



System i

Hálózatkezelés:

Tartománynév-rendszer (DNS)

6. változat 1. kiadás





System i

Hálózatkezelés:

Tartománynév-rendszer (DNS)

6. változat 1. kiadás

Megjegyzés

Mielőtt a jelen leírást és a vonatkozó terméket használná, olvassa el a “Nyilatkozatok”, oldalszám: 41 helyen lévő tájékoztatót.

Ez a kiadás az IBM i5/OS (termékszám: 5761-SS1) 6. változat, 1. kiadás, 0 módosítására, valamint az ezt követő összes kiadásra és módosításra vonatkozik kivéve, ha az új kiadások azt másképpen jelzik. Ez a változat nem fut minden csökkentett utasításkészletű (RISC) rendszeren illetve a CISC modelleken.

© Szerzői jog IBM Corporation 1998, 2008. Minden jog fenntartva

Tartalom

Tartománynév-rendszer	1
A V6R1 újdonságai	1
Tartománynév-rendszer PDF fájl	2
Tartománynév-rendszer fogalmak	3
Zónák bemutatása	3
Tartománynév-rendszer lekérdezések bemutatása	4
Tartománynév-rendszer tartomány beállítás.	6
Dinamikus frissítések	6
BIND 9 szolgáltatások	8
DNS erőforrásrekordok	9
Posta és MX rekordok	12
Példák: Tartománynév-rendszer.	13
Példa: Egyedülálló Tartománynév-rendszer szerver intranethez	14
Példa: Egyedülálló Tartománynév-rendszer szerver Internet-hozzáféréssel.	15
Példa: Tartománynév-rendszer és Dinamikus hoszt konfigurációs protokoll ugyanazon a System i platformon	17
Példa: DNS felosztása tűzfalon keresztül, két DNS szervert telepítve ugyanarra a System i platformra	19
Példa: DNS felosztása tűzfalon keresztül nézet segítségével.	21
Tartománynév-rendszer tervezése	23
Tartománynév-rendszer jogosultságok megállapítása	23
Tartományszerkezet meghatározása.	23
Biztonsági intézkedések tervezése	24
Tartománynév-rendszer követelmények	25
Tartománynév-rendszer telepítésének ellenőrzése	26
Tartománynév-rendszer telepítése	26
Tartománynév-rendszer beállítása	26
Tartománynév-rendszer elérése a System i navigátor programban.	26
Névszerverek beállítása	26
Névszerver példány létrehozása	27
Tartománynév-rendszer szerver tulajdonságainak szerkesztése	27
Zónák beállítása névszerveren	27
Nézetek beállítása névszerveren.	28
Tartománynév-rendszer beállítása dinamikus frissítések fogadására	28
Tartománynév-rendszer fájlok importálása	29
Rekord érvényesítés	29
Külső Tartománynév-rendszer adatok elérése.	29
Tartománynév-rendszer kezelése	30
Tartománynév-rendszer funkció működésének ellenőrzése	30
Biztonsági kulcsok kezelése	31
Tartománynév-rendszer kulcsok kezelése	31
Dinamikus frissítési kulcsok kezelése	31
Tartománynév-rendszer szerver statisztika elérése	32
Szerver statisztika elérése	32
Aktív szerver adatbázis elérése	32
Tartománynév-rendszer konfigurációs fájlok karbantartása	33
Fejlett Tartománynév-rendszer funkciók	35
Tartománynév-rendszer szerverek indítása és leállítása.	35
Hibakeresési értékek módosítása	36
Tartománynév-rendszer hibaelhárítása	36
Tartománynév-rendszer szerver üzenetek naplózása	36
Tartománynév-rendszer hibakeresési beállításainak módosítása	39
Tartománynév-rendszer témakörhöz kapcsolódó információk.	39
. Nyilatkozatok	41
Programozási felületre vonatkozó információk	42
Védjegyek	43
Feltételek és kikötések	43

Tartománynév-rendszer

A *Tartománynév-rendszer (DNS)* hosztnevek és a hozzájuk tartozó Internet protokoll (IP) címek kezelésére szolgáló osztott adatbázis rendszer.

| DNS esetén a hoszt keresésére egyszerű nevek (például `www.jkltoys.com`) használhatók IP címek helyett (például `192.168.12.88` IPv4 esetén vagy `2001:D88::1` IPv6 esetén). Egyetlen szerver csak a zóna kis részében ismerheti a hosztneveket és IP címeket, de a DNS szerverek együttműködve képesek az összes tartománynevet leképezni IP címekre. Az együttműködő DNS szerverek a számítógépek számára lehetővé teszik a kommunikációt az Interneten keresztül.

| Az IBM i5/OS 6. verzió 1. kiadás (V6R1) esetében a DNS szolgáltatások a Berkeley Internet névtartomány (BIND) 9. változatként ismert ipari szabvány DNS megvalósításon alapulnak. A korábbi i5/OS kiadások esetében a DNS szolgáltatások a BIND 8.2.5 változatra épültek. Az új, BIND 9. változatra épülő DNS szerver használatához telepített i5/OS 31. opcióval (DNS) és 33. opcióval (Hordozható alkalmazásmegoldás környezet (PASE)) kell rendelkeznie a IBM System i modellen. Az i5/OS V6R1 óta biztonsági okokból a BIND 4. és 8. változatot BIND 9. változatra cserélték le. Így a DNS szerveren az áttelepítés BIND 9. változatra kötelező.

A V6R1 újdonságai

| Az alábbiakban a Tartománynév-rendszer (DNS) témakör gyűjtemény új vagy jelentősen megváltozott információiról olvashat.

BIND 9

| A Berkeley Internet névtartomány (BIND) ebben a kiadásban bevezetett 9. változata számos szolgáltatást kínál a Tartománynév-rendszer (DNS) szerver teljesítményének javítása céljából. Az összes jelenleg meghatározott IPv6 formátumban támogatja például a név-cím és a cím-név kikereséseket. A *nézet* utasítást használja, ami egyetlen DNS példány számára ugyanazon lekérdezés különböző megválaszolását teszi lehetővé attól függően, hogy a lekérdezés honnan érkezik (például az Internetről vagy intranetből). Ezenkívül a zóna dinamikus frissítéseinek tárolására naplófájlokat használ.

| A korábbi BIND változatok (4.9.3 és 8.2.5) már nem támogatottak és áttelepítésük BIND 9. változatra kötelező.

Új konfigurációs parancsok

| A következő konfigurációs parancsok kerültek hozzáadásra a rendszeren található DNS konfigurációs fájlok kezelésének megkönnyítésére.

RNDC konfiguráció létrehozása (CRTRNDCCFG)

| Az RNDC konfigurációs segédprogram (CRTRNDCCFG) parancsot RNDC konfigurációs fájlok előállítására használják. Kényelmes alternatívája ez az `rndc.conf` fájl írásának, valamint a megfelelő vezérlőelemek és kulcs utasítások írásának a `named.conf` fájlba.

DNS konfigurációs segédprogram (CHKDNSCFG)

| A DNS konfigurációs segédprogram (CHKDNSCFG) parancs a `named.conf` nevű konfigurációs fájl szintaxisát ellenőrzi. Nem biztosít azonban támogatást a konfigurációs fájl szemantikájának ellenőrzéséhez.

DNS zóna segédprogram (CHKDNSZNE)

| A DNS zóna segédprogram (CHKDNSZNE) parancs zóna adatfájl szintaxisát és integritását ellenőrzi. Jól használható a zóna adatfájlok ellenőrzésére, mielőtt a DNS szerverhez hozzáadja azokat.

Új lekérdezési és frissítési segédprogramok

Az alábbi lekérdezési és frissítési segédprogramok a DNS szerver felügyeleti képességeinek bővítése céljából kerültek hozzáadásra.

Tartományinformáció kereső (DIG)

A DIG lekérdezési eszköz segítségével hosztokra, tartományokra és más DNS szerverekre vonatkozó DNS információkat kérhet le a DNS szerver válasza alapján. A segítségével azt is ellenőrizheti, hogy a DNS szerver helyes válaszokat ad-e, mielőtt rendszerét beállítja annak használatára.

HOST lekérdezés indítása(HOST)

A HOST lekérdezés indítása (HOST) parancsot DNS kikeresésekhez használják. Tartományneveket IP címekké (akár IPv4, akár IPv6) alakít át és vissza.

Dinamikus frissítési segédprogram (NSUPDATE)

A Dinamikus frissítési segédprogram (NSUPDATE) parancs segítségével DNS szervernek Dinamikus DNS frissítési kérések küldhetők, az RFC 2136-os dokumentumban meghatározottaknak megfelelően. Ez erőforrásrekordok hozzáadását és eltávolítását teszi lehetővé a zónában, miközben a DNS szerver fut. Így a rekordok frissítéséhez nincs szükség a zóna fájl kézi szerkesztésére. Egyetlen frissítési kérés több erőforrásrekord hozzáadására vagy eltávolítására vonatkozó kéréseket is tartalmazhat, de az NSUPDATE parancs segítségével dinamikusan hozzáadott vagy eltávolított erőforrásrekordoknak ugyanabban a zónában kell lenniük.

Távoli névdémon felügyelet (RNDC)

A Távoli névdémon felügyelet (RNDC) parancs a rendszeradminisztrátor számára névszerver működésének felügyeletét teszi lehetővé. Az *rndc.conf* konfigurációs fájl beolvasva megállapítja, hogy miként kell a névszerverrel a kapcsolatot felvenni és eldönti, hogy milyen algoritmust és kulcsot kell használni. Ha az *rndc.conf* fájl nem található, akkor alapértelmezésben a telepítés során létrehozott *rndc-key._KID* fájl kerül felhasználásra, amely a hozzáférést automatikusan biztosítja a loopback csatolón keresztül.

Új vagy megváltozott információk azonosítása

A technikai változásokon keresztülment helyeket az Információs központ az alábbiak szerint jelöli:

- A ➤ kép jelzi az új vagy módosított információk kezdetét.
- A ⏪ kép jelöli az új vagy megváltozott információk végének helyét.

A PDF fájlokban az új vagy módosított információk mellett felülvizsgálati jelek (I) láthatók a bal oldali margón.

Kapcsolódó hivatkozás

“BIND 9 szolgáltatások” oldalszám: 8

A BIND 9 és a BIND 8 hasonlóak; az előbbi azonban a Tartománynév-rendszer (DNS) szerver teljesítményének javítására számos szolgáltatást biztosít (például nézeteket).

Tartománynév-rendszer PDF fájl

Az információkat tartalmazó PDF fájlt megjelenítheti és kinyomtathatja.


A PDF változat megtekintéséhez vagy letöltéséhez válassza ki a Tartománynév-rendszer (kb. 625 KB) hivatkozást.

PDF fájlok mentése

A PDF fájl munkaállomáson történő mentése megjelenítés vagy nyomtatás céljából:

1. Kattintson a jobb egérgombbal a böngészőben a PDF hivatkozásra.
2. Kattintson a PDF helyi mentésére szolgáló opcióra.
3. Válassza ki azt a katalógust, ahová menteni kívánja a PDF fájlt.
4. Kattintson a **Mentés** gombra.

Adobe Acrobat Reader letöltése

A PDF fájlok megjelenítéséhez és nyomtatásához a rendszerre telepített Adobe Reader szükséges. Ingyenes példánya az Adobe webhelyről (www.adobe.com/products/acrobat/readstep.html)  letölthető.

Kapcsolódó hivatkozás

“Tartománynév-rendszer témakörhöz kapcsolódó információk” oldalszám: 39

Az IBM Redbooks kiadványok, webhelyek és egyéb információs központi témakör gyűjtemények is tartalmazzák a Tartománynév-rendszer (DNS) témakör gyűjteményhez kapcsolódó információkat. A PDF fájlokat megtekintheti vagy kinyomtathatja.

Tartománynév-rendszer fogalmak

- | A Tartománynév-rendszer (DNS) olyan osztott adatbázis rendszer, amely az Internet protokoll (IP) címekhez tartozó hosztnév kezelésére szolgál. DNS esetén a hoszt keresésére egyszerű nevek (például www.jkltoys.com) használhatók
- | IP címek helyett (például 192.168.12.88 IPv4 esetén vagy 2001:D88::1 IPv6 esetén).

Egyetlen szerver csak a zóna kis részében ismerheti a hosztnéveket és IP címet, de a DNS szerverek együttműködve képesek az összes tartománynevet leképezni IP címekre. Az együttműködő DNS szerverek a számítógépek számára lehetővé teszik a kommunikációt az Interneten keresztül.

A DNS adatok véget vetnek a tartományok hierarchiájának. A szerverek csak az adatok egy kis részének ismeretért felelősek, mint például egyetlen altartomány adataiért. A tartomány adott részét - amelyért a szerver közvetlenül felelős - zónának hívják. A DNS szerver, amely a zóna hoszt információit és adatait kezeli, hitelesnek tekinthető a zóna vonatkozásában. A hiteles szerver válaszolni tud a zónájában lévő hosztokra vonatkozó lekérdezésekre saját erőforrásrekordjai segítségével. A lekérdezési folyamat a tényezők számától függ. A DNS lekérdezések bemutatása rész azokat a módszereket magyarázza el, amelyeket a kliens lekérdezés feloldására használhat.

Zónák bemutatása

A Tartománynév-rendszer (DNS) adatok kezelhető adatkészletekre (úgynevezett *zónákra*) oszlanak. Minden ilyen készlet egy bizonyos zóna típus.

- | A zónák a DNS tartomány egy vagy több részének neveit és IP címeket tartalmazzák. A zóna összes információit tartalmazó szerver a tartomány hiteles szervere, amelyet *szülő zónának* neveznek. Időnként érdemes lehet átadni egy adott altartományra vonatkozó DNS lekérdezések megválaszolásának jogosultságát egy másik DNS szervernek, amit *utódzónának* neveznek. Ebben az esetben a tartomány DNS szerverét úgy kell konfigurálni, hogy az adott altartományra vonatkozó lekérdezések esetén a megfelelő szerverre hivatkozzon.

Biztonsági mentés és redundancia céljából a zóna adatokat gyakran tárolják a hiteles DNS szervertől eltérő szervereken is. Ezek az egyéb szerverek a másodlagos szerverek, amelyek a hiteles szerverről töltik fel a zóna adatokat. A másodlagos szerverek megadása lehetővé teszi a szervereken fellépő igények kiegyensúlyozását, valamint tartalékként is szolgál abban az esetben, ha az elsődleges szerver meghibásodik. A másodlagos szerverek zóna átvitel révén szerzik meg a zóna adatokat a hiteles szervertől. Amikor a másodlagos szerver inicializálódik, a zóna adatok egy teljes példányát betölti az elsődleges szerverről. A másodlagos szerver akkor is újra betölti a zóna adatokat az elsődleges szerverről vagy a tartomány egy másik másodlagos szerveréről, amikor változnak a zóna adatok.

DNS zónatípusok

A i5/OS DNS segítségével megadhatja a zónák számos típusát, amelyek a DNS adatok kezelését segítik:

Elsődleges zóna

Az elsődleges zóna a zóna adatokat közvetlenül a hoszton lévő fájlból tölti be. Az elsődleges zóna tartalmazhat alzónát vagy utódzónát. Tartalmazhat továbbá erőforrásrekordokat, mint például hoszt, álnév (CNAME), IPv4 cím (A), IPv6 cím (AAAA) vagy fordított leképezési mutató (PTR) rekordokat.

Megjegyzés: Az elsődleges zónákat időnként *mester vagy fő zónaként* is emlegetik más BIND dokumentációk.

Alzóna Az alzóna egy zónát határoz meg az elsődleges zónán belül. Az alzónák lehetővé teszik, hogy a zóna adatokat kezelhető darabokba szervezze.

Utódzóna

Az utódzóna megad egy alzónát, és delegálja az alzóna adatokra vonatkozó felelősséget egy vagy több névszervernek.

Álnév (CNAME)

Az álnév megad egy alternatív nevet az elsődleges tartomány nevére.

Hoszt A hoszt objektum leképezi az A és a PTR rekordokat a hoszt számára. A hoszthoz további erőforrásrekordok tartozhatnak.

Másodlagos zóna

A másodlagos zóna betölti a zóna adatokat a zóna elsődleges szerveréről vagy egy másik másodlagos szerverről. A másodlagos szerver karbantartja annak a zónának teljes példányát, amelyre nézve másodlagos.

Megjegyzés: A másodlagos zónákat *alárendelt zónaként* is említik más BIND dokumentációban.

| Csonk zóna

| A csonk zóna hasonló a másodlagos zónához, de ez csak a névszerver (NS) rekordokat viszi át.

| Továbbítási zóna

| A továbbítási zóna egy adott zónára vonatkozó minden lekérdezést más szerverekhez irányít.

Kapcsolódó fogalmak

“Tartománynév-rendszer lekérdezések bemutatása”

A Tartománynév-rendszer (DNS) kliensek lekérdezések feloldására DNS szervereket használnak. A lekérdezések érkezhetnek közvetlenül a klientsől vagy a kliensen futó alkalmazástól.

Kapcsolódó feladatok

“Zónák beállítása névszerveren” oldalszám: 27

Miután konfigurálta a Tartománynév-rendszer (DNS) szerver példányt, be kell állítania a zónákat az adott névszerverre.

Kapcsolódó hivatkozás

“Példa: Egyedülálló Tartománynév-rendszer szerver intranethez” oldalszám: 14

A példa egyszerű alhálózatot mutat DNS szerverrel belső használatra.

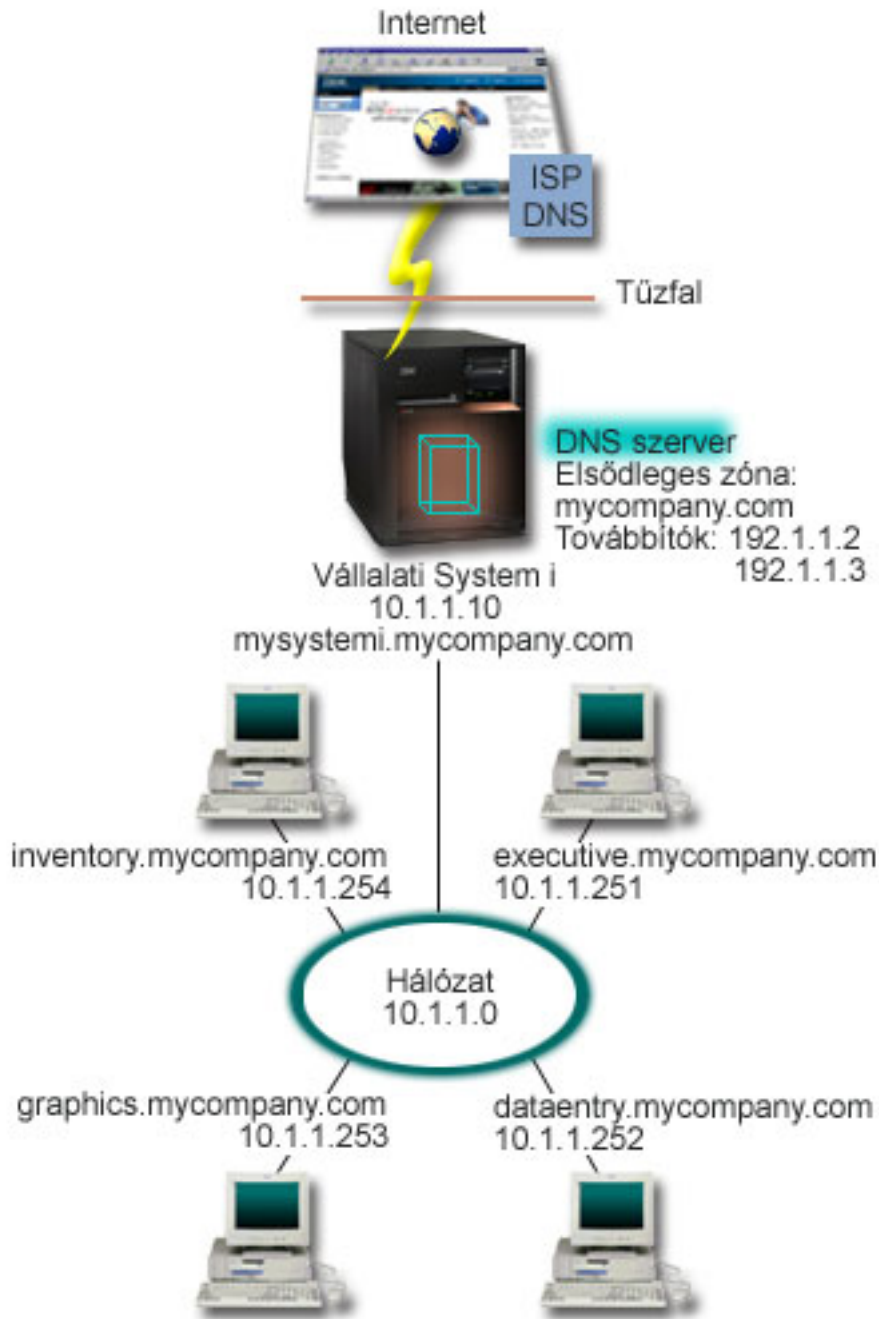
“DNS erőforrásrekordok” oldalszám: 9

Az erőforrásrekordok a tartománynevek és az IP címek adatainak tárolására szolgálnak. Az i5/OS operációs rendszer esetén támogatott erőforrásrekordokat az Erőforrásrekord kikeresési táblában tekintheti meg.

