System i

Lucrul în reţea - DNS (Domain Name System)

Versiunea 6 Ediţia 1

System i

Lucrul în reţea - DNS (Domain Name System)

Versiunea 6 Ediţia 1

Notă

Înainte de a folosi aceste informaţii şi produsul la care se referă, citiţi informaţiile din “Observaţii”, la pagina 41.

Această ediţie este valabilă pentru IBM i5/OS (număr de produs 5761-SS1) versiunea 6, ediţia 1, 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 este un sistem de bază de date distribuită pentru gestionarea numelor de gazde şi a adreselor IP asociate.

Cu DNS, pot fi folosite nume simple, cum ar fi www.jkltoys.com, pentru a localiza o gazdă, în loc de a folosi adrese IP, de exemplu 192.168.12.88 în IPv4 sau 2001:D88::1 în IPv6. Un singur server ar putea fi responsabil doar pentru cunoaşterea numelor de gazdă şi a adreselor IP pentru o mică parte a unei zone, dar serverele DNS pot lucra împreună pentru a mapa toate numele de domenii la adresele lor IP. Serverele DNS care lucrează împreună permit calculatoarelor să comunice pe internet.

Pentru IBM i5/OS Versiunea 6 Ediţia 1 (V6R1), serviciile DNS sunt bazate pe implementarea DNS standard, cunoscută ca BIND versiunea 9. În ediţii anterioare de i5/OS, serviciile DNS erau bazate pe BIND versiunea 8.2.5. Pentru a folosi noul server de DNS BIND versiunea 9, trebuie să aveţi i5/OS opţiunea 31 (DNS) şi opţiunea 33 (PASE) instalate pe modelul IBM System i. Începând cu i5/OS V6R1, din motive de securitate, BIND 4 şi 8 sunt înlocuite cu BIND 9. Ca urmare, este necesară migrarea la BIND 9 pentru serverul DNS.

Ce este nou pentru V6R1

Citiţi despre informaţii noi sau modificate semnificativ pentru colecţia de subiecte DNS.

BIND 9

BIND versiunea 9, introdus în această ediţie, furnizează mai multe caracteristici pentru a îmbunătăţii performanţa serverului DNS. De exemplu, suportă căutări nume-adresă şi adresă-nume în toate formele definite curent ale IPv6. Foloseşte instrucţiunea *view*, care permite unei singure instanţe DNS să răspundă la o interogare diferit în funcţie de sursa interogării, cum ar fi internet sau un intranet. În plus, foloseşte fişiere de jurnal pentru a păstra actualizări dinamice pentru o zonă.

Versiunile anterioare BIND 4.9.3 şi BIND 8.2.5 nu mai sunt suportate şi trebuie să fie migrate la BIND 9.

Noi comenzi de configurare

Au fost adăugate următoarele comenzi de configurare pentru a face mai uşoară gestionarea fişierelor de configurare DNS din sistem.

CRTRNDCCFG
: Comanda CRTRNDCCFG este folosită pentru a genera fişiere de configuraţie RNDC. Este o alternativă convenabilă la scrierea fişierului rndc.conf şi a elementelor de control corespunzătoare şi a instrucţiunilor cheie în fişierul named.conf.

CHKDNSCFG
: Comanda CHKDNSCFG verifică sintaxa fişierului de configurare numit named.conf. Dar nu furnizează suportul pentru a verifica semantica fişierului de configurare.

CHKDNSZNE
: Comanda CHKDNSZNE verifică sintaxa şi integritatea unui fişier de date de zonă. Este utilă pentru a verifica fişierele de date ale zonei înainte de a le adăuga într-un server DNS.

Noi utilitare de interogare şi actualizare

Au fost adăugate următoarele utilitare de interogare şi de actualizare pentru a îmbunătăţi capabilităţile de gestionare ale serverului DNS.

DIG Puteţi folosi unealta de interogare DIG pentru a extrage informaţii DNS despre gazde, domenii şi alte servere

DNS bazate pe răspunsul unui server DNS. Îl puteţi folosi de asemenea pentru a verifica dacă un server de DNS răspunde corect înainte de a configura sistemul să îl folosească.

HOST Comanda de pornire a interogării HOST (HOST) este folosită pentru căutări DNS. Converteşte nume de domenii în adrese IP (IPv4 sau IPv6) şi invers.

NSUPDATE
Comanda NSUPDATE lansează cereri de actualizare dinamică DNS după cum este definit în RFC-ul 2136 la un server DNS. Această permite adăugarea sau înlăturatea înregistrărilor de resurse dintr-un zonă în timp ce serverul de DNS rulează. Ca urmare, nu trebuie să actualizaţi înregistrările editând manual fişierul de zonă. O singură cerere de actualizare poate conţine cereri pentru a adăuga sau înlătura mai multe înregistrări de resurse, dar înregistrările resurselor care sunt adăugate sau înlăturate dinamic cu comanda NSUPDATE trebuie să fie în aceeaşi zonă.

RNDC Comanda RNDC permite unui administrator de sistem să controleze operarea unui server de nume. Ea citeşte un fişier de configurare, numit *rndc.conf*, pentru a determina cum să contactaţi serverul de nume şi pentru a determina ce algoritm şi chei ar trebui folosite. Dacă nu este găsit niciun fişier rndc.conf, este folosit implicit un fişier rndc-key._KID care este creat în timpul instalării şi care acordă automat acces prin interfaţa loopback.

Cum puteţi vedea ce este nou sau modificat

Pentru a vă ajuta să vedeţi care sunt modificările tehnice, acest centru de informare foloseşte:

- Imaginea » pentru a marca locul unde încep informaţiile noi sau modificate.
- Imaginea «, pentru a marca locul în care se termină informaţiile noi sau modificate.

În fişierele PDF, puteţi vedea bare de revizuire (|) în marginea din stânga a informaţiilor noi sau modificate.

Referinţe înrudite

"Caracteristicile BIND 9" la pagina 7
BIND 9 este similar cu BIND 8; totuşi, furnizează mai multe caracteristici pentru a îmbunătăţii performanţa serverului DNS, cum ar fi vizualizările.

Fişierul PDF pentru DNS

Puteţi vizualiza şi tipări un fişier 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 legătura la PDF din acest browser.
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

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

Referinţe înrudite

"Informaţii înrudite pentru Domain Name System" la pagina 40
Publicaţiile IBM Redbooks, siturile web şi alte colecţii de subiecte din centrul de informare conţin informaţii înrudite cu cele din colecţia de subiecte DNS. Puteţi vizualiza sau tipări oricare dintre fişierele PDF.

Conceptele privind DNS

DNS (Domain Name System) reprezintă un sistem de baze de date distribuite pentru administrarea numelor de gazdă şi a adreselor lor IP (Internet Protocol) asociate. Cu DNS, puteţi folosi nume simple, cum ar fi www.jkltoys.com, pentru a localiza o gazdă, în loc de a folosi adrese IP, de exemplu 192.168.12.88 în IPv4 sau 2001:D88::1 în IPv6.

Un singur server ar putea fi responsabil doar pentru cunoaşterea numelor de gazdă şi a adreselor IP pentru o mică parte a unei zone, dar serverele DNS pot lucra împreună pentru a mapa toate numele de domenii la adresele lor IP. Serverele DNS care lucrează împreună permit calculatoarelor să comunice pe 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 explică căile pe care le poate folosi un client pentru a rezolva o interogare.

Înţelegerea zonelor

Datele DNS sunt împărţite în seturi de date gestionabile, numite *zone*. Fiecare dintre aceste seturi este un tip specific de zonă.

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 este serverul autoritativ pentru domeniu, numit *zonă părinte*. Uneori are sens să delegaţi autorizarea pentru a răspunde la interogări DNS pentru un anumit subdomeniu unui alt server de DNS, numit *zonă copil*. 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 i5/OS DNS pentru a defini mai multe tipuri de zone pentru a vă ajuta să gestionaţi date DNS:

Zona primară
O zonă primară încarcă datele de zonă direct dintr-un fişier de pe o gazdă. Poate conţine o subzonă sau o zonă copil. Poate de asemenea conţine înregistrări de resurse, cum ar fi gazdă, alias (CNAME), adresă IPv4 (A), adresă IPv6 (AAAA) sau înregistrări inverse (PTR).

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

O zonă secundară încarcă date de zonă de pe serverul primar al zonei sau de pe alt server secundar. Menţine o copie completă a zonei pentru care este secundară.

Notă: Zonele secundare sunt uneori referite ca *zone slave* în altă documentaţie BIND.

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"
Clienţii DNS folosesc servere DNS pentru a rezolva interogări. Interogările ar putea veni direct de la client sau dintr-o aplicaţie care rulează pe client.

Operaţii înrudite

"Configurarea de zone pe un server de nume" la pagina 28
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 14
Acest exemplu descrie o subreţea simplă cu un server DNS (Domain Name System) pentru utilizare internă.

"Înregistrările resursă Domain Name System" la pagina 9
Înregistrările resursă sunt utilizate pentru a stoca date despre numele de domeniu şi adresele IP. Puteţi folosi tabela de căutare înregistrare resursă pentru a căuta înregistrările de resurse suportate pentru sistemul de operare i5/OS.

Înţelegerea interogărilor Domain Name System

Clienţii DNS folosesc servere DNS pentru a rezolva interogări. Interogările ar putea veni direct de la client sau dintr-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.

