Systémy IBM - iSeries

Vytváření sítí
Domain Name System

Verze 5, vydání 4

Systémy IBM - iSeries

Vytváření sítí
Domain Name System

Verze 5, vydání 4

Poznámka

Dříve než použijete tyto informace a produkt, který podporují, nezapomeňte si přečíst informace uvedené v části “Poznámky”, na stránce 37.

Šesté vydání (únor 2006)

Toto vydání se týká verze 5, vydání 4, modifikace 0 operačního systému IBM i5/OS (5722-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)

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

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

V systému IBM OS/400, verzi 5, vydání 1 (V5R1) jsou služby DNS založeny na implementaci DNS, která je průmyslovým standardem a která je známá jako BIND (Berkeley Internet Name Domain) verze 8. Předchozí služby IBM OS/400 DNS byly založeny na standardu BIND, verze 4.9.3. Aby bylo možné používat nový server DNS založený na standardu BIND 8, musí být na vašem serveru IBM eServer iSeries nainstalována volba 33 operačního systému i5/OS - PASE (Portable Application Solutions Environment). Přestože nepoužíváte volbu PASE, můžete provozovat tentýž server DNS založený na standardu BIND verze 4.9.3, který byl k dispozici v předcházejících vydáních. Avšak migrace na BIND 8 umožňuje lepší funkci a přináší vyšší zabezpečení pro váš DNS server.

Poznámka: Toto téma pojednává o nových funkcích založených na BIND 8. Jestliže ke spuštění serveru DNS nepoužíváte PASE založený na BIND 8, prostudujte si téma V4R5 DNS information center uvádějící informace o serveru DNS založeném na BIND 4.9.3.

Tisknutelný soubor PDF

Tuto volbu použijte k prohlížení a tisku těchto informací v souboru PDF.

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 soubor PDF v prohlížeči (klepněte na výše uvedený odkaz).
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 společnosti Adobe (www.adobe.com/products/acrobat/readstep.html)  .

Koncepty DNS (Systém pojmenování domén)

Toto téma vysvětluje, co je DNS (Systém pojmenování domén) a jak funguje. Ukazuje také různé typy zón, které mohou být definovány na serveru DNS.

DNS (Systém pojmenování domén) je distribuovaný databázový systém pro správu hostitelských jmen a jejich asociovaných IP (Internet Protocol) adres. Prostřednictvím DNS mohou lidé vyhledávat hostitelský systém pomocí jednoduchého jména, jako např. www.jkltoys.com, místo toho, aby museli vypisovat IP adresu (xxx.xxx.xxx.xxx). Jeden server může být zodpovědný pouze za to, že zná hostitelská jména a IP adresy pro malou podmnožinu určité

zóny, avšak servery DNS mohou při mapování všech jmen domén na jejich IP adresy spolupracovat. Spolupráce serverů DNS umožňuje počítačům komunikovat přes Internet.

Data DNS jsou 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

Toto téma vysvětluje zóny DNS (Systém pojmenování domén) a typy zón.

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

Kvůli zálohování a možné redundanci jsou zónová data často ukládána na jiných serverech, než je 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 iSeries 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. Může obsahovat zdrojové záznamy, jako např. hostitelský systém, jméno alias (CNAME), adresa (A) 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
Podřízená zóna definuje podzónu a deleguje odpovědnost za data podzóny na jeden nebo více serverů jmen.

Jméno alias (CNAME)
Jméno alias definuje alternativní jméno pro primární jméno domény.

Hostitelský systém
Hostitelský objekt mapuje záznamy A a PTR do hostitelského systému. Další 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.

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)"
Toto téma vysvětluje, jak systém DNS (Systém pojmenování domén) řeší dotazy za klienty.

"Konfigurace zón na serveru jmen" na stránce 25
Jakmile nakonfigurujete instanci serveru DNS (Systém pojmenování domén), musíte nakonfigurovat zóny pro server jmen.

Související odkazy

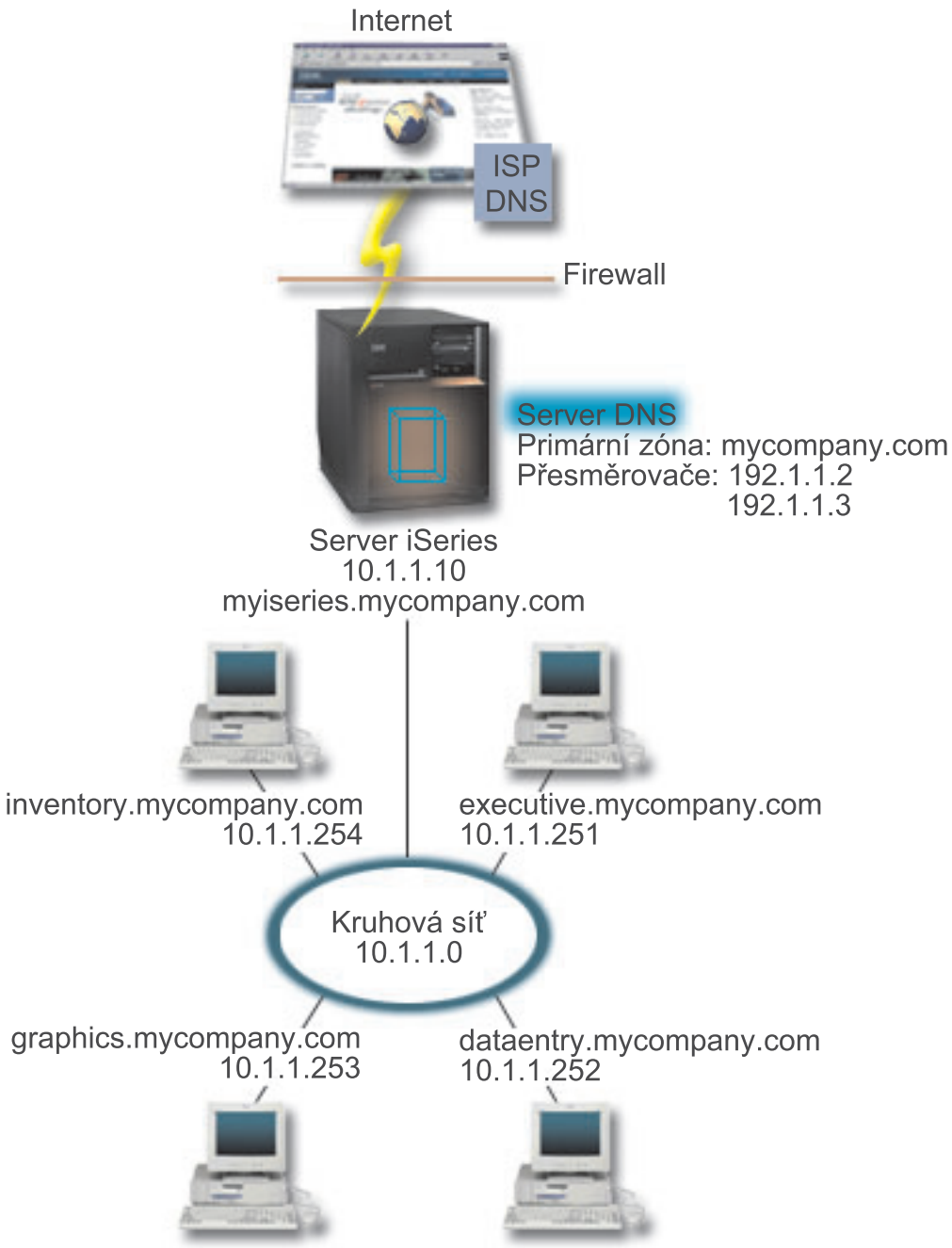
"Příklad: Jediný server DNS pro intranet" na stránce 12
Tento příklad popisuje jednoduchou podsíť se serverem DNS (Systém pojmenování domén) pro interní použití.

"Záznamy zdrojů DNS (Systém pojmenování domén)" na stránce 8
Toto téma vysvětluje, jak se záznamy zdrojů používají v systému DNS (Systém pojmenování domén). Zdrojové záznamy se používají k ukládání dat o jménech domén a IP adresách. Toto téma obsahuje prohledávatelný seznam zdrojových záznamů podporovaných v systému OS/400 ve verzi V5R1.

