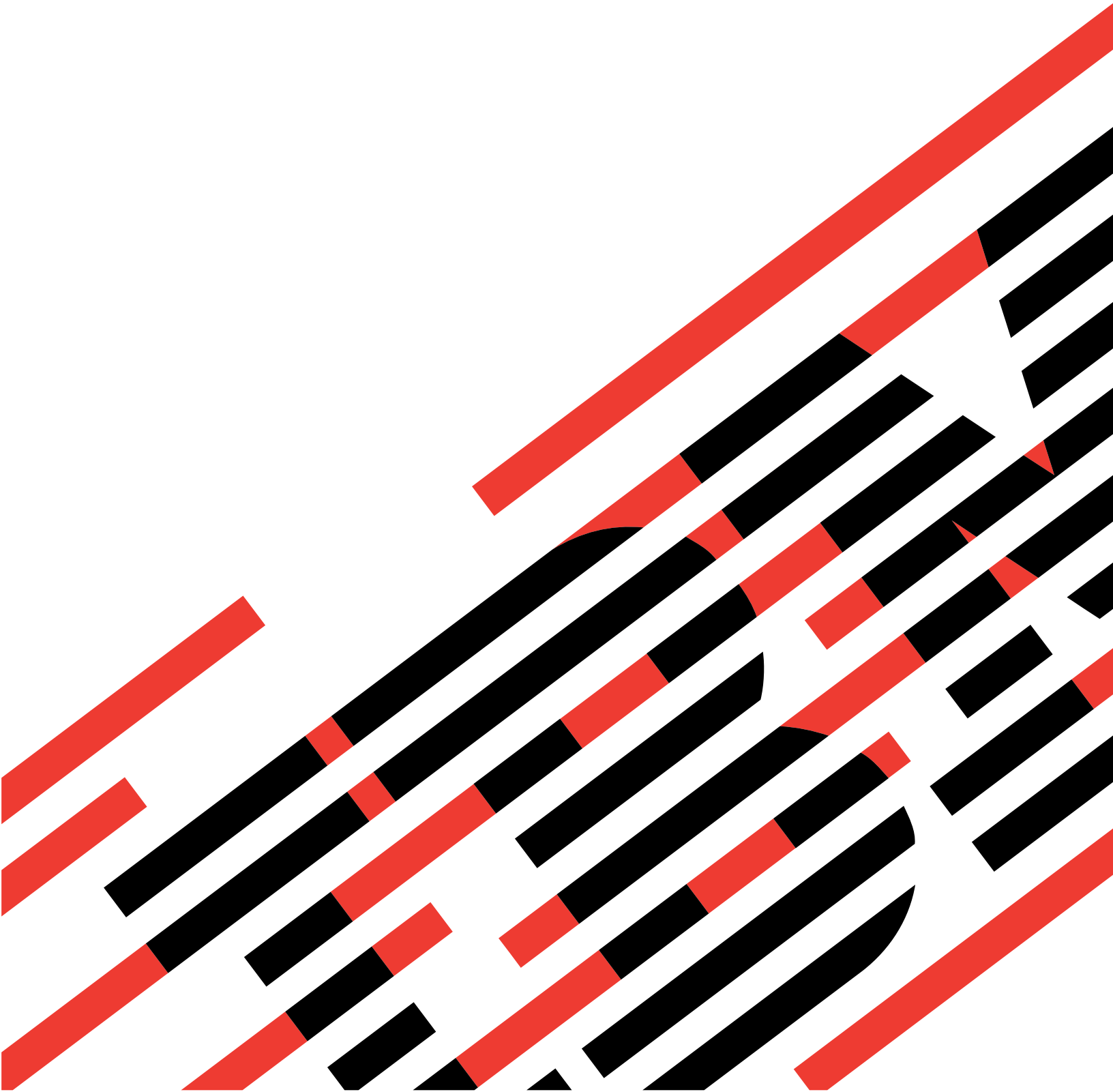
IBM Systems - iSeries

# Lucrul în reţea - DNS (Domain Name System)

*Versiunea 5 Ediţia 4*



IBM Systems - iSeries

# Lucrul în reţea - DNS (Domain Name System)

*Versiunea 5 Ediţia 4*

**Notă**

Înainte de a folosi aceste informaţii şi produsul la care se referă, citiţi informaţiile din “Observaţii”, la pagina 39.

**Ediţia a şasea (februarie 2006)**

Această ediţie este valabilă pentru IBM i5/OS (număr de produs 5722-SS1) versiunea 5, ediţia 4, modificarea 0 şi pentru toate ediţiile şi modificările ulterioare până se specifică altceva în noile ediţii. Această versiune nu rulează pe toate modelele RISC şi nici pe modelele CISC.

# Cuprins

# Domain Name System

DNS-ul este un sistem distribuit de baze de date ce administrează numele de gazdă şi adresele lor IP asociate.

DNS permite folosirea unor nume simple, cum ar fi www.jkltoys.com, pentru a localiza o gazdă, în loc să se folosească adresa IP (xxx.xxx.xxx.xxx). Un singur server poate asigura numai cunoaşterea numelor de gazdă şi a adreselor IP dintr-o mică subreţea a unei zone, dar serverele DNS pot funcţiona împreună pentru maparea tuturor numelor de domeniu la adresele lor IP. Conlucrarea serverelor DNS permite calculatoarelor să comunice prin Internet.

Pentru Versiunea 5 Ediţia 1 (V5R1) de IBM OS/400, serviciile DNS sunt bazate pe implementarea standardului industrial DNS numită BIND (Berkeley Internet Name Domain), versiunea 8. Serviciile DNS din versiunile anterioare de IBM OS/400 erau bazate pe BIND versiunea 4.9.3. Pentru a putea utiliza noul server DNS, bazat pe BIND versiunea 8, pe serverul IBM eServer iSeries trebuie să fie instalată opţiunea 33 din i5/OS, PASE (Portable Application Solutions Environment). Dacă nu aveţi instalat PASE, puteţi totuşi rula acelaşi server DNS bazat pe versiunea 4.9.3 a BIND disponibilă în ediţiile anterioare. Totuşi, migrarea către BIND 8 oferă o funcţionare îmbunătăţită şi integrează 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, vedeţi subiectul V4R5 DNS information center pentru informaţii privind DNS bazat pe BIND 4.9.3.

## PDF tipăribil

Aflaţi cum puteţi vizualiza sau tipări un PDF cu aceste informaţii.

Pentru a vizualiza sau descărca versiunea PDF a acestui document, selectaţi Domain Name System (aproximativ 625 KB).

### Salvarea fişierelor PDF

Pentru a salva un PDF pe staţia dumneavoastră de lucru pentru vizualizare sau tipărire:

1. Faceţi clic dreapta pe PDF în browser-ul dumneavoastră (faceţi clic dreapta pe legătura de mai sus).
2. Faceţi clic pe opţiunea de salvare locală a PDF-ului.
3. Navigaţi la directorul în care doriţi să salvaţi PDF-ul.
4. Faceţi clic pe **Save**.

### Descărcarea programului Adobe Reader

Trebuie să aveţi instalat pe sistem Adobe Reader pentru a vizualiza sau tipări aceste PDF-uri. Puteţi descărca o copie gratuită de pe situl Web Adobe (www.adobe.com/products/acrobat/readstep.html)  .

## Conceptele Domain Name System

Acest subiect explică ce este DNS-ul (Domain Name System) şi cum funcţionează acesta. De asemenea, prezintă diferitele tipuri de zone care pot fi definite pe un server DNS.

DNS-ul (Domain Name System) reprezintă un sistem de baze de date distribuite pentru administrarea numelor de gazdă şi a adreselor lor IP (Internet Protocol) asociate. DNS permite folosirea unor nume simple, cum ar fi as www.jkltoys.com, pentru a localiza o gazdă, în loc să se folosească adresa IP (xxx.xxx.xxx.xxx). Un singur server poate asigura numai cunoaşterea numelor de gazdă şi a adreselor IP dintr-o mică subreţea a unei zone, dar serverele DNS pot funcţiona împreună pentru maparea tuturor numelor de domeniu la adresele lor IP. Conlucrarea serverelor DNS permite calculatoarelor să comunice prin Internet.

Datele DNS sunt structurate într-o ierarhie de domenii. Serverele asigură cunoaşterea unei mici părţi a datelor, de exemplu datele dintr-un singur subdomeniu. Partea domeniului pentru care serverul este direct responsabil se numeşte zonă. Un server DNS care are informaţii şi date complete despre gazdele dintr-o zonă deţine autoritatea pentru zona respectivă. Un server cu autoritate poate răspunde la interogările despre gazdele din zona sa utilizând propriile sale înregistrări resursă. Procesarea interogărilor depinde de un anumit număr de factori. Înţelegerea interogărilor DNS oferă explicaţii cu privire la căile pe care un client le poate utiliza pentru a rezolva o interogare.

# Înţelegerea zonelor

Acest subiect explică zonele DNS (Domain Name System) şi tipurile de zone.

Datele DNS sunt împărţite în seturi de date administrative numite *zone*. Zonele conţin informaţii despre 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 interogările DNS pentru un subdomeniu particular către alt server DNS. În acest caz, serverul DNS pentru domeniu poate fi configurat pentru a transmite interogările subdomeniului către serverul corespunzător.

Pentru rezervă sau redundanţă, datele de zonă sunt adesea stocate pe alte servere decât serverele DNS cu autoritate. Aceste servere sunt numite servere secundare, care încarcă datele de zonă de pe serverul cu autoritate. Configurarea unor servere secundare vă permite să echilibraţi cererile pe servere şi de asemenea vă furnizează o rezervă în cazul în care serverul primar 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.

## Tipurile de zone DNS

Puteţi folosi serverul DNS iSeries pentru a defini diferite tipuri de zone, care vă ajută să administraţi datele DNS:

**Zona primară**
Zona primară încarcă datele de zonă direct dintr-un fişier de pe o gazdă. Poate conţine o subzonă sau o zonă copil. De asemenea, ea poate conţine înregistrări resursă, cum ar fi gazda, aliasul (CNAME), adresa (A) sau înregistrări PTR (reverse mapping pointer - pointer de mapare inversă).

**Notă:** În altă documentaţie BIND se face uneori referire la zonele primare 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 unuia sau mai multor servere de nume.

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

**Gazda** Un obiect gazdă mapează înregistrările A şi PTR la o gazdă. Cu o gazdă se pot asocia înregistrări resursă suplimentare.

**Zona secundară**
Zona secundară încarcă datele de zonă din serverul primar al unei zone sau de pe alt server secundar. Menţine o copie completă a zonei pentru care este secundară.

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

**Zona de înaintare**

O zonă de înaintare (forward) direcţionează toate interogările pentru acea zonă particulară către alte servere.

**Concepte înrudite**

“Înţelegerea interogărilor Domain Name System”
Acest subiect explică modul în care DNS-ul (Domain Name System) rezolvă interogările în numele clienţilor.

“Configurarea zonelor pe un server de nume” la pagina 25
După ce configuraţi un server DNS (Domain Name System), trebuie să configuraţi zonele pentru serverul de nume.

**Referinţe înrudite**

“Exemplu: Un singur server Domain Name System pentru o reţea internă” la pagina 13
Acest exemplu descrie o subreţea simplă cu un server DNS (Domain Name System) pentru utilizare internă.

“Înregistrările resursă Domain Name System” la pagina 8
Acest subiect explică modul în care înregistrările resursă sunt utilizate de către DNS (Domain Name System). Înregistrările resursă sunt utilizate pentru a stoca date despre numele de domeniu şi adresele IP. Acest subiect conţine o listă de căutare a înregistrărilor resursă suportate pentru OS/400 V5R1.

## Înţelegerea interogărilor Domain Name System

Acest subiect explică modul în care DNS-ul (Domain Name System) rezolvă interogările în numele clienţilor.

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 către serverul DNS conţinând un FQDN (Fully qualified domain name - nume de domaniu complet calificat), un tip de interogare, ca de exemplu o anumită înregistrare resursă de care clientul are nevoie şi clasa pentru numele de domeniu, care de obicei este clasa IN (Internet). Următoarea figură prezintă eşantionul de reţea din exemplul cu un singur server DNS cu acces la Internet.

