System i

Vytváření sítí
Domain Name System

verze 6 vydání 1

System i

Vytváření sítí
Domain Name System

verze 6 vydání 1

Poznámka

Dříve než použijete tyto informace a produkt, který podporují, nezapomeňte si přečíst informace uvedené v části “Poznámky”, na stránce 43.

Toto vydání se týká verze 6, vydání 1, modifikace 0 operačního systému IBM i5/OS (číslo produktu 5761-SS1) a všech následných 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.

Obsah

DNS (Systém pojmenování domén)

Systém DNS (Domain Name System) je distribuovaný databázový systém pro správu hostitelských jmen a jejich asociovaných IP (Internet Protocol) adres.

Se systémem DNS mohou lidé používat jednoduchá jména, jako například www.jkltoys.com, k vyhledání hostitele namísto použití IP adres, jako například 192.168.12.88 v IPv4 nebo 2001:D88::1 v IPv6.Jeden server může být zodpovědný pouze za to, že zná hostitelská jména a IP adresy pro malou část určité zóny, avšak servery DNS mohou při mapování všech jmen domén na jejich IP adresy spolupracovat. Spolupráce serverů DNS umožňuje počítačům komunikovat přes Internet.

V systému IBM i5/OS Version 6 Release 1 (V6R1) jsou služby DNS založeny na implementaci DNS, což je průmyslový standard známý jako BIND verze 9 (Berkeley Internet Name Domain). Předchozí služby vydání systému i5/OS DNS byly založeny na standardu BIND verze 8.2.5. Chcete-li použít novou verzi standardu BIND 9 serveru DNS, musíte mít na modelu systému IBM System i nainstalovanou volbu systému i5/OS 31 (DNS) a 33 (PASE). V systému i5/OS verze V6R1 je z bezpečnostních důvodů standard BIND 4 a 8 nahrazen standardem BIND 9. Z toho důvodu je pro server DNS vyžadován standard BIND 9.

Co je nového ve verzi V6R1

Pročtěte si nové nebo podstatným způsobem změněných informace obsažené v kolekci témat o systému DNS (Domain Name System).

BIND 9

Standard BIND (Berkeley Internet Name Domain) verze 9, představený v tomto vydání, poskytuje několik funkcí k vylepšení výkonu serveru DNS (Domain Name System). Podporuje například vyhledávání typu ″name-to-address″ a ″address-to-name″ ve všech aktuálně definovaných formách adres IPv6. Využívá funkci *pohledů*, která umožňuje jedné instanci serveru DNS odpovědět na stejný dotaz rozdílně, v závislosti na tom, odkud dotazy pocházejí, např. z Internetu nebo Intranetu. Kromě toho používá soubory žurnálu k uchovávání dynamických aktualizací zóny.

Předchozí standardy BIND 4.9.3 a BIND 8.2.5 nejsou již podporovány a vyžadovány při migraci na BIND 9.

Nové příkazy konfigurace

Byly přidány tyto příkazy konfigurace, které zjednodušují správu konfiguračních souborů DNS v systému.

CRTRNDCCFG (Vytvoření konfigurace RNDC)
Příkaz CRTRNDCCFG (Obslužný program RNDC) se používá pro generování konfiguračních souborů RNDC. Jedná se o výhodnou alternativu k zapsání souboru rndc.conf a jeho odpovídajícího ovládání a klíčových povelů v souboru named.conf.

CHKDNSCFG (Obslužný program konfigurace DNS)
Příkaz CHKDNSCFG (Obslužný program konfigurace DNS) zkontroluje syntaxi konfiguračního souboru jménem named.conf. Neposkytuje však podporu kontroly sémantiky konfiguračního souboru.

CHKDNSZNE (Obslužný program zóny DNS)
Příkaz CHKDNSZNE (Obslužný program zóny DNS) zkontroluje syntaxi a integritu souboru zóny dat. Je užitečné zkontrolovat soubory dat zóny předtím, než je přidáte na server DNS.

Nové dotazy a obslužné programy pro aktualizace

Za účelem vylepšení možností správy serveru DNS byly přidány tyto dotazy a obslužné programy pro aktualizaci.

DIG (Domain Information Groper)

Můžete použít nástroj pro dotazování DIG k získání informací DNS o hostitelích, doménách a ostatních serverech DNS pomocí odpovědí serveru DNS. Lze jej rovněž použít k ověření toho, zda server DNS odpovídá správně, předtím, než budete systém konfigurovat, aby jej použil.

HOST (Spuštění dotazu HOST)

Příkaz HOST (Spuštění dotazu HOST) se používá pro vyhledávání DNS. Konvertuje jména doména na IP adresy (IPv4 nebo IPv6) a naopak.

NSUPDATE (Obslužný program pro dynamickou aktualizaci)

Příkaz NSUPDATE (Obslužný program pro dynamickou aktualizaci) se podává požadavky na dynamické aktualizace DNS, jak to je definováno v RFC (Request for Comments) 2136 pro server DNS. To umožňuje přidávat nebo odebírat záznamy prostředků ze zóny během činnosti serveru DNS. Nemusíte tedy aktualizovat záznamy ručním editováním souboru zóny. Požadavek jedné aktualizace nemůže obsahovat požadavky přidání nebo odstranění víc než jednoho záznamu prostředků; záznamy prostředků, které jsou dynamicky přidány nebo odstraněni příkazem NSUPDATE by měly být ve stejné zóně.

RNDC (Vzdálené ovládání démona jmen)

Příkaz RNDC (Vzdálené ovládání démona jmen) umožňuje systémovým administrátorům ovládat operace na serveru jmen. Načte konfigurační soubor nazvaný *rndc.conf*, pomocí kterého určí, jak kontaktovat server jmen a zjistit jaký algoritmus a klíče použít. Pokud nenajde soubor rndc.conf, standardně použije soubor rndc-key._KID vytvořený během instalace, který automaticky poskytne přístup prostřednictvím smyčkového rozhraní.

Jak zjistit, co je nového nebo co se změnilo

Za účelem snadnější identifikace míst, kde byly provedeny technické změny, jsou tyto informace označeny symbolem:

- Obrázek » označuje, kde začínají nové nebo změněné informace.
- Obrázek « označuje, kde končí nové nebo změněné infromace.

V souborech PDF se mohou zobrazit revizní značky (|) v levém okraji nových nebo změněných informací.

Související odkazy

“Funkce odvětvového standardu BIND 8” na stránce 7
Standard BIND 9 je podobný standardu BIND 8; kromě dynamické aktualizace však nabízí několik funkcí pro zvýšení výkonu vašeho serveru DNS, například funkci pohledů.

PDF soubor pro server DNS

Soubor PDF s těmito informacemi můžete zobrazit nebo vytisknout.

Chcete-li si prohlédnout nebo stáhnout verzi PDF tohoto dokumentu, vyberte téma DNS (přibližně 625 KB).

Uložení PDF souborů

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

1. Klepněte pravým tlačítkem myši na odkaz PDF ve vašem prohlížeči.
2. Klepněte na volbu, kterou uložíte soubor PDF lokálně.
3. Vyhledejte adresář, do kterého chcete uložit soubor PDF.
4. Klepněte na **Save (Uložit)**.

Stažení programu Adobe Reader

Chcete-li zobrazit nebo tisknout tyto soubory PDF, musíte mít ve svém systému nainstalován program Adobe Reader. Bezplatnou kopii si můžete stáhnout z webových stránek Adobe (www.adobe.com/products/acrobat/readstep.html) .

Související odkazy

“Související informace o DNS (Systém pojmenování domén)” na stránce 40
IBM Redbooky, webové stránky a ostatní témata aplikace Informační centrum obsahují informace vztahující se ke kolekci témat o systému DNS. Kterýkoli z těchto dokumentů ve formátu PDF si můžete zobrazit a vytisknout.

Koncepty DNS (Systém pojmenování domén)

DNS (Systém pojmenování domén) je distribuovaný databázový systém pro správu hostitelských jmen a jejich asociovaných IP (Internet Protocol) adres. With DNS, you can use simple names, such as www.jkltoys.com, to locate a host, rather than using the IP addresses, for example, 192.168.12.88 in IPv4, or 2001:D88::1 in IPv6.

Jeden server může být zodpovědný pouze za to, že zná hostitelská jména a IP adresy pro malou část 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 rozdělená 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 pro tuto zónu směrodatný. Směrodatný server může odpovídat na dotazy o hostitelských systémech ve své zóně pomocí svých vlastních zdrojových záznamů. Proces dotazu závisí na řadě faktorů. Téma Jak rozumět dotazům DNS vysvětluje, jakým způsobem může klient dotazy řešit.

Co jsou zóny

Data DNS jsou rozdělena do spravovatelných sad dat, které se nazývají *zóny*. A každá z těchto sad je specifickým typem 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 směrodatným serverem pro doménu, která se nazývá *nadřízená zóna*. Někdy má význam delegovat oprávnění k odpovídání dotazů DNS pro určitou poddoménu na jiný server DNS, tato zóna se nazývá *podřízená zóna typu "child zone"*. 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 směrodatný server DNS. Tyto servery, které nahrávají zónová data ze směrodatného 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 směrodatného serveru. V případě, že je sekundární server inicializován, zavádí z primárního serveru úplnou kopii zónových dat. V případě změn zónových dat zavádí sekundární server opětně zónová data z primárního serveru nebo z ostatních sekundárních serverů této domény.

Typy zón DNS

Pomocí serveru i5/OS DNS můžete definovat několik typů zón, což vám pomůže při správě dat DNS:

Primární zóna
Primární zóna zavádí zónová data přímo ze souboru na hostitelském systému. Může obsahovat podzónu neboli podřízenou zónu typu ″child zone″. Může obsahovat zdrojové záznamy, jako např. hostitelský systém, jméno alias (CNAME), adresa IPv4 (A), adresa IPv6 (AAAA) nebo záznamy ukazatele vyhledávání dozadu (PTR).

Poznámka: 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 uspořádávat zónová data do spravovatelných částí.

Podřízená zóna typu ″child zone″
Podřízená zóna typu ″child zone″ 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 záznamy zdrojů mohou být asociovány s hostitelským systémem.

Sekundární zóna
Sekundární zóna zavádí zónová data z primárního serveru zóny nebo ze sekundárního serveru. Udržuje úplnou kopii zóny, vůči níž je sekundárním serverem.

Poznámka: Sekundární zóny jsou někdy v jiné dokumentaci odvětvového standardu BIND nazývány *podřízené zóny typu ″slave zone″*.

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

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

Související pojmy

“Jak rozumět dotazům DNS (Systém pojmenování domén)”
Klienti serveru DNS (Domain Name System) využívají servery DNS pro vyřízení dotazů. Dotazy mohou vyjít přímo od klienta nebo od aplikace, která pracuje na tomto klientovi.

Související úlohy

“Konfigurace zón na serveru jmen” na stránce 28
Jakmile nakonfigurujete instanci serveru DNS (Systém pojmenování domén), musíte nakonfigurovat zóny pro server jmen.

Související odkazy

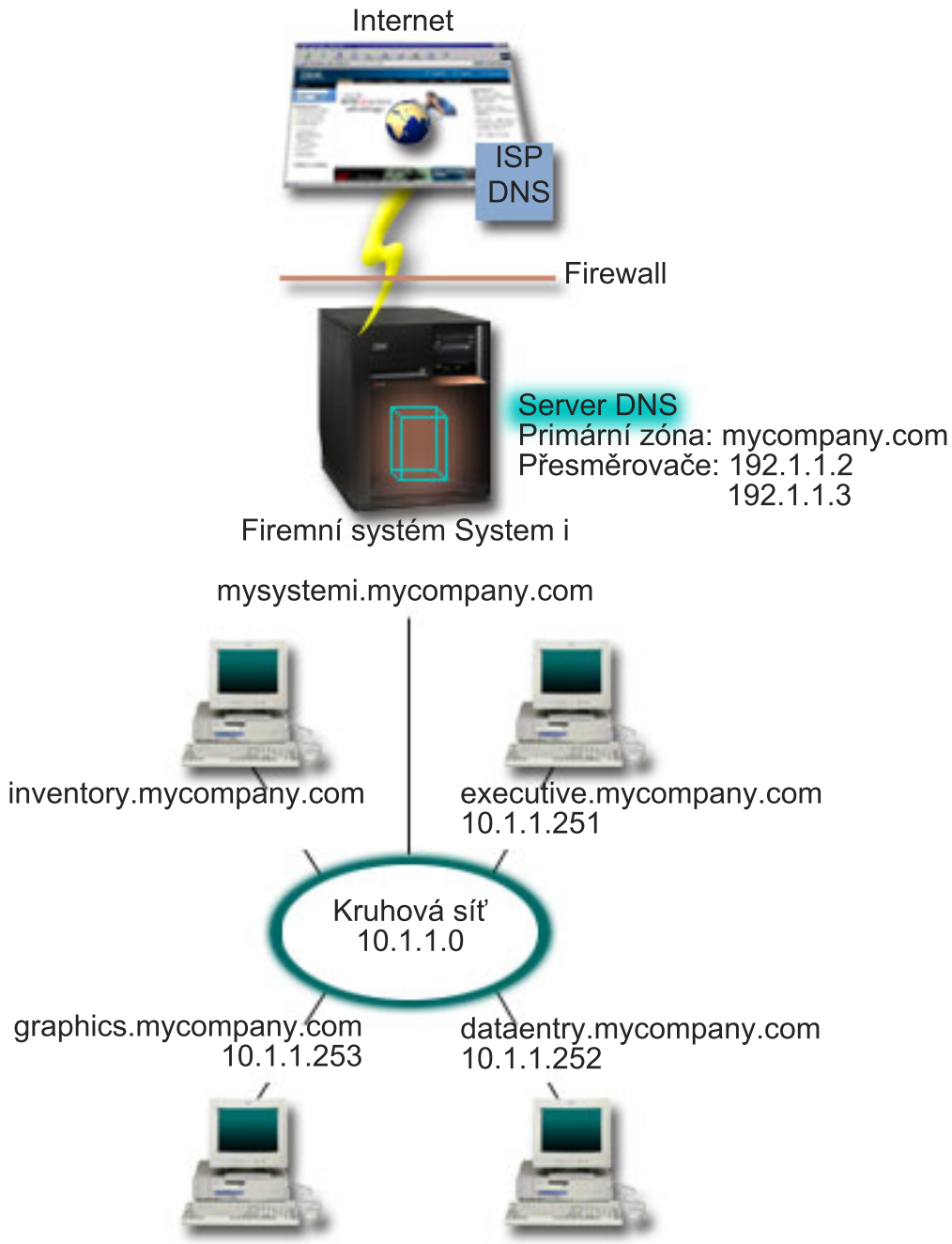
“Příklad: Jediný server DNS pro intranet” na stránce 14
Tento příklad popisuje jednoduchou podsíť se serverem DNS (Systém pojmenování domén) pro interní použití.

