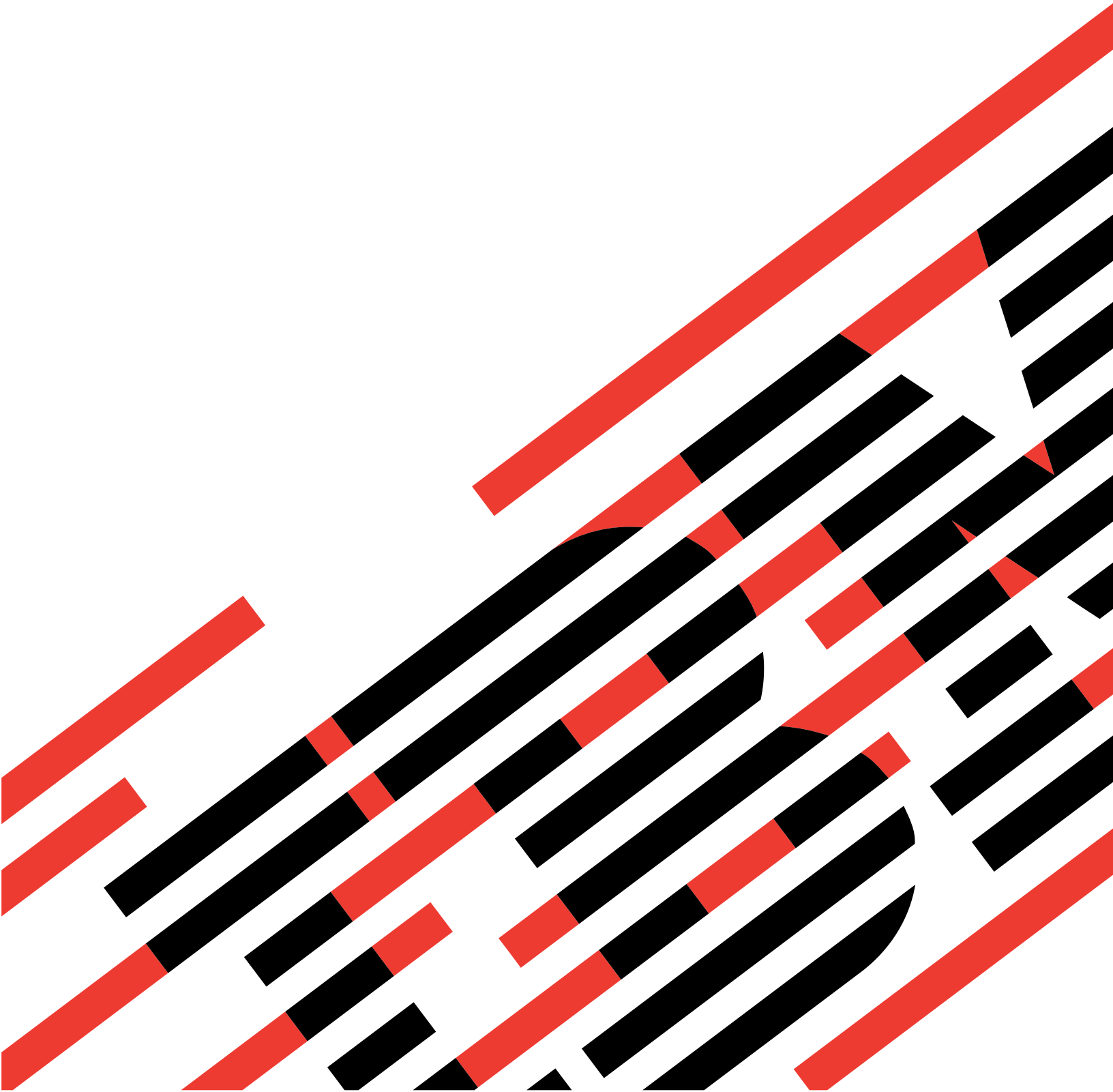
IBM

eserver

iSeries

Kvalita služby (QoS)

Verzia 5, vydanie 3



IBM

@server

iSeries

Kvalita služby (QoS)

Verzia 5, vydanie 3

Poznámka

Pred použitím týchto informácií a nimi podporovaného produktu si určite prečítajte informácie v časti “Právne informácie”, na strane 63.

Štvrté vydanie (August 2005)

Toto vydanie sa týka verzie 5, vydania 3, modifikácie 0 operačného systému OS/400 (5722-SS1) a všetkých nasledujúcich vydaní a modifikácií, pokiaľ nebude v nových vydaniach uvedené inak. Táto verzia sa nedá spustiť na počítačoch s redukovanou inštrukčnou sadou (RISC), ani na modeloch CISC.

Obsah

Kvalita služby (QoS)

Všetka prevádzka na vašej sieti má rovnakú prioritu. Bežná prevádzka prehliadača sa považuje za rovnako dôležitú, ako závažné obchodné aplikácie. Ak váš generálny riaditeľ (CEO) robí prezentáciu prostredníctvom audio/video aplikácie, význam priority IP paketov je zrejmý. Je dôležité, aby táto aplikácia mala počas prezentácie vyšší výkon ako ostatné aplikácie.

Riešenie iSeries(TM) QoS umožňuje politikám požadovať sieťovú prioritu a šírku pásma pre aplikácie TCP/IP v celej sieti. Priorita paketov je pre vás významná, ak odosielate aplikácie, ktoré potrebujú predvídateľné a spoľahlivé výsledky, ako napríklad multimédiá. Politiky QoS na serveri iSeries(TM) môžu tiež obmedziť dáta odchádzajúce z vášho servera, spravovať požiadavky na pripojenie a riadiť zaťaženie servera.

Je dôležité pochopiť QoS pred tým, ako začnete konfigurovať politiky. Nasledujúce odkazy vám poskytujú informácie, ktoré potrebujete na realizáciu QoS.

Čo je nové pre V5R3?
Uvádza zmeny v sieťovej funkcii kvality služieb a v téme Informačného centra.

Vytlačiť túto tému
Vytlačiť celú tému.

Koncepty QoS
Ak ešte nie ste oboznámený s kvalitou služby, zobrazte niektoré základné koncepty QoS. Toto vám dá prehľad o tom, ako QoS pracuje a ako spolupracujú funkcie QoS.

Scenáre QoS
Pozrite si scenáre politiky QoS, kde uvidíte, prečo a ako používať QoS.

Plánovanie QoS
Pripojí vás na poradcu plánovaním a sieťové informácie, ktoré musíte poznať, aby ste QoS používali efektívne.

Konfigurácia QoS
Tieto pokyny nasledujte, ak chcete vytvoriť nové politiky diferencovaných služieb, politiky integrovaných služieb a politiky povolenia vstupu.

Manažovať QoS
Tieto pokyny nasledujte, ak chcete manažovať existujúce vlastnosti a politiky QoS. Tieto odseky vám ukážu, kde hľadať aktuálne úlohy pre úpravu, povolenie, zobrazenie a používanie iných techník riadenia politiky. Tiež tam nájdete vysvetlenie spôsobu používania monitora QoS a zhromažďovania údajov, čo vám pomôže pri analýze vašej premávky IP prechádzajúcej cez váš server.

Odstránenie problémov QoS
Časť o odstraňovaní problémov vám pomôže napraviť problém s QoS.

Informácie týkajúce sa QoS
Nájdite odkazy na ďalšie užitočné zdroje QoS. Je tu množstvo publikácií, webových stránok, požiadaviek na komentár (RFC) a bielych stránok.

Čo je nové pre V5R3?

Tento odstavec opisuje nové funkcie pridané pre Verziu 5, vydanie 3.

Nové funkcie

- **Nová zdokonalená politika diferencovaných služieb (DiffServ)**
  V predošlých verziách vám politiky diferencovaných služieb umožňovali priradiť úrovne služieb odchádzajúcej

premávke na základe adresy IP zdroja/cieľa, portov, aplikácií a klientov. Vo V5R3 môžu vaše aplikácie iSeries(TM) dostávať úrovne služieb založené na špecifickejších informáciách o aplikácii. Viac informácií nájdete v koncepte diferencovaných služieb.

- **Dve možnosti uchovávania politík QoS**
  V predošlých verziách boli politiky exportované do adresárového servera pomocou najnovšej verzie protokolu LDAP, verzie 3. Teraz sú vaše politiky vždy uchovávané vo vašom lokálnom serveri. Stále však máte možnosť exportovať ich do adresárového servera. Táto téma vám vysvetlí výhody oboch metód, pričom vám poskytne aj dodatočné informácie o adresárovom serveri.
- **Identifikovať aplikácie podľa názvu servera**
  V predošlých verziách ste priraďovali úrovne služieb aplikáciám TCP/UDP podľa ich dobre známych portov. Identifikácia aplikácie portom však nefunguje pre každú aplikáciu. Napríklad FTP v pasívnom režime používa dynamický port pre dátové pripojenia. Teraz môžete identifikovať aplikáciu podľa jedinečného znakového reťazca označovaného ako názov servera (ako napríklad TFTP). Tento zoznam názvov serverov je preddefinovaný. Pri konfigurácii politiky si môžete vybrať z preddefinovaného zoznamu alebo môžete vytvoriť vlastný názov servera. Používanie názvu servera nahradzuje používanie portov alebo rozsahu portov na definíciu aplikácie.
- **Vylepšenia triedy služby**
  Sprievodca triedy služby vám teraz umožňuje definovať triedu služby, ktorá sa dá zdieľať medzi politikami vstupu a výstupu. Ako súčasť triedy služby definujete spracovanie mimo profilu. Existuje nová voľba na redukovanie okna preťaženia TCP. Ak je toto vybraté, na obmedzenie premávky sa používa okno preťaženia TCP.
- **Váhované prioritné fronty**
  Ak sa akceptuje prichádzajúce pripojenie, umiestni sa do frontu akceptácie, ktorý definuje politika vstupu. Každý front akceptácie má istú váhu, ktorou určuje prioritu frontu.

Zmeny informácií

- **Monitorovanie informácií o QoS**
  Monitor je skvelý nástroj na analýzu a meranie toku premávky vo vašej sieti. Použite príklad pre monitor a informácie z neho vyplývajúce na pomoc k práci s týmto nástrojom.
- **Zavedenie nových API**
  Informácie o API sa stali viac významnejšie pre tie politiky, ktoré ich využívajú. Informácie vás privedú k špecifickým rozhrania API pre každý typ politiky QoS.

Ako zistiť, čo je nové, alebo sa zmenilo

Aby ste videli, aké technické zmeny boli vykonané, tieto informácie obsahujú:

- Obrázok

  ktorý označuje miesto, kde sa začínajú nové alebo zmenené informácie.
- Obrázok

  ktorý označuje miesto, kde sa končia nové alebo zmenené informácie.

Keď chcete nájsť iné informácie o tom čo je nové alebo zmenené v tomto vydaní, pozrite si Memo to Users

.

Vytlačiť túto tému

Ak chcete zobraziť alebo prevziať verziu PDF, vyberte Kvalita služby (asi 525 KB).

Na uloženie dokumentu typu PDF na svoju pracovnú stanicu pre prezeranie alebo tlač:

1. Otvorte dokument typu PDF vo svojom prehliadači (kliknite na odkaz vyššie).
2. V ponuke svojho prehliadača kliknite na **Súbor**.
3. Kliknite na **Uložiť ako...**
4. Vyberte adresár, do ktorého chcete uložiť súbor PDF.
5. Kliknite na **Uložiť**.

Ak potrebujete Adobe Acrobat Reader na prezeranie alebo tlač týchto PDF, môžete si stiahnuť kópiu z webovej stránky spoločnosti Adobe

.

Koncepty QoS

Pred spustením vykonávania QoS sa dôrazne odporúča preskúmanie tejto témy, čím sa uistíte, že táto služba uspokojí vaše potreby. Pojem Kvalita služby (QoS) sa dá nájsť vo viacerých zdrojoch, preto táto téma vysvetlí len jej základné funkcie.

Na uskutočnenie QoS nakonfigurujete politiky pomocou sprievodcov v iSeries(TM) Navigator. **Politika** je sada pravidiel, ktorá určuje akciu. Politika v podstate určuje, ktorý klient, aplikácia a plán (ktorý predurčíte), musí prijať konkrétnu službu. Konfigurovať môžete tri typy politík:

- Diferenčný servis
- Integrovaná služba
- Povolenie vstupu

Diferencovaná služba a integrovaná služba sa považujú za politiky výstupnej šírky pásma. Politiky výstupu obmedzujú údaje opúšťajúce vašu sieť a pomáhajú riadiť záťaž servera. Vami nastavené rýchlosti v politike výstupu riadia, ako a aké údaje sú alebo nie sú obmedzené v serveri. Oba typy politiky výstupu môžu vyžadovať SLA s vaším ISP. Viac informácií nájdete v časti Dohody úrovne služieb.

Politiky povolenia vstupu riadia požiadavky o pripojenie prichádzajúce do vašej siete z niektorého vonkajšieho zdroja. Politiky vstupu nie sú závislé na úrovni služby od vášho ISP. Aby ste rozhodli, ktoré politiky musíte používať, vyhodnoťte dôvody, pre ktoré chcete používať QoS a uvážte rolu vášho servera iSeries.

Jednou z najdôležitejších častí realizácie QoS je samotný server. Nielen, že musíte pochopiť nižšie uvedené koncepty, ale tiež sa musíte oboznámiť s rolou vášho servera, ktorú vykonáva v týchto konceptoch. Server iSeries môže vystupovať len ako klient, alebo server, ale nie smerovač. Napríklad server iSeries správajúci sa ako klient môže používať politiky diferencovaných služieb aby skontroloval, že požiadavkám o informácie odosielané iným serverom je prostredníctvom siete pridelená vyššia priorita. Server iSeries správajúci sa ako server môže využiť politiku povolenia vstupu na obmedzenie požiadaviek o URI, ktoré server akceptuje.

Viac informácií nájdete na nasledujúcich linkách:

Diferencovaná služba
Toto je prvý typ politiky šírky pásma pre prístup smerom von, ktorú môžete na svojom serveri vytvoriť. Diferencovaná služba rozdeľuje vašu premávku do tried. Ak chcete realizovať politiku diferencovaných služieb, musíte určiť, ako chcete klasifikovať vašu sieťovú prevádzku a spracúvať rozdielne triedy.

Integrovaná služba
Druhý typ politiky šírky pásma pre prístup smerom von, ktorý môžete vytvoriť, je politika integrovaných služieb. Integrovaná služba poskytuje aplikáciám IP možnosť na odoslanie požiadaviek o pridelenie a rezervovanie šírky pásma použitím protokolu RSVP a rozhraní API QoS. Politiky integrovaných služieb používajú protokol RSVP a RAPI API (alebo API qtoq socket) na garantovanie pripojenia medzi dvomi koncami. Toto je najvyššia úroveň služby, ktorú môžete určiť; je ale aj najkomplexnejšia.

Povolenie vstupu
Politika povolenia vstupu sa používa na riadenie požiadaviek o pripojenie prichádzajúcich do vašej siete.

Trieda služby
Táto téma vysvetľuje časti, ktoré vytvárajú triedu služby. Pri vytváraní politiky diferencovaných služieb alebo politiky povolenia vstupu taktiež vytvárate a používate triedu služby.

Rozhrania API QoS
Táto podtéma opisuje protokol a rozhrania API potrebné pre každý typ politiky QoS. Tiež sa tu rozoberá, ako na smerovači povoliť RSVP. Aktuálne rozhrania API QoS zahrňujú API RAPI, API qtoq sockets, API funkcie sendmsg() a rozhrania API pre monitor.

Monitor QoS
Táto podtéma opisuje monitor QoS umožňujúci skontrolovať, či politiky QoS pracujú tak, ako očakávate.

Adresárový server
Vaše politiky môžete exportovať do adresárového servera. Zobrazte túto tému, ak chcete zistiť výhody používania alebo nepoužívania adresárového servera, konceptov a konfigurácie LDAP, ako aj schémy QoS.

Dodatočné informácie nájdete na stránke informácie súvisiace s QoS

Diferencovaná služba

Diferencovaná služba (DiffServ) rozdelí vašu premávku do tried. Ak chcete realizovať politiky DiffServ vo vašej sieti, musíte určiť ako chcete klasifikovať vašu sieťovú prevádzku (Pozrite 4) a ako spracúvať rozdielne triedy (Pozrite 6).

Triedy s prioritou: Ako klasifikovať sieťovú prevádzku

Diferencované služby delia premávku do tried. Najčastejšie sa triedy definujú pomocou adresy IP klienta, aplikačných portov, typu servera, protokolu, lokálnej adresy IP a plánu. Celá premávka zodpovedajúca rovnakej triede je spracovaná rovnako. Aby sa klasifikácia vylepšila, niektoré z vašich aplikácií iSeries™ môžu prijať rozdielne úrovne služieb pomocou špecifikácie údajov servera. Používanie údajov servera je voliteľné, ale môže napomôcť, ak vyžadujete jemnejšiu úroveň klasifikácie.

Údaje servera sú založené na dvoch rôznych typoch údajov aplikácie: tokene aplikácie a URI. Ak premávka zodpovedá tokenu alebo URI, ktorý ste špecifikovali v politike, politika sa aplikuje na odchádzajúcu odpoveď. Tým sa použije odchádzajúca premávka, bez ohľadu na prioritu zadanú v politike diferencovaných služieb.

Používanie tokenu aplikácie s politikami diferencovaných služieb

Používanie údajov aplikácie povie politike, aby odpovedala na špecifické parametre (token a priorita), ktoré aplikácia odovzdala serveru prostredníctvom sendmsg() API. Táto voľba je voliteľná. Ak nepotrebujete takúto úroveň granularity vo vašich politikách výstupu, v sprievodcovi vyberte **Všetky tokeny**. Ak zistíte, že chcete porovnať token a prioritu aplikácie so špecifickým tokenom a prioritou nastavenou v politike výstupu, môžete to vykonať. V politike existujú dve časti pre nastavenie údajov aplikácie - token a priorita.

- Čo je token aplikácie?
  Token aplikácie je ľubovoľný znakový reťazec reprezentujúci daný prostriedok, napríklad myFTP. Vami zadaný token v politike QoS sa porovná s tokenom poskytnutým vonkajšou aplikáciou. Aplikácia poskytuje hodnotu tokenu prostredníctvom sendmsg() API. Ak sú tokeny rovnaké, premávka aplikácie sa zahrnie do politiky diferencovaných služieb.

  Ak chcete použiť token aplikácie v politike diferencovaných služieb, vykonajte toto:
  1. V okne konfigurácie QoS kliknite pravým tlačidlom na **DiffServ** a vyberte **Nová politika**. Spustite sprievodcu.
  2. Ak nájdete stránku *Požiadavka o údaje servera*, vyberte **Vybratý token aplikácie**.
  3. Ak chcete vytvoriť nový token, kliknite na **Nový**. Zobrazí sa dialógové okno *Nové URI*.
  4. V poli *Názov* zadajte zmysluplný názov pre token aplikácie.
  5. V poli *URI* vymažte (/) a zadajte token aplikácie (reťazec nie dlhší ako 128 znakov). Napríklad myFTPapp, čo je výhodnejšie ako typické URI.
- Čo je priorita aplikácie?
  Vami zadaná priorita aplikácie sa porovná s prioritou aplikácie poskytnutou vonkajšou aplikáciou. Aplikácia poskytuje hodnotu priority použitím sendmsg() API. Ak sú priority rovnaké, premávka aplikácie sa zahrnie do politiky diferencovaných služieb. Celá premávka definovaná v politike diferencovaných služieb bude stále prijímať prioritu udelenú celej politike.

Keď špecifikujete token aplikácie, aplikácia poskytujúca túto informáciu serveru musí byť špecificky nakódovaná na použitie Sendmsg() API. Toto realizuje aplikačný programátor. Dokumentácia aplikácie musí poskytnúť platné hodnoty (tokeny a priority), ktoré administrátor QoS použije v politike diferencovaných služieb. Potom politika diferencovaných služieb použije svoju vlastnú prioritu a klasifikáciu pre premávku, ktorá zodpovedá tokenu nastaveného v politike. Ak aplikácia nemá hodnoty, ktoré zodpovedajú hodnotám nastaveným v politike, buď musíte aplikáciu vymeniť, alebo musíte použiť iné parametre pre údaje aplikácie pre politiku diferencovaných služieb.

Ak chcete zobraziť programátorské detaily týkajúce sa rozšírení QoS pre sendmsg() API, pozrite si sendmsg() API.

Používanie URI s politikami diferencovaných služieb
Pri vytváraní politiky diferencovaných služieb vám sprievodca umožní nastaviť informácie o údajoch servera, ako bolo uvedené vyššie. Aj keď vás polia v sprievodcovi vyzývajú na zadanie tokenu aplikácie, môžete namiesto toho zadať relatívne URI. Znovu, toto je voliteľné. Ak nepotrebujete takúto úroveň granularity vo vašich politikách výstupu, v sprievodcovi vyberte **Všetky tokeny**. Ak zistíte, že chcete porovnať špecifické URI s URI nastaveným v politike výstupu, môžete to vykonať.

Relatívne URI je v skutočnosti podsada absolútneho URI (podobné starému absolútnemu URL). Pozrite si tento príklad: http://www.ibm.com/software. **http://www.ibm.com/software** segment sa považuje za absolútne URI. Segment **/software** je relatívne URI. Všetky relatívne URI hodnoty musia začať s jedným lomítkom (/). Nasledujú platné príklady relatívneho URI:

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

Predtým, ako nastavíte politiku diferencovaných služieb používajúcej URI skontrolujte, či port aplikácie priradený pre URI zodpovedá direktíve 'Listen' povolenej pre FRCA v konfigurácii webového servera Apache Web Server. Ak chcete zmeniť alebo zobraziť port pre váš server HTTP, pozrite si túto tému: Manažovať adresy a porty pre váš server HTTP (založený na Apache).

