND 8, informácie týkajúce sa DNS založeného na BIND 4.9.3 nájdete v téme informačného centra DNS V4R5

(približne 357 KB).

- Tlač tejto témy vám umožní stiahnuť alebo vytlačiť tému DNS.

Pochopenie DNS
Tieto témy vám majú pomôcť pochopiť základy DNS pre iSeries.

Príklady DNS poskytujú diagramy a vysvetlenia spôsobu práce DNS.

Koncepty DNS vysvetľujú procesy a objekty, ktoré DNS používa.

Plánovanie DNS vám pomôže vytvoriť plán vašej konfiguráciu DNS.

Použitie DNS
Tieto témy vám majú pomôcť pri konfigurovaní a riadení DNS na vašom iSeries. Zároveň vysvetľujú, ako využívať nové momentálne dostupné vlastnosti.

Systémové požiadavky na DNS
Táto téma opisuje softvérové požiadavky na spustenie DNS na vašom serveri iSeries.

Konfigurácia DNS
Táto téma vysvetľuje, ako používať iSeries Navigator na konfiguráciu názvových serverov a na rozlišovanie dotazov mimo vašej domény.

Riadenie DNS
Táto téma sa zaoberá spôsobom overovania funkcie DNS, monitorovania výkonu a údržby súborov a údajov DNS.

Odstraňovanie problémov DNS
Táto téma vysvetľuje nastavenia protokolovania a ladenia DNS, ktoré vám môže pomôcť pri rozlišovaní problémov s vašim serverom DNS.

Ak máte otázky, ktoré nie sú zodpovedané v informačnom centre, časť Ďalšie informácie o DNS poskytuje zoznam iných zdrojov a referenčných materiálov.

Tlač tejto témy

Ak si chcete prezerať alebo stiahnuť tento dokument vo formáte PDF, vyberte DNS (približne 357 KB).

Ak si chcete dokument PDF uložiť na svojej pracovnej stanici za účelom prezerania alebo vytlačenia, postupujte takto:

1. Otvorte dokument PDF v prehliadači (kliknite na vyššie uvedený odkaz).
2. V ponuke prehliadača kliknite na **File**.
3. Kliknite na **Save As...**
4. Prejdite do adresára, do ktorého chcete PDF uložiť.
5. Kliknite na **Save**.

Ak chcete, aby Adobe Acrobat Reader prezeral alebo vytlačil tieto PDF, môžete si stiahnuť kópiu z webovej stránky spoločnosti Adobe (www.adobe.com/products/acrobat/readstep.html)

.

Príklady DNS

DNS je distribuovaný databázový systém určený na riadenie hostiteľských názvov a ich príslušných IP adries. Nasledujúce príklady pomáhajú vysvetliť ako DNS funguje a ako ho možno použiť vo vašej sieti. Tieto príklady opisujú nastavenie a dôvody jeho použitia a odkazujú na súvisiace koncepty, ktoré môžu byť užitočné pri pochopení obrázkov.

Príklad: Jeden server DNS pre intranet
Zobrazuje jednoduchú podsieť so serverom DNS na interné použitie.

Príklad: Jeden server DNS s prístupom na internet
Zobrazuje jednoduchú podsieť so serverom DNS pripojeným priamo na internet.

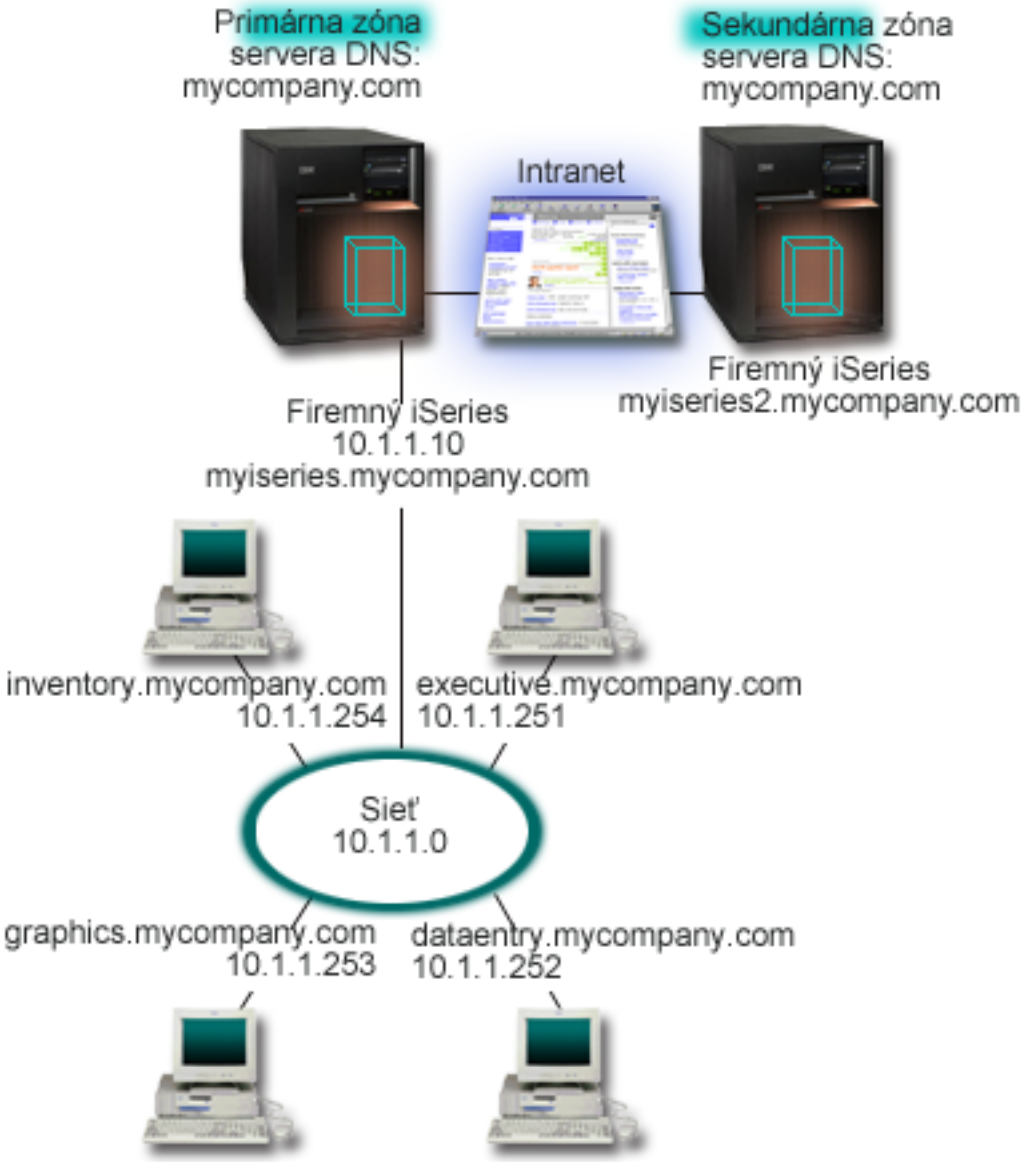
Príklad: DNS a DHCP na tom istom serveri iSeries(TM)
Zobrazuje DNS a DHCP na rovnakom serveri. Konfiguráciu možno použiť na dynamickú aktualizáciu zónových údajov DNS, keď DHCP prirađuje IP adresy hostiteľom. Ak sa váš server DHCP bude nachádzať na inom iSeries, ďalšie konfiguračné požiadavky DHCP nájdete v časti Príklad: DNS a DHCP na iných serveroch iSeries.

Príklad: Rozdelenie DNS cez firewall
Zobrazuje prevádzku DNS cez firewall s cieľom chrániť interné údaje z internetu a zároveň umožniť interným užívateľom prístup k údajom na internete.

Príklad: Jeden server DNS pre intranet

Nasledujúca ilustrácia znázorňuje DNS spustený na iSeries(TM) pre internú sieť. Táto jedna inštancia servera DNS je nastavená na počúvanie dotazov na všetkých IP adresách rozhrania. Server je primárnym názvovým serverom pre zónu ″mycompany.com″.

Obrázok 1. Jeden server DNS pre intranet.



Každý hostiteľ v zóne má IP adresu a názov domény. Správca musí manuálne definovať hostiteľov v údajoch zóny DNS vytvorením záznamov prostriedkov. Záznamy mapovania adries (A) mapujú názov počítača do jeho priradených IP adries. Ostatným hostiteľom v sieti to umožňuje dotazovať server DNS s cieľom nájsť IP adresu priradenú danému názvu hostiteľa. Záznamy ukazovateľa reverzného vyhľadávania (PTR) mapujú IP adresy počítača do názvu k nemu priradeného. Ostatným užívateľom v sieti to umožňuje dotazovať server DNS s cieľom nájsť názov hostiteľa zodpovedajúci IP adrese.

DNS podporuje okrem záznamov A a PTR aj mnohé iné zdrojové záznamy, ktoré sa môžu vyžadovať v závislosti od toho, ktoré ďalšie aplikácie založené na TCP/IP na vašom intranete spúšťate. Ak napríklad spúšťate interné systémy elektronickej pošty, možno budete musieť pridať záznamy poštovej výmeny (MX), aby SMTP mohol dotazovať DNS s cieľom zistiť, ktoré systémy spúšťajú poštové servery.

Ak bola táto malá sieť súčasťou väčšieho intranetu, možno budete musieť definovať interné koreňové servery.

Sekundárne servery
Sekundárne servery zavádzajú zónové údaje z autoritatívneho servera. Sekundárne servery získavajú zónové údaje vykonávaním prenosov zón z autoritatívneho servera. Sekundárny názvový server pri svojom spúšťaní žiada o všetky údaje pre uvedenú doménu z primárneho názvového servera. Sekundárny názvový server žiada o aktualizované údaje z primárneho servera buď preto, že prijíma hlásenie z primárneho názvového servera (ak sa používa funkcia NOTIFY) alebo preto, že dotazuje primárny názvový server a zistí, že sa dané údaje zmenili.
Na vyššie uvedenom obrázku je server myiseries súčasťou intranetu. Ďalší server iSeries myiseries2 bol nakonfigurovaný ako sekundárny server DNS pre zónu mycompany.com. Tento sekundárny server možno použiť na vyrovnanie požiadaviek na servery a môže tiež poskytovať zálohu pre prípad výpadku primárneho servera. Je dobré mať pre každú zónu aspoň jeden sekundárny server.

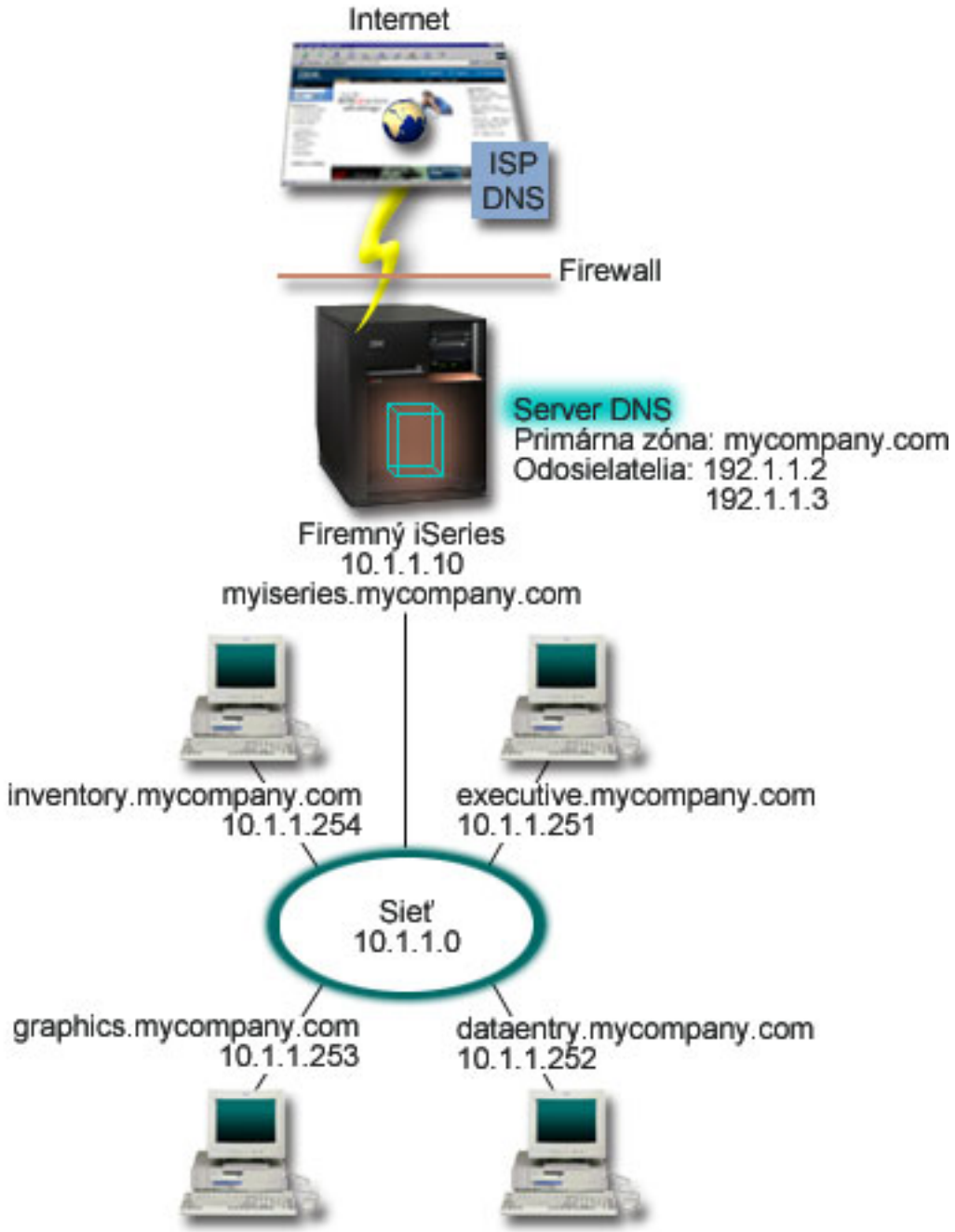
Podrobnejšie informácie o objektoch opisovaných v tomto príklade nájdete v nasledujúcich témach:

- Téma Pochopenie DNS vysvetľuje, čo je DNS a ako funguje. Táto téma tiež definuje rôzne typy zón, ktoré môžu byť definované na serveri DNS.
- Téma Zdrojové záznamy DNS vysvetľuje spôsob, akým DNS používa zdrojové záznamy.

Príklad: Jeden server DNS s prístupom na internet

Nasledujúci obrázok znázorňuje tú istú vzorovú sieť ako v príklade Jeden server DNS pre intranet, ale v tomto príklade spoločnosť pridala pripojenie na internet. V uvedenom príklade je spoločnosť schopná prístupu na internet, ale firewall je nakonfigurovaný na blokovanie internetovej prevádzky smerom do siete.

Obrázok 1. Jeden server DNS s prístupom na internet



Ak chcete rozlíšiť internetové adresy, musíte vykonať aspoň jeden z nasledujúcich krokov:

Definovať internetové koreňové servery
Môžete automaticky zaviesť predvolené internetové koreňové servery, ale možno budete musieť aktualizovať zoznam. Tieto servery vám pomôžu rozlíšiť adresy mimo vašej vlastnej zóny. Pokyny na získavanie aktuálnych internetových koreňových serverov nájdete v téme Prístup k externým údajom DNS.

Povoliť zasielanie
Môžete nastaviť zasielanie s cieľom odovzdávať dotazy pre zóny mimo mycompany.com externým serverom DNS, ako napríklad serverom DNS, ktoré prevádzkuje váš poskytovateľ internetových

služieb (ISP). Ak chcete povoliť vyhľadávanie zasielajúcimi aj koreňovými servermi, budete musieť nastaviť voľbu **forward** na **first**. Server sa najprv pokúsi o zaslanie a potom bude dotazovať koreňové servery len v prípade, ak zasielanie nerozlíši daný dotaz.