Jak rozumět dotazům DNS (Systém pojmenování domén)

Toto téma vysvětluje, jak systém DNS (Systém pojmenování domén) řeší dotazy za klienty.

Klienti vyhledávají informace pomocí serverů DNS. Požadavek může vyjít přímo od klienta nebo od aplikace, která pracuje na tomto klientovi. Klient odešle k serveru DNS zprávu s dotazem, který obsahuje plně kvalifikované jméno domény (FQDN), typ dotazu (např. konkrétní záznam 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. Existují dva způsoby, jak postupovat dále, rekurze nebo iterace. Pokud je server DNS nastaven tak, aby používal rekurzi, může se tento server dotazovat ostatních serverů DNS nebo se na ně obracet v zájmu žádajícího klienta, aby plně rozlišil jméno, a potom odešle zpět odpověď klientovi. Jestliže se server DNS dotazuje jiného serveru DNS, uloží dotazující se server odpověď do rychlé vyrovnávací paměti, takže ji bude moci využít příště, jakmile obdrží tento dotaz. Klient se může za účelem rozlišení jména pokusit o kontakt s ostatními servery DNS. V tomto procesu nazvaném *iterace* používá klient samostatné a dodatečné dotazy založené na referenčních odpovědích od serverů.

Související odkazy

“Co jsou zóny” na stránce 2
Toto téma vysvětluje zóny DNS (Systém pojmenování domén) a typy zón.

“Příklad: Jediný server DNS s přístupem k Internetu” na stránce 14
Tento příklad popisuje jednoduchou podsíť se serverem DNS (Systém pojmenování domén), který je přímo připojen k Internetu.

Nastavení domény DNS

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

DNS (Systém pojmenování domén) 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 14
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

OS/400 DNS V5R1 založený na odvětvovém standardu BIND 8 podporuje dynamickou aktualizaci. To umožňuje vnějším zdrojům, jako např. DHCP (protokol dynamické konfigurace hostitele), odesílat aktualizace k serveru DNS (Systém pojmenování domén).

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. Nyní mohou být servery DNS provozující standard BIND 8 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), záznamy PTR, nebo obojí v zastoupení klienta. Záznamy A mapují hostitelské jméno počítače na jeho IP adresu. Záznamy PTR mapují IP adresu počítače na jeho hostitelské jméno. Když se změní adresa klienta, DHCP může automaticky odeslat aktualizaci serveru DNS, takže ostatní hostitelské systémy v síti mohou vyhledat klienta prostřednictvím dotazů DNS na jeho nové adrese. Pro každý dynamicky aktualizovaný záznam bude zapsán asociovaný textový záznam (TXT), který bude identifikovat, že záznam zapsal DHCP.

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. Ne všichni klienti DHCP podporují provádění vlastních požadavků na aktualizaci záznamu A. Předtím, než zvolíte tuto metodu, prostudujte si dokumentaci k platformě vašeho klienta.

Dynamické zóny jsou zabezpečeny vytvořením seznamu autorizovaných zdrojů, které smějí odesílat aktualizace. Autorizované zdroje můžete definovat pomocí individuálních IP adres, celých podsítí, paketů, které byly označeny sdíleným tajným klíčem (nazývaným *transakční podpis*, neboli TSIG) nebo libovolnou kombinací uvedených metod. DNS ověřuje před provedením aktualizace zdrojových záznamů, zda příchozí pakety požadavků přicházejí z autorizovaného zdroje.

Dynamická aktualizace může být prováděna mezi DNS a DHCP na jednom serveru iSeries, mezi různými servery iSeries, nebo mezi jedním serverem iSeries a ostatními servery, které jsou schopné dynamické aktualizace.

Poznámka: U serverů, které odesílají dynamické aktualizace do serveru DNS, je vyžadováno rozhraní API pro dynamickou aktualizaci QTOBUPT. Toto rozhraní se instaluje automaticky s volbou 31 operačního systému i5/OS, DNS.

Související pojmy

DHCP (protokol dynamické konfigurace hostitele)

Související úlohy

“Konfigurace DNS (Systém pojmenování domén) pro přijímání dynamických aktualizací” na stránce 25
Nyní mohou být servery DNS (Systém pojmenování domén) provozující standard BIND 8 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 odesílání dynamických aktualizací

Související odkazy

“Příklad: Systém pojmenování domén a protokol DHCP na stejném serveru iSeries” na stránce 16
Tento příklad uvádí DNS (Systém pojmenování domén) a protokol DHCP (protokol dynamické konfigurace hostitele) na stejném serveru.

“Záznamy zdrojů DNS (Systém pojmenování domén)” na stránce 8
Toto téma vysvětluje, jak se záznamy zdrojů používají v systému DNS (Systém pojmenování domén). Zdrojové záznamy se používají k ukládání dat o jménech domén a IP adresách. Toto téma obsahuje prohledávatelný seznam zdrojových záznamů podporovaných v systému OS/400 ve verzi V5R1.

QTOBUPT

“Funkce odvětvového standardu BIND 8”
Kromě dynamické aktualizace nabízí standard BIND 8 několik funkcí pro zvýšení výkonu vašeho serveru DNS (Systém pojmenování domén).

Funkce odvětvového standardu BIND 8

Kromě dynamické aktualizace nabízí standard BIND 8 několik funkcí pro zvýšení výkonu vašeho serveru DNS (Systém pojmenování domén).

DNS byl přepracován, aby používal odvětvový standard BIND 8 pro systém OS/400, verzi V5R1. Pokud nemáte nainstalovanou volbu PASE, můžete pokračovat v konfiguraci a spouštění dřívějšího vydání serveru OS/400

založeného na standardu BIND 4.9.3. Téma Požadavky na DNS systém vysvětluje, co je potřeba ke spuštění serveru DNS založeného na odvětvovém standardu BIND 8 na vašem serveru iSeries. Používání nového DNS vám umožní využívat těchto funkcí:

Několik serverů DNS provozovaných na jednom serveru iSeries

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

Jedním z praktických využití násobných serverů je rozdělení serveru DNS, kdy je jeden server směrodatným serverem pro interní síť a druhý server se používá pro externí dotazy.

Podmíněné přesměrování

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

Zabezpečené dynamické aktualizace

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

Funkce NOTIFY

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

Přenosy zón (IXFR a AXFR)

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

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

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

Související pojmy

“Požadavky na DNS (Systém pojmenování domén)” na stránce 22
Téma popisuje softwarové požadavky pro spuštění DNS (Systém pojmenování domén) na serveru iSeries.

“Dynamická aktualizace” na stránce 5
OS/400 DNS V5R1 založený na odvětvovém standardu BIND 8 podporuje dynamickou aktualizaci. To umožňuje vnějším zdrojům, jako např. DHCP (protokol dynamické konfigurace hostitele), odesílat aktualizace k serveru DNS (Systém pojmenování domén).

Související odkazy

“Příklad: Rozdělení systému pojmenování domén v rámci ochranné bariéry” na stránce 18
Tento příklad popisuje DNS (Systém pojmenování domén), který pracuje nad ochrannou bariérou (firewall) tak, aby ochránil interní data před přístupem z Internetu, zatímco interním uživatelům umožňuje přístup k datům na Internetu.

“Plánování opatření pro zabezpečení dat” na stránce 21
DNS (Systém pojmenování domén) poskytuje volby pro zabezpečení dat, které omezují externí přístup k vašemu serveru.

Záznamy zdrojů DNS (Systém pojmenování domén)

Toto téma vysvětluje, jak se záznamy zdrojů používají v systému DNS (Systém pojmenování domén). Zdrojové záznamy se používají k ukládání dat o jménech domén a IP adresách. Toto téma obsahuje prohledávatelný seznam zdrojových záznamů podporovaných v systému OS/400 ve verzi V5R1.

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.

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.
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.

Tabulka 1. Vyhledávací tabulka zdrojových záznamů (pokračování)

Zdrojový záznam	Zkratka	Popis
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. Záznamy AAAA jsou používány stejně jako záznamy A k mapování hostitelského jména na jeho IP adresu. Použijte záznamy AAAA pro podporu IP adres verze 6, které nevyhovují standardům formátu záznamu A. Tento typ záznamů je definován v RFC 1886.
Záznamy místa	LOC	Záznam LOC uvádí fyzické umístění síťových komponent. Aplikace mohou tyto záznamy používat k posouzení 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.
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.

