Systémy IBM - iSeries

Siete
Domain Name System

Verzia 5, vydanie 4

Systémy IBM - iSeries

Siete
Domain Name System

Verzia 5, vydanie 4

Poznámka

Pred použitím týchto informácií a nimi podporovaného produktu si prečítajte informácie v časti “Poznámky”, na strane 37.

Šieste vydanie (február 2006)

Toto vydanie sa týka verzie 5, vydania 4, modifikácie 0 produktu IBM i5/OS (číslo produktu 5722-SS1) a všetkých nasledujúcich vydaní a modifikácií, ak nie je v nových vydaniach určené inak. Táto verzia sa nespúšťa na modeloch RISC (reduced instruction set computer) ani na modeloch CISC.

Obsah

Systém DNS

DNS je systém distribuovaných databáz, určený na manažovanie názvov hostiteľov a priradených adries IP.

Používanie systému DNS znamená, že ľudia môžu používať jednoduché názvy, ako napríklad www.jkltoys.com, na lokalizovanie hostiteľa a nemusia používať adresy IP (xxx.xxx.xxx.xxx). Jeden server môže byť zodpovedný len za názvy hostiteľov a adresy IP pre malú podmnožinu jednej zóny, ale servery DNS môžu spolupracovať pri mapovaní všetkých názvov v doméne a ich adries IP. Spolupracujúce servery DNS umožňujú počítačom komunikovať cez internet.

V prípade systému IBM OS/400 verzia 5, vydanie 1 (V5R1), sú služby DNS založené na implementácii DNS známej ako BIND (Berkeley Internet Name Domain) verzie 8, ktorá predstavuje priemyselný štandard. Predošlé systémy IBM OS/400 obsahovali služby DNS založené na verzii BIND 4.9.3. Ak chcete používať nový server DNS založený na verzii BIND 8, musíte nainštalovať prostredie PASE (Portable Application Solutions Environment), ktorému odpovedá voľba i5/OS 33, vo vašom serveri IBM eServer iSeries. Ak prostredie PASE nie je nainštalované, môžete spustiť ten istý server DNS založený na verzii BIND 4.9.3, ktorý bol dostupný v predošlých vydaniach. Avšak, migrácia na verziu BIND 8 poskytuje vylepšené funkcie a takisto zvýšenú bezpečnosť pre váš server DNS.

Poznámka: Táto téma opisuje nové vlastnosti založené na verzii BIND 8. Ak nepoužívate prostredie PASE na spustenie systému DNS založeného na verzii BIND 8, pozrite si tému Informačného centra Systém DNS pre verziu 4, vydanie 5, kde nájdete informácie pre systém DNS založený na verzii BIND 4.9.3.

Vytlačiteľné PDF

Tento pohľad môžete použiť na zobrazenie a vytlačenie dokumentu PDF obsahujúceho tieto informácie.

Ak chcete zobraziť alebo prevziať verziu PDF tohto dokumentu, vyberte Domain Name System (veľkosť 625 KB).

Uloženie súborov PDF

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

1. Pravým tlačidlom myši kliknite na dokument PDF vo vašom prehliadači (pravým tlačidlom myši kliknite na odkaz vyššie).
2. Kliknite na voľbu, ktorá ukladá súbor PDF lokálne.
3. Prejdite do adresára, kde chcete súbor PDF uložiť.
4. Kliknite na **Save**.

Prevzatie programu Adobe Reader

Na zobrazenie alebo tlač súborov PDF potrebujete program Adobe Reader. Kópiu si môžete prevziať z Webovej lokality Adobe (www.adobe.com/products/acrobat/readstep.html)  .

Koncepty systému DNS

Táto téma vysvetľuje, čo je systém DNS a ako pracuje. Takisto ukazuje rozličné typy zón, ktoré môžu byť definované v serveri DNS.

DNS je systém distribuovaných databáz, určený na manažovanie názvov hostiteľov a priradených adries IP. Používanie systému DNS znamená, že ľudia môžu používať jednoduché názvy, ako napríklad www.jkltoys.com, na lokalizovanie hostiteľa a nemusia používať adresy IP (xxx.xxx.xxx.xxx). Jeden server môže byť zodpovedný len za názvy hostiteľov a

adresy IP pre malú podmnožinu jednej zóny, ale servery DNS môžu spolupracovať pri mapovaní všetkých názvov v doméne a ich adries IP. Spolupracujúce servery DNS umožňujú počítačom komunikovať cez internet.

Údaje DNS sú rozdelené do hierarchie domén. Servery zodpovedajú len za poznanie malej časti údajov, ako je napríklad jedna poddoména. Časť domény, za ktorú je server priamo zodpovedný sa nazýva zóna. Server DNS, ktorý má úplné informácie o hostiteľovi a údaje pre zónu, je autoritatívny pre zónu. Autoritatívny server môže odpovedať na dotazy o hostiteľoch vo vlastnej zóne pomocou vlastných zdrojových záznamov. Proces dotazovania závisí na množstve faktorov. Téma Pochopenie dotazov DNS vysvetľuje cesty, ktoré klient používa na preloženie dotazu.

Pochopenie zón

Táto téma vysvetľuje zóny DNS a typy zón.

Údaje systému DNS sú rozdelené do lepšie manažovateľných množín nazývaných *zóny*. Zóny obsahujú informácie o názve a IP adrese jednej alebo viacerých častí domény DNS. Server obsahujúci všetky informácie pre zónu je autoritatívnym serverom pre danú doménu. V niektorých prípadoch je výhodné delegovať oprávnenie na odpovedanie dotazov DNS pre konkrétnu doménu inému serveru DNS. V takom prípade možno nakonfigurovať server DNS pre túto doménu tak, aby odkazoval dotazy poddomény na príslušný server.

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

Typy zón DNS

Systém DNS servera iSeries môžete použiť na definovanie niekoľkých typov zón, ktoré vám pomôžu manažovať údaje DNS:

Primárna zóna
Primárna zóna načíta zónové údaje priamo zo súboru na hostiteľovi. Môže obsahovať podzónu alebo dcérsku zónu. Môže obsahovať aj zdrojové záznamy, ako je hostiteľ, alias (CNAME), adresa (A), alebo záznamy ukazovateľa spätného mapovania (PTR).

Poznámka: Primárne zóny sú niekedy uvedené ako *hlavné zóny* v inej dokumentácii systému BIND.

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

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

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

Hostiteľ
Objekt hostiteľa mapuje záznamy A a PTR do hostiteľa. Dodatočné zdrojové záznamy môžu byť priradené k hostiteľovi.

Sekundárna zóna
Sekundárna zóna načíta zónové údaje z primárneho servera zóny alebo z iného sekundárneho servera. Udržiava úplnú kópiu zóny, pre ktorú je sekundárna.

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

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

Súvisiace koncepty

"Pochopenie dotazov systému DNS"
Táto téma vysvetľuje spôsob prekladu dotazov DNS.

"Konfigurovať zóny v názvovom serveri" na strane 24
Po konfigurácii inštancie servera DNS potrebujete nakonfigurovať zóny pre názvový server.

Súvisiaci odkaz

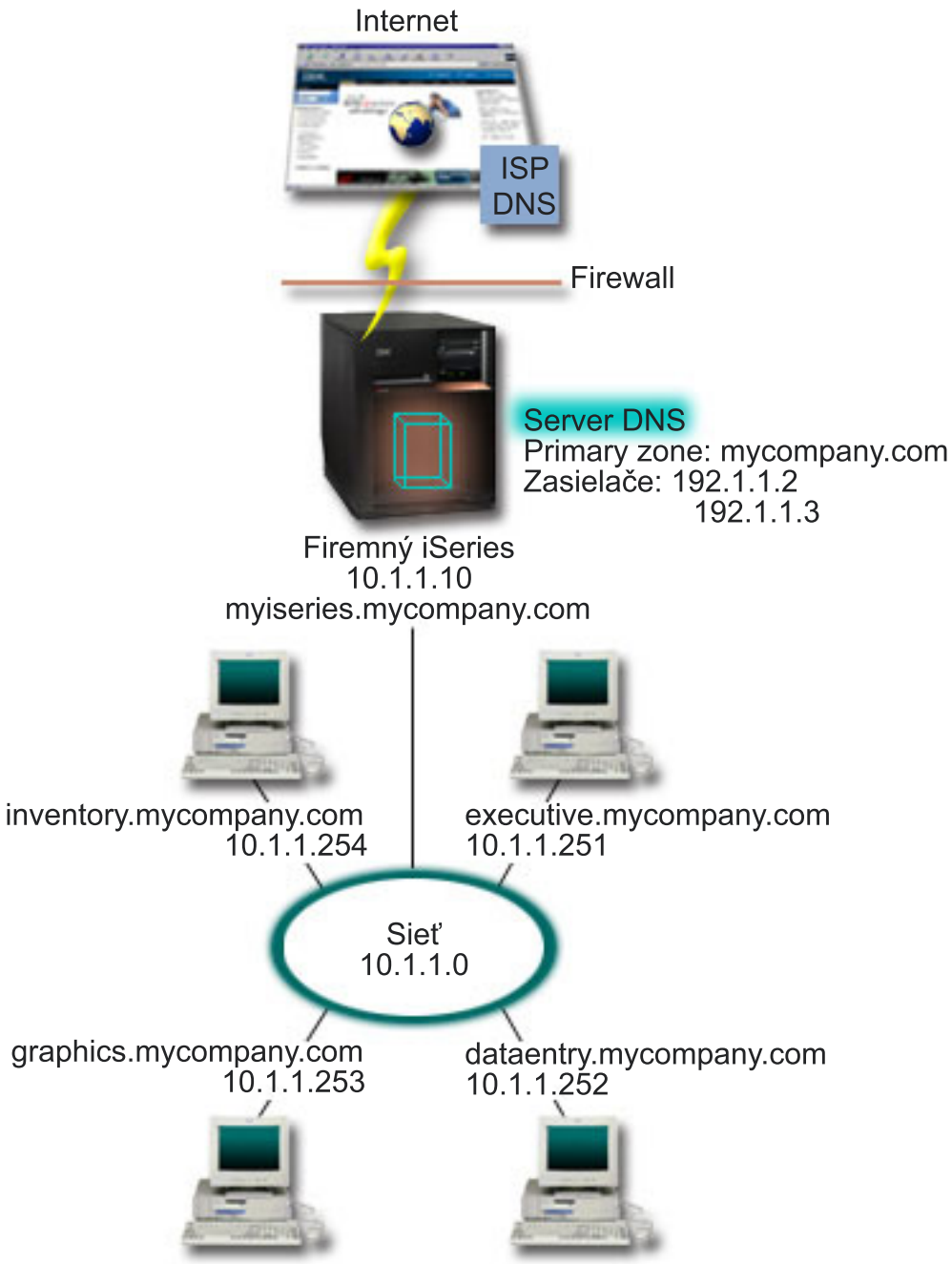
"Príklad: Jeden server DNS pre intranet" na strane 12
Tento príklad znázorňuje jednoduchú podsieť so serverom DNS pre interné použitie.

"Zdrojové záznamy systému DNS" na strane 8
Táto téma vysvetľuje spôsob použitia zdrojových záznamov systémom DNS. Zdrojové záznamy sa používajú na ukladanie údajov o názvoch domén a IP adries. Táto téma obsahuje zoznam zdrojových záznamov pre operačný systém OS/400 verzia 5, vydanie 1.

Pochopenie dotazov systému DNS

Táto téma vysvetľuje spôsob prekladu dotazov DNS.

Klienti používajú servery DNS s cieľom nájsť pre ne informácie. Požiadavka môže byť prijatá priamo od klienta alebo od aplikácie spustenej v klientovi. Klient odošle dotazovaciu správu obsahujúcu plne kvalifikovaný názov domény (FQDN), typ dotazu, ako napríklad konkrétny zdrojový záznam, ktorý klient vyžaduje a triedu názvu domény. Trieda názvu domény je väčšinou Internet (IN). Nasledujúci obrázok znázorňuje vzorovú sieť z príkladu Jeden server DNS s prístupom do internetu.



Obrázok 1. Jeden server DNS s prístupom do internetu

Predpokladajte, že hostiteľ *dataentry* dotazuje server DNS adresou graphics.mycompany.com. Server DNS použije vlastné zónové údaje a odpovie adresou IP 10.1.1.253.

Predpokladajte, že hostiteľ *dataentry* požiada o adresu IP pre názov www.jkl.com. Tento hostiteľ sa nenachádza v zónových údajoch servera DNS. Teraz existujú dve cesty, po ktorých možno ísť, rekurzia alebo opakovanie. Ak je server DNS nastavený na použitie rekurzie, môže dotazovať alebo kontaktovať iné servery DNS v mene požadujúceho klienta s cieľom úplne rozlíšiť názov a potom zaslať odpoveď späť klientovi. Ak server DNS odošle dotaz inému serveru DNS, odpoveď sa uloží do vyrovnávacej pamäte a použije sa pri nasledujúcom dotaze obsahujúcom rovnaký názov. Klient sa môže pokúsiť vo svojom mene kontaktovať ostatné servery DNS s cieľom rozlíšiť názov. V tomto procese, ktorý sa nazýva *iterácia*, klient použije ďalšie samostatné dotazy podľa odpovedí od serverov.

Súvisiaci odkaz

“Pochopenie zón” na strane 2
Táto téma vysvetľuje zóny DNS a typy zón.

“Príklad: Jeden server DNS s prístupom do internetu” na strane 14
Tento príklad znázorňuje jednoduchú podsieť so serverom DNS pripojeným priamo do internetu.

Nastavenie domény systému DNS

Táto téma poskytuje prehľad procesu registrácie domény a obsahuje odkazy na ďalšie referenčné lokality, kde sa môžete dozvedieť viac o nastavení vášho vlastného priestoru domény.

Systém DNS vám umožňuje prideliť mená a adresy v intranete alebo v internej sieti. Takisto vám umožňuje prideliť mená a adresy zvyšku sveta pomocou internetu. Ak chcete nastaviť domény na internete, budete musieť zaregistrovať názov domény.

Ak nastavujete intranet, pre interné použitie nemusíte zaregistrovať názov domény. Whether to register an intranet name depends on whether you want to ensure that no one else can ever use the name on the Internet, independent of your internal use. Registrácia názvu, ktorý budete používať interne, zabezpečí, že nikdy nebudete mať problém, ak budete chcieť neskôr použiť názov domény externe.

Registráciu domény môžete vykonať kontaktovaním autorizovaného registrátora názvov domén alebo prostredníctvom poskytovateľa internetových služieb (ISP). Niektorí ISP ponúkajú službu podávania žiadostí o registráciu názvu domény vo vašom mene. The Internet Network Information Center (InterNIC) maintains a directory of all domain name registrars that are authorized by the Internet Corporation for Assigned Names and Numbers (ICANN).