FRCA (Fast Response Cache Accelerator) identifikuje URI pre každú odchádzajúcu odpoveď HTTP. Porovná URI súvisiace s odchádzajúcou odpoveďou s URI definovaným v každej politike diferencovaných služieb. Prvá politika s tokenom typu reťazec (URI), ktorý sa najviac zhoduje s URI identifikovaným pomocou FRCA, sa použije pre všetky odpovede pre URI.

Nastavenie vlastností: Ako zaobchádzať s triedami

Po klasifikácii premávky diferencovaná služba tiež vyžaduje skokové správanie (PHB) na definovanie spôsobu zaobchádzania s premávkou. Server používa bajty v IP hlavičke na identifikáciu servisnej úrovne IP paketu. Smerovače a prepínače vyhradzujú prostriedky na základe informácií PHB v oktetovom poli typu služby (TOS) v hlavičke IP. Pole TOS bolo znovu definované v požiadavke na komentár (RFC) 1349 a OS/400(R) V5R1. PHB je postupujúce správanie, ktoré paket získava v sieťovom uzle. Je reprezentované hodnotou známou ako kódový bod. Pakety môžu byť označené na serveri, alebo na inej časti sieti, ako smerovač. Ak si má paket zachovať požadovanú službu, každý sieťový uzol musí byť typu diferencovanej služby (DiffServ). To znamená, že zariadenie musí byť schopné presadiť správania vykonávané po skokoch. Na presadenie PHB zaobchádzania musí byť sieťový uzol schopný používať plánovania frontu a správy odchádzajúcej priority. Ak chcete získať viac informácií o tom, čo znamená byť typu DiffServ, pozrite si stránku Udržiavače premávky.

Ak váš paket prechádza cez smerovač alebo prepínač, ktorý nie je typu DiffServ, paket v ňom stratí svoju úroveň služby. Paket sa spracuje, ale môže sa stať, že sa neočakávane oneskorí. Vo vašom serveri iSeries môžete použiť preddefinované kódové body PHB alebo môžete definovať váš vlastný kódový bod. Neodporúča sa, aby ste si vytvárali vaše vlastné kódové body pre používanie mimo vašej privátnej sieti. Ak neviete, ktorý kódový bod máte priradiť, zobrazte Použiť koncové body na priradenie skokového správania.

Na rozdiel od integrovanej služby, diferencovaná služba nevyžaduje rezerváciu ani zaobchádzanie počas toku. Celá premávka umiestnená v rovnakej triede je spracúvaná rovnako.

Diferencované služby sa tiež môžu použiť na obmedzenie premávky opúšťajúcej server. To znamená, že váš server iSeries naozaj používa diferencovanú službu na obmedzenie výkonu. Obmedzovanie menej kritickej aplikácie umožňuje kľúčovým aplikáciám, aby opustili vašu privátnu sieť najskôr. Pri vytváraní triedy služby pre túto politiku budete musieť nastaviť rôzne limity pre váš server. Stránka Limity pre výkon zahŕňa veľkosť bloku tokenov, maximálnu hodnotu špičkovej rýchlosti a maximálnu hodnotu priemernej rýchlosti. Témy pomoci v rámci funkcie QoS programu iSeries Navigator vám dajú omnoho konkrétnejšie informácie o týchto hodnotách.

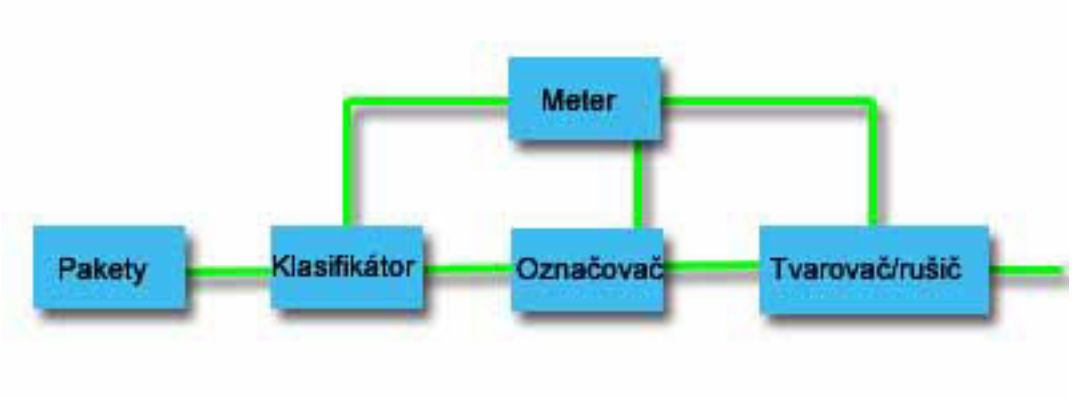
Udržiavače premávky

Sieťové vybavenie používajúce politiky kvality služieb musí byť typu DiffServ. Znamená to, že sieťové zariadenie, ako smerovače a prepínače musia mať nasledujúce schopnosti: triediče, merače, označovače, tvarovače a vypínače. Súhrn týchto pojmov sa nazýva *udržiavače premávky*. Ak má sieťové vybavenie všetky tieto udržiavače premávky, označuje sa ako vybavenie typu DiffServ.

Poznámka: Tieto hardvérové požiadavky nie sú špecifické pre iSeries (TM). Tieto pojmy neuvidíte použité v rozhraní QoS, pretože server neumožňuje riadiť externý hardvér. Mimo súkromnej siete musí mať hardvér schopnosť spracúvať všeobecné požiadavky QoS. V konkrétnych manuáloch pre používané vybavenie skontrolujte, či hardvér umožňuje spracúvať požiadavky diferencovaných služieb. Tiež sa odporúča, aby ste preskúmali všeobecné koncepty a požiadavky QoS pred implementáciou politík.

Nasledujúca schéma predstavuje logickú reprezentáciu spôsobu, akým udržiavače premávky pracujú.

Obrázok 11. Udržiavače premávky



Nasledujúce informácie popisujú každý z udržiavačov premávky podrobnejšie.

Klasifikátory
Triediče paketov vyberajú pakety v toku premávky na základe obsahu v ich IP hlavičke. iSeries server definuje dva typy triedičov. BA (Súhrn správania) triedi pakety výhradne na základe kódového bodu diferencovaných služieb. Klasifikátor MF (Multi-field) vyberie pakety založené na kombinácii hodnôt z jedného alebo viacerých polí v hlavičke, ako zdrojovej adresy, cieľovej adresy, poľa diferencovaných služieb, ID protokolu, zdrojového portu, URI, typu servera a čísiel cieľových portov.

Merače
Merače premávky merajú, či pakety IP postúpené klasifikátorom zodpovedajú profilu premávky pre hlavičku IP. Informácie v IP hlavičke sú určované hodnotami, ktoré nastavíte v QoS politike pre túto premávku. Merač posunie informácie iným podmienkovým funkciám, aby spustil akciu. Akcia je spustená pri každom pakete, či je v profile, alebo mimo profilu.

Značky
Značkovače paketov nastavujú pole diferencovaných služieb (DS). Značkovač môže byť nakonfigurovaný, aby značil všetky pakety na jediný kódový bod, alebo na sadu kódových bodov používanú na výber správania vykonávaného po skokoch.

Tvarovače
Tvarovače oneskoria niektoré, alebo všetky pakety v toku premávky, aby zosúladili tok s profilom premávky. Tvarovač má konečnú veľkosť pamäťového bloku a smerovače môžu vyradiť pakety v prípade, ak už nie je dostatok priestoru na uloženie oneskorených paketov.

Vypínače
Vypínače zrušia niektoré, alebo všetky pakety v toku premávky. Deje sa tak, aby bol tok zosúladený s profilom premávky.

Integrovaná služba

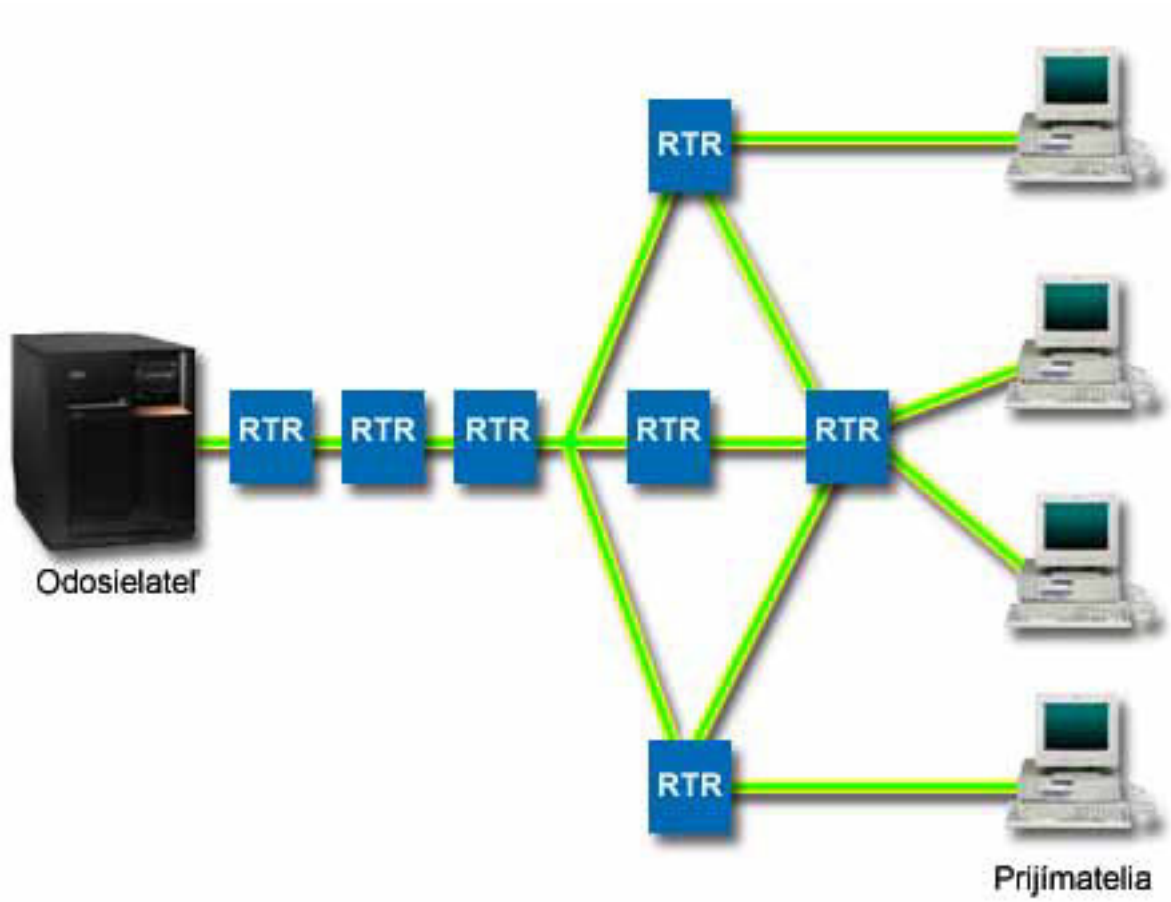
Integrovaná služba sa zaoberá časom doručenia premávky a priradením osobitných špeciálnych inštrukcií na spracovanie premávky. Dôležité je byť konzervatívny s vašimi politikami integrovaných služieb, pretože je ešte stále relatívne drahé garantovať prenos údajov. Avšak nadmerné zabezpečenie vašich zdrojov môže byť ešte nákladnejšie.

Pred odoslaním údajov integrovaná služba rezervuje prostriedky pre príslušnú politiku. Smerovače dostávajú signály pred dátovým prenosom a sieť v skutočnosti schvaľuje a riadi (koniec-ku-koncu) dátový prenos na základe politiky. **Politika** je sada pravidiel, ktorá určuje akciu. V skutočnosti to je kontrolný zoznam prijatia. Požiadavka šírky pásma prichádza v rezervácii od klienta. Ak všetky smerovače na ceste súhlasia s požiadavkami prichádzajúcimi z požadujúceho klienta, požiadavka sa dostane k serveru a intserv politike. Ak požiadavka spadá do obmedzení definovaných politikou, QoS server udelí povolenie pre RSVP pripojenie a potom vyhradí šírku pásma pre aplikáciu. Rezervácia sa uskutoční pomocou protokolu RSVP (Resource Reservation Protocol) a API RAPI, alebo pomocou protokolu RSVP a rozhraní API qtoq QoS sockets. Pozrite si Rozhrania API QoS, kde nájdete viac informácií.

Každý uzol, cez ktorý prechádza vaša prevádzka, musí mať schopnosť používať protokol RSVP. Smerovače poskytujú kvalitu služieb prostredníctvom nasledujúcich funkcií kontroly premávky: plánovač paketov, triedič paketov a kontrola prijatia. Schopnosť vykonávať túto kontrolu premávky sa často označuje ako RSVP umožnené. Následne je najdôležitejšia časť implementácie politík integrovaných služieb schopná kontrolovať a predpovedať zdroje vo vašej

sieti. Aby sa získali predpovedateľné údaje, každý uzol v sieti musí podporovať RSVP. Napríklad, ak je vaša premávka smerovaná na základe prostriedkov, poznačte si, ktoré cesty majú smerovače podporujúce RSVP. Prechod cez smerovače, ktoré nepodporujú RSVP môže spôsobiť nepredvídateľné problémy s výkonom. Pripojenie je aj tak uskutočnené, ale výkon požadovaný aplikáciou nie je zaručený smerovačom. Nasledujúca schéma ukazuje, ako funkcia integrovanej služby logicky pracuje.

Obrázok 13. Cesta RSVP medzi klientom a serverom.



Aplikácia s povoleným RSVP na serveri zistí požiadavku na pripojenie od klienta. Ako odpoveď aplikácia servera vydá príkaz PATH klientovi. Tento príkaz je zadaný za použitia API RAPI alebo API qtoq QoS soketov a obsahuje informácie o IP adrese smerovača. Príkaz PATH obsahuje informácie o disponibilných zdrojoch na serveri a smerovačoch pozdĺž cesty, ako aj smerovacie informácie medzi serverom a klientom. RSVP umožnená aplikácia na klientovi potom pošle príkaz RESV späť po sieťovej ceste, aby signalizovala serveru, že sieťové zdroje boli pridelené. Tento príkaz vykonáva rezerváciu na základe informácií smerovača z príkazu PATH. Server a všetky smerovače pozdĺž cesty rezervujú zdroje pre RSVP pripojenie. Keď server prijme príkaz RESV, aplikácia začne prenášať dáta na klienta. Dáta sú prenášané pozdĺž rovnakej cesty, ako rezervácia. Opäť to dokazuje dôležitosť schopnosti smerovačov vykonávať rezervácie pre úspešnosť vašich politík.

Integrovaná služba nie je určená pre pripojenia RSVP trvajúce krátko, ako napríklad HTTP. Samozrejme záleží na vašom uvážení. Len vy môžete rozhodnúť, čo je pre vašu sieť najlepšie. Zvážte, ktoré oblasti a aplikácie majú výkonnostné problémy a potrebujú kvalitu služby. Aplikácie používané v politike integrovaných služieb musia byť schopné používať protokol RSVP. V súčasnosti váš server nemá žiadne aplikácie a povoleným RSVP, takže budete musieť napísať svoje vlastné aplikácie s povoleným RSVP. Pozrite si časť Rozhrania API QoS, kde nájdete viac detailov o rozhraniach API pre Integrovanú službu.

Po príchode paketov a ich pokuse opustiť vašu sieť váš server určí, či má paket prostriedky, aby mohol paket odoslať. Toto prijatie je určené množstvom miesta v bloku symbolu. Manuálne môžete nastaviť počet dovolených bitov pre váš blok tokenov, limity šírky pásma, limity rýchlosti tokenov a maximálny počet pripojení, ktorý dovoľuje váš server. Tieto hodnoty sa nazývajú limity pre výkon. Ak pakety zostanú v rámci obmedzení servera, pakety súhlasia a sú poslané von. V integrovaných službách má každé pripojenie vyhradené svoj vlastný blok symbolu.

Integrovaná služba používajúca značky diferencovanej služby
Ak si nie ste istý, či môže celá sieť garantovať pripojenie RSVP, môžete vytvoriť politiku integrovaných služieb. Predsa len, ak sieťové prostriedky nevedia používať protokol RSVP, pripojenie nie je možné garantovať. V takejto situácii možno budete chcieť použiť pre danú politiku kódový bod. Tento kódový bod sa typicky používa v politikách diferencovaných služieb na pridelenie triedy služby premávke. Aj keď pripojenie nie je garantované, tento kódový bod sa pokúsi prideliť pripojeniu prioritu. Pozrite si Integrovaná služba používajúca značky diferencovanej služby, kde nájdete viac informácií.

Funkcie riadenia premávky
Funkcie riadenia premávky sa týkajú len integrovanej služby a nie sú špecifické pre iSeries(TM). Tieto pojmy neuvidíte použité v rozhraní QoS, pretože server neumožňuje riadiť externý hardvér. Mimo súkromnej siete musí mať hardvér schopnosť spracúvať všeobecné požiadavky QoS. Všeobecné požiadavky pre smerovač pre politiky IntServ sú opísané nižšie. Odporúča sa, aby ste preskúmali všeobecné koncepty a požiadavky QoS pred implementáciou politík.

Ak chcete získať očakávané výsledky, musíte mať na ceste premávky hardvér povoľujúci RSVP. Aby mohli smerovače používať protokol RSVP, musia mať určité funkcie riadenia premávky. Zvyčajne ich označujeme, že majú povolené RSVP, alebo QoS. Pamätajte, že váš server plní úlohu buď klienta, alebo servera. V tomto prípade ho nie je možné použiť ako smerovač. Pozrite sa do manuálov vášho sieťového vybavenia, aby ste overili, že umožňujú spracúvať požiadavky QoS.

Funkcie riadenia premávky môžu obsahovať toto:

Plánovač paketov
Plánovač paketov spravuje posielanie paketov ďalej v závislosti na informáciách v hlavičke IP. Tento plánovač paketov zabezpečuje, že sa doručovanie paketov riadi parametrami, ktoré ste stanovili vo svojej politike. Plánovač vstupuje do platnosti tam, kde sa pakety zoraďujú vo fronte.

Triedič paketov
Triedič paketov určuje, znova na základe informácie v hlavičke IP, ktoré pakety toku IP obdržia určitú úroveň služieb. Každý prichádzajúci paket je triedičom zaradený do príznačnej triedy. So všetkými paketmi, ktoré sú zaradené v tej istej triede, sa zaobchádza rovnako. Táto úroveň služby je založená na informáciách, ktoré ste poskytli vo vašej politike.

Riadenie vstupu
Riadenie vstupu obsahuje algoritmus rozhodovania, ktorý smerovač používa pri rozhodovaní, či je dostatok smerovacích prostriedkov na to, aby bol akceptovaný požadovaný QoS na nový tok. Ak nie je dostatok prostriedkov, je nový tok zamietnutý. Ak je tok akceptovaný, vyhradí smerovač požadovaný QoS priradením plánovača a triedič paketov. Kontrola vstupu sa na každom smerovači objavuje zároveň s cestou rezervovania.

Táto diskusia o triedičoch a plánovačoch neobsahuje úplné informácie. Ak chcete vyhľadať alternatívne zdroje informácií, zobrazte si stránku s informáciami súvisiacimi s QoS.

Typy integrovaných služieb
Existujú dva typy integrovaných služieb: riadená záťaž a typ s garanciou.

Riadené zaťaženie

Služba riadeného zaťaženia podporuje aplikácie, ktoré sú vysoko citlivé na preplnené siete, ako sú aplikácie v reálnom čase. Aplikácie musia tiež byť tolerantné voči nízkym množstvám strát a oneskorení. Ak aplikácia používa službu riadeného zaťaženia, jej výkon nebude trpieť zvýšením zaťaženia siete. Prevádzka bude zabezpečovaná službou, podobnou prevádzke v sieti za bežných okolností.

Smerovače musia zabezpečiť, že služba riadeného zaťaženia dostáva adekvátnu šírku pásma a zdroje spracúvania paketov. Aby to tak bolo, musia podporovať QoS s podporou integrovaných služieb. Musíte skontrolovať špecifikácie smerovačov, aby ste zistili, či poskytujú QoS cez funkciu riadenia prevádzky. Riadenie prevádzky pozostáva z nasledujúcich komponentov: rozvrhový program paketov, klasifikátor paketov a riadenie prístupu.

Garantovaná služba
Garantovaná služba zabezpečuje, že pakety dorazia v určenej dodacej lehote. Aplikácie, ktoré potrebujú garantovanú službu, zahŕňajú systémy video a audio vysielania, ktoré používajú technológie vysielania na internete. Garantovaná služba riadi maximálne oneskorenie radenia, takže pakety nebudú oneskorené viac ako o určené množstvo času. Každý smerovač pozdĺž cesty paketu musí poskytovať schopnosti RSVP na zaručenie doručenia. Keď priraďujete limity bloku tokenov a limity šírky pásma, definujete garantovanú službu. Garantovaná služba sa dá použiť len na aplikácie používajúce protokol TCP.

Limity pre blok tokenov a šírku pásma
Limity pre blok tokenov a šírku pásma sú známe pod pojmom limity pre výkon. Tieto limity výkonu pomáhajú garantovať doručenie paketov vo výstupných politikách šírky pásma, a to pre integrovanú aj diferencovanú službu.

Veľkosť bloku tokenov
Veľkosť bloku tokenov určuje množstvo informácií, ktoré môže váš server v každom okamihu spracovať. Ak aplikácia odosiela informácie vášmu serveru rýchlejšie, ako server dokáže odosielať údaje von zo siete, pamäťový blok pretečie. So všetkými dátovými paketmi presahujúcimi túto hranicu sa zaobchádza ako s paketmi mimo profilu. Politiky integrovaných služieb sú pre toto pravidlo výnimkou. Môžete si vybrať Neobmedziť, čím povolíte požiadavku o pripojenie RSVP. Pre všetky ostatné politiky môžete určiť spôsob spracovania premávky mimo profilu. Maximálna veľkosť bloku tokenov je 1 GB.

