System i

Siete
Domain Name System

Verzia 6 vydanie 1

System i

Siete
Domain Name System

Verzia 6 vydanie 1

Poznámka

Pred použitím týchto informácií a nimi podporovaného produktu si prečítajte informácie v časti “Poznámky”, na strane 41.

Toto vydanie sa vzťahuje na verziu 6, vydanie 1, modifikáciu 0 produktu IBM i5/OS (produktové číslo 5761-SS1) a na všetky následné vydania a modifikácie, až kým to nebude v nových vydaniach určené inak. Táto verzia nebeží na všetkých modeloch počítačov typu RISC a ani na modeloch typu CISC.

Obsah

Systém DNS

DNS (Domain Name System) je systém distribuovaných databáz určený na správu názvov hostiteľov a im priradených IP adries.

Vďaka serveru DNS môžu ľudia nájsť hostiteľa pomocou jednoduchých názvov, ako napríklad www.jkltoys.com, namiesto toho, aby museli použiť jeho IP adresu, napríklad 192.168.12.88 v protokole IPv4 alebo 2001:D88::1 v protokole IPv6. Jediný server môže byť zodpovedný len za znalosť názvov hostiteľov a IP adries malej časti zóny, zatiaľ čo servery DNS môžu vďaka vzájomnej spolupráci mapovať všetky názvy domén s ich IP adresami. Spolupracujúce servery DNS tak umožňujú komunikáciu počítačov prostredníctvom internetu.

V prípade IBM i5/OS Verzia 6 Vydanie 1 (V6R1) sú služby DNS založené na implementácii DNS podľa priemyselných štandardov známej ako BIND (Berkeley Internet Name Domain) verzie 9. V predošlých vydaniach systému i5/OS boli služby DNS založené na BIND verzia 8.2.5. Ak chcete využívať novú verziu servera DNS založenej na BIND 9, musia byť na vašom modeli IBM System i nainštalované dve voľby systému i5/OS, menovite voľba 31, ktorou je server DNS a voľba 33, ktorou je prostredie PASE (Portable Application Solutions Environment). Počnúc i5/OS V6R1 sú BIND 4 a 8 z bezpečnostných dôvodov nahradené verziou BIND 9. Preto je vyžadovaná migrácia vášho servera DNS na BIND 9.

Čo je nové vo V6R1

Prečítajte si o nových alebo významne zmenených informáciách v súhrne tém DNS (Domain Name System).

BIND 9

BIND (Berkeley Internet Name Domain) verzia 9 uvedený v tomto vydaní poskytuje rozličné funkcie, ktoré vylepšujú výkonnosť vášho servera DNS (Domain Name System). Podporuje napríklad vyhľadávania názov-adresa a adresa-názov vo všetkých aktuálne zadefinovaných formátoch protokolu IPv6. Využíva príkaz *view*, ktorý umožňuje inštancii jediného servera DNS odpovedať rozdielne na dotazy v závislosti na tom, odkiaľ dotaz prichádza, napríklad či prichádza z internetu alebo z intranetu. Navyše využíva žurnálové súbory, ktoré podržia dynamické aktualizácie zóny.

Predošlé verzie BIND 4.9.3 a BIND 8.2.5 už viac nie sú podporované, ale nie je nutné ich migrovať na verziu BIND 9.

Nové konfiguračné príkazy

Boli pridané nasledujúce konfiguračné príkazy, ktoré vám uľahčia riadenie týchto konfiguračných súborov DNS vo vašom systéme.

CRTRNDCCFG (Create RNDC Configuration)
Príkaz CRTRNDCCFG (RNDC Configuration Utility) je využívaný pri generovaní konfiguračných súborov RNDC. Slúži ako pohodlná alternatíva voči napísaniu súboru rndc.conf a s ním súvisiacich ovládačov a kľúčových príkazov v súbore named.conf.

CHKDNSCFG (DNS Configuration Utility)
Príkaz CHKDNSCFG (DNS Configuration Utility) kontroluje syntax konfiguračného súboru s názvom named.conf. Neposkytuje však podporu pri kontrole sémantiky tohto konfiguračného súboru.

CHKDNSZNE (DNS Zone Utility)
Príkaz CHKDNSZNE (DNS Zone Utility) kontroluje syntax a integritu súboru zónových údajov. Je užitočné kontrolovať vaše súbory zónových údajov predtým, než ich pridáte na váš server DNS.

Nové pomocné programy pre dotazy a aktualizácie

Boli pridané nasledujúce pomocné programy pre dotazy a aktualizácie, ktoré vylepšujú možnosti riadenia vášho servera DNS.

DIG (Domain Information Groper)
Nástroj DIG, zameraný na dotazy, môžete využiť pri opakovanom získavaní informácií DNS o hostiteľoch, doménach a ostatných serveroch DNS v závislosti na odpovediach servera DNS. S jeho pomocou si predtým, než budete konfigurovať využitie vášho systému, môžete overiť, či váš server DNS správne reaguje.

HOST (Start HOST Query)
Príkaz HOST (Start HOST Query) slúži na vyhľadávania v DNS. Konvertuje názvy domén na IP adresy (buď na IPv4 alebo na IPv6) a naopak.

NSUPDATE (Dynamic Update Utility)
Príkaz NSUPDATE (Dynamic Update Utility) odovzdáva požiadavky typu Dynamic DNS Update tak, ako sú zadefinované v štandarde RFC (Request for Comments) 2136 odosielania požiadaviek na server DNS. Umožňuje pridať, alebo odstrániť zdrojové záznamy zo zóny, zatiaľ čo je server DNS spustený. Vďaka nemu nemusíte záznamy aktualizovať manuálnou úpravou zónového súboru. Jediná aktualizačná požiadavka môže obsahovať požiadavky na pridanie alebo odstránenie viac než jedného zdrojového záznamu, ale zdrojové záznamy ktoré sú dynamicky pridávané, alebo odstraňované príkazom NSUPDATE, by mali byť v tej istej zóne.

RNDC (Remote Name Daemon Control)
Príkaz RNDC (Remote Name Daemon Control) umožňuje administrátorovi systému riadiť prevádzku názvového servera. Načítava konfiguračný súbor s názvom *rndc.conf* a na jeho základe určuje, ako sa obracať na názvový server a rozhoduje, aký algoritmus a kľúč použiť. Ak nenájde súbor rndc.conf, potom zvyčajne použije počas inštalácie vytvorený súbor rndc-key._KID, ktorý automaticky určí prístup prostredníctvom návratového rozhrania.

Ako zistíte čo je nové alebo čo sa zmenilo

Aby ste mali jednoduchší prehľad v technických zmenách, sú v informačnom centre použité tieto označenia:

- Značka  , ktorá označuje, kde začínajú nové alebo zmenené informácie.
- Značka  , ktorá označuje, kde nové alebo zmenené informácie končia.

Nové alebo zmenené informácie v dokumentoch PDF sú na ľavom okraji zvýraznené lištou označujúcou revízie (|).

Súvisiaci odkaz

“Funkcie BIND 9” na strane 8
BIND 9 je podobný ako BIND 8, poskytuje však viacero funkcií, ktoré zvyšujú výkonnosť vášho servera DNS (Domain Name System), ako napríklad zobrazenia.

Súbor PDF k téme DNS (Domain Name System)

Môžete zobraziť alebo vytlačiť súbor PDF týchto informácií.

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. Kliknite pravým tlačidlom myši na odkaz na PDF vo vašom prehliadači.
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

Aby ste tieto dokumenty PDF mohli zobraziť, alebo tlačiť, musí byť vo vašom systéme nainštalovaný program Adobe Reader. Jeho bezplatnú kópiu si môžete stiahnuť na webových stránkach Adobe

(www.adobe.com/products/acrobat/readstep.html) .

Súvisiaci odkaz

"Súvisiace informácie pre systém DNS" na strane 40
informácie súvisiace so súhrnom tém DNS (Domain Name System) obsahujú publikácie IBM Redbooks, webové stránky a ostatné súhrny tém informačného centra. Ľubovoľný z týchto súborov PDF môžete zobraziť alebo vytlačiť.

Koncepty systému DNS

DNS je systém distribuovaných databáz, určený na manažovanie názvov hostiteľov a priradených adries IP. Vďaka systému DNS môžete nájsť hostiteľa pomocou jednoduchých názvov, ako napríklad www.jkltoys.com, namiesto toho, aby ste museli použiť jeho IP adresu, napríklad 192.168.12.88 v protokole IPv4 alebo 2001:D88::1 v protokole IPv6.

Jediný server môže byť zodpovedný len za znalosť názvov hostiteľov a IP adries malej časti zóny, zatiaľ čo servery DNS môžu vďaka vzájomnej spolupráci mapovať všetky názvy domén s ich IP adresami. Spolupracujúce servery DNS tak umožňujú komunikáciu počítačov prostredníctvom internetu.

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. Cesty, ktorými môže klient rozlíšiť dotazy, sú vysvetlené v téme Pochopenie dotazov DNS.

Pochopenie zón

Údaje servera DNS (Domain Name System) sú rozdelené do ľahšie ovládateľných skupín údajov nazývaných *zóny*. Každej z týchto skupín je priradený špecifický typ zóny.

Zóny obsahujú informácie o názve a IP adrese jednej alebo viacerých častí domény DNS. Server, ktorý obsahuje všetky informácie zóny, je autoritatívnym serverom domény, nazývaným *rodičovská zóna*. Niekedy má zmysel splnomocniť iný server DNS ako *dcérsku zónu*, teda aby odpovedal na dotazy DNS pre konkrétnu poddoménu. 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

Pomocou DNS v i5/OS môžete zadefinovať viacero typov zón, ktoré vám uľahčia riadenie údajov DNS:

Primárna zóna

Primárna zóna zavádza zónové údaje priamo zo súboru na hostiteľovi. Môže obsahovať podzónu alebo dcérsku zónu. Taktiež môže obsahovať zdrojové záznamy, ako napríklad záznamy hostiteľov, aliasov (CNAME), IP adries verzie IPv4 (A), IP adries verzie IPv6 (AAAA) alebo spätných smerníkov 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

Dcérska zóna 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 zavádza zónové údaje zo servera primárnej zóny alebo z iného sekundárneho servera. Udržiava úplnú kópiu zóny, pre ktorú je sekundárna.

Poznámka: V ďalšej dokumentácii k systému BIND sú sekundárne zóny niekedy označované ako *podriadené zóny*.

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”
Klienti DNS (Domain Name System) prekladajú požiadavky pomocou serverov DNS. Dotazy môžu prichádzať priamo od klienta alebo od aplikácie, ktorá je na klientovi spustená.

Súvisiace úlohy

“Konfigurácia zóny na názvovom serveri” na strane 28
Po konfigurácii inštancie servera DNS potrebujete nakonfigurovať zóny pre názvový server.

Súvisiaci odkaz

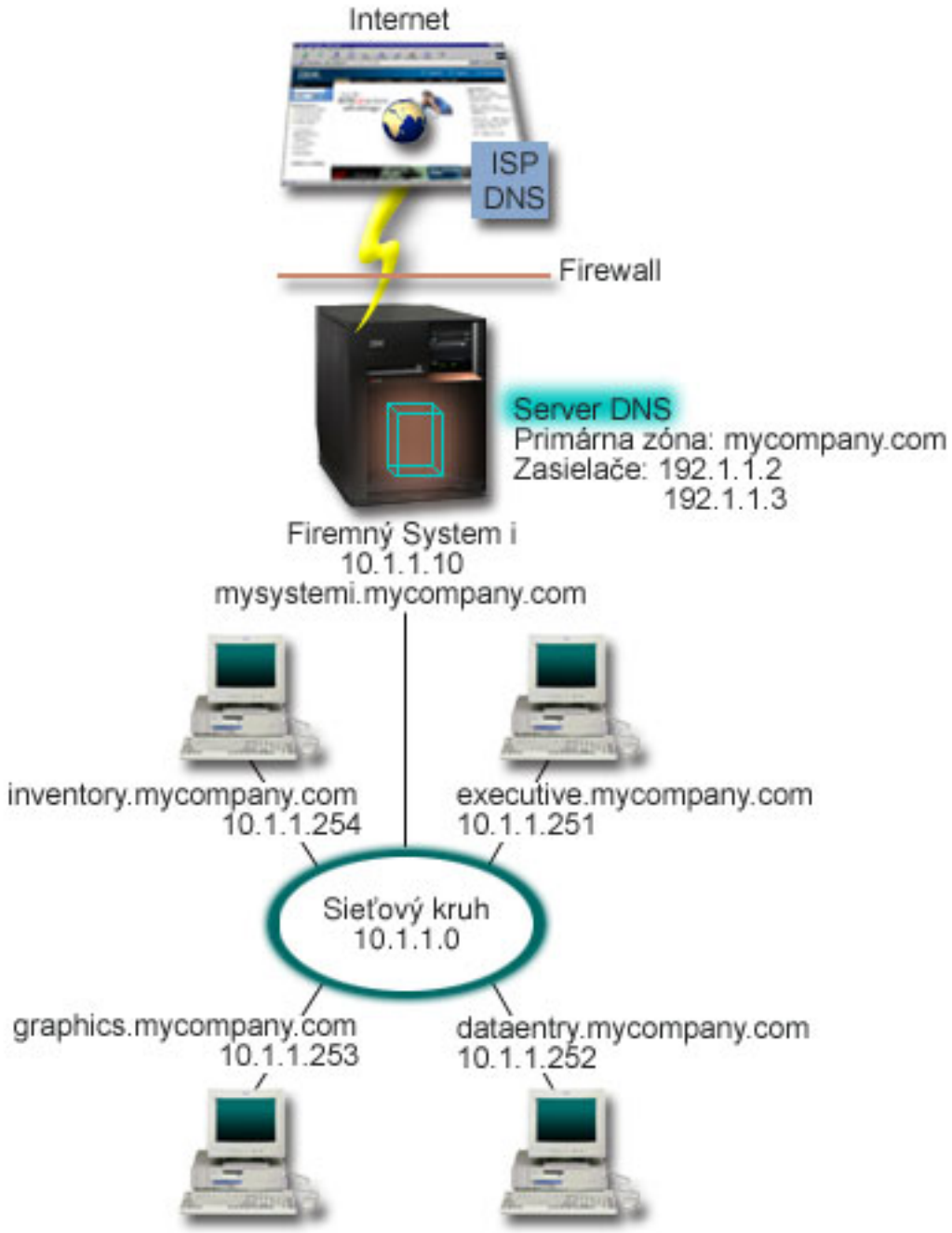
“Príklad: Jeden server DNS pre intranet” na strane 14
Tento príklad znázorňuje jednoduchú podsieť so serverom DNS pre interné použitie.