Súvisiaci odkaz

“Príklad: Jeden server DNS s prístupom do internetu” na strane 14
Tento príklad znázorňuje jednoduchú podsieť so serverom DNS pripojeným priamo do internetu.

Súvisiace informácie

Internet Network Information Center (InterNIC)

Dynamické aktualizácie

Systém DNS operačného systému OS/400 verzia 5, vydanie 1 na báze BIND 8 podporuje dynamické aktualizácie. Toto umožňuje vonkajším zdrojom, ako je protokol DHCP, odoslať aktualizácie serveru DNS.

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

V minulosti boli všetky údaje DNS uložené v statických databázach. Všetky zdrojové záznamy systému DNS by mali byť vytvorené a udržiavané administrátorom. Servery DNS spúšťajúce BIND 8 môžu byť teraz nakonfigurované na prijímanie požiadaviek z ostatných zdrojov s cieľom dynamicky aktualizovať zónové údaje.

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

V mene klienta môžete nakonfigurovať DHCP na aktualizáciu záznamov mapovania adries (A), záznamov ukazovateľa reverzného vyhľadávania (PTR) alebo oboch. Záznam A mapuje hostiteľský názov počítača do jeho IP adresy. Záznam PTR mapuje IP adresu počítača do jeho hostiteľského názvu. Keď sa mení adresa klienta, DHCP môže automaticky

zaslať aktualizáciu serveru DNS, aby ostatní hostitelia v sieti mohli tohto klienta lokalizovať cez dotazy DNS na jeho novej IP adrese. For each record that is updated dynamically, an associated Text (TXT) record is written to identify that the record was written by DHCP.

Poznámka: Ak nastavíte protokol DHCP len na aktualizovanie záznamov PTR, musíte nakonfigurovať systém DNS na povolenie aktualizácií od klientov tak, že každý klient môže aktualizovať jeho záznam A. Nie všetci klienti DHCP podporujú vytváranie svojich vlastných požiadaviek na aktualizáciu záznamu A. Skôr než si zvolíte túto metódu, pozrite si dokumentáciu pre vašu klientsku platformu.

Dynamické zóny sú zabezpečené vytvorením zoznamu autorizovaných zdrojov, ktoré majú povolené zasielať aktualizácie. Autorizované zdroje môžete definovať použitím individuálnych adries IP, celých podsietí, paketov, ktoré boli podpísané použitím zdieľaného tajného kľúča (nazývaným *Transaction Signature* alebo TSIG) alebo ľubovoľnou kombináciou týchto metód. Pred aktualizáciou zdrojových záznamov DNS overuje, či prichádzajúce pakety požiadaviek pochádzajú z autorizovaného zdroja.

Dynamické aktualizácie môžu byť vykonané medzi DNS a DHCP v jednom serveri iSeries, medzi rozličnými servermi iSeries, alebo medzi serverom iSeries a ostatnými servermi, ktoré podporujú dynamické aktualizácie.

Poznámka: Aplikačné programové rozhranie (API) dynamických aktualizácií QTOBUPT sa vyžaduje v serveroch, ktoré odosielajú dynamické aktualizácie serveru DNS. Nainštaluje sa automaticky pri inštalácii voľby 31 systému i5/OS, DNS.

Súvisiace koncepty

Protokol DHCP (Dynamic Host Configuration Protocol)

Súvisiace úlohy

“Konfigurácia systému DNS na príjem dynamických aktualizácií” na strane 25
Servery DNS na báze BIND 8 sa dajú nakonfigurovať na akceptovanie požiadaviek o dynamickú aktualizáciu zónových údajov od iných zdrojov. Táto téma poskytuje pokyny na konfiguráciu voľby na povolenie aktualizácie, aby mohol DNS prijímať dynamické zmeny.

Konfigurácia DHCP na odosielanie dynamických aktualizácií

Súvisiaci odkaz

“Príklad: DNS (Domain Name System) a DHCP (Dynamic Host Configuration Protocol) v jednom serveri iSeries” na strane 16
Tento príklad znázorňuje systémy DNS aj DHCP v jednom serveri.

“Zdrojové záznamy systému DNS” na strane 8
Táto téma vysvetľuje spôsob použitia zdrojových záznamov systémom DNS. Zdrojové záznamy sa používajú na ukladanie údajov o názvoch domén a IP adries. Táto téma obsahuje zoznam zdrojových záznamov pre operačný systém OS/400 verzia 5, vydanie 1.

QTOBUPT

“Vlastnosti BIND 8”
Popri dynamických aktualizáciách, systém BIND 8 ponúka niekoľko vlastností na zvýšenie výkonu vášho servera DNS.

Vlastnosti BIND 8

Popri dynamických aktualizáciách, systém BIND 8 ponúka niekoľko vlastností na zvýšenie výkonu vášho servera DNS.

Systém DNS po zmene návrhu používa BIND 8 pre OS/400 verzia 5, vydanie 1. Ak prostredie PASE nie je nainštalované, môžete pokračovať v konfigurácii a používaní predošlého vydania servera DNS v systéme OS/400 verzie BIND 4.9.3. Téma Požiadavky systému DNS vysvetľuje, čo potrebujete na spustenie systému DNS na báze BIND 8 vo vašom serveri iSeries. Použitie nového DNS vám umožní využívať nasledujúce vlastnosti:

Viaceré servery DNS spustené v jednom serveri iSeries

V predošlých vydaniach ste mohli nakonfigurovať iba jeden server DNS. Teraz môžete nakonfigurovať viacero serverov alebo inštancií DNS. To vám umožní nastaviť logické rozdelenie medzi servermi. Keď vytvoríte viaceré inštancie, musíte explicitne definovať pre každú z nich IP adresy rozhrania, na ktorom budú počúvať. Dve inštancie DNS nemôžu počúvať na tom istom rozhraní.

Jedným z praktických využití viacerých serverov je rozdelenie DNS, kde jeden server je autoritatívny pre internú sieť a druhý sa používa na externé dotazy.

Podmienečné posielanie ďalej

Podmienečné posielanie ďalej vám umožní nakonfigurovať váš server DNS na jemné ladenie vašich preferencií odosielania. Server môžete nastaviť na odosielanie všetkých dotazov, na ktoré nepozná odpoveď. You can set forwarding at a global level, but add exceptions to domains for which you want to force normal iterative resolution. Alebo môžete nastaviť normálne iteratívne rozlíšenie na globálnej úrovni a vynútiť postupovanie v rámci určitých domén.

Bezpečné dynamické aktualizácie

Protokol DHCP a iné autorizované zdroje môžu odoslať dynamické aktualizácie zdrojových záznamov pomocou TSIG (Transaction Signatures) alebo autorizáciou zdrojovej adresy IP, alebo obidvoma spôsobmi. Znižuje to potrebu manuálnych aktualizácií zónových údajov a zároveň sa tým zabezpečí, že na aktualizáciu sa používajú len autorizované zdroje.

NOTIFY

Keď sa zapne NOTIFY, funkcia DNS NOTIFY sa aktivuje vždy, keď sa na primárnom serveri aktualizujú zónové údaje. Primárny server odošle správu oznamujúcu zmenu údajov všetkým sekundárnym serverom. Sekundárne servery potom môžu odpovedať požiadavkou o zónový prenos pre aktualizované zónové údaje. Udržiavanie aktuálnosti zónových údajov pomáha zlepšiť podporu sekundárneho servera.

Zónové prenosy (IXFR a AXFR)

Vždy keď v minulosti sekundárne servery potrebovali opätovne zaviesť zónové údaje, museli zaviesť celú sadu údajov do prenosu celej zóny (AXFR). BIND 8 podporuje novú metódu zónového prenosu: prírastkový zónový prenos (IXFR). IXFR predstavuje spôsob, akým môžu ostatné servery prenášať len zmenené údaje a nie celú zónu.

Ak je nasledujúca vlastnosť na primárnom serveri zapnutá, zmenám údajov sa priradí návestie, ktoré určuje, že nastala zmena. Keď sekundárny server požiada o aktualizáciu zóny v IXFR, primárny server zašle len nové údaje. IXFR je obzvlášť užitočný, keď je zóna dynamicky aktualizovaná. Tento transfer znižuje záťaž premávky odosielaním menších množstiev údajov.

Poznámka: Primárny aj sekundárny server musia mať zapnuté IXFR, aby mohli používať túto vlastnosť.

Súvisiace koncepty

“Požiadavky systému DNS” na strane 22
Táto téma opisuje softvérové požiadavky na spustenie systému DNS vo vašom serveri iSeries.

“Dynamické aktualizácie” na strane 5
Systém DNS operačného systému OS/400 verzia 5, vydanie 1 na báze BIND 8 podporuje dynamické aktualizácie. Toto umožňuje vonkajším zdrojom, ako je protokol DHCP, odoslať aktualizácie serveru DNS.

Súvisiaci odkaz

“Príklad: Rozdelenie systému DNS cez firewall” na strane 18
Tento príklad znázorňuje systém DNS pracujúci nad firewallom, ktorý chráni interné údaje proti prístupu z internetu a zároveň umožňuje interným užívateľom pristupovať k údajom v internete.

“Plánovanie mier bezpečnosti” na strane 21
Systém DNS poskytuje bezpečnostné voľby, ktoré umožňujú obmedziť vonkajší prístup k vášmu serveru.

Zdrojové záznamy systému DNS

Táto téma vysvetľuje spôsob použitia zdrojových záznamov systémom DNS. Zdrojové záznamy sa používajú na ukladanie údajov o názvoch domén a IP adries. Táto téma obsahuje zoznam zdrojových záznamov pre operačný systém OS/400 verzia 5, vydanie 1.

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

Tabuľka 1. Vyhľadávacia tabuľka zdrojových záznamov

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

Tabuľka 1. Vyhľadávacia tabuľka zdrojových záznamov (pokračovanie)

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

Tabuľka 1. Vyhľadávacia tabuľka zdrojových záznamov (pokračovanie)

Zdrojový záznam	Skratka	Opis
Záznamy Network Service Access Protocol	NSAP	Záznam NSAP uvádza adresu prostriedku NSAP. Záznamy NSAP sa používajú na mapovanie názvov domény do adries NSAP. Tento typ záznamu je definovaný v RFC 1706.
Záznamy Public Key	KEY	Záznam KEY uvádza verejný kľúč priradený k názvu DNS. Kľúč môže patriť zóne, užívateľovi alebo hostiteľovi. Tento typ záznamu je definovaný v RFC 1065.
Záznamy Responsible Person	RP	Záznam RP uvádza internetovú poštovú adresu a opis osoby zodpovednej za túto zónu alebo hostiteľa. Tento typ záznamu je definovaný v RFC 1183.
Záznamy Reverse-lookup Pointer	PTR	Záznam PTR uvádza názov domény hostiteľa, pre ktorého chcete definovaný záznam PTR. Záznamy PTR umožňujú vyhľadanie názvu hostiteľa s danou IP adresou. Tento typ záznamu je definovaný v RFC 1035.
Záznamy Route Through	RT	Záznam RT uvádza názov hostiteľskej domény, ktorá môže konať ako zasielateľ IP paketov pre tohto hostiteľa. Tento typ záznamu je definovaný v RFC 1183.
Záznamy Start of Authority	SOA	Záznam SOA uvádza, že tento server je pre danú zónu autoritatívny. Autoritatívny server je najlepším zdrojom pre údaje v rámci zóny. Záznam SOA obsahuje všeobecné informácie o zóne a predzavedených pravidlách pre sekundárne servery. Na jednu zónu môže existovať len jeden záznam SOA. Tento typ záznamu je definovaný v RFC 1035.
Záznamy Text	TXT	Záznam TXT uvádza viaceré textové reťazce, každý s dĺžkou až 255 znakov, ktoré majú byť priradené k názvu domény. Záznamy TXT sa dajú použiť spoločne so záznamami RP (zodpovedná osoba) za účelom poskytnutia informácií o zodpovednosti za zónu. Tento typ záznamu je definovaný v RFC 1035. Záznamy TXT používa server DHCP iSeries na dynamické aktualizácie. Server DHCP napíše priradený záznam TXT pre každú aktualizáciu záznamu A a PTR vykonanú serverom DHCP. Záznamy DHCP majú predponu servera DHCP AS400.
Záznamy Well-Known Services	WKS	Záznam WKS uvádza dobre známe služby podporované objektom. Záznamy WKS najčastejšie uvádzajú, či sa pre túto adresu podporujú protokoly tcp alebo udp alebo oba. Tento typ záznamu je definovaný v RFC 1035.

Tabuľka 1. Vyhľadávacia tabuľka zdrojových záznamov (pokračovanie)

Zdrojový záznam	Skratka	Opis
Záznamy X.400 Address Mapping	PX	Záznamy PX sú ukazovateľom na informácie o mapovaní X.400/RFC 822. Tento typ záznamu je definovaný v RFC 1664.
Záznamy X25 Address Mapping	X25	Záznam X25 uvádza adresu prostriedku X25. Tento záznam mapuje hostiteľský názov do adresy PSDN. Používajú sa len v sieťach X25. Tento typ záznamu je definovaný v RFC 1183.

Súvisiace koncepty

"Dynamické aktualizácie" na strane 5
Systém DNS operačného systému OS/400 verzia 5, vydanie 1 na báze BIND 8 podporuje dynamické aktualizácie. Toto umožňuje vonkajším zdrojom, ako je protokol DHCP, odoslať aktualizácie serveru DNS.

"Poštové záznamy a záznamy výmeny pošty"
Systém DNS podporuje rozšírené smerovanie pošty prostredníctvom poštových záznamov a záznamov výmeny pošty (MX).

Súvisiaci odkaz

"Príklad: Jeden server DNS pre intranet" na strane 12
Tento príklad znázorňuje jednoduchú podsieť so serverom DNS pre interné použitie.

"Pochopenie zón" na strane 2
Táto téma vysvetľuje zóny DNS a typy zón.

Poštové záznamy a záznamy výmeny pošty

Systém DNS podporuje rozšírené smerovanie pošty prostredníctvom poštových záznamov a záznamov výmeny pošty (MX).

Poštové záznamy a záznamy MX používajú poštové smerovacie programy ako napríklad programy používajúce protokol SMTP (Simple Mail Transfer Protocol). Vyhľadávacia tabuľka v zdrojových záznamoch DNS obsahuje typy poštových záznamov podporovaných serverom DNS iSeries.

DNS obsahuje informácie na zasielanie elektronickej pošty pomocou informácií výmeny pošty. Ak sieť používa DNS, aplikácia SMTP nedoručí poštu pre hostiteľa TEST.IBM.COM prostredníctvom otvorenia pripojenia TCP k adrese TEST.IBM.COM. SMTP najprv dotazuje server DNS s cieľom zistiť, ktoré hostiteľské servery možno použiť na doručenie správy.