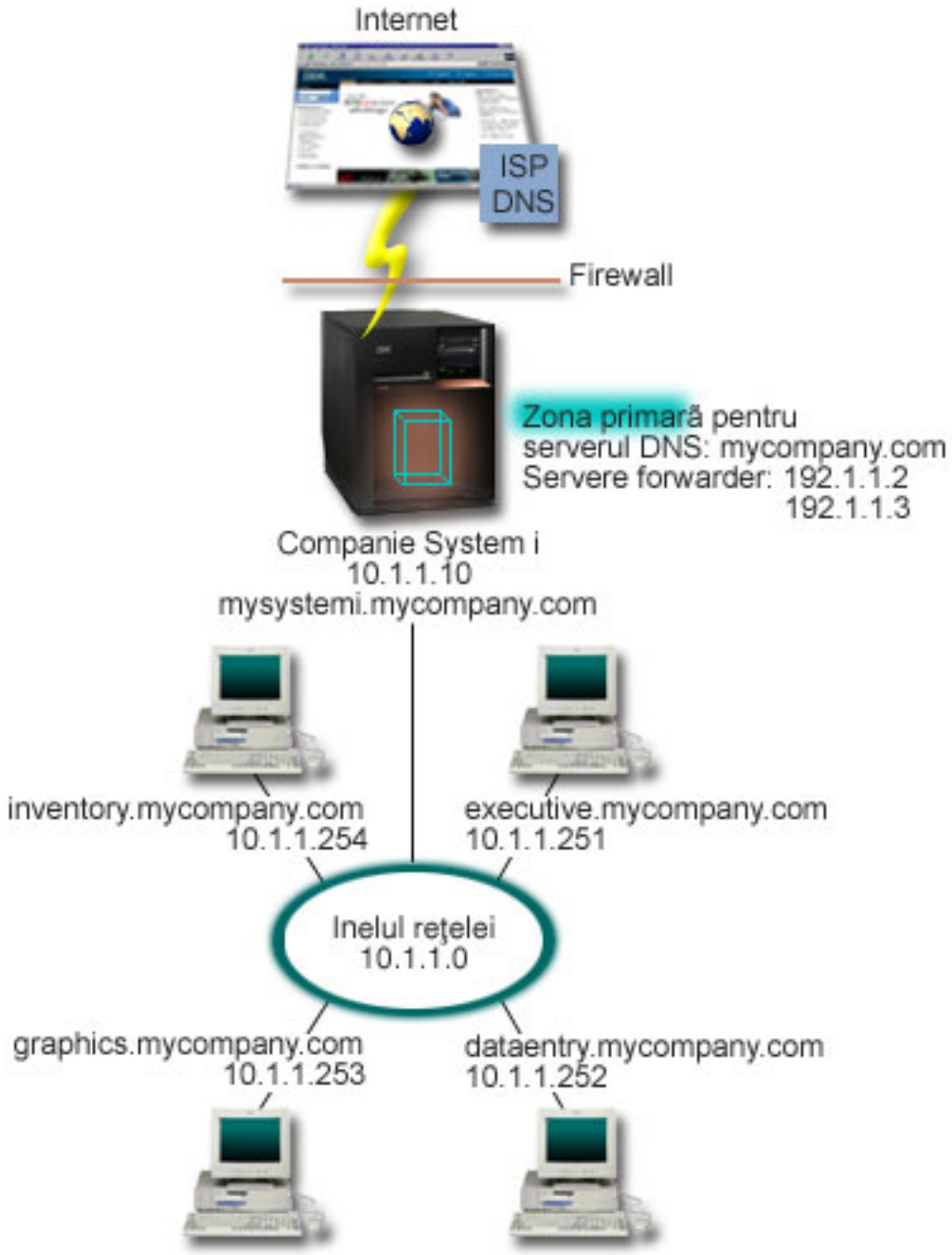

Figura 1. Un singur server DNS cu acces la Internet

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. Pot fi urmate două căi: *recursivitatea* sau *iteraţia*. Dacă un server DNS este setat să folosească *recursivitatea*, serverul poate interoga sau contacta alte servere DNS din partea clientului solicitant, pentru a rezolva complet numele, şi apoi trimite un răspuns înapoi la client. În plus, serverul solicitant stochează răspunsul în cache, astfel încât răspunsul să poată fi folosit următoarea dată când serverul primeşte acea interogare. Dacă un server DNS este setat să folosească *iteraţia*, un client poate încerca să contacteze alte servere DNS pentru a rezolva un nume. În acest proces, clientul foloseşte interogări separate şi suplimentare pe baze răspunsurilor referral de la servere.

Referinţe înrudite

"Înţelegerea zonelor" la pagina 3
Datele DNS sunt împărţite în seturi de date gestionabile, numite *zone*. Fiecare dintre aceste seturi este un tip specific de zonă.

"Exemplu: Un singur server Domain Name System cu acces la Internet" la pagina 16
Acest exemplu descrie o subreţea simplă cu un server DNS (Domain Name System) conectat direct la Internet.

Setarea domeniului DNS (Domain Name System)

Setarea domeniului DNS necesită înregistrarea domeniului de nume pentru a-i împiedica pe alţii să folosească numele de domeniu.

DNS vă permite să serviţi nume şi adrese într-un intranet sau o reţea internă. 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 16
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

i5/OS DNS care este bazat pe BIND 9 suportă actualizări dinamice. Surse externe, cum ar fi DHCP, pot trimite actualizări unui server DNS. În plus, puteţi de asemenea folosi unelte client DNS, cum ar fi NSUPDATE, pentru a realiza actualizări dinamice.

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. Dar, serverele DNS care sunt bazate pe BIND 8 sau mai recent, pot fi configurate pentru
| a accepta cereri de la alte surse pentru a actualiza datele zonei dinamic.

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 înregistrări de mapare de adrese (A pentru IPv4 sau AAAA pentru IPv6), înregistrări inverse (PTR), sau ambele din partea unui client. Înregistrarea de mapare de adresă (A sau AAAA) mapează numele de gazdă al maşinii pe adresele sale IP. Înregistrarea PTR mapează adresa IP a unei maşini o adresă la numele ei de gazdă. Când adresa unui client se modifică, DHCP poate trimite automat o actualizare serverului DNS astfel încât alte gazde din reţea să poată localiza clientul prin interogări DNS la noua adresă IP a clientului. Pentru fiecare înregistrare care este actualizată dinamic se scrie o înregistrare TXT (Text) asociată pentru a identifica faptul că înregistrarea a fost scrisă de DHCP.

Notă: Dacă setaţi DHCP să actualizeze doar înregistrări PTR, trebuie să configuraţi DNS pentru a permite actualizări de la clienţi, astfel încât fiecare client să poată actualiza înregistrarea sa A (când clientul foloseşte adresa IPv4) sau înregistrarea sa AAAA (când clientul foloseşte adresa IPv6). Nu toţi clienţii DHCP suportă marcarea cererilor de actualizare înregistrare A sau AAAA. 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.

Actualizări dinamice pot fi realizate între DNS şi DHCP pe o singură platformă System i, între platforme diferite System i sau între o platformă System i şi alte sisteme care sunt capabile de actualizări dinamice.

Notă: API-ul Actualizare dinamică DNS (QTOBUPDT) este necesar pe serverele care trimit actualizări dinamice la DNS. Este instalat automat cu i5/OS opţiunea 31, DNS. Totuşi, în BIND 9, comanda NSUPDATE este metoda preferată pentru a face actualizări pe platforma System i.

Concepte înrudite

Dynamic Host Configuration Protocol

Operaţii înrudite

“Configurarea DNS pentru a primi actualizări dinamice” la pagina 29
Serverele DNS care rulează BIND 9 pot fi configurate să accepte cereri din alte surse pentru a actualiza datele de zonă dinamic. Acest subiect furnizează instrucţiuni pentru configurarea opţiunii de permitere-actualizare pentru ca DNS să poată recepţiona actualizări dinamice.

Configurarea DHCP pentru a trimite actualizări dinamice de DNS

Referinţe înrudite

“Exemplu: DNS şi DHCP pe acelaşi System i” la pagina 18
Acest exemplu arată DNS şi DHCP pe aceeaşi platformă System i.

“Înregistrările resursă Domain Name System” la pagina 9
Înregistrările resursă sunt utilizate pentru a stoca date despre numele de domeniu şi adresele IP. Puteţi folosi tabela de căutare înregistrare resursă pentru a căuta înregistrările de resurse suportate pentru sistemul de operare i5/OS.

QTOBUPT

“Caracteristicile BIND 9”
BIND 9 este similar cu BIND 8; totuşi, furnizează mai multe caracteristici pentru a îmbunătăţii performanţa serverului DNS, cum ar fi vizualizările.

Caracteristicile BIND 9

BIND 9 este similar cu BIND 8; totuşi, furnizează mai multe caracteristici pentru a îmbunătăţii performanţa serverului DNS, cum ar fi vizualizările.

Vizualizările pe un singur server DNS i5/OS

Instrucţiunea *view* permite unei singure instanţe DNS să răspunsă la o interogare diferit în funcţie de sursa interogării, cum ar fi internet sau intranet.

O aplicaţie practică a caracteristicii de vizualizare este să împărţiţi setări DNS fără a trebui să rulaţi mai multe servere de DNS. De exemplu, într-un singur server DNS, puteţi definiţi o vizualizare pentru a răspunde la interogările dintr-o reţea internă, în timp ce definiţi altă vizualizare pentru a răspunde la interogările dintr-o reţea externă.

Noi comenzi client

Următoarele comenzi client îmbunătăţesc capabilitatea de gestiune a serverului de DNS:

NSUPDATE
Comanda NSUPDATE este folosită pentru a lansa cereri de actualizare dinamică DNS după cum este definit în RFC-ul 2136 pe un server DNS. Această permite adăugarea sau înlăturatea înregistrărilor de resurse dintr-un zonă în timp ce serverul de DNS rulează. Ca urmare, nu trebuie să actualizaţi înregistrările editând manual fişierul de zonă. O singură cerere de actualizare poate conţine cereri pentru a adăuga sau înlătura mai multe înregistrări de resurse, dar înregistrările resurselor care sunt adăugate sau înlăturate dinamic cu comanda NSUPDATE trebuie să fie în aceeaşi zonă.

Notă: Nu editaţi manual zonele care sunt sub control dinamic folosind comanda NSUPDATE sau printr-un server DHCP. Editările manuale ar putea intra în conflict cu actualizările dinamice şi pot duce la pierderea datelor.

DIG DIG (Domain Information Groper) este o unealtă de interogare mai puternică decât comanda NSLOOKUP (Name Server Lookup), pe care o puteţi folosi pentru a extrage informaţii de pe un server de DNS sau pentru a testa răspunsul unui server de DNS. Comanda NSLOOKUP este depreciată şi este furnizată doar pentru compatibilitate cu versiunile anterioare. Puteţi folosi DIG pentru a verifica dacă un server DNS răspunde corect înainte să configuraţi sistemul pentru a-l folosi. Puteţi de asemenea extrage informaţii DNS despre gazde, domenii şi alte servere DNS folosind DIG.

Puteţi folosi comanda de pornire interogare DIG (STRDIGQRY) sau alias-ul său DIG pentru a porni unealta Domain Information Groper.

HOST Comanda de pornire a interogării HOST (HOST) este folosită pentru căutări DNS. O puteţi folosi pentru a converti nume de domenii în adrese IP (IPv4 sau IPv6) şi invers.

RNDC

Comanda RNDC (Remote Name Daemon Control) este un utilitar puternic, ce permite unui administrator de sistem să controleze operarea unui server de nume. Ea citeşte un fişier de configurare, numit rndc.conf, pentru a determina cum să contactaţi serverul de nume şi pentru a determina ce algoritm şi cheie ar trebui folosite. Dacă nu este găsit niciun fişier rndc.conf, este folosit implicit un fişier rndc-key._KID care este creat în timpul instalării şi care acordă automat acces prin interfaţa loopback.

Suportul IPv6

BIND 9 suportă căutări nume-adresă şi adresă-nume în toate formele definite curent de IPv6. Pentru căutări înainte, BIND 9 suportă înregistrări AAAA şi A6, dar înregistrările A6 sunt acum depreciate. Pentru cereri inverse IPv6, suportă formatul tradiţional ”nibble” folosit în domeniul ip6.arpa, precum şi domeniul mai vechi, depreciat, ip6.int.

Fişierele de jurnal

Fişierele de jurnal sunt folosite pentru a ţine actualizări dinamice pentru o zonă. Fişierul este creat automat când este primită prima actualizare dinamică de la un client şi nu dispare. Acesta este un fişier binar, care nu ar trebui editat.

Cu fişierul de jurnal, când un server este repornit după o oprire sau o cădere, rulează din nou fişierul de jurnal pentru a încorpora în zona orice actualizări care au avut loc după ultimul dump de zonă. Fişierele de jurnal sunt de asemenea folosite pentru a stoca actualizări pentru metoda IXFR.

DNS pentru i5/OS a fost reproiectat pentru a folosi BIND 9. Pentru a rula BIND 9 DNS pe sistem, sistemul trebuie să îndeplinească anumite cerinţe software.

Concepte înrudite

"Cerinţele Domain Name System" la pagina 26
Luaţi în considerare acele cerinţe software pentru a rula DNS pe platforma System i.

"Actualizările dinamice" la pagina 6
i5/OS DNS care este bazat pe BIND 9 suportă actualizări dinamice. Surse externe, cum ar fi DHCP, pot trimite actualizări unui server DNS. În plus, puteţi de asemenea folosi unelte client DNS, cum ar fi NSUPDATE, pentru a realiza actualizări dinamice.

"Ce este nou pentru V6R1" la pagina 1
Citiţi despre informaţii noi sau modificate semnificativ pentru colecţia de subiecte DNS.

