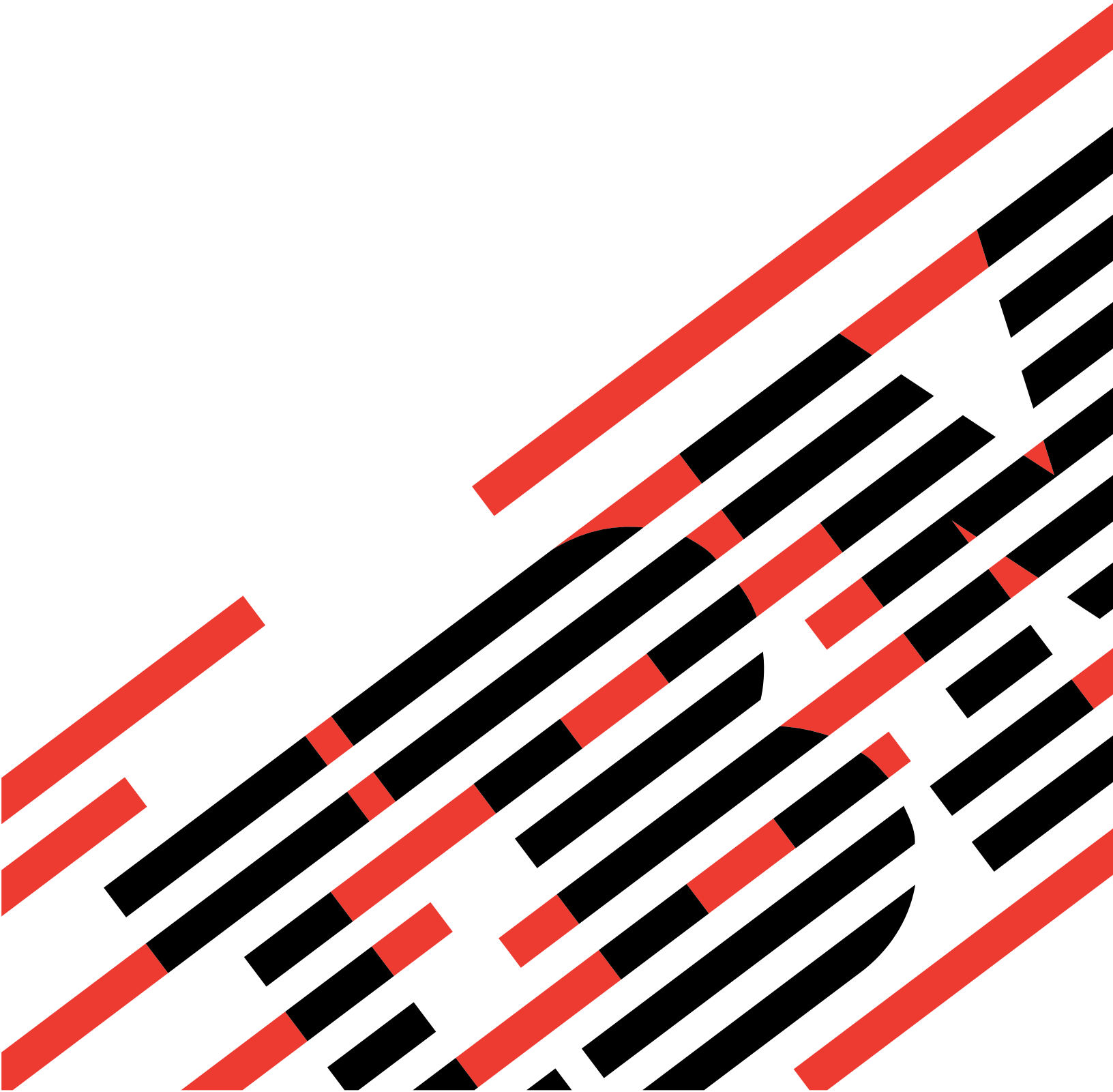
IBM

eserver

iSeries

DNS

Versiunea 5 Ediţia 3



IBM

@server

iSeries

DNS

Versiunea 5 Ediţia 3

Notă

Înainte de utilizarea acestor informaţii şi a produsului pe care îl suportă, fiţi siguri că aţi citit informaţiile corespunzâtoare. “Observaţii”, la pagina 37.

Ediţia a cincea (august 2005)

Această ediţie se aplică versiunii 5, ediţiei 3, modificării 0 a sistemului de operare IBM Operating System/400 (număr produs 5722-SS1) şi tuturor ediţiilor şi modificărilor următoare până la modificările apărute în noile ediţii. Această versiune nu rulează pe toate modelele RISC şi nici pe modelele CISC.

Cuprins

DNS

DNS-ul este un sistem distribuit de baze de date ce administrează numele de gazdă şi adresele lor IP asociate. Prin utilizarea DNS se pot folosi nume simple, ca de exemplu ″www.jkltoys.com″, pentru a găsi o gazdă, în loc să se folosească adresele IP (xxx.xxx.xxx.xxx). Un singur server poate fi responsabil doar pentru cunoaşterea numelor gazdă şi a adreselor IP pentru o mică subreţea dintr-o zonă, dar serverele DNS pot lucra împreună pentru a mapa toate numele din domeniu la adresele lor IP. Faptul că serverele DNS lucrează împreună este lucrul ce permite comunicarea prin Internet.

Pentru Versiunea 5 Ediţia 1 (V5R1), serviciile DNS se bazează pe standardul industrial de implementare DNS cunoscut sub numele BIND (Berkeley Internet Name Domain) versiunea 8. Serviciile anterioare DNS OS/400(R) se bazau pe BIND versiunea 4.9.3. OS/400 opţiunea 33, Portable Application Solutions Environment (PASE), trebuie să fie instalată pe serverul dumneavoastră iSeries(TM) pentru a utiliza noul server DNS bazat pe BIND 8. Dacă nu aveţi PASE instalat, încă mai puteţi rula acelaşi server DNS bazat pe BIND 4.9.3 care era disponibil pentru ediţiile anterioare. Oricum, migrarea către BIND 8 va furniza o funcţionare îmbunătăţită şi va încorpora o securitate mai bună pentru serverul dumneavoastră DNS.

Notă: Acest subiect discută noile caracteristici bazate pe BIND 8. Dacă nu utilizaţi PASE pentru a rula DNS bazat pe BIND 8, consultaţi subiectul despre DNS din Centrul de informare pentru V4R5

(aproximativ 357 KB) pentru informaţii privind DNS bazat pe BIND 4.9.3.

- Tipăriţi acest subiect vă permite să descărcaţi sau să tipăriţi subiectul DNS.

Înţelegerea DNS-ului
Aceste subiecte sunt desemnate să vă ajute să înţelegeţi elementele fundamentale DNS referitoare la serverele DNS pentru iSeries.

Exemple DNS furnizează diagrame şi explicaţii despre cum funcţionează serverul DNS.

Concepte DNS explică obiectele şi procesele pe care le foloseşte DNS pentru a funcţiona.

Planificare DNS vă ajută să creaţi un plan pentru configurarea serverului dumneavoastră DNS.

Utilizarea DNS
Aceste subiecte sunt concepute pentru a vă asista la configurarea şi administrarea DNS pe serverele dumneavoastră iSeries. De asemenea, ele explică cum să beneficiaţi de noile caracteristici care sunt acum disponibile.

Cerinţele sistemului DNS
Acest subiect descrie cerinţele sistemului pentru a rula DNS pe serverul iSeries

Configurarea DNS
Acest subiect explică cum să utilizaţi Navigator iSeries pentru a configura numele serverelor şi să rezolvaţi cererile din afara domeniului.

Administrarea DNS
Acest subiect explică cum să verificaţi funcţionarea DNS, să monitorizaţi performanţa şi să menţineţi datele şi fişierele DNS.

Depanarea DNS
Acest subiect explică înregistrarea DNS şi setările de depanare care vă ajută să rezolvaţi problemele pe care le aveţi cu serverul dumneavoastră DNS.

Dacă aveţi întrebări la care nu găsiţi răspunsul în Centrul de informare, Alte informaţii privind DNS furnizează o listă de alte resurse şi referinţe.

Tipăriţi acest subiect

Pentru a vizualiza sau pentru a descărca versiunea PDF, selectaţi DNS (aproximativ 357 KB).

Pentru salvarea unui PDF pe staţia dumneavoastră de lucru pentru vizualizare sau tipărire:

1. Deschideţi PDF în browser-ul dumneavoastră (clic pe legătura de mai sus).
2. În meniul din browser-ul dumneavoastră, faceţi clic pe **File**.
3. Faceţi clic pe **Save As...**
4. Navigaţi către directorul în care doriţi să salvaţi fişierul PDF.
5. Faceţi clic pe **Save**.

Dacă aveţi nevoie de Adobe Acrobat Reader pentru a vizualiza sau tipări aceste PDF-uri, puteţi descărca o copie de pe situl Adobe Web (www.adobe.com/products/acrobat/readstep.html)

.

Exemple DNS

DNS este un sistem distribuit de bază de date pentru administrarea numelor de gazdă şi a adreselor asociate acestora. Următoarele exemple explică cum funcţionează DNS şi cum îl puteţi folosi în reţeaua dumneavoastră. Exemplele descriu setările şi raţionamentele care pot fi folosite. De asemenea ele fac legături la conceptele înrudite pe care le puteţi găsi folositoare pentru înţelegerea ilustraţiilor.

Exemplu: Un singur server DNS pentru intranet
Prezintă o subreţea simplă cu un server DNS pentru utilizare internă.

Exemplu: Un singur server DNS cu acces la Internet
Prezintă o subreţea simplă cu un server DNS conectat direct la Internet

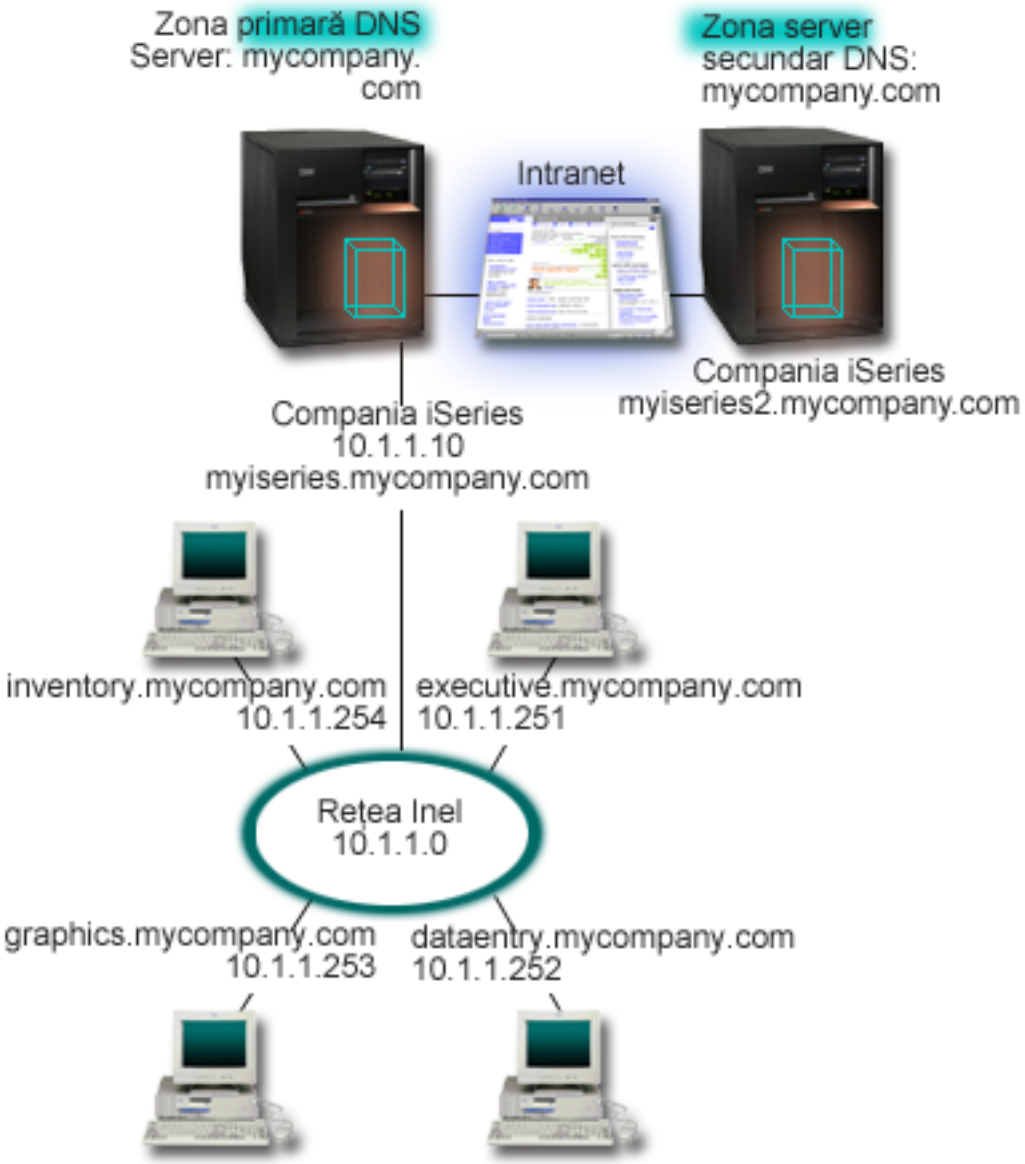
Exemplu: DNS şi DHCP pe acelaşi server iSeries(TM)
Prezintă folosirea DNS şi DHCP pe acelaşi server. Configuraţia poate fi folosită pentru actualizarea dinamică a datelor de zonă DNS, când DHCP asignează adresele IP la gazde. Dacă serverul dumneavoastră DHCP se va afla pe un alt sistem iSeries, consultaţi Exemplu: DNS şi DHCP pe servere iSeries diferite pentru cerinţe suplimentare de configurare DHCP.

Exemplu: Împărţire DNS peste firewall
Descrie funcţionarea DNS peste un firewall pentru a proteja datele interne de pe internet, în timp ce li se permite utilizatorilor interni accesul la datele de pe Internet.

Exemplu: Un server DNS singur pentru intranet

În următoarea ilustraţie DNS rulează pe un iSeries(TM) într-o reţea internă. Această unică instanţă de server DNS este setată pentru a asculta interogările pentru toate adresele IP. Serverul este un server de nume primar pentru zona ″mycompany.com″.

Figura 1. Un singur server pentru o reţea internă.



Fiecare gazdă din zonă are o adresă IP şi un nume de domeniu. Administratorul trebuie să definească manual gazdele în datele de zonă DNS prin crearea înregistrărilor resursă. Înregistrările de mapare adresă (A) mapează numele gazdei la adresa IP asociată. Aceasta permite ca alte gazde din reţea să interogheze serverul DNS pentru a afla adresa IP asignată pentru un nume particular de gazdă. Înregistrările PTR mapează adresa IP a unei maşini la numele ei asociat. Aceasta permite altor gazde din reţea să interogheze serverul DNS pentru a afla numele gazdei care corespunde unei adrese IP.

Pe lângă înregistrările A şi PTR, DNS suportă multe alte înregistrări resursă care pot fi solicitate, depinzând de ce fel de alte aplicaţii bazate pe TCP/IP rulaţi pe reţeaua dumneavoastră locală. Spre exemplu, dacă rulaţi sisteme interne de e-mail, veţi avea nevoie să adăugaţi înregistrări MX pentru ca SMTP să poată interoga DNS pentru a afla pe care sisteme rulează serverele de poştă.

Dacă această reţea mică a fost parte dintr-o reţea mai mare intranet, va fi necesar să definiţi servere root interne.

Serverele secundare
Serverele secundare încarcă datele de zonă din serverul cu autoritate. Serverele secundare obţin datele de zonă prin transferuri de zonă din serverele cu autoritate. Când porneşte un server secundar, el va cere toate datele pentru domeniul specificat de la serverul principal. Un server secundar cere datele actualizate de la serverul primar, fie pentru că el primeşte notificare de la serverul primar (dacă se foloseşte funcţia NOTIFY), fie pentru că el interoghează serverul primar şi determină că datele au fost modificate.
În figura de mai sus, serverul myiseries face parte dintr-o reţea locală. Alt server iSeries, myiseries2, a fost configurat pentru a acţiona ca server secundar pentru zona mycompany.com. Serverul secundar poate fi folosit pentru a balansa cererile de pe server şi de asemenea pentru a furniza o rezervă în cazul în care serverul primar cade. Este o practică bună să aveţi cel puţin un server secundar pentru fiecare zonă.