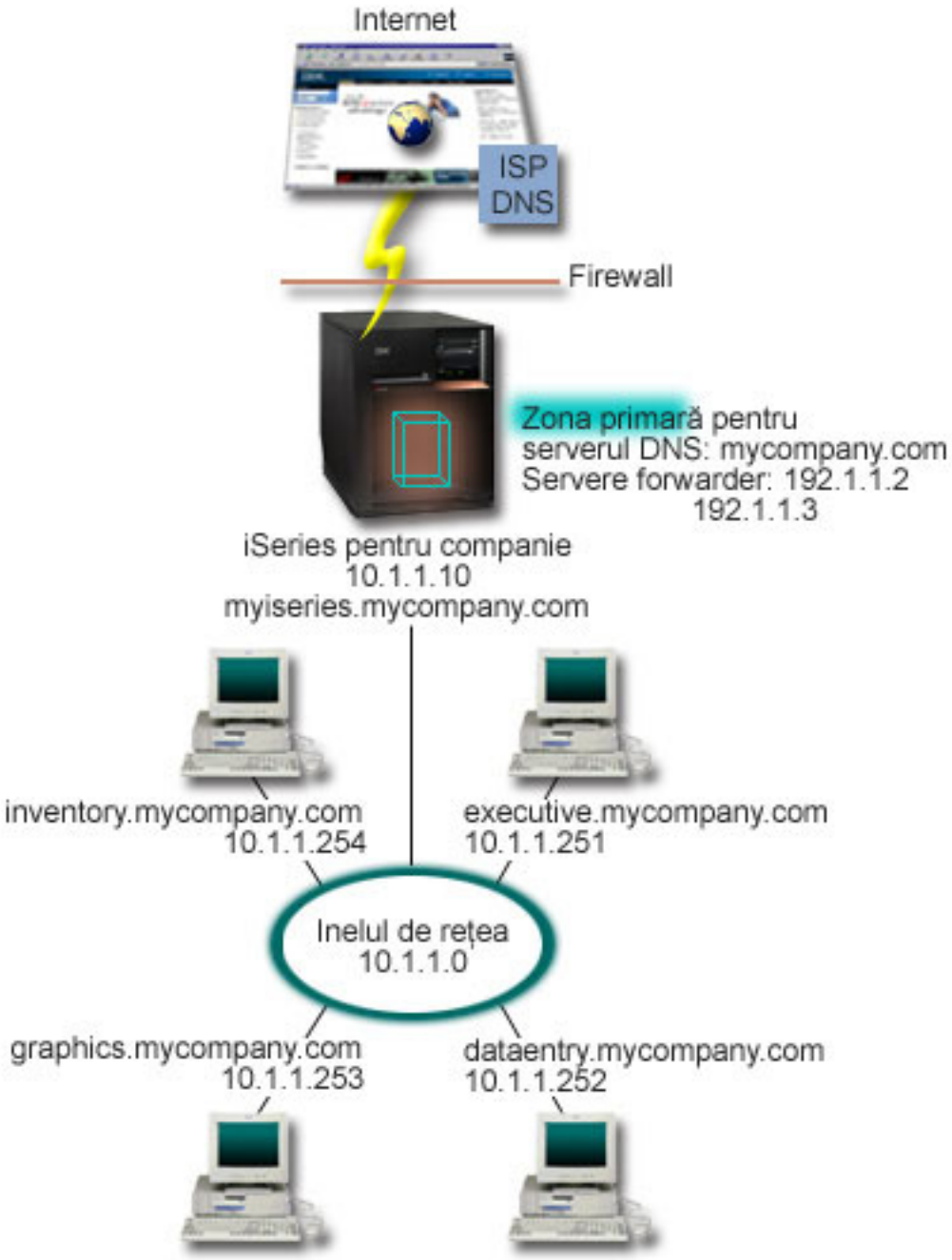



*Figura 1. Un singur server DNS cu acces la Internet*

Să presupunem că gazda *dataentry* interoghează serverul DNS pentru graphics.mycompany.com. Serverul DNS utilizează propriile sale date de zonă şi răspunde cu adresa IP 10.1.1.253.

Acum să presupunem că *dataentry* cere adresa IP pentru www.jkl.com. Această gazdă nu se află în datele de zonă ale serverului DNS. Acum există două căi de urmat, recursivitate sau iteraţie. Dacă un server DNS este setat să utilizeze recursivitatea, atunci serverul poate întreba sau poate contacta alt server DNS în numele clientului care a făcut cererea pentru a rezolva în totalitate problema numelui, după care trimite răspunsul înapoi la client. Dacă serverul DNS interoghează un alt server DNS, serverul care face cererea va stoca răspunsul în memoria cache pentru a-l putea folosi

ulterior la o astfel de interogare. Un client poate încerca să contacteze în nume propriu alte servere DNS pentru a rezolva un nume. În acest proces, numit *iteraţie*, clientul utilizează interogări separate şi suplimentare bazate pe răspunsurile referral primite de la servere.

**Referinţe înrudite**

"Înţelegerea zonelor" la pagina 2
Acest subiect explică zonele DNS (Domain Name System) şi tipurile de zone.

"Exemplu: Un singur server Domain Name System cu acces la Internet" la pagina 14
Acest exemplu descrie o subreţea simplă cu un server DNS (Domain Name System) conectat direct la Internet.

## Setarea domeniului DNS (Domain Name System)

Acest subiect oferă o privire generală asupra înregistrării domeniilor, având legături la alte situri de referinţă pentru setarea spaţiului dumneavostră de domeniu.

DNS (Domain Name System) vă permite să beneficiaţi de nume şi adrese într-o reţea internă sau intranet. De asemenea, vă permite să beneficiaţi de nume şi adrese către restul lumii prin intermediul Internetului. Dacă doriţi să setaţi domenii pe Internet, trebuie să înregistraţi un nume de domeniu.

Dacă setaţi o reţea internă, nu este necesar să înregistraţi un nume de domeniu pentru utilizarea internă. Înregistrarea sau nu a unui nume de domeniu intranet depinde de dorinţa dumneavoastră de a vă asigura că nimeni altcineva nu va putea folosi numele respectiv pe Internet, independent de utilizarea dumneavoastră internă. Prin înregistrarea unui nume pe care intenţionaţi să îl utilizaţi pe plan intern vă asiguraţi că nu veţi avea niciodată conflicte în cazul în care veţi dori să utilizaţi numele respectiv de domeniu într-o reţea externă.

Înregistrarea unui domeniu poate fi realizată printr-un contact direct cu un registrator autorizat de nume de domeniu sau prin anumite ISP-uri (Internet Service Provider - Furnizor de servicii Internet). 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 registru cu toţi registratorii de nume de domeniu care sunt autorizaţi de ICANN (Internet Corporation for Assigned Names and Numbers - Corporaţia Internet pentru nume şi numere alocate).

**Referinţe înrudite**

"Exemplu: Un singur server Domain Name System cu acces la Internet" la pagina 14
Acest exemplu descrie o subreţea simplă cu un server DNS (Domain Name System) conectat direct la Internet.

**Informaţii înrudite**

InterNIC (Internet Network Information Center)

## Actualizările dinamice

DNS-ul OS/400 V5R1 bazat pe BIND 8 suportă actualizări dinamice. Acestea permit surselor din exterior, cum este fi DHCP (Dynamic Host Configuration Protocol), să trimită actualizări către serverul DNS (Domain Name System).

DHCP reprezintă un standard TCP/IP care utilizează un server central pentru gestionarea adreselor IP şi a 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 să automatizaţi configuraţia gazdelor. Este adesea utilizată pentru alocarea de adrese IP temporare 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 trebuia să fie create şi întreţinute 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 către serverul DNS, ori de câte ori el asignează o nouă adresă la o gazdă. Această procesare automatizată reduce administrarea serverului DNS în reţelele care se extind sau care modifică rapid TCP/IP-ul şi în reţelele unde gazdele îşi schimbă frecvent locaţiile. Când un client care utilizează DHCP primeşte o adresă IP, acele date sunt imediat trimise către serverul DNS. Utilizând această metodă, DNS-ul poate continua rezolvarea cu succes a interogărilor pentru gazde, chiar dacă adresele lor IP se schimbă.

Puteţi configura DHCP pentru a actualiza în numele unui client înregistrările (A) (address mapping - mapare adrese), înregistrările PTR (reverse-lookup pointer) sau ambele. Înregistrarea A mapează numele de gazdă al unei maşini la adresa ei IP. Înregistrarea PTR mapează adresa IP a unei maşini o adresă la numele ei de gazdă. Când se modifică o adresă a unui client, DHCP poate trimite automat o actualizare către serverul DNS, astfel încât alte gazde din reţea să poată localiza clientul prin interogările DNS la noua sa adresă IP. Pentru fiecare înregistrare care este actualizată dinamic se scrie o înregistrare TXT (Text) asociată pentru a identifica că înregistrarea a fost scrisă de DHCP.

**Notă:** Dacă setaţi DHCP-ul să actualizeze doar înregistrările PTR, trebuie să configuraţi DNS-ul pentru a permite actualizări de la clienţi, astfel încât fiecare client să-şi poată actualiza înregistrarea A care îi aparţine. Nu toţi clienţii DHCP îşi pot face cererile de actualizare la înregistrarea 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 sursele autorizate utilizând adrese IP individuale, subreţele întregi, pachete care au fost semnate folosindu-se o cheie partajată secretă (numită TSIG, sau *Transaction Signature* - Semnătură de tranzacţie), sau orice combinaţie a acestor metode. Înainte de actualizarea înregistrărilor resursă, DNS-ul verifică dacă pachetele de cereri de intrare provin de la o sursă autorizată.

Actualizările dinamice pot fi realizate între DNS şi DHCP pe un singur server iSeries, între diferite servere iSeries, sau între un server iSeries şi alte servere care sunt capabile de actualizări dinamice.

**Notă:** API-ul (Application programming interface) de actualizare dinamică QTOBUPT este necesar pe serverele care trimit actualizări dinamice către DNS. Este instalat automat cu Opţiunea 31 a i5/OS, DNS.

**Concepte înrudite**

DHCP (Dynamic Host Configuration Protocol - Protocolul de configurare a gazdei dinamice)

**Operaţii înrudite**

“Configurarea Domain Name System pentru recepţionarea de actualizări dinamice” la pagina 25
Serverele DNS (Domain Name System) care rulează BIND 8 pot fi configurate pentru a accepta cereri de la alte surse pentru actualizarea dinamică a datelor de zonă. Acest subiect furnizează instrucţiuni pentru configurarea opţiunii de permitere-actualizare pentru ca DNS să poată recepţiona actualizări dinamice.

Configurarea DHCP pentru trimiterea de actualizări dinamice

**Referinţe înrudite**

“Exemplu: Domain Name System şi Dynamic Host Configuration Protocol pe acelaşi server iSeries” la pagina 16
Acest exemplu descrie DNS (Domain Name System) şi DHCP (Dynamic Host Configuration Protocol) pe acelaşi server.

“Înregistrările resursă Domain Name System” la pagina 8
Acest subiect explică modul în care înregistrările resursă sunt utilizate de către DNS (Domain Name System). Înregistrările resursă sunt utilizate pentru a stoca date despre numele de domeniu şi adresele IP. Acest subiect conţine o listă de căutare a înregistrărilor resursă suportate pentru OS/400 V5R1.

QTOBUPT

“Caracteristici BIND 8”
Pe lângă actualizările dinamice, BIND 8 oferă mai multe opţiuni pentru îmbunătăţirea performanţei serverului dumneavoastră DNS (Domain Name System).

## Caracteristici BIND 8

Pe lângă actualizările dinamice, BIND 8 oferă mai multe opţiuni pentru îmbunătăţirea performanţei serverului dumneavoastră DNS (Domain Name System).

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

## Rularea mai multor servere DNS pe un singur sistem iSeries.

În ediţiile anterioare se putea configura doar un singur server DNS. 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 instanţe DNS nu pot asculta pe aceeaşi interfaţă.

O aplicaţie practică de servere multiple este DNS-ul divizat, un server având autoritatea pentru o reţea internă, iar un al doilea server fiind utilizat pentru cereri externe.

## Înaintarea condiţionată

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

## Securizarea actualizărilor dinamice

DHCP (Dynamic Host Configuration Protocol) şi alte surse autorizate pot trimite actualizările dinamice ale înregistrărilor resursă utilizând TSIG (Transaction Signatures) 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.

## 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 datele s-au modificat. 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 curentă a unei rezerve a datelor de zonă.

## Transferuri de zonă (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 (AXFR) (All zone transfer - transfer pentru toate zonele). BIND 8 suportă o nouă metodă de transfer de zonă: IXFR (Incremental zone transfer - transfer incremental de zone). IXFR este o modalitate prin care alte servere pot transfera doar datele schimbate, în loc de a transfera întreaga zonă.

Când sunt activate pe serverul primar, modificărilor de date li se alocă un steguleţ pentru a indica faptul că a apărut o schimbare. Când un server secundar cere actualizarea unei zone într-un mod IXFR, serverul primar va trimite doar datele noi. IXFR este util mai ales atunci când o zonă este actualizată dinamic. Acest tip de transfer reduce încărcarea de trafic prin trimiterea de cantităţi reduse de date.

**Notă:** Atât serverul primar, cât şi serverul secundar trebuie să suporte activarea IXFR pentru a utiliza această caracteristică.

**Concepte înrudite**

“Cerinţele Domain Name System” la pagina 22
Acest subiect descrie cerinţele software pentru a putea rula DNS (Domain Name System) pe serverul dumneavoastră iSeries.

“Actualizările dinamice” la pagina 5
DNS-ul OS/400 V5R1 bazat pe BIND 8 suportă actualizări dinamice. Acestea permit surselor din exterior, cum este fi DHCP (Dynamic Host Configuration Protocol), să trimită actualizări către serverul DNS (Domain Name System).

**Referinţe înrudite**

"Exemplu: Divizarea Domain Name System peste firewall" la pagina 18
Acest exemplu descrie operarea DNS (Domain Name System) peste un firewall pentru protejarea datelor interne împotriva Internetului, permiţând totodată utilizatorilor interni să acceseze date de pe Internet.

"Proiectarea măsurilor de securitate" la pagina 21
DNS (Domain Name System) oferă opţiuni de securitate pentru limitarea accesului din exterior la serverul dumneavoastră.

## Înregistrările resursă Domain Name System

Acest subiect explică modul în care înregistrările resursă sunt utilizate de către DNS (Domain Name System). Înregistrările resursă sunt utilizate pentru a stoca date despre numele de domeniu şi adresele IP. Acest subiect conţine o listă de căutare a înregistrărilor resursă suportate pentru OS/400 V5R1.

O bază de date a zonei DNS constituie o colecţie de înregistrări resursă. Fiecare înregistrare resursă specifică informaţiile despre un anumit obiect. Spre exemplu, înregistrările (A) (Address mapping - Mapare adresă) mapează un nume gazdă la o adresă IP, iar înregistrările PTR (Reverse-lookup pointer - Pointer căutare inversă) mapează o adresă IP la un nume gazdă. Serverul utilizează aceste înregistrări pentru a răspunde la interogări pentru gazdele din zona sa. Pentru mai multe informaţii, utilizaţi tabela de mai jos pentru a vizualiza înregistrările resursă DNS.