“Zdrojové záznamy systému DNS” na strane 9
Zdrojové záznamy sa používajú na ukladanie údajov o názvoch domén a IP adries. Pomocou Vyhľadávacej tabuľky zdrojových záznamov môžete získať prehľad o zdrojových záznamoch podporovaných operačným systémom i5/OS.

Pochopenie dotazov systému DNS

Klienti DNS (Domain Name System) prekladajú požiadavky pomocou serverov DNS. Dotazy môžu prichádzať priamo od klienta alebo od aplikácie, ktorá je na klientovi spustená.

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. Je možné postupovať dvoma cestami: *rekurziou* alebo *iteráciou*. Ak nastavenie servera DNS predpokladá využitie *rekurzie*, môže sa server v mene klienta, ktorý požiadavku odoslal, obrátiť na iné servery DNS s dotazom na plný preklad názvu, a potom odoslať odpoveď naspäť klientovi. Následne server, ktorý zadal požiadavku, dodatočne uloží odpoveď do svojej pamäte cache, aby ju bolo možné použiť pri ďalšom prijatí rovnakého

dotazu. Ak nastavenie servera DNS predpokladá použitie *iterácie*, môže sa samotný klient s dotazom na preklad názvu pokúsiť obrátiť na iné servery DNS. Počas tohto procesu klient v závislosti na odvolávkach v odpovediach serverov použije samostatné a dodatočné dotazy.

Súvisiaci odkaz

"Pochopenie zón" na strane 3
Údaje servera DNS (Domain Name System) sú rozdelené do ľahšie ovládateľných skupín údajov nazývaných *zóny*. Každej z týchto skupín je priradený špecifický typ zóny.

"Príklad: Jeden server DNS s prístupom do internetu" na strane 16
Tento príklad znázorňuje jednoduchú podsieť so serverom DNS pripojeným priamo do internetu.

Nastavenie domény systému DNS

Nastavenie domény DNS (Domain Name System) vyžaduje, aby ste mali zaregistrovaný názov vašej domény, ktorý nebude môcť využívať nikto iný.

DNS vám umožňuje obsluhovať názvy a adresy na 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 16
Tento príklad znázorňuje jednoduchú podsieť so serverom DNS pripojeným priamo do internetu.

Súvisiace informácie

Internet Network Information Center (InterNIC)

Dynamické aktualizácie

Server DNS (Domain Name System) i5/OS založený na systéme BIND 9 podporuje dynamické aktualizácie. Vďaka tomu môžu tomuto serveru DNS posielať aktualizácie vonkajšie zdroje, akým je napríklad server DHCP (Dynamic Host Configuration Protocol). Okrem toho môžete na vykonanie dynamických aktualizácií využívať aj klientske nástroje DNS, napríklad NSUPDATE (Dynamic Update Utility).

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 založené na systéme BIND 8 (alebo novší) však môžete nakonfigurovať tak, aby akceptovali požiadavky od ostatných zdrojov a aktualizovali zónové údaje dynamicky.

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.

Server DHCP môžete nakonfigurovať tak, aby v mene klienta aktualizoval buď záznamy mapovania adries (A v prípade protokolu IPv4 alebo AAAA v prípade IPv6), záznamy smerníkov spätného vyhľadávania (PTR) alebo oboje. Záznam mapovania adresy (A alebo AAAA) mapuje názov hostiteľa počítača na jeho IP adresu. Záznam PTR mapuje IP adresu počítača do jeho hostiteľského názvu. Pri zmene tejto adresy klienta môže DHCP automaticky odoslať aktualizáciu serveru DNS, vďaka čomu môžu ostatní hostitelia v sieti prostredníctvom dotazov DNS nájsť klienta 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 DHCP, aby aktualizoval len záznamy PTR, musíte nakonfigurovať DNS, aby umožňoval aktualizácie od klientov, vďaka čomu bude môcť každý klient aktualizovať vlastný záznam A (ak klient používa adresu IPv4) alebo záznam AAAA (ak klient používa adresu IPv6). Vytváranie vlastných požiadaviek na aktualizáciu záznamu A alebo AAAA nepodporujú všetci klienti DHCP. 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 je možné vykonávať medzi DNS a DHCP, ktorú sa nachádzajú na jedinej platforme System i, medzi rozličnými platformami System i alebo medzi platformou System i a inými systémami, ktoré majú schopnosť dynamických aktualizácií.

Poznámka: Je nevyhnutné, aby servery, ktoré odosielajú dynamické aktualizácie serveru DNS, mali rozhranie Update DNS (QTOBUPDT) API. Toto rozhranie je možné nainštalovať automaticky voľbou 31 DNS i5/OS. Preferovanou metódou systému BIND 9 na vykonávania aktualizácii na platforme System i je však príkaz NSUPDATE.

Súvisiace koncepty

Dynamic Host Configuration Protocol

Súvisiace úlohy

“Konfigurácia DNS na príjem dynamických aktualizácií” na strane 29
Servery DNS (Domain Name System), na ktorých je spustená verzia BIND 9, je možné nakonfigurovať tak, aby akceptovali požiadavky od ostatných zdrojov a dynamicky aktualizovali zónové údaje. Táto téma poskytuje pokyny na konfiguráciu voľby na povolenie aktualizácie, aby mohol DNS prijímať dynamické zmeny.

Konfigurácia DHCP na odosielanie dynamických aktualizácií systému DNS

Súvisiaci odkaz

“Príklad: DNS a DHCP na rovnakej platforme System i” na strane 18
V tomto príklade je zobrazený server DNS (Domain Name System) a DHCP (Dynamic Host Configuration Protocol) na rovnakej platforme System i.

“Zdrojové záznamy systému DNS” na strane 9
Zdrojové záznamy sa používajú na ukladanie údajov o názvoch domén a IP adries. Pomocou Vyhľadávacej tabuľky zdrojových záznamov môžete získať prehľad o zdrojových záznamoch podporovaných operačným systémom i5/OS.

QTOBUPT

“Funkcie BIND 9” na strane 8
BIND 9 je podobný ako BIND 8, poskytuje však viacero funkcií, ktoré zvyšujú výkonnosť vášho servera DNS (Domain Name System), ako napríklad zobrazenia.

Funkcie BIND 9

BIND 9 je podobný ako BIND 8, poskytuje však viacero funkcií, ktoré zvyšujú výkonnosť vášho servera DNS (Domain Name System), ako napríklad zobrazenia.

Zobrazenia na jedinom serveri DNS i5/OS

Príkaz *view* umožňuje inštancii jediného servera DNS odpovedať rozdielne na dotazy v závislosti na tom, odkiaľ dotaz prichádza, napríklad či prichádza z internetu alebo z intranetu.

Jedným z praktických využití funkcie zobrazení je možnosť rozdeliť nastavenia DNS bez toho, aby ste museli spustiť viacero serverov DNS. Na jedinom serveri DNS môžete napríklad zadefinovať zobrazenie, ktoré bude odpovedať na dotazy z internej siete, zatiaľ čo ďalšie zobrazenie zadefinujete tak, aby odpovedalo na dotazy z externej siete.

Nové klientske príkazy

Schopnosť riadenia vášho servera DNS vylepšujú nasledujúce klientske príkazy:

NSUPDATE (Dynamic Update Utility)
Pomocou príkazu NSUPDATE (Dynamic Update Utility) môžete odovzdať požiadavky typu Dynamic DNS Update tak, ako sú zadefinované v štandarde RFC (Request for Comments) 2136 odosielania požiadaviek na server DNS. Umožňuje pridať, alebo odstrániť zdrojové záznamy zo zóny, zatiaľ čo je server DNS spustený. Vďaka nemu nemusíte záznamy aktualizovať manuálnou úpravou zónového súboru. Jediná aktualizačná požiadavka môže obsahovať požiadavky na pridanie alebo odstránenie viacerých zdrojových záznamov, ale zdrojové záznamy ktoré sú dynamicky pridávané, alebo odstraňované príkazom NSUPDATE, by mali byť v tej istej zóne.

Poznámka: Zóny, ktoré sú riadené dynamicky, neupravujte manuálne príkazom NSUPDATE ani prostredníctvom servera DHCP. Pri manuálnych úpravách môže dôjsť ku konfliktu s dynamickými aktualizáciami a môžu spôsobiť stratu údajov.

DIG (Start DIG Query)
DIG (Domain Information Groper) je výkonný nástroj na vytváranie dotazov porovnateľný s príkazom NSLOOKUP (Name Server Lookup), pomocou ktorého môžete zo servera DNS získavať informácie, alebo testovať jeho odozvu. Príkaz NSLOOKUP bol vyradený a je súčasťou BIND 9 len kvôli kompatibilite so staršími verziami. Pomocou nástroja DIG si predtým, než budete konfigurovať použitie vášho systému, môžete overiť, či váš server DNS správne reaguje. Môžete ho využiť aj pri opakovanom získavaní informácií DNS o hostiteľoch, doménach a ostatných serveroch DNS.

Nástroj DIG (Domain Information Groper) môžete spustiť príkazom STRDIGQRY (Start DIG Query) alebo pomocou jeho aliasu DIG.

HOST (Start HOST Query)
Príkaz HOST (Start HOST Query) slúži na vyhľadávania v DNS. Môžete pomocou neho konvertovať názvy domén na IP adresy (buď na IPv4 alebo na IPv6) a naopak.

RNDC (Remote Name Daemon Control)

Príkaz RNDC (Remote Name Daemon Control) je výkonný pomocný program, ktorý administrátorovi systému umožňuje riadiť prevádzku názvového servera. Načítava konfiguračný súbor s názvom rndc.conf, a na jeho základe určuje, ako sa obracať na názvový server a rozhoduje, aký algoritmus a kľúč použiť. Ak nenájde súbor rndc.conf, potom zvyčajne použije počas inštalácie vytvorený súbor rndc-key._KID, ktorý automaticky určí prístup prostredníctvom návratového rozhrania.

Podpora protokolu IPv6

Verzia BIND 9 podporuje vyhľadávania meno-adresa a adresa-meno vo všetkých aktuálne zadefinovaných formátoch protokolu IPv6. V prípade priamych vyhľadávaní verzia BIND 9 podporuje tak záznamy AAAA, ako aj záznamy A6,

ktoré sú už zrušené. V prípade spätných vyhľadávaní IPv6 podporuje tradičný ”štvorbitový” formát používaný v doméne ip6.arpa, ako aj v staršej, zrušenej doméne ip6.int.

Žurnálové súbory

Žurnálové súbory sú využívané pri podržaní dynamických aktualizácií zóny. Je vytvorený automaticky pri prvom prijatí dynamickej aktualizácie od klienta a nie je automaticky odstránený. Ide o binárny súbor, ktorý by ste nemali upravovať.

Ak server reštartujete po vypnutí alebo havárii, prehrá server tento žurnálový súbor a začlení do zóny všetky aktualizácie, ku ktorým došlo po poslednom výpise z pamäti zóny. Pomocou žurnálových súborov je tiež možné uložiť aktualizácie pri použití metódy prírastkových prenosov zóny (IXFR).