“Záznamy zdrojů DNS (Systém pojmenování domén)” na stránce 9
Zdrojové záznamy se používají k ukládání dat o jménech domén a IP adresách. Chcete-li zobrazit zdrojové záznamy podporované operačním systémem i5/OS, můžete použít vyhledávací tabulku zdrojových záznamů.

Jak rozumět dotazům DNS (Systém pojmenování domén)

Klienti serveru DNS (Domain Name System) využívají servery DNS pro vyřízení dotazů. Dotazy mohou 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 zdroje, který klient požaduje, a třídu pro jméno domény, což je obvykle třída Internetu (IN). Následující obrázek ukazuje 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. Lze sledovat dvě cesty: *rekurzi* nebo *iteraci*. 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. Kromě toho server vysílající požadavek uloží odpověď do své mezipaměti, takže odpověď lze použít při příštím dotazu tohoto serveru. Pokud je server DNS nastaven tak, aby používal *iteraci* , může se klient za účelem rozlišení jména pokusit o kontakt s ostatními servery DNS. V tomto procesu používá klient samostatné a dodatečné dotazy založené na referenčních odpovědích od serverů.

Související odkazy

“Co jsou zóny” na stránce 3
Data DNS jsou rozdělena do spravovatelných sad dat, které se nazývají *zóny*. A každá z těchto sad je specifickým typem zóny.

“Příklad: Jediný server DNS s přístupem k Internetu” na stránce 16
Tento příklad popisuje jednoduchou podsíť se serverem DNS (Systém pojmenování domén), který je přímo připojen k Internetu.

Nastavení domény DNS

Nastavení DNS vyžaduje registraci jména domény, aby se zabránilo ostatním používat vaše jméno domény.

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 konfigurujete intranet, pak si jméno domény pro interní použití registrovat nemusíte. Rozhodnutí o registraci intranetového jména závisí na tom, 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. InterNIC (Internet Network Information Center) udržuje adresář všech registrátorů jmen domén, kteří mají autorizaci od společnosti ICANN (Internet Corporation for Assigned Names and Numbers).

Související odkazy

“Příklad: Jediný server DNS s přístupem k Internetu” na stránce 16
Tento příklad popisuje jednoduchou podsíť se serverem DNS (Systém pojmenování domén), který je přímo připojen k Internetu.

Související informace

Internet Network Information Center (InterNIC)

Dynamická aktualizace

i5/OS DNS (Domain Name System) založený na standardu BIND 9 poskytuje podporu dynamickým aktualizacím. Vnější zdroje, jako např. DHCP (protokol dynamické konfigurace hostitele) mohou odesílat aktualizace k serveru DNS. Kromě toho můžete k provádění dynamických aktualizací používat také nástroje klienta DNS, jako například NSUPDATE (Obslužný program pro dynamickou aktualizaci).

Protokol DHCP (protokol dynamické konfigurace hostitele) 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 záznamy zdrojů DNS musí vytvořit a udržovat administrátor. Avšak servery DNS provozující standard BIND 8 nebo novější mohou být konfigurovány tak, aby přijímaly požadavky z ostatních zdrojů a dynamicky aktualizovaly zónová data.

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 na server 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 pro IPv4 a AAAA pro IPv6), záznamy PTR, nebo obojí v zastoupení klienta. Záznamy mapování adres (A nebo AAAA) 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 klientské nové adrese. Pro každý dynamicky aktualizovaný záznam bude zapsán asociovaný textový záznam (TXT), který bude identifikovat, že záznam zapsal DHCP.

Poznámka: 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, pokud klient používá adresu IPv4, nebo AAAA, pokud klient používá adresu IPv6. Ne všichni klienti DHCP podporují provádění vlastních požadavků na aktualizaci záznamu A nebo AAAA. 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.

Dynamické aktualizace lze provádět mezi servery DNS a DHCP na jediné platformě System i, mezi různými platformami System i nebo mezi platformou System i a jinými systémy, které jsou schopné provádět dynamické aktualizace.

Poznámka: U serverů, které odesílají dynamické aktualizace do serveru DNS, je vyžadováno dynamické rozhraní API QTOBUPDT (Update DNS). Toto rozhraní se instaluje automaticky s volbou 31 operačního systému i5/OS. Ve standardu BIND 9 je vhodnější metodou příkaz NSUPDATE, chcete-li provést aktualizaci na platformě System i .

Související pojmy

DHCP (Dynamic Host Configuration Protocol)

Související úlohy

“Konfigurace DNS (Systém pojmenování domén) pro přijímání dynamických aktualizací” na stránce 29
Nyní mohou být servery DNS (Systém pojmenování domén) provozující standard BIND 9 konfigurovány tak, aby přijímaly požadavky z ostatních zdrojů a dynamicky aktualizovaly zónová data. Toto téma poskytuje návod, jak nakonfigurovat volbu Povolit aktualizaci tak, aby mohl server DNS přijímat dynamické aktualizace.

Konfigurace DHCP pro zasílání dynamických aktualizací na DNS

Související odkazy

“Příklad: Systém DNS a protokol DHCP na stejném serveru System i” na stránce 18
Tento příklad uvádí DNS (Systém pojmenování domén) a protokol DHCP (protokol dynamické konfigurace hostitele) na stejné platformě System i.

“Záznamy zdrojů DNS (Systém pojmenování domén)” na stránce 9
Zdrojové záznamy se používají k ukládání dat o jménech domén a IP adresách. Chcete-li zobrazit zdrojové záznamy podporované operačním systémem i5/OS, můžete použít vyhledávací tabulku zdrojových záznamů.

QTOBUPT

“Funkce odvětvového standardu BIND 8”
Standard BIND 9 je podobný standardu BIND 8; kromě dynamické aktualizace však nabízí několik funkcí pro zvýšení výkonu vašeho serveru DNS, například funkci pohledů.

Funkce odvětvového standardu BIND 8

Standard BIND 9 je podobný standardu BIND 8; kromě dynamické aktualizace však nabízí několik funkcí pro zvýšení výkonu vašeho serveru DNS, například funkci pohledů.

Funkce pohledů na jednom serveru i5/OS

Funkce *pohledů* umožňuje jedné instanci serveru DNS odpovědět na stejný dotaz rozdílně, v závislosti na tom, odkud dotazy pochází, např. z Internetu nebo Intranetu.

Jednou z praktických aplikací funkce pohledů je rozdělit nastavení bez nutnosti spustit několik serverů DNS. Na jednom serveru DNS můžete například definovat funkci pohledů tak, aby odpovídala na dotazy z interní sítě a současně definovat jinou funkci zobrazení pro odpovědi na dotazy z externí sítě.

Nové příkazy klienta

Tyto příkazy klienta vylepšují možnosti správy serveru DNS:

NSUPDATE (Obslužný program pro dynamickou aktualizaci)
Příkaz NSUPDATE (Obslužný program pro dynamickou aktualizaci) se používá k podání požadavku dynamické aktualizace DNS, jak to je definováno v RFC (Request for Comments) 2136 pro server DNS. To umožňuje přidávat nebo odebírat záznamy prostředků ze zóny během činnosti serveru DNS. Nemusíte tedy aktualizovat záznamy ručním editováním souboru zóny. Požadavek jedné aktualizace nemůže obsahovat požadavky přidání nebo odstranění několika záznamů prostředků; záznamy prostředků, které jsou dynamicky přidány nebo odstraněni příkazem NSUPDATE by měly být ve stejné zóně.

Poznámka: Příkazem NSUPDATE, ani pomocí serveru DHCP needitujte ručně zóny, které jsou řízeny dynamicky. Ruční editování by mohlo způsobit konflikt s dynamickými aktualizacemi a ztrátu dat.

DIG (Spuštění dotazu DIG)
DIG (Spuštění dotazu DIG) je ve srovnání s příkazem NSLOOKUP (Vyhledání jména serveru) ještě účinějším nástrojem pro dotazy, který lze použít pro získání informací ze serveru DNS nebo testování odpovědí na server DNS. Příkaz NSLOOKUP je zrušený a je podporován pouze z důvodu kompatibility s předchozími verzemi. Příkaz DIG lze použít k ověření toho, zda server DNS správně odpovídá, a to ještě předtím, než nakonfigurujete váš systém k jeho používání. Můžete také načíst informace serveru DNS o hostitelích, doménách a ostatních serverech DNS používající DIG.

Chcete-li spustit nástroj DIG (Domain Information Groper), můžete použít příkaz STRDIGQRY (Spuštění dotazu DIG) nebo jeho alias příkaz DIG.

HOST (Spuštění dotazu HOST)
Příkaz HOST (Spuštění dotazu HOST) se používá pro vyhledávání DNS. Můžete ho použít ke konvertování jmen domén na IP adresy (IPv4 nebo IPv6) a naopak.

RNDC (Vzdálené ovládání démona jmen)

Příkaz RNDC (Vzdálené ovládání démona jmen) je účinný nástroj umožňující systémovým administrátorům ovládat operace na serveru jmen. Načte konfigurační soubor nazvaný rndc.conf, jehož pomocí se určí, jak kontaktovat server jmen a jak zjistit, který algoritmus a klíč použít. Pokud nenajde soubor rndc.conf, standardně použije soubor rndc-key._KID vytvořený během instalace, který automaticky poskytne přístup prostřednictvím smyčkového rozhraní.

Podpora IPv6

Standard BIND 9 podporuje například vyhledávání typu ″name-to-address″ a ″address-to-name″ ve všech aktuálně definovaných formách adres IPv6. Pro přesměrování vyhledávání podporuje BIND 9 záznamy AAAA i A6; záznamy A6 jsou však nyní zrušeny. Pro přesměrování vyhledávání IPv6 je podporován tradiční čtyřbitový, který se používá v doméně ip6.arpa, stejně jako ve starší zrušené doméně ip6.int.

Soubory žurnálu

Soubory žurnálu se používají pro uchování dynamických aktualizací zóny. Jedná se o soubor, který je vytvořený automaticky při první dynamické aktualizaci z klienta, a poté nezmizí. Je to binární soubor a neměli byste jej editovat.

Pokud je server restartován po vypnutí nebo selhání, přehraje soubor žurnálu a zahrne tak do zóny všechny aktualizace, ke kterým došlo po posledním výpisu zóny. Soubory žurnálu se rovněž používají pro uchování aktualizací pro metodu IXFR (incremental zone transfers).

DNS pro systémy i5/OS byl nově navržen tak, aby používal BIND 9. Chcete-li v systému spustit BIND 9, musí systém splňovat určitá softwarová kritéria.

Související pojmy

"Požadavky na DNS (Systém pojmenování domén)" na stránce 26
Chcete-li spustit DNS na vaší platformě System i, zvažte tyto softwarové požadavky.

"Dynamická aktualizace" na stránce 6
i5/OS DNS (Domain Name System) založený na standardu BIND 9 poskytuje podporu dynamickým aktualizacím. Vnější zdroje, jako např. DHCP (protokol dynamické konfigurace hostitele) mohou odesílat aktualizace k serveru DNS. Kromě toho můžete k provádění dynamických aktualizací používat také nástroje klienta DNS, jako například NSUPDATE (Obslužný program pro dynamickou aktualizaci).

"Co je nového ve verzi V6R1" na stránce 1
Pročtěte si nové nebo podstatným způsobem změněných informace obsažené v kolekci témat o systému DNS (Domain Name System).

Související odkazy

"Příklad: Rozdělení DNS v rámci ochranné bariéry pomocí nastavení dvou serverů DNS na jediném serveru System i" na stránce 20
Tento příklad systém popisuje DNS, který pracuje nad ochrannou bariérou (firewall) tak, aby chránil interní data před přístupem z Internetu, zatímco interním uživatelům umožňuje přístup k datům na Internetu. Tato konfigurace umožňuje ochranu pomocí nastavení dvou serverů DNS na jedné platformě System i.