Limit rýchlosti tokenov
Limit rýchlosti špecifikuje dlhodobú prenosovú rýchlosť alebo počet bitov za sekundu, ktoré je možné do siete odoslať. Politika QoS berie požadovanú šírku pásma a porovnáva ju s limitmi rýchlosti a toku pre túto politiku. Ak požiadavka zapríčiní presiahnutie limitov servera, server požiadavku zamietne. Limit rýchlosti symbolu sa používa iba pre riadenie prístupu v rámci politík integrovaných služieb. Táto hodnota sa môže pohybovať od 10 Kb/s až do 1 Gb/s. Môžete taktiež nastaviť voľbu Neobmedziť. Ak pre rýchlosť nastavíte Neobmedziť, vytvoríte hranicu pre dostupné prostriedky.

Odporúčanie: Ak chcete zistiť, aké limity máte nastaviť, spustite monitor. Vytvorte politiku so súhrnným limitom rýchlosti symbolov dostatočne veľkým, aby zhromaždila väčšinu prevádzky údajov na vašej sieti. Potom spustite zhromažďovanie údajov na tejto politike. Pozrite si príklad Monitorovať aktuálne štatistiky siete, kde nájdete jednu z možností, ako zhromaždiť všetky rýchlosti, ktoré vaša aplikácia a sieť aktuálne používa. Prostredníctvom týchto výsledkov môžete limity náležite znížiť.

Ak chcete zobraziť údaje monitora v reálnom čase namiesto zobrazenia konkrétneho zhromažďovania údajov, spustite monitor. Monitor dokáže zobraziť štatistiky v reálnom čase pre všetky aktívne politiky.

Integrovaná služba používajúca značky diferencovanej služby
Táto politika sa najčastejšie používa, keď máte zmiešané prostredie. Zmiešané prostredie nastane v prípade, ak rezervácia integrovanej služby prechádza cez smerovače, ktoré nepodporujú rezervácie integrovaných služieb, ale podporujú diferencovanú službu. Keďže vaša prevádzka prechádza cez rôzne domény, zmluvy o úrovni služieb a možnosti zariadení, nemusíte vždy dostať službu, ktorú chcete.

Aby ste zmiernili tento potenciálny problém, vašej politike integrovaných služieb môžete pripojiť značku diferencovanej služby. V prípade, že politika prechádza smerovačom, ktorý nemôže používať protokol RSVP, si vaša politika stále zachová istú prioritu. Označenie, ktoré pridávate, sa nazýva správanie pri skoku.

Bez signalizácie

Ako doplnok k používaniu značiek, ako je opísané vyššie, môžete tiež použiť funkciu ″bez signálu″. Ak si vyberiete toto, rozhrania API vo verzii ″bez signálu″ vám umožnia napísať aplikáciu, ktorá spôsobí zavedenie pravidla RSVP na serveri a bude vyžadovať, aby musela byť schopná používania RSVP len aplikácia konverzácie TCP/IP na strane

servera. Signalizácia RSVP sa pre klientsku stranu vykoná automaticky. Pripojenie RSVP sa pre aplikáciu vytvorí, aj keď klientska strana nie je schopná používať protokol RSVP.

Funkcia ″bez signálu″ je špecifikovaná v rámci politiky integrovaných služieb. Funkciu bez signálu stanovujete v paneli **Vlastnosti** akejkoľvek politiky integrovanej služby.

1. V iSeries(TM) Navigator rozviňte váš server —> **Sieť—> Politiky IP**.
2. Kliknite pravým tlačidlom na **Kvalita služieb** a zvoľte **Konfigurácia**.
3. Rozviňte **Politiky výstupnej šírka pásma —> IntServ**.
4. Pravým tlačidlom kliknite na požadovaný názov politiky IntServ a vyberte **Vlastnosti**. Otvorí sa dialógové okno Vlastnosti IntServ.
5. Vyberte záložku **Manažment prevádzky** na zakázanie alebo povolenie signalizácie. Takisto tam môžete upravovať rozvrh, klienta, aplikácie a manažment prevádzky.

Pozrite si témy trieda služby a integrovaná služba, kde nájdete viac informácií.

Politika povolenia vstupu

Politika povolenia vstupu sa používa na obmedzenie premávky snažiacej sa pripojiť k vášmu serveru. Prístup na váš server iSeries(TM) môžete obmedziť podľa klienta, URI, aplikácie alebo lokálneho rozhrania. Okrem toho môžete zlepšiť výkon servera použitím triedy služby pre vstupujúcu premávku. Túto politiku nadefinujete prostredníctvom Sprievodcu povolenia vstupu v programe iSeries Navigator.

Pre politiku vstupu existujú tri komponenty, ktoré vyžadujú viac informácií. Sú to URI na obmedzenie premávky, rýchlosti pripojenia definované v triede služby a prioritné fronty na zoradenie úspešných pripojení. Pozrite si nasledujúce, kde nájdete viac informácií:

- URI (Pozrite 11)
- Rýchlosť pripojenia (Pozrite 12)
- Váhované prioritné fronty (Pozrite 12)

URI
Uvážte použitie politiky vstupu na obmedzenie premávky HTTP pripájajúcej sa k vášmu webovému serveru. V tomto prípade môžete vytvoriť politiku povolenia vstupu, ktorá obmedzuje premávku podľa špecifického URI. Rýchlosť požiadaviek o URI je súčasť riešenia, pomáhajúca chrániť servery pred ich možným zahltením. Určením konkrétnych URI sa aplikuje použitie riadenia vstupov, založené na informáciách z aplikačnej úrovne, na obmedzenie požiadaviek o URI akceptovaných serverom. V odvetví sa to nazýva aj *kontrola požiadavky pripojenia založená na hlavičke*, ktorá používa URI na nastavenie priorít.

Špecifikovanie URI umožní politike vstupu preskúmať aj obsah, nie len hlavičky paketov. Preskúmaným obsahom je názov URI. V iSeries môžete použiť relatívny názov URI (napríklad, **/products/clothing**). Doleuvedené príklady popisujú relatívne URI.

Relatívne URI
Relatívne URI je v skutočnosti podsada absolútneho URI (podobné starému absolútnemu URL). Pozrite si tento príklad: http://www.ibm.com/software. **http://www.ibm.com/software** segment sa považuje za absolútne URI. Segment **/software** je relatívne URI. Všetky relatívne URI hodnoty musia začať s jedným lomítkom (/). Nasledujú platné príklady relatívneho URI:

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

Poznámka:

- Pri používaní URI musíte špecifikovať protokol TCP. Okrem toho sa musí port a adresa IP zhodovať s portom a adresou IP nakonfigurovanou pre váš server HTTP. Typicky to je port 80.
- Pri zadávaní URI sa používa implicitný zástupný znak. Napríklad zadaním /software zahrniete všetko vnútri adresára software.
- V URI nepoužívajte znak *. Tento znak nie je platný.
- Informácie o URI sa dajú použiť buď v politikách vstupu, alebo v (výstupnej) politike diferencovaných služieb.

Predtým, ako nastavíte politiku vstupu používajúcu URI skontrolujte, či port aplikácie priradený pre URI zodpovedá direktíve 'Listen' povolenej pre FRCA v konfigurácii webového servera Apache Web Server. Ak chcete zmeniť alebo zobraziť port pre váš server HTTP, pozrite si túto tému: Manažovať adresy a porty pre váš server HTTP (založený na Apache).

Rýchlosť pripojenia
Súčasťou politiky povolenia vstupu je aj to, že musíte vybrať triedu služby. Táto trieda služby definuje rýchlosti pripojenia, ktoré slúžia ako riadenie vstupu na obmedzenie pripojení akceptovaných serverom.

Limity rýchlosti pripojenia akceptujú alebo zamietnu nový paket na základe priemerného počtu pripojení za sekundu a na základe maximálneho počtu okamžitých pripojení definovaného v politike, ktorú vytvárate. Tieto limity pripojení sa skladajú z limitov priemernej a maximálnej hodnoty rýchlosti, na zadanie ktorých vás v programe iSeries Navigator vyzvú sprievodcovia. Ak prichádzajúce požiadavky o pripojenie dosiahnu server, server zanalyzuje informácie v hlavičke paketu aby zistil, či je táto premávka definovaná v politike. Systém overuje tieto informácie voči profilu obmedzení pripojenia. Ak sa paket nachádza vnútri medzných hodnôt, uloží sa do frontu.

Vyššie uvedené informácie použite po dokončení Sprievodcu povolenia vstupu. Po dokončení konfigurácie politiky môžete v programe iSeries Navigator tiež použiť priradenú Pomoc, kde môžete nájsť podobné informácie.

Váhované prioritné fronty
Ako súčasť riadenia vstupu môžete špecifikovať prioritu, v ktorej sa budú požiadavky o pripojenie spracúvať po vyhodnotení pomocou politík. Priradením váhy prioritnému frontu v skutočnosti riadite dobu odozvy frontu po príchode pripojenia. Ak sa pripojenie uloží do frontu, pripojenie sa spracuje podľa hodnoty priority frontu (vysoká, stredná, nízka alebo premávka s nízkou prioritou). Ak si nie ste istý, ktorú váhu máte priradiť, použite predvolené hodnoty. Súčet všetkých váh sa musí rovnať 100. Napríklad: Ak je špecifikované 25 pre všetky priority, potom všetky fronty budú spracúvané rovnako. Predstavte si, že špecifikujete tieto váhy: Vysoká (50), Stredná (30), Nízka (15) a premávka s nízkou prioritou (5). Akceptované pripojenia potom zahrňujú:

- 50% z pripojení s vysokou prioritou
- 30% z pripojení so strednou prioritou
- 15% z pripojení s nízkou prioritou
- 5% pripojení premávky s nízkou prioritou

Trieda služby

Politiky diferencovaných služieb a politiky povolenia vstupu používajú triedu služby na zoskupenie premávky do tried. Napriek tomu, že veľa z tohto sa uskutočňuje prostredníctvom hardvéru, vy riadite spôsob, akým sa premávka zoskupuje a akú prioritu musí premávka prijať.

Politiky budete definovať až po realizácii QoS. Politiky určujú kto, čo, kde a kedy. Potom musíte priradiť triedu služby vašej politike. Triedy služby sú definované osobitne a môžu byť opätovne použité politikami. Pri definovaní triedy služby špecifikujete, či je ju možné aplikovať na politiku vstupu, výstupu alebo obidva typy politík. Ak si vyberiete poslednú voľbu (vstup aj výstup), potom danú triedu služby môže používať politika diferencovaných služieb aj politika povolenia vstupu.

Nastavenia v rámci triedy služby závisia na tom, či je používaná pre politiku vstupu, výstupu alebo obidva typy politík. Pri vytváraní triedy služby môžete naraziť na nasledujúce požiadavky:

Značkovanie kódovým bodom
Kvalita služby používa odporúčané kódové body na priradenie skokového správania premávke. Smerovače a prepínače používajú tieto kódové body na priradenie úrovne priority premávke. Váš server nedokáže použiť tieto kódové body, pretože sa nespráva ako smerovač. Na základe vašej individuálnej potreby pre vašu sieť musíte určiť, ktoré kódové body sa pre ňu použijú. Uvážte, ktoré aplikácie sú pre vás najdôležitejšie a ktorým politikám treba priradiť vyššiu prioritu. Najdôležitejšou vecou je, aby boli konzistentné s vašimi označeniami, aby ste dosiahli výsledky, ktoré očakávate. Tieto kódové body budú kľúčovou časťou diferenciácie rôznych tried premávky.

Meranie premávky
Kvalita služby používa limity riadenia rýchlosti na obmedzenie premávky prechádzajúcej cez vašu sieť. Tieto limity sú dané nastavením veľkosti bloku tokenov, limitu špičkovej rýchlosti a limitu priemernej rýchlosti. Viac informácií o konkrétnych hodnotách nájdete na stránke Limit veľkosti bloku tokenov a šírky pásma.

Premávka mimo profilu
Konečná časť triedy služieb je spracúvanie mimo profilu. Ak priradíte vyššie uvedené limity riadenia rýchlosti, nastavíte hodnoty na obmedzenie premávky. Keď premávka presiahne tieto obmedzenia, pakety sa považujú za mimo profilu. Informácia v triede služby hovorí serveru, či má zrušiť premávku UDP a redukovať okno preťaženia TCP, tvarovať alebo zaznamenávať pakety mimo profilu.

Zrušiť pakety UDP alebo redukovať okno preťaženia TCP: Ak sa rozhodnete zrušiť a prispôsobiť pakety mimo profilu, pakety UDP sa zrušia. Predsa len, okno preťaženia TCP sa zredukuje, takže prenosová rýchlosť sa vyrovná rýchlosti bloku tokenov. Počet paketov, ktoré je možné kedykoľvek odoslať do siete, sa zníži a teda sa zredukuje aj preťaženie.

Oneskorenie (Tvarovať): Ak oneskoríte pakety mimo profilu, tvarovaním sa prispôsobia vašim definovaným prenosovým vlastnostiam.

Znovu označkovať kódovými bodmi DifffServ: Ak znovu označkujete pakety mimo profilu kódovými bodmi, znovu im priradíte nový kódový bod. Pakety sa neobmedzia, aby vyhovovali vašej charakteristike spracovania, len na nanovo označia. Keď priradíte tieto inštrukcie spracovania v sprievodcovi, kliknite na Pomoc pre špecifickejšie informácie.

Priorita
Ak chcete, môžete priradiť priority pripojeniam, ktoré sú zriadené pre váš server pomocou rôznych politík riadenia povolenia vstupu. Toto vám umožní definovať poradie, podľa ktorého váš server bude spracúvať dokončené pripojenia. Môžete si zvoliť medzi vysokou, strednou a nízkou prioritou alebo premávku s nízkou prioritou.

Použiť kódové body na priradenie skokového správania

Kvalita služby (QoS) používa nasledujúce odporúčané kódové body na priradenie skokového správania premávke. V sprievodcovi triedy služby musíte priradiť skokové správanie pre vašu politiku. Na základe vašej individuálnej potreby pre vašu sieť musíte určiť, ktoré kódové body sa pre ňu použijú. Iba vy môžete rozhodnúť, aké schémy kódových bodov majú zmysel pre vaše prostredie. Musíte uvážiť, ktoré aplikácie sú pre vás najdôležitejšie a ktorým politikám možno treba priradiť vyššiu prioritu. Najdôležitejšou vecou je, aby boli konzistentné s vašimi označeniami, aby ste dosiahli výsledky, ktoré očakávate. Napríklad politikám majúcim rovnakú dôležitosť môžete priradiť podobné kódové body, čím dosiahnete konzistentné výsledky pre tieto politiky. Ak si nie ste istý, ktoré kódové body máte priradiť, použite metódu pokusu a omylu. Vytvorte testovacie politiky, monitorujte tieto politiky a v súlade s tým uskutočnite prispôsobenia.

Nižšie uvedená tabuľka zobrazuje odporúčané kódové body založené na priemyselných štandardoch. Aj keď veľa ISP bude podporovať kódové body založené na priemyselných štandardoch, overte podporu vášho ISP. Ak chcete získať

viac informácií o dohodách úrovne služieb a role vášho ISP, pozrite si stránku Dohody úrovne služieb. Tiež môžete vytvoriť vaše vlastné kódové body; toto sa ale neodporúča pre externé použitie. Vaše vlastné kódové body sú najlepšie použiteľné v testovacom prostredí.

Urýchlené postupovanie (Pozrite 14)
101110

Selektor triedy (Pozrite 14)
Trieda 0 - 000000
Trieda 1 - 001000
Trieda 2 - 010000
Trieda 3 - 011000
Trieda 4 - 100000
Trieda 5 - 101000
Trieda 6 - 110000
Trieda 7 - 111000

Zaistené postupovanie (Pozrite 15)
Zaistené odosielanie, trieda 1, nízke - 001010
Zaistené odosielanie, trieda 1, stredné - 001100
Zaistené odosielanie, trieda 1, vysoké - 001110
Zaistené odosielanie, trieda 2, nízke - 010010
Zaistené odosielanie, trieda 2, stredné - 010100
Zaistené odosielanie, trieda 2, vysoké - 010110
Zaistené odosielanie, trieda 3, nízke - 011010
Zaistené odosielanie, trieda 3, stredné - 011100
Zaistené odosielanie, trieda 3, vysoké - 011110
Zaistené odosielanie, trieda 4, nízke - 100010
Zaistené odosielanie, trieda 4, stredné - 100100
Zaistené odosielanie, trieda 4, vysoké - 100110

Urýchlené postupovanie
Urýchlené postupovanie je jedným z typov skokového správania. Používa sa hlavne na poskytovanie garantovanej služby medzi sieťami. Zrýchlené odosielanie dáva prevádzke nízkostratovú, stabilnú, službu medzi dvomi koncami garantovaním šírky pásma medzi sieťami. Rezervácia sa vykoná pred odoslaním paketu. Hlavným cieľom je zabrániť oneskoreniu a doručiť paket včas.

Poznámka: Za obdržanie dohody o urýchlenom postupovaní typicky platíte vysokou cenou, preto sa neodporúča použiť tento typ skokového správania ako bežné východisko.

Selektor triedy
Kódové body selektora triedy predstavujú iný typ správania. Existuje sedem tried. Trieda 0 dáva paketom najnižšiu

prioritu a Trieda 7 dáva paketom najvyššiu prioritu v rámci hodnôt kódových bodov selektora triedy. Je to najbežnejšia skupina správaní pri skokoch, lebo väčšina smerovačov už používa podobné kódové body.

Zaistené postupovanie
Zaistené odosielanie sa delí na štyri triedy správaní pri skokoch, z ktorých každá má nízku, strednú alebo vysokú úroveň precedensu zrušenia. Úroveň precedensu zrušenia určuje pravdepodobnosť zrušenia paketov. Každá trieda má vlastnú špecifikáciu šírky pásma. Trieda 1, Vysoká priorita, politike priradí najnižšiu prioritu a trieda 4, Nízka priorita, priradí politike najvyššiu prioritu. Nízka úroveň zrušenia označuje, že pakety v tejto politike majú najmenšiu pravdepodobnosť na zrušenie v tejto úrovni triedy.

Limity priemernej a maximálnej rýchlosti pripojení

Rýchlosti pripojení a maximálne rýchlosti sú dokopy známe ako limity rýchlosti. Tieto obmedzenia úrovne pomáhajú ohraničiť vstupné pripojenia pokúšajúce sa vstúpiť na váš server. Limity rýchlostí sa nastavujú v triede služby, ktorá sa používa spolu s politikami povolenia vstupu.

Maximálna rýchlosť pripojenia
Veľkosť maximálnej rýchlosti pripojenia určuje kapacitu pamäťového bloku, ktorá uchováva maximálne rýchlosti pripojení. Nárazy pripojenia môžu vstupovať na server rýchlejšou úrovňou, ako môže zvládať, alebo akú chcete povoliť. Ak počet pripojení v náraze prekročí nastavenú úroveň nárazu pripojenia, potom sú dodatočné spojenia zrušené.

Priemerná úroveň pripojenia
Priemerná úroveň pripojenia určuje obmedzenie nových, vytvorených pripojení, alebo úroveň prijatých URI požiadaviek pripustených na server. Ak by požiadavka zapríčinila presiahnutie vami nastavených limitov, server požiadavku zamietne. Obmedzenie požiadavky priemerného pripojenia sa meria v pripojeniach za sekundu.

Odporúčanie: Ak chcete zistiť, aké limity máte nastaviť, spustite monitor. Pozrite si stránku Monitorovať aktuálne štatistiky siete pre vzorovú politiku, ktorá vám pomôže zhromaždiť väčšinu údajov prechádzajúcich cez váš server. Použitím týchto výsledkov môžete limity okamžite nastaviť.

Ak chcete zobraziť údaje monitora v reálnom čase namiesto zobrazenia konkrétneho zhromažďovania údajov, spustite monitor. Monitor dokáže zobraziť štatistiky v reálnom čase pre všetky aktívne politiky.

Rozhrania API QoS

Väčšina politík QoS vyžaduje používanie API. Nasledujúce rozhrania API sa dajú používať v spojení s politikami diferencovaných alebo integrovaných služieb. Existuje tiež istý počet rozhraní API, ktoré sa dajú použiť s Monitorom QoS.

- Rozhrania API integrovaných služieb (Pozrite 15)
- Rozhrania API diferencovaných služieb (Pozrite 16)
- Rozhrania API monitora (Pozrite 16)

Rozhrania API integrovaných služieb

Protokol rezervovania zdrojov (RSVP), spolu s RAPI API alebo qtoq QoS sockets API, vykonáva vašu rezerváciu integrovaných služieb. Každý uzol, cez ktorý prechádza vaša prevádzka, musí mať schopnosť používať protokol RSVP. Schopnosť vykonávať politiky integrovaných služieb je často označovaná ako povolený RSVP. Viac informácií o funkciách smerovačov, ktoré sú potrebné pre použitie protokolu RSVP nájdete v časti Funkcie riadenia premávky.

Protokol RSVP sa používa na vytváranie rezervácií RSVP na všetkých sieťových uzloch na celej trase prevádzky. Udržiava rezervácie dosť dlho na to, aby poskytol služby, požadované vašou politikou. Rezervácia definuje spracovanie a šírku pásma, ktorú budú údaje v tejto konverzácii vyžadovať. Každý zo sieťových uzlov súhlasí s poskytnutím spracovania údajov, definovaného v rezervácii.

RSVP je jednoduchý protokol, v ktorom sa rezervácie vykonávajú iba jedným smerom (od prijímateľa). Pre komplexnejšie pripojenia, ako sú audio- a videokonferencie, je každý odosielateľ súčasne prijímateľom. V tomto prípade musíte nastaviť dve relácie RSVP pre každú stranu.