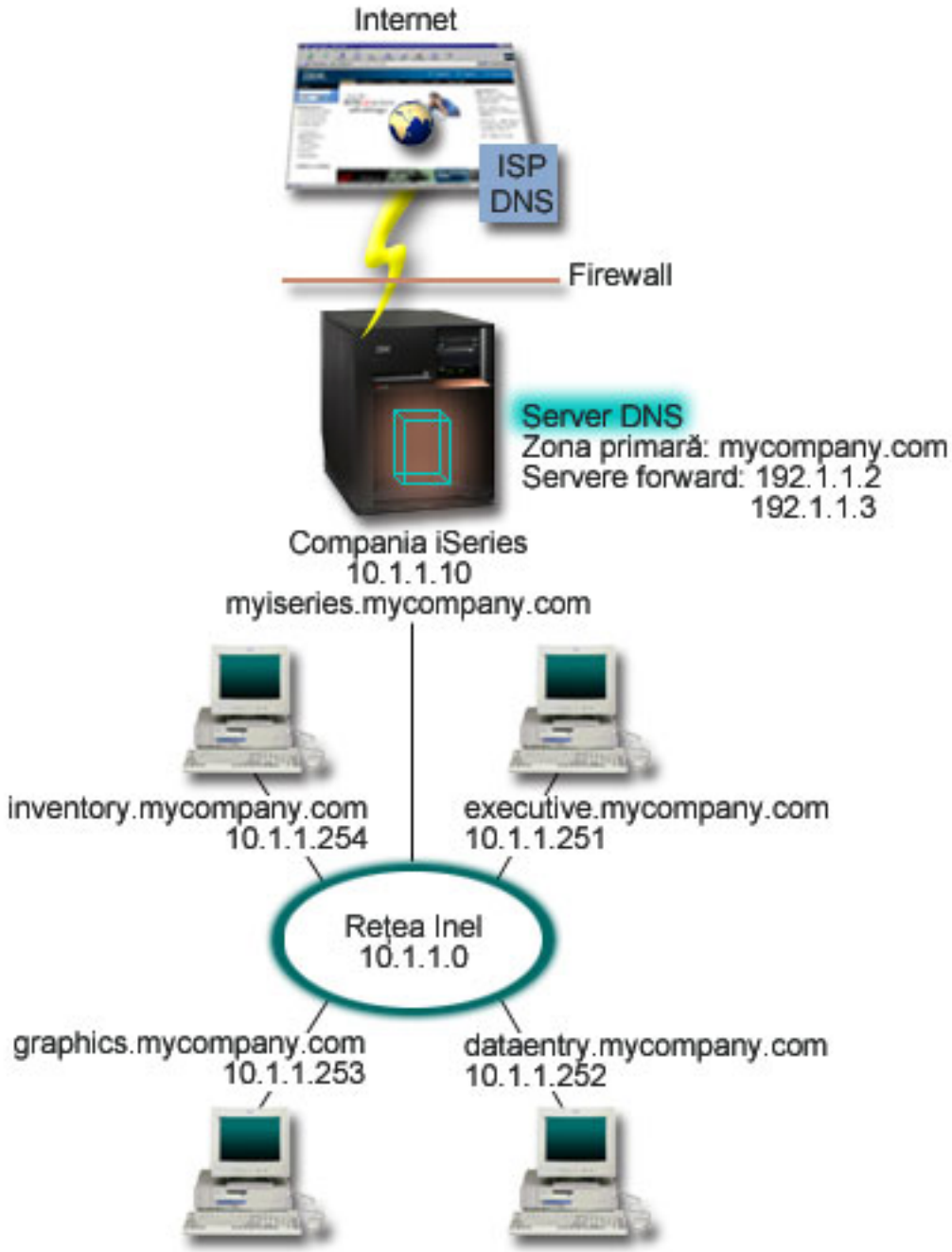
Referiţi-vă la următoarele subiecte pentru mai multe informaţii despre obiectele discutate în acest exemplu:

- Înţelegerea DNS explică ce este şi cum funcţionează DNS. De asemenea, ea defineşte diferitele tipuri de zone care pot fi definite pe un server DNS.
- Înregistrările resursă DNS explică cum sunt utilizate înregistrările resursă de către DNS.

Exemplu: Un singur server DNS cu acces la Internet

Următoarea ilustraţie prezintă acelaşi exemplu de reţea de la exemplul Un singur server DNS pentru reţea internă, dar acum a fost adăugată o conexiune la Internet. În acest exemplu, compania poate accesa Internet-ul, dar firewall-ul este configurat pentru a bloca traficul Internet in interiorul reţelei.

Figura 1. Un server DNS singur cu acces la Internet.



Pentru a rezolva adresa Internet, trebuie să faceţi cel puţin unul din următoarele lucruri:

Definirea serverelor rădăcină (root) Internet
Puteţi încărca automat serverele rădăcină (root) Internet implicite, dar s-ar putea să fie nevoie să actualizaţi lista. Aceste servere vă vor ajuta să rezolvaţi adresele din afara zonei dumneavoastră. Pentru instrucţiuni de obţinere a serverelor rădăcină (root) Internet, consultaţi Accesarea datelor externe DNS .

Activarea acţiunii de înaintare
Puteţi seta acţiunea de înaintare (forward) pentru a transmite cererile pentru zonele din afara zonei mycompany.com către serverele externe DNS, cum sunt serverele DNS ale furnizorului de servicii

Internet (ISP). Dacă vreţi să activaţi căutarea atât de către serverele de înaintare (forward), cât şi de cele rădăcină (root), va trebui să setaţi mai întâi opţiunea **înaintare (forward)** la **primul (first)**. Serverul va încerca mai întâi acţiunea de înaintare şi după aceea va interoga serverele rădăcină (root), doar dacă activitatea de înaintare eşuează în a rezolva cererea.

Următoarele modificări de configurare pot fi de asemenea cerute:

Asignarea adreselor IP nerestricţionate
În exemplul de mai sus, sunt arătate adresele 10.x.x.x. Oricum, aceste adrese sunt restricţionate şi nu pot fi utilizate în afara reţelei intranet. Ele sunt arătate mai jos ca exemplu, dar adresele dumneavoastră IP vor fi determinate de ISP şi alţi factori care depind de reţea.

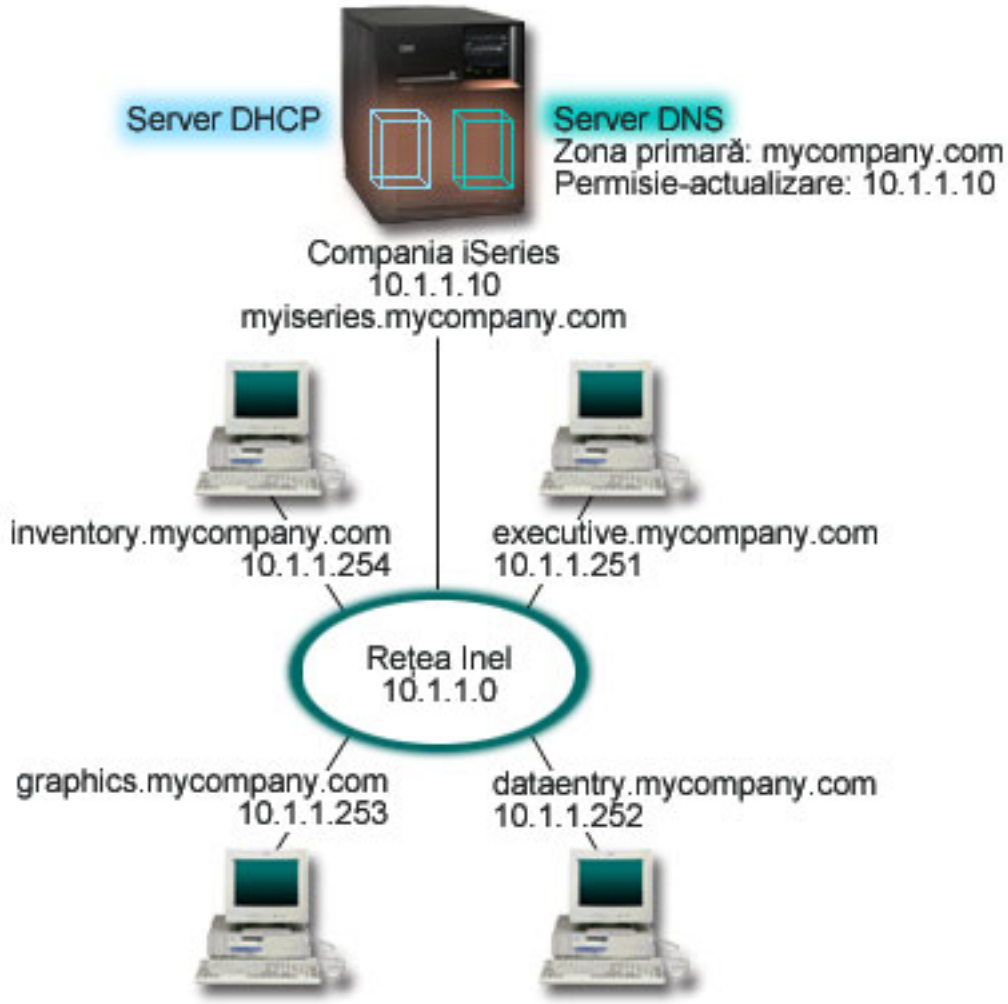
Înregistrarea numelui dumneavoastră de domeniu
Dacă veţi fi vizibil pe Internet, şi încă nu sunteţi înregistrat, va trebui să înregistraţi un nume de domeniu.

Stabilirea unui firewall
Se recomandă să permiteţi serverului dumneavoastră DNS să fie conectat direct la Internet. Ar trebui să configuraţi un firewall sau să luaţi alte măsuri de precauţie pentru securizarea sistemului dumneavoastră iSeries(TM). Pentru mai multe informaţii, consultaţi IBM(R) Secureway: iSeries şi Internetul în Centrul de informare.

Exemplu: DNS şi DHCP pe acelaşi server iSeries(TM)

Următoarea figură descrie o mică subreţea cu un singur server iSeries acţionând ca un server DHCP şi DNS către patru clienţi. În acest mediu de lucru, să presupunem că clienţii care se ocupă cu inventarul, cu introducerea datelor şi clienţii executivi creează documente cu grafice de la serverul de fişiere grafice. Ei se conectează la serverul de fişiere grafice printr-un drive de reţea la numele gazdei.

Figura 1. DNS şi DHCP pe acelaşi server iSeries



Versiunile anterioare de DHCP şi DNS au fost independente una de cealaltă. Dacă DHCP asigna o nouă adresă IP către un client, înregistrările DNS trebuiau să fie actualizate manual de către administrator. În acest exemplu, dacă se modifică adresa IP a serverului de fişiere grafice, deoarece este asignată de DHCP, atunci clienţii lui dependenţi nu vor putea să mapeze un drive de reţea către numele lui de gazdă deoarece înregistrările DNS ar putea să conţină adresa anterioară IP a serverului de fişiere.

Cu serverul DNS V5R1 bazat pe BIND 8, puteţi configura zona dumneavoastră DNS pentru a accepta actualizări dinamice către înregistrările DNS în conjuncţie cu modificările intermitente de adresă prin DHCP. Spre exemplu, când serverul de fişiere grafice reînnoieşte închirierea adresei şi îi este asignată o adresă IP 10.1.1.250 prin serverul DHCP, înregistrările DNS asociate vor fi actualizate automat. Aceasta va permite altor clienţi să interogheze serverul DNS pentru serverul de fişiere grafice prin numele său de gazdă, fără întrerupere.

Pentru a configura o zonă DNS pentru acceptarea actualizărilor dinamice, completaţi următoarele task-uri:

Identificarea zonei dinamice
Nu puteţi face actualizare manuală la o zonă dinamică în timp ce serverul rulează. Făcând asta ar putea cauza interferenţa cu actualizările dinamice care sosesc. Actualizările manuale pot fi făcute când serverul este oprit, dar veţi pierde orice actualizări dinamice trimise în timp ce serverul este oprit. Din acest motiv, poate veţi vrea să configuraţi o zonă dinamică separată pentru a minimiza nevoile pentru

actualizările manuale. Referiţi-vă la Determinarea structurii domeniului pentru mai multe informaţii despre configurarea zonelor dumneavoastră pentru utilizarea funcţiei de actualizare dinamică.

Configurarea opţiunii permitere-actualizare
Orice zonă cu opţiunea permitere-actualizare configurată este considerată o zonă dinamică. Opţiunea permitere-actualizare este setată pentru fiecare zonă. Pentru a accepta actualizările dinamice, opţiunea permitere-actualizare trebuie activată pentru această zonă. Pentru acest exemplu, zona mycompany.com ar avea date permitere-actualizare, dar alte zone definite pe server ar putea fi configurate să fie statice sau dinamice.

Configurarea DHCP pentru a trimite actualizări dinamice
Trebuie să autorizaţi serverul dumneavoastră DHCP pentru a face actualizarea înregistrărilor DNS pentru adresele IP pe care le-a distribuit. Pentru mai multe informaţii în configurarea serverului DHCP pentru a trimite actualizări dinamice, consultaţi Configurarea DHCP pentru trimiterea actualizărilor dinamice.

Configurarea preferinţele serverului secundar
Pentru a menţine curente serverele secundare, puteţi configura DNS pentru a utiliza funcţia NOTIFY pentru a trimite un mesaj către serverele secundare pentru zona mycompany.com când datele de zonă se modifică. De asemenea, puteţi configura transferurile de zonă incrementale, IXFR, care vor permite serverelor secundare activate-IXFR să urmărească şi să încărce doar datele de zonă actualizate, în locul întregii zone.

Dacă veţi rula DNS şi DHCP pe servere diferite, există cerinţe suplimentare de configurare pentru serverul DHCP. Pentru mai multe informaţii, consultaţi Exemplu: DNS şi DHCP pe servere diferite iSeries.

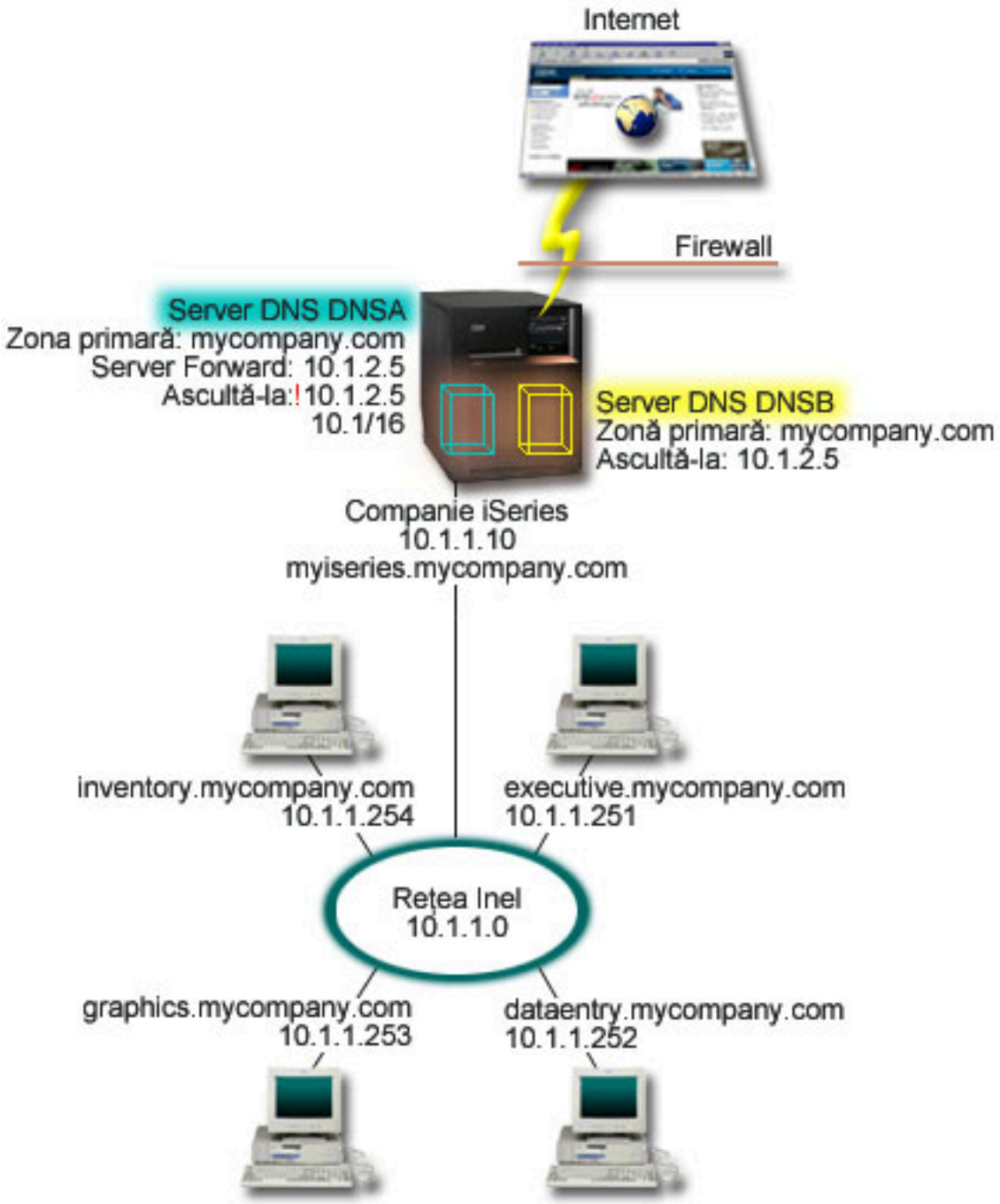
Exemplu: Împărţirea DNS peste firewall

Următoarea ilustraţie prezintă o subreţea simplă care utilizează un firewall pentru securizare. DNS V5R1 bazat pe BIND 8 vă permite setarea de servere DNS multiple pe un singur sistem iSeries(TM). Să presupunem că această companie are o reţea internă cu spaţiu IP rezervat şi o secţiune externă de reţea care este disponibilă public.

