

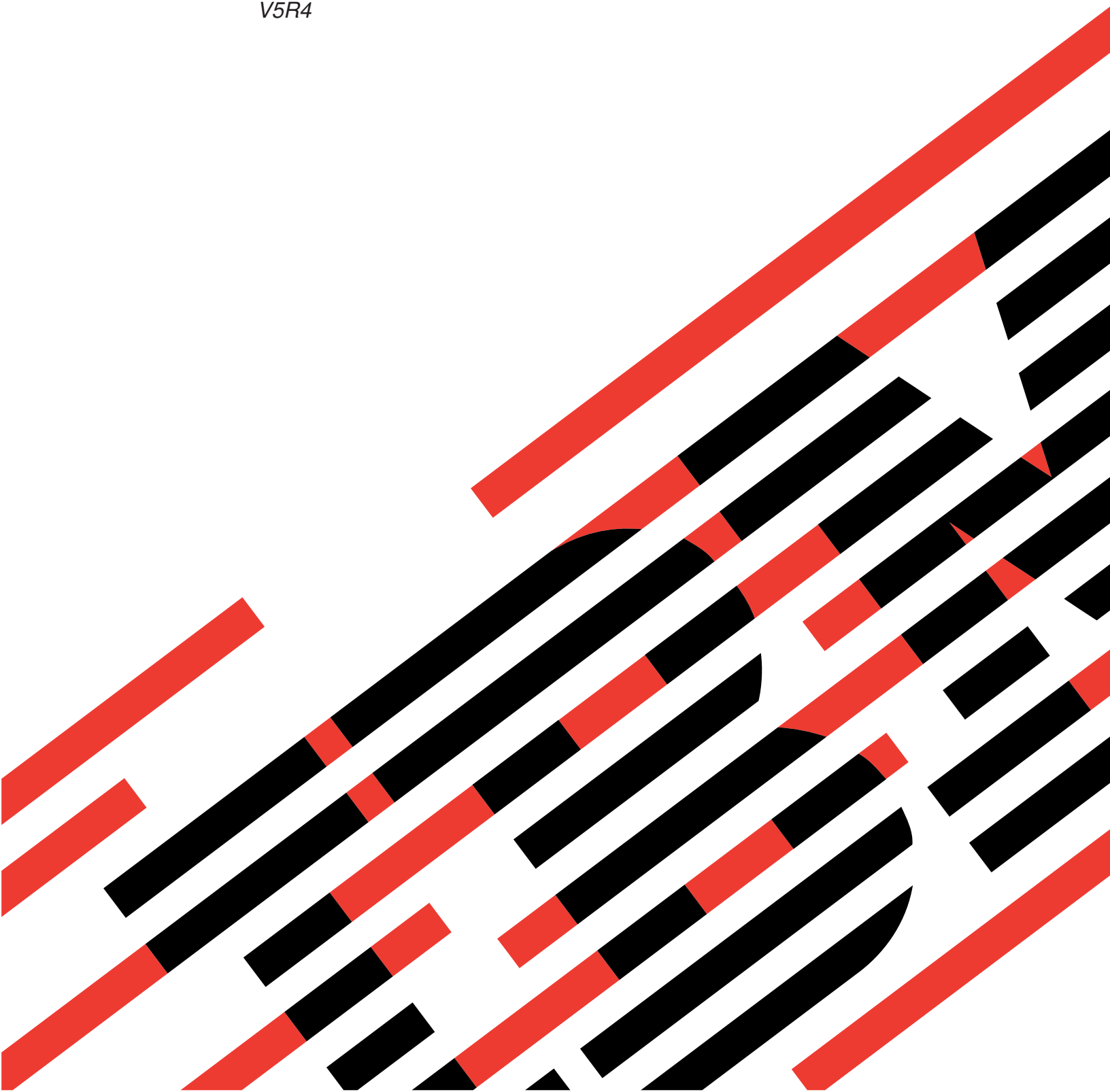


IBM Systems - iSeries

Hálózat

Domain Name System

V5R4





IBM Systems - iSeries
Hálózat
Domain Name System

V5R4

Megjegyzés

Mielőtt a jelen leírást és a vonatkozó terméket használná, olvassa el a “Nyilatkozatok” oldalszám: 37 helyen lévő tájékoztatót.

Hatodik kiadás (2006. február)

Ez a kiadás a V5R4M0 szintű IBM i5/OS (száma: 5722-SS1) termékre, és minden azt követő változatra és módosításra vonatkozik, amíg ez másképpen nincs jelezve. Ez a verzió nem fut minden csökkentett utasításkészletű (RISC) rendszeren és CISC modellen.

© Szerzői jog IBM Corporation 1998, 2006. Minden jog fenntartva

Tartalom

Domain Name System	1	Domain Name System elérése az iSeries navigátorban	23
Nyomtatható PDF	1	Névszerverek konfigurálása	24
Domain Name System koncepciók	1	Domain Name System konfigurálása dinamikus frissítések fogadásához	25
A zónák alapjai	2	Domain Name System fájlok importálása	26
Domain Name System lekérdezések alapjai.	3	Külső DNS adatok elérése	26
Domain Name System tartomány beállítás	5	DNS kezelése	27
Dinamikus frissítések	5	Domain Name System funkció ellenőrzése NSLookup segítségével.	27
BIND 8 jellemzők	6	Biztonsági kulcsok kezelése	28
DNS erőforrás rekordok	8	DNS kulcsok kezelése	28
Posta és MX rekordok	11	Dinamikus frissítések kulcsainak kezelése.	28
Domain Name System példák	12	Domain Name System szerver statisztika elérése.	29
Példa: Egy Domain Name System szerver az intranet számára	12	DNS konfigurációs fájlok karbantartása	29
Példa: Egy Domain Name System szerver Internet hozzáféréssel	14	Fejlett Domain Name System funkciók	32
Példa: Domain Name System és Dynamic Host Configuration Protocol ugyanazon az iSeries szerveren .	16	Domain Name System hibaelhárítás	33
Példa: Domain Name System felosztása tűzfalon keresztül	18	Domain Name System szerver üzenetek naplózása	33
Domain Name System tervezése	20	Domain Name System hibakeresési beállítások módosítása	35
Domain Name System jogosultságok meghatározása	20	Domain Name System témakörhöz kapcsolódó információk.	36
Tartomány struktúra meghatározása	20		
Biztonsági intézkedések tervezése	21	Nyilatkozatok	37
Domain Name System követelmények	22	Programozási csatolóra vonatkozó megjegyzés	38
Domain Name System telepítésének ellenőrzése	23	Védjegyek	39
Domain Name System telepítése	23	Feltételek	39
Domain Name System konfigurálása	23		

Domain Name System

A Domain Name System (DNS) egy osztott adatbázis rendszer, amely az Internet Protocol (IP) címekhez tartozó hoszt (gazdagép) nevek kezelésére szolgál.

A DNS használata azt jelenti, hogy az emberek egyszerű neveket használhatnak, mint például www.jkltoys.com, a hoszt kereséséhez a nehezen megjegyezhető IP cím (xxx.xxx.xxx.xxx) helyett. Egyetlen szerver is lehet felelős a zónarész hosztneveinek vagy IP címeknek ismeretéért, de a DNS szerverek képesek együtt is működni az összes tartománynév IP címekre történő leképezésében. A DNS szerverek együttműködése teszi lehetővé, hogy a számítógépek kommunikáljanak egymással az Interneten keresztül.

Az IBM OS/400 Verzió 5 Változat 1 (V5R1) kiadásban lévő DNS szolgáltatások a BIND (Berkeley Internet Name Domain) verzió 8 néven ismert ipari szabványú DNS megvalósításon alapulnak. Az előző IBM OS/400 DNS szolgáltatások a BIND 4.9.3 szabványon alapultak. Az új BIND 8 alapú DNS szerver használatához telepíteni kell az i5/OS 33-as opcióját, Portable Application Solutions Environment (PASE), az IBM eServer iSeries szerveren. Ha nem rendelkezik telepített PASE programmal, még futtatni tudja az előző változatokban rendelkezésre álló, BIND 4.9.3-ra épülő DNS szerveret. Azonban a BIND 8-ra történő frissítés javított funkciókat és jobb biztonságot testesít meg a DNS szerver számára.

Megjegyzés: Ez a témakör a BIND 8 alapú új funkciókat tárgyalja. Ha nem használ PASE programot a BIND 8 alapú DNS futtatásához, olvassa el a BIND 4.9.3 alapú DNS szerverről szóló V4R5 DNS Információs központ témakört.

Nyomtatható PDF

A témakör az itt leírtak PDF változatának megtekintését vagy nyomtatását ismerteti.


A PDF változat megtekintéséhez vagy letöltéséhez válassza ki a Domain Name System (about 625 KB) hivatkozást.

PDF fájlok mentése

A PDF fájl munkaállomáson történő mentése megjelenítés vagy nyomtatás céljából:

1. Kattintson a jobb egérgombbal a PDF fájlra a böngészőjében (kattintás a jobb oldali egérgombbal a fenti hivatkozásra).
2. Kattintson a PDF helyi mentésére szolgáló opcióra.
3. Válassza ki azt a könyvtárat, ahová menteni kívánja a PDF fájlt.
4. Kattintson a **Mentés** gombra.

Adobe Acrobat Reader letöltése

- 1. A PDF állományok megtekintéséhez vagy nyomtatásához telepített Adobe Acrobat Reader programra van szükség.
- 2. Ingyenes példányát letöltheti az Adobe honlapjáról (www.adobe.com/products/acrobat/readstep.html) .

Domain Name System koncepciók

A témakör ismerteti a Domain Name System (DNS) elvét és működését. Bemutatja a különböző típusú zónákat, amelyek megadhatók a DNS szerveren.

A Domain Name System (DNS) egy osztott adatbázis rendszer, amely az Internet Protocol (IP) címekhez tartozó hoszt (gazdagép) nevek kezelésére szolgál. A DNS használata azt jelenti, hogy az emberek egyszerű neveket használhatnak, mint például www.jkltoys.com, a hoszt kereséséhez a nehezen megjegyezhető IP cím (xxx.xxx.xxx.xxx) helyett.

Egyetlen szerver is lehet felelős a zónarész hosztneveinek vagy IP címeinek ismeretéért, de a DNS szerverek képesek együtt is működni az összes tartomány név IP címekre történő leképezésében. A DNS szerverek együttműködése teszi lehetővé, hogy a számítógépek kommunikáljanak egymással az Interneten keresztül.

A DNS adatok véget vetnek a tartományok hierarchiájának. A szerverek csak az adatok egy kis részének ismeretéért 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 erőforrás rekordjai segítségével. A lekérdezési folyamat a tényezők számától függ. A DNS lekérdezések alapjai című rész magyarázza el azokat az utakat, ahogy a kliens meg tudja oldani a lekérdezést.

A zónák alapjai

A témakör ismerteti a Domain Name System (DNS) zónákat és zónatípusokat.

A DNS adatok kezelhető adatkészletekre (úgynevezett *zónákra*) oszlanak. A zónák a DNS tartomány egy vagy több részének neveit és IP címét tartalmazzák. A szerver, amely a zónára vonatkozó összes információt tartalmazza, hiteles szerver a tartományra vonatkozóan. Időnként, átadhatja egy adott altartományra vonatkozó DNS lekérdezésekre való válaszadási jogosultságot egy másik DNS szervernek. 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

Az iSeries DNS segítségével megadhatja a zónák számos típusát, amelyek a DNS adatok kezelését segítik:

Elsődleges zóna

Az elsődleges zóna betölti a zóna adatokat közvetlenül a hoszton lévő fájlból. Az elsődleges zóna tartalmazhat alzónát vagy utódzónát. Tartalmazhat továbbá erőforrás rekordokat, mint például hoszt, álnév (CNAME), cím (A) 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 erőforrás rekordok 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.

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

“Domain Name System lekérdezések alapjai”

A témakör elmagyarázza, hogyan oldja fel a Domain Name System (DNS) a kliensek lekérzéseit.

“Zónák konfigurálása a névszerveren” oldalszám: 25

Miután konfigurálta a Domain Name System (DNS) szerver példányt, be kell állítania a zónákat az adott névszerverre.

Kapcsolódó hivatkozás

“Példa: Egy Domain Name System szerver az intranet számára” oldalszám: 12

A példa egyszerű alhálózatot mutat DNS szerverrel belső használatra.