*Tabela 1. Tabela de căutare a înregistrărilor resursă*

| **Înregistrarea resursă** | **Abrevierea** | **Descrierea** |
|---|---|---|
| Înregistrările Address Mapping (Mapare adrese) | A | Înregistrarea A specifică adresa IP a acestei gazde. Înregistrările A sunt utilizate pentru a rezolva o interogare pentru adresa IP a unui nume de domeniu specific. Acest tip de înregistrare este definit în RFC (Request for Comments) 1035. |
| Înregistrările Andrew File System Database (Baze de date în 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 sa AFSDB; sau pentru maparea din numele domeniului a unei celule la serverele de nume autentificate pentru acea celulă. Acest tip de înregistrări este definit în RFC 1183. |
| Înregistrările Canonical Name (Nume canonic) | CNAME | Înregistrarea CNAME specifică numele real de domeniu al acestui obiect. 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. |
| Înregistrările Host Information (Informaţii gazdă) | HINFO | Înregistrarea HINFO specifică informaţiile generale despre o maşină gazdă. Numele de CPU-uri standard şi de sisteme de operare sunt definite în Assigned Numberers RFC 1700. Totuşi, utilizarea numerelor standard nu este necesară. Acest tip de înregistrare este definit în RFC 1035. |

*Tabela 1. Tabela de căutare a înregistrărilor resursă (continuare)*

| Înregistrarea resursă | Abrevierea | Descrierea |
|---|---|---|
| Înregistrările Integrated Services Digital Network (Reţea digitală de servicii integrate) | 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. |
| Înregistrările IP Version 6 Address (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 potrivesc cu formatul standard de înregistrare A. Acest tip de înregistrare este definit în RFC 1886. |
| Înregistrările Location (Locaţie) | LOC | Înregistrarea LOC specifică locaţia fizică a componentelor de reţea. Aceste înregistrări pot fi utilizate de către aplicaţii pentru a evalua eficienţa reţelei sau pentru a mapa reţeaua fizică. Acest tip de înregistrare este definit în RFC 1876. |
| Înregistrările Mail Exchanger (Schimbare poştă) | MX | Înregistrările MX definesc o gazdă de schimbare poştă pentru poşta trimisă la acest domeniu. Aceste înregistrări sunt utilizate de SMTP (Simple Mail Transfer Protocol) pentru a localiza gazdele care procesează sau înaintează poşta pentru acest domeniu, împreună cu valorile de preferinţă pentru fiecare gazdă de schimbare poştă. Fiecare gazdă de schimbare poştă trebuie să aibă o înregistrare A de adresă gazdă corespunzătoare într-o zonă validă. Acest tip de înregistrare este definit în RFC 1035. |
| Înregistrările Mail Group (Grup de poştă) | MG | Înregistrările MG specifică numele de domeniu al grupului de poştă. Acest tip de înregistrare este definit în RFC 1035. |
| Înregistrările Mailbox (Cutie poştală) | MB | Înregistrările MB specifică numele domeniului gazdă care conţine cutia poştală pentru acest obiect. Poşta trimisă către domeniul respectiv este direcţionată către gazda specificată în înregistrarea MB. Acest tip de înregistrare este definit în RFC 1035. |
| Înregistrarea Mailbox Information (Informaţii cutie poştală) | MINFO | Înregistrările MINFO specifică cutia poştală care ar trebui să primească mesaje sau erori pentru acest obiect. Înregistrarea MINFO este mult mai frecvent utilizată pentru liste de corespondenţă decât pentru o singură cutie poştală. Acest tip de înregistrare este definit în RFC 1035. |

*Tabela 1. Tabela de căutare a înregistrărilor resursă (continuare)*

| **Înregistrarea resursă** | **Abrevierea** | **Descrierea** |
|---|---|---|
| Înregistrările Mailbox Rename (Redenumire cutie poştală) | MR | Înregistrările MR specifică un nou nume de domeniu pentru o cutie poştală. Utilizaţi înregistrarea MR ca o intrare de expediere pentru un utilizator care şi-a schimbat cutia poştală. Acest tip de înregistrare este definit în RFC 1035. |
| Înregistrările Name Server (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. |
| Înregistrările 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. |
| Înregistrările Public Key (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 o gazdă. Acest tip de înregistrare este definit în RFC 2065. |
| Înregistrările Responsible Person (Persoana responsabilă) | RP | Înregistrarea RP specifică adresa de poştă Internet şi descrierea persoanei responsabile pentru această zonă sau gazdă. Acest tip de înregistrare este definit în RFC 1183. |
| Înregistrările Reverse-lookup Pointer (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. |
| Înregistrările Route Through (Rută prin) | RT | Înregistrarea RT specifică un nume domeniu gazdă care poate acţiona ca un forwarder de pachete IP pentru această gazdă. Acest tip de înregistrări este definit în RFC 1183. |
| Înregistrările Start of Authority (Început de 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 zonă şi regulile de reîncărcare pentru serverele secundare. Nu poate exista decât o singură înregistrare SOA per zonă. Acest tip de înregistrare este definit în RFC 1035. |

*Tabela 1. Tabela de căutare a înregistrărilor resursă (continuare)*

| Înregistrarea resursă | Abrevierea | Descrierea |
|---|---|---|
| Înregistrările 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 (Responsible person - persoana responsabilă), pentru a furniza informaţii despre cine este responsabil pentru o anumită zonă. Acest tip de înregistrare este definit în RFC 1035.<br><br>Înregistrările TXT sunt utilizate de către 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 au un prefix de AS400 DHCP. |
| Înregistrările Well-Known Services (Servicii binecunoscute) | WKS | Înregistrarea WKS specifică serviciile binecunoscute 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. |
| Înregistrările X.400 Address Mapping (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. |
| Înregistrările X25 Address Mapping (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. |

**Concepte înrudite**

“Actualizările dinamice” la pagina 5
DNS-ul OS/400 V5R1 bazat pe BIND 8 suportă actualizări dinamice. Acestea permit surselor din exterior, cum este fi DHCP (Dynamic Host Configuration Protocol), să trimită actualizări către serverul DNS (Domain Name System).

“Înregistrările Mail şi Mail Exchanger”
DNS (Domain Name System) suportă rutarea avansată de poştă prin utilizarea înregistrărilor Mail şi MX (Mail Exchanger - Schimbare de poştă).

**Referinţe înrudite**

“Exemplu: Un singur server Domain Name System pentru o reţea internă” la pagina 13
Acest exemplu descrie o subreţea simplă cu un server DNS (Domain Name System) pentru utilizare internă.

“Înţelegerea zonelor” la pagina 2
Acest subiect explică zonele DNS (Domain Name System) şi tipurile de zone.

## Înregistrările Mail şi Mail Exchanger

DNS (Domain Name System) suportă rutarea avansată de poştă prin utilizarea înregistrărilor Mail şi MX (Mail Exchanger - Schimbare de poştă).

Înregistrările Mail şi MX sunt utilizate de programele de rutare poştă, cum ar fi SMTP (Simple Mail Transfer Protocol). Tabela de căutare în înregistrările de resursă DNS conţin tipurile de înregistrări de poştă suportate de DNS-ul iSeries.

DNS include informaţii pentru trimiterea poştei electronice prin utilizarea informaţiei de 'mail exchanger'. Dacă reţeaua utilizează DNS, o aplicaţie SMTP nu livrează poşta 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 specifică

Serverele DNS utilizează înregistrări resursă cunoscute sub numele de înregistrări MX *schimbare poştă*. Înregistrările MX mapează un domeniu sau un nume de domeniu la o valoare de preferinţă şi nume de gazdă. În general, înregistrările MX sunt utilizate pentru a indica că o gazdă este utilizată pentru a procesa mail pentru altă gazdă. De asemenea, înregistrările sunt utilizate pentru a desemna o altă gazdă către care să fie livrată poşta, în cazul în care prima gazdă nu poate fi contactată. Cu alte cuvinte, ele permit ca poşta adresată unei gazde să fie livrată altei gazde.

Pot exista multiple înregistrările resursă MX pentru acelaşi nume de domeniu sau de gazdă. Când există mai multe înregistrări MX pentru acelaşi domeniu sau gazdă, valoarea de preferinţă a fiecărei înregistrări determină ordinea în care ele sunt încercate. Cea mai mică valoare de preferinţă corespunde celei mai preferate înregistrări, care este prima încercată. 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, este posibil ca aplicaţia de trimitere poştă să încerce să stabilească o conexiune directă cu gazda de destinaţie.

**Notă:** Nu se recomandă utilizarea unui caracter de înlocuire (de exemplu: *.mycompany.com) în înregistrările MX pentru un domeniu.