Okrem smerovačov, podporujúcich RSVP, musíte mať na používanie integrovaných služieb aj aplikácie, ktoré podporujú RSVP. Pretože server iSeries(TM) teraz nemá aplikácie podporujúce RSVP, budete musieť napísať tieto aplikácie pomocou RAPI API alebo qtoq QoS Sockets API. To umožní aplikáciám používať protokol RSVP. Ak chcete podrobnejšie vysvetlenie, existuje veľa zdrojov vysvetľujúcich tieto modely, ich operácie a manažment správ. Potrebujete dôkladné znalosti protokolu RSVP a obsahu Internet RFC 2205.

Rozhrania API qtoq sockets
Teraz môžete používať qtoq QoS sockets API na zjednodušenie práce, potrebnej na používanie protokolu RSVP na systéme iSeries. qtoq sockets API volajú RAPI API a vykonávajú niektoré z komplexnejších úloh. qtoq sockets API nie sú také flexibilné ako RAPI API, ale poskytujú rovnakú funkčnosť s nižšou námahou. Verzie API ″Bez signálu″ vám umožnia napísať nasledujúcim spôsobom:

- Aplikáciu, ktorá zavedie pravidlo RSVP na server.
- Aplikáciu, ktorá na to, aby podporovala RSVP, potrebuje iba aplikáciu (konverzácie TCP/IP) na strane servera.

Signalizácia RSVP sa pre klientsku stranu vykoná automaticky.

Pozrite si stránku API Connection oriented functional flow QoS, alebo stránku API Connectionless functional flow QoS, kde nájdete typický tok API QoS pre aplikáciu/protokol používajúci spojovo-orientované alebo bezspojové sokety qtoq QoS.

Rozhrania API diferencovaných služieb

Poznámka: API funkcie sendmsg() sa používa pre politiky diferencovaných služieb, ktoré definujú špecifický token aplikácie. Pri vytváraní politiky diferencovaných služieb môžete (voliteľne) poskytnúť charakteristiky aplikácie (token a prioritu). Toto je rozšírená definícia politiky a ak sa nepoužije, toto API sa môže ignorovať. Nezabudnite, že smerovače a iné servery pozdĺž siete musia byť typu DiffServ.

Ak sa rozhodnete použiť token aplikácie v politike diferencovaných služieb, aplikácia poskytujúca túto informáciu musí byť špecificky nakódovaná na používanie API funkcie sendmsg(). Toto realizuje aplikačný programátor. Dokumentácia aplikácie musí poskytnúť platné hodnoty (tokeny a priority), ktoré administrátor QoS použije v politike diferencovaných služieb. Potom politika diferencovaných služieb použije svoju vlastnú prioritu a klasifikáciu pre premávku, ktorá zodpovedá tokenu nastaveného v politike. Ak aplikácia nemá hodnoty, ktoré zodpovedajú hodnotám nastaveným v politike, buď musíte aplikáciu vymeniť, alebo musíte použiť iné parametre pre údaje aplikácie pre politiku diferencovaných služieb.

Nasledujúce informácie stručne opisujú parametre údajov servera: token aplikácie a prioritu aplikácie.

Čo je token aplikácie?
Token aplikácie je URI reprezentujúce definovaný prostriedok. Vami zadaný token v politike QoS sa porovná s tokenom poskytnutým vonkajšou aplikáciou. Aplikácia poskytuje hodnotu tokenu prostredníctvom API funkcie sendmsg(). Ak sú tokeny rovnaké, premávka aplikácie sa zahrnie do politiky diferencovaných služieb.

Čo je priorita aplikácie?
Vami zadaná priorita aplikácie sa porovná s prioritou aplikácie poskytnutou vonkajšou aplikáciou. Aplikácia poskytuje hodnotu priority prostredníctvom API funkcie sendmsg(). Ak sú priority rovnaké, premávka aplikácie sa zahrnie do politiky diferencovaných služieb. Celá premávka definovaná v politike diferencovaných služieb bude stále prijímať prioritu udelenú celej politike.

Ak chcete získať viac informácií o politike typu DiffServ, pozrite si časť diferencovaná služba.

Rozhrania API monitora

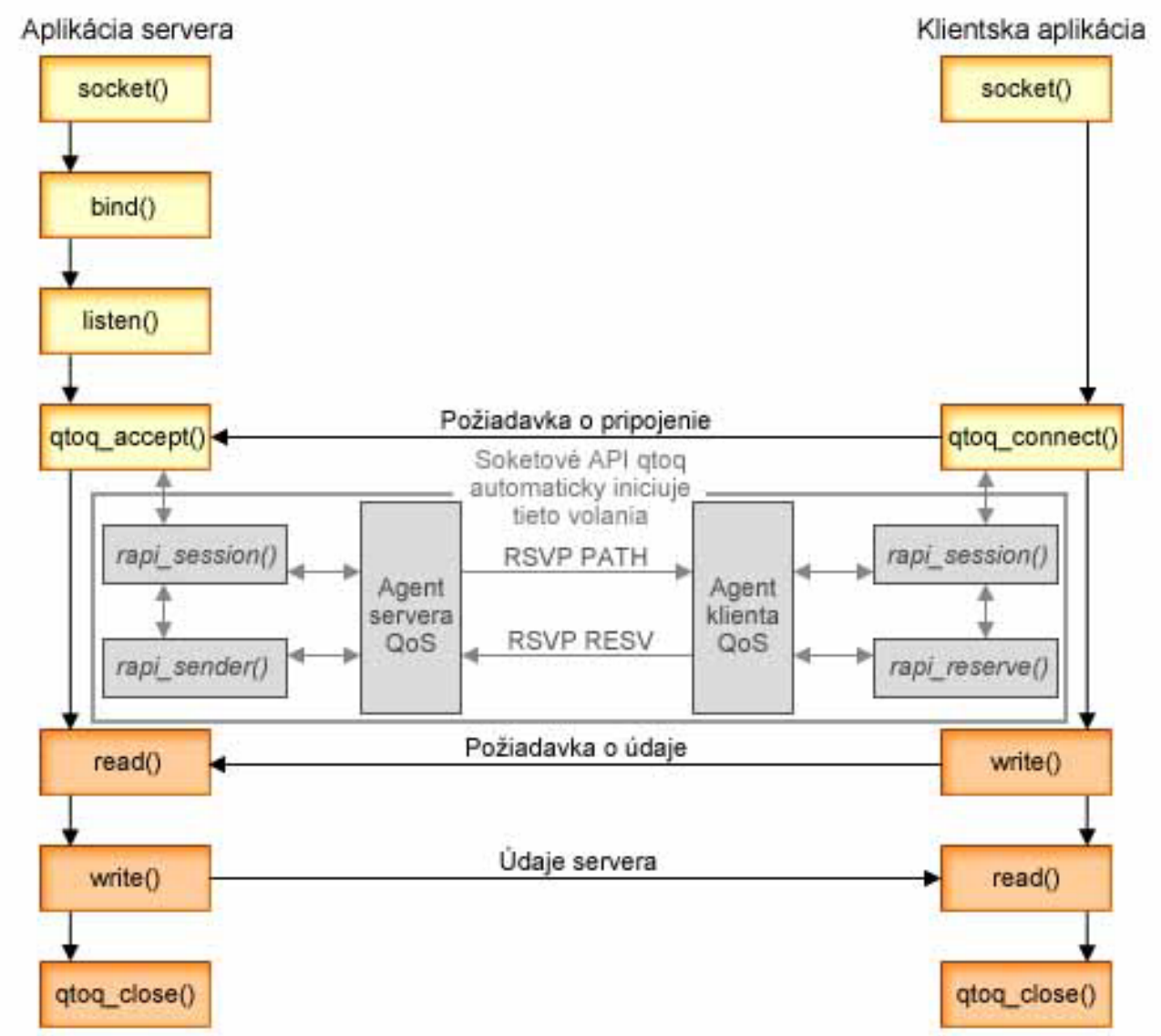
Ak chcete používať rozhrania API monitora, pozrite si Rozhrania API protokolu nastavenia rezervácie prostriedkov. Rozhrania API, ktoré sa použijú s monitorom, budú mať ako nadpis reťazec ″monitor″. Napríklad *QgyOpenListQoSMonitorData*. Nasledujúci zoznam stručne opisuje každé API monitora:

- QgyOpenListQoSMonitorData (Otvoriť zoznam údajov monitora QoS) získa informácie súvisiace so službami QoS.
- QtoqDeleteQoSMonitorData (Vymazať údaje monitora QoS) vymaže jednu alebo viac množín zhromaždených údajov monitora QoS.
- QtoqEndQoSMonitor (Ukončiť monitor QoS) zastaví získavanie informácií súvisiacich so službami QoS.
- QtoqListSavedQoSMonitorData (Zobraziť uložené údaje monitora QoS) vráti zoznam všetkých uložených zhromaždených údajov monitora.
- QtoqSaveQoSMonitorData (Uložiť údaje monitora QoS) uloží kópiu zhromaždených údajov monitora QoS pre neskoršie použitie.
- QtoqStartQoSMonitor (Spustiť monitor QoS) získa informácie súvisiace so službami QoS.

API Connection Oriented Functional Flow QoS

Nasledujúci obrázok zobrazuje vzťah klient/server soketových funkcií qtoq API podporujúceho QoS pre spojovo-orientovaný protokol, ako je TCP (Transmission Control Protocol).

Keď sa funkcie API podporujúce QoS volané pre tok s pripojením a požadujú, aby sa inicializoval RSVP, inicializujú sa i ďalšie funkcie. Tieto funkcie spôsobujú, že agenti QoS na klientovi a serveri nastavia protokol RSVP pre tok údajov medzi klientom a serverom.



Tok udalostí qtoq: Nasledujúca sekvencia volaní soketov poskytuje popis grafiky. Taktiež popisuje vzťah medzi serverom a klientskou aplikáciou v dizajne, orientovanom na pripojenie. Tieto sú modifikáciami základných soketov API.

Strana servera

Funkcia qtoq_accept() pre pravidlo označené ako ″Bez signálu″

1. Aplikácia volá funkciu socket() na získanie deskriptora soketu.
2. Aplikácia volá listen() na zadanie, na aké pripojenie bude čakať.
3. Aplikácia zavolá funkciu qtoq_accept(), aby čakala na požiadavku o pripojenie od klienta.
4. Aplikácia volá rapi_session() API, a ak je úspešná, bude priradené ID relácie QoS.
5. API volá štandardnú funkciu accept() na čakanie požiadavky na pripojenie klienta.

6. Keď je požiadavka na pripojenie prijatá, vykoná sa kontrola prístupu na požadovanom pravidle. Pravidlo sa odošle do zásobníka TCP/IP. Ak je platné, vráti sa do volajúcej aplikácie s výsledkami a ID relácie.
7. Aplikácie pre server a pre klienta vykonávajú požadovaný prenos údajov.
8. Aplikácia zavolá funkciu qtoq_close() na zatvorenie soketu a zrušenie zavedenia pravidla.
9. Server QoS vymaže pravidlo zo Správcu QoS, vymaže reláciu QoS a vykoná všetky ďalšie potrebné akcie.

Funkcia qtoq_accept() s normálnou signalizáciou RSVP

1. Aplikácia volá funkciu socket() na získanie deskriptora soketu.
2. Aplikácia volá listen() na zadanie, na aké pripojenie bude čakať.
3. Aplikácia zavolá funkciu qtoq_accept(), aby čakala na požiadavku o pripojenie od klienta.
4. Ak do funkcie rapi_session() príde požiadavka o pripojenie, zavolá sa API na vytvorenie relácie pre toto pripojenie so serverom QoS a na získanie ID relácie QoS, ktoré sa odovzdá volajúcemu.
5. Bude volané API rapi_sender() na inicializovanie správy PATH zo servera QoS, ktoré informuje server QoS, že má očakávať správu RESV z klienta.
6. API rapi_getfd() je volané na obstaranie deskriptora, ktorý aplikácie používajú na čakanie na správy o udalostiach QoS.
7. Deskriptor akceptácie a deskriptor QoS sú vrátené do aplikácie.
8. Server QoS čaká na prijatie novej správy RESV. Ak sa správa prijme, server pomocou Správcu QoS zavedie príslušné pravidlo a odošle správu aplikácii, ak aplikácia požadovala notifikáciu vo volaní qtoq_accept() API.
9. Server QoS pokračuje v poskytovaní obnovení pre vytvorenú reláciu.
10. Po dokončení pripojenia aplikácia zavolá funkciu qtoq_close().
11. Server QoS vymaže pravidlo zo Správcu QoS, vymaže reláciu QoS a vykoná všetky ďalšie potrebné akcie.

Strana klienta

Funkcia qtoq_connect() s normálnou signalizáciou RSVP

1. Aplikácia volá funkciu socket() na získanie deskriptora soketu.
2. Aplikácia zavolá funkciu qtoq_connect(), aby informovala aplikáciu servera o požiadavke o vytvorenie pripojenia.
3. Funkcia qtoq_connect() zavolá API funkcie rapi_session() na vytvorenie relácie so serverom QoS pre toto pripojenie.
4. Server QoS sa pri čakaní na príkaz PATH z požadovaného pripojenia uprednostní.
5. API rapi_getfd() je volané na obstaranie deskriptora, ktorý aplikácie používajú na čakanie na správy QoS.
6. Je volaná funkcia connect(). Výsledky connect() a deskriptor QoS sú vrátené aplikácii.
7. Server QoS čaká na prijatie správy PATH. Keď je správa prijatá, bude odpovedať správou RESV na server QoS na počítači aplikačného servera.
8. Ak aplikácia požadovala notifikáciu, server QoS odošle notifikáciu aplikácii cez deskriptor QoS.
9. Server QoS pokračuje v poskytovaní obnovení pre vytvorenú reláciu.
10. Po dokončení pripojenia aplikácia zavolá funkciu qtoq_close().
11. Server QoS zatvorí reláciu QoS a vykoná všetky ďalšie nevyhnutné akcie.

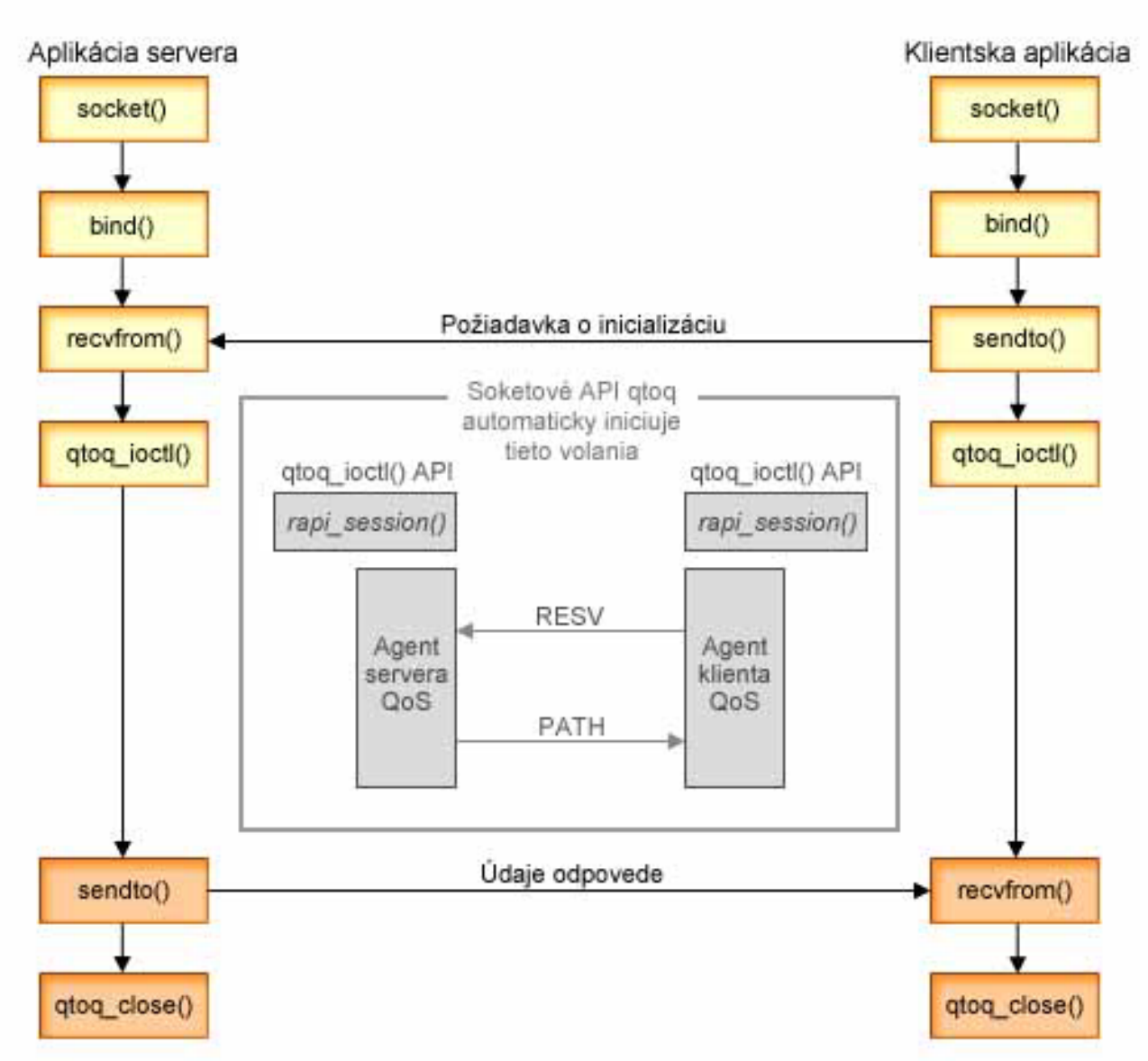
Funkcia qtoq_connect() pre pravidlo označené ako ″Bez signálu″

Táto požiadavka nie je platná pre stranu klienta, pretože v tomto prípade sa od klienta nevyžaduje žiadna odpoveď.

API Connectionless Functional Flow QoS

Tieto príklady servera a klienta ilustrujú soketové rozhrania API qtoq QoS, napísané pre bezspojový tok.

Keď sú funkcie API podporujúce QoS volané pre tok bez pripojenia a požadujú, aby sa inicializoval RSVP, iniciujú sa ďalšie funkcie. Tieto funkcie spôsobujú, že agenti QoS na klientovi a serveri nastavia protokol RSVP pre tok údajov medzi klientom a serverom.



Tok udalostí qtoq: Nasledujúca sekvencia volaní soketov poskytuje popis grafiky. Taktiež popisuje vzťah medzi serverom a klientskou aplikáciou v dizajne bez pripojenia. Tieto sú modifikáciami základných soketov API.

Strana servera

Funkcia qtoq_ioctl() pre pravidlo označené ako ″Bez signálu″

1. Odosiela správu na server QoS a žiada ho o vykonanie kontroly prístupu na požadovanom pravidle.
2. Ak je pravidlo akceptovateľné, volá funkciu, ktorá odosiela správu na server QoS a žiada ho o zavedenie pravidla.
3. Vracia stav volajúcemu a udáva úspech alebo zlyhanie požiadavky.

4. Keď aplikácia skončila používanie pripojenia, zavolá funkciu qtoq_close() na zatvorenie pripojenia.
5. Server QoS vymaže pravidlo zo Správcu QoS, vymaže reláciu QoS a vykoná všetky ďalšie potrebné akcie.

Funkcia qtoq_ioctl() s normálnou signalizáciou RSVP

1. Odosiela správu na server QoS a žiada ho o vykonanie kontroly prístupu pre požadované pripojenie.
2. Volá rapi_session() na požiadanie o nastavenie relácie pre pravidlo a získanie ID relácie QoS, ktoré sa má vrátiť volajúcemu.
3. Volá rapi_sender() na inicializovanie správy PATH späť na klienta.
4. Volá rapi_getfd() na získanie deskriptora súboru, aby čakal na udalosti QoS.
5. Vracia deskriptor select(), ID relácie QoS a stav volajúcemu.
6. Server QoS načítava pravidlo, keď je prijatá správa RESV.
7. Po dokončení pripojenia aplikácia zavolá funkciu qtoq_close().
8. Server QoS vymaže pravidlo zo Správcu QoS, vymaže reláciu QoS a vykoná všetky ďalšie potrebné akcie.

Strana klienta

Funkcia qtoq_ioctl() s normálnou signalizáciou RSVP

1. Volá rapi_session() na požiadanie o nastavenie relácie pre pripojenie. Funkcia rapi_session() žiada o kontrolu prístupu pre pripojenie. Pripojenie bude na klientskej strane odmietnuté, iba ak je na nej nakonfigurované pravidlo pre klienta a nie je momentálne aktívne. Táto funkcia vracia ID relácie QoS, ktoré je vrátené späť do aplikácie.
2. Volá rapi_getfd() na získanie deskriptora súboru, aby čakal na udalosti QoS.
3. qtoq_ioctl() sa vracia späť k volajúcemu s čakaním na deskriptor a ID relácie.
4. Server QoS čaká na prijatie správy PATH. Keď je správa PATH prijatá, odpovedá správou RESV a potom cez deskriptor relácie signalizuje aplikácii, že došlo k udalosti.
5. Server QoS pokračuje v poskytovaní obnovení pre vytvorenú reláciu.
6. Po dokončení pripojenia kód klienta zavolá funkciu qtoq_close().

Funkcia qtoq_ioctl() pre pravidlo označené ako ″Bez signálu″

Táto požiadavka nie je platná pre stranu klienta, pretože v tomto prípade sa od klienta nevyžaduje žiadna odpoveď.

Rozšírenia API QoS Sendmsg()

Funkcia sendmsg() sa používa na odosielanie údajov, podporných údajov, alebo kombinácie týchto údajov prostredníctvom pripojeného alebo nepripojeného soketu. Vo V5R3 sú pridané rozšírenia sendmsg(), ktoré umožňujú klasifikáciu údajov QoS. Politiky QoS používajú túto funkciu na definovanie jemnejšej úrovne klasifikácie pre odchádzajúcu alebo prichádzajúcu premávku TCP/IP. Konkrétne používajú podporné údaje, ktoré sa aplikujú do vrstvy IP. Používaný typ správy je IP_QOS_CLASSIFICATION_DATA. Tieto podporné údaje môže aplikácia použiť na definovanie atribútov pre premávku v konkrétnom pripojení TCP. Ak aplikáciou odovzdané atribúty zodpovedajú atribútom definovaným v politike QoS, potom politika QoS obmedzí premávku TCP. Ak chcete použiť Sendmsg() API, pozrite si Sendmsg() - Odoslať správu cez soket v informáciách o programovaní API. Informácie uvedené nižšie použite na inicializáciu štruktúry IP_QOS_CLASSIFICATION_DATA.