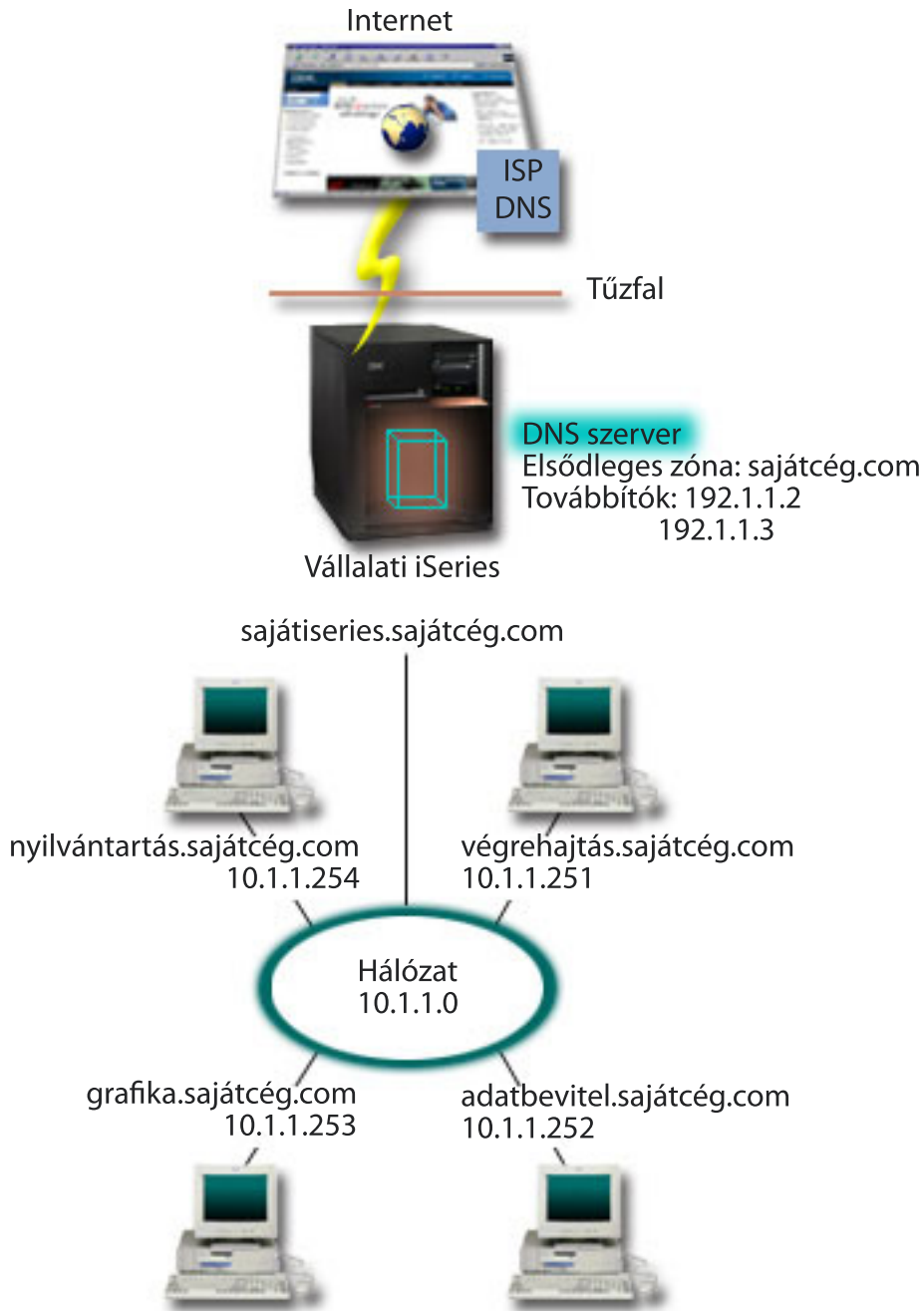
“DNS erőforrás rekordok” oldalszám: 8

Ez a témakör ismerteti, hogyan használja fel a DNS az erőforrás rekordokat. Az erőforrás rekordok a tartománynevek és az IP címek adatainak tárolására szolgálnak. Ez a témakör az OS/400 V5R1 változatban elérhető erőforrás rekordok kereshető listáját tartalmazza.

Domain Name System lekérdezések alapjai

A témakör elmagyarázza, hogyan oldja fel a Domain Name System (DNS) a kliensek lekérzéseit.

A kliensek DNS szervereket vesznek igénybe az információk megtalálásához. A kérés jöhet közvetlenül a kientől, vagy a kliensen futó alkalmazástól. A kliens elküldi a lekérzési üzenetet a DNS szervernek, amely tartalmazza a teljesen megadott tartománynevet (FQDN), a lekérzés típusát, mint például egy adott erőforrás rekord, 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 *adatbevitel* 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 *adatbevitel* kéri a *www.jkl.com* IP címet. Ez a hoszt nincs benne a DNS szerver zóna adataiban. Most két út van, amit követni lehet: a rekurzió vagy az iteráció. Ha a DNS szervernél be van állítva a rekurzió, akkor a szerver lekérdezheti vagy kapcsolatba léphet más DNS szerverekkel a kérő kliens nevében, hogy teljesen megoldja a nevet, amelyet azután válaszként visszaküld a kliensnek. Ha a DNS szerver egy másik DNS szervert kérdez le, akkor a kérő szerver tárolni fogja a feleletet, hogy egy következő hasonló kérésnél már használni tudja. A kliens is

megkísérelheti felvenni a kapcsolatot más DNS szerverekkel saját maga nevében a név felbontása érdekében. Ezt a folyamatot nevezzük *iterációnak*, amikor is a kliens önálló és további lekérdezésekkel operál a szerverektől érkező válaszok alapján.

Kapcsolódó hivatkozás

“A zónák alapjai” oldalszám: 2

A témakör ismerteti a Domain Name System (DNS) zónákat és zónatípusokat.

“Példa: Egy Domain Name System szerver Internet hozzáféréssel” oldalszám: 14

A példa egyszerű alhálózatot mutat Domain Name System (DNS) szerverrel, közvetlen Internet kapcsolattal.

Domain Name System tartomány beállítás

A témakör áttekintést nyújt a tartomány regisztrációjáról, valamint hivatkozásokat más helyekre a saját tartományterület beállításához.

A DNS lehetővé teszi nevek és címek kiszolgálását az intraneten vagy a 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 szolgáltatón (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: Egy Domain Name System szerver Internet hozzáféréssel” oldalszám: 14

A példa egyszerű alhálózatot mutat Domain Name System (DNS) szerverrel, közvetlen Internet kapcsolattal.

Kapcsolódó tájékoztatás

Internet Network Information Center (InterNIC)

Dinamikus frissítések

A BIND 8-ra épülő OS/400 V5R1 DNS támogatja a dinamikus frissítéseket. Ez lehetővé teszi a külső forrásoknak, mint például a DHCP-nek, hogy frissítéseket küldjön a DNS szervernek.

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 rendeli 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 sztatikus adatbázis tárolta. Az összes DNS erőforrás rekordot a rendszergazdának kellett létrehozni és karbantartani. Most, a BIND 8-at futtató DNS konfigurálható úgy, hogy elfogadjon kéréseket más forrásoktól a zóna adatok dinamikus frissítésére.

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 (gazdagépek) 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 gazdagépekre vonatkozó lekérdezések sikeres megoldását, még akkor is, ha az IP címek változnak.

A DHCP úgy is konfigurálható, hogy frissítse a cím kiosztási (A) rekordokat, a fordított keresési mutató (PTR) rekordokat, vagy mindkettőt a kliens nevében. Az A rekord leképezi a gép nevét IP címre. A PTR rekord leképezi a gép IP címét hoszt névre. Amikor a kliens címe változik, a DHCP automatikusan elküldhet egy frissítést a DNS szervernek, így a hálózat többi gazdagépe meg tudja találni a klienst az új IP címen is a DNS lekérdezésen keresztül. 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-t úgy állítja be, hogy csak a PTR rekordokat frissítse, akkor úgy kell konfigurálni a DNS-t, hogy az megengedje a kliensektől jövő frissítéseket, s így a kliensek frissíteni tudják az A rekordokat. Nem minden DHCP kliens támogatja a saját A rekord frissítési kéréseket. 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 (*Transaction Signature* vagy TSIG), vagy ezen módszerek valamilyen kombinációjával. A DNS ellenőrzi, hogy a bejövő kérés csomagjai felhatalmazott forrástól jönnek-e, mielőtt frissítené az erőforrás rekordokat.

A dinamikus frissítés végrehajtható DNS és DHCP között egyetlen iSeries szerveren, különböző iSeries szerverek között, valamint egy iSeries és más egyéb szerverek között, amelyek képesek a dinamikus frissítésre.

Megjegyzés: A szervereken a dinamikus frissítés megköveteli a QTOBUPT nevű alkalmazásprogramozási csatolót (API), amely elküldi a dinamikus frissítést a DNS számára. Az i5/OS Option 31, DNS rendszerprogram telepítéskor automatikusan telepítésre kerül az API is.

Kapcsolódó fogalmak

Dynamic Host Configuration Protocol (DHCP)

Kapcsolódó feladatok

“Domain Name System konfigurálása dinamikus frissítések fogadásához” oldalszám: 25

A BIND 8-at futtató Domain Name System (DNS) konfigurálható úgy, hogy elfogadjon kéréseket más forrásoktól a zóna adatok dinamikus frissítésére. Ez a témakör az engedélyezés-frissítés opció konfigurálására vonatkozó utasításokat tartalmazza, amelynek révén a DNS fogadni tudja a dinamikus frissítéseket.

A DHCP konfigurálása dinamikus frissítések küldéséhez

Kapcsolódó hivatkozás

“Példa: Domain Name System és Dynamic Host Configuration Protocol ugyanazon az iSeries szerveren” oldalszám: 16

A példa arra mutat be megoldást, amikor a Domain Name System (DNS) és a Dynamic Host Configuration Protocol (DHCP) ugyanazon a szerveren van.

“DNS erőforrás rekordok” oldalszám: 8

Ez a témakör ismerteti, hogyan használja fel a DNS az erőforrás rekordokat. Az erőforrás rekordok a tartománynevek és az IP címek adatainak tárolására szolgálnak. Ez a témakör az OS/400 V5R1 változatban elérhető erőforrás rekordok kereshető listáját tartalmazza.

QTOBUPT

“BIND 8 jellemzők”

A dinamikus frissítésen túl a BIND 8 is ajánl néhány funkciót a DNS szerver teljesítményének javítására.

BIND 8 jellemzők

A dinamikus frissítésen túl a BIND 8 is ajánl néhány funkciót a DNS szerver teljesítményének javítására.

A DNS át lett tervezve a BIND 8 használata érdekében az OS/400 V5R1 változatban. Ha nem rendelkezik telepített PASE programmal, folytassa a konfigurálást és futtassa az előző változat BIND 4.9.3 alapú OS/400 DNS szerverét. A DNS rendszer követelmények című témakör elmagyarázza, hogy mi szükséges a BIND 8 alapú DNS futtatásához az iSeries szerveren. Az új DNS használata lehetővé teszi a következő funkciók előnyeinek kihasználását:

Több DNS szerver futhat egyetlen iSeries rendszeren

A korábbi változatokban csak egy DNS szervert lehetett konfigurálni. Most több DNS szervert vagy példányt konfigurálhat. Ez lehetővé teszi a logikai megosztást a szerverek között. Amikor több példányt hoz létre, mindegyiknek kifejezetten meg kell adni a figyelő interfész IP címet. Két DNS példány nem figyelheti ugyanazt az interfészt.

A több szerver egyik praktikus alkalmazási módja a DNS felosztása, ahol az egyik szerver jogosult a belső hálózatra, míg a második szerver a külső lekérdezések kezelésére.

Feltételes továbbítás

A feltételes továbbítás lehetővé teszi a DNS szerver konfigurálását, hogy a továbbítási beállításokat pontosabban behangolja. Beállíthatja a szervert úgy, hogy minden olyan lekérdezést továbbítson, amelyekre nem tudja a választ. A továbbítást beállíthatja globális szinten is, de adhat kivételeket is a tartományokhoz, amelyekre a szokásos iterációs felbontást kívánja rákényszeríteni. Vagy beállíthatja a szokásos iterációs felbontást globális szinten, és azután erőlteti rá néhány tartományra a továbbítást.

Biztonságos dinamikus frissítések

A DHCP és az egyéb felhatalmazott források elküldhetik dinamikus erőforrás rekord frissítéseiket a Transaction Signatures (TSIG) és/vagy a forrás IP cím jogosultság alapján. Ez csökkenti a zóna adatok kézi frissítését, miközben bizonyos lehet benne, hogy csak a felhatalmazott források lesznek felhasználva a frissítéshez.

NOTIFY funkció

Amikor a NOTIFY be van kapcsolva, a DNS NOTIFY funkció aktivizálódik valahányszor frissülnek a zóna adatok az elsődleges szerverben. Az elsődleges szerver kiküld minden ismert másodlagos szervernek egy üzenetet, amelyben jelzi az adatok módosulását. A másodlagos szerverek erre egy zóna átviteli kérelemmel válaszolhatnak a frissített zóna adatok lekérése érdekében. Ez javítja a másodlagos szerver szolgáltatásait, hiszen így a tartalék zóna adatok aktuálisak maradnak.