Doručenie pošty na špecifickú adresu

Servery DNS používajú zdrojové záznamy nazývané záznamy *výmeny pošty* (MX). Záznamy MX mapujú doménu alebo názov hostiteľa do preferenčnej hodnoty a názvu hostiteľa. Záznamy MX sa zvyčajne používajú na určenie toho, že jeden hostiteľ sa používa na spracovanie pošty pre iného hostiteľa. Záznamy sa takisto používajú na určenie iného hostiteľa, ktorému sa má pošta doručiť v prípade, ak prvý hostiteľ je nedosiahnuteľný. Inými slovami umožňujú, aby bola pošta adresovaná jednému hostiteľovi doručená inému hostiteľovi.

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

Ak sa názov nachádza v oprávnení servera DNS, ale nemá priradený žiadny MX, server DNS môže odpovedať prázdnym zoznamom zdrojových záznamov MX. V tomto prípade aplikácia na odosielanie pošty najprv vytvorí priame spojenie s cieľovým hostiteľom.

Poznámka: Používanie zástupných znakov (napríklad: *.mycompany.com) v záznamoch MX pre doménu sa neodporúča.

Príklad: Záznam MX pre hostiteľa

V nasledujúcom príklade systém, podľa preferencií, doručuje poštu pre adresu fsc5.test.ibm.com samotnému hostiteľovi. Ak ho nemožno dosiahnuť, systém by mal doručiť túto poštu psfred.test.ibm.com alebo mvs.test.ibm.com (v prípade, že psfred.test.ibm.com takisto nemožno dosiahnuť). Toto je príklad, ako budú vyzerať záznamy MX:

```
fsc5.test.ibm.com   IN MX 0 fsc5.test.ibm.com
                                        IN MX 2 psfred.test.ibm.com
                                        IN MX 4 mvs.test.ibm.com
```

Súvisiaci odkaz

"Zdrojové záznamy systému DNS" na strane 8
Táto téma vysvetľuje spôsob použitia zdrojových záznamov systémom DNS. Zdrojové záznamy sa používajú na ukladanie údajov o názvoch domén a IP adries. Táto téma obsahuje zoznam zdrojových záznamov pre operačný systém OS/400 verzia 5, vydanie 1.

Príklady systému DNS

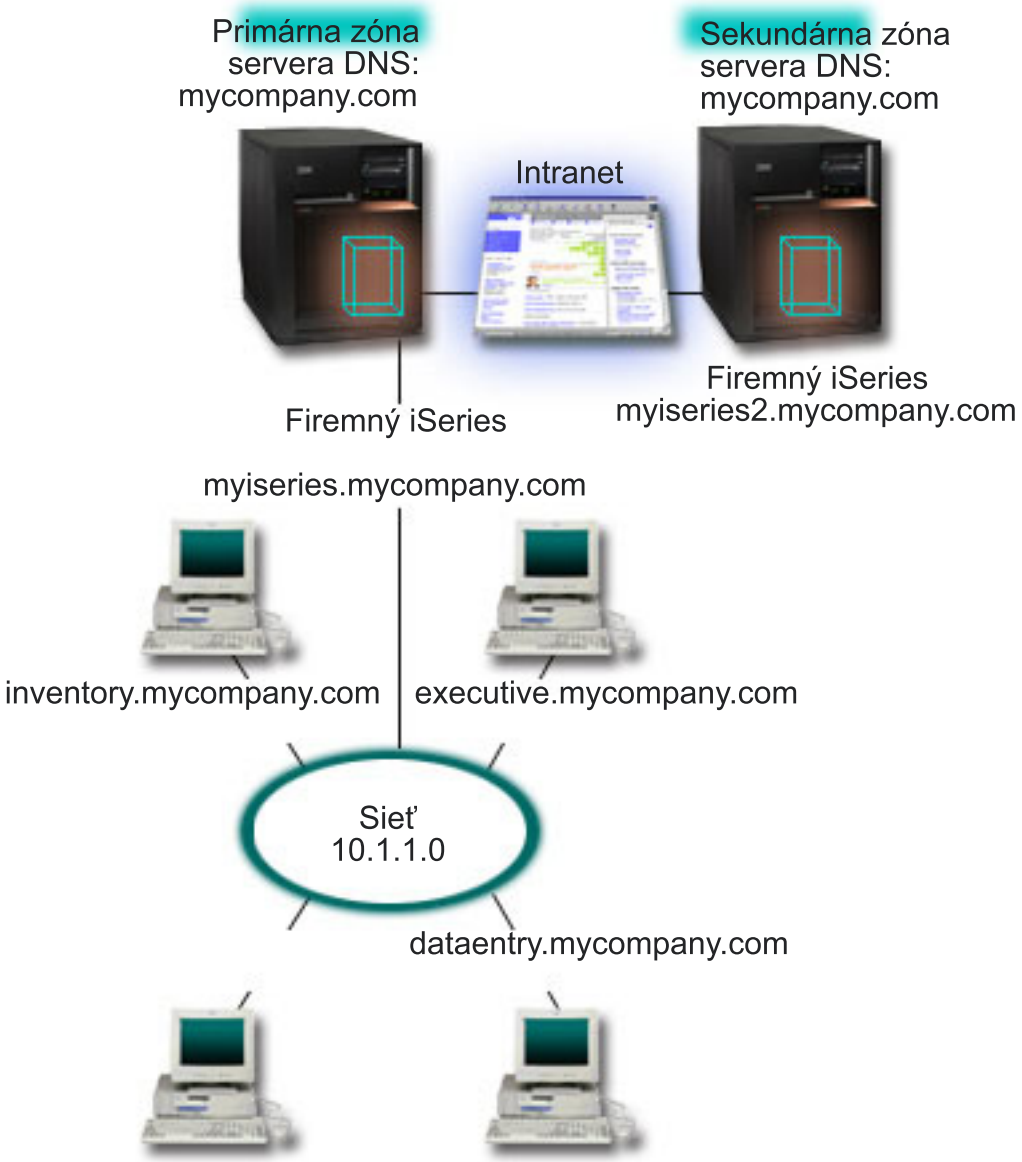
Pomocou týchto príkladov môžete porozumieť spôsobu použitia systému DNS vo vašej sieti.

DNS je distribuovaný databázový systém určený na riadenie hostiteľských názvov a ich príslušných IP adries. Nasledujúce príklady pomáhajú vysvetliť ako DNS funguje a ako ho možno použiť vo vašej sieti. Príklady opisujú nastavenia a dôvody použitia. Takisto obsahujú odkazy na súvisiace koncepty, ktoré vám môžu pomôcť porozumieť obrázkom.

Príklad: Jeden server DNS pre intranet

Tento príklad znázorňuje jednoduchú podsieť so serverom DNS pre interné použitie.

Nasledujúca ilustrácia zobrazuje server DNS spustený v serveri iSeries pre internú sieť. Táto jedna inštancia servera DNS je nastavená na počúvanie dotazov na všetkých IP adresách rozhrania. Server je primárnym názvovým serverom pre zónu mycompany.com.



Obrázok 2. Jeden server DNS pre intranet

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

Okrem záznamov typu A a PTR, systém DNS podporuje aj ďalšie typy zdrojových záznamov, ktoré sa môžu vyžadovať v závislosti od ostatných aplikácií na báze TCP/IP, ktoré spúšťate vo vašom intranete. Napríklad, ak používate interné systémy elektronickej pošty, možno budete musieť pridať záznamy výmeny pošty (MX). Týmto umožníte serveru SMTP dotazovať server DNS a zistiť tak, ktoré systémy majú spustené poštové servery.

Ak by táto malá sieť bola časťou väčšieho intranetu, mohlo by byť potrebné definovať interné koreňové servery.

Sekundárne servery

Sekundárne servery zavádzajú zónové údaje z autoritatívneho servera. Sekundárne servery získavajú zónové údaje vykonávaním prenosov zón z autoritatívneho servera. Sekundárny názvový server pri svojom spúšťaní žiada o všetky údaje pre uvedenú doménu z primárneho názvového servera. Sekundárny názvový server žiada o aktualizované údaje z primárneho servera buď preto, že prijíma hlásenie z primárneho názvového servera (ak sa používa funkcia NOTIFY) alebo preto, že dotazuje primárny názvový server a zistí, že sa dané údaje zmenili. Na obrázku 2 je server myiseries častou intranetu. Iný server iSeries, myiseries2, bol nakonfigurovaný ako sekundárny server DNS pre zónu mycompany.com. Tento sekundárny server možno použiť na vyrovnanie požiadaviek na servery a môže tiež poskytovať zálohu pre prípad výpadku primárneho servera. Je dobré mať pre každú zónu aspoň jeden sekundárny server.

Súvisiaci odkaz

"Zdrojové záznamy systému DNS" na strane 8
Táto téma vysvetľuje spôsob použitia zdrojových záznamov systémom DNS. Zdrojové záznamy sa používajú na ukladanie údajov o názvoch domén a IP adries. Táto téma obsahuje zoznam zdrojových záznamov pre operačný systém OS/400 verzia 5, vydanie 1.

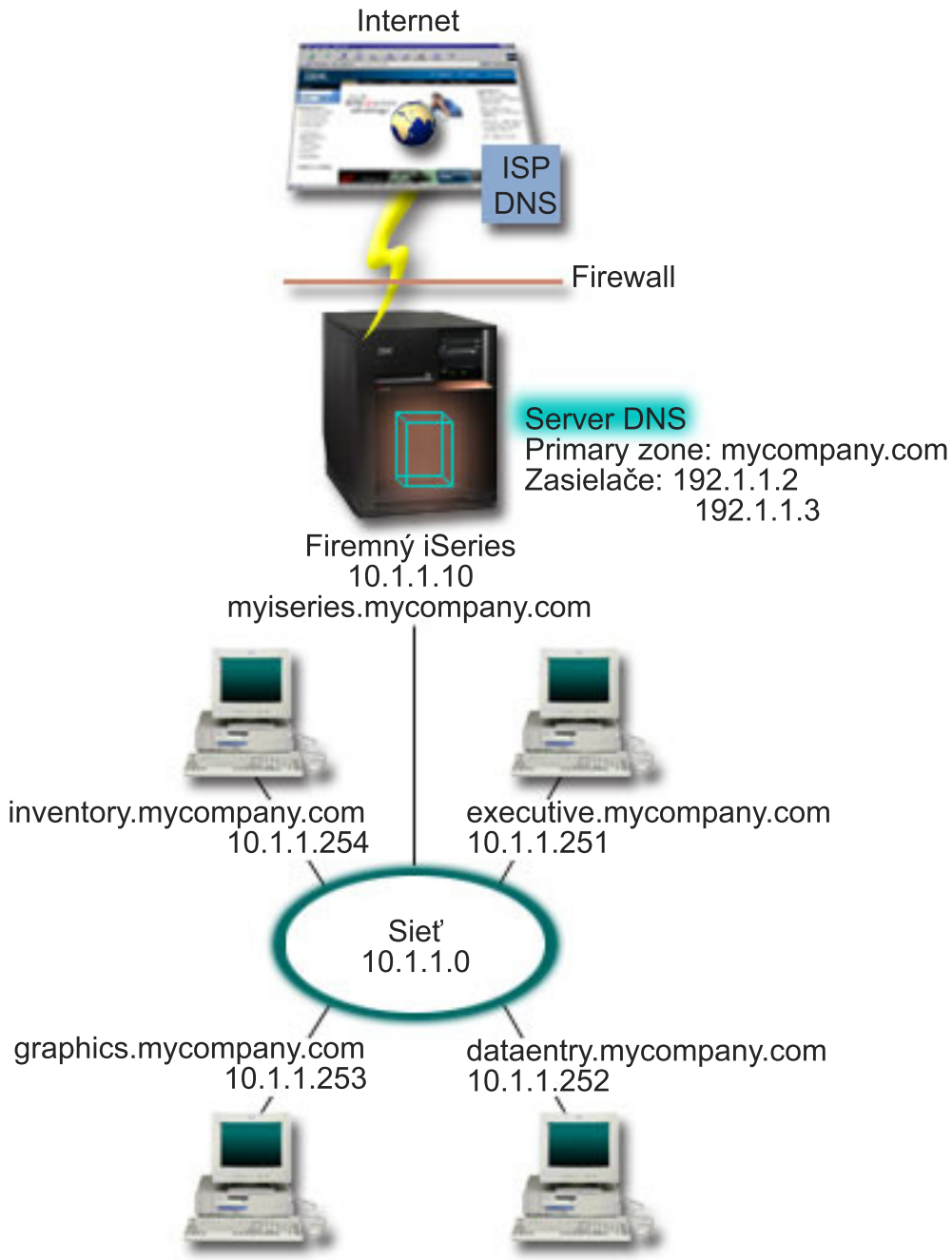
"Pochopenie zón" na strane 2
Táto téma vysvetľuje zóny DNS a typy zón.

"Príklad: Jeden server DNS s prístupom do internetu"
Tento príklad znázorňuje jednoduchú podsieť so serverom DNS pripojeným priamo do internetu.

Príklad: Jeden server DNS s prístupom do internetu

Tento príklad znázorňuje jednoduchú podsieť so serverom DNS pripojeným priamo do internetu.

Nasledujúca ilustrácia zobrazuje rovnakú sieť ako v príklade Jeden server DNS pre intranet, avšak s pridaným pripojením do internetu. V uvedenom príklade je spoločnosť schopná prístupu na internet, ale firewall je nakonfigurovaný na blokovanie internetovej prevádzky smerom do siete.



Obrázok 3. Jeden server DNS s prístupom do internetu

Na preklad internetových adries musíte vykonať aspoň jednu z nasledujúcich úloh:

- Definovať internetové koreňové servery

  Môžete automaticky načítať predvolené internetové koreňové servery. V niektorých prípadoch však musíte zoznam aktualizovať. Tieto servery vám môžu pomôcť preložiť adresy mimo vašej vlastnej zóny. Pokyny k získaniu aktuálnych internetových koreňových serverov nájdete v dokumente “Pristupovať k externým údajov systému DNS” na strane 26.
- Aktivovať postupovanie

  Môžete nastaviť postupovanie dotazov na zóny mimo mycompany.com externým serverom DNS, napríklad serverom DNS prevádzkovaným vašim poskytovateľom internetových služieb (ISP). Ak chcete aktivovať hľadanie oboma

spôsobmi (postupovaním a prostredníctvom koreňových serverov), musíte nastaviť voľbu forward na hodnotu **first**. Server najprv použije postupovanie a následne vykoná dotaz koreňových serverov len ak postupovanie zlyhá a dotaz ostane nepreložený.

