

IBM

@server

iSeries

DNS

Verze 5 vydání 3





@server

iSeries

DNS

Verze 5 vydání 3

Poznámka

Před použitím těchto informací a odpovídajícího produktu si přečtěte informace v části "Poznámky", na stránce 37.

Páté vydání (říjen 2005)

Toto vydání se týká verze 5, vydání 3, modifikace 0 licenčního programu IBM Operating System/400 (číslo produktu 5722-SS1) a všech následujících vydání a modifikací, dokud nebude v nových vydáních uvedeno jinak. Tato verze nefunguje na všech modelech počítačů RISC (reduced instruction set computer) ani na modelech CISC.

© Copyright International Business Machines Corporation 1998, 2005. Všechna práva vyhrazena.

Obsah

DNS	1
Tisk tohoto tématu	2
Příklady DNS	2
Příklad: Jediný server DNS pro intranet	2
Příklad: Jediný server DNS s přístupem k Internetu	4
Příklad: DNS a DHCP na jednom serveru iSeries ^(TM)	6
Příklad: Rozdělení DNS v rámci ochranné bariéry	8
Koncepce DNS	10
Co je to DNS	11
Co jsou dotazy DNS	12
Nastavení domény DNS	14
Dynamická aktualizace	14
Funkce odvětvového standardu BIND 8	15
Zdrojové záznamy DNS	16
Poštovní záznamy a záznamy MX	19
Plánování DNS	20
Určení oprávnění DNS	20
Určení struktury domény	21
Plánování opatření pro zabezpečení dat	21
Systémové požadavky DNS	22
Konfigurace DNS	23
Přístup k DNS v produktu iSeries Navigator	23
Konfigurace serverů jmen	24
Vytvoření instance serveru jmen	24
Editování vlastností serveru DNS	24
Konfigurace zón na serveru jmen	25
Konfigurace DNS pro přijímání dynamických aktualizací	25
Import souborů DNS	26
Přístup k externím datům DNS	26
Správa serveru DNS	27
Ověření funkčnosti DNS pomocí funkce NSLookup	27
Správa bezpečnostních klíčů	28
Statistika serveru DNS	28
Údržba konfiguračních souborů DNS	29
Rozšířené funkce DNS	31
Odstraňování problémů s DNS	32
Vytváření protokolů serveru DNS	33
Nastavení ladění DNS	34
Další informace o DNS	35
Dodatek. Poznámky	37
Ochranné známky	38
Ustanovení a podmínky pro stahování a tisk publikací	38

DNS

DNS (Domain Name System) je distribuovaný databázový systém pro správu hostitelských jmen a jejich asociovaných IP (Internet Protocol) adres. Prostřednictvím DNS mohou lidé vyhledávat hostitelský systém pomocí jednoduchého jména, jako např. "www.jklttoys.com", místo toho, aby museli vypisovat IP adresu (xxx.xxx.xxx.xxx). Jeden server může být zodpovědný pouze za to, že zná hostitelská jména a IP adresy pro malou podmnožinu určité zóny, avšak servery DNS mohou při mapování všech jmen domén na jejich IP adresy spolupracovat. Spolupráce serverů DNS umožňuje počítačům komunikovat přes Internet.

Pro verzi 5 vydání 1 (V5R1) jsou služby DNS založeny na implementaci, která je známá jako BIND (Berkeley Internet Name Domain) verze 8 a je odvětvovým standardem. Dřívější služby OS/400 DNS byly založeny na odvětvovém standardu BIND verze 4.9.3. Aby bylo možné používat nový server DNS založený na standardu BIND 8, musí být na vašem serveru iSeries nainstalována volba 33 operačního systému OS/400 - Portable Application Solutions Environment (PASE). Přestože nepoužíváte volbu PASE, můžete provozovat tentýž server DNS založený na standardu BIND 4.9.3, který byl k dispozici v předcházejících vydáních. Přejít na verzi BIND 8 vám však umožní používat zdokonalené funkce a poskytnout zvýšenou ochranu vašeho serveru DNS.

Pozn.: Toto téma pojednává o nových funkcích založených na BIND 8. Jestliže ke spuštění DNS nepoužíváte PASE založený na BIND 8, prostudujte si téma V4R5 DNS v rámci aplikace Information Center



pojednávající o produktu BIND 4.9.3 (zhruba 357 KB).

- Tisk tohoto tématu. Zde se dozvíte, jak načíst nebo vytisknout téma týkající se DNS.

Co je to DNS

Níže uvedená témata jsou koncipována tak, aby vám pomohla pochopit základy DNS pro server iSeries.

Příklady DNS poskytují diagramy a vysvětlení, jak funguje DNS.

Koncepce DNS vysvětluje objekty a procesy, které používá DNS k vlastní funkci.

Plánování DNS vám pomůže vytvořit plán pro konfiguraci DNS.

Používání DNS

Následující témata jsou navržena tak, aby vám pomohla při konfiguraci a správě DNS na serveru iSeries. Také vysvětlují, jak využívat výhod nových funkcí, které máte nyní k dispozici.

Systémové požadavky DNS

Téma popisuje softwarové požadavky pro spuštění DNS na serveru iSeries.

Konfigurace DNS

Téma vysvětluje, jak je možné využít produkt iSeries Navigator ke konfiguraci serverů jmen a k rozlišování dotazů mimo vaší doménu.

Správa serveru DNS

Téma vás seznámí s postupy při ověřování funkce DNS, monitorování výkonu a údržbě dat a souborů DNS.

Odstraňování problémů s DNS

Téma se zabývá nastavením vytváření protokolů a ladění DNS, které vám může pomoci při řešení problémů s vaším serverem DNS.

Pokud máte dotazy, které nejsou zodpovězeny v aplikaci Information Center, najdete seznam ostatních zdrojů a referenčních materiálů v tématu Další informace o DNS.

Tisk tohoto tématu

Chcete-li si prohlédnout nebo stáhnout PDF verzi, vyberte DNS (přibližně 357 kB).

Chcete-li uložit soubor PDF na své pracovní stanici za účelem prohlížení nebo tisku, postupujte takto:

1. Otevřete soubor PDF v prostředí prohlížeče (klepněte na výše uvedený odkaz).
2. V menu prohlížeče klepněte na **File (Soubor)**.
3. Klepněte na **Save As... (Uložit jako...)**.
4. Vyhledejte adresář, do kterého chcete uložit soubor PDF.
5. Klepněte na **Save (Uložit)**.

Potřebujete-li k zobrazení nebo tisku těchto PDF program Adobe Acrobat Reader, můžete si stáhnout jeho kopii na webových stránkách společnosti Adobe (www.adobe.com/products/acrobat/readstep.html)



Příklady DNS

DNS je distribuovaný databázový systém pro správu hostitelských jmen a jejich asociovaných IP adres. Následující příklady vám pomohou vysvětlit, jak DNS pracuje a jak jej můžete využít ve své síti. Tyto příklady popisují nastavení a důvody použití tohoto serveru. Zároveň jsou propojeny se souvisejícími koncepcemi, což může být důležité proto, abyste porozuměli uvedeným obrázkům.

Příklad: Jediný server DNS pro intranet

Popisuje jednoduchou podsít se serverem DNS pro interní použití.

Příklad: Jediný server DNS s přístupem k Internetu

Popisuje jednoduchou podsít se serverem DNS, který je přímo připojen k Internetu.

Příklad: DNS a DHCP na jednom serveru iSeries^(TM)

Popisuje DNS a DHCP na stejném serveru. Tato konfigurace může být použita k dynamické aktualizaci zónových dat DNS, když DHCP přiřazuje IP adresy hostitelským systémům. Pokud je váš server DHCP na jiném serveru iSeries, prostudujte si informace o dodatečných požadavcích na konfiguraci DHCP uvedené v části Příklad: DNS a DHCP na různých serverech iSeries.

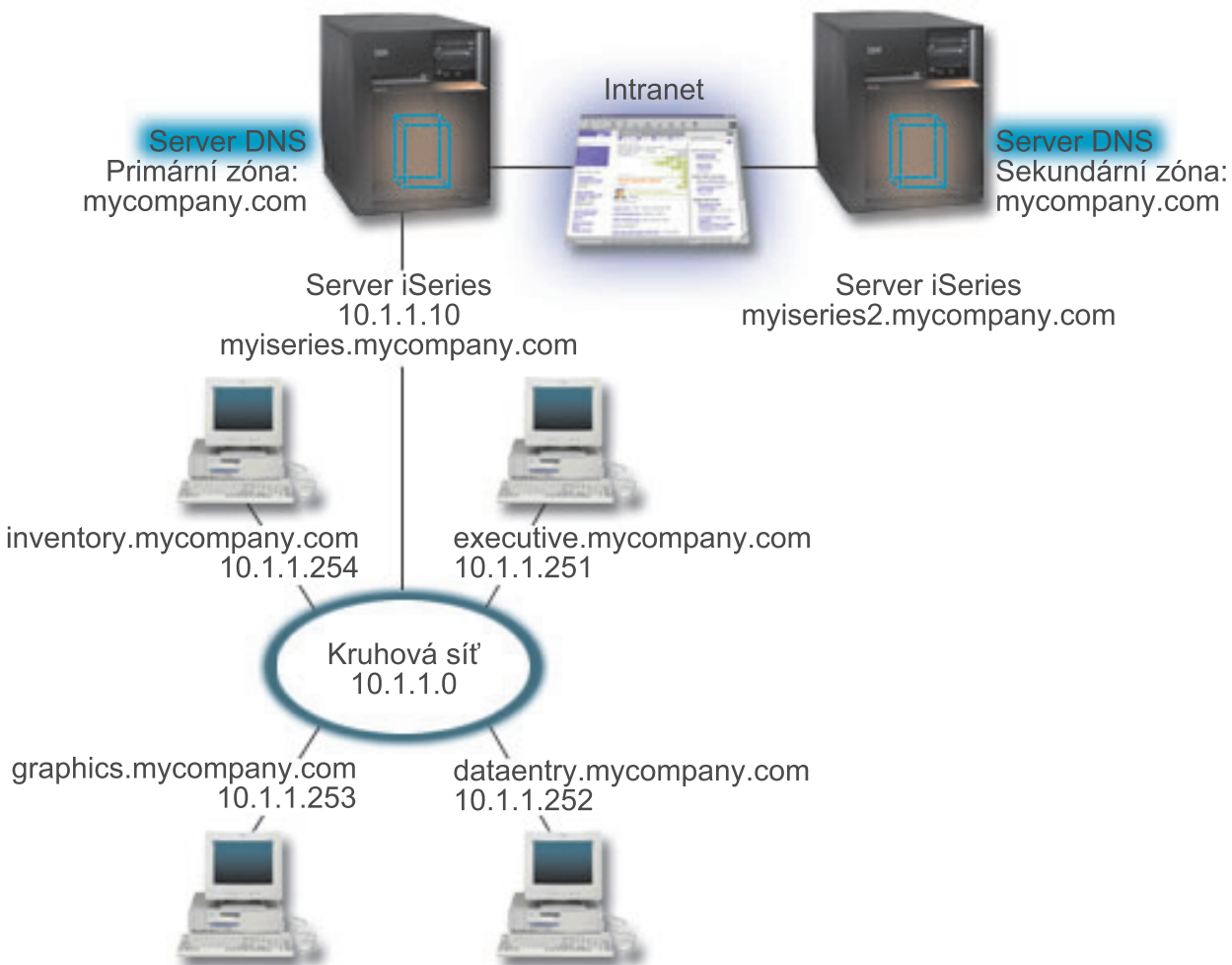
Příklad: Rozdělení DNS v rámci ochranné bariéry

Popisuje DNS, který pracuje nad ochrannou bariérou (firewall) tak, aby ochránil interní data před přístupem z Internetu, zatímco interním uživatelům umožňuje přístup k datům na Internetu.

Příklad: Jediný server DNS pro intranet

Následující ilustrace popisuje DNS spuštěný na serveru iSeries^(TM) v interní síti. Tato jediná instance (výskyt) serveru DNS je nastavena tak, aby naslouchala dotazům na všech IP adresách rozhraní. Takový server je primární server jmen pro zónu "mycompany.com".

Obrázek 1. Jediný server DNS pro intranet



Každý hostitelský systém v této zóně má IP adresu a jméno domény. Administrátor musí ručně definovat tyto hostitelské systémy v zónových datech DNS tak, že vytvoří zdrojové záznamy. Záznamy mapování adres (A) mapují jméno počítače na jeho asociovanou IP adresu. To umožňuje ostatním hostitelským systémům v síti dotazovat se serveru DNS na IP adresu přiřazenou konkrétnímu hostitelskému jménu. Záznamy PTR (Reverse-lookup pointer) mapují IP adresu systému na jeho asociované jméno. To dává ostatním hostitelským systémům v síti možnost dotazovat se serveru DNS na hostitelské jméno, které odpovídá určité IP adrese.

Kromě záznamů A a PTR podporuje server DNS mnoho jiných zdrojových záznamů, které mohou být požadovány v závislosti na tom, jaké další aplikace na bázi TCP/IP provozujete ve vaší vnitropodnikové síti. Pokud například spouštíte interní e-mailové systémy, pak možná budete chtít přidat záznamy výměníku pošty MX (Mail exchanger), aby se mohl SMTP dotazovat DNS na to, na kterých systémech jsou spuštěny poštovní servery.

V případě, že tato malá síť bude částí větší vnitropodnikové sítě, bude možná nezbytné definovat interní kořenové servery.

Sekundární servery

Sekundární servery nahrávají zónová data ze spolehlivého (authoritative) serveru prostřednictvím přenosů zón. Když se spouští sekundární server jmen, požaduje od primárního serveru jmen všechna data pro specifikovanou doménu. Sekundární server jmen požaduje aktualizovaná data z primárního serveru buď z toho důvodu, že obdrží oznámení z primárního serveru jmen (při použití funkce NOTIFY), nebo proto, že

se dotáže primárního serveru jmen a zjistí, že se data změnila.

Na výše uvedeném obrázku je server myiseries částí intranetu. Byl nakonfigurován další server iSeries, myiseries2, aby působil jako sekundární server DNS pro zónu mycompany.com. Sekundární server je možné použít k vyvážení požadavků na servery a zároveň k vytvoření zálohy pro případ selhání primárního serveru. Doporučuje se mít alespoň jeden sekundární server pro každou zónu.