Compania vrea ca clienţii ei interni să poată rezolva numele gazdă externe şi să schimbe informaţii mail cu oameni din afară. De asemenea, compania vrea ca dezvoltatorii ei interni să aibă acces către anumite zone numai-interne care nu sunt disponibile celor din afara reţelei interne. Oricum, nu vor ca oricare din rezolvatorii de nume din afară să poată avea acces la reţeaua internă.

Pentru a realiza aceasta, compania setează două instanţe server pe acelaşi sistem iSeries, una pentru intranet şi una pentru orice este public în domeniul ei. Aceasta se numeşte împărţirea DNS.

Figura 1. Împărţirea DNS peste firewall.



Serverul extern DNSB, este configurat cu o zonă primară mycompany.com. Această zonă include doar înregistrările de resurse care se intenţionează să facă parte dintr-un domeniu public. Serverul intern, DNSA este configurat cu o zonă primară mycompany.com, dar datele de zonă definite pe DNSA conţin înregistrări de resurse intranet. Opţiunea de înaintare (forwarder) este definită ca 10.1.2.5. Aceasta va forţa DNSA să înainteze cereri pe care nu le poate rezolva, către serverul DNSB.

Dacă vă faceţi probleme în ceea ce priveşte integritatea firewall-ului dumneavoastră şi alte ameninţări de securitate, aveţi posibilitatea de a utiliza opţiunea ascultă-la pentru a vă ajuta la protejarea datelor interne. Pentru aceasta, puteţi configura serverul intern pentru a permite doar cererile către zonele interne

mycompany.com de la gazdele interne. Pentru ca aceasta să funcţioneze corespunzător, clienţii interni vor trebui să fie configuraţi pentru a interoga doar serverul DNSA. Va trebui să luaţi în considerare următoarele setări de configurare pentru a seta divizarea DNS:

Ascultare
În exemplele anterioare, există doar un singur server DNS pe un sistem iSeries. A fost setat pentru a asculta la toate adresele IP de interfaţă. Dacă aveţi mai multe servere DNS pe iSeries, trebuie să definiţi adresele IP de interfaţă la care fiecare să asculte. Două servere DNS nu pot asculta la aceeaşi adresă. În acest caz, trebuie să vă asiguraţi că toate cererile care vin de la firewall vor fi trimise către 10.1.2.5. Aceste cereri ar trebui trimise către servere externe. De aceea, DNSB este configurat pentru a asculta la 10.1.2.5. Serverul intern, DNSA, este configurat pentru a accepta interogări de la orice adresă de tipul adresă IP 10.1.x.x. *exceptând* 10.1.2.5. Pentru a exclude efectiv această adresă, AML (Address Match List) trebuie să aibă listate adresele excluse înainte de prefixul de adresă inclus.

Ordinea AML (lista de potriviri adresă)
Primul element din AML care se potriveşte cu o adresă va fi utilizat. Spre exemplu, pentru a permite toate adresele pe reţeaua 10.1.x.x , exceptând 10.1.2.5, elementele AML trebuie să fie în ordinea (!10.1.2.5; 10.1/16). În acest caz, adresa 10.1.2.5 va fi comparată cu primul element şi va fi imediat refuzată.

Dacă elementele au fost inversate (10.1/16; !10.1.2.5), adresa IP 10.1.2.5 ar fi permis accesul deoarece serverul ar fi comparat-o cu primul element, care se potriveşte şi îl acceptă fără a verifica restul regulilor.

Conceptele DNS

DNS, V5R1 oferă noi opţiuni bazate pe BIND 8. Următoarele legături furnizează subiecte despre funcţionarea DNS-ului şi noile opţiuni pe care le puteţi folosi:

Funcţii de bază DNS:

Întelegerea DNS-ului
Furnizează informaţii despre ce este DNS-ul şi cum funcţionează acesta şi face o descriere a tipului de zone pe care le puteţi defini.

Înţelegerea cererilor DNS
Explică cum rezolvă DNS interogările în beneficiul clienţilor.

Setarea domeniului DNS
Furnizează informaţii despre înregistrarea domeniului, având legături la alte situri de referinţă pentru setarea spaţiului dumneavoastră de domeniu.

Noi caracteristici DNS:

Actualizările dinamice
DNS V5R1 bazat pe BIND 8 suportă actualizări dinamice. Acestea permit surselor externe, cum este DHCP, să trimită actualizări serverului DNS.

Caracteristici BIND 8
Pe lângă actualizările dinamice, BIND 8 oferă diferite opţiuni pentru îmbunătăţirea performanţei serverului dumneavoastră DNS.

Referinţe înregistrare resursă:

Înregistrările de resurse DNS
Înregistrările de resurse sunt utilizate pentru a stoca date despre numele de domeniu şi adresele IP. Acest subiect conţine o listă de căutare a înregistrărilor de resurse suportate pentru V5R1.

Înregistrări de resurse mail şi MX
DNS suportă rutarea avansată a poştei prin utilizarea acestor înregistrări.

Există multe resurse externe care explică mai detaliat DNS. Referiţi-vă la Alte informaţii privind DNS pentru surse de referinţă suplimentare.

Întelegerea DNS-ului

DNS-ul este un sistem distribuit de baze de date ce administrează numele de gazdă şi adresele lor IP asociate. Prin utilizarea DNS se pot folosi nume simple, ca de exemplu ″www.jkltoys.com″, pentru a găsi o gazdă, în loc să se folosească adresele IP (xxx.xxx.xxx.xxx). Un singur server poate fi responsabil doar pentru cunoaşterea numelor gazdă şi a adreselor IP pentru o mică subreţea dintr-o zonă, dar serverele DNS pot lucra împreună pentru a mapa toate numele din domeniu la adresele lor IP. Faptul că serverele DNS lucrează împreună este lucrul ce permite comunicarea prin Internet.

Datele DNS sunt structurate într-o ierarhie de domenii. Serverele sunt responsabile pentru a şti doar o mică parte din date, cum este un singur subdomeniu. Partea domeniului pentru care serverul este responsabil se numeşte zonă. Un server DNS care are toate informaţiile despre datele referitoare la o zonă este considerat cu autoritate pentru zona respectivă. Un server cu autoritate poate răspunde la interogările despre gazdele din zona lui utilizând doar propriile lui înregistrări resursă. Procesarea interogărilor depinde de un număr de factori. Înţelegerea interogărilor DNS explică căile pe care un client le poate folosi pentru rezolvarea unei interogări.

Înţelegerea zonelor
Datele DNS sunt împărţite în seturi de date administrative numite zone. Zonele conţin nume şi adrese IP ale uneia sau mai multor părţi dintr-un domeniu DNS. Un server care conţine toate informaţiile pentru o zonă se numeşte server cu autoritate pentru acel domeniu. Uneori se poate delega autoritatea de a răspunde la cererile DNS pentru un subdomeniu particular către alt server DNS. În acest caz, serverul DNS pentru domeniu poate fi configurat pentru a referi interogările subdomeniului către serverul corespunzător.

Pentru rezervă sau redundanţă, datele zonei sunt adesea stocate pe servere, altele decât serverele DNS cu autoritate. Aceste alte servere sunt numite servere secundare, care încarcă datele de zonă din serverul cu autoritate. Configurând serverele secundare vă permite să echilibraţi cererile pe servere şi de asemenea vă furnizează o rezervă în cazul în care primul server cade. Serverele secundare obţin datele de zonă prin transferuri de zonă din serverele cu autoritate. Când se iniţializează un server secundar, se încarcă o copie completă a datelor de zonă de la serverul primar. De asemenea, serverul secundar reîncarcă datele de zonă de la serverul primar sau de la alte servere secundare pentru acel domeniu, atunci când datele de zonă se schimbă.

Tipuri de zone DNS
Puteţi folosi serverul DNS iSeries(TM) pentru a defini diferite tipuri de zone care vă ajută să administraţi datele DNS:

Zona primară
Încarcă datele de zonă direct dintr-un fişier de pe o gazdă. O zonă primară poate conţine o subzonă sau o zonă copil. De asemenea, ea poate conţine înregistrări resursă, cum sunt gazda, aliasul (CNAME), adresa (A) sau înregistrări pointeri de mapare inversă (PTR).
Notă: În altă documentaţie BIND, zonele primare sunt uneori referite ca ″zone master″.

Subzona
O subzonă defineşte o zonă din zona primară. Subzonele vă permit să organizaţi datele de zonă în părţi administrative.

Zona copil
O zonă copil defineşte o subzonă şi încredinţează responsabilitatea pentru datele de subzonă la unul sau mai multe servere de nume.

Alias (CNAME)
Un alias defineşte un nume alternativ pentru un nume de domeniu primar.

Gazda
Un obiect gazdă mapează înregistrările A şi PTR către o gazdă. Se pot asocia cu o gazdă înregistrări resursă adiţionale.

Subzona secundară
Încarcă datele de zonă dintr-o zonă a serverului primar sau alt server secundar. Un server secundar păstrează o copie completă a zonei pentru care el este server secundar.
Notă: Uneori zonele secundare sunt referite ca ″zone slave″ în altă documentaţie BIND.

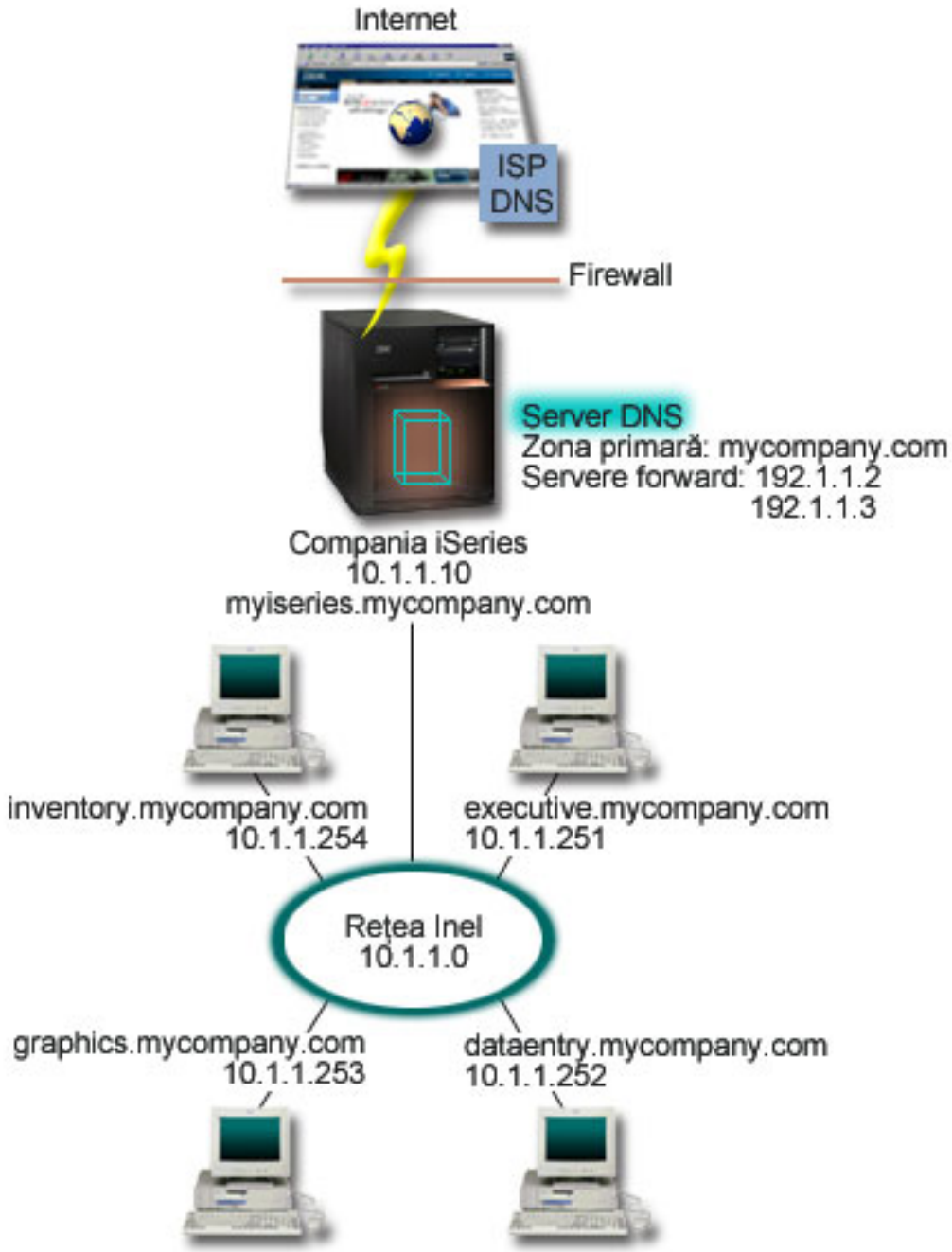
Zona stub
O zonă stub (ciot) este similară cu o zonă secundară, dar ea transferă doar înregistrările NS (server de nume) pentru acea zonă.

Zona forward
O zonă forward (înainte) direcţionează toate cererile pentru o această zonă particulară către alte servere.

Înţelegerea interogărilor DNS

Clienţii utilizează serverele DNS pentru a găsi informaţii necesare lor. Cererea poate veni direct de la client sau de la o aplicaţie care rulează pe client. Clientul trimite un mesaj de interogare pentru serverul DNS care conţine un FQDN (fully qualified domain name - nume de domeniu complet calificat), un tip de interogare, cum este o înregistrare resursă specifică, pe care o cere clientul şi clasa pentru numele de domeniu, care de obicei este clasa IN (Internet). Următoarea figură descrie exemplul de reţea de la exemplu Un singur server DNS cu acces la Internet.

Figura 1. Un server DNS singur cu acces la Internet.



Să presupunem că gazda *dataentry* interoghează serverul DNS pentru ″graphics.mycompany.com″. Serverul DNS va utiliza datele lui de zonă şi răspunsul lui va fi adresa IP 10.1.1.253.

Acum să presupunem *dataentry* cere adresa IP a lui ″www.jkl.com.″. Această gazdă nu este în datele de zonă ale serverului DNS. Acum există două căi de urmat, recursivitate sau iterare. Dacă un server DNS este setat să utilizeze recursivitatea, atunci serverul poate întreba sau poate contacta alt server DNS în numele clientului ce a făcut cererea pentru a rezolva în totalitate problema numelui, după care trimite răspunsul înapoi la client. Dacă serverul DNS întreabă alt server DNS, serverul care face cererea va stoca răspunsul în memoria cache pentru a-l putea folosi ulterior la o asfel de cerere. Un client poate încerca să contacteze alte servere DNS în numele lui pentru a rezolva un nume. În acest proces, numit iteraţie, clientul utilizează cereri separate şi adiţionale bazate pe răspunsuri de referal primite de la servere.