Tabulka 1. Vyhledávací tabulka zdrojových záznamů (pokračování)

Zdrojový záznam	Zkratka	Popis
Záznamy o přejmenování schránky elektronické pošty	MR	Záznamy MR uvádí nové jméno domény poštovní schránky. Záznam MR použijte jako směrovací položku pro uživatele, který se přesunul na jinou schránku elektronické pošty. Tento typ záznamů je definován v RFC 1035.
Záznamy serveru jmen	NS	Záznam NS uvádí 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.
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.

Tabulka 1. Vyhledávací tabulka zdrojových záznamů (pokračování)

Zdrojový záznam	Zkratka	Popis
Textové záznamy	TXT	Záznam TXT uvádí vícenásobné řetězce znaků, kde každý řetězec může obsahovat až 255 znaků; tyto řetězce jsou přiřazeny ke jménu domény. Záznamy TXT mohou být použity společně se záznamy RP (responsible person) a poskytovat informace o osobě odpovědné za danou zónu. Tento typ záznamů je definován v RFC 1035. Záznamy TXT jsou používány servery iSeries DHCP za účelem dynamických aktualizací. Server DHCP zapíše a přiřadí záznam TXT při každé aktualizaci záznamu PTR nebo A provedenou serverem DHCP. Záznamy serveru DHCP mají předponu AS400 DHCP.
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

"Dynamická aktualizace" na stránce 5
OS/400 DNS V5R1 založený na odvětvovém standardu BIND 8 podporuje dynamickou aktualizaci. To umožňuje vnějším zdrojům, jako např. DHCP (protokol dynamické konfigurace hostitele), odesílat aktualizace k serveru DNS (Systém pojmenování domén).

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

Související odkazy

"Příklad: Jediný server DNS pro intranet" na stránce 12
Tento příklad popisuje jednoduchou podsíť se serverem DNS (Systém pojmenování domén) pro interní použití.

"Co jsou zóny" na stránce 2
Toto téma vysvětluje zóny DNS (Systém pojmenování domén) a typy zón.

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 iSeries 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 8
Toto téma vysvětluje, jak se záznamy zdrojů používají v systému DNS (Systém pojmenování domén). Zdrojové záznamy se používají k ukládání dat o jménech domén a IP adresách. Toto téma obsahuje prohledávatelný seznam zdrojových záznamů podporovaných v systému OS/400 ve verzi V5R1.

Příklady DNS (Systém pojmenování domén)

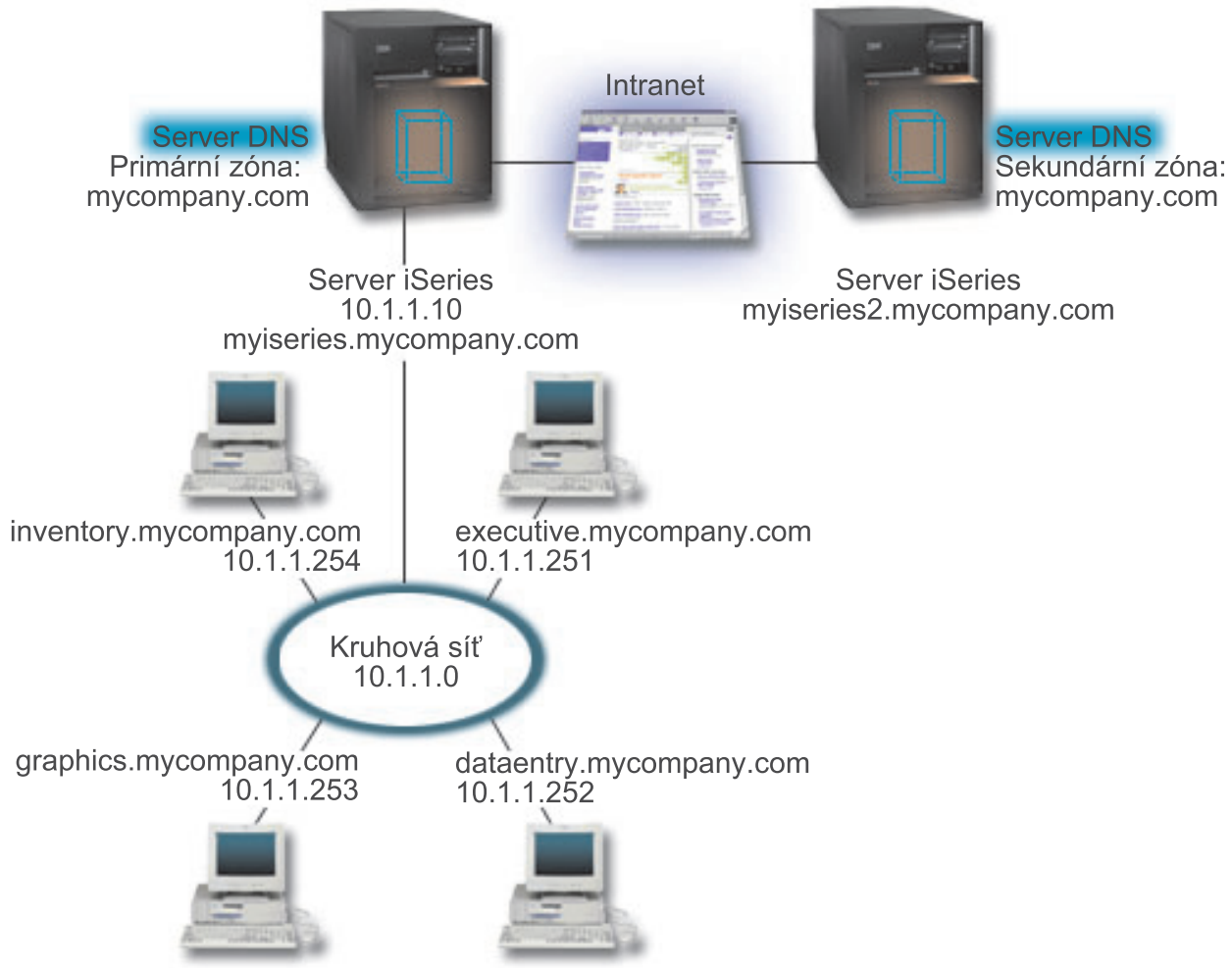
Z těchto příkladů můžete pochopit, jak používat systém DNS (Systém pojmenování domén) v síti.

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



Obrázek 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) mapují jméno počítače na jeho asociovanou IP adresu. To umožňuje ostatním hostitelským systémům v síti dotazovat se serveru DNS na IP adresu přiřazenou konkrétnímu hostitelskému jménu. Záznamy PTR (Reverse-lookup pointer) mapují IP adresu systému na jeho asociované jméno. To dává ostatním hostitelským systémům v síti možnost dotazovat se serveru DNS na hostitelské jméno, které odpovídá určité IP adrese.

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

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

Sekundární servery

Sekundární servery nahrávají zónová data ze 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 obrázku 2 je server myiseries částí intranetu. Byl nakonfigurován další server iSeries, myiseries2, aby působil jako sekundární server DNS pro zónu mycompany.com. Sekundární server je možné použít k vyvážení požadavků na servery a zároveň k vytvoření zálohy pro případ selhání primárního serveru. Doporučuje se mít alespoň jeden sekundární server pro každou zónu.

Související odkazy

"Záznamy zdrojů DNS (Systém pojmenování domén)" na stránce 8
Toto téma vysvětluje, jak se záznamy zdrojů používají v systému DNS (Systém pojmenování domén). Zdrojové záznamy se používají k ukládání dat o jménech domén a IP adresách. Toto téma obsahuje prohledávatelný seznam zdrojových záznamů podporovaných v systému OS/400 ve verzi V5R1.