Referinţe înrudite

"Exemplu: Împărţirea DNS peste firewall setând două servere DNS pe acelaşi System i" la pagina 20
Acest exemplu arată un server DNS care operează peste un firewall pentru a proteja datele interne din internet, permiţând utilizatorilor interni să acceseze date de pe internet. Această configuraţie realizează această protecţie setând două servere DNS pe aceeaşi platformă System i.

"Planificarea măsurilor de securitate" la pagina 25
DNS (Domain Name System) oferă opţiuni de securitate pentru limitarea accesului din exterior la serverul dumneavoastră.

Înregistrările resursă Domain Name System

Înregistrările resursă sunt utilizate pentru a stoca date despre numele de domeniu şi adresele IP. Puteţi folosi tabela de căutare înregistrare resursă pentru a căuta înregistrările de resurse suportate pentru sistemul de operare i5/OS.

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.

Notă: Intrările din tabela de căutare înregistrare resursă ar putea fi adăugate sau înlăturate conform cu modificările documentului BIND. De asemenea, aceasta nu este o listă completă a tuturor înregistrărilor de resurse listate în BIND.

Tabela 1. Tabela de căutare a înregistrărilor resursă

Înregistrare resursă	Abreviere	Descriere
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	O înregistrare 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.

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

Înregistrare resursă	**Abreviere**	**Descriere**
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 informaţii generale despre o 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.
Înregistrările Integrated Services Digital Network	ISDN	Înregistrarea ISDN specifică adresa acestui obiect. Această înregistrare mapează un nume gazdă la adresa ISDN. Ele sunt utilizate doar în reţelele ISDN. Acest tip de înregistrări este definit în RFC 1183.
Înregistrările IP Version 6 Address (Adresă IP versiunea 6)	AAAA	Înregistrarea AAAA specifică adresa IPv6 de 128 de biţi a unei gazde. Înregistrările AAAA, care sunt similare cu înregistrările A, sunt folosite pentru a rezolva interogările pentru adresa IPv6 a unui anumit nume de domeniu. 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.

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

Înregistrare resursă	Abreviere	Descriere
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.
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 înregistrări 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.

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

Înregistrare resursă	Abreviere	Descriere
Înregistrări de servicii	SRV	Înregistrarea SRV specifică gazdele care suportă serviciile definite în înregistrare. Acest tip de înregistrare este definită în RFC 2782.
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.
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. Înregistrările TXT sunt folosite de i5/OS DHCP pentru actualizări dinamice. Serverul DHCP scrie o înregistrare TXT asociată pentru fiecare actualizare de înregistrare PTR şi A care este făcută de serverul DHCP. Înregistrările DHCP au un prefix de AS400DHCP.
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

"Înregistrările Mail şi Mail Exchanger" la pagina 13
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 14
Acest exemplu descrie o subreţea simplă cu un server DNS (Domain Name System) pentru utilizare internă.
"Înţelegerea zonelor" la pagina 3
Datele DNS sunt împărţite în seturi de date gestionabile, numite *zone*. Fiecare dintre aceste seturi este un tip specific de zonă.

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 din înregistrările resurse DNS conţine tipurile de înregistrări mail pe care le suportă i5/OS DNS.

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 dacă este utilizată o gazdă 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, acestea permit unui mail care este adresat unei gazde să fie livrat unei gazde diferite.

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: Folosirea unui caracter de înlocuire (exemplu: *.mycompany.com) în înregistrări MX pentru un domeniu nu este indicată.

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 9
Înregistrările resursă sunt utilizate pentru a stoca date despre numele de domeniu şi adresele IP. Puteţi folosi tabela de căutare înregistrare resursă pentru a căuta înregistrările de resurse suportate pentru sistemul de operare i5/OS.

Exemple: DNS

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 figură arată DNS rulând pe o platformă System i pentru o reţea internă. Această unică instanţă de server DNS este setată pentru a asculta interogările pentru toate adresele IP. Sistemul este un server de nume primar pentru zona mycompany.com.

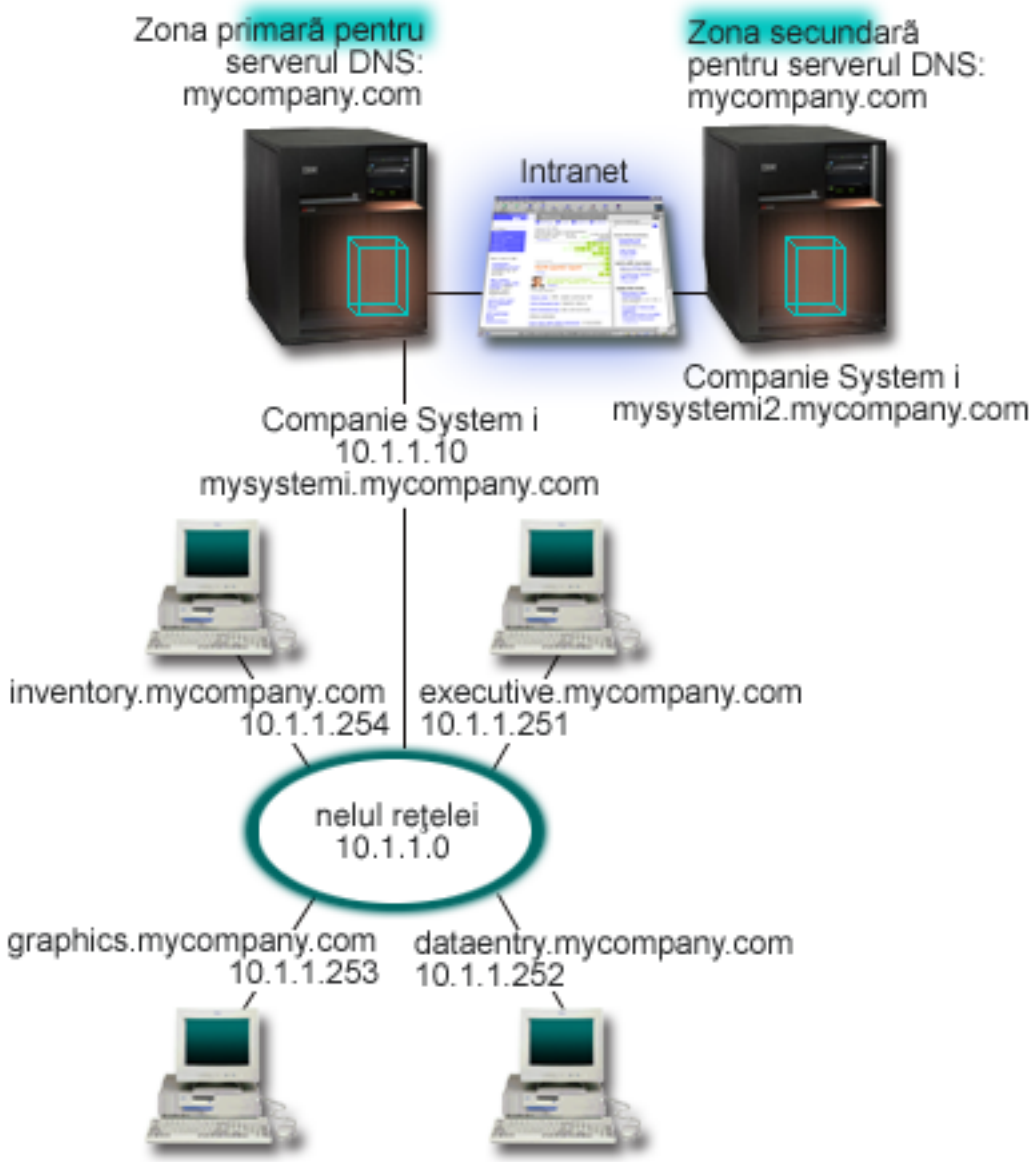

Figura 2. Un singur server DNS pentru o reţea internă

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 de adresă (A pentru IPv4 sau AAAA pentru IPv6) mapează numele unei maşini pe 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.

În afară de înregistrări A, AAAA şi PTR, DNS suportă multe alte înregistrări de resurse care ar putea fi necesare, în funcţie de ce alte aplicaţii bazate pe TCP/IP rulaţi în intranet. 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 de mai sus, serverul mysystemi face parte dintr-un intranet. Alt sistem, mysystemi2, a fost configurat să se comporte 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 9
Înregistrările resursă sunt utilizate pentru a stoca date despre numele de domeniu şi adresele IP. Puteţi folosi tabela de căutare înregistrare resursă pentru a căuta înregistrările de resurse suportate pentru sistemul de operare i5/OS.

"Înţelegerea zonelor" la pagina 3
Datele DNS sunt împărţite în seturi de date gestionabile, numite *zone*. Fiecare dintre aceste seturi este un tip specific de zonă.

"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 figură arată aceeaşi reţea exemplu din exemplul cu server DNS singular pentru intranet, dar 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.

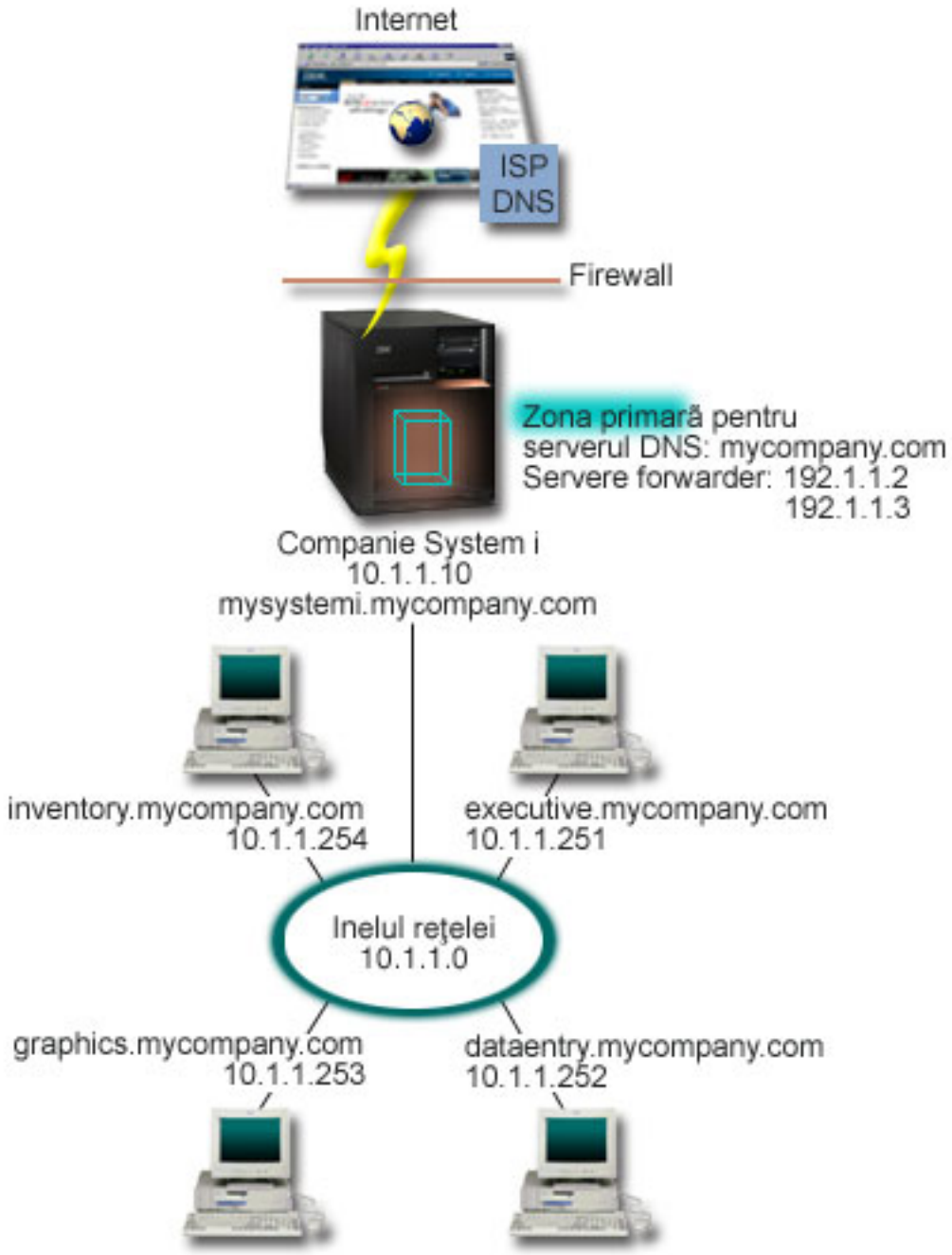

Figura 3. Un singur server DNS cu acces la Internet

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 pentru obţinerea serverelor rădăcină internet, consultaţi Accesarea datelor externe DNS.