V niektorých prípadoch sa môžu vyžadovať aj nasledujúce zmeny v konfigurácii:

- Pridelenie neobmedzených adries IP

  Vo vyššie uvedenom príklade sú zobrazené adresy 10.x.x.x. Ide však o obmedzené adresy, ktoré nemožno použiť mimo intranetu. Sú zobrazené len pre ilustračné účely. Vašu adresu IP určuje váš poskytovateľ internetových služieb (ISP) a iné faktory siete.
- Registrácia názvu domény

  Ak ste viditeľný v prostredí internetu a ešte nemáte zaregistrovanú doménu, musíte si zaregistrovať názov domény.
- Vytvorenie firewallu

  Neodporúča sa, aby ste DNS povolili priamo sa pripájať na internet. Mali by ste nakonfigurovať firewall alebo vykonať iné opatrenia na zabezpečenie vášho servera iSeries.

  Súvisiace koncepty

  "Nastavenie domény systému DNS" na strane 5
  Táto téma poskytuje prehľad procesu registrácie domény a obsahuje odkazy na ďalšie referenčné lokality, kde sa môžete dozvedieť viac o nastavení vášho vlastného priestoru domény.

  iSeries a bezpečnosť Internetu

  "Pochopenie dotazov systému DNS" na strane 3
  Táto téma vysvetľuje spôsob prekladu dotazov DNS.

  Súvisiaci odkaz

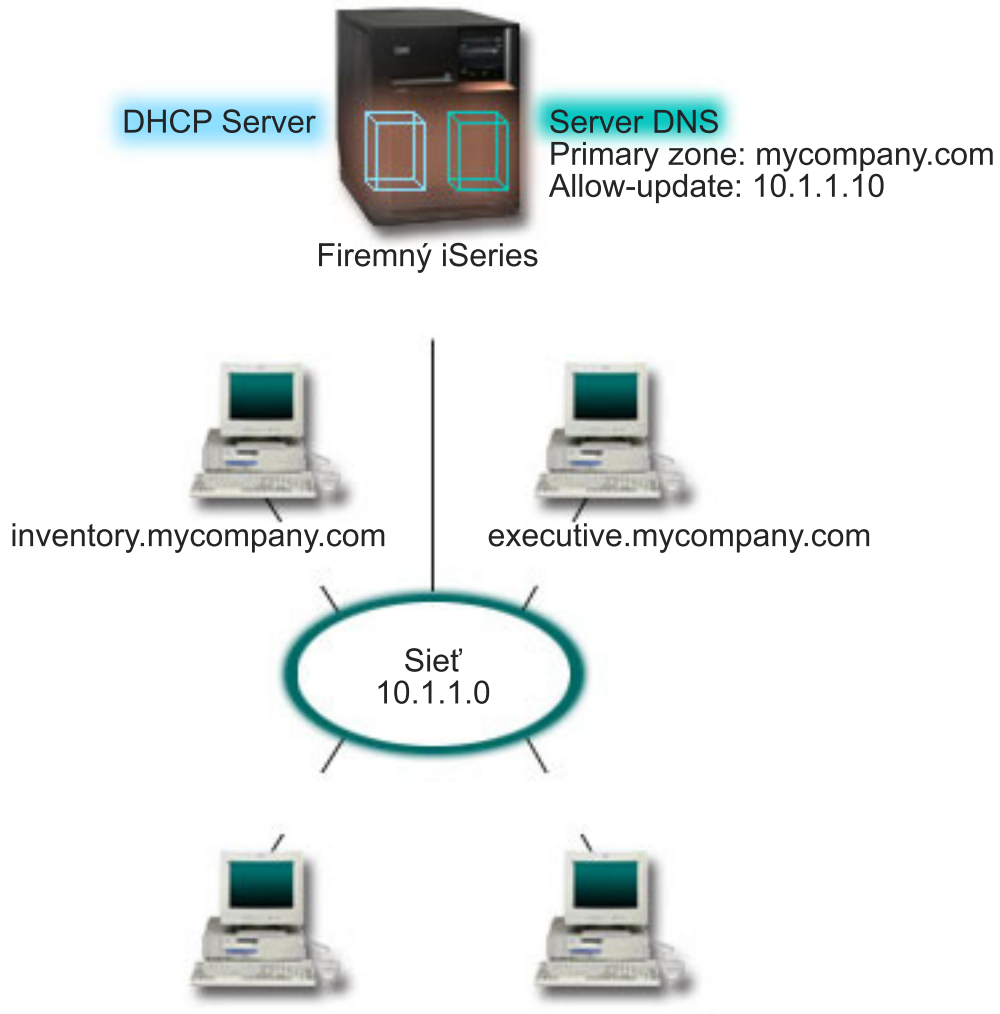
  "Príklad: Jeden server DNS pre intranet" na strane 12
  Tento príklad znázorňuje jednoduchú podsieť so serverom DNS pre interné použitie.

Príklad: DNS (Domain Name System) a DHCP (Dynamic Host Configuration Protocol) v jednom serveri iSeries

Tento príklad znázorňuje systémy DNS aj DHCP v jednom serveri.

Konfiguráciu možno použiť na dynamickú aktualizáciu zónových údajov DNS, keď DHCP priraďuje IP adresy hostiteľom.

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



Obrázok 4. DNS a DHCP v jednom serveri iSeries

Predchádzajúce verzie DHCP a DNS boli od seba navzájom nezávislé. Ak DHCP priradil klientovi novú IP adresu, správca musel manuálne aktualizovať záznamy DNS. V tomto príklade, ak sa adresa IP grafického súborového servera zmení z dôvodu pridelenia inej adresy serverom DHCP, závislí klienti nebudú schopní namapovať sieťovú jednotku na názov hostiteľa, pretože záznamy DNS budú obsahovať predošlú adresu IP súborového servera.

Pomocou servera systému OS/400 verzia 5, vydanie 1 na báze BIND 8 môžete nakonfigurovať vašu zónu DNS tak, že bude akceptovať aktualizácie záznamov DNS spolu so zmenami adries prostredníctvom servera DHCP. Napríklad, keď grafický súborový server obnoví svoj prenájom adresy a server DHCP mu priradí adresu IP 10.1.1.250, zodpovedajúce záznamy DNS sa automaticky aktualizujú. Toto umožňuje ostatným klientom dotazovať server DNS na grafický súborový server prostredníctvom jeho názvu bez prerušenia.

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

- Identifikovať dynamickú zónu

  Kým je server v chode, nemôžete manuálne aktualizovať dynamickú zónu. Mohlo by to spôsobiť rušenie s prichádzajúcimi dynamických aktualizáciami. Manuálne aktualizácie možno vykonať po zastavení servera, ale stratíte zas všetky dynamické aktualizácie zasielané počas zastavenia servera. Z tohto dôvodu môžete chcieť nakonfigurovať samostatnú dynamickú zónu a minimalizovať tak potrebu manuálnych aktualizácií. Pozrite si dokument “Určenie štruktúry domény” na strane 20, kde nájdete viac informácií o konfigurácii vašich zón na používanie funkcie dynamickej aktualizácie.
- Konfigurácia voľby allow-update

Každá zóna s voľbou povolenia aktualizácie sa bude považovať za dynamickú zónu. Voľba povolenia aktualizácie sa nastavuje pre každú zónu zvlášť. Aby mohla zóna prijímať dynamické aktualizácie, voľba povolenia aktualizácie musí byť pre danú zónu povolená. Pre tento príklad, zóna mycompany.com má údaje allow-update, ale ostatné zóny, ktoré sú definované v serveri, môžu byť nakonfigurované staticky alebo dynamicky.

- Konfigurácia DHCP na odosielanie dynamických aktualizácií

  Vášmu serveru DHCP musíte dať oprávnenie na aktualizáciu záznamov DNS pre IP adresy, ktoré distribuoval.

- Konfigurácia preferencií aktualizácií sekundárneho servera

  Ak chcete mať sekundárne servery aktuálne, môžete nakonfigurovať DNS na použitie funkcie NOTIFY na odosielanie správy o zmenách údajov zóny sekundárnym serverom pre zónu mycompany.com. Takisto by ste mali nakonfigurovať inkrementálne zónové prenosy (IXFR), ktoré umožňujú sekundárnym serverom sledovať a načítať len aktualizované zónové údaje namiesto všetkých zónových údajov.

Ak spúšťate systémy DNS a DHCP v rozdielnych serveroch, vyžaduje sa dodatočná konfigurácia servera DHCP.

Súvisiace koncepty

“Dynamické aktualizácie” na strane 5
Systém DNS operačného systému OS/400 verzia 5, vydanie 1 na báze BIND 8 podporuje dynamické aktualizácie. Toto umožňuje vonkajším zdrojom, ako je protokol DHCP, odoslať aktualizácie serveru DNS.

“Určenie štruktúry domény” na strane 20
Ak prvýkrát nastavujete doménu je potrebné ešte pred vytvorením zón naplánovať požiadavky a údržbu.

Súvisiace úlohy

Konfigurácia DHCP na odosielanie dynamických aktualizácií

Súvisiaci odkaz

Príklad: DNS a DHCP v rozličných serveroch iSeries

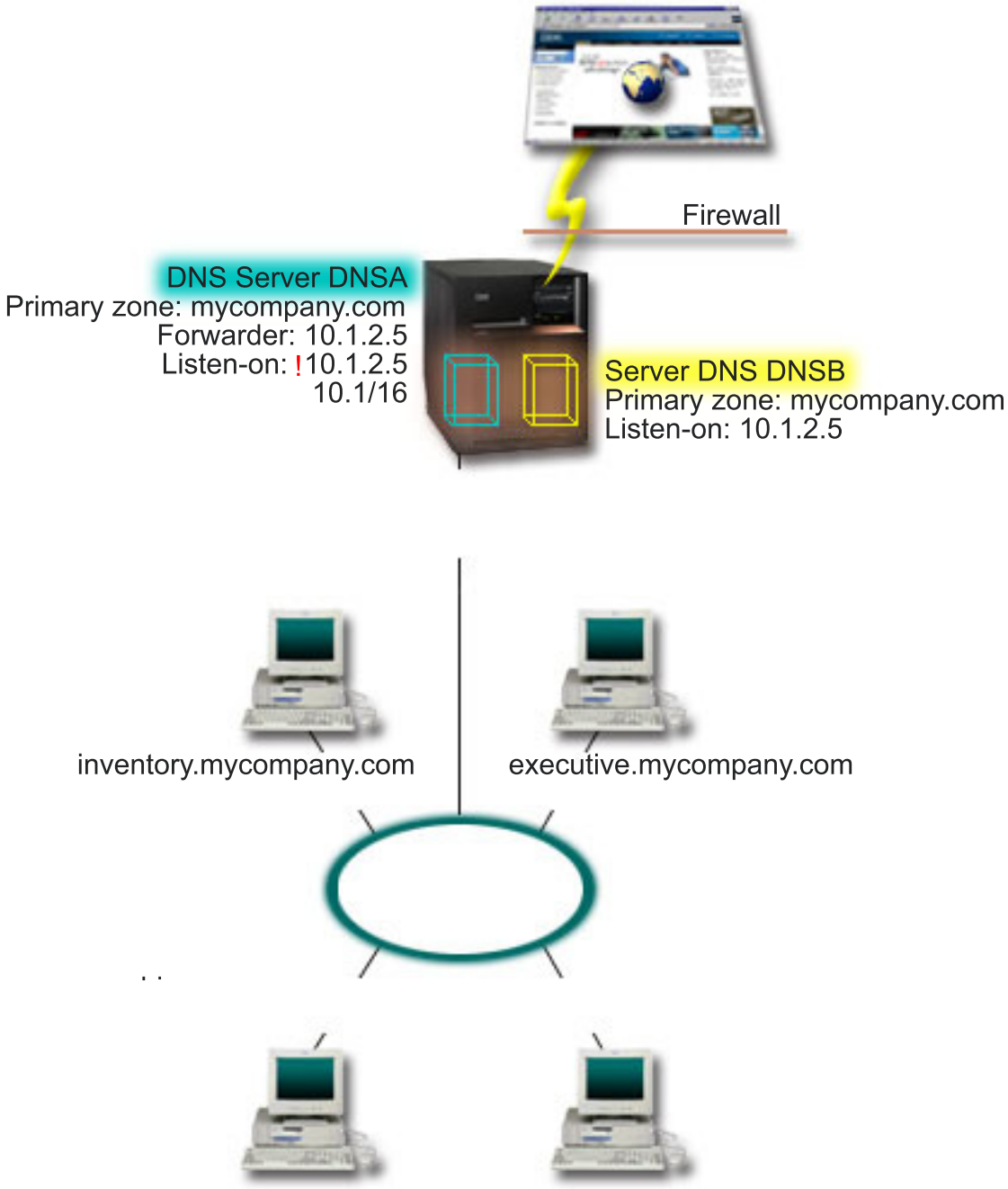
Príklad: Rozdelenie systému DNS cez firewall

Tento príklad znázorňuje systém DNS pracujúci nad firewallom, ktorý chráni interné údaje proti prístupu z internetu a zároveň umožňuje interným užívateľom pristupovať k údajom v internete.

Nasledujúci obrázok znázorňuje jednoduchú podsieť, ktorá používa pre bezpečnosť firewall. Systém DNS v operačnom systéme OS/400 verzia 5, vydanie 1 na báze BIND 8 umožňuje nastavenie viacerých serverov DNS v jednom serveri iSeries. Predpokladajte, že spoločnosť má internú sieť s vyhradeným priestorom adries IP a externú časť siete dostupnú verejnosti.

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

Ak to chce dosiahnuť, musí nastaviť dve inštancie servera DNS v jednom serveri iSeries. Jeden server DNS pre intranet a druhý pre všetko vo verejnej doméne. Tento proces sa nazýva *rozdelenie DNS*.



Obrázok 5. Rozdelenie DNS cez firewall

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

Ak máte obavy týkajúce sa integrity vášho firewallu alebo bezpečnosti, na pomoc pri ochrane interných údajov existuje možnosť použiť voľbu počúvania na určitej adrese. Ak ju chcete využiť, môžete nakonfigurovať interný server tak, aby povoľoval dotazy do internej zóny mycompany.com len od interných hostiteľov. Ak chcete, aby všetko správne pracovalo, interní klienti musia byť nakonfigurovaní na dotazovanie servera DNSA. Ak chcete nastaviť rozdelenie DNS, musíte zvážiť nasledujúce konfiguračné nastavenia:

- Listen-on

  V predošlých prípadoch bol iba jeden server DNS v serveri iSeries. Bol nastavený na počúvanie na všetkých adresách IP rozhrania. Ak používate viaceré servery DNS v serveri iSeries, musíte definovať adresy IP rozhrania, na ktorých servery počúvajú. keďže dva servery DNS nemôžu počúvať na tej istej adrese. V tomto prípade predpokladajte, že všetky dotazy prichádzajúce z firewallu sú odoslané na adresu 10.1.2.5. Tieto dotazy by mali byť zaslané na externý server. Preto je DNSB nakonfigurovaný na počúvanie na adrese 10.1.2.5. Interný server DNSA je nakonfigurovaný na prijímanie dotazov z akýchkoľvek IP adries rozhrania 10.1.x.x *s výnimkou* 10.1.2.5. Ak chcete túto adresu účinne vylúčiť, zoznam zhôd adries (AML) musí mať túto vylúčenú adresu uvedenú pred zahrnutou predponou adresy.
- Poradie zoznamu zhôd adries (AML)

  Použije sa prvý prvok v zozname AML, ktorý sa zhoduje so zadanou adresou. Ak chcete napríklad povoliť všetky adresy v sieti 10.1.x.x s výnimkou adresy 10.1.2.5, elementy ACL musia byť v nasledujúcom poradí (!10.1.2.5; 10.1/16). V tomto prípade sa adresa 10.1.2.5 porovná s prvým prvkom a okamžite sa zakáže.