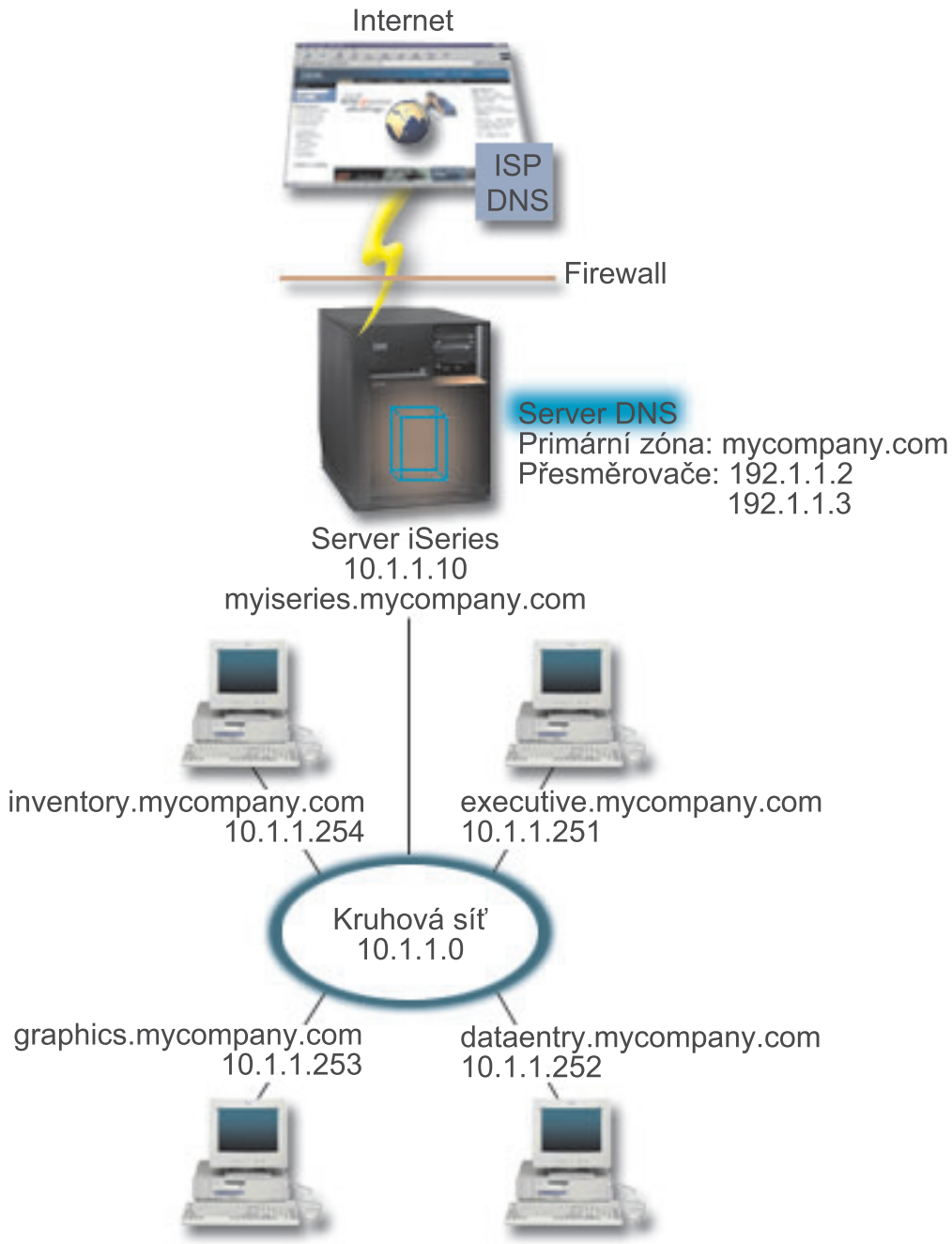
"Co jsou zóny" na stránce 2
Toto téma vysvětluje zóny DNS (Systém pojmenování domén) a typy zón.

"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 ilustrace 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 (Systém pojmenování domén)” na stránce 26.
- 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. Měli byste nakonfigurovat ochrannou bariéru nebo přijmout jiná opatření k zabezpečení vašeho serveru iSeries.

Související pojmy

"Nastavení domény DNS" na stránce 5
Toto téma uvádí přehled registrace domény s odkazy na ostatní referenční stránky týkající se nastavení vaší vlastní doménové oblasti.

iSeries a zabezpečení na internetu

"Jak rozumět dotazům DNS (Systém pojmenování domén)" na stránce 3
Toto téma vysvětluje, jak systém DNS (Systém pojmenování domén) řeší dotazy za klienty.

Související odkazy

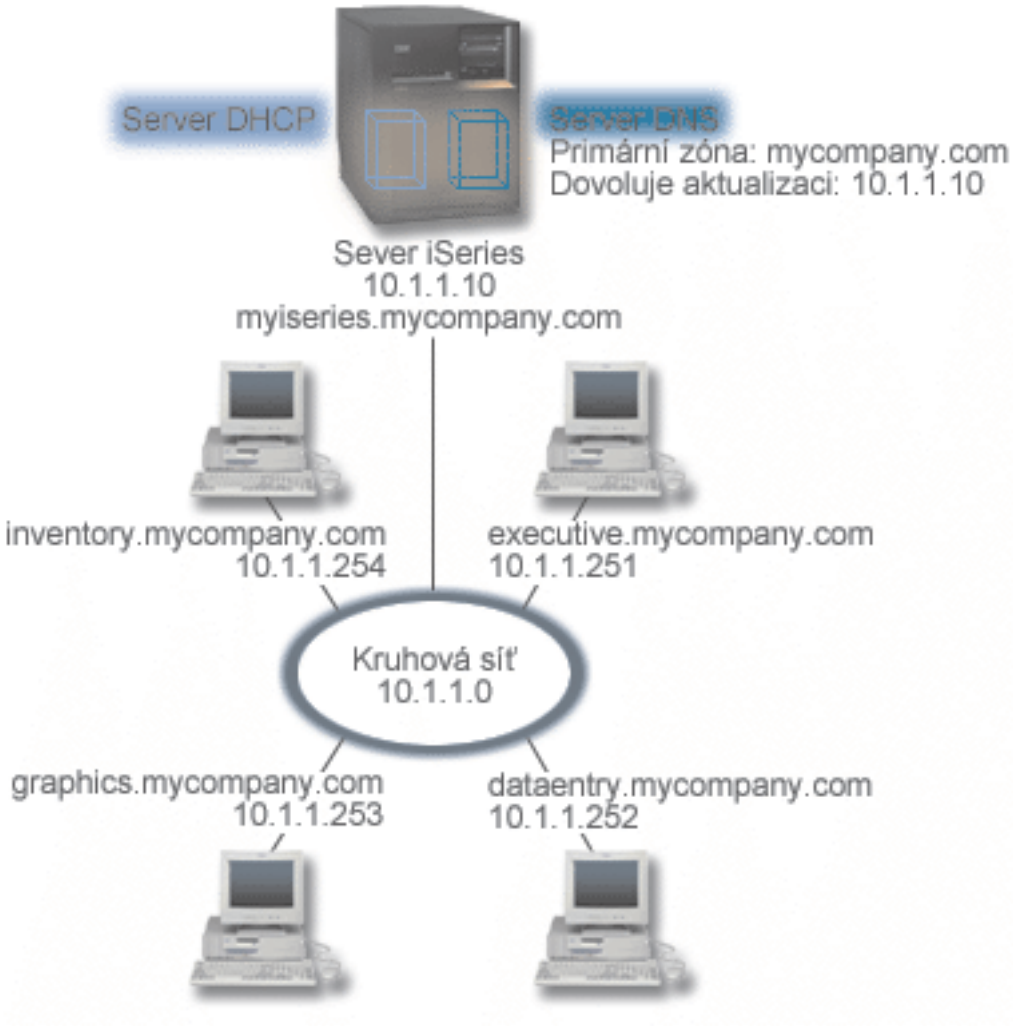
"Příklad: Jediný server DNS pro intranet" na stránce 12
Tento příklad popisuje jednoduchou podsíť se serverem DNS (Systém pojmenování domén) pro interní použití.

Příklad: Systém pojmenování domén a protokol DHCP na stejném serveru iSeries

Tento příklad uvádí DNS (Systém pojmenování domén) a protokol DHCP (protokol dynamické konfigurace hostitele) na stejném serveru.

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

Následující obrázek popisuje malou podsíť s jediným serverem iSeries, který působí 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 jednom serveru iSeries.

Předcházející verze DHCP a DNS byly vzájemně nezávislé. Pokud DHCP přiřadil klientovi novou IP adresu, musel administrátor ručně aktualizovat záznamy DNS. Jestliže 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 V5R1 DNS OS/400 založeným na odvětvovém standardu BIND 8 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 jeho hostitelským jménem.