Tartománynév-rendszer lekérdezések bemutatása

A Tartománynév-rendszer (DNS) kliensek lekérdezések feloldására DNS szervereket használnak. A lekérdezések érkezhetnek közvetlenül a klientsől vagy a kliensen futó alkalmazástól.

A kliens elküldi a lekérdezési üzenetet a DNS szervernek, amely tartalmazza a teljes képzésű tartománynevet (FQDN), a lekérdezés típusát, mint például egy adott erőforrásrekord, amelyet a kliens kér, valamint a tartománynév osztályát, amely általában az Internet (IN) osztály. A következő ábra a minta hálózatot mutatja be az Egy DNS szerver Internet hozzáféréssel példából.



1. ábra: Egyetlen DNS szerver Internet hozzáféréssel

Tételezzünk fel, hogy a hoszt *adatrögzítés* lekérdezi a DNS szerverről a grafika.sajátcég.com címet. A DNS szerver saját zóna adatait fogja használni, és a 10.1.1.253 IP címmel fog válaszolni.

- | Tegyük fel, hogy az *adatrögzítés* kéri a www.jkl.com IP címet. Ez a hoszt nincs benne a DNS szerver zóna adataiban.
- | Két járható út áll rendelkezésre: *rekurzió* vagy *iteráció*. Ha a DNS szervernél be van állítva a *rekurzió*, akkor a szerver
- | lekérdezhet vagy kapcsolatba léphet más DNS szerverekkel a kérő kliens nevében, hogy teljesen feloldja a nevet,
- | amelyet azután válaszként visszaküld a kliensnek. Ezenkívül a kérő szerver a választ az ideiglenes tárolójában tárolja,
- | így a válasz legközelebb is felhasználható, amikor a szerver ugyanazt a kérést fogadja. Ha a DNS szerver *iteráció*

- | használatára van beállítva, akkor a kliens név feloldása céljából maga kísérelhet meg kapcsolatba lépni más DNS
- | szerverekkel. Ebben a folyamatban a kliens a szerverek hivatkozás válaszain alapuló, különálló és kiegészítő
- | lekérdezéseket használ.

Kapcsolódó hivatkozás

“Zónák bemutatása” oldalszám: 3

A Tartománynév-rendszer (DNS) adatok kezelhető adatkészletekre (úgynevezett *zónákra*) oszlanak. Minden ilyen készlet egy bizonyos zóna típus.

“Példa: Egyedülálló Tartománynév-rendszer szerver Internet-hozzáféréssel” oldalszám: 15

A példa egyszerű alhálózatot mutat Tartománynév-rendszer (DNS) szerverrel, közvetlen Internet-kapcsolattal.

Tartománynév-rendszer tartomány beállítás

A Tartománynév-rendszer (DNS) tartomány beállítása tartománynév regisztrálását követeli meg megakadályozandó, hogy mások is használják a tartománynevet.

A DNS nevek és címek kiszolgálását teszi lehetővé intraneten vagy belső hálózaton. Ugyancsak lehetővé teszi nevek és címek kiszolgálását a világ fennmaradó részén is, az Interneten keresztül. Ha tartományokat állít be az Interneten, akkor a tartománynevet regisztráltatni kell.

Ha intranetet épít fel, akkor nem szükséges regisztráltatni a tartománynevet belső használat esetén. Az intranet nevének regisztráltatása csak attól függ, akarja-e, hogy senki más ne használhassa ezt a nevet az Interneten, függetlenül attól, hogy egyelőre csak belső célra használja. Az egyelőre belső célra használt név bejegyeztetésével biztos lehet abban, hogy sohasem kerül konfliktusba, ha később külsőleg is használni akarja a tartománynevet.

A tartománynév bejegyzését elintézheti, ha közvetlen kapcsolatba lép egy felhatalmazott tartománynév bejegyzővel, vagy esetleg egy Internet szolgáltató (ISP) keresztül. Egyes ISP szolgáltatók vállalják a tartománynév bejegyzési kérések benyújtását a kérő nevében. Az Internet Network Information Center (InterNIC) karbantartja az összes tartománynév bejegyző katalógusát, amelyeket az Internet Corporation for Assigned Names and Numbers (ICANN) jogosított fel.

Kapcsolódó hivatkozás

“Példa: Egyedülálló Tartománynév-rendszer szerver Internet-hozzáféréssel” oldalszám: 15

A példa egyszerű alhálózatot mutat Tartománynév-rendszer (DNS) szerverrel, közvetlen Internet-kapcsolattal.

Kapcsolódó tájékoztatás



Internet hálózati információs központ (InterNIC)

Dinamikus frissítések

A BIND 9. változaton alapuló i5/OS Tartománynév-rendszer (DNS) támogatja a dinamikus frissítéseket. Külső források, például Dinamikus hoszt konfigurációs protokoll (DHCP), a DNS szervernek frissítéseket küldhetnek. Ezenkívül a dinamikus frissítések végrehajtására DNS kliens eszközök, például Dinamikus frissítési segédprogram (NSUPDATE), is használhatók.

A DHCP egy TCP/IP szabvány, amely egy központi szervert használ az IP címek és egyéb konfigurációs elemek kezelésére az egész hálózat számára. A DHCP szerver válaszol a kliensektől érkező kérésekre azzal, hogy dinamikusan hozzájuk rendelje a tulajdonságokat. A DHCP lehetővé teszi, hogy megadjon egy hálózati hoszt konfigurációs paramétert egy központi helyen, és automatizálja a hosztok konfigurálását. Gyakran használatos arra, hogy a kliensekhez hozzárendelje az ideiglenes IP címet a hálózaton, amely több klienst tartalmaz, mint ahány IP cím áll rendelkezésre.

- | Korábban az összes DNS adatot egy statikus adatbázis tárolta. Az összes DNS erőforrásrekordot az adminisztrátornak
- | kellett létrehozni és karbantartani. A BIND 8. vagy újabb változatán alapuló DNS szerverek azonban úgy is
- | konfigurálhatók, hogy egyéb forrásoktól fogadjanak kéréseket a zóna adatok frissítése céljából.

Konfigurálhatja úgy a DHCP szervert, hogy küldje el a frissítési kérést a DNS szervernek, valahányszor egy új címet rendel hozzá a hoszthoz. Az automatizált folyamat csökkenti a DNS szerver adminisztrációját a gyorsan növekvő vagy

változó TCP/IP hálózatok esetében, valamint azokban a hálózatokban, ahol a hosztok helye gyakran változik. Amikor a DHCP funkciót használó kliens kap egy IP címet, az adatok azonnal elküldésre kerülnek a DNS szerverhez is. Ezzel a módszerrel a DNS folytatni tudja a hosztokra vonatkozó lekérdezések sikeres megoldását, még akkor is, ha az IP címek változnak.

| A DHCP konfigurálható úgy, hogy a kliens nevében frissítse a címlekepezési rekordokat (A IPv4 esetén és AAAA IPv6
| esetén), a fordított kikeresési mutató (PTR) rekordokat, vagy mindkét rekordot. A címlekepezési rekord (A vagy
| AAAA) a gép nevét képezi le annak IP címére. A PTR rekord leképezi a gép IP címét hoszt névre. Amikor megváltozik
| egy kliens címe, a DHCP automatikusan frissítést küld a DNS szervernek, ezért a hálózat többi hosztja mindig képes
| megtalálni a klienst DNS lekérdezéseken keresztül, az új IP címe alapján. Minden egyes rekordhoz, amely dinamikusan
| frissül, egy Szöveg (TXT) rekord is hozzá lesz írva, amely azonosítja, hogy a rekordot a DHCP írta.

| **Megjegyzés:** Ha a DHCP szervert úgy állítja be, hogy csak a PTR rekordokat frissítse, akkor úgy kell konfigurálni a
| DNS rendszert, hogy az megengedje a kliensektől jövő frissítéseket, hogy minden kliens frissíteni tudja
| A rekordját (IPv4 címek használata esetén) vagy AAAA rekordját (IPv6 címek használata esetén). Nem
| minden DHCP kliens támogatja saját A vagy AAAA rekordjának frissítési kéréseit. Tanulmányozza a
| kliens platformra vonatkozó dokumentációt, mielőtt ezt a módszert választja.

A dinamikus zónák biztonságosak, ha készít egy listát azokról a felhatalmazott forrásokról, amelyeknek megengedte a frissítések küldését. A felhatalmazott forrásokat definiálhatja egyedi IP címekkel, teljes alhálózattal, csomagokkal, amelyek egy megosztott titkosítási kulcs segítségével meg vannak jelölve (*Tranzakciós aláírás* vagy TSIG), vagy ezen módszerek valamilyen kombinációjával. A DNS, mielőtt frissítené az erőforrásrekordokat, ellenőrzi, hogy a beérkező kérés csomag felhatalmazott forrástól származik-e.

A DNS és a DHCP közötti dinamikus frissítések végrehajthatók egyetlen System i platformon, különböző System i platformok között vagy System i platform és egyéb, dinamikus frissítések támogatására képes rendszerek között.

| **Megjegyzés:** A DNS felé dinamikus frissítéseket küldő szervereken a dinamikus frissítés DNS (QTOBUPDT) API
| telepítése kötelező. Az API az i5/OS 31. opcióval (DNS) együtt automatikusan telepítésre kerül. A BIND
| 9. változatában azonban az NSUPDATE parancs a System i platformon végzett frissítések előnyben
| részesített módszere.

Kapcsolódó fogalmak

Dinamikus hoszt konfigurációs protokoll

Kapcsolódó feladatok

“Tartománynév-rendszer beállítása dinamikus frissítések fogadására” oldalszám: 28

A BIND 9. változatot futtató Tartománynév-rendszer (DNS) szerverek beállíthatók úgy, hogy a zóna adatok frissítése céljából más forrásoktól fogadjanak el kéréseket. Ez a témakör az engedélyezés-frissítés opció konfigurálására vonatkozó utasításokat tartalmazza, amelynek révén a DNS fogadni tudja a dinamikus frissítéseket.

DHCP konfigurálása dinamikus frissítések küldésére

Kapcsolódó hivatkozás

“Példa: Tartománynév-rendszer és Dinamikus hoszt konfigurációs protokoll ugyanazon a System i platformon” oldalszám: 17

Ez a példa Tartománynév-rendszert (DNS) és Dinamikus hoszt konfigurációs protokollt (DHCP) mutat be ugyanazon a System i platformon.

“DNS erőforrásrekordok” oldalszám: 9

Az erőforrásrekordok a tartománynevek és az IP címek adatainak tárolására szolgálnak. Az i5/OS operációs rendszer esetén támogatott erőforrásrekordokat az Erőforrásrekord kikeresési táblában tekintheti meg.

QTOBUPDT

“BIND 9 szolgáltatások” oldalszám: 8

A BIND 9 és a BIND 8 hasonlóak; az előbbi azonban a Tartománynév-rendszer (DNS) szerver teljesítményének javítására számos szolgáltatást biztosít (például nézeteket).

| **BIND 9 szolgáltatások**

| A BIND 9 és a BIND 8 hasonlóak; az előbbi azonban a Tartománynév-rendszer (DNS) szerver teljesítményének javítására számos szolgáltatást biztosít (például nézeteket).

| **Nézetek egyetlen i5/OS DNS szerveren**

| A *nézet* utasítás egyetlen DNS példány számára ugyanazon lekérdezés különböző megválaszolását teszi lehetővé attól függően, hogy a lekérdezés honnan érkezik (például az Internetről vagy intranetből).

| A nézet szolgáltatás egyik gyakorlati alkalmazása a DNS telepítések felosztása több DNS szerver futtatása nélkül. Egyedülálló DNS szerveren meghatározhat például olyan nézetet, amely a belső hálózat lekérdezéseit válaszolja meg, ugyanakkor meghatározhat másik nézetet is, amely külső hálózatról érkező lekérdezésekre válaszol.

| **Új kliens parancsok**

| A következő kliens parancsok a DNS szerver kezelési képességeit terjesztik ki:

| **Dinamikus frissítési segédprogram (NSUPDATE)**

| A Dinamikus frissítési segédprogram (NSUPDATE) parancs segítségével DNS szervernek Dinamikus DNS frissítési kérések küldhetők, az RFC 2136-os dokumentumban meghatározottaknak megfelelően. Ez erőforrásrekordok hozzáadását és eltávolítását teszi lehetővé a zónában, miközben a DNS szerver fut. Így a rekordok frissítéséhez nincs szükség a zóna fájl kézi szerkesztésére. Egyetlen frissítési kérés több erőforrásrekord hozzáadására vagy eltávolítására vonatkozó kéréseket is tartalmazhat, de az NSUPDATE parancs segítségével dinamikusan hozzáadott vagy eltávolított erőforrásrekordoknak ugyanabban a zónában kell lenniük.

| **Megjegyzés:** Az NSUPDATE parancs vagy DHCP szerver segítségével dinamikusan felügyelt zónákat soha nem szerkessze saját kezűleg. A kézi szerkesztések a dinamikus frissítésekkel ütközhetnek és adatvesztést okozhatnak.

| **DIG lekérdezés indítása (DIG)**

| A Tartományinformáció kereső (DIG) a Névszerver kikeresés (NSLOOKUP) parancshoz képest sokkal hatékonyabb lekérdező eszköz, amelyet DNS szerver információinak lekérésére, illetve a DNS szerver válaszának tesztelésére használhat. Az NSLOOKUP parancs elavult és kizárólag azért biztosítják, hogy a kompatibilitás a korábbi változatokkal fennmaradjon. A DIG segítségével ellenőrizheti, hogy a DNS szerver helyes válaszokat ad-e, mielőtt rendszerét beállítja annak használatára. A DIG használatával hosztokra, tartományokra és más DNS szerverekre vonatkozó DNS információkat is lekérhet.

| A DIG lekérdezés indítása (STRDIGQRY) parancsot vagy annak álnévét, a DIG parancsot a Tartományinformáció kereső eszköz indítására használhatja.

| **HOST lekérdezés indítása (HOST)**

| A HOST lekérdezés indítása (HOST) parancsot DNS kikeresésekhez használják. Segítségével tartományneveket IP címekké (akár IPv4, akár IPv6) alakíthat át és vissza.

| **Távoli névdémon felügyelet (RNDC)**

| A Távoli névdémon felügyelet (RNDC) parancs olyan hatékony segédprogram, amely a rendszeradminisztrátor számára névszerver működésének felügyeletét teszi lehetővé. Az rndc.conf konfigurációs fájl beolvasva megállapítja, hogy miként kell a névszerverrel a kapcsolatot felvenni és eldönti, hogy milyen algoritmust és kulcsot kell használni. Ha az rndc.conf fájl nem található, akkor alapértelmezésben a telepítés során létrehozott rndc-key._KID fájl kerül felhasználásra, amely a hozzáférést automatikusan biztosítja a loopback csatolón keresztül.

| **IPv6 támogatás**

| A BIND 9 az összes jelenleg meghatározott IPv6 formátumban támogatja a név-cím és a cím-név kikereséseket. Egyenes kikeresések esetén a BIND 9 mind az AAAA, mind az A6 rekordokat támogatja, de az A6 rekordok most már

| elavultnak számítanak. IPv6 fordított kikeresésekben a hagyományos "fél byte" formátumot támogatja, amit az ip6.arpa tartományban, valamint a régebbi, elavult ip6.int tartományban használnak.

| **Naplófájlok**

| A naplófájlok a zóna dinamikus frissítéseit tárolják. Automatikusan kerül létrehozásra, amikor a klientsől az első dinamikus frissítés megérkezik, és később sem tűnik el. A naplófájl olyan bináris fájl, amely nem szerkeszthető.

| Ha van naplófájl, akkor a szerver leállítás vagy összeomlás utáni újraindításakor a szerver a naplófájlt lejátszva elvégzi a zónán az utolsó zóna kiíratás óta történt frissítéseket. A naplófájlokat növekményes zónaátviteli (IXFR) módszerek frissítéseinek tárolására is használják.

| A DNS for i5/OS terméket úgy tervezték újra, hogy BIND 9. változatot használjon. A BIND 9 DNS futtatásához a rendszernek bizonyos szoftverkövetelményeknek meg kell felelnie.

| **Kapcsolódó fogalmak**

| "Tartománynév-rendszer követelmények" oldalszám: 25

| Tartománynév-rendszer (DNS) futtatásához System i platformon az alábbi szoftverkövetelményeket kell szem előtt tartani.

| "Dinamikus frissítések" oldalszám: 6

| A BIND 9. változaton alapuló i5/OS Tartománynév-rendszer (DNS) támogatja a dinamikus frissítéseket. Külső források, például Dinamikus hoszt konfigurációs protokoll (DHCP), a DNS szervernek frissítéseket küldhetnek. Ezenkívül a dinamikus frissítések végrehajtására DNS kliens eszközök, például Dinamikus frissítési segédprogram (NSUPDATE), is használhatók.

| "A V6R1 újdonságai" oldalszám: 1

| Az alábbiakban a Tartománynév-rendszer (DNS) témakör gyűjtemény új vagy jelentősen megváltozott információiról olvashat.

| **Kapcsolódó hivatkozás**

| "Példa: DNS felosztása tűzfalon keresztül, két DNS szervert telepítve ugyanarra a System i platformra" oldalszám: 19

| Ez a példa tűzfalon keresztüli Tartománynév-rendszer (DNS) szerver működését mutatja be, amely révén a belső adatok megvédhetők az Internettől, miközben a belső felhasználóknak lehetővé teszi az adatok elérését az Interneten. Ez a konfiguráció ezt a védelmet két DNS szerver telepítésével valósítja meg ugyanazon a System i platformon.

| "Biztonsági intézkedések tervezése" oldalszám: 24

| A Tartománynév-rendszer (DNS) védelmi beállításokat biztosít a szerver külső hozzáféréseinek korlátozására.

DNS erőforrásrekordok

Az erőforrásrekordok a tartománynevek és az IP címek adatainak tárolására szolgálnak. Az i5/OS operációs rendszer esetén támogatott erőforrásrekordokat az Erőforrásrekord kikeresési táblában tekintheti meg.

A DNS zóna adatbázis erőforrásrekordok gyűjteményéből áll. Minden egyes erőforrásrekord egy adott objektum adatait adja meg. Például, a cím kiosztási (A) rekordok egy hosztnevet IP címre, míg a fordított keresési mutató (PTR) rekordok egy IP címet hosztnévre képeznek le. A szerver használja ezeket a rekordokat a zónában jelentkező hoszt lekérdezésekre való válasz céljára. További információkért nézze meg a DNS erőforrásrekordokat a táblázatban.

| **Megjegyzés:** Az erőforrásrekord kikeresési tábla bejegyzései a BIND dokumentum változásai szerint hozzáadhatók, illetve eltávolíthatók. Ezenkívül ez nem a BIND erőforrásrekordok teljes listája.