  Ak sú prvky vyhradené (10.1/16; !10.1.2.5), adrese IP 10.1.2.5 sa povolí prístup, pretože server ju porovná s prvým prvkom, ktorý sa zhoduje a povolí prístup bez kontroly ostatných pravidiel.

  Súvisiaci odkaz

  "Vlastnosti BIND 8" na strane 6
  Popri dynamických aktualizáciách, systém BIND 8 ponúka niekoľko vlastností na zvýšenie výkonu vášho servera DNS.

Plánovanie pre systému DNS

Systém DNS ponúka množstvo riešení. Pred jeho konfiguráciou by ste mali naplánovať spôsob, akým bude pracovať vo vašej sieti. Pred implementáciou DNS by ste mali vyhodnotiť subjekty ako štruktúra siete, výkon a bezpečnosť.

Určenie oprávnení systému DNS

Pre administrátora DNS existujú špeciálne požiadavky na oprávnenia. Je potrebné zvážiť aj bezpečnostné aspekty autorizácie.

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

Pre vášho administrátora systému iSeries sa vyžaduje minimálna úroveň oprávnení na konfiguráciu a spravovanie systému DNS. Udelenie prístupu k všetkým objektom správcovi umožní vykonávať úlohy správy DNS. Odporúča sa prístup správcu bezpečnosti s oprávnením pre všetky objekty (*ALLOBJ) pre tých užívateľov, ktorí konfigurujú systém DNS. Na autorizáciu užívateľov môžete použiť program Navigátor iSeries. Ak potrebujete viac informácií, prečítajte si dokument Udelenie oprávnenia administrátorovi DNS v online pomoci k systému DNS.

Poznámka: Ak profil administrátora nemá úplné oprávnenie, musíte udeliť špecifický prístup a oprávnenie pre všetky adresáre DNS a súvisiace konfiguračné súbory.

Súvisiaci odkaz

"Udržiavanie konfiguračných súborov systému DNS" na strane 29
Táto téma vám pomôže porozumieť súborom používaným systémom DNS a pokynom na ich zálohovanie a udržiavanie.

Určenie štruktúry domény

Ak prvýkrát nastavujete doménu je potrebné ešte pred vytvorením zón naplánovať požiadavky a údržbu.

Je dôležité určiť spôsob rozdelenia vašej domény alebo poddomén do zón, najlepší spôsob obslúženia záťaže, prístupu do internetu a dohôd s firewallom. Tieto faktory môžu byť zložité a je potrebné riešiť ich od prípadu k prípadu. Podrobné pokyny nájdete v autoritatívnych zdrojoch, napríklad v knihe DNS and BIND od vydavateľstva O'Reilly.

Ak nakonfigurujete zónu DNS ako dynamickú, nemôžete v nej vykonávať manuálne zmeny, ak je server spustený. Mohlo by to spôsobiť rušenie s prichádzajúcimi dynamických aktualizáciami. V prípade potreby manuálnej aktualizácie server vypnite, vykonajte zmeny a reštartujte ho. Dynamické aktualizácie odoslané na zastavený server DNS nebudú nikdy vykonané. Z tohto dôvodu môžete chcieť nakonfigurovať dynamickú zónu a statickú zónu samostatne. Môžete to vykonať vytvorením úplne samostatných zón, alebo definovaním novej poddomény, napríklad dynamic.mycompany.com, pre klientov udržiavaných dynamicky.

Systém DNS servera iSeries poskytuje grafické rozhranie na konfiguráciu vašich serverov. V niektorých prípadoch toto rozhranie používa terminológiu alebo koncepty, ktoré sú v iných zdrojoch reprezentované rozdielne. Ak pri plánovaní vašej konfigurácie systému DNS používate aj iné informačné zdroje, môže byť užitočné, ak si zapamätáte toto:

- Všetky zóny a objekty definované v serveri sú organizované v rámci zložiek **zón dopredného vyhľadávania** a **spätného vyhľadávania**. Zóny dopredného vyhľadávania sú zóny, ktoré sa používajú na mapovanie názvov domén do IP adries, ako napríklad záznamy A. Zóny spätného vyhľadávania sú zóny, ktoré sa používajú na mapovanie IP adries do názvov domén, ako napríklad záznamy PTR.
- Systém DNS iSeries používa odkazy na *primárne zóny* a *sekundárne zóny*.
- Rozhranie používa *podzóny*, pre ktoré niektoré zdroje používajú termín *poddomény*. Zóna potomka je podzónou, pre ktorú ste delegovali zodpovednosť za jeden alebo viacero názvových serverov.

Súvisiaci odkaz

"Príklad: DNS (Domain Name System) a DHCP (Dynamic Host Configuration Protocol) v jednom serveri iSeries" na strane 16
Tento príklad znázorňuje systémy DNS aj DHCP v jednom serveri.

Plánovanie mier bezpečnosti

Systém DNS poskytuje bezpečnostné voľby, ktoré umožňujú obmedziť vonkajší prístup k vášmu serveru.

Zabezpečenie vášho servera DNS je zásadnou vecou. Okrem úvah o bezpečnosti v tejto téme sú otázky bezpečnosti DNS a servera iSeries pokryté aj v iných zdrojoch vrátane témy Server iSeries a internet v Informačnom centre. Kniha DNS and BIND sa takisto zaoberá otázkou bezpečnosti vo vzťahu k DNS.

Zoznamy zhôd adries

Systém DNS používa zoznamy zhôd adries na povolenie alebo zakázanie prístupu vonkajším entitám k určitým funkciám DNS. Tieto zoznamy môžu obsahovať špecifické IP adresy, podsieť (používajúcu IP predponu) alebo určité kľúče na podpisovanie transakcií TSIG (Transaction Signature). V zozname zhôd adries môžete definovať zoznam entít, ktorým chcete povoliť alebo zakázať prístup. Ak chcete zoznam zhôd adries opakovane použiť, môžete ho uložiť ako zoznam riadenia prístupu (ACL). Ak budete niekedy tento zoznam potrebovať, môžete použiť volanie ACL na jeho načítanie.

Poradie prvkov v zozname zhôd adries

Použije sa prvý prvok v zozname zhôd adries, s ktorým sa zhoduje zadaná adresa. Ak chcete napríklad povoliť všetky adresy v sieti 10.1.1.x s výnimkou 10.1.1.5, elementy zoznamu zhôd musia byť v tomto poradí (!10.1.1.5; 10.1.1/24). V tomto prípade sa adresa 10.1.1.5 porovná s prvým prvkom a okamžite sa zakáže.

Ak sú prvky vyhradené (10.1.1/24; !10.1.1.5), adrese IP 10.1.1.5 sa povolí prístup, pretože server ju porovná s prvým prvkom, ktorý sa zhoduje a povolí prístup bez kontroly ostatných pravidiel.

Voľby riadenia prístupu

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

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

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

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

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

blackhole
Určuje zoznam adries, od ktorých server neakceptuje dotazy a ktoré nepoužíva na preklad dotazov. Na dotazy z týchto adries nebude server odpovedať.

Súvisiace koncepty

iSeries a bezpečnosť Internetu

Súvisiaci odkaz

“Vlastnosti BIND 8” na strane 6
Popri dynamických aktualizáciách, systém BIND 8 ponúka niekoľko vlastností na zvýšenie výkonu vášho servera DNS.

Požiadavky systému DNS

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

Voľba DNS (Voľba 31) sa neinštaluje automaticky spolu so základným operačným systémom. DNS musíte na inštaláciu špecificky vybrať. Nový server DNS pridaný do operačného systému OS/400 verzia 5, vydanie 1 je založený na implementácii známej ako BIND 8, ktorá predstavuje priemyselný štandard. Predošlé služby DNS systému OS/400 boli založené na verzii BIND 4.9.3 a sú stále dostupné aj v systéme OS/400 verzia 5, vydanie 1.

Po nainštalovaní DNS obsahuje predvolená konfigurácia nastavenie jedného servera DNS pomocou verzie BIND 4.9.3, ktorá bola dostupná v predošlých vydaniach. Ak chcete spustiť jeden alebo viac serverov DNS pomocou verzie BIND 8, musíte nainštalovať prostredie PASE. PASE je SS1 voľba 33. Po inštalácii prostredia PASE program Navigátor iSeries automaticky nakonfiguruje správnu implementáciu systému BIND.

Ak nepoužívate PASE, nebudete môcť využívať všetky vlastnosti BIND 8. Ak nepoužívate PASE, môžete ešte stále spúšťať ten istý server DNS založený na BIND 4.9.3 dostupný v predchádzajúcich vydaniach. Pozrite si tému Informačného centra Systém DNS pre verziu 4, vydanie 5, kde nájdete dokumentáciu k systému BIND 4.9.3.

Ak chcete nakonfigurovať server DHCP v inom serveri iSeries tak, aby odosielal aktualizácie tomuto serveru DNS, musíte v serveri DHCP (v serveri iSeries) nainštalovať Voľbu 31. Server DHCP používa programové rozhrania poskytnuté Voľbou 31 na vykonanie dynamických aktualizácií.

Súvisiace koncepty

Portable Application Solutions Environment (PASE)

“Konfigurácia systému DNS” na strane 23
Táto téma vysvetľuje spôsob použitia programu Navigátor iSeries na konfiguráciu názvových serverov a na preklad dotazov mimo vašej domény.

Súvisiaci odkaz

“Vlastnosti BIND 8” na strane 6
Popri dynamických aktualizáciách, systém BIND 8 ponúka niekoľko vlastností na zvýšenie výkonu vášho servera DNS.

Súvisiace informácie

Téma Informačného centra DNS pre verziu 4, vydanie 5

Určiť, či je systém DNS nainštalovaný

Ak chcete určiť, či je systém DNS nainštalovaný, vykonajte tieto kroky:

1. Na príkazovom riadku zadajte GO LICPGM a stlačte kláves Enter.
2. Zadajte 10 (Zobraziť nainštalované licenčné programy) a stlačte kláves Enter.
3. Presuňte sa o stranu dole na **5722SS1 Systém DNS** (SS1 Voľba 31). Ak je systém DNS úspešne nainštalovaný, položka Stav inštalácie bude *compatible, podobne ako je uvedené nižšie:

```
LicPgm     Installed Status     Description
5722SS1    *COMPATIBLE          Systém DNS
```

4. Stlačte kláves F3 na opustenie obrazovky.

Inštalácia systému DNS

Ak chcete nainštalovať systém DNS, vykonajte tieto kroky:

1. Na príkazovom riadku zadajte GO LICPGM a stlačte kláves Enter.
2. Zadajte 11 (Nainštalovať licenčné programy) a stlačte kláves Enter.
3. Zadajte 1 (Inštalovať) v poli **Voľba** vedľa položky Systém DNS a stlačte kláves Enter.
4. Znovu stlačte kláves Enter na potvrdenie inštalácie.

Konfigurácia systému DNS

Táto téma vysvetľuje spôsob použitia programu Navigátor iSeries na konfiguráciu názvových serverov a na preklad dotazov mimo vašej domény.

Predtým ako začnete pracovať s konfiguráciou systému DNS, pozrite si systémové požiadavky a nainštalujte všetky potrebné komponenty DNS.

Súvisiace koncepty

"Požiadavky systému DNS" na strane 22
Táto téma opisuje softvérové požiadavky na spustenie systému DNS vo vašom serveri iSeries.

Pristupovať k systému DNS v programe Navigátor iSeries

V tejto téme sa dozviete o spôsobe prístupu k systému DNS pomocou programu Navigátor iSeries.

Nasledujúce pokyny vás navedú ku konfiguračnému rozhraniu DNS v programe Navigátor iSeries. Ak používate PASE, budete môcť nakonfigurovať servery DNS založené na BIND 8. Ak nepoužívate PASE, môžete ešte stále spúšťať ten istý server DNS založený na BIND 4.9.3, ktorý bol dostupný v predchádzajúcich vydaniach. Informácie o DNS na báze BIND 4.9.3. nájdete v téme Informačného centra DNS pre verziu 4, vydanie 5.

Ak konfigurujete DNS prvýkrát, postupujte takto:

1. V programe Navigátor iSeries rozviňte **váš server iSeries → Sieť → Servery → DNS**.
2. Pravým tlačidlom myši kliknite na **DNS** a vyberte **New Configuration**.

Súvisiace koncepty

Program Navigátor iSeries

Konfigurovať názvové servery

Systém DNS vám umožňuje vytvoriť viaceré inštancie názvového servera. Táto téma poskytuje pokyny na konfiguráciu názvového servera.

DNS iSeries na báze BIND 8 podporuje viaceré inštancie názvového servera. Nasledujúce úlohy vás prevedú procesom vytvorenia jednej inštancie názvového servera vrátane nastavenia vlastností a zón.

Ak chcete vytvoriť viaceré inštancie, zopakujte tieto procedúry, kým nevytvoríte všetky inštancie. Pre každú inštanciu názvového servera môžete uviesť nezávislé vlastnosti, ako napríklad úrovne ladenia a hodnoty automatického spustenia. Keď vytvoríte novú inštanciu, vytvoria sa samostatné konfiguračné súbory.

Súvisiaci odkaz

"Udržiavanie konfiguračných súborov systému DNS" na strane 29
Táto téma vám pomôže porozumieť súborom používaným systémom DNS a pokynom na ich zálohovanie a udržiavanie.

Vytvoriť inštanciu názvového servera

Na definovanie inštancie servera DNS použite sprievodcu Nová konfigurácia DNS.

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

1. V programe **Navigátor iSeries** rozviňte **váš servera iSeries → Sieť → Servery → DNS**.
2. V pravej časti okna pravým tlačidlom myši kliknite na **DNS** a vyberte **Nový názvový server...**.
3. Sprievodca vás prevedie procesom konfigurácie.