Štruktúru ip_qos_classification_data musíte vyplniť podľa týchto pokynov:

- ip_qos_version: Označuje verziu štruktúry. Toto musíte vyplniť konštantou *IP_QOS_CURRENT_VERSION*
- ip_qos_classification_scope: Špecifikuje rozsah úrovne pripojenia (použite konštantu *IP_QOS_CONNECTION_LEVEL*) alebo rozsah úrovne správy (konštanta *IP_QOS_MESSAGE_LEVEL*).

  Rozsah úrovne pripojenia označuje, že úroveň služby QoS, získaná prostredníctvom klasifikácie tejto správy ostane nezmenená pre všetky nasledujúce správy až po výskyt ďalšej funkcie sendmsg() s údajmi klasifikácie QoS. Rozsah úrovne správy označuje, že sa použije len priradená úroveň služby QoS pre údaje správy zahrnuté v tomto volaní

funkcie sendmsg(). Ďalšie údaje odoslané bez údajov klasifikácie QoS zdedia predošlé priradenie úrovne pripojenia QoS (od poslednej klasifikácie úrovne pripojenia prostredníctvom funkcie sendmsg() alebo od pôvodnej klasifikácie pripojenia TCP počas zriadenia pripojenia).

- ip_qos_classification_type: Táto špecifikácia určuje typ odovzdávaných údajov klasifikácie. Aplikácia si môže zvoliť medzi odovzdaním tokenu definovaného aplikáciou, priority špecifikovanej aplikáciou alebo medzi odovzdaním obidvoch možností, aj tokenu aj priority. Ak sa vyberie posledná možnosť, dva vybraté typy klasifikácie musia byť logicky sčítané (OR). Dajú sa špecifikovať nasledujúce typy:
  - Klasifikácia tokenu definovaného aplikáciou. Musí byť špecifikovaný práve jeden typ, ak sa špecifikuje viac typov, výsledky môžu byť nepredvídateľné.
    - IP_SET_QOSLEVEL_W_APPL_TOKEN_ASCII : Toto označuje, že údaje klasifikácie sú znakový reťazec vo formáte ASCII. Ak je špecifikovaná táto voľba, token aplikácie je potrebné odovzdať v poli ip_qos_appl_token.

      Poznámka: Ak aplikácia vyžaduje odovzdanie číselných hodnôt pre údaje klasifikácie, musí ich najprv skonvertovať do tlačiteľného formátu ASCII. Nezabudnite, že špecifikovaný reťazec môže obsahovať malé aj veľké písmená a presne tento formát sa použije pre prípady porovnávania.
    - IP_SET_QOSLEVEL_W_APPL_TOKEN_EBCDIC : Označuje to isté ako voľba uvedená vyššie okrem toho, že reťazec je vo formáte EBCDIC.

      Poznámka: Voľba IP_SET_QOSLEVEL_W_APPL_TOKEN_ASCII sa realizuje trochu lepšie ako táto voľba, pretože údaje aplikácie špecifikované v politike sa uchovávajú vo formáte ASCII vnútri protokolového zásobníka TCP/IP, čím sa eliminuje potreba konverzie aplikáciou definovaného tokenu pri každej požiadavke funkcie sendmsg().
  - Klasifikácia priority definovanej aplikáciou. Musí byť špecifikovaný práve jeden typ, ak sa špecifikuje viac typov, výsledky môžu byť nepredvídateľné.
    - IP_SET_QOSLEVEL_EXPIDITED: Označuje, že sa vyžaduje Odoslaná priorita
    - IP_SET_QOSLEVEL_HIGH: Označuje, že sa vyžaduje Vysoká priorita
    - IP_SET_QOSLEVEL_MEDIUM: Označuje, že sa vyžaduje Stredná priorita
    - IP_SET_QOSLEVEL_LOW: Označuje, že sa vyžaduje Nízka priorita
    - IP_SET_QOSLEVEL_BEST_EFFORT: Označuje, že sa požaduje premávka s nízkou prioritou.
  - ip_qos_appl_token_len: dĺžka tokenu ip_qos_appl_token.
  - ip_qos_appl_token: Toto ″virtuálne pole″ okamžite nasleduje za poľom ip_qos_classification_type. Označuje reťazec tokenu klasifikácie aplikácie buď vo formáte ASCII alebo EBCIDIC v závislosti od tokenu IP_SET_QOSLEVEL_W_APPL_TOKEN_xxxx špecifikovaného pre typ klasifikácie. Toto pole je referencované len v prípade špecifikácie tokenu definovaného aplikáciou. Nezabudnite, že dĺžka tohto poľa nesmie presiahnuť 128 bajtov. Ak je špecifikovaná väčšia dĺžka, použije sa len prvých 128 bajtov. Nezabudnite, že dĺžka reťazca sa určuje na základe hodnoty špecifikovanej pre cmsg_len (cmsg_len - sizeof(cmsghdr) - sizeof(ip_qos_classification_data)). Táto vypočítaná dĺžka nesmie obsahovať žiadne ukončujúce nulové znaky.

«

Adresárový server

Konfigurácia politiky QoS sa dá exportovať do adresárového servera pri použití najnovšej verzie protokolu LDAP, verzie 3.

Výhody používania adresárového servera

Exportovanie politík QoS do adresárového servera umožní jednoduchší manažment vašich politík. Existujú tri spôsoby použitia adresárového servera:

- Konfiguračné údaje sa dajú uložiť do jedného lokálneho adresárového servera pre zdieľanie viacerými systémami.
- Konfiguračné údaje však môže konfigurovať, uložiť a používať len jeden systém (zdieľanie nie je povolené).

- Konfiguračné údaje môžu byť uložené v adresárovom serveri, ktorý uchováva údaje aj pre iné systémy, ale tieto údaje nie sú zdieľané medzi ostatnými systémami. Toto vám umožňuje použiť jediné umiestnenie na zálohovanie a uloženie údajov pre niekoľko systémov.

Výhody uchovávania výlučne len vo vašom lokálnom serveri
Uchovávanie politík QoS vo vašom lokálnom serveri nie je také komplikované. Existuje niekoľko výhod používania politík lokálne:

- Eliminuje sa zložitosť konfigurácie LDAP pre užívateľov, ktorí to nepotrebujú.
- Zvýši sa výkon, pretože písanie do LDAP nie je najrýchlejšia možná metóda.
- Jednoduchšie duplikovanie konfigurácie medzi rôznymi iSeries(TM). Môžete kopírovať súbor z jedného systému do druhého. Pretože v tomto prípade neexistuje primárny alebo sekundáry počítač, každú politiku môžete prispôsobiť priamo na samotné servery.

Prostriedky LDAP
Ak sa rozhodnete exportovať vaše politiky do servera LDAP, najskôr sa musíte oboznámiť s konceptmi LDAP a so štruktúrami adresárov. Zobrazte tému Adresárový server IBM pre iSeries(LDAP) v Informačnom centre iSeries. Ak chcete získať viac informácií o spôsobe konfigurácie adresárového servera v rámci funkcie Kvalita služby v programe iSeries Navigator, pozrite si Konfigurovať adresárový server.

Pozrite si stránku Blízke informácie pre QoS, kde nájdete niektoré alternatívne zdroje LDAP.

Kľúčové slová
Pri konfigurácii vášho adresárového servera budete musieť určiť, či chcete priradiť kľúčové slová ku každej konfigurácii QoS. Polia kľúčových slov nie sú povinné a môžu sa ignorovať. Nasledujúce informácie pomôžu vysvetliť koncept kľúčových slov a prečo by ste ich mali chcieť používať.

V Sprievodcovi úvodnou konfiguráciou QoS môžete konfigurovať adresárový server. Môžete zadať, či konfigurovaný server bude primárny alebo sekundárny systém. Server, v ktorom máte všetky vaše politiky QoS sa nazýva primárny systém.

Kľúčové slová sa používajú na identifikáciu konfigurácií vytvorených primárnymi systémami. Hoci sú vytvorené na primárnom systéme kľúčové slová sú skutočne užitočné na sekundárnom systéme. Umožňujú sekundárnym systémom načítať a používať konfigurácie vytvorené primárnym systémom. Doleuvedený popis pomôže vysvetliť, ako používať kľúčové slová na každom systéme.

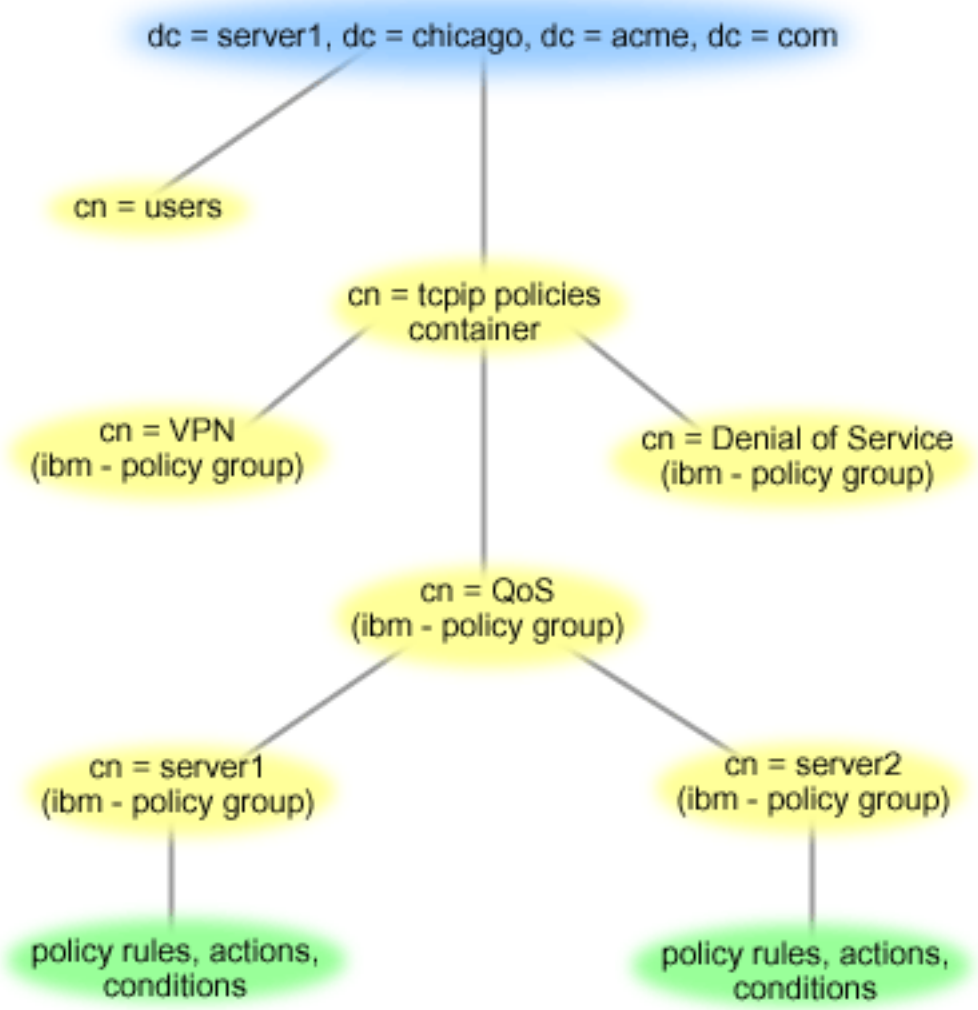
Kľúčové slová na primárnych systémoch
Kľúčové slová sú priradené QoS konfiguráciám vytvoreným a udržiavaným primárnym systémom. Používajú sa, takže sekundárne systémy dokážu identifikovať konfiguráciu vytvorenú primárnym systémom.

Kľúčové slová na sekundárnych systémoch
Sekundárne systémy používajú kľúčové slová na vyhľadávanie konfigurácií. Sekundárny systém načítava a používa konfigurácie vytvorené primárnym systémom. Keď konfigurujete sekundárny systém, môžete si vybrať špecifické kľúčové slová. V závislosti na zvolenom kľúčovom slove sekundárny systém načíta akékoľvek konfigurácie priradené vybranému kľúčovému slovu. Toto umožňuje sekundárnemu systému načítať viaceré konfigurácie vytvorené viacerými primárnymi systémami.

Keď začnete s konfiguráciou adresárového servera v iSeries(TM) Navigator, použite špecifické pokyny v pomoci pre úlohu QoS.

Rozlišovací názov
Ak chcete manažovať časť vášho adresára, pozrite si **Rozlišovací názov (DN)** alebo kľúčové slovo (ak si ho zvolíte). DN špecifikujete pri konfigurácii adresárového servera v rámci Sprievodcu úvodnou konfiguráciou QoS. DN sú typicky zložené z názvu samotnej položky, ako aj objektov (zhora dole) nachádzajúcich sa nad položkou v adresári. Server môže sprístupniť všetky objekty v adresári, ktoré sú pod DN. Povedzme, že server LDAP obsahuje túto adresárovú štruktúru:

Obrázok 12. Vzorová adresárová štruktúra QoS



Server1 hore (dc=server1,dc=chicago,dc=acme,dc=com) je server, na ktorom sa nachádza adresárový server. Ostatné servery, ako sú politiky cn=QoS alebo cn=tcpip, sú tam, kde sa nachádzajú servery QoS. Takže v serveri cn=server1 predvolené DN je cn=server1,cn=QoS,cn=tcpip policies,dc=server1,dc=chicago,dc=acme,dc=com. V serveri cn=server2 predvolené DN je cn=server2,cn=QoS,cn=tcpip policies,dc=server1,dc=chicago,dc=acme,dc=com.

Pri riadení vášho adresára je dôležité zmeniť správny server v DN, ako je cn alebo dc. Pri úprave DN buďte pozorný, pretože typický reťazec je príliš dlhý na to, aby mohol byť zobrazený bez potreby posunu.

Pozrite si stránku Blízke informácie pre QoS, kde nájdete niektoré alternatívne zdroje LDAP.

Scenáre QoS

Jednou z najlepších ciest, ako sa rýchlo naučiť o kvalite služieb, je vidieť, ako funkcia pracuje v celkovej schéme siete. Nasledujúce základné príklady vám vysvetľujú, prečo potrebujete používať politiky kvality služieb a tiež poskytujú postupné kroky s pokynmi na vytváranie politík a tried služieb.

Scenár: Obmedziť premávku prehliadača
Na kontrolu výkonu premávky môžete použiť QoS. Použite politiku diferencovaných služieb buď na obmedzenie, alebo rozšírenie výkonu aplikácie v rámci vašej siete.

Scenár: Bezpečné a predpovedateľné výsledky (VPN a QoS)
Ak používate virtuálnu súkromnú sieť (VPN), ešte stále môžete vytvoriť politiky kvality služieb. Tento príklad vám ukazuje spoločné použitie oboch.

Scenár: Obmedziť prichádzajúce pripojenia
Ak potrebujete kontrolovať požiadavky na prichádzajúce pripojenia uskutočnené na vašom serveri, použite politiku prijatia vstupov.

Scenár: Predvídateľná B2B premávka
Ak potrebujete predpovedateľné doručenie a zároveň potrebujete vyžadovať rezerváciu, použijete taktiež politiku integrovaných služieb. Avšak tento príklad používa službu kontrolovaného zaťaženia.

Scenár: Vyhradené doručenie (IP telefónia)
Ak potrebujete vyhradené doručenie a chcete vyžadovať rezerváciu, použijete politiku integrovaných služieb. Existujú dva typy politík integrovaných služieb, ktoré možno vytvoriť: Zaručená a kontrolovaná záťaž. V tomto príklade sa používa garantovaná služba.

Scenár: Monitorovať aktuálne štatistiky siete QoS
V rámci sprievodcov budete vyzvaný zadať limity výkonu. Sú to však hodnoty, ktoré sa neodporúčajú, pretože sú založené na individuálnych potrebách sietí. Na nastavenie týchto limitov musíte reálne poznať aktuálny výkon vašej siete. Keďže sa pokúšate konfigurovať politiky kvality služieb, pravdepodobne už máte vhodnú predstavu o aktuálnych potrebách vašej siete. Ak chcete určiť presné limity rýchlosti, ako rýchlosť tokenov, môžete monitorovať všetku premávku vo vašom serveri, aby ste mohli lepšie určiť limity rýchlosti na nastavenie.

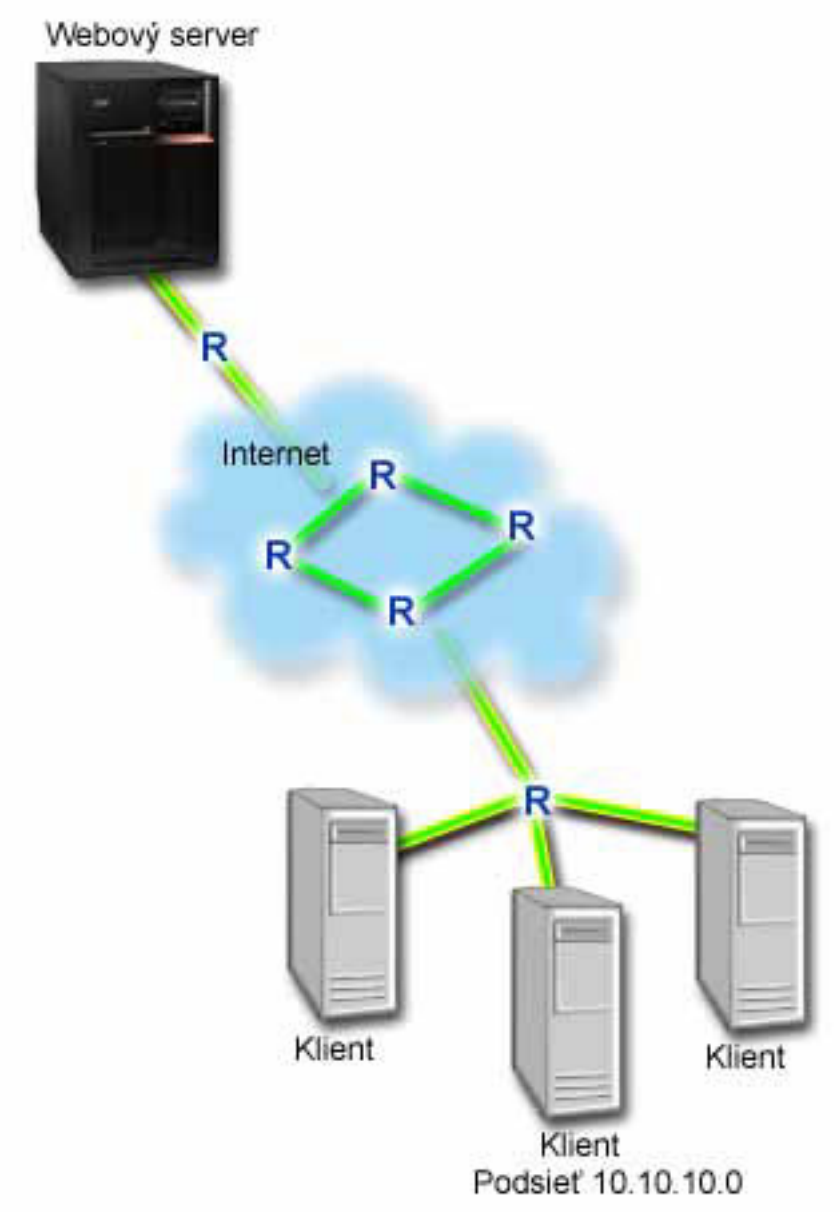
Poznámka: IP adresy a diagramy sú fiktívne a použité len na účely príkladu.

Scenár QoS: Obmedziť premávku prehliadača

Situácia

Vaša spoločnosť zaznamenala vysoké úrovne premávky prehliadača zo skupiny zaoberajúcej sa užívateľským dizajnom (UCD) počas piatkov. Táto premávka interferovala s účtovným oddelením, ktoré taktiež požaduje dobrý výkon od ich účtovných aplikácií počas piatkov. Rozhodnete sa obmedziť premávku prehliadačov z UCD skupiny. Nasledujúca schéma ilustruje nastavenie siete v tomto scenári. Váš server iSeries(TM) beží na OS/400(R) V5R3.

Obrázok 1. Webový server obmedzujúci premávku prehliadača na klienta.



Ciele

Ak chcete obmedziť premávku prehliadača smerom von z vašej siete, vytvorte politiku diferencovaných služieb. Diferencovaná politika služieb rozdeľuje vašu premávku do tried. Všetka premávka v rámci tejto politiky má priradený kódový bod. Tento kódový bod oznamuje smerovačom, ako zaobchádzať s premávkou. V tomto scenári môže byť politike priradená nízka hodnota kódového bodu, čo bude mať vplyv na spôsob stanovenia priorít pre premávku prehliadača sieťou.

Požiadavky a predpoklady

- S vaším ISP máte uzavretú dohodu úrovne služieb (SLA), aby ste zaručili, že politiky prijímajú požadovanú prioritu. Politika QoS, ktorú vytvárate umožňuje premávke (v politike) prijímať prioritu z celej siete. Nezaručuje to a je závislá na vašom SLA. V skutočnosti vám výhody politík QoS dávajú možnosť vysporiadať sa s konkrétnymi úrovňami služieb a rýchlosťami. Použite odkaz na dohodu úrovne služieb, ak sa chcete dozvedieť viac.

- Politiky diferencovaných služieb vyžadujú smerovače typu DiffServ pozdĺž sieťovej cesty. Väčšina smerovačov je typu DiffServ; ak sa chcete dozvedieť viac, pozrite si stránku Diferencovaná služba.