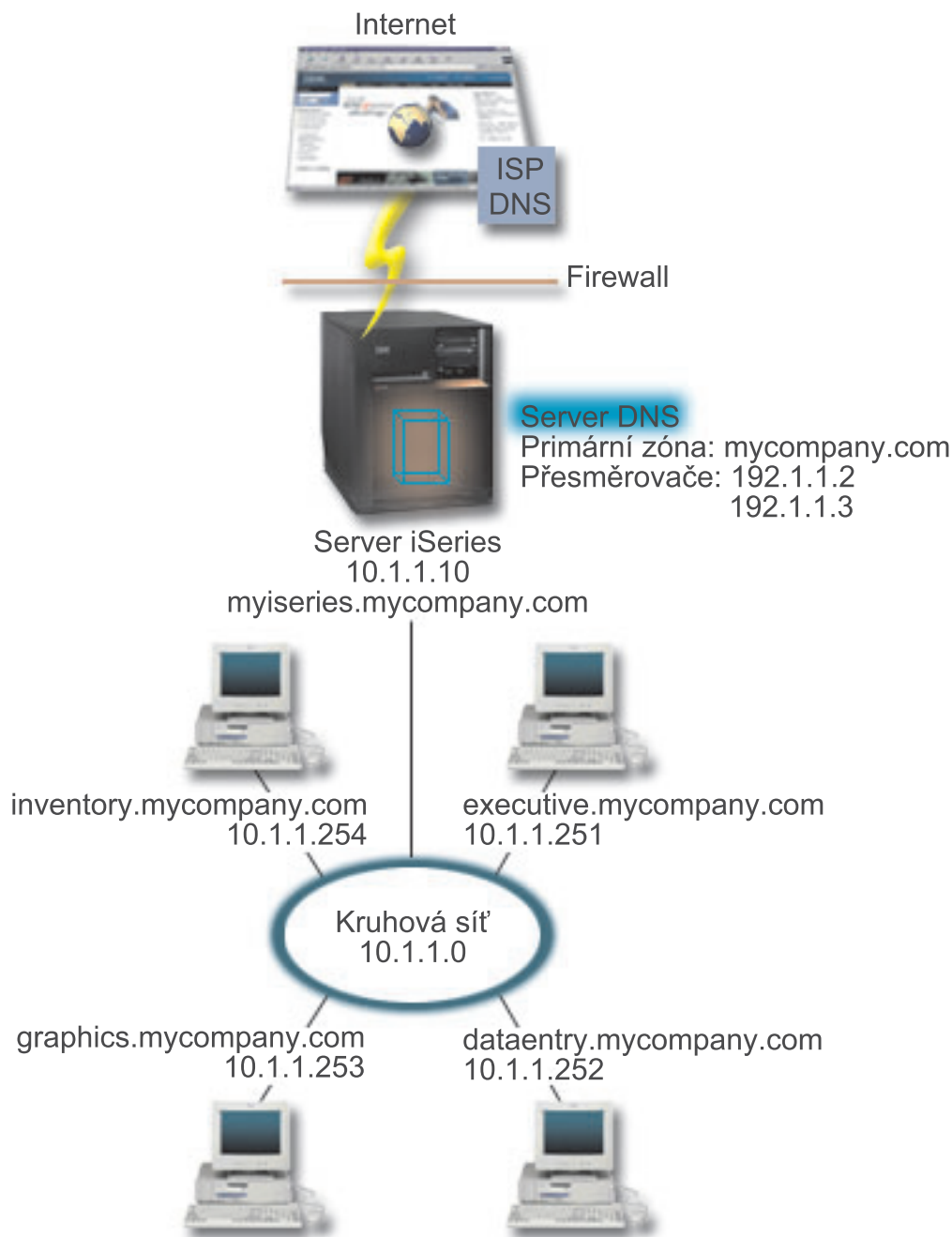
Další informace o objektech diskutovaných v tomto příkladě najdete v následujících tématech:

- Co je to DNS. Toto téma vysvětluje, co je to DNS a jak pracuje. Definuje také různé typy zón, které mohou být definovány na serveru DNS.
- Zdrojové záznamy DNS. Toto téma popisuje, jak server DNS používá zdrojové záznamy.

Příklad: Jediný server DNS s přístupem k Internetu

Následující ilustrace popisují stejnou vzorovou síť z příkladu jediného serveru DNS pro intranet s tím rozdílem, že je společnost připojena k Internetu. V tomto příkladu má společnost přístup k Internetu, avšak ochranná bariéra (firewall) je nakonfigurována tak, aby blokovala internetový provoz směrem do sítě.

Obrázek 1. Jediný server DNS s přístupem k Internetu



Pro rozlišování internetových adres musíte provést alespoň jednu z níže uvedených činností:

Definování internetových kořenových serverů

Internetové kořenové servery můžete zavést automaticky, avšak budete možná potřebovat aktualizovat seznam. Tyto servery budou pomáhat s rozlišováním adres mimo rozsah vaší vlastní zóny. Pokyny týkající se získání aktuálních internetových kořenových serverů najdete tématu [Přístup k externím datům DNS](#).

Aktivace přesměrování

Přesměrování můžete nastavit tak, aby předávalo dotazy pro zóny mimo rozsah zóny mycompany.com k externím serverům DNS, jako např. serverům DNS, které provozuje váš poskytovatel služeb sítě

Internet (ISP). Jestliže chcete umožnit vyhledávání jak pomocí přesměrování, tak pomocí kořenových serverů, budete muset nastavit volbu **Přesměrovat na první**. Server se nejprve pokusí o přesměrování a pouze v případě, že přesměrování při rozlišování dotazu selže, se dotáže kořenových serverů.

Mohou být také vyžadovány níže uvedené změny v konfiguraci:

Přiřazení neomezených IP adres

V předchozím příkladu jsou uváděny adresy 10.x.x.x. To jsou ovšem omezené adresy a není možné je používat mimo rámec vnitropodnikové sítě. Jsou uváděny dále pouze pro účely příkladů, ale vaše vlastní IP adresy budou determinovány vaším ISP a ostatními faktory vytváření sítí.

Registrace jména vaší domény

Pokud jste se dosud nezaregistrovali, je nutné provést registraci jména domény, abyste byli viditelní na Internetu.

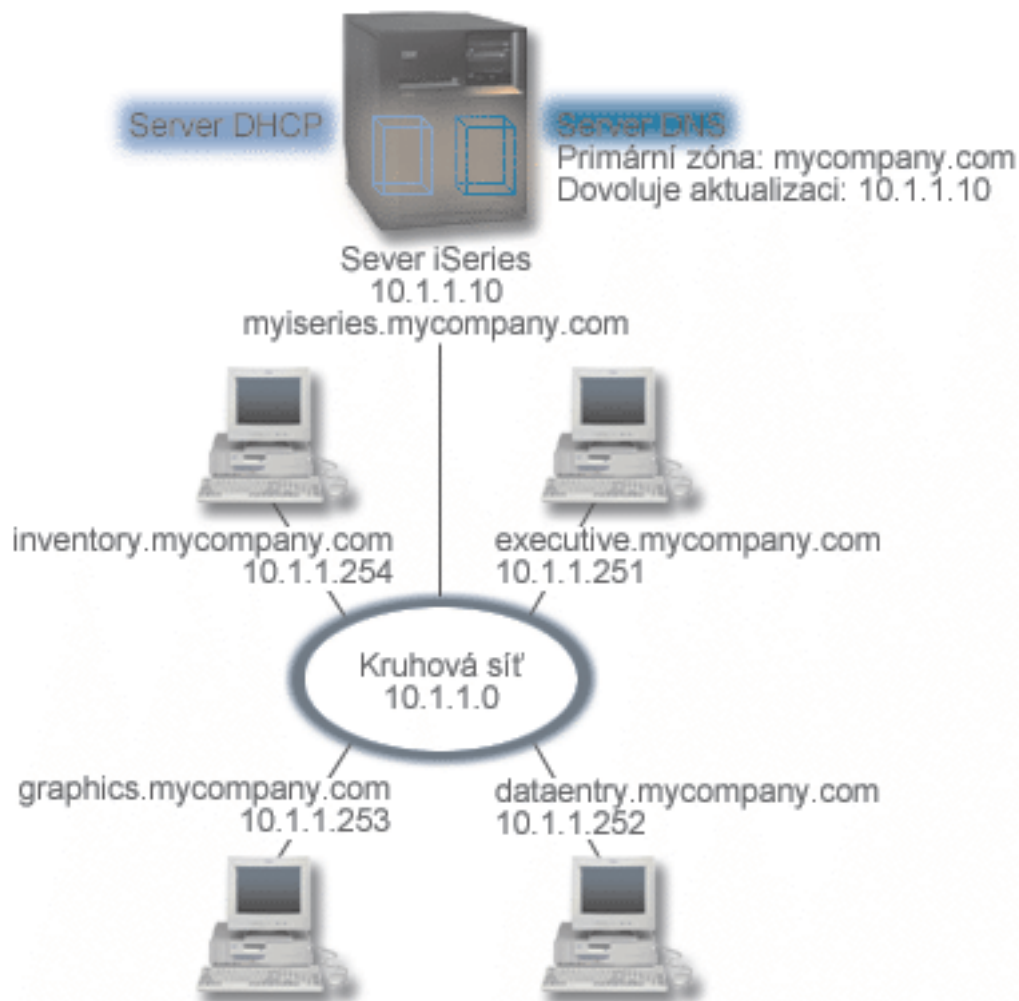
Vytvoření ochranné bariéry

Nedoporučuje se přímé připojení vašeho DNS k Internetu. Měli byste nakonfigurovat ochrannou bariéru nebo přijmout jiná opatření k zabezpečení vašeho serveru iSeries^(TM). Další informace naleznete v tématu IBM^(R) Secureway: iSeries and the Internet v rámci aplikace Information Center.

Příklad: DNS a DHCP na jednom serveru iSeries^(TM)

Následující obrázek popisuje malou podsít s jediným serverem iSeries, který působí jako server DHCP a DNS pro čtyři klienty. V tomto pracovním prostředí předpokládáme, že všichni klienti (inventory, data entry a executive) vytvářejí dokumenty s grafikou ze serveru grafických souborů. K serveru grafických souborů se připojují pomocí síťové jednotky k jeho hostitelskému jménu.

Obrázek 1. DNS a DHCP na jednom serveru iSeries



Předcházející verze DHCP a DNS byly vzájemně nezávislé. Pokud DHCP přiřadil klientovi novou IP adresu, musel administrátor ručně aktualizovat záznamy DNS. Jestliže by v tomto případě došlo ke změně IP adresy serveru grafických souborů, jelikož byla přiřazena serverem DHCP, pak by jeho závislí klienti nebyli schopni mapovat síťovou jednotku na jeho hostitelské jméno, protože by záznamy DNS obsahovaly předchozí IP adresu souborového serveru.

Se serverem DNS V5R1 založeném na odvětvovém standardu BIND 8 můžete konfigurovat vaši zónu DNS tak, aby akceptovala dynamické aktualizace záznamů DNS spolu s opakujícími se změnami adres prostřednictvím DHCP. Pokud například server grafických souborů obnoví své připojení a server DHCP mu přiřadí IP adresu 10.1.1.250, asociované záznamy DNS budou aktualizovány dynamicky. To umožní ostatním klientům dotazovat se bez přerušení serveru DNS na server grafických souborů jeho hostitelským jménem.

Chcete-li konfigurovat zónu DNS tak, aby akceptovala dynamické aktualizace, proveďte tyto kroky:

Identifikace dynamické zóny

Není možné ručně aktualizovat dynamickou zónu, jestliže je server spuštěn. Pokud tak učiníte, můžete způsobit rušení příchozích dynamických aktualizací. Ruční aktualizace může být provedena, až když je server zastaven. Veškeré dynamické aktualizace odeslané v době, kdy je server zastaven, budou ztraceny. Z tohoto důvodu je vhodné nakonfigurovat samostatnou dynamickou zónu pro minimalizaci

potřeby ručních aktualizací. Další informace o konfiguraci vašich zón pro využití funkce dynamické aktualizace najdete v tématu [Určení struktury domény](#).

Konfigurace volby povolení aktualizace

Jakákoli zóna nakonfigurovaná s volbou povolení aktualizace je považována za dynamickou zónu. Volba povolení aktualizace se nastavuje jednotlivě zóna po zóně. Aby bylo možné přijímat dynamické aktualizace, musí být pro zónu aktivována volba povolení aktualizace. V tomto případě by zóna `mycompany.com` měla data s povolením aktualizace, ale ostatní zóny definované na serveru by mohly být nakonfigurovány jako statické nebo dynamické.

Konfigurace DHCP pro odesílání dynamických aktualizací

Vašemu serveru DHCP musíte udělit oprávnění k aktualizaci záznamů DNS pro IP adresy, které distribuoval. Další informace o tom, jak nakonfigurovat server DHCP, aby odesílal dynamické aktualizace, naleznete v tématu [Konfigurace DHCP pro odesílání dynamických aktualizací](#).

Konfigurace preferencí aktualizace sekundárních serverů

Chcete-li zajistit, aby sekundární servery zůstávaly aktuální, nakonfigurujte DNS tak, aby při změně zónových dat používal funkci NOTIFY k odeslání zprávy k sekundárním serverům zóny `mycompany.com`. Také můžete nakonfigurovat přenosy IXFR, které umožní sekundárním serverům schopným přenosu IXFR sledovat a zavádět pouze aktualizovaná zónová data namísto celé zóny.

Pokud budete spouštět DNS a DHCP na různých serverech, existují určité dodatečné požadavky na konfiguraci serveru DHCP. Další informace uvádí téma [Příklad: DNS a DHCP na různých serverech iSeries](#).

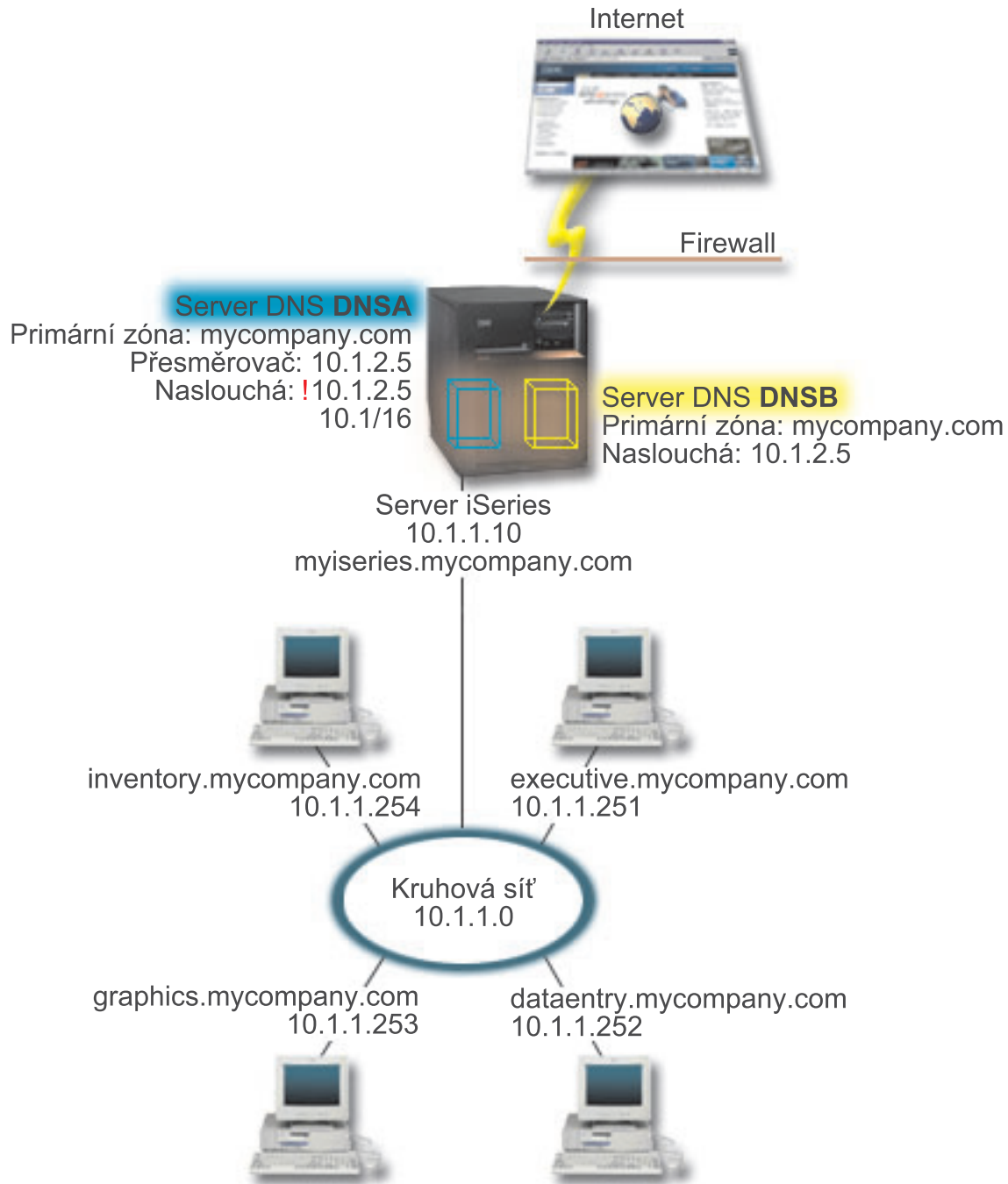
Příklad: Rozdělení DNS v rámci ochranné bariéry

Následující ilustrace popisuje jednoduchou podsít, která používá z bezpečnostních důvodů ochrannou bariéru (firewall). DNS V5R1 založený na standardu BIND 8 umožňuje nastavit na jediném serveru iSeries^(TM) několik serverů DNS. Předpokládejme, že společnost má interní síť s rezervovanou IP oblastí a externí částí sítě, která je k dispozici veřejnosti.