"Plánování opatření pro zabezpečení dat" na stránce 25
DNS (Systém pojmenování domén) poskytuje volby pro zabezpečení dat, které omezují externí přístup k vašemu serveru.

Záznamy zdrojů DNS (Systém pojmenování domén)

Zdrojové záznamy se používají k ukládání dat o jménech domén a IP adresách. Chcete-li zobrazit zdrojové záznamy podporované operačním systémem i5/OS, můžete použít vyhledávací tabulku zdrojových záznamů.

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.

Poznámka: Položky ve vyhledávací tabulce zdrojových záznamů lze přidat nebo odstranit v závislosti na změně dokumentu BIND. Toto však není vyčerpávající seznam všech zdrojových záznamů uvedených v BIND.

Tabulka 1. Vyhledávací tabulka zdrojových záznamů

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 dokumentu Request for Comments (RFC) 1035.

Tabulka 1. Vyhledávací tabulka zdrojových záznamů (pokračování)

Zdrojový záznam	Zkratka	Popis
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 ADSDB adresu, nebo pro mapování ze jména domény buňky na autentizované 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.
Záznamy IP adresy verze 6	AAAA	Záznam AAAA uvádí hostitelskou 128bitovou adresu IPv6. Záznamy AAAA, které jsou podobné záznamům A, se používají k vyřízení dotazů na adresu IPv6 určitého jména domény. 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 efektivity 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.

Tabulka 1. Vyhledávací tabulka zdrojových záznamů (pokračování)

Zdrojový záznam	Zkratka	Popis
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 se směruje 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.
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 směrodatný 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.

Tabulka 1. Vyhledávací tabulka zdrojových záznamů (pokračování)

Zdrojový záznam	Zkratka	Popis
Záznamy služeb	SRV	Záznam SRV určuje hostitelské systémy, které podporují definované služby v tomto záznamu. Tento typ záznamu je definován v RFC 2782.
Záznamy SOA (Start of Authority)	SOA	Záznam SOA uvádí, že tento server je směrodatný. Směrodatný 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.
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 systémem i5/OS DHCP používány pro dynamické aktualizace. 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 obyčejně 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.

Související pojmy

“Poštovní záznamy a záznamy MX” na stránce 13
DNS (Systém pojmenování domén) podporuje rozšířené směrování pošty pomocí poštovních záznamů a záznamů MX.

Související odkazy

“Příklad: Jediný server DNS pro intranet” na stránce 14
Tento příklad popisuje jednoduchou podsíť se serverem DNS (Systém pojmenování domén) pro interní použití.

“Co jsou zóny” na stránce 3
Data DNS jsou rozdělena do spravovatelných sad dat, které se nazývají *zóny*. A každá z těchto sad je specifickým typem zóny.

Poštovní záznamy a záznamy MX

DNS (Systém pojmenování domén) podporuje rozšířené směrování pošty pomocí poštovních záznamů a záznamů MX.

Poštovní záznamy a záznamy MX (Mail exchanger) používají programy na směrování pošty, jako např. SMTP (Simple Mail Transfer Protocol). Vyhledávací tabulka v záznamech zdrojů DNS obsahuje typy poštovních záznamů, které server i5/OS DNS podporuje.

DNS zahrnuje informace pro odesílání elektronické pošty pomocí informací MX. Pokud síť používá server DNS, aplikace SMTP nedoručuje 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 *mail exchanger* (MX). 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 pošta doručena, 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, leží-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.

Poznámka: Poznámka: Používání zástupných znaků (například: *.mycompany.com) v záznamech MX pro doménu se nedoporučuje.