Zóna átvitelek (IXFR és AXFR)

Korábban valahányszor a másodlagos szervernek be kellett tölteni a zóna adatokat, mindig az összes adatot kellett betölteni az Összes zóna átvitel (AXFR) keretében. A BIND 8 támogatja az új zóna átviteli módszert: növekményes zóna átvitel (IXFR). Az IXFR olyan módszer, amelynek révén a többi szervernek csak a változott adatokat kell elküldeni a teljes zóna helyett.

Amikor ezt engedélyezi az elsődleges szerveren, az adatváltozásokhoz hozzá lesz rendelve egy jelző, amely a változás tényét rögzíti. Amikor a másodlagos szerver kéri a zóna adatok frissítését egy IXFR formájában, az elsődleges szerver csak az új adatokat fogja elküldeni. Az IXFR különösen akkor hasznos, amikor a zóna dinamikusan frissül. Ez a fajta átvitel a kevesebb adatmennyiség elküldésével csökkenti a forgalmi terhelést.

Megjegyzés: Az elsődleges és a másodlagos szervernek is IXFR képességűnek kell lenni a funkció használhatósága érdekében.

Kapcsolódó fogalmak

“Domain Name System követelmények” oldalszám: 22

Ez a témakör ismerteti a DNS szerver futtatásának szoftverkövetelményeit az iSeries szerver esetében.

“Dinamikus frissítések” oldalszám: 5

A BIND 8-ra épülő OS/400 V5R1 DNS támogatja a dinamikus frissítéseket. Ez lehetővé teszi a külső forrásoknak, mint például a DHCP-nek, hogy frissítéseket küldjön a DNS szervernek.

Kapcsolódó hivatkozás

“Példa: Domain Name System felosztása tűzfalon keresztül” oldalszám: 18

Ez a példa tűzfalon keresztüli DNS működést ábrázol, amely révén a belső adatok megvédhetők az Internettől, miközben a belső felhasználóknak lehetővé teszi az adatok elérését az Interneten.

“Biztonsági intézkedések tervezése” oldalszám: 21

A Domain Name System (DNS) védelmi beállításokat biztosít a szerver külső hozzáféréseinek korlátozására.

DNS erőforrás rekordok

Ez a témakör ismerteti, hogyan használja fel a DNS az erőforrás rekordokat. Az erőforrás rekordok a tartománynevek és az IP címek adatainak tárolására szolgálnak. Ez a témakör az OS/400 V5R1 változatban elérhető erőforrás rekordok kereshető listáját tartalmazza.

A DNS zóna adatbázis erőforrás rekordok gyűjteményéből áll. Minden egyes erőforrás rekord egy adott objektum adatait adja meg. Például, a cím kiosztási (A) rekordok egy hosztnévet 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 erőforrás rekordokat a táblázatban.

1. táblázat: Erőforrás rekord kereső tábla

Erőforrás rekord	Rövidítés	Leírás
Cím leképezési rekordok	A	Az A rekord megadja az adott hoszt IP címét. A rekordok egy adott tartománynev 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 tartománynev AFSDB cím leképezésére, vagy a cella tartománynevének hitelesített névszerverekre való leképezésére szolgál. A rekord típusát RFC 1183 határozza meg.
Általános névrekordok	CNAME	A CNAME rekord az objektum tényleges tartománynevét adja meg. Amikor a DNS fedőnévre keres, és egy általános névre mutató CNAME rekordot talál, akkor lekérdezi az általános név tartománynevét is. A rekord típusát RFC 1035 határozza meg.
Hoszt információs rekordok	HINFO	A HINFO rekord megadja az általános információkat a hoszt berendezésről. 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 hosztnévet ISDN címre. Csak ISDN hálózatokban használatos. A rekord típusát RFC 1183 határozza meg.

1. táblázat: Erőforrás rekord kereső tábla (Folytatás)

Erőforrás rekord	Rövidítés	Leírás
IP Verzió 6 cím rekordok	AAAA	Az AAAA rekord megadja az adott hoszt 128 bites címét. Az AAA rekord az A rekordhoz hasonlóan leképezi a gép nevét IP címre. Az AAAA rekordokkal támogathatja a 6-os verziójú IP címeket, amelyekhez nem elegendő a szabványos A rekord formátum. A rekord típusát 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.
Levélkezelő 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.
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.

1. táblázat: Erőforrás rekord kereső tábla (Folytatás)

Erőforrás rekord	Rövidítés	Leírás
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 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.
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 iSeries DHCP használja dinamikus frissítés céljából. A DHCP szerver beír egy TXT rekordot minden PTR és A rekord frissítéshez, amelyet a DHCP szerver végez el. A DHCP rekordok AS400 DHCP 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.

1. táblázat: Erőforrás rekord kereső tábla (Folytatás)

Erőforrás rekord	Rövidítés	Leírás
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

“Dinamikus frissítések” oldalszám: 5

A BIND 8-ra épülő OS/400 V5R1 DNS támogatja a dinamikus frissítéseket. Ez lehetővé teszi a külső forrásoknak, mint például a DHCP-nek, hogy frissítéseket küldjön a DNS szervernek.

“Posta és MX rekordok”

A Domain Name System (DNS) támogatja a fejlett levéltovábbítást a posta és MX rekordok használata révén.

Kapcsolódó hivatkozás

“Példa: Egy Domain Name System szerver az intranet számára” oldalszám: 12

A példa egyszerű alhálózatot mutat DNS szerverrel belső használatra.

“A zónák alapjai” oldalszám: 2

A témakör ismerteti a Domain Name System (DNS) zónákat és zónatípusokat.

Posta és MX rekordok

A Domain Name System (DNS) támogatja a fejlett levéltovábbítást a posta és 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 kereső táblázat olyan típusú rekordokat tartalmaz, amelyeket támogat az iSeries DNS.

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 gazdagépnek 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 erőforrás rekordokat használnak, amelyek *levélkezelő* (MX) rekordokként ismertek. Az MX rekordok a tartomány- vagy hoszt nevet leképezik egy előszeretettel használt értékre és hoszt névre. Az MX rekordok általában annak a hosztnak a kijelölésére használatosak, amely postai feldolgozást végez másik gazdagép számára. A rekordok másik hoszt (ahová a postát megpróbálja továbbítani) kijelölésére is szolgálnak, ha az első gazdagép nem elérhető. Másrészt a rekordok lehetővé teszik, hogy az egyik gazdagéphez címzett postát egy másik gazdagéphez lehessen továbbítani.

Több MX erőforrás rekord is létezhet ugyanarra a tartományra vagy hoszt névre. Amikor több MX rekord létezik ugyanarra a tartományra vagy gazdagépre, 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 gazdagép nem elérhető, akkor a küldő postai alkalmazás megpróbálja felvenni a kapcsolatot a következő, kevésbé kedvelt MX gazdagéppel. A tartomány adminisztrátor, vagy az MX rekord létrehozója állítja be a kedvelt értéket.

A DNS szerver válaszolhat üres MX erőforrás rekord 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 gazdagéppel.

Megjegyzés: Helyettesítő karakteres (például: *.mycompany.com) MX rekordok használata nem ajánlott a tartomány számára.

Példa: MX rekord gazdagép számára

A következő példában a rendszer - a kedvelt értékkel - továbbítja a postát az fsc5.test.ibm.com címre, magához a gazdagéphez. Ha a gazdagép 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 erőforrás rekordok” oldalszám: 8

Ez a témakör ismerteti, hogyan használja fel a DNS az erőforrás rekordokat. Az erőforrás rekordok a tartománynevek és az IP címek adatainak tárolására szolgálnak. Ez a témakör az OS/400 V5R1 változatban elérhető erőforrás rekordok kereshető listáját tartalmazza.

Domain Name System példák

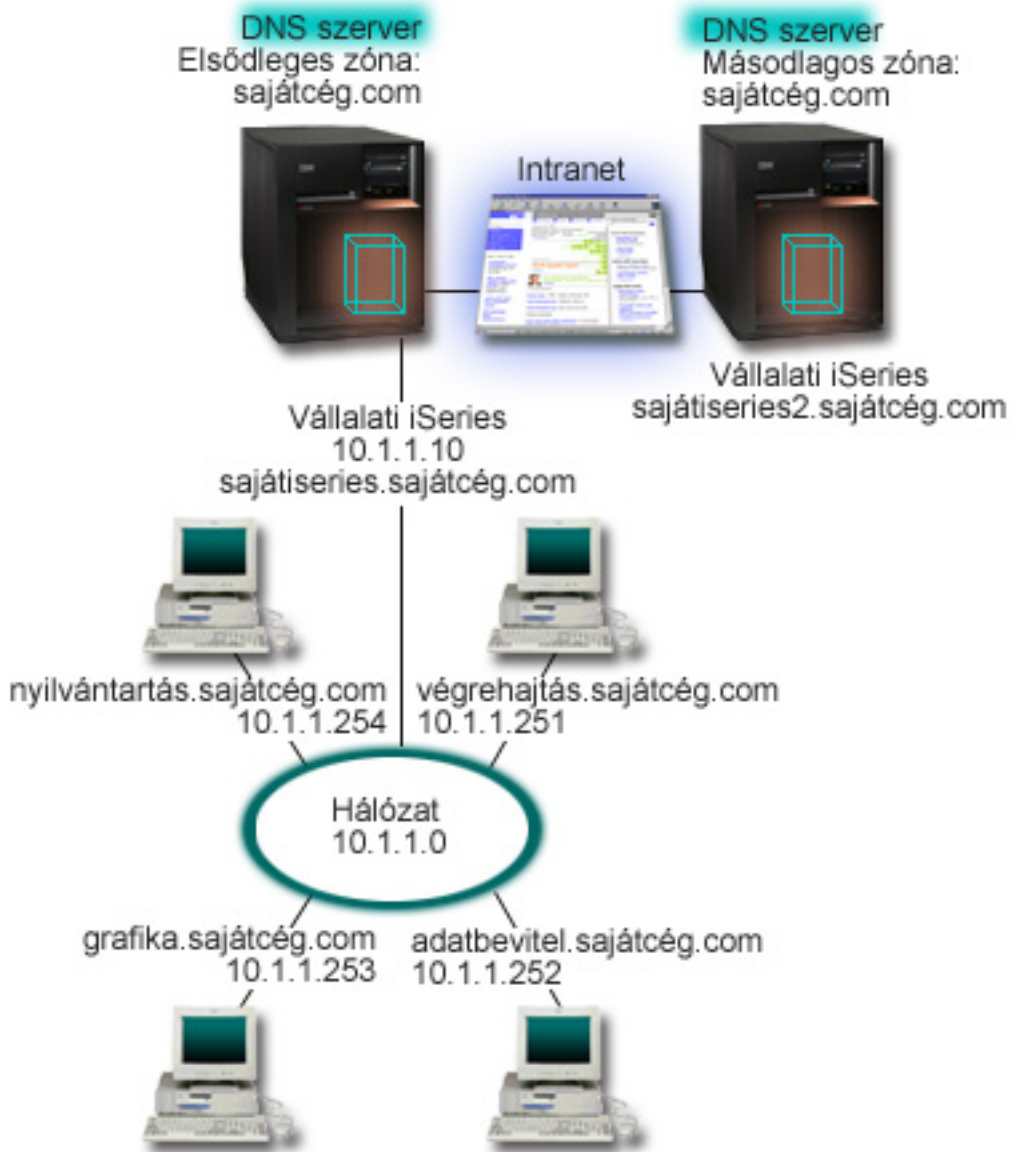
A példák révén megismerheti a Domain Name System (DNS) használatát a hálózaton.

A DNS egy osztott adatbázis rendszer, amely a hoszt (gazdagép) nevek 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: Egy Domain Name System szerver az intranet számára

A példa egyszerű alhálózatot mutat DNS szerverrel belső használatra.

A következő ábra az iSeries rendszeren futó DNS szerveret szemlélteti, amely a belső hálózatot szolgálja ki. Ez a DNS szerver példány úgy van beállítva, hogy az összes IP cím lekérdezését figyeli. A szerver a "sajátcég.com" zóna elsődleges névszervere.



2. ábra: Egy DNS szerver az intranet számára

A zónában lévő összes gazdagép rendelkezik IP címmel és tartománynévvel. A DNS zóna adatokban lévő gazdagépeket a rendszergazdának manuálisan kell megadnia úgynevezett erőforrás rekordok létrehozásával. A cím kiosztó (A) rekordok leképezik a gép nevét a hozzátartozó IP címre. Ez lehetővé teszi a hálózaton lévő többi hoszt számára, hogy lekérdezve a DNS szerveret megtalálja egy adott hosztnévhez a neki megfelelő IP címet. A fordított leképezési mutató (PTR) rekordok leképezik az IP címet a hozzátartozó névre. Ez lehetővé teszi a hálózaton lévő többi hoszt számára, hogy lekérdezve a DNS szerveret megtalálja egy adott IP címhez a neki megfelelő hoszt nevet.