Tato společnost chce, aby její interní klienti byli schopni rozlišovat externí hostitelská jména a vyměňovat poštu s lidmi mimo rámec této společnosti. Společnost také chce, aby její interní klienti typu resolver měli přístup k určitým, pouze interním zónám, které nejsou přístupné mimo interní síť. Nechce ovšem, aby žádní externí klienti typu resolver byli schopni přistupovat k její interní síti.

Aby toho dosáhla, nakonfiguruje společnost dvě instance serveru DNS na jednom serveru iSeries. Jednu instanci pro intranet a druhou pro vše ve veřejné doméně. Tomu se říká rozdělení DNS.

Obrázek 1. Rozdělení DNS v rámci ochranné bariéry



Externí server, DNSB, je nakonfigurován s primární zónou mycompany.com. Tato zónová data zahrnují pouze zdrojové záznamy, které mají být částí veřejné domény. Interní server, DNSA, je nakonfigurován s primární zónou mycompany.com, avšak zónová data definovaná na DNSA obsahují zdrojové záznamy intranetu. Volba přesměrovače je definována jako 10.1.2.5. To nutí server DNSA zasílat dotazy, které nemůže rozlišit, k serveru DNSB.

Jestliže potřebujete sledovat integritu vaší ochranné bariéry a bezpečnostní rizika, máte možnost použít volbu naslouchání, která vám pomůže ochránit interní data. Chcete-li to udělat, nakonfigurujte interní server tak, aby povoloval pouze dotazy na interní zónu mycompany.com od interních hostitelských systémů. Má-li vše fungovat řádně, bude nutné, aby byli interní klienti konfigurováni pro dotazování pouze serveru DNSA. Při nastavování rozdělení DNS vezměte do úvahy následující nastavení konfigurace:

Naslouchání

V předcházejících příkladech byl na jednom serveru iSeries pouze jeden server DNS. Byl nastaven tak, aby naslouchal na všech IP adresách rozhraní. Pokud máte několik serverů DNS na jednom serveru iSeries, musíte definovat IP adresy rozhraní, na kterých naslouchá každý z nich. Dva servery DNS nemohou naslouchat na stejné adrese. V tomto případě předpokládáme, že dotazy přicházející z ochranné bariéry budou odeslány na 10.1.2.5. Tyto dotazy by měly být odeslány k externímu serveru. Proto je server DNSB nakonfigurován tak, aby naslouchal na 10.1.2.5. Interní server, DNSA, je nakonfigurován pro přijímání libovolných dotazů na IP adresách rozhraní 10.1.x.x, *vyjma* 10.1.2.5. Aby se tato adresa vyloučila efektivně, musí být vyloučená adresa uvedena v seznamu AML (Address Match List) před předponou zahrnuté adresy.

Pořadí seznamu AML (Address Match List)

Použije se první prvek v seznamu AML, který odpovídá dané adrese. Chcete-li například povolit všechny adresy v síti 10.1.x.x, s výjimkou 10.1.2.5, musí být prvky přístupového seznamu (ACL) v tomto pořadí (!10.1.2.5; 10.1/16). V takovém případě bude adresa 10.1.2.5 porovnána s prvním prvkem a bude automaticky zamítnuta.

Jestliže by byly prvky uvedeny obráceně (10.1/16; !10.1.2.5), IP adrese 10.1.2.5 by byl povolen přístup. Server by ji totiž porovnal s prvním prvkem, jenž odpovídá, a povolil by ji bez kontroly zbylých pravidel.

Koncepce DNS

DNS V5R1 nabízí nové funkce založené na odvětvovém standardu BIND 8. Následující odkazy poskytují přehledný popis toho, jak DNS funguje a jaké nové funkce můžete využívat.

Základní funkce DNS:

Co je to DNS

Poskytuje přehled o tom, co DNS je a jak funguje, stejně jako popis typů zón, které můžete definovat.

Co jsou dotazy DNS

Vysvětluje jak DNS rozlišuje dotazy ve prospěch klientů.

Nastavení domény DNS

Nabízí přehled registrace domény s odkazy na ostatní referenční stránky týkající se nastavení vaší vlastní doménové oblasti.

Nové funkce DNS:

Dynamická aktualizace

DNS V5R1 založený na odvětvovém standardu BIND 8 podporuje dynamickou aktualizaci. To umožňuje vnějším zdrojům, jako např. DHCP, odesílat aktualizace k serveru DNS.

Funkce odvětvového standardu BIND 8

Kromě dynamické aktualizace nabízí standard BIND 8 několik nových funkcí pro zvýšení výkonu vašeho serveru DNS.

Odkazy na zdrojové záznamy:

Zdrojové záznamy DNS

Zdrojové záznamy se používají k ukládání dat o jménech domén a IP adresách. Toto téma obsahuje prohlédavatelny seznam zdrojových záznamů podporovaných ve verzi V5R1.

Poštovní zdrojové záznamy a zdrojové záznamy MX

DNS podporuje rozšířené poštovní směrování prostřednictvím použití těchto záznamů.

Existuje řada dalších zdrojů, které se zabývají problematikou DNS do větších podrobností. Ostatní referenční zdroje najdete v tématu Další informace o DNS.

Co je to DNS

DNS (Domain Name System) je distribuovaný databázový systém pro správu hostitelských jmen a jejich asociovaných IP (Internet Protocol) adres. Prostřednictvím DNS mohou lidé vyhledávat hostitelský systém pomocí jednoduchého jména, jako např. "www.jktoys.com", místo toho, aby museli vypisovat IP adresu (xxx.xxx.xxx.xxx). Jeden server může být zodpovědný pouze za to, že zná hostitelská jména a IP adresy pro malou podmnožinu určité zóny, avšak servery DNS mohou při mapování všech jmen domén na jejich IP adresy spolupracovat. Spolupráce serverů DNS umožňuje počítačům komunikovat přes Internet.

Data DNS jsou rozdělena do hierarchie domén. Servery jsou odpovědné za to, že znají pouze malou část těchto dat, jako např. jednu poddoménu. Část domény, za kterou je server přímo odpovědný, se nazývá zóna. Server DNS, který má kompletní hostitelské informace a data pro určitou zónu, je označován jako spolehlivý (authoritative) pro tuto zónu. Spolehlivý server může odpovídat na dotazy o hostitelských systémech ve své zóně pomocí svých vlastních zdrojových záznamů. Proces dotazu závisí na řadě faktorů. Téma Co jsou dotazy DNS vysvětluje způsob, jakým může klient řešit dotazy.

Co jsou zóny

Data DNS jsou rozdělena do spravovatelných sad dat, které se nazývají zóny. Zóny obsahují informace o jménu a IP adrese, týkající se jedné nebo více částí domény DNS. Server, který obsahuje všechny informace pro zónu, je spolehlivým serverem pro doménu. Někdy má význam delegovat oprávnění k odpovídání dotazů DNS pro určitou poddoménu na jiný server DNS. V tomto případě může být server DNS pro tuto doménu nakonfigurován tak, aby odkazoval dotazy týkající se dané poddomény na odpovídající server.

Kvůli zálohování a možné redundanci jsou zónová data často ukládána na jiných serverech, než je spolehlivý server DNS. Tyto servery, které nahrávají zónová data ze spolehlivého serveru, jsou nazývány sekundární servery. Nakonfigurování sekundárních serverů umožňuje vyvážit požadavky na servery a zároveň poskytuje zálohu v případě selhání primárního serveru. Sekundární servery získávají zónová data tak, že provádějí zónové přenosy ze spolehlivého serveru. V případě, že je sekundární server inicializován, zavádí z primárního serveru úplnou kopii zónových dat. V případě změn zónových dat zavádí sekundární server opět zónová data z primárního serveru nebo z ostatních sekundárních serverů této domény.

Typy zón DNS

Pomocí serveru iSeries (™) můžete definovat několik typů zón, což vám pomůže při správě dat DNS:

Primární zóna

Zavádí zónová data přímo ze souboru na hostitelském systému. Primární zóna může obsahovat podzónu nebo podřízenou zónu. Může obsahovat zdrojové záznamy, jako např. hostitelský systém, jméno alias (CNAME), adresa (A) nebo záznamy ukazatele vyhledávání dozadu (PTR).

Pozn.: Primární zóny jsou někdy v jiné dokumentaci odvětvového standardu BIND nazývány jako "hlavní zóny".

Podzóna

Podzóna definuje zónu v rámci primární zóny. Podzóny vám umožňují uspořádat zónová data do spravovatelných částí.

Podřízená zóna

Podřízená zóna definuje podzónu a deleguje odpovědnost za data podzóny na jeden nebo více serverů jmen.

Jméno alias (CNAME)

Jméno alias definuje alternativní jméno pro primární jméno domény.

Hostitelský systém

Hostitelský objekt mapuje záznamy A a PTR do hostitelského systému. Další zdrojové záznamy mohou být asociovány s hostitelským systémem.

Sekundární zóna

Zavádí zónová data z primárního serveru zóny nebo ze sekundárního serveru. Sekundární server udržuje úplnou kopii zóny vůči níž je sekundárním serverem.

Pozn.: Sekundární zóny jsou často v jiné dokumentaci BIND označovány jako "závislé zóny".

Stub zóna

Stub zóna je podobná sekundární zóně, avšak přenáší pouze záznamy serveru jmen (NS) pro tuto zónu.

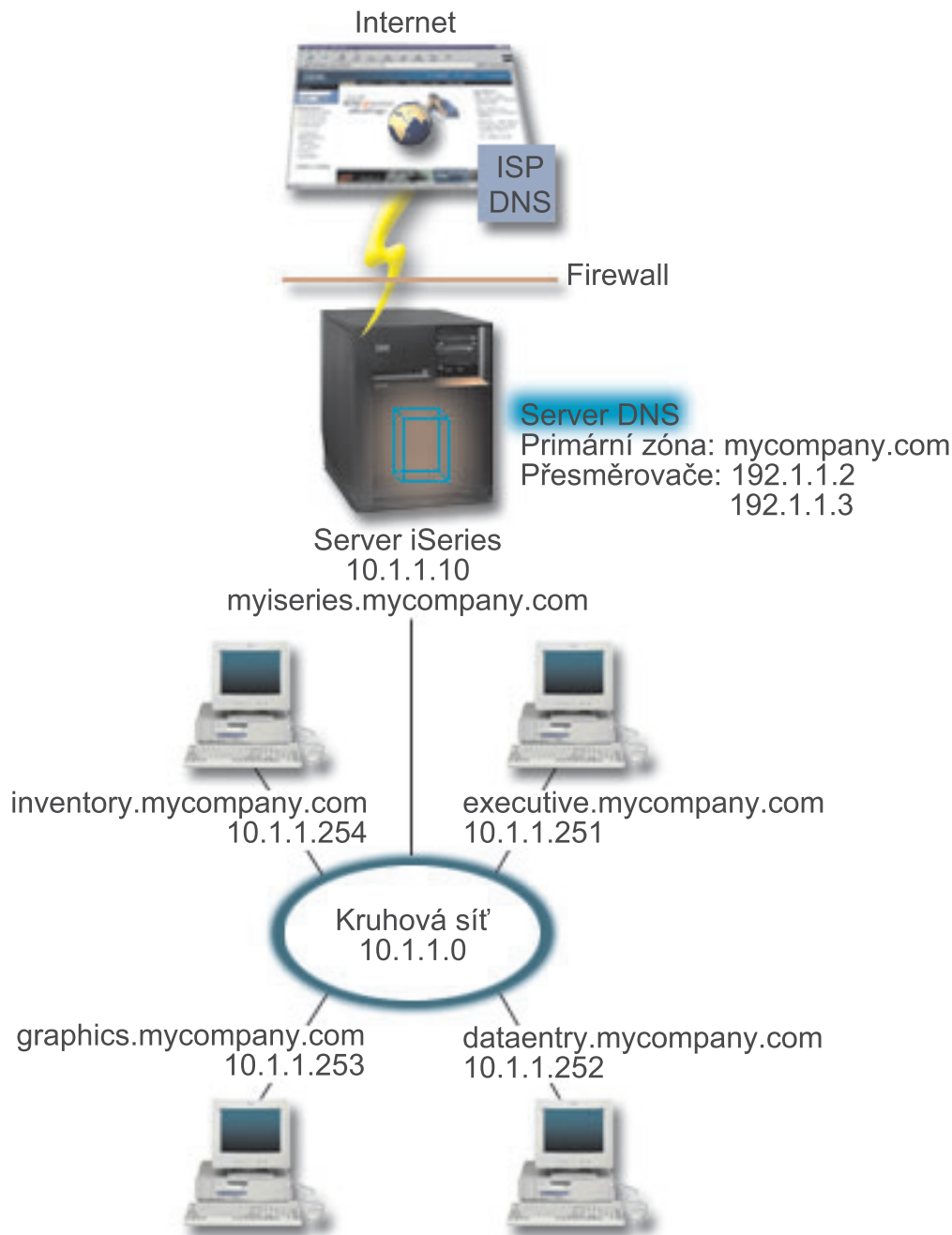
Zóna pro přesměrování

Zóna pro přesměrování směřuje všechny dotazy pro tuto konkrétní zónu k ostatním serverům.

Co jsou dotazy DNS

Klienti vyhledávají informace pomocí serverů DNS. Požadavek může vyjít přímo od klienta nebo od aplikace, která pracuje na tomto klientovi. Klient odešle k serveru DNS zprávu s dotazem, který obsahuje plně kvalifikované jméno domény (FQDN), typ dotazu (např. konkrétní záznam prostředku, který klient požaduje) a třídu pro jméno domény, což je obvykle třída Internetu (IN). Následující obrázek popisuje vzorovou síť z příkladu Jediný server DNS s přístupem k Internetu.

Obrázek 1. Jediný server DNS s přístupem k Internetu



Předpokládejme, že se hostitelský systém *dataentry* dotazuje serveru DNS na "graphics.mycompany.com". Server DNS použije svá vlastní zónová data a odpoví IP adresou 10.1.1.253.

Nyní předpokládejme, že *dataentry* požaduje IP adresu "www.jkl.com". Tento hostitelský systém není v zónových datech serveru DNS. Existují dva způsoby, jak postupovat dále, rekurze nebo iterace. Pokud je server DNS nastaven tak, aby používal rekurzi, může se tento server dotazovat ostatních serverů DNS nebo se na ně obracet v zájmu žádajícího klienta, aby plně rozlišil jméno, a potom odešle zpět odpověď klientovi. Jestliže se server DNS dotazuje jiného serveru DNS, uloží dotazující se server odpověď do rychlé vyrovnávací paměti, takže ji bude moci využít příště, jakmile obdrží tento dotaz. Klient se může za účelem rozlišení jména pokusit o kontakt s ostatními servery DNS. V tomto procesu, nazvaném iterace, používá klient samostatné a dodatečné dotazy založené na referenčních odpovědích od serverů.

Nastavení domény DNS

DNS umožňuje doručovat (obsluhovat) jména a adresy na intranetu nebo v interní síti. Také umožňuje doručování jmen a adres do celého světa prostřednictvím sítě Internet. Pokud chcete nastavit své domény pro Internet, musíte si nechat zaregistrovat jméno domény.

V případě, že konfiguruje intranet, pak si jméno domény pro interní použití registrovat nemusíte. Rozhodnutí, zda si budete nebo nebudete registrovat intranetové jméno, závisí na skutečnosti, zda chcete zajistit, aby nikdo jiný nemohl toto jméno použít v rámci Internetu, nezávisle na vašem interním používání. Registrace jména, které hodláte používat interně, zajistí, že se nedostanete do potíží, pokud budete chtít někdy později tuto doménu používat externě.