- 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

  Nu este recomandat să permiteţi ca DNS-ul să fie conectat direct la internet. Trebuie să configuraţi un firewall sau să luaţi alte precauţii pentru a vă securiza platforma System i.

  Concepte înrudite

  “Setarea domeniului DNS (Domain Name System)” la pagina 6
  Setarea domeniului DNS necesită înregistrarea domeniului de nume pentru a-i împiedica pe alţii să folosească numele de domeniu.

  System i şi securitate internet

  “Înţelegerea interogărilor Domain Name System” la pagina 4
  Clienţii DNS folosesc servere DNS pentru a rezolva interogări. Interogările ar putea veni direct de la client sau dintr-o aplicaţie care rulează pe client.

  Referinţe înrudite

  “Exemplu: Un singur server Domain Name System pentru o reţea internă” la pagina 14
  Acest exemplu descrie o subreţea simplă cu un server DNS (Domain Name System) pentru utilizare internă.

Exemplu: DNS şi DHCP pe acelaşi System i

Acest exemplu arată DNS şi DHCP pe aceeaşi platformă System i.

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

Următoarea figură arată o subreţea mică cu o platformă System i care se comportă ca server DHCP şi DNS la 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.

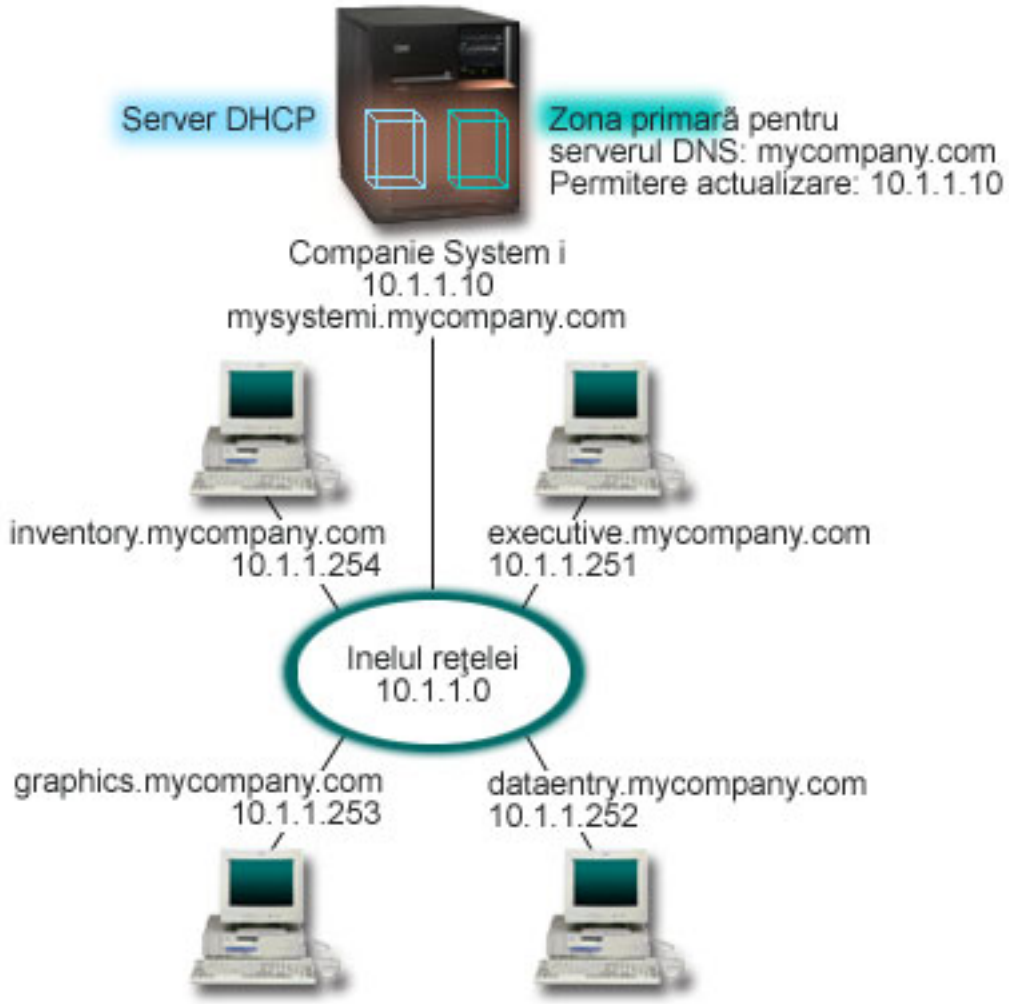

Figura 4. DNS şi DHCP pe aceeaşi platformă System i

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 i5/OS bazat pe BIND 9, puteţi configura zona DNS să accepte actualizări dinamice la înregistrări DNS în conjuncţie cu modificări intermitente de adresă prin DHCP. De exemplu, când serverul de fişier grafice îşi reînnoieşte chiria şi îi este asignată o adresă IP de 10.1.1.250 de către serverul DHCP, înregistrările DNS asociate sunt actualizate dinamic. Aceasta permite celorlalţi clienţi să interogheze serverul DNS pentru serverul de fişiere grafice după numele de gazdă fără întrerupere.

Pentru a configura o zonă DNS pentru acceptarea actualizărilor dinamice, completaţi următoarele taskuri:

- 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. Consultaţi Determinarea structurii domeniului pentru informaţii suplimentare despre configurarea zonelor să folosească funcţia 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 6
i5/OS DNS care este bazat pe BIND 9 suportă actualizări dinamice. Surse externe, cum ar fi DHCP, pot trimite actualizări unui server DNS. În plus, puteţi de asemenea folosi unelte client DNS, cum ar fi NSUPDATE, pentru a realiza actualizări dinamice.

Operaţii înrudite

Configurarea DHCP pentru a trimite actualizări dinamice de DNS

Referinţe înrudite

Exemplu: DNS şi DHCP pe platforme diferite System i

Exemplu: Împărţirea DNS peste firewall setând două servere DNS pe acelaşi System i

Acest exemplu arată un server DNS care operează peste un firewall pentru a proteja datele interne din internet, permiţând utilizatorilor interni să acceseze date de pe internet. Această configuraţie realizează această protecţie setând două servere DNS pe aceeaşi platformă System i.

Următoarea figură arată o subreţea simplă care foloseşte un firewall pentru securitate. Să presupunem că compania are o reţea internă cu spaţiu de IP-uri rezervat şi o secţiune externă a unei reţele care este disponibilă publicului. Compania doreşte să poată rezolva clienţii interni numele de gazdă externe şi să facă schimb de poştă cu persoane 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.

Cu i5/OS DNS bazat pe BIND 9, puteţi folosi două metode pentru a realiza aceasta. Prima metodă este că compania setează două instanţe de server de DNS pe aceeaşi platformă System i, una pentru intranet şi alta pentru orice este în domeniul său public, care este descris în acest exemplu. Altă metodă este de a folosi funcţia de vizualizare care este furnizată în BIND 9, care este descrisă în exemplul despre împărţirea DNS peste firewall folosind o vizualizare.

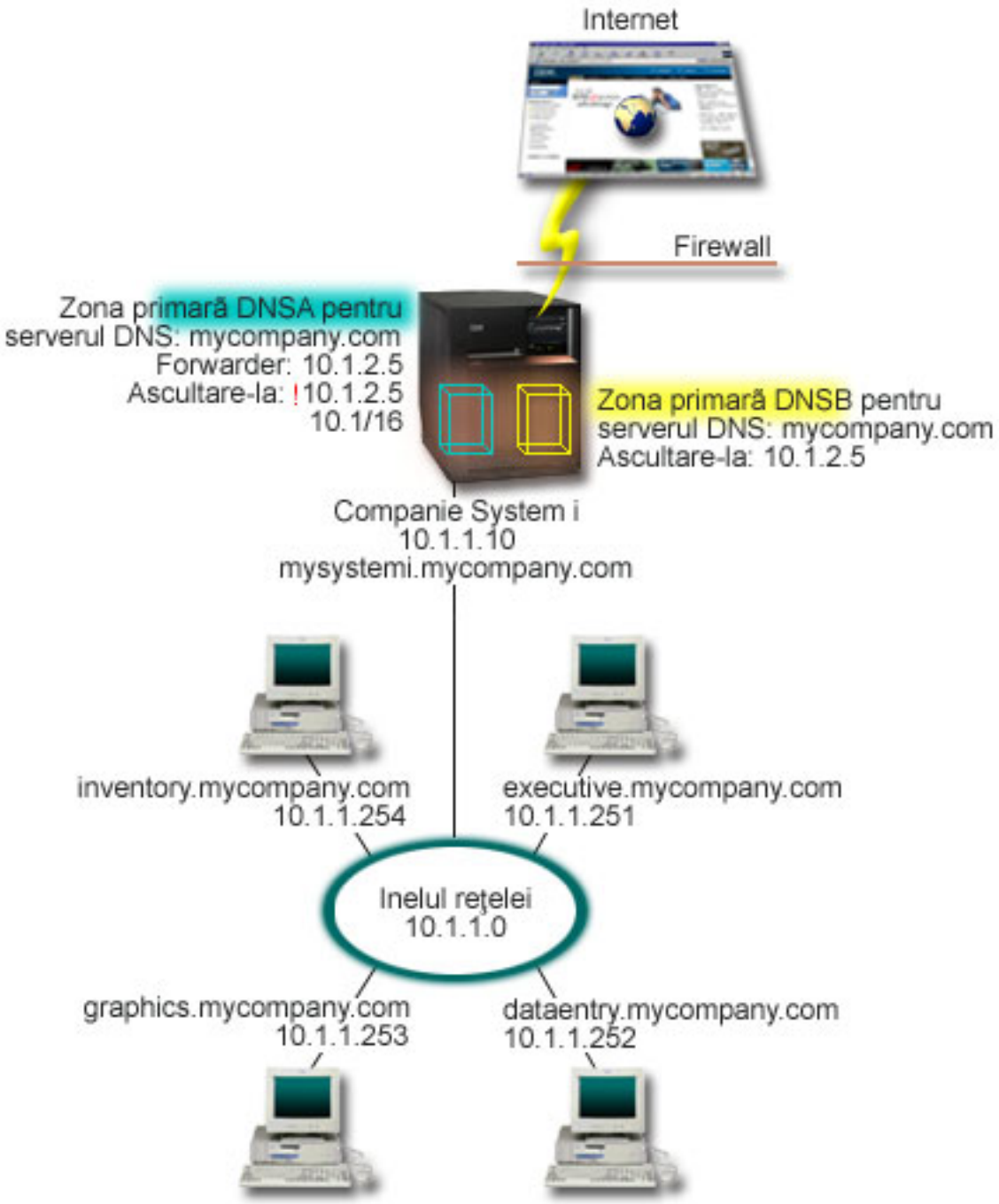

Figura 5. Împărţirea DNS peste un firewall setând două servere DNS pe acelaşi System i

Serverul extern, DNSB, este configurat cu zona 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 zona primară mycompany.com, dar datele zonei definite în DNSA conţin înregistrări de resurse intranet. Opţiunea de 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 corect, clienţii interni trebuie să fie configuraţi să interogheze doar serverul DNSA. Trebuie să luaţi în considerare următoarele setări de configurare pentru a împărţi DNS:

- Ascultare-la

  În alte exemple DNS, doar un server DNS este pe o platformă System i. Este setat să asculte la toate adresele IP de interfaţă. De fiecare dată când aveţi mai multe servere DNS pe o platformă System i, trebuie să definiţi adresele IP de interfaţă pe care ascultă fiecare. Două servere DNS nu pot asculta la aceeaşi adresă. În acest caz, să presupunem că toate interogările care vin din firewall sunt trimise pe 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 să accepte interogări de pe oricare din adresele de pe interfaţa 10.1.x.x cu excepţia 10.1.2.5. Pentru exclude efectiv această adresă, lista de potrivire adrese trebuie să aibă adresa exclusă listată înainte de prefixul adresei incluse.