Možno sa budú vyžadovať aj nasledujúce konfiguračné zmeny:

Priradiť neobmedzené IP adresy
Vo vyššie uvedenom príklade sú zobrazené adresy 10.x.x.x. Ide však o obmedzené adresy, ktoré nemožno použiť mimo intranetu. Tieto sa uvádzajú len ako príklad, ale vaše vlastné IP adresy určí váš ISP a ostatné sieťové faktory.

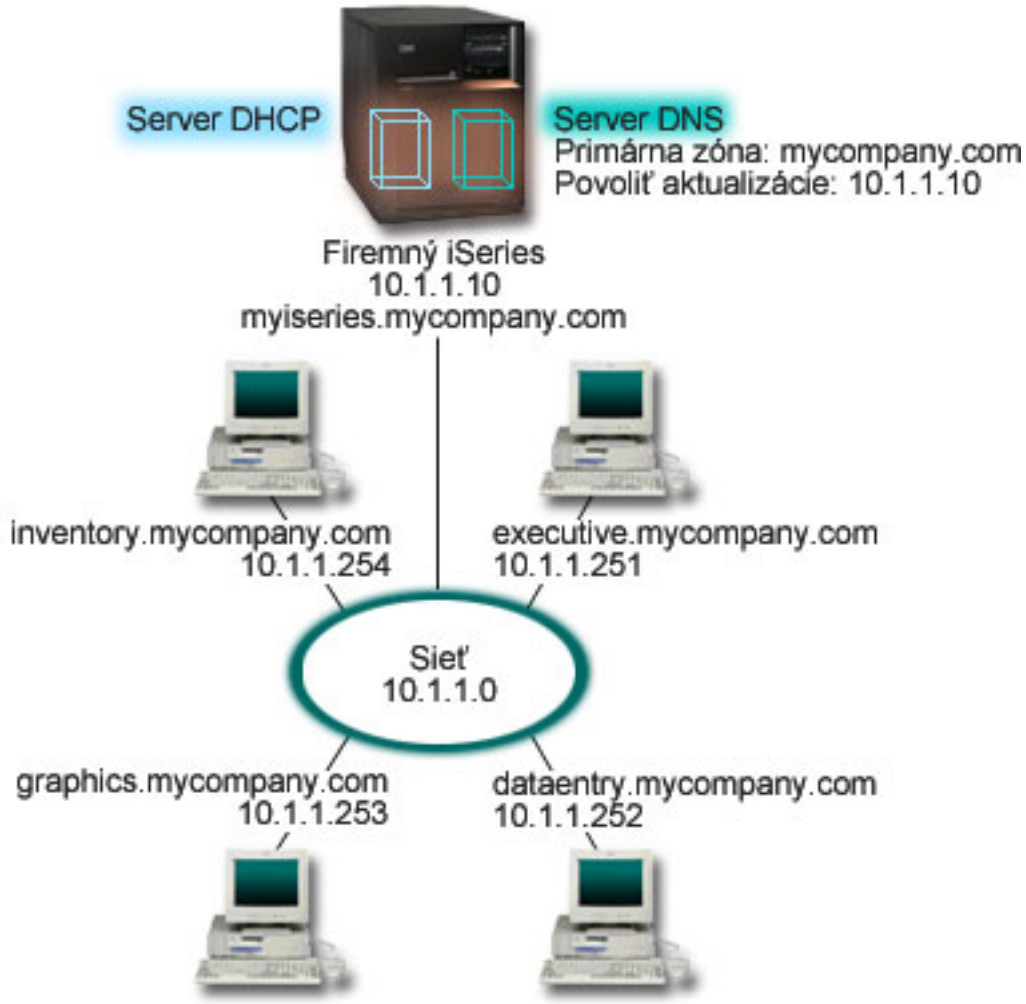
Zaregistrovať názov vašej domény
Ak budete viditeľní na internete a ešte ste sa nezaregistrovali, budete musieť zaregistrovať názov domény.

Vytvoriť firewall
Neodporúča sa, aby ste DNS povolili priamo sa pripájať na internet. Mali by ste nakonfigurovať firewall alebo prijať iné opatrenia na zabezpečenie vášho iSeries(TM). Podrobnejšie informácie nájdete v IBM(R) Secureway: iSeries and the Internet v Informačnom centre.

Príklad: DNS a DHCP na tom istom serveri iSeries(TM)

Nasledujúci obrázok znázorňuje malú podsieť s jedným serverom iSeries fungujúcim ako server DNS a DHCP pre štyroch klientov. Predpokladajme, že v tomto pracovnom prostredí inventár, položka údajov a výkonní klienti vytvárajú dokumenty s grafikou z grafického súborového servera. Títo sa pripájajú ku grafickému súborovému serveru pomocou sieťovej jednotky k svojmu hostiteľskému názvu.

Obrázok 1. DNS a DHCP na tom istom serveri iSeries.



Predchádzajúce verzie DHCP a DNS boli od seba navzájom nezávislé. Ak DHCP priradil klientovi novú IP adresu, správca musel manuálne aktualizovať záznamy DNS. Ak sa v tomto príklade zmenila IP adresa grafického súborového servera, pretože je priradená pomocou DHCP, príslušní závislí klienti nebudú môcť mapovať sieťovú jednotku do príslušného hostiteľského názvu, pretože záznamy DNS budú obsahovať predchádzajúcu IP adresu súborového servera.

So serverom DNS V5R1 založeným na BIND 8 môžete nakonfigurovať vašu zónu DNS na prijímanie dynamických aktualizácií záznamov DNS v spojení s občasnými zmenami adries prostredníctvom DHCP. Keď napríklad grafický súborový server obnovuje svoj prenájom a server DHCP mu priradí IP adresu 10.1.1.250, príslušné záznamy DNS budú dynamicky aktualizované. Ostatným klientom to umožní bez prerušenia dotazovať server DNS pre grafický súborový server svojim hostiteľským názvom.

Pri konfigurácii zóny DNS na prijímanie dynamických aktualizácií musíte vykonať nasledujúce úlohy:

Identifikovať dynamickú zónu
Kým je server v chode, nemôžete manuálne aktualizovať dynamickú zónu. Ak sa o to pokúsite, nastane interferencia s prichádzajúcimi dynamickými aktualizáciami. Manuálne aktualizácie možno vykonať po zastavení servera, ale stratíte zas všetky dynamické aktualizácie zasielané počas zastavenia servera. Z tohto dôvodu budete chcieť nakonfigurovať samostatnú dynamickú zónu s cieľom minimalizovať potrebu manuálnych aktualizácií. Podrobnejšie informácie o konfigurácii zón na použitie funkcie dynamickej aktualizácie nájdete v téme Stanovenie štruktúry domény.

Nakonfigurovať voľby povolenia aktualizácie
Každá zóna s voľbou povolenia aktualizácie sa bude považovať za dynamickú zónu. Voľba povolenia aktualizácie sa nastavuje pre každú zónu zvlášť. Aby mohla zóna prijímať dynamické aktualizácie, voľba povolenia aktualizácie musí byť pre danú zónu povolená. V tomto príklade bude mať zóna mycompany.com údaje povoľujúce aktualizáciu, ale ostatné zóny definované na serveri by mohli byť nakonfigurované ako statické alebo dynamické.

Nakonfigurovať DHCP na odosielanie dynamických aktualizácií
Vášmu serveru DHCP musíte dať oprávnenie na aktualizáciu záznamov DNS pre IP adresy, ktoré distribuoval. Podrobnejšie informácie o konfigurácii servera DHCP na odosielanie dynamických aktualizácií nájdete v téme Konfigurácia DHCP na odosielanie dynamických aktualizácií.

Nakonfigurovať preferencie aktualizácií sekundárneho servera
Ak chcete mať sekundárne servery aktuálne, môžete nakonfigurovať DNS na použitie funkcie NOTIFY na odosielanie správy o zmenách údajov zóny sekundárnym serverom pre zónu mycompany.com. Mali by ste tiež nakonfigurovať prírastkové prenosy zón (IXFR), ktoré umožnia sekundárnym serverom povoľujúcim IXFR sledovať a zavádzať len aktualizované zónové údaje a nie celú zónu.

Ak spustíte DNS a DHCP na iných serveroch, pre daný server DHCP sa vyžaduje ešte ďalšia konfigurácia. Podrobnejšie informácie nájdete v téme Príklad: DNS a DHCP na rôznych serveroch iSeries.

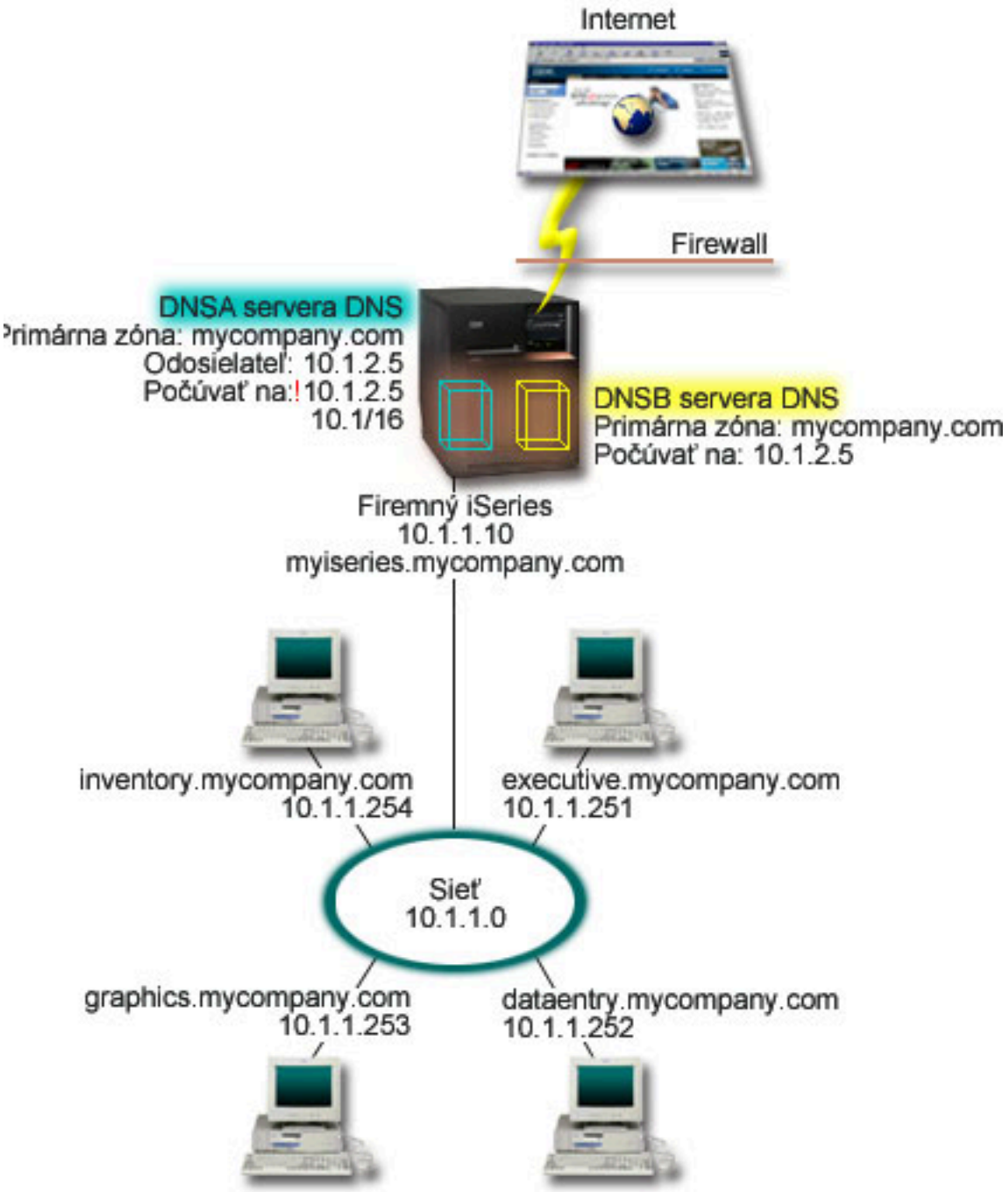
Príklad: Rozdelenie DNS cez firewal

Nasledujúci obrázok znázorňuje jednoduchú podsieť, ktorá používa pre bezpečnosť firewall. DNS V5R1 založený na BIND 8 vám umožní nastaviť viaceré servery DNS na jednom iSeries(TM). Predpokladajme, že spoločnosť má internú sieť s rezervovaným priestorom IP a externú časť siete prístupnú pre verejnosť.

Spoločnosť chce, aby jej interní klienti mohli rozlišovať mená externých hostiteľov a vymieňať si poštu s osobami zvonka. Spoločnosť ďalej chce, aby interné rozlišovače mali prístup k určitým výlučne interným zónam, ktoré nie sú prístupné všetkým osobám mimo internej siete, avšak nechce, aby rozlišovače zvonka mohli vstupovať do internej siete.

Aby to mohla spoločnosť zrealizovať, nastaví dve inštancie servera DNS na tom istom iSeries, jednu pre intranet a jednu slúžiacu na všetko vo svojej verejnej doméne. Uvedenému kroku hovoríme rozdelenie DNS.

Obrázok 1 Rozdelenie DNS cez firewall.



Externý server DNSB je nakonfigurovaný s primárnou zónou mycompany.com. Tieto zónové údaje zahŕňajú len zdrojové záznamy, ktoré majú byť súčasťou verejnej domény. Interný server DNSA je nakonfigurovaný s primárnou zónou mycompany.com, ale zónové údaje definované na DNSA obsahujú intranetové zdrojové záznamy. Voľba zasielania je definovaná ako 10.1.2.5. To prinúti DNSA zasielať nerozlíšiteľné dotazy ďalej serveru DNSB.

Ak máte obavy týkajúce sa integrity vášho firewallu alebo bezpečnosti, na pomoc pri ochrane interných údajov existuje možnosť použiť voľbu počúvania na určitej adrese. Ak ju chcete využiť, môžete nakonfigurovať interný server tak, aby povoľoval dotazy do internej zóny mycompany.com len od interných

hostiteľov. Aby to všetko riadne fungovalo, budú musieť byť interní klienti nakonfigurovaní len na dotazovanie servera DNSA. Ak chcete nastaviť rozdelenie DNS, budete musieť zvážiť nasledujúce nastavenia konfigurácie:

Počúvanie na určitej adrese
V predchádzajúcich príkladoch sa nachádzal na iSeries len jeden server DNS. Tento bol nastavený na počúvanie na všetkých IP adresách rozhrania. Vždy keď máte na iSeries viacero serverov DNS, musíte definovať IP adresu rozhrania, na ktorej každý z nich počúva, keďže dva servery DNS nemôžu počúvať na tej istej adrese. V takom prípade predpokladajme, že všetky dotazy prichádzajúce z firewallu budú zaslané na 10.1.2.5. Tieto dotazy by mali byť zaslané na externý server. Preto je DNSB nakonfigurovaný na počúvanie na adrese 10.1.2.5. Interný server DNSA je nakonfigurovaný na prijímanie dotazov z akýchkoľvek IP adries rozhrania 10.1.x.x *s výnimkou* 10.1.2.5. Ak chcete túto adresu účinne vylúčiť, zoznam zhôd adries (AML) musí mať túto vylúčenú adresu uvedenú pred zahrnutou predponou adresy.

