

IBM

@server

iSeries

Quality of Service (QoS)

Verze 5, vydání 3





@server

iSeries

Quality of Service (QoS)

Verze 5, vydání 3

Poznámka

Dříve než použijete tyto informace a produkt, který podporují, nezapomeňte si přečíst informace uvedené v části “Poznámky”, na stránce 65.

Čtvrté vydání (srpen 2005)

Toto vydání se týká verze 5, vydání 3, modifikace 0 operačního systému OS/400 (5722-SS1) a všech následných vydání a modifikací, dokud nebude v nových vydáních uvedeno jinak. Tato verze nemůže být spuštěna na žádném počítači RISC (reduced instruction set computer), ani na modelech CISC.

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

Obsah

Quality of service (QoS) 1

Co je nového ve verzi V5R3?	1
Tisk tohoto tématu	3
Koncepce QoS	3
Zásady odlišovaných služeb	4
Integrované služby	7
Zásada příchozích připojení	11
Provozní třída	13
Rozhraní QoS API.	16
Server adresářů.	22
Scénáře QoS	24
Scénář QoS: Omezení přenosu prohlížečů.	25
Scénář QoS: Zabezpečené a předvídatelné výsledky (VPN a QoS)	29
Scénář QoS: Omezení příchozích připojení	33
Scénář QoS: Předvídatelný provoz B2B	36
Scénář QoS: Vyhrazený přenos (IP telefonie).	39
Plánování použití QoS	43
Požadavky na oprávnění	43
Systémové požadavky	44
Smlouvy SLA (Service level agreement)	44
Síťový hardware a software	45

Konfigurování QoS	45
Konfigurování QoS pomocí průvodců	46
Konfigurování serveru adresářů	47
Pořadí zásad QoS	48
Správa QoS.	48
Přístup k nápovědě pro QoS v prostředí produktu iSeries Navigator	49
Zálohování zásad QoS	49
Kopírování existující zásady QoS	50
Úprava zásad QoS.	50
Monitorování QoS.	50
Odstraňování problémů v QoS	54
Žurnálování zásad QoS	55
Protokolování úloh serveru QoS.	56
Monitorování transakcí serveru	57
Sledování aplikací TCP	60
Související informace o QoS	63

Dodatek. Poznámky 65

Ochranné známky	67
Ustanovení a podmínky pro stahování a tisk publikací.	67

Quality of service (QoS)

Veškerý provoz ve vaší síti má stejnou prioritu. Nedůležitý přenos prohlížeče se považuje za stejně významný jako kritické podnikové aplikace. Když pak např. generální ředitel při své prezentaci používá multimediální aplikaci, nastane problém s prioritou IP paketů. Je nezbytné, aby tato aplikace měla po dobu prezentace zajištěn vyšší výkon než ostatní aplikace.

Řešení iSeries^(TM) QoS umožňuje, aby zásady požadovaly síťovou prioritu a šířku pásma pro aplikace TCP/IP. Priorita paketů je důležitá tehdy, pokud posíláte aplikace, které potřebují předvídatelné a spolehlivé výsledky, jako např. multimediální aplikace. Zásady QoS na serveru iSeries^(TM) také mohou limitovat data opouštějící server, řídit požadavky na připojení a kontrolovat zatížení serveru.

Předtím, než začnete konfigurovat zásady, je důležité, abyste pochopili principy QoS. Další informace, které potřebujete znát pro implementaci produktu QoS, obsahují níže uvedené odkazy.

Co je nového ve verzi V5R3?

Zde je uveden přehled změn týkajících se síťových funkcí pro QoS a změn v tématu o QoS v aplikaci Information Center.

Tisk tohoto tématu

Zde je postup pro výtisk celého tématu.

Koncepce QoS

Pokud je pro vás problematika QoS nová, zde se můžete seznámit se základními koncepty QoS. Získáte přehled o tom, jak produkt QoS pracuje a jak jsou jednotlivé funkce QoS vzájemně propojené.

Scénáře QoS

Zde je několik scénářů nasazení zásad QoS, ve kterých se můžete seznámit s důvody pro použití QoS a způsobem použití QoS.

Plánování použití QoS

Zde jsou odkazy na poradce pro plánování QoS a na další informace o sítích, které budete potřebovat pro efektivní použití QoS.

Konfigurování QoS

Postupujte dle uvedených postupů, chcete-li vytvořit nové zásady odlišovaných služeb, zásady integrovaných služeb a zásady příchozích připojení.

Správa QoS

Pomocí uvedených postupů lze spravovat existující zásady QoS. Následující odstavce popisují, kde lze najít aktuální úlohy pro úpravu, prohlížení a používání ostatních technik správy zásad. Také zde najdete popis toho, jak lze použít monitorování QoS a kolekci dat k analýze vašich přenosů IP.

Odstraňování problémů v QoS

V tomto tématu jsou informace o tom, jak řešit problémy související s QoS.

Související informace o QoS

Zde naleznete odkazy na další užitečné zdroje informací o QoS. Existuje mnoho dalších publikací, webových stránek, RFC (Request for comments) a analytických materiálů (white paper).

Co je nového ve verzi V5R3?

V této části jsou popsány nové funkce produktu QoS verze 5, vydání 3.

Nová funkce

- **Nová rozšířená zásada odlišovaných služeb (DiffServ)**

Dříve umožňovaly zásady odlišovaných služeb přiřadit úroveň služeb odchozím spojením dle zdrojových /cílových

IP adres, portů, aplikací nebo klientů. Ve verzi V5R3 mohou vaše aplikace systému iSeries^(TM) obdržet úroveň služby dle specifických informací aplikací. Další informace získáte, prostudujete-li si koncept odlišovaných služeb.

- **Dvě volby ukládání zásad QoS**

Dříve byly zásady QoS exportovány na server adresářů s nejnovějším protokolem LDAP verze 3. Nyní jsou vaše zásady QoS vždy uloženy ve vašem lokálním systému. Stále však máte možnost exportovat je také na server adresářů. Toto téma poskytuje informace o výhodách každé z těchto zásad, stejně jako další informace o serverech adresářů.

- **Identifikace aplikací dle jména serveru**

Dříve jste úroveň služeb protokolům TCP/UDP přiřazovali dle jejich známých portů. Identifikace aplikace dle portu však nefunguje správně v případě všech aplikací. Například přenosy FTP v pasivním režimu využívají pro datová spojení dynamický port. Nyní můžete aplikaci identifikovat dle jedinečného řetězce znaků nazývaného jméno serveru (jako například TFTP). Tento seznam jmen serverů je předdefinovaný. Pokud konfiguruje zásadu QoS můžete vybrat z předdefinovaného seznamu nebo vytvořit vaše vlastní jméno serveru. Použití jména serveru nahrazuje použití portu nebo rozsahu portů k definování aplikace.

- **Vylepšení třídy služeb**

Průvodce třídou služeb nyní umožňuje definovat třídu služeb, kterou lze sdílet mezi zásadami příchozích i odchozích připojení. V rámci třídy služeb definujete způsob zacházení s přenosy mimo profil. Máte k dispozici novou volbu umožňující snížit zahlcení TCP. Pokud je vybrána, lze prostřednictvím snížení zahlcení TCP regulovat přenosy.

- **Fronty s váženou prioritou**

Po přijetí příchozího připojení je toto připojení umístěno do schvalovací fronty, která je definována v rámci zásady příchozích připojení. Všechny schvalovací fronty mají přiřazenu váhu, která určuje prioritu každé fronty.

Změny informací

- **Monitorování transakcí serveru QoS**

Monitorování je skvělý způsob analýzy a měření toku přenosů v síti. Chcete-li využít tento nástroj, pomohou vám informace a příklad monitorování.

- **Úvod do nových rozhraní API**

Na informace o rozhraní API pro zásady QoS, které využívají rozhraní API, je nyní kladen větší důraz. Informace vás v případě každého typu zásady QoS navedou ke specifickým rozhraním API.

Jak zjistíte, které informace jsou nové nebo které byly změněny

Pro vaši lepší orientaci jsou do textů umístěny symboly, které označují nové nebo změněné pasáže:

- Symbol



označuje počátek nového nebo změněného textu.

- Symbol



označuje konec nového nebo změněného textu.

Další informace o tom, co bylo v tomto vydání doplněno nebo změněno, uvádí dokument Sdělení pro uživatele



Tisk tohoto tématu

Chcete-li zobrazit či stáhnout verzi ve formátu PDF, vyberte Quality of service (zhruba 525 KB).

Chcete-li uložit soubor typu PDF na svou pracovní stanici za účelem prohlížení nebo tisku:

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

Jestliže potřebujete ke stažení nebo vytištění tohoto souboru PDF produkt Adobe Acrobat Reader můžete si kopii tohoto produktu stáhnout z domovské stránky firmy Adobe



Koncepce QoS

Předtím, než se pokusíte implementovat QoS, doporučujeme vám důkladně prostudovat toto téma a ujistit se, že tato služba bude odpovídat vašim požadavkům. Pojmy související s QoS lze nalézt v mnoha informačních zdrojích, v tomto tématu se proto budeme zabývat pouze základními informacemi.

Produkt QoS budete implementovat prostřednictvím konfigurace zásad QoS pomocí průvodců v produktu iSeries^(TM) Navigator. **Zásada QoS** je sada pravidel, které určují způsob přenosu. Zásada QoS v podstatě udává, jakého klienta, aplikaci a časový plán (který stanovujete vy) obdrží konkrétní služba. Můžete implementovat tři typy zásad QoS:

- Zásady odlišovaných služeb QoS
- Zásady integrovaných služeb QoS
- Zásady příchozích připojení

Odlišované služby (DiffServ) a integrované služby (IntServ) jsou považovány za zásady řízení šířky pásma odchozích přenosů. Zásady odchozích připojení limitují data opouštějící síť a pomáhají řídit zátěž serveru. Přenosové rychlosti nastavené v rámci zásady odchozích připojení řídí to, které přenosy dat a jakým způsobem (a zda vůbec) jsou na serveru omezeny. Oba typy zásad odchozích připojení mohou vyžadovat smlouvu SLA (Service level agreement) s vaším ISP (poskytovatelem služeb sítě internet). Další informace najdete v tématu Smlouvy SLA.

Zásady příchozích připojení řídí požadavky na připojení přicházející do vaší sítě z nějakého vnějšího zdroje. Zásady příchozích připojení nejsou závislé na úrovni služeb vašeho ISP. Při rozhodování o vhodném typu zásady QoS je nutno zhodnotit důvody, proč chcete produkt QoS použít, stejně jako funkce vašeho serveru iSeries.

Jednou z nejdůležitějších částí implementace produktu QoS je váš server samotný. Kromě pochopení koncepcí produktu QoS musíte znát i to, jakou roli hraje server v této koncepci. Server iSeries může fungovat pouze jako klient nebo jako server, nikoliv jako směrovač. Server iSeries fungující jako klient může například používat zásady odlišovaných služeb k tomu, aby zajistil, že požadavkům na informace z ostatních serverů bude v síti přiřazena vyšší priorita. Server iSeries fungující jako server může používat zásady příchozích připojení k tomu, aby omezoval požadavky URI přijímané serverem.

Další informace získáte pomocí níže uvedených odkazů:

Odlišované služby

Toto je první z typů zásad odchozích připojení, který můžete na vašem serveru vytvořit. Pomocí odlišovaných služeb rozdělíte provoz na síti do tříd. Při implementaci QoS musíte stanovit, jak chcete klasifikovat síťový provoz a jak zacházet s různými provozními třídami.

Integrované služby

Druhým typem zásad odchozích připojení, který můžete vytvořit, je zásada integrovaných služeb QoS. Pomocí integrovaných služeb můžete zajistit, aby si IP aplikace za použití protokolu RSVP a rozhraní API produktu QoS vyžádala a rezervovala určitou šířku pásma. Zásady integrovaných služeb používají protokol RSVP a rozhraní RAPI API (nebo rozhraní qtoq socket API) k tomu, aby garantovaly spojení typu "end-to-end". Je to nejvyšší úroveň služeb, kterou můžete nastavit; je ovšem také nejsložitější.

Povolení příchozích připojení

Zásada příchozích připojení se používá pro řízení požadavků na spojení přicházejících do sítě.

Provozní třída

V tomto dílčím tématu je vysvětleno, ze kterých prvků se skládá provozní třída. Když tvoříte zásadu odlišovaných služeb QoS, vytvoříte také provozní třídu.

Rozhraní QoS API

Toto dílčí téma popisuje protokol a rozhraní API potřebná pro každý typ zásady QoS. Je zde rovněž vysvětleno, na základě čeho směrovač "podporuje RSVP". Aktuální rozhraní API k produktu QoS zahrnují RAPI API, qtoq sockets API, Sendmsg() API a rozhraní API monitoru.

Monitorování QoS

Toto dílčí téma popisuje monitorování produktu QoS, které vám umožní ověřit, zda zásady QoS fungují tak, jak si to přejete.

Server adresářů

Můžete zvolit exportovat vaše zásady QoS na server adresářů. V tomto tématu jsou popsány výhody použití či nepoužití serveru adresářů, koncepce a konfigurace LDAP a také schéma QoS.

Další informační zdroje najdete v tématu Související informace o QoS.

Zásady odlišovaných služeb



Odlišované služby (DiffServ) rozdělují přenosy do tříd. Chcete-li implementovat zásady odlišovaných služeb ve vaší síti, musíte určit jak klasifikovat vaše síťové přenosy (Viz 4) a jak zacházet s různými třídami (Viz 6).

Třídy provozu dle priorit: Jak klasifikovat síťové přenosy

Odlišované služby dělí přenosy do tříd. Nejběžněji definované třídy jsou definované dle IP adresy klienta, aplikačních portů, typu serveru, protokolu, lokální IP adresy nebo plánu. S veškerými přenosy zařazenými do určité třídy se zachází stejně. Při rozšířené klasifikaci mohou některé aplikace systému iSeriesTM obdržet různé úrovně dostupnosti služeb dle zadaných dat serveru. Použití dat serveru je volitelné, může vám však pomoci, pokud zamýšlíte třídít na jemnější úrovni.

Data serveru jsou založena na dvou rozdílných typech dat aplikace: tokenu aplikací nebo URI. Pokud přenosy odpovídají v rámci zásady zadanému tokenu či URI, bude tato zásada použita na odchozí odpověď. Bude tedy přiřazovat odchozím přenosům libovolnou prioritu, kterou jste zadali v rámci zásady odlišovaných služeb.

Použití tokenu aplikace se zásadami odlišovaných služeb

Pokud použijete data aplikace, bude zásada reagovat na specifické parametry (token a priorita), které aplikace postoupí serveru prostřednictvím API sendmsg(). Toto nastavení je volitelné. Pokud vaše zásady nevyžadují tento stupněm jemnosti třídění, zadejte v průvodci volbu **Všechny tokeny**. Pokud se rozhodnete, že chcete aby token aplikace a priorita odpovídala určitému tokenu a prioritě zadané v rámci zásady odchozích přenosů, můžete tak učinit. V rámci zásady jsou dvě části nastavení dat aplikace, které vyžadují token a prioritu.

- Co je token aplikace?
Token aplikace je libovolný řetězec znaků představující definovaný prostředek, například myFTP. Token zadaný v rámci zásady QoS je porovnán s tokenem poskytnutým aplikací odchozích přenosů. Aplikace poskytne hodnotu token prostřednictvím rozhraní sendmsg() API. Pokud si tokeny navzájem odpovídají, jsou přenosy aplikace zahrnuty do zásady odlišovaných služeb.

Chcete-li použít token aplikace v rámci zásady odlišovaných služeb, postupujte takto:

1. V okně Konfigurace serveru QoS klepněte pravým tlačítkem myši na volbu **DiffServ** a vyberte **Nová zásada**. Spusťte průvodce.
 2. Až narazíte na stránku *Požadavek na data serveru* vyberte volbu **Vybraný aplikační token**.
 3. Chcete-li vytvořit nový token, klepněte na **Nový**. Objeví se dialogové okno *Nový URI*.
 4. Do pole *Jméno* zadejte smysluplné jméno tokenu aplikace.
 5. V poli *URI* vymažte znak (/) a zadejte token aplikace (řetězec nepřesahující 128 znaků). Například myFTPapp, spíše než typický URI.
- Co je priorita aplikace?
Priorita aplikace, kterou zadáte, je porovnávána s prioritou aplikace poskytnutou aplikací odchozích přenosů. Aplikace poskytne hodnotu priority prostřednictvím rozhraní sendmsg() API. Pokud si priority navzájem odpovídají, jsou přenosy aplikace zahrnuty do zásady odlišovaných služeb. Veškeré přenosy definované v rámci zásady odlišovaných služeb přesto budou mít prioritu, která byla přiřazena celkové zásadě.

Pokud zadáte token aplikace, musí být aplikace poskytující tyto informace serveru specificky kódována pro použití rozhraní Sendmsg() API. To provádí vývojář aplikací. Dokumentace k aplikaci by měla poskytovat platné hodnoty (token a prioritu), které použije administrátor produktu QoS v rámci zásady odlišovaných služeb. Poté zásada odlišovaných služeb aplikuje pro přenosy, které odpovídají tokenu nastavenému v rámci zásady QoS, svoji vlastní prioritu a klasifikaci. Pokud aplikace neobsahuje hodnoty, které odpovídají hodnotám nastaveným v rámci zásady QoS, musíte buď změnit aplikaci, nebo použít pro zásadu odlišovaných služeb jiné parametry dat aplikace.

Podrobné informace o programování v oblasti rozšíření produktu QoS - sendmsg() API uvádí téma Rozhraní sendmsg() API.

Použití URI v rámci zásad odlišovaných služeb

Jak již bylo zmíněno výše, při vytváření zásady odlišovaných služeb vám průvodce umožní nastavit informace o datech serveru. Přestože vás průvodce vyzve, abyste do polí zadali token aplikace, můžete místo něj zadat relativní URI. Toto opět není povinné. Pokud vaše zásady nevyžadují tento stupeň jemnosti třídění, zadejte v průvodci volbu **Všechny tokeny**. Pokud se rozhodnete, že chcete aby URI odpovídal určitému URI zadanému v rámci zásady odchozích přenosů, můžete tak učinit.

Relativní URI je v podstatě podmnožina absolutního URI (obdoba dřívějšího absolutního URL). Vezměme si tento příklad: <http://www.ibm.com/software>. Segment **http://www.ibm.com/software** představuje absolutní URI. Segment **/software** je relativní URI. Každé relativní URI musí začínat dopředným lomítkem (/). Zde je několik příkladů platných relativních URI:

- /market/grocery#D5
- /software
- /market/grocery?q=green

Dříve, než nastavíte zásadu odlišovaných služeb využívající adresy URI, se musíte ujistit, že aplikační port přiřazený URI odpovídá direktivě "Listen" aktivované pro FRCA v konfiguraci produktu Apache Web Server. Informace o tom, jak lze změnit nebo zobrazit port HTTP serveru obsahuje téma: Správa adresa a portů pro HTTP server (provozovaný na Apache serveru).

FRCA (Fast Response Cache Accelerator) určí URI pro každou odchozí odpověď HTTP. Porovná URI vztahující se k odchozí odpovědi s URI definovaným v rámci každé zásady odlišovaných služeb. První zásada s řetězcem token (URI) odpovídající nejlépe URI určenému ve FRCA, je použita na všechny odevzy s tímto URI.

Nastavování priorit: Jak zacházet s třídami

Poté, co jsou přenosy klasifikovány, vyžadují odlišované služby také PHB (chování při jednotlivých přechodech) k tomu, aby mohli definovat "způsob", kterým jsou přenosy zpracovávány. Pomocí bitů v IP hlavičce server identifikuje úroveň služeb pro daný IP paket. Směrovače a přepínače alokují své prostředky na základě informace o PHB (chování při jednotlivých přechodech) obsažené v poli TOS (type of service octet) v IP hlavičce. Pole TOS bylo předdefinováno v RFC (Request for comment) 1349 a v operačním systému OS/400^(R) V5R1. Kód PHB určuje způsob, jakým je paket v jednotlivých síťových uzlech přeposílán. Je reprezentován hodnotou, která se nazývá identifikační bod. Pakety jsou označeny buď na serveru nebo v jiném prvku sítě, např. ve směrovači. Aby určitý paket obdržel úroveň služeb, kterou požaduje, musí každý uzel sítě umožňovat odlišované služby. To znamená, že dané zařízení musí být schopno provádět zpracování PHB. Základem pro zpracování PHB je to, že uzel sítě musí umět používat plánování front (queue scheduling) a správu výstupních priorit (outbound priority management). Další informace o tom, co znamená, že zařízení "umožňuje odlišované služby", najdete na stránce Faktory přenosů QoS.

Jestliže paket prochází přes směrovač nebo přepínač, který neumožňuje odlišované služby, ztratí paket svoji úroveň služeb. Paket bude zpracován, ale může dojít k neočekávanému zpoždění. Na serveru iSeries můžete použít buď předdefinované identifikační body PHB nebo můžete vytvořit své identifikační body. Nedoporučuje se však používat vlastní identifikační body mimo vaši privátní síť. Pokud si nejste jisti, které identifikační body máte přiřadit, prostudujte si téma Použití identifikačních bodů pro přiřazení chování při jednotlivých přechodech.

Na rozdíl od integrovaných služeb nevyžadují přenosy s odlišovanými službami rezervaci nebo manipulaci s jednotlivými toky dat. S veškerými přenosy zařazenými do určité třídy se zachází stejně.

Odlišované služby lze také použít pro omezení přenosů opouštějící server. To znamená, že server iSeries opravdu používá odlišované služby. Omezení méně důležitých aplikací umožní, aby životně důležité aplikace odcházely ze serveru přednostně. Při vytváření provozní třídy pro zásadu jste požádáni, abyste nastavili různé mezní hodnoty pro váš server. Mezi tyto limity výkonu patří velikost sektoru token, maximální přenosová rychlost a průměrná přenosová rychlost. Další informace o těchto parametrech najdete v příslušných heslech nápovědy pro QoS v rámci produktu iSeries Navigator



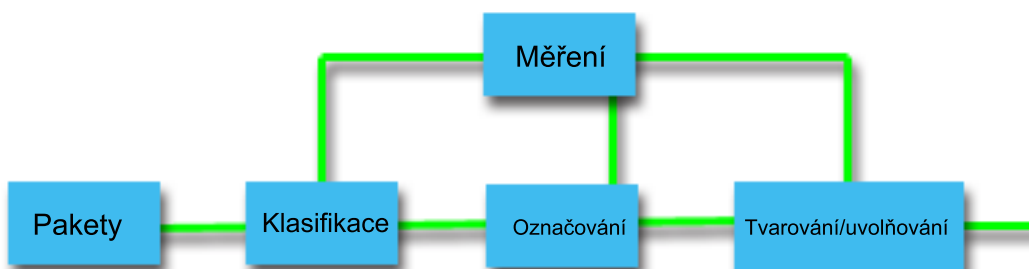
Faktory přenosů QoS

Síťová zařízení, která využívají zásady QoS, musí mít určité schopnosti, které podporují odlišované služby (DiffServ). Konkrétně to znamená, že síťová zařízení, jako jsou např. směrovače a přepínače, musí mít tyto schopnosti týkající se práce s pakety: klasifikace, měření, označování, tvarování a uvolňování. Tyto schopnosti se ve svém souhrnu nazývají *faktory přenosů QoS*. Pokud síťové zařízení splňuje všechny faktory přenosů QoS, pak se považuje za zařízení, které podporuje DiffServ (odlišované služby).

Poznámka: Tyto hardwarové požadavky nejsou pro systémy iSeries^(TM) charakteristické. Tyto termíny nejsou v rozhraní produktu QoS používány, protože tento server neumí řídit externí hardware. Mimo privátní síť musí mít hardware schopnost zpracovávat obecné požadavky produktu QoS. Ověřte si v dokumentaci k příslušnému vybavení, zda zařízení odpovídá všem požadavkům odlišovaných služeb. Dříve, než budete implementovat zásady QoS, vám také doporučujeme prostudovat obecné koncepce a nezbytné předpoklady produktu QoS.

Následující obrázek uvádí logické znázornění, jak na sebe jednotlivé faktory přenosů QoS navazují.

Obrázek 11. Faktory přenosů QoS



Níže jsou popsány jednotlivé faktory přenosů QoS podrobněji.

Klasifikace

Klasifikace provozu znamená, že se pakety v datovém toku vybírají na základě obsahu v jejich IP hlavičkách. Server iSeries definuje dva typy klasifikace. Klasifikace BA (Behavior aggregate) třídí pakety výhradně na základě identifikačního bodu odlišovaných služeb (DSCP). Klasifikace MF (Multi-field) třídí pakety na základě hodnoty kombinace jednoho nebo více polí hlavičky, např. zdrojové adresy, adresy určení, pole odlišovaných služeb, ID protokolu, čísla zdrojového portu, URI, typu serveru nebo čísla portu určení.

Měření

Při měření provozu se zjišťuje, zda IP pakety postoupené dále po klasifikaci odpovídají profilu IP hlavičky přenosu. Informace v IP hlavičce je určena hodnotami, které nastavujete v rámci zásady QoS pro tento typ přenosů. Výsledek měření se posílá dál za účelem vyvolání konkrétní akce. Akce se provádí pro každý paket, ať do profilu spadá, nebo je mimo profil.

Označování

Při označování paketů se nastavuje pole odlišovaných služeb (DS). Označování lze nakonfigurovat tak, že se všechny pakety označují jeden identifikační bod nebo sadou identifikačních bodů používaných pro volbu chování při jednotlivých přechodech (PHB).

Tvarování

Při tvarování dochází ke zpoždění některých nebo všech paketů v toku přenosu tak, aby se tok uvedl do souladu s profilem přenosu. Tvarování využívá určitou omezenou vyrovnávací paměť, a pokud v ní není dostatek místa pro opožděné pakety, mohou být pakety směrovači vyřazeny.

Uvolňování

Při uvolňování paketů dochází k vyřazení některých nebo všech paketů z toku přenosu. Dochází k tomu proto, aby se tok přenosu uvedl do souladu s profilem přenosu.

Integrované služby

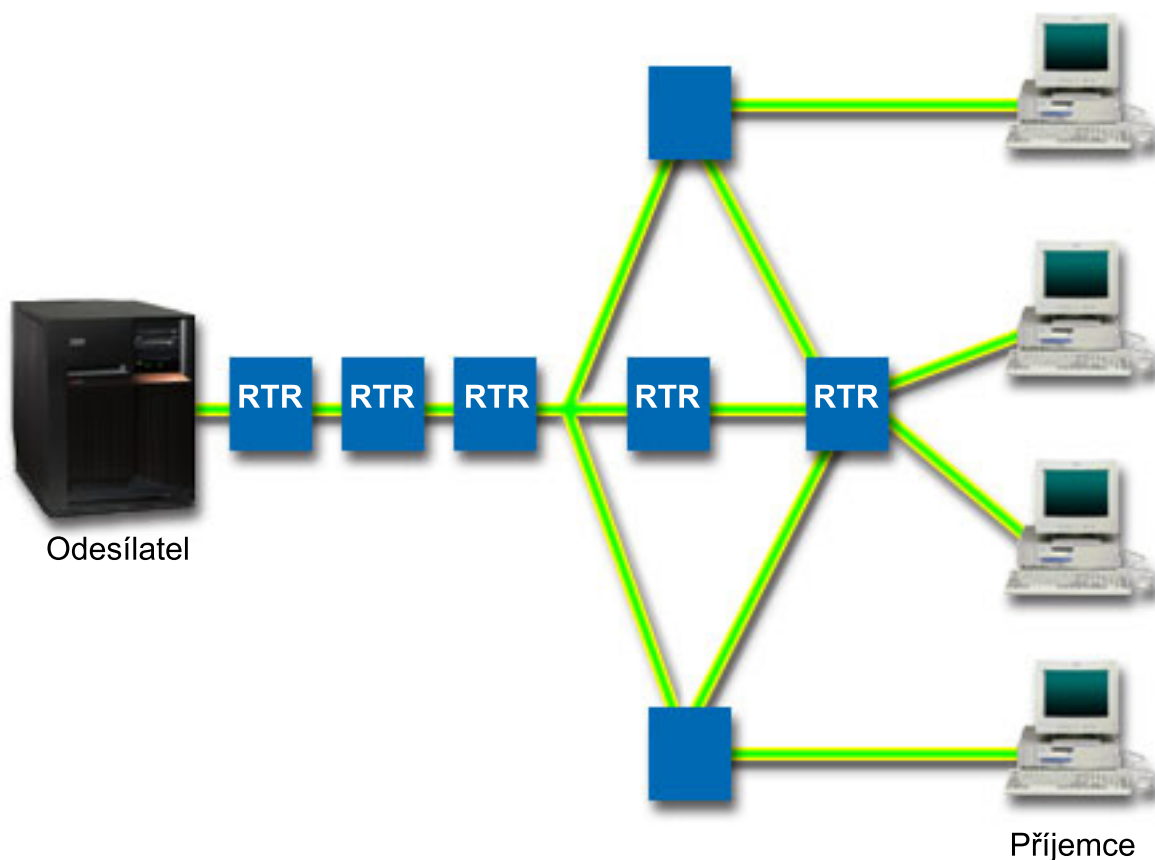
Integrované služby se zabývají dobou doručování přenosu a přiřazováním zvláštních instrukcí pro zacházení s konkrétními přenosy. Se zásadami integrovaných služeb je potřeba pracovat uvážlivě, protože garantování datového přenosu je stále poměrně nákladná záležitost. Avšak pořizování nadměrných kapacit vašich prostředků může být ještě nákladnější.