DNS pre i5/OS bol prebudovaný tak, aby využíval verziu BIND 9. Ak chcete vo vašom systéme spustiť server DNS založený na verzii BIND 9, musí tento systém spĺňať určité softvérové požiadavky.

Súvisiace koncepty

“Požiadavky systému DNS” na strane 26
Pred spustením DNS (Domain Name System) na vašej platforme System i zvážte tieto softvérové požiadavky.

“Dynamické aktualizácie” na strane 6
Server DNS (Domain Name System) i5/OS založený na systéme BIND 9 podporuje dynamické aktualizácie. Vďaka tomu môžu tomuto serveru DNS posielať aktualizácie vonkajšie zdroje, akým je napríklad server DHCP (Dynamic Host Configuration Protocol). Okrem toho môžete na vykonanie dynamických aktualizácií využívať aj klientske nástroje DNS, napríklad NSUPDATE (Dynamic Update Utility).

“Čo je nové vo V6R1” na strane 1
Prečítajte si o nových alebo významne zmenených informáciách v súhrne tém DNS (Domain Name System).

Súvisiaci odkaz

“Príklad: Rozdelenie DNS pomocou firewallu s nastavením dvoch serverov DNS na tej istej platforme System i” na strane 20
V tomto príklade je popísaný server DNS (Domain Name System), ktorý funguje cez firewall, aby chránil interné údaje pred prienikmi z internetu a zároveň umožnil interným užívateľom pristupovať k údajom na internete. Táto konfigurácia zabezpečuje ochranu nastavením dvoch serverov DNS na tej istej platforme System i.

“Plánovanie bezpečnostných opatrení” na strane 25
Systém DNS poskytuje bezpečnostné voľby, ktoré umožňujú obmedziť vonkajší prístup k vášmu serveru.

Zdrojové záznamy systému DNS

Zdrojové záznamy sa používajú na ukladanie údajov o názvoch domén a IP adries. Pomocou Vyhľadávacej tabuľky zdrojových záznamov môžete získať prehľad o zdrojových záznamoch podporovaných operačným systémom i5/OS.

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.

Poznámka: Položky vo vyhľadávacej tabuľke zdrojových záznamov je môžete pridať alebo odstrániť podľa zmeny dokumentu BIND. Nie je to ale úplný zoznam všetkých zdrojových záznamov uvedených v BIND.

Tabuľka 1. Vyhľadávacia tabuľka zdrojových záznamov

Zdrojový záznam	Skratka	Opis
Záznamy Address Mapping	A	Záznam A uvádza IP adresu tohto hostiteľa. Záznamy A 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 adresu 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 určuje všeobecné informácie o hostiteľovi. 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.
Záznamy IP Version 6 Address	AAAA	Záznam AAAA určuje adresu hostiteľa v 128-bitovom formáte protokolu IPv6. Záznamy AAAA, ktoré sú podobné ako záznamy A, sú použité pri rozlíšení dotazu na adresu IPv6 konkrétneho názvu domény. Tento typ záznamu je zadefinovaný 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.

Tabuľka 1. Vyhľadávacia tabuľka zdrojových záznamov (pokračovanie)

Zdrojový záznam	Skratka	Opis
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.
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.

Tabuľka 1. Vyhľadávacia tabuľka zdrojových záznamov (pokračovanie)

Zdrojový záznam	Skratka	Opis
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.
Servisné záznamy	SRV	Záznam SRV určuje hostiteľov, ktorí podporujú služby zadefinované v tomto zázname. Tento typ záznamu je zadefinovaný v RFC 2782.
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 využíva DHCP systému i5/OS pri dynamických aktualizáciách. Pri každej aktualizácii PTR a záznamu A, ktorú server DHCP vykoná, zapíše záznam TXT, ktorý je priradený tejto aktualizácii. Záznamy DHCP majú predponu AS400DHCP.
Záznamy Well-Known Services	WKS	Záznam WKS uvádza dobre známe služby podporované objektom. Záznamy WKS najčastejšie uvádzajú, či sa pre túto adresu podporujú protokoly tcp alebo udp alebo oba. Tento typ záznamu je definovaný v RFC 1035.
Záznamy X.400 Address Mapping	PX	Záznamy PX sú ukazovateľom na informácie o mapovaní X.400/RFC 822. Tento typ záznamu je definovaný v RFC 1664.
Záznamy X25 Address Mapping	X25	Záznam X25 uvádza adresu prostriedku X25. Tento záznam mapuje hostiteľský názov do adresy PSDN. Používajú sa len v sieťach X25. Tento typ záznamu je definovaný v RFC 1183.

Súvisiace koncepty

“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 14
Tento príklad znázorňuje jednoduchú podsieť so serverom DNS pre interné použitie.

“Pochopenie zón” na strane 3
Údaje servera DNS (Domain Name System) sú rozdelené do ľahšie ovládateľných skupín údajov nazývaných *zóny*. Každej z týchto skupín je priradený špecifický typ zóny.

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). Tabuľka vyhľadávania v zdrojových záznamoch DNS obsahuje typy poštových záznamov podporované serverom DNS v systéme i5/OS.

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. Inak povedané, umožňujú, aby pošta adresovaná jednému hostiteľovi bola 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: V záznamoch MX niektorej domény neodporúčame používať zástupné znaky (príklad: *.mycompany.com).

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 9
Zdrojové záznamy sa používajú na ukladanie údajov o názvoch domén a IP adries. Pomocou Vyhľadávacej tabuľky zdrojových záznamov môžete získať prehľad o zdrojových záznamoch podporovaných operačným systémom i5/OS.

Príklady: DNS (Domain Name System)

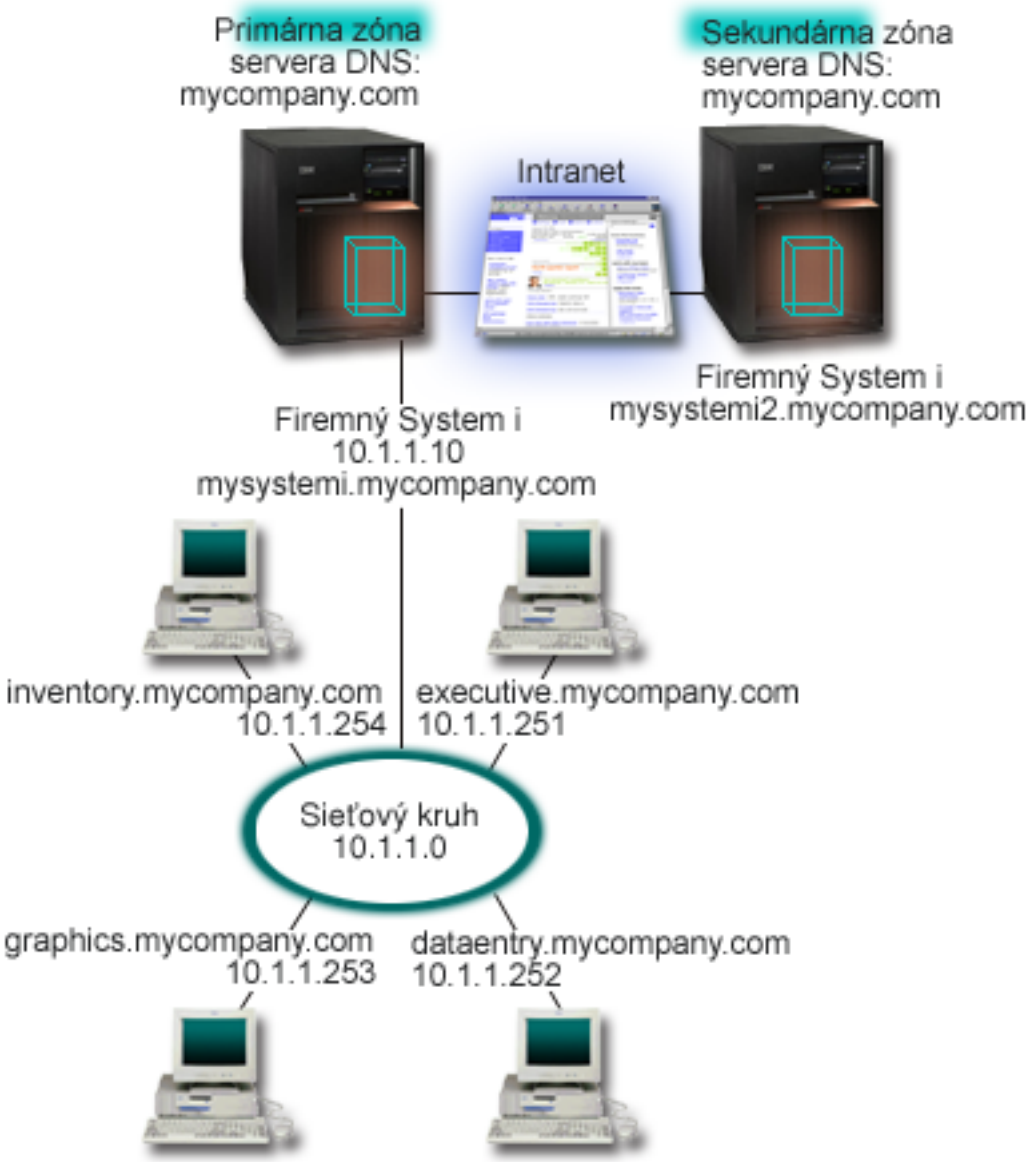
Pomocou týchto príkladov môžete porozumieť spôsobu použitia systému DNS vo vašej sieti.

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.

Na nasledujúcom obrázku je znázornený server DNS pre internú sieť spustený na platforme System i. Táto jedna inštancia servera DNS je nastavená na počúvanie dotazov na všetkých IP adresách rozhrania. Systém je primárnym názvovým serverom zóny 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 pre protokol IPv4 alebo AAAA pre protokol IPv6) mapujú názov počítača s jemu priradenou IP adresou. 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 A, AAAA a PTR podporuje server DNS mnoho ďalších zdrojových záznamov, ktoré môžu byť vyžadované v závislosti na tom, čo vyžadujú aplikácie TCP/IP spustené 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 vyššie zobrazenom obrázku je server mysystemi súčasťou intranetu. Ďalší systém, mysystemi2, bol nakonfigurovaný, aby vystupoval 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 9
Zdrojové záznamy sa používajú na ukladanie údajov o názvoch domén a IP adries. Pomocou Vyhľadávacej tabuľky zdrojových záznamov môžete získať prehľad o zdrojových záznamoch podporovaných operačným systémom i5/OS.

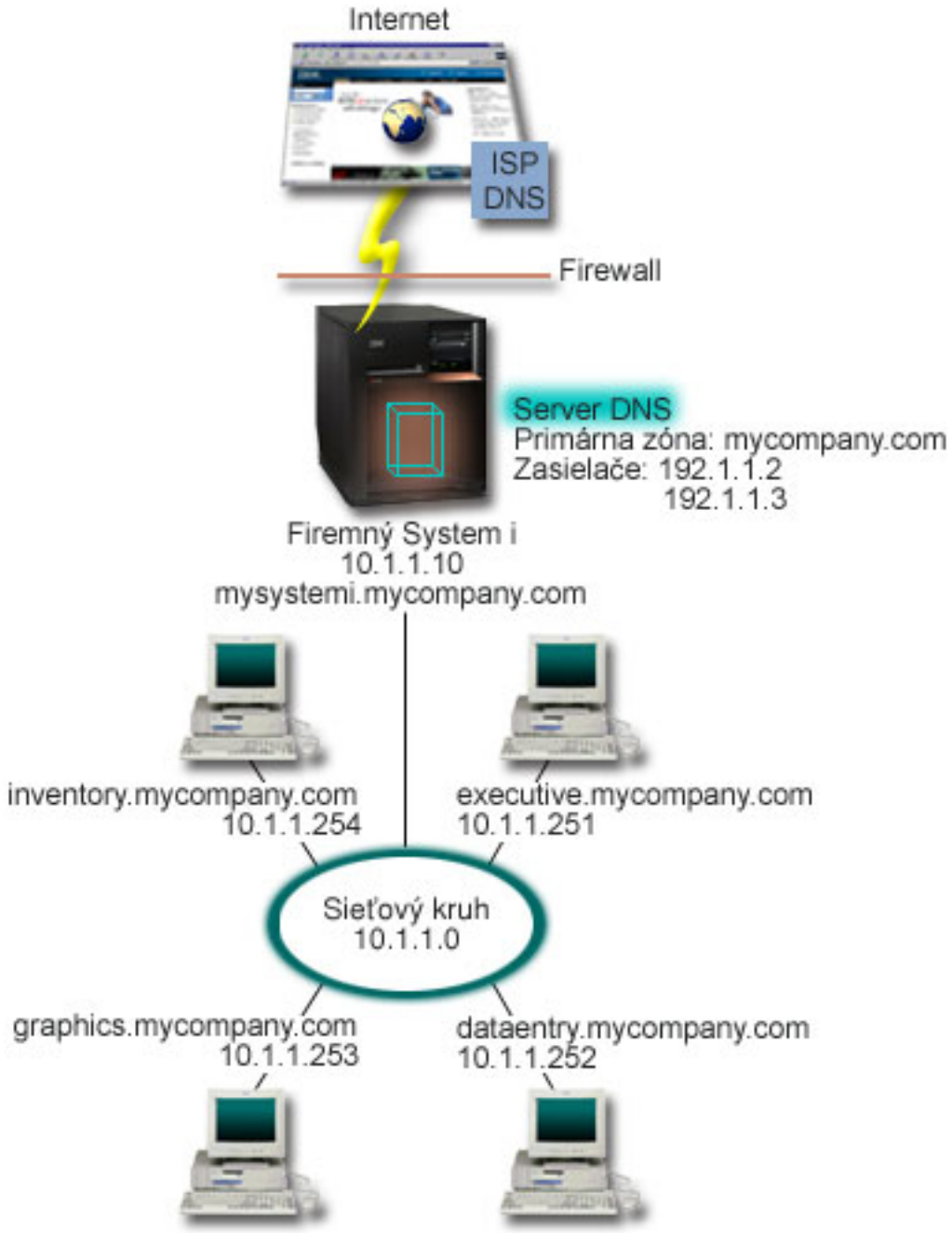
“Pochopenie zón” na strane 3
Údaje servera DNS (Domain Name System) sú rozdelené do ľahšie ovládateľných skupín údajov nazývaných *zóny*. Každej z týchto skupín je priradený špecifický typ zóny.