1. táblázat: Erőforrásrekord kikeresési tábla

Erőforrásrekord	Rövidítés	Leírás
Cím leképezési rekordok	A	Az A rekord megadja az adott hoszt IP címét. A rekordok egy adott tartománynév IP címének lekérdezésére szolgálnak. A rekord típusát RFC 1035 határozza meg.
Andrew fájlrendszer adatbázis rekordok	AFSDB	Az AFSDB rekord az objektum AFS vagy DCE címét adja meg. Az AFSDB rekordok az A rekordokhoz hasonlóan a tartománynév AFSDB cím leképezésére, vagy a cella tartománynévének hitelesített névszerverekre való leképezésére szolgál. A rekord típusát RFC 1183 határozza meg.
Általános névrekordok	CNAME	A CNAME rekord az objektum tényleges tartománynévét adja meg. Amikor a DNS álnévre keres, és egy általános névre mutató CNAME rekordot talál, akkor lekérdezi az általános név tartománynévét is. A rekord típusát RFC 1035 határozza meg.
Hoszt információs rekordok	HINFO	A HINFO rekord a hosztra vonatkozó általános információkat ad meg. A szabványos CPU-t és operációs rendszert RFC 1700 határozza meg. Egyébként a szabvány számok használata nem követelmény. A rekord típusát RFC 1035 határozza meg.
Integrált szolgáltatású digitális hálózat rekordok	ISDN	Az ISDN rekord megadja az adott objektum címét. A rekord leképezi a hosztnevet ISDN címre. Csak ISDN hálózatokban használatos. A rekord típusát RFC 1183 határozza meg.
IP Verzió 6 cím rekordok	AAAA	Az AAAA rekord a hoszt 128 bites IPv6 címét adja meg. Az A rekordokhoz hasonló AAAA rekordokat adott tartománynév IPv6 címére vonatkozó lekérdezések feloldására használják. Ezt a rekordtípust az RFC 1886 határozza meg.
Helyszín rekordok	LOC	A LOC rekord megadja a hálózati alkotórészek fizikai helyét. A rekordokat az alkalmazások használják a hálózat hatékonyságának kiértékelésére vagy a fizikai hálózat feltérképezésére. A rekord típusát RFC 1876 határozza meg.
Levéltovábbító rekordok	MX	Az MX rekordok a tartományhoz küldött postát továbbító hosztot adják meg. A rekordokat az SMTP (Egyszerű Postai Átvitel Protokoll) használja a hoszt keresésére, amely feldolgozza vagy továbbítja a tartomány leveleit, valamint az egyes levéltovábbító hosztok kedvenc beállításainak keresésére. Minden hosztnak megfelelő cím (A) rekordjainak kell lenni az érvényes zónában. A rekord típusát RFC 1035 határozza meg.

1. táblázat: Erőforrásrekord kikeresési tábla (Folytatás)

Erőforrásrekord	Rövidítés	Leírás
Levél csoport rekordok	MG	Az MG rekordok a levelezési csoport tartománynevét adják meg. A rekord típusát RFC 1035 határozza meg.
Postaláda rekordok	MB	A MB rekordok megadják a hoszt tartománynevét, amely az adott objektum postaládáját tartalmazza. A tartománynak küldött levél az MB rekordban megadott hoszthoz lesz irányítva. A rekord típusát RFC 1035 határozza meg.
Postaláda információs rekordok	MINFO	A MINFO rekordok kijelölik a postaládát, amely fogadja az objektum üzeneteit vagy a hibákat. A MINFO rekord sokkal inkább levelezési listákhoz használatos, mint egyedi postaládának. A rekord típusát RFC 1035 határozza meg.
Postaláda átnevezési rekordok	MR	Az MR rekordok új tartománynevet jelölnek ki a postaládának. Az MR rekord továbbítási bejegyzésnek tekinthető annál a felhasználónál, aki másik postaládát kapott. A rekord típusát RFC 1035 határozza meg.
Névszerver rekordok	NS	Az NS rekord az adott hoszt hiteles névszerverét adja meg. A rekord típusát RFC 1035 határozza meg.
Hálózati szolgáltatás elérési protokoll rekordok	NSAP	Az NSAP rekord az NSAP erőforrás címét adja meg. Az NSAP rekordok a tartománynevek NSAP címekre való leképezésére szolgál. A rekord típusát RFC 1706 határozza meg.
Nyilvános kulcs rekordok	KEY	A KEY rekord a DNS névhez tartozó nyilvános kulcsot adja meg. A kulcs vonatkozhat zónára, felhasználóra vagy hosztra. A rekord típusát RFC 2065 határozza meg.
Felelős személy rekordok	RP	Az RP rekord a zónáért vagy a hosztért felelős személy internetes levelezési címét és leírását adja meg. A rekord típusát az RFC 1183 határozza meg.
Fordított kikeresési mutató rekordok	PTR	A PTR rekord megadja azon hoszt tartománynevét, amelyre egy PTR rekordot akar definiálni. A PTR rekordok lehetővé teszik a hosztnév kikeresést, és egy IP címet adnak. A rekord típusát RFC 1035 határozza meg.
Útválasztó rekordok	RT	Az RT rekord egy hoszt tartománynevét adja meg, amely egy másik hoszt IP csomagjainak továbbítójaként szerepel. A rekord típusát RFC 1183 határozza meg.
Szolgáltatás rekordok	SRV	Az SRV rekord azt a hosztot adja meg, amely a rekordban meghatározott szolgáltatásokat támogatja. Ezt a rekordtípust az RFC 2782 határozza meg.

1. táblázat: Erőforrásrekord kikeresési tábla (Folytatás)

Erőforrásrekord	Rövidítés	Leírás
Fennhatóság kezdete rekordok	SOA	A SOA rekord megadja, hogy a szerver hiteles a zóna számára. A hiteles szerver a legjobb adatforrás a zónán belül. A SOA rekord általános információkat tartalmaz a zónáról és a másodlagos szerverek újratöltési szabályairól. Zónánként csak egy SOA rekord lehet. A rekord típusát RFC 1035 határozza meg.
Szöveg rekordok	TXT	A TXT rekord megadja a szöveg több karakterláncát (egyenként legfeljebb 255 karakter hosszúsággal), amelyeket társítani fog a tartománynévvel. A TXT rekordok együtt használhatók a felelős személyek (RP) rekordokkal, hogy megadható legyen, ki felelős a zónáért. A rekord típusát RFC 1035 határozza meg. A TXT rekordokat az i5/OS DHCP dinamikus frissítésekhez használja. A DHCP szerver minden általa végzett PTR és A rekord frissítésről hozzá tartozó TXT rekordot ír. A DHCP rekordok AS400DHCP előtaggal rendelkeznek.
Közismert szolgáltatások rekordok	WKS	A WKS rekord megadja az objektum által támogatott közismert szolgáltatásokat. Leggyakrabban a WKS rekordok jelzik, hogy a tcp vagy az udp, illetve mindkét protokoll támogatott-e az adott cím estén. A rekord típusát RFC 1035 határozza meg.
X.400 Cím leképezési rekordok	PX	A PX rekordok az X.400/RFC 822 leképezési információkra mutatnak rá. A rekord típusát RFC 1664 határozza meg.
X25 Cím leképezési rekordok	X25	Az X25 rekord az X25 erőforrás címét adja meg. A rekord leképezi a hosztnevet PSDN címre. Csak X25 hálózatokban használatos. A rekord típusát RFC 1183 határozza meg.

Kapcsolódó fogalmak

“Posta és MX rekordok”

A Tartománynév-rendszer (DNS) támogatja a fejlett levéltovábbítást a Levelezési és Levéltovábbító (MX) rekordok használata révén.

Kapcsolódó hivatkozás

“Példa: Egyedülálló Tartománynév-rendszer szerver intranethez” oldalszám: 14

A példa egyszerű alhálózatot mutat DNS szerverrel belső használatra.

“Zónák bemutatása” oldalszám: 3

A Tartománynév-rendszer (DNS) adatok kezelhető adatkészletekre (úgynevezett *zónákra*) oszlanak. Minden ilyen készlet egy bizonyos zóna típus.

Posta és MX rekordok

A Tartománynév-rendszer (DNS) támogatja a fejlett levéltovábbítást a Levelezési és Levéltovábbító (MX) rekordok használata révén.

A posta és az MX rekordokat a posta továbbító programok, mint például az Egyszerű posta átviteli protokoll (SMTP), használják. A DNS erőforrás rekordokban lévő kikeresési táblázat olyan típusú levelezési rekordokat tartalmaz, amelyeket az i5/OS DNS támogat.

A DNS magában foglalja az elektronikus posta elküldésére vonatkozó információkat is. Ha a hálózat használja a DNS-t, akkor az SMTP (Simple Mail Transfer Protocol) alkalmazás nem fogja egyszerűen leszállítani a TEST.IBM.COM hosztnak címzett postát a TEST.IBM.COM címre vonatkozó TCP összeköttetés megnyitása útján. Ilyenkor az SMTP először lekérdezi a DNS szervert, hogy melyik hoszt szerver használható fel az üzenet továbbításához.

Posta leszállítása egy adott címre

A DNS szerverek olyan erőforrásrekordokat használnak, amelyek *levéltovábbító* (MX) rekordokként ismertek. Az MX rekordok a tartomány- vagy hosztnevet leképezik egy előszeretettel használt értékre és hoszt névre. Az MX rekordok általában annak a hosztnak a kijelölésére használatosak, amely postai feldolgozást végez másik hoszt számára. A rekordok másik hoszt (ahová a postát megpróbálja továbbítani) kijelölésére is szolgálnak, ha az első hoszt nem elérhető. Másszóval lehetővé teszik az egyik hosztnak címzett levél továbbítását másik hosztnak.

Több MX erőforrásrekord is létezhet ugyanarra a tartományra vagy hoszt névre. Amikor több MX rekord létezik ugyanarra a tartományra vagy hosztra, akkor az egyes rekordok előszeretettel használt (vagy prioritás) értéke meghatározza azt a sorrendet, amely szerint a próbálkozás történik. A legalacsonyabb kedvelt érték megfelel a leginkább előnyben részesített rekordnak, amely először lesz megpróbálva. Amikor a leginkább kedvelt hoszt nem elérhető, akkor a küldő postai alkalmazás megpróbálja felvenni a kapcsolatot a következő, kevésbé kedvelt MX hoszttal. A tartomány adminisztrátor, vagy az MX rekord létrehozója állítja be a kedvelt értéket.

A DNS szerver válaszolhat üres MX erőforrásrekord listával is, amikor a név ugyan a DNS szerver jogosultságban van, de nincs hozzárendelve MX. Amikor ez fordul elő, a küldő postai alkalmazás megpróbálhat közvetlenül kapcsolatot létesíteni a címzett hoszttal.

Megjegyzés: A helyettesítő karakterek használata (például: *.mycompany.com) MX rekordokban nem ajánlott.

Példa: MX rekord hoszt számára

A következő példában a rendszer - a kedvelt értékkel - továbbítja a postát az fsc5.test.ibm.com címre, magához a hoszthoz. Ha a hoszt nem elérhető, akkor a rendszer a postát továbbíthatja a psfred.test.ibm.com vagy az mvs.test.ibm.com (ha a psfred.test.ibm.com ugyancsak nem érhető el) címre is. Az alábbi példa megmutatja, hogyan néznek ki ezek az MX rekordok:

```
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
```

Kapcsolódó hivatkozás

“DNS erőforrásrekordok” oldalszám: 9

Az erőforrásrekordok a tartománynevek és az IP címek adatainak tárolására szolgálnak. Az i5/OS operációs rendszer esetén támogatott erőforrásrekordokat az Erőforrásrekord kikeresési táblában tekintheti meg.

Példák: Tartománynév-rendszer

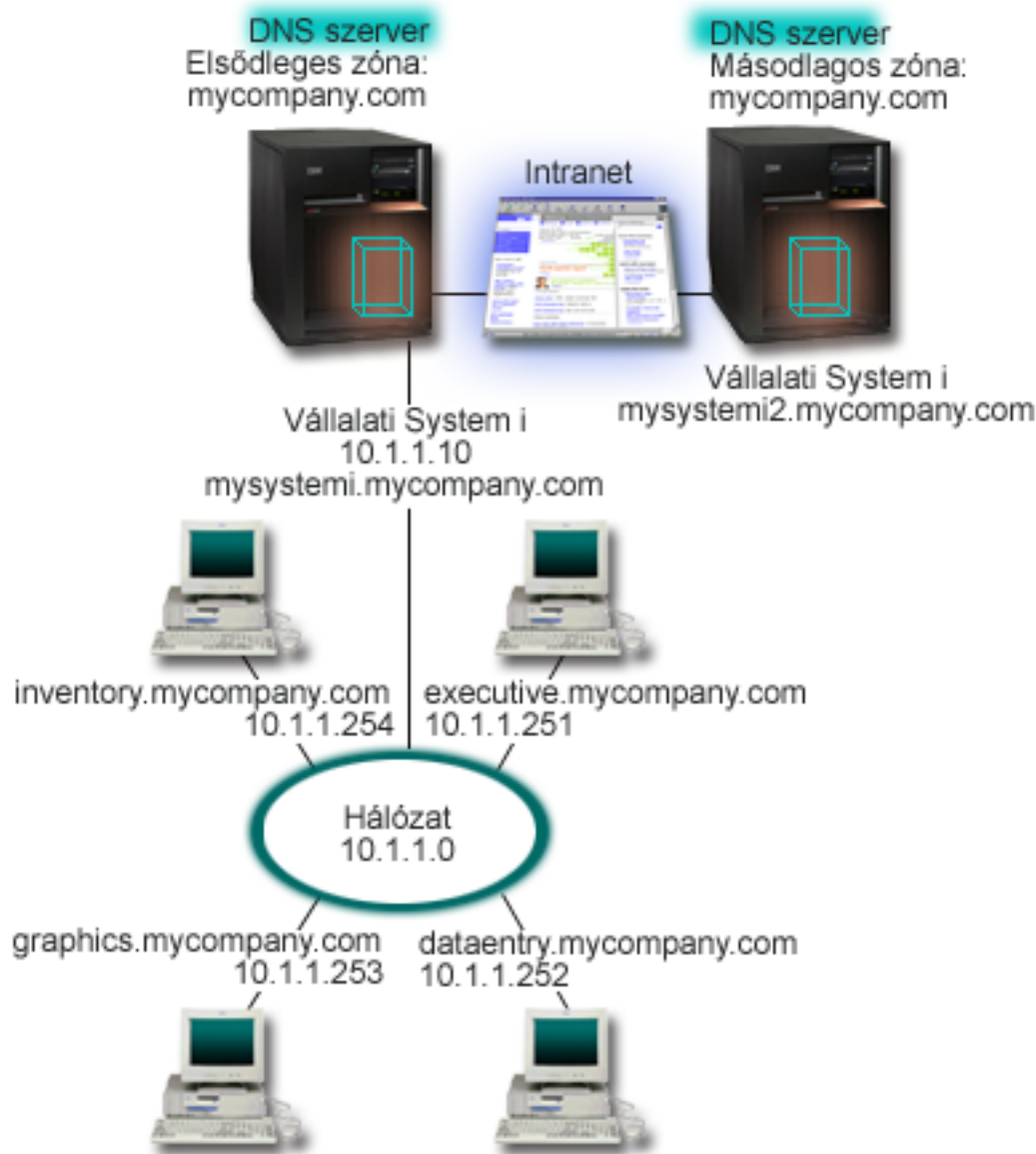
A példák révén megismerheti a Tartománynév-rendszer (DNS) használatát a hálózaton.

A DNS egy osztott adatbázis rendszer, amely a hosztnevek és a hozzájuk tartozó IP címek kezelésére szolgál. A következő példák segítenek elmagyarázni a DNS működését, és használati lehetőségét saját hálózatában. A példák leírják a beállítást és az azok használatát kiváltó okokat. Hivatkozásokat is tartalmaznak kapcsolódó koncepciókhoz, amelyek hasznosak lehetnek a képek megértéséhez.

Példa: Egyedülálló Tartománynev-rendszer szerver intranethez

A példa egyszerű alhálózatot mutat DNS szerverrel belső használatra.

A következő ábra belső hálózatot kiszolgáló, System i platformon futó DNS szerveret mutat be. Ez a DNS szerver példány úgy van beállítva, hogy az összes IP cím lekérdezését figyeli. A rendszer a mycompany.com zóna elsődleges névszervere.



2. ábra: Egy DNS szerver az intranet számára

A zónában lévő összes hoszt rendelkezik IP címmel és tartománynévvel. A DNS zóna adatokban lévő hosztokat az adminisztrátornak manuálisan kell megadnia úgynevezett erőforrásrekordok létrehozásával. A címleképezési rekordok (A IPv4 esetén, illetve AAAA IPv6 esetén) a gép nevét a hozzá tartozó IP címre képezik le. Ez lehetővé teszi a hálózaton lévő többi hoszt számára, hogy lekérdezve a DNS szervert megtalálja egy adott hosztnévhez a neki megfelelő IP címet. A fordított leképezési mutató (PTR) rekordok leképezik az IP címet a hozzá tartozó névre. Ez lehetővé teszi a hálózaton lévő többi hoszt számára, hogy lekérdezve a DNS szervert megtalálja egy adott IP címhez a neki megfelelő hosztnévet.

| Az A, AAAA és PTR rekordokon kívül a DNS sok egyéb erőforrásrekordot támogat, amelyekre attól függően lehet
| szükség, hogy az intraneten milyen más TCP/IP alapú alkalmazások futnak. Például, ha belső elektronikus levelező
| rendszert futtat, esetleg hozzáadhatja a levéltovábbító (MX) rekordokat, hogy az SMTP a DNS szerver lekérdezésével
| megtudja, mely rendszereken fut levelező szerver.

Ha ez a kicsi hálózat egy nagy intranet része, akkor meg kell adni a belső gyökér szervereket is.

Másodlagos szerverek

A másodlagos szerverek a hiteles szerverről töltik fel a zóna adatokat. A másodlagos szerverek zóna átvitel révén szerzik meg a zóna adatokat a hiteles szervertől. Amikor a másodlagos névszerver elindul, az adott tartományra vonatkozó összes adatot lekéri az elsődleges névszervertől. A másodlagos névszerver azért kéri a frissített adatokat az elsődleges szervertől, mert vagy kapott egy üzenetet az elsődleges névszervertől (ha használja a NOTIFY funkciót) vagy mert lekérdezi az elsődleges névszervert és megállapítja, hogy az adatok megváltoztak. A fenti ábrán a mysystemi szerver intranet része. A másik rendszer (mysystemi2) lett úgy beállítva, hogy a mycompany.com zóna másodlagos szervereként működjön. A másodlagos szerver a szervereken fellépő igények kiegyensúlyozására használható, valamint tartalékként is szolgál abban az esetben, ha az elsődleges szerver meghibásodik. Nagyon jó gyakorlatnak bizonyul, ha minden zónára van legalább egy másodlagos szervere.

Kapcsolódó hivatkozás

“DNS erőforrásrekordok” oldalszám: 9

Az erőforrásrekordok a tartománynevek és az IP címek adatainak tárolására szolgálnak. Az i5/OS operációs rendszer esetén támogatott erőforrásrekordokat az Erőforrásrekord kikeresési táblában tekintheti meg.

“Zónák bemutatása” oldalszám: 3

A Tartománynév-rendszer (DNS) adatok kezelhető adatkészletekre (úgynevezett *zónákra*) oszlanak. Minden ilyen készlet egy bizonyos zóna típus.

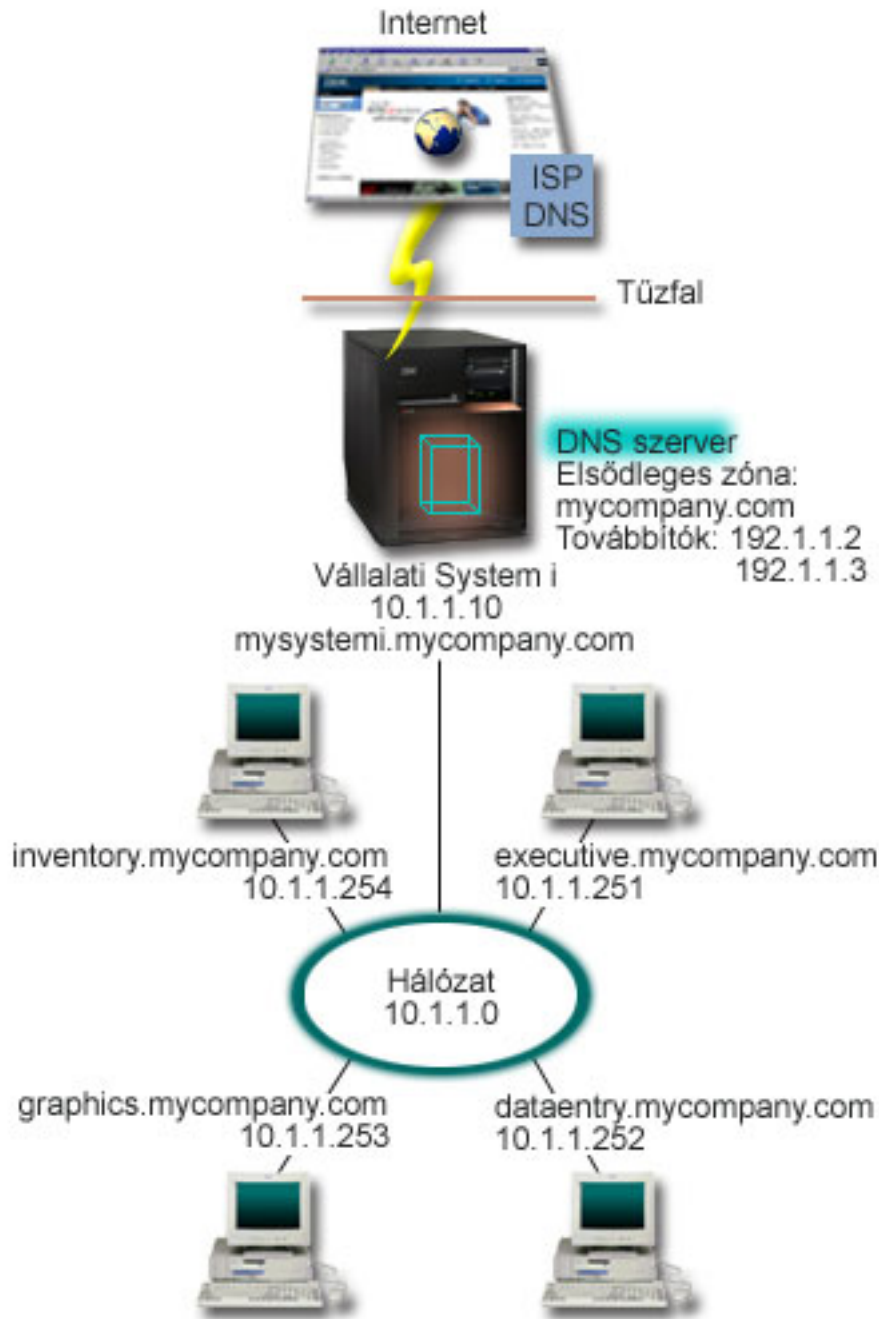
“Példa: Egyedülálló Tartománynév-rendszer szerver Internet-hozzáféréssel”

A példa egyszerű alhálózatot mutat Tartománynév-rendszer (DNS) szerverrel, közvetlen Internet-kapcsolattal.