Sprievodca vyžaduje nasledujúce vstupy:

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

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

Koreňové servery:
Môžete načítať zoznam predvolených internetových koreňových serverov, alebo môžete zadať vlastné koreňové servery, napríklad interné koreňové servery pre intranet.

Poznámka: Načítanie predvolených internetových koreňových serverov by ste mali vziať do úvahy len ak ste v internete a váš systém DNS bude prekladať internetové názvy.

Spustenie servera:
Môžete zadať, či požadujete automatické spustenie servera pri spustení protokolu TCP/IP. Pri prevádzkovaní viacerých serverov možno jednotlivé inštancie spustiť a ukončiť nezávisle od seba.

Upraviť vlastnosti servera DNS

Po vytvorení názvového servera môžete upravovať vlastnosti, ako napríklad povolenie úrovní aktualizácie a ladenia. Tieto voľby platia len pre inštanciu servera, ktorú meníte.

Ak chcete upraviť vlastnosti inštancie servera DNS, vykonajte tieto kroky:

1. V programe **Navigátor iSeries** rozviňte **váš server iSeries → Sieť → Servery → DNS**.
2. V pravej časti kliknite pravým tlačidlom myši na **your DNS server** a vyberte **Configuration**.
3. Kliknite pravým tlačidlom myši na **DNS Server** a vyberte **Properties**.

Konfigurovať zóny v názvovom serveri

Po konfigurácii inštancie servera DNS potrebujete nakonfigurovať zóny pre názvový server.

Váš server sa zobrazuje v pravej časti okna. Ak chcete nakonfigurovať zóny na vašom serveri, kliknite pravým tlačidlom myši na názov servera a zvoľte si **Configuration**. Zobrazí sa okno Konfigurácia DNS.

Všetky zóny sú nakonfigurované pomocou sprievodcov. Kliknutím pravým tlačidlom myši na zodpovedajúcu zložku vytvorte **zóny dopredného vyhľadávania** alebo **zóny spätného vyhľadávania**. Zobrazia sa voľby dostupné pre typ zóny. Sprievodcu spustíte výberom typu zóny, ktorú chcete vytvoriť.

Súvisiace koncepty

"Pristupovať k externým údajov systému DNS" na strane 26
Ak vytvoríte zónové údaje systému DNS, váš server bude môcť prekladať dotazy patriace do tejto zóny.

Súvisiace úlohy

"Konfigurácia systému DNS na príjem dynamických aktualizácií"
Servery DNS na báze BIND 8 sa dajú nakonfigurovať na akceptovanie požiadaviek o dynamickú aktualizáciu zónových údajov od iných zdrojov. Táto téma poskytuje pokyny na konfiguráciu voľby na povolenie aktualizácie, aby mohol DNS prijímať dynamické zmeny.

"Importovať súbory systému DNS" na strane 26
Systém (DNS) dokáže importovať existujúce súbory zónových údajov. Postupujte podľa týchto čas šetriacich procedúr na vytvorenie novej zóny z existujúceho konfiguračného súboru.

Súvisiaci odkaz

"Pochopenie zón" na strane 2
Táto téma vysvetľuje zóny DNS a typy zón.

Konfigurácia systému DNS na príjem dynamických aktualizácií

Servery DNS na báze BIND 8 sa dajú nakonfigurovať na akceptovanie požiadaviek o dynamickú aktualizáciu zónových údajov od iných zdrojov. Táto téma poskytuje pokyny na konfiguráciu voľby na povolenie aktualizácie, aby mohol DNS prijímať dynamické zmeny.

Keď sa vytvárajú dynamické zóny, mali by ste si pozrieť štruktúru svojej siete. Ak časti vašej domény vyžadujú manuálne aktualizácie, môžete zvážiť nastavenie samostatných statických a dynamických zón. Ak je potrebné aktualizovať dynamickú zónu manuálne, musíte zastaviť server dynamickej zóny a po vykonaní aktualizácií ho reštartovať. Zastavenie prinúti server zosynchronizovať všetky dynamické aktualizácie, vykonané odkedy server zaviedol svoje zónové údaje z databázy zóny. Ak server nezastavíte, stratíte všetky dynamické aktualizácie, ktoré sa spracovali od jeho spustenia. Avšak, vypnutie servera za účelom vykonania manuálnych aktualizácií znamená, že môžete prísť o dynamické aktualizácie odoslané v čase, keď bol server vypnutý.

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

1. V programe Navigátor iSeries rozviňte **váš server iSeries → Sieť → Servery → DNS**.
2. V pravej časti kliknite pravým tlačidlom myši na **your DNS server** a vyberte **Configuration**.
3. V okne Konfigurácia DNS rozviňte **Zóna dopredného prehľadania** alebo **Zóna spätného prehľadania**.
4. Pravým tlačidlom myši kliknite na primárnu zónu, ktorú chcete upraviť a vyberte **Vlastnosti**.
5. Na strane Vlastnosti primárnej zóny kliknite na záložku **Možnosti**.
6. Na strane Možnosti rozviňte **Riadenie prístupu → allow-update**.
7. Na overovanie autorizovaných aktualizácií používa DNS zoznam zhôd adries. Ak chcete pridať objekt do zoznamu zhôd adries, vyberte typ prvku v zozname zhôd adries a kliknite na **Pridať**. Môžete pridať adresu IP, predponu IP, zoznam riadenia prístupu alebo kľúč.
8. Po dokončení aktualizácie zoznamu zhôd adries kliknite na **OK** na zatvorenie strany Možnosti.

Súvisiace koncepty

"Dynamické aktualizácie" na strane 5
Systém DNS operačného systému OS/400 verzia 5, vydanie 1 na báze BIND 8 podporuje dynamické aktualizácie. Toto umožňuje vonkajším zdrojom, ako je protokol DHCP, odoslať aktualizácie serveru DNS.

"Konfigurovať zóny v názvovom serveri" na strane 24
Po konfigurácii inštancie servera DNS potrebujete nakonfigurovať zóny pre názvový server.

Súvisiace úlohy

Konfigurácia DHCP na odosielanie dynamických aktualizácií

Importovať súbory systému DNS

Systém (DNS) dokáže importovať existujúce súbory zónových údajov. Postupujte podľa týchto čas šetriacich procedúr na vytvorenie novej zóny z existujúceho konfiguračného súboru.

Importom súboru zónových údajov alebo konverziou existujúcich hostiteľských tabuliek môžete vytvoriť primárnu zónu. Ak chcete vytvoriť zónové údaje z tabuľky hostiteľov, pozrite si dokument Konverzia tabuliek hostiteľov.

Je možné importovať ľubovoľný súbor, ktorý je platným súborom zónovej konfigurácie založeným na syntaxi BIND. Súbor by mal byť umiestnený v adresári IFS. Systém DNS pri importe skontroluje platnosť súboru zónových údajov a pridá ho do súboru NAMED.CONF pre túto inštanciu servera.

Ak chcete naimportovať zónový súbor, postupujte takto:

1. V programe Navigátor iSeries rozviňte **váš server iSeries → Sieť → Servery → DNS**.
2. V pravej časti dvakrát kliknite na inštanciu servera DNS, do ktorej chcete túto zónu importovať.
3. V ľavej časti kliknite pravým tlačidlom myši na **DNS server** a zvoľte si **Import Zone**.
4. Pri importovaní primárnej zóny postupujte podľa pokynov sprievodcu.

Súvisiace koncepty

"Konfigurovať zóny v názvovom serveri" na strane 24
Po konfigurácii inštancie servera DNS potrebujete nakonfigurovať zóny pre názvový server.

Validácia záznamu

Funkcia importu údajov domény číta a overuje každý záznam importovaného súboru.

Po dokončení importu údajov domény môžete všetky chybné záznamy skontrolovať samostatne na strane vlastností Ostatné záznamy v importovanej zóne.

Poznámky:

1. Importovanie veľkej primárnej domény môže trvať niekoľko minút.
2. Funkcia importu údajov domény nepodporuje direktívu $include. Proces kontroly platnosti importu údajov domény označí riadky obsahujúce direktívu $include ako chybné.

Pristupovať k externým údajov systému DNS

Ak vytvoríte zónové údaje systému DNS, váš server bude môcť prekladať dotazy patriace do tejto zóny.

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

Aby server DNS získal viac informácií, musí vedieť, kde má hľadať. Prvé miesto v internete, kde server DNS hľadá záznamy, predstavujú koreňové servery. Koreňové servery smerujú server DNS na iné servery v hierarchii, až kým sa nenájde odpoveď, alebo určia, že odpoveď neexistuje.

Predvolený zoznam koreňových serverov programu Navigátor iSeries

Koreňové servery internetu by ste mali používať len vtedy, ak máte internetové pripojenie a chcete rozlíšiť názvy na internete, ak nie sú rozlíšené na vašom serveri DNS. Predvolený zoznam internetových koreňových serverov dodávaný v programe Navigátor iSeries. Zoznam je aktuálny pri každom ďalšom vydaní programu Navigátor iSeries. Kontrolu aktuálnosti predvoleného zoznamu môžete vykonať jeho porovnaním so zoznamom na stránke InterNIC. Aktualizujte si konfiguračný zoznam koreňových serverov.

Kde získať adresy internetových koreňových serverov

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

1. Vytvorte anonymné pripojenie FTP k serveru InterNIC FTP.RS.INTERNIC.NET
2. Prevezmite tento súbor: /domain/named.root
3. Uložte ho do nasledujúcej adresárovej cesty: Integrovaný súborový systém/Root/QIBM/ProdData/OS400/DNS/ROOT.FILE

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

Intranetové koreňové servery

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

Súvisiace koncepty

"Konfigurovať zóny v názvovom serveri" na strane 24
Po konfigurácii inštancie servera DNS potrebujete nakonfigurovať zóny pre názvový server.

Manažovať systém DNS

Táto téma opisuje spôsob kontroly funkcií systému DNS, monitorovanie výkonu a údržbu údajov a súborov systému DNS.

Kontrola funkcií DNS pomocou nástroja Name Server Lookup

Nástroj NSLookup (Name Server Lookup) môžete použiť na kontrolu funkcií systému DNS.

Nástroj NSLookup použite na vykonanie dotazu servera DNS na adresu IP. Tým overíte, či server DNS odpovedá na dotazy. Požiadajte o názov hostiteľa priradený k návratovej IP adrese (127.0.0.1). Server by mal odpovedať názvom hostiteľa (localhost). Takisto by ste mali vykonať dotazy na špecifické názvy definované v inštancii servera, ktorú chcete skontrolovať. Tým sa potvrdí, či konkrétna testovaná inštancia servera funguje správne.

Ak chcete overiť funkčnosť DNS pomocou NSLookup, postupujte takto:

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

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

   kde n.n.n.n predstavuje IP adresu servera vášho DNS.
4. Na príkazovom riadku zadajte 127.0.0.1 a stlačte kláves Enter.

   Mali by sa zobraziť nasledujúce informácie vrátane názvu hostiteľa návratu.

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

```
Názov:    localhost
    Address:  127.0.0.1
```

Server DNS odpovedá správne, ak vráti názov hostiteľa návratu: **localhost**.

5. Zadajte exit a stlačením klávesu Enter ukončite reláciu terminálu NSLOOKUP.

Poznámka: Pomoc k používaniu nástroja NSLookup získate zadaním ? a stlačením klávesu Enter.

Manažovať bezpečnostné kľúče

Bezpečnostné kľúče umožňujú obmedziť prístup k vašim údajom DNS.

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

Manažovať kľúče systému DNS

Kľúče systému DNS sú kľúče definované pre systém BIND a používané serverom DNS ako časť kontroly prichádzajúcej aktualizácie.

Kľúč môžete nakonfigurovať a priradiť mu názov. Potom, keď budete chcieť chrániť objekt DNS, ako napríklad dynamickú zónu, môžete tento kľúč zadať na zozname zhôd adries.

Pri riadení kľúčov DNS postupujte takto:

1. V programe Navigátor iSeries rozviňte **váš server iSeries → Sieť → Servery → DNS**.
2. V pravej časti okna pravým tlačidlom myši kliknite na inštanciu servera DNS, ktorú chcete otvoriť a vyberte **Konfigurácia**.
3. V okne Konfigurácia DNS vyberte **Súbor → Manažovať kľúče**.

Manažovať kľúče dynamickej aktualizácie

Kľúče dynamickej aktualizácie sa používajú na zabezpečenie dynamických aktualizácií serverom DHCP (Dynamic Host Configuration Protocol).

Tieto kľúče musia byť k dispozícii, ak sa servery DNS aj DHCP nachádzajú v jednom serveri iSeries. Ak sa server DHCP nachádza v inom serveri iSeries, musíte vytvoriť rovnaký kľúč dynamickej aktualizácie v každom serveri iSeries, kde chcete povoliť bezpečné dynamické aktualizácie.

Pri riadení kľúčov dynamických zmien postupujte takto:

1. V programe Navigátor iSeries rozviňte **váš server iSeries → Sieť → Servery → DNS**.
2. Pravým tlačidlom myši kliknite na **DNS** a vyberte **Manažovať kľúče dynamickej aktualizácie**.

Pristupovať k štatistikám servera DNS

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

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

Súvisiaci odkaz

“Udržiavanie konfiguračných súborov systému DNS” na strane 29
Táto téma vám pomôže porozumieť súborom používaným systémom DNS a pokynom na ich zálohovanie a udržiavanie.

Štatistika servera
Štatistika servera sumarizuje počet dotazov a odpovedí, ktoré server prijal od posledného reštartu alebo opakovaného načítania svojej databázy.

Systém DNS vám umožňuje zobraziť štatistiku pre inštanciu servera. Informácie sa kontinuálne pridávajú do tohto súboru, až kým ho nevymažete. Tieto informácie môžu byť užitočné pri vyhodnocovaní množstva premávky, ktorú server prijal a pri sledovaní problémov. Viac informácií o štatistike servera je dostupných v téme online pomoci pre server DNS s názvom Pochopenie štatistiky servera DNS.

Ak chcete vstupovať do štatistiky servera, postupujte takto:

1. V programe Navigátor iSeries rozviňte **váš server iSeries → Sieť → Servery → DNS**.
2. V pravej časti kliknite pravým tlačidlom myši na **your DNS server** a vyberte **Configuration**.
3. V okne konfigurácie DNS vyberte **Zobraziť → Štatistika servera**.

Databáza aktívneho servera
Databáza aktívneho servera obsahuje informácie o zóne a hostiteľovi vrátane vlastností zóny, napríklad informácie o spustení oprávnenia (SOA - start of authority), vlastnosti hostiteľa alebo informácie o výmene pošty (MX), ktoré môžu byť užitočné pri riešení problémov.