Registraci domény je možné provést tak, že se obrátíte přímo na autorizovaného registrátora jmen domén nebo na poskytovatele služeb sítě Internet (ISP). Někteří ISP nabízejí službu předání požadavku na registraci jména domény v zastoupení. Centrum InterNIC (Internet Network Information Center)



udržuje adresář všech registrátorů jmen domén, kteří mají autorizaci od společnosti ICANN (Internet Corporation for Assigned Names and Numbers).

Existuje mnoho dalších zdrojů, které poskytují informace o registraci a přípravě domény DNS. Dodatečnou pomoc nabízí téma Další informace o DNS.

Dynamická aktualizace

DHCP (Dynamic Host Configuration Protocol) je standardem TCP/IP, který používá centrální server ke správě IP adres a ostatních podrobností o konfiguraci pro celou síť. Server DHCP odpovídá na dotazy od klientů a dynamicky jim přiřazuje vlastnosti. DHCP umožňuje definovat síťové parametry konfigurace hostitelského systému jako centrálního místa a automatizovat konfiguraci hostitelských systémů. Často se používá k přiřazování dočasných IP adres klientům u sítí, které obsahují více klientů, než je dostupný počet IP adres.

V minulosti byla všechna data DNS uložena ve statických databázích. Všechny zdrojové záznamy DNS musel vytvářet a spravovat administrátor. Nyní mohou být servery DNS provozující standard BIND 8 konfigurovány tak, aby přijímaly požadavky z ostatních zdrojů na dynamickou aktualizaci zónových dat.

Server DHCP můžete nakonfigurovat tak, aby odesílal požadavky na aktualizaci do serveru DNS pokaždé, když přiřadí hostitelskému systému novou adresu. Tento automatizovaný proces snižuje administraci serveru DNS v rychle rostoucích nebo měnících se sítích TCP/IP a v sítích, kde hostitelské systémy často mění umístění. Když klient používající DHCP obdrží IP adresu, jsou tato data okamžitě odeslána k serveru DNS. Pomocí této metody může DNS úspěšně pokračovat v rozlišování dotazů od hostitelských systémů, i když se jejich IP adresy mění.

DHCP je možné nakonfigurovat tak, aby aktualizoval záznamy mapování adres (A), záznamy PTR, nebo obojí v zastoupení klienta. Záznamy A mapují hostitelské jméno počítače na jeho IP adresu. Záznamy PTR mapují IP adresu počítače na jeho hostitelské jméno. Když se změní adresa klienta, DHCP může automaticky odeslat aktualizaci serveru DNS, takže ostatní hostitelské systémy v síti mohou vyhledat klienta prostřednictvím dotazů DNS na jeho nové adrese. Pro každý dynamicky aktualizovaný záznam bude zapsán asociovaný textový záznam (TXT), který bude identifikovat, že záznam zapsal DHCP.

Pozn.: Jestliže nastavujete DHCP tak, aby aktualizoval pouze záznamy PTR, musíte nakonfigurovat DNS, aby umožňoval aktualizace z klientů, což znamená, že si každý klient může aktualizovat svůj záznam A. Ne všichni klienti DHCP podporují provádění vlastních požadavků na aktualizaci záznamu A. Předtím, než zvolíte tuto metodu, prostudujte si dokumentaci k platformě vašeho klienta.

Dynamické zóny jsou zabezpečeny vytvořením seznamu autorizovaných zdrojů, které smějí odesílat aktualizace. Autorizované zdroje můžete definovat pomocí individuálních IP adres, celých podsítí, paketů, které byly označeny sdíleným tajným klíčem (nazývaným transakční podpis, neboli TSIG) nebo libovolnou

kombinací uvedených metod. DNS ověřuje před provedením aktualizace zdrojových záznamů, zda příchozí pakety požadavků přicházejí z autorizovaného zdroje.

Dynamická aktualizace může být prováděna mezi DNS a DHCP na jednom serveru iSeries^(TM), mezi různými servery iSeries, nebo mezi jedním serverem iSeries a ostatními servery, které jsou schopné dynamické aktualizace. Více informací o konfiguraci dynamické aktualizace na serveru iSeries najdete v těchto tématech:

- Konfigurace DNS pro přijímání dynamických aktualizací.
- Konfigurace DHCP pro odesílání dynamických aktualizací.
- U serverů, které odesílají dynamické aktualizace do serveru DNS, je vyžadováno rozhraní pro dynamickou aktualizaci - API QTOBUPT. Toto rozhraní se instaluje automaticky s volbou 31 operačního systému OS/400^(R), DNS.

Funkce odvětvového standardu BIND 8

DNS byl přepracován, aby používal odvětvový standard BIND 8 pro verzi V5R1. Pokud nemáte nainstalovanou volbu PASE, můžete pokračovat v konfiguraci a spuštění dřívějšího vydání serveru OS/400^(R) založeného na standardu BIND 4.9.3. Téma Systémové požadavky DNS vysvětluje, co je potřeba ke spuštění DNS založeného na standardu BIND 8 na vašem serveru iSeries^(TM). Používání nového DNS vám umožní využívat těchto funkcí:

Několik serverů DNS provozovaných na jednom serveru iSeries

V dřívějších vydáních mohl být konfigurován pouze jeden server DNS. Nyní můžete konfigurovat několik serverů DNS nebo instancí. To vám umožní nastavit logické rozdělení mezi servery. Když vytváříte násobné instance, musíte explicitně definovat IP adresy naslouchacího rozhraní pro každou instanci. Dvě instance serveru DNS nemohou naslouchat na stejném rozhraní.

Jedním z praktických využití násobných serverů je rozdělení serveru DNS, kdy je jeden server spolehlivým (authoritative) serverem pro interní síť a druhý server se používá pro externí dotazy. Více informací o rozdělení DNS uvádí téma Rozdělení DNS v rámci ochranné bariéry.

Podmíněné přesměrování

Podmíněné přesměrování umožňuje konfigurovat server DNS pro jemné vyladění vašich přesměrovacích preferencí. Server můžete nastavit tak, aby přesměroval všechny dotazy, na které nezná odpověď. Přesměrování je možné nastavit na globální úrovni, avšak je možné přidat výjimky k doménám, u nichž chcete vynutit normální iterační rozlišení. Také můžete na globální úrovni nastavit normální iterační rozlišení a potom u určitých domén vynucovat přesměrování.

Zabezpečená dynamická aktualizace

DHCP a ostatní autorizované zdroje mohou odesílat dynamické aktualizace zdrojových záznamů pomocí TSIG (Transaction Signatures) a/nebo pomocí autorizace zdrojových IP adres. Sníží se tak potřeba ručních aktualizací zónových dat a zároveň se tím zajistí, aby se pro aktualizace používaly pouze autorizované zdroje.

Další informace o dynamické aktualizaci najdete pod tématem Dynamická aktualizace. Další informace o autorizování aktualizací z externích zdrojů uvádí téma "[rzakkplanningsecurity.htm](#)">Plánování bezpečnostních opatření.

Funkce NOTIFY

Jestliže je funkce NOTIFY zapnuta, aktivuje se funkce DNS NOTIFY, kdykoliv jsou na primárním serveru aktualizována zónová data. Primární server odesílá ke všem známým sekundárním serverům zprávu indikující, že data byla změněna. Sekundární servery potom mohou odpovědět požadavkem na přenos zóny s aktualizovanými zónovými daty. Tím se zdokonaluje podpora sekundárních serverů, neboť jsou záložní zónová data aktuální.

Přenosy zón (IXFR a AXFR)

Dříve, kdykoliv sekundární servery potřebovaly opětně zavést zónová data, zaváděla se všechna data pomocí úplného přenosu zóny, neboli AXFR (All zone transfer). Odvětvový standard BIND 8 podporuje novou metodu přenosu zóny - přenos IXFR (Incremental zone transfer). Přenos IXFR je způsob, jakým ostatní servery mohou přenášet pouze změněná data namísto celé zóny.

V případě, že je tento přenos aktivován na primárním serveru, změnám dat se přiřazuje příznak indikující, že došlo ke změně. Jestliže sekundární server požaduje aktualizaci zóny pomocí přenosu IXFR, odešle primární server pouze nová data. Přenos IXFR je zvláště užitečný, pokud je zóna aktualizovaná dynamicky, neboť snižuje provozní zátěž odesíláním menšího objemu dat.

Pozn.: Jak primární, tak sekundární server musí být schopny přenosů IXFR, aby mohly používat tuto funkci.

Zdrojové záznamy DNS

Zónová databáze DNS je tvořena kolekcí zdrojových záznamů. Každý zdrojový záznam uvádí informace o konkrétním objektu. Například záznamy mapování adres (A) mapují hostitelské jméno na IP adresu a záznamy ukazatele vyhledávání dozadu (PTR) mapují IP adresu na hostitelské jméno. Server používá tyto záznamy k odpovědím na dotazy hostitelských systémů ve své zóně. Chcete-li získat další informace, použijte k prohlédnutí zdrojových záznamů DNS níže uvedenou tabulku.

Zdrojový záznam	Zkratka	Popis
Záznamy mapování adres	A	Záznam A uvádí hostitelskou IP adresu. Záznamy A se používají k vyřešení dotazů na IP adresu specifického jména domény. Tento typ záznamů je definován v RFC 1035.
Záznamy databáze systému souborů Andrew	AFSDB	Záznam AFSDB uvádí adresu AFS nebo DCE příslušného objektu. Záznamy AFSDB se používají jako A záznamy pro mapování jména domény na její AFSDB adresu, nebo pro mapování ze jména domény buňky na ověřené servery jmen pro tuto buňku. Tento typ záznamů je definován v RFC 1183.
Záznamy kanonického jména	CNAME	Záznam CNAME specifikuje skutečné jméno domény příslušného objektu. Když se DNS dotazuje na krycí jméno a najde záznam CNAME odkazující na toto kanonické jméno, potom se dotazuje na toto kanonické jméno domény. Tento typ záznamů je definován v RFC 1035.
Záznamy informací o hostitelském systému	HINFO	Záznam HINFO specifikuje obecné informace o hostitelském systému. Standardní jména CPU a operačního systému jsou definována v dokumentu Assigned Numbers RFC 1700. Použití standardních čísel však není povinné. Tento typ záznamů je definován v RFC 1035.
Záznamy ISDN	ISDN	Záznam ISDN uvádí adresu tohoto objektu. Tento záznam mapuje hostitelské jméno na příslušnou ISDN adresu. Jsou používány pouze v sítích ISDN. Tento typ záznamů je definován v RFC 1183.

Zdrojový záznam	Zkratka	Popis
Záznamy IP adresy verze 6	AAAA	Záznam AAAA uvádí hostitelskou 128bitovou adresu. Záznamy AAAA jsou používány stejně jako záznamy A k mapování hostitelského jména na jeho IP adresu. Použijte záznamy AAAA pro podporu IP adres verze 6, které nevyhovují standardům formátu záznamu A. Tento typ záznamů je definován v RFC 1886.
Záznamy místa	LOC	Záznam LOC uvádí fyzické umístění síťových komponent. Aplikace mohou tyto záznamy používat k posouzení efektivitu sítě nebo k mapování fyzické sítě. Tento typ záznamů je definován v RFC 1876.
Záznamy serveru pro výměnu elektronické pošty	MX	Záznam MX definuje hostitelský systém výměny pošty zasílané na tuto doménu. Tyto záznamy jsou používány protokolem SMTP (Simple Mail Transfer Protocol) pro vyhledání hostitelů, kteří zpracovávají nebo doručují poštu pro tuto doménu, současně s předvolenými hodnotami pro každý hostitelský systém výměny elektronické pošty. Každý hostitelský systém výměny elektronické pošty musí mít záznam odpovídající hostitelské adresy (A) v platné zóně. Tento typ záznamů je definován v RFC 1035.
Záznamy o skupině pošty	MG	Záznamy MG specifikují jméno domény skupiny pošty. Tento typ záznamů je definován v RFC 1035.
Záznamy schránky elektronické pošty	MB	Záznamy MB specifikují jméno domény hostitelského serveru, které obsahuje schránku elektronické pošty tento objekt. Pošta došlá na tuto doménu bude nasměrována do hostitelského systému specifikovaného v záznamu MB. Tento typ záznamů je definován v RFC 1035.
Záznamy informací o schránce elektronické pošty	MINFO	Záznamy MINFO uvádí schránku elektronické pošty, která může přijímat zprávy nebo chyby pro tento objekt. Záznam MINFO se používá spíše pro seznamy elektronické pošty než pro jednotlivou schránku elektronické pošty. Tento typ záznamů je definován v RFC 1035.

Zdrojový záznam	Zkratka	Popis
Záznamy o přejmenování schránky elektronické pošty	MR	Záznamy MR uvádí nové jméno domény poštovní schránky. Záznam MR použijte jako směrovací položku pro uživatele, který se přesunul na jinou schránku elektronické pošty. Tento typ záznamů je definován v RFC 1035.
Záznamy serveru jmen	NS	Záznam NS uvádí ověřený (authoritative) server jmen pro tento hostitelský systém. Tento typ záznamů je definován v RFC 1035.
Záznamy protokolu NSAP (Network Service Access Protocol)	NSAP	Záznam NSAP uvádí adresu zdroje NSAP. Záznamy NSAP se používají k mapování jmen domén do NSAP adres. Tento typ záznamu je definován v RFC 1706.
Záznamy veřejného klíče	KEY	Záznam KEY uvádí veřejný klíč, který je asociován se jménem DNS. Klíč může být pro zónu, uživatele, nebo hostitelský systém. Tento typ záznamu je definován v RFC 2065.
Záznamy odpovědné osoby	RP	Záznam RP uvádí internetovou adresu elektronické pošty a popis osoby odpovědné za tuto zónu nebo hostitelský systém. Tento typ záznamů je definován v RFC 1183.
Záznamy ukazatele zpětného vyhledávání	PTR	Záznam PTR uvádí jméno domény hostitelského systému, pro který chcete definovat PTR záznam. Záznamy PTR umožňují vyhledání hostitelského jména dle dané IP adresy. Tento typ záznamů je definován v RFC 1035.
Záznamy Route Through	RT	Záznam RT uvádí jméno domény hostitelského systému, které může působit jako směrovač IP paketů pro tento hostitelský systém. Tento typ záznamů je definován v RFC 1183.
Záznamy SOA (Start of Authority)	SOA	Záznam SOA uvádí, že tento server je ověřený (authoritative). Ověřený (authoritative) server je nejvhodnější zdroj dat v dané zóně. Záznam SOA obsahuje všeobecné informace o zóně a opětovném zavádění pravidel sekundárními servery. V dané zóně může existovat pouze jeden záznam SOA. Tento typ záznamů je definován v RFC 1035.

Zdrojový záznam	Zkratka	Popis
Textové záznamy	TXT	Záznam TXT uvádí vícenásobné řetězce znaků, kde každý řetězec může obsahovat až 255 znaků; tyto řetězce jsou přiřazeny ke jménu domény. Záznamy TXT mohou být použity společně se záznamy RP (responsible person) a poskytovat informace o osobě odpovědné za danou zónu. Tento typ záznamů je definován v RFC 1035. Záznamy TXT jsou používány servery iSeries DHCP za účelem dynamických aktualizací. Server DHCP zapíše a přiřadí záznam TXT při každé aktualizaci záznamu PTR nebo A provedenou serverem DHCP. Záznamy serveru DHCP mají předponu AS400DHCP .
Záznamy dobře známých služeb	WKS	Záznam WKS uvádí dobře známé služby, které jsou podporovány daným objektem. Záznamy WKS obvykle indikují, zda jsou pro tuto adresu podporovány protokoly tcp, udp nebo oba dva. Tento typ záznamů je definován v RFC 1035.
Záznamy mapování adresy X.400	PX	Záznamy PX jsou ukazatelem na informace o mapování X.400/RFC 822. Tento typ záznamu je definován v RFC 1664.
Záznamy mapování adresy adresy X25	X25	Záznam X25 uvádí adresu zdroje X25. Tento záznam mapuje hostitelské jméno na příslušnou PSDN adresu. Jsou používány pouze v sítích X25. Tento typ záznamů je definován v RFC 1183.