Poradie zoznamu zhôd adries (AML)
Použije sa prvý element AML, s ktorým sa uvedená adresa zhoduje. Ak chcete napríklad povoliť všetky adresy v sieti 10.1.x.x s výnimkou adresy 10.1.2.5, elementy ACL musia byť v nasledujúcom poradí (!10.1.2.5; 10.1/16). V takom prípade sa bude adresa 10.1.2.5 porovnávať s prvým elementom a bude ihneď odmietnutá.

Ak by boli elementy uvedené v opačnom poradí (10.1/16; !10.1.2.5), IP adrese 10.1.2.5 by bol prístup povolený, pretože server ju bude porovnávať s prvým elementom, ktorý sa zhoduje a povolí ju bez toho, aby skontroloval zvyšok pravidiel.

Koncepty DNS

DNS V5R1 ponúka nové vlastnosti založené na BIND 8. Nasledujúce odkazy poskytujú prehľad spôsobu fungovania DNS a nových vlastností, ktoré môžete použiť:

Základná funkcia DNS

Pochopenie DNS
Poskytuje prehľad toho, čo je DNS a ako funguje, ako aj opis typov zón, ktoré môžete definovať.

Pochopenie dotazov DNS
Vysvetľuje, ako DNS rozlišuje dotazy v mene klientov.

Nastavenie vašej domény DNS
Poskytuje prehľad registrácie domény s odkazmi na iné referenčné stránky pre nastavenie vášho vlastného doménového priestoru.

Nové vlastnosti DNS:

Dynamické aktualizácie
DNS V5R1 založený na BIND 8 podporuje dynamické aktualizácie. Tieto umožňujú vonkajším zdrojom, ako napríklad DHCP, zasielať aktualizácie serveru DNS.

Vlastnosti BIND 8
Okrem dynamických aktualizácií ponúka BIND 8 na rozšírenie výkonu vášho servera DNS niekoľko nových vlastností.

Odkaz na zdrojový záznam:

Zdrojový záznam DNS
Zdrojové záznamy sa používajú na ukladanie údajov o názvoch domén a IP adries. Táto téma obsahuje vyhľadávateľný zoznam zdrojových záznamov podporovaných pre V5R1.

Zdrojové záznamy pošty a MX
DNS podporuje rozšírené poštové smerovanie prostredníctvom použitia týchto záznamov.

Existuje mnoho vonkajších zdrojov podrobnejšie vysvetľujúcich DNS. Ďalšie referenčné zdroje nájdete v časti Ďalšie informácie o DNS.

Pochopenie DNS

DNS (Domain Name System) je distribuovaný databázový systém určený na riadenie hostiteľských názvov a k nim priradených adries internetového protokolu (IP). Použitie DNS znamená, že užívatelia môžu na lokalizáciu hostiteľa používať jednoduché názvy ako napríklad ″www.jkltoys.com″ a nemusia používať IP adresu (xxx.xxx.xxx.xxx). Jeden server môže zodpovedať len za poznanie hostiteľských názvov a IP adries pre malú podskupinu zóny, ale servery DNS môžu fungovať spolu a mapovať všetky názvy domény do ich IP adries. Spolupracujúce servery DNS umožňujú počítačom komunikovať cez internet.

Údaje DNS sú rozdelené do hierarchie domén. Servery zodpovedajú len za poznanie malej časti údajov, ako je napríklad jedna poddoména. Časť domény, za ktorú je server priamo zodpovedný sa nazýva zóna. Server DNS, ktorý má úplné hostiteľské informácie a údaje pre zónu sa považuje za autoritatívny pre danú zónu. Autoritatívny server môže odpovedať na dotazy o hostiteľoch vo svojej zóne pomocou vlastných zdrojových záznamov. Spracovanie dotazu závisí od množstva faktorov. Pochopenie dotazov DNS vysvetľuje cestu, ktorú môže klient použiť na rozlíšenie dotazu.

Pochopenie zón
Údaje DNS sú rozdelené do skupín údajov, ktoré je možné riadiť, a ktoré sa volajú zóny. Zóny obsahujú informácie o názve a IP adrese jednej alebo viacerých častí domény DNS. Server obsahujúci všetky informácie pre zónu je autoritatívnym serverom pre danú doménu. Niekedy je rozumné delegovať oprávnenie odpovedať na dotazy DNS pre určitú poddoménu na ďalší server DNS. V takom prípade možno nakonfigurovať server DNS pre túto doménu tak, aby odkazoval dotazy poddomény na príslušný server.

Údaje zóny určené na zálohovanie a nadbytočné údaje zóny sa často ukladajú na serveroch s výnimkou autoritatívneho servera DNS. Tieto servery sa nazývajú sekundárne servery a zavádzajú údaje z autoritatívneho servera. Konfigurácia sekundárnych serverov vám umožní udržiavať rovnováhu požiadaviek na servery a poskytuje aj zálohu v prípade výpadku primárneho servera. Sekundárne servery získavajú zónové údaje vykonávaním prenosov zón z autoritatívneho servera. Po inicializovaní sekundárneho servera tento zavedie úplnú kópiu zónových údajov z primárneho servera. Sekundárny server zavádza zónové údaje z primárneho alebo z iných sekundárnych serverov pre danú doménu aj pri zmene zónových údajov.

Typy zón DNS
Na pomoc pri riadení údajov DNS môžete použiť DNS iSeries(TM) s cieľom definovať niekoľko typov zón:

Primárna zóna
Zavádza zónové údaje priamo zo súboru na hostiteľovi. Primárna zóna môže obsahovať podzónu alebo zónu potomka. Môže obsahovať aj zdrojové záznamy, ako napríklad záznamy o hostiteľovi, aliase (CNAME), adrese (A) alebo ukazovateli reverzného mapovania (PTR).
Poznámka: Primárne zóny sa v dokumentácii BIND niekedy nazývajú ″hlavné zóny″.

Podzóna
Podzóna definuje zónu v primárnej zóne. Podzóny umožňujú užívateľom organizovať údaje zóny do kusov, ktoré možno riadiť.

Zóna potomka
Zóna potomka definuje podzónu a deleguje zodpovednosť za údaje podzóny na jeden alebo viacero názvových serverov.

Alias (CNAME)
Alias definuje alternatívny názov pre názov primárnej domény.

Hostiteľ
Objekt hostiteľa mapuje záznamy A a PTR do hostiteľa. K hostiteľovi možno priradiť ďalšie záznamy prostriedkov..

Sekundárna zóna
Zavádza údaje zóny z primárneho alebo iného sekundárneho servera zóny. Sekundárny server udržiava kompletnú kópiu zóny, pre ktorú je tento server sekundárnym.
Poznámka: Sekundárne zóny sa v dokumentácii BIND niekedy nazývajú ″podriadenými zónami″.

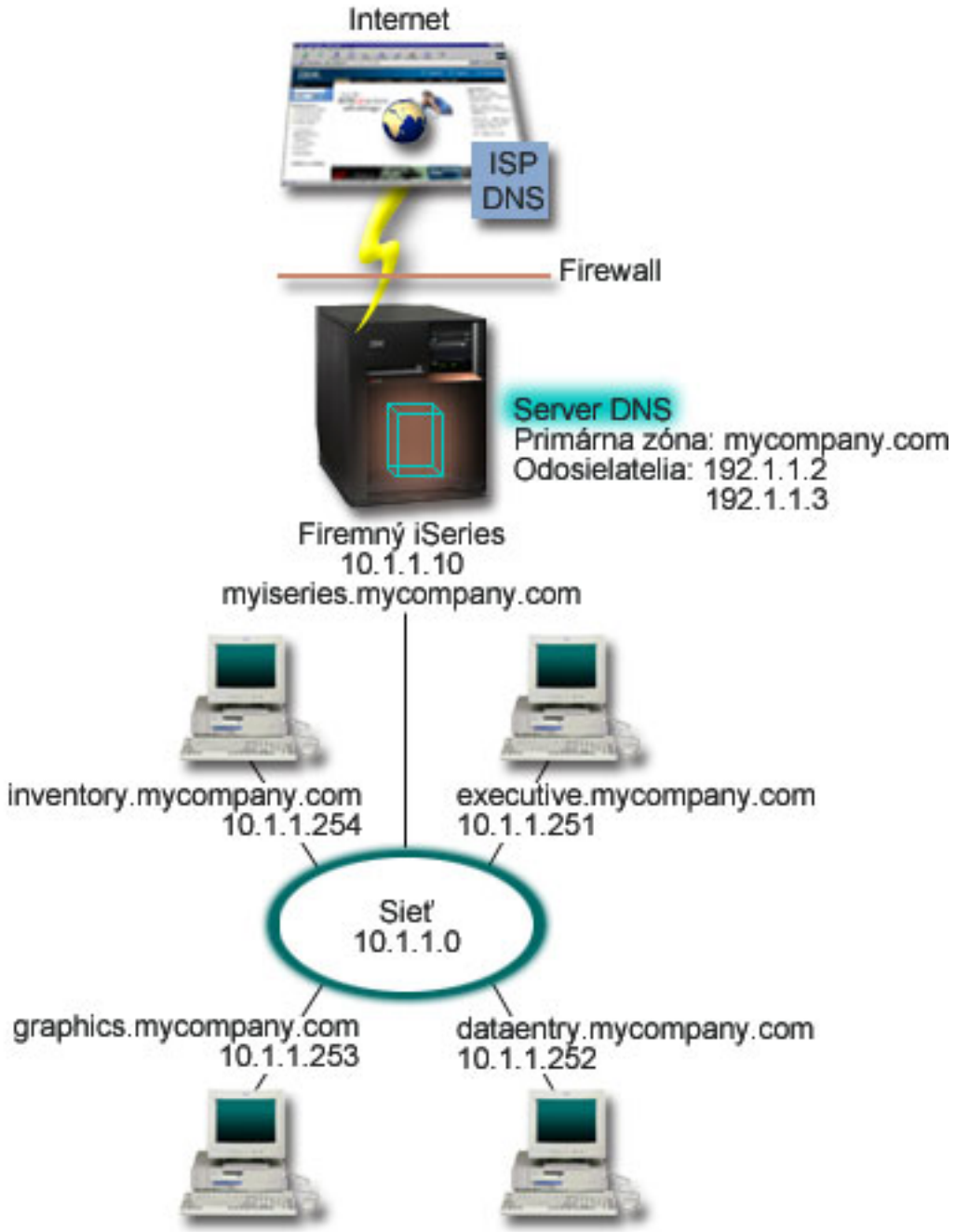
Čiastková zóna
Čiastková zóna je podobná sekundárnej zóne, ale táto prenáša pre danú zónu len záznamy o názve servera (NS).

Odosielacia zóna
Odosielacia zóna smeruje všetky dotazy pre danú zónu na iné servery.

Pochopenie dotazov DNS

Klienti používajú servery DNS s cieľom nájsť pre ne informácie. Požiadavka môže prísť priamo od klienta alebo z aplikácie spustenej na tomto klientovi. Klient zasiela dotazovaciu správu serveru DNS, ktorá obsahuje plne kvalifikovaný názov domény (FQDN), typ dotazu, ako napríklad konkrétny zdrojový záznam, ktorý tento klient požaduje a triedu pre názov domény, ktorá je zvyčajne internetovou triedou (IN). Nasledujúce číslo zobrazuje vzorovú sieť z príkladu Jeden server DNS s prístupom na internet.

Obrázok 1. Jeden server DNS s prístupom na internet



Predpokladajme, že hostiteľ *dataentry* dotazuje server DNS pre ″graphics.mycompany.com″. Server DNS použije svoje vlastné zónové údaje a odpovie s IP adresou 10.1.1.253.

Teraz predpokladajme, že *dataentry* žiada IP adresu ″www.jkl.com.″. Tento hostiteľ sa nenachádza v zónových údajoch servera DNS. Teraz existujú dve cesty, po ktorých možno ísť, rekurzia alebo opakovanie. Ak je server DNS nastavený na použitie rekurzie, môže dotazovať alebo kontaktovať iné servery DNS v mene požadujúceho klienta s cieľom úplne rozlíšiť názov a potom zaslať odpoveď späť klientovi. Ak server DNS dotazuje iný server DNS, požadujúci server uloží odpoveď do pamäte cache, aby ju mohol použiť pri nasledujúcom prijatí tohto dotazu. Klient sa môže pokúsiť vo svojom mene kontaktovať ostatné servery DNS s cieľom rozlíšiť názov. V tomto procese s názvom iterácia používa klient samostatné a dodatočné dotazy na základe referálnych odpovedí zo serverov.

Nastavenie vašej domény DNS

DNS vám umožňuje obsluhovať názvy a adresy na intranete alebo internej sieti, ako aj názvy a adresy zvyšku sveta cez internet. Ak chcete nastaviť domény na internete, budete musieť zaregistrovať názov domény.

Ak nastavujete intranet, pre interné použitie nemusíte zaregistrovať názov domény. Registrácia alebo neregistrácia názvu intranetu závisí od toho, či chcete zabezpečiť, aby už nikto iný nemohol použiť tento názov na internete nezávisle od vášho interného použitia. Registrácia názvu, ktorý chcete použiť interne zabezpečí, aby nikdy nenastal konflikt, ak budete chcieť neskôr použiť názov domény externe.

Registráciu domény môžete vykonať priamym kontaktom s autorizovaným registrátorom názvu domény alebo prostredníctvom niektorých poskytovateľov internetových služieb (ISP). Niektorí ISP ponúkajú službu podávania žiadostí o registráciu názvu domény vo vašom mene. Informačné centrum internetovej siete (InterNIC)

udržiava adresár všetkých registrátorov názvov domén, ktorí majú oprávnenie od spoločnosti Internet Corporation for Assigned Names and Numbers (ICANN).

Existuje veľa iných zdrojov poskytujúcich informácie o registrácii a príprave na hosťovanie domény DNS. Ďalšiu pomoc získate v časti Ďalšie informácie o DNS.

Dynamické aktualizácie

Dynamic Host Configuration Protocol (DHCP) je štandard TCP/IP, ktorý používa centrálny server na riadenie IP adries a ostatných konfiguračných detailov pre celú sieť. Server DHCP odpovedá na požiadavky klientov dynamickým priraďovaním vlastností týmto klientom. DHCP vám umožní definovať konfiguračné parametre sieťového hostiteľa na centrálnom umiestnení a automatizovať konfiguráciu hostiteľov. Často sa používa aj na priradenie dočasných IP adries klientom pre siete obsahujúce viacero klientov než je dostupný počet IP adries.

V minulosti boli všetky údaje DNS uložené v statických databázach. Všetky záznamy prostriedkov musel vytvoriť a udržiavať správca. Servery DNS spúšťajúce BIND 8 môžu byť teraz nakonfigurované na prijímanie požiadaviek z ostatných zdrojov s cieľom dynamicky aktualizovať zónové údaje.

Váš server DHCP možno nakonfigurovať na zasielanie požiadaviek na aktualizáciu servera DNS pri každom priradení novej adresy hostiteľovi. Tento automatizovaný proces znižuje požiadavky na správu servera DNS v rýchlo sa zväčšujúcich alebo meniacich sieťach TCP/IP a v sieťach, v ktorých hostitelia často menia svoje umiestnenie. Keď klient používajúci DHCP dostane IP adresu, tieto údaje sa ihneď zasielajú serveru DNS. Pomocou tejto metódy môže DNS pokračovať v úspešnom rozlišovaní dotazov pre hostiteľov, aj napriek zmenám ich adries.