- Ordine listă potrivire adrese

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

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

Referinţe înrudite

"Caracteristicile BIND 9" la pagina 7
BIND 9 este similar cu BIND 8; totuşi, furnizează mai multe caracteristici pentru a îmbunătăţii performanţa serverului DNS, cum ar fi vizualizările.

"Exemplu: Împărţirea DNS peste firewall folosind această vizualizare"
Acest exemplu arată un server DNS care operează peste un firewall pentru a proteja date interne de pe internet, permiţând utilizatorilor interni să acceseze date din internet folosind caracteristica *vizualizare* pe care o furnizează BIND 9.

Exemplu: Împărţirea DNS peste firewall folosind această vizualizare

Acest exemplu arată un server DNS care operează peste un firewall pentru a proteja date interne de pe internet, permiţând utilizatorilor interni să acceseze date din internet folosind caracteristica *vizualizare* pe care o furnizează BIND 9.

Următoarea figură arată o subreţea simplă care foloseşte un firewall pentru securitate. Să presupunem că compania are o reţea internă cu spaţiu de IP-uri rezervat şi o secţiune externă a unei reţele care este disponibilă publicului. Compania doreşte să poată rezolva clienţii interni numele de gazdă externe şi să facă schimb de poştă cu persoane din afara reţelei. Compania vrea de asemenea ca rezolvitorii interni să aibă acces la anumite zone interne care nu sunt disponibile în afara reţelei interne. Însă compania nu vrea ca rezolvatorii externi să aibă acces la reţeaua internă.

Cu i5/OS DNS bazat pe BIND 9, puteţi folosi două metode pentru a realiza aceasta. Metoda descrisă în acest exemplu este că puteţi configura serverul DNS cu două vizualizări diferite pentru a asculta diverse interogări, una pentru intranet şi alta pentru orice este în domeniul său public. Alt mod este de a seta instanţele de server DNS pe aceeaşi platformă System i, care este descris în exemplu despre împărţirea DNS peste un firewall folosind două servere DNS.

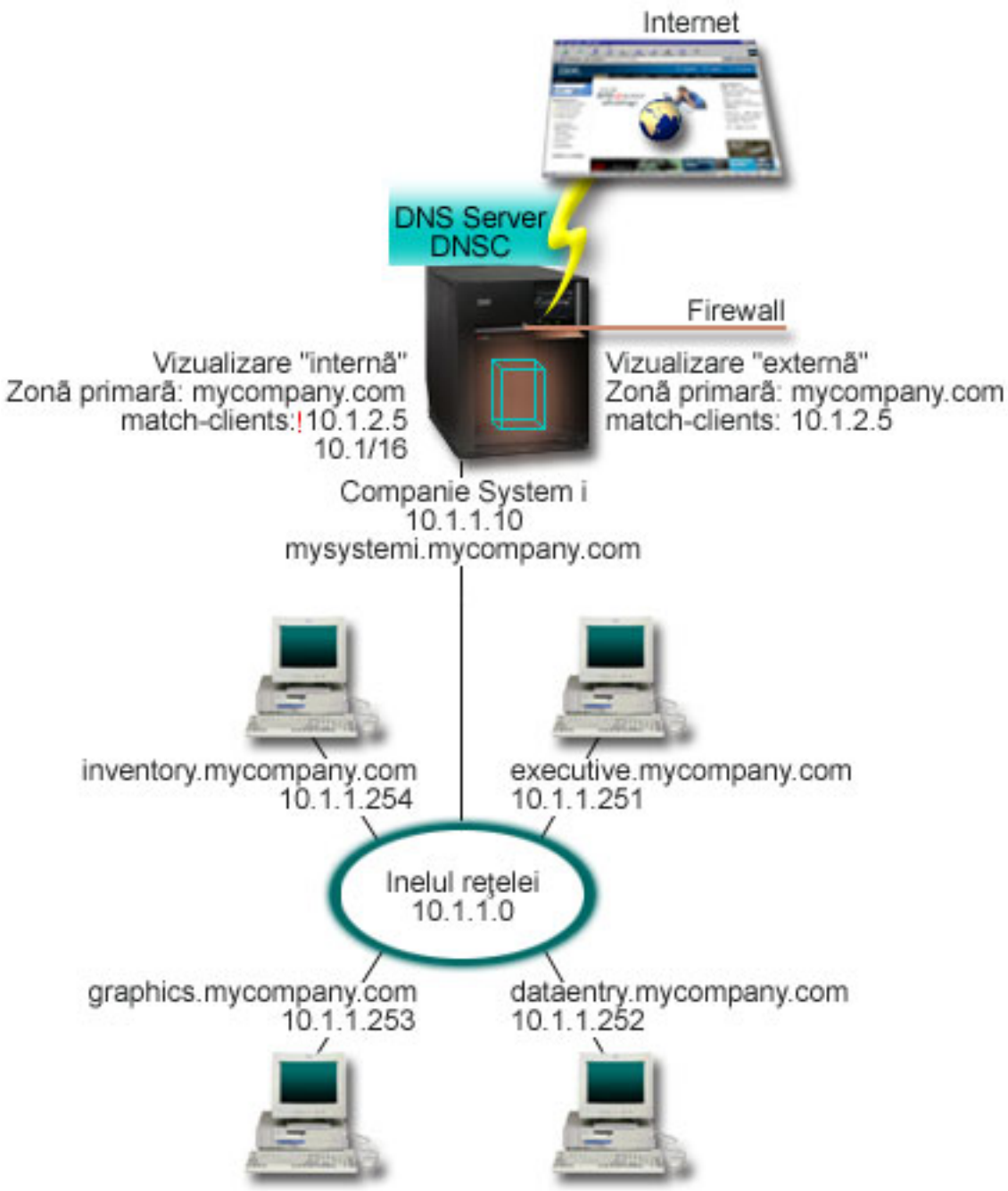

Figura 6. Împărţirea DNS peste un firewall folosind vizualizare

Serverul DNS, DNSC, defineşte două vizualizări, numite *externă* şi *internă*. Vizualizarea *externă* este configurată cu o zonă primară mycompany.com care include doar înregistrările de resurse care se intenţionează să facă parte din domeniul public, în timp ce vizualizarea *internă* este configurată cu o zonă primară mycompany.com care conţine înregistrări de resurse.

Dacă sunteţi preocupat despre integritatea firewall-ului şi a altor ameninţări de securitate, aveţi opţiunea de a folosi subinstrucţiunea match-clients pentru a ajuta la protejarea datelor interne. Pentru a face aceasta, puteţi configura vizualizarea internă pentru a permite doar interogări la zona internă mycompany.com de la gazde interne. Pentru a seta divizarea DNS, trebuie să luaţi în considerare următoarele setări de configurare:

- Match-clients

Match-clients într-o instrucţiune vizualizare ia o listă de potrivire de adrese ca argument. Doar adresa IP a unei interogări care se potriveşte cu lista de potrivire adrese poate vedea valorile de configuraţie definite în vizualizarea înconjurătoare. Dacă adresa IP a unei interogări se potriveşte cu mai multe intrări match-clients în diverse instrucţiuni de vizualizare, prima instrucţiune de vizualizare este cea care se aplică. În acest caz, să presupunem că toate interogările care vin din firewall sunt trimise în 10.1.2.5. Aceste interogări ar trebui manipulate de datele de zonă din vizualizarea externă. De aceea, 10.1.2.5 este setat să fie match-clients al vizualizării externe. Vizualizarea internă este configurată să accepte interogări de la oricine de pe adresele IP din interfaţa 10.1.x.x cu excepţia 10.1.2.5. Pentru exclude efectiv această adresă, lista de potrivire adrese trebuie să aibă adresa exclusă listată înainte de prefixul adresei incluse.

- Ordine listă potrivire adrese

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

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

Referinţe înrudite

"Exemplu: Împărţirea DNS peste firewall setând două servere DNS pe acelaşi System i" la pagina 20
Acest exemplu arată un server DNS care operează peste un firewall pentru a proteja datele interne din internet, permiţând utilizatorilor interni să acceseze date de pe internet. Această configuraţie realizează această protecţie setând două servere DNS pe aceeaşi platformă System i.

Planificarea pentru DNS

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. Subiecte, precum structură de reţea, performanţă şi securitate, ar trebui accesate.

Determinarea autorizărilor DNS

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.

Un nivel minim de autorizare este necesar pentru a permite administratorului să configureze şi să administreze 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). Folosiţi System i Navigator pentru a autoriza utilizatori. Dacă aveţi nevoie de informaţii suplimentare, consultaţi subiectul Acordarea de autorizare administratorului 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 DNS" la pagina 33
Puteţi folosi i5/OS DNS pentru a crea şi gestiona instanţe de server DNS pe platforma System i. Fişierele de configuraţie pentru DNS sunt gestionate de System i Navigator. Trebuie să nu editaţi manual fişierele. Folosiţi întotdeauna System i Navigator pentru a crea, modifica sau şterge fişierele de configuraţie DNS.

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.

i5/OS DNS furnizează o interfaţă grafică pentru configurarea sistemelor. În unele cazuri, interfaţa utilizează terminologii sau concepte care pot fi prezentate diferit în alte surse. Dacă consultaţi alte surse de informaţii când planificaţi configuraţia DNS, ar putea fi util să nu uitaţi următoarele elemente:

- Toate zonele şi obiectele definite pe o platformă System i sunt organizate în folderele Zone căutare directă şi Zone căutare inversă. Zonele de căutare directă sunt zonele care sunt folosite pentru a mapa nume de domenii la adrese IP, cum ar fi înregistrări A şi AAAA. Zonele de căutare inversă sunt zone care sunt utilizate pentru maparea adresei IP la numele de domeniu, ca şi înregistrările PTR.
- i5/OS DNS se referp la *zone primare* şi *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.

Planificarea măsurilor de securitate

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

Listele de potrivire a adreselor

DNS utilizează liste de potrivire a adreselor 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 în listă de potrivire a adreselor

Primul element dintr-o listă de potrivire adrese cu care se potriveşte o adresă dată este folosit. De exemplu, pentru a permite toate adresele din reţeaua 10.1.1.x cu excepţia 10.1.1.5, elementele din lista de potrivire trebuie să fie în ordine (!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 refuzată imediat.