Poštovní záznamy a záznamy MX

Poštovní záznamy a záznamy MX (Mail exchanger) používají programy na směrování pošty, jako např. SMTP (Simple Mail Transfer Protocol). Prostudujte si, prosím, vyhledávací tabulku v tématu Zdrojové záznamy DNS, pokud se chcete dozvědět více o typech poštovních záznamů podporovaných serverem iSeries^(TM) DNS.

DNS zahrnuje informace pro odesílání elektronické pošty pomocí informací MX. Pokud síť používá server DNS, aplikace SMTP nedoručuje jednoduše poštu adresovanou k hostitelskému systému TEST.IBM.COM takovým způsobem, že by otevřela spojení TCP k systému TEST.IBM.COM. Aplikace SMTP nejdříve pošle dotaz serveru DNS, aby zjistila, které hostitelské servery mohou být použity k doručení zprávy.

Doručení pošty na specifickou adresu

Servery DNS používají zdrojové záznamy známé jako záznamy výměníku pošty MX (Mail exchanger). Záznamy MX mapují jméno domény nebo hostitelské jméno na hodnotu preference a hostitelské jméno. Záznamy MX se obecně používají k označení skutečnosti, že se jeden hostitelský systém využívá pro zpracování pošty pro jiný hostitelský systém. Záznamy se také používají k označení jiného hostitelského systému, ke kterému má být proveden pokus o doručení pošty, pokud nebyl dosažen první hostitelský systém. Jinými slovy umožňují, aby pošta, která je adresována jednomu hostitelskému systému, byla doručena jinému hostitelskému systému.

Pro jedno jméno domény nebo hostitelské jméno mohou existovat vícenásobné zdrojové záznamy. V případě, že pro jednu doménu nebo hostitelský systém existují vícenásobné záznamy MX, určuje hodnota preference (neboli priorita) každého záznamu pořadí, podle kterého jsou zkoušeny. Nejnižší hodnota preference odpovídá nejvíce preferovanému záznamu, který zkoušíte jako první. Pokud nejvíce preferovaný hostitelský systém nemůže být dosažen, pokusí se odesílající poštovní aplikace kontaktovat další, méně preferovaný hostitelský systém MX. Hodnotu preference nastavuje administrátor domény nebo ten, kdo vytváří záznamy MX.

Server DNS může odpovídat i s prázdným seznamem zdrojových záznamů MX, leželi-li jméno v rozsahu jeho odpovědnosti a nemá k sobě přiřazen žádný záznam MX. Když nastane takováto situace, bude se odesílající poštovní aplikace pokoušet vytvořit spojení s cílovým hostitelským systémem přímo. **Pozn.:** Používání zástupných znaků (například: *.mycompany.com) v záznamech MX pro doménu se nedoporučuje.

Příklad: záznam MX pro hostitelský systém

V následujícím příkladu by systém měl podle preferencí doručit poštu pro fsc5.test.ibm.com samotnému hostitelskému systému. Pokud není hostitelský systém dosažitelný, může systém doručit poštu hostitelskému systému psfred.test.ibm.com nebo to mvs.test.ibm.com (v případě, že psfred.test.ibm.com je také nedosažitelný). V takovém případě by záznamy MX mohly vypadat následovně:

```
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
```

Plánování DNS

DNS nabízí řadu řešení. Předtím, než nakonfigurujete DNS, je důležité naplánovat, jak bude fungovat v rámci vaší sítě. Před implementací DNS by měly být ohodnoceny další subjekty, např. struktura sítě, výkon a zabezpečení ochrany dat. Při plánování vašich potřeb týkajících se DNS zvažte níže uvedená témata:

Určení oprávnění DNS

Pro administrátora DNS existují zvláštní požadavky na oprávnění. Měli byste promyslet bezpečnostní důsledky oprávnění. Toto téma vysvětluje tyto požadavky.

Určení struktury domény

Pokud konfiguruje doménu poprvé, měli byste před vytvářením zón naplánovat požadavky a údržbu.

Plánování opatření pro zabezpečení dat

DNS poskytuje volby pro zabezpečení dat, které omezují externí přístup k vašemu serveru. Toto téma vysvětluje uvedené volby a způsoby řízení přístupu.

Určení oprávnění DNS

Když nastavujete DNS, měli byste přijmout bezpečnostní opatření k ochraně vaší konfigurace. Musíte stanovit, kteří uživatelé mají oprávnění k provádění změn konfigurace.

K tomu, aby váš administrátor serveru iSeries^(TM) mohl provádět konfiguraci a spravovat server DNS, je zapotřebí minimální úroveň oprávnění. Poskytnutí přístupu ke všem objektům zaručuje, že je administrátor schopen provádět administrační úlohy serveru DNS. Doporučuje se, aby uživatelé, kteří budou konfigurovat DNS, měli přístup správce systému (Security officer) s oprávněním ke všem objektům (*ALLOBJ). Při přidělování oprávnění uživatelům použijte produkt iSeries Navigator. Pokud potřebujete další informace, prostudujte si téma **Udělení oprávnění administrátorovi DNS** v online nápovědě k serveru DNS.

Pozn.: Jestliže profil administrátora nemá úplné oprávnění, musí mu být přidělen specifický přístup a oprávnění ke všem adresářům a souvisejícím konfiguračním souborům DNS.

Určení struktury domény

Je důležité určit, jak rozdělíte doménu nebo poddomény do zón tak, aby co nejlépe vyhovovala požadavkům sítě a přístupu na Internet, a jak naplánujete bezpečnostní bariéry. Tyto faktory mohou být složité a musí být řešeny případ od případu. Podrobné návody uvádí například publikace O'Reilly: DNS and BIND.

Pokud nakonfigurujete zónu DNS jako dynamickou zónu, nemůžete do této zóny provádět za chodu serveru ruční změny. Pokud tak učiníte, můžete způsobit rušení příchozích dynamických aktualizací. Je-li nutné provést nějaké ruční aktualizace, zastavte server, proveďte tyto změny a potom server opětně spusťte. Dynamické aktualizace odeslané k zastavenému serveru DNS nebudou nikdy vykonány. Z tohoto důvodu je vhodné nakonfigurovat samostatně dynamickou a statickou zónu. To můžete provést vytvořením zcela samostatných zón nebo definováním nové poddomény, jako např. dynamic.mycompany.com, pro ty klienty, kteří budou spravováni dynamicky.

Server iSeries^(TM) DNS poskytuje grafické rozhraní pro konfiguraci vašich serverů. V některých případech toto rozhraní používá terminologii nebo koncepce, které mohou být v jiných zdrojích reprezentovány odlišně. Jestliže budete při plánování konfigurace vašeho DNS vycházet i z jiných informačních zdrojů, nezapomeňte na tyto skutečnosti:

- Všechny zóny a objekty definované na serveru jsou organizovány v pořadačích **Zóna pro vyhledávání dopředu** a **Zóna pro vyhledávání dozadu**. Zóny pro vyhledávání dopředu jsou zóny, které se používají k mapování jmen domén na IP adresy, jako např. záznamů A. Zóny pro vyhledávání dozadu jsou zóny, které se používají k mapování IP adres na jména domén, jako např. záznamů PTR.
- Server iSeries DNS se odkazuje na **primární zóny** a **sekundární zóny**. Ty jsou často v jiné dokumentaci standardu BIND nazývány hlavní zóny a závislé zóny.
- Rozhraní používá **podzóny**, které jsou v některých zdrojích označovány jako poddomény. Podřízená zóna je podzóna, za níž jste delegovali odpovědnost jednomu nebo více serverům jmen.

Plánování opatření pro zabezpečení dat

Zabezpečení vašeho serveru DNS je životně důležité. Kromě níže uvedených pokynů týkajících se zabezpečení ochrany dat je zabezpečení serverů DNS a iSeries^(TM) popisováno v řadě zdrojů, mimo jiné též v tématu IBM^(R) Secureway: iSeries and the Internet v rámci aplikace Information Center. Zabezpečením ochrany dat vztahujícím se k DNS se také zabývá publikace DNS and BIND.

Seznamy AML

DNS používá seznamy AML (Address Match Lists) k tomu, aby povolila nebo zamítla vnějším entitám přístup k určitým funkcím DNS. Tyto seznamy zahrnují specifické IP adresy, podsítí (za použití předpony IP) nebo použití klíče TSIG (Transaction Signature). V seznamu AML můžete definovat seznam entit, kterým chcete povolit přístup nebo jej zamítnout. Pokud chcete být schopni opětně používat seznam AML, můžete jej uložit jako přístupový seznam (ACL, neboli Access Control List). Kdykoliv potom budete potřebovat tento seznam, můžete jednoduše vyvolat přístupový seznam a celý seznam se zavede.

Pořadí prvků seznamu AML

Použije se první prvek v seznamu AML, který odpovídá dané adrese. Abyste například povolili všechny adresy v síti 10.1.1.x., s výjimkou 10.1.1.5, musí být prvky seznamu AML v tomto pořadí (!10.1.1.5; 10.1.1/24). V takovém případě bude adresa 10.1.1.5 porovnána s prvním prvkem a bude automaticky zamítnuta.

Jestliže by byly prvky obráceně (10.1.1/24; !10.1.1.5), byl by IP adrese 10.1.1.5 povolen přístup. Server byl jí totiž porovnal s prvním prvkem, který by jí odpovídal, a povolil by jí bez kontroly zbylých pravidel.

Volby kontroly přístupu

DNS umožňuje nastavit omezení, jako např. kdo může odesílat dynamické aktualizace k serveru, kdo se smí dotazovat na data a požadovat přenosy zón. Přístupové seznamy (ACL) je možné použít k omezení přístupu k serveru pro tyto volby:

Povolit aktualizaci

Aby váš server DNS mohl akceptovat dynamické aktualizace z jakýchkoliv vnějších zdrojů, musíte aktivovat volbu Povolit aktualizaci.

Povolit dotaz

Specifikuje, které hostitelské systémy mají povoleno dotazovat se serveru. Pokud není specifikováno jinak, je nastavena předvolba povolit dotazy ze všech hostitelských systémů.

Povolit přenos

Specifikuje, které hostitelské systémy mají povoleno přijímat přenosy zón ze serveru. Pokud není specifikováno jinak, je nastavena předvolba povolit přenosy ze všech hostitelských systémů.

Povolit rekurzi

Specifikuje, které hostitelské systémy mají povoleno pokládat rekurzivní dotazy prostřednictvím tohoto serveru. Pokud není specifikováno jinak, je nastavena předvolba povolit rekurzivní dotazy ze všech hostitelských systémů.

Blackhole

Specifikuje seznam adres, od nichž nebude server přijímat dotazy, ani je nebude používat k rozlišení dotazu. Dotazy z těchto adres zůstanou nezodpovězeny.

Systémové požadavky DNS

Volba DNS (Option 31) se neinstaluje automaticky se základním operačním systémem. Instalaci DNS musíte specificky vybrat. Nový server DNS přidaný do verze V5R1 je založen na implementaci, která je známá jako BIND 8 a je průmyslovým standardem. Dřívější služby OS/400^(R) DNS byly založeny na odvětvovém standardu BIND verze 4.9.3 a jsou dosud ve verzi V5R1 k dispozici.

Máte-li již DNS instalován, budete standardně nakonfigurováni pro nastavování jednoho serveru DNS za použití schopností serveru DNS založeného na standardu BIND 4.9.3, které byly k dispozici v předcházejících vydáních. Pokud budete chtít spustit jeden nebo více serverů DNS za použití standardu BIND 8, musíte instalovat volbu PASE (Portable Application Solutions Environment. PASE je produkt SS1 volba 33 (SS1 Option 33). Jakmile je volba PASE instalována, produkt iSeries Navigator automaticky zajistí konfiguraci správné implementace standardu BIND.

Jestliže nepoužíváte volbu PASE, nebudete schopni využívat výhod všech funkcí standardu BIND 8. Přestože nepoužíváte volbu PASE, můžete provozovat tentýž server DNS založený na standardu BIND 4.9.3, který byl k dispozici v předcházejících vydáních. Další informace o produktu BIND 4.9.3 naleznete v tématu V4R5 DNS v rámci aplikace Information Center



(zhruba 357 KB).

Pokud chcete konfigurovat server DHCP na různých serverech iSeries, abyste mohli odesílat aktualizace k tomuto serveru DNS, musí být na serveru DHCP iSeries také nainstalována volba 31. Server DHCP používá programové rozhraní poskytované volbou 31 k provádění dynamické aktualizace.

Chcete-li určit, zda je nainstalován DNS, postupujte podle těchto kroků:

1. Na příkazovou řádku napište **GO LICPGM** a stiskněte klávesu **Enter**.
2. Napište **10** (Display installed licensed programs) a stiskněte **Enter**.
3. Odstráňte dolů na **5722SS1 OS/400 - Domain Name System** (SS1 volba 31).

Je-li DNS úspěšně nainstalován, bude pod **Installed Status** uvedena hodnota ***compatible**, jak je vidět níže:

LicPgm	Installed Status	Description
5722SS1	*COMPATIBLE	OS/400 - Domain Name System

4. Stisknutím klávesy **F3** opusťte obrazovku.

Chcete-li nainstalovat DNS, postupujte podle těchto kroků:

1. Na příkazovou řádku napište **GO LICPGM** a stiskněte klávesu **Enter**.
2. Napište **11** (Install licensed programs) a stiskněte klávesu **Enter**.
3. Napište **1** (Install) do pole **Option** vedle OS/400 - Domain Name System a stiskněte klávesu **Enter**.
4. Opětným stisknutím klávesy **Enter** instalaci potvrďte.

Konfigurace DNS

Dříve, než začnete s konfigurací DNS, si prostudujte Systémové požadavky DNS a nainstalujte nezbytné komponenty DNS. Následující dílčí témata poskytují návod, jak nakonfigurovat server DNS:

Přístup k DNS v prostředí produktu iSeries Navigator

Pokyny pro přístup k DNS v prostředí produktu iSeries Navigator.

Konfigurace serverů jmen

DNS umožňuje vytváření násobných instancí serverů jmen. Toto téma poskytuje návod pro konfiguraci serveru jmen.

Konfigurace DNS pro přijímání dynamických aktualizací

Servery DNS provozující standard BIND 8 mohou být nakonfigurovány tak, aby přijímaly požadavky na dynamickou aktualizaci zónových dat z ostatních zdrojů. Toto téma poskytuje návod, jak nakonfigurovat volbu Povolit aktualizaci tak, aby mohl server DNS přijímat dynamické aktualizace.

Importování souborů DNS

DNS může importovat existující soubory zónových dat. Při efektivním vytváření nové zóny z existujícího konfiguračního souboru postupujte podle uvedených procedur.

Přístup k externím datům DNS

Jestliže vytvoříte zónová data DNS, bude váš server schopen rozlišit dotazy pro tuto zónu. Toto téma vysvětluje, jak nakonfigurovat server DNS, aby rozlišoval dotazy z vnějšího prostředí vaší domény.

Přístup k DNS v produktu iSeries Navigator

Následující instrukce vás povedou ke konfiguračnímu rozhraní DNS v produktu iSeries Navigator. Pokud používáte PASE, budete schopni nakonfigurovat servery DNS založené na odvětvovém standardu BIND 8. I když nepoužíváte volbu PASE, můžete provozovat stejný server DNS založený na standardu BIND 4.9.3, který byl k dispozici v předcházejících vydáních. Další informace o DNS založených na standardu 4.9.3 naleznete v tématu V4R5 DNS v rámci aplikace V4R5 DNS Information Center



(zhruba 62 stran).

Pokud provádíte konfiguraci serveru DNS poprvé, postupujte takto:

1. V prostředí produktu **iSeries Navigator** rozbalte položku **Server iSeries** → **Síť** → **Servery** → **DNS**.
2. Klepněte pravým tlačítkem myši na **DNS** a vyberte položku **Nová konfigurace**.