### Exemplu: înregistrare MX pentru o gazdă

În exemplul următor, sistemul ar trebui ca, după preferinţă, să livreze poşta pentru fsc5.test.ibm.com chiar către gazdă. Dacă gazda nu poate fi contactată, sistemul poate livra poşta la psfred.test.ibm.com sau la mvs.test.ibm.com (dacă nici psfred.test.ibm.com nu poate fi contactat). Acesta este un exemplu despre cum vor arăta 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
```

**Referinţe înrudite**

"Înregistrările resursă Domain Name System" la pagina 8
Acest subiect explică modul în care înregistrările resursă sunt utilizate de către DNS (Domain Name System). Înregistrările resursă sunt utilizate pentru a stoca date despre numele de domeniu şi adresele IP. Acest subiect conţine o listă de căutare a înregistrărilor resursă suportate pentru OS/400 V5R1.

## Exemple de Domain Name System

Puteţi utiliza aceste exemple pentru a înţelege modul de utilizare al DNS-ului (Domain Name System (DNS) în reţeaua dumneavoastră.

DNS reprezintă un sistem de baze de date distribuite pentru gestionarea numelor de gazdă şi a adreselor IP asociate acestora. Următoarele exemple vă explică cum funcţionează DNS-ul şi cum îl puteţi folosi în reţeaua dumneavoastră. Exemplele descriu setarea şi motivele pentru care va fi utilizată. De asemenea, fac legături către concepte înrudite care vă pot fi utile în înţelegerea pozelor.

## Exemplu: Un singur server Domain Name System pentru o reţea internă

Acest exemplu descrie o subreţea simplă cu un server DNS (Domain Name System) pentru utilizare internă.

Următoarea ilustrare imagine descrie DNS rulând pe un iSeries pentru 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.

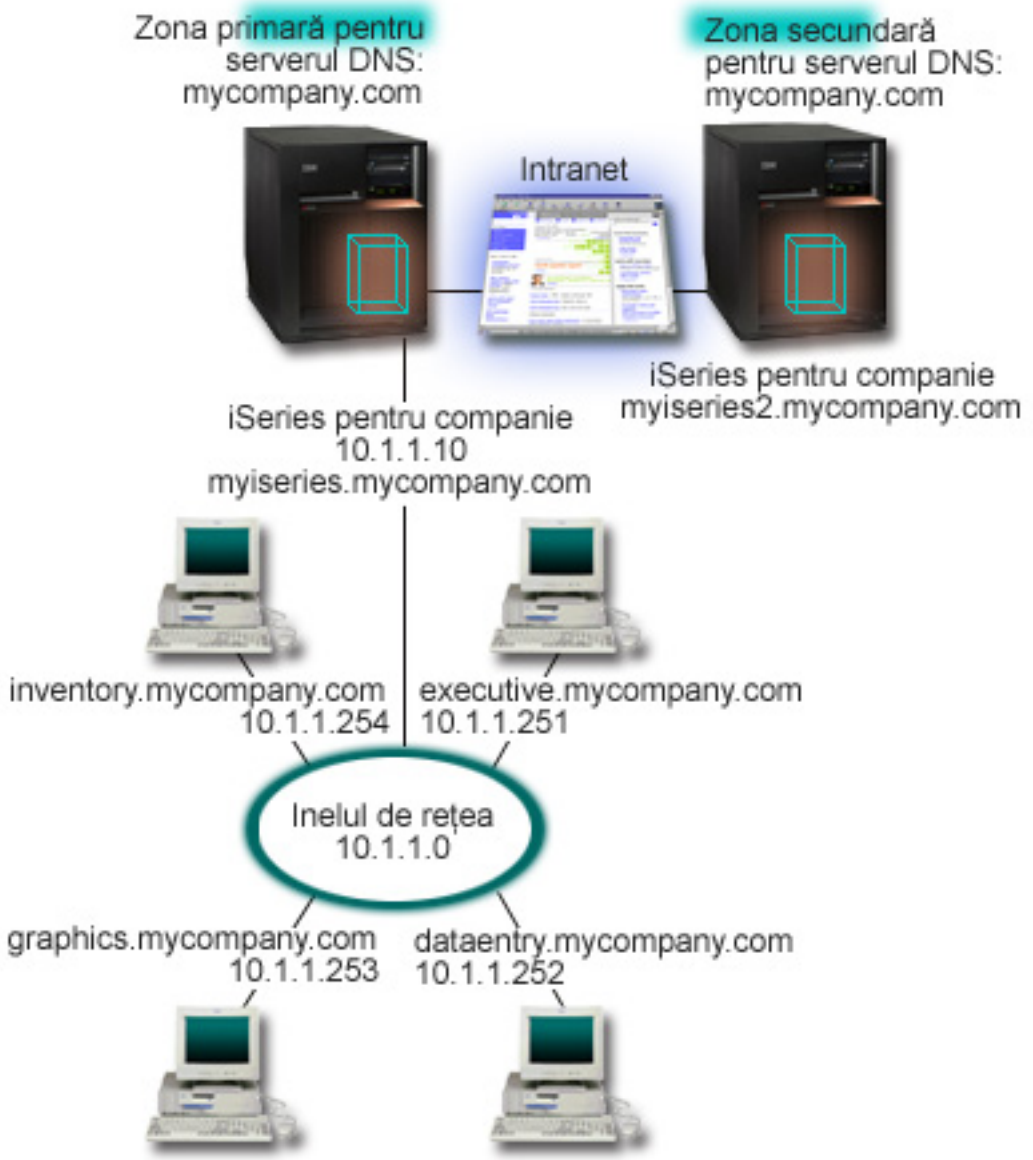



*Figura 2. Un singur server DNS pentru o reţea internă*

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 de înregistrări 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 în reţeaua dumneavoastră internă. Spre exemplu, dacă rulaţi sisteme interne de poştă electronică, s-ar putea sa fiţi nevoit să adăugaţi înregistrări MX (Mail exchanger - Schimbare de poştă), astfel încât SMTP să poată interoga DNS pentru a afla sistemele pe care rulează serverele de poştă.

Dacă această reţea mică ar face parte dintr-o reţea internă mai mare, ar fi necesar să definiţi servere rădăcină 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 2, serverul myiseries server face parte dintr-o reţea internă. Un alt server iSeries server, myiseries2, a fost configurat pentru a acţiona ca server DNS 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.

**Referinţe înrudite**

"Înregistrările resursă Domain Name System" la pagina 8
Acest subiect explică modul în care înregistrările resursă sunt utilizate de către DNS (Domain Name System). Înregistrările resursă sunt utilizate pentru a stoca date despre numele de domeniu şi adresele IP. Acest subiect conţine o listă de căutare a înregistrărilor resursă suportate pentru OS/400 V5R1.

"Înţelegerea zonelor" la pagina 2
Acest subiect explică zonele DNS (Domain Name System) şi tipurile de zone.

"Exemplu: Un singur server Domain Name System cu acces la Internet"
Acest exemplu descrie o subreţea simplă cu un server DNS (Domain Name System) conectat direct la Internet.

## Exemplu: Un singur server Domain Name System cu acces la Internet

Acest exemplu descrie o subreţea simplă cu un server DNS (Domain Name System) conectat direct la Internet.

Următoarea imagine descrie acelaşi exemplu de reţea ca şi exemplul de server DNS singur pentru reţea internă, însă acum compania a adăugat 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.

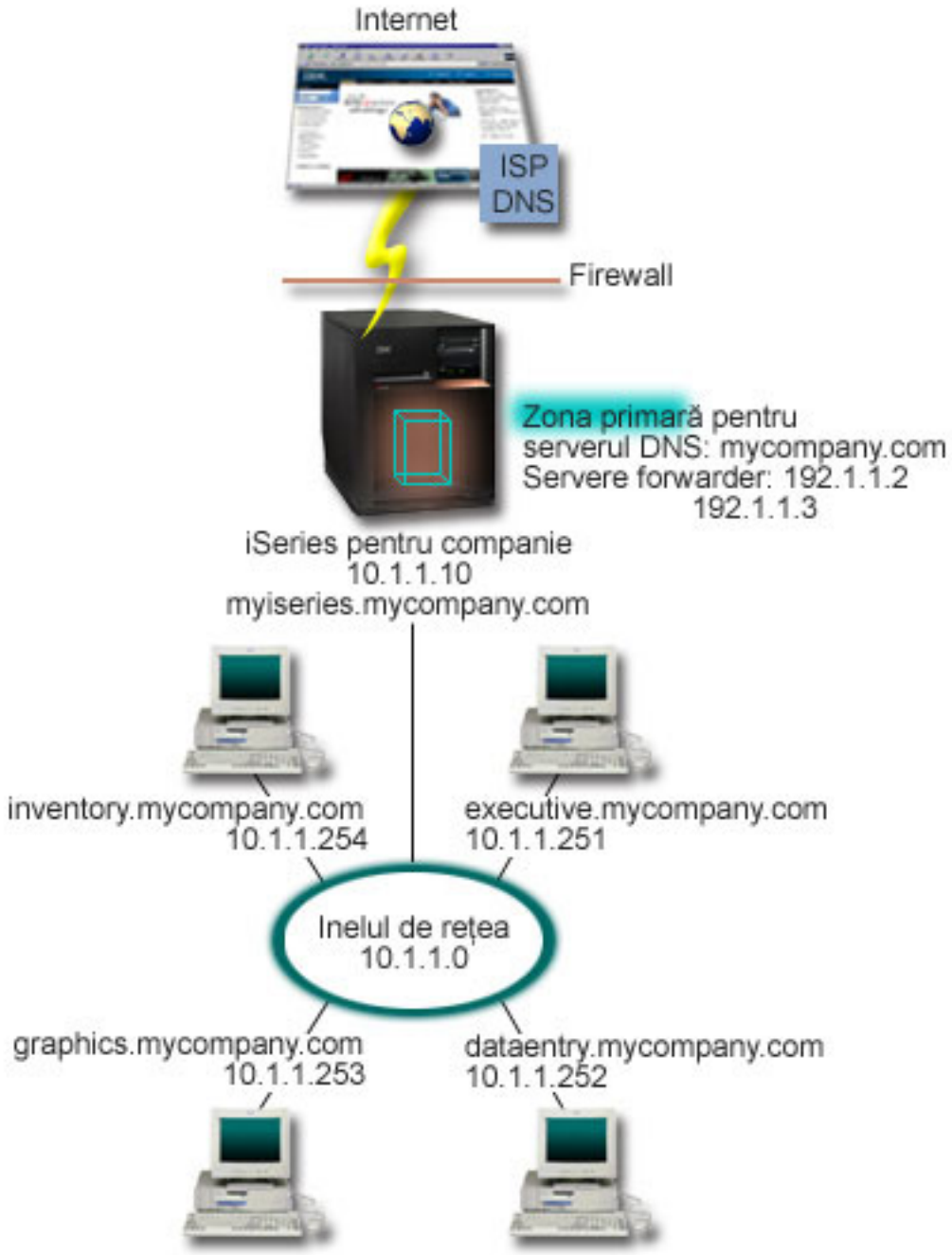



*Figura 3. Un singur server DNS cu acces la Internet*

Pentru a rezolva adresele Internet, trebuie să faceţi cel puţin una dintre următoarele operaţii:

- Definirea serverelor rădăcină Internet

  Puteţi încărca automat serverele rădăcină Internet implicite, dar s-ar putea să fie nevoie să actualizaţi lista. Aceste servere vă pot ajuta să rezolvaţi adresele din afara zonei dumneavoastră. Pentru instrucţiuni de obţinere a serverelor rădăcină Internet actuale, vedeţi “Accesarea datelor Domain Name System externe” la pagina 26.
- Activarea înaintării

  Puteţi seta acţiunea de înaintare pentru a transmite interogările pentru zonele din afara mycompany.com către servere DNS externe, cum ar fi serverele DNS rulate de ISP-ul (Internet service provider - Furnizor de servicii Internet) dumneavoastră. Dacă doriţi să activaţi căutarea atât de către serverele de înaintare, cât şi de către cele rădăcină,

trebuie să setaţi opţiunea înaintare la **prima**. Mai întâi, serverul încearcă acţiunea de înaintare, iar apoi interoghează serverele rădăcină doar dacă acţiunea de înaintare eşuează în rezolvarea interogării.

Pot fi de asemenea cerute următoarele modificări de configurare:

- Alocarea de adrese 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. Acestea sunt prezentate mai jos ca exemplu, însă propriile adrese IP sunt determinate de către ISP-ul dumneavoastră şi de alţi factori care depind de reţea.
- Înregistrarea numelui dumneavoastră de domeniu

  Dacă sunteţi vizibil pe Internet şi încă nu sunteţi înregistrat, trebuie 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 vă luaţi alte măsuri de precauţie pentru securizarea serverului dumneavoastră iSeries.

**Concepte înrudite**

“Setarea domeniului DNS (Domain Name System)” la pagina 5
Acest subiect oferă o privire generală asupra înregistrării domeniilor, având legături la alte situri de referinţă pentru setarea spaţiului dumneavostră de domeniu.

iSeries şi securitatea pe Internet

“Înţelegerea interogărilor Domain Name System” la pagina 3
Acest subiect explică modul în care DNS-ul (Domain Name System) rezolvă interogările în numele clienţilor.

**Referinţe înrudite**

“Exemplu: Un singur server Domain Name System pentru o reţea internă” la pagina 13
Acest exemplu descrie o subreţea simplă cu un server DNS (Domain Name System) pentru utilizare internă.

## Exemplu: Domain Name System şi Dynamic Host Configuration Protocol pe acelaşi server iSeries

Acest exemplu descrie DNS (Domain Name System) şi DHCP (Dynamic Host Configuration Protocol) pe acelaşi server.

Configuraţia poate fi folosită pentru actualizarea dinamică a datelor de zonă DNS, când DHCP asignează adresele IP la gazde.

Următoarea figură descrie o mică subreţea cu un server iSeries care acţionează ca un server DHCP şi DNS pentru 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.

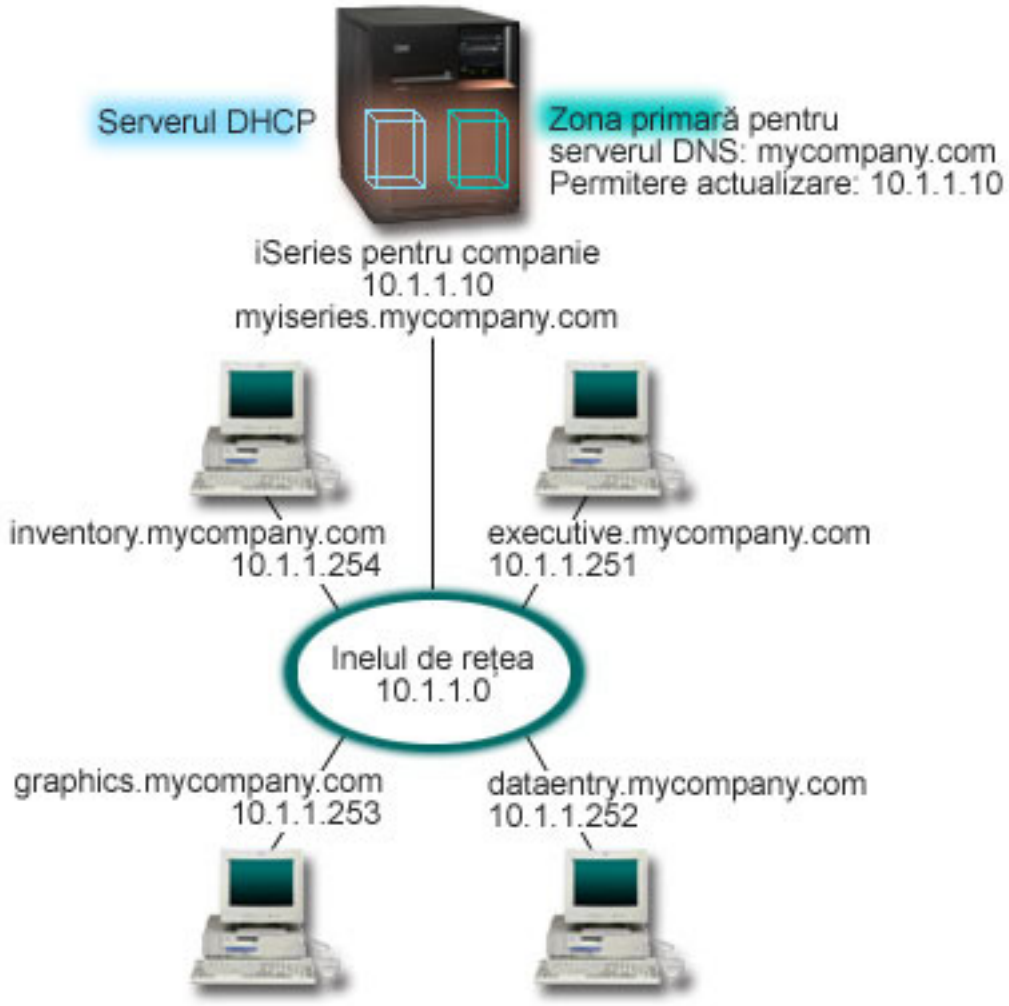



*Figura 4. DNS şi DHCP pe acelaşi server iSeries*

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 adresa IP a serverului de fişiere grafice se modifică pentru că este alocată de DHCP, atunci clienţii săi subordonaţi nu vor putea să mapeze un drive de reţea la numele său de gazdă deoarece înregistrările DNS vor conţine adresa IP anterioară a serverului de fişiere.

Cu serverul DNS V5R1 OS/400 bazat pe BIND 8, puteţi configura zona dumneavoastră DNS pentru a accepta actualizările dinamice la înregistrările DNS în conjuncţie cu modificările intermitente de adresă prin DHCP. Spre exemplu, atunci când serverul de fişiere grafice îşi va reînnoi închirierea adresei şi când serverul DHCP îi va aloca o adresă IP de 10.1.1.250, înregistrările DNS asociate vor fi actualizate în mod dinamic. 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. Dacă procedaţi aşa, este posibil să cauzaţi interferenţe 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 ar trebui să configuraţi o zonă dinamică separată pentru a minimiza necesitatea de actualizări manuale. Vedeţi “Determinarea structurii domeniului” la pagina 20 pentru mai multe informaţii privind 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 zone are date de permitere-actualizare, însă alte zone definite pe server pot 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.
- Configurarea preferinţelor de actualizare pentru serverul 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, ar trebui să configuraţi IXFR-urile (Incremental zone transfers - transferuri incrementale de zonă), ceea ce permite serverelor secundare cu IXFR activate să urmărească şi să încarce doar datele de zonă actualizate, în locul întregii zone.

Dacă rulaţi DNS şi DHCP pe servere diferite, există unele cerinţe de configurare suplimentare pentru serverul DHCP.

**Concepte înrudite**

“Actualizările dinamice” la pagina 5
DNS-ul OS/400 V5R1 bazat pe BIND 8 suportă actualizări dinamice. Acestea permit surselor din exterior, cum este fi DHCP (Dynamic Host Configuration Protocol), să trimită actualizări către serverul DNS (Domain Name System).

“Determinarea structurii domeniului” la pagina 20
Dacă setaţi un domeniu pentru prima dată, ar trebui să elaboraţi un plan pentru cerere şi întreţinere înainte de a crea zonele.

**Operaţii înrudite**

Configurarea DHCP pentru trimiterea de actualizări dinamice

**Referinţe înrudite**

Exemplu: DNS şi DHCP pe servere iSeries diferite

## Exemplu: Divizarea Domain Name System peste firewall

Acest exemplu descrie operarea DNS (Domain Name System) peste un firewall pentru protejarea datelor interne împotriva Internetului, permiţând totodată utilizatorilor interni să acceseze date de pe Internet.

Următoarea ilustraţie prezintă o subreţea simplă care utilizează un firewall pentru securizare. DNS V5R1 OS/400 bazat pe BIND 8 permite setarea de servere DNS multiple pe un singur iSeries. Să presupunem că respectiva companie are o reţea internă cu spaţiu IP rezervat şi o secţiune externă a unei reţele care este disponibilă publicului.

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 aceasta, compania setează două instanţe de server DNS pe acelaşi server iSeries, una pentru reţeaua internă şi alta pentru toate elementele din domeniul său public. Aceasta poartă numele de *divizare DNS*.

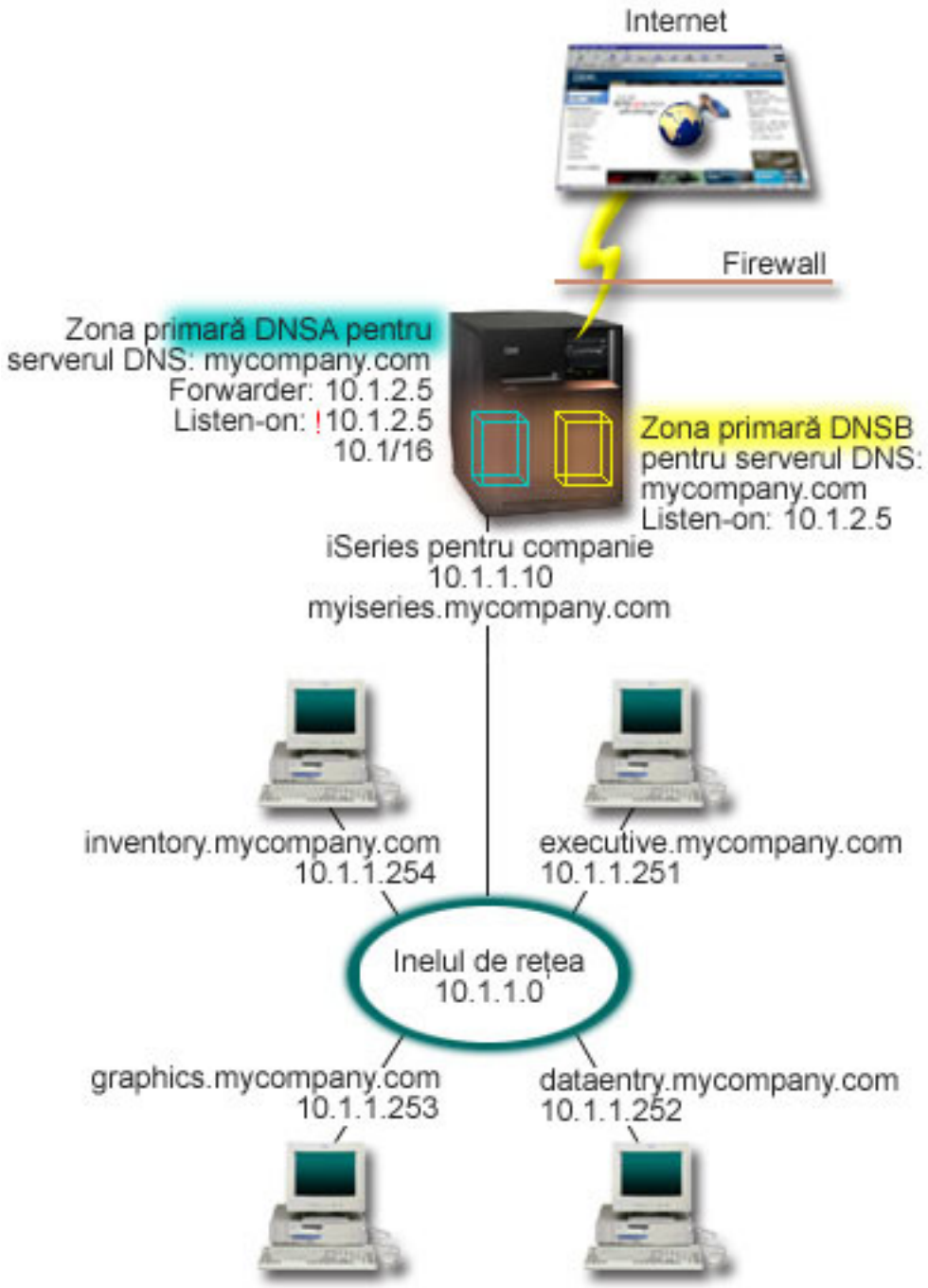



*Figura 5. Divizarea DNS peste firewall*