V mene klienta môžete nakonfigurovať DHCP na aktualizáciu záznamov mapovania adries (A), záznamov ukazovateľa reverzného vyhľadávania (PTR) alebo oboch. Záznam A mapuje hostiteľský názov počítača do jeho IP adresy. Záznam PTR mapuje IP adresu počítača do jeho hostiteľského názvu. Keď sa mení adresa klienta, DHCP môže automaticky zaslať aktualizáciu serveru DNS, aby ostatní hostitelia v sieti mohli tohto klienta lokalizovať cez dotazy DNS na jeho novej IP adrese. Pre každý dynamicky aktualizovaný záznam sa napíše sprievodný záznam textu (TXT) na identifikáciu toho, že uvedený záznam bol zapísaný pomocou DHCP.
Poznámka: Ak nastavíte DHCP len na aktualizáciu PTR, musíte nakonfigurovať DNS na povolenie aktualizácie od klientov, aby každý klient mohol aktualizovať svoj záznam A. Nie všetci klienti DHCP podporujú vytváranie svojich vlastných požiadaviek na aktualizáciu záznamu A. Skôr než si zvolíte túto metódu, pozrite si dokumentáciu pre vašu klientsku platformu.

Dynamické zóny sú zabezpečené vytvorením zoznamu autorizovaných zdrojov, ktoré majú povolené zasielať aktualizácie. Autorizované zdroje môžete definovať pomocou jednotlivých IP adries, celých podsád,

paketov podpísaných pomocou zdieľaného tajného kľúča (nazývaného podpis transakcie alebo TSIG) alebo ľubovoľnou kombináciou týchto metód. Pred aktualizáciou zdrojových záznamov DNS overuje, či prichádzajúce pakety požiadaviek pochádzajú z autorizovaného zdroja.

Dynamické aktualizácie možno vykonávať medzi DNS a DHCP na jednom serveri iSeries(TM), medzi rôznymi servermi iSeries alebo medzi iSeries a inými servermi schopnými dynamických aktualizácií. Podrobnejšie informácie o konfigurácii dynamických aktualizácií pre váš iSeries nájdete v nasledujúcich témach:

- Konfigurácia DNS na prijímanie dynamických aktualizácií
- Konfigurácia DHCP na zasielanie dynamických aktualizácií
- Na serveroch zasielajúcich dynamické aktualizácie do DNS sa vyžaduje API dynamickej aktualizácie QTOBUPT. Inštaluje sa automaticky s DNS OS/400(R) voľbou 31.

Vlastnosti BIND 8

DNS bol modifikovaný na použitie BIND 8 pre V5R1. Ak nemáte nainštalovaný PASE, môžete pokračovať s konfiguráciou a spustením predtým vydaného servera DNS OS/400(R) založeného na BIND 4.9.3. Téma Požiadavky systému DNS vysvetľuje, čo potrebujete, aby ste mohli spustiť DNS založený na BIND 8 na vašom iSeries (TM). Použitie nového DNS vám umožní využívať nasledujúce vlastnosti:

Viaceré servery DNS spustené na jednom iSeries
V minulých vydaniach bolo možné nakonfigurovať len jeden DNS. Teraz môžete nakonfigurovať viacero serverov alebo inštancií DNS. To vám umožní nastaviť logické rozdelenie medzi servermi. Keď vytvoríte viaceré inštancie, musíte explicitne definovať pre každú z nich IP adresy rozhrania, na ktorom budú počúvať. Dve inštancie DNS nemôžu počúvať na tom istom rozhraní.

Jedným z praktických využití viacerých serverov je rozdelenie DNS, kde jeden server je autoritatívny pre internú sieť a druhý sa používa na externé dotazy. Podrobnejšie informácie o rozdelení DNS nájdete v príklade Rozdelenie DNS cez firewall.

Podmienečné posielanie ďalej
Podmienečné posielanie ďalej vám umožní nakonfigurovať váš server DNS na jemné ladenie vašich preferencií odosielania. Server môžete nastaviť na odosielanie všetkých dotazov, na ktoré nepozná odpoveď. Odosielanie môžete nastaviť na globálnej úrovni, ale pridajte výnimky do domén, pre ktoré chcete vynútiť bežné opakované rozlíšenie. Alebo môžete nastaviť bežné opakované rozlíšenie na globálnej úrovni a potom vynútiť odosielanie v rámci určitých domén.

Bezpečné dynamické aktualizácie
DHCP a iné autorizované zdroje môžu zasielať dynamické aktualizácie zdrojových záznamov pomocou Transaction Signatures (TSIG) a/alebo autorizácie IP adries zdroja. Znižuje to potrebu manuálnych aktualizácií zónových údajov a zároveň sa tým zabezpečí, že na aktualizáciu sa používajú len autorizované zdroje.

Podrobnejšie informácie o dynamických aktualizáciách nájdete v časti Dynamické aktualizácie. Podrobnejšie informácie o autorizácii aktualizácií z externých zdrojov nájdete v časti Plánovanie bezpečnostných opatrení.

NOTIFY
Keď sa zapne NOTIFY, funkcia DNS NOTIFY sa aktivuje vždy, keď sa na primárnom serveri aktualizujú zónové údaje. Primárny server odosiela správu všetkým známym sekundárnym serverom, čo znamená, že sa údaje zmenili. Sekundárne servery môžu potom odpovedať s požiadavkou na prenos zóny pre aktualizované zónové údaje. Udržiavanie aktuálnosti zónových údajov pomáha zlepšiť podporu sekundárneho servera.

Zónové prenosy (IXFR a AXFR)
Vždy keď v minulosti sekundárne servery potrebovali opätovne zaviesť zónové údaje, museli zaviesť celú

sadu údajov do prenosu celej zóny (AXFR). BIND 8 podporuje novú metódu zónového prenosu: prírastkový zónový prenos (IXFR). IXFR predstavuje spôsob, akým môžu ostatné servery prenášať len zmenené údaje a nie celú zónu.

Ak je nasledujúca vlastnosť na primárnom serveri zapnutá, zmenám údajov sa priradí návestie, ktoré určuje, že nastala zmena. Keď sekundárny server požiada o aktualizáciu zóny v IXFR, primárny server zašle len nové údaje. IXFR je užitočný pri dynamickej aktualizácii zóny a znižuje prevádzkové zaťaženie tým, že posiela menšie množstvá údajov.
Poznámka: Aby mohol primárny aj sekundárny server používať túto vlastnosť, musia mať oba povolené IXFR.

Zdrojové záznamy DNS

Databáza zóny DNS sa skladá z kolekcie zdrojových záznamov. Každý zdrojový záznam uvádza informácie o určitom objekte. Napríklad záznamy Address Mapping (A) mapujú hostiteľský názov do IP adresy a záznamy ukazovateľa reverzného vyhľadávania (PTR) mapujú IP adresu do hostiteľského názvu. Server tieto záznamy používa ako odpoveď na dotazy pre hostiteľov v svojej zóne. Podrobnejšie informácie nájdete v tabuľke, kde si môžete prezerať zdrojové záznamy DNS.

Zdrojový záznam	Skratka	Opis
Záznamy Address Mapping	A	Záznam A uvádza IP adresu tohto hostiteľa. Záznamy sa používajú na rozlíšenie dotazu pre IP adresu špecifického názvu domény. Tento typ záznamu je definovaný v RFC 1035.
Záznamy Andrew File System Database	AFSDB	Záznam AFSDB uvádza adresu AFS alebo DCE objektu. Záznamy AFSDB sa používajú ako záznamy A na mapovanie názvu domény do jej adresy AFSDB; alebo na mapovanie bunky z názvu domény do autentifikovaných názvových serverov pre danú bunku. Tento typ záznamu je definovaný v RFC 1183.
Záznamy Canonical Name	CNAME	Záznam CNAME uvádza aktuálny názov domény tohto objektu. Keď DNS dotazuje aliasovaný názov a nájde záznam CNAME ukazujúci na kanonický názov, potom dotazuje daný kanonický názov domény. Tento typ záznamu je definovaný v RFC 1035.
Záznamy Host Information	HINFO	Záznam HINFO uvádza všeobecné informácie o počítači hostiteľa. Názvy operačného systému a štandardnej CPU sú definované v priradených číslach RFC 1700. Použitie štandardných čísel sa však nevyžaduje. Tento typ záznamu je definovaný v RFC 1035.
Záznamy Integrated Services Digital Network	ISDN	Záznam ISDN uvádza adresu tohto objektu. Tento záznam mapuje hostiteľský názov do adresy ISDN. Používajú sa len v sieťach ISDN. Tento typ záznamu je definovaný v RFC 1183.

Zdrojový záznam	Skratka	Opis
Záznamy IP Version 6 Address	AAAA	Záznam AAAA uvádza 128 bitovú adresu hostiteľa. Záznamy AAAA sa používajú ako záznamy A na mapovanie názvu hostiteľa do jeho IP adresy. Záznamy AAAA použite na podporu IP adries verzie 6, ktoré nevyhovujú štandardnému formátu záznamu A. Tento typ záznamu je definovaný v RFC 1886.
Záznamy Location	LOC	Záznam LOC uvádza fyzické umiestnenie sieťových komponentov. Aplikácie môžu použiť tieto záznamy na hodnotenie výkonnosti siete alebo na mapovanie fyzickej siete. Tento typ záznamu je definovaný v RFC 1876.
Záznamy Mail Exchanger	MX	Záznamy MX definujú hostiteľa výmeny pošty pre poštu zaslanú do tejto domény. Tieto záznamy používa protokol SMTP (Simple Mail Transfer Protocol) na lokalizáciu hostiteľov, ktorí budú spracovávať alebo zasielať poštu pre túto doménu spolu s hodnotami preferencií pre každého hostiteľa výmeny pošty. Každý hostiteľ výmeny pošty musí mať zodpovedajúce záznamy hostiteľskej adresy (A) v platnej zóne. Tento typ záznamu je definovaný v RFC 1035.
Záznamy Mail Group	MG	Záznamy MG uvádzajú názov domény poštovej skupiny. Tento typ záznamu je definovaný v RFC 1035.
Záznamy Mailbox	MB	Záznamy MB uvádzajú názov hostiteľskej domény obsahujúcu poštovú schránku pre tento objekt. Pošta zaslaná doméne bude smerovaná do hostiteľa uvedeného v zázname MB. Tento typ záznamu je definovaný v RFC 1035.
Záznamy Mailbox Information	MINFO	Záznamy MINFO uvádzajú poštovú schránku, ktorá má prijímať správy alebo chyby pre tento objekt. Záznam MINFO sa používa skôr na zasielanie zoznamov než pre jednu poštovú schránku. Tento typ záznamu je definovaný v RFC 1035.
Záznamy Mailbox Rename	MR	Záznamy MR uvádzajú nový názov domény pre poštovú schránku. Záznam MR použite na odoslanie položky užívateľovi, ktorý má teraz inú poštovú schránku. Tento typ záznamu je definovaný v RFC 1035.
Záznamy Name Server	NS	Záznam NS uvádza autoritatívny názvový server pre tohto hostiteľa. Tento typ záznamu je definovaný v RFC 1035.

Zdrojový záznam	Skratka	Opis
Záznamy Network Service Access Protocol	NSAP	Záznam NSAP uvádza adresu prostriedku NSAP. Záznamy NSAP sa používajú na mapovanie názvov domény do adries NSAP. Tento typ záznamu je definovaný v RFC 1706.
Záznamy Public Key	KEY	Záznam KEY uvádza verejný kľúč priradený k názvu DNS. Kľúč môže byť pre zónu, užívateľa alebo hostiteľa. Tento typ záznamu je definovaný v RFC 1065.
Záznamy Responsible Person	RP	Záznam RP uvádza internetovú poštovú adresu a opis osoby zodpovednej za túto zónu alebo hostiteľa. Tento typ záznamu je definovaný v RFC 1183.
Záznamy Reverse-lookup Pointer	PTR	Záznam PTR uvádza názov domény hostiteľa, pre ktorého chcete definovaný záznam PTR. Záznamy PTR umožňujú vyhľadanie názvu hostiteľa s danou IP adresou. Tento typ záznamu je definovaný v RFC 1035.
Záznamy Route Through	RT	Záznam RT uvádza názov hostiteľskej domény, ktorá môže konať ako zasielateľ IP paketov pre tohto hostiteľa. Tento typ záznamu je definovaný v RFC 1183.
Záznamy Start of Authority	SOA	Záznam SOA uvádza, že tento server je pre danú zónu autoritatívny. Autoritatívny server je najlepším zdrojom pre údaje v rámci zóny. Záznam SOA obsahuje všeobecné informácie o zóne a predzavedených pravidlách pre sekundárne servery. Na jednu zónu môže existovať len jeden záznam SOA. Tento typ záznamu je definovaný v RFC 1035.
Záznamy Text	TXT	Záznam TXT uvádza viaceré textové reťazce, každý s dĺžkou až 255 znakov, ktoré majú byť priradené k názvu domény. Záznamy TXT možno používať spolu so záznamami Responsible Person (RP) na poskytovanie informácií o tom, kto zodpovedá za zónu. Tento typ záznamu je definovaný v RFC 1035. Záznamy TXT používa DHCP iSeries na dynamické aktualizácie. Server DHCP napíše priradený záznam TXT pre každú aktualizáciu záznamu A a PTR vykonanú serverom DHCP. Záznamy DHCP budú mať predponu **AS400DHCP:**.

Zdrojový záznam	Skratka	Opis
Záznamy Well-Known Services	WKS	Záznam WKS uvádza dobre známe služby podporované objektom. Záznamy WKS najčastejšie uvádzajú, či sa pre túto adresu podporujú protokoly tcp alebo udp alebo oba. Tento typ záznamu je definovaný v RFC 1035.
Záznamy X.400 Address Mapping	PX	Záznamy PX sú ukazovateľom na informácie o mapovaní X.400/RFC 822. Tento typ záznamu je definovaný v RFC 1664.
Záznamy X25 Address Mapping	X25	Záznam X25 uvádza adresu prostriedku X25. Tento záznam mapuje hostiteľský názov do adresy PSDN. Používajú sa len v sieťach X25. Tento typ záznamu je definovaný v RFC 1183.

Poštové záznamy a záznamy MX

Poštu a záznamy MX používajú programy smerovania pošty, ako napríklad SMTP (Simple Mail Transfer Protocol). Podrobnejšie informácie o typoch poštových záznamov podporovaných DNS iSeries(TM) nájdete vo vyhľadávacej tabuľke v DNS záznamov prostriedkov.

DNS obsahuje informácie na zasielanie elektronickej pošty pomocou informácií výmeny pošty. Ak sieť používa DNS, aplikácia SMTP (Simple Mail Transfer Protocol) nedoručí poštu adresovanú hostiteľovi TEST.IBM.COM jednoducho otvorením pripojenia TCP k TEST.IBM.COM. SMTP najprv dotazuje server DNS s cieľom zistiť, ktoré hostiteľské servery možno použiť na doručenie správy.

Doručenie pošty na určitú adresu
Servery DNS používajú zdrojové záznamy známe ako záznamy výmeny pošty (MX). Záznamy MX mapujú doménu alebo názov hostiteľa do preferenčnej hodnoty a názvu hostiteľa. Záznamy MX sa zvyčajne používajú na určenie toho, že jeden hostiteľ sa používa na spracovanie pošty pre iného hostiteľa. Tieto záznamy sa používajú aj na stanovenie ďalšieho hostiteľa, ktorému sa má doručiť pošta, ak prvého hostiteľa nie je možné dosiahnuť. Inými slovami umožňujú, aby bola pošta adresovaná jednému hostiteľovi doručená inému hostiteľovi.

Pre tú istú doménu alebo názov hostiteľa môže existovať viacero zdrojových záznamov MX. Ak existujú viaceré záznamy MX pre rovnakú doménu alebo hostiteľa, hodnota preferencie (alebo priority) každého záznamu stanoví poradie, v ktorom sa tento pokus o doručenie vykoná. Najnižšia hodnota preferencie zodpovedá najpreferovanejšiemu záznamu, ktorý sa skúsi ako prvý. Ak najpreferovanejšieho hostiteľa nemožno dosiahnuť, zasielajúca poštová aplikácia sa pokúsi kontaktovať ďalšieho, menej preferovaného hostiteľa MX. Hodnotu preferencie nastavuje správca domény alebo osoba, ktorá vytvorila záznam MX.