Konfigurácia

Po tom, ako ste skontrolovali požiadavky krok po kroku, ste pripravený na vytvorenie politiky diferencovaných služieb.

1. Vytvoriť politiku diferencovaných služieb (Pozrite 27)
2. Spustiť alebo aktualizovať server QoS (Pozrite 28)
3. Použiť monitor na overenie správnej činnosti vašej politiky (Pozrite 28)
4. Zmeniť vlastnosti (ak treba) (Pozrite 28)

Krok 1: Vytvoriť politiku diferencovaných služieb

1. V programe iSeries Navigator, rozviňte iSeries A **—>Sieť —>Politiky IP**.
2. Pravým tlačidlom kliknite na **Kvalita služby** a vyberte **Konfigurácia**, aby ste otvorili rozhranie QoS.
3. V rozhraní QoS pravým tlačidlom kliknite na typ politiky DiffServ a vyberte **Nová politika**, aby ste spustili sprievodcu.
4. Prečítajte si Uvítaciu stránku a kliknite na tlačidlo **Ďalej**, aby ste sa dostali na stránku **Názov**.
5. V poli **Názov** zadajte UCD. Tiež môžete voliteľne zadať opis na lepšie zapamätanie si účelu tejto politiky. Kliknite na tlačidlo **Ďalej**.
6. Na stránke Klienti vyberte **Špecifická adresa alebo adresy** a kliknite na **Nový**, aby ste zadefinovali vášho klienta.
7. V dialógovom okne Nový klient zadajte nasledujúce informácie a kliknite na tlačidlo **OK**:
   - **Názov**: UCD_Client
   - **Adresa IP a maska**: 10.10.10.0 / 24

   Po kliknutí na tlačidlo OK sa vrátite do sprievodcu politikou. Ak ste už predtým mali vytvorených klientov, zrušte ich označenie a skontrolujte, či sú vybratí len relevantní klienti.
8. Na stránke Požiadavka o údaje servera skontrolujte, či sú vybraté voľby **Všetky tokeny** a **Všetky priority** a kliknite na tlačidlo **Ďalej**.
9. Na stránke aplikácie vyberte **Špecifický port, rozsah portov alebo typ servera** a kliknite na **Nový**.
10. V dialógovom okne Nová aplikácia zadajte nasledujúce informácie a kliknite na tlačidlo **OK**, aby ste sa vrátili do sprievodcu:
    - **Názov**: HTTP
    - **Port**: 80
11. Na stránke Aplikácie vyberte **Protokol** a skontrolujte, či je vybraté **TCP**. Kliknite na tlačidlo **Ďalej**.
12. Na stránke Lokálna adresa IP skontrolujte, či sú vybraté **Všetky adresy IP** a kliknite na tlačidlo **Ďalej**.
13. Na stránke Diferencovaná trieda služby kliknite na **Nový**, aby ste zadefinovali charakteristiky výkonu. Zobrazí sa Sprievodca novou triedou služby.
14. Prečítajte si Uvítaciu stránku a kliknite na tlačidlo **Ďalej**.
15. Na stránke Názov zadajte UCD_service. Tiež môžete voliteľne zadať opis na lepšie zapamätanie si účelu tejto politiky. Kliknite na tlačidlo **Ďalej**.
16. Na stránke Typ služby vyberte **Iba výstup** a kliknite na tlačidlo **Ďalej**. Táto trieda služby sa použije len pre politiky výstupu.
17. Na strane Označenie kódových bodov odchádzajúceho DiffServ vyberte **Trieda 4** a kliknite na **Ďalej**. Skokové správanie určuje, aký výkon prijme táto premávka od smerovačov a iných serverov v sieti. Použite Pomoc priradenú k rozhraniu na uľahčenie vášho rozhodovania.
18. Na stránke Vykonať meranie odchádzajúcej premávky skontrolujte, či je vybraté **Áno** a kliknite na tlačidlo **Ďalej**.
19. Na stránke Limity riadenia rýchlosti výstupu zadajte nasledujúce informácie a kliknite na tlačidlo **Ďalej**:
    - **Veľkosť bloku tokenov**: 100 kilobitov

- **Limit priemernej rýchlosti**: 512 kilobitov za sekundu
- **Limit špičkovej rýchlosti**: 1 megabit za sekundu

20. Na stránke Premávka odchádzajúca mimo profilu vyberte **Zrušiť pakety UDP alebo redukovať okno preťaženia TCP** a kliknite na tlačidlo **Ďalej**.
21. Zobrazte Sumárne informácie pre triedu služby. Ak sú správne, kliknite na tlačidlo **Dokončiť** na vytvorenie triedy služby. Po kliknutí na tlačidlo Dokončiť sa vrátite do sprievodcu politikou a vyberie sa vaša trieda služby. Kliknite na tlačidlo Ďalej.
22. Na stránke Naplánovať vyberte Aktívny počas vybratého plánu a kliknite na Nový.
23. V dialógovom okne Pridať nový plán zadajte nasledujúce informácie a kliknite na tlačidlo **OK**:
    - **Názov**: UCD_schedule
    - **Denná doba**: Aktívny 24 hodín
    - **Deň v týždni**: Piatok
24. Kliknite na tlačidlo Ďalej, aby sa zobrazil sumár politiky. Ak je to správne, kliknite na tlačidlo **Dokončiť**. V okne konfigurácie servera QoS sa v pravej časti okna zobrazí nová politika.

Týmto ste dokončili konfiguráciu politiky diferencovaných služieb pre iSeries A. Ďalším krokom je spustenie alebo aktualizácia servera.

Krok 2: Spustiť alebo aktualizovať server QoS

V okne konfigurácie servera QoS vyberte **Server—>Spustiť** alebo **Server—>Aktualizovať**.

Krok 3: Použiť monitor na overenie správnej činnosti vašej politiky

Ak chcete overiť, či sa politika správa, ako ste to nakonfigurovali v politike, použite monitor.

1. V okne konfigurácie QoS vyberte **Server—>Monitor**. Zobrazí sa okno monitora QoS.
2. Vyberte zložku s typom politiky DiffServ. Toto zobrazí všetky politiky DiffServ. Zo zoznamu vyberte **UCD**.

Najzaujímavejšie polia sú polia, ktoré získavajú svoje dáta z vašej premávky. Nezabudnite skontrolovať polia celkový počet bitov, bity v profile a pakety v profile. Bity mimo profilu označujú, že premávka presiahla nakonfigurované hodnoty politiky. V politike diferencovaných služieb číslo v poli mimo profilu (pre pakety UDP) označuje počet zrušených bitov. V TCP toto číslo označuje počet bitov s rýchlosťou presahujúcou rýchlosť bloku tokenov, ktoré sú odoslané do siete. Pre pakety TCP sa bity nikdy nerušia. Pakety v profile označujú počet paketov, ktoré táto politika manažuje (od času spustenia paketu až po aktuálny výstup monitora).

Hodnota, ktorú priradíte poľu priemernej úrovni obmedzenia je taktiež dôležitá. Keď pakety prekročia tento limit, server ich začne rušiť. Ako následok sa zvýši počet bitov mimo profilu. To vám ukazuje, že sa politika správa tak, ako ste ju nakonfigurovali. Popis všetkých polí monitora nájdete v časti monitor.

Poznámka: Nezabudnite, že výsledky budú presné len v prípade, ak je politika aktívna. Skontrolujte plán, ktorý ste špecifikovali v rámci politiky.

Krok 4: Zmeniť vlastnosti (ak treba)

Po prezretí výsledkov monitora môžete zmeniť ľubovoľné vlastnosti politiky alebo triedy služby, čo vám môže pomôcť dosiahnuť očakávané výsledky.

Môžete zmeniť ľubovoľné z hodnôt, ktoré ste v politike vytvorili.

1. V okne konfigurácie servera QoS vyberte zložku **DiffServ**. V zozname v pravej časti okna pravým tlačidlom kliknite na **UCD** a vyberte **Vlastnosti**, aby ste upravili politiku.
2. Dialógové okno Vlastnosti sa zobrazí s hodnotami, ktoré určujú všeobecnú politiku. Zmeňte príslušné hodnoty.
3. Ak chcete upraviť triedu služby, vyberte zložku **Triedy služieb**. V zozname v pravej časti okna pravým tlačidlom kliknite na **UCD_service** a vyberte **Vlastnosti**, aby ste upravili triedu služby.

4. Zobrazí sa dialógové okno Vlastnosti QoS s hodnotami, ktoré riadia premávku. Zmeňte príslušné hodnoty.
5. Po aktualizácii politiky alebo triedy služby musíte server aktualizovať, aby akceptoval vaše zmeny. V okne konfigurácie servera QoS vyberte **Server—>Aktualizovať**.

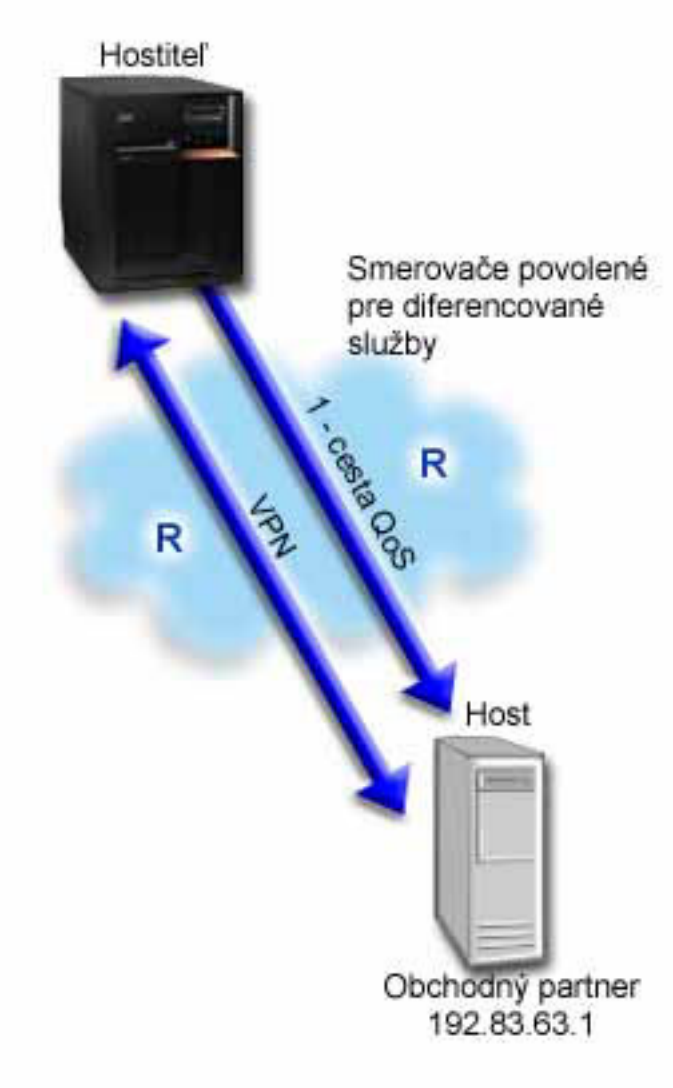
Scenár QoS: Bezpečné a predpovedateľné výsledky (VPN a QoS)

Situácia

Prostredníctvom VPN ste v spojení s istým obchodným partnerom a chcete skombinovať VPN s QoS, aby ste poskytli patričnú bezpečnosť a predpovedateľný tok údajov e-business v kritickej situácii. Konfigurácia QoS cestuje len jedným smerom. Preto, ak máte audio/video aplikáciu, potrebujete vytvoriť QoS pre aplikáciu na oboch stranách pripojenia.

Obrázok ukazuje váš server a vášho klienta v hostiteľ-hostiteľ VPN pripojení. Každé R predstavuje diferencované službou umožnené smerovače pozdĺž cesty premávky. Ako vidíte QoS politiky tečú len v jednom smere.

Obrázok 3. Pripojenie medzi dvomi hostiteľmi cez VPN použitím politiky diferencovaných služieb QoS.



Ciele

VPN a QoS môžete použiť nielen na zriadenie ochrany, ale aj na zriadenie priority pre toto pripojenie. Najprv nakonfigurujte pripojenie VPN medzi dvomi hostiteľmi. Pomoc pri konfigurácii VPN nájdete v príklade Hostiteľ-Hostiteľ VPN pripojenie. Len čo ste zabezpečili VPN pripojenia, môžete nastaviť svoju QoS politiku. Môžete vytvoriť politiku diferencovaných služieb. Tejto politike môžete priradiť urýchlene postupujúcu hodnotu kódového bodu, čo bude mať vplyv na spôsob stanovenia priorít pre premávku v kritickej situácii.

Požiadavky a predpoklady

- S vaším ISP máte uzavretú dohodu úrovne služieb (SLA), aby ste zaručili, že politiky prijímajú požadovanú prioritu. Politika QoS, ktorú vytvoríte na serveri iSeries(TM), povoľuje premávku (v politike) na získanie priority v celej sieti. Nezaručuje to a je závislá na vašom SLA. V skutočnosti vám výhody politík QoS dávajú možnosť vysporiadať sa s konkrétnymi úrovňami služieb a rýchlosťami. Použite odkaz na dohodu úrovne služieb, ak sa chcete dozvedieť viac.
- Politiky diferencovaných služieb vyžadujú smerovače typu DiffServ pozdĺž sieťovej cesty. Väčšina smerovačov je typu DiffServ; ak sa chcete dozvedieť viac, pozrite si stránku Diferencovaná služba.

Konfigurácia

Po tom, ako ste skontrolovali požiadavky krok po kroku, ste pripravený na vytvorenie politiky diferencovaných služieb.

1. Nakonfigurovať pripojenie VPN medzi dvomi hostiteľmi (Pozrite 31)
2. Vytvoriť politiku diferencovaných služieb (Pozrite 31)
3. Spustiť alebo aktualizovať server QoS (Pozrite 32)
4. Použiť monitor na overenie správnej činnosti vašej politiky (Pozrite 32)
5. Zmeniť vlastnosti (ak treba) (Pozrite 32)

Krok 1: Nakonfigurovať pripojenie VPN medzi dvomi hostiteľmi

Pomoc pri konfigurácii VPN nájdete v príklade Hostiteľ-Hostiteľ VPN pripojenie.

Krok 2: Vytvoriť politiku diferencovaných služieb

1. V programe iSeries Navigator, rozviňte iSeries A —**>Sieť —>Politiky IP**.
2. Pravým tlačidlom kliknite na **Kvalita služby** a vyberte **Konfigurácia**, aby sa otvorilo okno Konfigurácia servera QoS.
3. V okne konfigurácie servera QoS pravým tlačidlom kliknite na IntServ a vyberte **Nová politika**, aby ste spustili sprievodcu.
4. Prečítajte si Uvítaciu stránku a kliknite na tlačidlo **Ďalej**, aby ste sa dostali na stránku **Názov**.
5. V poli **Názov** zadajte VPN a kliknite na tlačidlo **Ďalej**. Tiež môžete voliteľne zadať opis na lepšie zapamätanie si účelu tejto politiky.
6. Na stránke Klienti vyberte **Špecifická adresa alebo adresy** a kliknite na **Nový**, aby ste zadefinovali vášho klienta.
7. V dialógovom okne Nový klient zadajte nasledujúce informácie:
   - **Názov**: VPN_Client
   - **Adresa IP**: 192.83.63.1
   - Kliknite na tlačidlo **OK**, aby ste vytvorili klienta a zároveň sa vrátili späť do sprievodcu diferencovanou službou.

   Po kliknutí na tlačidlo OK sa vrátite do sprievodcu politikou. Ak ste už predtým mali vytvorených klientov, zrušte ich označenie a skontrolujte, či sú vybratí len relevantní klienti.
8. Na stránke Požiadavka o údaje servera skontrolujte, či sú vybraté voľby **Všetky tokeny** a **Všetky priority**.
9. Na stránke Aplikácie skontrolujte, či sú vybraté voľby **Všetky porty** a **Všetko**.
10. Kliknite na tlačidlo **Ďalej**.
11. Na stránke Lokálna adresa IP použite predvolenú hodnotu a kliknite na tlačidlo **Ďalej**.
12. Na stránke Diferencovaná trieda služby kliknite na **Nový**, aby ste zadefinovali charakteristiky výkonu. Zobrazí sa Sprievodca novou triedou služby.
13. Prečítajte si Uvítaciu stránku a kliknite na tlačidlo **Ďalej**.
14. Na stránke Názov zadajte EF_VPN.
15. Na stránke Typ služby vyberte **Iba výstup** a kliknite na tlačidlo **Ďalej**. Táto trieda služby sa použije len pre politiky výstupu.
16. Na strane Označenie kódových bodov odchádzajúceho DiffServ vyberte **Trieda 3**. Výkon pre túto premávku v smerovačoch a iných serveroch v sieti je určený správaním jednotlivých skokov. Použite Pomoc priradenú k rozhraniu na uľahčenie vášho rozhodovania.
17. Na stránke Vykonať meranie odchádzajúcej premávky skontrolujte, či je vybraté **Áno** a kliknite na tlačidlo **Ďalej**.
18. Na stránke Limity riadenia rýchlosti výstupu zadajte nasledujúce informácie a kliknite na tlačidlo **Ďalej**:
    - **Veľkosť bloku tokenov**: 100 kilobitov
    - **Limit priemernej rýchlosti**: 64 megabitov za sekundu
    - **Limit špičkovej rýchlosti**: Neobmedziť

19. Na stránke Premávka odchádzajúca mimo profilu vyberte **Zrušiť pakety UDP alebo redukovať okno preťaženia TCP** a kliknite na tlačidlo **Ďalej**.
20. Pre triedu služby zobrazte stránku Sumárne informácie a kliknite na **Dokončiť**, aby ste sa vrátili do sprievodcu politikou.
21. Na stránke Diferencovaná trieda služby skontrolujte, či je vybraté **EF_VPN** a kliknite na tlačidlo **Ďalej**.
22. Na stránke Naplánovať vyberte **Aktívny počas vybratého plánu** a kliknite na **Nový**.
23. V dialógovom okne Pridať nový plán zadajte nasledujúce informácie a kliknite na tlačidlo **OK**:
    - **Názov**: FirstShift
    - **Čas dňa**: Aktívny v zadanom čase a pridajte 9:00 až 15:00.
    - **Deň týždňa**: Aktívny v zadaný deň a vyberte Pondelok až Piatok.
24. Na stránke Naplánovať kliknite na tlačidlo **Ďalej**.
25. Zobraziť Sumárne informácie. Ak sú správne, kliknite na tlačidlo **Dokončiť**, aby sa vytvorila politika. Okno konfigurácie servera QoS v zozname zobrazí všetky politiky vytvorené v serveri. Po ukončení sprievodcu sa politika zobrazí v pravej časti okna.

Týmto ste dokončili konfiguráciu politiky diferencovaných služieb pre iSeries A. Ďalším krokom je spustenie alebo aktualizácia servera.

Krok 3: Spustiť alebo aktualizovať server QoS

V okne konfigurácie servera QoS vyberte **Server—>Spustiť** alebo **Server—>Aktualizovať**.

Krok 4: Použiť monitor na overenie správnej činnosti vašej politiky

Na overenie, že sa prevádzka správa tak, ako ste ju nakonfigurovali, použite monitor.

1. V okne konfigurácie servera QoS vyberte **Server—>Monitor**. Zobrazí sa okno monitora QoS.
2. Pre typ politiky vyberte DiffServ. Toto zobrazí všetky politiky DiffServ.

Podobne, ako v príklade 1, najzaujímavejšie polia sú polia, ktoré získavajú svoje dáta z vašej premávky. Tieto polia zahrňujú všetky bity, bity v profile a pakety mimo profilu. Bity mimo profilu označujú, že premávka presiahla nakonfigurované hodnoty politiky. Pakety v profile označujú počet paketov, ktoré táto politika manažuje. Je veľmi dôležité, aké hodnoty priradíte poľu priemernej úrovni obmedzenia. Keď pakety TCP prekročia tento limit, budú sa posielať do siete, kým okno preťaženia TCP neklesne na front paketov mimo profil. Ako následok sa zvýši počet bitov mimo profilu. Rozdiel medzi touto politikou a scenárom obmedzenia premávky prehliadača je v tom, že tu sú pakety chránené pomocou protokolu VPN. Ako vidíte QoS pracuje s VPN pripojením. Popis všetkých polí monitora nájdete v časti monitor.

Poznámka: Nezabudnite, že výsledky budú presné len v prípade, ak je politika aktívna. Skontrolujte plán, ktorý ste špecifikovali v rámci politiky.

Krok 5: Zmeniť vlastnosti (ak treba)

Po prezretí výsledkov monitora môžete zmeniť ľubovoľné vlastnosti politiky alebo triedy služby, čo vám môže pomôcť dosiahnuť očakávané výsledky.

Rovnako môžete upraviť triedu služby po jej vytvorení.

1. V okne konfigurácie servera QoS vyberte zložku **DiffServ**. V zozname v pravej časti okna pravým tlačidlom kliknite na **VPN** a vyberte **Vlastnosti**, aby ste upravili politiku.
2. Dialógové okno Vlastnosti sa zobrazí s hodnotami, ktoré určujú všeobecnú politiku. Zmeňte príslušné hodnoty.
3. Ak chcete upraviť triedu služby, vyberte zložku **Triedy služieb**. V zozname v pravej časti okna pravým tlačidlom kliknite na **EF_VPN** a vyberte **Vlastnosti**, aby ste upravili triedu služby.
4. Zobrazí sa dialógové okno Vlastnosti QoS s hodnotami, ktoré riadia premávku. Zmeňte príslušné hodnoty.

5. Po aktualizácii politiky alebo triedy služby musíte server aktualizovať, aby akceptoval vaše zmeny. V okne konfigurácie servera QoS vyberte **Server—>Aktualizovať**.