“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.

Nasledujúci obrázok znázorňuje rovnaký príklad siete ako v príklade s jediným serverom DNS s prístupom na intranet, ale teraz spoločnosť pridala aj pripojenie k 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 aktuálneho zoznamu internetových koreňových serverov nájdete v téme Prístup k externým údajom DNS.
- 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

  Neodporúčame vám, aby ste vášmu serveru DNS umožnili priame pripojenie k internetu. Aby ste zabezpečili vašu platformu System i, potrebujete nakonfigurovať firewall alebo prijať iné predbežné opatrenia.

Súvisiace koncepty

"Nastavenie domény systému DNS" na strane 6
Nastavenie domény DNS (Domain Name System) vyžaduje, aby ste mali zaregistrovaný názov vašej domény, ktorý nebude môcť využívať nikto iný.

Internetová bezpečnosť produktu System i

"Pochopenie dotazov systému DNS" na strane 4
Klienti DNS (Domain Name System) prekladajú požiadavky pomocou serverov DNS. Dotazy môžu prichádzať priamo od klienta alebo od aplikácie, ktorá je na klientovi spustená.

Súvisiaci odkaz

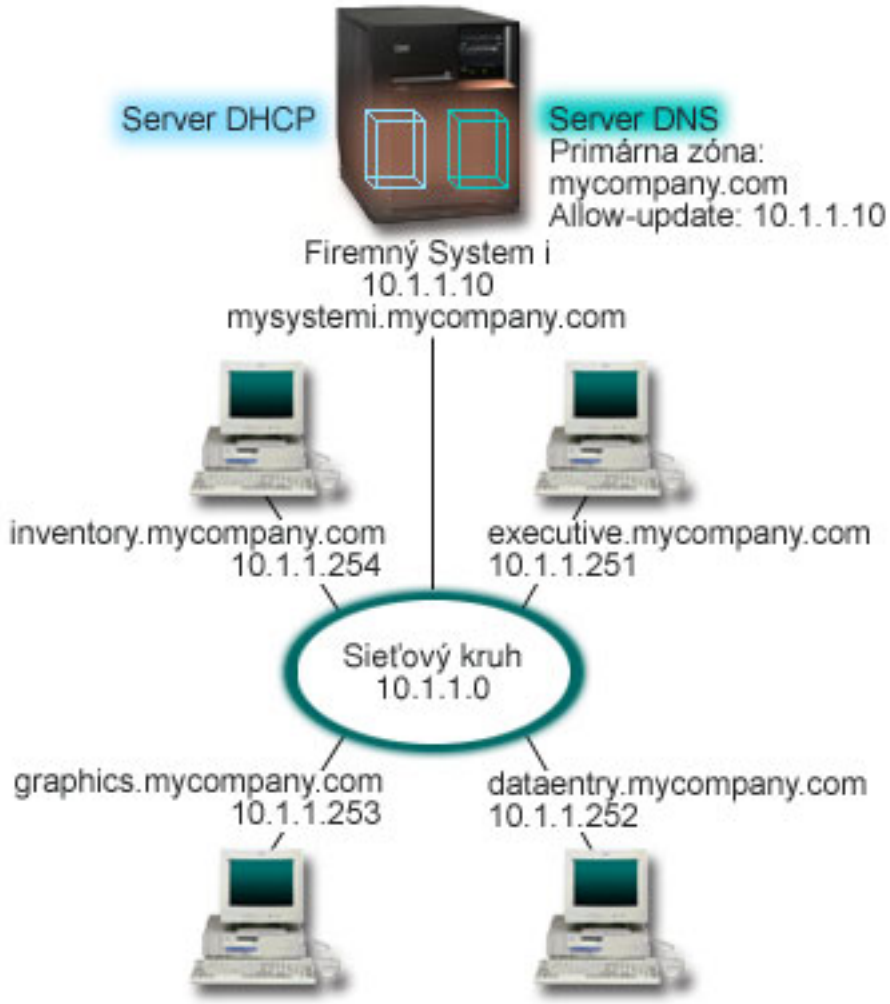
"Príklad: Jeden server DNS pre intranet" na strane 14
Tento príklad znázorňuje jednoduchú podsieť so serverom DNS pre interné použitie.

Príklad: DNS a DHCP na rovnakej platforme System i

V tomto príklade je zobrazený server DNS (Domain Name System) a DHCP (Dynamic Host Configuration Protocol) na rovnakej platforme System i.

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

Nasledujúci obrázok zobrazuje malú podsieť s jednou platformou System i, ktorá vystupuje ako DHCP a DNS server 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. Príklad: DNS a DHCP na rovnakej platforme System i

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.

So serverom DNS v systéme i5/OS (založenom na BIND 9), môžete zónu vášho servera DNS nakonfigurovať, aby akceptovala dynamické aktualizácie záznamov DNS spolu čiastkovými zmenami adries prostredníctvom DHCP. Ak napríklad grafický súborový server obnoví svoje pripojenie a je mu serverom DHCP pridelená IP adresa 10.1.1.250, budú súvisiace záznamy DNS automaticky aktualizované. To umožní ostatným klientom zadávať naďalej serveru DNS dotazy na grafický súborový server podľa názvu hostiteľa.

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. Bližšie informácie o konfigurovaní vašich zón na využívanie funkcie dynamických aktualizácií nájdete v téme Určenie štruktúry domény.
- 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 6
Server DNS (Domain Name System) i5/OS založený na systéme BIND 9 podporuje dynamické aktualizácie. Vďaka tomu môžu tomuto serveru DNS posielať aktualizácie vonkajšie zdroje, akým je napríklad server DHCP (Dynamic Host Configuration Protocol). Okrem toho môžete na vykonanie dynamických aktualizácií využívať aj klientske nástroje DNS, napríklad NSUPDATE (Dynamic Update Utility).

Súvisiace úlohy

Konfigurácia DHCP na odosielanie dynamických aktualizácií systému DNS

Súvisiaci odkaz

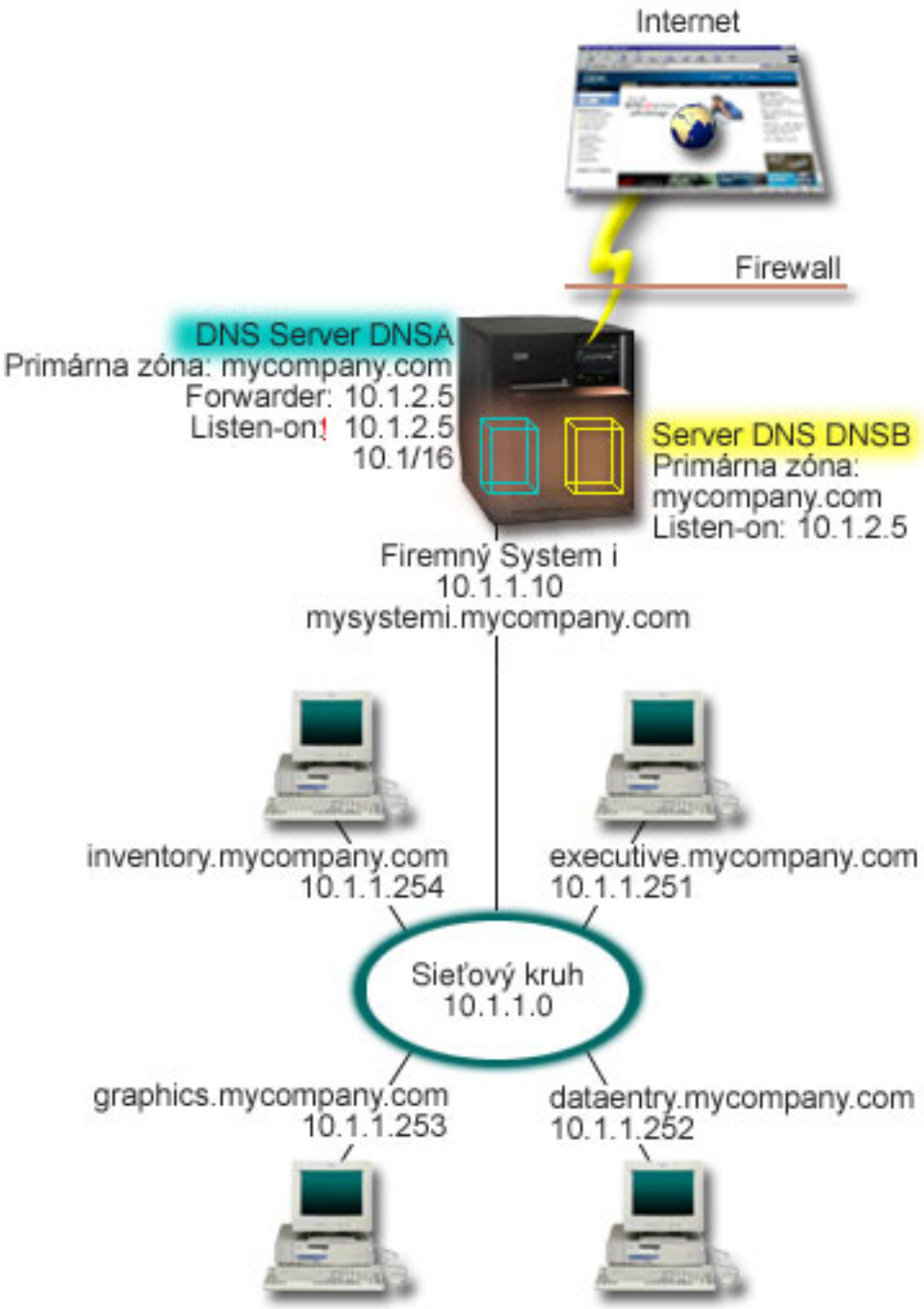
Príklad: DNS a DHCP na rozličných platformách System i

Príklad: Rozdelenie DNS pomocou firewallu s nastavením dvoch serverov DNS na tej istej platforme System i

V tomto príklade je popísaný server DNS (Domain Name System), ktorý funguje cez firewall, aby chránil interné údaje pred prienikmi z internetu a zároveň umožnil interným užívateľom pristupovať k údajom na internete. Táto konfigurácia zabezpečuje ochranu nastavením dvoch serverov DNS na tej istej platforme System i.

Na nasledujúcom obrázku je zobrazená jednoduchá sieť, ktorá na zaistenie bezpečnosti využíva firewall. Predpokladajme, že spoločnosť má internú sieť s rezervovaným priestorom IP a externú časť siete, ktorá je dostupná z verejnej siete. 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.

So serverom DNS (založeným na BIND 9) v systéme i5/OS to môžete dosiahnuť dvoma spôsobmi. Pri prvom spôsobe, popísanom v tomto príklade, spoločnosť nastaví dve inštancie servera DNS na tej istej platforme System i, jednu pre intranet a druhú pre všetko v ich verejnej doméne. Druhým spôsobom je použitie funkcie zobrazení, ktorú poskytuje BIND 9 a ktorá je popísaná v príklade o rozdelení servera DNS cez firewall s využitím zobrazení.