Ak sa názov nachádza v oprávnení servera DNS, ale nemá priradený žiadny MX, server DNS môže odpovedať prázdnym zoznamom zdrojových záznamov MX. Ak nastane táto situácia, zasielajúca poštová aplikácia sa môže pokúsiť o priame vytvorenie spojenia s cieľovým hostiteľom. **Poznámka:** Použitie zástupného znaku (príklad: *.mycompany.com) v záznamoch MX sa pre doménu neodporúča.

Príklad: Záznam MX pre hostiteľa
V nasledujúcom príklade by mal systém na základe preferencie doručiť poštu pre fsc5.test.ibm.com hostiteľovi samotnému. Ak ho nemožno dosiahnuť, systém by mal doručiť túto poštu psfred.test.ibm.com alebo mvs.test.ibm.com (v prípade, že psfred.test.ibm.com takisto nemožno dosiahnuť). Nasleduje príklad toho, ako by vyzerali tieto záznamy 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
```

Plánovanie DNS

DNS ponúka množstvo riešení. Skôr než nakonfigurujete DNS, je dôležité naplánovať, ako bude vo vašej sieti fungovať. Subjekty, ako napríklad sieťová štruktúra, výkon a bezpečnosť je potrebné vyhodnotiť pred implementáciou DNS. Pri plánovaní potrieb vášho DNS si pozrite nasledujúce témy:

Stanovenie autorít DNS
Na správcu DNS sa kladú špeciálne autorizačné požiadavky. Je potrebné zvážiť aj bezpečnostné aspekty autorizácie. Táto téma vysvetľuje požiadavky.

Stanovenie štruktúry vašej domény
Ak prvýkrát nastavujete doménu je potrebné ešte pred vytvorením zón naplánovať požiadavky a údržbu.

Plánovanie bezpečnostných opatrení
DNS poskytuje voľby bezpečnosti s cieľom obmedziť prístup na váš server zvonka. Táto téma objasňuje uvedené voľby a spôsob riadenia prístupu.

Stanovenie autorít DNS

Pri nastavovaní DNS je potrebné vykonať bezpečnostné opatrenia s cieľom chrániť vašu konfiguráciu. Musíte uviesť, ktorí užívatelia budú mať právo vykonávať zmeny konfigurácie.

Ak chcete povoliť správcovi vášho iSeries(TM) nakonfigurovať a spravovať DNS, vyžaduje sa minimálna úroveň oprávnenia. Udelenie prístupu k všetkým objektom správcovi umožní vykonávať úlohy správy DNS. Odporúča sa, aby užívatelia, ktorí budú konfigurovať DNS, mali prístup správcu bezpečnosti s oprávnením na všetky objekty (*ALLOBJ). Na udelenie oprávnenia užívateľom použite iSeries Navigator. Ak potrebujete podrobnejšie informácie, prečítajte si v online pomoci DNS tému **Udeľovanie oprávnenia správcovi DNS**.

Poznámka: Ak profil správcu nemá úplné oprávnenie, musí mu byť udelený špecifický prístup a oprávnenie na všetky adresáre DNS a súvisiace konfiguračné súbory.

Stanovenie štruktúry domény

Je dôležité stanoviť spôsob rozdelenia vašej domény alebo poddomén na zóny, ako čo najlepšie vyhovieť požiadavke siete, ako sa pripájať na internet a ako sa dohovoriť s firewallom. Tieto faktory môžu byť zložité a je potrebné riešiť ich od prípadu k prípadu. Podrobný návod nájdete v autoritatívnom zdroji, ako napríklad O'Reilly DNS and BIND.

Ak konfigurujete zónu DNS ako dynamickú zónu, nemôžete vykonávať manuálne zmeny zónových údajov, kým je server zapnutý. Ak tak urobíte, nastane interferencia s prichádzajúcimi dynamickými aktualizáciami. Ak je potrebné vykonať manuálne zmeny, zastavte server, vykonajte potrebné zmeny a reštartujte ho. Dynamické aktualizácie odoslané na zastavený server DNS nebudú nikdy vykonané. Preto budete možno chcieť nakonfigurovať dynamickú a statickú zónu samostatne, čo môžete vykonať vytvorením úplne samostatných zón alebo definovaním novej poddomény, ako napríklad dynamic.mycompany.com pre tých klientov, ktorú budú udržiavaní dynamicky.

DNS iSeries(TM) poskytuje grafické rozhranie pri konfigurácii vašich serverov. V niektorých prípadoch toto rozhranie používa terminológiu alebo koncepty, ktoré sa môžu v iných zdrojoch nazývať rozdielne. Ak pri plánovaní konfigurácie vášho DNS používate iné informačné zdroje, bude užitočné zapamätať si nasledovné:

- Všetky zóny a objekty definované na serveri sú organizované v rámci zložiek **zón dopredného vyhľadávania** a **spätného vyhľadávania**. Zóny dopredného vyhľadávania sú zóny, ktoré sa používajú na

mapovanie názvov domén do IP adries, ako napríklad záznamy A. Zóny spätného vyhľadávania sú zóny, ktoré sa používajú na mapovanie IP adries do názvov domén, ako napríklad záznamy PTR.

- DNS iSeries sa odvoláva na **primárne** a **sekundárne zóny**. Niekedy sa nazývajú aj hlavné a podriadené zóny.
- Rozhranie používa **podzóny**, ktoré nazývajú niektoré zdroje aj poddomény. Zóna potomka je podzónou, pre ktorú ste delegovali zodpovednosť za jeden alebo viacero názvových serverov.

Plánovanie bezpečnostných opatrení

Zabezpečenie vášho servera DNS je zásadnou vecou. Okrem nižšie uvedených bezpečnostných úvah sa bezpečnosťou DNS a iSeries(TM) zaoberá aj množstvo zdrojov v Informačnom centre vrátane IBM(R) Secureway: iSeries and the Internet. Príručka DNS and BIND sa takisto zaoberá bezpečnosťou súvisiacou s DNS.

Zoznam zhôd adries
DNS používa zoznam zhôd adries na povolenie alebo odmietnutie prístupu vonkajších entít k určitým funkciám DNS. Tieto zoznamy môžu obsahovať špecifické IP adresy, podsieť (používajúcu IP predponu) alebo určité kľúče na podpisovanie transakcií TSIG (Transaction Signature). Na zozname zhôd adries môžete definovať zoznam entít, ktorým chcete povoliť alebo zakázať prístup. Ak chcete tento zoznam znova použiť, môžete ho uložiť ako zoznam riadenia prístupu (ACL). Vždy keď ho budete potrebovať, jednoducho zavoláte ACL a celý zoznam sa zavedie.

Poradie elementov zoznamu zhôd adries
Použije sa prvý element na zozname zhôd adries, s ktorým sa daná adresa zhoduje. Ak chcete napríklad povoliť všetky adresy v sieti 10.1.1.x s výnimkou 10.1.1.5, elementy zoznamu zhôd musia byť v tomto poradí (!10.1.1.5; 10.1.1/24). V takom prípade sa bude adresa 10.1.1.5 porovnávať s prvým elementom a bude ihneď odmietnutá.

Ak by boli elementy uvedené v opačnom poradí (10.1.1/24; !10.1.1.5), IP adrese 10.1.1.5 by bol prístup povolený, pretože server ju bude porovnávať s prvým elementom, ktorý sa zhoduje a povolí ju bez toho, aby skontroloval zvyšok pravidiel.

Voľby riadenia prístupu
DNS umožňuje nastaviť obmedzenia, napríklad obmedzenie toho, kto môže zasielať dynamické aktualizácie na server, dotazovať údaje a žiadať o prenosy zón. Zoznamy riadenia prístupu môžete použiť na zamedzenie prístupu na server pre nasledujúce voľby:

allow-update
Aby mohol váš server DNS prijímať dynamické aktualizácie z ľubovoľných vonkajších zdrojov, musíte povoliť voľbu na povolenie aktualizácií.

allow-query
Uvádza, ktorí hostitelia majú povolené dotazovať tento server. Ak nie je uvedená, predvolenou hodnotou je povoliť dotazy zo všetkých hostiteľov.

allow-transfer
Uvádza, ktorí hostitelia majú povolené prijímať prenosy zón zo servera. Ak nie je uvedená, predvolenou hodnotou je povoliť prenosy zo všetkých hostiteľov.

allow-recursion
Uvádza, ktorí hostitelia majú povolené vykonávať rekurzívne dotazy cez tento server. Ak nie je uvedená, predvolenou hodnotou je povoliť rekurzívne dotazy zo všetkých hostiteľov.

blackhole
Uvádza zoznam adries, z ktorých server nebude prijímať dotazy alebo ktoré nebude používať na rozlišovanie dotazu. Na dotazy z týchto adries nebude server odpovedať.

Požiadavky systému DNS

Voľba DNS (Voľba 31) sa neinštaluje automaticky spolu so základným operačným systémom. DNS musíte na inštaláciu špecificky vybrať. Nový server DNS pridaný pre V5R1 vychádza zo zavedenia priemyselného štandardu DNS známeho pod názvom BIND 8. Predchádzajúce služby DNS OS/400(R) boli založené na BIND 4.9.3 a sú stále dostupné vo V5R1.

Po nainštalovaní DNS budete štandardne nakonfigurovaní na nastavenie jedného servera DNS používajúceho schopnosti servera DNS založeného na BIND 4.9.3 dostupné v predchádzajúcich vydaniach. Ak chcete spustiť jeden alebo viacero serverov DNS používajúcich BIND 8, musíte nainštalovať PASE (Portable Application Solutions Environment). PASE je SS1 voľba 33. Po nainštalovaní PASE iSeries Navigator automaticky spracuje konfiguráciu správnej implementácie BIND.

Ak nepoužívate PASE, nebudete môcť využívať všetky vlastnosti BIND 8. Ak nepoužívate PASE, môžete ešte stále spúšťať ten istý server DNS založený na BIND 4.9.3 dostupný v predchádzajúcich vydaniach. Dokumentáciu pre BIND 4.9.3 nájdete v téme informačného centra DNS V4R5

(približne 357 KB).

Ak chcete nakonfigurovať server DHCP na inom iSeries s cieľom zasielať aktualizácie na tento server DNS, voľba 31 musí byť tiež nainštalovaná na DHCP iSeries. Server DHCP používa programovacie rozhrania poskytované voľbou 31 na vykonávanie dynamických aktualizácií.

Ak chcete určiť, či je DNS nainštalovaný, postupujte takto:

1. V príkazovom riadku napíšte **GO LICPGM** a stlačte **Enter**.
2. Napíšte **10** (Zobraziť nainštalované licenčné programy) a stlačte **Enter**.
3. Presuňte sa nadol na **5722SS1 OS/400 - Domain Name System** (SS1 voľba 31)
   Ak je DNS úspešne nainštalovaný **Installed Status** bude ***compatible**:

```
LicPgm     Installed Status     Description
5722SS1    *COMPATIBLE          OS/400 - Domain Name System
```

4. Stlačením **F3** ukončíte obrazovku.

Ak chcete nainštalovať DNS, postupujte takto:

1. V príkazovom riadku napíšte **GO LICPGM** a stlačte **Enter**.
2. Napíšte **11** (Nainštalovať licenčné programy) a stlačte **Enter**.
3. Napíšte **1** (Inštalovať) v poli **Option** vedľa OS/400 - Domain Name System a stlačte **Enter**.
4. Opakovaným stlačením **Enter** potvrdíte inštaláciu.

Konfigurácia DNS

Skôr než začnete pracovať s vašou konfiguráciou DNS, pozrite si systémové požiadavky DNS a nainštalujte si potrebné komponenty DNS. Nasledujúca podtéma poskytuje návod na konfiguráciu vášho servera DNS:

Prístup na DNS v aplikácii iSeries Navigator
Pokyny na prístup k DNS v aplikácii iSeries Navigator.

Konfigurácia názvových serverov
DNS vám umožňuje vytvoriť viaceré inštancie názvového servera. Táto téma poskytuje pokyny na konfiguráciu názvového servera.

Konfigurácia DNS na prijímanie dynamických aktualizácií
Servery DNS spúšťajúce BIND 8 možno nakonfigurovať na prijímanie požiadaviek z iných zdrojov na

dynamickú aktualizáciu zónových údajov. Táto téma poskytuje pokyny na konfiguráciu voľby na povolenie aktualizácie, aby mohol DNS prijímať dynamické zmeny.

Import súborov DNS
DNS môže importovať existujúce súbory zónových údajov. Postupujte podľa týchto čas šetriacich procedúr na vytvorenie novej zóny z existujúceho konfiguračného súboru.

Prístup k externým údajom DNS
Keď vytvárate zónové údaje DNS, váš server bude môcť rozlíšiť dotazy do danej zóny. Táto téma vysvetľuje, ako nakonfigurovať DNS na rozlišovanie dotazov mimo vašej domény.

Prístup na DNS v aplikácii iSeries Navigator

Nasledujúce pokyny vás povedú konfiguračným rozhraním DNS v iSeries Navigator. Ak používate PASE, budete môcť nakonfigurovať servery DNS založené na BIND 8. Ak nepoužívate PASE, môžete ešte stále spúšťať ten istý server DNS založený na BIND 4.9.3, ktorý bol dostupný v predchádzajúcich vydaniach. Informácie týkajúce sa DNS založeného na BIND 4.9.3. nájdete v téme informačného centra V4R5 DNS

(približne 62 strán).

Ak konfigurujete DNS prvýkrát, postupujte takto:

1. V aplikácii **iSeries Navigator** rozviňte **your iSeries server** —> **Network** —> **Servers** —> **DNS**.
2. Pravým tlačidlom myši kliknite na **DNS** a vyberte **New Configuration**.

Ak máte nakonfigurovaný server DNS predchádzajúci V5R1, postupujte takto:

1. V aplikácii **iSeries Navigator** rozviňte **your iSeries server** —> **Network** —> **Servers** —> **DNS**.
2. V pravej časti kliknite dvakrát na server DNS a otvorte okno **DNS Configuration**.
3. Ak používate PASE, bude vám ponúknutá voľba migrovať vašu existujúcu konfiguráciu DNS do implementácie BIND 8. Keď však už migrujete BIND 8, nemôžete ho zmeniť na BIND 4.9.3. Ak nemáte istotu, vyberte **No**. Ak chcete vykonať migráciu, zvoľte **Yes**.
4. Ak chcete kedykoľvek migrovať váš server DNS na BIND 8, kliknite pravým tlačidlom myši na **DNS** z ľavej časti a vyberte **Migrate to Version 8**.

Konfigurácia názvových serverov

DNS iSeries(TM) založený na BIND 8 podporuje viaceré inštancie názvového servera. Nasledujúce úlohy vás povedú procesom vytvárania jednej inštancie názvového servera vrátane jeho vlastností a zón.

1. Vytvoriť inštanciu názvového servera
   Na definovanie inštancie servera DNS použite sprievodcu **New DNS Configuration**.
2. Upraviť vlastnosti servera DNS
   Definujte globálne vlastnosti pre vašu novú serverovú inštanciu.
3. Nakonfigurovať zóny na názvovom serveri
   Vytvorte zóny a zónové údaje a naplňte váš názvový server.

Ak chcete vytvoriť viaceré inštancie, opakujte vyššie uvedenú procedúru, až kým nebudú vytvorené všetky inštancie, ktoré si želáte. Pre každú inštanciu názvového servera môžete uviesť nezávislé vlastnosti, ako napríklad úrovne ladenia a hodnoty automatického spustenia. Keď vytvoríte novú inštanciu, vytvoria sa samostatné konfiguračné súbory. Podrobnejšie informácie o konfiguračných súboroch nájdete v časti Údržba konfiguračných súborov DNS.

Vytvorenie inštancie názvového servera

Ak chcete spustiť sprievodcu **New DNS Configuration**, postupujte takto:

1. V aplikácii **iSeries Navigator** rozviňte **your iSeries(TM) server** —> **Network** —> **Servers** —> **DNS**.

2. V ľavej časti kliknite pravým tlačidlom myši na **DNS** a zvoľte si **New Name Server...**
3. Sprievodca vás povedie procesom konfigurácie.

Sprievodca bude vyžadovať nasledujúci vstup:

DNS server name: Zadajte názov pre váš server DNS. Tento názov môže mať dĺžku až päť znakov a musí sa začínať písmenom abecedy. Ak vytvárate viacero serverov, každý musí mať jedinečný názov. Tento názov sa v iných oblastiach systému volá aj názov ″inštancie″ servera DNS.

Listen-on IP addresses: Dva servery DNS nemôžu počúvať na rovnakej IP adrese. Predvoleným nastavením je počúvať na všetkých (ALL) IP adresách. Ak vytvárate ďalšie inštancie servera, žiadna z nich nemôže byť nakonfigurovaná tak, aby počúvala na všetkých IP adresách. IP adresu musíte uviesť pre každý server.

Root servers: Môžete zaviesť zoznam predvolených internetových koreňových serverov alebo uviesť vaše vlastné koreňové servery, ako napríklad interné koreňové servery pre intranet.
Poznámka: O zavedení predvolených internetových koreňových serverov by ste mali uvažovať len vtedy, ak ste na internete a očakávate, že váš DNS bude plne rozlišovať internetové názvy.

Server start-up: Môžete uviesť, či sa má server automaticky spustiť pri spustení TCP/IP. Pri prevádzkovaní viacerých serverov možno jednotlivé inštancie spustiť a ukončiť nezávisle od seba.

Čo sa má vykonať ako ďalšie: Úprava vlastností servera DNS.

Úprava vlastností servera DNS

Po vytvorení názvového servera môžete upravovať vlastnosti, ako napríklad povolenie úrovní aktualizácie a ladenia. Tieto voľby sa použijú len pre inštanciu servera, ktorú meníte. Ak chcete upravovať vlastnosti inštancie servera DNS, postupujte takto:

1. V aplikácii **iSeries Navigator** rozviňte **your iSeries(TM) server** —> **Network** —> **Servers** —> **DNS**.
2. V pravej časti kliknite pravým tlačidlom myši na **your DNS server** a vyberte **Configuration**.
3. Kliknite pravým tlačidlom myši na **DNS Server** a vyberte **Properties**.

Čo sa má urobiť ako ďalšie: Konfigurácia zón na názvovom serveri.

Konfigurácia zón na názvovom serveri

Po vytvorení vášho názvového servera sa vráťte do hlavného okna **iSeries Navigator**. Váš server sa zobrazí v pravej časti. Ak chcete nakonfigurovať zóny na vašom serveri, kliknite pravým tlačidlom myši na názov servera a zvoľte si **Configuration**. Zobrazí sa okno **DNS Configuration**.

Všetky zóny sú nakonfigurované pomocou sprievodcov. Kliknutím pravým tlačidlom myši na zodpovedajúcu zložku vytvorte **zóny dopredného vyhľadávania** alebo **zóny spätného vyhľadávania**. Zobrazia sa voľby pre daný typ zóny. Ak chcete spustiť sprievodcu, zvoľte si typ zóny, ktorú chcete vytvoriť.

Opisy typov objektov, ktoré môžete v DNS V5R1 vytvoriť nájdete v časti Pochopenie DNS.

Po nakonfigurovaní vašich zón nájdete ďalšie konfiguračné informácie v nasledujúcich témach.

Konfigurácia zóny na prijímanie dynamických aktualizácií
Dynamické aktualizácie povoľujú autorizovaným zdrojom zasielať zdrojové záznamy s cieľom aktualizovať zónové údaje, čo znižuje potrebu manuálnych zmien zónových údajov.

Import zónových údajov
Ak máte existujúci súbor zónových údajov z ďalšieho servera DNS, môžete ho odoslať na váš nový server.

Prístup k externým údajom DNS
Možno budete chcieť nakonfigurovať váš server na rozlišovanie dotazov pre informácie mimo zónových údajov, ktoré obsahuje. Na pomoc pri rozlišovaní týchto dotazov ich môžete zasielať iným autoritatívnym serverom alebo môžete zaviesť koreňové servery.

Konfigurácia DNS na prijímanie dynamických aktualizácií

Keď sa vytvárajú dynamické zóny, mali by ste si pozrieť štruktúru svojej siete. Ak niektoré časti vašej domény budú ešte stále vyžadovať manuálne aktualizácie, možno by ste mali zvážiť nastavenie samostatných statických a dynamických zón. Ak je potrebné aktualizovať dynamickú zónu manuálne, musíte zastaviť server dynamickej zóny a po vykonaní aktualizácií ho reštartovať. Zastavenie prinúti server zosynchronizovať všetky dynamické aktualizácie, vykonané odkedy server zaviedol svoje zónové údaje z databázy zóny. Ak by ste server nezastavili, stratili by ste všetky dynamické aktualizácie spracované od jeho spustenia. Avšak zastavenie servera za účelom vykonania manuálnych aktualizácií znamená, že by ste mohli stratiť dynamické aktualizácie zasielané, v čase keď bol server vypnutý.

DNS určuje, že zóna je dynamická vtedy, keď sú objekty definované v príkaze na povolenie aktualizácií. Ak chcete nakonfigurovať voľbu na povolenie aktualizácií, postupujte takto:

1. V aplikácii **iSeries Navigator** rozviňte **your iSeries server** —> **Network** —> **Servers** —> **DNS**.
2. V pravej časti kliknite pravým tlačidlom myši na **your DNS server** a vyberte **Configuration**.
3. V okne **DNS Configuration** rozviňte **Forward Lookup Zone** alebo **Reverse Lookup Zone**.
4. Kliknite pravým tlačidlom myši na primárnu zónu, ktorú chcete upravovať a vyberte **Properties**.
5. Na stránke **Primary Zone Properties** kliknite na záložku **Options**.
6. Na stránke **Options** rozviňte **Access Control** —> **allow-update**.
7. Na overovanie autorizovaných aktualizácií používa DNS zoznam zhôd adries. Ak chcete na zoznam zhôd adries pridať objekt, zvoľte si typ elementu zoznamu zhôd adries a kliknite na **Add...** Môžete pridať IP adresu, IP predponu, zoznam riadenia prístupov alebo kľúč.
8. Po skončení aktualizácie zoznamu zhôd adries kliknite na **OK** a zatvorte stránku **Options**.

Ak nastavujete DNS na prijímanie dynamických aktualizácií zo servera iSeries DHCP, pozrite si tému Konfigurácia DHCP na zasielanie dynamických aktualizácií.

Import súborov DNS

Importom súboru zónových údajov alebo konverziou existujúcich hostiteľských tabuliek môžete vytvoriť primárnu zónu. Ak chcete vytvoriť zónové údaje z hostiteľskej tabuľky, pozrite si časť *Konverzia hostiteľských tabuliek* v téme informačného centra DNS V4R5

(okolo 357 KB).

Možné je importovať ľubovoľný súbor, ktorý je platným súborom zónovej konfigurácie založeným na syntaxi BIND. Súbor by mal byť umiestnený v adresári IFS. DNS overí po naimportovaní súboru, či je tento platným súborom zónových údajov a pridá ho do súboru NAMED.CONF pre túto inštanciu servera.

Ak chcete naimportovať zónový súbor, postupujte takto:

1. V aplikácii **iSeries Navigator** rozviňte **your iSeries(TM) server** —> **Network** —> **Servers** —> **DNS**.
2. V pravej časti dvakrát kliknite na inštanciu servera DNS, do ktorej chcete túto zónu importovať.
3. V ľavej časti kliknite pravým tlačidlom myši na **DNS server** a zvoľte si **Import Zone**.
4. Pri importovaní primárnej zóny postupujte podľa pokynov sprievodcu.

Overenie záznamu
Funkcia importu údajov domény číta a overuje každý záznam importovaného súboru. Po ukončení funkcie importu údajov domény možno všetky chybné záznamy prezrieť individuálne na stránke vlastností **ostatných záznamov** importovanej zóny.

- **Poznámka:**
- Import veľkej primárnej domény môže trvať niekoľko minút.
- Funkcia importu údajov domény nepodporuje direktívu $include. Proces kontroly platnosti importu údajov domény identifikuje riadky obsahujúce direktívu $include ako chybné.

Prístup k externým údajom DNS

Koreňové servery sú kritickým miestom pre funkciu servera DNS, ktorý je priamo pripojený na internet alebo veľký intranet. Servery DNS musia používať koreňové servery na odpovedanie na dotazy o hostiteľoch s výnimkou tých, ktorí sa nachádzajú v ich vlastných súboroch domény.

Aby server DNS získal viac informácií, musí vedieť, kde má hľadať. Prvým miestom na internete, kde server DNS hľadá, sú koreňové servery. Koreňové servery smerujú server DNS na iné servery v hierarchii, kým sa nenájde odpoveď alebo kým sa nezistí, že neexistuje žiadna odpoveď.

Zoznam predvolených koreňových serverov iSeries(TM) Navigator
Koreňové servery internetu by ste mali používať len vtedy, ak máte internetové pripojenie a chcete rozlíšiť názvy na internete, ak nie sú rozlíšené na vašom serveri DNS. iSeries Navigator poskytuje predvolený zoznam internetových koreňových serverov. Tento zoznam je aktuálny pri vydaní aplikácie iSeries Navigator. Kontrolu aktuálnosti predvoleného zoznamu môžete vykonať jeho porovnaním so zoznamom na stránke InterNIC. Aktualizujte si konfiguračný zoznam koreňových serverov.

Kde získať adresy internetových koreňových serverov
Adresy koreňových serverov vrchnej úrovne sa z času na čas menia a je úlohou správcu DNS ich aktualizovať. InterNIC udržiava aktuálny zoznam adries internetových koreňových serverov. Ak chcete získať aktuálny zoznam internetových koreňových serverov, postupujte takto:

1. Anonymný FTP pre server InterNIC: FTP.RS.INTERNIC.NET
2. Stiahnite si tento súbor: /domain/named.root
3. Uložte tento súbor v nasledujúcej adresárovej ceste: Integrated File System/Root/QIBM/ProdData/OS400/DNS/ROOT.FILE.

Server DNS za firewallom možno nemá definované žiadne koreňové servery. V takomto prípade môže server DNS rozlíšiť dotazy len z položiek, ktoré existujú vo svojich vlastných primárnych databázových súboroch domény. Dotazy mimo siete môže zaslať do DNS firewallu. V takomto prípade server DNS firewallu funguje ako zasielateľ.

Intranetové koreňové servery
Ak je váš server DNS súčasťou veľkého intranetu, môžete mať interné koreňové servery. Ak sa váš server DNS nebude pripájať na internet, nemusíte zavádzať predvolené internetové servery. Mali by ste však pridať vaše interné koreňové servery, aby mohol váš server DNS rozlíšiť interné adresy mimo domény.

Riadenie DNS

Po nakonfigurovaní DNS si možno budete chcieť pozrieť nasledujúce témy:

Overenie funkčnosti DNS pomocou NSLookup
NSLookup môžete použiť na overenie fungovania DNS.

Riadenie bezpečnostných kľúčov
Bezpečnostné kľúče umožňujú obmedzovať prístup k vašim údajom DNS.

Štatistika servera DNS
Nástroje výpisu z pamäte databázy a štatistiky pomáhajú pri zisťovaní a riadení výkonu servera.

Údržba konfiguračných súborov DNS
Snažte sa o pochopenie súborov, ktoré DNS používa a pozrite si návod na ich zálohovanie a údržbu.

Rozšírené voľby DNS
Táto téma sa zaoberá spôsobom, akým môžu skúsení správcovia vstupovať do rozšírených vlastností.

Overovanie funkčnosti DNS pomocou NSLookup

Ak chcete dotazovať server DNS kvôli IP adrese, použite NSLookup (Name Server Lookup). Tým overíte, či server DNS odpovedá na dotazy. Požiadajte o názov hostiteľa priradený k návratovej IP adrese (127.0.0.1). Server by mal odpovedať názvom hostiteľa (localhost). Mali by ste tiež dotazovať určité názvy definované v inštancii servera, ktorú sa snažíte overiť. Tým sa potvrdí, či konkrétna testovaná inštancia servera funguje správne.

Ak chcete overiť funkčnosť DNS pomocou NSLookup, postupujte takto:

1. Do príkazového riadka napíšte NSLOOKUP DMNNAMSVR(n.n.n.n), kde n.n.n.n je adresa nakonfigurovaná pre testovanú inštanciu servera, ktorá má na tejto adrese počúvať.
2. Do príkazového riadka napíšte NSLOOKUP a stlačte **Enter**. Tým sa začne relácia dotazu NSLookup.
3. Napíšte server, za ktorým bude nasledovať názov vášho servera a stlačte **Enter**. Napríklad: server myiseries.mycompany.com.
   Zobrazia sa tieto informácie:

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

   kde n.n.n.n predstavuje IP adresu servera vášho DNS.
4. V príkazovom riadku zadajte 127.0.0.1 a stlačte **Enter**.
   Mali by sa zobraziť nasledujúce informácie vrátane názvu hostiteľa návratu.

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

   Name:    localhost
   Address:  127.0.0.1
   ```

   Server DNS odpovedá správne, ak vráti názov hostiteľa návratu: **localhost**.
5. Napíšte exit a stlačte **Enter** kvôli odchodu z relácie terminálu NSLOOKUP.

Poznámka: Ak pri používaní LSLookup potrebujete pomoc, napíšte ? a stlačte **Enter**.

Riadenie bezpečnostných kľúčov

Existujú dva typy kľúčov týkajúcich sa DNS. Každý z nich má pri zabezpečovaní konfigurácie vášho DNS inú úlohu. Nasledujúce opisy vysvetľujú, ako ktorý súvisí s vašim serverom DNS.

Kľúč DNS
Kľúč DNS je kľúč definovaný pre BIND. Server DNS ho používa ako súčasť overovania prichádzajúcej aktualizácie. Kľúč môžete nakonfigurovať a priradiť mu názov. Potom, keď budete chcieť chrániť objekt DNS, ako napríklad dynamickú zónu, môžete tento kľúč zadať na zozname zhôd adries.

Pri riadení kľúčov DNS postupujte takto:

1. V aplikácii **iSeries Navigator** rozviňte **your iSeries(TM) server** —> **Network** —> **Servers** —> **DNS**.

2. V pravej časti kliknite pravým tlačidlom myši na inštanciu servera DNS, ktorú chcete otvoriť a vyberte **Configuration**.
3. V okne **DNS Configuration** zvoľte **File** > **Manage Keys...**

Kľúče dynamickej aktualizácie
Kľúče dynamickej aktualizácie sa používajú na zabezpečenie dynamických aktualizácií serverom DHCP. Keď sa DNS a DHCP nachádzajú na tom istom iSeries, tieto kľúče musia byť prítomné. Ak sa DHCP nachádza na inom iSeries, aby ste povolili bezpečné dynamické aktualizácie, musíte vytvoriť ten istý kľúč dynamickej aktualizácie na každom serveri iSeries.

Pri riadení kľúčov dynamických zmien postupujte takto:
1. V aplikácii **iSeries Navigator** rozviňte **your iSeries server** —> **Network** —> **Servers** —> **DNS**.
2. Kliknite pravým tlačidlom myši na **DNS** a vyberte **Manage Dynamic Update Keys...**

Štatistika servera DNS
DNS poskytuje niekoľko diagnostických nástrojov, ktoré možno použiť na monitorovanie výkonu vášho servera.