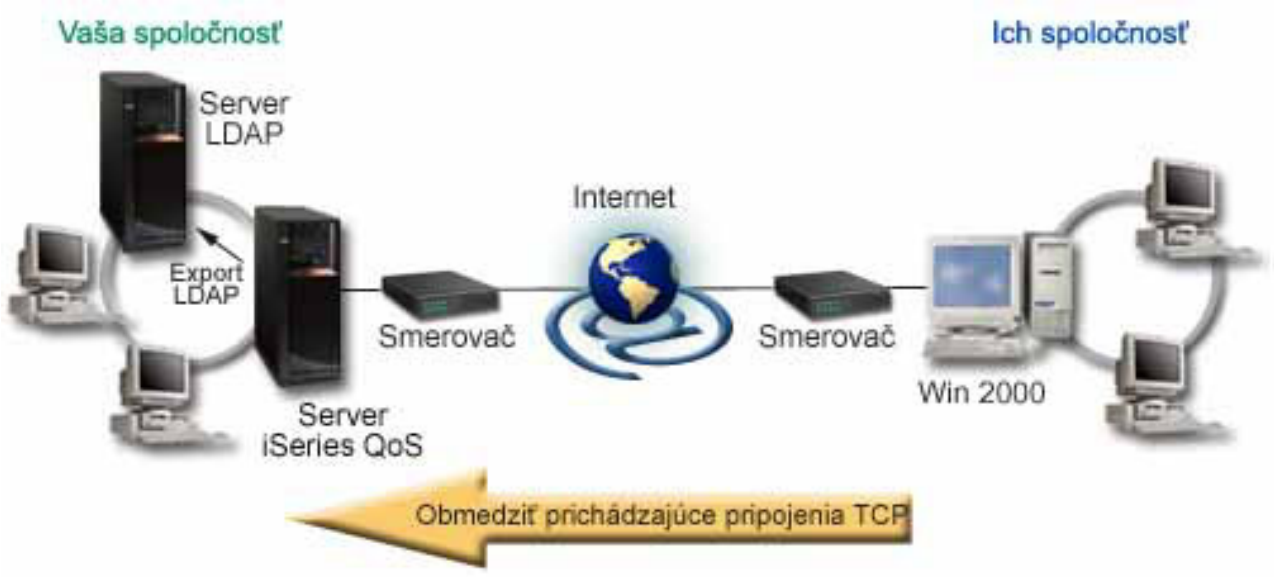
Scenár QoS: Obmedziť vstupné pripojenia

Situácia

Prostriedky vášho webového servera sú zahlcované požiadavkami klienta, vstupujúcimi do vašej siete. Musíte spomaliť prichádzajúcu premávku HTTP do vášho webového servera na lokálnom rozhraní 192.168.1.1. QoS vám môže pomôcť obmedziť akceptované pokusy o prichádzajúce pripojenia na váš server na základe atribútov pripojení (napríklad IP adresy). Aby ste toto dosiahli, rozhodnete sa spraviť politiku povolenia vstupu, ktorá obmedzí počet akceptovaných vstupných pripojení.

Ilustrácia znázorňuje vašu spoločnosť a spoločnosť klienta. Táto politika QoS môže riadiť tok prevádzky iba v jednom smere.

Obrázok 5. Obmedzenie vstupných pripojení TCP.



Cieľ

Ak chcete konfigurovať politiku vstupu, musíte určiť, či obmedzíte premávku pre lokálne rozhranie alebo špecifickú aplikáciu a určiť, či obmedzíte premávku z konkrétneho klienta. V tomto prípade môžete vytvoriť politiku obmedzujúcu pokusy o pripojenie z Their_Company, prichádzajúce na port 80 (protokol HTTP) na vašom lokálnom rozhraní 192.168.1.1.

Konfigurácia

Ak chcete vytvoriť politiku povolenia vstupu, musíte vykonať tieto kroky:

1. Vytvoriť politiku povolenia vstupu (Pozrite 34)
2. Spustiť alebo aktualizovať server QoS (Pozrite 35)
3. Použiť monitor na overenie správnej činnosti vašej politiky (Pozrite 35)
4. Zmeniť vlastnosti (ak treba) (Pozrite 35)

Krok 1: Vytvoriť politiku povolenia vstupu

1. V iSeries(TM) Navigator rozviňte iSeries A —**>Sieť** —**>IP politiky**.
2. Pravým tlačidlom kliknite na **Kvalita služby** a vyberte **Konfigurácia**, aby ste otvorili okno Konfigurácia servera QoS.
3. V okne konfigurácie servera QoS pravým tlačidlom kliknite na **Politiky povolenia vstupu** a vyberte **Nová politika**, aby ste spustili sprievodcu.
4. Prečítajte si Uvítaciu stránku a kliknite na tlačidlo **Ďalej**.
5. V poli **Názov** zadajte Restrict_TheirCo a kliknite na tlačidlo **Ďalej**. Tiež môžete voliteľne zadať opis na lepšie zapamätanie si účelu tejto politiky.
6. Na stránke Klienti vyberte **Špecifická adresa alebo adresy** a kliknite na **Nový**, aby ste zadefinovali vášho klienta.
7. V dialógovom okne Nový klient zadajte nasledujúce informácie:
   - **Názov**: Their_Co
   - **Rozsah adries IP**: 10.1.1.1 až 10.1.1.10
   - Kliknite na tlačidlo **OK**, aby ste vytvorili klienta a zároveň sa vrátili späť do sprievodcu politikou.

   Po kliknutí na tlačidlo OK sa vrátite do sprievodcu politikou. Ak ste už predtým mali vytvorených klientov, zrušte ich označenie a skontrolujte, či sú vybratí len relevantní klienti.
8. Na stránke URI skontrolujte, či je vybraté **Všetky URI** a kliknite na tlačidlo **Ďalej**.
9. Na stránke Aplikácie vyberte **Špecifický port, rozsah portov alebo typ servera** a kliknite na **Nový**.
10. V dialógovom okne Nová aplikácia zadajte nasledujúce informácie a kliknite na tlačidlo **OK**, aby ste sa vrátili do sprievodcu:
    - **Názov**: HTTP
    - **Port**: 80
11. Kliknite na tlačidlo Ďalej, aby ste prešli na stránku Kódový bod.
12. Na stránke Kódový bod skontrolujte, či je vybraté **Všetky kódové body** a kliknite na tlačidlo **Ďalej**.
13. Na stránke Lokálna adresa IP vyberte **adresa IP** a vyberte rozhranie, na ktoré prichádzajú požiadavky do vášho lokálneho systému. V tomto príklade je to adresa 192.168.1.1.
14. Na stránke Trieda služby kliknite na **Nový**, aby ste zadefinovali charakteristiky výkonu. Zobrazí sa Sprievodca novou triedou služby.
15. Prečítajte si Uvítaciu stránku a kliknite na tlačidlo **Ďalej**.
16. Na stránke Názov zadajte **vstup** a kliknite na tlačidlo **Ďalej**. Tiež môžete voliteľne pridať opis na lepšie zapamätanie si účelu tejto triedy služby.
17. Na stránke Typ služby vyberte **Iba vstup**. Táto trieda služby sa použije len pre politiky vstupu.
18. Na stránke Limity pre vstup zadajte nasledujúce informácie a kliknite na tlačidlo **Ďalej**:
    - Priemerná rýchlosť pripojenia: 50 za sekundu
    - Maximálna rýchlosť pripojenia: 50 pripojení
    - Priorita: Stredná
19. Kliknite na tlačidlo **Dokončiť**, aby ste sa vrátili do sprievodcu politikou.
20. Na stránke Trieda služby skontrolujte, či je vybratá trieda služby, ktorú ste práve vytvorili a kliknite na tlačidlo **Ďalej**.
21. Na stránke Naplánovať vyberte **Aktívny počas vybratého plánu** a kliknite na **Nový**.
22. V dialógovom okne Nový plán zadajte nasledujúce informácie a kliknite na tlačidlo **OK**:

- Názov: FirstShift
- Čas dňa: Aktívny v zadanom čase a pridajte 9:00 až 5:00.
- Deň týždňa: Aktívny v zadané dni a vyberte Pondelok až Piatok.

23. Na stránke Naplánovať kliknite na tlačidlo **Ďalej**.
24. Zobraziť Sumárne informácie. Ak sú správne, kliknite na tlačidlo **Dokončiť**, aby sa vytvorila politika. Konfigurácia servera QoS v zozname zobrazí všetky politiky vytvorené v serveri. Po ukončení sprievodcu sa politika zobrazí v pravej časti okna.

Týmto ste dokončili konfiguráciu politika povolenia vstupu pre iSeries A. Ďalším krokom je spustenie alebo aktualizácia servera.

Krok 2: Spustiť alebo aktualizovať server QoS

V okne konfigurácie servera QoS vyberte **Server—>Spustiť** alebo **Server—>Aktualizovať**.

Krok 3: Použiť monitor na overenie správnej činnosti vašej politiky

Na overenie, že sa prevádzka správa tak, ako ste ju nakonfigurovali, použite monitor.

1. V okne konfigurácie QoS vyberte **Server—>Monitor**. Zobrazí sa okno monitora QoS.
2. Ako typ politiky vyberte Povolenie vstupu. Toto zobrazí všetky politiky povolenia vstupu. Zo zoznamu vyberte **Restrict_TheirCo**.

   Skontrolujte všetky merané polia, akými sú akceptované požiadavky, zrušené požiadavky, požiadavky spolu a počet pripojení. Zrušené požiadavky označujú, že premávka presiahla nakonfigurované hodnoty politiky. Akceptované požiadavky indikujú počet bitov, riadených touto politikou (od momentu, keď bol paket spustený, po súčasný výstup monitora).

   Hodnota, ktorú priradíte poľu zvanému priemerný počet požiadaviek na pripojenie, je taktiež dôležitá. Keď pakety prekročia tento limit, server ich začne rušiť. Ako výsledok bude stúpať počet zrušených požiadaviek. To vám ukazuje, že sa politika správa tak, ako ste ju nakonfigurovali. Kvôli popisu všetkých polí monitora si pozrite časť monitor.

   Poznámka: Nezabudnite, že výsledky budú presné len v prípade, ak je politika aktívna. Skontrolujte plán, ktorý ste špecifikovali v rámci politiky.

Krok 4: Zmeniť vlastnosti (ak treba)

Po prezretí výsledkov monitora môžete zmeniť ľubovoľné vlastnosti politiky alebo triedy služby, čo vám môže pomôcť dosiahnuť očakávané výsledky.

1. V okne konfigurácie servera QoS vyberte zložku **Povolenie vstupu**. V zozname v pravej časti okna pravým tlačidlom kliknite na **Restrict_TheirCo** a vyberte **Vlastnosti**, aby ste upravili politiku.
2. Zobrazí sa strana Vlastnosti s hodnotami, ktoré určujú všeobecnú politiku. Zmeňte príslušné hodnoty.
3. Ak chcete upraviť triedu služby, vyberte zložku **Triedy služieb**. V zozname v pravej časti okna pravým tlačidlom kliknite na **vstup** a vyberte **Vlastnosti**, aby ste upravili triedu služby.
4. Zobrazí sa dialógové okno Vlastnosti QoS s hodnotami, ktoré riadia premávku. Zmeňte príslušné hodnoty.
5. Po aktualizácii politiky alebo triedy služby musíte server aktualizovať, aby akceptoval vaše zmeny. V okne konfigurácie servera QoS vyberte **Server—>Aktualizovať**.

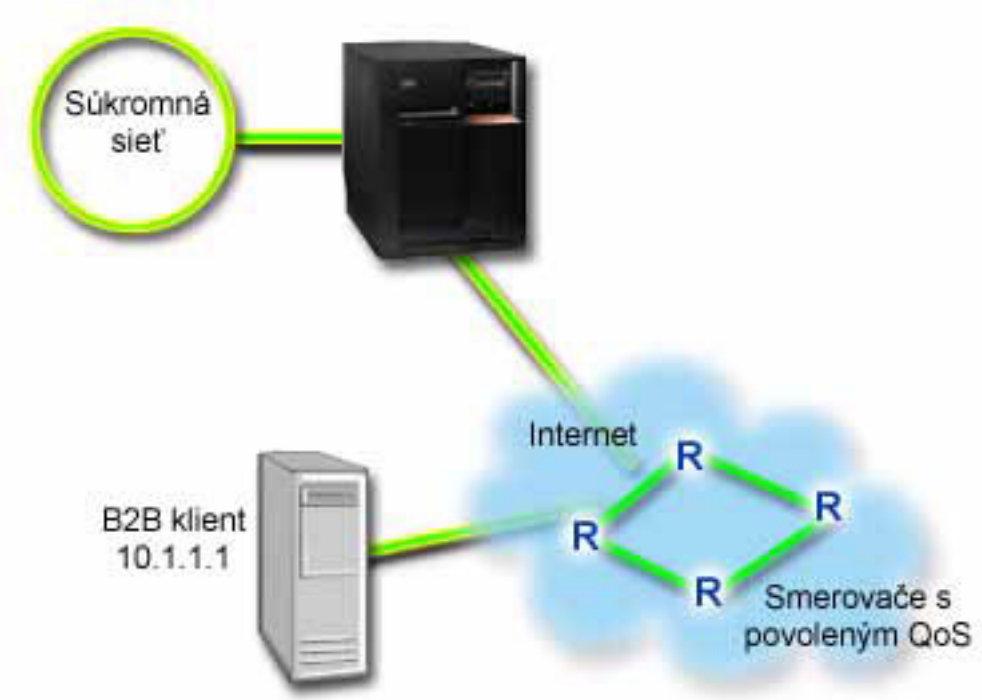
Scenár QoS: Predvídateľná B2B premávka

Situácia

Obchodné oddelenie hlási problémy, že sieťová prevádzka nefunguje podľa ich predstáv. Systém iSeries(TM) vašej spoločnosti. Politika QoS, ktorú vytvoríte na serveri iSeries(TM), sa nachádza v prostredí B2B (business-to-business), ktorý vyžaduje predvídateľnú e-business službu. Potrebujete poskytovať predpovedateľné transakcie vašim zákazníkom. Aplikácii na objednávanie v obchodnom oddelení chcete prideliť vyššiu kvalitu služby počas najrušnejšej doby dňa (medzi 10:00 a 16:00).

V doleuvedenej ilustrácii je predajný tím v rámci vašej súkromnej siete. Pozdĺž cesty premávky k B2B klientovi sú umiestnené smerovače s povoleným RSVP. Každé R predstavuje smerovač pozdĺž cesty premávky.

Obrázok 7. Politika integrovaných služieb pre B2B klienta s použitím smerovačov s povoleným RSVP.



Ciele

Služba kontrolovaného zaťaženia podporuje aplikácie, ktoré sú vysoko citlivé k upravovaným sieťam, ale zostávajú tolerantné k malým množstvám strát a oneskorení. Ak aplikácia používa službu kontrolovaného zaťaženia, jej výkon nebude trpieť pri zvýšení záťaže siete. Prevádzka bude zabezpečovaná službou, podobnou prevádzke v sieti za bežných okolností. Keďže táto zvláštna aplikácia je tolerantná voči určitému oneskoreniu, použite politiku integrovaných služieb za využitia služby kontrolovanej záťaže.

Politiky integrovaných služieb taktiež požadujú, aby boli pozdĺž cesty premávky smerovače s povoleným RSVP. Kvôli ďalším informáciám si pozrite koncept Integrovaná služba.

Požiadavky a predpoklady

Integrovaná politika služieb je rozšírená politika, ktorá môže vyžadovať značné prostriedky. Politiky integrovaných služieb vyžadujú nasledujúce predpoklady:

- **Aplikácie podporujúce RSVP**
  Keďže váš server nemá žiadne RSVP-umožnené aplikácie, musíte napísať svoje vlastné aplikácie s povoleným RSVP. Ak chcete napísať vlastné aplikácie, použite API protokolu Resource Reservation Setup (RAPI) alebo rozhrania API qtoq sockets QoS. Viac informácií nájdete na stránke rozhrania API QoS, v časti pre rozhrania API integrovaných služieb.

- **Smerovače a servery podporujúce RSVP pozdĺž sieťovej cesty**
  QoS je sieťové riešenie. Ak si nie ste istý, či celá sieť podporuje RSVP, vždy môžete vytvoriť integrovanú politiku služieb a použiť značkovanie na udelenie priority; priorita sa ale nedá zaručiť. Kvôli ďalším informáciám si pozrite koncept Integrovaná služba.
- **Dohodnutie úrovne služby**
  S vaším ISP máte uzavretú dohodu úrovne služieb (SLA), aby ste zaručili, že politiky prijímajú požadovanú prioritu. Politika QoS, ktorú vytvárate umožňuje premávke (v politike) prijímať prioritu z celej siete. Nezaručuje to a je závislá na vašom SLA. V skutočnosti vám výhody politík QoS dávajú možnosť vysporiadať sa s konkrétnymi úrovňami služieb a rýchlosťami. Použite odkaz na dohodu úrovne služieb, ak sa chcete dozvedieť viac. Poznámka: Ak sa nachádzate v rámci privátnej siete, SLA nepotrebujete.

Konfigurácia

Po tom, ako ste skontrolovali požiadavky krok po kroku, ste pripravený na vytvorenie integrovanej politiky služieb. Ak chcete vytvoriť politiku integrovaných služieb, musíte vykonať toto:

1. Vytvoriť integrovanú politiku služieb (Pozrite 37)
2. Spustiť alebo aktualizovať server QoS (Pozrite 38)
3. Použiť monitor na overenie správnej činnosti vašej politiky (Pozrite 38)
4. Zmeniť vlastnosti (ak treba) (Pozrite 38)

Krok 1: Vytvoriť integrovanú politiku služieb

1. V programe iSeries Navigator, rozviňte iSeries A —**>Sieť** —**>Politiky IP**.
2. Pravým tlačidlom kliknite na **Kvalita služby** a vyberte **Konfigurácia**, aby sa otvorilo okno Konfigurácia servera QoS.
3. V okne konfigurácie servera QoS pravým tlačidlom kliknite na typ politiky IntServ a vyberte **Nová politika**, aby ste spustili sprievodcu.
4. Prečítajte si Uvítaciu stránku a kliknite na tlačidlo **Ďalej**, aby ste sa dostali na stránku **Názov**.
5. V poli **Názov** zadajte B2B_CL a kliknite na tlačidlo **Ďalej**. Tiež môžete voliteľne zadať opis na lepšie zapamätanie si účelu tejto politiky.
6. Na stránke Klienti vyberte **Špecifická adresa alebo adresy** a kliknite na **Nový**, aby ste zadefinovali vášho klienta.
7. V dialógovom okne Nový klient zadajte nasledujúce informácie:
   - **Názov**: CL_client
   - **Adresa IP**: 10.1.1.1
   - Kliknite na tlačidlo **OK**, aby ste vytvorili klienta a zároveň sa vrátili späť do sprievodcu politikou.

   Po kliknutí na tlačidlo OK sa vrátite do sprievodcu politikou. Ak ste už predtým mali vytvorených klientov, zrušte ich označenie a skontrolujte, či sú vybratí len relevantní klienti. Na stránke aplikácie vyberte **Špecifický port, rozsah portov alebo typ servera** a kliknite na **Nový**.
8. V dialógovom okne Nová aplikácia zadajte nasledujúce informácie a kliknite na tlačidlo **OK**, aby ste sa vrátili do sprievodcu:
   - **Názov**: business_app
   - **Rozsah portov**: 7000-8000
9. Na stránke Aplikácie vyberte **Protokol** a skontrolujte, či je vybraté **TCP**. Kliknite na tlačidlo **Ďalej**.

   Poznámka: Aplikácia, ktorú si vyberiete pre politiku integrovaných služieb musí byť napísaná tak, aby mohla používať API RAPI alebo rozhrania API qtoq sockets. Spolu s protokolom rezervácie prostriedkov (RSVP) vykonávajú tieto rozhrania API rezervácie integrovaných služieb prostredníctvom siete. Ak nevyužijete tieto rozhrania API, aplikácia neprijme žiadnu prioritu alebo záruku. Tiež je dôležité uvedomiť si, že táto politika umožňuje vašim aplikáciám prijímať priority prostredníctvom siete, ale nedokáže to zaručiť. Všetky smerovače a servery pozdĺž cesty premávky musia používať protokol RSVP na zaručenie rezervácie. Rezervácia medzi dvomi koncami závisí na súčinnosti celej siete.

10. Na stránke Lokálna adresa IP použite predvolenú hodnotu a kliknite na tlačidlo **Ďalej**.
11. Na stránke Typ integrovaných služieb vyberte **Riadená záťaž** a kliknite na tlačidlo **Ďalej**.
12. Na stránke Značkovanie integrovaných služieb vyberte **Nie, nepriradiť skokové správanie** a kliknite na tlačidlo **Ďalej**.
13. Na stránke Limity pre výkon integrovaných služieb zadajte nasledujúce informácie a kliknite na tlačidlo **Ďalej**:
    - **Maximálny počet tokov**: 5
    - **Limit rýchlosti tokenov (R)**: Neobmedziť
    - **Veľkosť bloku tokenov**: 100 kilobitov
    - **Limit rýchlosti tokenov (R)**: 25 megabitov za sekundu
14. Na stránke Naplánovať vyberte **Aktívny počas vybratého plánu** a kliknite na **Nový**.
15. Na stránke Nový plán zadajte nasledujúce informácie a kliknite na tlačidlo **OK**:
    - **Názov**: primetime
    - **Čas dňa**: Aktívny v určitých časoch a pridajte 10:00 až 16:00
    - **Deň týždňa**: Aktívny v zadaný deň a vyberte Pondelok až Piatok.
16. Na stránke Naplánovať kliknite na tlačidlo **Ďalej**.
17. Zobraziť Sumárne informácie. Ak sú správne, kliknite na tlačidlo **Dokončiť**, aby sa vytvorila politika. Hlavé rozhranie QoS zobrazí všetky politiky vytvorené v serveri. Po ukončení sprievodcu sa politika zobrazí v pravej časti okna.

Týmto ste dokončili konfiguráciu integrovanej politiky služieb pre iSeries A. Ďalším krokom je spustenie alebo aktualizácia servera.

Krok 2: Spustiť alebo aktualizovať server QoS

V okne konfigurácie servera QoS vyberte **Server—>Spustiť** alebo **Server—>Aktualizovať**.