Példa: Egyedülálló Tartománynév-rendszer szerver Internet-hozzáféréssel

A példa egyszerű alhálózatot mutat Tartománynév-rendszer (DNS) szerverrel, közvetlen Internet-kapcsolattal.

Az alábbi ábra az Egyedülálló DNS szerver intranethez példában szereplő példa hálózatot mutatja be, de a cég most Internet-kapcsolatot is hozzáadott. Ebben a példában a vállalat ugyan el tudja érni az Internetet, de a tűzfal úgy van konfigurálva, hogy a hálózat felé áramló Internet forgalmat blokkolja.



3. ábra: Egyetlen DNS szerver Internet hozzáféréssel

Az Internet címek felbontása érdekében legalább az alábbi dolgok valamelyikét meg kell tenni:

- Internet gyökér szerverek meghatározása

Az Internet gyökér szervereket automatikusan betöltheti, de esetleg frissítenie kell a listát. Ezek a szerverek segítséget nyújtanak a zónán kívüli címek felbontásához. Az aktuális Internet gyökér szerverek lekérdezésével kapcsolatos útmutatást a Külső Tartománynév-rendszer adatok elérése részben talál.

- Továbbítás engedélyezése

Beállíthatja a továbbítást, amelynek hatására a saját cég.com zónán kívülről jövő lekérdezések átadásra kerülnek külső DNS szerverekhez, mint például az Internet szolgáltató (ISP) által futtatott DNS szerverekhez. Ha

engedélyezni kívánja mind a gyökér szerverek, mind a továbbítás szerinti keresést, akkor a továbbítás beállítását **első** értékre állítsa be. A szerver először megpróbálja a továbbítást, majd ha a továbbítással nem sikerül megoldani a lekérdezést, csak akkor kérdezi le a gyökér szervereket.

A következő konfigurációs módosításokra ugyancsak szükség lehet:

- Korlátlan IP címek hozzárendelése

A fenti példában a 10.x.x.x címek láthatók. Azonban ezek korlátozott címek, és nem használhatók az intraneten kívül. A címeket példa céljából láthatja, de a saját IP címeket az ISP és egyéb hálózati tényezők határozzák meg.

- A tartománynév bejegyeztetése

Ha "láthatóvá válik" az Internet számára, regisztráltassa a tartománynevet, ha még nem tette meg.

- A tűzfal létrehozása

Nem ajánlott a DNS számára engedélyezni a közvetlen kapcsolódást az Internethez. A System i platform biztosítása érdekében állítson be tűzfalat vagy használjon más óvintézkedéseket.

Kapcsolódó fogalmak

"Tartománynév-rendszer tartomány beállítás" oldalszám: 6

A Tartománynév-rendszer (DNS) tartomány beállítása tartománynév regisztrálását követeli meg megakadályozandó, hogy mások is használják a tartománynevet.

System i és Internet biztonság

"Tartománynév-rendszer lekérdezések bemutatása" oldalszám: 4

A Tartománynév-rendszer (DNS) kliensek lekérdezések feloldására DNS szervereket használnak. A lekérdezések érkehetnek közvetlenül a klientsől vagy a kliensen futó alkalmazástól.

Kapcsolódó hivatkozás

"Példa: Egyedülálló Tartománynév-rendszer szerver intranethez" oldalszám: 14

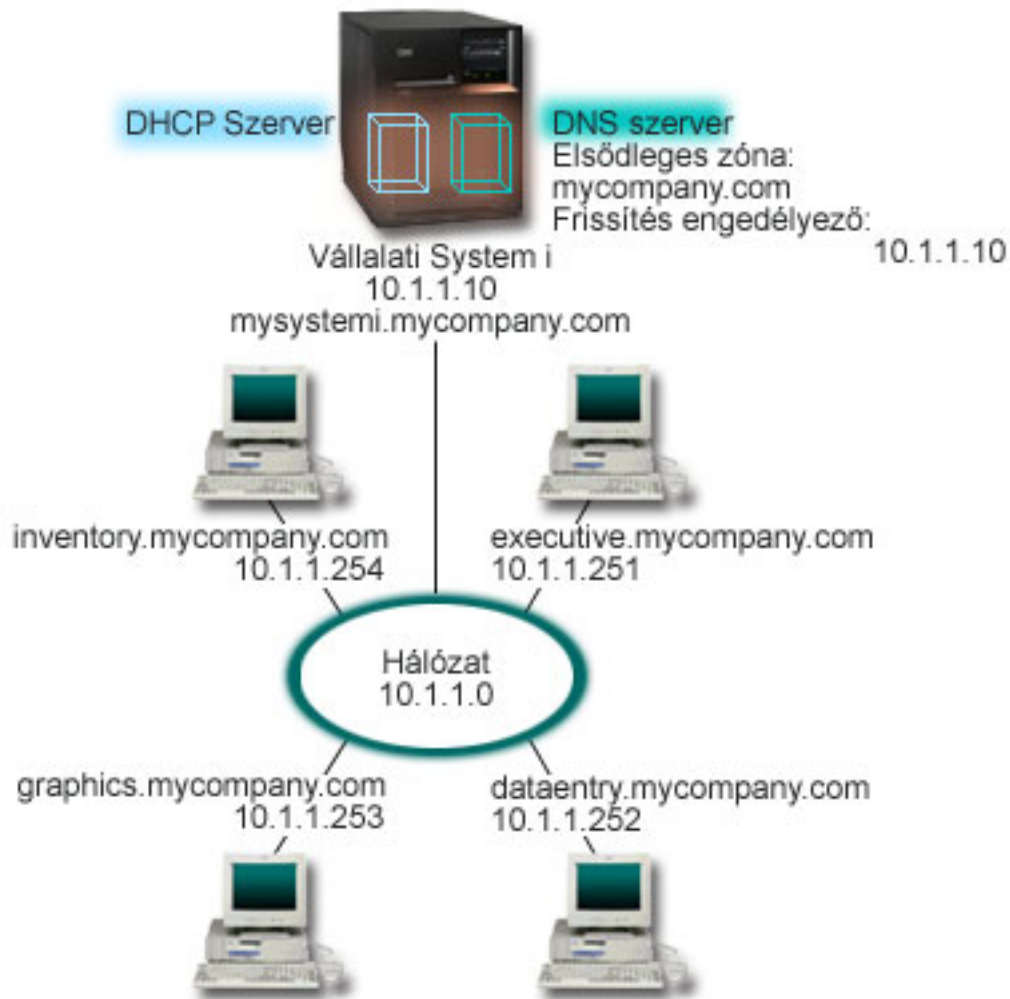
A példa egyszerű alhálózatot mutat DNS szerverrel belső használatra.

Példa: Tartománynév-rendszer és Dinamikus hoszt konfigurációs protokoll ugyanazon a System i platformon

Ez a példa Tartománynév-rendszert (DNS) és Dinamikus hoszt konfigurációs protokollt (DHCP) mutat be ugyanazon a System i platformon.

Ez a konfiguráció felhasználható a DNS zóna adatok dinamikus frissítésére, amikor a DHCP hozzárendel IP címeket a hosztokhoz.

A következő ábra kis alhálózatot mutat be egyetlen System i platformmal, amely 4 kliens DHCP és DNS szervereként működik. Tétélezzük fel, hogy ebben az elrendezésben raktári, adattároló és adminisztratív kliensek hoznak létre dokumentumokat grafikus fájlserverből származó grafikákkal. A kliensek a grafikus fájlserverhez egy hálózati lemezegység segítségével csatlakoznak a fájlserver hosztnevét használva.



4. ábra: DNS és DHCP ugyanazon a System i platformon

A DHCP és a DNS előző változatai függetlenek egymástól. Ha a DHCP hozzárendelt egy új IP címet egy klienshez, a DNS rekordokat az adminisztrátornak manuálisan kellett frissíteni. Ebben a példában, ha a grafikus fájlserver IP címe megváltozik, mert a DHCP rendelte hozzá, akkor a tőle függő kliensek nem képesek megtalálni a hálózati meghajtót a hosztnév alapján, mivel a DNS rekordok a fájlserver előző IP címét tartalmazzák még.

A BIND 9 alapú i5/OS DNS szerverrel DNS zónáját beállíthatja úgy, hogy időszakos címváltozásokkal összefüggő dinamikus DNS rekord frissítéseket fogadjon DHCP segítségével. Ha például megújításra kerül a grafikus fájlserver kölcsöne, és ekkor a DHCP szerver a 10.1.1.250 IP címet rendeli hozzá, a grafikus fájlserver DNS rekordjai dinamikusan frissítésre kerülnek. Ez a többi kliens számára lehetővé teszi, hogy a grafikus fájlserver DNS szerverét a hosztnéveik alapján folyamatosan lekérdezzék.

Hajtsa végre a következő feladatokat a DNS zóna konfigurálásához, hogy elfogadja a dinamikus frissítéseket:

- A dinamikus zóna azonosítása

A dinamikus zónát nem tudja manuálisan frissíteni a szerver futása közben. Ha így tenne, ütközést okozhatna a bejövő dinamikus frissítésekkel. A manuális frissítéseket akkor végezheti el, amikor a szerver áll, viszont a szerver leállása alatt érkező dinamikus frissítéseket elveszti. Éppen ezért, szándékában állhat, hogy egy különálló dinamikus zónát konfigurál a manuális frissítések iránti igény minimalizálása érdekében. A zónák beállításáról a dinamikus frissítési funkció használatára további információkat a Tartományszerkezet meghatározása részben talál.

- Az allow-update opció konfigurálása

Az allow-update beállítással konfigurált zónák dinamikusan tekinthetők. Az allow-update opció zóna szinten beállítható paraméter. A dinamikusan frissítések elfogadásához az allow-update opciót engedélyezni kell az adott zónára. Ebben a példában a sajtó.com zóna rendelkezhetne allow-update adatokkal, míg a szerveren definiált többi zónát statikusnak vagy dinamikusan kell beállítani.

- A DHCP konfigurálása dinamikusan frissítések küldéséhez

Fel kell hatalmazni a DHCP szervert, hogy frissítse a DNS rekordokat az általa kiosztott IP címekkel.

- Másodlagos szerver frissítési kedvezmények beállítása

A másodlagos szerver aktuális szinten tartásához konfigurálja a DNS szervert a NOTIFY használatára, amely így üzenetet küld a sajtó.com zóna másodlagos szervereinek, amikor a zóna adatok megváltoznak. Ugyancsak állítsa be a növekményes zóna átvitelt (IXFR), amely engedélyezni fogja az IXFR funkciót ismerő másodlagos szervereknek, hogy csak a frissített zóna adatokat kövessék és töltsék be a teljes zóna helyett.

Ha a DNS és a DHCP különböző szervereken fut, akkor néhány további konfigurálási követelmény merül fel a DHCP szerverre vonatkozóan.

Kapcsolódó fogalmak

“Dinamikusan frissítések” oldalszám: 6

A BIND 9. változaton alapuló i5/OS Tartománynév-rendszer (DNS) támogatja a dinamikusan frissítéseket. Külső források, például Dinamikus hoszt konfigurációs protokoll (DHCP), a DNS szervernek frissítéseket küldhetnek. Ezenkívül a dinamikusan frissítések végrehajtására DNS kliens eszközök, például Dinamikus frissítési segédprogram (NSUPDATE), is használhatók.

Kapcsolódó feladatok

DHCP konfigurálása dinamikusan frissítések küldésére

Kapcsolódó hivatkozás

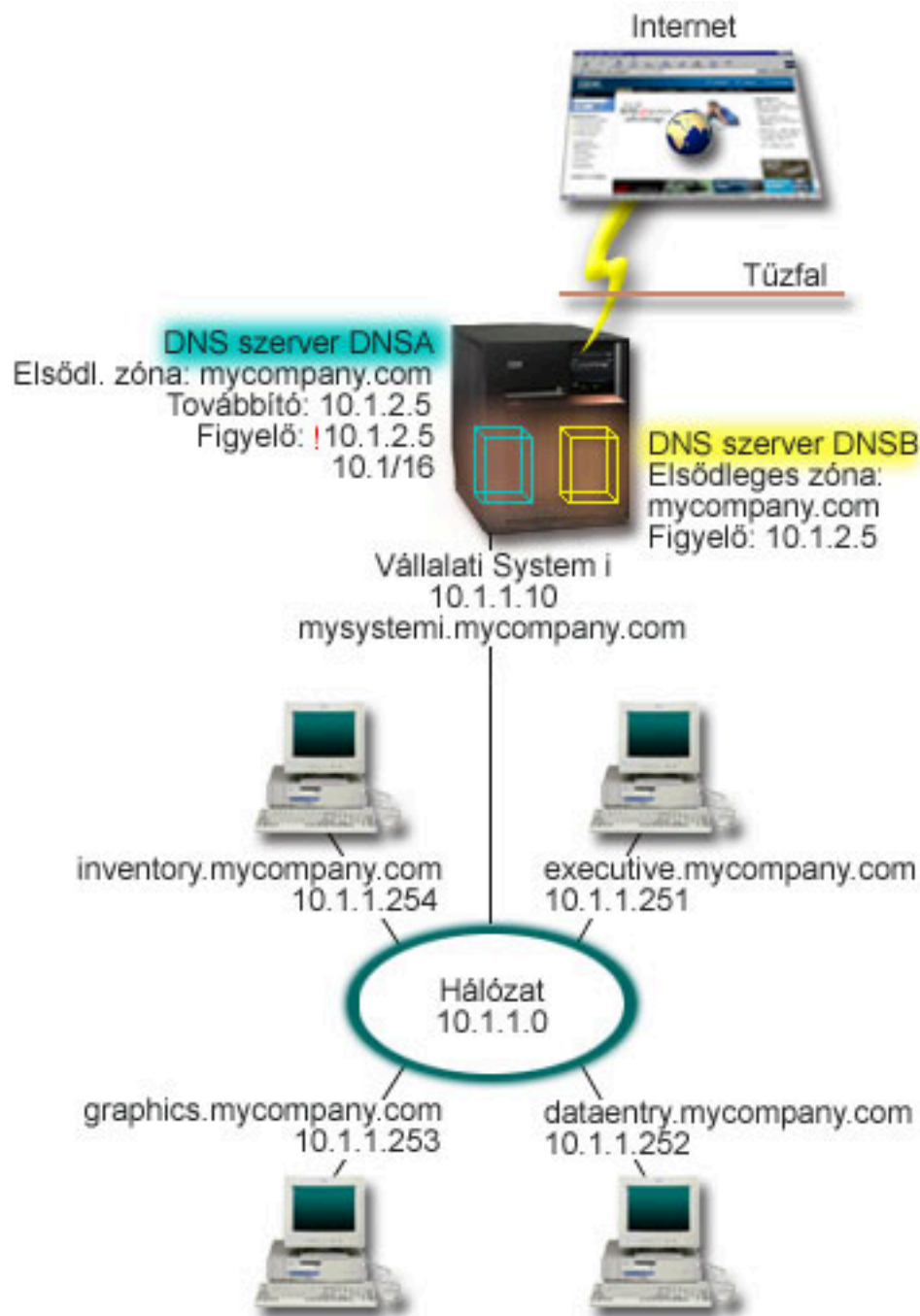
Példa: DNS és DHCP a System i platformokon

Példa: DNS felosztása tűzfalon keresztül, két DNS szerver telepítve ugyanarra a System i platformra

- | Ez a példa tűzfalon keresztüli Tartománynév-rendszer (DNS) szerver működését mutatja be, amely révén a belső adatok megvédhetők az Internetről, miközben a belső felhasználóknak lehetővé teszi az adatok elérését az Interneten.
- | Ez a konfiguráció ezt a védelmet két DNS szerver telepítésével valósítja meg ugyanazon a System i platformon.

- | A következő illusztráció egy egyszerű alhálózatból álló hálózatot mutat be, amelynek biztonságáról tűzfal gondoskodik. Tétélezzük fel, hogy a vállalat rendelkezik a hálózat belső, lefoglalt IP címterületű részével, valamint a hálózat olyan külső részével is, amely elérhető a nyilvánosság számára. A vállalat azt szeretné, hogy a belső felhasználók képesek legyenek feloldani a külső hosztneveket, és külső emberekkel levelezést folytatni. A vállalat azt is szeretné, hogy a belső feloldók elérjenek bizonyos olyan "csak-belső" zónákat, amelyek a belső hálózaton kívül egyáltalán nem érhetők el. Ugyanakkor azt nem szeretnék, hogy egy külső feloldó el tudja érni a belső hálózatot.

- | A BIND 9. változaton alapuló i5/OS DNS segítségével ez két módon valósítható meg. Az első módszer, hogy a cég két DNS szerver példányt telepít ugyanarra a System i platformra, egyet az intranet számára a másikat pedig a nyilvános tartományban lévő minden egyéb számára, amint azt ez a példa bemutatja. A másik mód a BIND 9 által biztosított nézet funkció használata, amelyet a DNS felosztása tűzfalon keresztül nézet segítségével példa ír le.



5. ábra: felosztása tűzfalon keresztül két DNS szervert telepítve ugyanarra a System i platformra

A külső szerver (DNSB) az elsődleges zónához van beállítva. Ez a zóna adat csak azokat az erőforrásrekordokat foglalja magában, amelyek a nyilvános tartomány részeként szolgálnak. A belső szerver (DNSA) a mycompany.com elsődleges zónával lesz konfigurálva, de a DNSA szerveren megadott zóna adatok intranet erőforrás rekordokat tartalmaznak. A továbbító paraméterben a 10.1.2.5 cím lesz megadva. Ez arra kényszeríti a DNSA-t, hogy továbbküldje a lekérdezéseket a DNSB-hez, ha nem tud válaszolni.

Ha nyugtalanodik a tűzfal sértetlensége vagy más biztonsági fenyegetések miatt, rendelkezik paraméterrel a figyelő opció beállítására, amely segíti a belső adatok védelmét. Ezért konfigurálhatja úgy a belső szerver, hogy csak a belső saját cég.com zónára vonatkozó lekérdezéseket engedélyezi a belső hosztoktól. Ahhoz, hogy mindez megfelelően

| működjön, a belső klienseket úgy kell konfigurálni, hogy lekérdezéseik csak a DNSA szerverre vonatkozzanak. A DNS felosztásához a következő konfigurálási beállításokat kell megfontolnia:

- | • Figyelő

| Más DNS példákban a System i platformon csak egy DNS szerver található. A beállítás szerint ez az összes csatoló IP címét figyeli. Ha azonban több DNS szerverrel rendelkezik a System i platformon, akkor meg kell határozni az egyes csatolók IP címét, amelyet az egyes szerverek figyelnek. Két DNS szerver nem figyelheti ugyanazt a címet. Ebben az esetben tételezzük fel, hogy a tűzfal felől bejövő összes lekérdezés a 10.1.2.5 címre lesz küldve. Ezeket a lekérdezéseket a külső szerverre kell küldeni. Ennek következtében DNSB a 10.1.2.5 cím figyelésére lesz beállítva. A DNSA belső szerver a 10.1.x.x csatoló IP címek felől jövő lekérdezéseket fogadja, kivéve a 10.1.2.5 címet. A cím hatékony kizárása érdekében a címegeztetési listában a kizárt címnek a beleértett cím előtagok előtt kell állnia.