Az A és a PTR rekordokon túlmenően a DNS számos egyéb erőforrás rekordot is támogat, amelyekre szükség lehet attól függően, hogy milyen egyéb TCP/IP alapú alkalmazásokat futtat az intraneten. Például, ha belső elektronikus levelező rendszert futtat, esetleg hozzáadhatja a levélkezelő (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 második példában a saját iseries szerver az intranet része. A másik iSeries szerver (sajátiseries2) a beállítás alapján a saját cég.com zóna másodlagos DNS szervereként szerepel. 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 erőforrás rekordok” oldalszám: 8

Ez a témakör ismerteti, hogyan használja fel a DNS az erőforrás rekordokat. Az erőforrás rekordok a tartománynevek és az IP címek adatainak tárolására szolgálnak. Ez a témakör az OS/400 V5R1 változatban elérhető erőforrás rekordok kereshető listáját tartalmazza.

“A zónák alapjai” oldalszám: 2

A témakör ismerteti a Domain Name System (DNS) zónákat és zónatípusokat.

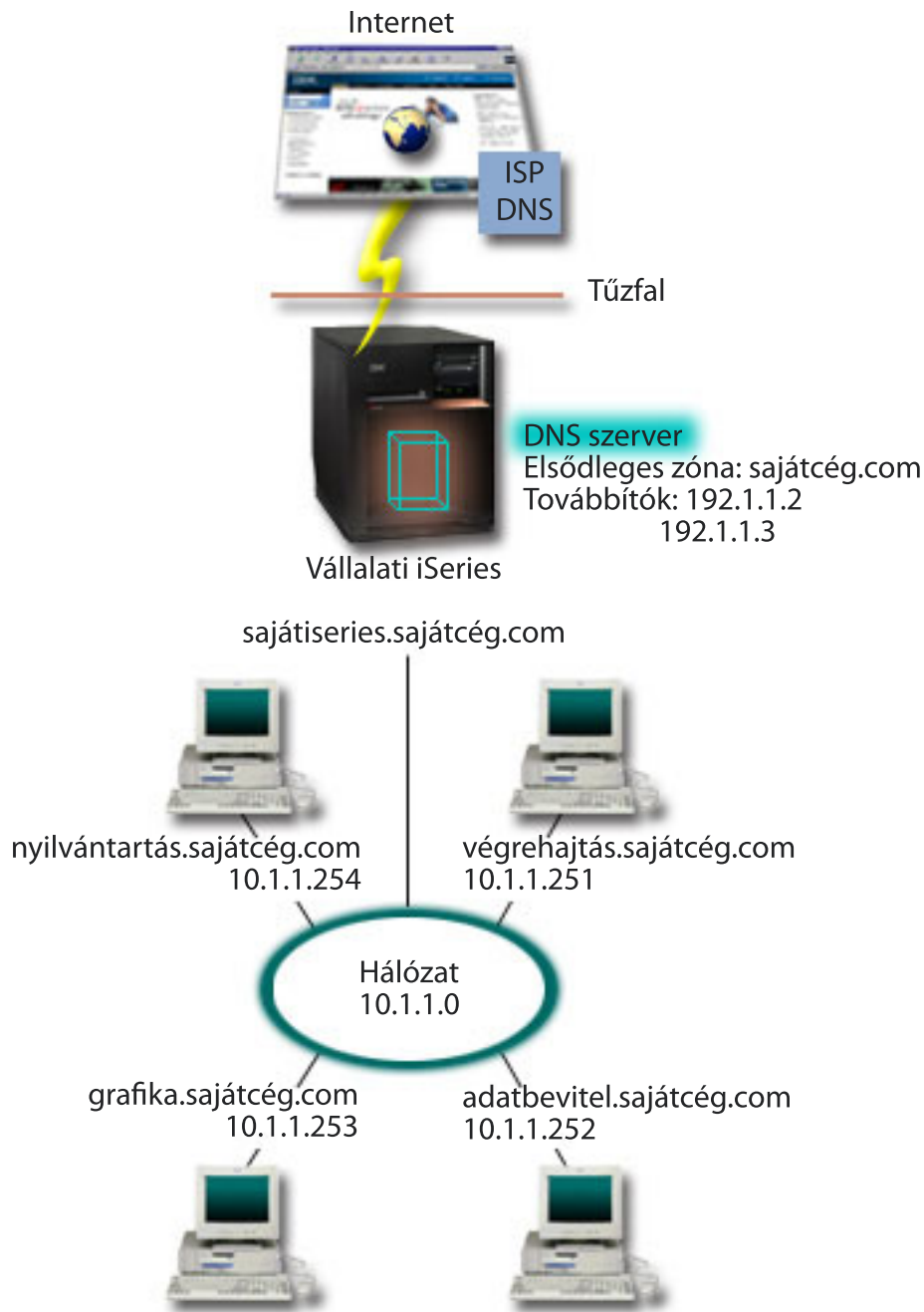
“Példa: Egy Domain Name System szerver Internet hozzáféréssel”

A példa egyszerű alhálózatot mutat Domain Name System (DNS) szerverrel, közvetlen Internet kapcsolattal.

Példa: Egy Domain Name System szerver Internet hozzáféréssel

A példa egyszerű alhálózatot mutat Domain Name System (DNS) szerverrel, közvetlen Internet kapcsolattal.

A következő szemléltető ábra az Egy DNS szerver az intranet számára című példában már megismert hálózatot mutatja, de most a cég Internet kapcsolattal bővítette a rendszert. 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 lekérdezéséhez olvassa el a megfelelő részt ("Külső DNS adatok elérése" oldalszám: 26).

- Továbbítás engedélyezése

Beállíthatja a továbbítást, amelynek hatására a sajátcég.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 forward (továbbítás)

opciót **first (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, hogy a DNS közvetlenül kapcsolódjon az Internethez. Az iSeries szerver biztonsága érdekében konfigurálja a tűzfalat, vagy egyéb óvőrendszerrel vezessen be.

Kapcsolódó fogalmak

"Domain Name System tartomány beállítás" oldalszám: 5

A témakör áttekintést nyújt a tartomány regisztrációjáról, valamint hivatkozásokat más helyekre a saját tartományterület beállításához.

iSeries és Internet biztonság

"Domain Name System lekérdezések alapjai" oldalszám: 3

A témakör elmagyarázza, hogyan oldja fel a Domain Name System (DNS) a kliensek lekérdezéseit.

Kapcsolódó hivatkozás

"Példa: Egy Domain Name System szerver az intranet számára" oldalszám: 12

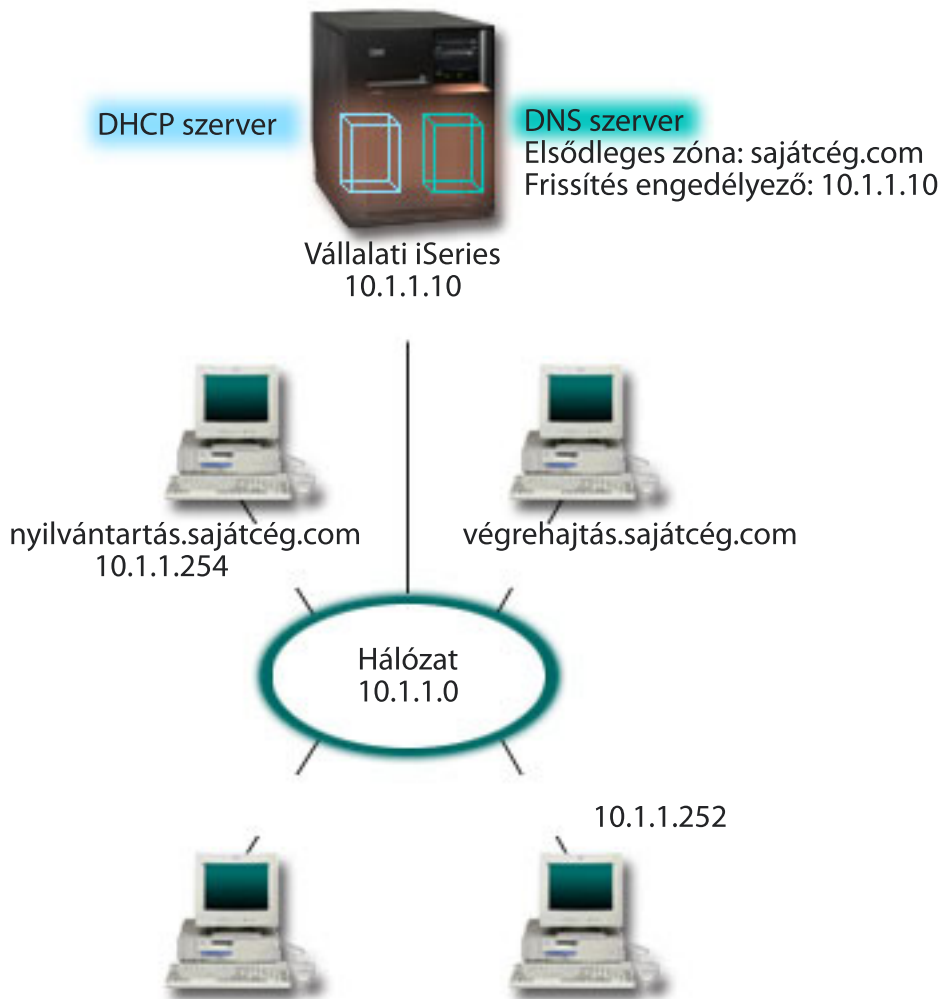
A példa egyszerű alhálózatot mutat DNS szerverrel belső használatra.

Példa: Domain Name System és Dynamic Host Configuration Protocol ugyanazon az iSeries szerveren

A példa arra mutat be megoldást, amikor a Domain Name System (DNS) és a Dynamic Host Configuration Protocol (DHCP) ugyanazon a szerveren van.

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

A következő ábra egy kis hálózatrészt mutat be egyetlen iSeries szerverrel, amely DHCP és DNS szerverként szerepel négy kliens számára. Ebben a működési környezetben tételezzük fel, hogy a leltár, az adatbevitel és a végrehajtó kliensek grafikát tartalmazó dokumentumokat készítene a grafikus fájlserverről. A grafikus fájlserver a hálózati meghajtóhoz történő csatlakozás révén éri el a hosztnév segítségével.



4. ábra: DNS és DHCP ugyanazon az iSeries szerveren

A DHCP és a DNS előző változatai függetlenek egymástól. Ha a DHCP hozzárendelt egy új IP címet egy klienshez, a DNS rekordokat a rendszergazdának 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 8 alapú OS/400 V5R1 DNS szervernél konfigurálhatja úgy a DNS zónát, hogy elfogadja a DNS rekordok dinamikusan frissítését, párosítva a DHCP révén megvalósuló címváltoztatásokkal. Például, amikor a grafikus fájlserver megújítja a címét a DHCP szerver által adott 10.1.1.250 IP címmel, a hozzá tartozó DNS rekordok dinamikusan frissítésre kerülnek. Ez lehetővé teszi a többi kliensnek, hogy megszakítás nélkül lekérdezze a grafikus fájlserveret a hoszt neve alapján a frissített DNS szerveren keresztül.

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

- A dinamikusan zóna azonosítása

A dinamikusan zónát nem tudja manuálisan frissíteni a szerver futása közben. Ha így tenné, ütközést okozhatna a bejövő dinamikusan frissítésekkel. A manuális frissítéseket akkor végezheti el, amikor a szerver áll, viszont a szerver leállása alatt érkező dinamikusan frissítéseket elveszti. Éppen ezért, szándékában állhat, hogy egy különálló dinamikusan zónát konfigurál a manuális frissítések iránti igény minimalizálása érdekében. A dinamikusan frissítési funkcióhoz használt zónák konfigurálásáról további tájékoztatást találhat itt: "Tartomány struktúra meghatározása" oldalszám: 20.

- Az allow-update opció konfigurálása

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

- A DHCP konfigurálása dinamikus frissítések küldéséhez

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

- Másodlagos szerver frissítési kedvezmények beállítása

A másodlagos szerver aktuális szinten tartásához konfigurálja a DNS szerveret a NOTIFY használatára, amely így üzenetet küld a sajtócég.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

“Dinamikus frissítések” oldalszám: 5

A BIND 8-ra épülő OS/400 V5R1 DNS támogatja a dinamikus frissítéseket. Ez lehetővé teszi a külső forrásoknak, mint például a DHCP-nek, hogy frissítéseket küldjön a DNS szervernek.