Dacă elementele sunt inversate (10.1.1/24; !10.1.1.5), adresei IP 10.1.1.5 îi va fi permis accesul deoarece serverul o va compara cu primul element, care se potriveşte şi o va permite vă a verifica restul regulilor.

Opţiunile de control al accesului

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.

Securizarea serverul dumneavoastră DNS este esenţială. În afară de considerentele de securitate din acest subiect, securitatea DNS şi securitatea System i sunt acoperite într-o varietate de surse inclusiv platforma System i şi colecţia de subiecte Internet. Cartea *DNS and BIND* acoperă de asemenea securitatea legată de DNS.

Concepte înrudite

System i şi securitate internet

Referinţe înrudite

"Caracteristicile BIND 9" la pagina 7
BIND 9 este similar cu BIND 8; totuşi, furnizează mai multe caracteristici pentru a îmbunătăţii performanţa serverului DNS, cum ar fi vizualizările.

Cerinţele Domain Name System

Luaţi în considerare acele cerinţe software pentru a rula DNS pe platforma System i.

Caracteristica DNS, opţiunea 31, nu poate fi instalată automat cu sistemul de operare. Trebuie să selectaţi DNS în mod specific pentru instalare. Serverul DNS adăugat pentru i5/OS este bazat pe implementarea DNS standard cunoscută ca BIND 9. Serviciile anterioare OS/400 DNS au fost bazate pe BIND 8.2.5 şi sunt încă disponibile în i5/OS.

După ce DNS este instalat, trebuie să migraţi şi să configuraţi serverul DNS de la BIND 4 sau 8 la BIND 9. Trebuie să aveţi i5/OS PASE instalat, care este opţiunea 33 a i5/OS. După ce i5/OS PASE este instalat, System i Navigator manipulează automat configurarea implementării curente BIND.

Dacă vreţi să configuraţi un server DHCP pe o platformă diferită pentru a trimite actualizări la acest server DNS, pe acel server DHCP trebuie instalată de asemenea opţiunea 31. Serverul DHCP foloseşte interfeţele de programare furnizate de opţiunea 31 pentru a realiza actualizări dinamice.

Concepte înrudite

i5/OS PASE

"Configurarea DNS" la pagina 27
Puteţi folosi System i Navigator pentru a configura servere de nume şi pentru a rezolva interogări în afara domeniului dumneavoastră.

Referinţe înrudite

"Caracteristicile BIND 9" la pagina 7
BIND 9 este similar cu BIND 8; totuşi, furnizează mai multe caracteristici pentru a îmbunătăţii performanţa serverului DNS, cum ar fi vizualizările.

Determinarea dacă DNS este instalat

Pentru a determina dacă DNS este instalat, urmaţi aceşti paşi.

1. La linia de comandă, tastaţi GO LICPGM şi apăsaţi Enter.

2. Tastaţi 10 (Afişarea programelor cu licenţă instalate) şi apăsaţi Enter.
3. Mergeţi la următoarea pagină la **5761SS1 DNS** (Opţiunea 31). Dacă DNS este instalat cu succes, starea instalată este *COMPATIBLE, după cum este arătat aici:

```
PgmLic       Starea de instalare       Descrierea
5761SS1    *COMPATIBLE          DNS
```

4. Apăsaţi F3 pentru a ieşi din ecran.

Instalarea DNS

Pentru a instala DNS, urmaţi aceşti paşi.

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 DNS

Puteţi folosi System i Navigator pentru a configura servere de nume şi pentru a rezolva interogări 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 26
Luaţi în considerare acele cerinţe software pentru a rula DNS pe platforma System i.

Accesarea DNS în System i Navigator

Aceste instrucţiuni vă ghidează în interfaţa de configurare DNS din System i Navigator.

Dacă folosiţi i5/OS PASE, veţi putea configura servere DNS bazate pe BIND 9.

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

1. În System i Navigator, expandaţi ***sistemul dumneavoastră*** → **Reţea** → **Servere** → **DNS**.
2. Faceţi clic dreapta pe **DNS** şi selectaţi **Configuraţie nouă**.

Concepte înrudite

Introducerea în System i Navigator

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.

i5/OS DNS pe bază de BIND 9 suportă mai multe instanţe 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 creaţi mai multe instanţe, repetaţi aceste proceduri până când toate instanţele pe care le vreţi 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 DNS" la pagina 33
Puteţi folosi i5/OS DNS pentru a crea şi gestiona instanţe de server DNS pe platforma System i. Fişierele de configuraţie pentru DNS sunt gestionate de System i Navigator. Trebuie să nu editaţi manual fişierele. Folosiţi întotdeauna System i Navigator pentru a crea, modifica sau şterge fişierele de configuraţie DNS.

Crearea unei instanţe de server de nume

Noul vrăjitor de configurare DNS vă poate ghida prin procesul de definire a unei instanţe de server DNS.

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

1. În System i Navigator, expandaţi ***sistemul dumneavoastră*** → **Reţea** → **Servere** → **DNS**.
2. În panoul din stânga, faceţi clic dreapta pe **DNS** şi selectaţi **Server de nume nou**.
3. Urmaţi instrucţiunile vrăjitorului pentru a finaliza procesul de configurare.

Vrăjitorul necesită următoarele intrări:

Numele serverului DNS:
Specificaţi un nume pentru serverul DNS. Poate avea maxim 5 caractere şi trebuie să înceapă cu un caracter alfabetic (A-Z). Dacă creaţi servere multiple, fiecare trebuie să aibă un nume unic. Acest nume este referit ca numele instanţei 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 pe toate adresele IP. Dacă creaţi instanţe de server suplimentare, acestea nu pot fi configurate să asculte pe toate adresele IP. Altfel, acestea nu pot rula simultan. 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: Ar trebui să luaţi în considerare încărcarea serverelor rădăcină internet implicite dacă aveţi acces la internet şi vă aşteptaţi ca DNS-ul să poată rezolva complet numele din internet.

Pornire server:
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 de server DNS

După ce aţi creat un server de nume, puteţi edita proprietăţi cum ar fi permiterea actualizării 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 System i Navigator, expandaţi ***sistemul dumneavoastră*** → **Reţea** → **Servere** → **DNS**.
2. În panoul din dreapta, faceţi clic dreapta pe ***server DNS*** şi selectaţi **Configurare**.
3. În fereastra Configurare DNS, faceţi clic dreapta pe **Server DNS** şi selectaţi **Proprietăţi**.
4. Editaţi proprietăţile corespunzătoare pe care le vreţi.

Configurarea de zone pe un server de nume

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

Pentru a configura zone pe server, urmaţi aceşti paşi:

1. În System i Navigator, expandaţi ***sistemul dumneavoastră*** → **Reţea** → **Servere** → **DNS**.
2. În panoul din dreapta, faceţi clic dreapta pe ***server DNS*** şi selectaţi **Configurare**.
3. În fereastra Configurare DNS, selectaţi tipul de zonă pe care aţi vrea să îl creaţi pentru a crea făcând clic dreapta pe folderul **Zonă căutare directă** sau **Zonă căutare inversă**.
4. Urmaţi instrucţiunile vrăjitorului pentru a finaliza procesul de creare.

Concepte înrudite

"Accesarea datelor externe DNS" la pagina 30
Atunci când creaţi datele de zonă DNS (Domain Name System), serverul dumneavoastră va putea rezolva interogările către acea zonă.

Operaţii înrudite

"Configurarea DNS pentru a primi actualizări dinamice"
Serverele DNS care rulează BIND 9 pot fi configurate să accepte cereri din alte surse pentru a actualiza datele de zonă dinamic. Acest subiect furnizează instrucţiuni pentru configurarea opţiunii de permitere-actualizare pentru ca DNS să poată recepţiona actualizări dinamice.

"Importarea fişierelor DNS" la pagina 30
DNS poate importa fişiere de zonă existente. Urmaţi aceste proceduri de economisire a timpului pentru crearea unei noi zone dintr-un fişier de configurare existent.

Referinţe înrudite

"Înţelegerea zonelor" la pagina 3
Datele DNS sunt împărţite în seturi de date gestionabile, numite *zone*. Fiecare dintre aceste seturi este un tip specific de zonă.

Configurarea vizualizărilor pe un server de nume

Una din caracteristicile pe care BIND 9 le oferă este instrucţiunea *vizualizare*, care permite unei singure instanţe DNS să răspundă la o interogare diferit în funcţie de sursa interogării, cum ar fi internet sau intranet. O aplicaţie practică de vizualizare este să împărţiţi setări DNS fără a trebui să rulaţi mai multe servere de DNS.

Pentru a configura vizualizări pe server, urmaţi aceşti paşi:

1. În System i Navigator, expandaţi ***sistemul dumneavoastră*** → **Reţea** → **Servere** → **DNS**.
2. În panoul din dreapta, faceţi clic dreapta pe ***server DNS*** şi selectaţi **Configurare**.
3. În fereastra Configurare DNS, faceţi clic dreapta pe **Vizualizări** şi selectaţi **Vizualizare nouă**.
4. Urmaţi instrucţiunile vrăjitorului pentru a finaliza procesul de creare.

Configurarea DNS pentru a primi actualizări dinamice

Serverele DNS care rulează BIND 9 pot fi configurate să accepte cereri din alte surse pentru a actualiza datele de zonă dinamic. 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 aveţi nevoie să faceţi actualizări manuale la o zonă dinamică, trebuie să opriţi serverul de zonă dinamic şi să îl reporniţi după ce aţi finalizat actualizările. Oprirea serverului îl forţează să actualizeze baza de date a zonei cu toate actualizările dinamice care au fost făcute de când serverul a încărcat prima dată datele de zonă din baza de date a zonei. Dacă nu opriţi serverul, veţi pierde orice actualizări manuale asupra bazei de date a zonei deoarece acestea vor fi suprascrise de serverul care rulează. 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 System i Navigator, expandaţi ***sistemul dumneavoastră*** → **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 de adrese, selectaţi un tip de element de listă de potrivire de adrese şi apăsaţi **Adăugare**. Puteţi adăuga o Adresă IP, 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.

Operaţii înrudite

"Configurarea de zone pe un server de nume" la pagina 28
După ce configuraţi un server DNS (Domain Name System), trebuie să configuraţi zonele pentru serverul de nume.

Configurarea DHCP pentru a trimite actualizări dinamice de DNS

Importarea fişierelor DNS

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

Puteţi crea o zonă primară importând un fişier de date zonă care este un fişier de configuraţie de zonă validă pe baza sintaxei BIND. Fişierul ar trebui localizat într-un directorul din sistemul de fişiere integrat. Când este importat, DNS verifică că este un fişier de date zonă validă şi în adaugă în fişierul named.conf pentru instanţa de server specificată.

Pentru a importa un fişier zonă, parcurgeţi următorii paşi:

1. În System i Navigator, expandaţi ***sistemul dumneavoastră*** → **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 al ferestrei Configurare DNS, faceţi clic dreapta pe **server DNS** şi selectaţi **Importare zonă**.
4. Urmaţi instrucţiunile vrăjitorului pentru a importa zona primară.

Operaţii înrudite

"Configurarea de zone pe un server de nume" la pagina 28
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 externe DNS

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 de servere rădăcină implicite pentru System i Navigator

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 internet este livrată în System i Navigator. Lista este curentă când System i Navigator este emisă. Puteţi să verificaţi 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.