Štatistika servera
DNS vám umožní prezerať si štatistiku pre inštanciu servera. Táto štatistika sumarizuje počet dotazov a odpovedí, ktoré server dostal od posledného reštartu servera alebo opätovného zavedenia jeho databázy. Informácie sa kontinuálne pridávajú do tohto súboru, až kým ho nevymažete. Tieto informácie môžu slúžiť pri hodnotení objemu prevádzky, ktorú server prijíma a pri odhaľovaní problémov. Podrobnejšie informácie o štatistike servera nájdete v téme online pomoci DNS **Pochopenie štatistiky servera DNS**.

Ak chcete vstupovať do štatistiky servera, postupujte takto:
1. V aplikácii **iSeries Navigator** rozviňte **your iSeries(TM) server** —> **Network** —> **Servers** —> **DNS**.
2. V pravej časti kliknite pravým tlačidlom myši na **your DNS server** a vyberte **Configuration**.
3. V okne **DNS configuration** zvoľte **View** —> **Server Statistics**.

Aktívna databáza servera
DNS vám umožní prezerať si výpis pamäte autoritatívnych údajov, údajov pamäte cache a údaje pomoci pre inštanciu servera. Výpis pamäte zahŕňa informácie zo všetkých primárnych a sekundárnych zón servera (zóny dopredného a spätného mapovania), ako aj informácie, ktoré server získal z dotazov. Databáza obsahuje informácie o zóne a hostiteľovi vrátane niektorých vlastností zóny, ako napríklad informácie o spustení oprávnenia (SOA) a priebežné vlastnosti hostiteľa, ako napríklad informácie o poštovej výmene (MX). Tieto informácie môžu slúžiť pri odhaľovaní problémov.

Pomocou aplikácie iSeries Navigator si môžete prezerať výpis pamäte databázy aktívneho servera. Ak si chcete uložiť kópiu súborov, názov súboru výpisu z pamäte databázy je NAMED_DUMP.DB v ceste adresára vášho iSeries: **Integrated File System**/**Root**/**QIBM**/**UserData**/**OS400**/**DNS**/**<server instance>**, kde ″<server instance>″ je názov inštancie servera DNS. Podrobnejšie informácie o databáze aktívneho servera nájdete v téme online pomoci DNS **Pochopenie výpisu z pamäte databázy servera DNS**.

Ak chcete mať prístup do výpisu z pamäte databázy servera, postupujte takto:
1. V aplikácii **iSeries Navigator** rozviňte **your iSeries server** —> **Network** —> **Servers** —> **DNS**.
2. V pravej časti kliknite pravým tlačidlom myši na **your DNS server** a vyberte **Configuration**.
3. V okne **DNS configuration** zvoľte **View** —> **Active Server Database**.

Údržba konfiguračných súborov DNS
DNS OS/400(R) môžete použiť na vytvorenie a riadenie inštancií servera DNS na vašom iSeries(TM). Konfiguračné súbory pre DNS riadi iSeries Navigator. Súbory by ste nemali upravovať manuálne. Na

vytváranie, zmenu alebo vymazávanie konfiguračných súborov DNS používajte vždy iSeries Navigator. Konfiguračné súbory DNS sú uložené v nasledujúcich cestách integrovaného súborového systému DNS.

Poznámka: Nasledujúca štruktúra súborov sa týka DNS spusteného na BIND 8. Ak používate DNS založený na BIND 4.9.3, pozrite si časť *Zálohovanie konfiguračných súborov DNS a údržba protokolových súborov* v téme informačného centra DNS V4R5

(približne 62 strán).

V nasledujúcej tabuľke sú súbory uvedené v hierarchii zobrazených ciest. Súbory s ikonou uloženia

by sa mali zálohovať s cieľom chrániť údaje. Súbory s ikonou vymazania

by sa mali pravidelne vymazávať.

Názov		**Opis**
QIBM/UserData/OS400/DNS/		Adresár počiatočného bodu pre DNS.
ATTRIBUTES		DNS používa tento súbor aby určil, ktorú verziu BIND používate.
QIBM/UserData/OS400/DNS/<*instance-n*>/		Adresár počiatočného bodu pre inštanciu DNS.
ATTRIBUTES		Konfiguračné atribúty, ktoré používa DNS iSeries.
NAMED.CONF		Tento súbor obsahuje konfiguračné údaje, ktoré povedia serveru, ktoré špecifické zóny riadi, kde sa nachádzajú zónové súbory, ktoré zóny možno dynamicky aktualizovať, kde sa nachádzajú jeho zasielacie servery a nastavenie ostatných volieb.
BOOT.AS400BIND4		Konfigurácia servera BIND 4.9.3 a súbor politiky, ktorý sa konvertuje do súboru BIND 8 NAMED.CONF pre túto inštanciu. Tento súbor sa vytvorí, ak migrujete server BIND 4.9.3 na BIND 8 a slúži ako záloha na migráciu, a ak server BIND 8 riadne funguje, možno ho vymazať.
NAMED.CA		Zoznam koreňových serverov pre túto inštanciu servera.
NAMED_DUMP.DB		Výpis údajov servera vytvorený pre aktívnu databázu servera.
NAMED.STATS		Server statistics.
NAMED.PID		Udržiava ID procesu spusteného servera. Tento súbor sa vytvorí pri každom spustení servera DNS. Používa sa pre funkcie servera Database, Statistics a Update. Nevymazávajte ani neupravujte tento súbor.

Názov		Opis
QUERYLOG		Prijatý protokol dotazov servera DNS. Tento súbor sa vytvára, keď je aktívny protokol servera DNS. Ak je tento súbor aktívny, zväčšuje sa a mal by sa pravidelne vymazávať.
<zone-name-a>.DB		Súbor zóny pre určitú doménu, ktorá má byť obsluhovaná týmto serverom. Obsahuje všetky zdrojové záznamy pre túto zónu.
<zone-name-b>.DB		Súbor zóny pre určitú doménu, ktorá má byť obsluhovaná týmto serverom. Obsahuje všetky zdrojové záznamy pre túto zónu. Každá zóna má samostatný súbor .DB.
.ixfr.		Prírastkové súbory zónového prenosu (IXFR). Sekundárne servery používajú tieto súbory na zavedenie len tých údajov, ktoré sa zmenili od posledného prenosu zóny. Pri vykonávaní aktualizácií sa bude počet súborov IXFR zvyšovať. Staršie súbory IXFR by ste mali pravidelne vymazávať. Ponechané súbory vytvorené počas jedného alebo dvoch dní umožnia väčšine sekundárnych serverov ešte stále zavádzať IXFR. Ak vymažete všetky súbory, sekundárny server požiada o úplný prenos (AXFR).
TMP		Adresár používaný inštanciou servera na vytvorenie dočasných pracovných súborov.
QIBM/UserData/OS400/DNS/TMP		Program QTOBH2N používa adresár temp na vytvorenie okamžitých súborov vypísaných z hostiteľskej tabuľky na neskorší import pomocou aplikácie iSeries Navigator.
QIBM/UserData/OS400/DNS/_DYN/		Adresár, ktorý udržiava súbory požadované na dynamické aktualizácie.
<key_id-name-x>._KID		Súbor obsahujúci príkaz kľúča BIND 8 pre key_id s názvom *<key_id-name-x>*.
<key_id-name-x>._DUK.*<zone-name-a>*		Kľúč dynamickej aktualizácie požadovaný na inicializáciu požiadavky na dynamickú aktualizáciu na *<zone-name-a>* pomocou kľúča *<key_id-name-x>*.
<key_id-name-y>._KID		Súbor obsahujúci príkaz kľúča BIND 8 pre key_id s názvom *<key_id-name-y>*.
<key_id-name-y>._DUK.*<zone-name-a>*		Kľúč dynamickej aktualizácie požadovaný na inicializáciu požiadavky na dynamickú aktualizáciu na *<zone-name-a>* pomocou kľúča *<key_id-name-y>*.
<key_id-name-y>._DUK.*<zone-name-b>*		Kľúč dynamickej aktualizácie požadovaný na inicializáciu požiadavky na dynamickú aktualizáciu na *<zone-name-b>* pomocou kľúča *<key_id-name-y>*.

Rozšírené vlastnosti DNS

DNS v aplikácii iSeries Navigator poskytuje rozhranie na konfiguráciu a riadenie vášho servera DNS. Nasledujúce úlohy sa poskytujú ako skratky pre správcov, ktorí poznajú grafické rozhranie iSeries. Tieto úlohy poskytujú rýchle metódy na zmenu stavu servera a jeho atribútov pre viaceré inštancie naraz.

Zmena atribútov DNS

Rozhranie DNS neumožňuje, aby ste menili naraz všetky úrovne automatického štartu a ladenia inštancie servera. Na zmenu týchto nastavení pre jednotlivé inštancie servera DNS alebo pre všetky inštancie naraz môžete použiť znakové rozhranie. Ak chcete použiť CHGDNSA, postupujte takto:

1. Do príkazového riadka napíšte CHGDNSA a stlačte **F4**.
2. Na stránke Change DNS Server Attributes (CHGDNSA) napíšte názov jednej inštancie servera alebo *ALL a stlačte **Enter**.

   Zobrazia sa dostupné voľby atribútov servera:
   Autostart server . . . . . *SAME *YES, *NO, *SAME
   Debug level . . . . . *SAME 0-11, *SAME, *DFT
3. **Autostart** Ak chcete uviesť, aby sa vybraté servery DNS spúšťali automaticky, keď sa spúšťa TCP/IP, napíšte *YES. Ak nechcete, aby sa server spustil pri spustení TCP/IP, napíšte *NO. Ak chcete ponechať terajšie nastavenie atribútu, napíšte *SAME.

   Debug level Ak chcete zmeniť úroveň ladenia vybratú servermi DNS ako úroveň, ktorá sa má použiť, napíšte hodnotu v rozsahu 0 až 11. Ak chcete uviesť, aby úroveň ladenia zdedila hodnotu ladenia pri spustení servera, napíšte *DFT. Ak chcete ponechať terajšie nastavenie atribútu, napíšte *SAME.

   Ak ste zadali všetky vaše preferencie, stlačením **Enter** nastavte atribúty DNS.

Spustenie alebo zastavenie serverov DNS

Rozhranie DNS neumožňuje, aby ste naraz spustili alebo zastavili viaceré inštancie servera. Ak chcete zmeniť tieto nastavenia pre viacero inštancií naraz, môžete použiť znakové rozhranie. Ak chcete použiť znakové rozhranie na spustenie všetkých inštancií servera DNS naraz, napíšte do príkazového riadka STRTCPSVR SERVER(*DNS) DNSSVR(*ALL). Ak chcete naraz zastaviť všetky servery DNS, napíšte do príkazového riadka ENDTCPSVR SERVER(*DNS) DNSSVR(*ALL).

Zmena hodnôt ladenia

DNS v rozhraní iSeries Navigator neumožňuje, aby ste zmenili úroveň ladenia počas chodu servera. Ak však chcete zmeniť úroveň ladenia počas chodu servera, môžete použiť znakové rozhranie. Táto vlastnosť je užitočná pre správcov, ktorí majú veľké zóny a nechcú mať veľké množstvo údajov o ladení, ktoré by dostali v čase, keď sa server spúšťa prvýkrát a zavádza všetky zónové údaje. Ak chcete zmeniť úroveň ladenia pomocou znakového rozhrania, postupujte nasledovne a nahraďte <instance> názvom inštancie servera:

1. Do príkazového riadka napíšte ADDLIBLE QDNS a stlačte **Enter**.
2. Zmeňte úroveň ladenia:
   - Ak chcete zapnúť ladenie alebo zvýšiť úroveň ladenia o 1, napíšte CALL QTOBDRVS ('BUMP' '<instance>') a stlačte **Enter**.
   - Ak chcete vypnúť ladenie, napíšte CALL QTOBDRVS ('OFF' '<instance>') a stlačte **Enter**.

Odstraňovanie problémov DNS

DNS funguje v mnohom rovnako ako ostatné aplikácie a funkcie TCP/IP. Podobne ako aplikácie FTP a SMTP sa úlohy DNS spúšťajú pod podsystémom QSYSWRK a vytvárajú protokoly úloh pod užívateľským profilom QTCP s informáciami priradenými k úlohe DNS. Ak úloha DNS skončí, môžete na stanovenie príčiny ukončenia použiť protokoly úlohy. Ak server DNS nevráti očakávanú odpoveď, informácie na pomoc pri analýze problému sa môžu nachádzať v protokoloch úlohy.

Konfigurácia DNS pozostáva z niekoľkých súborov s niekoľkými rozdielnymi typmi záznamov v každom súbore. Problémy so serverom DNS sú vo všeobecnosti výsledkom nesprávnych položiek v konfiguračných súboroch DNS. Pri vzniku problému skontrolujte, či konfiguračné súbory DNS obsahujú očakávané položky.

Protokolovanie
DNS poskytuje početné voľby protokolovania, ktoré možno pri pokuse o vyhľadanie zdroja problému upravovať. Protokolovanie poskytuje flexibilitu tým, že ponúka rôzne úrovne závažnosti, kategórie správ a výstupné súbory s cieľom jemne dolaďovať protokolovanie pri vyhľadávaní problémov.

Nastavenie ladenia
DNS ponúka 12 úrovní riadenia ladenia. Protokolovanie zvyčajne poskytuje jednoduchšiu metódu vyhľadávania problémov, ale v niektorých prípadoch môžete potrebovať ladenie. Za normálnych podmienok je ladenie vypnuté (hodnota = 0).

Ďalšie prostriedky na odstraňovanie problémov
Všeobecné informácie o odstraňovaní problémov DNS sú dostupné v mnohých zdrojoch. Príručka O'Reilly DNS and BIND predstavuje dobrý referenčný materiál týkajúci sa všeobecných otázok a adresár prostriedkov DNS poskytuje odkazy na diskusné skupiny pre správcov DNS.

Identifikácia úloh
Ak si pozeráte protokol úlohy s cieľom overiť funkciu servera DNS (napríklad pomocou WRKACTJOB), vezmite do úvahy nasledujúce pokyny na pomenovávanie:

- Ak používate BIND 4.9.3, názov úlohy servera bude QTOBDNS. Podrobnejšie informácie o ladení DNS 4.9.3 nájdete v časti *Odstraňovanie problémov serverov DNS* v téme Informačného centra DNS V4R5

  (približne 357 KB).
- Ak spúšťate servery založené na BIND 8, pre každú spúšťanú inštanciu bude existovať samostatná úloha. Názov úlohy bude pozostávať z 5 stálych znakov (QTOBD), za ktorými bude nasledovať názov inštancie. Ak máte napríklad dve inštancie INST1 a INST2, názvy ich úloh budú QTOBDINST1 a QTOBDINST2.

Protokolovanie servera DNS

BIND 8 ponúka niekoľko nových volieb protokolovania. Môžete uviesť aké typy správ sa protokolujú, kam sa každý typ správy zasiela a aká závažnosť daného typu správy sa má protokolovať. Vo všeobecnosti bude predvolené nastavenie protokolovania vyhovovať, ale ak ho chcete zmeniť, odporúča sa vyhľadať si informácie o protokolovaní v ďalších zdrojoch dokumentácie BIND 8.