“Tartomány struktúra meghatározása” oldalszám: 20

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

Kapcsolódó feladatok

A DHCP konfigurálása dinamikus frissítések küldéséhez

Kapcsolódó hivatkozás

Példa: DNS és DHCP különböző iSeries szervereken

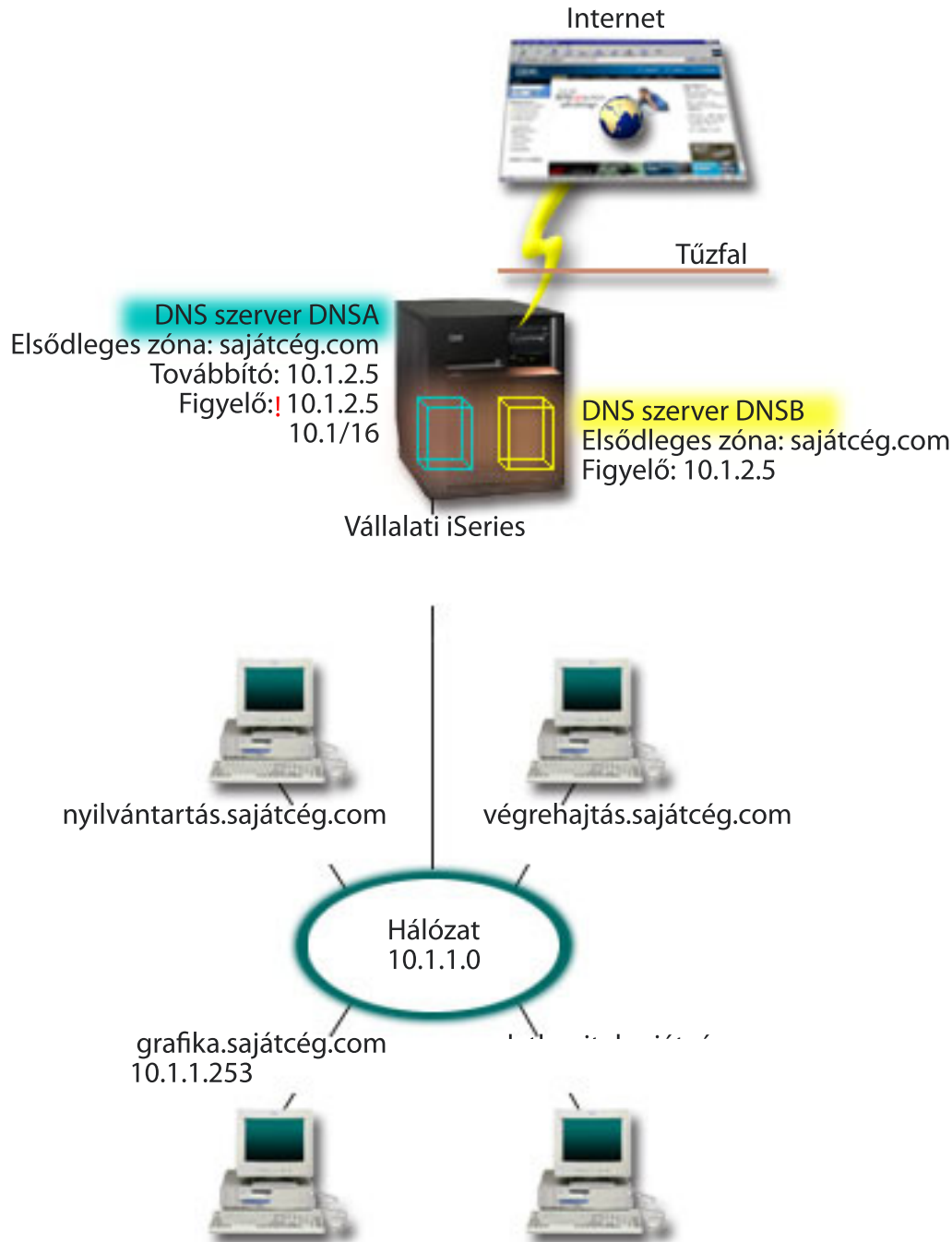
Példa: Domain Name System felosztása tűzfalon keresztül

Ez a példa tűzfalon keresztüli DNS működést ábrázol, amely révén a belső adatok megvédhetők az Internettől, miközben a belső felhasználóknak lehetővé teszi az adatok elérését az Interneten.

A következő illusztráció egy egyszerű alhálózatból álló hálózatot mutat be, amely tűzfalat használ védelmi célokból. A BIND 8 alapú OS/400 V5R1 DNS lehetővé teszi több DNS szerver kialakítását egyetlen iSeries szerveren. Tétélezzük fel, hogy a vállalat rendelkezik a hálózat egy belső, lefoglalt IP címtérületű részével, valamint a hálózat egy külső részével is, amely elérhető a nyilvánosság számára.

A vállalat azt szeretné, hogy a belső felhasználók képesek legyenek feloldani a külső hoszt (gazdagép) neveket, és külső emberekkel levelezést folytatni. A vállalat azt is szeretné, hogy a belső feloldók (resolvers) 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.

Az igények teljesítése érdekében a vállalat két DNS szerver példányt állított be ugyanazon az iSeries szerveren, egyet az intranet, míg egy másikat a nyilvános tartomány számára. Ezt hívják a *DNS felosztásának*.



5. ábra: DNS felosztása tűzfalon keresztül

A DNSB külső szerver konfigurálása a sajátcég.com elsődleges zónával történik. Ez a zóna adat csak azokat az erőforrás rekordokat foglalja magában, amelyek a nyilvános tartomány részeként szolgálnak. A belső szerver (DNSA) a sajátcég.com elsődleges zónával lesz konfigurálva, de a DNSA-ban megadott zóna adatok tartalmaznak intranet erőforrás rekordokat is. A továbbító opció 10.1.2.5 címként 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 sajátcég.com zónára vonatkozó lekérdezéseket engedélyezi a belső gazdagépektől. Ahhoz, hogy mindez megfelelően

működjön, a belső klienseket úgy kell konfigurálni, hogy lekérdezéseik a DNSA szerverre vonatkozzanak. A DNS felosztásához a következő konfigurálási beállítások szükségesek:

- **Figyelő**

Az előző példákban csak egy DNS szerver van az iSeries rendszeren. A beállítás szerint az összes interfész IP címet figyelni. Valahányszor több DNS szerver van az iSeries szerveren, meg kell határozni azokat az IP címeteket, amelyeket az egyes szerverek figyelnek. Két DNS szerver nem figyelheti ugyanazt a címet. Ebben az esetben tételezzük fel, hogy a tűzfal felől belépő 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 interfész IP címek felől jövő lekérdezéseket fogadja, *kivéve* a 10.1.2.5 címet. Ennek a címnek a hatékony kihagyására a Címegezési lista (AML) szolgál, ahol először a kirekesztett címet kell felsorolni a bennfoglalt címek előtt.

- **A címegezési lista sorrendje**

Az AML listában az első címegezés lesz használva. 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 lenne összehasonlítva, és azonnal visszautasításra kerülne.

Ha az elemek sorrendje fordított (10.1/16; !10.1.2.5), akkor a 10.1.2.5 IP cím hozzáférése megengedett lenne, mivel a szerver az első elemmel hasonlítaná össze, ami egyezést adna, s így engedélyezné a hozzáférést a többi szabály ellenőrzése nélkül.

Kapcsolódó hivatkozás

“BIND 8 jellemzők” oldalszám: 6

A dinamikus frissítésen túl a BIND 8 is ajánl néhány funkciót a DNS szerver teljesítményének javítására.

Domain Name System tervezése

A Domain Name System (DNS) számtalan megoldást kínál. Mielőtt konfigurálná a DNS szerveret, fontos, hogy megtervezze a hálózaton belüli működését. A DNS megvalósítása előtt becsülje meg az olyan dolgokat, mint például a hálózat szerkezetét, a teljesítményt és a biztonságot.

Domain Name System jogosultságok meghatározása

A Domain Name System (DNS) rendszergazdának 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.

Egy minimális szintű jogosultság kell ahhoz, hogy megengedje a rendszergazdának a DNS konfigurálását és adminisztrálását az iSeries rendszeren. 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 adminisztratori hozzáféréssel és összes objektum (*ALLOBJ) jogosultsággal rendelkezzenek. A jogosultságot az iSeries navigátor segítségével adhatja meg a felhasználóknak. Ha további információkra van szüksége, olvassa el a DNS online segítség Jogosultság adományozása a DNS rendszergazdának című témakörét.

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

Kapcsolódó hivatkozás

“DNS konfigurációs fájlok karbantartása” oldalszám: 29

A témakör segítségével megismerheti a Domain Name System (DNS) által használt fájlokat, és áttekintheti a mentésükre és karbantartásukra vonatkozó irányelveket.

Tartomány struktúra 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 Domain Name System (DNS) zónát dinamikus zónaként konfigurálja, akkor manuálisan nem változtathatja meg a zóna adatokat a szerver futása alatt. Ha így tenne, 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 dinamikusan lesznek karbantartva.

Az iSeries DNS grafikus kezelőfelület biztosít a szerverek konfigurálásához. Néhány esetben a kezelőfelület olyan szakkifejezéseket vagy koncepciókat használ, amelyek eltérnek a más forrásokban használtaktól. Ha a DNS konfiguráció tervezésekor más információs forrásokra hivatkozik, hasznos lehet a következőkre emlékezni:

- A szerveren megadott összes zóna és objektum az **Egyenes kikeresési zóna** és a **Fordított kikeresési zóna** mappába lesz szervezve. Az Egyenes kikeresési zónák azok a zónák, amelyek a tartománynevek IP címekké történő leképezésére szolgálnak, mint például az A rekordok. A Fordított kikeresési zónák azok a zónák, amelyek az IP címek tartománynevekre történő leképezésére szolgálnak, mint például a PTR rekordok.
- Az iSeries DNS az *elsődleges zóna* és a *másodlagos zóna* elnevezést használja.
- A kezelőfelület az *alzóna* elnevezést használja, míg egyes források *altartományként* emlegetik. Az utód zóna egy alzóna, amelyre vonatkozóan a felelősséget egy vagy több névszerverre áthárítja.

Kapcsolódó hivatkozás

“Példa: Domain Name System és Dynamic Host Configuration Protocol ugyanazon az iSeries szerveren”
oldalszám: 16

A példa arra mutat be megoldást, amikor a Domain Name System (DNS) és a Dynamic Host Configuration Protocol (DHCP) ugyanazon a szerveren van.

Biztonsági intézkedések tervezése

A Domain Name System (DNS) védelmi beállításokat biztosít a szerver külső hozzáféréseinek korlátozására.

A DNS szerver biztonsága létfontosságú. Az alábbi biztonsági szempontokon túlmenően a DNS és az iSeries biztonságáról számtalan forrásból értesülhet, beleértve az Információs központ iSeries és Internet című cikkét is. A DNS és BIND könyv ugyancsak tárgyalja a DNS biztonsági kérdéseit.

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 Transaction Signature (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 vezérlési listaként (ACL). Azután valahányszor szükség van egy listára, behívja az ACL-t, és az egész lista betöltődik.

Címegezési lista elemeinek sorrendje

A címegezési lista első eleme, amely megegyezik a megadott címmel, lesz használva. Például, az összes cím engedélyezéséhez a 10.1.1.x hálózaton, kivéve a 10.1.1.5 címet, a címegezési lista elemeinek (!10.1.1.5; 10.1.1/24) sorrendben kell lenniük. Ebben az esetben a 10.1.1.5 cím az első elemmel lenne összehasonlítva, és azonnal visszautasításra kerülne.

Ha az elemek sorrendje fordított (10.1.1/24; !10.1.1.5), akkor a 10.1.1.5 IP cím hozzáférése megengedett lenne, mivel a szerver az első elemmel hasonlítaná össze, ami egyezést adna, s így engedélyezné a hozzáférést a többi szabály ellenőrzése nélkül.

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 (gazdagép) lekérdezése engedélyezve van.

allow-transfer

Megadhatja, hogy mely hosztok fogadhatnak zóna átvitelt ettől a szervertől. Ha nem definiálja, akkor alapértelmezés szerint az összes hoszt (gazdagép) 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 (gazdagép) 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.

Kapcsolódó fogalmak

iSeries és Internet biztonság

Kapcsolódó hivatkozás

“BIND 8 jellemzők” oldalszám: 6

A dinamikus frissítésen túl a BIND 8 is ajánl néhány funkciót a DNS szerver teljesítményének javítására.

Domain Name System követelmények

Ez a témakör ismerteti a DNS szerver futtatásának szoftverkövetelményeit az iSeries szerver esetében.

A DNS komponens (31-es opció) nem kerül automatikusan telepítésre az alap operációs rendszerrel. A DNS opciót kimondottan ki kell választani a telepítéshez. Az OS/400 V5R1 változatban lévő új DNS szerver a BIND 8 néven ismert ipari szabványon alapuló DNS megvalósítás. Az előző OS/400 DNS szolgáltatások a BIND 4.9.3 szabványon alapultak, és még rendelkezésre állnak az OS/400 V5R1 változatban is.