Integrované služby zajišťují rezervaci prostředků pro konkrétní zásadu QoS předtím, než jsou data zaslaná. Směrovače jsou před datovým přenosem signalizovány a síť pak řídí průběžný přenos dat na základě této zásady QoS. **Zásada QoS** je sada pravidel, které určují způsob přenosu. V podstatě se jedná o seznam parametrů pro řízení přístupu. Žádost o rezervaci šířky pásma přichází ze strany klienta. Jestliže všechny směrovače na trase přenosu s požadavkem přicházejícím od klienta souhlasí, dostane se žádost na server a je porovnána se zásadou integrovaných služeb QoS. Jestliže žádost spadá do limitů definovaných danou zásadou QoS, poskytne server QoS povolení pro připojení RSVP

a vyhradí pro aplikaci požadovanou šířku pásma. Rezervace se provádí prostřednictvím protokolu RSVP (Resource Reservation Protocol) a rozhraní RAPI nebo rozhraní qtoq QoS sockets API. Další informace najdete v tématu Rozhraní QoS API.

Každý síťový uzel, kterým přenos prochází, musí mít schopnost používat protokol RSVP. Směrovače realizují QoS prostřednictvím následujících funkcí pro řízení provozu: plánování paketů, klasifikace paketů a řízení přístupu. Schopnost provádět tyto funkce pro řízení provozu se u směrovačů nazývá také tak, že směrovač "podporuje RSVP". Z uvedeného vyplývá, že nejdůležitější součástí implementace zásad integrovaných služeb QoS je schopnost řídit a předvídat prostředky ve vaší síti. Chcete-li získat předvídatelné výsledky (předvídatelnou úroveň služeb), musí každý uzel vaší sítě podporovat RSVP. Předpokládejme například, že provoz ve vaší síti je směrován na základě prostředků, ne na základě toho, která trasa obsahuje směrovače podporující RSVP. Jde-li pak přenosy přes směrovače, které neumožňují RSVP, může dojít k problémům s nepředvídaným výkonem sítě. Spojení se provede, ale výkon, který aplikace požaduje, tento směrovač negarantuje. Na následujícím obrázku je znázorněno, jak proces integrovaných služeb QoS logicky funguje.

Obrázek 13. Trasa RSVP mezi klientem a serverem.



Aplikace podporující RSVP na serveru zaznamenává žádost o připojení od klienta. Jako reakci vydá serverová aplikace klientovi příkaz PATH. Tento příkaz se vydá pomocí rozhraní RAPI nebo qtoq QoS sockets API a obsahuje informaci o IP adrese směrovače. Příkaz PATH obsahuje informace o dostupných prostředcích na serveru a směrovačích na trase přenosu, a také informace o trase mezi serverem a klientem. Aplikace podporující RSVP na klientovi pak pošle zpátky po síťové trase příkaz RESV, aby serveru signalizovala, že síťové prostředky byly alokovány. Tento příkaz provádí vlastní rezervaci na základě směrovacích informací v příkazu PATH. Server a všechny směrovače na cestě přenosu si rezervují prostředky pro spojení RSVP. Když server obdrží příkaz RESV, aplikace spustí

přenos dat klientovi. Data se přenášejí po stejné trase, jakou probíhala rezervace. Toto opět potvrzuje, jak je pro úspěšnou implementaci zásad QoS důležitá schopnost směrovačů provádět tuto rezervaci.

Integrované služby nejsou primárně určeny pro krátkodobá spojení RSVP, jako například HTTP. Záleží to samozřejmě na vás. Pouze vy můžete rozhodnout, co je pro vaši síť nejlepší. Je potřeba uvážit, které oblasti a které aplikace mají problémy s výkonností a potřebují služby s definovanou úrovní služeb, tedy QoS. Aplikace používané v rámci zásady integrovaných služeb musí být schopny používat protokol RSVP. V současné době váš server nemá aplikace podporující RSVP, musíte si proto napsat vlastní aplikaci podporující RSVP. Další informace o rozhraní API integrovaných služeb najdete v části Rozhraní QoS API.

S tím, jak pakety do sítě přicházejí a pokoušejí se opustit síť, určuje server, zda má prostředky na to, aby mohl pakety poslat. Potvrzení nebo odmítnutí závisí na množství prostoru v sektoru token. Počet bitů, který je povolen pro sektor token, limity pro šířku pásma, limity pro přenosovou rychlost a maximální počet spojení, které server povolí, nastavujete manuálně. Tyto hodnoty se souhrnně nazývají limity výkonu. Jestliže se pakety nacházejí v rámci limitních hodnot serveru, jsou pakety vyhovující a server je posílá dál. Při integrovaných službách QoS se každému spojení poskytuje vlastní sektor token.

Integrované služby s použitím označení odlišovaných služeb

Pokud si nejste jisti, zda může celá síť zaručit připojení RSVP, můžete přesto vytvořit zásadu integrovaných služeb. Pokud však síťové prostředky nemohou použít protokol RSVP, nelze spojení zaručit. V této situaci může být žádoucí použít pro zásadu identifikační bod. Tento identifikační bod je obvykle použit v rámci zásad odlišovaných služeb k tomu, aby byla přenosům přiřazena provozní třída. I v případě, že není připojení garantováno, pokusí se tento identifikační bod přidělit připojení nějakou prioritu. Další informace najdete v tématu Použití označování odlišovaných služeb pro integrované služby.

Funkce pro řízení přenosů

Funkce řízení se vztahují pouze na integrované služby a nejsou pro systémy iSeries^(TM) charakteristické. Tyto termíny nejsou v rozhraní produktu QoS používány, protože tento server neumí řídit externí hardware. Mimo privátní síť musí mít hardware schopnost zpracovávat obecné požadavky produktu QoS. O požadavcích obecného směrovače na zásady integrovaných služeb je pojednáno níže. Předtím, než budete implementovat zásady QoS, vám doporučujeme prostudovat obecné koncepty a nezbytné předpoklady produktu QoS.

Chcete-li zajistit předvídatelné výsledky, musí být na cestě přenosu hardware, který podporuje RSVP. Aby směrovače mohly používat protokol RSVP, musí mít určité funkce pro řízení provozu. Často se pro vyjádření této vlastnosti používá označení, že směrovač "podporuje RSVP" nebo "podporuje QoS". Nezapomeňte, že váš server může fungovat pouze jako server nebo jako klient. V tomto okamžiku nemůže být použit jako směrovač. Ověřte v publikacích, které se týkají vašich síťových zařízení, zda tato zařízení umí zacházet s požadavky QoS.

Funkce pro řízení přenosů zahrnují tyto funkce:

Plánování paketů

Tato funkce řídí posílání paketů na základě informace v IP hlavičce. Funkce plánování paketů zajišťuje, že bude paket doručen v souladu s parametry, které jste nastavili v rámci zásady QoS. Plánování paketů se provádí v místě, kde se pakety řadí ve frontě.

Klasifikace paketů

Tato funkce identifikuje, které pakety v rámci toku IP obdrží určitou úroveň služeb, a to opět na základě informace v IP hlavičce. Každý příchozí paket je touto funkcí zmapován a zařazen do určité třídy. Všechny pakety zařazené do stejné třídy jsou zpracovány stejným způsobem. Úroveň služeb je dána informací, kterou zadáváte v rámci definice zásady QoS.

Řízení přístupu

Funkce řízení přístupu obsahuje rozhodovací algoritmus, pomocí kterého směrovač určuje, zda má dost směrovacích prostředků, aby mohl akceptovat požadovanou úroveň QoS u nového datového toku. Pokud nemá dostatek prostředků, je nový datový tok odmítnut. Jestliže je tok přijatý, směrovač pro daný paket zaktivuje funkce plánování a klasifikace, aby rezervoval požadovanou úroveň QoS. Řízení přístupu se provádí v každém směrovači na rezervované trase přenosu.

V této části jsou uvedeny pouze základní informace o plánování a klasifikaci paketů. Další alternativní zdroje jsou uvedeny na stránce s tématem Související informace o QoS.

Typy integrovaných služeb

Existují dva typy integrovaných služeb: služby řízeného zavádění a garantované služby.

Služby řízeného zavádění

Služby řízeného zavádění podporují aplikace, které jsou vysoce citlivé na zahlcení sítě, např. aplikace v reálném čase. Aplikace také musí být tolerantní vůči určitým malým ztrátám nebo zpožděním. Jestliže aplikace využívá služby řízeného zavádění, její výkonnost se nebude se zvýšeným zatížením sítě zhoršovat. Provoz bude zajištěn pomocí služby, která udržuje normální provoz v síti za omezenějších podmínek.

Směrovače musí zajistit, aby služba řízeného zavádění obdržela adekvátní šířku pásma a prostředky na zpracování paketů. K tomu, aby mohly směrovače toto provádět, musí podporovat QoS a mít podporu pro integrované služby QoS. Musíte proto ve specifikacích ke směrovačům ověřit, zda poskytují QoS prostřednictvím funkcí pro řízení provozu. Funkce pro řízení provozu se skládají z těchto komponent: plánování paketů, klasifikace paketů a řízení přístupu.

Garantované služby

Garantované služby zajišťují, že pakety budou doručeny v rámci stanovené doby dodání. K aplikacím, které potřebují garantované služby, patří např. audio a video vysílací systémy, které používají kontinuální technologie (streaming). Garantované služby kontrolují maximální zpoždění ve frontě tak, aby se pakety nepožděly nad stanovený časový limit. Každý směrovač na trase přenosu musí podporovat RSVP, aby zajistil dodání paketu v souladu s touto zásadou QoS. Garantované služby se definují tak, že stanovujete pro přenos limit velikosti sektoru token a limity přenosové rychlosti. Garantovanou službu lze použít pouze pro aplikace využívající protokol TCP.

Limity pro sektor token a přenosovou rychlost

Limit pro sektor token a limity pro přenosovou rychlost se souhrnně nazývají limity výkonu. Tyto limity výkonu pomáhají garantovat dodání paketů v rámci zásad řízení šířky pásma u odchozích přenosů, a to jak v případě zásad integrovaných služeb QoS, tak v případě zásad odlišovaných služeb QoS.

Velikost sektoru token

Velikost sektoru token určuje množství informací, které může server v daném čas zpracovat. Pokud posílá aplikace serveru informace rychleji, než může server data poslat ven ze sítě, plní se vyrovnávací paměť. Všechny pakety dat překračující tento limit jsou považovány za pakety mimo profil. Vyjímkou z tohoto pravidla jsou zásady integrovaných služeb. Můžete vybrat volbu **Neomezit**, čímž povolíte požadavky na připojení RSVP. V případě všech ostatních zásad lze definovat, jak je zacházeno s přenosy mimo profil. Maximální velikost sektoru token je 1 GB.

Limit přenosové rychlosti tokenu

Limity přenosové rychlosti udávají dlouhodobou rychlost datových přenosů neboli počet bitů za sekundu, který může vstoupit do sítě. Zásada QoS zkontroluje požadovanou šířku pásma a porovná ji s limity pro přenosovou rychlost, které má v sobě definovány. Pokud požadavek způsobí, že server překročí nastavené limity, server žádost odmítne. Limity přenosové rychlosti jsou v rámci zásad integrovaných služeb QoS používány pouze při řízení přístupu. Tato hodnota se může pohybovat v rozmezí od 10 Kb/s do 1 Gb/s. Můžete zde také zadat **Neomezit**. Pokud rychlosti přiřadíte volbu **Neomezit**, budou limitem volné prostředky.

Rada: Chcete-li zjistit, jak nastavit limity, můžete použít funkci Monitorování QoS. Vytvořte zásadu QoS s dostatečně velkým celkovým limitem přenosové rychlosti, aby pokryl většinu datového provozu ve vaší síti. Pak spusíte sběr dat pro tuto zásadu QoS. V části Monitorování aktuálního stavu sítě najdete příklad, jak získat data o celkových přenosových rychlostech, které vaše aplikace a síť v současné době používá. Na základě výsledků monitorování pak příslušně snížíte limity přenosové rychlosti.

Chcete-li si prohlédnout monitorovaná data v reálném čase namísto určité kolekce dat, pouze použijte funkci monitor. Funkce monitorování poskytuje v reálném čase statistiky všech aktivních zásad.

Použití označování odlišovaných služeb pro integrované služby

Tato zásada QoS se nejčastěji používá ve smíšených prostředích. Smíšené prostředí znamená, že na trase rezervace integrovaných služeb existují různé směrovače, které nepodporují rezervaci integrovaných služeb, ale podporují odlišované služby. Vzhledem k tomu, že vaše přenosy procházejí přes různé domény, které používají různé smlouvy SLA (Service Level Agreement) a zařízení s různou úrovní funkcí, nemusíte být schopni získat takovou úroveň služeb, kterou si naplánujete.

Chcete-li zmenšit tento potenciální problém, můžete připojit k zásadě integrovaných služeb určité označení používané zásadami odlišovaných služeb. V případě, že zásada QoS prochází směrovačem, který nepoužívá protokol RSVP (a nepodporuje tedy integrované služby), udrží si zásada QoS alespoň nějakou úroveň priority. Označení, které k zásadě přidáváte, se nazývá PHB neboli chování při jednotlivých přenosech.

Deaktivace signalizace

Kromě použití označování odlišovaných služeb, jak je popsáno výše, můžete také použít novou funkci pro deaktivaci signalizace "no signal". Pokud je zvolena funkce "no signal", umožní vám odpovídající verze API napsat aplikaci, která zajistí, že se pravidla RSVP zavedou na server, a která bude vyžadovat, aby při konverzaci TCP/IP podporovala RSVP pouze strana serveru. Signalizace RSVP se automaticky provádí ze strany klienta. Toto řešení umožní, aby se pro aplikaci vytvořilo spojení RSVP i tehdy, když strana klienta není schopna RSVP používat.

Funkce "No Signal" je zadána v rámci zásady integrovaných služeb. Zadáváte ji v dialogovém okně **Properties** pro kteroukoliv zásadu integrovaných služeb QoS.

1. V prostředí produktu iSeries^(TM) Navigator rozbalte svůj server → **Síť** → **Zásady pro práci s IP**.
2. Klepněte pravým tlačítkem myši na **Quality of Service** a vyberte volbu **Configuration**.
3. Rozbalte **Šířka pásma odchozích přenosů** → **IntServ**.
4. Klepněte pravým tlačítkem myši na jméno požadované zásady IntServ a vyberte volbu **Vlastnosti**. Objeví se dialogové okno Vlastnosti IntServ.
5. Vyberte kartu **Traffic Management** a aktivujte nebo deaktivujte signalizaci. Zde také můžete upravovat časový plán, klienta, aplikace a správu provozu.

Další informace najdete v tématech Provozní třídy a Integrované služby.

Zásada příchozích připojení



Zásada příchozích připojení se používá k řízení přenosů pokoušejících se připojit k serveru. Přístup můžete omezit dle klienta, URI, aplikace nebo dle lokálního rozhraní na vašem serveru iSeries^(TM). Kromě toho můžete výkon serveru vylepšit použitím provozní třídy v případě příchozích přenosů. Tuto zásadu můžete definovat prostřednictvím průvodce povolením příchozích připojení v prostředí produktu iSeries Navigator.

Existují tři komponenty zásady příchozích připojení, ke kterým je třeba podat více informací. Mezi ně patří URI, prostřednictvím kterých lze omezit přenosy, počet připojení definovaný v rámci provozní třídy a prioritní fronty pro pořadí úspěšných připojení. Další informace získáte prostřednictvím níže uvedených odkazů:

- URI (Viz 11)
- Počet připojení (Viz 12)
- Fronty s váženou prioritou (Viz 12)

URI

Můžete zvážit možnost použití zásady příchozích připojení a omezit tak přenosy HTTP na váš webový server. V tomto případě můžete vytvořit zásadu příchozích připojení, která omezí přenosy dle určitého URI. Počet požadavků URI je součástí řešení, které pomáhá chránit servery před přetížením. Označením určitých URI použijete řízení přístupu

dle informací aplikační vrstvy a omezíte tak serverem přijaté požadavky URI. V odvětví IT se tento typ řízení nazývá také *header-based connection request control*, tj. řízení požadavků na připojení na základě hlavičky, které používá URI k nastavení priorit.

Zadáním URI umožníte zásadě příchozích připojení prověřovat obsah, nikoliv pouze hlavičky paketů. Zkoumaný obsah je jméno URI. V systému iSeries můžete použít relativní jméno URI (například **/products/clothing**). Relativní URI je popsáno v následujícím příkladu.

Relativní URI

Relativní URI je v podstatě podmnožina absolutního URI (obdoba dřívějšího absolutního URL). Vezměme si tento příklad: `http://www.ibm.com/software`. Segment **`http://www.ibm.com/software`** představuje absolutní URI. Segment **`/software`** je relativní URI. Každé relativní URI musí začínat dopředným lomítkem (/). Zde je několik příkladů platných relativních URI:

- `/market/grocery#D5`
- `/software`
- `/market/grocery?q=green`

Poznámka:

- Při použití URI musíte jako protokol určit protokol TCP. Kromě toho musí port a IP adresa odpovídat portu a IP adrese konfigurované v rámci vašeho HTTP serveru. Nejčastěji je to port 80.
- Při zadávání URI lze použít zástupné znaky. Například `/software` bude zahrnovat všechno v rámci adresáře `software`.
- Nepoužívejte znak "*" v rámci URI. To není platný znak.
- Informace URI lze použít v rámci zásady příchozích připojení nebo v rámci zásad odlišovaných služeb (odchozích připojení).

Dříve, než nastavíte zásadu příchozích připojení využívající adresy URI, se musíte ujistit, že aplikační port přiřazený URI odpovídá direktivě "Listen" aktivované pro FRCA v konfiguraci produktu Apache Web Server. Informace o tom, jak lze změnit nebo zobrazit port HTTP serveru obsahuje téma: Správa adresa a portů pro HTTP server (provozovaný na Apache serveru).

Počet připojení

Jakožto součást zásady příchozích připojení musíte také zvolit provozní třídu. Tato provozní třída definuje přenosové rychlosti, což funguje jako řízení přístupu za účelem omezení připojení akceptovaných serverem.

Prostřednictvím limitů počtu připojení jsou přijmuty nebo odmítnuty nové pakety dle v rámci zásady definovaného průměrného počtu připojení za sekundu a maximálního počtu připojení v daném okamžiku. Hodnoty pro tyto limity připojení, vyjádřené jako průměrná přenosová rychlost (average rate limit) a počet připojení v shluku (connection burst limit), zadáváte v rámci práce s průvodcem v produktu iSeries Navigator. Když server obdrží požadavek na připojení, analyzuje informace v hlavičce paketu, aby zjistil, zda je tento přenos definovaný v rámci některé zásady. Systém tuto informaci porovnává se stanovenými limity pro připojení. Jestliže je paket v rámci stanovených hodnot zásady, je zařazen do fronty.

Při vyplňování informací v rámci průvodce povolení příchozích připojení použijte výše uvedené informace. Po dokončení zásady také můžete v prostředí produktu iSeries Navigator použít přiřazenou nápovědu odkazující na obdobné informace.

Fronty s váženou prioritou

Jako součást tohoto řízení přístupů můžete také určit prioritu, podle které budou požadavky na připojení zpracovány, poté, co byly zásadami zhodnoceny. Tím, že přiřadíte frontě priorit určitou váhu, v podstatě kontrolujete dobu odezvy fronty po navázání spojení. Pokud je připojení umístěno do fronty, bude s ním zacházeno dle priority (vysoká (high), střední (medium), nízká (low) nebo nejlepšího výkonu (best effort)). Pokud si nejste jisti, jaké hodnoty máte použít, použijte předvolené hodnoty. Součet všech vah se musí rovnat 100. Například: Pokud je pro všechny priority zadáno

25, bude s nimi zacházeno stejně. Předpokládejme, že zadáte tyto váhy: Vysoká (High) 50, Střední (Medium) 30, Nízká (Low) 15 a nejlepšího výkonu (Best Effort) 5. Mezi přijaté připojení patří:

- 50% připojení s vysokou prioritou
- 30% připojení se střední prioritou
- 15% připojení s nízkou prioritou
- 5% připojení s prioritou nejlepšího výkonu



Provozní třída

Zásady odlišovaných služeb a zásady příchozích připojení používají provozní třídu k tomu, aby seskupily přenosy do tříd. I když většinu úkonů zajišťuje příslušný hardware, vy řídíte to, jakým způsobem jsou přenosy seskupovány a jakou prioritu jednotlivé provozní třídy musí obdržet.

Při implementaci QoS nejprve definujete zásady QoS. Zásady QoS určují: kdo, co, kde a kdy. Pak musíte konkrétní zásadě QoS přiřadit provozní třídu. Provozní třídy (CoS) se definují zvlášť a může je používat více zásad QoS. Při definování provozní třídy zadáváte zda ji lze použít pro zásady odchozích či příchozích připojení nebo pro oba typy zásad. Pokud zadáte oba typy (odchozí i příchozí), může tuto provozní třídu používat zásada odlišovaných služeb i zásada příchozích připojení.

Nastavení v rámci provozní třídy závisí na tom, zda je provozní třída používána zásadami příchozích připojení, odchozích připojení či oběmi typy. Při vytváření provozní třídy se můžete setkat s těmito požadavky:

Označení identifikačním bodem

QoS používá tyto doporučené identifikační body k přiřazení určitého typu chování při jednotlivých přechodech pro přenosy. Směrovače a prepínače používají tyto identifikační body, když poskytují přenosům určitou úroveň priority. Váš server tyto identifikační body neumí používat, protože nefunguje jako směrovač. Identifikační body, které budete používat, musíte stanovit na základě individuálních potřeb vaší sítě. Zvažte, které aplikace jsou pro vás nejdůležitější a kterým zásadám je nutné přiřadit vyšší prioritu. Nejdůležitější pro to, abyste dosáhli očekávaných výsledků, je, abyste byli konzistentní v přidělování identifikačních bodů. Tyto identifikační body jsou klíčovým prvkem pro rozlišování různých provozních tříd.

Měření provozu

Pomocí limitů řízení přenosové rychlosti omezuje produkt QoS přenosy v rámci sítě. Tyto limity jsou nastaveny prostřednictvím definování velikosti sektoru token, maximální přenosové rychlosti a průměrné přenosové rychlosti. Další informace o těchto konkrétních hodnotách najdete v tématu Limity pro sektor token a přenosovou rychlost.

Přenosy mimo profil

Poslední částí definice provozních tříd je způsob zacházení s přenosy mimo profil. Přiřazením limitů řízení přenosové rychlosti způsobem, který je uveden výše, nastavujete hodnoty pro omezení přenosů. Když provoz překročí tyto mezní hodnoty, považují se další pakety za pakety mimo profil. Tyto informace v rámci provozní třídy sdělují serveru, zda má přerušit provoz UDP a snížit zahlcení TCP, nebo zda má pakety mimo profil tvarovat či znovu označit.

Uvolnit pakety UDP či snížit zahlcení TCP: Pokud se rozhodnete uvolnit a přizpůsobit pakety mimo profil, budou pakety UDP vypuštěny. Zahlcení TCP je však sníženo, takže přenosová rychlost dat vyhovuje přenosové rychlosti sektoru token. Počet paketů, které lze poslat do sítě, se každým okamžikem snižuje a výsledkem je snížení zahlcení.

Zpozdít (Upravit): Jestliže pakety mimo profil zpozdíte, budou tvarovány tak, aby vyhovovaly definovaným charakteristikám pro zpracování.

Znovu označit identifikačním bodem DiffServ: Jestliže pakety mimo profil znovu označíte pomocí identifikačního bodu odlišovaných služeb, bude jim přidělen nový identifikační bod. Aby byly dosaženy vámi požadované charakteristiky zpracování, není přenos paketů zcela přerušeno, ale pakety jsou pouze znovu označeny. Při přiřazování těchto instrukcí pro zpracování v průvodci můžete klepnout na nápovědu a zjistit si podobnější informace.

Priorita

Připojením k serveru, která jsou realizována prostřednictvím různých zásad příchozích připojení, můžete přidělit priority. To vám umožní definovat pořadí, ve kterém jsou dokončena připojení serverem zpracována. Můžete vybrat prioritu vysokou (high), střední (medium), nízkou (low) nebo prioritu nejlepšího výkonu (best effort).

Použití identifikačních bodů pro přiřazení chování při jednotlivých přechodech

Pomocí následujících doporučených identifikačních bodů přiřazuje produkt QoS přenosům určitý typ chování při jednotlivých přechodech. V průvodci provozní třídou budete muset přiřadit zásadě chování při jednotlivých přechodech. Identifikační body, které budete používat, musíte stanovit na základě individuálních potřeb vaší sítě. Pouze vy můžete rozhodnout, jaké schéma identifikačních bodů bude mít smysl ve vašem prostředí. Musíte zvážit, které aplikace jsou pro vás nejdůležitější a kterým zásadám by měla být přidělena vyšší priorita. Nejdůležitější pro to, abyste dosáhli očekávaných výsledků, je, abyste byli konzistentní v přidělování identifikačních bodů. Zásady, které jsou zhruba stejně důležité, mohou používat stejné identifikační body, takže obdržíte v případě těchto zásad shodné výsledky. Pokud si nejste jisti, jaký identifikační bod přiřadit, použijte metodu pokusu a omylu. Vytvořte si testovací zásady QoS, vyzkoušejte je pomocí funkce Monitorování QoS a podle potřeby je přizpůsobujte.

Níže uvedená tabulka zobrazuje doporučené identifikační body založené na odvětvových standardech. Většina ISP podporuje identifikační body odvětvových standardů, podporu vašeho ISP však můžete ověřit. Další informace o smlouvách SLA a úloze vašeho ISP najdete v tématu Smlouvy SLA. Můžete také vytvořit své vlastní identifikační body, jejich externí použití se však nedoporučuje. Vaše vlastní identifikační body lze nejlépe využít v testovacím prostředí.

EF (Expedited forwarding) (Viz 15)
101110

Class selector (Viz 15)
Třída 0 - 000000
Třída 1 - 001000
Třída 2 - 010000
Třída 3 - 011000
Třída 4 - 100000
Třída 5 - 101000
Třída 6 - 110000
Třída 7 - 111000

AF (Assured forwarding) (Viz 15)
AF (Assured forwarding), Class 1, Low - 001010
AF (Assured forwarding), Class 1, Medium - 001100
AF (Assured forwarding), Class 1, High- 001110
AF (Assured forwarding), Class 2, Low - 010010

AF (Assured forwarding), Class 2, Medium - 010100
AF (Assured forwarding), Class 2, High - 010110
AF (Assured forwarding), Class 3, Low - 011010
AF (Assured forwarding), Class 3, Medium - 011100
AF (Assured forwarding), Class 3, High - 011110
AF (Assured forwarding), Class 4, Low - 100010
AF (Assured forwarding), Class 4, Medium - 100100
AF (Assured forwarding), Class 4, High - 100110

EF (Expedited forwarding)

EF (Expedited forwarding) je jedním z typů PHB (chování při jednotlivých přechodech). Používá se zejména pro zajištění garantovaných služeb mezi více sítěmi. EF (Expedited forwarding) poskytuje přenosům průběžné (end-to-end) služby s nízkým procentem ztrát a kolísání tím, že zaručuje určitou šířku pásma v rámci různých sítí. Rezervace šířky pásma je provedena předtím, než je paket zaslán. Hlavním cílem je vyhnout se zpožděním a doručit pakety včas.

Poznámka: Zasilání formou EF (expedited forwarding) je obvykle velmi nákladné, proto se nedoporučuje tento typ PBH používat běžně.

Class selector

Identifikační body v kategorii Class selector jsou jiným typem chování. Existuje sedm tříd - identifikačních bodů. V systému identifikačních bodů Class selector poskytuje Třída 0 paketům nejnižší prioritu a Třída 7 nejvyšší prioritu. Jedná se o nejběžněji používanou klasifikaci chování při jednotlivých přechodech (PHB), protože většina směrovačů používá podobné identifikační body.

AF (Assured forwarding)

AF (Assured forwarding) se dělí na čtyři třídy chování při jednotlivých přechodech (PHB), přičemž u každé třídy se rozlišuje stupeň priority uvolnění paketů - nízká, střední nebo vysoká. Stupeň priority uvolnění paketů určuje pravděpodobnost, s jakou mohou být pakety uvolněny. Každá třída má svá specifika. Třída Class 1, High přiděluje zásadě nejnižší prioritu a třída Class 4, low přiděluje zásadě prioritu nejvyšší. Nízká úroveň uvolnění znamená, že pakety v této zásadě mají nejmenší možnost být na této určité úrovni třídy uvolněny.

Limity průměrného počtu připojení a počtu požadavků přijatých současně (v shluku)

Limity pro počet připojení za vteřinu a počet požadavků přijatých současně (v shluku) se souhrnně označují jako limity přenosové rychlosti. Tyto limity omezují počet příchozích připojení pokoušejících se vstoupit na server. Limity počtu připojení se nastavují v rámci provozní třídy se zásadami příchozích připojení.

Limit počtu připojení ve shluku

Počet připojení ve shluku určuje kapacitu vyrovnávací paměti, ve které se ukládají shluky spojení. Shluky spojení mohou na server vstupovat vyšší přenosovou rychlostí, než může server zvládnout nebo než chcete povolit. Jestliže počet spojení ve shluku překročí limit pro počet spojení ve shluku, který nastavíte, budou spojení navíc odložena.

Průměrný počet přijatých požadavků

Průměrný počet přijatých požadavků udává limit pro počet nových navázaných spojení nebo přijatých požadavků URI, které se serveru povolují. Pokud požadavek způsobí, že server překročí nastavené limity, které jste nastavili, server žádost odmítne. Limit průměrného počtu požadavků na připojení se měří v počtu spojení za vteřinu.

Rada: Chcete-li zjistit, jak nastavit limity, můžete použít funkci Monitorování QoS. Příklad nastavení zásady QoS, prostřednictvím které budete moci provést monitorování pro většinu dat procházejících serverem najdete v tématu Monitorování aktuálního stavu sítě. Na základě výsledků monitorování pak můžete limity vhodně přizpůsobit.

Chcete-li si prohlédnout monitorovaná data v reálném čase namísto určité kolekce dat, pouze použijte funkci monitor. Funkce monitorování poskytuje v reálném čase statistiky všech aktivních zásad.