Protokolovacie kanály
Server DNS môže protokolovať správy do rôznych výstupných kanálov. Kanály uvádzajú, kam sa údaje protokolovania zasielajú. Môžete si zvoliť nasledujúce typy kanálov:

- **Kanály súborov**
  Správy protokolované do kanálov súborov sa zasielajú do súboru. Predvolenými kanálmi súboru sú as400_debug a as400_QPRINT. Štandardne sa správy o ladení protokolujú do kanála as400_debug, čo je súbor NAMED.RUN, ale do tohto súboru môžete zadať aj zasielanie iných kategórií správ. Kategórie správ protokolované do as400_QPRINT sa zasielajú do spoolového súboru QPRINT pre užívateľský profil QTCP. Okrem poskytovaných predvolených kanálov si môžete vytvoriť aj svoje vlastné kanály súborov.
- **Kanály Syslog**
  Správy zaprotokolované do tohto kanála sa zasielajú do protokolu úloh serverov. Predvoleným kanálom syslog je as400_joblog. Zaprotokolované správy smerované do tohto kanála sa zasielajú do protokolu úlohy inštancie servera DNS.
- **Nulové kanály**
  Všetky správy zaprotokolované do nulového kanála budú vymazané. Predvoleným nulovým kanálom je as400_null. Ak nechcete, aby sa správy objavili v niektorom protokolovom súbore, môžete kategórie nasmerovať do nulového kanála.

Kategórie správ
Správy sú zoskupené do kategórií. Môžete uviesť, ktoré kategórie správ sa majú protokolovať do ktorého kanála. Existuje množstvo kategórií vrátane:

- config: spracovanie konfiguračného súboru
- db: databázové operácie
- queries: generuje krátku protokolovú správu pre každý dotaz, ktorý daný server príjme
- lame-servers: zisťovanie nesprávneho delegovania
- update: dynamické aktualizácie
- xfer-in: prenosy zón, ktoré daný server prijíma
- xfer-out: prenosy zón, ktoré daný server odosiela

Protokolové súbory sa môžu zväčšovať a je ich potrebné pravidelne vymazávať. Pri zastavení a spustení servera DNS sa vymazáva obsah všetkých protokolových súborov servera DNS.

Závažnosť správy
Kanály vám umožňujú filtráciu podľa závažnosti správy. Pre každý kanál môžete uviesť úroveň závažnosti, pri ktorej sa správy protokolujú. K dispozícii sú nasledujúce úrovne závažnosti:
- Critical
- Error
- Warning
- Notice
- Info
- Debug (uveďte úroveň ladenia 0-11)
- Dynamic (zdediť úroveň ladenia pri spustení servera)

Protokolujú sa všetky správy vybratej závažnosti a všetky úrovne na zozname, nachádzajúce sa nad vybratou úrovňou. Ak si napríklad zvolíte Warning, kanál protokoluje správy Warning, Error a Critical. Ak si zvolíte úroveň Debug, môžete uviesť hodnotu v rozpätí 0 až 11, pri ktorej chcete protokolovať správy ladenia.

Zmena nastavení protokolovania
Ak chcete vstupovať do volieb protokolovania, postupujte takto:
1. V aplikácii **iSeries Navigator** rozviňte **your iSeries(TM) server** —> **Network** —> **Servers** —> **DNS**.
2. V pravej časti kliknite pravým tlačidlom myši na **your DNS server** a vyberte **Configuration**.
3. V okne **DNS configuration** kliknite pravým tlačidlom myši na **DNS server** a zvoľte si **Properties**.
4. V okne **Server Properties** zvoľte záložku **Channels** a vytvorte nové kanály súboru alebo vlastnosti kanála, napríklad závažnosť správy protokolovanej do daného kanála.
5. V okne **Server Properties** zvoľte záložku **Logging** a zadajte, ktoré kategórie správ sa protokolujú do daného kanála.

Tip na odstraňovanie problémov
Predvolená úroveň závažnosti kanála as400_joblog je nastavená na Error. Toto nastavenie sa používa na zníženie objemu informačných a varovných správ, ktoré by inak mohli znížiť výkon. Ak máte problémy, ale protokol úlohy nestanovuje ich zdroj, budete musieť zmeniť úroveň závažnosti. Ak chcete vstúpiť na stránku Channels a zmeniť úroveň závažnosti pre kanál as400_joblog na Warning, Notice alebo Info s cieľom vidieť viac protokolovacích údajov, postupujte podľa vyššie uvedenej procedúry. Po rozlíšení problému môžete úroveň závažnosti resetovať na Error a znížiť tým počet správ v protokole úlohy.

Nastavenie ladenia DNS

Funkcia ladenia DNS poskytuje informácie, ktoré vám pomôžu stanoviť problémy servera DNS a odstrániť ich. Pri pokuse o odstránenie problémov sa odporúča použiť najprv protokolovanie.

Platné hodnoty ladenia sú v rozsahu 0 až 11. Zástupca servisu IBM vám pomôže stanoviť príslušnú hodnotu ladenia s cieľom diagnostikovať problém vášho DNS. Hodnoty 1 alebo vyššie zapisujú informácie o ladení do súboru NAMED.RUN v ceste vášho adresára iSeries: **Integrated File**

System/Root/QIBM/UserData/OS400/DNS/<server instance>, kde ″<server instance>″ je názov inštancie servera DNS. Pokiaľ je úroveň ladenia nastavená na hodnotu 1 alebo vyššiu, súbor NAMED.RUN ďalej rastie a server DNS je naďalej v chode. Odporúča sa z času na čas vymazať tento súbor, aby nezaberal príliš veľa miesta. Na zadanie preferencií pre maximálnu veľkosť a počet verzií súboru NAMED.RUN môžete použiť aj stránku **Server Properties** - **Channels**.

Ak chcete zmeniť hodnotu ladenia pre inštanciu servera DNS, postupujte takto:

1. V aplikácii **iSeries Navigator** rozviňte **your iSeries server** —> **Network** —> **Servers** —> **DNS**.
2. V pravej časti kliknite pravým tlačidlom myši na **your DNS server** a vyberte **Configuration**.
3. V okne **DNS configuration** kliknite pravým tlačidlom myši na server DNS a vyberte **Properties**.
4. Na stránke **Server Properties - General** uveďte úroveň ladenia spustenia servera.
5. Ak je server spustený, zastavte a reštartujte ho.
   Poznámka: Zmeny v úrovni ladenia nenadobudnú účinnosť, kým je server v chode. Úroveň ladenia, ktorá je tu nastavená, sa použije pri ďalšom úplnom reštarte servera. Ak chcete zmeniť úroveň ladenia, kým je server v chode, pozrite si časť Rozšírené vlastnosti DNS.

Ďalšie informácie o DNS

Existuje množstvo zdrojov informácií týkajúcich sa DNS a BIND 8. Nasledujúci zoznam predstavuje len malú časť dostupných prostriedkov:

- DNS and BIND, third edition. Paul Albitz and Cricket Liu. Published by O'Reilly and Associates,Inc.

  Sebastopol, California, 1998. ISBN číslo: 1-56592-512-2. Toto je najdôležitejší zdroj na DNS.
- Webová stránka Internet Software Consortium

  obsahuje novinky, odkazy a iné zdroje pre BIND.
- InterNIC

  udržuje adresár všetkých registrátorov názvov domén oprávnených spoločnosťou ICANN (Internet Corporation for Assigned Names and Numbers).
- DNS Resources Directory

  poskytuje referenčný materiál DNS a odkazy na mnohé iné prostriedky DNS vrátane diskusných skupín. Taktiež poskytuje zoznam RFC súvisiacich s DNS.

IBM manuály a redbooky(TM)

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

  Táto publikácia Redbook opisuje podporu servera DNS (Domain Name System) a DHCP (Dynamic Host Configuration Protocol) zahrnutú v OS/400(R). Informácie v tejto publikácii Redbook vám pomôžu nainštalovať, upraviť, nakonfigurovať a odstrániť problémy DNS a DHCP prostredníctvom príkladov.
  Poznámka: Táto publikácia Redbook nebola aktualizovaná a neobsahuje nové vlastnosti BIND 8 dostupné pre V5R1. Je však dobrou referenciou pre všeobecné koncepty DNS.

Príloha. Poznámky

Tieto informácie boli vytvorené pre produkty a služby ponúkané v USA.

IBM nemusí ponúkať produkty, služby alebo komponenty spomínané v tomto dokumente v iných krajinách. Informácie o produktoch a službách, ktoré sú dostupné vo vašej krajine získate od lokálneho zástupcu IBM. Žiadny odkaz na produkt, program alebo službu IBM nemá v úmysle uviesť ani naznačiť, že možno použiť len produkt, program alebo službu IBM. Namiesto nich možno použiť ľubovoľné funkčne porovnateľné produkty, programy alebo služby, ktorá neporušujú intelektuálne vlastnícke práva IBM. Je však na zodpovednosti užívateľa, aby zhodnotil a overil fungovanie všetkých produktov, programov alebo služieb, ktoré nie sú od IBM.

IBM môže vlastniť patenty alebo nevybavené žiadosti o patentovanie zahŕňajúce predmetnú vec opisovanú v tomto dokumente. Poskytnutie tohto dokumentu nedáva užívateľom licenciu na tieto patenty. Dotazy týkajúce sa licencie môžete zasielať písomne na adresu:

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

Dotazy v súvislosti s licenciami týkajúce sa dvojbajtových (DBCS) informácií posielajte oddeleniu intelektuálneho vlastníctva IBM vo vašej krajine alebo ich zašlite písomne na adresu:

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

Nasledujúci odsek sa netýka Spojeného kráľovstva, ani žiadnej krajiny, kde tieto ustanovenia odporujú miestnym zákonom: SPOLOČNOSŤ INTERNATIONAL BUSINESS MACHINES POSKYTUJE TÚTO PUBLIKÁCIU ″TAK AKO JE″ BEZ ZÁRUK AKÉHOĽVEK DRUHU, ČI UŽ VYJADRENÝCH ALEBO PREDPOKLADANÝCH VRÁTANE, AVŠAK BEZ OBMEDZENIA LEN NA ZÁRUKY DODRŽIAVANIA AUTORSKÝCH PRÁV, PREDAJNOSTI ALEBO VHODNOSTI NA URČITÝ ÚČEL. Niektoré štáty nepovoľujú odmietnutie vyjadrených alebo predpokladaných záruk pri určitých transakciách, preto sa vás toto vyhlásenie nemusí týkať.

Dané informácie môžu obsahovať technické nepresnosti alebo typografické chyby. Uvedené informácie sa pravidelne menia; tieto zmeny sa zahŕňajú do nových vydaní publikácií. IBM môže kedykoľvek a bez oznámenia vykonávať zlepšenia a/alebo zmeny v produkte(och) a/alebo programe(och) opisovaných v tejto publikácii.

Všetky odkazy na webové stránky, ktoré nie sú stránkami IBM, sa poskytujú len pre vaše pohodlie a v žiadnom prípade neslúžia ako odporúčanie týchto webových stránok. Materiály uvedených webových stránok nie sú súčasťou materiálov pre tento produkt IBM a ich použitie je na vaše vlastné riziko.

IBM môže používať alebo distribuovať ľubovoľné vami poskytnuté informácie akýmkoľvek spôsobom, ktorý bude pokladať za vhodný bez toho, aby jej vznikol voči vám nejaký záväzok.

Užívatelia licencie na tento program, ktorí by chceli získať o ňom informácie za účelom povolenia: (i) výmeny informácií medzi nezávisle vytvorenými programami a ostatnými programami (vrátane tohto) a (ii) vzájomného používania vymenených informácií môžu kontaktovať:

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

Tieto informácie budú dostupné za určitých podmienok, ktoré budú v niektorých prípadoch zahŕňať úhradu poplatku.

Licencovaný program opísaný v týchto informáciách a všetky príslušné licenčné materiály poskytuje IBM na základe podmienok zákazníckej zmluvy IBM, Medzinárodnej programovej licenčnej zmluvy IBM alebo akejkoľvek ekvivalentnej zmluvy.

Ak si prezeráte elektronickú kópiu tohto dokumentu, fotografie a farebné ilustrácie sa nemusia zobraziť.

Ochranné známky

Nasledujúce výrazy sú ochrannými známkami spoločnosti International Business Machines v Spojených štátoch alebo iných krajinách:
Application System/400
AS/400
e (logo)
IBM
iSeries
Operating System/400
OS/400
400

Lotus, Freelance a WordPro sú ochrannými známkami spoločnosti International Business Machines Corporation a Lotus Development Corporation v Spojených štátoch alebo iných krajinách.

C-bus je ochrannou známkou spoločnosti Corollary, Inc. v Spojených štátoch alebo iných krajinách.

ActionMedia, LANDesk, MMX, Pentium a ProShare sú ochrannými známkami alebo registrovanými ochrannými známkami spoločnosti Intel Corporation v Spojených štátoch alebo iných krajinách.

Microsoft, Windows, Windows NT a logo Windows sú ochrannými známkami spoločnosti Microsoft Corporation v Spojených štátoch alebo iných krajinách.

SET a Logo SET sú ochrannými známkami vo vlastníctve spoločnosti SET Secure Electronic Transaction LLC.

Java a všetky ochranné známky týkajúce sa Javy sú ochrannými známkami spoločnosti Sun Microsystems, Inc. v Spojených štátoch alebo iných krajinách.

UNIX je registrovanou ochrannou známkou spoločnosti Open Group v Spojených štátoch a iných krajinách.

Ostatné názvy spoločností, produktov alebo služieb môžu byť ochrannými alebo servisnými známkami iných spoločností.

Podmienky na sťahovanie a tlač publikácií

Povolenie na používanie publikácií, ktoré ste sa rozhodli stiahnuť, sa udeľuje za predpokladu, že prijímate nasledujúce podmienky.

Na osobné použitie: Tieto publikácie môžete rozmnožovať na osobné, nekomerčné účely za predpokladu dodržiavania všetkých vlastníckych práv. Bez výslovného súhlasu IBM nemôžete distribuovať, zobrazovať ani vytvárať práce odvodené od týchto publikácií ani ich častí.

Na komerčné účely: Tieto publikácie môžete rozmnožovať, distribuovať a zobrazovať výlučne v rámci vášho podniku a to za predpokladu dodržiavania všetkých vlastníckych práv. Bez výslovného súhlasu IBM nemôžete vytvárať práce odvodené od týchto publikácií, reprodukovať, distribuovať alebo zobrazovať tieto publikácie ani ich časti mimo vášho podniku.

Na publikácie ani informácie, údaje, softvér alebo iné intelektuálne vlastníctvo v nich obsiahnuté sa neudeľujú žiadne iné povolenia, licencie ani práva, či už vyjadrené alebo predpokladané s výnimkou tých, ktoré sú výslovne udelené v tomto povolení.

Spoločnosť IBM si vyhradzuje právo stiahnuť týmto dokumentom udelené povolenie na základe svojho vlastného uváženia vždy, keď bude použitie publikácií škodiť jej záujmom alebo, ako to IBM stanovuje, kedykoľvek, keď sa nebudú riadne dodržiavať vyššie uvedené pokyny.

Tieto informácie nemožno sťahovať, exportovať, ani reexportovať s výnimkou prípadov, kedy je takéto stiahnutie, export alebo reexport plne v súlade so všetkými platnými zákonmi a predpismi vrátane zákonov a predpisov Spojených štátov týkajúcich sa exportu. IBM NERUČÍ ZA OBSAH TÝCHTO PUBLIKÁCIÍ. UVEDENÉ PUBLIKÁCIE SA POSKYTUJÚ ″TAK AKO SÚ″ BEZ ZÁRUK AKÉHOKOĽVEK DRUHU, ČI UŽ VYJADRENÝCH ALEBO PREDPOKLADANÝCH VRÁTANE, AVŠAK BEZ OBMEDZENIA LEN NA PREDPOKLADANÉ ZÁRUKY PREDAJNOSTI A VHODNOSTI NA URČITÝ ÚČEL.

Spoločnosť IBM vlastní autorské práva na všetky materiály.

Stiahnutím alebo vytlačením publikácie z tejto stránky ste vyjadrili svoj súhlas s uvedenými podmienkami.

Vytlačené v USA