Setarea domeniului DNS

DNS permite servirea de nume şi adrese într-o reţea intranet (internă). De asemenea, permite servirea de nume şi adrese pentru restul lumii, prin intermediul Internetului. Dacă doriţi să setaţi domenii pe Internet, trebuie să înregistraţi un nume de domeniu.

Dacă setaţi o reţea intranet, nu este necesar să înregistraţi un nume de domeniu pentru utilizarea internă. Înregistrarea sau nu a unui nume de intranet depinde de dorinţa dumneavoastră de a vă asigura ca nimeni altcineva să nu folosească numele în Internet, independent de utilizarea dumneavoastră internă. Înregistrând un nume, vă asiguraţi că dacă vreodată veţi dori să utilizaţi acest nume de domeniu în exterior nu veţi avea nici un fel de conflicte.

Înregistrările de domeniu pot fi făcute contactând direct un înregistrator autorizat de nume de domeniu sau prin furnizorii de servicii Internet (ISP). Unele ISP-uri oferă un serviciu pentru trimiterea în numele dumneavoastră a cererilor de înregistrare a numelui de domeniu. InterNIC (Internet Network Information Center)

păstrează un director cu toate înregistrările de nume de domeniu care sunt autorizate de ICANN (Iternet Corporation for Assigned Names and Numbers).

Există mai multe surse care furnizează informaţii despre înregistrarea şi pregătirea pentru găzduirea unui domeniu DNS. Pentru ajutor suplimentar consultaţi Alte informaţii privind DNS.

Actualizările dinamice

DHCP (Dynamic Host Configuration Protocol) este un standard TCP/IP care utilizează un server central pentru gestionarea adreselor IP şi altor detalii de configurare pentru o întreagă reţea. Un server DHCP răspunde la cererile clienţilor, asignând dinamic proprietăţi pentru acestea. DHCP vă permite să definiţi parametrii de configurare ai reţelei gazdă la o locaţie centrală şi automatizează configuraţia gazdei. Este adesea utilizată asignarea temporară de adrese IP pentru clienţii reţelelor care conţin mai mulţi clienţi decât numărul de adrese IP disponibile.

În trecut, toate datele DNS erau stocate în baze de date statice. Toate înregistrările de resurse DNS trebuiau să fie create şi menţinute de administrator. Acum, serverele DNS care rulează BIND 8 pot fi configurate pentru a accepta cererile de la alte surse pentru o actualizare dinamică a datelor de zonă.

Puteţi configura serverul dumneavoastră DHCP pentru a trimite cereri de actualizare la serverul DNS, ori de câte ori el asignează o nouă adresă la o gazdă. Această procesare automată reduce administrarea serverului DNS în reţelele care se extind şi modifică rapid TCP/IP-ul şi în reţelele unde gazdele schimbă locul frecvent. Când un client care utilizează DHCP primeşte o adresă IP, acele date sunt imediat trimise către serverul DNS. Utilizând această metodă, DNS poate continua rezolvarea cu succes a cererilor pentru gazdă, chiar dacă adresele lor IP se schimbă.

Puteţi configura DHCP pentru a actualiza înregistrări (A) de mapare adrese, înregistrări PTR sau ambele, în numele unui client. Înregistrarea A mapează un nume de gazdă maşină la adresa ei IP. Înregistrarea PTR mapează o adresă de maşină la numele ei de gazdă. Când se modifică o adresă a unui client, DHCP poate trimite automat o actualizare către serverul DNS pentru ca alte gazde din reţea să poată localiza clientul, prin interogările DNS, la noua lui adresă IP. Pentru fiecare înregistrare care este actualizată automat se va scrie o înregistrare TXT (text asociat) pentru a identifica că înregistrarea a fost scrisă de DHCP.
Notă: Dacă setaţi DHCP pentru a actualiza doar înregistrările PTR, trebuie să configuraţi DNS pentru a permite actualizările de la clienţi în aşa fel încât fiecare client poate să-şi facă actualizare la înregistrarea de tip A. Nu toţi clienţii DHCP îşi pot face actualizare la înregistrările lor de tip A. Consultaţi documentaţia pentru platforma clientului dumneavoastră înainte de alege această metodă.

Zonele dinamice sunt securizate prin crearea unei liste de surse autorizate cărora li se permite trimiterea actualizărilor. Puteţi defini surse autorizate utilizând adrese IP individuale, întregi subreţele, pachete care au

fost semnate utilizând o cheie partajată secretă (numită TSIG) sau orice combinaţie a acestor metode. DNS verifică dacă pachetele de cereri care vin, provin de la o sursă autorizată înainte de actualizarea înregistrărilor resursă.

Actualizările dinamice pot fi realizate între DNS şi DHCP pe un singur server iSeries(TM), între diferite servere iSeries sau între iSeries şi alte servere care pot face actualizări dinamice. Referiţi-vă la următoarele subiecte pentru mai multe informaţii despre configurarea actualizărilor dinamice pentru iSeries:

- Configurarea DNS pentru a primi actualizări dinamice
- Configurarea DHCP pentru a trimite actualizări dinamice
- API-ul de actualizare dinamică QTOBUPT este necesar pe serverele care trimit actualizări dinamice la DNS. Este instalat automat cu OS/400(R) Opţiunea 31, DNS.

Caracteristicile BIND 8

DNS a fost reproiectat pentru utilizarea BIND 8 pentru V5R1. Dacă nu aveţi instalat PASE, puteţi continua să configuraţi şi să rulaţi ediţiile anterioare ale serverului DNS, OS/400(R) bazate pe BIND 4.9.3. Cerinţele sistemului DNS vă explică ce aveţi nevoie pentru a rula serverul DNS bazat pe BIND 8, pe sistemul dumneavoastră iSeries(TM). Utilizând noul DNS beneficiaţi de avantajele următoarelor caracteristici:

Rularea mai multor servere DNS pe un singur sistem iSeries
În ediţiile anterioare doar un singur server DNS putea fi configurat. Acum puteţi configura servere sau instanţe DNS multiple. Aceasta vă permite să setaţi împărţiri logice între servere. Când creaţi instanţe multiple trebuie să definiţi explicit pentru fiecare instanţă adresele IP ale interfeţei ascultă-la. Două instaţe DNS nu pot asculta la aceeaşi interfaţă.

O aplicaţie practică de servere multiple reprezintă un DNS împărţit, unde un server este cu autoritate pentru o reţea internă şi un server secundar este utilizat pentru cereri externe. Referiţi-vă la exemplul Împărţirea DNS-ului peste firewall pentru mai multe informaţii despre împărţirea DNS-ului.

Înaintarea condiţionată
Înaintarea condiţionată vă permite să configuraţi serverul dumneavoastră DNS pentru un reglaj mai fin al preferinţelor dumneavoastră de înaintare (forwarding). Puteţi seta un server să înainteze (forward) toate cererile pentru care nu ştie răspunsul. Aţi putea seta înaintarea la un nivel global, dar să adăugaţi excepţiile pentru domeniile la care vreţi să forţaţi o rezoluţie iterativă normală. Sau puteţi seta rezoluţia iterativă normală la nivel global, după care forţaţi înaintarea la anumite domenii.

Actualizările dinamice sigure
DHCP şi alte surse autorizate pot trimite actualizările dinamice ale înregistrării resursă utilizând TSIG şi/sau autorizaţia adresei IP a sursei. Aceasta reduce necesitatea pentru actualizări manuale ale datelor de zonă în timp ce ne asigurăm că doar sursele autorizate sunt utilizate pentru actualizări.

Pentru mai multe informaţii despre actualizările dinamice, consultaţi Actualizările dinamice. Pentru mai multe informaţii despre autorizarea actualizărilor din surse externe, consultaţi Planificarea măsurilor de securitate.

NOTIFY
Când NOTIFY este activată, funcţia DNS NOTIFY este activată ori de câte ori datele de zonă sunt actualizate pe serverul primar. Serverul primar trimite un mesaj către toate serverele secundare cunoscute indicând că şi-a modificat datele. După aceea, serverele secundare pot răspunde cu o cerere de transfer zonă pentru actualizarea datelor de zonă. Aceasta ajută la îmbunătăţirea suportului de server secundar prin păstrarea unui rezerve a datelor de zonă curente.

Transferuri de zone (IXFR şi AXFR)
În trecut, ori de câte ori serverele secundare trebuia să încarce datele de zonă, ele trebuia să încarce întregul set de date într-un transfer zonă întreagă (AXFR). BIND 8 suportă o nouă metodă de transfer zonă: transfer zonă incremental IXFR. IXFR este o modalitate prin care alte servere pot transfera doar datele schimbate, în loc de a transfera întreaga zonă.

Când serverul primar a fost activat, datelor modificate li se asignează un steguleţ pentru a indica faptul că a apărut o schimbare. Când un server secundar cere actualizarea unei zone într-un mod IXFR, serverul va trimite doar datele noi. IXFR este util mai ales atunci când o zonă este actualizată dinamic şi reduce încărcarea traficului prin trimiterea unei cantităţi mici de date.
Notă: Atât serverul primar, cât şi cel secundar, trebuie să fie activate-IXFR pentru a putea utiliza această opţiune.

Înregistrările resursă DNS

O bază de date a zonei DNS constituie o colecţie de înregistrări resursă. Fiecare înregistrare resursă specifică informaţia despre un obiect paticular. Spre exemplu, înregistrările de mapare adresă (A) mapează un nume gazdă la o adresă IP şi înregistrările PTR mapează o adresă IP la un nume gazdă. Serverul utilizează aceste înregistrări pentru a răspunde la cereri pentru gazdele din zona lui. Pentru mai multe informaţii utilizaţi tabelul de mai jos pentru a vizualiza înregistrările resursă DNS.

Înregistrare resursă	Abreviere	Descriere
Înregistrări de mapare adrese	A	Înregistrările A specifică adresa IP a gazdei. Înregistrările A sunt utilizate pentru a rezolva o cerere de adresă IP pentru un nume de domeniu specific. Acest tip de înregistrare este definit în RFC 1035.
Înregistrări baze de date sistem de fişiere Andrew	AFSDB	Înregistrarea AFSDB specifică adresa AFS sau DCE a obiectului. Înregistrările AFSDB sunt utilizate ca şi înregistrările A pentru maparea unui nume de domeniu la adresa lui AFSDB; sau pentru maparea din numele domeniului unei celule la serverele de nume autentificate pentru acea celulă. Acest tip de înregistrări este definit în RFC 1183.
Înregistrări nume canonic	CNAME	Înregistrările CNAME specifică numele real de domeniu al obiectului. Când DNS interoghează un nume cu alias şi găseşte o înregistrare CNAME indicând spre numele canonic, atunci el va interoga acel nume de domeniu canonic. Acest tip de înregistrare este definit în RFC 1035.
Înregistrări informaţie gazdă	HINFO	Înregistrările HINFO specifică informaţia generală despre o maşină gazdă. CPU standard şi numele sistemului de operare sunt definite în Assigned Numberers RFC 1700. Dar, utilizarea numerelor standard nu este necesară. Acest tip de înregistrare este definit în RFC 1035.
Înregistrări ISDN (Integrated Services Digital Network)	ISDN	Înregistrarea ISDN specifică adresa acestui obiect. Această înregistrare mapează un nume gazdă la adresa ISDN. Ele sunt utilizate doar în reţelele ISDN. Acest tip de înregistrări este definit în RFC 1183.

Înregistrare resursă	Abreviere	Descriere
Înregistrări Adresă IP Versiunea 6	AAAA	Înregistrarea AAAA specifică adresa pe 128 de biţi a unei gazde. Înregistrările AAAA sunt utilizate ca înregistrările A pentru maparea unui nume gazdă la adresa ei IP. Utilizaţi înregistrările AAAA pentru suportul adreselor IP versiunea 6, care nu se portivesc cu formatul standard de înregistrare A. Acest tip de înregistrare este definit în RFC 1886.
Înregistrări Locaţie	LOC	Înregistrarea LOC specifică locaţia fizică a reţelelor componente. Aceste înregistrări ar putea fi utilizate de aplicaţii la evaluarea eficienţei reţelei sau la maparea reţelei fizice. Acest tip de înregistrare este definit în RFC 1876.
Înregistrări Mail Exchanger	MX	Înregistrarea MX defineşte o gazdă de transfer poştă (mail exchanger) pentru poşta trimisă la acest domeniu. Aceste înregistrări sunt utilizate de SMTP pentru a localiza gazdele care vor procesa sau vor expedia mail pentru acest domaniu, împreună cu valorile pentru fiecare gazdă de transferare poştă (mail exchanger). Fiecare gazdă mail exchanger trebuie să aibă o înregistrare A corespunzătoare într-o zonă validă. Acest tip de înregistrare este definit în RFC 1035.
Înregistrări Grup mail	MG	Înregistrarea MG specifică numele de domeniu al grupului de mail. Acest tip de înregistrare este definit în RFC 1035.
Înregistrări căsuţă poştală	MB	Înregistrarea MB specifică numele domeniului care conţine căsuţa poştală (mailbox) pentru acest obiect. Poşta trimisă la domeniu va fi direcţionată la gazda specificată în înregistrarea MB. Acest tip de înregistrare este definit în RFC 1035.
Înregistrare Informaţii căsuţă poştală	MINFO	Înregistrarea MINFO specifică căsuţa poştală care ar trebui să primească mesaje sau erori pentru acest obiect. Înregistrarea MINFO este mult mai frecvent utilizată pentru liste de destinaţii decât pentru o singură căsuţă poştală. Acest tip de înregistrare este definit în RFC 1035.
Înregistrări redenumire căsuţă poştală	MR	Înregistrarea MR specifică un nou nume de domeniu pentru o căsuţă poştală. Utilizaţi înregistrarea MR pentru expedierea către un utilizator care şi-a schimbat căsuţa poştală. Acest tip de înregistrare este definit în RFC 1035.

Înregistrare resursă	Abreviere	Descriere
Înregistrări Server de nume	NS	Înregistrarea NS specifică un server de nume cu autoritate pentru această gazdă. Acest tip de înregistrare este definit în RFC 1035.
Înregistrări NSAP (Network Service Access Protocol)	NSAP	Înregistrarea NSAP specifică adresa unei resurse NSAP. Înregistrările NSAP sunt utilizate pentru maparea numelor de domeniu la adresele NSAP. Acest tip de înregistrare este definit în RFC 1706.
Înregistrări Cheie publică	KEY	Înregistrarea KEY specifică o cheie publică care este asociată cu un nume DNS. Cheia poate fi pentru o zonă, un utilizator sau pentru o gazdă. Acest tip de înregistrare este definit în RFC 2065.
Înregistrări Persoană responsabilă	RP	Înregistrarea RP specifică adresa internet de mail şi descrierea persoanei responsabilă pentru această zonă sau gazdă. Acest tip de înregistrări este definit în RFC 1183.
Înregistrări Pointer căutare inversă	PTR	Înregistrarea PTR specifică numele de domeniu al unei gazde pentru care vreţi definită o înregistrare PTR. Înregistrările PTR permit căutarea numelui gazdei, fiind dată o adresă IP. Acest tip de înregistrare este definit în RFC 1035.
Înregistrări Prin rută (Route Through)	RT	Înregistrarea RT specifică un nume domeniu gazdă care poate acţiona ca un expeditor de pachete IP pentru această gazdă. Acest tip de înregistrări este definit în RFC 1183.
Înregistrări Început autoritate	SOA	Înregistrarea SOA specifică că acest server este cu autoritate pentru această zonă. Un server cu autoritate este cea mai bună sursă de date dintr-o zonă. Înregistrarea SOA conţine informaţii generale despre zonele şi regulile de reîncărcare pentru serverele secundare. Poate exista doar o singură înregistrare per zonă. Acest tip de înregistrare este definit în RFC 1035.

Înregistrare resursă	Abreviere	Descriere
Înregistrări Text	TXT	Înregistrarea TXT specifică mai multe şiruri de text, fiecare având lungimea de până la 255 de caractere, de asociat cu un nume de domeniu. Înregistrările TXT pot fi utilizate împreună cu înregistrările RP pentru a furniza informaţii despre cine este responsabil pentru o zonă. Acest tip de înregistrare este definit în RFC 1035. Înregistrările TXT sunt utilizate de serverele DHCP iSeries pentru actualizări dinamice. Serverul DHCP scrie o înregistrare TXT asociată pentru fiecare actualizare de înregistrare PTR şi A făcută de serverul DHCP. Înregistrările DHCP vor avea prefixul de **AS400DHCP:**.
Înregistrările Servicii bine cunoscute	WKS	Înregistrarea WKS specifică serviciile bine-cunoscute suportate de acest obiect. De obicei, înregistrările WKS indică dacă protocolul tcp sau udp sau ambele sunt suportate pentru această adresă. Acest tip de înregistrare este definit în RFC 1035.
Înregistrări Mapare adresă X.400	PX	Înregistrările PX sunt un pointer la informaţiile de mapare X.400/RFC 822. Acest tip de înregistrare este definit în RFC 1664.
Înregistrări Mapare adresă X25	X25	Înregistrarea X25 specifică adresa unei resurse X25. Această înregistrare mapează un nume gazdă la adresa PSDN. Ele sunt utilizate doar în reţelele X25. Acest tip de înregistrări este definit în RFC 1183.