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

- Identifikace dynamické zóny

  Není možné ručně aktualizovat dynamickou zónu, jestliže je server 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” na stránce 20.
- 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 5
OS/400 DNS V5R1 založený na odvětvovém standardu BIND 8 podporuje dynamickou aktualizaci. To umožňuje vnějším zdrojům, jako např. DHCP (protokol dynamické konfigurace hostitele), odesílat aktualizace k serveru DNS (Systém pojmenování domén).

"Určení struktury domény" na stránce 20
Pokud konfigurujete doménu poprvé, měli byste před vytvářením zón naplánovat požadavky a údržbu.

Související úlohy

Konfigurace DHCP pro odesílání dynamických aktualizací

Související odkazy

Příklad: DNS a DHCP na různých serverech iSeries

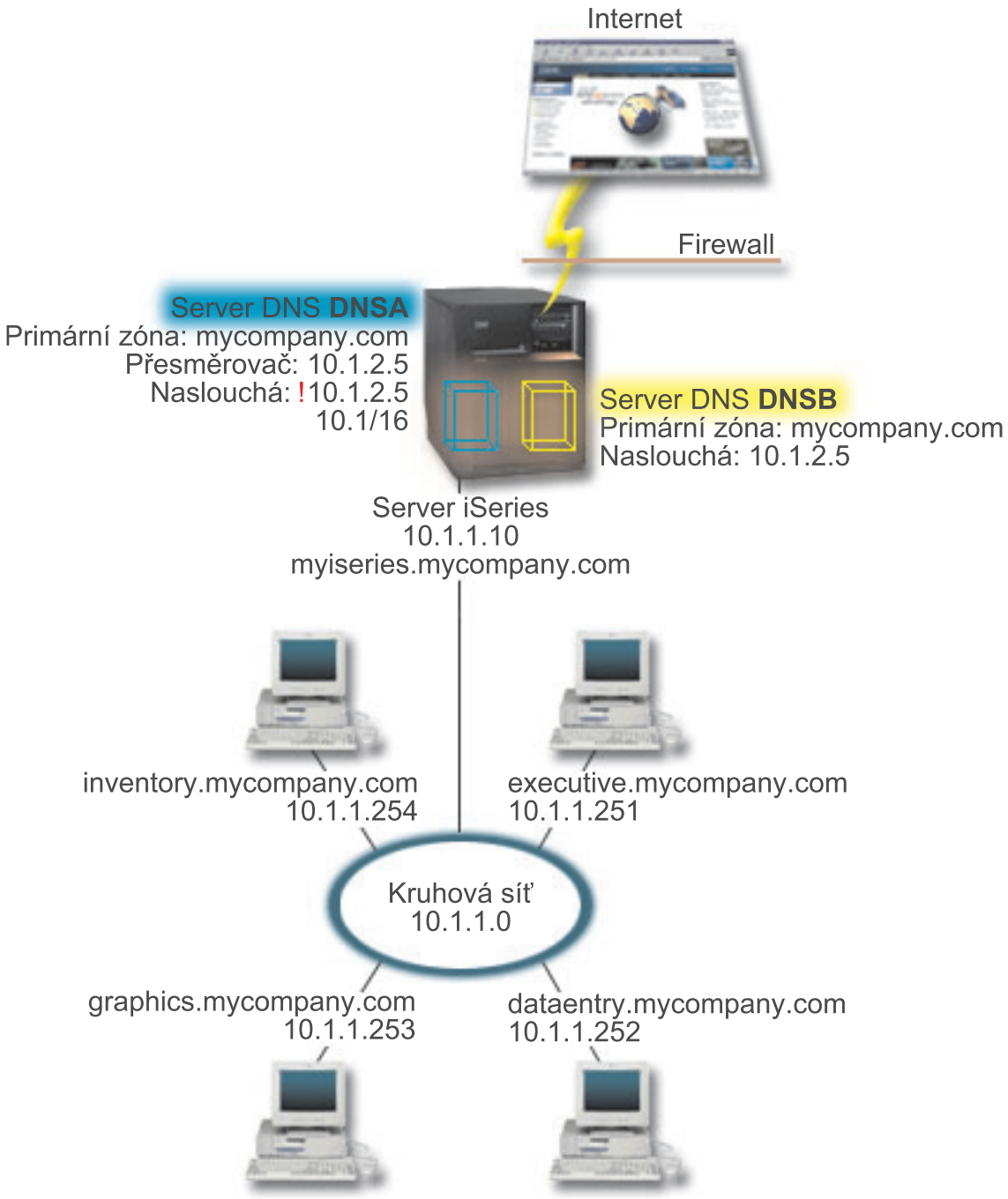
Příklad: Rozdělení systému pojmenování domén v rámci ochranné bariéry

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

Následující ilustrace popisuje jednoduchou podsíť, která používá z bezpečnostních důvodů ochrannou bariéru (firewall). DNS V5R1 v systému OS/400 založený na standardu BIND 8 umožňuje nastavit na jediném serveru iSeries několik serverů DNS. Předpokládejme, že společnost má interní síť s rezervovanou IP oblastí a externí částí sítě, která je k dispozici veřejnosti.

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

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



Obrázek 5. Rozdělení serveru DNS v rámci ochranné bariéry

Externí server (DNSB) je nakonfigurován s primární zónou mycompany.com. Tato zónová data zahrnují pouze zdrojové záznamy, které mají být částí veřejné domény. Interní server, DNSA, je nakonfigurován s primární zónou mycompany.com, avšak zónová data definovaná na DNSA obsahují zdrojové záznamy intranetu. Volba přesměrovače je definována jako 10.1.2.5. To nutí server DNSA zasílat dotazy, které nemůže rozlišit, 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 nastavování rozdělení DNS vezměte do úvahy následující nastavení konfigurace:

- Naslouchání

  V předcházejících příkladech byl na jednom serveru iSeries pouze jeden server DNS. Byl nastaven tak, aby naslouchal na všech IP adresách rozhraní. Pokud máte několik serverů DNS na jednom serveru iSeries, musíte definovat IP adresy rozhraní, na kterých naslouchá každý z nich. Dva servery DNS nemohou naslouchat na stejné adrese. V tomto případě 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 (Address Match List)

  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 prvky přístupového seznamu (ACL) v tomto pořadí (!10.1.2.5; 10.1/16). V takovém případě bude adresa 10.1.2.5 porovnána s prvním prvkem a bude automaticky zamítnuta.

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

Související odkazy

"Funkce odvětvového standardu BIND 8" na stránce 6
Kromě dynamické aktualizace nabízí standard BIND 8 několik funkcí pro zvýšení výkonu vašeho serveru DNS (Systém pojmenování domén).

Plánování DNS (Systém pojmenování domén)

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

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 iSeries 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 iSeries 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 29
Toto téma vám pomůže porozumět, jaké soubory systém DNS (Systém pojmenování domén) používá, a naleznete zde pokyny pro jejich zálohování a údržbu.

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.

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

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

Související odkazy

“Příklad: Systém pojmenování domén a protokol DHCP na stejném serveru iSeries” na stránce 16
Tento příklad uvádí DNS (Systém pojmenování domén) a protokol DHCP (protokol dynamické konfigurace hostitele) na stejném serveru.

Plánování opatření pro zabezpečení dat

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

Zabezpečení vašeho serveru DNS je životně důležité. Kromě pokynů týkajících se zabezpečení ochrany dat uvedených v tomto tématu je zabezpečení serverů DNS a iSeries popsáno v nejrůznějších zdrojích, včetně tématu iSeries a Internet v aplikaci Information Center. Kniha DNS a BIND se tak zabývá zabezpečením dat v souvislosti s DNS.

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 prvků 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 prvky seznamu AML v tomto pořadí (!10.1.1.5; 10.1.1/24). V takovém případě bude adresa 10.1.1.5 porovnána s prvním prvkem a bude automaticky zamítnuta.

Jestliže jsou prvky obráceně (10.1.1/24; !10.1.1.5), bude IP adrese 10.1.1.5 povolen přístup, protože server ji porovná s prvním prvkem, který 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.

Související pojmy

iSeries a zabezpečení na internetu

Související odkazy

“Funkce odvětvového standardu BIND 8” na stránce 6
Kromě dynamické aktualizace nabízí standard BIND 8 několik funkcí pro zvýšení výkonu vašeho serveru DNS (Systém pojmenování domén).