Obţinerea adreselor de server rădăcină din 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. Înregistraţi în istoric pe serverul InterNIC folosind FTP în metoda de anonimitate: FTP.INTERNIC.NET sau RS.INTERNIC.NET
2. Descărcaţi acest fişier: /domain/named.root
3. Stocaţi fişierul în următoarea cale de directoare: /QOpenSys/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.

Operaţii înrudite

"Configurarea de zone pe un server de nume" la pagina 28
După ce configuraţi un server DNS (Domain Name System), trebuie să configuraţi zonele pentru serverul de nume.

Gestionarea DNS

Gestionarea unui server DNS include verificarea că funcţia DNS funcţionează, monitorizarea performanţei şi întreţinerea datelor şi fişierelor DNS.

Verificarea funcţiei DNS

Unealta DIG vă poate ajuta să colectaţi informaţii şi să testaţi răspunsul unui server DNS. Puteţi folosi DIG pentru a verifica dacă un server DNS funcţionează corect.

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). Puteţi de asemenea interoga anumite nume care sunt definite în instanţa de server pe care încercaţi să o verificaţi. Aceasta confirmă că instanţa specifică de server pe care o testaţi funcţionează corect.

Pentru a verifica funcţia DNS cu DIG, urmaţi aceşti paşi:

1. În linia de comandă, tastaţi DIG HOSTNAME('127.0.0.1') REVERSE(*YES).

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

```
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id:865
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL:1

;; QUESTION SECTION:
;1.0.0.127.in-addr.arpa.          IN   PTR

;; ANSWER SECTION:
1.0.0.127.in-addr.arpa.  86400   IN    PTR  localhost.

;; AUTHORITY SECTION:
0.0.127.in-addr.arpa.   86400   IN    NS   ISA2LP05.RCHLAND.IBM.COM.

;; ADDITIONAL SECTION:
```

```
ISA2LP05.RCHLAND.IBM.COM. 38694   IN    A   9.5.176.194

;; Query time: 552 msec
;; SERVER: 9.5.176.194#53(9.5.176.194)
;; WHEN: Thu May 31 21:38:12 2007
;; MSG SIZE rcvd: 117
```

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

2. Apăsaţi Enter pentru a părăsi sesiunea.

Notă: Dacă aveţi nevoie de ajutor la folosirea DIG, tastaţi ?DIG 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 legate de DNS, care sunt chei DNS şi chei de actualizare dinamică. 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

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 să specificaţi cheia în lista de potrivire adrese.

Pentru administrarea cheilor DNS, parcurgeţi următorii paşi:

1. În System i Navigator, expandaţi ***sistemul dumneavoastră*** → **Reţea** → **Servere** → **DNS**.
2. În panoul din dreapta, faceţi clic dreapta pe instanţa de server DNS pe care vreţi să o gestionaţi şi selectaţi **Configurare**.
3. În fereastra Configurare DNS, selectaţi **Fişier** → **Gestionare chei**.

În fereastra Gestionare chei, puteţi realiza taskurile de gestiune corespunzătoare.

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 când DNS şi DHCP sunt pe aceeaşi platformă System i. Dacă DHCP este pe o platformă diferită System i, trebuie să distribuiţi aceleaşi fişiere cheie de actualizare dinamică pentru fiecare platformă la distanţă System i care are nevoie de ele pentru a trimite actualizări dinamice la serverele autoritative. Le puteţi distribui prin FTP, e-mail şi aşa mai departe.

Pentru a administra cheile de actualizare dinamică parcurgeţi următorii paşi:

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

Puteţi apoi realiza taskurile de gestiune corespunzătoare în fereastra Gestionare chei dinamice de actualizare.

Accesarea statisticilor serverului DNS

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 DNS"
Puteţi folosi i5/OS DNS pentru a crea şi gestiona instanţe de server DNS pe platforma System i. Fişierele de configuraţie pentru DNS sunt gestionate de System i Navigator. Trebuie să nu editaţi manual fişierele. Folosiţi întotdeauna System i Navigator pentru a crea, modifica sau şterge fişierele de configuraţie DNS.

Accesarea statisticilor de server

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 System i Navigator, expandaţi ***sistemul dumneavoastră*** → **Reţea** → **Servere** → **DNS**.
2. În panoul din dreapta, faceţi clic dreapta pe ***server DNS*** şi selectaţi **Configurare**.
3. În fereastra Configurare DNS, selectaţi **Vizualizare** → **Statistici server**.

| Puteţi de asemenea folosind comanda Control demon de nume la distanţă (RNDC) pentru a afişa informaţii despre
| statistici de server în fişierul named.stats. Comanda corespunzătoare este cum urmează.

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

Accesarea unei baze de date server active

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 activ al bazei de date server folosind System i Navigator. Dacă trebuie să salvaţi o copie a fişierelor, numele fişierului dump al bazei de date este named_dump.db în calea de directoare i5/OS: /QIBM/UserData/OS400/DNS/<server instance>/, unde <*instanţă server*> este numele instanţei de server DNS. Informaţii suplimentare despre baza de date server activă sunt disponibile în subiectul de ajutor online DNS Înţelegerea dump-ului de bază de date server DNS.

Pentru a accesa dump-ul bazei de date a serverului activ, parcurgeţi următorii paşi:

1. În System i Navigator, expandaţi ***sistemul dumneavoastră*** → **Reţea** → **Servere** → **DNS**.
2. În panoul din dreapta, faceţi clic dreapta pe ***server DNS*** şi selectaţi **Configurare**.
3. În fereastra Configurare DNS, selectaţi **Vizualizare** → **Baza de date a serverului activ**.

| Puteţi de asemenea folosi comanda Control demon de nume la distanţă (RNDC) pentru a afişa informaţiile bază de date
| server activ din fişierul named_dump.db. Comanda corespunzătoare este cum urmează.

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

Întreţinerea fişierelor de configurare DNS

Puteţi folosi i5/OS DNS pentru a crea şi gestiona instanţe de server DNS pe platforma System i. Fişierele de configuraţie pentru DNS sunt gestionate de System i Navigator. Trebuie să nu editaţi manual fişierele. Folosiţi întotdeauna System i Navigator pentru a crea, modifica sau şterge fişierele de configuraţie DNS.

Fişierele de configurare DNS sunt stocate în căile sistemului de fişiere integrat listate mai jos.

Notă: Structura de fişiere de mai jos este valabilă pentru DNS rulând pe BIND 9.

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.
/QIBM/UserData/OS400/DNS/ <*instance-n*>/		Directorul punct de plecare pentru o instanţă DNS.
ATTRIBUTES		DNS utilizează acest fişier pentru a determina ce versiune BIND utilizaţi.
BOOT.AS400BIND4		Fişierul de configuraţie şi politici server BIND 4.9.3 care este convertit la fişierul BIND 8 named.conf pentru această instanţă. Acest fişier este creat dacă migraţi un server BIND 4.9.3 la BIND 9. Serveşte ca rezervă pentru migrare şi poate fi şters când serverul BIND 9 funcţionează corect.
named.ca		Lista serverelor rădăcină pentru această instanţă server.
named.conf		Acest fişier conţine date de configurare. Spune serverului ce zone specifice gestionează, unde sunt fişierele de zonă, care zone pot fi actualizate dinamic, unde sunt serverele de înaintare şi alte setări de opţiuni.
named_dump.db		Dump de date server creat pentru baza de date a serverului activ.
named.memstats		Statistici de memorie server (dacă este configurat în named.conf).
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.
named.random		Fişier de entropie generat de server.
named.recursing		Interogările de servere care sunt recursive (dacă este cerut de System i Navigator).
named.run		Istoric de depanare implicit (dacă este cerut). Poate roll over ca named.run.0, named.run.1 şi aşa mai departe.
named.stats		Statisticile serverului.

Nume	Icoană	Descriere
<*primary-zone-n*>.db		Este fişierul primar de zonă pentru un anumit domeniu pe acest server. Fişierul conţine toate înregistrările de resursă pentru această zonă. Fiecare zonă are un fişier separat .db.
<*primary-zone-n*>.jnl		Fişier de jurnal care păstrează actualizări dinamice pentru o zonă. Este creat când prima actualizare dinamică este primită. Când un server este repornit după o oprire sau o cădere, răspunde fişierul de jurnal pentru a încorpora în zonă orice actualizări care au avut loc după ultimul dump de zonă. Acest fişier este de asemenea folosit pentru transfere incrementale de zonă (IXFR). Aceste fişiere de istoric nu dispar. Acesta este un fişier binar şi nu ar trebui editat.
db.<*secondary-zone-n*>		Fişier secundar de zonă pentru un anumit domeniu de pe acest server. Conţine toate înregistrările resursă pentru această zonă. Acest fişier este folosit pentru a încărca iniţial serverul secundar la pornire dacă serverul primar este intangibil. Fiecare zonă are un fişier separat .db.
/QIBM/UserData/OS400/DNS/_DYN/		Directorul care reţine fişierele cerute pentru actualizările dinamice.
<*key_id-n*>._KEY		.Symlink pentru cheia DNSSEC cu cheia <*key_id-n*>. Indică întotdeauna la ultima cheie K<*key_id-n*>.+*aaa*+*nnnnn*.key care este creată.
<*key_id-x*>._DUK. <*zone-a*>		Cheia de actualizare dinamică necesară pentru a iniţia cererea de actualizare dinamică pentru <*zone-a*> folosind cheia <*key_id-x*>.
<*key_id-x*>._KID		Fişier care conţine o instrucţiune cheie pentru key_id numit <*key_id-x*>
<*key_id-y*>._DUK. <*zone-a*>		Cheia de actualizare dinamică necesară pentru a iniţia cererea de actualizare dinamică pentru <*zone-a*> folosind cheia <*key_id-y*>.
<*key_id-y*>._DUK. <*zone-b*>		Cheia de actualizare dinamică necesară pentru a iniţia cererea de actualizare dinamică pentru <*zone-b*> folosind cheia <*key_id-y*>.
<*key_id-y*>._KID		Fişier care conţine o instrucţiune cheie pentru key_id numită <*key_id-y*>
rndc-confgen.random.*nnnnnn*		Fişiere de entropie pentru diverse comenzi care le necesită. Componenta *nnnnn* este un număr de job al jobului care a creat fişierul. Acestea sunt lăsate în urmă dacă comanda anulează pentru un motiv şi nu curăţă.

Concepte înrudite

"Determinarea autorizărilor DNS" la pagina 24
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 DNS" la pagina 32
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 27
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 subiect explică modul în care administratorii cu experienţă pot utiliza caracteristicile avansate DNS (Domain Name System) pentru gestionarea mai facilă a serverului DNS.

DNS în System i Navigator furnizează o interfaţă cu caracteristici avansate pentru configurarea şi gestionarea serverului DNS. Următoarele taskuri sunt furnizate ca scurtături pentru administratorii care sunt familiarizaţi cu interfaţa grafică i5/OS. Acestea furnizează metode rapide pentru modificarea stării şi atributelor serverului pentru mai multe instanţe simultan.

Operaţii înrudite

"Modificarea setărilor de depanare DNS" la pagina 39
Funcţia de depanare DNS (Domain Name System) poate oferi informaţii care vă pot ajuta să determinaţi şi să corectaţi problemele serverului DNS.

Pornirea sau oprirea serverelor DNS

Dacă DNS în interfaţa System i Navigator nu vă permite să porniţi sau să opriţi mai multe instanţe de server simultan, puteţi folosi interfaţa bazată pe caractere pentru a modifica aceste setări pentru mai multe instanţe simultan.