Înregistrările Mail şi MX

Înregistrările Mail şi MX sunt utilizate de programele de rutare poştă, cum este SMTP. Referiţi-vă la tabelul Înregistrările resursă DNS pentru mai multe informaţii despre tipurile de înregistrări mail suportate de serverul DNS iSeries(TM).

DNS include informaţii pentru trimiterea poştei electronice prin utilizarea informaţiei de 'mail exchanger'. Dacă reţeaua utilizează DNS, o aplicaţie SMTP nu livrează pur şi simplu poştă adresată gazdei TEST.IBM.COM, prin deschiderea unei conexiuni TCP la TEST.IBM.COM. Mai întâi SMTP interoghează serverul DNS pentru a afla care din serverele gazdă pot fi utilizate pentru a livra mesaje.

Livrarea poştei către o adresă specificată

Serverele DNS utilizează înregistrări resursă care sunt cunoscute ca înregistrări 'mail exchanger' (MX). Înregistrările MX mapează un domeniu sau un nume domeniu la o valoare de prefrerinţă şi nume gazdă. În general, înregistrările MX sunt utilizate pentru a indica că o gazdă este utilizată pentru a procesa mail pentru altă gazdă. Înregistrările sunt, de asemenea, utilizate pentru a indica o altă gazdă care să încerce livrarea poştei, dacă prima gazdă nu reuşeşte. Cu alte cuvinte, ele permit ca mail-ul adresat unei gazde să fie livrat unei alte gazde.

Pot exista multiple înregistrări MX pentru acelaşi nume gazdă sau domeniu. Când există mai multe înregistrări MX pentru acelaşi domeniu sau gazdă, valoarea de preferinţă a fiecărei înregistrări determină ordinea în care ele sunt încercate. Valoare de preferinţă cea mai mică corespunde înregistrării celei mai preferate şi care va fi încercată prima. Când gazda cea mai preferată nu poate fi contactată, aplicaţia de trimitere mail încearcă să contacteze următoarea gazdă MX mai puţin preferată. Administratorul de domeniu sau cel care creează înregistrarea este cel care setează valoarea de preferinţă.

Un server DNS poate răspunde cu o listă goală de înregistrări resursă MX când numele se află în autoritatea serverului DNS, dar nu are asignată nici o înregistrare MX. Când apare această problemă, aplicaţia de trimitere mail poate încerca să stabilească o conexiune directă cu gazda destinaţie. **Notă:** Nu se recomandă utilizarea unui caracter de înlocuire (exemplu: *.mycompany.com) în înregistrările MX pentru un domeniu.

Exemplu: Înregistrarea MX pentru o gazdă
În următoarele exemple, sistemul ar trebui, după preferinţă, să livreze mail pentru fsc5.test.ibm.com chiar către gazdă. Dacă gazda nu poate fi contactată, sistemul poate livra mail-ul către psfred.test.ibm.com sau către mvs.test.ibm.com (dacă psfred.test.ibm.com de asemenea nu poate fi contactat). Acesta este un exemplu care arată cum arată aceste înregistrări 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
```

Planificarea DNS

DNS oferă o varietate de soluţii. Înainte de a configura DNS, este important să planificaţi cum va funcţiona acesta în reţeaua dumneavoastră. Pentru a implementa DNS-ul ar trebui să consultaţi subiecte cum ar fi cele referitoare la structura, performanţa şi securitatea reţelei. Luaţi în considerare subiectele de mai jos pentru planificarea necesităţilor privind DNS-ul.

Determinarea autorizărilor DNS
Există cerinţe speciale de autorizări pentru administratorul DNS. De asemenea, ar trebui să luaţi în considerare implicaţiile autorizării privind securitatea. Acest subiect prezintă cerinţele.

Determinarea structurii domeniului
Dacă setaţi un domeniu pentru prima dată, ar trebui să elaboraţi un plan pentru cerere şi întreţinere înainte de a crea zonele.

Planificarea măsurilor de securitate
DNS furnizează opţiuni de securitate pentru a limita accesul din afara serverului dumneavoastră. Acest subiect explică opţiunile şi modul în care puteţi să controlaţi accesul.

Determinarea autorizărilor DNS

Când setaţi DNS pentru activare, ar trebui să va luaţi măsuri de siguranţă pentru a vă proteja configuraţia. Trebuie să stabiliţi care dintre utilizatori sunt autorizaţi să facă modificări în configuraţie.

Se cere un nivel minim de autorizare pentru a permite administratorului dumneavoastră pe iSeries(TM) să configureze şi să administreze serverul DNS. Acordarea accesului pentru toate obiectele asigură că administratorul este capabil pentru realizarea activităţilor administrative pentru DNS. Se recomandă ca utilizatorii care vor configura DNS să beneficieze să aibă acces de responsabil (officer) de securitate cu autorizarea pentru toate obiectele (*ALLOBJ). Utilizaţi Navigator iSeries pentru a autoriza utilizatorii. Dacă aveţi nevoie de mai multe informaţii, citiţi **Acordarea autorizării către administratorul DNS** din ajutorul online DNS.

Notă: Dacă un profil administrator nu are autorizare completă, trebuie să i se acorde accesul corespunzător şi autorizare către toate directoarele DNS şi la fişierele de configurare asociate.

Determinarea structurii domeniului

Este important să determinaţi cum veţi diviza domeniul sau subdomeniile dumneavoastră în zone, cum să satisfaceţi cel mai bine cererile reţelei, să accesaţi Internetul şi cum să trataţi cu firewall-urile. Aceşti factori pot fi complexi şi trebuie trataţi caz-după-caz. Pentru sfaturi mai amănunţite şi mai în profunzime consultaţi surse de autoritate, cum este cartea O'Reilly DNS and BIND.

Dacă configuraţi o zonă DNS ca o zonă dinamică, nu puteţi modifica datele de zonă în timp ce serverul rulează. Făcând aşa ar putea cauza interferenţa cu actualizările dinamice care vin. Dacă trebuie să faceţi actualizare manuală, opriţi serverul, faceţi modificările, după care reporniţi serverul. Actualizările dinamice trimise către un server DNS care este oprit, nu vor fi niciodată executate. Din acest motiv, veţi vrea să configuraţi o zonă dinamică şi o zonă statică separat. Aţi putea face asta prin crearea unor zone total separate sau prin definirea unui nou subdomeniu, cum este dynamic.mycompany.com, pentru acei clienţi care vor fi întreţinuţi dinamic.

DNS iSeries(TM) furnizează o interfaţă grafică pentru configurarea serverelor. În unele cazuri, interfaţa utilizează terminologii sau concepte care pot fi prezentate diferit în alte surse. Dacă vă referiţi la alte surse de informare când plănuiţi configurarea serverului dumneavoastră DNS, vă poate fi de ajutor să ţineţi minte următoarelor informaţii:

- Toate zonele şi obiectele definite într-un server sunt organizate în folderele **Zone de căutare înainte** şi **Zone de căutare inversă**. Zonele de căutare înainte sunt zone care sunt utilizate pentru maparea numelor domeniu la adresele IP, ca şi înregistrările A. Zonele de căutare inversă sunt zone care sunt utilizate pentru maparea adresei IP la numele de domeniu, ca şi înregistrările PTR.
- DNS iSeries se referă la **zone primare** şi **zone secundare**. Acestea sunt uneori referite ca zone master şi slave în altă documentaţie BIND.
- Interfaţa utilizează **subzonele**, la care se referă unele surse ca subdomenii. O zonă copil este o subzonă pentru care aţi delegat responsabilitatea către unu sau mai multe servere de nume.

Planificarea măsurilor de securitate

Securizarea serverul dumneavoastră DNS este esenţială. Pe lângă măsurile de securitate de mai jos, securitatea DNS şi securitatea iSeries(TM) sunt acoperite de o varietate de surse, incluzând IBM(R) Secureway: iSeries şi Internet-ul din Centrul de informare. Cartea DNS and BIND de asemenea acoperă subiectul despre securitatea legată de DNS.

Listele de potrivire adresă (AML)
DNS utilizează listele de potrivire adresă pentru a permite sau pentru a nega accesul entităţilor din afară către anumite funcţii DNS. Acestea pot include adrese IP specifice, o subreţea (utilizând un prefix IP) sau utilizarea de chei TSIG (Transaction Signature). Într-o listă puteţi defini o listă de entităţi la care vreţi să acordaţi sau să negaţi accesul. Dacă vreţi sa refolosiţi o listă AML, puteţi salva lista ca o lista ACL (Access Control List). După care ori de câte ori aveţi nevoie de listă puteţi apela lista ACL şi va fi încărcată toată lista.

Ordinea elementelor din lista adrese de potrivire
Primul element dintr-o listă care dă o adresă care se potriveşte, va fi utilizat. Spre exemplu, pentru a permite toate adresele din reţeaua 10.1.1.x, exceptând 10.1.1.5, elementele listei trebuie să fie în ordinea (!10.1.1.5; 10.1.1/24). În acest caz, adresa 10.1.1.5 va fi comparată cu primul element şi va fi imediat refuzată.

Dacă elementele erau inversate(10.1.1/24; !10.1.1.5), adresei IP 10.1.1.5 i s-ar permite accesul deoarece serverul o va compara cu primul element, care se potriveşte şi o va accepta fără să mai verifice restul de reguli.

Opţiunea de control acces
DNS vă permite să setaţi limitări, cum ar fi cele referitoare la cine poate trimite actualizări dinamice către server, să ceară date şi să ceară transferuri de zonă. Puteţi utiliza listele de control acces pentru a restricţiona accesul la server pentru următoarele opţiuni:

permitere-actualizare
Pentru ca serverul dumneavoastră DNS să accepte actualizări dinamice de la orice sursă din afară, trebuie să activaţi opţiunea permitere-actualizare.

permitere-interogare
Specifică care din gazde au voie să interogheze acest server. Dacă nu se specifică, implicit se va acorda dreptul tuturor gazdelor să facă interogări către server.

permitere-transfer
Specifică cărora dintre gazde li se acordă dreptul să primească tranferuri de zonă de la server. Dacă nu se specifică, implicit se va permite transferuri de la toate gazdele.

permitere-recursivitate
Specifică căror gazde li se permite să facă cereri recursive prin acest server. Dacă nu se specifică, implicit se permit cereri recursive de la toate gazdele.

gaură neagră
Specifică o listă de adrese de la care serverul nu va accepta interogări şi nu le va utiliza ca să rezolve o interogare. Interogările de la aceste adrese nu vor fi satisfăcute.

Cerinţele sistemului DNS

Opţiunea DNS (Opţiunea 31) nu se instalează automat cu sistemul de operare de bază. Trebuie să selectaţi DNS pentru instalare. Noul server DNS adăugat la V5R1 se bazează pe implementarea standard industrială de DNS cunoscută ca BIND 8. Serverele anterioare DNS OS/400(R) se bazau pe BIND 4.9.3 şi încă sunt disponibile pentru V5R1.

O dată ce s-a instalat DNS, veţi fi configurat implicit să setaţi un singur server DNS, care utilizează capabilităţile serverului DNS bazat pe BIND 4.9.3, care erau disponibile în ediţiile anterioare. Dacă vreţi să rulaţi unul sau mai multe servere DNS utilizând BIND 8, trebuie să instalaţi Portable Application Solutions Environment (PASE). PASE este Opţiunea 33 a lui SS1. O dată ce aţi instalat PASE, Navigator iSeries va trata automat configurarea implementării versiunii corecte de BIND.

Dacă nu utilizaţi PASE, nu veţi putea beneficia de toate avantajele caracteristicilor BIND 8. Dacă nu utilizaţi PASE, încă mai puteţi rula acelaşi server DNS bazat pe BIND 4.9.3, care a fost disponibil în ediţiile anterioare. Referiţi-vă la subiectul Centrului de informare DNS V4R5

(aproximativ 357 KB) pentru documentaţia BIND 4.9.3.

Dacă vreţi să configuraţi un server DHCP pe un alt sistem iSeries pentru a trimite actualizări la acest server DNS, trebuie instalată Opţiunea 31 şi pe acest iSeries cu DHCP. Serverul DHCP utilizează interfeţele de programare furnizate de Opţiunea 31 pentru a realiza actualizări dinamice.

Pentru a determina dacă este instalat DNS, parcurgeţi următorii paşi:

1. La linia de comandă introduceţi **GO LICPGM** şi apăsaţi **Enter**.
2. Introduceţi **10** (Afişare programe instalate) şi apăsaţi **Enter**.
3. Apăsaţi Page down până ajungeţi la **5722SS1 OS/400 - Domain Name System** (SS1 Option 31) Dacă DNS este instalat cu succes, **Starea instalare** va fi ***compatible**, aşa cum se arată aici:

```
PgmLic     Starea instalare     Descriere
5722SS1    *COMPATIBLE          OS/400 - Domain Name System
```

4. Apăsaţi **F3** pentru a ieşi din ecran.

Pentru a instala DNS, parcurgeţi următorii paşi:

1. La linia de comandă introduceţi **GO LICPGM** şi apăsaţi **Enter**.
2. Introduceţi **11** (Instalare programe licenţiate) şi apăsaţi **Enter**.
3. Introduceţi **1** (Instalare) în câmpul **Opţiune** de lângă OS/400 - Domain Name System şi apăsaţi **Enter**.
4. Apăsaţi **Enter** din nou pentru a confirma instalarea.

Configurarea DNS

Înainte de a lucra cu configuraţia serverului dumneavoastră DNS, consultaţi cerinţele sistemului DNS pentru a instala componentele DNS necesare. Următoarele sub-subiecte furnizează indicaţii pentru configurarea serverului dumneavoastră DNS:

Accesarea DNS din Navigator iSeries
Instrucţiuni pentru accesarea DNS din Navigator iSeries.

Configurarea serverelor de nume
DNS vă permite să creaţi instanţe multiple de server de nume. Acest subiect furnizează instrucţiuni pentru configurarea unui server de nume.

Configurarea DNS pentru a primi actualizări dinamice
Serverele DNS care rulează BIND 8 pot fi configurate pentru a accepta cererile de la alte surse pentru a face actualizare dinamică la datele de zonă. Acest subiect furnizează instrucţiuni pentru configurarea opţiunii de permitere-actualizare pentru ca DNS să poată recepţiona actualizări dinamice.

Importarea fişierelor DNS
DNS poate importa fişiere existente de date de zonă. Urmăriţi aceste proceduri de economisire a timpului pentru crearea unei noi zone dintr-un fişier de configurare existent.

Accesarea externă a datelor DNS
Când creaţi datele de zonă DNS, serverul dumneavoastră va putea rezolva cererile către acea zonă. Acest subiect explică cum se configurează DNS pentru a rezolva cererile din afara domeniului.

Accesarea DNS în Navigator iSeries

Următoarele instrucţiuni vă vor ghida prin interfaţa de configurare DNS din Navigator iSeries. Dacă utilizaţi PASE, veţi putea să configuraţi serverele DNS bazate pe BIND 8. Dacă nu utilizaţi PASE, încă mai puteţi rula serverul DNS pe BIND 4.9.3, care era disponibil în ediţiile anterioare. Referiţi-vă la subiectul DNS V4R5 din Centrul de informare

(aproximativ 62 pagini) pentru informaţiile privind serverul DNS pe BIND 4.9.3.

Dacă configuraţi DNS pentru prima dată, parcurgeţi următorii paşi:

1. În **Navigator iSeries**, expandaţi **serverul iSeries** —> **Reţea** —> **Servere** —> .
2. Faceţi clic dreapta pe **DNS** şi selectaţi **Configuraţie nouă**.

Dacă aveţi o versiune anterioară V5R1 de server DNS configurată, parcurgeţi următorii paşi:

1. În **Navigator iSeries**, expandaţi **serverul iSeries** —> **Reţea** —> **Servere** —> .
2. În panoul din dreapta, faceţi dublu clic pe serverul DNS pentru a deschide fereastra **Configurare DNS**.
3. Dacă utilizaţi PASE, veţi putea alege opţiunea de migrare de la configuraţia dumneavoastră existentă către implementarea BIND 8. Oricum, odată de aţi migrat către BIND 8, nu vă puteţi întoarce la versiunea anterioară BIND 4.9.3. Dacă sunteţi nesigur selectaţi **Nu**. Dacă vreţi să migraţi selectaţi **Da**.
4. Pentru a migra serverul dumneavoastră DNS către BIND 8 în orice moment, faceţi clic dreapta **DNS** din panoul stâng şi selectaţi **Migrare la versiunea 8**.

Configurarea serverelor de nume

Serverul DNS iSeries(TM) bazat pe BIND 8 suportă instanţe multiple de servere de nume. Task-ul de mai jos vă va ghida prin procesul de creare a unei singure instanţe server de nume, incluzând proprietăţile şi zonele lui.

1. Crearea unei instanţe server de nume
   Utilizaţi vrăjitorul **Configurare DNS nou** pentru a defini o instanţă server DNS.
2. Editaţi proprietăţile serverului DNS
   Definiţi proprietăţile globale pentru noile dumneavoastră instanţe server.
3. Configuraţi zonele pe un server de nume
   Creaţi zonele şi datele de zonă pentru a popula serverului dumneavoastră de nume.

Dacă vreţi să creaţi instanţe multiple, repetaţi procedura de mai sus pentru toate instanţele pe care vreţi să le creaţi. Puteţi specifica proprietăţi independente, cum sunt niveluri de depanare şi valori de pornire automată, pentru fiecare instanţă server de nume. Când creaţi o nouă instanţă sunt create fişierele separate de configurare. Pentru mai multe informaţii despre fişierele de configurare, consultaţi Întreţinerea fişierelor de configurare DNS.

Crearea unei instanţe server de nume

Pentru a porni vrăjitorul **Configurare DNS nou**, parcurgeţi următorii paşi:

1. În **Navigator iSeries**, expandaţi **serverul iSeries(TM)** —> **Reţea** —> **Servere** —> **DNS**.
2. În panoul din stânga, faceţi clic dreapta pe **DNS** şi selectaţi **Server de nume nou...**
3. Vrăjitorul vă va ghida în procesul de configurare.

Vrăjitorul va cere să introduceţi următoarele:

Nume server DNS: Introduceţi un nume pentru serverul dumneavoastră DNS. Numele poate avea până la 5 caractere şi trebuie să înceapă cu un caracter alfabetic. Dacă creaţi servere multiple, fiecare trebuie să aibă un nume unic. Acest nume este referit ca nume ″instanţă″ server DNS în alte arii ale sistemului.

Adresele IP de ascultare: Două servere DNS nu pot asculta la aceeaşi adresă IP. Setarea implicită este de a asculta toate adresele IP. Dacă creaţi instanţe server adiţionale, nici una din ele nu pot fi configurate pentru a asculta toate adresele. Trebuie să specificaţi adresa IP pentru fiecare server.

Servere rădăcină: Puteţi încărca lista serverelor rădăcină (root) Internet implicite sau puteţi specifica serverele dumneavoastră rădăcină, cum sunt serverele rădăcină interne pentru o reţea intranet.
Notă: Ar trebui să consideraţi doar încărcarea serverelor rădăcină Internet implicite dacă vă aflaţi pe Internet şi aşteptaţi ca serverul dumneavoastră DNS să fie capabil să rezolve toate numele Internet.

Pornire server: Puteţi specifica dacă serverul ar trebui pornit automat la pornirea TCP/IP. Cand lucraţi pe mai multe servere, instanţele individuale pot fi pornite şi oprite independent una de cealaltă.

Ce să faceţi în continuare: Editaţi proprietăţile serverului DNS.

Editarea proprietăţilor serverului DNS

După ce creaţi un server de nume, puteţi edita proprietăţile, cum sunt permite-actualizare şi nivelurile de depanare. Aceste opţiuni se vor aplica doar instanţei serverului pe care-l modificaţi. Pentru a edita proprietăţile instanţei serverului DNS, parcurgeţi următorii paşi:

1. În **Navigator iSeries**, expandaţi **serverul iSeries(TM)** —> **Reţea** —> **Servere** —> **DNS**.
2. În panoul din dreapta, faceţi clic dreapta pe **serverul DNS** şi selectaţi **Configurare**.
3. Faceţi clic dreapta **serverul DNS** şi selectaţi **Proprietăţi**.

Ce să faceţi în continuare: Configuraţi zonele pe serverul dumneavoastră de nume..

Configurarea zonelor pe un server de nume

O dată ce aţi creat serverul dumneavoastră de nume, întoarceţi-vă în fereastra principală din **Navigator iSeries**. Serverul dumneavoastră va fi afişat în panoul din dreapta. Pentru a configura zonele de pe serverul dumneavoastră, faceţi clic dreapta pe numele serverului şi selectaţi **Configurare**. Va fi afişată fereastra **Configurare DNS**.

Toate zonele sunt configurate folosind vrăjitori. Creaţi **Zona de căutare înainte** sau **Zona de căutare inversă** prin clic dreapta pe folderul corespunzător. Vor fi afişate opţiunile pentru acel tip de zonă. Selectaţi tipul de zonă pe care doriţi să o creaţi pentru a porni vrăjitorul.

Pentru descrierea tipurilor de obiecte pe care le puteţi crea în DNS V5R1, consultaţi Întelegerea serverului DNS.

O dată ce aţi configurat zona dumneavoastră, vă puteţi referi la aceste subiecte pentru mai multe informaţii despre configurare.

Configurarea unei zone pentru a accepta actualizări dinamice.
Actualizările dinamice permit surselor autorizate să trimită înregistrări resursă pentru a face actualizarea datelor de zonă. Aceasta poate reduce necesitatea pentru modificarea manuală a datelor de zonă.

Importarea datelor de zonă
Dacă aveţi un fişier existent de date de zonă de la alt server DNS, îl puteţi încărca pe noul dumneavoastră server.

Accesarea datelor externe DNS
Puteţi să configuraţi serverul dumneavoastră pentru a rezolva interogările de informaţii din afara datelor lui de zonă pe care le conţine. Puteţi înainta cereri către alte servere cu autoritate sau să încărcaţi servere rădăcină (root) pentru a ajuta la rezolvarea interogărilor.

Configurarea DNS pentru a primi actualizări dinamice

Când creaţi zone dinamice ar trebui să luaţi în considerare structura reţelei dumneavoastră. Dacă părţi din domeniu dumneavoastră încă mai cer actualizări manuale, poate veţi vrea să setaţi separat zone statice şi zone dinamice. Dacă trebuie să faceţi actualizare manuală la o zonă dinamică, trebuie să opriţi serverul zonei dinamice şi să-l reporniţi după ce aţi terminat de făcut actualizările. Oprirea serverului îl forţează pe acesta să sincronizeze toate actualizările dinamice care s-au făcut de când serverul a încărcat datele lui de zonă din baza de date zone. Dacă nu aţi oprit serverul, veţi pierde toate actualizările dinamice care s-au făcut de la pornirea serverului. Oricum, oprirea serverului pentru a face actualizare manuală semnifică, că aţi putea pierde actualizările dinamice, care sunt trimise în timp ce serverul este oprit.

DNS indică faptul că o zona este dinamică atunci când obiectele sunt definite în procedura permitere-actualizare. Pentru a configura opţiunea permitere-actualizare, parcurgeţi următorii paşi:

1. În **Navigator iSeries**, expandaţi **serverul iSeries** —> **Reţea** —> **Servere** —> .
2. În panoul din dreapta, faceţi clic dreapta pe **serverul DNS** şi selectaţi **Configurare**.
3. În fereastra **Configurare DNS**, expandaţi **Zonă de căutare înainte** sau **Zonă de căutare inversă**.
4. Faceţi clic dreapta pe zona primară pe care vreţi să o editaţi şi selectaţi **Proprietăţi**.
5. În pagina **Proprietăţi zonă primară**, faceţi clic pe fişa **Opţiuni**.
6. În pagina **Opţiuni**, expandaţi **Control acces** —> **permitere-actualizare**.
7. DNS utilizează o listă de potrivire adrese pentru a verifica actualizările autorizate. Pentru a adăuga un obiect la lista de potrivire adrese, selectaţi un tip de element din listă şi faceţi clic pe **Adăugare...**. Puteţi adăuga o adresă IP, un prefix IP, o listă de control acces sau o cheie.
8. Când aţi terminat actualizarea listei daţi clic pe **OK** pentru a închide pagina **Opţiuni**.

Dacă setaţi un DNS să primească actualizări dinamice de la serverul DHCP iSeries, consultaţi Configurarea DHCP pntru a trimite actualizări dinamice.

Importarea fişierelor DNS

Puteţi crea o zonă primară prin importarea unui fişier date de zonă sau prin convertirea unor tabele gazdă existente. Referiţi-vă la *Convertirea tabelelor gazdă* în subiectul DNS V4R5 din Centrul de informare

(aproximativ 357 KB) pentru a crea datele de zonă din tabelul gazdă.

Puteţi importa orice fişier care este un fişier de configurare a unei zone valide bazat pe sintaxa BIND. Fişierul ar trebui localizat într-un director IFS. Când este importat, DNS va verifica dacă este un fişier date de zonă valid şi îl adaugă la fişierul NAMED.CONF pentru această instanţă de server.

Pentru a importa un fişier zonă, parcurgeţi următorii paşi:

1. În **Navigator iSeries**, expandaţi **serverul iSeries(TM)** —> **Reţea** —> **Servere** —> **DNS**.
2. În panoul din dreapta, faceţi dublu-clic pe instanţa server DNS în care vreţi să importaţi zona.
3. În panoul din stânga, faceţi clic dreapta pe serverul **DNS** şi selectaţi **Importare zonă**.
4. Urmăriţi instrucţiunile vrăjitorului pentru a importa zona primară.

Validarea înregistrării

Funcţia de importare domeniu date citeşte şi validează fiecare înregistrare a fişierului ce se importă. După terminarea funcţiei de importare de date de domeniu, oricare din înregistrările în eroare pot fi examinate individual pe pagina de proprietăţi **Alte înregistrări** a zonei importate.

- **Notă:**
- Importarea unui domeniu primar mare poate dura câteva minute.
- Funcţia de importare domeniu date nu suportă directiva $include. Procesul de verificare validitate a importării datelor de domeniu identifică liniile care conţin directiva $include ca linii în eroare.

Accesarea datelor externe DNS

Serverele rădăcină (root) sunt critice la funcţionarea unui server DNS care este direct conectat la Internet sau o reţea mare intranet. Serverele DNS trebuie să utilizeze servere rădăcină (root) pentru a răspunde la cererile despre gazde, altele decât acelea care sunt conţinute în fişierele lor domeniu.

Pentru a ajunge în afara reţelei pentru a obţine mai multă informaţie, un server DNS trebuie să ştie unde să caute. În Internet, primul loc unde caută un server DNS sunt serverele rădăcină (root). Serverele rădăcină (root) direcţionează un server DNS spre alte servere din ierarhie până este găsit un răspuns sau se determină că nu există nici un răspuns.

Lista serverelor rădăcină (root) implicite ale Navigator iSeries(TM)

Ar trebui să utilizaţi servere rădăcină (root) Internet doar dacă aveţi o conexiune Internet şi vreţi să rezolvaţi nume pe Internet dacă ele nu sunt rezolvate pe serverul dumneavoastră DNS. O listă implicită de servere rădăcină (root) Internet este livrată în Navigator iSeries. Conţinutul listei este corespunzător momentului când a fost lansat pe piaţă versiunea de Navigator iSeries. Puteţi verifica că lista implicită este actuală prin compararea ei cu lista de pe situl InterNIC. Faceţi o actualizare la configuraţia listei de servere rădăcină (root) pentru a o menţine actualizată.

Unde se obţin adresele de servere rădăcină (root) Internet

Adresele serverelor rădăcina de la nivelul de vârf se schimbă din timp în timp şi este resposabilitatea administratorului să le menţină actualizate. InterNIC menţine o listă actuală a adreselor serverului rădăcină Internet. Pentru a obţine o listă actuală a serverelor rădăcină Internet, parcurgeţi următorii paşi:

1. FTP ca anonim la serverul InterNIC: FTP.RS.INTERNIC.NET

2. Descărcaţi acest fişier: /domain/named.root
3. Stocaţi fişierul în următorul director: Integrated File System/Root/QIBM/ProdData/OS400/DNS/ROOT.FILE.

Un server DNS în spatele unui firewall poate să nu aibă definite servere rădăcină (root). În acest caz, serverul DNS poate rezolva cererile doar din intrările care există în fişierele de baze de date din domeniul lui principal sau în memoria cache. El poate înainta interogările din afara sitului la serverul DNS de pe firewall. În acest caz, serverul DNS de pe firewall acţionează ca un transmiţător mai departe (forwarder).

Serverele rădăcină (root) Intranet
Dacă serverul dumneavoastră DNS face parte dintr-o reţea largă intranet, puteţi avea servere rădăcină interne. Dacă serverul dumneavoastră DNS nu va accesa Internetul nu aveţi nevoie de încărcarea serverelor implicite Internet. Oricum, trebuie să adăugaţi serverele dumneavoastră interne rădăcină pentru ca serverul dumneavoastră DNS să poată rezolva adresele interne în afara domeniului lui.

Administrarea DNS-ului

O dată ce aţi configurat DNS-ul, poate că vreţi să revedeţi următoarele subiecte:

Verificarea funcţionării DNS cu NSLookup
Puteţi utiliza NSLookup pentru a verifica cum funcţionează DNS.

Administrarea cheii de securitate
Cheia de securitate vă permite să limitaţi accesul la datele dumneavoastră DNS.

Statisticile serverului DNS
Dump-ul bazei de date şi uneltele de statistică vă pot ajuta să treceţi în revistă şi să gestionaţi performanţa serverului.

Întreţinerea fişierelor de configurare DNS
Înţelegeţi la ce folosesc fişierele DNS şi treceţi în revistă câteva indicaţii de salvare şi de menţinere a lor.

Opţiunile DNS avansate
Acest subiect explică cum administratorii cu experienţă pot accesa opţiunile avansate.

Verificarea funcţionării DNS cu NSLookup

Utilizaţi NSLookup pentru a interoga serverul DNS pentru o adresă IP. Acesta verifică dacă serverul DNS răspunde la interogări. Cereţi numele gazdei care este asociat cu adresa IP a gazdei locale (127.0.0.1). Ar trebui să răspundă cu numele de gazdă (localhost). De asemenea, ar trebui să cereţi numele specifice care sunt definite în instanţa server pe care încercaţi să o verificaţi. Acesta va confirma că instanţa server specificată, pe care o testaţi, funcţionează corespunzător.

Pentru a verifica funcţionarea DNS cu NSLookup, parcurgeţi următorii paşi:

1. La linia de comandă, introduceţi NSLOOKUP DMNNAMSVR(n.n.n.n), unde n.n.n.n este o adresă la care dumneavoastră aţi configurat instanţa server pe care o testaţi pentru ascultare.
2. La linia de comandă, introduceţi NSLOOKUP şi apăsaţi **Enter**. Aceasta va porni o sesiune de interogare NSLookup.
3. Introduceţi server urmat de numele serverului dumneavoastră şi apăsaţi **Enter**. Spre exemplu: server myiseries.mycompany.com.
   Această informaţie afişează:

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

Unde n.n.n.n reprezintă adresa IP a serverului dumneavoastră.

4. Introduceţi 127.0.0.1 la linia de comandă şi apăsaţi **Enter**.

   Ar trebui să apară această informaţie, incluzând numele gazdei locale:

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

Name:    localhost
Address:  127.0.0.1
```

   Serverul DNS răspunde corect dacă el întoarce numele gazdei locale: **localhost**.

5. Introduceţi exit şi apăsaţi **Enter** pentru a ieşi din sesiunea NSLOOKUP.

Notă: Dacă aveţi nevoie de ajutor la utilizarea NSLookup, introduceţi ? şi apăsaţi **Enter**.

Administrarea cheii de securitate

Există două tipuri de chei compatibile cu DNS. Fiecare dintre ele joacă un rol diferit în securizarea configuraţiei serverului dumneavoastră. Următoarele descrieri explică cum sunt înrudite fiecare dintre chei cu serverul dumneavoastră.