A DNS telepítése után alapértelmezés szerint egy DNS szerver konfigurálódik, amely BIND 4.9.3 alapú DNS szerver képességekkel rendelkezik, ami az előző változatokban rendelkezésre állt. Ha egy vagy több, BIND 8 alapú DNS szervert kíván futtatni, akkor telepítenie kell a PASE programot. A PASE az SS1 rendszerprogram 33-as opciója. A PASE program telepítése után az iSeries navigátor automatikusan kezeli a helyes BIND konfigurálást.

Ha nem használ PASE programot, akkor nem tudja kihasználni a BIND 8 funkció összes előnyét. Ha nem használja a PASE programot, akkor még futtatni tudja ugyanazt a DNS szerveret ugyan, amely azonban az előző változatokban rendelkezésre álló BIND 4.9.3-ra épül. A BIND 4.9.3 dokumentációját a V4R5 Információs központban találja meg.

Ha a DHCP szervert egy másik iSeries rendszeren kívánja konfigurálni, hogy frissítéseket küldjön a DNS szervernek, akkor a 31-es opciót is telepíteni kell a DHCP iSeries rendszeren. A Dynamic Host Configuration Protocol (DHCP) szerver a 31-es opció által nyújtott programozási kezelőfelületet használja a dinamikus frissítések végrehajtásához.

Kapcsolódó fogalmak

Portable Application Solutions Environment (PASE)

“Domain Name System konfigurálása”

Ez a témakör elmagyarázza, hogyan konfigurálja a névszervereket, valamint a tartományon kívül eső lekérdezések feloldását az iSeries navigátor segítségével.

Kapcsolódó hivatkozás

“BIND 8 jellemzők” oldalszám: 6

A dinamikus frissítésen túl a BIND 8 is ajánl néhány funkciót a DNS szerver teljesítményének javítására.

Kapcsolódó tájékoztatás

V4R5 DNS Információs központbeli témakör

Domain Name System telepítésének ellenőrzése

Annak meghatározásához, hogy a DNS telepítve van-e, kövesse ezeket a lépéseket:

1. A parancssorba gépelje be a GO LICPGM parancsot, és nyomja meg az Enter billentyűt.
2. Írjon be 10-et (Display installed licensed programs), és nyomja meg az Enter billentyűt.
3. Lapozzon le az **5722SS1 - Domain Name System** (SS1 Option 31) sorig. Ha a DNS telepítése sikeresen megtörtént, az Installed Status oszlopban *compatible kijelzés jelenik meg, ahogy alább látható:

LicPgm	Installed Status	Description
5722SS1	*COMPATIBLE	Domain Name System

4. Nyomja meg az F3 billentyűt a kilépéshez.

Domain Name System telepítése

A DNS telepítéséhez kövesse ezeket a lépéseket:

1. A parancssorba gépelje be a GO LICPGM parancsot, és nyomja meg az Enter billentyűt.
2. Írjon be 11-et (Install licensed programs), és nyomja meg az Enter billentyűt.
3. Gépeljen be 1-et (Install) az **Option** mezőbe az OS/400 - Domain Name System mellé, és nyomja meg az Enter billentyűt.
4. Nyomja meg ismét az Enter billentyűt a telepítés jóváhagyásához.

Domain Name System konfigurálása

Ez a témakör elmagyarázza, hogyan konfigurálja a névszervereket, valamint a tartományon kívül eső lekérdezések feloldását az iSeries navigátor segítségével.

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

Kapcsolódó fogalmak

“Domain Name System követelmények” oldalszám: 22

Ez a témakör ismerteti a DNS szerver futtatásának szoftverkövetelményeit az iSeries szerver esetében.

Domain Name System elérése az iSeries navigátorban

A témakör segítségével tanulmányozhatja a Domain Name System (DNS) elérését iSeries navigátorból.

A következő utasítások elvezetik az iSeries navigátor DNS konfiguráló kezelőfelületéhez. Ha PASE opciót használ, konfigurálni tudja a BIND 8 alapú DNS szervereket. Ha nem használja a PASE programot, akkor még futtatni tudja ugyanazt a DNS szerveret ugyan, amely azonban az előző változatokban rendelkezésre álló BIND 4.9.3-re épül. A BIND 4.9.3 alapú DNS-ről a V4R5 Információs központ DNS témakörében olvashat.

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

1. Az iSeries navigátorban bontsa ki az **iSeries szerver** → **Hálózat** → **Szerverek** → **DNS** elemeket.
2. Kattintson a jobb egérgombbal a **DNS** elemre, és válassza ki az **Új konfigurációt**.

Kapcsolódó fogalmak

iSeries navigátor

Névszerverek konfigurálása

A Domain Name System (DNS) lehetővé teszi több névszerver példány létrehozását. Ez a témakör a névszerver konfigurálására vonatkozó utasításokat tartalmazza.

A BIND 8-ra épülő iSeries DNS támogatja, hogy a névszerverből több példány legyen. Az alábbi feladatok végigvezetik egy névszerver példány létrehozásának folyamatán, beleértve annak tulajdonságait és zóna adatait is.

Ha több példányt kíván létrehozni, ismételje 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

“DNS konfigurációs fájlok karbantartása” oldalszám: 29

A témakör segítségével megismerheti a Domain Name System (DNS) által használt fájlokat, és áttekintheti a mentésükre és karbantartásukra vonatkozó irányelveket.

Névszerver példány létrehozása

A DNS szerver példány meghatározásához használja az Új Domain Name System (DNS) konfigurációs varázslót.

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

1. Az **iSeries navigátorban** bontsa ki az **iSeries szerver** → **Hálózat** → **Szerverek** → **DNS** elemeket.
2. A bal kereten kattintson a jobb egérgombbal a **DNS** elemre, és válassza ki az **Új névszerver...** opciót.
3. A varázsló végigvezeti a konfigurálási folyamaton.

A varázsló a következő bevitelleket kéri:

DNS szerver naplózás

Írjon be egy nevet a DNS szerver számára. Legfeljebb 5 karakteres lehet, és betűvel kell kezdődnie. Ha több szervert hoz létre, mindegyiknek egyedi nevének kell lenni. Erre a névre a rendszer más területein mint 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 azonban további szerver példányokat hoz létre, egyiket sem állíthatja be az ÖSSZES figyelésére. 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 az Interneten van és azt várja, hogy a DNS teljes egészében képes legyen az Internet nevek felbontására.

Szerver indítás:

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.

Domain Name System 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. Az **iSeries navigátorban** bontsa ki az **iSeries szerver** → **Hálózat** → **Szerverek** → **DNS** elemeket.
2. A jobb kereten kattintson a jobb egérgombbal a **DNS szerverre**, és válassza ki a **Konfigurációt**.
3. Kattintson a jobb egérgombbal a **DNS szerverre**, és válassza ki a **Tulajdonságokat**.

Zónák konfigurálása a névszerveren

Miután konfigurálta a Domain Name System (DNS) szerver példányt, be kell állítania a zónákat az adott névszerverre.

A szerver a jobboldali kereten jelenik meg. A zónák konfigurálásához a szerveren, kattintson a jobb egérgombbal a szerver nevére és válassza ki a **Konfigurációt**. A DNS konfiguráció ablak jelenik meg.

Az összes zóna konfigurálása a varázsló segítségével történik. Hozzon létre **Egyenes kikeresési zónákat** vagy **Fordított kikeresési zónákat** azáltal, hogy a jobb egérgombbal rákattint a megfelelő mappára. Az adott zónatípusra vonatkozó beállítások jelennek meg. A varázsló elindításához válassza ki a létrehozni kívánt zónatípust.

Kapcsolódó fogalmak

“Külső DNS adatok elérése” oldalszám: 26

Amikor Domain Name System (DNS) zóna adatokat hoz létre, a szerver képes lesz megoldani a kérdéses zónára vonatkozó lekérdezéseket.

Kapcsolódó feladatok

“Domain Name System konfigurálása dinamikus frissítések fogadásához”

A BIND 8-at futtató Domain Name System (DNS) konfigurálható úgy, hogy elfogadjon kéréseket más forrásoktól a zóna adatok dinamikus frissítésére. Ez a témakör az engedélyezés-frissítés opció konfigurálására vonatkozó utasításokat tartalmazza, amelynek révén a DNS fogadni tudja a dinamikus frissítéseket.

“Domain Name System fájlok importálása” oldalszám: 26

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

Kapcsolódó hivatkozás

“A zónák alapjai” oldalszám: 2

A témakör ismerteti a Domain Name System (DNS) zónákat és zónatípusokat.

Domain Name System konfigurálása dinamikus frissítések fogadásához

A BIND 8-at futtató Domain Name System (DNS) konfigurálható úgy, hogy elfogadjon kéréseket más forrásoktól a zóna adatok dinamikus frissítésére. 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 is manuálisan kell frissíteni, le kell állítani a dinamikus zóna szerverét, majd újra el kell indítani a frissítések elvégzése után. A szerver leállítása kikényszeríti az összes dinamikus frissítés összehangolását, amelyek a szerver zóna adatokkal való feltöltése (a zóna adatbázisból) óta történtek. Ha nem állítja le a szervert, akkor elvesztené a szerver elindítása óta feldolgozott összes dinamikus frissítést. 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. Az **iSeries navigátorban** bontsa ki az **iSeries szerver** → **Hálózat** → **Szerverek** → **DNS** elemeket.
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 Címegezési listát használ a felhatalmazott frissítések ellenőrzéséhez. Ha egy objektumot akar felvenni a címegezési listába, válassza ki a címegezési lista elemének típusát, és kattintson a **Hozzáadás** gombra. Felvehet a listába IP címet, IP előtagot, Hozzáféres vezérlési listát vagy kulcsot.
8. Amikor befejezi a címegezési lista frissítését, kattintson az **OK** gombra a Beállítások lap bezárásához.

Kapcsolódó fogalmak

“Dinamikus frissítések” oldalszám: 5

A BIND 8-ra épülő OS/400 V5R1 DNS támogatja a dinamikus frissítéseket. Ez lehetővé teszi a külső forrásoknak, mint például a DHCP-nek, hogy frissítéseket küldjön a DNS szervernek.

“Zónák konfigurálása a névszerveren” oldalszám: 25

Miután konfigurálta a Domain Name System (DNS) szerver példányt, be kell állítania a zónákat az adott névszerverre.

Kapcsolódó feladatok

A DHCP konfigurálása dinamikus frissítések küldéséhez

Domain Name System fájlok importálása

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

Elsődleges zónát létrehozhat egy zóna adatfájl importálásával, vagy a meglévő hoszttáblázat konvertálásával. Ha hoszttáblázatból zóna adatokat kíván létrehozni, olvassa el a Hoszttáblázatok konvertálását.

Minden olyan zóna konfigurációs fájl importálható, amely a BIND szintaxis alapján érvényes. Az állománynak egy IFS könyvtárban kell lenni. Amikor importálja, a DNS ellenőrzi, hogy egy érvényes zóna adatfájlról van-e szó, és hozzáadja az adott szerver példány NAMED.CONF állományához.

A zóna fájl importálásához kövesse ezeket a lépéseket:

1. Az iSeries navigátorban bontsa ki az **iSeries szerver** → **Hálózat** → **Szerverek** → **DNS** elemeket.
2. A jobb kereten kattintson duplán arra a DNS szerver példányra, ahová importálni szeretné a zónát.
3. A bal kereten kattintson a jobb egérgombbal a **DNS szerver** elemre, és válassza ki a **Zóna importálása** opciót.
4. Az elsődleges zóna importálásához kövesse a varázsló utasításait.

Kapcsolódó fogalmak

“Zónák konfigurálása a névszerveren” oldalszám: 25

Miután konfigurálta a Domain Name System (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 DNS adatok elérése

Amikor Domain Name System (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 gazdagépekre 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 szervert más szerverek felé a hierarchiában, amíg választ nem talál, vagy amíg meg nem állapítja, hogy nincs válasz.

Az iSeries navigátor alapértelmezett gyökér szervereinek listája

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 listáját az iSeries navigátor tartalmazza. A lista az iSeries navigátor kiadásakor aktuális állapotnak megfelelő. Az alapértelmezett lista aktualitását ellenőrizheti, ha összehasonlítja az InterNIC helyen lévővel. Frissítse a konfiguráció gyökér szerver listáját, hogy aktuális szinten tartsa.

Honnan szerezhető be az Internet gyökér (root) szerverek címei?

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

1. Névtelen (anonymous) FTP az InterNIC szerverhez: FTP.RS.INTERNIC.NET
2. Töltse le ezt a fájlt: /domain/named.root
3. Tárolja a fájlt a következő alkönyvtárban: Integrált
fájlrendszer/Root/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-állományaiban 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 fogalmak

“Zónák konfigurálása a névszerveren” oldalszám: 25

Miután konfigurálta a Domain Name System (DNS) szerver példányt, be kell állítania a zónákat az adott névszerverre.