Příklad: záznam MX pro hostitelský systém

V následujícím příkladu systém podle preferencí doručuje 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 záznamy MX mohou 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
```

Související odkazy

“Záznamy zdrojů DNS (Systém pojmenování domén)” na stránce 9
Zdrojové záznamy se používají k ukládání dat o jménech domén a IP adresách. Chcete-li zobrazit zdrojové záznamy podporované operačním systémem i5/OS, můžete použít vyhledávací tabulku zdrojových záznamů.

Příklady : Systém DNS

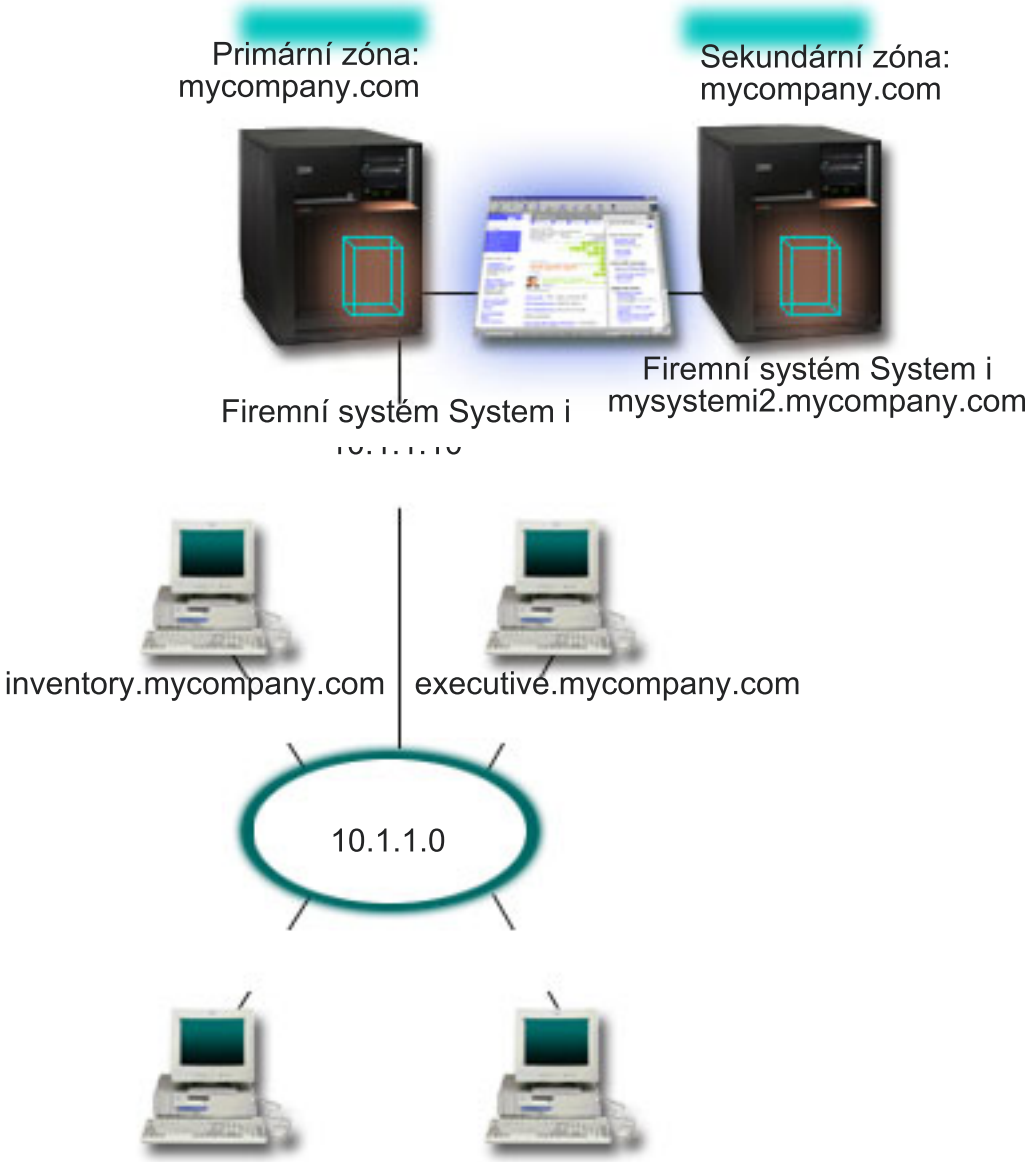
Z těchto příkladů můžete pochopit, jak používat systém DNS (Systém pojmenování domén) v síti.

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, které mohou být důležité pro porozumění uvedeným obrázkům.

Příklad: Jediný server DNS pro intranet

Tento příklad popisuje jednoduchou podsíť se serverem DNS (Systém pojmenování domén) pro interní použití.

Následující ilustrace ukazuje DNS spuštěný na platformě System i v interní síti. Tato jediná instance (výskyt) serveru DNS je nastavena tak, aby naslouchala dotazům na všech IP adresách rozhraní. Tento systém je primární server jmen pro zónu mycompany.com.



Obrázek 2. Jediný server DNS pro intranet

Každý hostitelský systém v této zóně má IP adresu a jméno domény. Administrátor musí ručně definovat hostitelské systémy v zónových datech DNS tak, že vytvoří zdrojové záznamy. Záznamy mapování adres (A pro IPv4 a AAAA pro IPv6) 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, AAAA 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 směrodatného serveru. Sekundární servery získávají zónová data tak, že provádějí zónové přenosy ze směrodatného serveru. 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 mysystemi částí intranetu. Byl nakonfigurován další systém, mysystemi2, 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.

Související odkazy

"Záznamy zdrojů DNS (Systém pojmenování domén)" na stránce 9
Zdrojové záznamy se používají k ukládání dat o jménech domén a IP adresách. Chcete-li zobrazit zdrojové záznamy podporované operačním systémem i5/OS, můžete použít vyhledávací tabulku zdrojových záznamů.

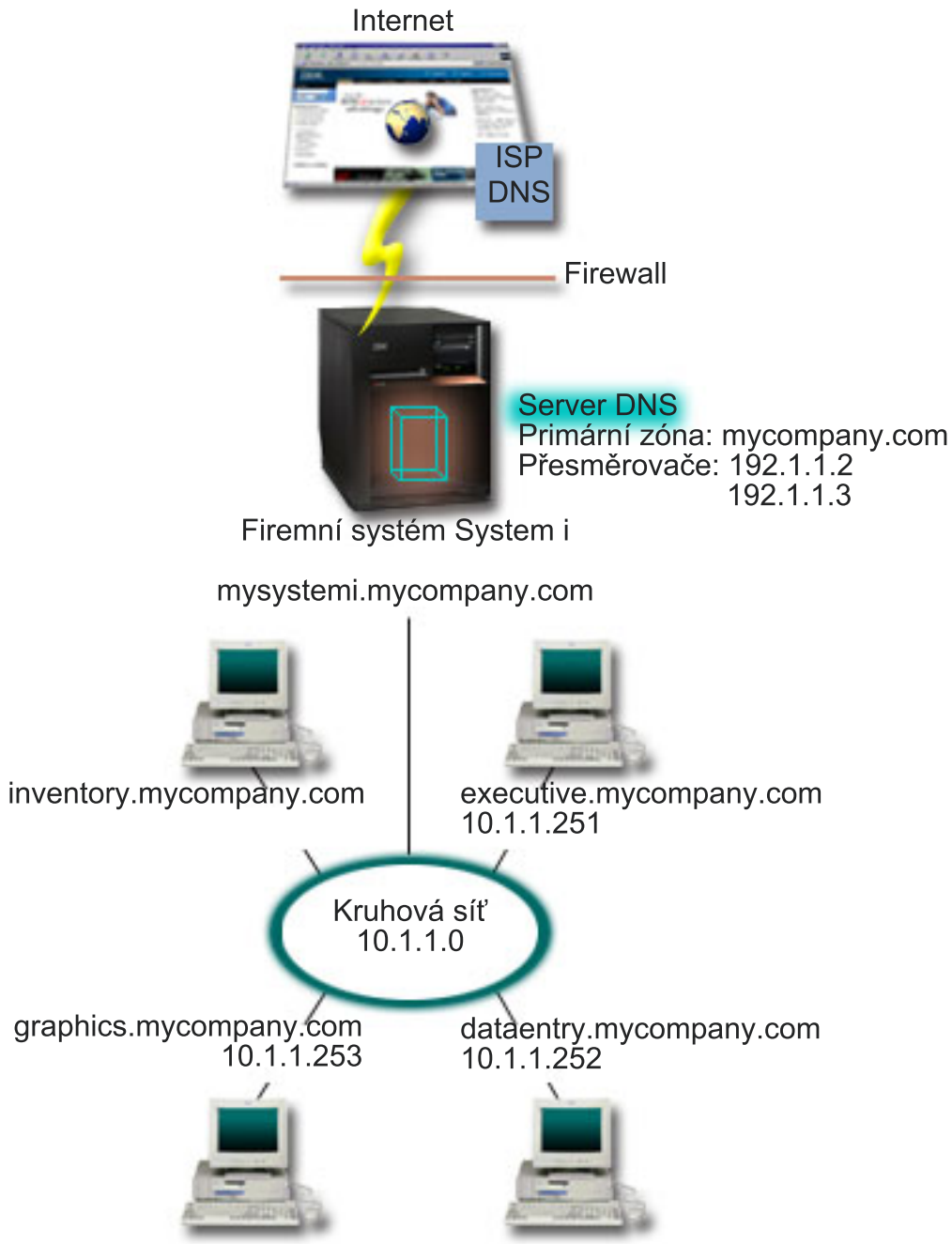
"Co jsou zóny" na stránce 3
Data DNS jsou rozdělena do spravovatelných sad dat, které se nazývají *zóny*. A každá z těchto sad je specifickým typem zóny.

"Příklad: Jediný server DNS s přístupem k Internetu"
Tento příklad popisuje jednoduchou podsíť se serverem DNS (Systém pojmenování domén), který je přímo připojen k Internetu.

Příklad: Jediný server DNS s přístupem k Internetu

Tento příklad popisuje jednoduchou podsíť se serverem DNS (Systém pojmenování domén), který je přímo připojen k Internetu.

Následující obrázek ukazuje stejnou vzorovou síť z příkladu intranetu s jedním serverem DNS s tím rozdílem, že společnost přidala připojení 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 3. Jediný server DNS s přístupem k Internetu

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

- Definování internetových kořenových serverů

  Internetové kořenové servery můžete zavést automaticky, avšak budete možná potřebovat aktualizovat seznam. Tyto servery vám mohou pomoci s rozlišováním adres mimo rozsah vaší vlastní zóny. Pokyny týkající se získání aktuálních internetových kořenových serverů najdete v 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, musíte 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 jsou dány vaším ISP a ostatními faktory vytváření sítí.
- Registrace jména vaší domény

  Jestliže jste vidět na internetu a nejste ještě registrováni, musíte zaregistrovat jméno domény.
- Vytvoření ochranné bariéry

  Nedoporučuje se přímé připojení serveru DNS k Internetu. Je třeba nakonfigurovat ochrannou bariéru nebo přijmout jiná opatření k zabezpečení vaší platformy System i.

  Související pojmy

  “Nastavení domény DNS” na stránce 6
  Nastavení DNS vyžaduje registraci jména domény, aby se zabránilo ostatním používat vaše jméno domény.

  Systém a zabezpečení Internetu

  “Jak rozumět dotazům DNS (Systém pojmenování domén)” na stránce 4
  Klienti serveru DNS (Domain Name System) využívají servery DNS pro vyřízení dotazů. Dotazy mohou vyjít přímo od klienta nebo od aplikace, která pracuje na tomto klientovi.

  Související odkazy

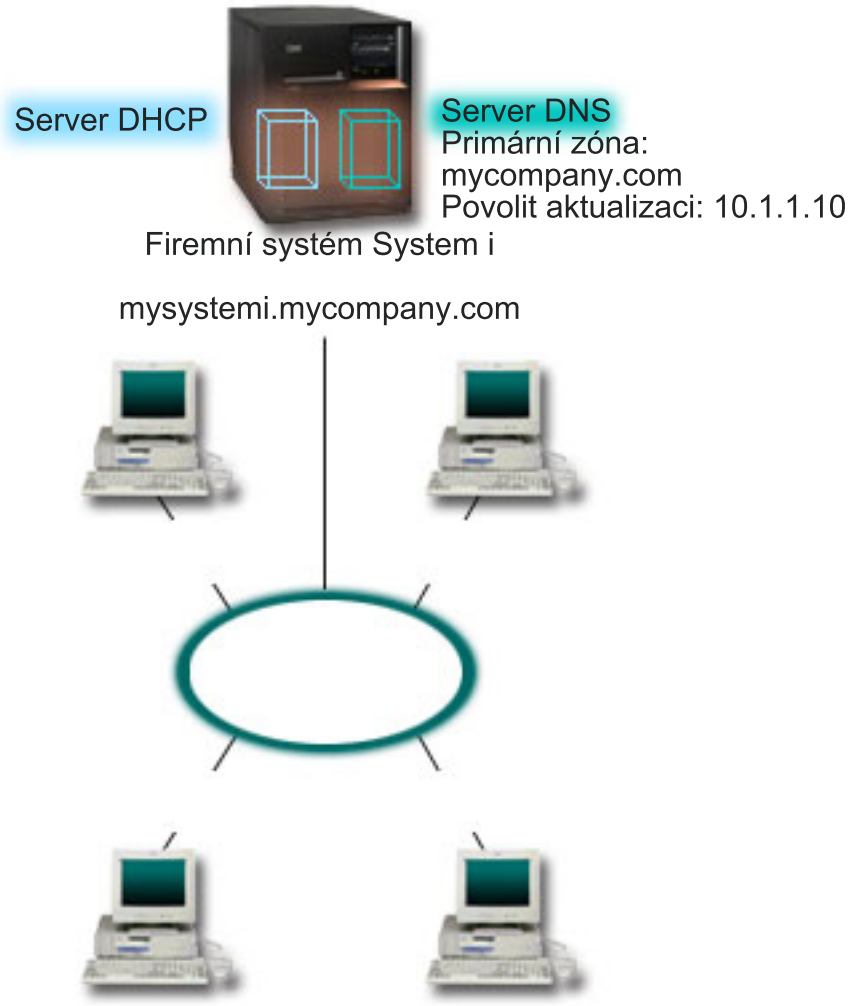
  “Příklad: Jediný server DNS pro intranet” na stránce 14
  Tento příklad popisuje jednoduchou podsíť se serverem DNS (Systém pojmenování domén) pro interní použití.

Příklad: Systém DNS a protokol DHCP na stejném serveru System i

Tento příklad uvádí DNS (Systém pojmenování domén) a protokol DHCP (protokol dynamické konfigurace hostitele) na stejné platformě System i.

Tato konfigurace může být použita k dynamické aktualizaci zónových dat DNS, když DHCP přiřazuje IP adresy hostitelským systémům.

Následující obrázek popisuje malou podsíť s jednou platformou System i, která funguje jako server DHCP a DNS pro čtyři klienty. V tomto pracovním prostředí předpokládejme, 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 4. DNS a DHCP na jedné platformě System i

Předcházející verze DHCP a DNS byly vzájemně nezávislé. Pokud DHCP přiřadil klientovi novou IP adresu, musel administrátor ručně aktualizovat záznamy DNS. Jestliže se v tomto případě změní IP adresa serveru grafických souborů, jelikož byla přiřazena serverem DHCP, pak jeho závislí klienti nebudou schopni mapovat síťovou jednotku na jeho hostitelské jméno, protože záznamy DNS budou obsahovat předchozí IP adresu souborového serveru.

Se serverem i5/OS založenýmm na odvětvovém standardu BIND 9 můžete konfigurovat vaši zónu DNS tak, aby akceptovala dynamickou aktualizaci záznamů DNS spolu s opakujícími se změnami adres prostřednictvím serveru 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 jejich hostitelskými jmény.

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 v provozu. 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

Jakákoliv zóna nakonfigurovaná s volbou povolení aktualizace je považována za dynamickou zónu. Volba povolení aktualizace se nastavuje jednotlivě, zónu po zóně. Aby bylo možné přijímat dynamické aktualizace, musí být pro zónu aktivována volba povolení aktualizace. V tomto případě zóna mycompany.com má data s povolením aktualizace, ale ostatní zóny definované na serveru mohou být konfigurovány 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.

- Konfigurace preferencí aktualizace sekundárních serverů

  Chcete-li zajistit, aby sekundární servery zůstávaly aktuální, nakonfigurujte server 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 spouštíte DNS a DHCP na různých serverech, existují určité dodatečné požadavky na konfiguraci serveru DHCP.

Související pojmy

"Dynamická aktualizace" na stránce 6
i5/OS DNS (Domain Name System) založený na standardu BIND 9 poskytuje podporu dynamickým aktualizacím. Vnější zdroje, jako např. DHCP (protokol dynamické konfigurace hostitele) mohou odesílat aktualizace k serveru DNS. Kromě toho můžete k provádění dynamických aktualizací používat také nástroje klienta DNS, jako například NSUPDATE (Obslužný program pro dynamickou aktualizaci).

Související úlohy

Konfigurace DHCP pro zasílání dynamických aktualizací na DNS

Související odkazy

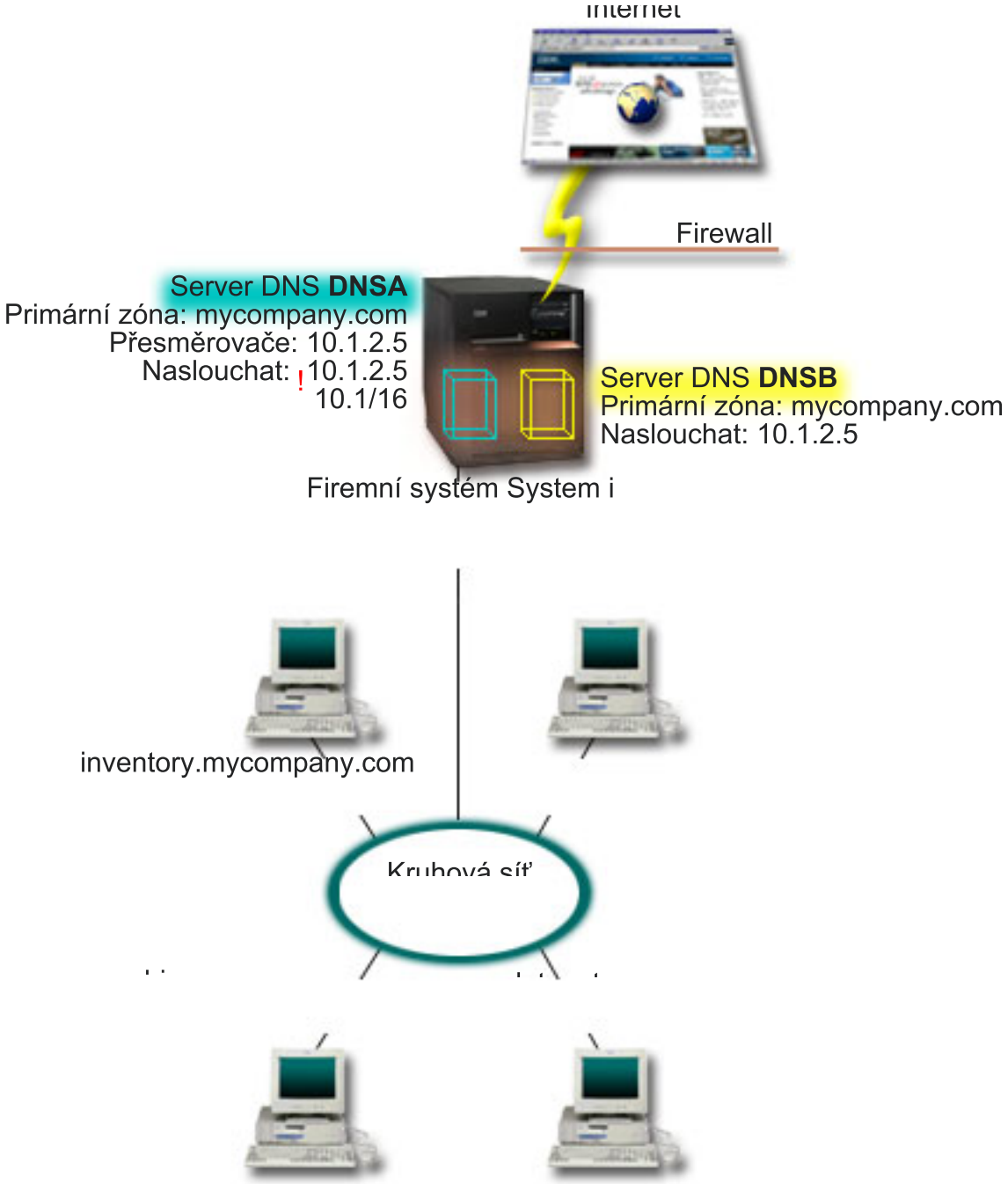
Příklad: DNS a DHCP na různých platformách System i

Příklad: Rozdělení DNS v rámci ochranné bariéry pomocí nastavení dvou serverů DNS na jediném serveru System i

Tento příklad systém popisuje DNS, který pracuje nad ochrannou bariérou (firewall) tak, aby chránil interní data před přístupem z Internetu, zatímco interním uživatelům umožňuje přístup k datům na Internetu. Tato konfigurace umožňuje ochranu pomocí nastavení dvou serverů DNS na jedné platformě System i.

Následující obrázek popisuje jednoduchou podsíť, která používá z bezpečnostních důvodů ochrannou bariéru. 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 byli nějací externí klienti typu resolverschopni přistupovat k její interní síti.

Se systémem DNS i5/OS založeném na standardu BIND 9 toho lze dosáhnout dvěma způsoby. První způsob je ten, že společnost nastaví dvě instance serveru DNS na jednom systému System i, jednu pro Intranet a druhou pro vše ostatní ve veřejné doméně, což je popsáno v tomto příkladu. Druhým způsobem je použít funkci pohledů, kterou poskytuje standard BIND 9, což je popsáno v příkladu o rozdělování systému DNS v rámci ochranné bariéry.



Obrázek 5. Rozdělení DNS v rámci ochranné bariéry pomocí nastavení dvou serverů DNS na jediném systému System i

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, do 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 rozdělování DNS vezměte do úvahy toto nastavení konfigurace:

- Naslouchání