Chei DNS

Cheia DNS este o cheie definită pentru BIND. Este folosită de serverul DNS ca parte din verificarea unei actualizări ce vine. Puteţi configura o cheie şi să-i asignaţi un nume. După aceea, când vreţi să protejaţi un obiect DNS, cum este o zonă dinamică, puteţi specifica cheia în lista de potrivire adrese.

Pentru administrarea cheilor DNS, parcurgeţi următorii paşi:

1. În **Navigator iSeries**, expandaţi **serverul iSeries(TM)** —> **Reţea** —> **Servere** —> **DNS**.
2. În panoul din dreapta faceţi clic dreapta pe instanţa server DNS pe care vreţi să o deschideţi şi selectaţi **Configurare**.
3. În fereastra **Configurare DNS**, selectaţi **Fişier** > **Gestionare chei...**

Actualizarea dinamică a cheilor

Actualizarea dinamică al cheilor este utilizată pentru securizarea actualizărilor dinamice de către serverul DHCP. Aceste chei trebuie să existe atunci când DNS şi DHCP sunt pe acelaşi iSeries. Dacă DHCP este pe un iSeries diferit, trebuie să creaţi aceeaşi cheie de actualizare dinamică pe fiecare server iSeries pentru a permite actualizări dinamice sigure.

Pentru a administra cheile de actualizare dinamică parcurgeţi următorii paşi:

1. În **Navigator iSeries**, expandaţi **serverul iSeries** —> **Reţea** —> **Servere** —> .
2. Faceţi clic dreapta pe **DNS** şi selectaţi **Gestionare chei actualizare dinamică...**

Statisticile serverului DNS

DNS furnizează diferite unelte de diagnosticare. Ele pot fi utilizate pentru a monitoriza performanţa serverului dumneavoastră.

Statisticile serverului

DNS vă permite să vizualizaţi statisticile pentru o instanţă server. Aceste statistici însumează numărul de interogări şi răspunsuri pe care le-a primit serverul de la ultima repornire sau reîncărcare a bazei lui de date. Informaţia este adăugată continuu la acest fişier până la ştergerea acestuia. Această informaţie poate fi utilă la evaluarea traficului serverului şi în urmărirea problemelor. Mai multe informaţii despre statisticile serverului sunt disponibile în subiectul de ajutor online DNS **Înţelegerea statisticilor DNS**.

Pentru a accesa statisticile serverului, parcurgeţi următorii paşi:

1. În **Navigator iSeries**, expandaţi **serverul iSeries(TM)** —> **Reţea** —> **Servere** —> **DNS**.

2. În panoul din dreapta, faceţi clic dreapta pe **serverul DNS** şi selectaţi **Configurare**.
3. În fereastra **Configurare DNS**, selectaţi **Vizualizare**—> **Statistici server**.

Baza de date a serverului activ
DNS vă permite să vizualizaţi un dump de date de autoritate, date cache şi date sugestive pentru o instanţă server. Dump-ul include informaţii de la toate zonele primare şi secundare ale serverului (zonele de mapare inainte şi inversă) la fel de bine ca şi informaţia pe care serverul o obţine din cereri. Baza de date conţine informaţii despre zonă şi gazdă, incluzând unele proprietăţi de zonă, cum sunt informaţiile de început de autoritate (SOA) şi proprietăţile de trecere (through) prin gazdă, cum ar fi informaţiile MX (mail exchanger). Această informaţie poate fi utilă în urmărirea problemelor.

Puteţi vizualiza dump-ul bazei de date a serverului activ utilizând Navigator iSeries. Dacă trebuie să salvaţi o copie a fişierelor, numele fişierului de baze de date dump este NAMED_DUMP.DB din directorul sistemului dumneavoastră iSeries: **IFS**/**Root**/**QIBM**/**UserData**/**OS400**/**DNS**/**<instanţă_server>**, unde ″<instanţă_server>″ este numele instanţei server DNS. Mai multe informaţii despre baza de date a serverului activ sunt disponibile în subiectul de ajutor online al serverului DNS **Înţelegerea bazei de date a serverului DNS**.

Pentru a accesa dump-ul bazei de date a serverului activ, parcurgeţi următorii paşi:
1. În **Navigator iSeries**, expandaţi **serverul iSeries** —> **Reţea** —> **Servere** —> .
2. În panoul din dreapta, faceţi clic dreapta pe **serverul DNS** şi selectaţi **Configurare**.
3. În fereastra **Configurare DNS**, selectaţi **Vizualizare**—> **Baza de date server activ**.

Întreţinerea fişierelor de configurare DNS
Puteţi folosi serverul DNS OS/400(R) pentru a crea şi administra instanţele serverului DNS pe sistemul dumneavoastră iSeries(TM). Fişierele de configurare pentru DNS sunt administrate de Navigator iSeries. Puteţi edita manual aceste fişiere. Întotdeauna să folosiţi Navigator iSeries pentru a crea, a modifica sau a şterge fişierele de configurare DNS. Fişierele de configurare DNS sunt stocate în căile sistemului de fişiere integrat care sunt listate mai jos:

Notă: Structura de fişiere de mai jos se aplică DNS-ului ce rulează pe BIND 8. Dacă utilizaţi DNS bazat pe BIND 4.9.3, consultaţi *Salvarea de rezervă a fişierelor de configurare DNS şi menţinerea fişierelor istoric* din subiectul Centrului de informare DNS V4R5

(aproximativ 62 de pagini).

În tabelul de mai jos, fişierele sunt listate în ierarhia de căi arătată. Fişierele cu o icoană de salvare

ar trebui copiate salvate pentru a proteja datele. Fişierele cu o icoană de ştergere

ar trebui şterse în mod regulat.

Nume		Descriere
QIBM/**UserData**/**OS400**/**DNS**/		Directorul punct de pornire pentru DNS.
ATRIBUTE		DNS utilizează acest fişier pentru a determina ce versiune BIND utilizaţi.
QIBM/**UserData**/**OS400**/**DNS**/***<instanţă-n>***/		Directorul punct de pornire pentru o instanţă DNS.

Nume		Descriere
ATRIBUTE		Configurarea atributelor utilizate de DNS iSeries.
NAMED.CONF		Acest fişier conţine date de configurare. Folosit pentru a-i indica serverului ce zone specifice le gestionează, unde sunt fişierele de zonă, ce zone pot fi actualizate dinamic, unde sunt serverele lui de înaintare (forwarding) şi alte setări de opţiuni.
BOOT.AS400BIND4		Configuraţia serverului BIND 4.9.3 şi fişierul de politici care este convertit la fişierul NAMED.CONF la BIND 8, pentru această instanţă. Acest fişier este creat dacă aţi migrat de la un server BIND 4.9.3, la un server BIND 8. Serveşte ca o copie de rezervă pentru migrare şi poate fi şters când serverul BIND 8 funcţionează cum se cuvine.
NAMED.CA		Lista serverelor rădăcină pentru această instanţă server.
NAMED_DUMP.DB		Dump cu date server creat pentru baza de date server activ.
NAMED.STATS		Statisticile serverului.
NAMED.PID		Păstrează ID-ul de proces al serverului ce rulează. Acest fişier este creat de fiecare dată când serverul DNS este pornit. El este folosit pentru funcţiile server bază de date, statistică şi actualizare. Nu editaţi sau ştergeţi acest fişier.
QUERYLOG		Istoricul serverului DNS de înterogări primite. Fişierul este creat atunci când istoricul serverului DNS este activ. Când este activ, acest fişier devine destul de mare şi ar trebui şters periodic.
<nume-zonă-a>.DB		Fişier zonă pentru un domeniu particular deservit de acest server. Conţine toate înregistrările resursă pentru această zonă.
<nume-zonă-b>.DB		Fişier zonă pentru un domeniu particular deservit de acest server. Conţine toate înregistrările resursă pentru această zonă. Fiecare zonă are un fişier separator .DB.

Nume		Descriere
.ixfr.		Fişiere IXFR. Aceste fişiere sunt utilizate de serverele secundare pentru a încărca datele modificate de la ultimul transfer de zonă. Pe măsură ce se fac actualizările, numărul de fişiere IXFR va creşte. Ar trebui să ştergeţi periodic fişierele IXFR vechi. Păstrând fişierele care au fost create cu o zi sau două în urmă va permite mai multor servere secundare să încarce în continuare IXFR-uri. Dacă ştergeţi toate fişierele, serverele secundare vor cere un transfer total (AXFR).
TMP		Director utilizat de instanţa de server pentru crearea fişierelor de lucru temporare.
QIBM/UserData/OS400/DNS/TMP		Directorul Temp utilizat de programul QTOBH2N pentru a crea fişiere intermediare descărcate din tabelul gazdă pentru a fi importate mai târziu utilizând Navigator iSeries.
QIBM/UserData/OS400/DNS/_DYN/		Directorul care păstrează fişierele cerute pentru actualizările dinamice.
<nume-id-cheie-x>._KID		Fişierul ce conţine o instrucţiune de cheie BIND 8 pentru id_cheie numit *<nume-id-cheie-x>*.
<nume-id-cheie-x>._DUK.*<nume-zonă-a>*		Cheia de actualizare dinamică necesară pentru a iniţia o cerere de actualizare dinamică la *<nume-zonă-a>* utilizând cheia *<nume-id-cheie-x>*.
<nume-id-cheie-y>._KID		Fişierul ce conţine o instrucţiune de cheie BIND 8 pentru id_cheie numit *<nume-id-cheie-y>*.
<nume-id-cheie-y>._DUK.*<nume-zonă-a>*		Cheia de actualizare dinamică necesară pentru a iniţia o cerere de actualizare dinamică la *<nume-zonă-a>* utilizând cheia *<nume-id-cheie-y>*.
<nume-id-cheie-y>._DUK.*<nume-zonă-b>*		Cheia de actualizare dinamică necesară pentru a iniţia o cerere de actualizare dinamică la *<nume-zonă-b>* utilizând cheia *<nume-id-cheie-y>*.

Opţiunile DNS avansate

DNS din Navigator iSeries furnizează o interfaţă pentru configurarea şi administrarea serverului dumneavoastră DNS. Următoarele task-uri sunt furnizate ca scurtături pentru administratorii care sunt familiari cu interfaţa grafică iSeries. Ele furnizează metode rapide pentu modificarea stării serverului şi a atributelor pentru mai multe instanţe printr-o singură acţiune.

Modificarea atributelor DNS

Interfaţa DNS nu vă permite să modificaţi printr-o singură acţiune toate instanţele de pornire automată a serverului şi nivelurile de depanare. Puteţi utiliza interfaţa bazată pe caracter pentru a modifica aceste setări pentru instanţele individuale ale serverului DNS sau pentru toate instaţele în acelaşi timp. Parcurgeţi următorii paşi pentru a utiliza CHGDNSA:

1. La linia de comandă, introduceţi CHGDNSA şi apăsaţi **F4**.
2. În pagina de modificare atribute server DNS (CHGDNSA), introduceţi numele unei singure instanţe server sau *ALL şi apăsaţi **Enter**.

   Vor fi afişate opţiunile disponibile de atribute server:
   Autostart server . . . . . *SAME *YES, *NO, *SAME
   Debug level . . . . . *SAME 0-11, *SAME, *DFT
3. **Autostart** Pentru a specifica că serverele DNS selectate ar trebui pornite automat la pornirea TCP/IP, introduceţi *YES. Dacă nu vreţi ca serverul să pornească la pornirea TCP/IP, introduceţi *NO. Pentru a lăsa atributele la setarea curentă, introduceţi *SAME.

   Debug level Pentru a schimba nivelul de depanare pe care ar trebui să-l folosească serverele DNS selectate, introduceţi o valoarea între 0 şi 11. Pentru a specifica faptul că nivelul de depanare ar trebui să moştenească valoarea de depanare a serverului la pornire, introduceţi *DFT. Pentru a lăsa atributele la setările lor curente, introduceţi *SAME.

   Când aţi introdus toate priorităţile dumneavoastră, apăsaţi **Enter** pentru a seta atributele DNS.

Pornirea sau oprirea serverelor DNS
Interfaţa DNS nu vă permite să porniţi sau să opriţi instanţe server multiple în acelaşi timp. Puteţi utiliza interfaţa bazată pe caracter pentru a modifica aceste setări pentru instanţe multiple în acelaşi timp. Pentru a utiliza interfaţa bazată pe caracter ca să puteţi porni toate instanţele server DNS în acelaşi timp, introduceţi STRTCPSVR SERVER(*DNS) DNSSVR(*ALL) la linia de comandă. Pentru a opri toate serverele DNS în acelaşi timp, introduceţi ENDTCPSVR SERVER(*DNS) DNSSVR(*ALL) la linia de comandă.

Modificarea valorilor de depanare
DNS din interfaţa Navigator iSeries nu vă permite să modificaţi nivelul de depanare in timp ce serverul rulează. Oricum, puteţi utiliza interfaţa bazată pe caracter pentru a modifica nivelul de depanare în timp ce serverul rulează. Această caracteristică poate fi folositoare administratorilor care au zone mari şi nu doresc cantitatea mare de date de depanare pe care le-ar obţine la prima pornire a serverului şi la încărcarea tuturor datelor de zonă. Pentru a modifica nivelul de depanare utilizând interfaţa bazată pe caractere, pargurgeţi următorii paşi, înlocuind <instanţă> cu numele instanţei server:
1. La linia de comandă introduceţi ADDLIBLE QDNS şi apăsaţi **Enter**.
2. Modificaţi nivelul de depanare:
   - Pentru a activa acţiunea de depanare sau pentru creşte nivelul de depanare cu 1, introduceţi CALL QTOBDRVS (’BUMP’ ’<instanţă>’) şi apăsaţi **Enter**.
   - Pentru a dezactiva acţiunea de depanare, introduceţi CALL QTOBDRVS (’OFF’ ’<instanţă>’) şi apăsaţi **Enter**.

Depanarea DNS-ului

DNS funcţionează în mare parte ca alte funcţii şi aplicaţii TCP/IP. Asemenea aplicaţiilor SMTP sau FTP, joburile DNS rulează sub subsistemul QSYSWRK şi produc istorice de joburi sub profilul utilizator QTCP, cu informaţiile asociate cu jobul DNS. Dacă un job DNS se termină, puteţi utiliza înregistrările jobului pentru a determina cauza. Dacă serverul DNS nu întoarce răspunsurile aşteptate, înregistrările job pot conţine informaţii care vă pot ajuta la analizarea problemei.

Configurarea DNS constă din diferite fişiere cu tipuri diferite de înregistrări în fiecare fişier. Problemele cu serverul DNS sunt în general rezultatul intrărilor incorecte din fişierul de configurare DNS. Când apare o problemă, verificaţi dacă fişierele de configurare DNS conţine intrări corespunzătoare aşteptărilor dumneavoastră.

Înregistrarea în istoric
DNS furnizează numeroase opţiuni de înregistrare care pot fi ajustate când încercaţi să găsiţi sursa problemei. Înregistrarea furnizează flexibilitate prin oferirea diferitelor niveluri de gravitate, categorii de mesaje şi fişiere de ieşire, ajutându-vă în acest fel să găsiţi problemele.

Setări depanare
DNS oferă 12 niveluri al controlului de depanare. În general, înregistrarea furnizează o metodă mai uşoară de găsire a problemelor, dar în unele cazuri depanarea poate fi necesară. În condiţii normale, depanarea este dezactivată (valoare = 0).

Alte resurse de depanare
Informaţiile generale de depanare DNS se pot găsi în mai multe surse. În special, cartea lui O'Reilly, DNS and BIND, este o bună referinţă pentru întrebările generale şi directorul de resurse DNS furnizează legături către grupurile de discuţie pentru administratorii DNS.

Identificarea joburilor
Dacă vă uitaţi în istoricele joburilor pentru a verifica funcţionarea serverului DNS (folosind WRKACTJOB, spre exemplu), consideraţi următoarele indicaţii de denumire:

- Dacă utilizaţi BIND 4.9.3, numele jobului serverului va fi QTOBDNS. Pentru mai multe informaţii despre depanarea DNS 4.9.3, consultaţi *Depanarea serverelor DNS* din subiectul DNS V5R1 din Centrul de informare

  (aproximativ 357 KB).
- Dacă rulaţi servere bazate pe BIND 8, vor fi joburi separate pentru fiecare instanţă de server pe care o rulaţi. Numele jobului are 5 caractere fixe (QTOBD) urmate de numele instanţei. Spre exemplu, dacă aveţi două instanţe, INST1 şi INST2, numele joburilor lor vor fi QTOBDINST1 şi QTOBDINST2.