- | • Címegeztetési lista sorrendje

| A címegeztetési lista első olyan eleme kerül felhasználásra, amellyel az adott cím egyezik. Például, az összes cím engedélyezéséhez a 10.1.x.x hálózaton, kivéve a 10.1.2.5 címet, az ACL elemeinek (!10.1.2.5; 10.1/16) sorrendben kell lenniük. Ebben az esetben a 10.1.2.5 cím az első elemmel lesz összehasonlítva és azonnal megtagadásra kerül.

| Ha az elemek sorrendje fordított (10.1/16; !10.1.2.5), akkor a 10.1.2.5 IP cím engedélyezett lesz, mert a szerver az első elemmel hasonlítja össze (ami egyezik) és a maradék szabályok ellenőrzése nélkül engedélyezi azt.

| **Kapcsolódó hivatkozás**

| “BIND 9 szolgáltatások” oldalszám: 8

| A BIND 9 és a BIND 8 hasonlóak; az előbbi azonban a Tartománynév-rendszer (DNS) szerver teljesítményének javítására számos szolgáltatást biztosít (például nézeteket).

| “Példa: DNS felosztása tűzfalon keresztül nézet segítségével”

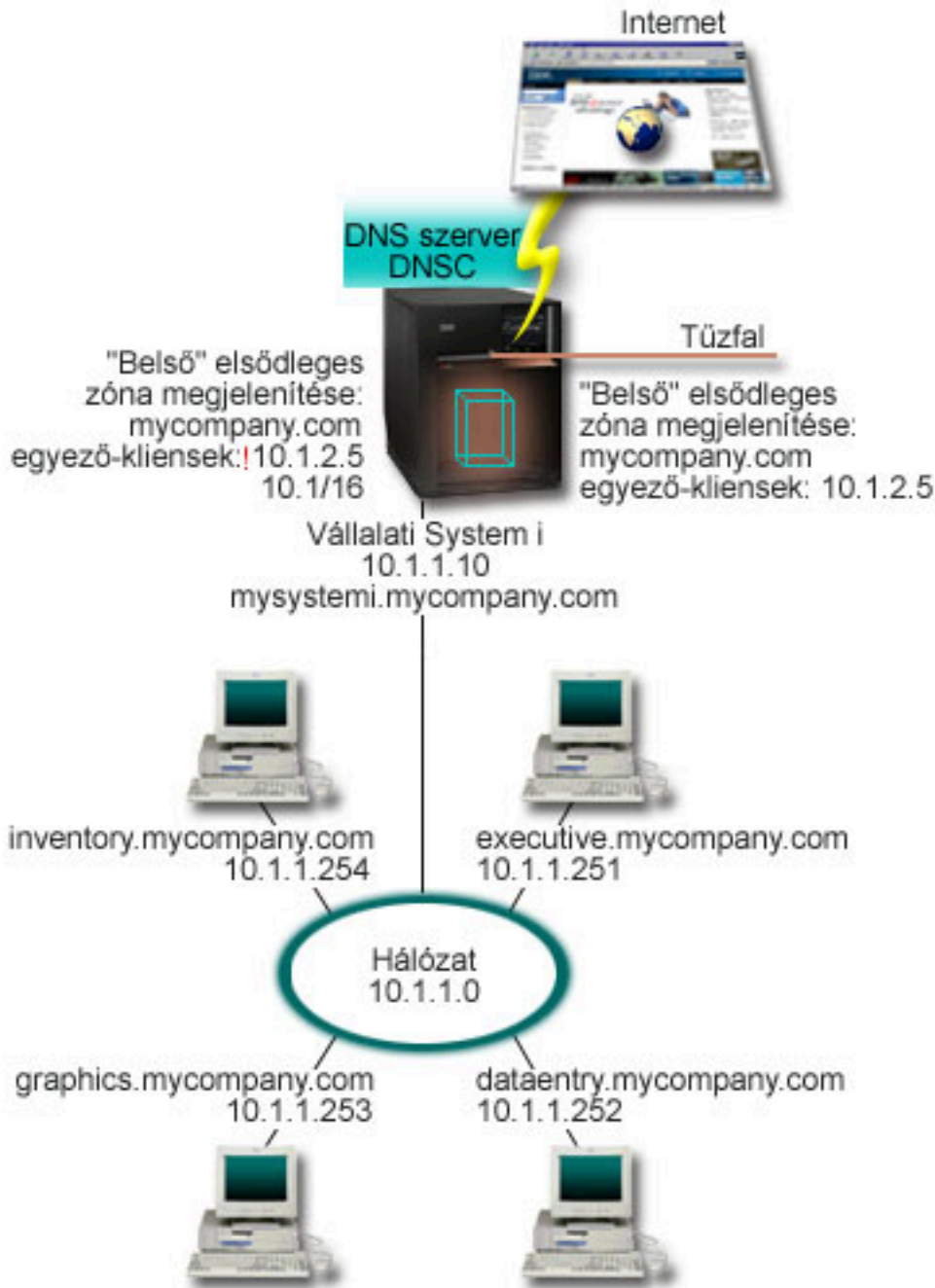
| Ez a példa a belső adatok védelme érdekében tűzfalon keresztül működő Tartománynév-rendszer (DNS) szervert mutat be, amely ugyanakkor az Interneten lévő adatok elérést a belső felhasználók számára a BIND 9 által biztosított *nézet* szolgáltatás segítségével lehetővé teszi.

| **Példa: DNS felosztása tűzfalon keresztül nézet segítségével**

| Ez a példa a belső adatok védelme érdekében tűzfalon keresztül működő Tartománynév-rendszer (DNS) szervert mutat be, amely ugyanakkor az Interneten lévő adatok elérést a belső felhasználók számára a BIND 9 által biztosított *nézet* szolgáltatás segítségével lehetővé teszi.

| A következő illusztráció egy egyszerű alhálózattól álló hálózatot mutat be, amelynek biztonságáról tűzfal gondoskodik. Tételezzük fel, hogy a vállalat rendelkezik a hálózat belső, lefoglalt IP címtérületű részével, valamint a hálózat olyan külső részével is, amely elérhető a nyilvánosság számára. A vállalat azt szeretné, hogy a belső felhasználók képesek legyenek feloldani a külső hosztneveket, és külső emberekkel levelezést folytatni. A vállalat azt is szeretné, hogy a belső feloldók elérjenek bizonyos olyan “csak-belső” zónákat, amelyek a belső hálózaton kívül egyáltalán nem érhetők el. Ugyanakkor a cég azt nem szeretné, hogy külső feloldó el tudja érni a belső hálózatot.

| A BIND 9. változaton alapuló i5/OS DNS segítségével ez két módon valósítható meg. Az ebben a példában leírt módszer a DNS szerver beállítása két, különböző lekérdezéseket figyelő nézettel, amelyekből az egyik az intranetet szolgálja ki, a másik pedig minden mást a nyilvános tartományában. A másik módszer két DNS szerver példány telepítése ugyanarra a System i platformra, amit a DNS felosztása tűzfalon keresztül két DNS szerver segítségével példa mutat be.



6. ábra: DNS felosztása tűzfalon keresztül nézet segítségével

A DNS szerver (DNSC) két nézetet határoz meg, amelyeket *külsőnek* és *belsőnek* hívnak. A *külső* nézet a mycompany.com elsődleges zónával kerül konfigurálásra, amely csak a nyilvános tartomány részének szánt erőforrásrekordokat tartalmazza, ugyanakkor a *belső* nézet a mycompany.com elsődleges zónával úgy beállítva, hogy intranet erőforrásrekordokat tartalmaz.

Ha a tűzfal integritása vagy egyéb biztonsági kérdés miatt aggódik, akkor a belső adatok védelmének kiegészítésére felhasználhatja a match-clients alutasítást. Ehhez a belső nézetet beállíthatja úgy, hogy csak a belső mycompany.com zónára irányuló lekérdezéseket engedélyezzen, belső hosztokról. A DNS felosztásához a következő konfigurálási beállítások szükségesek:

- Match-clients

A match-clients alutasítás nézet utasításon belül címegeztetési listát használ argumentumként. Csak a címegeztetési listának megfelelő lekérdezés IP címe láthatja a csatolt nézetben meghatározott konfigurációs értékeket. Ha a lekérdezés IP címe több match-clients bejegyzésnek is megfelel különböző nézet utasításokban, akkor az első nézet utasítás kerül alkalmazásra. Ebben az esetben tételezzük fel, hogy a tűzfal felől bejövő összes lekérdezés a 10.1.2.5 címre lesz küldve. Ezeket a lekérdezéseket a belső nézetben lévő zóna adatoknak kell kezelniük. Ezért a 10.1.2.5 cím úgy van beállítva, hogy a külső nézet match-clients bejegyzése legyen. A belső nézet a 10.1.x.x csatoló IP címek felől jövő lekérdezéseket fogadja, kivéve a 10.1.2.5 címet. A cím hatékony kizárása érdekében a címegeztetési listában a kizárt címnek a beleértett cím előtagok előtt kell állnia.

- Címegeztetési lista sorrendje

A címegeztetési lista első olyan eleme kerül felhasználásra, amellyel az adott cím egyezik. Például, az összes cím engedélyezéséhez a 10.1.x.x hálózaton, kivéve a 10.1.2.5 címet, az ACL elemeinek (!10.1.2.5; 10.1/16) sorrendben kell lenniük. Ebben az esetben a 10.1.2.5 cím az első elemmel lesz összehasonlítva és azonnal megtagadásra kerül.

Ha az elemek sorrendje fordított (10.1/16; !10.1.2.5), akkor a 10.1.2.5 IP cím engedélyezett lesz, mert a szerver az első elemmel hasonlítja össze (ami egyezik) és a maradék szabályok ellenőrzése nélkül engedélyezi azt.

Kapcsolódó hivatkozás

“Példa: DNS felosztása tűzfalon keresztül, két DNS szerverrel telepítve ugyanarra a System i platformra” oldalszám: 19

Ez a példa tűzfalon keresztüli Tartománynév-rendszer (DNS) szerver működését mutatja be, amely révén a belső adatok megvédhetők az Internetről, miközben a belső felhasználóknak lehetővé teszi az adatok elérését az Interneten. Ez a konfiguráció ezt a védelmet két DNS szerver telepítésével valósítja meg ugyanazon a System i platformon.

Tartománynév-rendszer tervezése

A Tartománynév-rendszer (DNS) számtalan megoldást kínál. Mielőtt konfigurálná a DNS szerveret, fontos, hogy megtervezze a hálózaton belüli működését. Az olyan dolgokat, mint például a hálózat szerkezete, a teljesítmény és a biztonság, mindenképpen érdemes felmérni.

Tartománynév-rendszer jogosultságok megállapítása

A Tartománynév-rendszer (DNS) adminisztrátornak különleges jogosultsági szükségletei vannak. Vegye figyelembe a jogosultság biztonsági vonatkozásait is.

Amikor felépíti a DNS szerveret, tegye meg a szükséges óvintézkedéseket a konfiguráció védelme érdekében. Alakítsa ki, hogy mely felhasználók legyenek jogosultak a konfiguráció módosítására.

Minimális szintű jogosultság kell ahhoz, hogy megengedje az adminisztrátornak a DNS konfigurálását és adminisztrálását. Ha "összes objektum hozzáférést" adományoz, akkor biztos lehet benne, hogy az adminisztrátor végre tudja hajtani a DNS adminisztrációs feladatokat. Ajánlatos, hogy a DNS konfigurálását végző felhasználók biztonsági adminisztrátori hozzáféréssel és összes objektum (*ALLOBJ) jogosultsággal rendelkezzenek. Felhasználók felhatalmazására használja a System i navigátor programot. Ha további információkra van szüksége, olvassa el a DNS online súgó Jogosultság adományozása a DNS adminisztrátornak című témakörét.

Megjegyzés: Ha az adminisztrátori profil nem rendelkezik a teljes jogosultsággal, akkor hozzáférést és jogosultságot kell adományozni az összes DNS katalógushoz és kapcsolódó konfigurációs fájlhoz.

Kapcsolódó hivatkozás

“Tartománynév-rendszer konfigurációs fájlok karbantartása” oldalszám: 33

Az i5/OS DNS segítségével DNS szerver példányokat hozhat létre és kezelhet saját System i platformján. A DNS konfigurációs fájlok kezelése a System i navigátor segítségével történik. A fájlokat nem szabad saját kezűleg szerkeszteni. DNS konfigurációs fájlok létrehozására, módosítására és törlésére mindig a System i navigátor programot használja.

Tartományszerkezet meghatározása

Ha első alkalommal alakítja ki a tartományt, a zónák létrehozása előtt tervezze meg az igényeket és a karbantartásokat.

Fontos meghatározni, hogyan fogja felosztani tartományát vagy altartományát zónákra, hogyan tudja a legjobban kiszolgálni a hálózati igényeket, hogyan éri el az Internetet és hogyan juthat át a tűzfalakon. Ezek a tényezők összetettek lehetnek, és egyesével kell foglalkozni velük. Mélyebb irányelvek érdekében olvasson el más hiteles forrást is, mint például az O'Reilly DNS and BIND könyvet.

Ha a Tartománynév-rendszer (DNS) zónát dinamikus zónaként konfigurálja, akkor manuálisan nem változtathatja meg a zóna adatokat a szerver futása alatt. Ha így tenné, ütközést okozhatna a bejövő dinamikus frissítésekkel. Ha szükség van manuális frissítésre, állítsa le a szervert, hajtsa végre a változtatásokat, majd indítsa újra a szervert. A leállított DNS szervernek küldött dinamikus frissítés sosem fog befejeződni. Éppen ezért, szándékában állhat, hogy a dinamikus és a statikus zónát különállónak konfigurálja. Ezt teljesen külön zónák létrehozásával tudja megtenni, vagy egy új altartomány meghatározásával - mint például a dinamikus.sajátcég.com megadásával - azokra a kliensekre, amelyek dinamikus lesznek karbantartva.

Az i5/OS DNS a rendszerek konfigurálásához grafikus felületet biztosít. Néhány esetben a kezelőfelület olyan szak kifejezéseket vagy koncepciókat használ, amelyek eltérnek a más forrásokban használtaktól. Ha a DNS konfiguráció tervezésekor más információs forrásokra hivatkozik, akkor hasznos lehet a következőkre emlékezni:

- A System i platformon meghatározott összes zóna és objektum az Egyenes kikeresési zónák és a Fordított kikeresési zónák mappákon belül van rendszerezve. Az Egyenes kikeresési zónák azok a zónák, amelyek segítségével tartománynevek IP címekre képezhetők le (például A és AAAA rekordok). A Fordított kikeresési zónák azok a zónák, amelyek az IP címek tartománynevekre történő leképezésére szolgálnak, mint például a PTR rekordok.
- Az i5/OS DNS az *elsődleges zónák* és *másodlagos zónák* kifejezéseket használja.
- A kezelőfelület az *alzóna* elnevezést használja, míg egyes források *altartományként* emlegetik. Az utódzóna egy alzóna, amelyre vonatkozóan a felelősséget egy vagy több névszerverre áthárítja.

Biztonsági intézkedések tervezése

A Tartománynév-rendszer (DNS) védelmi beállításokat biztosít a szerver külső hozzáféréseinek korlátozására.

Címegezési listák

A DNS úgynevezett Címegezési listákat használ arra a célra, hogy engedélyezze vagy megtagadja a külső egyedeknek bizonyos DNS funkciókhoz való hozzáférést. Ezek a listák magukban foglalnak adott IP címeket, egy alhálózatot (IP előtag használatával) vagy Tranzakció aláírás (TSIG) kulcsok használatával. A címegezési listában felsorolhatja az egyedeket, akiknek meg akarja engedni vagy vissza akarja utasítani a hozzáférést. Ha egy Címegezési listát újra fel akar használni, elmentheti Hozzáférés felügyeleti listaként (ACL). Azután valahányszor szükség van egy listára, behívja az ACL-t, és az egész lista betöltődik.

Címegeztetési lista elemsorrendje

A címegeztetési lista első olyan eleme kerül felhasználásra, amellyel az adott cím egyezik. Ha például az 10.1.1.x hálózatban a 10.1.1.5 cím kivételével minden címet engedélyezni kíván, akkor az egyeztetési lista elemeinek sorrendje a következő: (!10.1.1.5; 10.1.1/24). Ebben az esetben a 10.1.1.5 cím az első elemmel lesz összehasonlítva és azonnal megtagadásra kerül.

Ha az elemek sorrendje fordított (10.1.1/24; !10.1.1.5), akkor a 10.1.1.5 IP cím engedélyezett lesz, mert a szerver az első elemmel hasonlítja össze (ami egyezik) és a maradék szabályok ellenőrzése nélkül engedélyezi azt.

Hozzáférés vezérlési beállítások

A DNS lehetővé teszi korlátozások beállítását, mint például azt, hogy ki küldhet dinamikus frissítést, lekérdezési adatokat és zóna átviteli kéréseket a szervernek. A Hozzáférés vezérlési listák segítségével korlátozhatja a szerver elérését a következő opciók számára:

allow-update

Engedélyezni kell ezt az opciót, ha azt akarja, hogy a DNS szerver elfogadjon dinamikus frissítéseket valamilyen külső forrásból.

allow-query

Megadhatja, hogy mely hosztok küldhetnek lekérdezést ennek a szervernek. Ha nem definiálja, akkor alapértelmezés szerint az összes hoszt lekérdezése engedélyezve van.

allow-transfer

Megadhatja, hogy mely hosztok fogadhatnak zóna átvitelt ettől a szervertől. Ha nem definiálja, akkor alapértelmezés szerint az összes hoszt átvitele engedélyezve van.

allow-recursion

Megadhatja, hogy mely hosztok végezhetnek rekurzív lekérdezést ezen a szerveren keresztül. Ha nem definiálja, akkor alapértelmezés szerint az összes hoszt rekurzív lekérdezése engedélyezve van.

blackhole

Meghatároz egy címlistát, amelyekről a szerver nem fog elfogadni lekérdezéseket, vagy nem fogja felhasználni őket egy lekérdezés megoldásához. Az ilyen címekről jövő lekérdezésekre a szerver nem fog válaszolni.

A DNS szerver biztonsága létfontosságú. A témakörben tárgyalt biztonsági szempontokon kívül a DNS biztonsággal és a System i biztonsággal számos forrás foglalkozik, a System i platformot és az Internet témakör gyűjteményt is beleértve. A *DNS és BIND* című könyv szintén foglalkozik a DNS rendszerhez kapcsolódó biztonsági szolgáltatásokkal.

Kapcsolódó fogalmak

System i és Internet biztonság

Kapcsolódó hivatkozás

“BIND 9 szolgáltatások” oldalszám: 8

A BIND 9 és a BIND 8 hasonlóak; az előbbi azonban a Tartománynév-rendszer (DNS) szerver teljesítményének javítására számos szolgáltatást biztosít (például nézeteket).

Tartománynév-rendszer követelmények

| Tartománynév-rendszer (DNS) futtatásához System i platformon az alábbi szoftverkövetelményeket kell szem előtt tartani.

| A DNS szolgáltatás (31. opció) az operációs rendszerrel automatikusan nem telepíthető. A DNS szolgáltatást kimondottan ki kell választani a telepítéshez. Az i5/OS rendszerhez hozzáadott DNS szerver a BIND 9 néven ismert ipari szabvány DNS megvalósításon alapul. A korábbi OS/400 DNS szolgáltatások a BIND 8.2.5 változatra épültek és az i5/OS rendszerben továbbra is elérhetőek.

| A DNS telepítése után a DNS szervert BIND 4 vagy 8 változatokról BIND 9 változatra kell áttelepíteni és konfigurálni. Telepített i5/OS PASE környezettel is rendelkeznie kell, ami az i5/OS 33. opciója. Az i5/OS PASE telepítése után a System i navigátor az aktuális BIND megvalósítás beállítását automatikusan végzi.

| Ha másik platformon Dinamikus hoszt konfigurációs protokoll (DHCP) szervert kíván konfigurálni, ami ennek a DNS szervernek frissítéseket küld, akkor a 31. opciót azon a DHCP szerveren is telepíteni kell. A DHCP szerver a 31. opció által biztosított programozási felületeket használja a dinamikus frissítések megvalósításakor.