Rozhraní QoS API



Většina zásad QoS vyžaduje použití rozhraní API. Následující rozhraní API lze použít ve spojení se zásadami odlišovaných služeb nebo zásadami integrovaných služeb. Existuje také množství rozhraní API, které lze použít společně s funkcí monitorování QoS.

- Rozhraní API integrovaných služeb (Viz 16)
- Rozhraní API odlišovaných služeb (Viz 16)
- Rozhraní API pro monitorování (Viz 17)

Rozhraní API integrovaných služeb

Protokol RSVP (Resource Reservation Protocol) spolu s rozhraním RAPI API nebo qtoq QoS sockets API provádějí rezervaci šířky pásma pro integrované služby QoS. Každý síťový uzel, kterým přenos prochází, musí mít schopnost používat protokol RSVP. Schopnost realizovat zásady integrovaných služeb se také nazývá tak, že zařízení "podporuje RSVP". Další informace o směrovacích funkcích, nutných pro použití protokolu RSVP, najdete v tématu Funkce pro řízení provozu.

Pomocí protokolu RSVP se provádí rezervace RSVP ve všech síťových uzlech na trase vašeho přenosu. Protokol udržuje rezervaci dostatečně dlouho, aby poskytl vaši zásadě QoS požadovanou úroveň služeb. Rezervace definuje způsob zacházení s daty a šířku pásma, kterou data při této konverzaci obdrží. Každý ze síťových uzlů odsouhlasuje, že poskytne zacházení s daty definované v rezervaci.

RSVP je jednoduchý protokol v tom, že rezervace se provádí pouze v jednom směru (od příjemce). Při náročnějších spojeních, jako jsou např. audio nebo video konference, je každý odesílatel zároveň příjemcem. V tom případě musíte nastavit relace RSVP na obou stranách spojení.

Chcete-li používat integrované služby QoS, musíte mít kromě směrovačů podporujících RSVP speciální aplikace podporující RSVP. Vzhledem k tomu, že server iSeriesTM v současné době nemá žádné aplikace umožňující RSVP, budete si muset aplikace napsat za použití rozhraní RAPI API nebo rozhraní qtoq QoS Sockets API. To aplikacím umožní, aby používaly protokol RSVP. Jestliže máte zájem o podrobnější vysvětlení, je k dispozici mnoho zdrojů, které tyto modely, jejich fungování a zpracovávání zpráv popisují. Potřebujete k tomu důkladnou znalost protokolu RSVP a obsahu RFC (Request for Comments) 2205.

Rozhraní qtoq Sockets API

Nyní můžete pomocí rozhraní qtoq QoS sockets API zjednodušit úkony nezbytné k tomu, abyste mohli v systému iSeries používat protokol RSVP. Rozhraní qtoq sockets API vyvolají rozhraní RAPI API a provedou některé složitější úkoly. Rozhraní qtoq sockets API nejsou natolik flexibilní jako rozhraní RAPI API, ale poskytují stejné funkce s menším úsilím. Verze "No Signal" rozhraní API vám umožní, abyste vytvořili tyto aplikace:

- Aplikace, která zavede pravidlo RSVP na server.
- Aplikace, která vyžaduje, aby pouze strana serveru (při konverzaci TCP/IP) podporovala RSVP.

Signalizace RSVP se automaticky provádí ze strany klienta.

Typický příklad fungování rozhraní QoS API pro aplikaci/protokol používající qtoq QoS sokety spojově orientované nebo bezspojově najdete na stránkách Rozhraní QoS API ve spojově orientovaném prostředí a Rozhraní QoS API v bezspojovém prostředí.

Rozhraní API odlišovaných služeb

Poznámka: Rozhraní Sendmsg() API se používá pro určité typy zásad odlišovaných služeb definující specifický token aplikace. Pokud vytvoříte zásadu odlišovaných služeb QoS, můžete (volitelně) poskytnout charakteristiky aplikace

(token a prioritu). Toto je pokročilá definice zásady QoS a pokud není využita, lze toto rozhraní API ignorovat. Uvědomte si však, že směrovače a ostatní servery v síti přesto musí podporovat odlišované služby.

Pokud se rozhodnete pro použití tokenu aplikace v rámci zásady odlišovaných služeb QoS, musí být aplikace poskytující tyto informace specificky kódována pro použití rozhraní Sendmsg() API. To provádí vývojář aplikací. Dokumentace k aplikaci musí poskytovat platné hodnoty (token a prioritu), které použije administrátor produktu QoS v rámci zásady odlišovaných služeb. Poté zásada odlišovaných služeb aplikuje pro přenosy, které odpovídají tokenu nastavenému v rámci zásady QoS, svoji vlastní prioritu a klasifikaci. Pokud aplikace neobsahuje hodnoty, které odpovídají hodnotám nastaveným v rámci zásady QoS, musíte buď změnit aplikaci, nebo použít pro zásadu odlišovaných služeb jiné parametry dat aplikace.

Tyto informace stručně popisují parametry dat serveru: token aplikace a priorita aplikace.

Co je token aplikace?

Token aplikace je URI, který představuje definovaný prostředek. Token, který zadáte v rámci zásady QoS, je porovnáván s tokenem poskytnutým aplikací odchozích přenosů. Aplikace poskytne hodnotu token prostřednictvím rozhraní sendmsg() API. Pokud si tokeny navzájem odpovídají, jsou přenosy aplikace zahrnuty do zásady odlišovaných služeb.

Co je priorita aplikace?

Priorita aplikace, kterou zadáte, je porovnávána s prioritou aplikace poskytnutou aplikací odchozích přenosů. Aplikace poskytne hodnotu priority prostřednictvím rozhraní sendmsg() API. Pokud si priority navzájem odpovídají, jsou přenosy aplikace zahrnuty do zásady odlišovaných služeb. Veškeré přenosy definované v rámci zásady odlišovaných služeb přesto budou mít prioritu, která byla přiřazena celkové zásadě.

Další informace o typu zásad QoS - odlišované služby (DiffServ) najdete v tématu Odlišované služby.

Rozhraní API pro monitorování

Chcete-li použít rozhraní API pro monitorování, najdete potřebné informace v tématu Resource Reservation Setup Protocol API. Rozhraní API, která mají souvislost s monitorováním, obsahují v názvu výraz "monitor". Například *QgyOpenListQoSMonitorData*. Následující seznam stručně popisuje každé rozhraní API pro monitorování:

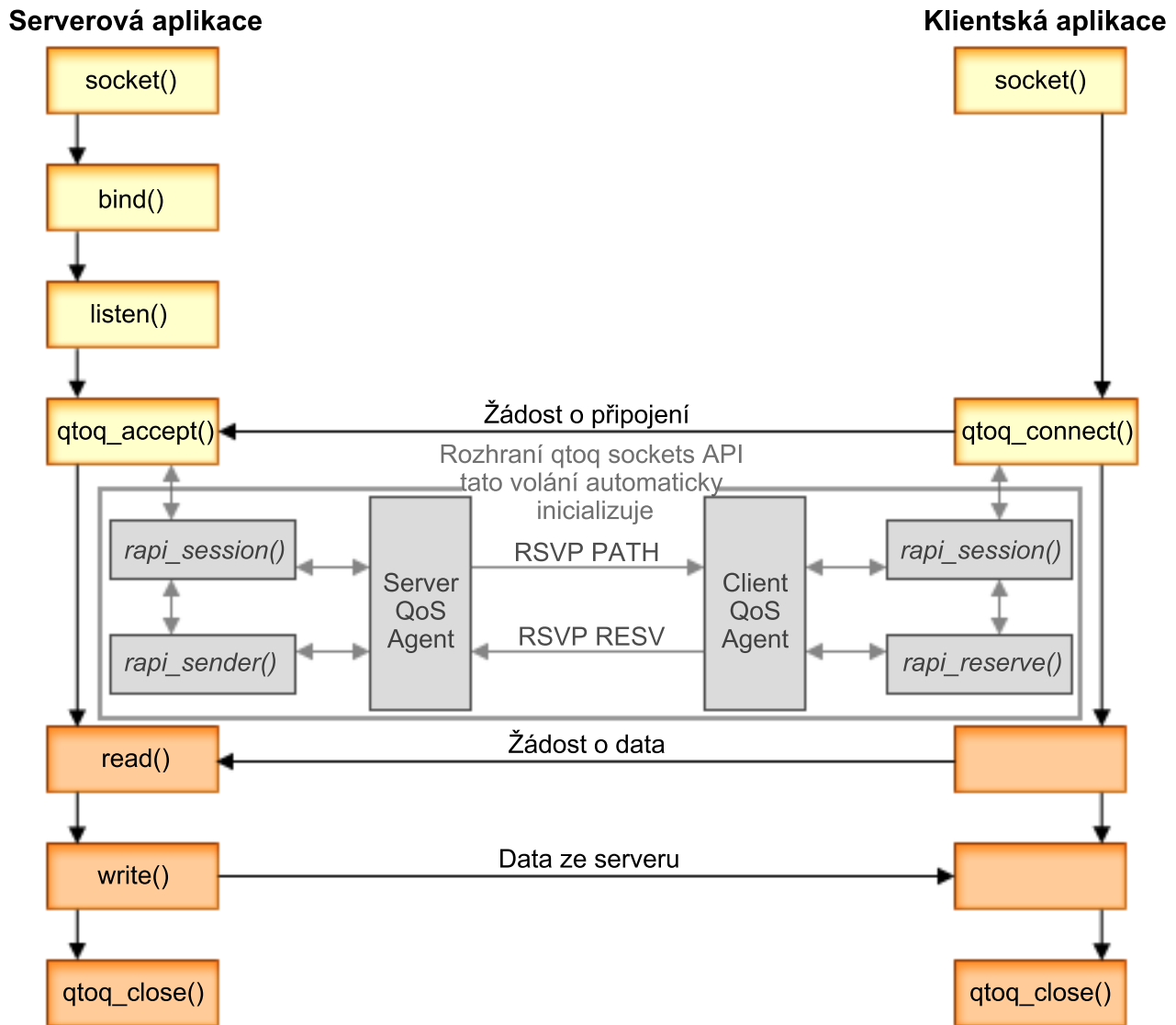
- *QgyOpenListQoSMonitorData* (Open List of QoS Monitor Data) shromažďuje informace související se službami produktu QoS.
- *QtoqDeleteQoSMonitorData* (Delete QoS Monitor Data) vymaže jednu nebo více sad dat monitorování shromážděných produktem QoS.
- *QtoqEndQoSMonitor* (End QoS Monitor) ukončí shromažďování informací v souvislosti se službami QoS.
- *QtoqListSavedQoSMonitorData* (List Saved QoS Monitor Data) vrátí seznam všech shromážděných dat monitorování, která již byla dříve uložena.
- *QtoqSaveQoSMonitorData* (Save QoS Monitor Data) uloží kopii shromážděných dat monitorování QoS pro pozdější použití.
- *QtoqStartQoSMonitor* (Start QoS Monitor) shromažďuje informace související se službami QoS.



Rozhraní QoS API ve spojově orientovaném přenosu

Na následujícím obrázku je zobrazen vztah klient/server pro funkce rozhraní qtoq sockets API, které podporuje QoS, pro protokol orientovaný na připojení, jako je protokol TCP (Transmission Control Protocol).

Když se vyvolají funkce pro rozhraní API podporující QoS pro tok orientovaný na spojení, který vyžaduje zahájení RSVP, spustí se další funkce. Tyto funkce způsobí, že QoS agenti na klientovi a na serveru nastaví protokol RSVP pro tok dat mezi klientem a serverem.



Postup událostí qtoq: Následující série volání socketů poskytuje vysvětlení ke schématu. Popisuje také vztah mezi serverovou a klientskou aplikací v prostředí orientovaném na spojení. Toto jsou modifikace základních rozhraní Sockets API.

Strana serveru

Funkce qtoq_accept() pro pravidlo označené "No Signaling"

1. Aplikace volá funkci socket() a získá deskriptor socketů.
2. Aplikace volá funkci listen() a specifikuje, na která spojení bude čekat.
3. Aplikace volá funkci qtoq_accept() a čeká na žádost o připojení od klienta.
4. Rozhraní API volá rozhraní rapi_session() API a pokud je volání úspěšné, přiřadí se ID relace QoS.
5. Rozhraní API volá standardní funkci accept() a čeká na žádost o připojení klienta.

6. Když přijde žádost o připojení, provede se proces řízení přístupu pro požadované pravidlo. Pravidlo je zasláno do zásobníku TCP/IP; pokud je platné, vrátí se aplikaci pro volání s výsledky a ID relace.
7. Aplikace pro server a pro klienta provedou požadované přenosy dat.
8. Aplikace vyvolá funkci `qtoq_close()`, aby uzavřela socket a uvolnila pravidlo.
9. Server QoS vymaže pravidlo ze správce QoS, vymaže relaci QoS a vykoná další potřebné úkony.

Funkce `qtoq_accept()` s normální signalizací RSVP

1. Aplikace volá funkci `socket()` a získá deskriptor socketů.
2. Aplikace volá funkci `listen()` a specifikuje, na která spojení bude čekat.
3. Aplikace volá funkci `qtoq_accept()` a čeká na žádost o připojení od klienta.
4. V okamžiku, kdy dorazí žádost o připojení, vyvolá se rozhraní `rapi_session()` API, aby se pro toto připojení navázala relace se serverem QoS a získalo se ID relace QoS.
5. Vyvolá se rozhraní `rapi_sender()` API, aby se inicializovala zpráva PATH ze serveru QoS a aby se server QoS informoval, že má očekávat od klienta zprávu RESV.
6. Vyvolá se rozhraní `rapi_getfd()` API, aby se získal deskriptor, který aplikace používá, když čeká na zprávy o událostech QoS.
7. Přijatý deskriptor a QoS deskriptor se vrací do aplikace.
8. Server QoS čeká na zprávu RESV, kterou má přijmout. Když je zpráva obdržena, zavede server pomocí správce QoS příslušné pravidlo a pošle zprávu aplikaci, jestliže aplikace vyžadovala oznámení o volání rozhraní `qtoq_accept()` API.
9. Server QoS stále obnovuje navázanou relaci.
10. Když je spojení ukončeno, klientský kód vyvolá funkci `qtoq_close()`.
11. Server QoS vymaže pravidlo ze správce QoS, vymaže relaci QoS a vykoná další potřebné úkony.

Strana klienta

Funkce `qtoq_connect()` s normální signalizací RSVP

1. Aplikace volá funkci `socket()` a získá deskriptor socketů.
2. Aplikace volá funkci `qtoq_connect()`, aby informovala serverovou aplikaci, že by chtěla navázat spojení.
3. Funkce `qtoq_connect()` vyvolá rozhraní `rapi_session()` API, aby pro toto spojení navázala relaci se serverem QoS.
4. Server QoS bude informován, že má čekat na příkaz PATH od požadovaného spojení.
5. Vyvolá se rozhraní `rapi_getfd()` API, aby se získal deskriptor QoS, který aplikace používá při čekání na zprávy QoS.
6. Vyvolá se funkce `connect()`. Výsledky funkce `connect()` a deskriptor QoS se vrací do aplikace.
7. Server QoS čeká na zprávu PATH, kterou má přijmout. Když zprávu obdrží, odpoví zprávou RESV pro QoS server na počítači aplikačního serveru.
8. Jestliže aplikace vyžadovala oznámení, pošle server QoS aplikaci oznámení přes deskriptor QoS.
9. Server QoS stále obnovuje navázanou relaci.
10. Když je spojení ukončeno, vyvolá aplikace funkci `qtoq_close()`.
11. Server QoS zavře relaci QoS a vykoná další potřebné úkony.

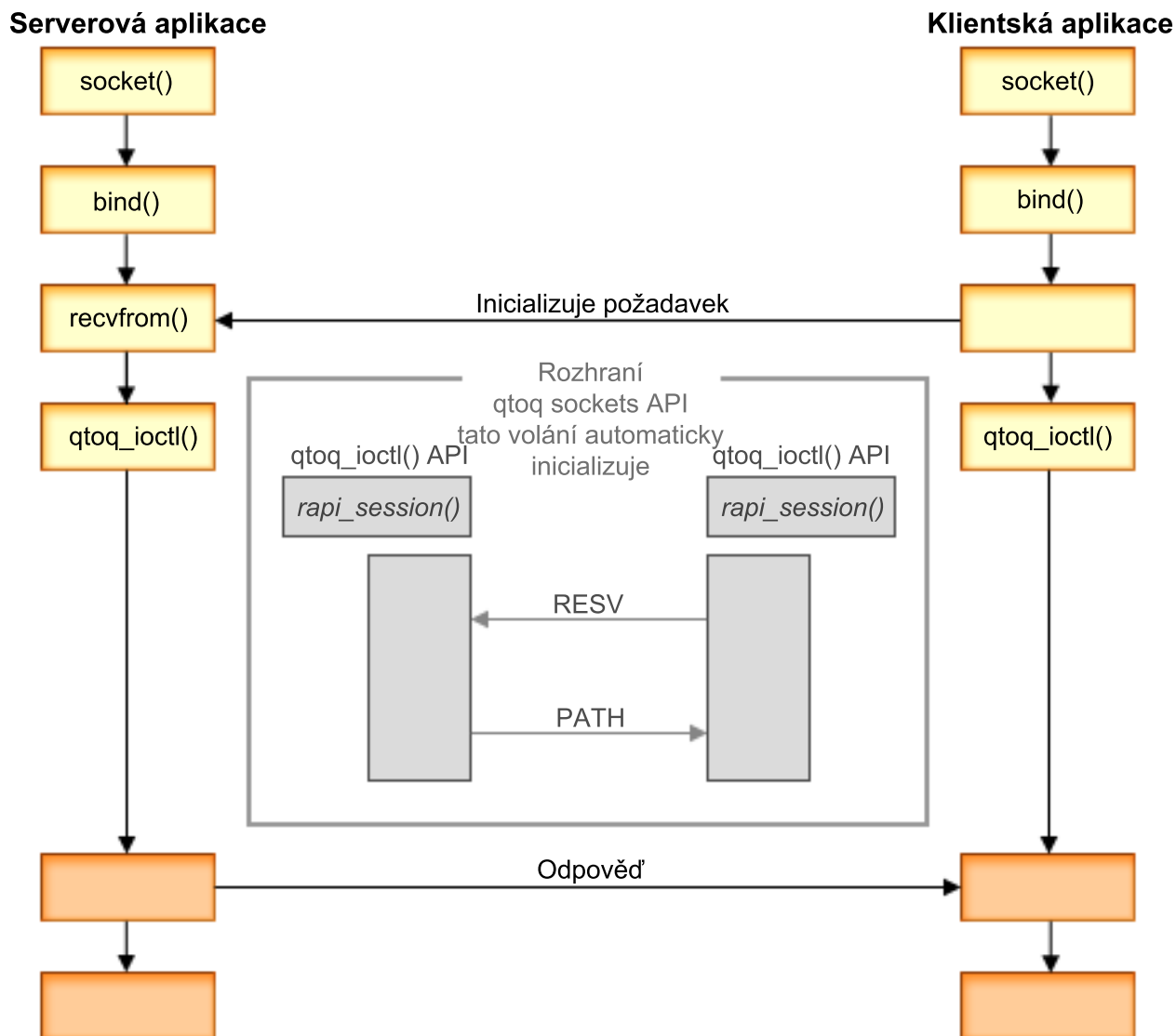
Funkce `qtoq_connect()` pro pravidlo označené "No Signaling"

Tato žádost není na straně klienta platná, protože v tomto případě se od klienta nevyžaduje žádná odezva.

Rozhraní QoS API v bezspojovém přenosu

Tyto příklady relací serveru a klienta ilustrují rozhraní `qtoq` QoS socket API napsaná pro bezspojové přenosy.

Když se vyvolají funkce pro rozhraní API podporující QoS pro bezspojový přenos, který vyžaduje zahájení RSVP, spustí se další funkce. Tyto funkce způsobí, že QoS agenti na klientovi a na serveru nastaví protokol RSVP pro tok dat mezi klientem a serverem.



Postup událostí qtoq: Následující série volání socketů poskytuje vysvětlení ke schématu. Popisuje také vztah mezi serverovou a klientskou aplikací v bezspojovém prostředí. Toto jsou modifikace základních rozhraní Sockets API.

Strana serveru

Funkce qtoq_ioctl() pro pravidlo označené "No Signaling"

1. Zasílá zprávu serveru QoS a žádá ho aby provedl řízení přístupu pro požadované pravidlo.
2. Jestliže je pravidlo přijatelné, vyvolá funkci, která zašle serveru QoS zprávu s požadavkem, aby pravidlo zavedl.
3. Vrací volajícímu stav, který indikuje, zda žádost byla úspěšná nebo neúspěšná.

4. Když aplikace dokončí využívání spojení, vyvolá funkci `qtoq_close()` a ukončí spojení.
5. Server QoS vymaže pravidlo ze správce QoS, vymaže relaci QoS a vykoná další potřebné úkony.

Funkce `qtoq_ioctl()` s normální signalizací RSVP

1. Zasílá správu na server QoS s požadavkem na řízení přístupu pro požadované spojení.
2. Vyvolá funkci `rapi_session()` a požádá o vytvoření relace pro pravidlo a přidělení ID relace QoS, které se vrátí volajícímu.
3. Vyvolá funkci `rapi_sender()`, aby se inicializovala zpráva PATH zpátky klientovi.
4. Vyvolá funkci `rapi_getfd()`, aby se získal deskriptor souborů, který se použije při čekání na události QoS.
5. Vrací descriptor `select()`, ID relace QoS a stav volajícímu.
6. Když server QoS obdrží zprávu RESV, zavede pravidlo.
7. Když je spojení ukončeno, vyvolá aplikace funkci `qtoq_close()`.
8. Server QoS vymaže pravidlo ze správce QoS, vymaže relaci QoS a vykoná další potřebné úkony.

Strana klienta

Funkce `qtoq_ioctl()` s normální signalizací RSVP

1. Vyvolá funkci `rapi_session()` a požádá o vytvoření relace pro spojení. Funkce `rapi_session()` žádá o kontrolu přístupu pro spojení. Spojení bude na straně klienta odmítnuto pouze tehdy, pokud je pro klienta konfigurované pravidlo a není v dané době aktivní. Tato funkce vrátí ID relace QoS, které přechází zpátky do aplikace.
2. Vyvolá funkci `rapi_getfd()`, aby se získal deskriptor souborů, který se použije při čekání na události QoS.
3. Funkce `qtoq_ioctl()` vrací volajícímu zpátky deskriptor a ID relace.
4. Server QoS čeká na zprávu PATH, kterou má přijmout. Když zprávu PATH obdrží, odpoví zprávou RESV a signalizuje aplikaci prostřednictvím deskriptoru, že došlo k události QoS.
5. Server QoS stále obnovuje navázanou relaci.
6. Když je spojení ukončeno, klientský kód vyvolá funkci `qtoq_close()`.

Funkce `qtoq_ioctl()` pro pravidlo označené "No Signaling"

Tato žádost není na straně klienta platná, protože v tomto případě se od klienta nevyžaduje žádná odezva.

Rozšíření rozhraní QoS `Sendmsg()` API



Funkce `sendmsg()` se používá pro přenos dat, doplňkových dat nebo kombinaci obojího přes připojený nebo nepřipojený soket. Ve verzi V5R3 byla funkce `sendmsg()` vylepšena a nyní umožňuje klasifikaci dat QoS. Zásady QoS používají tuto funkci k definování jemnější úrovně klasifikace odchozích nebo příchozích přenosů TCP/IP. Využívají doplňkové typy dat vztahující se k vrstvě IP. Použitý typ zprávy je `IP_QOS_CLASSIFICATION_DATA`. Tato doplňková data mohou být aplikací použita k definování atributů pro přenosy v rámci určitého připojení TCP. Pokud atributy předávané aplikací odpovídají atributům definovaným v rámci zásady QoS, zásada omezí přenosy TCP. Chcete-li použít rozhraní `sendmsg()` API, přečtěte si téma `Sendmsg() - Send a message over a socket` v informacích o programování rozhraní API. Chcete-li inicializovat strukturu `IP_QOS_CLASSIFICATION_DATA`, použijte informace uvedené níže.

Strukturu `ip_qos_classification_data` je třeba vyplnit tímto způsobem:

- `ip_qos_version`: Označuje verzi struktury. Zde při vyplňování musíte použít konstantu `IP_QOS_CURRENT_VERSION`.
- `ip_qos_classification_scope`: Zadejte rozsah úrovně připojení (použijte konstantu `IP_QOS_CONNECTION_LEVEL`) nebo rozsah úrovně zpráv (konstanta `IP_QOS_MESSAGE_LEVEL`).

Rozsah úrovně připojení indikuje, že úroveň služeb produktu QoS získaná z klasifikace této zprávy, zůstává v platnosti pro všechny následující poslané zprávy až do dalšího použití funkce `sendmsg()` s klasifikačními daty

produktu QoS. Rozsah úrovně zpráv indikuje, že úroveň služby QoS bude použita pouze pro data zpráv zahrnutá ve volání této funkce sendmsg(). Následující data poslaná bez dat klasifikace produktu QoS převezmou předchozí přiřazení úrovně připojení produktu QoS (z předchozí klasifikace úrovně připojení funkce sendmsg() nebo z původní klasifikace připojení TCP během vytváření připojení).

- **ip_qos_classification_type**: Tato specifikace označuje typ předávaných klasifikačních dat. Aplikace může předávat aplikaci definovaný token, aplikaci specifikovanou prioritu nebo token i prioritu. Pokud je vybrána poslední volba, logicky musí být mezi vybranými druhy klasifikace nastaven vztah OR (nebo). Lze zadat tyto typy:
 - Klasifikace dle aplikací definovaného tokenu. Musí být zadán jeden typ. Pokud je zadáno více typů, nelze předpovědět následky.
 - **IP_SET_QOSLEVEL_W_APPL_TOKEN_ASCII** : Indikuje, že klasifikační data jsou řetězcem znaků ve formátu ASCII. Pokud je nastavena tato volba musí být token aplikace předáván v poli `ip_qos_appl_token`.
Poznámka: Pokud aplikace potřebuje předávat pro klasifikovaná data numerické hodnoty, musí je nejprve konvertovat do tisknutelného formátu ASCII. Také si uvědomte, že zadaný řetězec může obsahovat malá i velká písmena a že bude použitý přesně ve formátu stanoveném pro účely porovnání.
 - **IP_SET_QOSLEVEL_W_APPL_TOKEN_EBCDIC** : Stejně jako v předchozím případě, s tím rozdílem, že formát je EBCDIC.
Poznámka: Typ **IP_SET_QOSLEVEL_W_APPL_TOKEN_ASCII** poskytuje o něco lepší výkon než tato volba, protože data aplikace ve formátu ASCII zadaná v rámci zásady jsou v zásobníku TCP/IP. Není tedy nutné překládat aplikací definovaný token při každém požadavku sendmsg().
 - Třídění dle aplikací definované priority. Musí být zadán jeden typ. Pokud je zadáno více typů priorit, nelze předpovědět následky.
 - **IP_SET_QOSLEVEL_EXPEDITED**: Indikuje, že je požadována urychlená priorita (Expedited priority).
 - **IP_SET_QOSLEVEL_HIGH**: Indikuje, že je požadována vysoká priorita.
 - **IP_SET_QOSLEVEL_MEDIUM**: Indikuje, že je požadována střední priorita.
 - **IP_SET_QOSLEVEL_LOW**: Indikuje, že je požadována nízká priorita.
 - **IP_SET_QOSLEVEL_BEST_EFFORT**: Indikuje, že je požadována priorita nejvyššího výkonu (Best effort).
 - **ip_qos_appl_token_len**: Délka zadané položky `ip_qos_appl_token`.
 - **ip_qos_appl_token**: Toto "virtuální pole" bezprostředně následuje pole `ip_qos_classification_type`. Token řetězec třídění aplikace ve formátu ASCII nebo EBCDIC podle toho jaký druh klasifikace byl zadán v položce **IP_SET_QOSLEVEL_W_APPL_TOKEN_xxxx**. Na toto pole je odkazováno pouze v případě, že je zadán typ aplikací definovaného tokenu. Všimněte si, že tento řetězec nesmí přesahovat 128 bytů. Pokud je zadána větší velikost, bude použito pouze prvních 128 bytů. Také si uvědomte, že délka tohoto řetězce je určena dle hodnoty zadané pro parametr `cmsg_len` (`cmsg_len - sizeof(cmsg_hdr) - sizeof(ip_qos_classification_data)`). Takto vypočtená délka nesmí obsahovat žádné ukončovací nuly.



Server adresářů

Konfiguraci zásad QoS lze exportovat na server adresářů prostřednictvím nejnovějšího protokolu LDAP verze 3.

Výhody použití serveru adresářů

Prostřednictvím exportování zásad QoS na server adresářů budete moci vaše zásady snadněji spravovat. Existují tři způsoby, jak lze server adresářů použít.

- Data konfigurace lze uložit na lokální server adresářů, kde jej mohou sdílet ostatní servery.
- Data konfigurace mohou být konfigurována, uložena a používána pouze jedním systémem (nejsou sdílena).
- Data konfigurace také mohou být na serveru adresářů, který obsahuje data pro další systémy; nemusí však být sdílena mezi těmito dalšími systémy. To vám umožní použít jedno umístění pro zálohování a ukládání dat různých systémů.

Výhody ukládání výhradně na lokální server

Ukládání zásad QoS na lokální server není tak složité. Existuje množství výhod používání zásad lokálně:

- Vyloučíte složitost konfigurace LDAP v případě uživatelů, kteří toto nepotřebují.
- Zlepšíte výkon, protože zapisování LDAP není nejrychlejší metodou zápisu.
- Zjednodušíte vytváření kopií konfigurace mezi různými systémy iSeries^(TM). Soubor můžete kopírovat z jednoho systému do druhého. Protože zde není žádný primární ani sekundární systém, můžete každou zásadu přizpůsobit přímo jednotlivým serverům.