Máte-li nakonfigurován server DNS verze nižší než V5R1, postupujte takto:

1. V prostředí produktu **iSeries Navigator** rozbalte položku **Server iSeries** → **Síť** → **Servery** → **DNS**.
2. V pravém podokně dvakrát klikněte na server DNS, čímž otevřete okno **Konfigurace DNS**.
3. Pokud používáte volbu PASE, nabídne se vám možnost migrace vaší stávající konfigurace DNS na odvětvový standard BIND 8. Jakmile však jednou přejdete na standard BIND 8, nebudete se moci vrátit na BIND 4.9.3. Pokud si nejste jisti, vyberte **Ne**. Chcete-li provést migraci, označte **Ano**.

4. Pokud budete chtít kdykoliv provést migraci vašeho serveru DNS na standard BIND 8, klepněte pravým tlačítkem myši na **DNS** v levém podokně a vyberte volbu **Migrace na verzi 8**.

Konfigurace serverů jmen

Server iSeries^(TM) DNS založený na odvětveném standardu BIND 8 podporuje několik instancí serveru jmen. Níže uváděné úlohy vás provedou procesem vytvoření jedné instance serveru jmen, včetně jejích vlastností a zón.

1. Vytvoření instance serveru jmen
K definování instance serveru DNS použijte **průvodce novou konfigurací DNS**.
2. Editování vlastností serveru DNS
Definujte globální vlastnosti nové instance serveru.
3. Konfigurace zón na serveru jmen
Vytvořte zóny a zónová data, abyste váš server jmen zaplnili.

Pokud chcete vytvářet násobné instance, opakujte výše uvedený postup, dokud nevytvoříte všechny požadované instance. Pro každou instanci serveru jmen můžete specifikovat nezávislé vlastnosti, jako např. úroveň ladění (debug levels) a hodnoty automatického spuštění (autostart). Jestliže vytváříte novou instanci, vytvářejí se samostatné konfigurační soubory. Další informace o konfiguračních souborech uvádí téma Údržba konfiguračních souborů DNS.

Vytvoření instance serveru jmen

Chcete-li spustit **průvodce novou konfigurací DNS**, postupujte takto:

1. V prostředí produktu **iSeries Navigator** rozbalte **Server iSeries^(TM)** → **Síť** → **Servery** → **DNS**.
2. V levém podokně klepněte pravým tlačítkem myši na **DNS** a vyberte položku **Nový server jmen...**
3. Průvodce vás provede procesem konfigurace.

Průvodce bude požadovat následující vstupní údaje:

Jméno serveru DNS: Zadejte jméno vašeho serveru DNS. Může být až 5 znaků dlouhé a musí začínat abecedním znakem. Pokud vytváříte několik serverů, musí mít každý z nich jedinečné jméno. Toto jméno je v ostatních oblastech systému označováno jako jméno "instance" serveru DNS.

IP adresy pro naslouchání: Dva servery DNS nemohou naslouchat na stejné IP adrese. Předvolené nastavení je naslouchat na VŠECH IP adresách. Pokud vytváříte dodatečné instance serverů, nesmí být žádný z nich nakonfigurován tak, aby naslouchal VŠEM IP adresám. Pro každý server musíte specifikovat IP adresy.

Kořenové servery: Můžete zavést seznam předvolených internetových kořenových serverů nebo specifikovat své vlastní kořenové servery, jako např. interní kořenové servery pro intranet.

Pozn.: O zavádění předvolených internetových kořenových serverů byste měli uvažovat pouze v tom případě, pokud jste připojeni k Internetu a očekáváte, že váš server DNS bude schopen plně rozlišovat internetová jména.

Spuštění serveru: Můžete zadat, zda se má server spustit automaticky při spuštění TCP/IP. Pokud obsluhujete několik serverů, mohou být jednotlivé instance spouštěny a ukončovány nezávisle na sobě.

Následující téma: Editování vlastností serveru DNS.

Editování vlastností serveru DNS

Poté, co vytvoříte server jmen, můžete editovat vlastnosti, jako např. povolení aktualizace a úroveň ladění. Tyto volby se budou týkat pouze té serverové instance, kterou měníte. Chcete-li upravovat vlastnosti instance serveru DNS, postupujte podle těchto kroků:

1. V prostředí produktu **iSeries Navigator** rozbalte **Server iSeries^(TM)** → **Síť** → **Servery** → **DNS**.

2. V pravém podokně klepněte pravým tlačítkem myši na **server DNS** a vyberte položku **Konfigurace**.
3. Klepněte pravým tlačítkem myši na **Server DNS** a vyberte položku **Vlastnosti**.

Následující téma: Konfigurování zón na serveru jmen.

Konfigurace zón na serveru jmen

Po vytvoření serveru jmen se vraťte do hlavního okna produktu **iSeries Navigator**. Váš server se bude zobrazovat v pravém podokně. Chcete-li na serveru konfigurovat zóny, klepněte pravým tlačítkem myši na jméno serveru a vyberte položku **Konfigurace**. Objeví se okno **Konfigurace DNS**.

Všechny zóny se konfigurují pomocí průvodců. Klepnutím pravým tlačítkem myši na odpovídající pořadač vytvoříte **Zóny pro vyhledávání dopředu** nebo **Zóny pro vyhledávání dozadu**. Zobrazí se volby pro daný typ zóny. Tím, že vyberete typ zóny, kterou chcete vytvořit, spustíte průvodce.

Popis typů objektů, které můžete vytvořit v DNS V5R1, uvádí téma **Co je to DNS**.

Po nakonfigurování zón můžete najít další informace o konfiguraci v těchto tématech:

Konfigurace zóny pro přijímání dynamických aktualizací

Dynamická aktualizace umožňuje autorizovaným zdrojům odesílat zdrojové záznamy, aby se aktualizovala zónová data. Může se tak snížit potřeba ručních změn zónových dat.

Import zónových dat

Pokud máte existující soubor zónových dat z jiného serveru DNS, můžete jej přenést na váš nový server.

Přístup k externím datům DNS

Váš server je možné nakonfigurovat tak, aby rozlišoval dotazy týkající se informací mimo rámec zónových dat, která obsahuje. Dotazy lze přeměrovat na jiné spolehlivé servery nebo jako pomoc při rozlišování dotazů zavést kořenové servery.

Konfigurace DNS pro přijímání dynamických aktualizací

Při vytváření dynamických zón byste měli zvážit strukturu vaší sítě. Pokud části vaší domény stále vyžadují ruční aktualizace, mohli byste uvažovat o nastavení samostatné statické a dynamické zóny. Jestliže musíte provádět ruční aktualizace do dynamické zóny, musíte zastavit server dynamické zóny a opět jej spustit poté, co dokončíte aktualizace. Zastavení serveru si vynutí synchronizaci všech dynamických aktualizací, které byly provedeny, jelikož server zavedl svá zónová data ze zónové databáze. Pokud server nezastavíte, přijmete o všechny dynamické aktualizace, které byly zpracovány od doby jeho spuštění. Zastavení serveru za účelem provedení ručních aktualizací znamená, že ztratíte aktualizace, které byly odeslány, zatímco byl server vypnut.

DNS indikuje, že je zóna dynamická, když jsou v příkazu Povolit aktualizaci definovány nějaké objekty. Chcete-li konfigurovat volbu Povolit aktualizaci, postupujte takto:

1. V prostředí produktu **iSeries Navigator** rozbalte položku **Server iSeries** → **Síť** → **Servery** → **DNS**.
2. V pravém podokně klepněte pravým tlačítkem myši na **server DNS** a vyberte položku **Konfigurace**.
3. V okně **Konfigurace DNS** rozbalte položku **Zóna pro vyhledávání dopředu** nebo **Zóna pro vyhledávání dozadu**.
4. Klepněte pravým tlačítkem myši na primární zónu, kterou chcete editovat, a vyberte položku **Vlastnosti**.
5. Na stránce **Vlastnosti primární zóny** klepněte na ouško **Volby**.
6. Na stránce **Volby** rozbalte položku **Kontrola přístupu** → **Povolit aktualizaci**.
7. DNS používá seznam AML k ověření autorizovaných aktualizací. Chcete-li přidat nějaký objekt do seznamu AML, vyberte typ položky Seznam AML a klepněte na **Přidat...** Můžete přidat IP adresu, IP předponu, přístupový seznam (ACL) nebo klíč.

8. Poté, co jste dokončili aktualizaci seznamu AML, klepněte na **OK**, čímž zavřete stránku **Volby**.

Pokud konfiguruje server DNS pro přijímání dynamických aktualizací ze serveru iSeries DHCP, další informace najdete v tématu Konfigurace DHCP pro odesílání dynamických aktualizací.

Import souborů DNS

Primární zónu můžete vytvořit tak, že naimportujete soubor zónových dat nebo že provedete konverzi existujících hostitelských tabulek. Chcete-li vytvořit data zóny z tabulky hostitelského serveru, prostudujte si, prosím, téma *Converting host tables* v rámci aplikace V4R5 DNS Information Center



(zhruba 357 KB).

Můžete importovat libovolný soubor, pokud se jedná o platný konfigurační soubor zónových dat založený na syntaxi odvětvového standardu BIND. Tento soubor by měl být umístěn v adresáři IFS. Po naimportování DNS ověří, zda se jedná o platný soubor zónových dat, a přidá jej do souboru NAMED.CONF pro tuto instanci serveru.

Chcete-li importovat zónový soubor, postupujte takto:

1. V prostředí produktu **iSeries Navigator** rozbalte **Server iSeriesTM** → **Síť** → **Servery** → **DNS**.
2. V pravém podokně klepněte dvakrát na instanci serveru DNS, do které chcete importovat zónu.
3. V levém podokně klepněte pravým tlačítkem myši na **Server DNS** a vyberte položku **Zóna pro import**.
4. Při importu primární zóny se řiďte pokyny průvodce.

Ověření záznamů

Funkce Import dat domény čte a ověřuje každý záznam, který je importován. Po dokončení funkce Import dat mohou být všechny chybné záznamy prověřeny jednotlivě na stránce vlastností pro **Ostatní záznamy** importované zóny.

- **Pozn.:**
- Importování velké primární domény může trvat i několik minut.
- Funkce pro importování dat domény nepodporuje direktivu \$include. Proces ověřování platnosti dat domény při jejich importu identifikuje řádky, které obsahují direktivu \$include, jako chybné.

Přístup k externím datům DNS

Kořenové servery jsou životně důležité pro funkci serveru DNS, který je přímo připojen k Internetu nebo k rozsáhlé vnitropodnikové síti. Servery DNS musí používat kořenové servery k odpovídání na dotazy o hostitelských systémech, které nejsou obsaženy v jejich vlastních souborech domén.

Aby dosáhl na více informací, musí server DNS vědět, kam se má podívat. Na Internetu jsou prvním místem, kam se server DNS dívá, kořenové servery. Kořenové servery směřují server DNS k ostatním serverům v hierarchii, dokud není nalezena odpověď nebo dokud se nezjistí, že odpověď neexistuje.

Předvolený seznam kořenových serverů produktu iSeriesTM Navigator

Internetové kořenové servery byste měli používat pouze tehdy, pokud máte připojení k Internetu a chcete rozlišovat jména na Internetu v případě, že nejsou rozlišena vaším serverem DNS. Produkt iSeries Navigator poskytuje předvolený seznam internetových kořenových serverů. Seznam je aktuální, když je uvolněn produkt iSeries Navigator. Můžete si ověřit, zda je předvolený seznam aktuální. To učiníte tak, že jej porovnáte se seznamem na stránce společnosti InterNIC. Aktualizujte svůj konfigurační seznam kořenových serverů, abyste jej uchovali aktuální.

Kde získáte adresy internetových kořenových serverů

Adresy kořenových serverů nejvyšší úrovně se čas od času mění a je v odpovědnosti administrátora DNS,

aby je uchoval aktuální. InterNIC udržuje aktuální seznam adres internetových kořenových serverů. Chcete-li získat aktuální seznam internetových kořenových serverů, postupujte takto:

1. Anonymní FTP k serveru InterNIC: FTP.RS.INTERNIC.NET.
2. Stáhněte tento soubor: /domain/named.root.
3. Uložte soubor do adresáře: Integrated File System/Root/QIBM/ProdData/OS400/DNS/ROOT.FILE.

Server DNS za ochrannou bariérou nesmí mít definovány žádné kořenové servery. V tomto případě je server DNS schopen rozlišovat pouze dotazy od položek, které existují v jeho vlastních databázových souborech primární domény nebo v jeho rychlé vyrovnávací paměti. Externí dotazy může přeměňovat na ochrannou bariéru DNS (firewall). V tomto případě působí ochranná bariéra DNS jako přeměňovač.

Intranetové kořenové servery

Pokud je váš server DNS částí rozsáhlé vnitropodnikové sítě, můžete mít interní kořenové servery. Jestliže váš DNS server nemá přístup k Internetu, nepotřebujete si zavádět předvolené internetové servery. Měli byste ovšem přidat interní kořenové servery, aby váš server DNS mohl rozlišovat interní adresy mimo rámec své domény.

Správa serveru DNS

Poté, co jste nakonfigurovali DNS, prostudujte si níže uvedená témata:

Ověření funkčnosti DNS pomocí funkce NSLookup

Funkci NSLookup můžete použít k ověření toho, zda DNS pracuje.

Správa bezpečnostních klíčů

Bezpečnostní klíče umožňují omezit přístup k datům vašeho serveru DNS.

Statistika serveru DNS

Nástroje pro výpis databáze a statistiky vám mohou pomoci revidovat a spravovat výkon serveru.

Údržba konfiguračních souborů DNS

Porozumějte tomu, jaké soubory DNS používá, a prostudujte návod pro jejich zálohování a údržbu.

Rozšířené funkce DNS

Toto téma popisuje, jak mohou zkušení administrátoři pracovat s rozšířenými funkcemi.

Ověření funkčnosti DNS pomocí funkce NSLookup

Pomocí funkce NSLookup (Name Server Lookup) se dotážete serveru DNS na nějakou IP adresu. Tím ověříte, že server DNS odpovídá na dotazy. Požadujte hostitelské jméno, které je asociované s IP adresou pro smyčkový test (127.0.0.1). Odpovědí by mělo být hostitelské jméno (localhost). Rovněž byste se měli dotazovat na specifická jména definována v instanci serveru, kterou se pokoušíte ověřit. To vám potvrdí, že specifická instance serveru, kterou testujete, funguje správně.

Chcete-li ověřit fungování DNS pomocí funkce NSLookup, postupujte takto:

1. Na příkazovou řádku napište NSLOOKUP DMNNAMSVR(n.n.n.n), kde n.n.n.n je adresa, které má naslouchat vámi nakonfigurovaná testovaná instance serveru.
2. Na příkazovou řádku napište NSLOOKUP a stiskněte klávesu **Enter**. Tím se spustí dotazovací relace NSLookup.
3. Napište server, za toto slovo napište jméno vašeho serveru a stiskněte klávesu **Enter**. Například: server myiseries.mycompany.com.

Měly by se zobrazit tyto informace:

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

Kde n.n.n.n představuje IP adresu vašeho serveru DNS.

4. Na příkazovou řádku napište 127.0.0.1 a stiskněte klávesu **Enter**.

Měly by se zobrazit níže uvedené informace včetně hostitelského jména pro smyčkový test:

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

```
Name:    localhost
Address: 127.0.0.1
```

Server DNS odpovídá správně, pokud vrací jako hostitelské jméno pro smyčkový test: **localhost**.

5. Terminálovou relaci funkce NSLOOKUP ukončete napsáním exit a stisknutím klávesy **Enter**.

Pozn.: Pokud potřebujete pomoc při použití funkce NSLookup, napište ? a stiskněte klávesu **Enter**.

Správa bezpečnostních klíčů

Existují dva typy klíčů, které se vztahují k DNS. Každý z nich hraje odlišnou roli v zabezpečení konfigurace vašeho DNS. Následující popis vysvětluje, jak každý z nich souvisí se serverem DNS.

Klíče DNS

Klíč DNS je klíč definovaný pro standard BIND. Je používán serverem DNS jako část verifikace příchozí aktualizace. Klíč můžete konfigurovat a přiřadit mu jméno. Potom, když chcete chránit nějaký objekt DNS, např. dynamickou zónu, můžete specifikovat tento klíč v seznamu AML.