Obrázok 5. Rozdelenie DNS pomocou firewallu s nastavením dvoch serverov DNS na tej istej platforme System i

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 zadefinované v DNSA obsahujú zdrojové záznamy intranetu. Voľba zasielateľa je zadefinovaná 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. Aby všetky tieto nastavenia správne fungovali, musia byť interní klienti nakonfigurovaní zasielať dotazy len na server DNSA. Pri rozdelení DNS by ste mali zvážiť nasledujúce nastavenia:

- Listen-on

  V ostatných príkladoch k DNS sa na platforme System i nachádza len jeden server DNS. Bol nastavený na počúvanie na všetkých adresách IP rozhrania. Zakaždým, keď máte na platforme System i viac serverov DNS, musíte zadefinovať IP adresy rozhrania, na ktorých každý z nich počúva. keďže dva servery DNS nemôžu počúvať na tej istej adrese. V tomto prípade predpokladajte, že všetky požiadavky, ktoré cez firewall prichádzajú do vnútra siete, sú odoslané na IP 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 tak, aby akceptoval dotazy od kohokoľvek na všetky IP adresy rozhrania 10.1.x.x, okrem 10.1.2.5. Ak chcete adresu účinne vylúčiť, musí byť táto adresa vyčlenená zo zoznamu zhôd adries tým, že bude uvedená pred predponou povolených adries.

- Poradie zoznamu zhôd adries

  Je použitý prvý element v zozname zhôd adries, ktorý je zhodný s danou 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 je IP adresa 10.1.2.5 porovnaná s prvým elementom a je hneď zamietnutá.

  Ak by boli tieto elementy v opačnom poradí (10.1/16; !10.1.2.5), bola by IP adresa 10.1.2.5 povolená, pretože by ju server porovnal s prvým zhodným elementom a povolil by ju bez kontroly ostatných pravidiel.

Súvisiaci odkaz

"Funkcie BIND 9" na strane 8
BIND 9 je podobný ako BIND 8, poskytuje však viacero funkcií, ktoré zvyšujú výkonnosť vášho servera DNS (Domain Name System), ako napríklad zobrazenia.

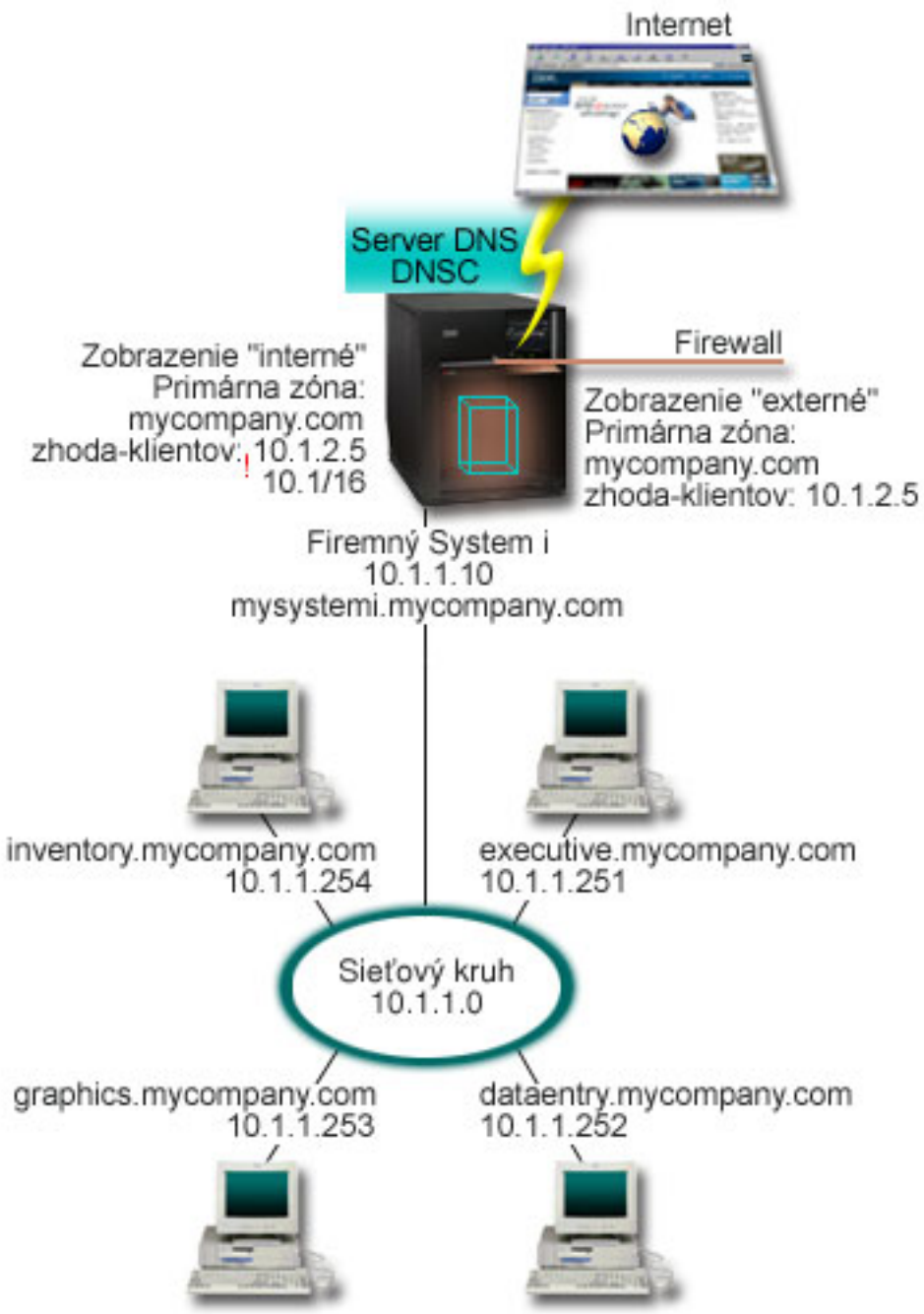
"Príklad: Rozdelenie DNS pomocou firewallu s použitím zobrazení"
V tomto príklade je popísaný server DNS (Domain Name System), ktorý funguje cez firewall, aby chránil interné údaje pred prienikmi z internetu a zároveň umožnil interným užívateľom pristupovať k údajom na internete s použitím funkcie *view*, ktorú poskytuje verzia BIND 9.

Príklad: Rozdelenie DNS pomocou firewallu s použitím zobrazení

V tomto príklade je popísaný server DNS (Domain Name System), ktorý funguje cez firewall, aby chránil interné údaje pred prienikmi z internetu a zároveň umožnil interným užívateľom pristupovať k údajom na internete s použitím funkcie *view*, ktorú poskytuje verzia BIND 9.

Na nasledujúcom obrázku je zobrazená jednoduchá sieť, ktorá na zaistenie bezpečnosti využíva firewall. Predpokladajme, že spoločnosť má internú sieť s rezervovaným priestorom IP a externú časť siete, ktorá je dostupná z verejnej siete. Spoločnosť chce, aby boli interní klienti schopní rozpoznávať názvy externých hostiteľov a vymieňať si poštové správy s ľuďmi z vonkajšej siete. Taktiež chce, aby mali interné rozlišovače prístup k určitým interne vyhradeným zónam, ktoré nie sú z vonkajšej siete dostupné. Nechce však, aby vonkajšie rozlišovače mali prístup k internej sieti.

So serverom DNS (založeným na BIND 9) v systéme i5/OS to môžete dosiahnuť dvoma spôsobmi. V tomto príklade je popísaný spôsob, pri ktorom môžete nakonfigurovať server DNS s dvoma rozličnými zobrazeniami, ktoré počúvajú rozličné dotazy, jeden pre intranet a druhý pre všetko na jeho verejnej doméne. Ďalším spôsobom, ktorý je popísaný v príklade Rozdelenie DNS pomocou firewallu s nastavením dvoch serverov DNS, je nastavenie dvoch inštancií servera DNS na tej istej platforme System i.



Obrázok 6. Rozdelenie DNS pomocou firewallu s použitím zobrazení

Server DNS (DNSC) definuje dve zobrazenia nazvané *externé* a *interné*. *Externé* zobrazenie je nakonfigurované s primárnou zónou mycompany.com, ktorá obsahuje len zdrojové záznamy, ktoré majú byť súčasťou verejnej domény, zatiaľ čo *interné* zobrazenie je nakonfigurované s primárnou zónou mycompany.com, ktorá obsahuje zdrojové záznamy intranetu.

Ak vás znepokojuje integrita vášho firewallu alebo iné bezpečnostné hrozby, máte možnosť použiť podpríkaz zhody klientov, ktorý vám pomôže ochrániť interné údaje. Dosiahnete to takým nakonfigurovaním interného zobrazenia, aby umožňovalo len dotazy na internú zónu mycompany.com od interných hostiteľov. Ak chcete nastaviť rozdelenie DNS, musíte zvážiť nasledujúce konfiguračné nastavenia:

- zhoda-klientov

Zhoda-klientov (match-clients) v príkaze zobrazenia preberá ako argument zoznam zhôd adries. Hodnoty konfigurácie zadefinované v poslaní zobrazenia môžu vidieť len IP adresy dotazov, ktoré sa zhodujú s týmto zoznamom zhôd adries. Ak sa IP adresa dotazu zhoduje s viacerými položkami zhody klientov v rozličných príkazoch zobrazenia, bude použitý len prvý zhodný príkaz. V tomto prípade predpokladajte, že všetky požiadavky, ktoré cez firewall prichádzajú do vnútra siete, sú odoslané na IP adresu 10.1.2.5. Tieto dotazy by mali byť spracované zónovými údajmi v externom zobrazení. Preto je ako zhoda klientov v externom zobrazení nastavená IP adresa 10.1.2.5. Interné zobrazenie je nakonfigurované, aby akceptovalo dotazy od kohokoľvek na všetky IP adresy rozhrania 10.1.x.x, okrem 10.1.2.5. Ak chcete adresu účinne vylúčiť, musí byť táto adresa vyčlenená zo zoznamu zhôd adries tým, že bude uvedená pred predponou povolených adries.

- Poradie zoznamu zhôd adries

  Je použitý prvý element v zozname zhôd adries, ktorý je zhodný s danou 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 je IP adresa 10.1.2.5 porovnaná s prvým elementom a je hneď zamietnutá.

  Ak by boli tieto elementy v opačnom poradí (10.1/16; !10.1.2.5), bola by IP adresa 10.1.2.5 povolená, pretože by ju server porovnal s prvým zhodným elementom a povolil by ju bez kontroly ostatných pravidiel.

Súvisiaci odkaz

“Príklad: Rozdelenie DNS pomocou firewallu s nastavením dvoch serverov DNS na tej istej platforme System i” na strane 20
V tomto príklade je popísaný server DNS (Domain Name System), ktorý funguje cez firewall, aby chránil interné údaje pred prienikmi z internetu a zároveň umožnil interným užívateľom pristupovať k údajom na internete. Táto konfigurácia zabezpečuje ochranu nastavením dvoch serverov DNS na tej istej platforme System i.

Plánovanie servera DNS

Systém DNS ponúka množstvo riešení. Pred jeho konfiguráciou by ste mali naplánovať spôsob, akým bude pracovať vo vašej sieti. Mali by ste zvážiť témy ako štruktúra, výkonnosť a bezpečnosť siete.

Určenie oprávnení servera 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.

Na konfiguráciu a administrovanie servera DNS je od vášho administrátora vyžadovaná minimálna úroveň oprávnení. 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. Užívateľov môžete autorizovať pomocou programu System i Navigator. V prípade potreby nájdete bližšie informácie v online pomoci k DNS v téme Prideľovanie oprávnení administrátorovi 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 DNS” na strane 34
Pomocou DNS v rozhraní i5/OS môžete na vašej platforme System i vytvárať a riadiť inštancie servera DNS. Konfiguračné súbory DNS sú riadené programom System i Navigator. Tieto súbory musíte upravovať manuálne. Pri ich vytvorení, zmene alebo vymazaní používajte vždy program System i Navigator.

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.

DNS v programe i5/OS poskytuje grafické rozhranie určené na konfiguráciu vašich systémov. V niektorých prípadoch toto rozhranie používa terminológiu alebo koncepty, ktoré sú v iných zdrojoch reprezentované rozdielne. Ak budete pri plánovaní konfigurácie vášho servera DNS využívať aj iné zdroje informácií, bude užitočné, ak si zapamätáte nasledujúce body:

- Všetky zóny a objekty zadefinované na platforme System i sú usporiadané v zložkách Zóny priamych vyhľadávaní a Zóny spätných vyhľadávaní. Zóny priamych vyhľadávaní sú zóny, ktoré sú využívané pri mapovaní názvov domén na IP adresy, akými sú napríklad záznamy A alebo AAAA. Zóny spätného vyhľadávania sú zóny, ktoré sa používajú na mapovanie IP adries do názvov domén, ako napríklad záznamy PTR.
- DNS v systéme i5/OS používa odkazy na *primárne zóny* a *sekundárne zóny*.
- Rozhranie používa *podzóny*, pre ktoré niektoré zdroje používajú termín *poddomény*. Dcérska zóna je podzónou, pre ktorú ste delegovali zodpovednosť za jeden alebo viacero názvových serverov.