Prostředky LDAP

Pokud se rozhodnete vaše zásady exportovat na server LDAP, musíte být obeznámeni s koncepty LDAP a strukturami adresářů. Prostudujte si téma Server adresářů IBM v systémech iSeries (LDAP) v rámci aplikace iSeries Information Center. Informace týkající se konfigurování serveru adresářů v rámci funkce QoS v produktu iSeries Navigator najdete v tématu Konfigurování serveru adresářů.

Další informační zdroje o LDAP najdete na stránce Související informace o QoS.

Klíčová slova

Když konfiguruje server adresářů, musíte určit, zda budete přiřazovat jednotlivým konfiguracím QoS klíčová slova. Pole klíčových slov jsou volitelná a můžete je ignorovat. V následující části je vysvětlen princip klíčových slov a proč byste je mohli používat.

V průvodci počáteční konfigurací QoS můžete konfigurovat server adresářů. Můžete zadat, zda server, který konfiguruje, bude primárním nebo sekundárním systémem. Server, na kterém uchovávejte všechny zásady QoS, se nazývá primární systém.

Pomocí klíčových slov se identifikují konfigurace vytvořené primárními systémy. Ačkoliv jsou klíčová slova vytvořena v primárním systému, vlastní přínos mají pro sekundární systémy. Umožňují sekundárním systémům, aby si zavedly a používaly konfigurace vytvořené primárním systémem. V níže uvedených popisech je vysvětleno, jak se klíčová slova na jednotlivých systémech používají.

Klíčová slova a primární systémy

Klíčová slova se přiřazují ke konfiguracím QoS vytvořeným a udržovaným primárním systémem. Používají se proto, aby sekundární systémy mohly identifikovat konfiguraci vytvořenou primárním systémem.

Klíčová slova a sekundární systémy

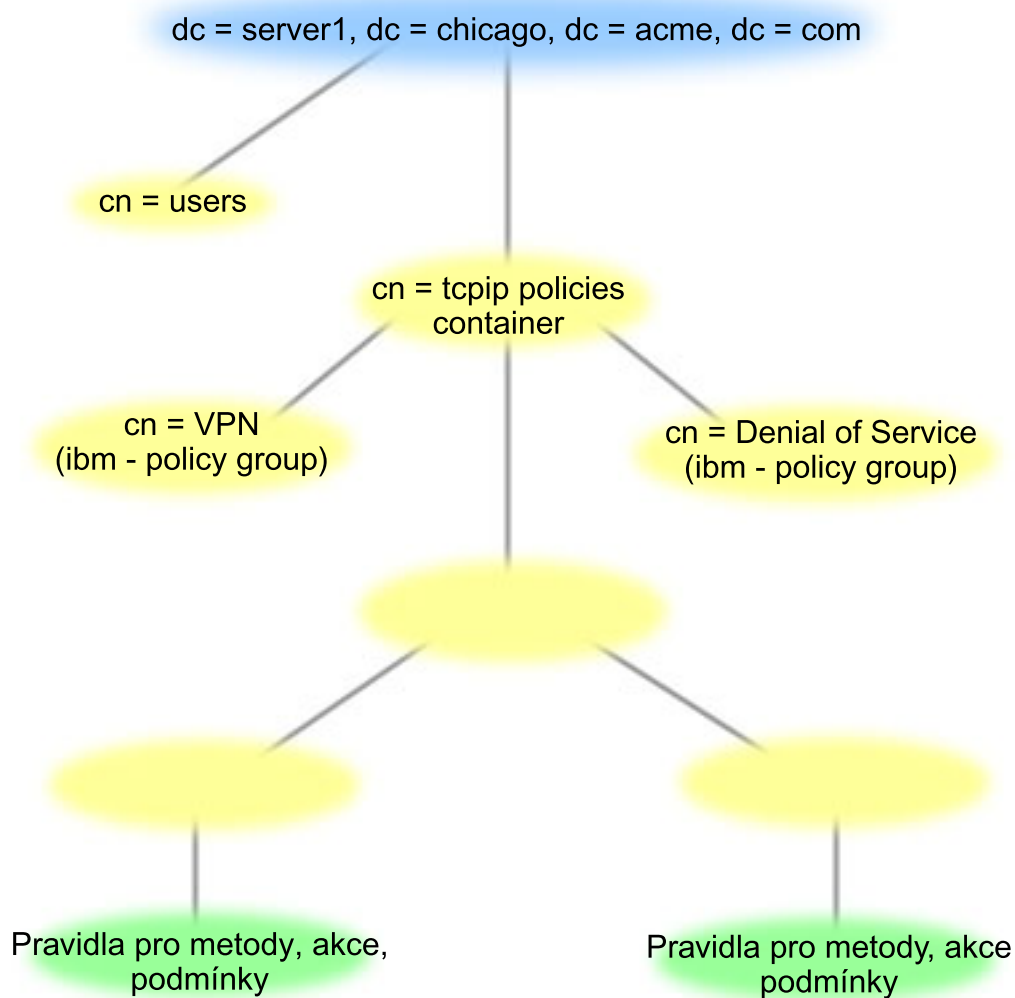
Sekundární systémy používají klíčová slova k vyhledávání konfigurací. Sekundární systémy si nahrávají a používají konfigurace vytvořené primárním systémem. Když konfiguruje sekundární systém, můžete vybrat konkrétní klíčová slova. Podle toho, jaké klíčové slovo vyberete, nahraje pak sekundární systém všechny konfigurace přiřazené k vybranému klíčovému slovu. Sekundární systém si tak může nahrát více konfigurací vytvořených více primárními systémy.

Když začnete konfigurovat server adresářů v prostředí produktu iSeries^(TM) Navigator, vyhledávejte si v nápovědě pro QoS konkrétní pokyny.

Rozlišovací jméno

Když chcete pracovat s určitou částí vašeho adresáře, používáte **rozlišovací jméno (DN)** anebo můžete (pokud chcete), použít klíčové slovo. Rozlišovací jméno zadáváte, když konfiguruje server adresářů v rámci průvodce počáteční konfigurací produktu QoS. Rozlišovací jména se obvykle skládají ze jména pro záznam samotný, ale také z objektů (shora dolů) nad daným záznamem v adresáři. Server může přistupovat ke všem objektům v adresáři, které jsou pod daným rozlišovacím jménem. Řekněme, například, že by server LDAP obsahoval strukturu adresářů znázorněnou níže.

Obrázek 12. Ukázka struktury adresářů QoS



Server1 nahoře (dc=server1,dc=chicago,dc=acme,dc=com) je server, na kterém je server adresářů. Ostatní servery, jako např. cn=QoS nebo cn=tcpip policie, jsou servery, kde jsou servery QoS. Takže na serveru cn=server1 bude předvolené DN (rozlišovací jméno) cn=server1,cn=QoS,cn=tcpip policie,dc=server1,dc=chicago,dc=acme,dc=com. A na serveru cn=server2 bude předvolené DN (rozlišovací jméno) cn=server2,cn=QoS,cn=tcpip policie,dc=server1,dc=chicago,dc=acme,dc=com.

Při správě adresáře je důležité změnit správný server v DN, jako např. cn nebo dc. Při úpravách DN buďte velmi pozorní, protože řetězec je obvykle hodně dlouhý a při jeho zobrazení musíte použít posouvání.

Další informační zdroje o LDAP najdete na stránce [Související informace o QoS](#).

Scénáře QoS

Nejlépe princip QoS (Quality of service) pochopíte, když se seznámíte s konkrétními příklady použití této funkce v celkovém prostředí sítě. Z následujících scénářů vyplývá, proč byste mohli potřebovat použít zásady QoS. Také jsou zde uvedeny některé kroky s pokyny, jak vytvořit zásady QoS a provozní třídy.

Scénář: Omezení přenosu prohlížeče

Pomocí QoS lze řídit výkon síťového provozu. Prostřednictvím zásady odlišovaných služeb QoS můžete buď omezit nebo rozšířit výkon určité aplikace v síti.

Scénář: Zabezpečené a předvídatelné výsledky (VPN a QoS)

Používáte-li VPN (virtual private network), můžete také tvořit zásady QoS. V tomto scénáři je popsáno současné použití obou funkcí.

Scénář: Omezení příchozích připojení

Potřebujete-li řídit požadavky na příchozí připojení přicházející na váš server, použijete zásadu příchozích připojení.

Scénář: předvídatelný provoz B2B

Potřebujete-li zajistit předvídatelný přenos a současně i rezervaci, rovněž použijete zásadu integrovaných služeb QoS. V tomto scénáři však použijeme služby řízeného zavádění.

Scénář: Vyhrazený přenos (IP telefonie)

Jestliže potřebujete vyhrazený přenos a chcete si vyžádat rezervaci šířky pásma, použijete zásadu integrovaných služeb QoS. Existují dva typy zásad integrovaných služeb QoS, které můžete vytvořit: služby řízeného zavádění a garantované služby. V tomto scénáři je použita zásada garantovaných služeb.



Scénář: Monitorování aktuálních síťových statistik QoS

V rámci práce s průvodci QoS nastavujete určité limity výkonu. Jsou to parametry, jejichž hodnoty nelze doporučit, neboť jsou založeny na požadavcích konkrétní sítě. Při nastavování těchto limitů musíte velmi dobře znát aktuální výkon sítě. Vzhledem k tomu, že hodláte konfigurovat zásady QoS, pravděpodobně již máte určitou představu o vašich současných síťových potřebách. Chcete-li určit přesné limity výkonu, jako je např. přenosová rychlost sektoru token, bude užitečné provést monitorování pro veškerý provoz na serveru, abyste mohli lépe určit, jaké limity nastavit.



Poznámka: Uvedené IP adresy a diagramy jsou fiktivní a slouží pouze jako příklady.

Scénář QoS: Omezení přenosu prohlížečů

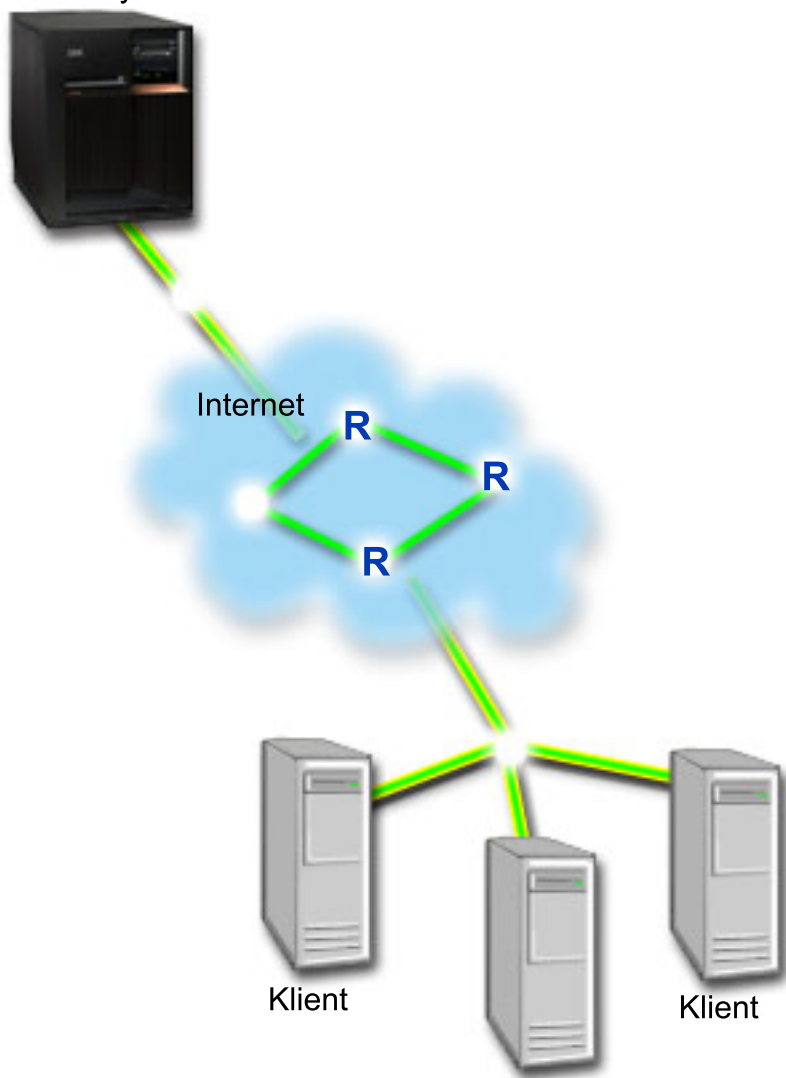
Situace



Ve vašem podniku zaznamenáváte v pátky vysokou úroveň přenosů prohlížečů ze skupiny UCD (user-centered design). Tento provoz koliduje s provozem účetního oddělení, které také v pátky vyžaduje zvýšený výkon u svých účetních aplikací. Rozhodnete se omezit přenos prohlížečů ze skupiny UCD (user-centered design). Na následujícím obrázku je znázorněno nastavení sítě podle tohoto scénáře. Na serveru iSeries^(TM) je provozován operační systém OS/400^(R) verze V5R3.

Obrázek 1. Webový server omezující přenos prohlížeče pro určitého klienta.

Webový server



Podsít' 10.10.10.0

Cíl

Chcete-li omezit přenosy prohlížečů v rámci vaší sítě, můžete použít zásadu odlišovaných služeb QoS. Pomocí zásady odlišovaných služeb QoS rozdělíte provoz na síti do určitých provozních tříd. Veškerým přenosům v rámci této zásady QoS je přidělen určitý identifikační bod. Tento identifikační bod udává směrovačům, jak mají ke kterému druhu přenosu přistupovat. V tomto scénáři bude mít zásada QoS přiřazený identifikační bod nízké hodnoty, a tím ovlivníme, že bude síť přenosům prohlížečů přidělovat nízkou prioritu.

Předpoklady a nezbytné podmínky

- S vaším ISP máte uzavřenou smlouvu SLA (service level agreement), čímž zajišťujete, že vaše zásady QoS obdrží požadovanou prioritu. Zásada QoS, kterou vytvoříte na serveru iSeries, umožňuje, aby přenosy (v rámci této zásady QoS) obdržely v síti příslušnou prioritu. Negarantuje ji však; to je závislé na vaší smlouvě SLA. Využití zásad QoS vám v podstatě může poskytnout určitou výhodu při vyjednávání některých úrovní služeb i poplatků. Použijte odkaz smlouvy SLA, chcete-li se dozvědět více.

- Zásady odlišovaných služeb vyžadují na celé síťové trase směrovače, které podporují odlišované služby (DiffServ). Většina směrovačů podporuje odlišované služby. Chcete-li se však dozvědět více, najdete další informace v části Odlišované služby.

Konfigurace

Poté, co ověříte a provedete všechny nezbytné předchozí kroky, jste připraveni vytvořit zásadu odlišovaných služeb QoS.

1. Vytvořte zásadu odlišovaných služeb QoS (Viz 27)
2. Spusťte nebo aktualizujte server QoS. (Viz 28)
3. Prostřednictvím funkce Monitorování QoS ověříte, zda vytvořená zásada QoS funguje. (Viz 28)
4. Změňte její vlastnosti (je-li to třeba). (Viz 28)

Krok 1: Vytvořte zásadu odlišovaných služeb QoS

1. V prostředí produktu iSeries Navigator rozbalte Server iSeries A →**Síť** →**Zásady pro práci s IP**.
2. Klepněte pravým tlačítkem myši na **Quality of Service**, vyberte volbu **Konfigurace** a otevře se rozhraní produktu QoS.
3. V rozhraní produktu QoS klepněte pravým tlačítkem myši na typ zásady odlišovaných služeb QoS a vyberte volbu **Nová zásada**, čímž spustíte se průvodce.
4. Přečtěte si uvítací stránku, klepněte na **Další** a přejděte na stránku **Jméno**.
5. Do pole **Jméno** zadejte UCD. Volitelně také můžete zadat popis, který vám pomůže upamatovat se na účel této zásady QoS. Klepněte na **Další**.
6. Na stránce Klienti vyberte volbu **Určitá adresa nebo adresy** a klepněte na volbu **Nová**, chcete-li definovat vašeho klienta.
7. V dialogovém okně Nový klient zadejte tyto informace a klepněte na **OK**:
 - **Jméno:** UCD_Client
 - **IP adresa a maska:** 10.10.10.0 / 24

Poté, co klepnete na OK, se vrátíte do průvodce zásadou. Pokud jste již dříve vytvořili klienty, zrušte u nich označení a zkontrolujte, že jsou označeni pouze příslušní klienti.
8. Na stránce Požadavek na data serveru ověříte, že jsou vybrány volby **Libovolný token** a **Všechny priority**. Pak klepněte na **Další**.
9. Na stránce Aplikace vyberte volbu **Specifický port, rozsah portů nebo typ serveru** a klepněte na **Nový**.
10. V dialogovém okně Nová aplikace zadejte tyto informace a klepněte na **OK**, čímž se vrátíte do průvodce:
 - **Jméno:** HTTP
 - **Port:** 80
11. Na stránce Aplikace vyberte volbu **Protokol** a ověříte, že je vybrána volba **TCP**. Klepněte na **Další**.
12. Na stránce IP adresa lokálního systému ověříte, že je vybrána volba **Všechny IP adresy** a klepněte na **Další**.
13. Na stránce Provozní třída DiffServ klepněte na **Nová**, chcete-li definovat charakteristiky výkonu. Objeví se průvodce novou provozní třídou.
14. Přečtěte si uvítací stránku a klepněte na **Další**.
15. Na stránce Jméno zadejte UCD_service. Volitelně lze zadat popis, který vám pomůže upamatovat se na účel této zásady. Klepněte na **Další**.
16. Na stránce Typ služby vyberte **Pouze odchozí** a klepněte na **Další**. Tato provozní třída bude používána pouze pro zásady odchozích připojení.
17. Na stránce Označení kódového bodu DiffServ page vyberte volbu **Třída 4** a klepněte na **Další**. Chování při jednotlivých přechodech určuje, jaký výkon přenosy od směrovačů a ostatních serverů v síti obdrží. Potřebujete-li pomoc s vaším rozhodnutím, použijte nápovědu týkající se tohoto rozhraní.
18. Na stránce Omezení rychlosti odchozích připojení ověříte, že je zadáno **Ano** a klepněte na **Další**.
19. Na stránce Limity počtu odchozích připojení zadejte tyto informace a klepněte na **Další**:

- **Velikost sektoru token:** 100 Kilobitů
 - **Limit průměrné přenosové rychlosti:** 512 Kilobitů za vteřinu
 - **Limit maximální přenosové rychlosti:** 1 Megabitů za vteřinu
20. Na stránce Odchozí provoz mimo profil vyberte volbu **Uvolnění paketů UDP nebo snížení zahlcení TCP** a klepněte na **Další**.
 21. Prohlédněte si stránku se souhrnnými informacemi o provozní třídě. Pokud jsou správné, klepněte na **Dokončit**, čímž vytvoříte provozní třídu. Po klepnutí na "Dokončit" se vrátíte do průvodce zásadou a bude zvolena vaše provozní třída. Klepněte na "Další".
 22. Na stránce Plánovat vyberte volbu "Aktivní během zvoleného plánu" a pak klepněte na Nový.
 23. V dialogovém okně Přidat nový plán zadejte tyto informace a klepněte na **OK**:
 - **Jméno:** UCD_schedule
 - **Čas dne:** Aktivní 24 hodin
 - **Den v týdnu:** Pátek
 24. Klepněte na volbu "Další" a prohlédněte si přehled příslušné zásady. Pokud jsou správné, klepněte na **Dokončit**. V okně Konfigurace serveru QoS si můžete novou zásadu QoS prohlédnout v seznamu v pravém podokně.

V tomto okamžiku jste dokončili konfiguraci zásady odlišovaných služeb QoS v systému iSeries A. Dalším krokem je spustit nebo aktualizovat server.

Krok 2: Spusťte nebo aktualizujte server QoS.

V okně Konfigurace serveru QoS vyberte **Server**→**Spustit** nebo **Server**→**Aktualizovat**.

Krok 3: Pomocí funkce Monitorování QoS ověřte, zda vytvořená zásada QoS funguje.

Chcete-li ověřit, zda zásada QoS funguje tak, jak jste ji nakonfigurovali, použijte funkci Monitorování QoS.

1. V okně Konfigurace serveru QoS vyberte **Server**→**Monitor**. Otevře se okno "Monitorování "QoS".
2. Vyberte složku s typem zásady odlišovaných služeb (DiffServ). Zobrazí se všechny zásady odlišovaných služeb. Vyberte ze seznamu **UCD**.

Nejzajímavější pole jsou ta, která obsahují údaje o vašich přenosech. Zkontrolujte zejména pole Total bits (celkový počet bitů), Bits in-profile (počet vyhovujících bitů) a Packets in profile (počet vyhovujících paketů). Pole Bits out-of-profile označuje část přenosů, která přesahuje nakonfigurované hodnoty dané zásady QoS. U zásady odlišovaných služeb QoS udává počet bitů mimo profil (v případě paketů UDP) počet bitů, které byly uvolněny. V případě TCP, udává počet bitů mimo profil počet bitů přesahující přenosovou rychlost sektoru token, které jsou do sítě poslány. V případě TCP bity nejsou nikdy uvolněny. Počet vyhovujících paketů udává počet paketů kontrolovaných danou zásadou QoS (od okamžiku, kdy byl paket spuštěn, do okamžiku současného výstupu monitorování).

Také hodnota, kterou přiřadíte poli Average rate limit (limitu průměrné přenosové rychlosti) je důležitá. Když počet paketů tuto hranici překročí, server je začne uvolňovat. V důsledku toho se zvýší počet nevyhovujících bitů (Bits out of profile). To dokládá, že zásada QoS funguje v souladu s tím, jak jste ji nakonfigurovali. Soupis všech polí ve výstupu monitorování najdete v tématu monitor.

Poznámka: Pamatujte si, že výsledky budou přesné pouze v případě, že je zásada QoS aktivní. Ověřte plán, který jste zadali v rámci zásady QoS.

Krok 4: Změňte vlastnosti (je-li to třeba).

Poté, co si prohlédnete výsledky monitorování, můžete změnit vlastnosti libovolné zásady QoS či provozní třídy a dosáhnout tak očekávaných výsledků.

Kteroukoliv hodnotu, kterou jste zadali při vytváření zásady QoS, můžete změnit.

1. V okně Konfigurace serveru QoS vyberte složku **DiffServ**. Chcete-li upravit zásadu QoS, klepněte pravým tlačítkem na volbu **UCD** v seznamu v pravém podokně a vyberte **Vlastnosti**.
2. Objeví se dialogové okno Vlastnosti s hodnotami, které řídí obecnou zásadu. Změňte příslušné hodnoty.
3. Chcete-li upravit provozní třídu, vyberte složku **Provozní třída**. Chcete-li upravit provozní třídu, klepněte pravým tlačítkem myši na **UCD_service** v seznamu v pravém podokně a vyberte volbu **Vlastnosti**.
4. Objeví se dialogové okno Vlastnosti CoS s hodnotami, které řídí přenosy sítě. Změňte příslušné hodnoty.
5. Poté, co aktualizujete zásadu nebo provozní třídu, musíte server aktualizovat, aby byly změny potvrzeny. V okně Konfigurace serveru QoS vyberte **Server**—>**Aktualizovat**.



Scénář QoS: Zabezpečené a předvídatelné výsledky (VPN a QoS)

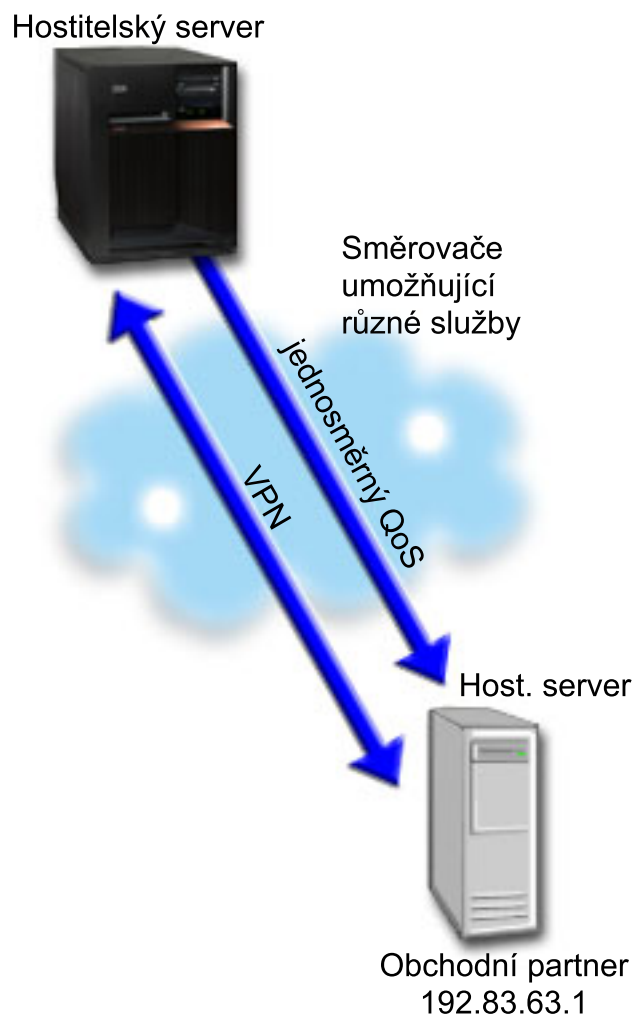
Situace



Jeden z vašich obchodních partnerů je připojen prostřednictvím VPN a vy chcete zkombinovat VPN a QoS tak, abyste zajistili bezpečný a předvídatelný přenos elektronického podnikání pro životně důležitá data. Konfigurace QoS se však promítá pouze jedním směrem. Takže pokud by se jednalo o nějakou audio/video aplikaci, museli byste nastavit QoS pro aplikaci na obou stranách spojení.

Obrázek znázorňuje spojení v síti VPN typu host-to-host mezi vaším serverem a počítačem vašeho obchodního partnera. Jednotlivá R označují směrovače na trase přenosu, které podporují odlišované služby QoS. Jak je z obrázku patrné, zásady QoS se uplatňují pouze v jednom směru.

Obrázek 3. Spojení VPN typu host-to-host využívající zásadu odlišovaných služeb QoS.



Cíl

Pomocí VPN a QoS nemusíte nastavovat pouze ochranu, ale také prioritu pro toto spojení. Nejprve nastavte spojení VPN typu host-to-host. Při konfiguraci VPN vám může pomoci příklad uvedený v tématu Host-to-Host VPN connection. Jakmile máte vytvořenou ochranu spojení VPN, můžete nastavit zásadu QoS. Můžete vytvořit zásadu odlišovaných služeb. Této zásadě QoS lze přiřadit vysokou hodnotu identifikačního bodu (EF, Expedited forwarding), abyste ovlivnili prioritu životně důležitého přenosu.

Předpoklady a nezbytné podmínky

- S vaším ISP máte uzavřenou smlouvu SLA (service level agreement), čímž zajišťujete, že vaše zásady QoS obdrží požadovanou prioritu. Zásada QoS, kterou vytvoříte na serveru iSeries^(TM), umožňuje, aby přenosy (v rámci této zásady QoS) obdržely v síti příslušnou prioritu. Negarantuje ji však; to je závislé na vaší smlouvě SLA. Využití zásad QoS vám v podstatě může poskytnout určitou výhodu při vyjednávání některých úrovní služby i poplatků. Použijte odkaz smlouvy SLA, chcete-li se dozvědět více.
- Zásady odlišovaných služeb vyžadují na celé síťové trase směrovače, které podporují odlišované služby (DiffServ). Většina směrovačů podporuje odlišované služby. Chcete-li se však dozvědět více, najdete další informace v části Odlišované služby.

Konfigurace

Poté, co ověříte a provedete všechny nezbytné předchozí kroky, jste připraveni vytvořit zásadu odlišovaných služeb QoS.

1. Nastavte spojení VPN typu host-to-host. (Viz 31)
2. Vytvořte zásadu odlišovaných služeb QoS (Viz 31)
3. Spusíte nebo aktualizujete server QoS. (Viz 32)
4. Prostřednictvím funkce Monitorování QoS ověřte, zda vytvořená zásada QoS funguje. (Viz 32)
5. Změňte její vlastnosti (je-li to třeba). (Viz 32)

Krok 1: Nastavte spojení VPN typu host-to-host

Při konfiguraci VPN vám může pomoci příklad uvedený v tématu Host-to-Host VPN connection.