Systém DNS (Domain Name System) vám umožňuje zobraziť výpis autoritatívnych údajov, údajov vo vyrovnávacej pamäti a rád pre inštanciu servera. Výpis pamäte zahŕňa informácie zo všetkých primárnych a sekundárnych zón servera (zóny dopredného a spätného mapovania), ako aj informácie, ktoré server získal z dotazov.

Výpis z databázy aktívneho servera môžete zobraziť pomocou programu Navigátor iSeries. Ak potrebujete uložiť kópiu súborov, názov súboru s výpisom z databázy je NAMED_DUMP.DB vo vašej adresárovej ceste iSeries: **Integrovaný súborový systém/Root/QIBM/UserData/OS400/DNS/<inštancia servera>**, kde ″<inštancia servera>″ je názov inštancie servera DNS. Bližšie informácie o databáze aktívneho servera nájdete v téme online pomoci DNS **Pochopenie výpisu z pamäte databázy servera DNS**.

Ak chcete mať prístup do výpisu z pamäte databázy servera, postupujte takto:

1. V programe Navigátor iSeries rozviňte **váš server iSeries → Sieť → Servery → DNS**.
2. V pravej časti kliknite pravým tlačidlom myši na **your DNS server** a vyberte **Configuration**.
3. V okne konfigurácie DNS vyberte **Zobraziť → Databáza aktívneho servera**.

Udržiavanie konfiguračných súborov systému DNS
Táto téma vám pomôže porozumieť súborom používaným systémom DNS a pokynom na ich zálohovanie a udržiavanie.

Na vytvorenie a manažovanie inštancií servera DNS vo vašom serveri iSeries môžete použiť DNS i5/OS. Konfiguračné súbory systému DNS manažuje program Navigátor iSeries. Súbory by ste nemali upravovať manuálne. Na vytvorenie, zmenu alebo vymazanie konfiguračných súborov DNS vždy používajte program Navigátor iSeries. Konfiguračné súbory DNS sú uložené v cestách integrovaného súborového systému uvedených nižšie.

Poznámka: Štruktúra súborov nižšie platí pre DNS spustené v prostredí BIND 8. Ak používate DNS na báze BIND 4.9.3, pozrite si dokument Zálohovanie konfiguračných súborov DNS a udržiavanie protokolových súborov v téme Informačného centra DNS pre verziu 4, vydanie 5.

Súbory v nasledujúcej tabuľke sú uvedené v zobrazenej hierarchii ciest. Súbory s ikonou uloženia  by sa mali zálohovať s cieľom chrániť údaje. Súbory s ikonou vymazania  by sa mali pravidelne vymazávať.

Názov	Ikona	Opis
QIBM/UserData/OS400/DNS/		Adresár počiatočného bodu pre DNS.

Názov	Ikona	Opis
ATTRIBUTES		DNS používa tento súbor aby určil, ktorú verziu BIND používate.
QIBM/UserData/OS400/DNS/ <inštancia-n>/		Adresár počiatočného bodu pre inštanciu DNS.
ATTRIBUTES		Konfiguračné atribúty používané systémom DNS iSeries.
NAMED.CONF		Tento súbor obsahuje konfiguračné údaje, ktoré povedia serveru, ktoré špecifické zóny riadi, kde sa nachádzajú zónové súbory, ktoré zóny možno dynamicky aktualizovať, kde sa nachádzajú jeho zasielacie servery a nastavenie ostatných volieb.
BOOT.AS400BIND4		Konfigurácia servera BIND 4.9.3 a súbor politiky, ktorý sa konvertuje do súboru BIND 8 NAMED.CONF pre túto inštanciu. Tento súbor sa vytvorí, ak migrujete server BIND 4.9.3 na BIND 8 a slúži ako záloha na migráciu, a ak server BIND 8 riadne funguje, možno ho vymazať.
NAMED.CA		Zoznam koreňových serverov pre túto inštanciu servera.
NAMED_DUMP.DB		Vytvorený výpis údajov z pamäte servera pre aktívnu databázu servera.
NAMED.STATS		Štatistika servera.
NAMED.PID		Udržiava ID procesu spusteného servera. Tento súbor sa vytvorí pri každom spustení servera DNS. Používa sa pre funkcie servera Database, Statistics a Update. Nevymazávajte ani neupravujte tento súbor.
QUERYLOG		Prijatý protokol dotazov servera DNS. Tento súbor sa vytvára, keď je aktívny protokol servera DNS. Ak je tento súbor aktívny, zväčšuje sa a mal by sa pravidelne vymazávať.
<*zone-name-a*>.DB		Súbor zóny pre určitú doménu, ktorá má byť obsluhovaná týmto serverom. Obsahuje všetky zdrojové záznamy pre túto zónu.
<*zone-name-b*>.DB		Súbor zóny pre určitú doménu, ktorá má byť obsluhovaná týmto serverom. Obsahuje všetky zdrojové záznamy pre túto zónu. Každá zóna má samostatný súbor .DB.

Názov	Ikona	Opis
.ixfr.		Prírastkové súbory zónového prenosu (IXFR). Sekundárne servery používajú tieto súbory na zavedenie len tých údajov, ktoré sa zmenili od posledného prenosu zóny. Pri vykonávaní aktualizácií sa bude počet súborov IXFR zvyšovať. Staršie súbory IXFR by ste mali pravidelne vymazávať. Ponechané súbory vytvorené počas jedného alebo dvoch dní umožnia väčšine sekundárnych serverov ešte stále zavádzať IXFR. Ak vymažete všetky súbory, sekundárny server požiada o úplný prenos (AXFR).
TMP		Adresár používaný inštanciou servera na vytvorenie dočasných pracovných súborov.
QIBM/UserData/OS400/DNS/TMP		Dočasný adresár používaný programom QTOBH2N na vytvorenie súborov z výpisu tabuľky hostiteľov pre neskorší import programom Navigátor iSeries.
QIBM/UserData/OS400/DNS/_DYN/		Adresár, ktorý udržiava súbory požadované na dynamické aktualizácie.
<*key_id-name-x*>._KID		Súbor obsahujúci príkaz kľúča BIND 8 pre key_id s názvom <*key_id-name-x*>.
<*key_id-name-x*>._DUK.<*zone-name-a*>		Kľúč pre dynamickú aktuailzáciu, vyžadovaný na inicializáciu požiadavky o dynamickú aktualizáciu pre <*zone-name-a*> pomocou kľúča <*key_id-name-x*>.
<*key_id-name-y*>._KID		Súbor obsahujúci príkaz kľúča BIND 8 pre key_id s názvom <*key_id-name-y*>.
<*key_id-name-y*>._DUK.<*zone-name-a*>		Kľúč pre dynamickú aktuailzáciu, vyžadovaný na inicializáciu požiadavky o dynamickú aktualizáciu pre <*zone-name-a*> pomocou kľúča <*key_id-name-y*>.
<*key_id-name-y*>._DUK.<*zone-name-b*>		Kľúč pre dynamickú aktuailzáciu, vyžadovaný na inicializáciu požiadavky o dynamickú aktualizáciu pre <*zone-name-b*> pomocou kľúča <*key_id-name-y*>.

Súvisiace koncepty

“Určenie oprávnení systému DNS” na strane 20
Pre administrátora DNS existujú špeciálne požiadavky na oprávnenia. Je potrebné zvážiť aj bezpečnostné aspekty autorizácie.

“Pristupovať k štatistikám servera DNS” na strane 28
Nástroje výpisu z pamäte databázy a štatistiky pomáhajú pri zisťovaní a riadení výkonu servera.

Súvisiace úlohy

“Konfigurovať názvové servery” na strane 23
Systém DNS vám umožňuje vytvoriť viaceré inštancie názvového servera. Táto téma poskytuje pokyny na konfiguráciu názvového servera.

Rozšírené vlastnosti systému DNS

Táto téma vysvetľuje spôsob použitia rozšírených vlastností systému DNS skúsenými administrátormi na ľahšie manažovanie servera DNS.

DNS v programe Navigátor iSeries poskytuje rozhranie na konfiguráciu a manažovanie vášho servera DNS. Nasledujúce úlohy predstavujú skratky pre administrátorov, ktorí poznajú grafické rozhranie systému iSeries. Tieto úlohy poskytujú rýchle metódy na zmenu stavu servera a jeho atribútov pre viaceré inštancie naraz.

Súvisiace úlohy

"Zmena nastavení ladenia systému DNS" na strane 35
Funkcia ladenia systému DNS môže poskytnúť informácie, ktoré vám pomôžu určiť a opraviť problémy so serverom DNS.

Zmeniť atribúty systému DNS

Nastavenia DNS môžete zmeniť, ak rozhranie DSN nepovoľuje zmenu úrovní automatického spustenia a ladenia pre všetky inštancie serverov súčasne.

Na zmenu týchto nastavení pre jednotlivé inštancie servera DNS alebo pre všetky inštancie naraz môžete použiť znakové rozhranie. Ak chcete použiť CHGDNSA, postupujte takto:

1. Na príkazovom riadku zadajte CHGDNSA a stlačte kláves F4.
2. Na stránke Zmeniť atribúty servera DNS (CHGDNSA) zadajte názov jednej inštancie servera alebo *ALL a stlačte kláves Enter.

   Zobrazia sa dostupné voľby atribútov servera:

   ```
   Automatické
   spustenie servera.. . . . . *SAME *YES, *NO, *SAME
   Úroveň ladenia. . . . . *SAME 0-11, *SAME, *DFT
   ```

3. **Autostart** Ak chcete uviesť, aby sa vybraté servery DNS spúšťali automaticky, keď sa spúšťa TCP/IP, napíšte *YES. Ak nechcete, aby sa server spustil pri spustení TCP/IP, napíšte *NO. Ak chcete ponechať aktuálne nastavenia atribútu, zadajte *SAME.

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

   Po zadaní všetkých preferencií nastavte atribúty DNS stlačením klávesu Enter.

Spustenie alebo zastavenie serverov DNS

Ak rozhranie DNS nepovoľuje spustenie alebo zastavenie viacerých inštancií servera súčasne, môžete zmeniť nastavenia.

Ak chcete zmeniť tieto nastavenia pre viacero inštancií naraz, môžete použiť znakové rozhranie. Ak chcete použiť znakové rozhranie na spustenie všetkých inštancií servera DNS naraz, napíšte do príkazového riadka STRTCPSVR SERVER(*DNS) DNSSVR(*ALL). Ak chcete naraz zastaviť všetky servery DNS, napíšte do príkazového riadka ENDTCPSVR SERVER(*DNS) DNSSVR(*ALL).

Zmeniť úroveň ladenia

Zmena úrovne ladenia je výhodná pre administrátorov veľkých zón, ktorí nechcú prijať veľké množstvo údajov z ladenia pri spustení servera a načítaní zónových údajov.

Systém DNS v rozhraní programu Navigátor iSeries vám neumožňuje zmeniť úroveň ladenia, pokiaľ je spustený server. Ak však chcete zmeniť úroveň ladenia počas chodu servera, môžete použiť znakové rozhranie. Ak chcete zmeniť úroveň ladenia pomocou znakového rozhrania, vykonajte tieto kroky a nahraďte <inštancia> názvom inštancie servera:

1. Na príkazovom riadku zadajte ADDLIBLE QDNS a stlačte kláves Enter.
2. Zmeňte úroveň ladenia:
   - Ak chcete zapnúť ladenie alebo zvýšiť úroveň ladenia o 1, zadajte CALL QTOBDRVS ('BUMP' '<inštancia>') a stlačte kláves Enter.

- Ak chcete vypnúť ladenie, zadajte CALL QTOBDRVS ('OFF' '<inštancia>') a stlačte kláves Enter.

Riešenie problémov so systémom DNS

Táto téma vysvetľuje nastavenia protokolovania a ladenia systému DNS, ktoré vám môžu pomôcť vyriešiť problémy so serverom DNS.

DNS funguje v mnohom rovnako ako ostatné aplikácie a funkcie TCP/IP. Podobne ako aplikácie FTP a SMTP sa úlohy DNS spúšťajú pod podsystémom QSYSWRK a vytvárajú protokoly úloh pod užívateľským profilom QTCP s informáciami priradenými k úlohe DNS. Ak úloha DNS skončí, môžete na stanovenie príčiny ukončenia použiť protokoly úlohy. Ak server DNS nevracia očakávané odpovede, protokol úlohy môže obsahovať informácie, ktoré vám pomôžu s analýzou problému.

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

Identifikovať úlohy

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

- Ak používate BIND 4.9.3, názov úlohy servera bude QTOBDNS. Viac informácií o ladení servera DNS 4.9.3 nájdete v dokumente *Riešenie problémov so servermi DNS*.
- Ak spúšťate servery založené na BIND 8, pre každú spúšťanú inštanciu bude existovať samostatná úloha. Názov úlohy bude pozostávať z 5 stálych znakov (QTOBD), za ktorými bude nasledovať názov inštancie. Napríklad, ak máte dve inštancie INST1 a INST2, názvy ich úloh budú QTOBDINST1 a QTOBDINST2.

  Súvisiace koncepty

  "Protokolovanie správ servera DNS"
  Systém DNS poskytuje množstvo volieb protokolovania, ktoré môžete prispôsobiť pri hľadaní zdroja problému. Protokolovanie poskytuje flexibilitu tým, že ponúka rôzne úrovne závažnosti, kategórie správ a výstupné súbory s cieľom jemne dolaďovať protokolovanie pri vyhľadávaní problémov.

  Súvisiace úlohy

  "Zmena nastavení ladenia systému DNS" na strane 35
  Funkcia ladenia systému DNS môže poskytnúť informácie, ktoré vám pomôžu určiť a opraviť problémy so serverom DNS.

Protokolovanie správ servera DNS

Systém DNS poskytuje množstvo volieb protokolovania, ktoré môžete prispôsobiť pri hľadaní zdroja problému. Protokolovanie poskytuje flexibilitu tým, že ponúka rôzne úrovne závažnosti, kategórie správ a výstupné súbory s cieľom jemne dolaďovať protokolovanie pri vyhľadávaní problémov.

BIND 8 ponúka niekoľko nových volieb protokolovania. Môžete uviesť aké typy správ sa protokolujú, kam sa každý typ správy zasiela a aká závažnosť daného typu správy sa má protokolovať. Vo všeobecnosti sú vhodné predvolené nastavenia protokolovania. Ak ich chcete zmeniť, pozrite si iné zdroje dokumentácie BIND 8, kde nájdete viac informácií o protokolovaní.

Protokolovacie kanály

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

- **Kanály súborov**

  Správy protokolované do kanálov súborov sa zasielajú do súboru. Predvolenými kanálmi súboru sú as400_debug a as400_QPRINT. Štandardne sa správy o ladení protokolujú do kanála as400_debug, čo je súbor NAMED.RUN, ale

do tohto súboru môžete zadať aj zasielanie iných kategórií správ. Kategórie správ protokolované do as400_QPRINT sa zasielajú do spoolového súboru QPRINT pre užívateľský profil QTCP. Okrem poskytovaných predvolených kanálov si môžete vytvoriť aj svoje vlastné kanály súborov.