  V ostatních příkladech týkajících se DNS je na platformě System i instalován pouze jeden server DNS. Byl nastaven tak, aby naslouchal na všech IP adresách rozhraní. Pokud máte na platformě System i několik serverů DNS, musíte definovat rozhraní IP adres, na které každý z nich naslouchá. Dva servery DNS nemohou naslouchat na stejné adrese. V tomto případě předpokládejme, 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 v seznamu AML

  Používá 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 položky přístupového seznamu (ACL) v tomto pořadí (!10.1.2.5; 10.1/16). V takovém případě je adresa 10.1.2.5 porovnána s první položkou a je automaticky zamítnuta.

  Jestliže jsou položky uvedeny obráceně (10.1/16; !10.1.2.5), IP adrese 10.1.2.5 je povolen přístup. Server ji totiž porovná s první položkou, jenž odpovídá, a povolí ji bez kontroly zbylých pravidel.

Související odkazy

“Funkce odvětvového standardu BIND 8” na stránce 7
Standard BIND 9 je podobný standardu BIND 8; kromě dynamické aktualizace však nabízí několik funkcí pro zvýšení výkonu vašeho serveru DNS, například funkci pohledů.

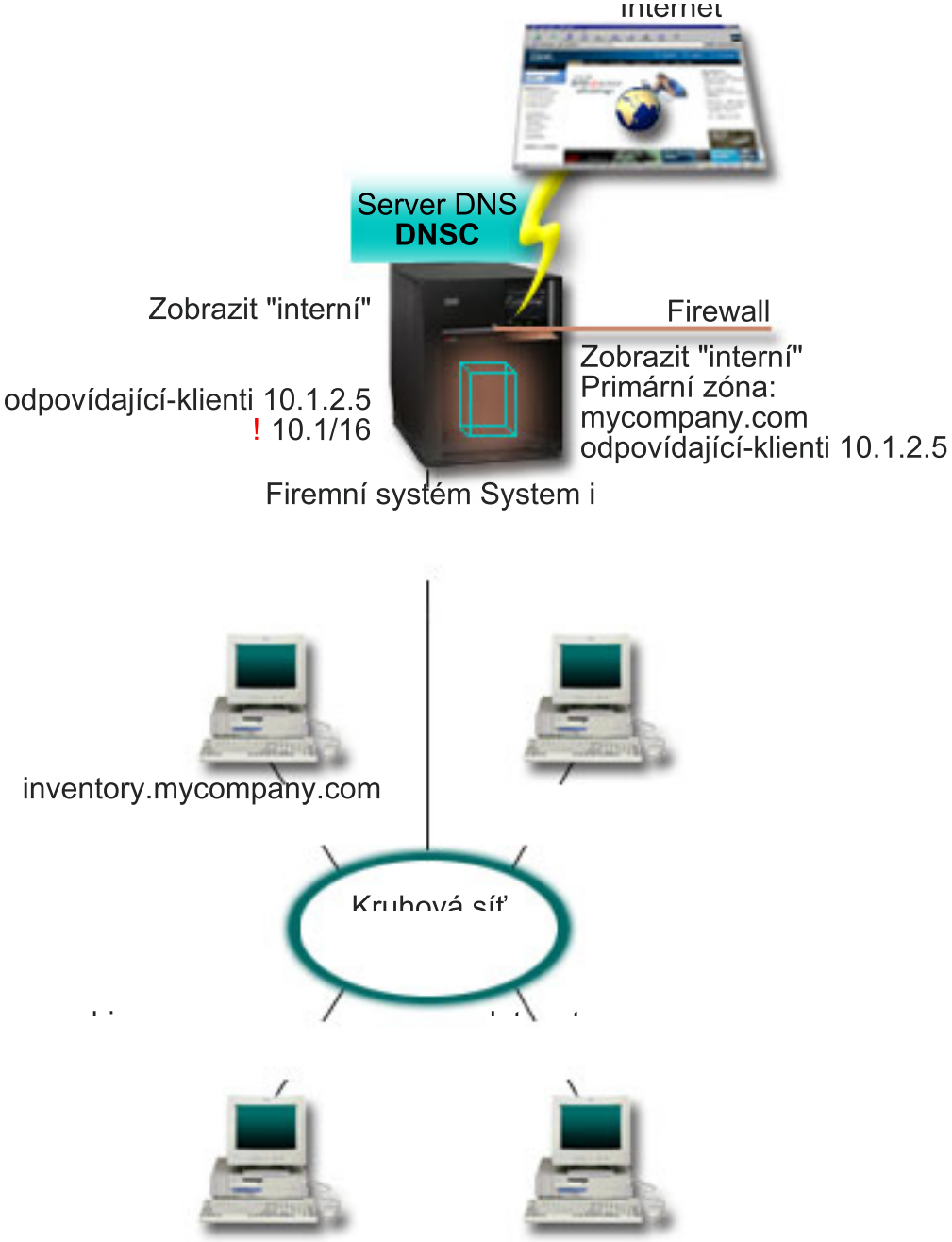
“Příklad: Rozdělení DNS v rámci ochranné bariéry pomocí pohledů”
Tento příklad popisuje DNS (Systém pojmenování domén), který pracuje nad ochrannou bariérou tak, aby chránil interní data před přístupem z Internetu, zatímco interním uživatelům umožňuje přístup k datům na Internetu pomocí funkce *Pohledy* standardu BIND 9.

Příklad: Rozdělení DNS v rámci ochranné bariéry pomocí pohledů

Tento příklad popisuje DNS (Systém pojmenování domén), který pracuje nad ochrannou bariérou tak, aby chránil interní data před přístupem z Internetu, zatímco interním uživatelům umožňuje přístup k datům na Internetu pomocí funkce *Pohledy* standardu BIND 9.

Následující obrázek popisuje jednoduchou podsíť, která používá z bezpečnostních důvodů ochrannou bariéru. 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 sítě. Společnost také chce, aby její interní klienti typu resolver měli přístup k určitým, pouze interním zónám, které nejsou přístupné mimo interní síť. Společnost však nechce, aby byli nějací klienti typu resolver schopni přistupovat k její interní síti.

Se systémem DNS i5/OS založeném na standardu BIND 9 toho lze dosáhnout dvěma způsoby. Způsob, který je popsaný v tomto příkladu, spočívá v tom, že konfigurujete server DNS s dvěma funkcemi pohledů na naslouchání různým dotazům, jeden pro Intranet a druhý pro vše ostatní ve veřejné doméně. Další způsob spočívá v nastavení dvou instancí serveru DNS na jediné platformě System i, což je popsáno v příkladu rozdělení DNS v rámci ochranné bariéry pomocí dvou serverů DNS .



Obrázek 6. Rozdělení DNS v rámci ochranné bariéry použitím funkce pohledů

Server DNS, DNSC definuje dva pohledy, a to *externí* a *interní*. *Externí* pohled je konfigurován s primární zónou mycompany.com, která zahrnuje pouze záznamy prostředků, jež mají být součástí veřejné domény, zatímco *interní* pohled je konfigurován s primární zónou mycompany.com obsahující záznamy prostředků Intranetu.

Jestliže potřebujete sledovat integritu vaší ochranné bariéry a bezpečnostní rizika, máte možnost použít volbu odpovídající-klienti, která vám pomůže ochránit interní data. Chcete-li to udělat, nakonfigurujte interní pohled tak, aby povoloval pouze dotazy na interní zónu mycompany.com od interních hostitelských systémů. Při nastavování rozdělení DNS vezměte do úvahy toto nastavení konfigurace:

- Odpovídající-klienti

Konfigurace odpovídající-klienti ve funkci pohledů použije jako argument seznam adres. Hodnoty konfigurace definované v přiloženém pohledu se zobrazí pouze IP adrese dotazu, která odpovídá adrese v tomto seznamu. Pokud IP adresa dotazu odpovídá několika položkám odpovídajících-klientů v různých příkazech použije se první příkaz pohledu. V tomto případě předpokládejme, že dotazy přicházející z ochranné bariéry budou odeslány na 10.1.2.5. Tyto dotazy by měly být zpracovány zónovými daty v externím pohledu. Proto je adresa 10.1.2.5 nastavena tak, aby byla odpovídajícím-klientem pro externí pohled. Interní pohled 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 v seznamu AML

  Používá 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 položky přístupového seznamu (ACL) v tomto pořadí (!10.1.2.5; 10.1/16). V takovém případě je adresa 10.1.2.5 porovnána s první položkou a je automaticky zamítnuta.

  Jestliže jsou prvky uvedeny obráceně (10.1/16; !10.1.2.5), IP adrese 10.1.2.5 je povolen přístup. Server ji totiž porovná s první položkou, jenž odpovídá, a povolí ji bez kontroly zbylých pravidel.

Související odkazy

"Příklad: Rozdělení DNS v rámci ochranné bariéry pomocí nastavení dvou serverů DNS na jediném serveru System i" na stránce 20
Tento příklad systém popisuje DNS, který pracuje nad ochrannou bariérou (firewall) tak, aby chránil interní data před přístupem z Internetu, zatímco interním uživatelům umožňuje přístup k datům na Internetu. Tato konfigurace umožňuje ochranu pomocí nastavení dvou serverů DNS na jedné platformě System i.

Plánování systému DNS

DNS (Systém pojmenování domén) nabízí řadu řešení. Předtím, než nakonfigurujete DNS, je důležité naplánovat, jak bude fungovat v rámci vaší sítě. Subjekty, jako např. struktura sítě, výkon a zabezpečení ochrany dat by měly být ohodnoceny.

Zjištění oprávnění DNS (Systém pojmenování domén)

Pro administrátora DNS (Systém pojmenování domén) existují zvláštní požadavky na oprávnění. Měli byste promyslet bezpečnostní důsledky oprávnění.

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 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 konfigurují DNS, měli přístup správce systému (Security officer) s oprávněním ke všem objektům (*ALLOBJ). Při přidělování oprávnění uživatelům použijte produkt System i Navigator. Pokud potřebujete další informace, prostudujte si téma Udělení oprávnění administrátorovi DNS v online nápovědě k serveru DNS.

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

Související odkazy

"Údržba konfiguračních souborů DNS (Systém pojmenování domén)" na stránce 34
K vytvoření a údržbě instancí serveru DNS na serveru System i můžete použít server i5/OS. Konfigurační soubory pro DNS jsou spravovány produktem System i Navigator. Tyto soubory nesmíte upravovat ručně. Při vytváření, změnách nebo výmazu konfiguračních souborů DNS používejte vždy produkt System i Navigator.

Určení struktury domény

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

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 (Systém pojmenování domén) jako dynamickou zónu, nemůžete v této zóně 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 znovu 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.

Systém i5/OS DNS poskytuje grafické rozhraní pro konfiguraci vašich systémů. 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 platformě System i jsou organizovány ve složkách 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 nebo AAAA. Zóny pro vyhledávání dozadu jsou zóny, které se používají k mapování IP adres na jména domén, jako např. záznamů PTR.
- Server i5/OS DNS se odkazuje na *primární zóny* a *sekundární zóny*.
- Rozhraní používá *podzóny*, které jsou v některých zdrojích označovány jako *poddomény*. Podřízená zóna typu ″child zone″ je podzóna, za níž jste delegovali odpovědnost jednomu nebo více serverům jmen.

Plánování opatření pro zabezpečení dat

DNS (Systém pojmenování domén) poskytuje volby pro zabezpečení dat, které omezují externí přístup k vašemu serveru.

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, podsíť (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 vyvolat přístupový seznam a celý seznam se zavede.

Pořadí položek seznamu AML

Používá 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 položky seznamu AML v tomto pořadí (!10.1.1.5; 10.1.1/24). V takovém případě bude adresa 10.1.1.5 porovnána s první položkou a bude automaticky zamítnuta.

Jestliže jsou položky obráceně (10.1.1/24; !10.1.1.5), bude IP adrese 10.1.1.5 povolen přístup, protože server ji porovná s první položkou, která jí odpovídá, a povolí ji bez kontroly zbylých pravidel.

Volby kontroly přístupu

DNS umožňuje nastavit omezení, jako např. kdo může odesílat dynamické aktualizace na server, 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 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 předvolba povolit rekurzivní dotazy ze všech hostitelských systémů.

Blackhole
Specifikuje seznam adres, od nichž nepřijímá dotazy, ani je nepoužívá k rozlišení dotazu. Dotazy z těchto adres zůstanou nezodpovězeny.