Plánovanie bezpečnostných opatrení

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

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 položiek zoznamu zhôd adries

Prvá položka v zozname zhôd adries, ktorá je zhodná s danou adresou. Ak chcete napríklad povoliť všetky adresy v sieti 10.1.1.x okrem adresy 10.1.1.5, musia byť položky zoznamu zhôd zoradené v poradí (!10.1.1.5; 10.1.1/24). V tomto prípade bude adresa 10.1.1.5 porovnaná s prvou položkou a bude ihneď odmietnutá.

Ak by boli tieto elementy v opačnom poradí (10.1.1/24; !10.1.1.5), bola by IP adresa 10.1.1.5 povolená, pretože by ju server porovnal s prvou položkou, zistil by zhodu a povolil by ju 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 rozlíšenie dotazov. Na dotazy z týchto adries nebude server odpovedať.

Zabezpečenie vášho servera DNS je zásadnou vecou. Okrem bezpečnostných hľadísk uvedených v tejto téme pokrývajú bezpečnosť servera DNS a bezpečnosť platformy System i rozličné zdroje informácií vrátane súhrnu tém k Platforma System i a internet. Bezpečnosti súvisiacej so severmi DNS sa venuje aj kniha *DNS and BIND*.

Súvisiace koncepty

Internetová bezpečnosť produktu System i

Súvisiaci odkaz

“Funkcie BIND 9” na strane 8
BIND 9 je podobný ako BIND 8, poskytuje však viacero funkcií, ktoré zvyšujú výkonnosť vášho servera DNS (Domain Name System), ako napríklad zobrazenia.

Požiadavky systému DNS

Pred spustením DNS (Domain Name System) na vašej platforme System i zvážte tieto softvérové požiadavky.

Funkciu DNS (Voľba 31) nie je možné nainštalovať automaticky s operačným systémom. DNS musíte na inštaláciu špecificky vybrať. Server DNS, ktorý je pridaný k operačnému systému i5/OS, je založený na implementácii DNS podľa priemyselných štandardov známej ako BIND 9. Predošlé služby DNS v OS/400 boli založené na BIND 8.2.5 a v systéme i5/OS sú aj naďalej dostupné.

Po inštalácii DNS je vyžadovaná migrácia a konfigurácia servera DNS z BIND 4 alebo 8 na BIND 9. Taktiež musíte mať v systéme i5/OS nainštalovanú voľbu 33, teda i5/OS PASE. Po inštalácii prostredia i5/OS PASE program System i Navigator automaticky zabezpečí konfiguráciu aktuálnej implementácie systému BIND.

Ak chcete server DHCP (Dynamic Host Configuration Protocol) na inej platforme nakonfigurovať tak, aby odosielal aktualizácie vášmu serveru DNS, musí byť aj na tomto serveri DHCP nainštalovaná Voľba 31. Server DHCP vykonáva dynamické aktualizácie prostredníctvom programovacieho rozhrania, ktoré poskytuje Voľba 31.

Súvisiace koncepty

i5/OS PASE

“Konfigurácia DNS” na strane 27
Pri konfigurácii názvových serverov a rozlišovaní dotazov mimo vašu doménu môžete využívať program System i Navigator.

Súvisiaci odkaz

“Funkcie BIND 9” na strane 8
BIND 9 je podobný ako BIND 8, poskytuje však viacero funkcií, ktoré zvyšujú výkonnosť vášho servera DNS (Domain Name System), ako napríklad zobrazenia.

Spôsob zistenia existujúcej inštalácie DNS

Nasledujúcim postupom môžete zistiť, či je systém DNS nainštalovaný.

1. Na príkazovom riadku zadajte GO LICPGM a stlačte kláves Enter.
2. Zadajte 10 (Zobraziť nainštalované licenčné programy) a stlačte kláves Enter.
3. Prejdite nižšie na **5761SS1 Domain Name System** (Voľba 31). Ak je server DNS úspešne nainštalovaný, bude hodnota Installed Status uvedená ako *COMPATIBLE (ako je to zobrazené nižšie):

```
LicPgm     Installed Status     Description
5761SS1    *COMPATIBLE          Domain Name System
```

4. Stlačte kláves F3 na opustenie obrazovky.

Inštalácia DNS

Pri inštalácii DNS (Domain Name System) postupujte podľa týchto krokov.

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 DNS

Pri konfigurácii názvových serverov a rozlišovaní dotazov mimo vašu doménu môžete využívať program System i Navigator.

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 26
Pred spustením DNS (Domain Name System) na vašej platforme System i zvážte tieto softvérové požiadavky.

Prístup k DNS v programe System i Navigator

V tejto príručke nájdete pokyny ku konfiguračnému rozhraniu DNS v programe System i Navigator.

Ak používate systém i5/OS PASE, budete môcť konfigurovať servery DNS založené na verzii BIND 9.

Ak konfigurujete DNS prvýkrát, postupujte takto:

1. V System i Navigator rozviňte ***váš systém*** → **Network** → **Servers** → **DNS**.
2. Pravým tlačidlom myši kliknite na **DNS** a vyberte **New Configuration**.

Súvisiace koncepty

Oboznámenie sa s produktom System i Navigator

Konfigurácia názvových serverov

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

DNS v systéme i5/OS založený na BIND 9 podporuje viacero inštancií názvového servera. Nasledujúce úlohy vás prevedú procesom vytvorenia jednej inštancie názvového servera vrátane nastavenia vlastností a zón.

Ak chcete vytvoriť viac inštancií, opakujte tento postup, kým nevytvoríte všetky požadované 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 DNS" na strane 34
Pomocou DNS v rozhraní i5/OS môžete na vašej platforme System i vytvárať a riadiť inštancie servera DNS. Konfiguračné súbory DNS sú riadené programom System i Navigator. Tieto súbory musíte upravovať manuálne. Pri ich vytvorení, zmene alebo vymazaní používajte vždy program System i Navigator.

Vytvorenie inštancie názvového servera

Procesom zadefinovania inštancie servera DNS vás môže previesť sprievodca Nová konfigurácia DNS.

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

1. V System i Navigator rozviňte ***váš systém*** → **Network** → **Servers** → **DNS**.
2. V ľavej časti okna kliknite pravým tlačidlom myši na **DNS** a vyberte **New Name Server**.
3. Postupujte podľa pokynov sprievodcu a dokončite proces konfigurácie.

Sprievodca vyžaduje nasledujúce vstupy:

Názov servera DNS:
Zadajte názov vášho servera DNS. Môže mať maximálne 5 znakov a musí sa začínať abecedným znakom (A-Z). Ak vytvárate viacero serverov, každý musí mať jedinečný názov. Na tento názov sa ostatné časti systému odkazujú ako na názov inštancie servera DNS .

Adresy IP pre počúvanie:
Dva servery DNS nemôžu počúvať na tej istej adrese IP. Predvolené nastavenie je počúvať na všetkých IP adresách. Ak však vytvárate dodatočné inštancie servera, nesmú byť nakonfigurované na počúvanie na všetkých IP adresách. V opačnom prípade by nemohli byť spustené v rovnakom čase. 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: Zavedenie predvolených internetových koreňových systémov by ste mali zvážiť len v prípade, ak máte prístup na internet a očakávate, že váš server DNS bude musieť byť schopný plne rozpoznávať internetové názvy.

Spustenia 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.

Úprava vlastností 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 System i Navigator rozviňte ***váš systém*** → **Network** → **Servers** → **DNS**.
2. V pravej časti kliknite pravým tlačidlom myši na ***your DNS server*** a vyberte **Configuration**.
3. V okne DNS Configuration kliknite pravým tlačidlom myši na **DNS Server** a vyberte **Properties**.
4. Upravte vlastnosti, ktoré chcete upraviť.

Konfigurácia zóny na názvovom serveri

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

Pri konfigurácii zón na vašom serveri postupujte podľa týchto krokov:

1. V System i Navigator rozviňte ***váš systém*** → **Network** → **Servers** → **DNS**.
2. V pravej časti kliknite pravým tlačidlom myši na ***your DNS server*** a vyberte **Configuration**.
3. V okne DNS Configuration kliknite pravým tlačidlom myši buď na zložku **Forward Lookup Zone** alebo na zložku **Reverse Lookup Zone**, čím vyberiete typ zóny, ktorú chcete vytvoriť.

4. Postupujte podľa pokynov sprievodcu a dokončite proces vytvorenia zóny.

Súvisiace koncepty

"Prístup k externým údajom DNS" na strane 30
Ak vytvoríte zónové údaje systému DNS, váš server bude môcť rozlíšiť dotazy patriace do tejto zóny.

Súvisiace úlohy

"Konfigurácia DNS na príjem dynamických aktualizácií"
Servery DNS (Domain Name System), na ktorých je spustená verzia BIND 9, je možné nakonfigurovať tak, aby akceptovali požiadavky od ostatných zdrojov a dynamicky aktualizovali zónové údaje. Táto téma poskytuje pokyny na konfiguráciu voľby na povolenie aktualizácie, aby mohol DNS prijímať dynamické zmeny.

"Import súborov DNS" na strane 30
DNS (Domain Name System) môže importovať už existujúce súbory zónových údajov. Postupujte podľa týchto čas šetriacich procedúr na vytvorenie novej zóny z existujúceho konfiguračného súboru.

Súvisiaci odkaz

"Pochopenie zón" na strane 3
Údaje servera DNS (Domain Name System) sú rozdelené do ľahšie ovládateľných skupín údajov nazývaných *zóny*. Každej z týchto skupín je priradený špecifický typ zóny.

Konfigurácia zobrazení na názvovom serveri

Jedna z funkcií, ktoré vám ponúka verzia BIND 9, je príkaz *view*, ktorý umožňuje jedinej inštancii DNS (Domain Name System) odpovedať na prichádzajúce dotazy rozdielne v závislosti na tom, odkiaľ dotaz prichádza, napríklad či prichádza z internetu alebo z intranetu. Jedným z praktických využití zobrazení je možnosť rozdeliť nastavenia bez toho, aby ste museli mať spustené viaceré servery DNS.

Pri konfigurácii zobrazení na vašom serveri postupujte podľa týchto krokov:

1. V System i Navigator rozviňte ***váš systém*** → **Network** → **Servers** → **DNS**.
2. V pravej časti kliknite pravým tlačidlom myši na ***your DNS server*** a vyberte **Configuration**.
3. V okne DNS Configuration kliknite pravým tlačidlom myši na **Views** a vyberte **New View**.
4. Postupujte podľa pokynov sprievodcu a dokončite proces vytvorenia zobrazenia.

Konfigurácia DNS na príjem dynamických aktualizácií

Servery DNS (Domain Name System), na ktorých je spustená verzia BIND 9, je možné nakonfigurovať tak, aby akceptovali požiadavky od ostatných zdrojov a dynamicky aktualizovali zónové údaje. 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 potrebujete v dynamickej zóne vykonať manuálne aktualizácie, musíte server dynamickej zóny zastaviť a po dokončení vašich aktualizácií ho znova reštartovať. Zastavenie servera si vynúti aktualizáciu databázy zóny všetkými dynamickými aktualizáciami, ktoré boli vykonané od momentu, keď server po prvý raz zaviedol z databázy zóny svoje zónové údaje. Ak server nezastavíte, prídete o všetky manuálne aktualizácie v databáze zóny, pretože budú prepísané bežiacim serverom. 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 System i Navigator rozviňte ***váš systém*** → **Network** → **Servers** → **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 tohto zoznamu zhôd adries, vyberte typ položky v tomto zozname a kliknite na **Add**. 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 úlohy

"Konfigurácia zóny na názvovom serveri" na strane 28
Po konfigurácii inštancie servera DNS potrebujete nakonfigurovať zóny pre názvový server.

Konfigurácia DHCP na odosielanie dynamických aktualizácií systému DNS

Import súborov DNS

DNS (Domain Name System) môže importovať už existujúce súbory zónových údajov. Postupujte podľa týchto čas šetriacich procedúr na vytvorenie novej zóny z existujúceho konfiguračného súboru.

Primárnu zónu môžete vytvoriť importom súboru zónových údajov, ktorý je platným konfiguračným súborom zóny založeným na syntaxi BIND. Tento súbor by mal byť umiestnený v adresári integrovaného súborového systému. Po jeho importe DNS overí, či ide o platný súbor zónových údajov a pridá ho do súboru named.conf zadanej inštancie servera.