Krok 2: Vytvořte zásadu odlišovaných služeb QoS

1. V prostředí produktu iSeries Navigator rozbalte Server iSeries A →**Síť**→**Zásady pro práci s IP**.
 2. Klepněte pravým tlačítkem myši na **Quality of Service**, vyberte volbu **Configuration** a otevře se okno s konfigurací serveru QoS.
 3. V okně Konfigurace serveru QoS klepněte pravým tlačítkem myši na volbu "DiffServ", vyberte **Nová zásada** a spustí se průvodce.
 4. Přečtete si uvítací stránku, klepněte na **Další** a přejdete na stránku **Jméno**.
 5. Do pole **Jméno** zadejte VPN a klepněte na **Další**. Volitelně lze zadat popis, který vám pomůže upamatovat se na účel této zásady.
 6. Na stránce Klienti vyberte volbu **Určitá adresa nebo adresy** a klepněte na volbu **Nová**, chcete-li definovat vašeho klienta.
 7. V dialogovém okně Nový klient zadejte tyto informace:
 - **Jméno:** VPN_Client
 - **IP adresa:** 192.83.63.1
 - Klepněte na **OK**, čímž vytvoříte klienta a vrátíte se do průvodce zásadou odlišovaných služeb.
- Poté, co klepnete na OK, se vrátíte do průvodce zásadou. Pokud jste již dříve vytvořili klienty, zrušte u nich označení a zkontrolujte, že jsou označeni pouze příslušní klienti.
8. Na stránce Požadavek na data serveru ověřte, že jsou vybrány volby **Libovolný token** a **Všechny priority**.
 9. Na stránce "Aplikace" ověřte, že jsou vybrány volby **Všechny porty** a **Vše**.
 10. Klepněte na **Další**.
 11. Na stránce IP adresa lokálního systému potvrďte předvolenou hodnotu a klepněte na **Další**.
 12. Na stránce Provozní třída DiffServ klepněte na **Nová**, chcete-li definovat charakteristiky výkonu. Objeví se průvodce novou provozní třídou.
 13. Přečtete si uvítací stránku a klepněte na **Další**.
 14. Na stránce Jméno zadejte EF_VPN.
 15. Na stránce Typ služby vyberte **Pouze odchozí** a klepněte na **Další**. Tato provozní třída bude používána pouze pro zásady odchozích připojení.
 16. Na stránce Označení kódového bodu DiffServ vyberte volbu **Třída 3**. Chování při jednotlivých přechodech určuje, jaký výkon přenosy od směrovačů a ostatních serverů v síti obdrží. Potřebujete-li pomoc s vaším rozhodnutím, použijte nápovědu týkající se tohoto rozhraní.
 17. Na stránce Omezení rychlosti odchozích připojení ověřte, že je zadáno **Ano** a klepněte na **Další**.
 18. Na stránce Limity počtu odchozích připojení zadejte tyto informace a klepněte na **Další**:
 - **Velikost sektoru token:** 100 Kilobitů
 - **Limit průměrné přenosové rychlosti:** 64 Megabitů za vteřinu

- **Limit maximální přenosové rychlosti:** Neomezit
19. Na stránce Odchozí provoz mimo profil vyberte volbu **Uvolnění paketů UDP nebo snížení zahlcení TCP** a klepněte na **Další**.
 20. Prohlédněte si stránku Provozní třída se souhrnnými informacemi, klepněte na volbu **Dokončit** a vrátíte se do průvodce zásadou.
 21. Na stránce Provozní třída DiffServ ověřte, že je vybrána volba **EF_VPN** a klepněte na **Další**.
 22. Na stránce Plán vyberte volbu **Aktivní během zvoleného plánu** a klepněte **Nový**.
 23. V dialogovém okně Přidat nový plán zadejte tyto informace a klepněte na **OK**:
 - **Jméno:** FirstShift
 - **Čas dne:** Aktivní v určitý čas a přidejte 9:00 AM do: 5:00 PM.
 - **Den v týdnu:** Aktivní v určitých dnech a vyberte Pondělí až Pátek.
 24. Na stránce Plán klepněte na **Další**.
 25. Prohlédněte si stránku se souhrnnými informacemi. Pokud jsou správné, klepněte na **Dokončit**, čímž vytvoříte zásadu QoS. Okno Konfigurace serveru QoS obsahuje seznam všech zásad QoS vytvořených na serveru. Poté, co dokončíte práci s průvodcem, objeví se zásada QoS v pravém podokně.

V tomto okamžiku jste dokončili konfiguraci zásady odlišovaných služeb QoS v systému iSeries A. Dalším krokem je spustit nebo aktualizovat server.

Krok 3: Spusťte nebo aktualizujte server QoS.

V okně Konfigurace serveru QoS vyberte **Server—>Spustit** nebo **Server—>Aktualizovat**.

Krok 4: Pomocí funkce Monitorování QoS ověřte, zda vytvořená zásada QoS funguje.

Chcete-li ověřit, zda zásada QoS funguje tak, jak jste ji nakonfigurovali, použijte funkci Monitorování QoS.

1. V okně Konfigurace serveru QoS vyberte **Server—>Monitor**. Otevře se okno "Monitorování "QoS".
2. Vyberte typ zásad odlišovaných služeb (DiffServ). Zobrazí se všechny zásady odlišovaných služeb.

Podobně jako v příkladu 1 jsou nejzajímavější pole ta, která obsahují údaje o vašem provozu. K těmto polím patří pole bits total, bits in-profile a packets out-of-profile. Pole bits out-of-profile označuje část přenosů, která přesahuje nakonfigurované hodnoty dané zásady QoS. Pole in-profile packets udává počet paketů, které byly řízeny touto zásadou QoS. Hodnota, kterou přiřadíte poli average rate limit, je také důležitá. Pokud počet paketů TCP překročí tento limit, jsou pakety posílány do sítě do té doby, dokud nelze snížit zahlcení TCP a nevyhovující pakety zařadit do fronty. V důsledku toho se zvýší počet nevyhovujících bitů (Bits out of profile). Rozdíl mezi touto zásadou a scénářem Omezení přenosu prohlížečů je ten, že v tomto případě jsou pakety chráněny prostřednictvím protokolu VPN. Jak vidíte, QoS může fungovat v kombinaci se spojením VPN. Popis všech polí monitorování najdete v tématu Monitorování QoS.

Poznámka: Pamatujte si, že výsledky budou přesné pouze v případě, že je zásada QoS aktivní. Ověřte plán, který jste zadali v rámci zásady QoS.

Krok 5: Změňte vlastnosti (je-li to třeba).

Poté, co si prohlédnete výsledky monitorování, můžete změnit vlastnosti libovolné zásady QoS či provozní třídy a dosáhnout tak očekávaných výsledků.

Také provozní třídu můžete upravit poté, co jste ji vytvořili.

1. V okně Konfigurace serveru QoS vyberte složku **DiffServ**. Chcete-li upravit zásadu QoS, klepněte pravým tlačítkem na volbu **VPN** v seznamu v pravém podokně a vyberte **Vlastnosti**.
2. Objeví se dialogové okno Vlastnosti s hodnotami, které řídí obecnou zásadu. Změňte hodnoty, kde je to vhodné.
3. Chcete-li upravit provozní třídu, vyberte složku **Provozní třída**. Poté klepněte pravým tlačítkem myši na **EF_VPN** ze seznamu v pravém podokně a vyberte volbu **Vlastnosti**.

4. Objeví se dialogové okno Vlastnosti CoS s hodnotami, které řídí přenosy sítě. Změňte hodnoty, kde je to vhodné.
5. Poté, co aktualizujete zásadu nebo provozní třídu, musíte server aktualizovat, aby byly změny potvrzeny. V okně Konfigurace serveru QoS vyberte **Server**—>**Aktualizovat**.



Scénář QoS: Omezení příchozích připojení

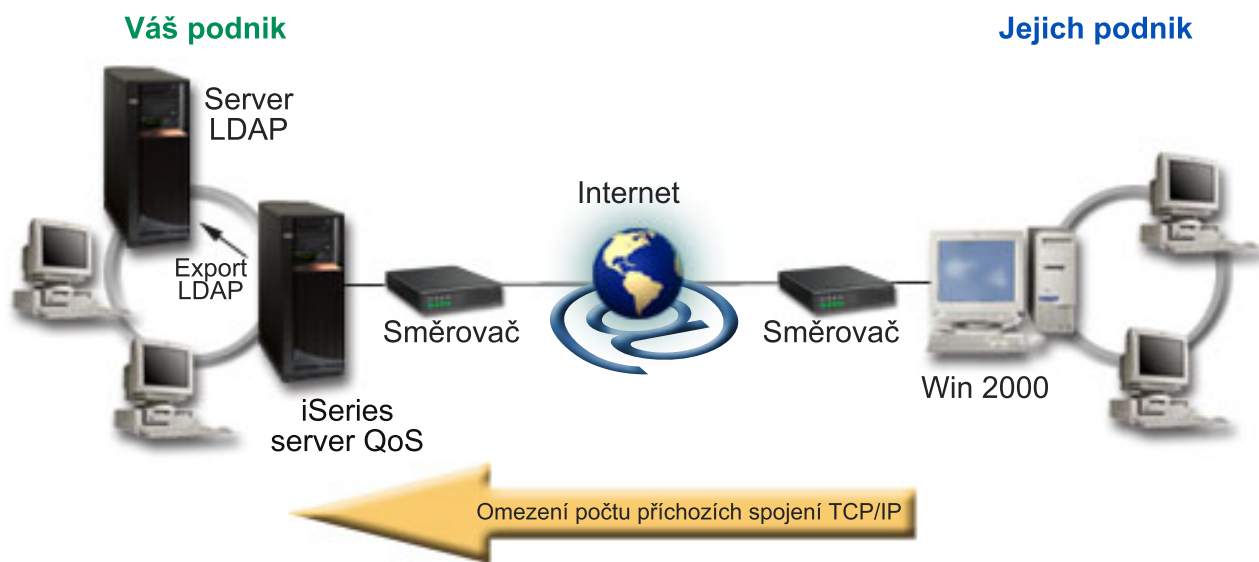
Situace



Prostředky vašeho webového serveru jsou přetíženy požadavky klientů vstupujících do sítě. Jste požádáni, abyste zpomalili přenosy HTTP přicházející do webového serveru v lokálním rozhraní 192.168.1.1. Pomocí QoS můžete omezit počet přijatých pokusů o příchozí připojení, a to na základě určitých atributů spojení k vašemu serveru (např. IP adresy). Rozhodnete se proto implementovat zásadu příchozích připojení, která bude omezovat počet přijatých příchozích připojení.

Na obrázku je znázorněna vaše společnost a společnost klienta. Tento druh zásady QoS může řídit přenosy pouze v jednom směru.

Obrázek 5. Omezení příchozích připojení TCP.



Cíl

Při konfigurování zásady příchozích připojení se musíte rozhodnout, zda budete omezovat přenosy pro určité lokální rozhraní nebo pro konkrétní aplikaci, a dále zda budete omezovat přenosy od konkrétního klienta. V tomto případě budete chtít vytvořit zásadu, která bude omezovat pokusy o připojení ze strany nějaké jiné společnosti - nazvěme ji Their_Company, které přicházejí na port 80 (protokol HTTP) v lokálním rozhraní 192.168.1.1.

Konfigurace

Chcete-li vytvořit zásadu příchozích připojení, postupujte takto:

1. Vytvořte zásadu příchozích připojení. (Viz 34)
2. Spusťte nebo aktualizujte server QoS. (Viz 35)
3. Prostřednictvím funkce Monitorování QoS ověřte, zda vytvořená zásada QoS funguje. (Viz 35)
4. Změňte její vlastnosti (je-li to třeba). (Viz 35)

Krok 1: Vytvořte zásadu příchozích připojení.

1. V prostředí produktu iSeries^(TM) Navigator, rozbalte svůj server Series A →Síť→Zásady pro práci s IP.
2. Klepněte pravým tlačítkem myši na **Quality of Service**, vyberte volbu **Configuration** a otevře se okno s konfigurační serveru QoS.
3. V okně konfigurace serveru QoS klepněte pravým tlačítkem myši na volbu **Zásady řízení příchozích připojení**, vyberte **Nová zásada** a spustí se průvodce.
4. Přečtěte si uvítací stránku a klepněte na **Další**.
5. Do pole **Jméno** zadejte **Restrict_TheirCo** a klepněte na **Další**. Volitelně lze zadat popis, který vám pomůže upamatovat se na účel této zásady.
6. Na stránce Klienti vyberte volbu **Určitá adresa nebo adresy** a klepněte na volbu **Nová**, chcete-li definovat vašeho klienta.
7. V dialogovém okně Nový klient zadejte tyto informace:
 - **Jméno:** Their_Co
 - **Rozsah IP adres:** 10.1.1.1 to 10.1.1.10
 - Klepněte na **OK**, čímž vytvoříte klienta a vrátíte se do průvodce zásadou.Poté, co klepnete na OK, se vrátíte do průvodce zásadou. Pokud jste již dříve vytvořili klienty, zrušte u nich označení a zkontrolujte, že jsou označeni pouze příslušní klienti.
8. Na stránce URI ověřte, že je vybrána volba **Libovolná URI** a klepněte na **Další**.
9. Na stránce Aplikace vyberte **Specifický port, rozsah portů nebo typ serveru** a klepněte na **Nový**.
10. V dialogovém okně Nová aplikace zadejte tyto informace a klepněte na **OK**, čímž se vrátíte do průvodce:
 - **Jméno:** HTTP
 - **Port:** 80
11. Klepněte na volbu "Další" a přejdete na stránku Identifikační bod.
12. Na stránce Kódový bod ověřte, že je vybrána volba **Všechny kódové body**. Pak klepněte na **Next**.
13. Na stránce IP adresa lokálního systému vyberte volbu **IP adresa** a vyberte rozhraní, ze kterého jsou učiněny požadavky na váš lokální systém. V tomto příkladu použijte 192.168.1.1.
14. Na stránce Provozní třída klepněte na **Nová**, chcete-li definovat charakteristiky výkonu. Objeví se průvodce novou provozní třídou.
15. Přečtěte si uvítací stránku a klepněte na **Další**.
16. Na stránce Jméno zadejte **příchozí** a klepněte na **Další**. Volitelně lze zadat popis, který vám pomůže upamatovat se na účel této provozní třídy.
17. Na stránce Typ služby vyberte **Pouze příchozí**. Tato provozní třída bude používána pouze pro zásady příchozích připojení.
18. Na stránce Omezení odchozích připojení zadejte tyto informace a klepněte na **Další**:
 - Průměrná rychlost připojení: 50 za sekundu
 - Limit počtu připojení ve shluku: 50 připojení
 - Priorita: Střední
19. Klepněte na **Ukončit** a vrátíte se do průvodce zásadou.
20. Na stránce Provozní třída ověřte, že je zvolena provozní třída, kterou jste právě vytvořili, a klepněte na **Další**.
21. Na stránce Plán vyberte volbu **Aktivní během zvoleného plánu** a klepněte **Nový**.

22. V dialogovém okně Nový plán zadejte tyto informace a klepněte na **OK**:
 - Jméno: FirstShift
 - Čas dne: Aktivní v určitý čas a přidejte 9:00 do: 5:00.
 - Den v týdnu: Aktivní v určitých dnech a zadejte Pondělí až Pátek.
23. Na stránce Plány klepněte na **Další**.
24. Prohlédněte si stránku se souhrnnými informacemi. Pokud jsou správné, klepněte na **Dokončit**, čímž vytvoříte zásadu QoS. Konfigurace serveru QoS obsahuje seznam všech zásad QoS vytvořených na serveru. Poté, co dokončíte práci s průvodcem, objeví se zásada QoS v pravém podokně.

V tomto okamžiku jste dokončili konfiguraci zásady příchozích připojení v systému iSeries A. Dalším krokem je spustit nebo aktualizovat server.

Krok 2: Spusťte nebo aktualizujte server QoS.

V okně Konfigurace serveru QoS vyberte **Server**—>**Spustit** nebo **Server**—>**Aktualizovat**.

Krok 3: Pomocí funkce Monitorování QoS ověřte, zda vytvořená zásada QoS funguje.

Chcete-li ověřit, zda zásada QoS funguje tak, jak jste ji nakonfigurovali, použijte funkci Monitorování QoS.

1. V okně Konfigurace serveru QoS vyberte **Server**—>**Monitor**. Otevře se okno "Monitorování QoS".
2. Vyberte zásadu příchozích připojení. Zobrazí se všechny zásady příchozích připojení. Vyberte ze seznamu položku **Restrict_TheirCo**.

Zkontrolujte především pole obsahující výsledky měření, jako je např. pole Accepted request (počet přijatých požadavků), Dropped requests (počet uvolněných požadavků), Total requests (celkový počet požadavků) a Connection rate (počet požadavků na připojení přijatých za vteřinu). Počet uvolněných požadavků označuje, že část přenosu přesahuje nakonfigurované hodnoty příslušné zásady QoS. Pole přijatých požadavků udává počet bitů kontrolovaných danou zásadou QoS (od okamžiku, kdy byl paket spuštěn do okamžiku současného výstupu monitorování).

Také hodnota, kterou přiřadíte poli Average connection rate (limitu průměrného počtu připojení), je důležitá. Když pakety tento limit překročí, server je začne uvolňovat. V důsledku toho se zvýší počet uvolněných požadavků. To dokládá, že zásada QoS funguje v souladu s tím, jak jste ji nakonfigurovali. Popis všech polí výstupu monitorování najdete v tématu Monitorování QoS.

Poznámka: Pamatujte si, že výsledky budou přesné pouze v případě, že je zásada QoS aktivní. Ověřte plán, který jste zadali v rámci zásady QoS.

Krok 4: Změňte vlastnosti (je-li to třeba).

Poté, co si prohlédnete výsledky monitorování, můžete změnit vlastnosti libovolné zásady QoS či provozní třídy a dosáhnout tak očekávaných výsledků.

1. V okně Konfigurace serveru QoS vyberte složku **Povolání příchozích připojení**. Klepněte pravým tlačítkem myši na **Restrict_TheirCo** v seznamu v pravém podokně a vyberte **Vlastnosti**, chcete-li upravit zásadu QoS.
2. Objeví se dialogové okno "Vlastnosti" s hodnotami, které řídí obecnou zásadu. Změňte hodnoty, kde je to vhodné.
3. Chcete-li upravit provozní třídu, vyberte složku **Provozní třída**. Poté klepněte pravým tlačítkem myši na volbu **příchozí** v seznamu v pravém podokně a vyberte volbu **Vlastnosti**.
4. Objeví se dialogové okno Vlastnosti CoS s hodnotami, které řídí přenosy sítě. Změňte hodnoty, kde je to vhodné.
5. Poté, co aktualizujete zásadu nebo provozní třídu, musíte server aktualizovat, aby byly změny potvrzeny. V okně Konfigurace serveru QoS vyberte **Server**—>**Aktualizovat**.



Scénář QoS: Předvídatelný provoz B2B

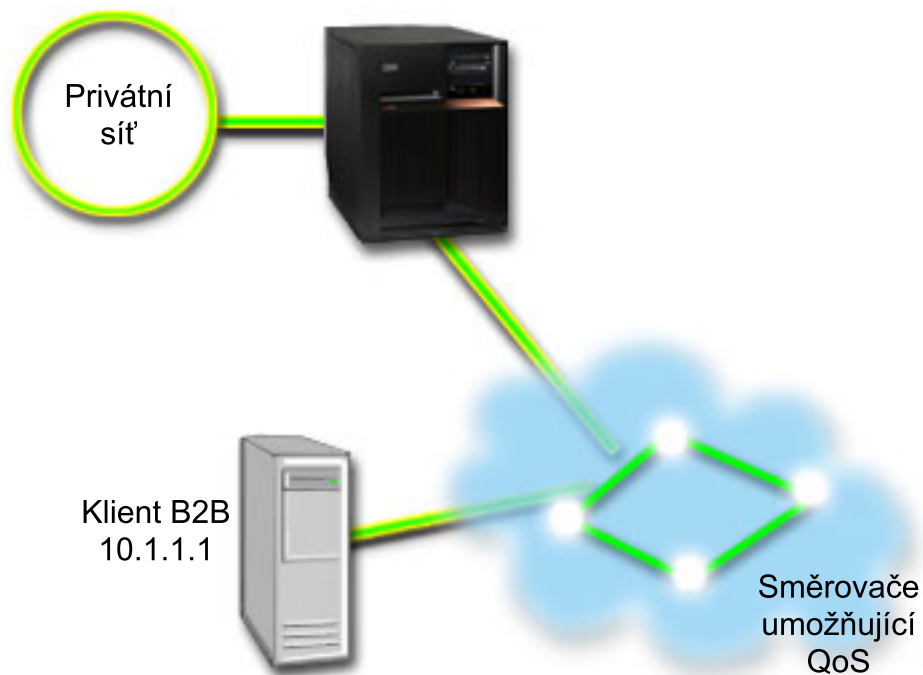
Situace



Obchodní oddělení vašeho podniku hlásí problémy - síťový provoz nemá takový výkon, jaký očekávali. Zásada QoS, kterou vytváříte na podnikovém serveru iSeries[™], je zamýšlena pro prostředí business-to-business (B2B), které vyžaduje předvídatelné služby pro elektronické podnikání. Musíte zákazníkům zajistit předvídatelné transakce. Chcete proto obchodnímu oddělení poskytnout vyšší úroveň QoS pro jejich aplikaci pro příjem objednávek v době obchodní špičky, tj. od 10.00 do 16.00 hod.

Na obrázku dole tvoří obchodní skupina součást vaší privátní sítě. Na trase přenosu směrem ke klientovi typu B2B jsou směrovače, které podporují protokol RSVP. Jednotlivá R na obrázku představují směrovače na trase přenosu.

Obrázek 7. Zásada integrovaných služeb QoS pro klienta B2B využívající směrovače s podporou pro RSVP.



Cíl

Služby řízeného zavádění podporují aplikace, které jsou vysoce citlivé na zahlcení sítě, ale které snesou určitou míru ztrát nebo zpoždění při přenosu. Pokud aplikace používá služby řízeného zavádění, její výkonnost se nebude se zvýšeným zatížením zhoršovat. Provoz bude zajištěn pomocí služby, která udržuje normální provoz v síti za omezenějších podmínek. Vzhledem k tomu, že tato konkrétní aplikace toleruje určitá zpoždění, rozhodnete se zavést zásadu integrovaných služeb QoS používající služby řízeného zavádění.

Zásady integrovaných služeb QoS dále vyžadují, aby směrovače na trase přenosu podporovaly RSVP. Další informace najdete v tématu Zásady integrovaných služeb QoS.

Předpoklady a nezbytné podmínky

Zásada integrovaných služeb je pokročilá zásada, která v některých případech vyžaduje značné systémové prostředky. Zásady integrovaných služeb QoS vyžadují tyto nezbytné předpoklady:

- **Aplikace podporující RSVP**

Vzhledem k tomu, že váš server nemá žádné aplikace podporující RSVP, musíte si napsat vlastní aplikace podporující RSVP. K napsání vlastních aplikací použijete rozhraní RAPI (Resource Reservation Setup Protocol) nebo rozhraní qtoq QoS socket API. Další informace najdete v tématu Rozhraní QoS API v části pojednávající o rozhraní API integrovaných služeb.

- **Směrovače a servery na síťové trase, které podporují RSVP**

Produkt QoS je síťové řešení. Pokud si nejste jisti, zda celá síť podporuje RSVP, můžete přesto vytvořit zásadu integrovaných služeb a použít označení, čímž ji přidělíte určitou prioritu; prioritu však nelze zaručit. Další informace najdete v tématu Zásady integrovaných služeb QoS.

- **Smlouva SLA (Service level agreement)**

S vaším ISP máte uzavřenou smlouvu SLA (service level agreement), čímž zajišťujete, že vaše zásady QoS obdrží požadovanou prioritu. Zásada QoS, kterou vytvoříte na serveru iSeries, umožňuje, aby přenosy (v rámci této zásady QoS) obdržely v síti příslušnou prioritu. Negarantuje ji však; to je závislé na vaší smlouvě SLA. Využití zásad QoS vám v podstatě může poskytnout určitou výhodu při vyjednávání některých úrovní služby i poplatků. Použijte odkaz smlouvy SLA, chcete-li se dozvědět více. Poznámka: V rámci soukromé sítě není potřeba smlouvy SLA.

Konfigurace

Poté, co ověříte a provedete všechny nezbytné předchozí kroky, jste připraveni vytvořit zásadu integrovaných služeb QoS. Chcete-li vytvořit zásadu integrovaných služeb, postupujte takto:

1. Vytvoříte zásadu integrovaných služeb. (Viz 37)
2. Spustíte nebo aktualizujete server QoS. (Viz 38)
3. Prostřednictvím funkce Monitorování QoS ověříte, zda vytvořená zásada QoS funguje. (Viz 38)
4. Změňte její vlastnosti (je-li to třeba). (Viz 38)

Step 1: Vytvoříte zásadu integrovaných služeb QoS.

1. V prostředí produktu iSeries Navigator rozbalte Server iSeries A →**Síť**→**Zásady pro práci s IP**.
2. Klepněte pravým tlačítkem myši na **Quality of Service**, vyberte volbu **Configuration** a otevře se okno s konfiguračním serverem QoS.
3. V okně Konfigurace serveru QoS klepněte pravým tlačítkem myši na typ zásady integrovaných služeb QoS (IntServ), vyberte volbu **Nová zásada** a spustí se průvodce.
4. Přečtěte si uvítací stránku, klepněte na **Další** a přejděte na stránku **Jméno**.
5. Do pole **Jméno** zadejte **B2B_CL** a klepněte na **Další**. Volitelně lze zadat popis, který vám pomůže upamatovat se na účel této zásady.
6. Na stránce **Klienti** vyberte volbu **Určitá adresa nebo adresy** a klepněte na volbu **Nová**, chcete-li definovat vašeho klienta.
7. V dialogovém okně **Nový klient** zadejte tyto informace:
 - **Jméno:** CL_client
 - **IP adresa:** 10.1.1.1
 - Klepněte na **OK**, čímž vytvoříte klienta a vrátíte se do průvodce zásadou.

Poté, co klepnete na OK, se vrátíte do průvodce zásadou. Pokud jste již dříve vytvořili klienty, zrušte u nich označení a zkontrolujte, že jsou označeni pouze příslušní klienti. Na stránce **Aplikace** vyberte volbu **Specifický port, rozsah portů nebo typ serveru** a klepněte na **Nový**.

8. V dialogovém okně **Nová aplikace** zadejte tyto informace a klepněte na **OK**, čímž se vrátíte do průvodce:
 - **Jméno:** business_app
 - **Rozsah portů:** 7000-8000
9. Na stránce **Aplikace** vyberte volbu **Protokol** a ověřte, že je vybrána volba **TCP**. Klepněte na **Další**.

Poznámka: Aplikace, kterou jste vybrali pro zásadu integrovaných služeb, musí být napsána tak, aby používala rozhraní RAPI API nebo rozhraní qtoq sockets API. Tato rozhraní API společně s protokolem RSVP (Resource Reservation Protocol) provádějí rezervaci šířky pásma pro integrované služby QoS. Pokud tato rozhraní API nevyužijete, neobdrží aplikace žádné priority ani garance. Je třeba zdůraznit, že tato zásada QoS umožňuje, aby aplikace obdrželi prostřednictvím sítě prioritu, neposkytuje však v tomto ohledu žádné záruky. Je-li třeba zajistit rezervaci, musí všechny směrovače a servery na trase přenosů také používat protokol RSVP. Rezervace typu "end-to-end" je závislá na tom, jak se na ni jednotlivé prvky v síti podílí.

10. Na stránce IP adresa lokálního systému potvrďte předvolenou hodnotu a klepněte na **Další**.
11. Na stránce Typ integrovaných služeb vyberte volbu **Řízené zavádění** a klepněte na **Další**.
12. Na stránce Označení IntServ vyberte **Ne, nepřirázovat chování při jednotlivých přechodech** a klepněte na **Další**.
13. Na stránce Omezení výkonu integrovaných služeb zadejte tyto informace a klepněte na **Další**:
 - **Maximální počet toků:** 5
 - **Omezení přenosové rychlosti token (r):** Neomezit
 - **Velikost sektoru token:** 100 Kilobitů
 - **Omezení přenosové rychlosti token (r):** 25 Megabitů za vteřinu
14. Na stránce Plán vyberte volbu **Aktivní během zvoleného plánu** a klepněte **Nový**.
15. Na stránce Nový plán zadejte tyto informace a klepněte na **OK**:
 - **Jméno:** primetime
 - **Čas dne:** Aktivní v určitý čas a přidejte 10:00 AM do 4:00 PM
 - **Den v týdnu:** Aktivní v určitých dnech a vyberte Pondělí až Pátek.
16. Na stránce Plány klepněte na **Další**.
17. Prohlédněte si stránku se souhrnnými informacemi. Pokud jsou správné, klepněte na **Dokončit**, čímž vytvoříte zásadu QoS. Hlavní rozhraní produktu QoS uvádí seznam všech zásad QoS, které jsou na serveru vytvořeny. Poté, co dokončíte práci s průvodcem, objeví se zásada QoS v pravém podokně.

V tomto okamžiku jste dokončili konfiguraci zásady integrovaných služeb QoS v systému iSeries A. Dalším krokem je spustit nebo aktualizovat server.

Krok 2: Spusťte nebo aktualizujte server QoS.

V okně Konfigurace serveru QoS vyberte **Server—>Spustit** nebo **Server—>Aktualizovat**.

Krok 3: Pomocí funkce Monitorování QoS ověřte, zda vytvořená zásada QoS funguje.

Chcete-li ověřit, zda zásada QoS funguje správně, použijte funkci Monitorování QoS.

1. V okně Konfigurace serveru QoS vyberte **Server—>Monitor**. Otevře se okno "Monitorování "QoS".
2. Vyberte typ zásady QoS integrované služby (IntServ). Zobrazí se všechny zásady integrovaných služeb.

Nejzajímavější pole jsou ta, která obsahují údaje o vašem provozu. Zkontrolujte zejména pole Bits total (celkový počet bitů), Bits in-profile (počet vyhovujících bitů) a Packets in profile (počet vyhovujících paketů). Počet nevyhovujících bitů naznačuje, že ostatní provoz byl v tomto rozsahu opožděn nebo uvolněn, aby se vyhovělo požadavkům této zásady integrovaných služeb QoS. Podrobný popis výstupu monitorování uvádí část Monitorování QoS.

Poznámka: Pamatujte si, že výsledky budou přesné pouze v případě, že je zásada QoS aktivní. Ověřte plán, který jste zadali v rámci zásady QoS. Kromě toho zobrazuje monitor pouze zásady integrovaných služeb QoS poté, co jsou aplikace spuštěny. Před monitorováním je třeba vytvořit rezervaci protokolu RSVP.

Krok 4: Změňte vlastnosti (je-li to třeba).

Poté, co si prohlédnete výsledky monitorování, můžete změnit vlastnosti libovolné zásady QoS a dosáhnout tak očekávaných výsledků.

Poté, co jste zásadu QoS vytvořili, můžete změnit hodnoty, které jste pomocí průvodce nastavili.