Při správě klíčů DNS postupujte takto:

1. V prostředí produktu **iSeries Navigator** rozbalte **Server iSeries^(TM)** → **Síť** → **Servery** → **DNS**.
2. V pravém podokně klepněte pravým tlačítkem myši na instanci serveru DNS, kterou chcete otevřít, a vyberte položku **Konfigurace**.
3. V okně **Konfigurace DNS** vyberte položku **Soubor > Správa klíčů...**

Klíče pro dynamickou aktualizaci

Klíče pro dynamickou aktualizaci se používají k zabezpečení dynamických aktualizací u serveru DHCP. Tyto klíče musí být přítomny, pokud jsou servery DNS a DHCP na jednom serveru iSeries. Jestliže je DHCP na jiném serveru iSeries, musíte vytvořit klíč pro dynamickou aktualizaci na každém serveru iSeries, abyste umožnili dynamické aktualizace.

Při správě klíčů pro dynamickou aktualizaci postupujte takto:

1. V prostředí produktu **iSeries Navigator** rozbalte položku **Server iSeries** → **Síť** → **Servery** → **DNS**.
2. Klepněte pravým tlačítkem myši na **DNS** a vyberte položku **Správa klíčů pro dynamickou aktualizaci...**

Statistika serveru DNS

DNS poskytuje několik diagnostických nástrojů, které mohou být využity k monitorování výkonu vašeho serveru.

Statistika serveru

DNS umožňuje prohlížení statistiky pro instanci serveru. Tato statistika sumarizuje počet dotazů a odpovědí, které server obdržel od posledního opětovného spuštění nebo od opětovného zavedení databáze. Informace se průběžně přidávají na konec tohoto souboru, dokud soubor nevymažete. Tyto informace mohou být užitečné při vyhodnocování provozu, který server přijímá, a při vyhledávání problémů. Další informace o statistice serveru získáte v tématu online nápovědy k serveru DNS **Statistika serveru DNS**.

Chcete-li získat přístup ke statistice serveru, postupujte takto:

1. V prostředí produktu **iSeries Navigator** rozbalte **Server iSeries^(TM)** → **Síť** → **Servery** → **DNS**.
2. V pravém podokně klepněte pravým tlačítkem myši na **server DNS** a vyberte položku **Konfigurace**.
3. V okně **Konfigurace DNS** vyberte položku **Zobrazit** → **Statistika serveru**.

Databáze aktivního serveru

DNS umožňuje prohlížení výpisu spolehlivých (authoritative) dat, dat rychlé vyrovnávací paměti a dat zóny hint pro instanci serveru. Výpis zahrnuje informace ze všech primárních a sekundárních zón serveru (pro vyhledávání dopředu i pro vyhledávání dozadu), stejně jako informace, které server získal z dotazů. Databáze obsahuje informace o zónách a hostitelských systémech, včetně některých vlastností zóny, jakými jsou například informace SOA (start of authority) a vlastnosti hostitelského systému, včetně informací výměníku pošty (MX). Tyto informace mohou být užitečné při vyhledávání problémů.

Výpis databáze aktivního serveru si můžete prohlížet pomocí produktu Operations Navigator. Jestliže potřebujete uložit kopii souborů, je jméno souboru s výpisem databáze NAMED_DUMP.DB v adresářové cestě serveru iSeries: **Integrated File System/Root/QIBM/UserData/OS400/DNS/<instance_server>**, kde "<instance_server>" je jméno instance serveru DNS. Další informace o databázi aktivního serveru získáte v tématu online nápovědy k serveru DNS **Výpis databáze serveru DNS**.

Chcete-li získat přístup k výpisu databáze aktivního serveru, postupujte takto:

1. V prostředí produktu **iSeries Navigator** rozbalte položku **Server iSeries** → **Síť** → **Servery** → **DNS**.
2. V pravém podokně klepněte pravým tlačítkem myši na **server DNS** a vyberte položku **Konfigurace**.
3. V okně **Konfigurace DNS** vyberte položku **Zobrazit** → **Databáze aktivního serveru**.

Údržba konfiguračních souborů DNS

K vytvoření a údržbě instancí serveru DNS na serveru iSeries^(TM) můžete použít server OS/400^(R) DNS. Konfigurační soubory pro DNS jsou spravovány produktem iSeries Navigator. Tyto soubory byste neměli editovat ručně. Při vytváření, změnách nebo výmazu konfiguračních souborů DNS používejte vždy produkt iSeries Navigator. Konfigurační soubory DNS jsou uloženy v níže uvedených cestách integrovaného systému souborů.

Pozn.: Struktura níže uvedeného souboru se týká serveru DNS, který je provozován na BIND 8. Pokud používáte server DNS založený na BIND 4.9.3, prostudujte si prosím část *Backing up DNS configuration files and maintaining log files* v rámci aplikace V4R5 DNS Information Center



(zhruba 62 stran).


V níže uvedené tabulce jsou soubory uvedeny v zobrazené hierarchii cest. Soubory s ikonou uložení


















by měly být za účelem ochrany dat zálohovány. Soubory s ikonou výmazu



by měly být pravidelně vymazávány.

Jméno		Popis
QIBM/UserData/OS400/DNS/		Adresář výchozího bodu pro DNS.
ATRIBUTY		DNS používá tento soubor k určení toho používané verze odvětvového standardu BIND.
QIBM/UserData/OS400/DNS/<instance-n>/		Adresář výchozího bodu pro instanci serveru DNS.

Jméno		Popis
ATRIBUTY		Konfigurační atributy používané serverem iSeries DNS.
NAMED.CONF		Tento soubor obsahuje konfigurační data. Používá se k tomu, aby sdělil serveru, jaké specifické zóny spravuje, kde jsou soubory zón, které zóny mohou být dynamicky aktualizovány, kde jsou přesměrovací servery, a další nastavení voleb.
BOOT.AS400BIND4		Soubor pro metodiku a konfiguraci serveru BIND 4.9.3, který je konvertován na soubor BIND 8 NAMED.CONF pro tuto instanci. Tento soubor se vytváří při migraci serveru BIND 4.9.3 na BIND 8. Slouží jako záloha migrace a může být vymazán, pokud server BIND 8 pracuje správně.
NAMED.CA		Seznam kořenových serverů pro tuto instanci.
NAMED_DUMP.DB		Výpis dat serveru vytvořený pro databázi aktivního serveru.
NAMED.STATS		Statistika serveru.
NAMED.PID		Udržuje ID procesu běžícího serveru. Tento soubor se vytváří pokaždé, když je server DNS spuštěn. Používá se pro funkce serveru Databáze, Statistika a Aktualizace. Tento soubor nemažte ani neupravujte.
QUERYLOG		Protokol přijatých dotazů serveru DNS. Tento soubor se vytváří, pokud je aktivní protokol serveru DNS. Je-li aktivní, neustále se zvětšuje a měl by být pravidelně vymazáván.
<zone-name-a>.DB		Soubor zóny pro konkrétní doménu, která má být obsluhována daným serverem. Obsahuje všechny zdrojové záznamy pro tuto zónu.
<zone-name-b>.DB		Soubor zóny pro konkrétní doménu, která má být obsluhována daným serverem. Obsahuje všechny zdrojové záznamy pro tuto zónu. Každá zóna má samostatný soubor .DB.

Jméno		Popis
.ixfr.		Soubory přenosu IXFR. Tyto soubory používají sekundární servery k zavádění pouze změněných dat od posledního přenosu zóny. Jak jsou prováděny aktualizace, počet souborů IXFR bude narůstat. Měli byste pravidelně vymazávat starší soubory IXFR. Uchování souborů, které byly vytvořeny v rámci jednoho nebo dvou dní umožní většině sekundárních serverů, aby si zavedly přenosy IXFR. Pokud vymažete všechny tyto soubory, bude sekundární server vyžadovat úplný přenos (AXFR).
TMP		Adresář používaný instancí serveru pro vytváření dočasných pracovních souborů.
QIBM/UserData/OS400/DNS/TMP		Dočasný adresář používaný programem QTOBH2N k vytváření přechodných souborů vypsanych z hostitelské tabulky pro pozdější import pomocí produktu Operations Navigator.
QIBM/UserData/OS400/DNS/_DYN/		Adresář, který uchovává soubory požadované pro dynamickou aktualizaci.
<key_id-name-x>._KID		Soubor obsahující klíčový povel BIND 8 pro id_klíče označené <key_id-name-x>.
<key_id-name-x>._DUK.<zone-name-a>		Klíč pro dynamickou aktualizaci požadovaný k inicializaci požadavku na dynamickou aktualizaci v zóně <zone-name-a> pomocí klíče <key_id-name-x>.
<key_id-name-y>._KID		Soubor obsahující klíčový povel BIND 8 pro id_klíče označené <key_id-name-y>.
<key_id-name-y>._DUK.<zone-name-a>		Klíč pro dynamickou aktualizaci požadovaný k inicializaci požadavku na dynamickou aktualizaci v zóně <zone-name-a> pomocí klíče <key_id-name-y>.
<key_id-name-y>._DUK.<zone-name-b>		Klíč pro dynamickou aktualizaci požadovaný k inicializaci požadavku na dynamickou aktualizaci v zóně <zone-name-b> pomocí klíče <key_id-name-y>.

Rozšířené funkce DNS

DNS v produktu iSeries Navigator poskytuje rozhraní pro konfiguraci a správu vašeho serveru DNS. Níže uváděné úlohy představují zkrácený výběr příkazů pro administrátory, kteří mají zkušenosti s grafickým rozhraním serveru iSeries. Nabízejí rychlé metody pro změnu stavu serveru a atributů několika instancí serveru najednou.

Změna atributů DNS

Rozhraní DNS neumožňuje měnit atributy Autostart (automatické spuštění) a Debug levels (úroveň ladění) u všech instancí serveru najednou. Ke změně tohoto nastavení u jednotlivých instancí serveru DNS nebo u všech instancí najednou můžete použít znakově orientované rozhraní. Následujícími kroky použijte příkaz CHGDNSA:

1. Na příkazovou řádku napište CHGDNSA a stiskněte klávesu **F4**.
2. Na stránce Change DNS Server Attributes (CHGDNSA) napište jméno jedné instance serveru nebo hodnotu *ALL a stiskněte klávesu **Enter**.
Zobrazí se dostupné volby atributů serveru:
Autostart server *SAME *YES, *NO, *SAME
Debug level *SAME 0-11, *SAME, *DFT
3. **Autostart** - Chcete-li zadat, aby se vybrané servery DNS automaticky spustily při spuštění TCP/IP, napište *YES. Pokud nechcete, aby se server spustil při spuštění TCP/IP, napište *NO. Jestliže chcete ponechat tento atribut na jeho aktuálním nastavení, napište *SAME.
Debug level - Pokud chcete změnit úroveň ladění, kterou by měly vybrané servery používat, napište hodnotu v rozmezí od 0 do 11. Chcete-li specifikovat, že by úroveň ladění měla zdědit hodnotu ladění při spuštění serveru, napište *DFT. Jestliže chcete ponechat tento atribut na jeho aktuálním nastavení, napište *SAME.
Po zadání všech preferovaných hodnot stiskněte klávesu **Enter**, aby se atributy DNS nastavily.

Spuštění nebo zastavení serverů DNS

Rozhraní DNS neumožňuje spouštět nebo zastavovat několik instancí serveru najednou. Ke změně tohoto nastavení u všech instancí najednou můžete použít znakově orientované rozhraní. Chcete-li použít znakově orientované rozhraní ke spuštění všech instancí serveru DNS najednou, napište na příkazovou řádku STRTCPSVR SERVER(*DNS) DNSSVR(*ALL). Pokud chcete najednou zastavit všechny servery DNS, napište na příkazovou řádku ENDTCPSPVR SERVER(*DNS) DNSSVR(*ALL).

Změna hodnot ladění

DNS v rozhraní produktu iSeries Navigator neumožňuje měnit úroveň ladění, zatímco je server spuštěn. Ke změně úrovně ladění za běhu serveru však můžete použít znakově orientované rozhraní. Tato funkce může být užitečná pro administrátory, kteří spravují rozsáhlé zóny a kteří nechtějí mít velké objemy ladicích dat, vznikajících při prvním spuštění serveru a zavedení všech zónových dat. Jestliže chcete změnit úroveň ladění pomocí znakově orientovaného rozhraní, postupujte podle níže uvedených kroků a výraz <instance> nahraďte jménem instance serveru:

1. Na příkazovou řádku napište ADDLIBILE QDNS a stiskněte klávesu **Enter**.
2. Změňte úroveň ladění:
 - Pokud chcete ladění zapnout nebo zvýšit úroveň ladění o 1, napište CALL QTOBDRVS ('BUMP' '<instance>') a stiskněte klávesu **Enter**.
 - Pokud chcete ladění vypnout, napište CALL QTOBDRVS ('OFF' '<instance>') a stiskněte klávesu **Enter**.

Odstraňování problémů s DNS

DNS pracuje téměř stejně jako ostatní funkce a aplikace TCP/IP. Podobně jako aplikace SMTP nebo FTP pracují úlohy DNS v podsystému QSYSWRK a vytvářejí pod uživatelským profilem QTCP protokoly úloh, které obsahují informace vztahující se k úlohám DNS. Jestliže se úloha DNS předčasně ukončí, můžete použít tyto protokoly úloh k určení příčiny poruchy. Pokud server DNS nevrací očekávané odpovědi, mohou protokoly úloh obsahovat informace, které vám mohou pomoci s analýzou problému.

Konfigurace DNS je tvořena několika soubory, z nichž každý obsahuje odlišný typ záznamů. Problémy se serverem DNS jsou obecně způsobeny nesprávnými položkami v konfiguračních souborech DNS. V případě, že dojde k problému, ověřte, že konfigurační soubory DNS obsahují položky, které očekáváte.

Vytváření protokolů

DNS poskytuje množství voleb pro vytváření protokolů, které si můžete při hledání příčiny problému přizpůsobit. Vytváření protokolů poskytuje flexibilitu, neboť nabízí různé úrovně závažnosti, různé kategorie zpráv a výstupní soubory. Tak si můžete jemně vyladit vytváření protokolů, abyste byli schopni nalézt problém.

Nastavení ladění

DNS nabízí 12 úrovní řízení ladění. Vytváření protokolů obvykle představuje jednodušší metodu pro vyhledání příčiny problému, avšak v některých případech je ladění nezbytné. V normálních podmínkách je ladění vypnuto (hodnota = 0).

Další zdroje informací o odstraňování problémů

Obecné informace týkající se odstraňování problémů z DNS jsou k dispozici v mnoha dalších zdrojích. Jedním z nich je kniha O'Reilly: DNS and BIND. Odkazy na diskusní skupiny pro administrátory DNS nabízí zdrojový adresář DNS.

Identifikace úloh

Pokud studujete protokol úlohy kvůli ověření funkčnosti serveru DNS (například za použití příkazu WRKACTJOB) prostudujte si následující pokyny týkající se pojmenování:

- Jestliže používáte standard BIND 4.9.3, bude jméno úlohy serveru QTOBDNS. Další informace o ladění serveru DNS 4.9.3 naleznete v části *Troubleshooting DNS servers* pod tématem V4R5 DNS v rámci aplikace Information Center



(zhruba 357 KB).

- V případě, že provozujete servery založené na standardu BIND 8, budete mít samostatnou úlohu pro každou spouštěnou instanci serveru. Jméno úlohy je tvořeno pěti pevnými znaky (QTOBD), za nimiž následuje jméno instance. Máte-li například dvě instance, INST1 a INST2, budou jména jejich úloh QTOBDINST1 a QTOBDINST2.