Ak chcete naimportovať zónový súbor, postupujte takto:

1. V System i Navigator rozviňte ***váš systém*** → **Network** → **Servers** → **DNS**.
2. V pravej časti dvakrát kliknite na inštanciu servera DNS, do ktorej chcete túto zónu importovať.
3. V ľavej časti okna DNS Configuration kliknite pravým tlačidlom myši na **DNS server** a vyberte **Import Zone**.
4. Pri importovaní primárnej zóny postupujte podľa pokynov sprievodcu.

Súvisiace úlohy

"Konfigurácia zóny na názvovom serveri" na strane 28
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.

Prístup k externým údajom DNS

Ak vytvoríte zónové údaje systému DNS, váš server bude môcť rozlíšiť 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 System i Navigator

Koreňové servery internetu by ste mali používať len vtedy, ak máte internetové pripojenie a chcete rozlíšiť názvy na internete, ak nie sú rozlíšené na vašom serveri DNS. Predvolený zoznam internetových koreňových serverov nájdete v System i Navigator. ide o zoznam aktuálny v čase vydania System i Navigator. Kontrolu aktuálnosti predvoleného zoznamu môžete vykonať jeho porovnaním so zoznamom na stránke InterNIC. Aktualizujte si konfiguračný zoznam koreňových serverov.

Získanie adries 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. Prostredníctvom protokolu FTP (File Transfer Protocol) sa prihláste sa k serveru InterNIC ako anonymný užívateľ: FTP.INTERNIC.NET alebo RS.INTERNIC.NET
2. Prevezmite tento súbor: /domain/named.root
3. Uložte stiahnutý súbor v adresári s nasledujúcou cestou: /QOpenSys/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 úlohy

"Konfigurácia zóny na názvovom serveri" na strane 28
Po konfigurácii inštancie servera DNS potrebujete nakonfigurovať zóny pre názvový server.

Riadenie servera DNS

Riadenie servera DNS (Domain Name System) zahŕňa kontrolu funkčnosti DNS, monitorovanie výkonu a údržbu údajov a súborov DNS.

Kontrola funkčnosti DNS

Pomocou nástroja DIG (Domain Information Groper) môžete zhromažďovať informácie zo servera DNS (Domain Name System) a testovať jeho odozvu. Prostredníctvom nástroja DIG si môžete overiť, či váš server DNS správne funguje.

Požiadajte o názov hostiteľa priradený k návratovej IP adrese (127.0.0.1). Server by mal odpovedať názvom hostiteľa (localhost). Môžete zadať aj dotaz na konkrétne názvy zadefinované v tej inštancii servera, ktorej fungovanie sa snažíte overiť. Tým si potvrdíte, či konkrétna testovaná inštancia servera funguje bezchybne.

Pri overovaní funkčnosti DNS prostredníctvom nástroja DIG postupujte podľa týchto krokov:

1. V príkazovom riadku napíšte DIG HOSTNAME('127.0.0.1') REVERSE(*YES).
   Mali by sa zobraziť nasledujúce informácie vrátane názvu hostiteľa návratu.

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

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

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

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

;; ADDITIONAL SECTION:
ISA2LP05.RCHLAND.IBM.COM. 38694   IN    A   9.5.176.194

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

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

2. Reláciu ukončíte stlačením klávesu Enter.

Poznámka: Ak budete pri použití nástroja DIG potrebovať pomoc, napíšte ?DIG a stlačte kláves Enter.

Riadenie bezpečnostných kľúčov

Bezpečnostné kľúče umožňujú obmedziť prístup k vašim údajom DNS.

V súvislosti s DNS existujú dva typy kľúčov, menovite kľúče DNS a kľúče dynamických aktualizácií. Každý z nich má pri zabezpečovaní konfigurácie vášho DNS inú úlohu. Nasledujúce opisy vysvetľujú, ako ktorý súvisí s vašim serverom DNS.

Riadenie kľúčov 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 System i Navigator rozviňte ***váš systém*** → **Network** → **Servers** → **DNS**.
2. V pravej časti okna kliknite pravým tlačidlom myši na inštanciu servera DNS, ktorú chcete riadiť a vyberte **Configuration**.
3. V okne DNS Configuration vyberte **File** → **Manage Keys**.

V okne Manage Keys môžete vykonávať príslušné úlohy riadenia.

Riadenie kľúčov dynamickej aktualizácie

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

Tieto kľúče musia byť prítomné, ak je DNS (Domain Name System) umiestnený na rovnakej platforme System i, ako DHCP. Ak je DHCP na inej platforme System i, musíte tie isté súbory kľúčov dynamickej aktualizácie distribuovať na každú vzdialenú platformu System i, ktorá ich potrebuje, aby mohla odosielať dynamické aktualizácie autoritatívnym serverom. Distribuovať ich môžete prostredníctvom FTP, elektronickou poštou a podobne.

Pri riadení kľúčov dynamických zmien postupujte takto:

1. V System i Navigator rozviňte ***váš systém*** → **Sieť** → **Servery** → **DNS**.
2. Pravým tlačidlom myši kliknite na **DNS** a vyberte **Manažovať kľúče dynamickej aktualizácie**.

| Potom môžete v okne Riadenie kľúčov dynamickej aktualizácie vykonať príslušné úlohy riadenia kľúčov.

Prístup 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 DNS" na strane 34
Pomocou DNS v rozhraní i5/OS môžete na vašej platforme System i vytvárať a riadiť inštancie servera DNS. Konfiguračné súbory DNS sú riadené programom System i Navigator. Tieto súbory musíte upravovať manuálne. Pri ich vytvorení, zmene alebo vymazaní používajte vždy program System i Navigator.

Prístup k štatistikám 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 System i Navigator rozviňte ***váš systém*** → **Network** → **Servers** → **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**.

| Pri zobrazení informácií o štatistikách servera, ktoré sú uložené v súbore named.stats môžete použiť aj príkaz RNDC
| (Remote Name Daemon Control). Príslušný príkaz použite nasledovným spôsobom.

| RNDC RNDCCMD('stats')

Prístup k databáze 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 pamäte databázy aktívneho servera môžete zobraziť pomocou System i Navigator. Ak si potrebujete uložiť kópiu týchto súborov, názov súboru výpisu z pamäte je named_dump.db a je uložený v adresári i5/OS s cestou: /QIBM/UserData/OS400/DNS/<server instance>/, pričom <*server instance*> je názov inštancie servera DNS. Bližšie informácie o databáze aktívneho servera sú dostupné v online pomoci k DNS v téme Pochopenie výpisov z pamäte databázy servera DNS.

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

1. V System i Navigator rozviňte ***váš systém*** → **Network** → **Servers** → **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**.

| Pri zobrazení informácií o databáze aktívneho servera, ktoré sú uložené v súbore named_dump.db, môžete použiť aj
| príkaz RNDC (Remote Name Daemon Control). Príslušný príkaz použite nasledovným spôsobom.

RNDC RNDCCMD('dumpdb -all')

Udržiavanie konfiguračných súborov DNS

Pomocou DNS v rozhraní i5/OS môžete na vašej platforme System i vytvárať a riadiť inštancie servera DNS. Konfiguračné súbory DNS sú riadené programom System i Navigator. Tieto súbory musíte upravovať manuálne. Pri ich vytvorení, zmene alebo vymazaní používajte vždy program System i Navigator.

Konfiguračné súbory DNS sú uložené v cestách integrovaného súborového systému uvedených nižšie.

Poznámka: Nižšie použitá štruktúra súborov sa týka servera DNS spusteného v systéme BIND 9.

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.
/QIBM/UserData/OS400/DNS/ <*instance-n*>/		Adresár počiatočného bodu pre inštanciu DNS.
ATTRIBUTES		DNS používa tento súbor aby určil, ktorú verziu BIND používate.
BOOT.AS400BIND4		Konfiguračný súbor a súbor politík servera BIND 4.9.3, ktorý je v tejto inštancii konvertovaný do súboru named.conf BIND 8. Tento súbor je vytvorený, ak migrujete server BIND 4.9.3 na verziu BIND 9. Slúži ako záloha pre migráciu a ak server BIND 9 funguje bez problémov, je možné ho vymazať.
named.ca		Zoznam koreňových serverov pre túto inštanciu servera.
named.conf		Tento súbor obsahuje konfiguračné údaje, Oznamuje serveru, ktoré konkrétne zóny riadi, kde sú zónové súbory umiestnené, ktoré zóny je možné aktualizovať dynamicky, kde sú preposielacie servery a ďalšie nastavenia volieb.
named_dump.db		Vytvorený výpis údajov z pamäte servera pre aktívnu databázu servera.
named.memstats		Štatistiky pamäte servera (ak je to nakonfigurované v súbore named.conf).
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.
named.random		Serverom generovaný súbor entropy.
named.recursing		Rekurzívne dotazy serverov (ak je to vyžadované programom System i Navigator).

Názov	Ikona	Opis
named.run		Predvolený protokol ladenia (ak je vyžadovaný). V prípade nárastu nad maximálnu povolenú veľkosť sú ukladané jeho verzie pod názvom named.run.0, named.run.1 a tak ďalej.
named.stats		Štatistika servera.
<*primary-zone-n*>.db		Ide o súbor primárnej zóny niektorej konkrétnej domény na tomto serveri. Tento súbor obsahuje všetky zdrojové záznamy danej zóny. Každá zóna má svoj vlastný osobitný súbor .db.
<*primary-zone-n*>.jnl		Žurnálový súbor, ktorý drží dynamické aktualizácie zóny. Je vytvorený pri prijatí prvej dynamickej aktualizácie. Ak reštartujete server po vypnutí alebo havárii, prehrá server tento žurnálový súbor a začlení do zóny všetky aktualizácie, ku ktorým došlo po poslednom výpise z pamäti zóny. Je využívaný aj pri prírastkových zónových prenosoch (IXFR). Tieto protokolové súbory nemiznú. Ide o binárny súbor, ktorý by ste nemali upravovať.
db.<*secondary-zone-n*>		Ide o súbor sekundárnej zóny niektorej konkrétnej domény na tomto serveri. Obsahuje všetky zdrojové záznamy pre túto zónu. Tento súbor je použitý pri úvodnom zavedení pri spustení sekundárneho servera, ako bol primárny server nedostupný. Každá zóna má svoj vlastný osobitný súbor .db.
/QIBM/UserData/OS400/DNS/_DYN/		Adresár, ktorý udržiava súbory požadované na dynamické aktualizácie.
<*key_id-n*>._KEY		Symbolický odkaz na kľúč DNSSEC s kľúčom <*key_id-n*>. Smeruje vždy na najnovší vytvorený kľúč K<*key_id-n*>.+*aaa*+*nnnnn*.key.
<*key_id-x*>._DUK. <*zone-a*>		Kľúč dynamickej aktualizácie vyžadovaný pri inicializácii požiadavky na dynamickú aktualizáciu zóny <*zone-a*> pomocou kľúča <*key_id-x*>.
<*key_id-x*>._KID		Súbor, ktorý obsahuje príkaz kľúča pre key_id named <*key_id-x*>
<*key_id-y*>._DUK. <*zone-a*>		Kľúč dynamickej aktualizácie vyžadovaný pri inicializácii požiadavky na dynamickú aktualizáciu zóny <*zone-a*> pomocou kľúča <*key_id-y*>.
<*key_id-y*>._DUK. <*zone-b*>		Kľúč dynamickej aktualizácie vyžadovaný pri inicializácii požiadavky na dynamickú aktualizáciu zóny <*zone-b*> pomocou kľúča <*key_id-y*>.
<*key_id-y*>._KID		Súbor, ktorý obsahuje príkaz kľúča pre key_id named <*key_id-y*>

Názov	Ikona	Opis
rndc-confgen.random.*nnnnnn*		Entropické súbory vyžadované rozličnými súbormi. Časť *nnnnn* je číslo úlohy, ktorá súbor vytvorila. Ak je príkaz z nejakého dôvodu zrušený, ostane po ňom len tento súbor, ktorý nie je automaticky vymazaný.

Súvisiace koncepty

"Určenie oprávnení servera DNS" na strane 24
Pre administrátora DNS existujú špeciálne požiadavky na oprávnenia. Je potrebné zvážiť aj bezpečnostné aspekty autorizácie.

"Prístup k štatistikám servera DNS" na strane 33
Nástroje výpisu z pamäte databázy a štatistiky pomáhajú pri zisťovaní a riadení výkonu servera.

Súvisiace úlohy

"Konfigurácia názvových serverov" na strane 27
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 System i Navigator vám poskytuje rozhranie s rozšírenými funkciami, pomocou ktorých je možné konfigurovať a riadiť váš server DNS. Administrátori, ktorí sú už oboznámení s grafickým rozhraním systému i5/OS, majú k nasledujúcim úlohám prístup prostredníctvom ich zástupcov. Poskytujú rýchly spôsob, ktorým môžete naraz vo viacerých inštanciách zmeniť stav a atribúty servera.

Súvisiace úlohy

"Zmena nastavení ladenia DNS" na strane 39
Funkcia ladenia systému DNS môže poskytnúť informácie, ktoré vám pomôžu určiť a opraviť problémy so serverom DNS.