Kapcsolódó fogalmak

i5/OS PASE

“Tartománynév-rendszer beállítása” oldalszám: 26

A System i navigátor segítségével névszervereket állíthat be és tartományon kívüli lekérdezéseket oldhat fel.

Kapcsolódó hivatkozás

“BIND 9 szolgáltatások” oldalszám: 8

A BIND 9 és a BIND 8 hasonlóak; az előbbi azonban a Tartománynév-rendszer (DNS) szerver teljesítményének javítására számos szolgáltatást biztosít (például nézeteket).

Tartománynév-rendszer telepítésének ellenőrzése

Annak eldöntésére, hogy a Tartománynév-rendszer (DNS) telepítve van-e, tegye a következőket.

1. A parancssorba gépelje be a GO LICPGM parancsot, és nyomja meg az Enter billentyűt.
2. Írjon be 10-et (Telepített licencprogramok megjelenítése) és nyomja meg az Entert.
3. Lapozzon lefelé az **5761SS1 Tartománynév-rendszer** (31. opció) elemig. Ha a DNS sikeresen telepítésre került, akkor a Telepített állapot értéke *COMPATIBLE, ahogyan az alábbiakban látható:

LicPgm	Installed Status	Description
5761SS1	*COMPATIBLE	Domain Name System

4. Nyomja meg az F3 billentyűt a kilépéshez.

Tartománynév-rendszer telepítése

A Tartománynév-rendszer telepítéséhez tegye a következőket:

1. A parancssorba gépelje be a GO LICPGM parancsot, és nyomja meg az Enter billentyűt.
2. Írjon be 11 értéket (Licencprogramok telepítése) és nyomja meg az Entert.
3. Gépeljen be 1-et (Telepítés) az **Option** mezőbe az OS/400 - Tartománynév-rendszer mellé, és nyomja meg az Enter billentyűt.
4. Nyomja meg ismét az Enter billentyűt a telepítés jóváhagyásához.

Tartománynév-rendszer beállítása

A System i navigátor segítségével névszervereket állíthat be és tartományon kívüli lekérdezéseket oldhat fel.

A DNS konfigurálása előtt olvassa el a DNS rendszer követelményeit a szükséges DNS összetevők telepítéséhez.

Kapcsolódó fogalmak

“Tartománynév-rendszer követelmények” oldalszám: 25

Tartománynév-rendszer (DNS) futtatásához System i platformon az alábbi szoftverkövetelményeket kell szem előtt tartani.

Tartománynév-rendszer elérése a System i navigátor programban

A következő utasítások elvezetik a System i navigátor DNS konfigurációs felületéhez.

Ha i5/OS PASE környezetet használ, akkor képes lesz BIND 9. változaton alapuló DNS szervereket konfigurálni.

Ha első alkalommal konfigurálja a DNS szerveret, kövesse ezeket a lépéseket:

1. A System i navigátor programban bontsa ki a **saját rendszer** → **Hálózat** → **szerverek** → **DNS** elemet.
2. Kattintson a jobb egérgombbal a **DNS** elemre, és válassza ki az **Új konfigurációt**.

Kapcsolódó fogalmak

Ismerkedés a System i navigátorral

Névszerverek beállítása

A Tartománynév-rendszer (DNS) lehetővé teszi több névszerver példány létrehozását. Ez a témakör a névszerver konfigurálására vonatkozó utasításokat tartalmazza.

A BIND 9. változaton alapuló i5/OS DNS több névszerver példányt támogat. Az alábbi feladatok végigvezetik egy névszerver példány létrehozásának folyamatán, beleértve annak tulajdonságait és zóna adatait is.

Ha több példányt kíván létrehozni, ismétlje meg a fenti eljárást addig, amíg létre nem hozta az összes példányt. Az egyes névszerver példányokra megadhat független tulajdonságokat is, mint például a hibakeresés szintjeit és az automatikus indítás értékeit. Amikor egy új példányt hoz létre, külön konfigurációs fájlok jönnek létre.

Kapcsolódó hivatkozás

“Tartománynév-rendszer konfigurációs fájlok karbantartása” oldalszám: 33

Az i5/OS DNS segítségével DNS szerver példányokat hozhat létre és kezelhet saját System i platformján. A DNS konfigurációs fájlok kezelése a System i navigátor segítségével történik. A fájlokat nem szabad saját kezűleg szerkeszteni. DNS konfigurációs fájlok létrehozására, módosítására és törlésére mindig a System i navigátor programot használja.

Névszerver példány létrehozása

Az Új Tartománynév-rendszer (DNS) konfigurációs varázsló végigvezeti a felhasználót a DNS szerver példány meghatározásának folyamatán.

Az **Új DNS konfiguráció** varázsló elindításához kövesse ezeket a lépéseket:

1. A System i navigátor programban bontsa ki a **saját rendszer** → **Hálózat** → **szerverek** → **DNS** elemet.
2. A bal oldali ablakrészben kattintson a jobb egérgombbal a **DNS** elemre, majd válassza az előugró menü **Új névszerver** menüpontját.
3. A konfigurációs folyamat befejezéséhez kövesse a varázsló utasításait.

A varázsló a következő beviteleket kéri:

DNS szerver naplózás

Adja meg a DNS szerver nevét. Legfeljebb 5 karakteres lehet, és betűvel (A-Z) kell kezdődnie. Ha több szervert hoz létre, mindegyiknek egyedi névének kell lenni. Erre a névre a rendszer más területein mint a DNS szerver példány nevére utalnak.

Figyelő IP címek:

Két DNS szerver nem figyelhet ugyanazon a címen. Az alapértelmezett beállítás az összes IP cím figyelése. Ha további szerver példányokat hoz létre, akkor azokat nem állíthatja be az összes IP cím figyelésére. Ellenkező esetben nem futtathatók egyszerre. Meg kell adnia az IP címeket mindegyik szerverre.

Gyökér szerverek:

Betöltheti az alapértelmezett Internet gyökér szerverek listáját, vagy megadhatja a saját gyökér szervereit is, mint például az intranet céljára szolgáló belső gyökér szervereket.

Megjegyzés: Az alapértelmezett Internet gyökér szerverek betöltését csak akkor fontolja meg, ha hozzáféréssel rendelkezik az Internethez és azt várja el, hogy a DNS teljes egészében képes legyen az Internet nevek feloldására.

Szerver indítása:

Megadhatja, hogy a szerver elinduljon-e automatikusan, amikor a TCP/IP is elindul. Amikor több szervert üzemeltet, az egyedi példányok egymástól függetlenül indíthatók el és állíthatók le.

Tartománynév-rendszer szerver tulajdonságainak szerkesztése

Miután létrehozta a névszervert, szerkesztheti a tulajdonságait, mint például a frissítés engedélyezést és a hibakeresési szinteket. Ezek a beállítások csak arra a szerver példányra érvényesek, amelyet módosít.

A DNS szerver példány tulajdonságainak szerkesztéséhez kövesse ezeket a lépéseket:

1. A System i navigátor programban bontsa ki a **saját rendszer** → **Hálózat** → **szerverek** → **DNS** elemet.
2. A jobb kereten kattintson a jobb egérgombbal a **DNS szerverre**, és válassza ki a **Konfigurációt**.
3. A DNS beállítása ablakban kattintson a jobb egérgombbal a **DNS szerver** elemre, majd válassza az előugró menü **Tulajdonságok** menüpontját.
4. Szerkessze a kívánt tulajdonságokat.

Zónák beállítása névszerveren

Miután konfigurálta a Tartománynév-rendszer (DNS) szerver példányt, be kell állítania a zónákat az adott névszerverre.

Zónák beállításához a szerveren tegye a következőket:

1. A System i navigátor programban bontsa ki a **saját rendszer** → **Hálózat** → **szerverek** → **DNS** elemet.

2. A jobb kereten kattintson a jobb egérgombbal a **DNS szerverre**, és válassza ki a **Konfigurációt**.
3. A DNS beállítása ablakban válassza ki a létrehozandó zónatípust a jobb egérgombbal az **Egyenes kikeresési zóna** vagy a **Fordított kikeresési zóna** mappára kattintva.
4. A létrehozási folyamat befejezéséhez kövesse a varázsló utasításait.

Kapcsolódó fogalmak

“Külső Tartománynév-rendszer adatok elérése” oldalszám: 29

Amikor Tartománynév-rendszer (DNS) zóna adatokat hoz létre, a szerver képes lesz megoldani a kérdéses zónára vonatkozó lekérdezéseket.

Kapcsolódó feladatok

“Tartománynév-rendszer beállítása dinamikus frissítések fogadására”

A BIND 9. változatot futtató Tartománynév-rendszer (DNS) szerverek beállíthatók úgy, hogy a zóna adatok frissítése céljából más forrásoktól fogadjanak el kéréseket. Ez a témakör az engedélyezés-frissítés opció konfigurálására vonatkozó utasításokat tartalmazza, amelynek révén a DNS fogadni tudja a dinamikus frissítéseket.

“Tartománynév-rendszer fájlok importálása” oldalszám: 29

A Tartománynév-rendszer (DNS) importálni tudja a meglévő zóna adat fájlokat. Kövesse ezt az időtakarékos eljárást, amikor új zónát hoz létre a meglévő konfigurációs fájlból.

Kapcsolódó hivatkozás

“Zónák bemutatása” oldalszám: 3

A Tartománynév-rendszer (DNS) adatok kezelhető adatkészletekre (úgynevezett *zónákra*) oszlanak. Minden ilyen készlet egy bizonyos zóna típus.

| Nézetek beállítása névszerveren

| A BIND 9 által ajánlott szolgáltatások egyike a *nézet* utasítás, amely egyetlen Tartománynév-rendszer (DNS) példány számára ugyanazon lekérdezés különböző megválaszolását teszi lehetővé attól függően, hogy a lekérdezés honnan érkezik (például az Internetről vagy intranetből). A nézet egyik gyakorlati alkalmazása a DNS telepítések felosztása több DNS szerver futtatása nélkül.

| Nézetek beállításához a szerveren tegye a következőket:

1. A System i navigátor programban bontsa ki a **saját rendszer** → **Hálózat** → **szerverek** → **DNS** elemet.
2. A jobb kereten kattintson a jobb egérgombbal a **DNS szerverre**, és válassza ki a **Konfigurációt**.
3. A DNS beállítása ablakban kattintson a jobb egérgombbal a **Nézetek** elemre, majd válassza az előugró menü **Új nézet** menüpontját.
4. A létrehozási folyamat befejezéséhez kövesse a varázsló utasításait.

Tartománynév-rendszer beállítása dinamikus frissítések fogadására

A BIND 9. változatot futtató Tartománynév-rendszer (DNS) szerverek beállíthatók úgy, hogy a zóna adatok frissítése céljából más forrásoktól fogadjanak el kéréseket. Ez a témakör az engedélyezés-frissítés opció konfigurálására vonatkozó utasításokat tartalmazza, amelynek révén a DNS fogadni tudja a dinamikus frissítéseket.

| Amikor dinamikus zónákat hoz létre, figyelembe kell venni a hálózat szerkezetét. Ha a tartomány egyes részei még manuális frissítést igényelnek, szándékában állhat külön statikus és dinamikus zónák kialakítása. Ha a dinamikus zónát manuálisan kell frissíteni, le kell állítani a dinamikus zóna szerverét, majd újra el kell indítani a frissítések elvégzése után. A szerver leállítása kikényszeríti a zóna adatbázis frissítését az összes olyan dinamikus frissítéssel, ami azóta került végrehajtásra, hogy a szerver a zóna adatait először betöltötte a zóna adatbázisból. Ha nem állítja le a szervert, akkor a zóna adatbázison végzett összes kézi frissítés elveszik, mert a működő szerver azokat felülírja. Azonban, ha a manuális frissítés elvégzése céljából leállítja a rendszert, akkor pedig a szerver leállása alatt elküldött dinamikus frissítéseket veszti el.

A DNS jelzi, hogy a zóna dinamikus, amikor az objektumokat definiálja az allow-update utasításban. Az allow-update opció konfigurálásához kövesse ezeket a lépéseket:

1. A System i navigátor programban bontsa ki a **saját rendszer** → **Hálózat** → **szerverek** → **DNS** elemet.
2. A jobb kereten kattintson a jobb egérgombbal a **DNS szerverre**, és válassza ki a **Konfigurációt**.

3. A DNS konfiguráció ablakban bontsa ki az **Egyenes kikeresési zóna** vagy a **Fordított kikeresési zóna** elemet.
4. Kattintson a jobb egérgombbal a szerkeszteni kívánt elsődleges zónára, majd válassza ki a **Tulajdonságokat**.
5. Az Elsődleges zóna tulajdonságok lapon kattintson a **Beállítások** fülre.
6. A Beállítások lapon bontsa ki a **Hozzáférés vezérlés** → **allow-update** elemeket.
7. A DNS Címegeyeztési listát használ a felhatalmazott frissítések ellenőrzéséhez. Ha objektumot akar felvenni a címegeyeztetési listába, válassza ki a címegeyeztetési lista elemének típusát, majd kattintson a **Hozzáadás** lehetőségre. Felvehet a listába IP címet, IP előtagot, Hozzáférés vezérlési listát vagy kulcsot.
8. Amikor befejezi a címegeyeztetési lista frissítését, kattintson az **OK** gombra a Beállítások lap bezárásához.

Kapcsolódó feladatok

“Zónák beállítása névszerveren” oldalszám: 27

Miután konfigurálta a Tartománynév-rendszer (DNS) szerver példányt, be kell állítania a zónákat az adott névszerverre.

DHCP konfigurálása dinamikus frissítések küldésére

Tartománynév-rendszer fájlok importálása

A Tartománynév-rendszer (DNS) importálni tudja a meglévő zóna adat fájlokat. Kövesse ezt az időtakarékos eljárást, amikor új zónát hoz létre a meglévő konfigurációs fájlból.

Létrehozhat elsődleges zónát olyan zóna adatfájlt importálva, amely a BIND szintaxis alapján érvényes zóna konfigurációs fájl. A fájlnak integrált fájlrendszeri katalógusban kell lennie. Amikor importálja, a DNS ellenőrzi, hogy egy érvényes zóna adatfájlról van-e szó, és hozzáadja a megadott szerver példány named.conf állományához.

A zóna fájl importálásához kövesse ezeket a lépéseket:

1. A System i navigátor programban bontsa ki a **saját rendszer** → **Hálózat** → **szerverek** → **DNS** elemet.
2. A jobb kereten kattintson duplán arra a DNS szerver példányra, ahová importálni szeretné a zónát.
3. A DNS beállítása ablak jobb oldali ablakrészében kattintson a jobb egérgombbal a **DNS szerver** lehetőségre, majd válassza az előugró menü **Zóna importálása** menüpontját.
4. Az elsődleges zóna importálásához kövesse a varázsló utasításait.

Kapcsolódó feladatok

“Zónák beállítása névszerveren” oldalszám: 27

Miután konfigurálta a Tartománynév-rendszer (DNS) szerver példányt, be kell állítania a zónákat az adott névszerverre.

Rekord érvényesítés

A Tartomány adatok importálása funkció a behozatalra kerülő fájl minden egyes rekordját beolvassa és érvényesíti.

A Tartomány adatok importálása funkció befejezését követően a hibás rekordok egyedileg ellenőrizhetők a behozott zóna Egyéb rekordok nevű tulajdonságlapján.

Megjegyzések:

1. A nagy méretű elsődleges tartományok behozatala több percet vehet igénybe.
2. A Tartomány adatok importálása funkció nem támogatja az \$include direktívát. A behozott tartomány adatok érvényesség ellenőrzési folyamata hibás sorként azonosítja azokat a sorokat, amelyek \$include direktívát tartalmaznak.

Külső Tartománynév-rendszer adatok elérése

Amikor Tartománynév-rendszer (DNS) zóna adatokat hoz létre, a szerver képes lesz megoldani a kérdéses zónára vonatkozó lekérdezéseket.

A gyökér szerverek fontosak a DNS szerver működéséhez, amelyek közvetlenül kapcsolódnak az Internethez vagy egy nagy Intranethez. A DNS szervereknek a gyökér szervereket kell használni, hogy válaszolni tudjanak az olyan hosztokra vonatkozó lekérdezésekre, amelyeket a saját tartomány állományaik nem tartalmaznak.

További információ eléréséhez a DNS szervernek tudnia kell, hogy hol keresse. Az Interneten az első, amit a DNS szerver lát, a gyökér szerverek. A gyökér szerver addig irányítja a DNS szerveret más szerverek felé a hierarchiában, amíg választ nem talál, vagy amíg meg nem állapítja, hogy nincs válasz.

Alapértelmezett gyökér szerverek listája a System i navigátor programban

Az Internet gyökér szervereket csak akkor használja, ha van Internet kapcsolata, és a neveket az Interneten akarja felbontani, ha a saját DNS szerverén ez nem történne meg. Az Internet gyökér szerverek alapértelmezett listája a System i navigátor programban áll rendelkezésre. A lista a System i navigátor kiadásakor aktuális. Az alapértelmezett lista aktualitását ellenőrizheti, ha összehasonlítja az InterNIC helyen lévővel. Frissítse a konfiguráció gyökér szerver listáját, hogy aktuális szinten tartsa.

Internet gyökér szerver címek beszerzése

A legfelső szintű gyökér szerverek címei időről-időre változnak, a címek aktuális állapotban tartása a DNS adminisztrátor felelőssége. Az InterNIC karbantartja az Internet gyökér szerverek címeinek aktuális listáját. Az Internet gyökér szerverek aktuális listájának megszerzéséhez kövesse a következő lépéseket:

1. jelentkezzen be az InterNIC szerverre Fájltviteli protokollt (FTP) használva anonim módszerrel:
FTP.INTERNIC.NET vagy RS.INTERNIC.NET
2. Töltse le ezt a fájlt: /domain/named.root
3. Tárolja a fájlt a következő katalógusban: /QOpenSys/QIBM/ProdData/OS400/DNS/ROOT.FILE

A tűzfal mögötti DNS szerver lehet, hogy nem rendelkezik megadott gyökér szerverekkel. Ebben az esetben a DNS szerver a lekérdezéseket csak a saját elsődleges tartomány adatbázis-állományában vagy gyorsítótárában meglévő bejegyzésekből oldhatja fel. A külső lekérdezéseket lehet, hogy továbbítja a tűzfal DNS számára. Ebben az esetben a tűzfal DNS szerver mint továbbító szerepel.

Intranet gyökér (root) szerverek

Ha a DNS szerver egy nagy intranet része, esetleg rendelkezhet belső gyökér szerverekkel. Ha a DNS szerver nem fogja elérni az Internetet, akkor nem kell betöltenie az alapértelmezett Internet szervereket. Azonban adja hozzá a belső gyökér szervereket, hogy a DNS szerver képes legyen felbontani a tartományán kívül eső belső címeket.

Kapcsolódó feladatok

“Zónák beállítása névszerveren” oldalszám: 27

Miután konfigurálta a Tartománynév-rendszer (DNS) szerver példányt, be kell állítania a zónákat az adott névszerverre.

Tartománynév-rendszer kezelése

A Tartománynév-rendszer (DNS) szerver kezelése magában foglalja a DNS funkció működésének ellenőrzését, a teljesítmény megfigyelését és a DNS adatok és fájlok karbantartását.

Tartománynév-rendszer funkció működésének ellenőrzése

- | A Tartományinformáció kereső (DIG) eszköz a Tartománynév-rendszer (DNS) szerver információinak összegyűjtésében és válaszainak tesztelésében nyújt segítséget. A DIG segítségével ellenőrizheti, hogy a DNS szerver helyesen működik-e.
- | Lekéri a loopback IP címhez (127.0.0.1) tartozó hosztnevet. A válasznak a hosztnevet kell tartalmaznia (localhost).
- | Lekérdezhet bizonyos neveket is, amelyek az ellenőrizni próbált szerver példányon vannak meghatározva. Ezáltal megbizonyosodhat arról, hogy a tesztelt szerver példány helyesen működik.

| Ha a DNS működését DIG segítségével kívánja ellenőrizni, akkor tegye a következőket:
| 1. A parancsorbba írja be a következőket: DIG HOSTNAME('127.0.0.1') REVERSE(*YES).

| A következő információnak kell megjelenni, beleértve a loopback hosztnevét is:

```
| ;; 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
```

| A DNS szerver helyesen válaszol, ha a loopback hosztnevet adja vissza: **localhost**.

| 2. Az Entert lenyomva lépjen ki a szekcióból.

| **Megjegyzés:** Ha a DIG használatához segítségre van szüksége, akkor írja be a ?DIG parancsot és nyomja meg az
| Entert.

| Biztonsági kulcsok kezelése

A biztonsági kulcsok lehetővé teszik a Tartománynév-rendszer (DNS) adatokhoz való hozzáférés korlátozását.