Vytváření protokolů serveru DNS

Odvětvový standard BIND 8 nabízí několik nových voleb pro vytváření protokolů (protokolování). Můžete specifikovat, jaký typ zpráv bude zapisován do protokolu, kam se každá zpráva odesílá a jak závažné zprávy se do protokolu zapisují. Obecně předvolené nastavení vytváření protokolů vyhovuje. Pokud je však budete chtít změnit, doporučujeme, abyste si prostudovali další zdroje dokumentace BIND 8, které uvádějí více informací o vytváření protokolů.

Protokolovací kanály

Server DNS může zapisovat zprávy do rozdílných výstupních kanálů. Kanály specifikují, kam jsou protokolovaná data odesílána. Můžete si vybrat z těchto typů kanálů:

• Kanály File Channels

Zprávy, které jsou protokolovány do kanálů File channels, jsou odesílány do souboru. Předvolené kanály File channels jsou as400_debug a as400_QPRINT. Standardně jsou ladící zprávy protokolovány do kanálu as400_debug, kterým je soubor NAMED.RUN. Můžete ale zadat, aby se do tohoto souboru odesílaly také ostatní kategorie zpráv. Kategorie zpráv protokolovaných v as400_QPRINT jsou odesílány do souboru pro souběžný tisk QPRINT pro uživatelský profil QTCP. Kromě poskytovaných kanálů si můžete vytvořit navíc své vlastní kanály tohoto typu.

• Kanály Syslog Channels

Zprávy protokolované do tohoto kanálu jsou odesílány do protokolu úlohy serveru. Předvolený kanál Syslog channel je as400_joblog. Protokolované zprávy směřované k tomuto kanálu jsou odesílány do protokolu úlohy instance serveru DNS.

• Kanály Null Channels

Všechny zprávy předávané do kanálů Null channels budou vymazány. Předvolený kanál Null channel je as400_null. Ke kanálu Null channel můžete směřovat kategorie zpráv, pokud se určité zprávy nemají objevovat v žádném souboru protokolu.

Kategorie zpráv

Zprávy jsou seskupeny do kategorií. Můžete specifikovat, jaké kategorie zpráv by měly být protokolovány v každém kanálu. Existuje mnoho kategorií, mezi které patří například:

- config: zpracování konfiguračních souborů
- db: databázové operace
- queries: generování krátkých zpráv protokolu pro každý dotaz, který obdrží server
- lame-servers: detekce špatného delegování
- update: dynamická aktualizace
- xfer-in: přenosy zóny, které server přijímá
- xfer-out: přenosy zóny, které server odesílá

Soubor protokolu se neustále zvětšuje a měl by být pravidelně vymazáván. Obsah všech souborů protokolu serveru DNS se vymaže, když je server DNS zastaven a spuštěn.

Závažnost zpráv

Kanály vám umožňují filtrování podle závažnosti zpráv. U každého kanálu můžete zadat úroveň závažnosti, pro kterou je zpráva protokolována. K dispozici jsou tyto úrovně závažnosti:

- critical (kritické)
- error (chyba)
- warning (varování)
- notice (upozornění)
- info (informace)
- debug (ladění - specifikuje úroveň ladění 0-11)
- dynamic (zdědí úroveň ladění spuštění serveru)

Do protokolu budou zapisovány všechny zprávy vybrané závažnosti a všech úrovní, které jsou ve výše uvedeném přehledu nad touto závažností. Pokud například vyberete Warning, budou do kanálu protokolovány zprávy Warning, Error a Critical. Jestliže vyberete Debug level, můžete specifikovat hodnotu od 0 do 11, pro níž chcete, aby byly ladící zprávy zapisovány do protokolu.

Změna nastavení vytváření protokolů

Chcete-li získat přístup k volbám vytváření protokolů, postupujte takto:

1. V prostředí produktu **iSeries Navigator** rozbalte **Server iSeries^(TM)** → **Síť** → **Servery** → **DNS**.
2. V pravém podokně klepněte pravým tlačítkem myši na **server DNS** a vyberte položku **Konfigurace**.
3. V okně **Konfigurace DNS** klepněte pravým tlačítkem myši na **Server DNS** a vyberte **Vlastnosti**.
4. V okně **Vlastnosti serveru** vyberte ouško **Kanály**, abyste vytvořili nové kanály typu File Channels nebo vlastnosti kanálu, jako je např. závažnost zpráv zapisovaných do protokolu pro každý kanál.
5. V okně **Vlastnosti serveru** vyberte ouško **Protokolování**, abyste mohli specifikovat, jaké kategorie budou protokolovány do každého kanálu.

Rada pro odstraňování problémů

Předvolená úroveň závažnosti kanálu as400_joblog je nastavená na hodnotu Error. Toto nastavení se používá k tomu, aby se snížil objem informačních zpráv a varování, které by mohly snížit výkon. V případě, že jste zaznamenali problémy, ale protokol úlohy neindikuje zdroj těchto problémů, musíte změnit úroveň závažnosti. Při přístupu ke stránce Kanály postupujte podle výše uvedených pokynů a změňte úroveň závažnosti pro kanál as400_joblog na Warning, Notice nebo Info, abyste si mohli zobrazit více dat zapisovaných do protokolu. Poté, co problém vyřešíte, nastavte opět úroveň závažnosti na původní hodnotu Error, čímž snížíte množství zpráv v protokolu úlohy.

Nastavení ladění DNS

Funkce ladění DNS může poskytovat informace, které vám mohou pomoci určit a opravit závady serveru DNS. Doporučuje se, abyste při pokusu o odstranění závad nejdříve použili protokoly.

Platné úrovně ladění jsou 0 až 11. Váš servisní zástupce IBM vám pomůže určit odpovídající hodnotu ladění pro diagnostikování vašeho problému se serverem DNS. Hodnoty 1 nebo vyšší zapisují ladicí informace do souboru NAMED.RUN na cestě k adresáři vašeho serveru iSeries: **Integrated File System/Root/QIBM/UserData/OS400/DNS/<instance_serveru>**, kde "<instance_serveru>" je jméno instance serveru DNS. Pokud je úroveň ladění nastavena na hodnotu 1 nebo vyšší a jestliže server DNS pokračuje v práci, soubor NAMED.RUN neustále narůstá. Doporučujeme vám tento soubor čas od času vymazat, aby nezabíral příliš mnoho místa na disku. Ke specifikaci preferencí pro maximální velikost a počet verzí souboru NAMED.RUN také můžete použít stránku **Vlastnosti serveru - Kanály**.

Chcete-li změnit hodnoty ladění pro instanci serveru DNS, postupujte podle těchto kroků:

1. V prostředí produktu **iSeries Navigator** rozbalte položku **Server iSeries** → **Síť** → **Servery** → **DNS**.
2. V pravém podokně klepněte pravým tlačítkem myši na **server DNS** a vyberte položku **Konfigurace**.
3. V okně **konfigurace DNS** klepněte pravým tlačítkem myši na **Vlastnosti**.
4. Na stránce **Vlastnosti serveru - Obecné** zadejte úroveň ladění při spuštění serveru.
5. Pokud je server spuštěn, zastavte jej a potom jej znovu spusťte.
Pozn.: Změny do úrovně ladění se neuplatní, dokud je server spuštěn. Zde nastavená úroveň ladění se použije při příštím úplném opětovném spuštění serveru. Pokud potřebujete změnit úroveň ladění za běhu serveru, prostudujte si téma **Rozšířená funkce DNS**.

Další informace o DNS

Existuje řada zdrojů informací, které se zabývají DNS a odvětvovým standardem BIND 8. Níže uvedený seznam je pouze malou reprezentací dostupných zdrojů:

- DNS and BIND, třetí vydání. Paul Albitz a Cricket Liu. Vydáno společností O'Reilly and Associates, Inc.



Sebastopol, California, 1998. Číslo ISBN: 1-56592-512-2. Toto je nejdůležitější zdroj informací o serveru DNS.

- Webová stránka Internet Software Consortium



obsahuje novinky, odkazy a další zdroje týkající se standardu BIND.

- Webová stránka InterNIC (Internet Network Information Center)



udržuje adresář všech registrátorů jmen domén, kteří mají autorizaci od společnosti ICANN (Internet Corporation for Assigned Names and Numbers).

- DNS Resources Directory



poskytuje referenční informace týkající se serveru DNS a odkazy na mnoho dalších zdrojů zaměřených na DNS, včetně diskusních skupin. Také poskytuje seznam RFC vztahujících se k DNS



Manuály a červené knihy IBM^(TM)

- AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support



Tato červená kniha popisuje podporu serveru DNS (Domain Name System) a serveru DHCP (Dynamic Host Configuration Protocol), která je zahrnuta v operačním systému OS/400^(R). Informace v této červené knize vám pomohou za použití příkladů při instalaci, úpravách, konfiguraci a odstraňování problémů v serverech DNS a DHCP.

Pozn.: Tato červená kniha dosud nebyla aktualizována tak, aby zahrnovala nové funkce standardu BIND 8 dostupné ve verzi V5R1. Je však zdrojem kvalitních informací pro obecné koncepty serveru DNS.

Dodatek. Poznámky

Tyto informace platí pro produkty a služby nabízené v USA.

Společnost IBM nemusí v ostatních zemích nabídnout produkty, služby a funkce popsané v tomto dokumentu. Informace o produktech a službách, které jsou momentálně dostupné ve vašem regionu, můžete získat od místního zástupce IBM. Žádný odkaz na produkt, program nebo službu IBM neznámá a ani z něj nelze vyvozovat, že smí být použit pouze uvedený produkt, program či služba společnosti IBM. Použití lze jakýkoli funkčně ekvivalentní produkt, program či službu neporušující práva IBM k duševnímu vlastnictví. Za vyhodnocení a ověření činnosti libovolného produktu, programu či služby jiného výrobce než IBM však odpovídá uživatel.

Společnost IBM může mít patenty nebo podané žádosti o patent, které zahrnují předmět tohoto dokumentu. Získání tohoto dokumentu uživateli neposkytuje licenci na tyto patenty. Písemné dotazy ohledně licencí můžete zaslat na adresu:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594-1785
U.S.A.

Pokud máte zájem o licenci v zemi s dvoubajtovou znakovou sadou (DBCS), kontaktujte zastoupení společnosti IBM ve vaší zemi, nebo písemně zastoupení společnosti IBM na adrese:

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

Následující odstavec se netýká Velké Británie nebo kterékoliv jiné země, kde taková opatření odporují místním zákonům: SPOLEČNOST INTERNATIONAL BUSINESS MACHINES CORPORATION TUTO PUBLIKACI POSKYTUJE TAKOVOU, JAKÁ JE, BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH NEBO ODVOZENÝCH, VČETNĚ, BEZ OMEZENÍ, ODVOZENÉ ZÁRUKY NEPORUŠENÍ PRÁV TŘETÍCH STRAN, ZÁRUKY PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL. Právní řády některých zemí nepřipouštějí vyloučení vyjádřených nebo odvozených záruk v určitých transakcích a proto se na vás výše uvedené omezení nemusí vztahovat.

Tato publikace může obsahovat technické nepřesnosti nebo typografické chyby. Informace zde uvedené jsou pravidelně aktualizovány a v nových vydáních této publikace již budou tyto změny zahrnuty. Společnost IBM má právo kdykoliv bez upozornění zdokonalovat nebo měnit produkty a programy popsané v této publikaci.

Jakékoli odkazy v této publikaci na webové stránky jiných společností než IBM jsou poskytovány pouze pro pohodlí uživatele a nemohou být žádným způsobem vykládány jako doporučení těchto webových stránek ze strany IBM. Materiály obsažené na takovýchto webových stránkách nejsou součástí materiálů k tomuto produktu IBM a tyto webové stránky mohou být používány pouze na vlastní nebezpečí.

IBM může použít nebo distribuovat jakékoli informace, které jí sdělíte, libovolným způsobem, který společnost považuje za odpovídající, bez vzniku jakýchkoli závazků vůči vám.

Držitelé licence na tento program, kteří si přejí mít přístup i k informacím o programu za účelem (i) výměny informací mezi nezávisle vytvořenými programy a jinými programy (včetně tohoto) a (ii) vzájemného použití sdílených informací, mohou kontaktovat:

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Informace tohoto typu mohou být dostupné za určitých podmínek. V některých případech připadá v úvahu zaplacení poplatku.

IBM poskytuje licencovaný program popsáný v těchto informacích a veškeré dostupné licencované materiály na základě podmínek uvedených ve smlouvě IBM Customer Agreement, v Mezinárodní licenční smlouvě IBM na programy nebo v jiné ekvivalentní smlouvě.

Jestliže si prohlížíte tyto informace ve formě softcopy, nemusí se zobrazit fotografie a barevné ilustrace.

Ochranné známky

Následující výrazy jsou ochrannými známkami IBM v USA a případně v dalších jiných zemích:

Application System/400

AS/400

e (logo)

IBM

Server iSeries

Operating System/400

OS/400

400

Lotus, Freelance a WordPro jsou registrované ochranné známky společnosti International Business Machines Corporation a společnosti Lotus Development Corporation ve Spojených státech a případně v dalších jiných zemích.

C-bus je registrovaná ochranná známka společnosti Corollary, Inc. ve Spojených státech a případně v dalších jiných zemích.

ActionMedia, LANDesk, MMX, Pentium a ProShare jsou registrované ochranné známky společnosti Intel Corporation ve Spojených státech a případně v dalších jiných zemích.

Microsoft, Windows, Windows NT a logo Windows jsou registrované ochranné známky společnosti Microsoft Corporation ve Spojených státech a případně v dalších jiných zemích.

SET a logo SET jsou registrované ochranné známky společnosti SET Secure Electronic Transaction LLC.

Java a všechny ochranné známky obsahující slovo Java jsou ochranné známky společnosti Sun Microsystems, Inc. ve Spojených státech a případně v dalších jiných zemích.

UNIX je registrovaná ochranná známka skupiny The Open Group ve Spojených státech a jiných zemích.

Další jména společností, produktů nebo služeb mohou být ochrannými známkami jiných společností.

Ustanovení a podmínky pro stahování a tisk publikací

Oprávnění k používání publikací, které jste se rozhodli stáhnout, závisí na níže uvedených ustanoveních a podmínkách a na vašem potvrzení, že je akceptujete.

Osobní použití: Pokud zachováte všechny výhrady týkající se vlastnických práv, můžete tyto publikace kopírovat pro své osobní nekomerční použití. Tyto publikace ani jakékoliv jejich části nesmíte bez výslovného souhlasu IBM distribuovat, prezentovat ani z nich vytvářet odvozená díla.

Komerční použití: Pokud zachováte všechny výhrady týkající se vlastnických práv, můžete tyto publikace kopírovat, distribuovat a prezentovat výhradně uvnitř svého podniku. Bez výslovného souhlasu IBM nesmíte z těchto publikací vytvářet odvozená díla ani je (nebo jejich části) nesmíte kopírovat, distribuovat či prezentovat mimo rámec svého podniku.

Kromě oprávnění, která jsou zde výslovně udělena, se na publikace a veškeré informace, data, software a další duševní vlastnictví obsažené v těchto publikacích nevztahují žádná další vyjádřená ani odvozená oprávnění, povolení či práva.

IBM si vyhrazuje právo odvolat oprávnění zde udělená, kdykoli usoudí, že používání publikací poškozuje její zájmy nebo že výše uvedené pokyny nejsou řádně dodržovány.

Tyto informace můžete stahovat, exportovat či reexportovat pouze při dodržení všech příslušných zákonů a nařízení včetně veškerých vývozních zákonů a nařízení USA. IBM NEPOSKYTUJE ŽÁDNOU ZÁRUKU, POKUD JDE O OBSAH TĚCHTO PUBLIKACÍ. PUBLIKACE JSOU POSKYTOVÁNY NA BÁZI "JAK JSOU" (AS-IS), BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH NEBO ODVOZENÝCH, VČETNĚ, BEZ OMEZENÍ, ODVOZENÉ ZÁRUKY PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL.

Autorská práva na veškeré materiály náleží společnosti IBM Corporation.

Stažením nebo vytištěním publikace z tohoto serveru vyjadřujete svůj souhlas s těmito ustanoveními a podmínkami.



Vytištěno v Dánsku společností IBM Danmark A/S.