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 forţează DNSA să înainteze către serverul DNSB interogările pe care nu le poate rezolva.

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 toate acestea să funcţioneze corespunzător, clienţii interni vor trebui să fie configuraţi pentru a interoga doar serverul DNSA. Pentru a seta divizarea DNS, trebuie să luaţi în considerare următoarele setări de configurare:

- Ascultare-la

  În exemplele anterioare, nu exista decât un singur server DNS pe un iSeries. Este setat să asculte la toate adresele IP de interfaţă. Oricând aveţi mai multe servere DNS pe un iSeries, trebuie să definiţi adresele IP de interfaţă la care să asculte fiecare. Două servere DNS nu pot asculta la aceeaşi adresă. În acest caz, să presupunem că toate interogările care vin de la firewall sunt 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 (Address Match List - Lista de potrivire adresă)

  Este utilizat primul element din AML cu care se potriveşte o adresă. 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 este comparată cu primul element şi este refuzată imediat.

  Dacă elementele vor fi inversate (10.1/16; !10.1.2.5), adresei IP 10.1.2.5 i se va permite accesul deoarece serverul o va compara cu primul element, cu care se potriveşte şi deci îi va permite accesul fără a mai verifica şi restul regulilor.

  **Referinţe înrudite**

  “Caracteristici BIND 8” la pagina 6
  Pe lângă actualizările dinamice, BIND 8 oferă mai multe opţiuni pentru îmbunătăţirea performanţei serverului dumneavoastră DNS (Domain Name System).

## Proiectarea Domain Name System

DNS-ul (Domain Name System) oferă o varietate de soluţii. Înainte de a configura DNS, este important să proiectaţi modul în care acesta funcţionează în cadrul reţelei dumneavoastră. Se recomandă să accesaţi subiecte cum ar fi structura, performanţa şi securitatea reţelei înainte de a implementa DNS.

## Stabilirea autorizărilor Domain Name System

Există cerinţe de autorizaţie speciale pentru administratorul DNS (Domain Name System). De asemenea, ar trebui să luaţi în considerare implicaţiile autorizării privind securitatea.

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.

Este nevoie de un nivel minim de autorizare pentru a permite administratorului serverului dumneavoastră iSeries 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 configurează DNS să aibă acces de responsabil cu securitatea asupra autorizării *ALLOBJ (all object - toate obiectele). Utilizaţi Navigator iSeries pentru a autoriza utilizatorii. Dacă doriţi mai multe informaţii, citiţi Acordarea autorizării către administratorul DNS din ajutorul online DNS.

**Notă:** Dacă profilul unui administrator nu are autorizare deplină, trebuie să i se acorde acces şi autorizare specifice la toate directoarele DNS şi la fişierele de configurare înrudite din serverul respectiv.

**Referinţe înrudite**

“Întreţinerea fişierelor de configurare Domain Name System” la pagina 30
Acest subiect vă ajută să înţelegeţi fişierele pe care le foloseşte DNS-ul (Domain Name System) şi să treceţi în revistă indicaţiile pentru a le face copii de rezervă şi a le întreţine.

## 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.

Este important să determinaţi cum să divizaţi domeniul sau subdomeniile dumneavoastră în zone, cum să satisfaceţi cel mai bine cerinţele reţelei, să accesaţi Internetul şi cum să trataţi firewall-urile. Aceşti factori pot fi complecşi şi trebuie trataţi caz cu caz. Pentru indicaţii mai amănunţite, referiţi-vă la surse cu autoritate, cum ar fi cartea O'Reilly despre DNS şi BIND.

Dacă configuraţi o zonă DNS (Domain Name System) ca zonă dinamică, nu puteţi face modificări manuale asupra datelor de zonă în timp ce serverul rulează. Dacă procedaţi aşa, este posibil să provocaţi interferenţe cu actualizările dinamice care sosesc. Dacă trebuie să faceţi actualizări manuale, opriţi serverul, faceţi modificările şi apoi reporniţi serverul. Actualizările dinamice trimise către un server DNS care este oprit, nu vor fi niciodată executate. Din acest motiv, poate ar trebui să configuraţi separat o zonă dinamică şi o zonă statică. Puteţi face aceasta prin crearea unor zone complet separate sau prin definirea unui nou subdomeniu, cum ar fi dynamic.mycompany.com, pentru acei clienţi care vor fi întreţinuţi în mod dinamic.

DNS iSeries furnizează o interfaţă grafică pentru configurarea serverelor dumneavoastră. 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 vă proiectaţi configuraţia DNS, vă poate fi de ajutor să ţineţi minte următoarele 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 la *zone secundare*.
- Interfaţa utilizează *subzonele*, la care unele surse se referă ca *subdomenii*. O zonă copil este o subzonă pentru care aţi delegat responsabilitatea către unu sau mai multe servere de nume.

**Referinţe înrudite**

"Exemplu: Domain Name System şi Dynamic Host Configuration Protocol pe acelaşi server iSeries" la pagina 16
Acest exemplu descrie DNS (Domain Name System) şi DHCP (Dynamic Host Configuration Protocol) pe acelaşi server.

## Proiectarea măsurilor de securitate

DNS (Domain Name System) oferă opţiuni de securitate pentru limitarea accesului din exterior la serverul dumneavoastră.

Securizarea serverul dumneavoastră DNS este esenţială. Pe lângă considerentele de securitate din acest subiect, securitatea DNS şi securitatea iSeries sunt tratate de o varietate de surse, incluzând iSeries şi Internetul din Centrul de informare. De asemenea, cartea DNS şi BIND tratează subiectul despre securitatea legată de DNS.

### Listele de potrivire adresă

DNS utilizează listele de potrivire adresă pentru a permite sau a refuza accesul entităţilor din exterior la anumite funcţii ale DNS. Acestea pot include adrese IP specifice, o subreţea (utilizând un prefix IP) sau utilizarea de chei TSIG (Transaction Signature). Puteţi defini o listă de entităţi cărora vreţi să le acordaţi sau să le refuzaţi accesul la o listă de potrivire adresă. Dacă vreţi să puteţi reutiliza o listă de potrivire adresă, puteţi salva lista respectivă ca un ACL (Access control list - Listă de control acces). După aceea, ori de câte ori aveţi nevoie să furnizaţi lista, puteţi apela ACL-ul şi întreaga listă va fi încărcată.

### Ordinea elementelor din lista de potrivire adresă

Este utilizat primul element dintr-o listă de potrivire adresă cu care se potriveşte o adresă. 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 vor fi inversate (10.1.1/24; !10.1.1.5), adresei IP 10.1.1.5 i se va permite accesul deoarece serverul o va compara cu primul element, cu care se potriveşte şi deci îi va permite accesul fără a verifica şi restul regulilor.

### Opţiunile 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 ACL-uri 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 transferuri de zonă de la server. Dacă nu se specifică, implicit se va permite transferuri de la toate gazdele.

**permitere-recursie**
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 acceptă interogări şi pe care nu le utilizează pentru a rezolva o interogare. Interogările de la aceste adrese nu vor fi satisfăcute.

**Concepte înrudite**

iSeries şi securitatea pe Internet

**Referinţe înrudite**

"Caracteristici BIND 8" la pagina 6
Pe lângă actualizările dinamice, BIND 8 oferă mai multe opţiuni pentru îmbunătăţirea performanţei serverului dumneavoastră DNS (Domain Name System).

---

## Cerinţele Domain Name System

Acest subiect descrie cerinţele software pentru a putea rula DNS (Domain Name System) pe serverul dumneavoastră iSeries.

Opţiunea DNS (Opţiunea 31) nu se instalează automat cu sistemul de operare de bază. Trebuie să selectaţi DNS în mod specific pentru instalare. Noul server DNS adăugat pentru V5R1 OS/400 se bazează pe implementarea DNS la standarde industriale cunoscută drept BIND 8. Serviciile DNS OS/400 anterioare se bazau pe BIND 4.9.3 şi sunt încă disponibile pe V5R1 OS/400.

Odată ce DNS s-a instalat, sistemul este configurat implicit pentru setarea unui singur server DNS prin utilizarea capabilităţilor serverului DNS bazat pe BIND 4.9.3, care erau disponibile în ediţiile anterioare. Dacă doriţi să rulaţi unul sau mai multe servere DNS utilizând BIND, trebuie să instalaţi PASE. PASE este Opţiunea 33 din SS1. Odată ce PASE este instalată, Navigator iSeries va manipula automat configurarea implementării BIND corecte.

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. Vedeţi subiectul V4R5 DNS din centrul de informare pentru documentaţia BIND 4.9.3.

Dacă vreţi să configuraţi un server DHCP pe un sistem iSeries diferit pentru a trimite actualizări către acest server DNS, Opţiunea 31 trebuie să fie instalată şi pe serverul DHCP iSeries. Serverul DHCP (Dynamic Host Configuration Protocol) utilizează interfeţele de programare furnizate de Opţiunea 31 pentru a realiza actualizări dinamice.

**Concepte înrudite**

PASE (Portable Application Solutions Environment - Mediul de soluţii pentru aplicaţiile portabile)

"Configurarea Domain Name System"
Acest subiect explică modul de utilizare al Navigator iSeries pentru configurarea serverelor de nume şi pentru rezolvarea interogărilor în afara domeniului dumneavoastră.

**Referinţe înrudite**

"Caracteristici BIND 8" la pagina 6
Pe lângă actualizările dinamice, BIND 8 oferă mai multe opţiuni pentru îmbunătăţirea performanţei serverului dumneavoastră DNS (Domain Name System).

**Informaţii înrudite**

Subiectul pentru Centrul de Informare V4R5 DNS

## Stabilirea existenţei unui Domain Name System instalat

Pentru a stabili dacă DNS-ul (Domain Name System) este instalat, parcurgeţi următorii paşi:

1. La linia de comandă, tastaţi GO LICPGM şi apăsaţi Enter.
2. Tastaţi 10 (Afişarea programelor cu licenţă instalate) şi apăsaţi Enter.
3. Defilaţi cu Page down până la **5722SS1 Domain Name System** (SS1 Opţiunea 31). Dacă DNS-ul este instalat cu succes, Starea de instalare va fi *compatible,după cum se arată aici:

```
PgmLic       Starea de instalare       Descrierea
5722SS1      *COMPATIBLE               Domain Name System
```

4. Apăsaţi F3 pentru a ieşi din ecran.

## Instalarea Domain Name System

Pentru a instala DNS-ul (Domain Name System), parcurgeţi paşii următori:

1. La linia de comandă, tastaţi GO LICPGM şi apăsaţi Enter.
2. Tastaţi 11 (Instalare programe cu licenţă) şi apăsaţi Enter.
3. Tastaţi 1 (Instalare) în câmpul **Opţiune** de lângă Domain Name System şi apăsaţi Enter.
4. Apăsaţi din nou Enter pentru a confirma instalarea.

---

## Configurarea Domain Name System

Acest subiect explică modul de utilizare al Navigator iSeries pentru configurarea serverelor de nume şi pentru rezolvarea interogărilor în afara domeniului dumneavoastră.

Înainte de a lucra cu configuraţia DNS-ului (Domain Name System) dumneavoastră, vedeţi cerinţele sistemului DNS pentru a instala componentele DNS necesare.

**Concepte înrudite**

"Cerinţele Domain Name System" la pagina 22
Acest subiect descrie cerinţele software pentru a putea rula DNS (Domain Name System) pe serverul dumneavoastră iSeries.

## Accesarea Domain Name System din Navigator iSeries

În acest subiect puteţi învăţa cum să accesaţi DNS-ul (Domain Name System) din Navigator iSeries.

Următoarele instrucţiuni vă vor ghida prin interfaţa de configurare DNS din Navigator iSeries. Dacă utilizaţi PASE, veţi putea configura serverele DNS bazate pe BIND 8. Dacă nu utilizaţi PASE, puteţi totuşi rula acelaşi server DNS bazat pe BIND 4.9.3 care era disponibil în ediţiile anterioare. Vedeţi subiectul DNS V4R5 din Centrul de Informare pentru informaţii privind DNS-ul bazat pe BIND 4.9.3.

Dacă configuraţi DNS-ul pentru prima dată, parcurgeţi următorii paşi:

1. În Navigator iSeries, expandaţi **serverul dumneavoastră iSeries → Reţea → Servere → DNS**.

2. Faceţi clic dreapta pe **DNS** şi selectaţi **Configuraţie nouă**.

**Concepte înrudite**

Navigator iSeries

# Configurarea serverelor de nume

DNS-ul (Domain Name System) vă permite să creaţi instanţe multiple de server de nume. Acest subiect furnizează instrucţiuni pentru configurarea unui server de nume.

DNS-ul iSeries bazat pe BIND 8 suportă instanţe multiple de server de nume. Următoarele operaţii vă vor ghida prin procesul de creare a unei singure instanţe de server de nume, inclusiv proprietăţile şi zonele sale.

Dacă vreţi să creaţi instanţe multiple, repetaţi procedura de mai sus până când toate instanţele dorite au fost create. Puteţi specifica proprietăţi independente, cum sunt niveluri de depanare şi valori de pornire automată, pentru fiecare instanţă de server de nume. Când creaţi o nouă instanţă sunt create fişiere separate de configurare.

**Referinţe înrudite**

"Întreţinerea fişierelor de configurare Domain Name System" la pagina 30
Acest subiect vă ajută să înţelegeţi fişierele pe care le foloseşte DNS-ul (Domain Name System) şi să treceţi în revistă indicaţiile pentru a le face copii de rezervă şi a le întreţine.

## Crearea unei instanţe server de nume

Utilizaţi vrăjitorul Configurare DNS (Domain Name System) nou pentru a defini o instanţă server DNS.

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

1. În **Navigator iSeries**, expandaţi **serverul dumneavoastră iSeries → Reţea → Servere → DNS**.
2. În panoul din stânga, faceţi clic dreapta pe **DNS** şi selectaţi **Server de nume nou...**
3. Vrăjitorul vă poate ghida în procesul de configurare.

Vrăjitorul necesită următoarele intrări:

**Numele serverului DNS:**
Introduceţi un nume pentru serverul dumneavoastră DNS server. 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 zone ale sistemului.

**Adresele IP Ascultare-la (Listen-on):**
Două servere DNS nu pot asculta la aceeaşi adresă IP. Setarea implicită este de a asculta la TOATE adresele IP. Dacă creaţi instanţe server suplimentare, nici una dintre ele nu poate fi configurată pentru a asculta la TOATE adresele. Trebuie să specificaţi adresele IP pentru fiecare server.

**Serverele rădăcină:**
Aţi putea să încărcaţi lista serverelor rădăcină de pe Internet implicite sau să specificaţi propriile servere rădăcină, cum sunt serverele rădăcină interne pentru o reţea internă.

**Notă:** Nu ar trebui să luaţi în considerare încărcarea serverelor rădăcină de pe Internet implicite decât dacă vă aflaţi pe Internet şi vă aşteptaţi ca DNS-ul dumneavoastră să fie capabil să rezolve complet nume de pe Internet.

**Pornirea serverului:**
Puteţi specifica dacă serverul ar trebui să pornească automat la pornirea TCP/IP. Când lucraţi pe mai multe servere, instanţele individuale pot fi pornite şi terminate independent una de cealaltă.

## Editarea proprietăţilor serverului Domain Name System

După ce aţi creat un server de nume, puteţi edita proprietăţi cum sunt sunt permitere-actualizare şi nivelurile de depanare. Aceste opţiuni se aplică doar instanţei serverului pe care o modificaţi.

Pentru a edita proprietăţile instanţei serverului DNS (Domain Name System), parcurgeţi următorii paşi:

1. În **Navigator iSeries**, expandaţi **serverul dumneavoastră iSeries → Reţea → Servere → DNS**.
2. În panoul din dreapta, faceţi clic dreapta pe **serverul dumneavoastră DNS** şi selectaţi **Configurare**.
3. Faceţi clic dreapta pe **serverul DNS** şi selectaţi **Proprietăţi**.

### Configurarea zonelor pe un server de nume

După ce configuraţi un server DNS (Domain Name System), trebuie să configuraţi zonele pentru serverul de nume.

Serverul dumneavoastră este afişat în panoul din dreapta. Pentru a configura zonele de pe serverul dumneavoastră, faceţi clic dreapta pe numele serverului şi selectaţi **Configurare**. Se va afişa fereastra Configurare DNS.

Toate zonele sunt configurate folosind vrăjitori. Creaţi **Zonele de căutare înainte** sau **Zonele de căutare inversă** prin clic dreapta pe folderul corespunzător. Se vor afişa opţiunile pentru tipul respectiv de zonă. Selectaţi tipul de zonă pe care doriţi să îl creaţi pentru a porni vrăjitorul.

**Concepte înrudite**

"Accesarea datelor Domain Name System externe" la pagina 26
Atunci când creaţi datele de zonă DNS (Domain Name System), serverul dumneavoastră va putea rezolva interogările către acea zonă.

**Operaţii înrudite**

"Configurarea Domain Name System pentru recepţionarea de actualizări dinamice"
Serverele DNS (Domain Name System) care rulează BIND 8 pot fi configurate pentru a accepta cereri de la alte surse pentru actualizarea dinamică a datelor de zonă. Acest subiect furnizează instrucţiuni pentru configurarea opţiunii de permitere-actualizare pentru ca DNS să poată recepţiona actualizări dinamice.

"Importarea fişierelor Domain Name System" la pagina 26
DNS-ul (Domain Name System) poate importa fişiere existente de date de zonă. Urmaţi aceste proceduri de economisire a timpului pentru crearea unei noi zone dintr-un fişier de configurare existent.

**Referinţe înrudite**

"Înţelegerea zonelor" la pagina 2
Acest subiect explică zonele DNS (Domain Name System) şi tipurile de zone.

## Configurarea Domain Name System pentru recepţionarea de actualizări dinamice

Serverele DNS (Domain Name System) care rulează BIND 8 pot fi configurate pentru a accepta cereri de la alte surse pentru actualizarea dinamică a datelor de zonă. Acest subiect furnizează instrucţiuni pentru configurarea opţiunii de permitere-actualizare pentru ca DNS să poată recepţiona actualizări dinamice.

Când creaţi zone dinamice ar trebui să luaţi în considerare structura reţelei dumneavoastră. Dacă anumite părţi din domeniul dumneavoastră necesită totuşi actualizări manuale, atunci poate ar trebui să luaţi în considerare setarea separată de zone statice şi 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 opriţi serverul, veţi pierde toate actualizările dinamice procesate din momentul pornirii serverului. Cu toate acestea, oprirea serverului pentru realizarea de actualizări manuale poate însemna pierderea actualizărilor dinamice trimise în perioada în care serverul era 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 dumneavoastră iSeries → Reţea → Servere → DNS**.
2. În panoul din dreapta, faceţi clic dreapta pe **server DNS** şi selectaţi **Configurare**.
3. În fereastra Configurare DNS, expandaţi **Zonă de căutare înainte inversă 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 Address, un Prefix IP, o Listă de control acces sau o Cheie.
8. Când aţi terminat actualizarea listei de potrivire adrese, faceţi clic pe **OK** pentru a închide pagina Opţiuni.

**Concepte înrudite**

"Actualizările dinamice" la pagina 5
DNS-ul OS/400 V5R1 bazat pe BIND 8 suportă actualizări dinamice. Acestea permit surselor din exterior, cum este fi DHCP (Dynamic Host Configuration Protocol), să trimită actualizări către serverul DNS (Domain Name System).

"Configurarea zonelor pe un server de nume" la pagina 25
După ce configuraţi un server DNS (Domain Name System), trebuie să configuraţi zonele pentru serverul de nume.

**Operaţii înrudite**

Configurarea DHCP pentru a trimite actualizări dinamice

## Importarea fişierelor Domain Name System

DNS-ul (Domain Name System) poate importa fişiere existente de date de zonă. Urmaţi aceste proceduri de economisire a timpului pentru crearea unei noi zone dintr-un fişier de configurare existent.

Puteţi crea o zonă primară prin importarea unui fişier de date de zonă sau prin convertirea tabelelor de gazde existente. Consultaţi Convertirea tabelelor de gazde pentru a crea date de zonă dintr-o tabelă de gazdăe.

Puteţi importa orice fişier care este un fişier de configurare a unei zone valide bazat pe sintaxa BIND. Fişierul ar trebui să fie localizat într-un director IFS. Atunci când este importat, DNS verifică dacă este un fişier valid de date de zonă 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 dumneavoastră iSeries → 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. Urmaţi instrucţiunile vrăjitorului pentru a importa zona primară.

**Concepte înrudite**

"Configurarea zonelor pe un server de nume" la pagina 25
După ce configuraţi un server DNS (Domain Name System), trebuie să configuraţi zonele pentru serverul de nume.

### Validarea înregistrării

Funcţia de Importare date de domeniu citeşte şi validează fiecare înregistrare a fişierului care este importat.

După ce funcţia de Importare date de domeniu s-a încheiat, oricare dintre înregistrările în eroare poate fi examinată individual în pagina proprietăţi Alte înregistrări a zonei importate.

**Note:**

1. Importarea unui domeniu primar mare poate dura mai multe minute.
2. Funcţia de importare date de domeniu nu suportă directiva $include. Procesul de verificare a validităţii importării datelor de domeniu identifică liniile care conţin directiva $include ca linii în eroare.

## Accesarea datelor Domain Name System externe

Atunci când creaţi datele de zonă DNS (Domain Name System), serverul dumneavoastră va putea rezolva interogările către acea zonă.

Serverele rădăcină sunt critice la funcţionarea unui server DNS care este conectat direct la Internet sau la o reţea internă mare. Serverele DNS trebuie să utilizeze servere rădăcină 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 informaţii suplimentare, un server DNS trebuie să ştie unde să caute. Pe Internet, primul loc unde caută un server DNS sunt serverele rădăcină. Serverele rădăcină direcţionează un server DNS spre alte servere din ierarhie până se găseşte un răspuns sau se determină că nu există nici un răspuns.

### Lista implicită de servere rădăcină ale NavigatoriSeries

Ar trebui să utilizaţi servere rădăcină de pe 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 de pe Internet este livrată în Navigator iSeries. Conţinutul listei este corespunzător momentului când a fost lansat pe piaţă Navigator iSeries. Puteţi verifica că lista implicită este actuală prin compararea ei cu lista de pe situl InterNIC. Actualizaţi lista de servere rădăcină a configuraţiei dumneavoastră de servere rădăcină (root) pentru a o menţine actuală.

### De unde se obţin adresele de servere rădăcină de pe Internet

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

1. FTP anonim la serverul InterNIC: FTP.RS.INTERNIC.NET
2. Descărcaţi acest fişier: /domain/named.root
3. Stocaţi fişierul în următoarea cale de director: Integrated File System/Root/QIBM/ProdData/OS400/DNS/ROOT.FILE

Un server DNS aflat în spatele unui firewall poate să nu aibă definite servere rădăcină. În acest caz, serverul DNS poate rezolva interogările doar din intrările care există în fişierele de baze de date din domeniul său principal sau în memoria sa cache. Serverul respectiv poate înainta interogările externe către serverul DNS de pe firewall. În acest caz, serverul DNS de pe firewall acţionează ca un forwarder.

### Serverele rădăcină de pe Intranet

Dacă serverul dumneavoastră DNS face parte dintr-o reţea internă largă, este posibil să aveţi servere rădăcină interne. Dacă serverul dumneavoastră DNS nu va accesa Internetul, nu aveţi nevoie de încărcarea serverelor implicite de pe Internet. Totuşi, ar trebui să vă adăugaţi serverele rădăcină interne pentru ca serverul dumneavoastră DNS să poată rezolva adresele interne în afara domeniului său.

**Concepte înrudite**

"Configurarea zonelor pe un server de nume" la pagina 25
După ce configuraţi un server DNS (Domain Name System), trebuie să configuraţi zonele pentru serverul de nume.

## Gestionarea Domain Name System

Acest subiect discută modul de verificare a funcţionării DNS (Domain Name System), de monitorizare a performanţei şi de întreţinere a datelor şi fişierelor DNS.

## Verificarea funcţionării Domain Name System cu Name Server Lookup

Puteţi utiliza NSLookup (Name Server Lookup - Căutare server de nume) pentru a verifica dacă DNS-ul (Domain Name System) funcţionează.

Utilizaţi NSLookup pentru interogarea serverului DNS pentru a 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 interogaţi 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, tastaţi NSLOOKUP şi apăsaţi Enter. Aceasta va porni o sesiune de interogare NSLookup.
3. Tastaţi server, urmat de numele serverului dumneavoastră şi apăsaţi Enter. Spre exemplu: server myiseries.mycompany.com. Această informaţie afişează:

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


   Nume:    gazdă locală
       Adresă:  127.0.0.1
   ```