Zabezpečení vašeho serveru DNS je životně důležité. Kromě pokynů týkajících se zabezpečení ochrany dat uvedených v tomto tématu je zabezpečení serverů DNS a System i popsáno v nejrůznějších zdrojích, včetně tématu System i a Internet v aplikaci informační centrum. Kniha *DNS a BIND* se také zabývá zabezpečením dat v souvislosti s DNS.

Související pojmy

Systém a zabezpečení Internetu

Související odkazy

“Funkce odvětvového standardu BIND 8” na stránce 7
Standard BIND 9 je podobný standardu BIND 8; kromě dynamické aktualizace však nabízí několik funkcí pro zvýšení výkonu vašeho serveru DNS, například funkci pohledů.

Požadavky na DNS (Systém pojmenování domén)

Chcete-li spustit DNS na vaší platformě System i, zvažte tyto softwarové požadavky.

Funkci DNS, volbu 31 nelze instalovat automaticky s operačním systémem. Instalaci DNS musíte specificky vybrat. Server DNS přidaný k systému i5/OS je založený na průmyslovém standardu implementace DNS zvaném BIND 9. Předchozí služby systému OS/400 DNS byly založeny na odvětvovém standardu BIND verze 8.2.5 a jsou dosud ve verzi V5R1 k dispozici v systému i5/OS.

Po instalaci DNS je nutné migrovat a konfigurovat server DNS ze standardu BIND 4 nebo 8 na BIND 9. Rovněž musíte instalovat i5/OS PASE, což je volba 33 systému i5/OS. Po instalaci volby i5/OS PASE produkt System i Navigator automaticky zajistí konfiguraci aktuální implementace BIND.

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

Související pojmy

i5/OS PASE

“Konfigurace systému DNS” na stránce 27
Pomocí produktu System i Navigator lze konfigurovat servery jmen a vyřizovat dotazy mimo vaši doménu.

Související odkazy

“Funkce odvětvového standardu BIND 8” na stránce 7
Standard BIND 9 je podobný standardu BIND 8; kromě dynamické aktualizace však nabízí několik funkcí pro zvýšení výkonu vašeho serveru DNS, například funkci pohledů.

Jak zjistit, zda je systém DNS nainstalovaný

Chcete-li zjistit, zda je nainstalován DNS, postupujte takto.

1. Na příkazovou řádku napište GO LICPGM a stiskněte klávesu Enter.
2. Napište 10 (Display installed licensed programs) a stiskněte Enter.
3. Přestránkujte dolů na **5761SS1 Domain Name System** (volba 31). Je-li DNS úspěšně nainstalován, bude pod Installed Status uvedena hodnota *COMPATIBLE, jak je vidět níže.

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

4. Stisknutím klávesy F3 opusťte obrazovku.

Instalace systému DNS

Chcete-li instalovat DNS (Systém pojmenování domén), postupujte takto.

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 Systém pojmenování domén a stiskněte klávesu Enter.
4. Opětným stisknutím klávesy Enter instalaci potvrďte.

Konfigurace systému DNS

Pomocí produktu System i Navigator lze konfigurovat servery jmen a vyřizovat dotazy mimo vaši doménu.

Dříve než začnete s konfigurací serveru DNS (Systém pojmenování domén), prostudujte si systémové požadavky na DNS, abyste mohli nainstalovat nezbytné komponenty DNS.

Související pojmy

"Požadavky na DNS (Systém pojmenování domén)" na stránce 26
Chcete-li spustit DNS na vaší platformě System i, zvažte tyto softwarové požadavky.

Přístup k serveru DNS v prostředí produktu System i Navigator

Tyto instrukce vás povedou ke konfiguračnímu rozhraní DNS v produktu System i Navigator.

Pokud používáte i5/OS PASE, budete schopni nakonfigurovat servery DNS založené na odvětvovém standardu BIND 9.

Pokud provádíte konfiguraci serveru DNS poprvé, postupujte takto:

1. V prostředí produktu System i Navigator rozbalte ***váš systém*** → **Síť** → **Servery** → **DNS**.
2. Klepněte pravým tlačítkem myši na **DNS** a vyberte volbu **Nová konfigurace**.

Související pojmy

Začínáme s produktem System i Navigator

Konfigurace serverů jmen

DNS (Systém pojmenování domén) umožňuje vytváření vícenásobných instancí serverů jmen. Toto téma poskytuje návod pro konfiguraci serveru jmen.

Server i5/OS DNS založený na odvětvovém standardu BIND 9 podporuje několik instancí serveru jmen. Následující úlohy vás provedou procesem vytvoření jedné instance serveru jmen, včetně jejích vlastností a zón.

Jestliže chcete vytvořit více instancí, opakujte tyto procedury, až vytvoříte všechny požadované instance. Pro každou instanci serveru jmen můžete specifikovat nezávislé vlastnosti, jako např. úrovně ladění (debug levels) a hodnoty automatického spuštění (autostart). Jestliže vytváříte novou instanci, vytvářejí se samostatné konfigurační soubory.

Související odkazy

"Údržba konfiguračních souborů DNS (Systém pojmenování domén)" na stránce 34
K vytvoření a údržbě instancí serveru DNS na serveru System i můžete použít server i5/OS. Konfigurační soubory pro DNS jsou spravovány produktem System i Navigator. Tyto soubory nesmíte upravovat ručně. Při vytváření, změnách nebo výmazu konfiguračních souborů DNS používejte vždy produkt System i Navigator.

Vytvoření instance serveru jmen

Průvodce novou konfigurací DNS vás provede procesem definice instance serveru DNS.

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

1. V prostředí produktu System i Navigator rozbalte ***váš systém*** → **Síť** → **Servery** → **DNS**.
2. V levém podokně klepněte pravým tlačítkem myši na **DNS** a vyberte **Nový server jmen**
3. Při dokončení procesu konfigurace se řiďte pokyny průvodce.

Průvodce požaduje následující vstupní údaje:

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

Naslouchání na IP adresách:
Dva DNS servery nemohou naslouchat na stejné IP adrese. Předvoleným nastavením je naslouchat na všech IP adresách. Pokud vytváříte dodatečné instance serverů, nemohou být konfigurovány tak, aby naslouchaly na všech IP adresách. V opačném případě je nelze spustit současně. 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.

Poznámka: O zavádění předvolených internetových kořenových serverů byste měli uvažovat pouze v tom případě, že máte přístup na Internet 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.

Editování vlastností serveru DNS

Poté, co vytvoříte server jmen, můžete upravit jeho vlastnosti, jako např. povolení aktualizace a úrovně ladění. Tyto volby se týkají pouze té serverové instance, kterou měníte.

Chcete-li upravovat vlastnosti instance serveru DNS (Systém pojmenování domén), postupujte podle těchto kroků:

1. V prostředí produktu System i Navigator rozbalte ***váš systém*** → **Síť** → **Servery** → **DNS**.
2. V pravém podokně klepněte pravým tlačítkem myši na ***server DNS*** a vyberte volbu **Konfigurace**.
3. V okně Konfigurace DNS klepněte pravým tlačítkem myši na **Server DNS** a vyberte **Vlastnosti**.
4. Editujte odpovídající požadované vlastnosti.

Konfigurace zón na serveru jmen

Jakmile nakonfigurujete instanci serveru DNS (Systém pojmenování domén), musíte nakonfigurovat zóny pro server jmen.

Chcete-li konfigurovat na serveru zóny, postupujte takto:

1. V prostředí produktu System i Navigator rozbalte ***váš systém*** → **Síť** → **Servery** → **DNS**.
2. V pravém podokně klepněte pravým tlačítkem myši na ***server DNS*** a vyberte volbu **Konfigurace**.

3. V okně Konfigurace DNS vyberte typ zóny, který chcete vytvořit tak, že klepnete pravým tlačítkem myši buď na složku **Zóna dopředného vyhledávání** nebo na **Zóna zpětného vyhledávání**.
4. Při dokončení procesu vytvoření konfigurace se řiďte pokyny průvodce.

Související pojmy

"Přístup k externím datům DNS (Systém pojmenování domén)" na stránce 30
Jestliže vytvoříte zónová data DNS (Systém pojmenování domén), bude váš server schopen rozlišit dotazy pro tuto zónu.

Související úlohy

"Konfigurace DNS (Systém pojmenování domén) pro přijímání dynamických aktualizací"
Nyní mohou být servery DNS (Systém pojmenování domén) provozující standard BIND 9 konfigurovány tak, aby přijímaly požadavky z ostatních zdrojů a dynamicky aktualizovaly zónová data. Toto téma poskytuje návod, jak nakonfigurovat volbu Povolit aktualizaci tak, aby mohl server DNS přijímat dynamické aktualizace.

"Importování souborů DNS" na stránce 30
Systém DNS může importovat existující soubory zónových dat. Při efektivním vytváření nové zóny z existujícího konfiguračního souboru postupujte podle uvedených procedur.

Související odkazy

"Co jsou zóny" na stránce 3
Data DNS jsou rozdělena do spravovatelných sad dat, které se nazývají *zóny*. A každá z těchto sad je specifickým typem zóny.

Konfigurace funkce pohledů na serveru jmen

Jednou z funkcí, kterou nabízí standard BIND 9 je funkce *pohledů*, která umožňuje instanci DNS odpovídat na dotazy rozdílně v závislosti na tom, odkud dotaz pochází, například z Internetu nebo Intranetu. Jedna praktická aplikace funkce pohledů je rozdělit nastavení bez toho, aby bylo nutné spustit několik serverů DNS.

Chcete-li konfigurovat na serveru funkci pohledů, postupujte takto:

1. V prostředí produktu System i Navigator rozbalte ***váš systém*** → **Síť** → **Servery** → **DNS**.
2. V pravém podokně klepněte pravým tlačítkem myši na ***server DNS*** a vyberte volbu **Konfigurace**.