1. V okně Konfigurace serveru QoS vyberte složku **IntServ**. Klepněte pravým tlačítkem myši na **B2B_CL** v seznamu v pravém podokně a vyberte **Vlastnosti**, chcete-li upravit zásadu QoS.
2. Objeví se dialogové okno Vlastnosti s hodnotami, které řídí obecnou zásadu. Změňte hodnoty, kde je to vhodné.
3. Poté, co zásadu aktualizujete, musíte aktualizovat server, aby byly změny potvrzeny. V okně Konfigurace serveru QoS vyberte **Server**—>**Aktualizovat**.



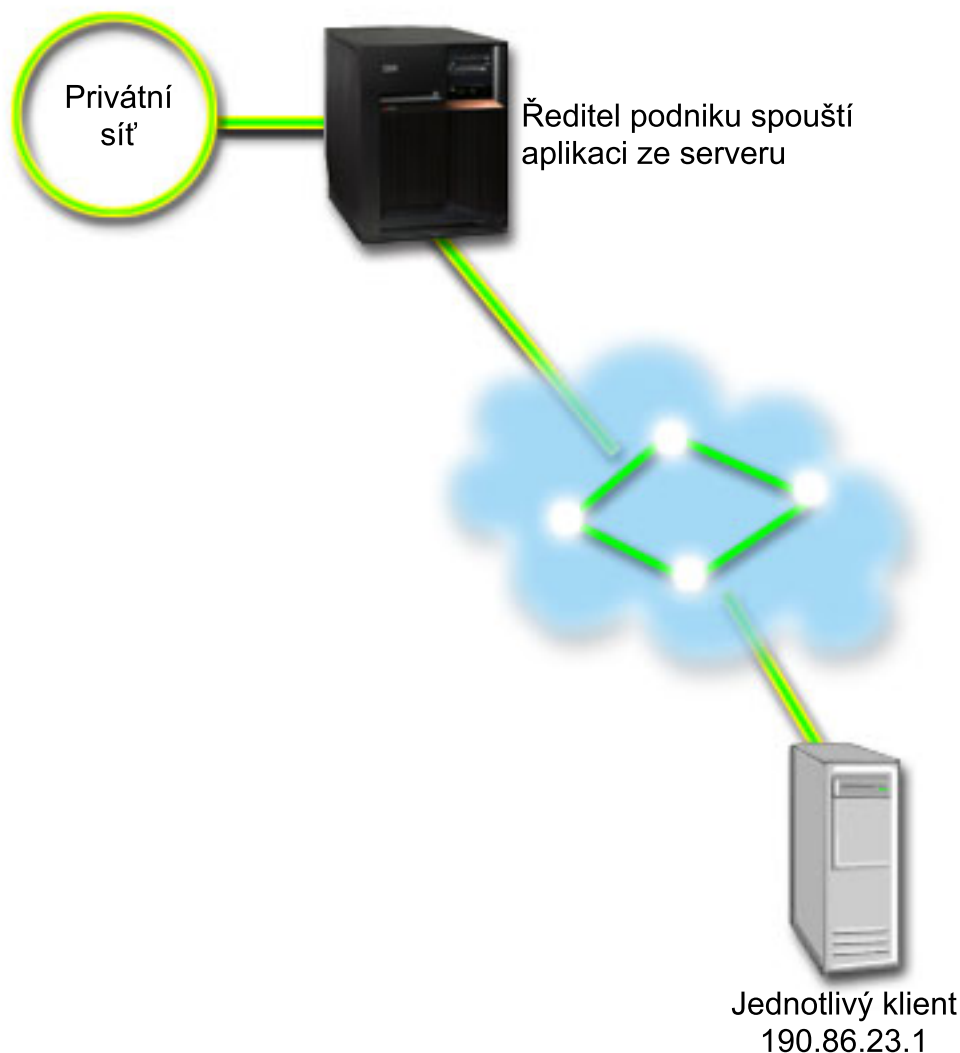
Scénář QoS: Vyhrazený přenos (IP telefonie)

Situace



Ředitel vašeho podniku chce provést živé vysílání pro klienta na druhém konci státu, a to v době od 13.00 do 14.00 hod. Musíte proto pro IP telefonii zajistit garantovanou šířku pásma, aby během přenosu nedocházelo k přerušením. V tomto scénáři je aplikace umístěna na serveru.

Obrázek 9. Ředitelova prezentace pro klienta zajištěná pomocí zásady integrovaných služeb QoS.



Cíle

Vzhledem k tomu, že aplikace, kterou používá váš ředitel, vyžaduje plynulý nepřerušovaný přenos, rozhodli jste se použít zásadu garantovaných integrovaných služeb QoS. Zásady garantovaných služeb řídí maximální zpoždění ve frontě tak, aby se pakety neopoždovaly nad určitý stanovený časový úsek.

Předpoklady a nezbytné podmínky

Zásada integrovaných služeb je pokročilá zásada, která v některých případech vyžaduje značné systémové prostředky. Zásady integrovaných služeb QoS vyžadují tyto nezbytné předpoklady:

- **Aplikace podporující RSVP**

Vzhledem k tomu, že váš server nemá žádné aplikace podporující RSVP, musíte si napsat vlastní aplikace podporující RSVP. K napsání vlastních aplikací použijete rozhraní RAPI (Resource Reservation Setup Protocol) nebo rozhraní qtoq QoS socket API. Další informace najdete v tématu Rozhraní QoS API v části pojednávající o rozhraní API integrovaných služeb.

- **Směrovače a servery na síťové trase, které podporují RSVP**

Produkt QoS je síťové řešení. Pokud si nejste jisti, zda celá síť podporuje RSVP, můžete přesto vytvořit zásadu integrovaných služeb a použít označení, čímž ji přidělíte určitou prioritu; prioritu však nelze zaručit. Další informace najdete v tématu Zásady integrovaných služeb QoS.

- **Smlouva SLA (Service level agreement)**

S vaším ISP máte uzavřenou smlouvu SLA (service level agreement), čímž zajišťujete, že vaše zásady QoS obdrží

požadovanou prioritu. Zásada QoS, kterou vytvoříte na serveru iSeries™, umožňuje, aby přenosy (v rámci této zásady QoS) obdržely v síti příslušnou prioritu. Negarantuje ji však; to je závislé na vaší smlouvě SLA. Využití zásad QoS vám v podstatě může poskytnout určitou výhodu při vyjednávání některých úrovní služby i poplatků. Použijte odkaz smlouvy SLA, chcete-li se dozvědět více.

Konfigurace

Poté, co ověříte a provedete všechny nezbytné předchozí kroky, jste připraveni vytvořit zásadu integrovaných služeb QoS. Chcete-li vytvořit zásadu integrovaných služeb, postupujte takto:

1. Vytvoříte zásadu integrovaných služeb. (Viz 41)
2. Spustíte nebo aktualizujete server QoS. (Viz 42)
3. Prostřednictvím funkce Monitorování QoS ověříte, zda vytvořená zásada QoS funguje. (Viz 42)
4. Změňte její vlastnosti (je-li to třeba). (Viz 42)

Step 1: Vytvoříte zásadu integrovaných služeb QoS.

1. V prostředí produktu iSeries Navigator rozbalte Server iSeries A → **Síť** → **Zásady pro práci s IP**.
2. Klepněte pravým tlačítkem myši na **Quality of Service**, vyberte volbu **Configuration** a otevře se okno s konfigurací serveru QoS.
3. V okně Konfigurace serveru QoS klepněte pravým tlačítkem myši na typ zásady integrovaných služeb QoS (IntServ), vyberte volbu **Nová zásada** a spustí se průvodce.
4. Přečtěte si uvítací stránku, klepněte na **Další** a přejdete na stránku **Jméno**.
5. Do pole **Jméno** zadejte **CEO_guaranteed** a klepněte na **Další**. Volitelně lze zadat popis, který vám pomůže upamatovat se na účel této zásady.
6. Na stránce **Klienti** vyberte volbu **Určitá adresa nebo adresy** a klepněte na volbu **Nová**, chcete-li definovat vašeho klienta.
7. V dialogovém okně **Nový klient** zadejte tyto informace:
 - **Jméno:** Branch1
 - **IP adresa:** 190.86.23.1
 - Klepněte na **OK**, čímž vytvoříte klienta a vrátíte se do průvodce zásadou integrovaných služeb.

Poté, co klepnete na OK, se vrátíte do průvodce zásadou. Pokud jste již dříve vytvořili klienty, zrušte u nich označení a zkontrolujte, že jsou označeni pouze příslušní klienti. Na stránce **Aplikace** vyberte volbu **Specifický port, rozsah portů nebo typ serveru** a klepněte na **Nový**.

8. V dialogovém okně **Nová aplikace** zadejte tyto informace a klepněte na **OK**, čímž se vrátíte do průvodce:
 - **Jméno:** IP telephony
 - **Port:** 2427
9. Na stránce **Aplikace** vyberte volbu **Protokol** a ověřte, že je vybrána volba **TCP**. Klepněte na **Další**.

Poznámka: Aplikace, kterou jste vybrali pro zásadu integrovaných služeb, musí být napsána tak, aby používala rozhraní RAPI API nebo rozhraní qtoq sockets API. Tato rozhraní API společně s protokolem RSVP (Resource Reservation Protocol) provádějí rezervaci šířky pásma pro integrované služby QoS. Pokud tato rozhraní API nevyužijete, neobdrží aplikace žádné priority ani garance. Je třeba zdůraznit, že tato zásada QoS umožňuje, aby aplikace obdrželi prostřednictvím sítě prioritu, neposkytuje však v tomto ohledu žádné záruky. Je-li třeba zajistit rezervaci, musí všechny směrovače a servery na trase přenosu také používat protokol RSVP. Rezervace typu "end-to-end" je závislá na tom, jak se na ni jednotlivé prvky v síti podílí.
10. Na stránce **IP adresa lokálního systému** potvrďte předvolenou hodnotu **Všechny IP adresy**.
11. Na stránce **Typ integrovaných služeb** vyberte volbu **Garantované** a klepněte na **Další**.
12. Na stránce **Označení IntServ** vyberte **Ne, nepřirazovat chování při jednotlivých přechodech** a klepněte na **Další**.
13. Na stránce **Omezení výkonu integrovaných služeb** zadejte tyto informace a klepněte na **Další**:

- **Maximální počet toků:** 1
 - **Agregovaný limit šířky pásma (R):** Neomezit
 - **Velikost sektoru token:** 100 Kilobitů
 - **Omezení šířky pásma (R):** 16 Megabitů za vteřinu
14. Na stránce Plán vyberte volbu **Aktivní během zvoleného plánu** a klepněte **Nový**.
 15. Na stránce Nový plán zadejte tyto informace a klepněte na **OK**:
 - **Jméno:** one_hour
 - **Čas dne:** Aktivní v určitý čas a přidejte 1:00 PM do: 2:00 PM.
 - **Den v týdnu:** Aktivní v určitých dnech a vyberte Pondělí.
 16. Na stránce Plán klepněte na **Další**.
 17. Prohlédněte si stránku se souhrnnými informacemi. Pokud jsou správné, klepněte na **Dokončit**, čímž vytvoříte zásadu QoS. Hlavní okno Konfigurace serveru QoS obsahuje seznam všech zásad QoS vytvořených na serveru. Poté, co dokončíte práci s průvodcem, objeví se zásada QoS v pravém podokně.

V tomto okamžiku jste dokončili konfiguraci zásady integrovaných služeb QoS v systému iSeries A. Dalším krokem je spustit nebo aktualizovat server.

Krok 2: Spusťte nebo aktualizujte server QoS.

V okně Konfigurace serveru QoS vyberte **Server**—>**Spustit** nebo **Server**—>**Aktualizovat**.

Krok 3: Pomocí funkce Monitorování QoS ověřte, zda vytvořená zásada QoS funguje.

Chcete-li ověřit, zda zásada QoS funguje správně, použijte funkci Monitorování QoS.

1. V okně Konfigurace serveru QoS vyberte **Server**—>**Monitor**. Otevře se okno "Monitorování "QoS".
2. Vyberte složku s typem zásady integrovaných služeb (IntServ). Zobrazí se všechny zásady integrovaných služeb.

Nejzajímavější údaje jsou v měřených polích, která obsahují výsledky o vašem provozu. K těmto polím patří pole bits total, bits in-profile a packets in-profile. Pole Bits out-of-profile udává rozsah přenosu, které byly opožděny nebo uvolněny, aby se vyhovělo požadavkům této zásady integrovaných služeb QoS. Popis všech polí výstupu monitorování najdete v tématu Monitorování QoS.

Poznámka: Pamatujte si, že výsledky budou přesné pouze v případě, že je zásada QoS aktivní. Ověřte plán, který jste zadali v rámci zásady QoS. Kromě toho zobrazuje monitor pouze zásady integrovaných služeb QoS poté, co jsou aplikace spuštěny. Před monitorováním je třeba vytvořit rezervaci protokolu RSVP.

Krok 4: Změňte vlastnosti (je-li to třeba).

Poté, co si prohlédnete výsledky monitorování, můžete změnit vlastnosti libovolné zásady QoS a dosáhnout tak očekávaných výsledků.

Když jste si zobrazili výsledky pro tuto zásadu QoS, můžete nyní změnit některé hodnoty, které jste předtím pomocí průvodce nastavili.

1. V okně Konfigurace serveru QoS vyberte složku integrovaných služeb (IntServ). Klepněte pravým tlačítkem myši na **CEO_guaranteed** v seznamu v pravém podokně a vyberte **Vlastnosti**, chcete-li upravit zásadu QoS.
2. Objeví se dialogové okno Vlastnosti s hodnotami, které řídí obecnou zásadu. Změňte hodnoty, kde je to vhodné.
3. Poté, co zásadu aktualizujete, musíte aktualizovat server, aby byly změny potvrzeny. V okně Konfigurace serveru QoS vyberte **Server**—>**Aktualizovat**.



Plánování použití QoS

Nejdůležitější fází při implementaci produktu QoS je plánování. Chcete-li dosáhnout očekávaných výsledků, musíte přezkoumat vaše síťová zařízení a provést monitorování provozu sítě. Poradce pro plánování QoS vás provede základními otázkami, které byste si měli položit v průběhu plánovacího procesu. Kromě poradce pro plánování QoS byste si měli před konfigurováním produktu QoS projít tato témata.

Seznamte se se smlouvami SLA.

Smlouvy SLA (Service level agreement) představují významnou součást QoS. Při plánování QoS musíte pochopit princip smluv SLA a nastavit potřebnou smlouvu SLA se svým poskytovatelem síťových služeb.

Seznamte se s funkcemi síťového hardwaru a softwaru.

QoS bude účinné jen tak, jako jeho nejslabší článek. Na výsledky QoS mají mimořádný vliv schopnosti vašich interních zařízení a dalších zařízení mimo vaši síť.

Udělte administrátorovi produktu QoS vhodné oprávnění.

V této části je seznam všech oprávnění, které potřebujete ke konfigurování QoS a serveru adresářů.

Ověřte požadavky systému.

V této části je seznam všech požadavků, které jsou potřeba pro úspěšný provoz QoS.

Zvažte výkon sítě

QoS se týká především výkonu sítě. Hlavním důvodem, proč uvažujete o zavedení QoS, je pravděpodobně to, že už jste zažili zahlcení sítě a ztrátu paketů. Předtím, než budete implementovat konkrétní zásady QoS, je vhodné pomocí funkce Monitorování QoS zjistit současnou úroveň výkonu provozu ve vaší síti. Na základě těchto výsledků určíte, kde dochází k zahlcením. Další informace o monitorování aktuálních přenosů najdete v tématu Monitorování transakcí serveru.

Použijte Poradce pro plánování QoS.

Zvažte tyto základní otázky předtím, než budete implementovat QoS. Obdržíte pracovní formulář s navrhovanými zásadami QoS založenými na schopnostech vašich aplikací.

Plánování pořadí zásad QoS

Pořadí, ve kterém jsou zásady QoS zobrazeny v produktu iSeries[™] Navigator (také v souboru polycyd.conf), určuje pořadí, ve kterém jsou zpracovány. Pořadí zásad QoS je nejdůležitější v případě, když se zásady QoS překrývají.

Je-li to nezbytné použijte rozhraní QoS API.

Obsahuje informace o tom, která rozhraní API (a zda vůbec nějaká) jsou třeba pro používání různých typů zásad QoS. Pokud například konfigurujete zásadu integrovaných služeb QoS, budete muset použít rozhraní API k tomu, aby jste napsali aplikace, které mohou využívat RSV.

Požadavky na oprávnění



Zásady QoS mohou obsahovat citlivé informace o vaší síti. Oprávnění k administraci QoS by tedy mělo být uděleno pouze v případě, že je to nutné. Pro konfigurování zásad QoS a (volitelně) serveru adresářů LDAP jsou třeba níže uvedená oprávnění.

Udělení oprávnění potřebných pro správu serveru adresářů

Administrátor QoS bude potřebovat tato oprávnění: oprávnění *ALLOBJ a *IOSYSCFG. Informace o alternativních oprávněních najdete v tématu Konfigurování serveru adresářů.

Udělení oprávnění pro spuštění serveru TCP/IP

Chcete-li udělit oprávnění k objektu pro příkazy STRTCPSVR a ENDTCPSVR, postupujte takto:

1. **STRTCPSVR:** Na příkazový řádek napište GRTOBJAUT OBJ (QSYS/STRTCPSVR) OBJTYPE (*CMD) USER (ADMINPROFILE) AUT (*USE), kde ADMINPROFILE nahradíte jménem profilu vašeho administrátora, a stiskněte klávesu **Enter**.

2. **ENDTCPSVR**: Na příkazový řádek napište GRTOBJAUT OBJ (QSYS/ENDTCPSVR) OBJTYPE (*CMD) USER (ADMINPROFILE) AUT (*USE), kde ADMINPROFILE nahradíte jménem profilu vašeho administrátora, a stisknete klávesu **Enter**.

Udělení oprávnění k přístupu ke všem objektům a ke konfiguraci systému

Doporučuje se, aby uživatelé, kteří budou konfigurovat QoS, měli přístupy na úrovni správce systému. Chcete-li udělit oprávnění k přístupu ke všem objektům a ke konfiguraci systému, postupujte takto:

1. V prostředí produktu iSeries^(TM) Navigator rozbalte svůj server → **Uživatelé a skupiny**.
2. Dvakrát klepněte na volbu **Všichni uživatelé**.
3. Klepněte pravým tlačítkem myši na uživatelský profil administrátora a vyberte volbu **Vlastnosti**.
4. V dialogovém okně Vlastnosti klepněte na volbu **Schopnosti**.
5. Na stránce Schopnosti vyberte **Přístup ke všem objektům a konfigurace systému**.
6. Klepněte na **OK**, abyste zavřeli stránku Schopnosti.
7. Klepněte na **OK**, chcete-li zavřít dialogové okno Vlastnosti.



Systémové požadavky

QoS je integrální součástí operačního systému. Musíte splnit tyto požadavky:

1. Nainstalovat produkt TCP/IP Connectivity Utilities (57xx-TC1).
2. Nainstalovat na svůj osobní počítač produkt iSeries Navigator. Ujistěte se, že jste v rámci instalace modulu iSeries Access nainstalovali sekci Síť. Produkt QoS je umístěn v sekci Síť v rámci menu Zásady pro práci s IP.

Poznámka: Další informace o TCP/IP, vytváření sítí nebo IP adresách najdete v části Související informace o QoS.

Smlouvy SLA (Service level agreement)



Smyslem této části je ukázat některé důležité aspekty smlouvy SLA (service level agreement), které mohou ovlivnit kvalitu vaší implementace produktu QoS. Produkt QoS je síťové řešení a aby obdržel síťovou prioritu mimo privátní síť, budete možná potřebovat smlouvu SLA s vaším poskytovatelem služeb sítě Internet (ISP).

Kdy potřebujete smlouvu SLA?

Smlouvu SLA potřebujete pouze v případě, že vaše zásady QoS vyžadují prioritu mimo vaši privátní síť. Pokud používáte zásady odchozích připojení k omezení přenosů opouštějících váš server, není potřeba žádná garantovaná služba. Můžete například na serveru vytvořit zásadu QoS, která přidělí jedné aplikaci vyšší prioritu než jiné. Váš server tuto prioritu rozpozná, ale vše mimo server tuto prioritu rozpoznat nemusí. Pokud pracujete v soukromé síti a směrovače jsou konfigurovány, tak, aby rozpoznaly označení identifikačního bodu (používané pro přiřazení úrovně služeb zásadám odchozích připojení), poskytují směrovače prioritu v celé vaší soukromé síti. Pokud však přenosy opustí vaši soukromou síť, neexistuje v tomto ohledu žádná jistota. Bez smlouvy SLA nemáte kontrolu na tím, jak bude síťový hardware s přenosy zacházet. Mimo vaši soukromou síť budete potřebovat smlouvu SLA, aby byla pro provozní třídu či vyhrazení prostředků zaručena příslušná priorita.

Proč potřebujete smlouvu SLA?

Účinnost zásad QoS a rezervací je určena nejslabším spojem sítě. To znamená, že zásady QoS umožňují, aby aplikace obdržely v celé síti určitou prioritu. Jestliže však jeden síťový uzel na trase mezi serverem a klientem není schopen provádět funkce pro zpracování přenosů, které jsou popsány v tématech odlišované služby a integrované služby, zásady QoS nebudou fungovat tak, jak zamýšlíte. Jestliže vám smlouva SLA nezajišťuje dostatek prostředků, ani ty nejlepší zásady QoS vám nepomohou vyřešit problémy se zahlcením sítě.

To se týká také smluv s dalšími poskytovateli služeb sítě Internet (ISP). Každý poskytovatel služeb sítě Internet (ISP) ve všech doménách musí souhlasit, že bude podporovat požadavky na QoS. Schopnost spolupráce systémů může být příčinou problémů.

Ujistěte se, že rozumíte úrovni služeb, která je vám v současné době poskytována. Smlouvy o zpracování provozu konkrétně zahrnují, jak se zachází s přenosy, které jsou uvolněny, označeny, tvarovány nebo znovu odeslány. Hlavním důvodem pro poskytování QoS je možnost řídit latenci, kolísání, šířku pásma, ztrátu paketů, dostupnost a průchodnost. Smlouva SLA musí poskytovat vašim zásadám QoS to, co vyžadují. Ověřte si také, zda máte zajištěn takový rozsah služeb, který skutečně potřebujete. Pokud ne, může docházet k plýtvání s prostředky. Když např. požádáte o rezervaci 500 Kbit/s pro IP telefonii, ale vaše aplikace potřebuje jen 20 Kbit/s, budete platit zbytečně více, aniž byste byli na tuto skutečnost poskytovatelem služeb sítě Internet (ISP) upozorněni.

Poznámka: Zásady QoS vám umožní sjednat s vaším ISP (poskytovatelem služeb sítě Internet) úroveň služeb, což může snížit náklady síťové služby. Váš ISP může být například ochoten poskytnout vám určitou peněžní slevu v případě, že nepřekročíte dohodnutou úroveň šířky pásma. Nebo můžete uvést, že s použitím zásad QoS budete využívat pouze množství "x" šířky pásma během denních hodin a množství "y" šířky pásma v noci a dohodnout se na ceně pro každý časový rámec. A pokud bude tato šířka pásma překročena, může si ISP účtovat více. Bude však třeba, aby ISP souhlasil s určitou úrovní služby a měl možnost sledovat šířku pásma, kterou využíváte.



Síťový hardware a software

Na výsledky QoS mají mimořádný vliv schopnosti vašich interních zařízení a dalších zařízení mimo vaši síť.

Aplikace

Zásady integrovaných služeb QoS vyžadují aplikace umožňující RSVP. Vzhledem k tomu, že aplikace systému iSeriesTM v současné době neumožňují RSVP, musíte zajistit, aby tuto vlastnost získaly. Chcete-li zajistit, aby vaše aplikace podporovaly RSVP, musíte napsat speciální program pomocí rozhraní RAPI (Resource Reservation Setup Protocol) API nebo rozhraní qtoq QoS sockets API. Tyto programy vašim aplikacím umožní, aby používaly protokol RSVP. Další informace najdete v tématu Protokol RSVP a rozhraní QoS API.

Síťové uzly

Směrovače, přepínače a také vaše vlastní servery musí být schopny používat QoS. V případě zásad odlišovaných služeb QoS musí mít síťová zařízení funkce pro odlišované služby. To znamená, že síťový uzel musí být schopen klasifikovat, měřit, označovat, tvarovat a uvolňovat IP pakety. Podrobnější informace o těchto vlastnostech (klasifikace, měření, označování, tvarování a uvolňování) najdete v tématu Faktory přenosů QoS.

Chcete-li používat zásady integrovaných služeb QoS, musí zařízení podporovat protokol RSVP. To znamená, že síťové uzly musí být schopny podporovat protokol RSVP. Podrobnější informace o protokolu RSVP najdete v tématu Protokol RSVP a rozhraní QoS API.

Konfigurování QoS

Poté, co naplánujete použití produktu QoS, vytvoříte zásady QoS prostřednictvím průvodců v prostředí produktu iSeriesTM Navigator. Pomocí průvodců se vám práce zjednoduší, neboť vás provedou celou konfigurací.

Po nakonfigurování zásad QoS můžete pomocí konfiguračních objektů v produktu iSeries Navigator upravovat konfiguraci vašich zásad QoS. Konfigurační objekty jsou různé díly nebo části, které dohromady tvoří zásadu QoS. Když otevřete QoS v prostředí produktu iSeries Navigator, máte zde k dispozici složky označené clients, applications, schedules, policies, classes of service, per-hop behaviors a URI. Tyto objekty vám umožní vytvořit zásadu QoS. Další podrobné informace o těchto objektech najdete v přehledu nápovědy pro QoS v rámci produktu iSeries Navigator.

Konfigurování QoS pomocí průvodců

V tomto tématu najdete popis jednotlivých průvodců pro QoS.

Konfigurování serveru adresářů

Tyto informace použijte pouze v případě, že hodláte data zásad exportovat na server adresářů. Průvodce vám umožní určit který server adresářů použít.

Je-li to nezbytné použijte rozhraní QoS API.

Dle typu zásady QoS, kterou chcete vytvořit, budete možná k realizaci příslušné zásady QoS potřebovat použít rozhraní QoS API.

Aktivace zásad QoS

Dříve, než zásady QoS vstoupí v platnost, musí být aktivovány. Jestliže jste použili průvodce, server zásady QoS aktivuje automaticky. Jestliže jste však některou zásadu QoS změnili pomocí konfiguračních objektů, budete muset dynamicky aktualizovat server, chcete-li zásady aktivovat. Než budete zásady aktivovat, zkontrolujte, zda se některé zásady nepřekrývají, což by mohlo způsobovat problémy. Další informace najdete v tématu Pořadí zásad QoS.

Konfigurování QoS pomocí průvodců



Chcete-li konfigurovat zásady QoS, musíte použít průvodce QoS, kteří se nacházejí v produktu iSeries^(TM) Navigator. Zde je seznam jednotlivých průvodců a popis jejich funkcí:

Průvodce počáteční konfigurací

Pomocí tohoto průvodce nastavujete konfiguraci pro specifický systém a informace pro server adresářů.

Průvodce novou zásadou IntServ

Pomocí tohoto průvodce vytvoříte zásadu integrovaných služeb QoS. Tato zásada povoluje nebo zakazuje žádosti RSVP, což nepřímo řídí šířku pásma serveru. Limity výkonu u dané zásady (které nastavujete) rozhodují, zda server může zpracovat žádost o šířku pásma přicházející z aplikace RSVP klienta. Pro implementaci zásad integrovaných služeb QoS, vytvořených pomocí tohoto průvodce, budete potřebovat směrovače a aplikace podporující RSVP.

Poznámka: Předtím, než budete nastavovat zásadu integrovaných služeb QoS, musíte napsat svoji vlastní aplikaci pro použití protokolu RSVP. Další informace najdete v tématu Rozhraní QoS API.

Průvodce novou zásadou DiffServ

Tento průvodce vám umožní diferencovat provoz TCP/IP a přiřazovat v něm priority. Diferencovat provoz budete schopni tak, že vytvoříte zásady odlišovaných služeb QoS. V rámci této zásady přiřazujete odchozím spojením úroveň služby dle zdrojových/cílových IP adres, portů, aplikací a dokonce i klientů. Ve verzi V5R3 mohou vaše aplikace systému iSeries obdržet úroveň služby dle specifitějších informací aplikací. Předtím, než vytvoříte tuto zásadu, můžete najít více informací v tématu Zásady odlišovaných služeb .

Průvodce novou provozní třídou

Pomocí průvodce pro provozní třídy se nastavuje označování paketů, které pak používají směrovače a přepínače v rámci sítě. Také zde přiřazujete limity výkonu pro přenosy odcházející z vaší sítě. Provozní třídy používáte u zásad odlišovaných služeb a zásad příchozích připojení.

Průvodce povolením nového připojení

Pomocí tohoto průvodce lze omezit spojení přicházející na server. Přístup můžete omezit podle adresy TCP/IP, podle aplikace nebo podle lokálního rozhraní. To administrátorovi systému umožní řídit přístup na váš server dle konkrétních klientů, serverových aplikací nebo dle adresy URI. Navíc tím docílíte zvýšení výkonu serveru.

Poznámka: Dříve, než nastavíte zásadu příchozích připojení využívající adresy URI, se musíte ujistit, že aplikační port přiřazený URI odpovídá direktivě "Listen" aktivované pro FRCA v konfiguraci produktu Apache Web Server. Informace o tom, jak lze změnit nebo zobrazit port HTTP serveru obsahuje téma: Správa adresy a portů pro HTTP server (provozovaný na Apache serveru).

Jakmile se rozhodnete, který typ zásady QoS chcete tvořit, můžete zásadu QoS nakonfigurovat pomocí příslušného průvodce. Chcete-li začít konfigurovat zásadu QoS, přejděte k tématu Přístup k průvodcům QoS v produktu iSeries Navigator.