Két DNS rendszerhez kapcsolódó kulcstípus létezik, a DNS kulcsok és a dinamikus frissítési kulcsok. Mindegyik más szerepet játszik a DNS konfiguráció védelmében. Az alábbi leírás elmagyarázza, hogyan kapcsolódnak a DNS szerverhez.

| Tartománynév-rendszer kulcsok kezelése

A DNS kulcsok a BIND számára megadott kulcsok, amelyeket a DNS szerver használ a bejövő frissítések ellenőrzésének részeként.

Először konfigurálhat egy kulcsot, majd hozzárendelhet egy nevet. Majd, amikor védeni akar egy DNS objektumot, mint például a dinamikus zónát, akkor megadhatja a kulcsot a Címegezési (Address Match) listában.

A DNS kulcsok kezeléséhez kövesse ezeket a lépéseket:

1. A System i navigátor programban bontsa ki a **saját rendszer** → **Hálózat** → **szerverek** → **DNS** elemet.
2. A jobb oldali ablakrészben kattintson a jobb egérgombbal a kezelni kívánt DNS szerver példányra, majd válassza az előugró menü **Beállítás** menüpontját.
3. A DNS beállítása ablakban válassza ki a **Fájl** → **Kulcsok kezelése** lehetőséget.

| A Kulcsok kezelése ablakban elvégezheti a megfelelő kezelési feladatokat.

| Dinamikus frissítési kulcsok kezelése

A dinamikus frissítés kulcsai a DHCP szerver által végzett dinamikus frissítések védelmére szolgálnak.

| Ezeknek a kulcsoknak létezniük kell, ha a Tartománynév-rendszer (DNS) és a DHCP ugyanazon a System i platformon található. Ha a DHCP másik System i platformon van, akkor mindegyik távoli System i platformnak ugyanazokat a

- | dinamikus frissítési kulcsokat kell szétosztania, amelynek segítségével azok dinamikus frissítéseket küldenek a hiteles szervereknek. A szétosztást végezheti FTP, e-mail, stb. segítségével.

A dinamikus frissítési kulcsok kezeléséhez kövesse ezeket a lépéseket:

1. A System i navigátor programban bontsa ki a **saját rendszer** → **Hálózat** → **szerverek** → **DNS** elemet.
2. Kattintson a jobb egérgombbal a **DNS** ikonra, majd válassza ki a **Dinamikus frissítési kulcsok kezelése** elemet.

- | A Dinamikus frissítési kulcsok kezelése ablakban ezután elvégezheti a megfelelő kezelési feladatokat.

Tartománynév-rendszer szerver statisztika elérése

Az adatbázis kiírás és statisztikai eszközök segítséget nyújtanak a szerver teljesítményének felügyeletében és kezelésében.

A DNS több diagnosztikai eszközt is biztosít. Ezek a szerver teljesítményének figyelésére szolgálnak.

Kapcsolódó hivatkozás

“Tartománynév-rendszer konfigurációs fájlok karbantartása” oldalszám: 33

Az i5/OS DNS segítségével DNS szerver példányokat hozhat létre és kezelhet saját System i platformján. A DNS konfigurációs fájlok kezelése a System i navigátor segítségével történik. A fájlokat nem szabad saját kezűleg szerkeszteni. DNS konfigurációs fájlok létrehozására, módosítására és törlésére mindig a System i navigátor programot használja.

Szerver statisztika elérése

A szerver statisztika összegzi a szerver által fogadott lekérdezések és válaszok számát, mióta a szerver utoljára újraindította vagy újratöltötte az adatbázisát.

A Tartománynév-rendszer (DNS) lehetővé teszi a szerver példányra vonatkozó statisztika megtekintését. Az információk folyamatosan hozzáadódnak ehhez a fájlhoz, amíg nem törli a fájlt. Ez az információ hasznos lehet annak kiértékelésében, hogy milyen forgalmat fogadott a szerver, valamint a hibák nyomkövetésében. A szerver statisztikáról további információkat talál a DNS online segítség DNS szerver statisztika alapjai című részében.

A DNS szerver statisztika eléréséhez kövesse ezeket a lépéseket:

1. A System i navigátor programban bontsa ki a **saját rendszer** → **Hálózat** → **szerverek** → **DNS** elemet.
2. A jobb kereten kattintson a jobb egérgombbal a **DNS szerverre**, és válassza ki a **Konfigurációt**.
3. A DNS konfiguráció ablakban válassza a **Megjelenítés** → **Szerver statisztika** elemeket.

- | A named.stats fájlban lévő szerver statisztikai információk megjelenítésére a Távoli névdémon felügyelet (RNDC) parancsot is használhatja. A megfelelő parancs a következő:

- | `RNDC RNDCCMD('stats')`

Aktív szerver adatbázis elérése

Az aktív szerver adatbázis tartalmazza a zóna és a hoszt információkat, beleértve néhány zóna tulajdonságot, mint például a fennhatóság kezdetét (start of authority - SOA), illetve hoszt tulajdonságot, mint például a levéltovábbító (MX) információkat, amelyek hasznosak lehetnek hibakereséskor.

A DNS lehetővé teszi a szerver példány hiteles-, gyorsítótáras- és célzott adatairól készült kiírás megtekintését. A kiírás éppen úgy magában foglalja a szerver elsődleges és másodlagos zónáiról (egyenes és fordított kiosztási zónák) szóló információkat, mint azokat az információkat, amelyeket a szerver szerzett meg a lekérdezésekből.

Az aktív szerver adatbázis kiírás a System i navigátor segítségével tekinthető meg. Ha a fájlokról másolatot kell készítenie, akkor a az adatbázis kiírás fájl neve `named_dump.db` és az i5/OS katalógus útvonalon található: `/QIBM/UserData/OS400/DNS/<szerver példány>/`, ahol a `<szerver példány>` a DNS szerver példány neve. Az aktív szerver adatbázissal kapcsolatos további információkat a DNS szerver adatbázis kiírás bemutatása című online DNS súgótémakörben talál.

Az aktív szerver adatbázis kiíratás eléréséhez kövesse ezeket a lépéseket:

1. A System i navigátor programban bontsa ki a *saját rendszer* → **Hálózat** → **szerverek** → **DNS** elemet.
2. A jobb kereten kattintson a jobb egérgombbal a *DNS szerverre*, és válassza ki a **Konfigurációt**.
3. A DNS konfiguráció ablakban válassza a **Megjelenítés** → **Aktív szerver adatbázis** elemeket.

A named_dump.db fájlban lévő aktív szerver adatbázis információk megjelenítésére a Távoli névdémon felügyelet (RNDC) parancsot is használhatja. A megfelelő parancs a következő:



RNDC RNDCCMD('dumpdb -all')







Tartománynév-rendszer konfigurációs fájlok karbantartása









Az i5/OS DNS segítségével DNS szerver példányokat hozhat létre és kezelhet saját System i platformján. A DNS konfigurációs fájlok kezelése a System i navigátor segítségével történik. A fájlokat nem szabad saját kezűleg szerkeszteni. DNS konfigurációs fájlok létrehozására, módosítására és törlésére mindig a System i navigátor programot használja.





A DNS konfigurációs fájlok az integrált fájlrendszer alább felsorolt elérési útvonalában tárolódnak.

Megjegyzés: Az alábbi fájlszerkezet BIND 9. változaton futó DNS rendszerre vonatkozik.

Az alábbi táblázatban a fájlok az elérési útvonal hierarchiája szerint láthatók. A mentési ikonnal  jelzett fájlokat kell menteni az adatok védelme érdekében. A törlés ikonnal  jelzett fájlokat kell törölni szabályos időközönként.

Név	Ikon	Leírás
/QIBM/UserData/OS400/DNS/		A DNS alkatalógus kezdőpontja.
/QIBM/UserData/OS400/DNS/ <példány-n>/		A DNS példány alkatalógusának kezdőpontja.
ATTRIBUTES		A DNS használja ezt a fájlt az alkalmazott BIND verzió meghatározásához.
BOOT.AS400BIND4		BIND 4.9.3 szerver konfigurációs és irányelv fájl, amely az adott példány BIND 8 named.conf állományára konvertálódik. Ez a fájl akkor jön létre, ha BIND 4.9.3 szerverről BIND 9 szerverre tér át. Az áttérés biztonsági mentéseként funkcionál, és törölhető amint a BIND 9 szerver megfelelően működik.
named.ca		Az adott szerver példány gyökér szervereinek listája.
named.conf		Ez a fájl konfigurációs adatokat tartalmaz. Megmondja a szervernek, milyen zónákat kezel, hol vannak a zóna fájlok, mely zónák frissülhetnek dinamikusan, hol vannak a zóna továbbító szerverei, és milyen egyéb beállítások vannak.
named_dump.db		Az aktív szerver adatbázis számára létrehozott szerveradat kiíratás.
named.memstats		Szerver memória statisztika (ha a named.conf fájlban be van állítva).

Név	Ikon	Leírás
named.pid		A futó szerver Folyamat azonosítóját őrzi. A fájl létrehozásra kerül, valahányszor a DNS szerver elindul. Az Adatbázis, a Statisztikai és a Frissítési szerver funkciók számára használatos. Ne törölje és ne szerkessze ezt a fájlt.
named.random		Szerver által előállított entrópia fájl.
named.recurse		Rekurzív szerver lekérdezések (ha a System i navigátor kéri).
named.run		Alapértelmezett hibakeresési napló (kérésre). Újrakezdhető mint named.run.0, named.run.1 és így tovább.
named.stats		Szerver statisztika.
<elsődleges-zóna-n>.db		A szerveren lévő adott tartomány elsődleges zóna fájlja. A fájl a zóna össze erőforrásrekordját tartalmazza. Minden egyes zóna külön .db fájlal rendelkezik.
<elsődleges-zóna-n>.jnl		A zóna dinamikus frissítéseit tartalmazó naplófájl. Az első dinamikus frissítés fogadásakor jön létre. Ha a szerver leállítás vagy összeomlás után újraindul, akkor a a naplófájlt lejátszva elvégzi a zónán az utolsó zóna kiírás óta történt frissítéseket. A fájlt növekményes zónaátvitelhez (IXFR) is használják. Ezek a naplófájlok nem tűnnek el. A naplófájl olyan bináris fájl, amely szerkeszthető.
db.<másodlagos-zóna-n>		A szerveren lévő adott tartomány másodlagos zóna fájlja. A zónára vonatkozó összes erőforrásrekordot tartalmazza. A fájlt a másodlagos szerver kezdeti betöltésére használják indításkor, amennyiben az elsődleges szerver elérhetetlen. Minden egyes zóna külön .db fájlal rendelkezik.
/QIBM/UserData/OS400/DNS/_DYN/		A dinamikus frissítéshez szükséges fájlok őrzésére szolgáló alkatalógus.
<kulcs_azonosító-n>._KEY		.Symlink fájl a <kulcs_azonosító-n> kulccsal rendelkező DNSSEC kulcshoz. Mindig az utoljára létrehozott K<kulcs_azonosító-n>.+aaa+nmmnn.key kulcsra mutat.
<kulcs_azonosító-x>._DUK. <zóna-a>		Dinamikus frissítési kulcs, amely a <zóna-a> felé irányuló, <kulcs_azonosító-x> kulcsot használó dinamikus frissítési kérés kezdeményezéséhez szükséges.
<kulcs_azonosító-x>._KID		A <kulcs_azonosító-x> nevű kulcs_azonosítóhoz tartozó kulcs sort tartalmazó fájl.

Név	Ikon	Leírás
<kulcs_azonosító-y>._DUK. <zóna-a>		Dinamikus frissítési kulcs, amely a <zóna-a> felé irányuló, <kulcs_azonosító-y> kulcsot használó dinamikus frissítési kérés kezdeményezéséhez szükséges.
<kulcs_azonosító-y>._DUK. <zóna-b>		Dinamikus frissítési kulcs, amely a <zóna-b> felé irányuló, <kulcs_azonosító-y> kulcsot használó dinamikus frissítési kérés kezdeményezéséhez szükséges.
<kulcs_azonosító-y>._KID		A <kulcs_azonosító-y> nevű kulcs_azonosítóhoz tartozó kulcs sort tartalmazó fájl.
rndc-confgen.random.nnnnnn		Entrópia fájlok különféle parancsokhoz, amelyeknek erre szüksége van. Az nnnnn rész a fájl létrehozó job száma. Ezek csak akkor maradnak vissza, ha a parancs valamely okból megszakításra kerül és nem takarít maga után.

Kapcsolódó fogalmak

“Tartománynév-rendszer jogosultságok megállapítása” oldalszám: 23

A Tartománynév-rendszer (DNS) adminisztrátornak különleges jogosultsági szükségletei vannak. Vegye figyelembe a jogosultság biztonsági vonatkozásait is.

“Tartománynév-rendszer szerver statisztika elérése” oldalszám: 32

Az adatbázis kiírás és statisztikai eszközök segítséget nyújtanak a szerver teljesítményének felügyeletében és kezelésében.

Kapcsolódó feladatok

“Névszerverek beállítása” oldalszám: 26

A Tartománynév-rendszer (DNS) lehetővé teszi több névszerver példány létrehozását. Ez a témakör a névszerver konfigurálására vonatkozó utasításokat tartalmazza.

Fejlett Tartománynév-rendszer funkciók

A témakör elmagyarázza, hogyan használhatják a gyakorlott adminisztrátorok a Tartománynév-rendszer (DNS) fejlett funkcióit a DNS szerver könnyebb kezelésére.

A System i navigátor programban található DNS fejlett szolgáltatásokat tartalmazó felületet biztosít a DNS szerver beállításához és kezeléséhez. Az i5/OS grafikus felületet jól ismerő adminisztrátorok számára a következő feladatok parancsikon formájában állnak rendelkezésre. Segítségükkel gyorsan módosíthatja a szerver állapotát és attribútumait egyszerre több példányon is.

Kapcsolódó feladatok

“Tartománynév-rendszer hibakeresési beállításainak módosítása” oldalszám: 39

A Tartománynév-rendszer (DNS) hibakeresési funkciója olyan információkkal szolgál, amelyek segíthetik a DNS szerver problémák meghatározását és javítását.

Tartománynév-rendszer szerverek indítása és leállítása

Ha a System i navigátor felületen található Tartománynév-rendszer (DNS) lehetőség több szerver példány egyidejű indítását vagy leállítását nem teszi lehetővé, akkor ezen beállítások egyidejű módosítására (több példányon) használhat karakteres felületet.

A karakteres felület segítségével az összes DNS szerver példányt egyszerre elindíthatja, ha beírja az STRTCPSVR SERVER(*DNS) DNSSVR(*ALL) parancsot egy parancssorba. Az összes DNS szerver egyszerre történő leállításához írja be egy parancssorba az ENDTCPSVR SERVER(*DNS) DNSSVR(*ALL) parancsot.

Hibakeresési értékek módosítása

A hibakeresési szint módosítása hasznos lehet az adminisztrátoroknak, akik nagy zónákért felelnek, és nem akarnak nagy mennyiségű hibakeresési adatot kapni, amikor a szervert első alkalommal indítják és az összes zóna adatot betöltik.

A System i navigátor felületen található Tartománynév-rendszer (DNS) lehetőség a hibakeresési szint módosítását nem teszi lehetővé, amíg a szerver fut. A karakteres felület segítségével azonban módosíthatja a hibakeresési szintet a szerver futása közben. A karakteres felület segítségével módosítsa a hibakeresési szintet az alábbi lépések révén, kicserélve az *nnnnn* kifejezést a szerver példány tényleges nevével:

1. A parancssorba gépelje be az `ADDLIBLE QDNS` parancsot, és nyomja meg az Enter billentyűt.
2. Változtassa meg a hibakeresési szintet:
 - Ha a hibakeresést be kívánja kapcsolni vagy a hibakeresési szintet kívánja eggyel növelni, akkor írja be az `RNDC RNDCCMD('trace')` parancsot és nyomja meg az Entert.
 - A hibakeresés kikapcsolásához írja be az `RNDC RNDCCMD('notrace')` parancsot és nyomja meg az Entert.

Tartománynév-rendszer hibaelhárítása

A Tartománynév-rendszer (DNS) naplózási és hibakeresési beállítások a DNS szerverrel kapcsolatos problémák megoldásában lehetnek segítségére.

A DNS szinte ugyanúgy működik, mint más TCP/IP funkciók és alkalmazások. Az SMTP vagy az FTP alkalmazásokhoz hasonlóan a DNS jobok is a QSYSWRK alrendszerben futnak, és a feladattal kapcsolatos információkat tartalmazó logokat is a QTCP felhasználói profil birtokolja. Amikor a DNS job véget ér, a job log segítségével meghatározhatja a munka eredményét. Ha a DNS szerver nem a várt válaszokat adja vissza, a job log tartalmazhat olyan információkat, amelyek segíthetik a hibaelemzést.

A DNS konfiguráció több fájlból áll, amelyek mindegyike több különböző típusú rekordot tartalmaz. A DNS szerver hibák általában a DNS konfigurációs fájlokba történt hibás bejegyzések eredménye. Amikor hiba jelentkezik, ellenőrizze, hogy a DNS konfigurációs fájlok az elvárt bejegyzéseket tartalmazzák-e.

Jobok azonosítása

Ha belenéz a munkanaplóba a DNS szerver funkcióinak ellenőrzése végett (például a WRKACTJOB segítségével), vegye figyelembe a következő elnevezési irányelveket:

- Ha BIND 9 alapú szervereket futtat, akkor minden egyes futó szerver példányhoz külön job tartozik. A job neve öt rögzített karakterből (QTOBD) és az azt követő példánynévből áll. Például, ha két példány van, INST1 és INST2, akkor a jobok nevei QTOBDINST1 és QTOBDINST2 lesznek.

Tartománynév-rendszer szerver üzenetek naplózása

A Tartománynév-rendszer (DNS) számos naplózási paramétert biztosít, amelyeknek a beállításával megpróbálhatja megtalálni a hiba okát. A naplózás rugalmasságot nyújt a különféle súlyossági szintek, üzenet kategóriák és kimeneti fájlok kínálatával, s ezáltal finoman hangolhatja a naplózási funkciót a hibák felderítése végett.

A BIND 9 számos naplózási lehetőséget kínál. Megadhatja, hogy milyen típusú üzenetek legyenek naplózva, hova legyenek küldve a különböző típusú üzenetek, és az egyes üzenettípusok milyen súlyossági foka legyen naplózva. Általában az alapértelmezett naplózási beállítások megfelelőek, de ha változtatni akarja őket, olvassa el a BIND 9 dokumentációk más forrásait a naplózási információkkal kapcsolatban.

Naplózási csatornák

A DNS szerver különböző kimeneti csatornák felé naplózhatja az üzeneteket. A csatornák megadják, hogy hová lettek küldve az adatok. A következő csatorna típusokat választhatja ki:

- **Fájl csatornák**

A fájl csatornába naplózott üzenetek egy fájlba lesznek elküldve. Az alapértelmezett fájlcsatornák az `i5os_debug` és az `i5os_QPRINT`. Alapértelmezésben a hibakeresési üzenetek az `i5os_debug` csatornába (a `named.run` fájlba) lesznek naplózva, de megadhatja azt is, hogy más üzenetkategoróriák is ebbe a fájlba legyenek küldve. Az `i5os_QPRINT` csatornába naplózott üzenetkategoróriák a `QPRINT` spoolfájlba kerülnek a `QTCP` felhasználói profil alatt. Létrehozhat saját fájl csatornát is az alapértelmezés szerint meglévő csatornákon túlmenően.

- **Rendszernapló csatornák**

Az ide naplózott üzenetek a szerver munkanaplójába kerülnek. Az alapértelmezett rendszernapló csatorna az `i5os_joblog`. Az ide irányított naplóüzenetek a DNS szerver példány munkanaplójába kerülnek.

- **Null csatornák**

A null csatornába naplózott összes üzenet eldobásra kerül. Az alapértelmezett null csatorna az `i5os_null`. A kategóriákat a null csatornába irányíthatja, ha azt akarja, hogy egyetlen fájl sem jelenjen meg a naplófájlokban.