DNS kezelése

Ez a témakör ismerteti a Domain Name System (DNS) funkció ellenőrzését, a teljesítmény figyelését, valamint a DNS adatok és fájlok karbantartását.

Domain Name System funkció ellenőrzése NSLookup segítségével

Az NSLookup segítségével ellenőrizheti, hogy működik-e a Domain Name System (DNS).

Használja az NSLookup (Name Server Lookup) opciót egy IP cím DNS szerverről való lekérdezésére. Így ellenőrzi, hogy a DNS szerver válaszol-e a lekérdezésre. Lekéri a loopback IP címhez (127.0.0.1) tartozó hosztnevet. Válaszként hoszt névvel kell jelentkezni (helyi gazdagép). Futtasson lekérdezést kijelölt nevekre is, amelyek az ellenőrizni próbált szerver példányon meg vannak adva. Ezáltal megbizonyosodhat arról, hogy a tesztelt szerver példány megfelelően működik.

A DNS funkció NSLookup segítségével történő ellenőrzéséhez kövesse ezeket a lépéseket:

1. A parancssorba gépelje be az NSLOOKUP DMNNAMSVR(n.n.n.n) parancsot, ahol n.n.n.n egy cím, amelyet a tesztelés alatt álló szerver példányon figyelő címként konfigurált.
2. A parancssorba gépelje be az NSLOOKUP parancsot, és nyomja meg az Enter billentyűt. Ez elindítja az NSLookup lekérdezési szekciót.
3. Gépelje be a **server** szót, majd azt követően a szerver nevét, és nyomja meg az Enter billentyűt. Például: **server sajátiseries.sajátcég.com**. A következő információ jelenik meg:

```
Szerver: sajátiseries.sajátcég.com
Címe: n.n.n.n
```

Ahol n.n.n.n a DNS szerver IP címét jelenti.

4. Írja be a 127.0.0.1 címet a parancssorba, és nyomja meg az Enter billentyűt.
A következő információnak kell megjelenni, beleértve a loopback hoszt nevet is:

```
> 127.0.0.1
Szerver: sajátiseries.sajátcég.com
Címe: n.n.n.n
```

```
Neve: localhost
Címe: 127.0.0.1
```

A DNS szerver helyesen válaszol, ha a loopback hoszt nevet adja vissza: **localhost**.

5. Írja be az **exit** parancsot, és nyomja meg az Enter billentyűt az NSLOOKUP terminál szekció befejezéséhez.

Megjegyzés: Ha segítségre van szüksége az NSLookup használatához, gépeljen be kérdőjelet **?**, és nyomja meg az Enter billentyűt.

Biztonsági kulcsok kezelése

A biztonsági kulcsok lehetővé teszik a Domain Name System (DNS) adatokhoz való hozzáférés korlátozását.

A DNS-hez a kulcsok két típusa kapcsolódik. Mindegyik más szerepet játszik a DNS konfiguráció védelmében. Az alábbi leírás elmagyarázza, hogyan kapcsolódnak a DNS szerverhez.

DNS 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 Címegeyezési (Address Match) listában.

A DNS kulcsok kezeléséhez kövesse ezeket a lépéseket:

1. Az iSeries navigátorban bontsa ki az **iSeries szerver** → **Hálózat** → **Szerverek** → **DNS** elemeket.
2. A jobb kereten kattintson a jobb egérgombbal a megnyitni kívánt DNS szerver példányra, és válassza ki a **Konfigurációt**.
3. A DNS konfiguráció ablakban válassza a **Fájl** → **Kulcsok kezelése** elemeket.

Dinamikus frissítések kulcsainak kezelése

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

Ezeknek a kulcsoknak létezniük kell, amikor a DNS és a DHCP ugyanazon az iSeries rendszeren találhatók. Ha a DHCP egy másik iSeries rendszeren van, akkor ugyanazokat a kulcsokat kell létrehozni mindkét iSeries szerveren ahhoz, hogy a biztonságos dinamikus frissítés lehetővé váljon.

A dinamikus frissítési kulcsok kezeléséhez kövesse ezeket a lépéseket:

1. Az iSeries navigátorban bontsa ki az **iSeries szerver** → **Hálózat** → **Szerverek** → **DNS** elemeket.
2. Kattintson a jobb egérgombbal a **DNS** ikonra, majd válassza ki a **Dinamikus frissítési kulcsok kezelése** elemet.

Domain Name System szerver statisztika elérése

Az adatbázis dump 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

“DNS konfigurációs fájlok karbantartása”

A témakör segítségével megismerheti a Domain Name System (DNS) által használt fájlokat, és áttekintheti a mentésükre és karbantartásukra vonatkozó irányelveket.

Szerver statisztika

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

A Domain Name System (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. Az iSeries navigátorban bontsa ki az **iSeries szerver** → **Hálózat** → **Szerverek** → **DNS** elemeket.
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.

Aktív szerver adatbázis

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 levélkezelő (MX) információkat, amelyek hasznosak lehetnek hibakereséskor.

A DNS lehetővé teszi a szerver példány hiteles-, gyorsítótáras- és célzott adatairól készült dump megtekintését. A dump 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 iSeries navigátor segítségével megtekintheti az aktív szerver adatbázisának kiírását (dump). Ha szüksége van a fájlok egy példányára, a NAMED_DUMP.DB nevű adatbázis dump fájl iSeries elérési útvonala: **Integrált fájlrendszer/Root/QIBM/UserData/OS400/DNS/<szerver példány>**, ahol "<szerver példány>" a DNS szerver példány neve. Az aktív szerver adatbázisról további információkat talál a DNS online segítség **DNS szerver adatbázis kiírásának alapjai** című részében.

Az aktív szerver adatbázis dump eléréséhez kövesse ezeket a lépéseket:

1. Az iSeries navigátorban bontsa ki az **iSeries szerver** → **Hálózat** → **Szerverek** → **DNS** elemeket.
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.



DNS konfigurációs fájlok karbantartása









A témakör segítségével megismerheti a Domain Name System (DNS) által használt fájlokat, és áttekintheti a mentésükre és karbantartásukra vonatkozó irányelveket.









Az i5/OS DNS segítségével DNS szerver példányokat hozhat létre és kezelhet az iSeries rendszeren. A DNS konfigurációs fájlokat az iSeries navigátor kezeli. A fájlokat nem kell kézi módon szerkeszteni. Mindig az iSeries

navigátort használja a DNS konfigurációs fájlok létrehozásához, módosításához vagy törléséhez. A DNS konfigurációs fájlok az integrált fájlrendszer alább felsorolt elérési útvonalában tárolódnak.

Megjegyzés: Az alábbi fájlstruktúra a BIND 8-on futó DNS szerverre vonatkozik. Ha BIND 4.9.3 alapú DNS-t használ, olvassa el a DNS konfigurációs fájlok mentése és naplófájlok kezelése című részt a V4R5 Információs központ DNS témakörében.

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 alkönyvtár kezdőpontja.
ATTRIBUTES		A DNS használja ezt a fájlt az alkalmazott BIND verzió meghatározásához.
QIBM/UserData/OS400/DNS/ <i><példány-n>/</i>		A DNS példány alkönyvtárának kezdőpontja.
ATTRIBUTES		Az iSeries DNS által használt konfigurációs tulajdonságok.
NAMED.CONF		Ez a fájl konfigurációs adatokat tartalmaz. Megmondja a szervernek, milyen adott zónákat kezel, hol vannak a zóna fájlok, mely zónák frissülhetnek dinamikusan, hol vannak a zóna továbbító szerverei, és milyen egyéb beállítások vannak.
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 8 szerverre tér át. Ez az áttérés biztonsági mentéseként funkcionál, és törölhető amint a BIND 8 szerver megfelelően működik.
NAMED.CA		Az adott szerver példány gyökér szervereinek listája.
NAMED_DUMP.DB		Az aktív szerver adatbázis számára létrehozott szerveradat dump.
NAMED.STATS		Szerver statisztika.
NAMED.PID		A futó szerver Folyamat azonosítóját (Process ID) 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.
QUERYLOG		A DNS szerver által fogadott lekérdezések naplója. A fájl akkor lesz létrehozva, amikor a DNS szerver napló aktív. Amikor aktív, a fájl egészen nagyra megnőhet, ezért szabályos időközönként törölni kell.

Név	Ikon	Leírás
<zóna-neve-a>.DB		A szerver által kiszolgálandó, adott tartományra vonatkozó zóna fájl. A zónára vonatkozó összes erőforrás rekordot tartalmazza.
<zóna-neve-b>.DB		A szerver által kiszolgálandó, adott tartományra vonatkozó zóna fájl. A zónára vonatkozó összes erőforrás rekordot tartalmazza. Minden egyes zóna külön .DB állománnyal rendelkezik.
.ixfr.		Növekményes zónaátvitel (IXFR) fájlok. A másodlagos szerverek használják ezeket a fájlokat az utolsó zónaátvitel óta megváltozott adatok betöltésére. Amint a frissítés megtörténik, az IXFR fájlok száma megnő. A régebbi IXFR fájlokat rendszeres időközönként törölni kell. Az egy-két nappal ezelőtt létrehozott fájlok meghagyása a legtöbb másodlagos szervernél lehetővé teszi még az IXFR betöltését. Ha az összes fájlt törli, a másodlagos szerver kérni fogja a teljes átvitelt (AXFR).
TMP		A szerver példány által használt alkönyvtár az ideiglenes munkafájlok létrehozására.
QIBM/UserData/OS400/DNS/TMP		A QTOBH2N program által használt alkönyvtár, a hoszttáblázatból kiíratott közbenső fájlok létrehozásához, amelyeket később az iSeries navigátor segítségével importálhat.
QIBM/UserData/OS400/DNS/_DYN/		A dinamikus frissítéshez szükséges fájlok őrzésére szolgáló alkönyvtár.
<kulcs_id-neve-x>._KID		BIND 8 kulcs utasítást tartalmaz a <kulcs_id-neve-x> nevű kulcs_id számára.
<kulcs_id-neve-x>._DUK.<zóna-neve-a>		Dinamikus frissítési kulcs, amely a <kulcs_id-neve-x> kulcs segítségével a <zóna-neve-a> dinamikus frissítésének kezdeményezéséhez szükséges.
<kulcs_id-neve-y>._KID		BIND 8 kulcs utasítást tartalmaz a <kulcs_id-neve-y> nevű kulcs_id számára.
<kulcs_id-neve-y>._DUK.<zóna-neve-a>		Dinamikus frissítési kulcs, amely a <kulcs_id-neve-y> kulcs segítségével a <zóna-neve-a> dinamikus frissítésének kezdeményezéséhez szükséges.
<kulcs_id-neve-y>._DUK.<zóna-neve-b>		Dinamikus frissítési kulcs, amely a <kulcs_id-neve-y> kulcs segítségével a <zóna-neve-b> dinamikus frissítésének kezdeményezéséhez szükséges.

Kapcsolódó fogalmak

“Domain Name System jogosultságok meghatározása” oldalszám: 20

A Domain Name System (DNS) rendszergazdának különleges jogosultsági szükségletei vannak. Vegye figyelembe a jogosultság biztonsági vonatkozásait is.

“Domain Name System szerver statisztika elérése” oldalszám: 29

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

Kapcsolódó feladatok

“Névszerverek konfigurálása” oldalszám: 24

A Domain Name System (DNS) lehetővé teszi több névszerver példány létrehozását. Ez a témakör a névszerver konfigurálására vonatkozó utasításokat tartalmazza.

Fejlett Domain Name System funkciók

A témakör elmagyarázza, hogyan használhatják a gyakorlott rendszergazdák a Domain Name System (DNS) fejlett funkcióit a DNS szerver könnyebb kezelésére.

Az iSeries navigátor kezelőfelületet nyújt a DNS szerver konfigurálásához és irányításához. A következő feladatok mintegy parancsiként szolgálnak a rendszergazdák számára, akik jól ismerik az iSeries grafikus kezelőfelületét. Segítségükkel gyorsan megváltoztathatja a szerver állapotát és tulajdonságait egyszerre több példányon is.

Kapcsolódó feladatok

“Domain Name System hibakeresési beállítások módosítása” oldalszám: 35

A Domain Name System (DNS) hibakeresési funkciója olyan információkkal szolgál, amelyek segíthetik a DNS szerver problémák meghatározását és javítását.

DNS tulajdonságok módosítása

A DNS beállításait módosíthatja, ha a kezelőfelület nem teszi lehetővé, hogy az összes szerver példányon egyszerre változtassa meg az automatikus indítást és a hibakeresési szintet.