   Serverul DNS răspunde corect dacă el întoarce numele gazdei locale: **localhost**.
5. Tastaţi ieşire şi apăsaţi Enter pentru a ieşi din sesiunea terminală NSLOOKUP.

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

## Gestionarea cheilor de securitate

Cheile de securitate vă permit să limitaţi accesul la datele dumneavoastră DNS (Domain Name System).

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.

## Gestionarea cheilor DNS (Domain Name System)

Cheile DNS (Domain Name System) reprezintă chei definite pentru BIND şi utilizate de serverul DNS ca parte din verificarea unei actualizări de intrare.

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 dumneavoastră iSeries → Reţea → Servere → DNS**.
2. În panoul din dreapta, faceţi clic dreapta pe instanţa de server DNS pe care vreţi să o deschideţi şi selectaţi **Configurare**.
3. În fereastra Configurare DNS, selectaţi **Fişier → Gestionare chei.**

## Gestionarea cheilor de actualizare dinamică

Cheile de actualizare dinamică sunt utilizate pentru asigurarea actualizărilor dinamice de către serverul DHCP (Dynamic Host Configuration Protocol).

Aceste chei trebuie să fie prezente atunci când DNS (Domain Name System) 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 în siguranţă.

Pentru a administra cheile de actualizare dinamică parcurgeţi următorii paşi:

1. În Navigator iSeries, expandaţi **serverul dumneavoastră iSeries → Reţea → Servere → DNS**.
2. Faceţi clic dreapta pe **DNS** şi selectaţi **Gestionarea cheilor de actualizare dinamică**.

# Accesarea statisticilor serverului Domain Name System

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

DNS-ul (Domain Name System) furnizează mai multe unelte de diagnoză. Ele pot fi utilizate pentru a monitoriza performanţa serverului dumneavoastră.

**Referinţe înrudite**

"Întreţinerea fişierelor de configurare Domain Name System" la pagina 30
Acest subiect vă ajută să înţelegeţi fişierele pe care le foloseşte DNS-ul (Domain Name System) şi să treceţi în revistă indicaţiile pentru a le face copii de rezervă şi a le întreţine.

## Statisticile serverului

Statisticile serverului rezumă numărul de interogări şi răspunsuri primite de server de la ultima repornire sau reîncărcare a bazei sale de date.

DNS (Domain Name System) vă permite să vizualizaţi statisticile pentru o instanţă server. Informaţia este adăugată continuu la acest fişier până la ştergerea acestuia. Aceste informaţii s+ar putea dovedi utile în evaluarea cantitativă a traficului primit de server şi în depistarea problemelor. Informaţii suplimentare despre statisticile serverului sunt disponibile în subiectul de ajutor online DNS Înţelegerea statisticilor serverului DNS.

Pentru a accesa statisticile serverului, parcurgeţi următorii paşi:

1. În Navigator iSeries, expandaţi **serverul dumneavoastră iSeries → 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

Baza de date a serverului activ conţine informaţii despre zonă şi gazdă, incluzând unele proprietăţi de zonă, cum sunt informaţiile SOA (start of authority - început de autoritate) şi proprietăţile de trecere prin gazdă (through host), cum ar fi informaţiile MX (mail exchanger - schimbare de poştă), care ar putea fi utile la urmărirea problemelor.

DNS-ul (Domain Name System) vă permite să vizualizaţi un dump al datelor de autoritate, al datelor cache şi datelor de indicaţie pentru o instanţă server. Dump-ul include informaţiile din toate zonele primare şi secundare ale serverului (zonele de mapare directă şi inversă), cât şi informaţiile pe care serverul le-a obţinut din interogări.

Puteţi vizualiza dump-ul bazei de date a serverului activ utilizând Navigator iSeries. Dacă trebuie să salvaţi o copie a fişierelor, numele fişierului dump-ului de baze de date este NAMED_DUMP.DB (nume_dump.db) din calea de director a sistemului dumneavoastră iSeries: **Integrated File System/Root/QIBM/UserData/OS400/DNS/<instanţă server >**, unde ″<instanţă server >″ este numele instanţei server. Informaţii suplimentare 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 dumneavoastră iSeries → Reţea → Servere → DNS**.
2. În panoul din dreapta, faceţi clic dreapta pe **serverul DNS** şi selectaţi **Configurare**.
3. În fereastra Configurare DNS, selectaţi **Vizualizare → Baza de date a serverului activ**.

# Întreţinerea fişierelor de configurare Domain Name System

Acest subiect vă ajută să înţelegeţi fişierele pe care le foloseşte DNS-ul (Domain Name System) şi să treceţi în revistă indicaţiile pentru a le face copii de rezervă şi a le întreţine.

Puteţi utiliza DNS din i5/OS pentru a crea şi administra instanţe de server DNS pe sistemul iSeries. Fişierele de configurare pentru DNS sunt administrate de Navigator iSeries. Nu editaţi fişierele manual. Utilizaţi întotdeauna Navigator iSeries pentru a crea, modifica sau şterge fişierele de configurare DNS. Fişierele de configurare DNS sunt stocate în căile sistemului de fişiere integrat listate mai jos.

**Notă:** Structura de fişiere de mai jos se aplică DNS-ului ce rulează pe BIND 8. Dacă utilizaţi un DNS bazat pe BIND 4.9.3, vedeţi Realizarea de copii de rezervă pentru fişierele de configurare DNS şi menţinerea fişierelor istoric din subiectul DNS, în Centrul de informare V4R5.

În tabela de mai jos, fişierele sunt listate în ierarhia de căi prezentată. Fişierele cu o icoană de salvare  ar trebui salvate pentru a proteja datele. Fişierele cu o icoană de ştergere  ar trebui şterse în mod regulat.

| Nume | Icoană | Descriere |
|---|---|---|
| **QIBM/UserData/OS400/DNS/** | | Directorul punct de plecare pentru DNS. |
| ATTRIBUTES |  | DNS utilizează acest fişier pentru a determina ce versiune BIND utilizaţi. |
| **QIBM/UserData/OS400/DNS/ <*instanţă*>/** | | Directorul punct de plecare pentru o instanţă DNS. |
| ATTRIBUTES |  | Atributele de configurare utilizate de DNS-ul iSeries. |
| NAMED.CONF |  | Acest fişier conţine date de configurare. Este utilizat pentru a-i indica serverului ce zone specifice gestionează, unde sunt fişierele de zonă, ce zone pot fi actualizate dinamic, unde sunt serverele forwarder şi alte setări de opţiuni. |
| BOOT.AS400BIND4 |  | Configuraţia serverului BIND 4.9.3 şi fişierul de politici care este convertit la fişierul NAMED.CONF din 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 de date server creat pentru baza de date a serverului activ. |
| NAMED.STATS |  | Statisticile serverului. |
| NAMED.PID | | Reţine ID-ul de proces al serverului ce rulează. Acest fişier este creat de fiecare dată când serverul DNS este pornit. Este folosit pentru funcţiile Database (Bază de date), Statistics (Statistici) şi Update server (Actualizare server). Nu editaţi sau ştergeţi acest fişier. |

| Nume | Icoană | Descriere |
|---|---|---|
| QUERYLOG |  | Istoricul serverului DNS de interogări 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 de zonă pentru un anumit domeniu deservit de acest server. Conţine toate înregistrările resursă pentru această zonă. |
| <*nume-zonă-b*>.DB |  | Fişier de zonă pentru un anumit domeniu deservit de acest server. Conţine toate înregistrările resursă pentru această zonă. Fiecare zonă are un fişier .DB separat. |
| *.ixfr.* |  | Fişierele IXFR (incremental zone transfer). Aceste fişiere sunt utilizate de serverele secundare pentru a încărca numai 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. Păstrarea fişierelor care au fost create cu o zi sau două în urmă va permite majorităţii serverelor secundare să încarce în continuare IXFR-uri. Dacă ştergeţi toate fişierele, serverul secundar va cere un transfer complet (AXFR). |
| TMP | | Director utilizat de instanţa de server pentru crearea fişierelor de lucru temporar. |
| **QIBM/UserData/OS400/DNS/TMP** | | Directorul Temp utilizat de programul QTOBH2N pentru a crea fişiere intermediare produse prin dump din tabela de gazde pentru importarea ulterioară folosind Navigator iSeries. |
| **QIBM/UserData/OS400/DNS/_DYN/** | | Directorul care reţine 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.<br><*nume-zonă-a*> |  | Cheia de actualizare dinamică necesară pentru a iniţia o cerere de actualizare automată 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.<br><*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.<br><*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*>. |

**Concepte înrudite**

"Stabilirea autorizărilor Domain Name System" la pagina 20
Există cerinţe de autorizaţie speciale pentru administratorul DNS (Domain Name System). De asemenea, ar trebui să luaţi în considerare implicaţiile autorizării privind securitatea.

"Accesarea statisticilor serverului Domain Name System" la pagina 29
Dump-ul bazei de date şi uneltele de statistică vă pot ajuta să treceţi în revistă şi să gestionaţi performanţa serverului.

**Operaţii înrudite**

"Configurarea serverelor de nume" la pagina 24
DNS-ul (Domain Name System) vă permite să creaţi instanţe multiple de server de nume. Acest subiect furnizează instrucţiuni pentru configurarea unui server de nume.

# Caracteristicile avansate Domain Name System

Acest topic explică modul în care administratorii cu experienţă pot utiliza caracteristicile avansate DNS (Domain Name System) pentru gestionarea mai facilă a serverului DNS.

DNS din Navigator iSeries furnizează o interfaţă pentru configurarea şi gestionarea serverului dumneavoastră DNS. Următoarele operaţii sunt furnizate drept scurtături pentru administratorii care sunt familiarizaţi cu interfaţa grafică a iSeries. Ele furnizează metode rapide pentru modificarea stării serverului şi a atributelor pentru mai multe instanţe printr-o singură acţiune.

**Operaţii înrudite**

"Modificarea setărilor de depanare Domain Name System" la pagina 35
Funcţia de depanare DNS (Domain Name System) poate oferi informaţii care vă pot ajuta să determinaţi şi să corectaţi problemele serverului DNS.

## Modificarea atributelor Domain Name System

Puteţi modifica setările DNS (Domain Name System) dacă interfaţa DNS nu vă permite să modificaţi simultan 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 instanţele în acelaşi timp. Parcurgeţi următorii paşi pentru a utiliza CHGDNSA:

1. La linia de comandă, tastaţi CHGDNSA şi apăsaţi F4.
2. În pagina CHGDNSA (Change DNS Server Attributes - Modificarea atributelor serverului DNS), tastaţi numele unei singure instanţe server, sau *ALL şi apăsaţi Enter.

   Vor fi afişate opţiunile disponibile pentru atributele de server:

   ```
   Pornire automată server. . . . . *SAME *YES, *NO, *SAME
   Nivel de depanare . . . . . *SAME 0-11, *SAME, *DFT
   ```

3. **Pornire automată** 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 atributul cu setările actuale, tastaţi *SAME.

   **Nivel de depanare** 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 atributul cu setările actuale, tastaţi *SAME.

   După ce aţi introdus toate preferinţele dumneavoastră, apăsaţi Enter pentru a seta atributele DNS.

## Pornirea sau oprirea serverelor Domain Name System

Puteţi modifica setările dacă interfaţa DNS (Domain Name System) nu vă permite să porniţi sau să opriţi mai multe instanţe server 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

Puteţi modifica nivelul de depanare, opţiune utilă pentru administratorii care au zone mari şi nu doresc cantitatea mare de date de depanare pe care ar obţine-o la prima pornire a serverului şi la încărcarea tuturor datelor de zonă.