Přístup k průvodcům QoS v prostředí produktu iSeries Navigator



Chcete-li pracovat s průvodci QoS a vytvořit novou zásadu QoS, postupujte takto:

1. V prostředí produktu iSeriesTM Navigator rozbalte server → **Síť** → **Zásady pro práci s IP**.
2. Klepněte pravým tlačítkem myši na **QoS (Quality of Service)** a poté klepněte na **Konfigurace**.
Poznámka: Za následujících okolností se v tomto okamžiku objeví průvodce počáteční konfigurací:
 - Je to poprvé, co používáte grafické uživatelské rozhraní QoS v tomto systému.
 - Chcete manuálně odstranit nějaké dřívější informace o konfiguraci a znovu začít. K tomu dojde pouze tehdy, když je rozhraní QoS již otevřené.
3. Postupujte v souladu s **průvodcem počáteční konfigurací**. Pokud se průvodce počáteční konfigurací neobjeví, přejděte na krok 4.
4. Vyberte volbu **Zásady**. Klepněte pravým tlačítkem myši buď na volbu **IntServ**, **DiffServ**, nebo **Povolení příchozích připojení**.
5. Vyberte volbu **Nová zásada**.



Konfigurování serveru adresářů

Konfiguraci zásad QoS lze exportovat na server adresářů LDAP. Takto lze vaše řešení QoS učinit z hlediska správy jednodušším. Není třeba konfigurovat zásady QoS na všech serverech, ale uložíte data konfigurace na jednom lokálním serveru adresářů a ostatní systémy je pak mohou sdílet. Když na serveru poprvé konfiguruje QoS, objeví se průvodce počáteční konfigurací. V rámci tohoto průvodce budete konfigurovat také server adresářů.

Při konfigurování serveru adresářů budete potřebovat znát tyto informace, resp. o těchto položkách rozhodnout:

- Jméno serveru adresářů.
- Zjistěte si DN (rozlišovací jméno) pro odkazy na zásady QoS.
- Rozhodněte, zda používat společně se serverem adresářů LDAP zabezpečení SSL.
- Rozhodněte, zda používat klíčová slova, která umožňují snadnější vyhledávání zásad QoS na serveru adresářů.

Poznámka: V současné době nelze jako zásadu autentizace, kterou bude server QoS používat při přístupu k adresáři, nakonfigurovat zásadu Kerberos.

Pro administraci serveru adresářů LDAP musíte mít jednu z následujících kombinací oprávnění:

- oprávnění *ALLOBJ a oprávnění *IOSYSCFG
- oprávnění *JOBCTL a oprávnění k objektu pro příkazy ENDTCP (End TCP/IP), STRTCP (Start TCP/IP), STRTCPSVR (Start TCP/IP Server) a ENDTCPSVR (End TCP/IP Server)
- oprávnění *AUDIT pro konfigurování prověřování zabezpečení OS/400^(R)

Jestliže používáte produkt iSeriesTM Navigator, budete již mít přístup k předvolenému schématu QoS. Umístění souboru s aktuálním schématem na vašem serveru je /QIBM/UserData/OS400/DirSrv. Pokud však používáte jiný editor než produkt iSeries Navigator, budete muset provést import souboru LDIF popsaného níže. Můžete si tento soubor naimportovat také v případě, když po jeho úpravě budete chtít znovu zavést původní předvolený soubor.

Schéma QoS

Sada pravidel, nazývaná schéma, specifikuje, které typy objektů LDAP jsou platné pro server QoS. Toto schéma na obsahuje nezbytná pravidla pro QoS. Pokud však použitý server LDAP není server iSeries, tato pravidla se musí na server LDAP importovat. To se provede pomocí souboru LDIF (LDAP Data Interchange Format). Chcete-li si stáhnout soubor LDIF, použijte odkaz na webovou stránku iSeries LDAP



. Soubor najdete v rámci menu **Kategorie** → **Zásady TCP/IP** v levém podokně. Vzorové schéma QoS najdete v tématu Koncepce serveru adresářů.

Pořadí zásad QoS



Kdykoliv máte dvě zásady, které se překrývají, bude mít význam pořadí těchto zásad v prostředí produktu iSeries^(TM) Navigator. Zásady QoS se překrývají, pokud používají stejného klienta, aplikaci, časový plán, lokální IP adresu nebo protokol. Zásady QoS jsou na obrazovce produktu iSeries Navigator seřazeny v seznamu. Přednost zásad závisí na jejich pořadí v tomto seznamu. Jestliže chcete, aby měla určitá zásada QoS přednost před jinou, musí se zásada s vyšší prioritou uvést do seznamu výše.

Chcete-li zjistit, zda se určitá zásada QoS překrývá s jinou zásadou QoS, postupujte takto:

1. V prostředí produktu iSeries Navigator rozbalte **Server** → **Síť** → **Zásady pro práci s IP**.
2. Klepněte pravým tlačítkem myši na volbu **Quality of Service**.
3. Vyberte volbu **Configuration**.
4. Vyberte konkrétní složku zásady.
5. Klepněte pravým tlačítkem myši na zásadu QoS, která má přiřazeny překrývající se zásady QoS. Překrývající se zásady QoS mají u svého jména ikonu, která naznačuje překrývání.
6. Vyberte volbu **Zobrazit překryv**. Zobrazí se panel s informacemi o překrývání.

Chcete-li změnit pořadí zásad QoS, postupujte takto:

- Zvýrazněte zásadu QoS a pomocí šipky nahoru a šipky dolů na obrazovce změňte pořadí zásad QoS.
- Klepněte pravým tlačítkem myši na jméno zásady QoS a vyberte volbu **Move up** nebo **Move down**.
- Aktualizujte server QoS. Můžete použít tlačítko Update server na panelu nástrojů nebo si najdete podrobnější instrukce v nápovědě pro QoS.



Správa QoS

Poté, co budou zásady QoS vytvořené a aktivní, je pravděpodobné, že budete potřebovat provádět aktualizace. Správu QoS můžete provádět pomocí následujících činností:

Přístup k nápovědě pro QoS v prostředí produktu iSeries Navigator

Zřejmě jste si všimli, že se v tomto tématu často odkazuje na nápovědu pro QoS v prostředí produktu iSeries™ Navigator. Pokud si nejste jisti, jak se k nápovědě dostat, zde najdete pokyny.

Zálohování zásad QoS

Vytvořené zásady QoS můžete zálohovat, a chránit se tak pro případ ztráty souborů.

Kopírování existující zásady QoS

Chcete-li vytvořit zásadu QoS, která se podobá nějaké existující zásadě, můžete si tuto zásadu QoS zkopírovat.

Dynamická aktualizace zásad QoS

Zásady můžete dynamicky aktualizovat, zatímco je server spuštěný. Podrobné pokyny najdete v tématu *Aktualizace serveru QoS* v rámci nápovědy pro QoS v prostředí produktu iSeries Navigator.

Úprava zásad QoS

Můžete změnit parametry existujících zásad QoS.

Úprava vlastností konfigurace QoS

Můžete změnit vlastnosti konfigurace zásad QoS. Tyto vlastnosti zahrnují nastavení pro konfiguraci serveru adresářů, pro žurnálování a pro automatické spuštění serveru. Podrobné pokyny najdete v tématu *Úprava vlastností QoS* v nápovědě pro QoS v prostředí produktu iSeries Navigator.

zásad QoS

Pokud se rozhodnete použít průvodce, je zásada aktivována automaticky. Je však třeba aktualizovat server, aby zásada začala účinkovat. Ověřte, že server QoS aktivní a případně jej aktualizujte. Nezapomeňte manuálně zkontrolovat případné chyby. Například se ujistěte, že jsou zásady QoS ve správném pořadí. Další informace o pořadí zásad QoS najdete v tématu *Pořadí zásad QoS*. Jinak najdete podrobné pokyny v tématu *Umožnění zásad QoS* v nápovědě pro QoS v prostředí produktu iSeries Navigator.

Monitorování zásad QoS

Při správě zásad QoS může být užitečné analyzovat zásady pomocí funkce Monitorování QoS a ověřit, zda zásady QoS fungují tak, jak jste zamýšleli.

Prohlížení překrývajících se zásad QoS

Při prohlížení zásad QoS, které se překrývají, můžete určit, kde mohou nastat jiné výsledky, než očekáváte. Můžete zkontrolovat všechna patrná překrytí mezi zásadami, která mohou způsobovat problém. Tato překrytí je vhodné si prohlédnout nejen před aktivací a testováním zásad QoS, ale také před tiskem a zálohováním. Je to užitečný způsob, jak minimalizovat nebo odstranit chyby před testováním. Informace o tom, jak si můžete prohlédnout překrývající se zásady QoS najdete v tématu *Pořadí zásad QoS*.

Přístup k nápovědě pro QoS v prostředí produktu iSeries Navigator

Chcete-li použít nápovědu pro QoS, postupujte v prostředí produktu iSeries™ Navigator takto :

1. V prostředí produktu iSeries Navigator rozbalte **Server** → **Síť** → **Zásady pro práci s IP**.
2. Klepněte pravým tlačítkem myši na **QoS (Quality of Service)** a poté klepněte na **Konfigurace**.
3. Vyberte z pruhu nabídky volbu **Nápověda** → **Témata nápovědy**. Na obrazovce se otevře okno s nápovědou.

Zálohování zásad QoS

Zálohování konfiguračních souborů je rozhodně dobrým nápadem. Zásady QoS mohou být uloženy lokálně nebo je lze exportovat na server adresářů. Speciálně musíte zálohovat tyto adresáře integrovaného systému souborů:

QIBM/UserData/OS400/QOS/ETC, QIBM/UserData/OS400/QOS/TEMP

a QIBM/UserData/OS400/QOS/USR. Také je třeba, aby byl pro server QoS zálohován publishing agent serveru QoS. Publishing agent obsahuje jméno serveru adresářů, rozlišovací jméno (DN) serveru QoS, port používaný pro přístup k serveru adresářů a autentizační informace. V případě ztráty vám tyto zálohy mohou ušetřit čas a práci nutné pro opětovné vytváření zásad QoS úplně od začátku. Toto jsou obecné rady, pomocí kterých si zajistíte, že budete moci snadno nahradit ztracené soubory.

1. **Používejte programy pro zálohování a obnovu integrovaného systému souborů.**

Použijte odkaz na publikaci *Zálohování a obnova* uvedený níže.

2. Vytiskněte si zásady QoS.

Výpisy konfigurací si můžete uložit kdekoliv, kde budou zabezpečené, a v případě potřeby informace podle nich znovu zadat.

3. Zkopírujte si informace na disk.

Zkopírování má oproti vytištění výhodu: informace nemusíte znovu zadávat manuálně, neboť je máte k dispozici v elektronické podobě. Poskytuje vám to přímočarou metodu pro přenos informací z jednoho online zdroje na jiný.

Poznámka: Server iSeriesTM kopíruje informace na systémový disk, nikoliv na disketu. Soubory s pravidly jsou v adresáři QIBM/UserData/OS400/QOS/ETC a také v rámci rozlišovacího jména na serveru adresářů, které jste konfigurovali, nikoliv na osobním počítači. Je také možno použít zásadu pro ochranu disku jako podpůrný prostředek ochrany dat, která jsou uložena na systémovém disku.

Při používání serveru iSeries musíte naplánovat strategii pro zálohování a obnovu. Další podrobné informace obsahuje publikace Zálohování a obnova



Kopírování existující zásady QoS

Můžete zjistit, že máte v plánu vytvořit několik zásad QoS, které se navzájem velmi podobají. Abyste nemuseli každou z nich tvořit úplně od začátku, existuje možnost vytvořit kopie jedné původní zásady QoS, a pak upravit pouze ty části nové zásady, které se od původní zásady odlišují. V prostředí produktu iSeriesTM Navigator se tato funkce QoS nazývá *New based on*. Chcete-li pracovat s dialogovým oknem QoS, kde budete moci kopírovat zásady, musíte použít produkt iSeries Navigator.

Chcete-li vytvořit kopii existující zásady QoS, postupujte podle pokynů v hesle nápovědy **Create a new policy based on an existing policy** v prostředí produktu iSeries Navigator.

Předtím, než mohou zásady QoS začít účinkovat, musíte je aktivovat, a to tak, že spustíte server QoS nebo provedete dynamickou aktualizaci serveru. Než budete zásady aktivovat, zkontrolujte, zda se některé zásady nepřekrývají, což by mohlo způsobovat problémy. Další informace najdete v tématu Pořadí zásad QoS.

Úprava zásad QoS

S tím, jak se vaše potřeby mění, je nutno zásady QoS upravovat, abyste zajistili odpovídající výkon sítě. Před aktivací zásad byste se měli pokusit opravit všechny chyby a provést potřebné změny v zásadách QoS. To je nejlepší způsob, jak se vyhnout komplikacím s výsledky používaných zásad QoS.

Poté, co nakonfigurujete zásady QoS, můžete pomocí konfiguračních objektů v produktu iSeriesTM Navigator upravovat konfiguraci vašich zásad QoS. Konfigurační objekty jsou různé díly nebo části, které dohromady tvoří zásadu QoS. Když otevřete QoS v prostředí produktu iSeries Navigator, máte zde k dispozici složky označené clients, applications, schedules, policies, classes of service, per-hop behaviors a URI. Tyto objekty vám umožní upravovat zásadu QoS.

Chcete-li upravit zásadu QoS v prostředí produktu iSeries Navigator, postupujte podle pokynů na stránce **Úprava zásady QoS** v rámci nápovědy produktu iSeries Navigator.

Monitorování QoS



Pomocí funkce Monitorování QoS můžete analyzovat provoz IP procházející přes váš server. To vám pomůže určit, kde v síti dochází k zahlcení. Tato funkce není užitečná jen ve fázi plánování QoS, je to také účinný nástroj pro odstraňování problémů. Pomocí funkce Monitorování QoS budete schopni průběžně monitorovat vaši síť a přizpůsobit

podle potřeby zásady QoS. Chcete-li monitorovat všechny aktivní zásady, vyberte v okně Konfigurace serveru QoS volbu **Server**—>**Monitor**. Pokud klepněte pravým tlačítkem myši na určitou zásadu a zvolíte volbu **Monitor**, zobrazí se informace monitorování pouze pro příslušnou zásadu.

Monitorování zásad můžete provést těmito způsoby:

- **Prohlížet data o aktivních zásadách v reálném čase**
Pokud spustíte funkci monitorování, jsou vždy zobrazena data o aktivních zásadách v reálném čase. Není nutné spouštět kolekci dat.
- **Shromažďovat a ukládat data za určité časové období**
Pokud chcete uložit výsledky monitorování, musíte spustit kolekci dat QoS. Monitorování pokračuje ve sběru dat do té doby, než kolekci ukončíte. Pokud zavřete okno monitorování, kolekce dat se nezastaví. Můžete také změnit vlastnosti, které funkce monitorování používá během kolekce dat. Chcete-li změnit vaše volby, zvýrazněte v okně Monitor QoS volbu *Monitorování QoS* a vyberte *Soubor*—>*Vlastnosti*. Další informace najdete v online nápovědě.
Pokud je zapnutá funkce kolekce dat QoS a jsou změněny vlastnosti monitorování, musíte provést tyto kroky, chcete-li zajistit, že budou změny v kolekci dat zohledněny.
 1. Ukončete kolekci dat QoS.
 2. Změňte vlastnosti monitorování.
 - a. V okně Monitor klepněte na volbu **Monitorování QoS**.
 - b. Vyberte **Soubor**—>**Vlastnosti**.
 - c. Změňte vlastnosti monitorování a klepněte na **OK**.
 3. Aktualizujte server QoS.
 4. Spusťte funkci kolekce dat QoS.

Výstup monitorování

Výstupní informace, které dostanete, budou záviset na typu zásady QoS, kterou jste monitorovali. Připomeňte si základní typy zásad QoS: zásady odlišovaných služeb (DiffServ), zásady integrovaných služeb - služby řízeného zavádění (IntServ - Controlled Load), zásady integrovaných služeb - garantované služby (IntServ - Guaranteed) a zásady příchozích připojení. Pole, která je potřeba hodnotit, závisí na typu zásady QoS. Nejzajímavější údaje jsou v polích udávajících výsledky měření. Tato pole obsahují výsledky měření, nikoliv definované údaje: přijaté požadavky, aktivní připojení, služby připojení, počet připojení, uvolněné požadavky, vyhovující pakety, vyhovující bity, bity mimo profil, celkový počet bitů, celkový počet paketů a celkový počet požadavků.

Na základě informací uvedených v polích s výsledky měření si budete schopni udělat dobrý obrázek o tom, jak síťový provoz vyhovuje vašim zásadám QoS. V následujících přehledech jsou uvedeny podrobnější informace o výstupních polích monitorování pro jednotlivé typy zásad. Konkrétní příklady použití funkce Monitorování QoS pro různé zásady najdete v tématu Scénáře QoS.

- zásady odlišovaných služeb QoS (Viz 51)
- zásady integrovaných služeb QoS - služby řízeného zavádění (Viz 52)
- zásady integrovaných služeb QoS - garantované služby (Viz 53)
- zásady příchozích připojení (Viz 54)

Zásady odlišovaných služeb QoS

Pole	Popis
Policy name	Jméno, které jste přiřadili této zásadě QoS.
Protocol	Protokol UDP, TCP, ALL.
Average token rate limit	Průměrná přenosová rychlost tokenů povolená touto zásadou QoS v každém směrovači a serveru na trase přenosu.
Token depth limit	Maximální velikost vyrovnávací paměti tokenů povolená touto zásadou QoS v každém směrovači a serveru na trase přenosu.
Peak token rate limit	Maximální přenosová rychlost povolená pro dané spojení.

Pole	Popis
Packets in-profile	Počet přenesených IP paketů, které vyhovovaly parametrům dané zásady QoS.
Bits in-profile	Počet přenesených bitů, které vyhovovaly parametrům dané zásady QoS.
Bits out-of-profile	Počet přenesených bitů, které přesáhly parametry dané zásady QoS.
Bits rate	Naměřený počet bitů povolených pro toto spojení.
Active connections	Celkový počet aktivních spojení.
Traffic profile	Typ zpracování paketů použitý pro pakety mimo profil. Formát může být tento: <ul style="list-style-type: none"> • Nové označení • Tvarování • Uvolnění
Bits total	Počet přenesených bitů použitých touto zásadou QoS od okamžiku, kdy byla spuštěna, do okamžiku výstupu monitorování.
Codepoint in-profile	Jestliže je paket opětovně označen novým identifikačním bodem, bude tento identifikační bod použitý, pokud bude IP paket vyhovovat parametrům dané zásady QoS.
Codepoint out-of-profile	Jestliže se pakety označují novým identifikačním bodem, bude tento identifikační bod použit, pokud IP paket přesáhne parametry dané zásady QoS.
Destination address range	Rozsah adres, který určuje místo určení paketů (řízených touto zásadou QoS).
Packet total	Počet paketů přenesených podle této zásady QoS od okamžiku, kdy byla spuštěna, do okamžiku výstupu monitorování.
Source port range	Rozsah zdrojových portů, který určuje, které aplikace jsou řízeny touto zásadou QoS.

Zásady integrovaných služeb QoS - služby řízeného zavádění

Poznámka: Zásady integrovaných služeb QoS se při použití funkce monitor nezobrazí, dokud nejsou spuštěné příslušné aplikace a dokud nejsou vytvořeny rezervace. Pokud vytváří zásady integrovaných služeb více než jednu rezervaci, zobrazí se ve funkci monitor více záznamů.

Pole	Popis
Policy name	Jméno, které jste přiřadili této zásadě QoS.
Protocol	Protokol UDP nebo TCP
Destination address	Rozsah adres, který určuje místo určení paketů (řízených touto zásadou QoS).
Average token rate limit	Průměrná přenosová rychlost tokenů povolená touto zásadou QoS v každém směrovači a serveru na trase spojení.
Token depth limit	Maximální velikost vyrovnávací paměti tokenů povolená touto zásadou QoS v každém směrovači a serveru na trase spojení.
Peak token rate limit	Maximální přenosová rychlost povolená pro dané spojení.
Packet total	Počet paketů přenesených podle této zásady QoS od okamžiku, kdy byla spuštěna, do okamžiku výstupu monitorování.

Pole	Popis
Bits out-of-profile	Počet přenesených bitů, které přesáhly parametry dané zásady QoS.
Bits total	Počet přenesených bitů použitých touto zásadou QoS od okamžiku, kdy byla spuštěna, do okamžiku výstupu monitorování.
Bit rate	Naměřený počet bitů povolených pro toto spojení.
Bits in-profile	Počet přenesených bitů, které vyhovovaly parametrům dané zásady QoS.
Maximum packet size	Maximální povolená velikost paketů řízená touto zásadou QoS.
Minimum policed unit	Nejmenší počet bitů, který bude odcházet ze sektoru token. Jestliže je, například, hodnota tohoto parametru 100 bitů, budou pakety menší než 100 bitů stejně odcházet při 100 bitech.
Packets in-profile	Počet přenesených IP paketů, které vyhovovaly parametrům dané zásady QoS.
Source port range	Rozsah zdrojových portů, který určuje, které aplikace jsou řízeny touto zásadou QoS.

Zásady integrovaných služeb QoS - garantované služby

Poznámka: Zásady integrovaných služeb QoS se při použití funkce monitor nezobrazí, dokud nejsou spuštěné příslušné aplikace a dokud nejsou vytvořeny rezervace. Pokud vytváří zásady integrovaných služeb více než jednu rezervaci, zobrazí se ve funkci monitor více záznamů.

Pole	Popis
Policy name	Jméno, které jste přiřadili této zásadě QoS.
Protocol	Protokol UDP nebo TCP
Destination address	Rozsah adres, který určuje místo určení paketů (řízených touto zásadou QoS).
Average token rate limit	Maximální přenosová rychlost tokenů povolená touto zásadou QoS v každém směrovači a serveru na trase spojení.
Token depth limit	Maximální velikost vyrovnávací paměti tokenů povolená touto zásadou QoS v každém směrovači a serveru na trase spojení.
Peak token rate limit	Maximální přenosová rychlost povolená pro dané spojení.
Packet total	Počet paketů přenesených podle této zásady QoS od okamžiku, kdy byla spuštěna, do okamžiku výstupu monitorování.
Bits total	Počet přenesených bitů použitých touto zásadou QoS od okamžiku, kdy byla spuštěna, do okamžiku výstupu monitorování.
Bits out-of-profile	Počet přenesených bitů, které přesáhly parametry dané zásady QoS.
Guaranteed rate	Garantovaná přenosová rychlost v bitech za vteřinu.
Bits in-profile	Počet přenesených bitů, které vyhovovaly parametrům dané zásady QoS.
Maximum packet size	Maximální povolená velikost paketů řízená touto zásadou QoS.
Minimum policed units	Nejmenší počet bitů, který bude odcházet ze sektoru token. Jestliže je, například, hodnota tohoto parametru 100 bitů, budou pakety menší než 100 bitů stejně odcházet při 100 bitech.

Pole	Popis
Packets in-profile	Počet přenesených IP paketů, které vyhovovaly parametrům dané zásady QoS.
Slack term	Rozdíl (ve vteřinách) mezi požadovaným zpožděním a získaným zpožděním.
Source port range	Rozsah zdrojových portů, který určuje, které aplikace jsou řízeny touto zásadou QoS.

Zásady příchozích připojení

Pole	Popis
Policy name	Jméno, které jste přiřadili této zásadě QoS.
Connection rate	Počet žádostí o připojení přijatých za vteřinu.
Total requests	Celkový počet žádostí o připojení směřovaných na tento server.
Accepted requests	Celkový počet žádostí o připojení přijatých tímto serverem.
Dropped requests	Celkový počet žádostí, které server uvolnil.
Average connection rate limit	Průměrný přípustný počet nových žádostí o připojení přijatý za vteřinu.
Connection burst limit	Maximální počet nových žádostí o připojení přijatých současně.
Peak connection rate limit	Maximální přípustná přenosová rychlost, kterou server přijímá připojení ze sítě.
Priority	Priorita přiřazená každému pravidlu zavedenému do funkce QoS Manager.
Queue Priority	Priorita přiřazená příchozím připojením umístěným do fronty.
Destination port range	Rozsah portů nebo port, kterému je určen příchozí provoz na vašem serveru.
Interface address	IP adresa systémového rozhraní, které se monitoruje.
Source address range	Rozsah IP adres klientů odesílajících žádosti na váš server.
URI	Identita URI, které je předmětem zásady QoS.



Odstraňování problémů v QoS

V tomto tématu jsou uvedeny rady pro odstraňování problémů v QoS.

Sledování komunikace

Váš server provádí sledování komunikace prostřednictvím sběru dat na určité komunikační lince, jako je např. rozhraní sítě LAN nebo sítě WAN. Průměrný uživatel nemusí rozumět celému obsahu výsledných dat sledování. Můžete však na základě výsledků sledování určit, zda mezi dvěma body skutečně proběhla výměna dat. Další informace najdete v části Trasování komunikací v rámci tématu Odstraňování problémů s TCP/IP.

Aktivace QoS na serveru

První věcí, kterou byste měli zkontrolovat, pokud se server QoS nespustí, je, zda je QoS na serveru povolený. Když poprvé konfigurujete zásady QoS, průvodce počáteční konfigurací automaticky zaktivuje QoS na serveru. Jestliže však byla tato hodnota z nějakého důvodu změněna, server se nespustí.

Chcete-li ověřit, zda je QoS na serveru povolený, postupujte takto:

1. V prostředí produktu iSeries^(TM) Navigator rozbalte svůj server → **Síť** → **Zásady pro práci s IP**.
2. Klepněte pravým tlačítkem myši na **Quality of service** a vyberte volbu **Configuration**.
3. Po zobrazení rozhraní produktu QoS klepněte pravým tlačítkem myši na volbu **QoS** a vyberte volbu **Properties**.
4. Na stránce vlastností QoS ověřte, že je vybrána volba **Enable QoS**.

Žurnálování zásad QoS

Funkce QoS zahrnuje také funkci pro žurnálování. Pomocí žurnálování můžete protokolovat přidávání, odstraňování nebo modifikaci zásad pro práci IP na vašem serveru. To vám umožní ladit zásady QoS, namátkově je kontrolovat a ověřovat, zda zásady QoS fungují tak, jak jste zamýšleli.

Protokolování zásad QoS

Když narazíte na problém se serverem, může být užitečné analyzovat protokoly úloh.

Monitorování transakcí serveru

Funkci Monitorování QoS použijte jako první krok při zjišťování a odstraňování problémů s QoS. Funkce zaznamenává a zobrazuje informace o provádění QoS.

Sledování aplikací TCP

Příkaz sledování použijete k tomu, abyste protokolovali několik úrovní akcí serveru. Může to být užitečné, když se snažíte určit problémy se zásadami QoS.

Pořadí zásad QoS

Pořadí zásad QoS v souboru je velmi důležité pro úspěch implementace QoS.

Žurnálování zásad QoS

Funkce QoS zahrnuje funkci pro žurnálování. Žurnálování vám umožňuje sledovat operace se zásadami QoS, jako např. přidávání, odstraňování nebo modifikaci zásad QoS. Po dobu, kdy máte žurnálování nastaveno na ON, vytváří žurnálování protokol operací se zásadami QoS. To vám pomůže při zjišťování, kde zásady nefungují tak, jak jste očekávali. Nastavíte například, aby byla zásada spuštěna v době od 9:00 AM do 4:00 PM. V protokolu žurnálu můžete zkontrolovat, zda zásada QoS byla přidána v 9:00 AM a odstraněna v 4:00 PM.

Jestliže je žurnálování zapnuto, záznamy žurnálu se generují pokaždé, když je nějaká zásada QoS přidána, odstraněna nebo modifikována. Pomocí těchto žurnálů vytvoříte obecný soubor na serveru iSeries^(TM). Následně můžete pomocí informací zaznamenaných v žurnálech systému zjistit, jak je systém využíván. To vám pomůže při rozhodování o změnách různých aspektů vašich zásad QoS.

Pečlivě vybírejte, co všechno budete žurnálovat. Žurnálování může představovat velkou zátěž pro prostředky vašeho systému. Spuštění a ukončení žurnálování provádíte v prostředí produktu iSeries Navigator. Chcete-li prohlížet protokoly žurnálu, musíte použít znakově orientované rozhraní.

Chcete-li spustit nebo ukončit žurnálování, postupujte takto:

1. V prostředí produktu iSeries Navigator rozbalte **Server** → **Síť** → **Zásady pro práci s IP**.
2. Klepněte pravým tlačítkem myši na **Quality of Service** a vyberte volbu **Konfigurace**.
3. Klepněte pravým tlačítkem myši na volbu **QoS** a vyberte volbu **Vlastnosti**.

4. Vyberte rámeček **Spustit žurnálování**, chcete-li, aby se zapnulo žurnálování.
5. Zrušte označení rámečku **Spustit žurnálování**, chcete-li vypnout žurnálování.

Upozornění: Jestliže v době, kdy provádíte tyto kroky, je již server spuštěný, musíte server ukončit a restartovat. Jakmile je žurnálování zapnuto, máte k dispozici dva způsoby, jak jej aktivovat. Buď můžete server ukončit a restartovat, nebo můžete provést aktualizaci serveru. Při obou způsobech se znovu načte soubor `policy.conf` a zkontroluje se atribut žurnálování.

Prohlížení záznamů žurnálu na obrazovce

Chcete-li si prohlížet záznamy žurnálu na obrazovce, postupujte takto:

1. Na příkazovém řádku na serveru iSeries zadejte: `DSPJRN JRN(QUSRSYS/QQOS)`. Vyberte **volbu 5** u záznamu žurnálu, který chcete prohlížet.

Prohlížení záznamů žurnálu prostřednictvím výstupního souboru

Jestliže byste chtěli vidět záznamy žurnálu formátované do jedné složky, prohlédněte si soubor `MODEL.OUT` v adresáři `QUSRSYS`. Jestliže zkopírujete záznamy žurnálu do výstupního souboru, budete moci záznamy snadno prohlížet pomocí dotazovacího obslužného programu, jako je `Query/400` nebo `SQL`. Můžete si také napsat vlastní program `HLL`, který bude zpracovávat záznamy ve výstupním souboru.