3. V okně Konfigurace DNS klepněte pravým tlačítkem myši na **Pohledy** a vyberte **Vlastnosti**.
4. Při dokončení procesu vytvoření konfigurace se řiďte pokyny průvodce.

Konfigurace DNS (Systém pojmenování domén) pro přijímání dynamických aktualizací

Nyní mohou být servery DNS (Systém pojmenování domén) provozující standard BIND 9 konfigurovány tak, aby přijímaly požadavky z ostatních zdrojů a dynamicky aktualizovaly zónová data. Toto téma poskytuje návod, jak nakonfigurovat volbu Povolit aktualizaci tak, aby mohl server DNS přijímat dynamické aktualizace.

Při vytváření dynamických zón byste měli zvážit strukturu vaší sítě. Pokud části vaší domény stále vyžadují ruční aktualizace, možná budete uvažovat o nastavení samostatné statické a dynamické zóny. Jestliže potřebujete provádět ruční aktualizace do dynamické zóny, musíte zastavit server dynamické zóny a opět jej spustit poté, co dokončíte aktualizace. Zastavení serveru si vynutí aktualizaci všech dynamických aktualizací, které byly provedeny, jelikož server poprvé zavedl svá zónová data ze zónové databáze. Pokud server nezastavíte, přijdete o všechny ruční aktualizace databáze zóny, protože budou přepsány spuštěným serverem. 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 System i Navigator rozbalte ***váš systém*** → **Síť** → **Servery** → **DNS**.
2. V pravém podokně klepněte pravým tlačítkem myši na ***server DNS*** a vyberte volbu **Konfigurace**.
3. V okně Konfigurace DNS rozbalte volbu **Zóna pro vyhledávání dopředu** nebo **Zóna pro vyhledávání dozadu**.
4. Klepněte pravým tlačítkem myši na primární zónu, kterou chcete upravit, a vyberte volbu **Vlastnosti**.

5. Na stránce Vlastnosti primární zóny klepněte na kartu **Volby**.
6. Na stránce Volby rozbalte **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.

Související úlohy

"Konfigurace zón na serveru jmen" na stránce 28
Jakmile nakonfigurujete instanci serveru DNS (Systém pojmenování domén), musíte nakonfigurovat zóny pro server jmen.

Konfigurace DHCP pro zasílání dynamických aktualizací na DNS

Importování souborů DNS

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

Primární zónu můžete vytvořit tak, že naimportujete soubor zónových dat, který je platným konfiguračním souborem zónových dat založeným 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 zadanou instanci serveru.

Chcete-li importovat zónový soubor, postupujte takto:

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

Související úlohy

"Konfigurace zón na serveru jmen" na stránce 28
Jakmile nakonfigurujete instanci serveru DNS (Systém pojmenování domén), musíte nakonfigurovat zóny pro server jmen.

Ověření platnosti 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.

Poznámky:

1. Importování velké primární domény může trvat i několik minut.
2. 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 (Systém pojmenování domén)

Jestliže vytvoříte zónová data DNS (Systém pojmenování domén), bude váš server schopen rozlišit dotazy pro tuto zónu.

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 směrují server DNS k ostatním serverům v hierarchii, dokud není nalezena odpověď nebo dokud se nezjistí, že odpověď neexistuje.

Předvolený seznam kořenových adresářů produktu System i 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 System i Navigator poskytuje předvolený seznam internetových kořenových serverů. Seznam je aktuální v okamžiku vydání produktu System i 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.

Získání adres 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. Pomocí protokolu FTP (File Transfer Protocol) se anonymně přihlaste k serveru InterNIC: FTP.INTERNIC.NET nebo RS.INTERNIC.NET
2. Stáhněte tento soubor: /domain/named.root
3. Uložte soubor do adresářové cesty: /QOpenSys/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 přesměrovávat na ochrannou bariéru DNS (firewall). V tomto případě působí ochranná bariéra DNS jako přesměrovač.

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.

Související úlohy

"Konfigurace zón na serveru jmen" na stránce 28
Jakmile nakonfigurujete instanci serveru DNS (Systém pojmenování domén), musíte nakonfigurovat zóny pro server jmen.

Správ systému DNS

Správa systému DNS (Domain Name System) spočívá v ověření, zda funkce DNS pracují, v monitorování výkonu a údržbě dat a souborů DNS.

Ověření funkčnosti systému DNS

Nástroj DIG (Domain Information Groper) vám může pomoci ve sběru informací serveru DNS a testovat jeho odpovědi. Nástroj DIG lze použít k ověření toho, zda pracuje server DNS správně.

Požadujte hostitelské jméno, které je asociované s IP adresou pro smyčkový test (127.0.0.1). Odpovědí by mělo být hostitelské jméno (localhost). Můžete se rovněž dotazovat na specifická jména definovaná 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 DIG, postupujte takto:

1. Na příkazovou řádku napište DIG HOSTNAME('127.0.0.1') REVERSE(*YES).
   Měly by se zobrazit níže uvedené informace včetně hostitelského jména pro smyčkový test:

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

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

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

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

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

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

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

2. Stisknutím klávesy Enter ukončíte relaci.

Poznámka: Pokud potřebujete pomoc při použití funkce DIG, napište ?DIG a stiskněte Enter.

Správa bezpečnostních klíčů

Bezpečnostní klíče umožňují omezit přístup k datům vašeho serveru DNS (Systém pojmenování domén).

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

Klíče pro správu DNS

Klíče pro správu DNS jsou definovány pro BIND a používá je DNS server jako součást ověřování příchozí aktualizace.

Klíč můžete konfigurovat a přiřadit mu jméno. Potom, když chcete chránit nějaký objekt DNS, např. dynamickou zónu, můžete tento klíč specifikovat v seznamu AML.

Při správě klíčů DNS postupujte takto:

1. V prostředí produktu System i Navigator rozbalte ***váš systém*** → **Síť** → **Servery** → **DNS**.
2. V pravém podokně klepněte pravým tlačítkem myši na instanci serveru DNS, kterou chcete spravovat, a vyberte volbu **Konfigurace**.
3. V okně Konfigurace DNS vyberte **Soubor** → **Správa klíčů**.

V okně Správa klíčů můžete provádět odpovídající úlohy správy.

Klíče pro správu dynamické aktualizace

Klíče pro dynamickou aktualizaci se používají k zabezpečení dynamických aktualizací u serveru DHCP (protokol dynamické konfigurace hostitele).

Tyto klíče musí být přítomny, pokud jsou servery DNS (Systém pojmenování domén) a DHCP na jedné platformě System i. Pokud je DHCP na jiné platformě System i, musíte distribuovat stejné soubory klíčů pro dynamickou aktualizaci na každou platformu System i, která je potřebuje pro poslání dynamických aktualizací na směrodatné servery. Můžete je distribuovat pomocí FTP, e-mailu, apod.

Při správě klíčů pro dynamickou aktualizaci postupujte takto:

1. V prostředí produktu System i Navigator rozbalte ***váš systém*** → **Síť** → **Servery** → **DNS**.

2. Klepněte pravým tlačítkem myši **DNS** a vyberte **Správa klíčů pro dynamickou aktualizaci**.

V menu Správa klíčů pro dynamickou aktualizaci můžete provádět odpovídající úlohy správy.

Přístup ke statistikám serveru DNS

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

DNS (Systém pojmenování domén) poskytuje několik diagnostických nástrojů, které mohou být využity k monitorování výkonu vašeho serveru.

Související odkazy

"Údržba konfiguračních souborů DNS (Systém pojmenování domén)" na stránce 34
K vytvoření a údržbě instancí serveru DNS na serveru System i můžete použít server i5/OS. Konfigurační soubory pro DNS jsou spravovány produktem System i Navigator. Tyto soubory nesmíte upravovat ručně. Při vytváření, změnách nebo výmazu konfiguračních souborů DNS používejte vždy produkt System i Navigator.

Přístup ke statistikám serveru

Statistika serveru sumarizuje počet dotazů a odpovědí, které server obdržel od posledního opětného spuštění nebo od opětného zavedení databáze.

DNS (Systém pojmenování domén) umožňuje prohlížení statistiky pro instanci serveru. 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 System i Navigator rozbalte ***váš systém*** → **Síť** → **Servery** → **DNS**.
2. V pravém podokně klepněte pravým tlačítkem myši na ***server DNS*** a vyberte volbu **Konfigurace**.
3. V okně Konfigurace DNS vyberte **Zobrazit** → **Statistika serveru**.

Chcete-li zobrazit informace o statistikách serveru v souboru named.stats, můžete také použít příkaz RNDC (Vzdálené ovládání démona jmen). Odpovídající příkaz je tento.