Înregistrare server DNS

BIND 8 oferă diferite opţiuni de înregistrare noi. Puteţi specifica ce tipuri de mesaje sunt înregistrate în istoric, unde este trimis fiecare tip de mesaj şi care este gravitatea fiecărui mesaj de înregistrat. În general, setările implicite de înregistrare în istoric vor fi cele dorite, dar dacă doriţi să le modificaţi se recomandă să vă referiţi la alte surse de documentaţie din BIND 8 pentru informaţii despre înregistrarea în istoric.

Canale de înregistrare în istoric
Serverul DNS poate înregistra mesaje către diferite canale de ieşire. Canalele specifică unde sunt trimise datele înregistrate. Puteţi selecta următoarele tipuri de canal:

- **Canale fişier**
  Mesajele înregistrate la canalele fişier sunt trimise către un fişier. Canalele fişier implicite sunt as400_debug şi as400_QPRINT. Implicit, mesajele de depanare sunt înregistrate la canalul as400_debug, care este fişierul NAMED.RUN, dar la fel de bine puteţi specifica să trimiteţi şi alte categorii de mesaje către acest fişier. Categoriile de mesaj înregistrate către as400_QPRINT sunt trimise către un fişier spool QPRINT pentru un profil utilizator QTCP. Puteţi crea propriile dumneavoastră canale fişiere pe lângă canalele implicit furnizate.
- **Canalele Syslog**
  Mesajele înregistrate către acest canal sunt trimise la istoricul joburilor de server. Canalul syslog implicit este as400_joblog. Mesajele înregistrate rutate către acest canal sunt trimise la istoricul de job al instanţei de server DNS.
- **Canale Null**
  La toate mesajele înregistrate către canalele null se va renunţa. Canalul null implicit este as400_null. Puteţi ruta categorii către canalul null, dacă nu vreţi ca mesajele să apară în nici un istoric.

Categorii de mesaje
Mesajele sunt grupate pe categorii. Puteţi specifica ce categorii de mesaj ar trebui înregistrate către fiecare canal. Există multe categorii, incluzând:

- config: procesarea fişierului de configurare
- db: operaţii cu baze de date
- queries: Generează un mesaj scurt de înregistrare pentru fiecare cerere pe care o primeşte serverul.

- lame-servers: Detectarea delegărilor greşite
- update: Actualizările dinamice
- xfer-in: Transferurile de zonă pe care le primeşte serverul.
- xfer-out: Transferuri de zonă pe care serverul le trimite

Fişierele de înregistrare pot deveni mari şi trebuie şterse în mod regulat. Toate conţinuturile fişierelor istoric ale serverului DNS sunt şterse atunci când serverul DNS este oprit şi pornit.

Gravitatea mesajelor
Canalele vă permit să filtraţi după gravitatea mesajelor. Pentru fiecare canal, puteţi specifica nivelul de gravitate pentru fiecare din mesajele înregistrate. Sunt disponibile următoarele niveluri de gravitate:
- Critică
- Eroare
- Avertisment
- Observaţie
- Informaţie
- Depanare (specifică nivelul de depanare 0-11)
- Dinamic (moşteneşte nivelul de depanare la pornire a serverului)

Sunt înregistrate, toate mesajele selectate care au gravitatea pe care aţi selectat-o şi orice niveluri mai sus de cea selectată din listă. De exemplu, dacă aţi selectat Avertisment, canalul înregistrează mesaje Avertisment, Eroare şi Critice. Dacă selectaţi nivelul Depanare, puteţi specifica o valoare de la 0 la 11 pentru care vreţi ca mesajele de depanare să fie înregistrate.

Schimbarea setărilor de înregistrare.
Pentru a accesa opţiunile de înregistrare, parcurgeţi următorii paşi:
1. În **Navigator iSeries**, expandaţi **serverul iSeries(TM)** —> **Reţea** —> **Servere** —> **DNS**.
2. În panoul din dreapta, faceţi clic dreapta pe **serverul DNS** şi selectaţi **Configurare**.
3. În fereastra **Configurare DNS**, faceţi clic dreapta pe serverul **DNS** şi selectaţi **Proprietăţi**.
4. În fereastra **Proprietăţi server** selectaţi fişa **Canale** pentru a crea noi canale fişier sau proprietăţi ale unui canal, cum este gravitatea mesajelor înregistrate pentru fiecare canal.
5. În fereastra **Proprietăţi server** selectaţi fişa **Înregistrare în istoric** pentru a specifica care categorie de mesaje sunt înregistrate către fiecare canal.

Tipuri de depanare
Nivelul de gravitate al canalului implicit as400_joblog este setat la Eroare. Această setare este utilizată pentru a reduce volumul de mesaje de informare şi avertizare, care altfel ar putea degrada performanţa. Dacă aveţi probleme şi istoricul jobului nu indică sursa problemei dumneavoastră aveţi nevoie să schimbaţi nivelul de gravitate. Urmaţi procedura de mai sus pentru a accesa pagina cu canale şi modificaţi nivelul de gravitate pentru canalul as400_joblog la Avertizare, Observaţii sau Informare pentru a putea vizualiza mai multe date înregistrate. O dată ce aţi rezolvat această problemă, resetaţi nivelul de gravitate la Eroare pentru a reduce numărul de mesaje din istoricul jobului.

Setările de depanare DNS

Funcţia de depanare DNS poate furniza informaţii care vă pot ajuta să determinaţi şi să corectaţi problemele serverului DNS. Se recomandă ca prima dată să folosiţi înregistrarea în istoric pentru a încerca să corectaţi problemele.

Nivelurile de depanare valide sunt între 0 şi 11. Reprezentantul dumneavoastră IBM vă poate ajuta să determinaţi valoare apropiată de depanare pentru diagnosticarea problemei dumneavoastră DNS. Valorile de 1 sau mai mari scriu informaţiile de depanare în fişierul NAMED.RUN din calea de directoare iSeries: **IFS/Root/QIBM/UserData/OS400/DNS/<instanţă_server>**, unde ″<instanţă_server>″ este numele instanţei

serverului DNS. Fişierul NAMED.RUN continuă să se mărească atât timp cât nivelul de depanare este setat la 1 sau mai mare şi serverul DNS continuă să ruleze. Se recomandă să ştergeţi fişierul din timp în timp pentru a nu ocupa mult spaţiu pe disc. De asemenea, puteţi utiliza pagina **Proprietăţi server** - **Canale** pentru a specifica preferinţele pentru dimensiunea maximă şi numărul de versiuni ale fişierului NAMED.RUN.

Pentru a modifica valoarea de depanare pentru o instanţă server DNS, urmaţi aceşti paşi:

1. În **Navigator iSeries**, expandaţi **serverul iSeries** —> **Reţea** —> **Servere** —> .
2. În panoul din dreapta, faceţi clic dreapta pe **serverul DNS** şi selectaţi **Configurare**.
3. În fereastra **Configurare DNS**, faceţi clic dreapta pe serverul DNS şi selectaţi **Proprietăţi**.
4. În pagina **Proprietăţi server - General**, specificaţi nivelul de depanare la pornirea severului.
5. Dacă serverul rulează, opriţi şi reporniţi severul.
   Notă: Modificările făcute la nivelul de depanare nu au efect dacă sunt făcute în timpul rulării serverului. Nivelul de depanare setat aici va fi folosit ulterior când serverul este repornit complet. Dacă vreţi să modificaţi nivelul de depanare în timp ce serverul rulează, consultaţi Caracteristici avansate DNS.

Alte informaţii privind DNS

Există multe surse de informare privind DNS şi BIND 8. Următoarea listă este doar o mică prezentare a resurselor disponibile:

- DNS and BIND, a treia ediţie. Paul Albitz şi Cricket Liu. Publicată de O'Reilly and Associates,Inc.

  Sebastopol, California, 1998. Număr ISBN : 1-56592-512-2. Aceasta este sursa cea mai bună sursă pentru DNS.
- Site-ul web Internet Software Consortium

  conţine noutăţi, legături şi alte resurse pentru BIND.
- Site-ul InterNIC

  menţine un director cu toate înregistrările nume domeniu care sunt autorizate de ICANN (Internet Corporation for Assigned Names and Numbers).
- DNS Resources Directory

  furnizează materiale de referinţă pentru DNS şi legături la alte resurse DNS, incluzând şi grupurile de discuţie. De asemenea, furnizează o listă de RFC-uri înrudite cu DNS

  .

Manuale şi cărţi Redbooks(TM) IBM

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

  Această carte Redbook descrie severul DNS şi serverul DHCP care sunt incluse în OS/400(R). Informaţia din această carte Redbook vă ajută să instalaţi, să adaptaţi, să configuraţi şi să depanaţi suportul DNS şi DHCP prin exemple.

Notă: Această carte Redbook nu a fost actualizată pentru a include noile caracteristici BIND 8 disponibile pentru V5R1. Oricum este o bună referinţă pentru conceptele generale DNS.

Anexa. Observaţii

Aceste informaţii au fost elaborate pentru produse şi servicii oferite în S.U.A.

Este posibil ca IBM să nu ofere în alte ţări produsele, serviciile sau caracteristicile discutate în acest document. Luaţi legătura cu reprezentantul IBM local pentru informaţii despre produsele şi serviciile disponibile în zona dumneavoastră. Referirea la un produs, program sau serviciu IBM nu înseamnă că se afirmă sau că se sugerează faptul că poate fi folosit numai acel produs, program sau serviciu IBM. Poate fi folosit în loc orice produs, program sau serviciu care este echivalent din punct de vedere funcţional şi care nu încalcă dreptul de proprietate intelectuală al IBM. Însă evaluarea şi verificarea modului în care funcţionează un produs, program sau serviciu non-IBM ţine de responsabilitatea utilizatorului.

IBM poate avea brevete sau aplicaţii în curs de brevetare care să acopere subiectele descrise în acest document. Oferirea acestui document nu vă conferă nici o licenţă cu privire la aceste patente. Puteţi trimite întrebări cu privire la licenţe, în scris, la:

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

Pentru întrebări privind licenţa pentru informaţiile DBCS (double-byte), contactaţi departamentul de Proprietate intelectuală al IBM-ului din ţara dumneavoastră sau trimiteţi întrebările în scris la:

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

Următorul paragraf nu se aplică în cazul Marii Britanii sau al altor ţări unde asemenea prevederi nu sunt în concordanţă cu legile locale: INTERNATIONAL BUSINESS MACHINES CORPORATION OFERĂ ACEASTĂ PUBLICAŢIE ″CA ATARE″, FĂRĂ NICI UN FEL DE GARANŢIE, EXPRIMATĂ SAU PRESUPUSĂ, INCLUSIV, DAR NELIMITÂNDU-SE LA ELE, GARANŢIILE IMPLICITE DE NEÎNCĂLCARE A UNOR DREPTURI SAU NORME, DE VANDABILITATE SAU DE POTRIVIRE LA UN ANUMIT SCOP. Unele state nu permit declinarea responsabilităţii pentru garanţiile exprese sau implicite în anumite tranzacţii şi de aceea este posibil ca aceste clauze să nu fie valabile în cazul dumneavoastră.

Aceste informaţii pot include inexactităţi tehnice sau erori tipografice. Se efectuează modificări periodice la informaţiile incluse aici; aceste modificări vor fi încorporate în noi ediţii ale publicaţiei. IBM poate aduce îmbunătăţiri şi/sau modificări produsului (produselor) descris în această publicaţie în orice moment, fără notificare.

Orice fel de referinţe din aceste informaţii către situri Web non-IBM sunt furnizate doar pentru convenienţă şi nu serveşte în nici un caz ca aprobare a acelor situri Web. Materialele de pe siturile Web respective nu fac parte din materialele pentru acest produs IBM, iar utilizarea acestor situri Web se face pe propriul risc.

IBM poate utiliza sau distribui oricare dintre informaţiile pe care le furnizaţi, în orice mod considerat adecvat, fără ca aceasta să implice vreo obligaţie faţă de dumneavoastră.

Posesorii de licenţe pentru acest program care doresc să aibă informaţii despre el în scopul de a permite: (I) schimbul de informaţii între programe create independent şi alte programe (inclusiv acesta) şi (II) utilizarea mutuală a informaţiilor care au fost schimbate, vor contacta:

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

Aceste informaţii pot fi disponibile, să fie supuse unor termeni şi condiţii, inclusiv în unele cazuri, plata unor taxe.

Programul licenţiat descris în acest information şi toate materialele licenţiate disponibile pentru el sunt furnizate de către IBM conform termenilor IBM Customer Agreement, IBM International Program License Agreement sau orice acord echivalent între noi.

Dacă vedeţi aceste informaţii folosind o copie electronică, fotografiile şi ilustraţiile color s-ar putea să nu apară.

Mărci comerciale

Următorii termeni sunt mărci comerciale deţinute de International Business Machines Corporation în Statele Unite, în alte ţări sau ambele:
Application System/400
AS/400
e (logo)
IBM
iSeries
Operating System/400
OS/400
400

Lotus, Freelance şi WordPro sunt mărci comerciale deţinute de International Business Machines Corporation şi Lotus Development Corporation în Statele Unite, în alte ţări sau ambele.

C-bus este o marcă comercială deţinută de Corollary, Inc. în Statele Unite, în alte ţări sau ambele.

ActionMedia, LANDesk, MMX, Pentium şi ProShare sunt mărci comerciale sau mărci comerciale înregistrate deţinute de Intel Corporation în Statele Unite, în alte ţări sau ambele.

Microsoft, Windows, Windows NT şi logo-ul Windows sunt mărci comerciale deţinute de Microsoft Corporation în Statele Unite, în alte ţări sau ambele.

SET şi log-ul SET sunt mărci comrciale deţinute de SET Secure Electronic Transaction LLC.

Java şi toate mărcile comerciale bazate pe Java sunt mărci comerciale deţinute de Sun Microsystems, Inc. în Statele Unite, în alte ţări sau ambele.

UNIX este o marcă comercială înregistrată deţinută de The Open Group în Statele Unite şi în alte ţări.

Alte nume de companii, produse şi servicii pot fi mărci comerciale sau mărci de serviciu ale altora.

Termeni şi condiţii pentru descărcarea şi tipărirea publicaţiilor

Permisiunile pentru utilizarea publicaţiilor pe care le-aţi selectat pentru descărcare sunt acordate ca urmare a termenilor şi condiţiilor următoare şi a indicaţiei dumneavoastră de acceptare a lor.

Utilizare personală: Puteţi reproduce aceste publicaţii pentru uzul dumneavoastră personal, necomercial cu condiţia să fie păstrate toate observaţiile privind proprietatea. Nu puteţi distribui, afişa sau realiza obiecte derivate din aceste publicaţii sau dintr-o porţiune a lor fără consimţământul explicit al IBM.

Utilizare comercială: Puteţi reproduce, distribui şi afişa aceste publicaţii doar în cadrul întreprinderii dumneavoastră, cu condiţia ca toate observaţiile privind proprietatea să fie păstrate. Nu puteţi realiza derivate ale acestor publicaţii sau să reproduceţi, să distribuiţi sau să afişaţi aceste publicaţii sau o porţiune din ele în afara întreprinderii dumneavoastră fără consimţământul explicit al IBM.

Cu excepţia a ceea ce este acordat explicit în această permisiune, nici o altă permisiune, licenţă sau drept nu vor mai fi acordate, explicit sau implicit, asupra publicaţiilor sau a altor informaţii, date, software sau altă proprietate intelectuală conţină aici.

IBM îşi rezervă dreptul de a retrage aceste permisiuni acordate aici oricând, în opinia sa, utilizarea publicaţiilor nu este în interesul său sau, instrucţiunile de mai sus nu sunt urmate corespunzător.

Nu puteţi descărca, exporta sau rexporta aceste informaţii decât în deplină conformitate cu legile şi regulamentele aplicabile, inclusiv toate legile şi regulamentele de export ale Statelor Unite. IBM NU OFERĂ GARANŢII DESPRE CONŢINUTUL ACESTOR PUBLICAŢII. PUBLICAŢIILE SUNT FURNIZATE ″AŞA CUM SUNT″ ŞI FĂRĂ GARANŢIE DE NICI UN FEL, FIE EXPLICITĂ, FIE IMPLICITĂ, INCLUSIV DAR NU LIMITAT LA GARANŢIILE IMPLCITE DE MERCANTIBILITATE ŞI POTRIVIRE PENTRU UN SCOP PARTICULAR.

Prin descărcarea sau tipărirea unei publicaţii de pe acest site, aţi indicat că sunteţi de acord cu aceşti termeni şi condiţii.

Tipărit în S.U.A.