Požadavky na DNS (Systém pojmenování domén)

Téma popisuje softwarové požadavky pro spuštění DNS (Systém pojmenování domén) na serveru iSeries.

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

Po instalaci DNS bude standardně provedena konfigurace pro nastavování jednoho serveru DNS za použití schopností serveru DNS založeného na standardu BIND 4.9.3, které byly k dispozici v předcházejících vydáních. Pokud budete chtít spustit jeden nebo více serverů DNS za použití standardu BIND 8, musíte instalovat volbu PASE. PASE je produkt SS1 volba 33 (SS1 Option 33). Po instalaci volby PASE produkt iSeries automaticky zajistí konfiguraci správné implementace BIND.

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

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

Související pojmy

Prostředí PASE (Portable Application Solutions Environment)

“Konfigurace DNS (Systém pojmenování domén)” na stránce 23
Téma vysvětluje, jak je možné využít produkt iSeries Navigator ke konfiguraci serverů jmen a k rozlišování dotazů mimo vaší doménu.

Související odkazy

“Funkce odvětvového standardu BIND 8” na stránce 6
Kromě dynamické aktualizace nabízí standard BIND 8 několik funkcí pro zvýšení výkonu vašeho serveru DNS (Systém pojmenování domén).

Související informace

Téma aplikace Information Center V4R5 DNS

Jak zjistit, zda je DNS (Systém pojmenování domén) nainstalovaný

Chcete-li zjistit, zda je nainstalován DNS (Systém pojmenování domén), postupujte podle těchto kroků:

1. Na příkazovou řádku napište GO LICPGM a stiskněte klávesu Enter.
2. Napište 10 (Display installed licensed programs) a stiskněte Enter.
3. Přestránkujte dolů na **5722SS1 Domain Name System** (SS1 volba 31). Je-li DNS úspěšně nainstalován, bude pod Installed Status uvedena hodnota *compatible, jak je vidět níže:

```
LicPgm     Installed Status     Description
5722SS1    *COMPATIBLE          Domain Name System
```

4. Stisknutím klávesy F3 opusťte obrazovku.

Instalace DNS (Systém pojmenování domén)

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 DNS (Systém pojmenování domén)

Téma vysvětluje, jak je možné využít produkt iSeries Navigator ke konfiguraci serverů jmen a k rozlišování dotazů mimo vaší 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 22
Téma popisuje softwarové požadavky pro spuštění DNS (Systém pojmenování domén) na serveru iSeries.

Přístup k DNS v prostředí produktu iSeries Navigator

V tomto tématu se dozvíte, jak přistupovat k DNS (Systém pojmenování domén) v produktu iSeries Navigator.

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

Pokud provádíte konfiguraci serveru DNS poprvé, postupujte takto:

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

Související pojmy

iSeries Navigator

Konfigurace serverů jmen

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

Server iSeries DNS založený na odvětvovém standardu BIND 8 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 tuto proceduru, 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 29
Toto téma vám pomůže porozumět, jaké soubory systém DNS (Systém pojmenování domén) používá, a naleznete zde pokyny pro jejich zálohování a údržbu.

Vytvoření instance serveru jmen

K definování instance serveru DNS (Systém pojmenování domén) použijte průvodce novou konfigurací DNS.

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

1. V produktu **iSeries Navigator** rozbalte **Server iSeries → Síť → Servery → DNS**.
2. V levém podokně klepněte pravým tlačítkem myši na **DNS** a vyberte **Nový server jmen...**
3. Průvodce vás může vést procesem konfigurace.

Průvodce požaduje následující vstupní údaje:

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

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

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

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

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

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 produktu **iSeries Navigator** rozbalte **Server iSeries → Síť → Servery → DNS**.
2. V pravém podokně klepněte pravým tlačítkem myši na **server DNS** a vyberte volbu **Konfigurace**.
3. Klepněte pravým tlačítkem myši na **Server DNS** a vyberte volbu **Vlastnosti**.

Konfigurace zón na serveru jmen

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

Váš server se zobrazuje v pravém podokně. Chcete-li na serveru konfigurovat zóny, klepněte pravým tlačítkem myši na jméno serveru a vyberte volbu **Konfigurace**. Je zobrazeno okno Konfigurace DNS.

Všechny zóny se konfigurují pomocí průvodců. Klepnutím pravým tlačítkem myši na odpovídající složku vytvořte **Zóny pro vyhledávání dopředu** nebo **Zóny pro vyhledávání dozadu**. Zobrazují se volby pro daný typ zóny. Tím, že vyberte typ zóny, kterou chcete vytvořit, spustíte průvodce.

Související pojmy

"Přístup k externím datům DNS (Systém pojmenování domén)" na stránce 26
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 8 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.

"Import souborů DNS (Systém pojmenování domén)" na stránce 26
DNS (Systém pojmenování domén) 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 2
Toto téma vysvětluje zóny DNS (Systém pojmenování domén) a typy zón.

Konfigurace DNS (Systém pojmenování domén) pro přijímání dynamických aktualizací

Nyní mohou být servery DNS (Systém pojmenování domén) provozující standard BIND 8 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 musíte provádět ruční aktualizace do dynamické zóny, musíte zastavit server dynamické zóny a opět jej spustit poté, co dokončíte aktualizace. Zastavení serveru si vynutí synchronizaci všech dynamických aktualizací, které byly provedeny, jelikož server zavedl svá zónová data ze zónové databáze. Pokud server nezastavíte, přijdete o všechny dynamické aktualizace, které byly zpracovány od doby jeho spuštění. Zastavení serveru za účelem provedení ručních aktualizací znamená, že ztratíte aktualizace, které byly odeslány, zatímco byl server vypnut.

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

1. V produktu iSeries Navigator rozbalte **Server iSeries → 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 pojmy

"Dynamická aktualizace" na stránce 5
OS/400 DNS V5R1 založený na odvětvovém standardu BIND 8 podporuje dynamickou aktualizaci. To umožňuje vnějším zdrojům, jako např. DHCP (protokol dynamické konfigurace hostitele), odesílat aktualizace k serveru DNS (Systém pojmenování domén).

"Konfigurace zón na serveru jmen" na stránce 25
Jakmile nakonfigurujete instanci serveru DNS (Systém pojmenování domén), musíte nakonfigurovat zóny pro server jmen.

Související úlohy

Konfigurace DHCP pro odesílání dynamických aktualizací

Import souborů DNS (Systém pojmenování domén)

DNS (Systém pojmenování domén) 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 nebo že provedete konverzi existujících hostitelských tabulek. Chcete-li vytvořit data zóny z tabulky hostitelského serveru, viz téma Converting host tables.

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

Chcete-li importovat zónový soubor, postupujte takto:

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

Související pojmy

"Konfigurace zón na serveru jmen" na stránce 25
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 serverů produktu iSeries Navigator

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

Kde získáte adresy internetových kořenových serverů

Adresy kořenových serverů nejvyšší úrovně se čas od času mění a je v odpovědnosti administrátora DNS, aby je uchoval aktuální. InterNIC udržuje aktuální seznam adres internetových kořenových serverů. Chcete-li získat aktuální seznam internetových kořenových serverů, postupujte takto:

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

Server DNS za ochrannou bariérou nesmí mít definovány žádné kořenové servery. V tomto případě je server DNS schopen rozlišovat pouze dotazy od položek, které existují v jeho vlastních databázových souborech primární domény nebo v jeho rychlé vyrovnávací paměti. Externí dotazy může 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 pojmy

"Konfigurace zón na serveru jmen" na stránce 25
Jakmile nakonfigurujete instanci serveru DNS (Systém pojmenování domén), musíte nakonfigurovat zóny pro server jmen.

Správa DNS (Systém pojmenování domén)

Téma vás seznámí s postupy při ověřování funkce DNS (Systém pojmenování domén), monitorování výkonu a údržbě dat a souborů DNS.

Ověření funkčnosti DNS (Systém pojmenování domén) vyhledáním serveru jmen

K ověření, že server DNS (Systém pojmenování domén) pracuje, můžete použít funkci NSLookup (Name Server Lookup).