Spustenie a zastavenie serverov DNS

Ak DNS (Domain Name System) v rozhraní System i Navigator neumožňuje spustenie alebo zastavenie viacerých súbežných inštancií servera, môžete tieto nastavenia zmeniť naraz pre viaceré inštancie prostredníctvom znakového rozhrania.

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

Zmena hodnôt ladenia

Zmena úrovne ladenia je vhodná pre administrátorov veľkých zón, ktorí nechcú, aby bolo pri prvom spustení servera a zavedení zónových údajov zhromažďované veľké množstvo údajov ladenia.

Pokiaľ je server DNS (Domain Name System) spustený, neumožní vám DNS v rozhraní System i Navigator zmeniť úroveň ladenia. Prostredníctvom znakového rozhrania však môžete zmeniť úroveň ladenia aj počas behu servera. Ak chcete zmeniť úroveň ladenia prostredníctvom znakového rozhrania, postupujte podľa týchto krokov a premennú *nnnnn* v príkaze nahraďte názvom inštancie servera:

1. Na príkazovom riadku zadajte ADDLIBLE QDNS a stlačte kláves Enter.
2. Zmeňte úroveň ladenia:
   - Ak chcete ladenie zapnúť, alebo zvýšiť jeho úroveň o 1, napíšte RNDC RNDCCMD('trace') a stlačte kláves Enter.
   - Ak chcete ladenie vypnúť, napíšte RNDC RNDCCMD('notrace') a stlačte kláves Enter.

Odstraňovanie problémov s DNS

pri riešení problémov s vaším serverom DNS vám môžu pomôcť nastavenia protokolovania a ladenia serverov DNS (Domain Name System).

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.

Identifikácia úloh

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

- Ak prevádzkujete servery založené na BIND 9, bude existovať osobitná úloha pre každú spustenú inštanciu servera. Názov úlohy je vytvorený nemenným päťznakovým reťazcom (QTOBD) za ktorým nasleduje názov inštancie. Napríklad, ak máte dve inštancie INST1 a INST2, názvy ich úloh budú QTOBDINST1 a QTOBDINST2.

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.

Verzia BIND 9 ponúka niekoľko možností protokolovania. Môžete uviesť aké typy správ sa protokolujú, kam sa každý typ správy zasiela a aká závažnosť daného typu správy sa má protokolovať. Zvyčajne sú postačujúce aj predvolené nastavenia protokolovania, ak ich ale chcete zmeniť, odporúčame vám, aby ste si pozreli ďalšiu dokumentáciu k systému BIND 9, v ktorej nájdete bližšie informácie 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. Predvolené kanály súborov sú i5os_debug a i5os_QPRINT. Správy ladenia sú štandardne protokolované kanálom i5os_debug, ktorým je súbor named.run, ale môžete zadefinovať, aby boli do tohto súboru odosielané aj správy iných kategórií. Kategórie správ zaprotokolované cez i5os_QPRINT sú odosielané do spoolového súboru QPRINT užívateľského profilu QTCP. Okrem poskytovaných predvolených kanálov si môžete vytvoriť aj svoje vlastné kanály súborov.

- **Kanály syslog**

  Správy zaprotokolované do tohto kanálu sú odosielané do protokolu úlohy servera. Predvoleným kanálom syslog je i5os_joblog. Protokolované správy smerované na tento kanál sú odosielané do protokolu úlohy inštancie servera DNS.

- **Nulové kanály**

  Všetky správy zaprotokolované do kanála null budú vymazané. Predvoleným kanálom null je i5os_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. Existujú nasledujúce kategórie:

klient Spracovanie požiadaviek klientov.

config Analýza a spracovanie konfiguračných súborov.

database
Správy súvisiace s databázami, ktoré využíva server DNS pri internom ukladaní zónových údajov a údajov z pamäte cache.

štandard
Definície volieb protokolovania tých kategórií, pre ktoré nebola zadefinovaná žiadna konkrétna konfigurácia.

delegation-only
Len odoslanie. Protokoluje dotazy, ktoré boli nanútené doméne NXDOMAIN ako výsledok zóny delegation-only alebo výsledok použitia delegation-only v deklarácii zóny náznakov alebo čiastkovej zóny.

odoslať
Prideľovanie prichádzajúcich paketov serverovým modulom, v ktorých budú spracované.

dnssec Spracovanie protokolov DNSSEC (DNS Security Extensions) a TSIG (Transaction Signature).

general
Všeobecná kategória využívaná na položky, ktoré nie sú zaradené do žiadnej z ostatných kategórií.

lame-servers
Poškodené servery, ktoré sú nesprávne nakonfigurované na vzdialených serveroch, zistené systémom BIND 9 pri pokusoch o zadanie dotazu na tieto servery počas rozlíšenia dotazu.

sieť Sieťové operácie.

notify Protokol NOTIFY.

resolver
Preklady servera DNS, ako napríklad rekurzívne vyhľadávania, ktoré server vykonáva v mene klientov zavedením názvu servera do pamäte cache.

bezpečnosti
Schválenia a zamietnutia požiadaviek.

xfer-in Zónové prenosy, ktoré server prijíma.

xfer-out
Zónové prenosy, ktoré server odosiela.

unmatched
Správy, ktoré sú pomenované, pre ktoré nebolo možné určiť triedu alebo pre ktoré neexistovalo zhodné zobrazenie. Jednoriadkový súhrn je zaprotokolovaný aj do kategórie klient. Túto kategóriu je najlepšie odosielať do niektorého súboru alebo do protokolu stderr. Štandardne je odosielaná kanálu null.

update Dynamické aktualizácie.

update-security
Schválenia a zamietnutia požiadaviek na aktualizáciu. Dotazy určujú, kam by mali byť zaprotokolované. Zadefinovanie kategórií dotazov pri spustení umožňuje protokolovanie dotazov až kým nebude zadefinovaná voľba querylog.

Položka protokolu dotazov oznamuje IP adresu a číslo portu, názov dotazu, triedu a typ klienta. Oznamuje aj to, či bol nastavený príznak Recursion Desired (+ ak bol nastavený, - ak nebol nastavený), či bol použitý mechanizmus EDNS (E), alebo či bol dotaz podpísaný (S).

Protokolové súbory môžu rásť a je možné ich pravidelne vymazávať. Pri zastavení a spustení servera DNS je celý obsah protokolového súboru DNS vymazaný.

Závažnosť správy

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

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

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

Zmena nastavení protokolovania

Ak chcete vstupovať do volieb protokolovania, postupujte takto:

1. V System i Navigator rozviňte ***váš systém*** → **Network** → **Servers** → **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 na odstraňovanie problémov (úroveň závažnosti)

Predvolená úroveň závažnosti kanála i5os_joblog je nastavená na úroveň Error. Toto nastavenie sa používa na zníženie objemu informačných a upozorňujúcich správ, ktoré by v opačnom prípade znížili výkon. Ak však zaznamenáte problémy, pričom protokol úloh nenaznačuje žiaden zdroj týchto problémov, budete možno musieť zmeniť protokolovanú úroveň závažnosti. Pomocou vyššie popísanej procedúry môžete pristupovať na stránku Channels a zmeniť úroveň závažnosti pre kanál i5os_joblog na Warning, Notice alebo Info, vďaka čomu budete môcť zobrazovať väčšie množstvo zaprotokolovaných údajov. Po vyriešení problému nastavte znova úroveň závažnosti na hodnotu Error, čím opäť znížite počet protokolovaných správ.

Zmena nastavení ladenia DNS

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

DNS ponúka 12 úrovní riadenia ladenia. Aj napriek tomu, že samotné protokolovanie zvyčajne poskytuje jednoduchšiu metódu vyhľadania problému, v niektorých prípadoch môže byť nevyhnutné použiť 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. Pri hodnotách 1 a vyšších je sú informácie ladenia zapisované do súboru named.run v adresári vášho systému i5/OS s cestou: /QIBM/UserData/OS400/DNS/<*server instance*>, pričom premenná <*server instance*> je názvom inštancie servera DNS. Súbor named.run rastie o celý čas,

kým máte úroveň ladenia nastavenú na hodnotu 1 alebo vyššiu a kým je spustený server DNS. Preferencie maximálnej veľkosti a počtu verzií súboru named.run môžete určiť na stránke Server Properties - Channels.

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

1. V System i Navigator rozviňte ***váš systém*** → **Network** → **Servers** → **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 36
Táto téma vysvetľuje spôsob použitia rozšírených vlastností systému DNS skúsenými administrátormi na ľahšie manažovanie servera DNS.

Súvisiace informácie pre systém DNS

informácie súvisiace so súhrnom tém DNS (Domain Name System) obsahujú publikácie IBM Redbooks, webové stránky a ostatné súhrny tém informačného centra. Ľubovoľný z týchto súborov PDF môžete zobraziť alebo vytlačiť.

Dokumenty IBM Redbook

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

V tejto publikácii Redbooks je popísaná podpora, ktorú serverom DNS (Domain Name System) a DHCP (Dynamic Host Configuration Protocol) poskytuje operačný systém i5/OS. Pomocou príkladov vám môže pomôcť pri inštalácii, úpravách, konfigurácii a odstraňovaní problémov s podporou DNS a DHCP.

Webové lokality

- *DNS and BIND*, piate vydanie. Paul Albitz and Cricket Liu. Vydalo O'Reilly and Associates,Inc. Sebastopol, California, 2006. Číslo ISBN: 0-59610-057-4.
- Referenčná príručka pre administrátorov systému BIND (vo verzii PDF) z webových stránok Internet System Consortium (ISC).
- Webové stránky Internet Software Consortium obsahujú novinky, odkazy a ostatné zdroje k systému BIND.
- Stránka InterNIC udržiava adresár všetkých registrátorov názvov domén autorizovaných asociáciou Internet Corporation for Assigned Names and Numbers (ICANN).
- Webové stránky DNS Resources Directory poskytujú referenčné materiály k DNS a odkazy na mnoho ďalších informačných zdrojov, vrátane diskusných skupín. Poskytujú tiež zoznam štandardov RFC súvisiacich s DNS.

Súvisiaci odkaz

"Súbor PDF k téme DNS (Domain Name System)" na strane 2
Môžete zobraziť alebo vytlačiť súbor PDF týchto informácií.

Príloha. Poznámky

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

V iných krajinách nemusí spoločnosť IBM ponúkať produkty, služby alebo vlastnosti, uvedené v tomto dokumente. Ak chcete získať informácie o produktoch a službách, ktoré sú aktuálne dostupné vo vašej oblasti, kontaktujte lokálneho zástupcu spoločnosti IBM. Žiadny odkaz na produkt, službu alebo program IBM nemá za účelom naznačiť, že je možné použiť len tento produkt, službu alebo program IBM. Namiesto toho je možné použiť ľubovoľný funkčne ekvivalentný produkt, službu alebo program, ktorý neporušuje právo na intelektuálne vlastníctvo spoločnosti IBM. Je však na zodpovednosti užívateľa, aby zhodnotil a overil fungovanie všetkých produktov, programov alebo služieb, ktoré nie sú od IBM.

Spoločnosť IBM môže vlastniť patenty alebo mať podané žiadosti o patenty, ktoré sa týkajú predmetu opísaného 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.

Požiadavky na licencie, týkajúce sa dvojbajtových (DBCS) informácií, smerujte na Oddelenie duševného vlastníctva spoločnostiIBM vo vašej krajine alebo ich pošlite 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. Spoločnosť IBM môže kedykoľvek bez ohlásenia urobiť vylepšenia a/alebo zmeny v produktoch alebo programoch opísaných 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 na týchto webových lokalitách nie sú súčasťou materiálov pre tento produkt IBM a použitie týchto webových lokalít je na vlastné riziko.

Spoločnosť IBM môže použiť alebo distribuovať všetky vami poskytnuté informácie ľubovoľným spôsobom, ktorý považuje za vhodný, bez toho, aby tým voči vám vznikli akékoľvek záväzky.

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 tomto dokumente, 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 programovacom rozhraní

Táto publikácia Domain Name System (DNS) dokumentuje určené programovacie rozhrania umožňujúce klientovi písať programy, ktorými bude pristupovať k službám systému IBM i5/OS.

Ochranné známky

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

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

Adobe, logo Adobe, PostScript a logo PostScript sú buď registrovanými ochrannými známkami alebo ochrannými známkami spoločnosti Adobe Systems Incorporated v USA a/alebo iných krajinách.

Ostatné názvy spoločnosti, produktov alebo služieb môžu byť ochranné známky alebo značky služieb iných.

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 nemôžete prevziať ani exportovať okrem prípadu, ak to dovoľujú všetky aplikovateľné zákony a regulácie, vrátane všetkých zákonov a regulácií USA pre export.

SPOLOČNOSŤ 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