```
RNDC RNDCCMD('stats')
```

Přístup k databázi aktivního serveru

Databáze aktivního serveru 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), které mohou být užitečné při zjišťování problému.

DNS (Systém pojmenování domén) umožňuje prohlížení výpisu spolehlivých 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.

Výpis databáze aktivního serveru si můžete prohlížet pomocí produktu System i Navigator. Jestliže potřebujete uložit kopii souborů, je jméno souboru s výpisem databáze named_dump.db v adresářové cestě serveru i5/OS: /QIBM/UserData/OS400/DNS/<instance serveru>/, kde <*instance serveru*> 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 System i Navigator rozbalte ***váš systém*** → **Síť** → **Servery** → **DNS**.
2. V pravém podokně klepněte pravým tlačítkem myši na ***server DNS*** a vyberte volbu **Konfigurace**.
3. V okně Konfigurace DNS vyberte **Zobrazit** → **Databáze aktivního serveru**.

Chcete-li zobrazit informace o databázi aktivního serveru v souboru names_dump.db, můžete také použít příkaz RNDC (Vzdálené ovládání démona jmen). Odpovídající příkaz je tento.

```
RNDC RNDCCMD('dumpdb -all')
```

Údržba konfiguračních souborů DNS (Systém pojmenování domén)

K vytvoření a údržbě instancí serveru DNS na serveru System i můžete použít server i5/OS. Konfigurační soubory pro DNS jsou spravovány produktem System i Navigator. Tyto soubory nesmíte upravovat ručně. Při vytváření, změnách nebo výmazu konfiguračních souborů DNS používejte vždy produkt System i Navigator.

Konfigurační soubory DNS jsou uloženy na níže uvedených cestách integrovaného systému souborů.

Poznámka: Struktura souborů uvedená níže se vztahuje na servery DNS provozované na BIND 9.

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	Ikona	Popis
/QIBM/UserData/OS400/DNS/		Adresář výchozího bodu pro DNS.
/QIBM/UserData/OS400/DNS/ <*instance-n*>/		Adresář výchozího bodu pro instanci serveru DNS.
ATRIBUTY		DNS používá tento soubor k určení používané verze odvětvového standardu BIND.
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 9. Slouží jako záloha migrace a může být vymazán, pokud server BIND 9 pracuje správně.
named.ca		Seznam kořenových serverů pro tuto instanci.
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.
named_dump.db		Výpis dat serveru vytvořený pro databáze aktivního serveru.
named.memstats		Statistiky paměti serveru (pokud je konfigurováno v named.conf).
named.pid		Udržuje ID procesu provozovaného 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.
named.random		Soubor typu ″entropy″ generovaný serverem.

Jméno	Ikona	Popis
named.recursing		Dotazy serverů, které jsou rekurzivní (pokud jsou vyžádány produktem System i Navigator).
named.run		Předvolený protokol ladění (pokud je vyžádán). Může být změněn na named.run.0 nebo named.run.1.
named.stats		Statistika serveru.
<*primární-zóna-n*>.db		Toto je soubor primární zóny určité domény na tomto serveru. Tento soubor obsahuje všechny zdrojové záznamy pro tuto zónu. Každá zóna má samostatný soubor typu .db.
<*primární zóna-n*>.jnl		Soubor žurnálu, který uchovává dynamické aktualizace zóny. Je vytvořen v okamžiku obdržení první dynamické aktualizace. Pokud je server restartován po vypnutí nebo selhání, přehraje soubor žurnálu a zahrne tak do zóny všechny aktualizace, ke kterým došlo po posledním výpisu zóny. Tento soubor je rovněž používán pro přenosy IXFR (incremental zone transfers). Tento typ souborů protokolu nezmizí. Je to binární soubor a neměli byste jej editovat.
db.<*sekundární-zóna-n*>		Soubor sekundární zóny určité domény na tomto serveru. Obsahuje všechny zdrojové záznamy pro tuto zónu. Tento soubor se používá k počátečnímu zavedení sekundárního serveru při spuštění, pokud je primární server nedostupný. Každá zóna má samostatný soubor typu .db.
/QIBM/UserData/OS400/DNS/_DYN/		Adresář, který uchovává soubory požadované pro dynamickou aktualizaci.
<*id-klíče-n*>._KEY		Symbolický odkaz na klíč DNSSEC s klíčem <*id_klíče-n*>. Vždy ukazuje na poslední vytvořený klíč K<*id_klíče-n*>.+*aaa*+*nnnnn*.key.
<*id_klíče-x*>._DUK. <*zóna-a*>		Klíč pro dynamickou aktualizaci požadovaný k inicializaci požadavku na dynamickou aktualizaci v zóně <*zóna-a*> pomocí klíče <*id_klíče-x*>.
<*id_klíče-x*>._KID		Soubor obsahující klíčový povel pro klíč s názvem <*id_klíče-x*>
<*id_klíče-y*>._DUK. <*zóna-a*>		Klíč pro dynamickou aktualizaci požadovaný k inicializaci požadavku na dynamickou aktualizaci v zóně <*zóna-a*> pomocí klíče <*id_klíče-y*>.
<*id_klíče-y*>._DUK. <*zóna-b*>		Klíč pro dynamickou aktualizaci požadovaný k inicializaci požadavku na dynamickou aktualizaci v zóně <*zóna-b*> pomocí klíče <*id_klíče-y*>.

Jméno	Ikona	Popis
<*id_klíče-y*>._KID		Soubor obsahující klíčový povel pro klíč s názvem <*id_klíče-y*>
rndc-confgen.random.*nnnnnn*		Soubory typu ″entropy″ pro různé příkazy, které je potřebují. Část *nnnnn* je číslo úlohy, která byla vytvořeny souborem. Ty jsou ponechány pouze v případě, že je příkaz z nějakého důvodu přerušen a neprovede vyčištění.

Související pojmy

“Zjištění oprávnění DNS (Systém pojmenování domén)” na stránce 24
Pro administrátora DNS (Systém pojmenování domén) existují zvláštní požadavky na oprávnění. Měli byste promyslet bezpečnostní důsledky oprávnění.

“Přístup ke statistikám serveru DNS” na stránce 33
Nástroje pro výpis databáze a statistiky vám mohou pomoci revidovat a spravovat výkon serveru.

Související úlohy

“Konfigurace serverů jmen” na stránce 27
DNS (Systém pojmenování domén) umožňuje vytváření vícenásobných instancí serverů jmen. Toto téma poskytuje návod pro konfiguraci serveru jmen.

Rozšířené funkce DNS (Systém pojmenování domén)

Toto téma vysvětluje, jak zkušení administrátoři mohou používat rozšířené funkce DNS (Systém pojmenování domén) ke snazší správě serveru DNS.

Systém DNS v produktu System i Navigator poskytuje rozhraní s rozšířenými funkcemi pro konfiguraci a správu vašeho serveru DNS. Níže uváděné úlohy představují zkrácený výběr příkazů pro administrátory, kteří mají zkušenosti s grafickým rozhraním serveru i5/OS. Nabízejí rychlé metody pro změnu stavu serveru a atributů několika instancí serveru současně.

Související úlohy

“Změna nastavení DNS (Systém pojmenování domén)” na stránce 39
Funkce ladění DNS (Systém pojmenování domén) může poskytovat informace, které vám mohou pomoci určit a opravit závady serveru DNS.

Spuštění a zastavení serverů DNS (Systém pojmenování domén)

Pokud systém DNS v prostředí produktu System i Navigator neumožňuje spustit nebo ukončit současně několik instancí serveru, můžete použít znakové rozhraní a změnit tato nastavení pro více instancí současně.

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 ENDTCPSVR SERVER(*DNS) DNSSVR(*ALL).

Změna hodnot ladění

Pro administrátory, kteří spravují rozsáhlé zóny a kteří nechtějí mít velké objemy ladících dat vznikajících při prvním spuštění serveru a zavedení všech zónových dat, je užitečné změnit úroveň ladění.

DNS v prostředí produktu System i Navigator neumožňuje měnit úroveň ladění, zatímco je server v provozu. Ke změně úrovně ladění za běhu serveru však můžete použít znakově orientované rozhraní. Jestliže chcete změnit úroveň ladění pomocí znakově orientovaného rozhraní, postupujte podle níže uvedených kroků a výraz *nnnnn* v příkazu nahraďte jménem instance serveru:

1. Na příkazovou řádku napište ADDLIBLE QDNS a stiskněte klávesu Enter.
2. Změňte úroveň ladění:

- Pokud chcete ladění zapnout nebo zvýšit úroveň ladění o 1, napište RNDC RNDCCMD('trace') a stiskněte klávesu Enter.
- Pokud chcete ladění vypnout, napište RNDC RNDCCMD('notrace') a a stiskněte klávesu Enter.

Odstraňování problémů se systémem DNS

Nastavení vytváření protokolů a ladění DNS vám může pomoci při řešení problémů s vaším serverem 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.

Identifikace úloh

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

- V případě, že provozujete servery založené na standardu BIND 9, 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.

Protokolování zpráv serveru DNS (Systém pojmenování domén)

DNS (Systém pojmenování domén) 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.

Odvětvový standard BIND 9 nabízí několik voleb pro vytváření protokolů (protokolování). Můžete specifikovat, jaký typ zpráv bude protokolován, kam se každá zpráva odesílá a jak závažné zprávy se protokolují. Předvolené nastavení vytváření protokolů je obvykle vyhovující. Jestliže je však budete chtít změnit, doporučujeme, abyste si prostudovali další zdroje informací o standardu BIND 9 a protokolování.

Protokolovací kanály

Server DNS může protokolovat 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 i5os_debug a i5os_QPRINT. Podle předvolby jsou ladicí zprávy protokolovány do kanálu i5os_debug, kterým je soubor named.run. Můžete ale zadat, aby se do tohoto souboru odesílaly také ostatní kategorie zpráv. Kategorie zpráv protokolovaných v i5os_QPRINT jsou odesílány do souboru pro souběžný tisk QPRINT pro uživatelský profil QTCP. Kromě předvolených 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 i5os_joblog. Protokolované zprávy směrované k tomuto kanálu jsou odesílány do protokolu úlohy instance serveru DNS.
- **Kanály Null channels**

Všechny zprávy předávané do kanálů Null channels jsou vymazány. Předvolený kanál Null channel je i5os_null. Ke kanálu Null channel můžete směrovat 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. Jsou to tyto kategorie:

client Zpracovávání požadavků klienta.

config Analýza a zpracování konfiguračního souboru.

database
Zprávy vztahující se k databázím, které se používají interně serverem DNS k uložení zóny a dat mezipaměti.

default Definice voleb přihlašování pro ty kategorie, kde nebyla definována žádná specifická konfigurace.

delegation-only
Pouze pověření. Zapíše do protokolu dotazy, které byly vynuceny na NXDOMAIN v důsledku zóny typu ″delegation-only″ nebo ″delegation-only″ v pokynu nebo stubu deklarace zóny.

dispatch
Odeslání příchozích paketů do modulů serverů, kde budou zpracovány.

dnssec Zpracování protokolu DNSSEC (DNS Security Extensions) a TSIG (Transaction Signature).

general
Svodná kategorie používaná pro záležitosti, které nejsou uvedeny v ostatních kategoriích.

lame-servers
Vadné servery, které jsou špatně nakonfigurovány ve vzdálených serverech, objevené standardem BIND 9 při pokusu o dotaz na tyto servery během rozpoznávání.

network
Síťové operace.

notify Protokol NOTIFY.

resolver
Rozlišení DNS, jako je rekurzivní vyhledávání, které jménem klientů provádí server typu caching name server.

security
Povolení a zamítnutí požadavků.

xfer-in Přenosy zón, které server přijímá.

xfer-out
Přenosy zón, které server odesílá.

unmatched
Jmenované zprávy, u kterých nebylo možné určit třídu nebo u nich nebyl žádný odpovídající pohled. Rovněž je zapsán jednořádkový přehled do kategorie klienta. Nejlépe je tuto kategorii poslat do souboru nebo stderr. Standardně je poslána do kanálu null.

update Dynamické aktualizace.

update-security
Povolení a zamítnutí požadavků na aktualizaci. Dotazy určují, kde by měly být dotazy zapsány. Při spuštění lze prostřednictvím specifikování kategorií dotazů povolit zapisování dotazů do protokolů. Výjimkou je případ, kdy je specifikována volba querylog.

| Položka protokolu dotazu poskytne sestavu s klientovu IP adresou a číslem portu, jménem dotazu, třídou a
| typem. Rovněž hlásí, zda je nastaven příznak typu Recursion Desired (+ pokud je nastaven, - pokud není
| nastaven), zda se používá EDNS (E) a zda byl dotaz podepsán (S).

| Soubor protokolu se neustále zvětšuje a lze jej pravidelně vymazávat. Veškerý obsah souboru protokolu DNS je
| vymazán při ukončení a spuštění serveru DNS.

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

Protokolovány budou 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 úroveň Debug, můžete specifikovat hodnotu od 0 do 11, pro niž chcete, aby byly ladicí zprávy protokolovány.

Změna nastavení vytváření protokolů

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

1. V prostředí produktu System i Navigator rozbalte ***váš systém*** → **Síť** → **Servery** → **DNS**.
2. V pravém podokně klepněte pravým tlačítkem myši na ***server DNS*** a vyberte volbu **Konfigurace**.
3. V okně Konfigurace DNS klepněte pravým tlačítkem myši na **Server DNS** a vyberte **Vlastnosti**.
4. V okně Vlastnosti serveru vyberte kartu **Kanály** a vytvořte nové kanály typu file channels nebo vlastnosti kanálu, jako je např. závažnost zpráv protokolovaných pro každý kanál.
5. V okně Vlastnosti serveru vyberte kartu **Vytváření protokolů**, abyste mohli specifikovat, které kategorie budou protokolovány do jednotlivých kanálů.

Rada k odstraňování problémů o úrovni závažnosti

Předvolená úroveň závažnosti kanálu i5os_joblog je nastavená na hodnotu Error. Toto nastavení se používá k tomu, aby se snížil objem informačních zpráv a varování, které mohou 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 i5os_joblog na Warning, Notice nebo Info, abyste si mohli zobrazit více protokolovaných dat. Jakmile problém vyřešíte, nastavte opět úroveň závažnosti na původní hodnotu Error, čímž snížíte množství zpráv v protokolu úlohy.

Změna nastavení DNS (Systém pojmenování domén)

Funkce ladění DNS (Systém pojmenování domén) může poskytovat informace, které vám mohou pomoci určit a opravit závady serveru DNS.

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). Doporučuje se, abyste při pokusu o odstranění závad nejdříve použili protokoly.

Platné úrovně ladění jsou 0 až 11. Servisní zástupce IBM vám pomůže určit odpovídající hodnotu ladění pro diagnostikování vašeho problému se serverem DNS. Hodnoty 1 nebo vyšší zapíší informaci ladění do souboru named.run v adresářové cestě systému i5/OS: /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. 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 System i Navigator rozbalte ***váš systém*** → **Síť** → **Servery** → **DNS**.
2. V pravém podokně klepněte pravým tlačítkem myši na ***server DNS*** a vyberte volbu **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 v provozu, zastavte jej a potom jej restartujte.

Poznámka: Změny úrovně ladění se neuplatní, dokud server není restartován. Zde nastavená úroveň ladění se použije při příštím úplném restartu serveru. Pokud potřebujete změnit úroveň ladění za běhu serveru, prostudujte si téma Rozšířené funkce DNS.

Související pojmy

"Rozšířené funkce DNS (Systém pojmenování domén)" na stránce 36
Toto téma vysvětluje, jak zkušení administrátoři mohou používat rozšířené funkce DNS (Systém pojmenování domén) ke snazší správě serveru DNS.

Související informace o DNS (Systém pojmenování domén)

IBM Redbooky, webové stránky a ostatní témata aplikace Informační centrum obsahují informace vztahující se ke kolekci témat o systému DNS. Kterýkoli z těchto dokumentů ve formátu PDF si můžete zobrazit a vytisknout.

IBM Redbooky

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

Tyto publikace Redbooks popisují podporu serveru DNS (Domain Name Server)a serveru DHCP (Dynamic Host Configuration Protocol), která je zahrnuta v operačním systému i5/OS. Tyto příklady vám pomohou při instalaci, úpravách, konfiguraci a odstraňování problémů v serverech DNS a DHCP.

Webové stránky

- *DNS and BIND*, páté vydání. Paul Albitz a Cricket Liu. Vydáno společností O'Reilly and Associates,Inc. Sebastopol, California, 2006. Číslo ISBN: 0-59610-057-4.
- The BIND Administrator Reference Manual (verze v PDF) z webových stránek Internet System Consortium (ISC) .
- Webová stránka Internet Software Consortium obsahuje zprávy, odkazy a další zdroje informací pro BIND.
- Webová stránka InterNIC udržuje adresář všech registrátorů, jmen domén, kteří mají autorizaci od společnosti ICANN (Internet Corporation for Assigned Names and Numbers).
- Publikace 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 .

Související odkazy

“PDF soubor pro server DNS” na stránce 2
Soubor PDF s těmito informacemi můžete zobrazit nebo vytisknout.

Dodatek. Poznámky

Tyto informace platí pro produkty a služby nabízené v USA.

IBM nemusí v ostatních zemích nabízet 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 IBM neznamená a ani z něj nelze vyvozovat, že smí být použit pouze uvedený produkt, program či služba společnosti IBM. Použít 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.

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 Česká republika, spol. s r.o.
North Castle Drive
Armonk, NY 10504-1785
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 106-0032, 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 VÝSLOVNĚ NEBO VYPLÝVAJÍCÍCH Z OKOLNOSTÍ VČETNĚ, A TO ZEJMÉNA, ZÁRUK NEPORUŠENÍ PRÁV TŘETÍCH STRAN, PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL VYPLÝVAJÍCÍCH Z OKOLNOSTÍ. Právní řády některých zemí nepřipouštějí vyloučení záruk vyjádřených výslovně nebo vyplývajících z okolností 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. IBM má právo kdykoliv bez upozornění zdokonalovat nebo měnit produkty a programy popsané v této publikaci.

Jakékoliv 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 serverech nejsou součástí materiálů k tomuto produktu IBM a užívání informací z takových webových serverů je na vaše 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 YBWA
Česká republika

Rochester, MN 55901
U.S.A.

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

Licencovaný program popsaný v tomto dokumentu a veškeré licencované materiály k tomuto programu poskytuje IBM na základě podmínek smlouvy IBM Customer Agreement, Mezinárodní licenční smlouvy IBM pro programy, Licenční smlouvy IBM na strojový kód nebo jiné ekvivalentní smlouvy s IBM.

Všechna zde obsažená data týkající se výkonu byla zjištěna v řízeném prostředí. Výsledky získané v jiných provozních prostředích se proto mohou významně lišit. Některá měření mohla být prováděna v systémech na úrovni vývoje a nelze tedy zaručit, že tato měření budou ve všeobecně dostupných systémech stejná. Některá měření mohla být navíc odhadnuta pomocí extrapolace. Skutečné výsledky se mohou lišit. Uživatelé tohoto dokumentu by si měli ověřit použitelnost dat pro svoje specifické prostředí.

Informace, týkající se produktů jiných firem než IBM, byly získány od dodavatelů těchto produktů, z jejich publikovaných sdělení, nebo z jiných veřejně dostupných zdrojů. IBM nezkoumala tyto produkty a nemůže tudíž potvrdit spolehlivost, kompatibilitu a další prohlášení vztahující se k těmto produktům. Dotazy, které se týkají vlastností produktů od jiných dodavatelů, musí být adresovány příslušným dodavatelům.

Veškerá prohlášení týkající se budoucích trendů nebo strategií IBM podléhají změnám bez předchozího upozornění a představují pouze cíle a záměry.

Tyto publikace obsahují příklady údajů a sestav, používaných v každodenních obchodních činnostech. Abyste si udělali co neúplnější představu, obsahují příklady názvy konkrétních podniků, firemních značek a produktů. Všechny tyto názvy jsou fiktivní a jakákoliv podobnost se jmény a adresami, používanými ve skutečných obchodních podnicích, je čistě náhodná.

COPYRIGHT

Tyto informace obsahují vzorové aplikační programy ve zdrojovém jazyce, které demonstrují techniku programování na různých operačních systémech. Jste oprávněni bezplatně, tj. aniž by Vám vznikl jakýkoli finanční závazek vůči IBM, kopírovat, modifikovat a distribuovat tyto vzorové programy v jakékoliv formě, a to pro účely vývoje, užívání, marketingu nebo distribuce aplikačních programů vhodných pro rozhraní API pro operační platformu, pro kterou byly vzorové programy napsány. Tyto příklady nebyly přísně testovány za všech podmínek. IBMproto nezaručuje ani nenaznačuje spolehlivost, provozuschopnost a funkčnost těchto programů.

Každá kopie nebo oblast těchto vzorových programů nebo odvozených prací musí zahrnovat níže uvedenou copyrightovou výhradu:

© (jméno Vaší společnosti) (rok). Části tohoto kódu jsou odvozeny ze vzorových programů IBM Corp. © Copyright IBM Corp. _zadejte rok nebo roky_. Všechna práva vyhrazena.

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

Informace programovacího rozhraní

Tato příručka Domain Name System (DNS) dokumentuje zamýšlena programovací rozhraní, která zákazníkům umožňují psát programy za účelem získání služeb operačního systému IBM i5/OS.

Ochranné známky

Následující výrazy jsou ochranné známky společnosti International Business Machines Corporation ve Spojených státech a případně v dalších jiných zemích:

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

Adobe, logo Adobe, PostScript a logo PostScript jsou buď registrované ochranné známky, nebo ochranné známky společnosti Adobe Systems Incorporated ve Spojených státech a případně v dalších jiných zemích.

Názvy jiných společností, produktů nebo služeb mohou být ochrannými nebo servisními známkami jiných společností.

Ustanovení a podmínky

Oprávnění k užívání těchto publikací je uděleno na základě následujících ustanovení a podmínek.

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 nebo jakékoliv 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 jeho 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. TYTO PUBLIKACE JSOU POSKYTOVÁNY NA BÁZI ″JAK JSOU″ (AS-IS), BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH VÝSLOVNĚ NEBO VYPLÝVAJÍCÍCH Z OKOLNOSTÍ VČETNĚ, A TO ZEJMÉNA, ZÁRUK PRODEJNOSTI, NEPORUŠENÍ PRÁV TŘETÍCH STRAN A VHODNOSTI PRO URČITÝ ÚČEL VYPLÝVAJÍCÍCH Z OKOLNOSTÍ.

Vytištěno v Dánsku společností IBM Danmark A/S.