Pomocí funkce NSLookup se dotažte serveru DNS na nějakou IP adresu. Tím ověříte, že server DNS odpovídá na dotazy. Požadujte hostitelské jméno, které je asociované s IP adresou pro smyčkový test (127.0.0.1). Odpovědí by mělo být hostitelské jméno (localhost). Rovněž byste se měli dotazovat na specifická jména 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 NSLookup, postupujte takto:

1. Na příkazovou řádku napište NSLOOKUP DMNNAMSVR(n.n.n.n), kde n.n.n.n je adresa, které má naslouchat vámi nakonfigurovaná testovaná instance serveru.

2. Na příkazovou řádku napište NSLOOKUP a stiskněte klávesu Enter. Tím se spustí dotazovací relace NSLookup.
3. Napište server, za toto slovo napište jméno vašeho serveru a stiskněte klávesu Enter. Například: server myiseries.mycompany.com. Měly by se zobrazit tyto informace:

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

   Kde n.n.n.n představuje IP adresu vašeho serveru DNS.
4. Na příkazovou řádku napište 127.0.0.1 a stiskněte klávesu Enter.

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

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


   Name:    localhost
   Address:  127.0.0.1
   ```

   Server DNS odpovídá správně, pokud vrací jako hostitelské jméno pro smyčkový test: **localhost**.
5. Terminálovou relaci funkce NSLOOKUP ukončete napsáním exit a stisknutím klávesy Enter.

Poznámka: Pokud potřebujete pomoc při použití funkce NSLookup, napište ? a stiskněte klávesu 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. 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 (Systém pojmenování domén)

Klíče pro správu DNS (Systém pojmenování domén) 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 produktu iSeries Navigator rozbalte **Server iSeries → Síť → Servery → DNS**.
2. V pravém podokně klepněte pravým tlačítkem myši na instanci serveru DNS, kterou chcete otevřít, a vyberte volbu **Konfigurace**.
3. V okně Konfigurace DNS vyberte **Soubor → Správa klíčů.**

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 jednom serveru iSeries. Jestliže je DHCP na jiném serveru iSeries, musíte vytvořit klíč pro dynamickou aktualizaci na každém serveru iSeries, abyste umožnili dynamické aktualizace.

Při správě klíčů pro dynamickou aktualizaci postupujte takto:

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

Statistika serveru DNS (Systém pojmenování domén)

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)"
Toto téma vám pomůže porozumět, jaké soubory systém DNS (Systém pojmenování domén) používá, a naleznete zde pokyny pro jejich zálohování a údržbu.

Statistika 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 produktu iSeries Navigator rozbalte **Server iSeries → 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**.

Databáze 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 iSeries Navigator. Jestliže potřebujete uložit kopii souborů, je jméno souboru s výpisem databáze NAMED_DUMP.DB v adresářové cestě serveru iSeries: **Integrated File System/Root/QIBM/UserData/OS400/DNS/<instance_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 produktu iSeries Navigator rozbalte **Server iSeries → 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**.

Údržba konfiguračních souborů DNS (Systém pojmenování domén)

Toto téma vám pomůže porozumět, jaké soubory systém DNS (Systém pojmenování domén) používá, a naleznete zde pokyny pro jejich zálohování a údržbu.

K vytvoření a údržbě instancí serveru DNS na serveru iSeries můžete použít server i5/OS DNS. Konfigurační soubory pro DNS jsou spravovány produktem iSeries Navigator. Tyto soubory byste neměli upravovat ručně. Při vytváření, změnách nebo výmazu konfiguračních souborů DNS používejte vždy produkt iSeries Navigator. Konfigurační soubory DNS jsou uloženy v níže uvedených cestách integrovaného systému souborů.

Poznámka: Struktura níže uvedeného souboru se týká serveru DNS, který je provozován na BIND 8. Pokud používáte server DNS založený na BIND 4.9.3, viz téma Backing up DNS configuration files and maintaining log files pod heslem V4R5 DNS v aplikaci Information Center.

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.
ATRIBUTY		DNS používá tento soubor k určení používané verze odvětvového standardu BIND.
QIBM/UserData/OS400/DNS/<*instance-n*>/		Adresář výchozího bodu pro instanci serveru DNS.
ATRIBUTY		Konfigurační atributy používané serverem iSeries DNS.
NAMED.CONF		Tento soubor obsahuje konfigurační data. Používá se k tomu, aby sdělil serveru, jaké specifické zóny spravuje, kde jsou soubory zón, které zóny mohou být dynamicky aktualizovány, kde jsou přesměrovací servery a další nastavení voleb.
BOOT.AS400BIND4		Soubor pro metodiku a konfiguraci serveru BIND 4.9.3, který je konvertován na soubor BIND 8 NAMED.CONF pro tuto instanci. Tento soubor se vytváří při migraci serveru BIND 4.9.3 na BIND 8. Slouží jako záloha migrace a může být vymazán, pokud server BIND 8 pracuje správně.
NAMED.CA		Seznam kořenových serverů pro tuto instanci.
NAMED_DUMP.DB		Výpis dat serveru vytvořený pro databáze aktivního serveru.
NAMED.STATS		Statistika serveru.
NAMED.PID		Udržuje ID procesu běžícího serveru. Tento soubor se vytváří pokaždé, když je server DNS spuštěn. Používá se pro funkce serveru Databáze, Statistika a Aktualizace. Tento soubor nemažte ani neupravujte.
QUERYLOG		Protokol přijatých dotazů serveru DNS. Tento soubor se vytváří, pokud je aktivní protokol serveru DNS. Je-li aktivní, neustále se zvětšuje a měl by být pravidelně vymazáván.
<*zone-name-a*>.DB		Soubor zóny pro konkrétní doménu, která má být obsluhována daným serverem. Obsahuje všechny zdrojové záznamy pro tuto zónu.

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

Související pojmy

“Zjištění oprávnění DNS (Systém pojmenování domén)” na stránce 20
Pro administrátora DNS (Systém pojmenování domén) existují zvláštní požadavky na oprávnění. Měli byste promyslet bezpečnostní důsledky oprávnění.

“Statistika serveru DNS (Systém pojmenování domén)” na stránce 29
Nástroje pro výpis databáze a statistiky vám mohou pomoci revidovat a spravovat výkon serveru.

Související úlohy

“Konfigurace serverů jmen” na stránce 24
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.

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

Související úlohy

“Změna nastavení DNS (Systém pojmenování domén)” na stránce 35
Funkce ladění DNS (Systém pojmenování domén) může poskytovat informace, které vám mohou pomoci určit a opravit závady serveru DNS.

Změna atributů DNS (Systém pojmenování domén)

Můžete změnit nastavení DNS (Systém pojmenování domén), jestliže vám rozhraní DNS neumožňuje měnit atributy Autostart (automatické spuštění) a Debug levels (úrovně ladění) u všech instancí serveru najednou.

Ke změně tohoto nastavení u jednotlivých instancí serveru DNS nebo u všech instancí najednou můžete použít znakově orientované rozhraní. Při použití příkazu CHGDNSA postupujte takto:

1. Na příkazovou řádku napište CHGDNSA a stiskněte klávesu F4.
2. Na stránce Change DNS Server Attributes (CHGDNSA) napište jméno jedné instance serveru nebo hodnotu *ALL, a stiskněte klávesu Enter.

   Zobrazí se dostupné volby atributů serveru:

   ```
   Autostart server . . . . . *SAME *YES, *NO, *SAME
   Debug level . . . . . *SAME 0-11, *SAME, *DFT
   ```
3. **Autostart** - Chcete-li zadat, aby se vybrané servery DNS automaticky spustily při spuštění TCP/IP, napište *YES. Pokud nechcete, aby se server spustil při spuštění TCP/IP, napište *NO. Jestliže chcete ponechat tento atribut na jeho aktuálním nastavení, napište *SAME.

   Debug level - Pokud chcete změnit úroveň ladění, kterou by měly vybrané servery používat, napište hodnotu v rozmezí od 0 do 11. Chcete-li specifikovat, že by úroveň ladění měla zdědit hodnotu ladění při spuštění serveru, napište *DFT. Jestliže chcete ponechat tento atribut na jeho aktuálním nastavení, napište *SAME.

   Po zadání všech preferovaných hodnot stiskněte klávesu Enter, aby se atributy DNS nastavily.

Spuštění a zastavení serverů DNS (Systém pojmenování domén)

Můžete změnit nastavení, jestliže vám rozhraní DNS (Systém pojmenování domén) neumožní najednou spustit nebo zastavit více instancí serveru.

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

Změna hodnot ladění

Můžete změnit úroveň ladění, což je užitečné pro administrátory, kteří spravují rozsáhlé zóny a kteří nechtějí mít velké objemy ladicích dat, vznikající při prvním spuštění serveru a zavedení všech zónových dat.

DNS (Systém pojmenování domén) v rozhraní produktu iSeries 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 <instance> 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 CALL QTOBDRVS ('BUMP' '<instance>') a stiskněte klávesu Enter.