DNS-ul din interfaţa Navigator iSeries nu vă permite să modificaţi nivelul de depanare în timp ce serverul rulează. Oricum, puteţi utiliza interfaţa bazată pe caracter pentru a modifica nivelul de depanare în timp ce serverul rulează. Pentru a modifica nivelul de depanare utilizând interfaţa bazată pe caractere, parcurgeţi următorii paşi, înlocuind <instanţă> cu numele instanţei server:

1. La linia de comandă, tastaţi ADDLIBLE QDNS şi apăsaţi Enter.
2. Modificaţi nivelul de depanare:
   - Pentru a activa depanarea sau pentru a creşte nivelul de depanare cu 1, tastaţi CALL QTOBDRVS ('BUMP' '<instanţă>') şi apăsaţi Enter.
   - Pentru dezactiva depanarea, tastaţi CALL QTOBDRVS ('OFF' '<instance>') şi apăsaţi Enter.

## Depanarea Domain Name System

Acest subiect explică setările DNS (Domain Name System) pentru înregistrare în istoric şi depanare, care vă pot ajuta să rezolvaţi problemele cu serverul dumneavoastră DNS.

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 returnează răspunsurile aşteptate, istoricele 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.

### 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 informaţii suplimentare despre depanarea DNS 4.9.3, referiţi-vă la *Depanarea serverelor DNS*.
- 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 veţi avea două instanţe, INST1 şi INST2, numele joburilor lor vor fi QTOBDINST1 şi QTOBDINST2.

**Concepte înrudite**

"Înregistrarea în istoric a mesajelor serverului Domain Name System" la pagina 34
DNS (Domain Name System) furnizează numeroase opţiuni de înregistrare în istoric care pot fi ajustate atunci când încercaţi să găsiţi sursa unei probleme. Înregistrarea furnizează flexibilitate prin oferirea diferitelor niveluri de gravitate, categorii de mesaje şi fişiere de ieşire, ajutându-vă în acest fel să găsiţi problemele.

**Operaţii înrudite**

"Modificarea setărilor de depanare Domain Name System" la pagina 35
Funcţia de depanare DNS (Domain Name System) poate oferi informaţii care vă pot ajuta să determinaţi şi să corectaţi problemele serverului DNS.

# Înregistrarea în istoric a mesajelor serverului Domain Name System

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

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 sunt cele dorite, însă dacă doriţi să le modificaţi, se recomandă să vă referiţi la alte surse din documentaţia BIND 8 pentru informaţii despre înregistrarea în istoric.

## Canalele 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 canale:

- **Canalele 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 mesaje 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.
- **Canalele 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.

## Categoriile de mesaje

Mesajele sunt grupate pe categorii. Puteţi specifica ce categorii de mesaje 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 (specificaţi 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.

### Modificarea setărilor de înregistrare

Pentru a accesa opţiunile de înregistrare, parcurgeţi următorii paşi:

1. În Navigator iSeries, expandaţi **serverul dumneavoastră iSeries → Reţea → Servere → DNS**.
2. În panoul din dreapta, faceţi clic dreapta pe **serverul DNS** şi selectaţi **Configurare**.
3. În fereastra de configurare DNS, faceţi clic dreapta pe **Serverul DNS** şi selectaţi **Proprietăţi**.
4. În fereastra Proprietăţi server, selectaţi fişa **Channels** pentru a crea noi canale fişsier sau proprietăţi ale unui canal, cum ar fi gravitatea mesajelor înregistrate în istoricul fiecărui canal.
5. În fereastra Proprietăţi server, selectaţi fişa **Înregistrare în istoric** pentru a specifica categoriile de mesaje care să fie înregistrate în istoricul fiecărui canal.

### Sugestie 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 scădea performanţa. Dacă întâmpinaţi probleme, dar istoricul jobului jnu indică sursa problemei respective, s-ar putea să fie necesar să modificaţi 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. După ce aţi rezolvat problema, resetaţi nivelul de gravitate la Eroare pentru reducerea numărului de mesaje din istoricul jobului.

**Operaţii înrudite**

“Depanarea Domain Name System” la pagina 33
Acest subiect explică setările DNS (Domain Name System) pentru înregistrare în istoric şi depanare, care vă pot ajuta să rezolvaţi problemele cu serverul dumneavoastră DNS.

## Modificarea setărilor de depanare Domain Name System

Funcţia de depanare DNS (Domain Name System) poate oferi informaţii care vă pot ajuta să determinaţi şi să corectaţi problemele serverului DNS.

DNS oferă 12 niveluri al controlului de depanare. În general, înregistrarea în istoric 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). 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 de service IBM vă poate ajuta să determinaţi valoarea corespunzătoare 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: **Integrated File System/Root/QIBM/UserData/OS400/DNS/<instanţă server>**, unde ″<instanţă server>″ reprezintă numele instanţei de server 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 dumneavoastră iSeries → 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 pagina Proprietăţi server - General, specificaţi nivelul de depanare la pornirea serverului.
5. Dacă serverul rulează, opriţi şi reporniţi severul.

**Notă:** Modificările făcute la nivelul de depanare nu au efect în timp ce serverul rulează. Nivelul de depanare setat aici va fi folosit ulterior când serverul este repornit complet. Dacă aveţi nevoie să modificaţi nivelul de depanare în timp ce serverul rulează, vedeţi Caracteristicile DNS avansate.

**Concepte înrudite**

"Caracteristicile avansate Domain Name System" la pagina 32
Acest topic explică modul în care administratorii cu experienţă pot utiliza caracteristicile avansate DNS (Domain Name System) pentru gestionarea mai facilă a serverului DNS.

**Operaţii înrudite**

"Depanarea Domain Name System" la pagina 33
Acest subiect explică setările DNS (Domain Name System) pentru înregistrare în istoric şi depanare, care vă pot ajuta să rezolvaţi problemele cu serverul dumneavoastră DNS.

---

# Informaţiile înrudite pentru Domain Name System

Mai jos sunt prezentate cărţi IBM Redbooks (în format PDF) şi situri Web care sunt legate de subiectul Domain Name System (DNS). Puteţi vizualiza sau tipări oricare dintre aceste PDF-uri.

## IBM Redbooks

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

Această carte descrie suportul pentru serverul DNS (Domain Name System) şi serverul DHCP (Dynamic Host Configuration Protocol) din i5/OS. Informaţiile din această carte vă ajută să instalaţi, să adaptaţi, să configuraţi şi să depanaţi suportul DNS şi DHCP prin exemple.

## Situri Web

- *DNS and BIND*, ediţia a treia. 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.
- Situl Web Internet Software Consortium conţine ştiri, legături şi alte resurse pentru BIND.
- Situl InterNIC menţine un director cu toţi înregistratorii de domenii care sunt autorizaţi de ICANN (Internet Corporation for Assigned Names and Numbers).
- DNS Resources Directory oferă materiale de referinţă pentru DNS şi legături către multe alte resurse DNS, inclusiv grupuri de discuţie. De asemenea, furnizează o listă cu RFC-uri referitoare la DNS .

## Salvarea fişierelor PDF

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

1. Faceţi clic dreapta pe PDF din browser-ul dumneavoastră (faceţi clic dreapta pe legătura de mai sus).
2. Faceşi clic pe opţiunea care salvează PDF-ul în plan local.
3. Navigaţi la directorul în care doriţi să salvaţi PDF-ul.
4. Faceţi clic pe **Save**.

## Descărcarea Adobe Reader

Aveţi nevoie ca Adobe Reader să fie instalat pe sistemul dumneavoastră pentru a vizualiza sau tipări aceste PDF-uri.

Puteţi descărca o copie gratuită de pe Situl web Adobe (www.adobe.com/products/acrobat/readstep.html)  .

# 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 brevete. Puteţi trimite întrebări cu privire la licenţe, în scris, la:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
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 106-0032, 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 PENTRU 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. Periodic, informaţiile incluse aici sunt modificate; aceste modificări vor fi încorporate în noile ediţii ale publicaţiei. IBM poate aduce îmbunătăţiri şi/sau modifcări produsului (produselor) şi/sau programului (programelor) descrise în această publicaţie în orice moment, fără notificare.

Referirile din aceste informaţii la adrese de situri Web non-IBM sunt făcute numai pentru a vă ajuta, fără ca prezenţa lor să însemne un gir acordat acestor 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 pentru 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 YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Aceste informaţii pot fi disponibile cu respectarea termenilor şi condiţiilor corespunzătoare, iar în unele cazuri cu plata unei taxe.

Programul licenţiat la care se referă aceste informaţii şi toate materialele licenţiate disponibile pentru el sunt furnizate de IBM în conformitate cu termenii din IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code sau din alt acord echivalent încheiat între noi.

Toate datele de performanţă din acest document au fost determinate într-un mediu controlat. De aceea, rezultatele obţinute în alte medii de funcţionare pot fi diferite. Unele măsurători s-ar putea să fi fost făcute pe sisteme la nivel de dezvoltare şi nu există nici o garanţie că aceste măsurători vor fi identice pe sistemele disponibile pe piaţă. Mai mult de atât, unele măsurători s-ar putea să fi fost estimate prin extrapolare. Rezultatele reale pot fi diferite. Utilizatorii acestui document trebuie să verifice datele aplicabile pentru mediul lor specific.

Informaţiile privind produsele non-IBM au fost obţinute de la furnizorii acestor produse, din anunţurile lor publicate sau din alte surse disponibile publicului. IBM nu a testat aceste produse şi nu poate confirma acurateţea performanţelor, compatibilitatea sau oricare alte pretenţii legate de produsele non-IBM. Întrebări legate de capacităţile produselor non-IBM le veţi adresa furnizorilor acestor produse.

Toate declaraţiile privind direcţiile de viitor şi intenţiile IBM-ului pot fi schimbate sau se poate renunţa la ele, fără notificare prealabilă şi reprezintă doar scopuri şi obiective.

Aceste informaţii conţin exemple de date şi rapoarte folosite în operaţiile comerciale de zi cu zi. Pentru a fi cât mai complete, exemplele includ nume de persoane, de companii, de mărci şi de produse. Toate aceste nume sunt fictive şi orice asemănare cu nume sau adrese folosite de o întreprindere reală este pură coincidenţă.

LICENŢĂ - COPYRIGHT:

Aceste informaţii conţin exemple de programe de aplicaţii în limbaje sursă, care ilustrează tehnici de programare pe diferite platforme de operare. Puteţi copia, modifica şi distribui aceste exemple de programe sub orice formă fără ca IBM să pretindă vreo plată, când o faceţi în scopul dezvoltării, folosirii, promovării şi distribuirii programelor de aplicaţii conform cu interfaţa de programare a aplicaţiilor pentru platforma de operare pentru care au fost scrise exemplele de program. Aceste exemple nu au fost testate amănunţit în toate condiţiile. De aceea, IBM nu poate garanta sau sugera fiabilitatea, suportul pentru service sau funcţionarea acestor programe.

Fiecare copie sau porţiune din aceste exemple de program sau orice lucrare derivată din acestea trebuie să includă un anunţ de copyright de genul următor:

© (numele companiei dumneavoastră) (anul). Unele porţiuni din acest cod sunt derivate din IBM Corp. Sample Programs. © Copyright IBM Corp. _introduceţi anul sau anii_. Toate drepturile rezervate.

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

## Informaţii privind interfaţa de programare

Această publicaţie referitoare la DNS conţine informaţii despre interfeţele de programare menite să permită beneficiarului obţinerea serviciilor IBM i5/OS.

## Mărci comerciale

Următorii termeni sunt mărci comerciale deţinute de International Business Machines Corporation în Statele Unite, în alte ţări sau ambele:

| AFS
| AS/400
| e(logo)server
| eServer
| i5/OS
| IBM
| IBM (logo)
| iSeries
| OS/400
| Redbooks

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

## Termenii şi condiţiile

Permisiunile pentru utilizarea acestor publicaţii sunt acordate în conformitate cu următorii termeni şi condiţii.

**Utilizare personală:** Puteţi reproduce aceste publicaţii pentru utilizarea personală, necomercială, cu condiţia ca toate anunţurile de proprietate să fie păstrate. Nu puteţi distribui, afişa sau realiza lucrări 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 anunţurile de proprietate să fie păstrate. Nu puteţi să realizaţi lucrări derivate din aceste informaţii, nici să reproduceţi, să distribuiţi sau să afişaţi aceste informaţii sau o porţiune a lor în afara întreprinderii dumneavoastră fără consimţământul explicit de la IBM.

În afara celor acordate expres prin această permisiune, nu se acordă nici o altă permisiune, licenţă sau drept, explicite sau implicite, pentru aceste publicaţii sau orice informaţii, date, software sau alte elemente pe care le conţin şi care reprezintă o proprietate intelectuală.

IBM îşi păstrează dreptul de a retrage permisiunile acordate aici oricând, la discreţia sa, dacă folosirea publicaţiilor este în detrimentul intereselor sale sau, după cum este determinat de IBM sau dacă instrucţiunile de mai sus nu sunt urmate corespunzător.

Nu puteţi descărca, exporta sau reexporta aceste informaţii decât în deplină conformitate cu legile şi regulamentele aplicabile, inclusiv toate legile şi regulamentele de export ale Statelor Unite.

IBM NU ACORDĂ NICI O GARANŢIE PENTRU CONŢINUTUL ACESTOR PUBLICAŢII. ACESTE PUBLICAŢII SUNT FURNIZATE ″CA ATARE″, FĂRĂ NICI UN FEL DE GARANŢIE, EXPLICITĂ SAU IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA ELE, GARANŢIILE IMPLICITE DE VANDABILITATE, DE NEÎNCĂLCARE A UNOR DREPTURI SAU NORME ŞI DE POTRIVIRE PENTRU UN ANUMIT SCOP.

Tipărit în S.U.A.