- **Kanály syslog**

  Správy zaprotokolované do tohto kanála sa zasielajú do protokolu úloh serverov. Predvoleným kanálom syslog je as400_joblog. Zaprotokolované správy smerované do tohto kanála sa zasielajú do protokolu úlohy inštancie servera DNS.

- **Nulové kanály**

  Všetky správy zaprotokolované do nulového kanála budú vymazané. Predvoleným nulovým kanálom je as400_null. Ak nechcete, aby sa správy objavili v niektorom protokolovom súbore, môžete kategórie nasmerovať do nulového kanála.

Kategórie správ

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

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

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

Závažnosť správy

Kanály vám umožňujú filtráciu podľa závažnosti správy. Pre každý kanál môžete uviesť úroveň závažnosti, pri ktorej sa správy protokolujú. K dispozícii sú nasledujúce úrovne závažnosti:

- Critical
- Error
- Warning
- Notice
- Info
- Debug (uveďte úroveň ladenia 0-11)
- Dynamic (zdediť úroveň ladenia pri spustení servera)

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

Zmeniť nastavenia protokolovania

Ak chcete vstupovať do volieb protokolovania, postupujte takto:

1. V programe Navigátor iSeries rozviňte **váš server iSeries → Sieť → Servery → DNS**.
2. V pravej časti kliknite pravým tlačidlom myši na **your DNS server** a vyberte **Configuration**.
3. V okne konfigurácie DNS pravým tlačidlom myši kliknite na **server DNS** a vyberte **Vlastnosti**.

4. V okne Vlastnosti servera vyberte záložku **Kanály**, ak chcete vytvoriť nový kanál súboru alebo vlastnosti kanála, ako napríklad závažnosť správ protokolovaných do kanálov.
5. V okne Vlastnosti servera vyberte záložku **Protokolovanie** a zadajte kategórie správ, ktoré chcete protokolovať pre každý kanál.

Tip pre riešenie problémov

Predvolená úroveň závažnosti kanála as400_joblog je nastavená na Error. Toto nastavenie sa používa na zníženie objemu informačných a upozorňujúcich správ, ktoré by v opačnom prípade znížili výkon. Ak ste zaznamenali problémy, ale protokol úlohy neoznamuje zdroj problému, musíte pravdepodobne zmeniť úroveň závažnosti. Ak chcete vstúpiť na stránku Channels a zmeniť úroveň závažnosti pre kanál as400_joblog na Warning, Notice alebo Info s cieľom vidieť viac protokolovacích údajov, postupujte podľa vyššie uvedenej procedúry. Po vyriešení problému vynulujte úroveň závažnosti na hodnotu Chyba. Týmto znížite počet správ v protokole úlohy.

Súvisiace úlohy

"Riešenie problémov so systémom DNS" na strane 33
Táto téma vysvetľuje nastavenia protokolovania a ladenia systému DNS, ktoré vám môžu pomôcť vyriešiť problémy so serverom DNS.

Zmena nastavení ladenia systému DNS

Funkcia ladenia systému DNS môže poskytnúť informácie, ktoré vám pomôžu určiť a opraviť problémy so serverom DNS.

DNS ponúka 12 úrovní riadenia ladenia. Protokolovanie väčšinou predstavuje jednoduchú metódu hľadania problémov, v niektorých prípadoch je však nevyhnutné ladenie. Za normálnych podmienok je ladenie vypnuté (hodnota = 0). Pri pokuse o odstránenie problémov sa odporúča použiť najprv protokolovanie.

Platné hodnoty ladenia sú v rozsahu 0 až 11. Váš predstaviteľ servisu IBM vám môže pomôcť určiť vhodnú hodnotu ladenia pre diagnostiku vášho problému so systémom DNS. Hodnoty 1 a vyššie zapisujú informácie z ladenia do súboru NAMED.RUN v adresárovej ceste iSeries: **Integrovaný súborový systém/Root/QIBM/UserData/OS400/DNS/<inštancia servera>**, kde ″<inštancia servera>″ je názov inštancie servera DNS. Pokiaľ je úroveň ladenia nastavená na hodnotu 1 alebo vyššiu, súbor NAMED.RUN ďalej rastie a server DNS je naďalej v chode. Odporúča sa z času na čas vymazať tento súbor, aby nezaberal príliš veľa miesta. Na zadanie preferencií pre maximálnu veľkosť a počet verzií súboru NAMED.RUN môžete použiť aj stránku **Server Properties** - **Channels**.

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

1. V programe Navigátor iSeries rozviňte **váš server iSeries → Sieť → Servery → DNS**.
2. V pravej časti kliknite pravým tlačidlom myši na **your DNS server** a vyberte **Configuration**.
3. V okne konfigurácie DNS pravým tlačidlom myši kliknite na server DNS a vyberte **Vlastnosti**.
4. Na strane Vlastnosti servera - Všeobecné zadajte úroveň ladenia servera pri spustení.
5. Ak je server spustený, zastavte a reštartujte ho.

Poznámka: Zmeny úrovne ladenia nenadobudnú účinnosť, ak je server spustený. Úroveň ladenia, ktorá je tu nastavená, sa použije pri ďalšom úplnom reštarte servera. Ak potrebujete zmeniť úroveň ladenia a server je spustený, pozrite si Rozšírené vlastnosti DNS.

Súvisiace koncepty

"Rozšírené vlastnosti systému DNS" na strane 32
Táto téma vysvetľuje spôsob použitia rozšírených vlastností systému DNS skúsenými administrátormi na ľahšie manažovanie servera DNS.

Súvisiace úlohy

“Riešenie problémov so systémom DNS” na strane 33
Táto téma vysvetľuje nastavenia protokolovania a ladenia systému DNS, ktoré vám môžu pomôcť vyriešiť problémy so serverom DNS.

Súvisiace informácie pre systém DNS

Nižšie sú uvedené Červené knihy spoločnosti IBM (vo formáte PDF) a webové lokality obsahujúce informácie súvisiace s témou DNS. Každý dokument PDF môžete zobraziť alebo vytlačiť.

Červené knihy spoločnosti IBM

AS/400 Automatická konfigurácia TCP/IP: Podpora DNS a DHCP (5181 KB)

Táto červená kniha opisuje podporu serverov DNS a DHCP v systéme i5/OS. Informácie v tejto červenej knihe vám pomôžu nainštalovať, prispôsobiť, nakonfigurovať a riešiť problémy so servermi DNS a DHCP prostredníctvom príkladov.

Webové lokality

- *DNS and BIND*, tretie vydanie. Paul Albitz and Cricket Liu. Vydané vo vydavateľstve O’Reilly and Associates,Inc. Sebastopol, California, 1998. ISBN číslo: 1-56592-512-2. Toto je najdôležitejší zdroj na DNS.
- Webová lokalita Internet Software Consortium obsahuje novinky, odkazy a ďalšie zdroje pre systém BIND.
- Webová lokalita InterNIC udržiava adresár všetkých registrátorov názvov domén, ktorí majú oprávnenie od organizácie ICANN (Internet Corporation for Assigned Names and Numbers).
- Webová lokalita DNS Resources Directory poskytuje referenčný materiál pre systém DNS a obsahuje odkazy na množstvo ďalších zdrojov pre DNS, vrátane diskusných skupín. Okrem toho poskytuje zoznam dokumentov RFC súvisiacich s DNS .

Uloženie súborov PDF

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

1. Pravým tlačidlom myši kliknite na dokument PDF vo vašom prehliadači (pravým tlačidlom myši kliknite na odkaz vyššie).
2. Kliknite na voľbu, ktorá ukladá súbor PDF lokálne.
3. Prejdite do adresára, kde chcete súbor PDF uložiť.
4. Kliknite na **Save**.

Prevzatie programu Adobe Reader

Na zobrazenie alebo tlač súborov PDF potrebujete program Adobe Reader. Kópiu si môžete prevziať z Webovej lokality Adobe (www.adobe.com/products/acrobat/readstep.html) .

Príloha. Poznámky

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

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

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

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

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

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

Nasledujúci odsek sa netýka Veľkej Británie ani žiadnej inej krajiny, kde sú takéto vyhlásenia nezlučiteľné s miestnym zákonom: SPOLOČNOSŤ INTERNATIONAL BUSINESS MACHINES POSKYTUJE TÚTO PUBLIKÁCIU "TAK AKO JE", BEZ AKÝCHKOĽVEK VÝSLOVNÝCH ALEBO MLČKY PREDPOKLADANÝCH ZÁRUK, VRÁTANE, ALE BEZ OBMEDZENIA NA ZÁRUKY NEPORUŠENIA PRÁV, PREDAJNOSTI ALEBO VHODNOSTI NA KONKRÉTNY ÚČEL. Niektoré štáty nepovoľujú odmietnutie vyjadrených alebo predpokladaných záruk pri určitých transakciách, preto sa vás toto vyhlásenie nemusí týkať.

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

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

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

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

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N

Rochester, MN 55901
U.S.A.

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

Licenčný program, opisovaný v týchto informáciách, a všetky preň dostupné licenčné materiály poskytuje IBM podľa podmienok zmluvy IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code, alebo ľubovoľnej ekvivalentnej zmluvy medzi nami.

Všetky údaje o výkone, uvádzané v tomto dokumente boli získané v riadenom prostredí. Výsledky získané v iných prevádzkových prostrediach sa môžu podstatne odlišovať. Niektoré merania boli vykonané v systémoch vývojovej úrovne a nie je žiadna záruka, že tieto merania budú rovnaké vo všeobecne dostupných systémoch. Okrem toho, niektoré výsledky boli odhadnuté extrapoláciou. Skutočné výsledky sa môžu odlišovať. Užívatelia tohto dokumentu by si mali overiť použiteľnosť týchto údajov pre svoje špecifické prostredie.

Informácie o produktoch iných ako od IBM boli získané od poskytovateľov týchto produktov, z ich uverejnených oznámení alebo z iných, verejne dostupných zdrojov. Spoločnosť IBM tieto produkty netestovala a nemôže potvrdiť presnosť ich výkonu, kompatibilitu ani iné parametre týkajúce sa produktov nepochádzajúcich od IBM. Otázky k schopnostiam produktov iných ako od IBM by ste mali adresovať poskytovateľom týchto produktov.

Všetky vyhlásenia týkajúce sa budúceho smerovania alebo úmyslov IBM sú predmetom zmeny alebo zrušenia bez ohlásenia a vyjadrujú len zámery a ciele.

Tieto informácie obsahujú príklady údajov a hlásení používaných v každodenných firemných operáciách. Kvôli ich čo najlepšej ilustrácii obsahujú tieto príklady mená osôb, názvy spoločností, pobočiek a produktov. Všetky tieto mená a názvy sú vymyslené a akákoľvek podobnosť s menami, názvami a adresami používanými skutočnými osobami a spoločnosťami je čisto náhodná.

LICENCIA NA AUTORSKÉ PRÁVA:

Tieto informácie obsahujú vzorové aplikačné programy v zdrojovom kóde, ktoré ilustrujú programovacie techniky v rôznych platformách. Tieto vzorové programy môžete kopírovať, upravovať a distribuovať v ľubovoľnej forme bez poplatku pre IBM, za účelom vývoja, používania, predaja alebo distribúcie aplikačných programov, vyhovujúcich aplikačnému programovému rozhraniu pre operačnú platformu, pre ktorú sú tieto programy napísané. Tieto príklady neboli dôkladne testované vo všetkých podmienkach. IBM preto nemôže garantovať ani implikovať spoľahlivosť, prevádzkyschopnosť ani funkčnosť týchto programov.

Každá kópia alebo časť týchto vzorových programov alebo odvodená práca musí obsahovať túto poznámku o autorských právach:

© (názov vašej spoločnosti) (rok). Časti tohto kódu sú odvodené od vzorových programov Corp. © Copyright IBM Corp. _Uveďte rok alebo roky_. Všetky práva vyhradené.

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

Informácie o programovom rozhraní

Táto publikácia, DNS, dokumentuje programové rozhrania, ktoré dovoľujú zákazníkovi písať programy na získanie služieb systémov IBM i5/OS.

Ochranné známky

Nasledujúce výrazy sú ochrannými známkami spoločnosti International Business Machines v Spojených štátoch alebo iných krajinách:

| AFS
| AS/400
| e(logo)server
| eServer
| i5/OS
| IBMIBM (logo)
| iSeriesOS/400
| Redbooks

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

Pojmy a podmienky

Oprávnenia na používanie týchto publikácií sú predmetom nasledujúcich pojmov a podmienok.

Osobné použitie: Tieto publikácie môžete reprodukovať pre svoje osobné, nekomerčné použitie za podmienky zachovania všetkých informácií o autorských právach. Bez výslovného povolenia autora ich nemôžete distribuovať, zobrazovať ani odvádzať práce z týchto publikácií ani žiadnej ich časti.

Komerčné použitie: Tieto publikácie môžete reprodukovať, distribuovať a zobrazovať výlučne vo vašej spoločnosti za podmienky zachovania všetkých informácií o autorských právach. Bez výslovného povolenia od autora nemôžete odvádzať práce z týchto publikácií ani reprodukovať, distribuovať a zobrazovať tieto publikácie ani žiadne ich časti.

S výnimkou ako je uvedené v týchto podmienkach, na publikácie ľubovoľné informácie, údaje, softvér alebo iné tu obsiahnuté intelektuálne vlastníctvo nemáte žiadne oprávnenia, licencie ani práva, vyjadrené ani implikované.

Spoločnosť IBM si vyhradzuje právo odobrať tu uvedené oprávnenia vždy, podľa vlastného uváženia, keď použitie týchto publikácií škodí autorovi, alebo ak spoločnosť IBM, že pokyny hore nie sú striktne dodržiavané.

Tieto informácie nemožno sťahovať, exportovať, ani reexportovať s výnimkou prípadov, kedy je takéto stiahnutie, export alebo reexport plne v súlade so všetkými platnými zákonmi a predpismi vrátane zákonov a predpisov Spojených štátov týkajúcich sa exportu.

IBM NERUČÍ ZA OBSAH TÝCHTO PUBLIKÁCIÍ. PUBLIKÁCIE SÚ POSKYTNUTÉ ″TAK AKO SÚ″ BEZ ZÁRUKY AKÉHOKOĽVEK DRUHU, VYJADRENEJ ALEBO IMPLIKOVANEJ, VRÁTANE (ALE NEOBMEDZENE) IMPLIKOVANÝCH ZÁRUK PREDAJNOSTI, NEPOŠKODENIA A VHODNOSTI NA KONKRÉTNY ÚČEL.

Vytlačené v USA