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

Este util să modificaţi nivelul de depanare pentru administratorii care au zone mari şi nu vreţi să fie colectate cantităţi mari de date de depanare când serverul este pornit prima dată şi încărcarea tuturor datelor de zonă.

DNS în interfaţa System i Navigator nu vă permite să modificaţi nivelul de depanare cât timp serverul rulează. Totuşi, puteţi folosi interfaţa bazată pe caractere pentru a modifica nivelul de depanare în timp ce serverul rulează. Pentru a modifica nivelul de depanare folosind interfaţa bazată pe caractere, urmaţi aceşti paşi, înlocuind *nnnnn* în comandă cu numele instanţei de server:

1. La linia de comandă, tastaţi ADDLIBLE QDNS şi apăsaţi Enter.
2. Modificaţi nivelul de depanare:
   - Pentru a porni depanarea sau pentru a incrementa nivelul de depanare, tastaţi RNDC RNDCCMD('trace') şi apăsaţi Enter.
   - Pentru a opri depanarea, tastaţi RNDC RNDCCMD('notrace') şi apăsaţi.

Depanarea DNS

Setările de înregistrare în istoric şi de depanare ale DNS vă pot ajuta să rezolva probleme cu serverul 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 rulaţi servere bazate pe BIND 9, va exista un job separat pentru fiecare instanţă de server pe care o rulaţi. Numele jobului este format din cinci 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.

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 9 oferă mai multe opţiuni de înregistrare în istoric. Puteţi specifica tipurile de mesaje 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 potrivite, dar dacă vreţi să le modificaţi, vă sugerăm să consultaţi alte surse ale documentaţiei BIND 9 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 implicite ale fişierului sunt i5os_debug şi i5os_QPRINT. Implicit, mesajele de depanare sunt înregistrate în istoric pe canalul i5os_debug, care este fişierul named.run, dar puteţi specifica să trimiteţi alte categorii de mesaje de asemenea în acest fişier. Categoriile de mesaje înregistrate în istoric în i5os_QPRINT sunt trimise într-un fişier spooled QPRINT pentru profilul utilizator QTCP. Puteţi crea propriile dumneavoastră canale fişiere pe lângă canalele implicit furnizate.
- **Canalele Syslog**

  Mesajele înregistrate în istoric în acest canal sunt trimise în istoricul de joburi al serverului. Canalul de înregistrare în istoric implicit este i5os_joblog. Mesajele de înregistrare în istoric rutate pe acest canal sunt trimise la istoricul de job al instanţei server DNS.
- **Canalele Null**

  Toate mesajele înregistrate în istoric pe canalul nul sunt ignorate. Canalul nul implicit este i5os_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 să specificaţi ce categorii de mesaje ar trebui înregistrate către fiecare canal. Categoriile sunt următoarele:

client Procesarea cererilor client.

config Parsare şi procesare fişier de configurare.

database
Mesajele care se leagă de bazele de date care sunt folosite intern de serverul DNS pentru a stoca date de zonă şi cache.

default Definiţiile opţiunilor de înregistrare în istoric pentru acele categorii unde nu a fost definită nicio configuraţie specifică.

delegation-only
Doar delegaţie. Înregistrează doar interogările care au fost forţate la NXDOMAIN ca rezultat al unei zone delegation-only sau o delegation-only într-o declaraţie de zonă stub sau o indicaţie.

dispatch
Dispecerizarea pachetelor de intrare la modulele de server unde vor fi procesate.

dnssec Procesare protocol Extensii de securitate DNS (DNSSEC) şi Semnătură tranzacţie (TSIG).

general
Categoria catch-all care este folosită pentru acele lucruri care nu sunt clasificate în nicio altă categorie.

lame-servers
Servere slabe care sunt configuraţii greşite în servere la distanţă, descoperite de BIND 9 când încearcă să interogheze acele servere în timpul rezolvării.

network
Operaţii reţea.

notify Protocolul NOTIFY.

resolver
Rezolvare DNS, cum ar fi căutări recursive, care este realizată în numele clienţilor de către un server de nume caching.

security
Aprobarea sau refuzarea de cereri.

xfer-in Transferurile de zonă pe care le primeşte serverul.

xfer-out
Transferurile de zonă pe care le trimite serverul.

unmatched
Mesajele pentru care named nu a putut determina clasa sau pentru care nu există nicio vizualizare care se potriveşte. Un rezumat de o linie este de asemenea înregistrat în istoric în categoria client. Această categorie este cel mai bine trimisă într-un fişier sau la stderr. Implicit, este trimisă la canalul nul.

update Actualizări dinamice.

update-security
Aprobarea sau refuzarea de cereri de actualizare. Interogările specifică unde ar trebui înregistrate în istoric interogările. La pornire, specificarea categoriilor interogărilor permite înregistrarea în istoric a interogărilor dacă nu este specificată opţiunea querylog.

Intrarea din istoricul de interogări raportează adresa IP a client-ului şi numărul portului, numele interogării, clasa şi tipul. Raportează de asemenea dacă steguleţul Recursivitate dorită a fost setat (+ dacă este setat, - dacă nu este setat), EDNS a fost folosit (E) sau dacă interogarea a fost semnată (S).

Fişierele de istoric pot deveni mari şi pot fi şterse regulat. Tot conţinutul din fişierul de istoric DNS sunt curăţate 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 în istoric

Pentru a accesa opţiunile de înregistrare, parcurgeţi următorii paşi:

1. În System i Navigator, expandaţi ***sistemul dumneavoastră*** → **Reţea** → **Servere** → **DNS**.
2. În panoul din dreapta, faceţi clic dreapta pe ***Server DNS*** şi selectaţi **Configurare**.
3. În fereastra de configurare DNS, faceţi clic dreapta pe **Server DNS** şi selectaţi **Proprietăţi**.
4. În fereastra Proprietăţi server, selectaţi fişa **Canale** pentru a crea noi canale de fişier 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** ca să specificaţi categoriile de mesaje care să fie înregistrate în istoricul fiecărui canal.

Sugestie de depanare pentru nivelul de gravitate

Nivelul implicit de gravitate i5os_joblog este setat la Eroare. Această setare este utilizată pentru a reduce volumul de mesaje de informare şi avertizare, care altfel ar putea să scadă performanţa. Dacă aveţi probleme şi istoricul de job nu indică sursa problemei, poate fi necesară modificarea nivelului de gravitate. Urmaţi procedura de mai sus pentru a accesa pagina Canale şi modificaţi nivelul de gravitate pentru canalul i5os_joblog la Avertisment, Notificare sau Info, astfel încât să puteţi vizualiza mai multe date de înregistrare în istoric. După ce aţi rezolvat problema, resetaţi nivelul de gravitate la Eroare, pentru a reduce numărul de mesaje din istoricul de job.

Modificarea setărilor de depanare DNS

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. Înregistrarea în istoric furnizează în general o metodă mai uşoară de a găsi probleme, dar în unele cazuri depanare 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. Valori de 1 sau mai mari scriu informaţii de depanare în fişierul named.run din calea de directoare i5/OS: /QIBM/UserData/OS400/DNS/*<instanţă server>*, unde *<instanţă server>* este numele instanţei serverului DNS. Fişierul named.run continuă să crească cât timp nivelul de depanare este setat la 1 sau mai mare şi serverul DNS continuă să ruleze. Puteţi de asemenea folosi pagina Proprietăţi server - Canale pentru a specifica preferinţe pentru dimensiunea maximă şi numărul de versiuni al fişierului named.run.

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

1. În System i Navigator, expandaţi ***sistemul dumneavoastră*** → **Reţea** → **Servere** → **DNS**.
2. În panoul din dreapta, faceţi clic dreapta pe ***server 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 serverul.

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 36
Acest subiect explică modul în care administratorii cu experienţă pot utiliza caracteristicile avansate DNS (Domain Name System) pentru gestionarea mai facilă a serverului DNS.

Informaţii înrudite pentru Domain Name System

Publicaţiile IBM Redbooks, siturile web şi alte colecţii de subiecte din centrul de informare conţin informaţii înrudite cu cele din colecţia de subiecte DNS. Puteţi vizualiza sau tipări oricare dintre fişierele PDF.

IBM Redbooks

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

Această publicaţie Redbooks descrie suportul de server DNS şi server DHCP care este inclus în i5/OS. Vă poate ajuta, prin exemple, să instalaţi, să ajustaţi, să configuraţi şi să depanaţi suportul DNS şi DHCP.

Situri Web

- *DNS and BIND*, ediţia a cincea. Paul Albitz şi Cricket Liu. Publicată de O’Reilly and Associates,Inc. Sebastopol, California, 2006. Număr ISBN: 0-59610-057-4.
- Manualul de referinţă al administratorilor BIND (în versiune PDF) de pe situl webInternet System Consortium (ISC) .
- Situl web Internet Software Consortium conţine ştiri, legături şi alte resurse pentru BIND.
- Situl InterNIC păstrează un director cu toţi registratorii de nume de domenii care sunt autorizaţi de ICANN.
- Directorul de resurse DNS furnizează material de referinţă DNS şi legături la multe alte resurse DNS, inclusiv grupuri de discuţii. Furnizează de asemenea o listare a RFC-urilor legate de DNS .

Referinţe înrudite

“Fişierul PDF pentru DNS” la pagina 2
Puteţi vizualiza şi tipări un fişier PDF cu aceste informaţii.

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 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 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. Prin furnizarea acestui document nu vi se acordă nicio licenţă pentru 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 IBM de proprietate intelectuală din ţara dumneavoastră sau trimiteţi întrebări 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. Se efectuează modificări periodice la informaţiile incluse aici; aceste modificări vor fi încorporate în noi ediţii ale publicaţiei. IBM poate aduce îmbunătăţiri şi/sau modificări produsului (produselor) despre care se discută 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 folosi sau distribui 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 obţină 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, trebuie să contacteze:

IBM Corporation
Software Interoperability Coordinator, Department YBWA

3605 Highway 52 N
Rochester, MN 55901
U.S.A.

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

Programul licenţiat prezentat în această publicaţie şi toate materialele licenţiate disponibile pentru el sunt furnizate de IBM conform termenilor din IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code sau 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. Este posibil ca unele măsurători să fi fost realizate pe sisteme de nivel evoluat şi nu există nici o garanţie că aceste măsurători vor fi identice pe sisteme general disponibile. Mai mult, unele măsurători pot fi estimări obţinute 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. Întrebările 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 o notificare prealabilă, reprezentând 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 aplicaţii 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). Părţi 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 despre interfaţa de programare

Această publicaţie, DNS, documentează interfeţele de programare concepute pentru a permite beneficiarului să scrie programe în vederea obţinerii 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:

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

Adobe, logo-ul Adobe, PostScript şi logo-ul PostScript sunt mărci comerciale înregistrate sau mărci comerciale deţinute de Adobe Systems Incorporated în Statele Unite şi/sau alte ţări.

Alte nume de companii, de produse sau de 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 obiecte derivate din aceste publicaţii sau dintr-o porţiune a lor fără consimţământul explicit al IBM.

Utilizare comercială: Puteţi reproduce, distribui şi afişa aceste publicaţii doar în cadrul întreprinderii dumneavoastră, cu condiţia ca toate 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 al IBM.

Cu excepţia a ceea ce este acordat explicit prin această permisiune, nu sunt acordate alte permisiuni, licenţe sau drepturi, explicit sau implicit, pentru Publicaţii sau alte informaţii, date, software sau altă proprietate intelectuală conţină în acestea.

IBM îşi rezervă dreptul de a retrage permisiunile acordate aici oricând consideră că folosirea publicaţiilor este în detrimentul intereselor sale sau când personalul IBM constată că 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.