A karakter alapú kezelőfelület segítségével módosíthatja ezeket a beállításokat az egyedi DNS szerver példányokon, vagy egyszerre az összesen. Kövesse ezeket a lépéseket a CHGDNSA használatához:

1. A parancssorba gépelje be a CHGDNSA parancsot, és nyomja meg az F4 billentyűt.
2. A Change DNS Server Attributes (CHGDNSA) lapon írja be a szerver példány nevét, vagy az *ALL kifejezést, és nyomja meg az Enter billentyűt.

A rendelkezésre álló szerver tulajdonságok jelennek meg:

```
Autostart server . . . . . *SAME *YES, *NO, *SAME  
Debug level . . . . . *SAME 0-11, *SAME, *DFT
```

3. **Autostart server** Annak megadásához, hogy a kiválasztott DNS szerverek automatikusan elinduljanak a TCP/IP indításakor, írjon be *YES értéket. Ha nem akarja, hogy a szerver elinduljon a TCP/IP indításakor, gépeljen be *NO értéket. Ha a tulajdonságot a pillanatnyi beállítással kívánja meghagyni, írjon be *SAME értéket.

Debug level A hibakeresési szint módosításához, amelyet a kiválasztott DNS szervereknek használniuk kellene, írjon be 0 és 11 közé eső értéket. Ha azt akarja megadni, hogy a hibakeresési szint a szerver indításkori hibakeresési szintje legyen, írjon be *DFT értéket. Ha a tulajdonságot a pillanatnyi beállítással kívánja meghagyni, írjon be *SAME értéket.

Amikor beírta az összes kívánságát, nyomja meg az Enter billentyűt a DNS tulajdonságok beállításához.

Domain Name System szerverek indítása vagy leállítása

A Domain Name System (DNS) beállításait módosíthatja, ha a kezelőfelület nem teszi lehetővé, hogy egyszerre több szerver példányt indítson el vagy állítson le.

A karakter alapú kezelőfelület segítségével módosíthatja ezeket a beállításokat egyszerre több példányon. A karakter alapú kezelőfelület 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 ENDTCPSPVR SERVER(*DNS) DNSSVR(*ALL) parancsot.

Hibakeresési értékek módosítása

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

Az iSeries navigátor kezelőfelülete nem teszi lehetővé a hibakeresési szint módosítását a szerver futása közben. A karakter alapú kezelőfelület segítségével azonban módosíthatja a hibakeresési szintet a szerver futása közben. A karakter alapú kezelőfelület segítségével módosítsa a hibakeresési szintet az alábbi lépések révén, kicserélve a <példány> 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:
 - A hibakeresés bekapcsolásához, vagy a szint 1 értékkel való növeléséhez írja be a CALL QTOBDRVS ('BUMP' '<példány>') parancsot, majd nyomja meg az Enter billentyűt.
 - A hibakeresés kikapcsolásához írja be a CALL QTOBDRVS ('OFF' '<példány>') parancsot, majd nyomja meg az Enter billentyűt.

Domain Name System hibaelhárítás

Ez a témakör ismerteti a Domain Name System (DNS) naplózási és hibakeresési beállításokat, amelyek segítséget nyújtanak a DNS szerverrel kapcsolatos problémák megoldásában.

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 fájlalba történt hibás bejegyzések eredménye. Amikor hiba jelentkezik, ellenőrizze, hogy a DNS konfigurációs fájlok az elvárt bejegyzéseket tartalmazzák-e.

Jobok azonosítása

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

- Ha BIND 4.9.3 verziót használ, a szerver job neve QTOBDNS lesz. A DNS 4.9.3 hibakereséséről további tájékoztatást kaphat a *DNS szerverek hibaelhárítása* című rész alatt.
- Ha BIND 8 alapú szervereket futtat, akkor minden egyes szerver példányra külön job fut. A job neve 5 rögzített karakterből (QTOBD) és az azt követő példánynévből áll. Például, ha két példánya van, INST1 és INST2, akkor a jobok nevei QTOBDINST1 és QTOBDINST2 lesznek.

Kapcsolódó fogalmak

“Domain Name System szerver üzenetek naplózása”

A Domain Name System (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.

Kapcsolódó feladatok

“Domain Name System hibakeresési beállítások módosítása” oldalszám: 35

A Domain Name System (DNS) hibakeresési funkciója olyan információkkal szolgál, amelyek segíthetik a DNS szerver problémák meghatározását és javítását.

Domain Name System szerver üzenetek naplózása

A Domain Name System (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 8 több új naplózási beállítást 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 8 dokumentációk más forrásait is a naplózás érdekében.

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 csatornához naplózott üzenetek egy fájlba lesznek elküldve. Az alapértelmezett fájlcsatornák az as400_debug és az as400_QPRINT. Alapértelmezés szerint a hibakeresési üzenetek az as400_debug csatornába (a NAMED.RUN fájlba) lesznek naplózva, de megadhatja azt is, hogy más üzenetkategoróriák is ebbe a fájlba legyenek küldve. Az as400_QPRINT csatornába naplózott üzenetkategoróriák a QPRINT spool fájlba mennek a QTCP felhasználói profil alatt. Létrehozhat saját fájl csatornát is az alapértelmezés szerint meglévő csatornákon túlmenően.

- **Rendszernapló csatornák**

Az ide naplózott üzenetek a szerver job naplójába mennek. Az alapértelmezett rendszernapló csatorna az as400_joblog. Az ide irányított naplóüzenetek a DNS szerver példány job naplójába mennek.

- **Null csatornák**

A null csatornához naplózott összes üzenet törlésre kerül. Az alapértelmezett null csatorna az as400_null. A kategóriákat a null csatornához 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. Számos kategória van, beleértve:

- config: Konfigurációs fájl feldolgozás
- db: Adatbázis műveletek
- queries: Rövid naplóüzenetet készít minden lekérdezésre, amelyet a szerver vesz
- lame-servers: Hibás átruházás észlelése
- update: Dinamikus frissítések
- xfer-in: Zóna átvitel, amelyet a szerver fogad
- xfer-out: Zóna átvitel, amelyet a szerver küld

A naplóállományok egészen nagyra megnőhetnek, szabályos időközönként törölni kell őket. A DNS szerver összes naplóállományának 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.

A naplózási beállítások módosítása

A naplózási beállítások eléréséhez kövesse ezeket a lépéseket:

1. Az iSeries navigátorban bontsa ki az **iSeries szerver** → **Hálózat** → **Szerverek** → **DNS** elemeket.
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.

Hibaelhárítási javaslat

Az as400_joblog csatorna alapértelmezett súlyossági szintjét állítsa Hiba szintre. Ez a beállítás csökkenti a tájékoztatást tartalmazó és a figyelmeztető üzenetek számát, amelyek egyébként lefokoznák a teljesítményt. Ha hibákat tapasztal, de a joblog nem jelzi a probléma forrását, esetleg változtassa meg a súlyossági szintet. Kövesse a fenti eljárást a Csatornák lap eléréséhez, majd módosítsa az as400_joblog csatorna súlyossági szintjét Figyelmeztetés, Megjegyzés vagy Információ szintre, hogy több naplódatot tudjon megnézni. Amint megoldja a problémát, állítsa vissza a súlyossági szintet Hiba értékre, hogy csökkentse a naplóban az üzenetek számát.

Kapcsolódó feladatok

“Domain Name System hibaelhárítás” oldalszám: 33

Ez a témakör ismerteti a Domain Name System (DNS) naplózási és hibakeresési beállításokat, amelyek segítséget nyújtanak a DNS szerverrel kapcsolatos problémák megoldásában.

Domain Name System hibakeresési beállítások módosítása

A Domain Name System (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 megtalálásában, 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. 1-es vagy magasabb szintnél a hibakeresési információkat a NAMED.RUN fájl tartalmazza az iSeries rendszer következő katalógusában: **Integrált fájlrendszer/Root/QIBM/UserData/OS400/DNS/<szerver példány>**, ahol "**<szerver példány>**" a DNS szerver példány nevét jelenti. A NAMED.RUN fájl mérete folyamatosan mindaddig növekszik, amíg a hibakeresési szint 1-es értékű vagy magasabb, és amíg a DNS szerver folytatja futását. Ajánlatos a fájl időnkénti törlése, hogy megakadályozza a túlzott mértékű lemezterület felhasználást. Használhatja a **Szerver tulajdonságok - Csatornák** lapot is, ahol szintén megadhatja a NAMED.RUN fájl verzióinak számát és maximális méretét.

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

1. Az iSeries navigátorban bontsa ki az **iSeries szerver** → **Hálózat** → **Szerverek** → **DNS** elemeket.
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 Domain Name System funkciók” oldalszám: 32

A témakör elmagyarázza, hogyan használhatják a gyakorlott rendszergazdák a Domain Name System (DNS) fejlett funkcióit a DNS szerver könnyebb kezelésére.

Kapcsolódó feladatok

“Domain Name System hibaelhárítás” oldalszám: 33

Ez a témakör ismerteti a Domain Name System (DNS) naplózási és hibakeresési beállításokat, amelyek segítséget nyújtanak a DNS szerverrel kapcsolatos problémák megoldásában.

Domain Name System témakörhöz kapcsolódó információk






A DNS témakörhöz kapcsolódó IBM Redbooks (PDF formátumban) kiadványok és webhelyek felsorolását találja itt. A PDF változatokat megnézheti vagy letöltheti.

IBM Redbooks kiadványok

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

Ez a könyv leírja a Domain Name System (DNS) szerver és a Dynamic Host Configuration Protocol (DHCP) szerver támogatást, amelyeket az i5/OS tartalmaz. A könyvben leírtak példákon keresztül segítenek a DNS és a DHCP telepítésében, testre szabásában, konfigurálásában és hibakeresésében.

Webhelyek


- *DNS és BIND*, harmadik kiadás. Paul Albitz és Cricket Liu. O'Reilly and Associates, Inc. kiadása  Sebastopol, Kalifornia, 1998. ISBN szám: 1-56592-512-2. Ez a legteljesebb forrás a DNS szerverről.
- Internet Software Consortium webhely , amely híreket, hivatkozásokat és egyéb forrásokat nyújt a BIND-hez.
- InterNIC  karbantartja az összes tartománynév bejegyző katalógusát, amelyeket az Internet Corporation for Assigned Names and Numbers (ICANN) jogosított fel.
- DNS Resources Directory , amely DNS referencia anyagokat és számtalan hivatkozást tartalmaz más DNS erőforrásokhoz, beleértve a tárgyalási csoportokat is. Felsorolja a DNS vonatkozású RFC-eket  is.

PDF fájlok mentése

A PDF fájl munkaállomáson történő mentése megjelenítés vagy nyomtatás céljából:

1. Kattintson a jobb egérgombbal a PDF fájlra a böngészőjében (kattintás a jobb oldali egérgombbal a fenti hivatkozásra).
2. Kattintson a PDF helyi mentésére szolgáló opcióra.
3. Válassza ki azt a könyvtárat, ahová menteni kívánja a PDF fájlt.
4. Kattintson a **Mentés** gombra.

Adobe Acrobat Reader letöltése

- | A PDF állományok megtekintéséhez vagy nyomtatásához telepített Adobe Acrobat Reader programra van szükség.
- | Ingyenes példányát letöltheti az Adobe honlapjáról (www.adobe.com/products/acrobat/readstep.html) .

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.

Az IBM-nek lehetnek szabadalmi, vagy szabadalmi intézés alatt álló alkalmazásai, amelyek fedik az ebben a dokumentumban leírt témákat. 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.

Ha duplabyte-os (DBCS) információkkal kapcsolatban van szüksége licencre, akkor lépjen kapcsolatba saját országában az IBM szellemi tulajdon osztályával, vagy írjon a következő 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 KERESKEDELMELI ÉRTÉKESÍTHETŐSÉGRE 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 legjobb 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 azonosak 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 szállítóitól, az általuk közzétett bejelentésekből, illetve egyéb nyilvánosan elérhető forrásokból szerezte be. Az IBM nem vizsgálta ezeket a termékeket, és nem tudja megerősíteni a nem IBM termékekre vonatkozó teljesítményadatok pontosságát, a kompatibilitást és egyéb követelményeket. A nem IBM termékekkel kapcsolatos kérdéseivel forduljon az adott termék szállítóhoz.

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. Ezek a példák nem kerültek minden állapotban 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 csatolóra vonatkozó megjegyzés

A DNS kiadvány leír olyan programozási csatolókat, amelyek révén a felhasználó írhat programokat az IBM i5/OS kiszolgálásához.

Védjegyek

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

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

Egyéb cég-, termék- és szolgáltatásnevek mások áru-, vagy szolgáltatási védjegyei lehetnek.

Feltételek

A kiadványok használata az alábbi feltételek és kikötések alapján lehetséges.

Személyes használat: A kiadványok másolhatók személyes, nem kereskedelmi célú használatra, de valamennyi tulajdonosi feljegyzést meg kell tartani. 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