Chcete-li zkopírovat záznamy žurnálu QoS do systémem dodávaného výstupního souboru, postupujte takto:

1. Vytvořte kopii systémem dodávaného výstupního souboru `QSYS/QATOQQOS` do uživatelské knihovny. Můžete to provést pomocí příkazu `CRTDUPOBJ` (Create Duplicate Object). Zde je příklad příkazu `CRTDUPOBJ`:
`CRTDUPOBJ OBJ(QADSPJR4) FROMLIB(Qsys) OBJTYPE(*FILE) TOLIB(userlib) NEWOBJ(userfile)`
2. Pomocí příkazu `DSPJRN` (Display Journal) zkopírujete záznamy žurnálu `QUSRSYS/QQOS` do výstupního souboru vytvořeného v předchozím kroku. Jestliže se pokusíte zkopírovat žurnál pomocí příkazu `DSPJRN` do výstupního souboru, který neexistuje, systém soubor vytvoří, ale tento soubor nebude obsahovat správné popisy polí.
 - a. `DSPJRN JRN(QUSRSYS/QQOS) JRNCDE((M)) ENTCTYP(MP) CMTCTYCID(*ALL) OUTPUT(*OUTFILE) OUTFILFMT(*TYPE4) OUTFILE(userlib/userfile)`
 - b. `DSPF FILE(userlib/userfile)`

Protokolování úloh serveru QoS

Pokud narazíte na problém se zásadami QoS, analyzujte protokoly úloh serveru iSeries™. Protokol úloh obsahuje chybové zprávy a další informace související s QoS.

Pouze jedna úloha QoS, `QTOQSRVR`, běží v subsystému `QSYSWRK`. Staré i aktuální protokoly úloh serveru QoS můžete prohlížet z produktu iSeries Navigator.

Chcete-li prohlížet protokol, postupujte takto:

1. Rozbalte **Síť** a klepněte na volbu **Zásady pro práci s IP**.
2. Klepněte pravým tlačítkem myši na volbu **Quality of Service**.
3. Vyberte volbu **Diagnostic tools** —> **QoS Server Log**.

Otevře se okno, ve kterém můžete pracovat s úlohou.

V následujícím seznamu jsou jména nejdůležitější úloh se stručným popisem, k čemu se úlohy používají.

QTCP

Tato úloha je základní úloha, která spouští všechna rozhraní TCP/IP. Jestliže máte závažné problémy s TCP/IP obecně, analyzujte protokol úlohy QTCPIP.

QTOQSRVR

Tato úloha je základní úloha QoS, která vám poskytne protokol informací specifických pro QoS. Spusťte příkaz WRKSPLF QTCP (Práce se souborem pro souběžný tisk) a hledejte záznam QTOQSRVR.

Chcete-li zkontrolovat pracovní soubor pro souběžné zpracování, abyste našli chyby, postupujte takto:

1. Z rozhraní příkazového řádku zadejte **WRKSPLF QTCP** a stiskněte klávesu **Enter**.
2. Objeví se okno Práce se všemi soubory pro souběžný tisk. Ve sloupci User Data vyhledejte řádek QTOQSRVR, abyste zjistili chyby týkající se speciálně serveru QoS.
3. Vyberte volbu **Option 5** pro řádek, který chcete zobrazit. Pročtete si informace a poznamenejte si ID zprávy, která vysvětluje daný problém. Například TCP920C.
4. Stiskněte dvakrát klávesu **F3** a vrátíte se do hlavního menu.
5. Z rozhraní příkazového řádku zadejte **WRKMSGF** a stiskněte klávesu **Enter**.
6. Na obrazovce Work with Message File zadejte následující informace a stiskněte klávesu **Enter**.
Message File: QTCPPMSG
Library: *LIBL
7. Na obrazovce Work with Message File vyberte volbu **option 5**, abyste zobrazili soubor zprávy, který chcete prohlížet, a stiskněte klávesu **Enter**.
8. Na obrazovce Display Message Descriptions zadejte následující informace:
Position to: zadejte ID zprávy z kroku 3 výše a stiskněte klávesu **Enter**. Například TCP920C.
9. Vyberte volbu **Option 5** pro požadované ID zprávy a stiskněte klávesu **Enter**.
10. V okně Select message details to display vyberte 30 (All of the Above) a stiskněte klávesu **Enter**.
11. Objeví se podrobný popis zprávy.

Monitorování transakcí serveru

Funkce Monitorování QoS vám pomůže nejen ve fázi plánování QoS, ale také ve fázi odstraňování problémů s QoS.

Pomocí funkce Monitorování QoS můžete analyzovat provoz IP procházející přes váš server. To vám pomůže určit, kde v síti dochází k zahlcení. Pomocí funkce Monitorování QoS budete schopni průběžně monitorovat vaši síť a přizpůsobit podle potřeby zásady QoS.

Plánování a udržování výkonu

Jednou z nejobtížnějších částí implementace QoS je určení toho, jaké limity výkonu se mají nastavit v rámci zásad QoS. V tomto ohledu neexistuje nějaké univerzální doporučení. Chcete-li zjistit, jaké hodnoty parametrů budou ve vašich podmínkách vhodné, bude pro vás užitečné použít funkci Monitorování QoS předtím, než nějakou zásadu QoS v praxi spustíte.

Pokuste se vytvořit zásadu odlišovaných služeb, aniž byste vybrali provádění měření za účelem zjištění chování aktuálního provozu v síti. Aktivujte tuto zásadu QoS a spusťte funkci Monitorování QoS. Na základě výsledků monitorování budete schopni upravit zásady QoS podle vašich specifických potřeb. Vyzkoušejte si vzorovou zásadu QoS, pomocí které zjistíte, jak se chová váš současný síťový provoz.

Odstraňování problémů s výkonem zásad QoS

Funkci Monitorování QoS můžete využít také při odstraňování problémů. Na základě výsledků monitorování můžete určit, zda se parametry, které jste k určité zásadě QoS přiřadili, dodržují. Pokud se zásady zobrazují v monitoru, ale zdá se, že neovlivňují přenosy, ověřte toto:

- Pokud zásada provádí filtrování dle URI, ověřte, že je FRCA je v aktivním a nakonfigurovaném stavu. Dříve, než nastavíte zásadu příchozích připojení využívající adresy URI, se musíte ujistit, že aplikační port přiřazený URI

odpovídá direktivě "Listen" aktivované pro FRCA v konfiguraci produktu Apache Web Server. Informace o tom, jak lze změnit nebo zobrazit port HTTP serveru obsahuje téma: Správa adres a portů pro HTTP server (provozovaný na Apache serveru).

- Ověřte plán zásady. Možná, že očekáváte výsledky v době neaktivity.
- Ověřte, že číslo portu je správné.
- Ověřte, že IP adresa je správná.

Příklady výsledků monitorování najdete v tématu Scénáře QoS, přehled a popis všech polí monitorování najdete v tématu Monitorování QoS.

Monitorování aktuálního stavu sítě



Cíl

V rámci práce s průvodci QoS nastavujete určité limity výkonu. Jsou to parametry, jejichž hodnoty nelze doporučit, neboť jsou založeny na požadavcích konkrétní sítě. Při nastavování těchto limitů musíte velmi dobře znát aktuální výkon sítě. Vzhledem k tomu, že hodláte konfigurovat zásady QoS, pravděpodobně již máte určitou představu o vašich současných síťových potřebách. Chcete-li určit přesné limity výkonu, jako je např. přenosová rychlost sektoru token, bude užitečné provést monitorování pro veškerý provoz na serveru, abyste mohli lépe určit, jaké limity nastavit.

Řešení

Vytvořte velmi širokou zásadu odlišovaných služeb QoS, která neobsahuje žádná omezení (žádné maximální hodnoty) a týká se všech rozhraní a všech IP adres. Pak pomocí funkce Monitorování QoS zaznamenejte data pro tuto zásadu QoS.

Krok 1: Otevřete QoS v rámci produktu iSeriesTM Navigator.

1. V prostředí produktu iSeries Navigator rozbalte Server → Síť → Zásady pro práci s IP.
2. Klepněte pravým tlačítkem myši na **Quality of Service** a vyberte volbu **Configuration**.
3. Rozbalte menu **Šířka pásma odchozích přenosů**.
4. Klepněte pravým tlačítkem myši na volbu **DiffServ** a vyberte volbu **Nová zásada**. Objeví se průvodce novou zásadou QoS.

Krok 2: Vytvořte zásadu odlišovaných služeb QoS.

Vzhledem k tomu, že chcete zahrnout co nejvíce provozu vstupujícího do vaší sítě, můžete zásadu nazvat např. **Network**. Použijte všechny IP adresy, všechny porty, všechny lokální IP adresy, a celý časový rozsah (je-li to vhodné). Při práci s průvodcem zadejte tato nastavení:

Jméno = Network (může to být jakékoliv jméno, které přiřadíte)

Klient = Všechny IP adresy

Aplikace = Všechny porty

Protokol = Všechny protokoly

Plán = Vždy

Produkt iSeries Navigator zobrazí všechny zásady odlišovaných služeb QoS, které jsou na vašem serveru vytvořeny.

Krok 3: Vytvořte novou provozní třídu.

Při práci s průvodcem jste vyzváni, abyste přiřadili typ chování při jednotlivých přechodech, limity výkonu a zacházení s přenosů mimo profil. Tyto parametry definují provozní třídu. Zvolte extrémně vysoké hodnoty, abyste povolili co nejvíce toků přenosu.

Provozní třídy vlastně určují úroveň výkonu, který daný přenos obdrží od směrovače. Provozní třídu můžete nazvat např. **Unlimited**, abyste naznačili, že tento přenos obdrží nejvyšší úroveň služeb. Produkt iSeries Navigator zobrazí všechny provozní třídy, které jsou na vašem serveru vytvořeny.

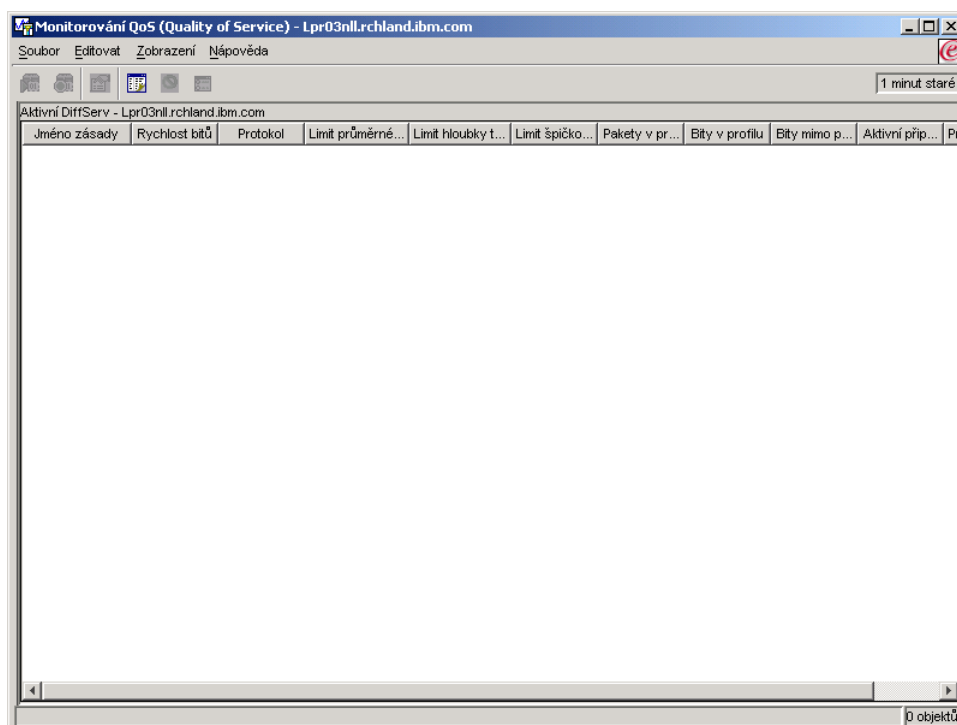
Krok 4: Proveďte monitorování vytvořené zásady QoS.

Chcete-li ověřit, že se provoz chová tak, jak jste nakonfigurovali v rámci zásady QoS, použijte funkci Monitorování QoS.

1. Vyberte příslušnou složku zásady (DiffServ, IntServ, povolení příchozích připojení).
2. Klepněte pravým tlačítkem myši na zásadu QoS, kterou chcete monitorovat, a vyberte volbu **Monitor**.

Níže je uveden příklad možného výstupu monitorování pro výše popsanou zásadu QoS.

Obrázek 14. Monitorování QoS.



Vyhledejte pole, která obsahují data o provozu. Zkontrolujte zejména pole total bits (počet bitů celkem), bits in-profile (počet vyhovujících bitů), packets in-profile (počet vyhovujících paketů) a bits out-of-profile (počet nevyhovujících bitů). Pole Počet bitů mimo profil označuje část přenosů, která přesahuje nakonfigurované hodnoty dané zásady QoS. U zásady odlišovaných služeb QoS udává počet nevyhovujících bitů počet bitů, které byly uvolněny. Počet vyhovujících paketů udává počet bajtů kontrolovaných danou zásadou QoS (od okamžiku, kdy byl paket spuštěn do okamžiku současného výstupu monitorování).

Hodnota, kterou přiřadíte poli average token rate limit (limit průměrné přenosové rychlosti tokenů) je také důležitá. Když počet paketů tuto hranici překročí, server je začne uvolňovat. V důsledku toho se zvýší počet nevyhovujících bitů. To dokládá, že zásada QoS funguje v souladu s tím, jak jste ji nakonfigurovali. Chcete-li změnit množství nevyhovujících bitů, musíte přizpůsobit limity výkonu. Popis všech polí výstupu monitorování najdete v tématu Monitorování QoS.

Krok 5: Změňte hodnoty, je-li to potřebné.

Poté, co provedete monitorování, můžete změnit kteroukoliv z hodnot, které jste předtím zadali. Klepněte pravým tlačítkem myši na jméno provozní třídy, kterou jste vytvořili v rámci této zásady. Pokud vyberete volbu **Vlastnosti**, objeví se dialogové okno Vlastnosti CoS s hodnotami, které řídí přenosy.

Krok 6: Proveďte znovu monitorování zásady QoS

Poté, co si prohlédnete výsledky, použijte metodu pokusů a omylů, abyste zjistili optimální limity pro potřeby vaší sítě.



Sledování aplikací TCP



Pomocí QoS můžete pracovat s funkcemi pro sledování a prohlížet si aktuální vyrovnávací paměť pro sledování. Chcete-li spustit sledování na serveru, postupujte dle jedné z následujících těchto možností:

- Z rozhraní příkazového řádku zadejte TRCTCPAPP.

Zde je příklad vyplnění parametrů pro sledování.

```
TCP/IP application.....> *QOS
Trace option setting.....> *ON
Maximum storage for trace....> *APP
Trace full action.....> *WRAP
Argument lists.....> 'lvl=4'
QoS trace type.....> *ALL
```

V následující tabulce jsou uvedeny možné parametry, které lze nastavit pro sledování. Jestliže se nastavení neobjeví ve znakově orientovaném rozhraní, musíte je zadat v příkazu. Například zadáte TRCTCPAPP APP(*QOS) MAXSTG(1000) TRCFULL(*STOPTRC) ARGLIST('l=4 c=i').

Nastavení	Volby
TCP/IP application	QOS
Trace option setting	*ON, *OFF, *END, *CHK
Maximum storage for trace (Viz 60) (MAXSTG)	1-16000, *APP
Trace full action (Viz 61) (TRCFULL)	*WRAP, *STOPTRC
Argument list (Viz 61) (ARGLIST)	Úrovně: 'lvl=1', 'lvl=2', 'lvl=3', 'lvl=4' Obsah: 'c=a', 'c=i', 'c=d', 'c=m'
QoS trace type	*ALL

Další informace o interpretaci výsledků sledování najdete v tématu Výstupy sledování. Na této stránce je uveden vzorový výstup s komentáři, které vám pomohou pochopit jeho význam. Služba typicky využívá funkci TRCTCPAPP. Pokud tedy máte problémy se čtením výstupu, kontaktujte vašeho servisního zástupce.

Parametr "Maximum storage for trace"

1-16000

Toto je maximální velikost paměti pro sledování dat. Když je dosaženo této velikosti, sledování se zastaví nebo data začnou přetékat na začátek souboru. Předvolená velikost je 4 MB. Chcete-li zadat předvolenou velikost, vyberte *APP.

***APP**

Toto je předvolená volba. Říká aplikacím, aby používaly předvolenou velikost paměti pro sledování. Předvolená velikost paměti pro sledování pro server QoS je 4 MB.

Parametr "Trace full action"

***WRAP**

Když sledování dosáhne maxima diskového prostoru (vyrovnávací paměť pro sledování), informace o sledování začnou přetékat. Přetékání umožní systému přepsat nejstarší informace v souboru, takže můžete pokračovat v zaznamenávání informací o sledování. Pokud nevyberete přetékání, pak když je disk plný, činnost sledování se zastaví.

***STOPTRC**

Když systém dosáhne maxima diskového prostoru, sběr informací se zastaví.

Parametr "Argument lists"

Tento parametr udává, jaká úroveň chyb a jaký obsah se bude protokolovat. V příkaze TRCTCPAPP existují dva povolené argumenty: trace level (úroveň sledování) a trace content (obsah sledování). Když zadáváte úroveň sledování a obsah sledování, ujistěte se, že všechny atributy jsou obsaženy v jedné souvislé citaci. Například TRCTCPAPP 'l=4 c=a'.

Poznámka: Zadaná úroveň protokolování zahrnuje úrovně nižší. To znamená, že když vyberete určitou úroveň protokolování, budou vybrány také všechny předcházející úrovně. Například když vyberete úroveň 3, pak budou automaticky zahrnuty také úrovně 1 a 2. V případě typického sledování se doporučuje zadat 'l=4'. **Úrovně sledování**

Úroveň 1: SYSERR (Systémové chyby)

Protokolují se chyby, ke kterým dochází při systémových operacích. Pokud se taková chyba vyskytne, server QoS nemůže pokračovat. Systémová chyba se může vyskytnout, jestliže vám například dochází systémová paměť, nebo jestliže systém nemůže komunikovat s TCP/IP. Toto je předvolená úroveň.

Úroveň 2: OBJERR (Chyby objektů)

Protokolují se chyby, ke kterým dochází v rámci kódu serveru QoS. Chyba objektu se může vyskytnout, například proto, že operace serveru narazila na nějaké nečekané výsledky. To je obvykle závažná situace, kterou je třeba hlásit službě.

Úroveň 3: EVENT (Konkrétní události)

Protokolují se všechny operace QoS, které se vyskytnou. Protokol události například zaznamenává příkazy a žádosti. Výsledky jsou podobné jako u funkce žurnálování QoS.

Úroveň 4: TRACE (Zprávy sledování)

Sledují se všechna data přenášená na server QoS a ze serveru QoS. Tuto nejvyšší úroveň sledování byste například mohli použít pro protokolování všeho, o čem myslíte, že by vám mohlo pomoci odstranit problémy. Tyto informace vám pomohou určit, kde dochází k problému a jak problém reprodukovat.

Parametr "Trace Content"

Poznámka: Zadejte pouze jeden typ obsahu. Jestliže nezadáte, jaký typ obsahu sledovat, pak se bude (standardně) sledovat veškerý obsah.

Content = All ('c=a')

Sledují se všechny funkce serveru QoS. Toto je zároveň předvolená hodnota.

Content = Intserv ('c=i')

Sledují se pouze operace zásad integrovaných služeb QoS. Použijte toto nastavení pokud zjistíte, že problém souvisí se zásadami integrovaných služeb.

Content = Diffserv ('c=d')

Sledují se pouze operace zásad odlišovaných služeb QoS. Použijte toto nastavení pokud zjistíte, že problém souvisí se zásadami odlišovaných služeb.

Content = Monitor ('c=m')

Sledují se pouze operace monitorování.

Kompletní informace o příkazu TRCTCPAPP najdete v části Popis příkazu TRCTCPAPP (Sledování aplikace TCP/IP) v rámci tématu Příkazy CL.



Přečtěte si výstup sledování

Toto téma neobsahuje celkový popis toho, jak číst výstup sledování. Jsou zde však vyzdvíženy klíčové události, které je potřeba ve výstupu sledování hledat.

U **zásad integrovaných služeb QoS** je nejdůležitější událostí, kterou je potřeba hledat, to, zda spojení RSVP bylo odmítnuto z důvodu, že zásada QoS pro dané spojení nebyla nalezena. Zde je příklad zprávy o úspěšném spojení:

```
12/15 11:36:14 [336,80] TRCE :.....rpapi_getPolicyData: Found action name vreStnl_kraMoNICvreStnl for
flow[sess=x.x.x.x:y:z:s, source=x.x.x.x:y]
```

Zde je příklad zprávy o neúspěšném spojení integrovaných služeb:

```
12/15 11:36:14 [336,80] TRCE :.....rpapi_getPolicyData: Unable to find action name for flow [sess=x.x.x.x:y]
```

U **zásad odlišovaných služeb QoS** jsou nejdůležitějšími zprávami ty, které udávají, zda server zavedl pravidlo zásady QoS, nebo zda se v konfiguračním souboru zásady QoS vyskytla chyba.

Příklad:

```
01/11 14:07:52 [376,57] TRCE :.....KernelAddPolicyRule: Installing rule = timed_42ring.
01/11 14:07:52 [376,57] EVNT :.....create_tcp_resv: No value in config file for DiffServInProfilePeakRate,
defaulted to 100000 00.
01/11 14:07:52 [376,57] TRCE :.....create_tcp_resv: Create resv - bRate: 537395 5722SS1 V5R1M0
010525 TRCTCPAPP Output RS004 Date-01/11/01 Time-14:08:03 Page-6
01/11 14:07:52 [376,57] TRCE :.....create_tcp_resv: bDepth: 32768
01/11 14:07:52 [376,57] TRCE :.....create_tcp_resv: peakR: 10000000
01/11 14:07:52 [376,57] TRCE :.....create_tcp_resv: m: 128
01/11 14:07:52 [376,57] TRCE :.....create_tcp_resv: M: 41452
01/11 14:07:52 [376,57] TRCE :.....create_tcp_resv: mark(TOS): a0
01/11 14:07:52 [376,57] TRCE :.....create_tcp_resv: flags: 15
01/11 14:07:52 [376,57] TRCE :.....create_tcp_resv: flowspe.form = 1, QOS_FORMAT_DS = 1
```

Můžete také obdržet zprávy udávající, že příznaky v konfiguračním souboru zásady QoS byly nesprávné. Zde je několik ukázek zpráv:

```
12/15 11:36:14 [336,80] TRCE :.....rpapi_getPolicyData: Unknown attribute %s in ServicePolicy-Ignoring. 12/15
11:36:14 [336,80] TRCE :.....rpapi_getPolicyData: Unknown attribute %s in Priority Mapping-Ignoring.
```

Poznámka: Znak % je proměnná, která reprezentuje nerozpoznaný příznak.

Související informace o QoS

O produktu QoS existuje v odvětví IT mnoho dalších informačních zdrojů. Můžete si projít nejnovější RFC (Request for Comments), bílé stránky, červené knihy^(TM) a další zdroje, které vám poskytnou obecné informace o QoS. Zde jsou některé zdroje, které je vhodné zvážit:

QoS RFC

RFC (Requests for Comments) jsou písemné definice standardů protokolu a navrhované standardy používané pro síť Internet. Pokud chcete porozumět produktu QoS a s ním souvisejícím funkcím, mohou vám být užitečné tyto RFC:

RFC 1349

Tento RFC popisuje nové definice polí TOS v hlavičce IP paketů.

RFC 2205

Tento RFC popisuje definici protokolu RSVP (Resource ReSerVation Protocol).

RFC 2210

Tento RFC popisuje použití protokolu RSVP v rámci zásad integrovaných služeb IETF.

RFC 2474

Tento RFC popisuje definici pole DS (pole Differentiated Services) v rámci zásad odlišovaných služeb.

RFC 2475

Tento RFC vysvětluje architekturu odlišovaných služeb.

Chcete-li zobrazit výše uvedenou RFC, navštivte webovou stránku RFC index search engine



umístěnou na adrese editoru RFC



. Vyhledejte číslo RFC, který si chcete prohlédnout. Výsledky vyhledávání zobrazí příslušný název RFC, autora, datum a status.

Červené knihy IBM^(R)

iSeries IP Networks: Dynamic!



Toto je nejnovější publikace o sítích IP. Popisuje, jak navrhnout síť IP, která je samokonfigurovatelná, zabezpečena proti selhání a efektivní ve svých operacích. Kromě mnoha ostatních funkcí popisuje základní teorii produktu QoS a jeho implementaci v systémech iSeries. Také zde najdete další scénáře s podrobnými pokyny.

TCP/IP More Cool Things than Ever



Tato publikace uvádí příklady scénářů, které demonstrují běžná řešení TCP/IP s příklady konfigurací. Zde uvedené informace vám pomohou při plánování, instalaci, přizpůsobování, konfigurování a odstraňování problémů v TCP/IP na serveru iSeries. Publikace se netýká přímo produktu QoS, ale uvádí informace o serveru adresářů LDAP.

TCP/IP Tutorial and Technical Overview



Tato publikace představuje úvod a také referenční publikaci k sadě protokolů a aplikací TCP/IP (Transmission Control Protocol/Internet Protocol). Tématu QoS je věnována část *Part 3. Advanced concepts and new technologies* v kapitole 22.

Související témata v aplikaci Information Center systému iSeries

LDAP

V tomto tématu získáte základní informace o serveru adresářů, jeho konfiguraci, správě a odstraňování problémů. V tématu o adresářových službách také najdete další zdroje informací o konfigurování serveru adresářů.

Dodatek. Poznámky

Tyto informace se týkají produktů a služeb nabízených 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 společnosti IBM. Použití lze jakýkoli funkčně ekvivalentní produkt, program či službu neporušující práva IBM k duševnímu vlastnictví. Za vyhodnocení a ověření činnosti libovolného produktu, programu či služby jiného výrobce než IBM však odpovídá uživatel.

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, VYJÁDRĚNÝCH NEBO ODVOZENÝCH, VČETNĚ, BEZ OMEZENÍ, ODVOZENÝCH ZÁRUK NEPORUŠENÍ PRÁV TŘETÍCH STRAN, ZÁRUKY PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL. Právní rády 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. 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 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

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

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

Všechny uváděné ceny IBM jsou maloobchodní ceny navržené společností IBM, jsou nyní platné a mohou se bez upozornění změnit. Ceny prodejců se mohou lišit.

Informace zde uvedené slouží pouze pro účely plánování. Informace v tomto dokumentu mohou být změněny, než se produkty popsáné v tomto dokumentu stanou obecně dostupnými.

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

COPYRIGHT LICENCE:

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.

KROMĚ JAKÝCHKOLIV ZÁKONNÝCH ZÁRUK, KTERÉ NEMOHOU BÝT VYLOUČENY, IBM, JEJÍ PROGRAMOVÍ VÝVOJÁŘI A DODAVATELÉ NEPOSKYTUJÍ ZÁRUKY ANI PODMÍNKY, VYJÁDŘENÉ NEBO ODVOZENÉ, VČETNĚ, BEZ OMEZENÍ, ODVOZENÝCH ZÁRUK PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL A ZÁRUK NEPORUŠENÍ PRÁV TŘETÍCH STRAN V SOUVISLOSTI S PROGRAMEM NEBO TECHNICKOU PODPOROU, POKUD EXISTUJE.

ZA ŽÁDNÝCH OKOLNOSTÍ NEJSOU IBM, JEJÍ PROGRAMOVÍ VÝVOJÁŘI NEBO DODAVATELÉ ODPOVĚDNI ZA ŽÁDNOU Z NÍŽE UVEDENÝCH SITUACÍ, ANI V PŘÍPADĚ, ŽE BYLI O MOŽNOSTI JEJICH VZNIKU PŘEDEM INFORMOVÁNI:

1. ZTRÁTA NEBO POŠKOZENÍ DAT;
2. ZVLÁŠTNÍ, NAHODILÉ NEBO NEPŘÍMÉ ŠKODY ANI NÁSLEDNÉ EKONOMICKÉ ŠKODY; NEBO
3. UŠLÝ ZISK, ZTRÁTA OBCHODNÍCH TRANSAKČÍ, ZTRÁTA VÝNOSŮ, DOBRÉHO JMÉNA NEBO PŘEDPOKLÁDANÝCH ÚSPOR

NĚKTERÉ JURISDIKCE NEPOVOLUJÍ VYLOUČENÍ NEBO OMEZENÍ NAHODILÝCH NEBO NÁSLEDNÝCH ŠKOD, TAKŽE SE NA VÁS NĚKTERÁ NEBO VŠECHNA VÝŠE UVEDENÁ OMEZENÍ NEMUSEJÍ VZTAHOVAT.

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.

Ochranné známky

Níže uvedené termíny jsou ochranné známky společnosti International Business Machines Corporation ve Spojených státech a případně v dalších jiných zemích.

IBM

iSeries

Operating System/400

OS/400

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

Ustanovení a podmínky pro stahování a tisk publikací

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

Osobní použití: Pokud zachováte všechny výhrady týkající se vlastnických práv, můžete tyto publikace kopírovat pro své osobní nekomerční použití. Tyto publikace ani jakékoli 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 Vašeho podniku. Bez výslovného souhlasu IBM nesmíte z těchto publikací vytvářet odvozená díla ani je (nebo jejich části) nesmíte kopírovat, distribuovat či prezentovat mimo rámec svého podniku.

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

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

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

Autorská práva na veškeré materiály náleží společnosti IBM Corporation.

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



Vytištěno v Dánsku společností IBM Danmark A/S.