Üzenet kategóriák

Az üzenetek kategóriákba vannak csoportosítva. Megadhatja, hogy mely üzenet kategóriákat kell az egyes csatornába naplózni. A kategóriák a következők:

kliens Kliens kérések feldolgozása.

config Konfigurációs fájl értelmezés és feldolgozás.

adatbázis

Azon adatbázisokra vonatkozó üzenetek, amelyeket a DNS szerver belsőleg használ zóna és ideiglenes tároló adatok tárolására.

alapértelmezett

Azon kategóriákhoz tartozó naplózási paraméterek meghatározása, ahol nincs specifikus konfiguráció meghatározva.

csak-delegálás

Csak delegálás. Olyan lekérdezéseket naplóz, amelyek csak-delegálás zóna, illetve hint vagy csonk zónadeklarációban található csak-delegálás beállítás eredményeképpen `NXDOMAIN` válaszra lettek kényszerítve.

elküldés

Bejövő csomagok elküldése a feldolgozást végző szerver moduloknak.

dnssec DNS Biztonsági bővítmények (DNSSEC) és Tranzakció aláírás (TSIG) protokoll feldolgozás.

általános

A mindenes kategória, amelyet a más kategóriákba be nem sorolt dolgokhoz használnak.

tökéletlen-szerverek

A tökéletlen szerverek olyan távoli szervereken található hibás konfigurációk, amelyeket a BIND 9 fedez fel, amikor a feloldás során megpróbálja lekérdezni ezeket a szervereket.

hálózat

Hálózati műveletek.

értesítés

A `NOTIFY` protokoll.

feloldó DNS feloldás, például a rekurzív kikeresések, amelyeket a kliens nevében az adatokat ideiglenesen tároló névszerver hajt végre.

biztonság

Kérések jóváhagyása és megtagadása.

xfer-in A szerver által fogadott zónaátvittelek.

xfer-out

A szerver által küldött zónaátvittelek.

| **nem egyező**

| Olyan üzenetek, amelyek osztályát a névszerver nem tudta megállapítani, illetve amelyekhez nincs megfelelő nézet. A kliens kategóriába egy egysoros összegzés is naplózásra kerül. Ezt a kategóriát legjobb fájlba vagy az stderr kimenetre küldeni. Alapértelmezésben a null csatornára kerül elküldésre.

| **frissítés**

| Dinamikus frissítések.

| **frissítés-biztonság**

| Frissítési kérések jóváhagyása és megtagadása. Lekérdezések határozzák meg, hogy a lekérdezéseket hová kell naplózni. Indításkor a kategória lekérdezések meghatározása a lekérdezések naplózását engedélyezi kivéve, ha a querylog beállítás meg van adva.

| A lekérdezőnapló-bejegyzés a kliens IP címét és portszámát, a lekérdező nevét, osztályát és típusát tartalmazza. Azt is tartalmazza továbbá, hogy a Rekúzió szükséges kapcsoló be van-e állítva (+ ha igen és - ha nem), az EDNS használatban van-e (E), illetve a lekérdező alá van-e írva (S).

| A naplófájlok egészen nagyra megnőhetnek, szabályos időközönként törölni kell őket. A DNS szerver összes naplófájljának tartalma törlődik, amikor a DNS szerver leáll és elindul.

Üzenet súlyossága

A csatornák lehetővé teszik az üzenetek szűrését súlyosságuk szerint. Minden egyes csatornára megadhatja a súlyossági szintet, amely meghatározza a naplózandó üzeneteket. A következő súlyossági szintek lehetségesek:

- Súlyos
- Hiba
- Figyelmeztetés
- Megjegyzés
- Információ
- Hibakeresés (adja meg a 0-11 hibakeresési szintet)
- Dinamikus (a szerver indítás hibakeresési szintjének öröklése)

A kiválasztott súlyosságú és az annál magasabb szintű összes üzenet naplózva lesz. Például, ha a Figyelmeztetést választotta ki, akkor a csatorna a Figyelmeztetés, a Hiba és a Súlyos szintű üzeneteket fogja naplózni. Ha a Hibakeresés szintet választja ki, akkor megadhat egy 0 és 11 közötti értéket, amelyekre vonatkozóan naplózni kívánja a hibakeresési üzeneteket.

Naplózási beállítások módosítása

A naplózási beállítások eléréséhez kövesse ezeket a lépéseket:

1. A System i navigátor programban bontsa ki a **saját rendszer** → **Hálózat** → **szerverek** → **DNS** elemet.
2. A jobb kereten kattintson a jobb egérgombbal a **DNS szerverre**, és válassza ki a **Konfigurációt**.
3. A DNS konfiguráció ablakban kattintson a jobb egérgombbal a **DNS szerverre**, és válassza ki a **Tulajdonságokat**.
4. A Szerver tulajdonságok ablakban válassza ki a **Csatornák** fület, hogy létrehozson új fájl csatornát vagy csatorna tulajdonságot, mint például az egyes csatornába naplózott üzenetek súlyossági szintjét.
5. A Szerver tulajdonságok ablakban válassza a **Naplózás** fület, hogy megadja, mely üzenet kategóriák legyenek naplózva az egyes csatornába.

Hibaelhárítás tipp a súlyossági szinttel kapcsolatban

Az i5os_joblog csatorna alapértelmezett súlyossági szintje Hiba szintre van beállítva. Ez a beállítás csökkenti a tájékoztatást tartalmazó és a figyelmeztető üzenetek számát, amelyek egyébként rontaná a teljesítményt. Ha hibákat tapasztal, de a munkanapló nem jelzi a probléma forrását, akkor esetleg változtassa meg a súlyossági szintet. Kövesse a fenti eljárást a Csatornák lap eléréséhez, majd módosítsa az i5os_joblog csatorna súlyossági szintjét Figyelmeztetés,

Megjegyzés vagy Információ szintre, hogy több naplótudjon megtekinteni. Amint megoldja a problémát, állítsa vissza a súlyossági szintet Hiba értékre, hogy csökkentse a munkanaplóban az üzenetek számát.

Tartománynév-rendszer hibakeresési beállításainak módosítása

A Tartománynév-rendszer (DNS) hibakeresési funkciója olyan információkkal szolgál, amelyek segíthetik a DNS szerver problémák meghatározását és javítását.

A DNS a hibakeresési vezérlés 12 szintjét kínálja. A naplózás általában könnyebb módszert jelent a problémák megtalálására, azonban néhány esetben szükség lehet hibakeresésre is. Normál üzemi feltételek esetén a hibakeresés kikapcsolt állapotban van (értéke = 0). A problémák javítása érdekében ajánlatos először a naplózást igénybe venni.

Az érvényes hibakeresési szint 0 és 11 közé esik. Az IBM szerviz képviselője segíteni tud a DNS probléma diagnosztizálásához szükséges hibakeresési érték meghatározásában. Az 1 vagy annál magasabb értékek a hibakeresési információkat a felhasználó i5/OS katalógusában található named.run fájlba írják: /QIBM/UserData/OS400/DNS/<szerver példány>, ahol a <szerver példány> a DNS szerver példány neve. A named.run fájl mérete folyamatosan növekszik, amíg a hibakeresési szint 1-es értékű vagy magasabb, és amíg a DNS szerver folytatja futását. Használhatja a Szerver tulajdonságok - Csatornák oldalt is, ahol megadhatja a named.run fájl változatainak számát és maximális méretét.

A DNS szerver példány hibakeresési értékének megváltoztatásához kövesse ezeket a lépéseket:

1. A System i navigátor programban bontsa ki a **saját rendszer** → **Hálózat** → **szerverek** → **DNS** elemet.
2. A jobb kereten kattintson a jobb egérgombbal a **DNS szerverre**, és válassza ki a **Konfigurációt**.
3. A DNS konfiguráció ablakban kattintson a jobb egérgombbal a DNS szerverre, és válassza ki a **Tulajdonságokat**.
4. A Szerver tulajdonságok - Általános lapon adja meg a szerver indításkori hibakeresési szintjét.
5. Ha a szerver fut, állítsa le, majd indítsa el újra a szervert.

Megjegyzés: A hibakeresési szint módosítása addig nem jut érvényre, amíg fut a szerver. Az itt beállított hibakeresési szint a szerver következő teljes újraindításakor jut érvényre. Ha a hibakeresési szintet a szerver futása alatt kell megváltoztatnia, olvassa el a Fejlett DNS funkciókat.

Kapcsolódó fogalmak

“Fejlett Tartománynév-rendszer funkciók” oldalszám: 35

A témakör elmagyarázza, hogyan használhatják a gyakorlott adminisztrátorok a Tartománynév-rendszer (DNS) fejlett funkcióit a DNS szerver könnyebb kezelésére.

Tartománynév-rendszer témakörhöz kapcsolódó információk

Az IBM Redbooks kiadványok, webhelyek és egyéb információs központi témakör gyűjtemények is tartalmaznak a Tartománynév-rendszer (DNS) témakör gyűjteményhez kapcsolódó információkat. A PDF fájlokat megtekintheti vagy kinyomtathatja.






IBM Redbooks kiadványok

AS/400 TCP/IP automatikus beállítás: DNS és DHCP támogatás  (5181 KB)

Ez a Redbooks kiadvány az i5/OS rendszerben található Tartománynév-rendszer (DNS) szerver és Dinamikus hoszt konfigurációs protokoll (DHCP) szerver támogatást mutatja be. Különböző példákon keresztül segít DNS és DHCP támogatás telepítésében, személyre szabásában, beállításában és hibaelhárításában.

| Webhelyek

- | • *DNS és BIND*, ötödik kiadás. Paul Albitz és Cricket Liu. Kiadó: O'Reilly and Associates, Inc.  Sebastopol, California, 2006. ISBN szám: 0-59610-057-4.

- | • A BIND adminisztrátorok kézikönyve(PDF változatban) az Internet System Consortium (ISC)  webhelyen.
- | • Internet Software Consortium webhely , amely híreket, hivatkozásokat és egyéb forrásokat nyújt a BIND-hez.
- | • Az InterNIC  karbantartja az összes tartománynév bejegyző katalógusát, amelyeket az Internet Corporation for Assigned Names and Numbers (ICANN) hatalmazott fel.
- | • A DNS erőforrás címjegyzék  DNS referencia anyagokat és sok egyéb DNS erőforrásra mutató hivatkozásokat biztosít, fórum csoportokat is beleértve. Biztosítja továbbá a DNS szolgáltatással kapcsolatos RFC dokumentumok listáját.  .

Kapcsolódó hivatkozás

“Tartománynév-rendszer PDF fájl” oldalszám: 2

Az információkat tartalmazó PDF fájlt megjelenítheti és kinyomtathatja.

. Nyilatkozatok

Ezek az információk az Egyesült Államokban forgalmazott termékekre és szolgáltatásokra vonatkoznak.

Az IBM lehet, hogy nem ajánlja az ebben a dokumentációban tárgyalt termékeket, szolgáltatásokat vagy kiegészítőket más országokban. Kérjen tanácsot a helyi IBM képviselőtől az adott területen pillanatnyilag rendelkezésre álló termékekről és szolgáltatásokról. Bármely hivatkozás IBM termékre, programra vagy szolgáltatásra nem szándékozik azt állítani vagy sugallni, hogy csak az az IBM termék, program vagy szolgáltatás alkalmazható. Bármely funkcionálisan azonos termék, program vagy szolgáltatás, amely nem sérti az IBM érvényes szellemi tulajdonával kapcsolatos jogokat, használható helyette. Bármely nem IBM termék, program vagy szolgáltatás működésének kiértékelése és ellenőrzése azonban a felhasználó felelőssége.

A dokumentum tartalmával kapcsolatban az IBM-nek bejegyzett, vagy bejegyzés alatt álló szabadalmi lehetnek. Ennek a dokumentumnak az átadása azonban nem jelenti ezen szabadalmak licencjogának átadását is. Licencjog iránti kéréseit írásban az alábbi címre küldje:

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

Kétbyte-os (DBCS) információkkal kapcsolatos engedélyezési kérésekkel forduljon az IBM Intellectual Property részleghez saját országában, vagy írjon az alábbi címre:

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

A következő bekezdés nem vonatkozik az Egyesült Királyságra, valamint azokra az országokra, amelyeknek jogi szabályozása ellentétes a bekezdés tartalmával: AZ INTERNATIONAL BUSINESS MACHINES CORPORATION JELEN KIADVÁNYT "ÖNMAGÁBAN", BÁRMIFÉLE KIFEJEZETT VAGY VÉLELMEZETT GARANCIA NÉLKÜL ADJA KÖZRE, IDEÉRTVE, DE NEM KIZÁRÓLAG A JOGSÉRTÉS KIZÁRÁSÁRA, A KERESKEDELMİ ÉRTÉKESİTHETŐSÉGRE ÉS BIZONYOS CÉLRA VALÓ ALKALMASSÁGRA VONATKOZÓ VÉLELMEZETT GARANCIÁT. Bizonyos államok nem engedélyezik egyes tranzakciók kifejezett vagy vélelmezett garanciáinak kizárását, így elképzelhető, hogy az előző bekezdés Önre nem vonatkozik.

Jelen dokumentum tartalmazhat technikai, illetve szerkesztési hibákat. Az itt található információk bizonyos időnként módosításra kerülnek; a módosításokat a kiadvány új kiadásai tartalmazzák. Az IBM mindennemű értesítés nélkül fejlesztheti és/vagy módosíthatja a kiadványban tárgyalt termékeket és/vagy programokat.

A könyvben a nem IBM webhelyekre történő hivatkozások csupán kényelmi célokat szolgálnak, és semmilyen módon sem kívánják azt a látszatot kelteni, hogy az IBM jóváhagyná ezeket a webhelyeket. Az ilyen webhelyeken található anyagok nem képezik az adott IBM termék dokumentációjának részét, így ezek használata csak saját felelősségre történhet.

Az IBM belátása szerint bármilyen formában felhasználhatja és továbbadhatja a felhasználóktól származó információkat anélkül, hogy a felhasználó felé ebből bármilyen kötelezettsége származna.

A programlicenc azon birtokosainak, akik információkat kívánnak szerezni a programról (i) a függetlenül létrehozott programok vagy más programok (beleértve ezt a programot is) közti információcseréhez, illetve (ii) a kicserélt információk kölcsönös használatához, fel kell venniük a kapcsolatot az alábbi címmel:

IBM Corporation

Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Az ilyen információk bizonyos feltételek és kikötések mellett állnak rendelkezésre, ideértve azokat az eseteket is, amikor ez díjfizetéssel jár.

A dokumentumban tárgyalt licencprogramokat és a hozzájuk tartozó licenc anyagokat az IBM az IBM Vásárlói megállapodás, az IBM Nemzetközi programlicenc szerződés, az IBM Gépi kódra vonatkozó licencszerződés vagy a felek azonos tartalmú megállapodása alapján biztosítja.

A dokumentumban található teljesítményadatok ellenőrzött környezetben kerültek meghatározásra. Ennek következtében a más működési körülmények között kapott adatok jelentősen különbözhetnek a dokumentumban megadottaktól. Egyes mérések fejlesztői szintű rendszereken kerültek végrehajtásra, így nincs garancia arra, hogy ezek a mérések az általánosan hozzáférhető rendszerek esetében is. Továbbá bizonyos mérések következtetés útján kerültek becslésre. A tényleges értékek eltérhetnek. A dokumentum felhasználóinak ellenőrizni kell az adatok alkalmazhatóságát az adott környezetben.

A nem IBM termékekre vonatkozó információkat az IBM a termékek szállítójától, az általuk közzétett bejelentésekből, illetve egyéb nyilvánosan elérhető forrásokból szerezte be. Az IBM nem tesztelte ezeket a termékeket, így a nem IBM termékek esetében nem tudja megerősíteni a teljesítményre és kompatibilitásra vonatkozó, valamint egyéb állítások pontosságát. A nem IBM termékekkel kapcsolatos kérdéseivel forduljon az adott termék szállítójához.

Az IBM jövőbeli elképzeléseivel és szándékaival kapcsolatos összes állítás előzetes értesítés nélkül megváltozhat vagy visszavonásra kerülhet, ezek csupán célokat képviselnek.

Az információk között példaként napi üzleti tevékenységekhez kapcsolódó jelentések és adatok lehetnek. A valóságot a lehető legjobban megközelítő illusztráláshoz a példákban egyének, vállalatok, márkák és termékek nevei szerepelnek. Minden ilyen név a képzelet szüleménye, és valódi üzleti vállalkozások neveivel és címeivel való bármilyen hasonlóságuk teljes egészében a véletlen műve.

Szerzői jogi licenc:

Jelen dokumentáció forrásnyelvű példa alkalmazásokat tartalmazhat, amelyek a programozási technikák bemutatására szolgálnak a különböző működési környezetekben. A példaprogramokat tetszőleges formában, az IBM-nek való díjfizetés nélkül másolhatja, módosíthatja és terjesztheti fejlesztési, használati, marketing célból, illetve olyan alkalmazási programok terjesztése céljából, amelyek megfelelnek azon operációs rendszer alkalmazásprogram illesztőjének, ahol a példaprogramot írta. A példák nem kerültek minden körülmények között tesztelésre. Az IBM így nem tudja garantálni a megbízhatóságukat, szervizelhetőségüket, de még a programok funkcióit sem.

A példaprogramok minden példányának, illetve a belőlük készített összes származtatott munkának tartalmaznia kell az alábbi szerzői jogi nyilatkozatot:

© (cégnév) (évszám). A kód bizonyos részei az IBM Corp. példaprogramjaiból származnak. © Copyright IBM Corp. (évszám vagy évszámok). Minden jog fenntartva.

Ha az információkat elektronikus formában tekinti meg, akkor elképzelhető, hogy a fotók és színes ábrák nem jelennek meg.

Programozási felületre vonatkozó információk

Ez a Tartománynév-rendszer (DNS) kiadvány leír olyan programozási felületeket, amelyek révén a vásárló az IBM i5/OS szolgáltatásait kihasználó programokat írhat.

Védjegyek

A következő kifejezések az International Business Machines Corporation védjegyei az Egyesült Államokban és/vagy más országokban:

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

Az Adobe, az Adobe logó, a PostScript és a PostScript logó az Adobe Systems Incorporated bejegyzett védjegyei vagy védjegyei az Egyesült Államokban és más országokban.

Más vállalatok, termékek vagy szolgáltatások nevei mások védjegyei vagy szolgáltatás védjegyei lehetnek.

Feltételek és kikötések

A kiadványok használata az alábbi feltételek és kikötések alapján lehetséges.

Személyes használat: A kiadványok másolhatók személyes, nem kereskedelmi célú felhasználásra, feltéve, hogy valamennyi tulajdonosi feljegyzés megmarad. Az IBM kifejezett engedélye nélkül nem szabad a kiadványokat vagy azok részeit terjeszteni, megjeleníteni, illetve belőlük származó munkát készíteni.

Kereskedelmi használat: A kiadványok másolhatók, terjeszthetők és megjeleníthetők, de kizárólag a vállalaton belül, és csak az összes tulajdonosi feljegyzés megtartásával. Az IBM kifejezett hozzájárulása nélkül nem készíthetők olyan munkák, amelyek a kiadványokból származnak, továbbá nem másolhatók, nem terjeszthetők és nem jeleníthetők meg, még részben sem, a vállalaton kívül.

A jelen engedélyben foglalt, kifejezetten megadott hozzájáruláson túlmenően a kiadványokra, illetve a bennük található információkra, adatokra, szoftvekre vagy egyéb szellemi tulajdonra semmilyen más kifejezett vagy vélelmezett engedély nem vonatkozik.

Az IBM fenntartja magának a jogot, hogy jelen engedélyeket saját belátása szerint bármikor visszavonja, ha úgy ítéli meg, hogy a kiadványokat az IBM érdekeit sértő módon használják fel, vagy a fenti útmutatásokat nem megfelelően követik.

Jelen információk kizárólag valamennyi vonatkozó törvény és előírás betartásával tölthetők le, exportálhatók és reexportálhatók, beleértve az Egyesült Államok exportra vonatkozó törvényeit és előírásait is.

AZ IBM A KIADVÁNYOK TARTALMÁRA VONATKOZÓAN SEMMIFÉLE GARANCIÁT NEM NYÚJT. A KIADVÁNYOK "ÖNMAGUKBAN", BÁRMIFÉLE KIFEJEZETT VAGY VÉLELMEZETT GARANCIA VÁLLALÁSA NÉLKÜL KERÜLNEK KÖZREADÁSRA, IDEÉRTVE, DE NEM KIZÁRÓLAG A KERESKEDELMI ÉRTÉKESÍTHETŐSÉGRE, A SZABÁLYOSSÁGRA ÉS AZ ADOTT CÉLRA VALÓ ALKALMASSÁGRA VONATKOZÓ VÉLELMEZETT GARANCIÁKAT IS.



Nyomtatva Dániában