   - Pokud chcete ladění vypnout, napište CALL QTOBDRVS ('OFF' '<instance>') a stiskněte klávesu Enter.

Odstraňování problémů DNS (Systém pojmenování domén)

Téma se zabývá nastavením vytváření protokolů a ladění DNS (Systém pojmenování domén), které 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.

Označení úloh

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

- Jestliže používáte standard BIND 4.9.3, bude jméno úlohy serveru QTOBDNS. Další informace o ladění serveru DNS 4.9.3 najdete v tématu *Troubleshooting DNS servers*.
- V případě, že provozujete servery založené na standardu BIND 8, budete mít samostatnou úlohu pro každou spouštěnou instanci serveru. Jméno úlohy je tvořeno pěti pevnými znaky (QTOBD), za nimiž následuje jméno instance. Máte-li například dvě instance, INST1 a INST2, budou jména jejich úloh QTOBDINST1 a QTOBDINST2.

Související pojmy

"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.

Související úlohy

"Změna nastavení DNS (Systém pojmenování domén)" na stránce 35
Funkce ladění DNS (Systém pojmenování domén) může poskytovat informace, které vám mohou pomoci určit a opravit závady serveru DNS.

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 8 nabízí několik nových 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 8 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 as400_debug a as400_QPRINT. Podle předvolby jsou ladicí zprávy protokolovány do kanálu as400_debug, kterým je soubor NAMED.RUN. Můžete ale zadat, aby se do tohoto souboru odesílaly také ostatní kategorie zpráv. Kategorie zpráv protokolovaných v as400_QPRINT jsou odesílány do souboru pro souběžný tisk QPRINT pro uživatelský profil QTCP. Kromě 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 as400_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 budou vymazány. Předvolený kanál Null channel je as400_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. Existuje mnoho kategorií, mezi které patří například:

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

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

Závažnost zpráv

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

- critical (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 produktu iSeries Navigator rozbalte **Server iSeries → 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

Předvolená úroveň závažnosti kanálu as400_joblog je nastavená na hodnotu Error. Toto nastavení se používá k tomu, aby se snížil objem informačních zpráv a varování, které 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 as400_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.

Související úlohy

"Odstraňování problémů DNS (Systém pojmenování domén)" na stránce 33
Téma se zabývá nastavením vytváření protokolů a ladění DNS (Systém pojmenování domén), které vám může pomoci při řešení problémů s vaším serverem DNS.

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 zapisují ladicí informace do souboru NAMED.RUN na cestě k adresáři vašeho serveru iSeries: **Integrated File System/Root/QIBM/UserData/OS400/DNS/<instance_serveru>**, kde ″<instance_serveru>″ je jméno instance serveru DNS. Pokud je úroveň ladění nastavena na hodnotu 1 nebo vyšší a jestliže server DNS pokračuje v práci, soubor NAMED.RUN neustále narůstá. Doporučujeme vám tento soubor čas od času vymazat, aby nezabíral příliš mnoho místa na disku. Ke specifikaci preferencí pro maximální velikost a počet verzí souboru NAMED.RUN také můžete použít stránku **Vlastnosti serveru** - **Kanály**.

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

1. V produktu iSeries Navigator rozbalte **Server iSeries → 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 32
Toto téma vysvětluje, jak zkušení administrátoři mohou používat rozšířené funkce DNS (Systém pojmenování domén) ke snazší správě serveru DNS.

Související úlohy

“Odstraňování problémů DNS (Systém pojmenování domén)” na stránce 33
Téma se zabývá nastavením vytváření protokolů a ladění DNS (Systém pojmenování domén), které vám může pomoci při řešení problémů s vaším serverem DNS.

Související informace o DNS (Systém pojmenování domén)

Zde jsou uvedeny knihy IBM Redbooks (ve formátu PDF) a webové stránky, které souvisejí s tématem DNS (Systém pojmenování domén). Prohlížet nebo vytisknout můžete libovolné soubory PDF.

IBM Redbooks

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

Tato červená kniha popisuje podporu serveru DNS (Systém pojmenování domén) a serveru DHCP (protokol dynamické konfigurace hostitele), která je zahrnuta v operačním systému i5/OS. Informace v této červené knize vám pomohou za použití příkladů při instalaci, úpravách, konfiguraci a odstraňování problémů v serverech DNS a DHCP.

Webové stránky

- *DNS and BIND*, třetí vydání. Paul Albitz a Cricket Liu. Vydáno společností O’Reilly and Associates, Inc. Sebastopol, California, 1998. Číslo ISBN: 1-56592-512-2. Toto je nejdůležitější zdroj informací o serveru DNS.
- Webová stránka Internet Software Consortium obsahuje 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).
- 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 .

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 soubor PDF v prohlížeči (klepněte na výše uvedený odkaz).
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 společnosti Adobe (www.adobe.com/products/acrobat/readstep.html) .

Dodatek. Poznámky

Tyto informace platí pro produkty a služby nabízené v USA.

IBM nemusí v ostatních zemích nabídnout produkty, služby a funkce popsané v tomto dokumentu. Informace o produktech a službách, které jsou momentálně dostupné ve Vašem regionu, můžete získat od místního zástupce IBM. Žádný odkaz na produkt, program nebo službu IBM neznamená a ani z něj nelze vyvozovat, že smí být použit pouze uvedený produkt, program či služba IBM. Použít lze jakýkoliv 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 Corporation
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 NEBO ODVOZENÝCH, VČETNĚ, BEZ OMEZENÍ, ODVOZENÝCH ZÁRUK NEPORUŠENÍ PRÁV TŘETÍCH STRAN, ZÁRUKY PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL. Právní řády některých zemí nepřipouštějí vyloučení vyjádřených nebo odvozených záruk v určitých transakcích a proto se na Vás výše uvedené omezení nemusí vztahovat.

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

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 stránkách nejsou součástí materiálů k tomuto produktu IBM a tyto webové stránky mohou být používány pouze na vlastní nebezpečí.

IBM může použít nebo distribuovat jakékoliv informace, které jí sdělíte, libovolným způsobem, který společnost považuje za odpovídající, bez vzniku jakýchkoliv 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
3605 Highway 52 N

Rochester, MN 55901
U.S.A.

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

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

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 konstatování, 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.

LICENČNÍ INFORMACE:

Tyto informace obsahují ukázkové aplikační programy ve zdrojovém jazyce ilustrující programovací techniky na různých operačních platformách. Tyto ukázkové programy můžete bez závazků vůči IBM jakýmkoliv způsobem kopírovat, měnit a distribuovat za účelem vývoje, používání, odbytu či distribuce aplikačních programů odpovídajících rozhraní API pro operační platformu, pro kterou byly ukázkové programy napsány. Tyto vzorové programy nebyly důkladně testovány za všech podmínek. Proto IBM nemůže zaručit ani naznačit spolehlivost, provozuschopnost ani funkčnost těchto programů.

Každá kopie nebo část těchto vzorových programů nebo odvozená práce musí zahrnovat níže uvedenou copyrightovou výhradu:

© (jméno Vaší společnosti) (rok). Části tohoto kódu jsou odvozeny ze vzorových programů od IBM Corporation. © 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 o programovacím rozhraní

Tato publikace DNS je určena pro programovací rozhraní umožňující zákazníkovi psát programy za účelem získání služeb operačního systému IBM i5/OS.

Ochranné známky

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

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

Další jména společností, produktů nebo služeb mohou být ochrannými 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 NEBO ODVOZENÝCH VČETNĚ, BEZ OMEZENÍ, ODVOZENÝCH ZÁRUK PRODEJNOSTI, NEPORUŠENÍ PRÁV TŘETÍCH STRAN NEBO ZÁRUKY VHODNOSTI PRO URČITÝ ÚČEL.

Vytištěno v Dánsku společností IBM Danmark A/S.