Krok 3: Použiť monitor na overenie správnej činnosti vašej politiky

Ak chcete overiť, či politika funguje správne, použite monitor.

1. V okne konfigurácie servera QoS vyberte **Server—>Monitor**. Zobrazí sa okno monitora QoS.
2. Pre typ politiky vyberte IntServ. Toto zobrazí všetky politiky IntServ.

Najzaujímavejšie polia sú polia, ktoré získavajú svoje dáta z vašej premávky. Nezabudnite skontrolovať polia celkový počet bitov, bity v profile a pakety v profile. Bity mimo profil označujú, že sa oneskoruje alebo ruší iná premávka, aby sa splnili požiadavky integrovanej politiky služieb. Kvôli úplnému popisu polí monitora si pozrite časť monitor.

Poznámka: Nezabudnite, že výsledky budú presné len v prípade, ak je politika aktívna. Skontrolujte plán, ktorý ste špecifikovali v rámci politiky. Okrem toho, monitor zobrazuje politiky IntServ až po spustení aplikácií. Pred monitorovaním sa musí zriadiť rezervácia RSVP.

Krok 4: Zmeniť vlastnosti (ak treba)

Po prezretí výsledkov monitora môžete zmeniť ľubovoľné vlastnosti politiky, čo vám môže pomôcť dosiahnuť očakávané výsledky.

Po vytvorení politiky môžete zmeniť hodnoty, ktoré ste predtým vytvorili pomocou sprievodcu.

1. V okne konfigurácie servera QoS vyberte zložku **IntServ**. V zozname v pravej časti okna pravým tlačidlom kliknite na **B2B_CL** a vyberte **Vlastnosti**, aby ste upravili politiku.
2. Dialógové okno Vlastnosti sa zobrazí s hodnotami, ktoré určujú všeobecnú politiku. Zmeňte príslušné hodnoty.

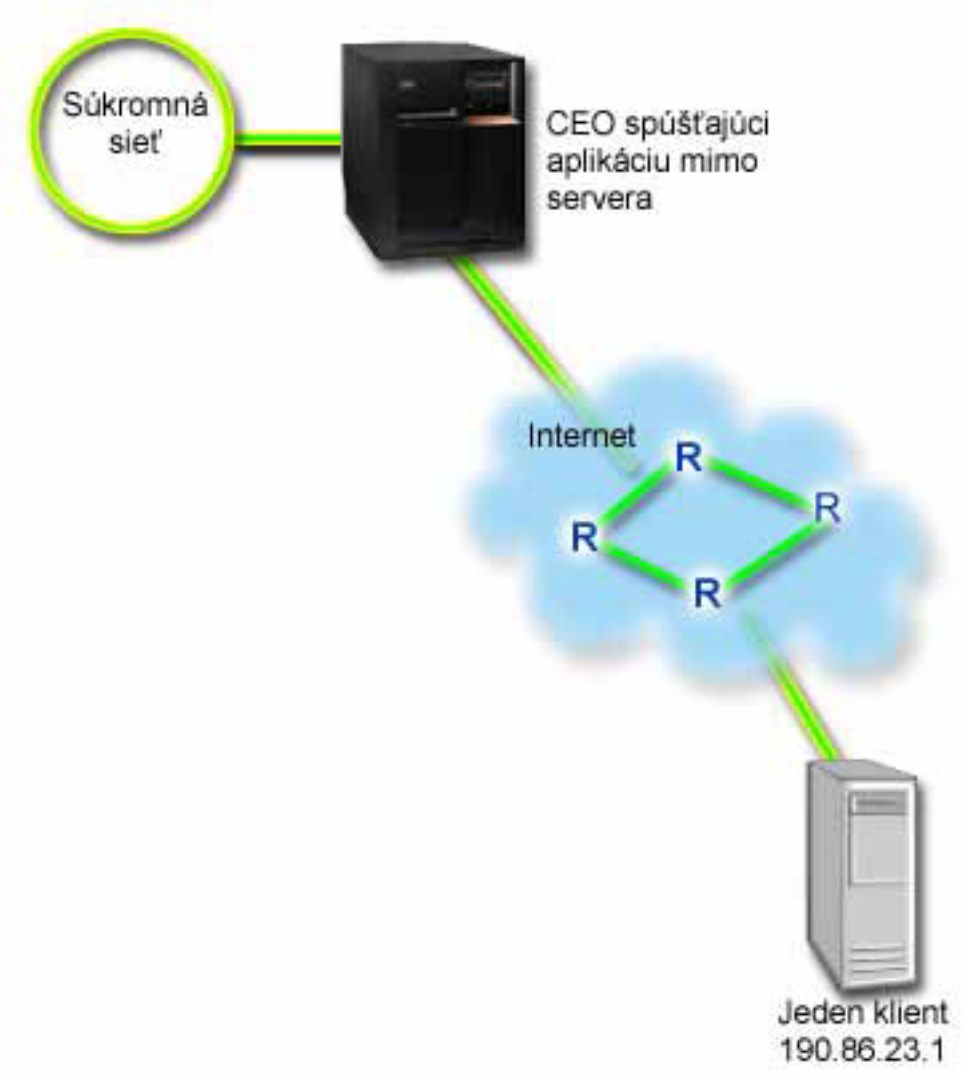
3. Po aktualizácii politiky musíte server aktualizovať, aby akceptoval vaše zmeny. V okne konfigurácie servera QoS vyberte **Server—>Aktualizovať**.

Scenár QoS: Vyhradené doručenie (IP telefónia)

Situácia

Výkonný riaditeľ (CEO) vašej spoločnosti ide uskutočniť živé vysielanie s klientom naprieč krajinou v čase 13:00 - 14:00. Musíte garantovať, že telefónia IP bude mať zaručenú šírku pásma, čo znamená, že počas vysielania sa nevyskytnú žiadne prerušenia. V tomto scenári je aplikácia umiestnená na serveri.

Obrázok 9. Prezentácia CEO klientovi, zaručená integrovanou politikou služieb.



Ciele

Aplikácia, ktorú váš CEO používa, vyžaduje hladký, neprerušovaný prenos, takže sa rozhodnete použiť zaručenú

integrovanú politiku služieb. Zaručená služba kontroluje maximálne zdržanie vo fronte, takže pakety nebudú oneskorené dlhšie, ako je určený čas.

Požiadavky a predpoklady

Integrovaná politika služieb je rozšírená politika, ktorá môže vyžadovať značné prostriedky. Politiky integrovaných služieb vyžadujú nasledujúce predpoklady:

- **Aplikácie podporujúce RSVP**
  Keďže váš server nemá žiadne RSVP-umožnené aplikácie, musíte napísať svoje vlastné aplikácie s povoleným RSVP. Ak chcete napísať vlastné aplikácie, použite API protokolu Resource Reservation Setup (RAPI) alebo rozhrania API qtoq sockets QoS. Viac informácií nájdete na stránke rozhrania API QoS, v časti pre rozhrania API integrovaných služieb.
- **Smerovače a servery podporujúce RSVP pozdĺž sieťovej cesty**
  QoS je sieťové riešenie. Ak si nie ste istý, či celá sieť podporuje RSVP, vždy môžete vytvoriť integrovanú politiku služieb a použiť značkovanie na udelenie priority; priorita sa ale nedá zaručiť. Kvôli ďalším informáciám si pozrite koncept Integrovaná služba.
- **Dohodnutie úrovne služby**
  S vaším ISP máte uzavretú dohodu úrovne služieb (SLA), aby ste zaručili, že politiky prijímajú požadovanú prioritu. Politika QoS, ktorú vytvoríte na serveri iSeries™, umožňuje premávku (v politike) na získanie priority v celej sieti. Nezaručuje to a je závislá na vašom SLA. V skutočnosti vám výhody politík QoS dávajú možnosť vysporiadať sa s konkrétnymi úrovňami služieb a rýchlosťami. Použite odkaz na dohodu úrovne služieb, ak sa chcete dozvedieť viac.

Konfigurácia

Po tom, ako ste skontrolovali požiadavky krok po kroku, ste pripravený na vytvorenie integrovanej politiky služieb. Ak chcete vytvoriť politiku integrovaných služieb, musíte vykonať toto:

1. Vytvoriť integrovanú politiku služieb (Pozrite 40)
2. Spustiť alebo aktualizovať server QoS (Pozrite 41)
3. Použiť monitor na overenie správnej činnosti vašej politiky (Pozrite 41)
4. Zmeniť vlastnosti (ak treba) (Pozrite 41)

Krok 1: Vytvoriť integrovanú politiku služieb

1. V programe iSeries Navigator, rozviňte iSeries A —**>Sieť** —**>Politiky IP**.
2. Pravým tlačidlom kliknite na **Kvalita služby** a vyberte **Konfigurácia**, aby sa otvorilo okno Konfigurácia servera QoS.
3. V okne konfigurácie servera QoS pravým tlačidlom kliknite na typ politiky IntServ a vyberte **Nová politika**, aby ste spustili sprievodcu.
4. Prečítajte si Uvítaciu stránku a kliknite na tlačidlo **Ďalej**, aby ste sa dostali na stránku **Názov**.
5. V poli **Názov** zadajte CEO_guaranteed a kliknite na tlačidlo **Ďalej**. Tiež môžete voliteľne zadať opis na lepšie zapamätanie si účelu tejto politiky.
6. Na stránke Klienti vyberte **Špecifická adresa alebo adresy** a kliknite na **Nový**, aby ste zadefinovali vášho klienta.
7. V dialógovom okne Nový klient zadajte nasledujúce informácie:
   - **Názov**: Branch1
   - **Adresa IP**: 190.86.23.1
   - Kliknite na tlačidlo **OK**, aby ste vytvorili klienta a zároveň sa vrátili späť do sprievodcu integrovanou službou.

   Po kliknutí na tlačidlo OK sa vrátite do sprievodcu politikou. Ak ste už predtým mali vytvorených klientov, zrušte ich označenie a skontrolujte, či sú vybratí len relevantní klienti. Na stránke aplikácie vyberte **Špecifický port, rozsah portov alebo typ servera** a kliknite na **Nový**.
8. V dialógovom okne Nová aplikácia zadajte nasledujúce informácie a kliknite na tlačidlo **OK**, aby ste sa vrátili do sprievodcu:

- **Názov**: Telefónia IP
- **Port**: 2427

9. Na stránke Aplikácie vyberte **Protokol** a skontrolujte, či je vybraté **TCP**. Kliknite na tlačidlo **Ďalej**.

   Poznámka: Aplikácia, ktorú si vyberiete pre politiku integrovaných služieb musí byť napísaná tak, aby mohla používať API RAPI alebo rozhrania API qtoq sockets. Spolu s protokolom rezervácie prostriedkov (RSVP) vykonávajú tieto rozhrania API rezervácie integrovaných služieb prostredníctvom siete. Ak nevyužijete tieto rozhrania API, aplikácia neprijme žiadnu prioritu alebo záruku. Tiež je dôležité uvedomiť si, že táto politika umožňuje vašim aplikáciám prijímať priority prostredníctvom siete, ale nedokáže to zaručiť. Všetky smerovače a servery pozdĺž cesty premávky musia používať protokol RSVP na zaručenie rezervácie. Rezervácia medzi dvomi koncami závisí na súčinnosti celej siete.
10. Na stránke Lokálna adresa IP použite predvolenú hodnotu **Všetky adresy IP**.
11. Na stránke Typ integrovaných služieb vyberte **Garantovaný** a kliknite na tlačidlo **Ďalej**.
12. Na stránke Značkovanie integrovaných služieb vyberte **Nie, nepriradiť skokové správanie** a kliknite na tlačidlo **Ďalej**.
13. Na stránke Limity pre výkon integrovaných služieb zadajte nasledujúce informácie a kliknite na tlačidlo **Ďalej**:
    - **Maximálny počet tokov**: 1
    - **Limit agregovanej šírky pásma (R)**: Neobmedziť
    - **Veľkosť bloku tokenov**: 100 kilobitov
    - **Limit šírky pásma (R)**: 16 megabitov za sekundu
14. Na stránke Naplánovať vyberte **Aktívny počas vybratého plánu** a kliknite na **Nový**.
15. Na stránke Nový plán zadajte nasledujúce informácie a kliknite na tlačidlo **OK**:
    - **Názov**: one_hour
    - **Čas dňa**: Aktívny v zadanom čase a pridajte 13:00 až 14:00.
    - **Deň týždňa**: Aktívny v zadaný deň a vyberte Pondelok.
16. Na stránke Naplánovať kliknite na tlačidlo **Ďalej**.
17. Zobraziť Sumárne informácie. Ak sú správne, kliknite na tlačidlo **Dokončiť**, aby sa vytvorila politika. Hlavné okno konfigurácie servera QoS v zozname zobrazí všetky politiky vytvorené v serveri. Po ukončení sprievodcu sa politika zobrazí v pravej časti okna.

Týmto ste dokončili konfiguráciu integrovanej politiky služieb pre iSeries A. Ďalším krokom je spustenie alebo aktualizácia servera.

Krok 2: Spustiť alebo aktualizovať server QoS

V okne konfigurácie servera QoS vyberte **Server—>Spustiť alebo Server—>Aktualizovať**.

Krok 3: Použiť monitor na overenie správnej činnosti vašej politiky

Ak chcete overiť, či politika funguje správne, použite monitor.

1. V okne konfigurácie servera QoS vyberte Server—>Monitor. Zobrazí sa okno monitora QoS.
2. Vyberte zložku s typom politiky IntServ. Toto zobrazí všetky politiky IntServ.

Najzaujímavejšie polia sú merané polia, ktoré získavajú svoje dáta z vašej premávky. Tieto polia zahrňujú všetky bity, bity v profile a pakety v profile. Bity mimo profil označujú, že sa oneskoruje alebo ruší iná premávka, aby sa splnili požiadavky integrovanej politiky služieb. Kvôli popisu všetkých polí monitora si pozrite časť monitor.

Poznámka: Nezabudnite, že výsledky budú presné len v prípade, ak je politika aktívna. Skontrolujte plán, ktorý ste špecifikovali v rámci politiky. Okrem toho, monitor zobrazuje politiky IntServ až po spustení aplikácií. Pred monitorovaním sa musí zriadiť rezervácia RSVP.

Krok 4: Zmeniť vlastnosti (ak treba)

Po prezretí výsledkov monitora môžete zmeniť ľubovoľné vlastnosti politiky, čo vám môže pomôcť dosiahnuť očakávané výsledky.

Po zobrazení výsledkov monitora pre túto politiku môžete zmeniť hodnoty, ktoré ste predtým vytvorili pomocou sprievodcu.

1. V okne konfigurácie servera QoS vyberte zložku IntServ. V zozname v pravej časti okna pravým tlačidlom kliknite na **CEO_guaranteed** a vyberte **Vlastnosti**, aby ste upravili politiku.
2. Dialógové okno Vlastnosti sa zobrazí s hodnotami, ktoré určujú všeobecnú politiku. Zmeňte príslušné hodnoty.
3. Po aktualizácii politiky musíte server aktualizovať, aby akceptoval vaše zmeny. V okne konfigurácie servera QoS vyberte **Server—>Aktualizovať**.

Plánovanie QoS

Najdôležitejším krokom v uskutočňovaní kvality služby je plánovanie. Kvôli očakávaným výsledkom musíte posúdiť svoje sieťové zariadenia a monitorovať sieťovú prevádzku. Poradca plánovania QoS vás prevedie cez základné otázky, na ktoré budete musieť poznať odpovede počas fázy plánovania. Ako dodatok k poradcovi si pred konfiguráciou QoS najprv prečítajte tieto podtémy.

Chápanie dohôd úrovne služieb
Zmluvy o úrovniach služieb sú dôležitou časťou QoS. Musíte poznať a nastaviť SLA so svojím sieťovým poskytovateľom ako časť svojho plánovania QoS.

Chápanie práce sieťového hardvéru a schopností softvéru
Kvalita služieb je dobrá iba tak ako jej najslabšia linka. Kapacita vašich interných zariadení a zariadení mimo vašej siete má na výsledky QoS obrovský vplyv.

Udeliť správne oprávnenie administrátorovi QoS
Vymenúva všetky oprávnenia, potrebné na úspešnú konfiguráciu QoS a adresárového servera.

Skontrolovať požiadavky systému
Vymenúva všetky požiadavky, potrebné na úspešnú prevádzku QoS.

Uvážiť výkon siete
QoS sa týka v skutočnosti výkonu siete. O QoS uvažujete zrejme preto, že začínate trpieť preťažením siete a strácaním paketov. Pred realizáciou politík môžete použiť Monitor QoS, aby ste skontrolovali aktuálne úrovne výkonu vašej premávky IP. Tieto výsledky vám pomôžu zistiť, kde dochádza k preťaženiu. Pozrite si stránku Monitorovať transakcie servera na monitorovanie aktuálnej premávky.

Použiť poradcu plánovania QoS
Uvážte tieto základné otázky pred realizáciou kvality služby. Dostanete plánovaciu tabuľku s odporúčanými politikami, založenými na možnostiach svojich aplikácií.

Plánovať pre poradie politiky QoS
Poradie vašich politík, ktoré sa objaví na obrazovke iSeries(TM) Navigator (aj v súbore policyd.conf), je poradie, v ktorom sú spracovávané. Poradie politiky má najväčší význam, ak sa politiky prekrývajú.

V prípade potreby použiť rozhrania API QoS
V tejto téme sa dozviete, aké API treba použiť (ak vôbec) na realizáciu rôznych typov politík. Ak napríklad konfigurujete politiku integrovaných služieb, musíte použiť API, ak chcete napísať aplikáciu podporujúcu RSVP.

Požiadavky na oprávnenia

Kvalita politík servisu môže obsahovať citlivé informácie o vašej sieti. Administratívne oprávnenie QoS sa preto musí udeliť len v prípade nutnosti. Nasledujúce oprávnenia budú vyžadované ešte pred tým, ako môžete začať konfigurovať politiky QoS a (voliteľne) adresárové servery LDAP.

Udeliť oprávnenia potrebné na manažovanie adresárového servera
QoS administrátor bude potrebovať nasledujúce oprávnenia: *ALLOBJ oprávnenie a *IOSYSCFG. Kvôli alternatívnym oprávneniam si pozrite Konfigurovať adresárový server.

Prideliť oprávnenie spustiť TCP/IP server.
Ak chcete prideliť objektové oprávnenie príkazom STRTCPSVR a ENDTCPSVR, nasledujte tieto kroky:

1. **STRTCPSVR**: V príkazovom riadku napíšte GRTOBJAUT OBJ (QSYS/STRTCPSVR) OBJTYPE (*CMD) USER (ADMINPROFILE) AUT (*USE), pričom názvom vášho administrátorského profilu nahraďte ADMINPROFILE a stlačte **Enter**.
2. **ENDTCPSVR**: V príkazovom riadku napíšte GRTOBJAUT OBJ (QSYS/ENDTCPSVR) OBJTYPE (*CMD) USER (ADMINPROFILE) AUT (*USE), pričom názvom vášho administrátorského profilu nahraďte ADMINPROFILE a stlačte **Enter**.

Poskytnúť všetky objektové prístupy a oprávnenia systémovej konfigurácie.
Odporúča sa, aby mali užívatelia, ktorí budú konfigurovať QoS prístup bezpečnostného pracovníka. Ak chcete poskytnúť všetky objektové prístupy a oprávnenia systémovej konfigurácie, nasledujte tieto kroky:

1. V iSeries(TM) Navigator, rozviňte váš server —> **Užívatelia a skupiny**.
2. Dvakrát kliknite na **Všetci užívatelia**.
3. Kliknite pravým tlačidlom na užívateľský profil administrátora a vyberte **Vlastnosti**.
4. V dialógovom okne Vlastnosti kliknite na **Schopnosti**.
5. Na stránke Schopnosti si vyberte **Všetky objektové prístupy a systémová konfigurácia**.
6. Kliknite na **OK**, ak chcete zatvoriť stránku Schopnosti.
7. Kliknite na tlačidlo **OK**, aby ste zatvorili dialógové okno Vlastnosti.

Systémové požiadavky

Kvalita služieb (QoS) je integrovanou časťou operačného systému. Musíte splniť tieto požiadavky:

1. Nainštalujte TCP/IP Connectivity Utilities (57*xx*-TC1).
2. Nainštalujte iSeries Navigator na váš PC. Skontrolujte, či ste počas inštalácie programu iSeries Access nainštalovali časť Budovanie siete. Kvalita služieb je umiestnená pod politikami IP v rámci časti Sieť.

Poznámka: Ak chcete získať viac informácií o TCP/IP, budovaní sietí alebo adresách IP, pozrite si Súvisiace informácie pre QoS.

Dohoda úrovne služby

Táto časť má za úmysel zdôrazniť niektoré dôležité aspekty dohody o úrovni služieb (SLA), ktoré môžu ovplyvniť implementáciu kvality služby. QoS je softvérové riešenie a ak chcete prijímať prioritu siete aj z mimo vašej súkromnej siete, potrebujete mať SLA s vaším poskytovateľom internetových služieb (ISP).

Kedy treba mať SLA?
SLA potrebujete len v prípade, ak vaše politiky vyžadovujú prioritu mimo vašej súkromnej siete. Ak používate politiky výstupu na obmedzenie premávky opúšťajúcej váš server, nevyžaduje sa garancia služby. Napríklad môžete v serveri vytvoriť politiku, ktorá pridelí jednej aplikácii vyššiu prioritu než druhej aplikácii. Váš server túto prioritu rozpozná, ale čokoľvek mimo servera túto prioritu nedokáže rozpoznať. Ak máte súkromnú sieť a konfigurujete vaše servery na

rozpoznávanie značiek kódových bodov (ktoré sa používajú na pridelenie úrovne služby politike výstupu), potom smerovače pridelia prioritu prostredníctvom vašej súkromnej siete. Ak premávka opustí vašu súkromnú sieť, neexistujú už žiadne garancie. Bez SLA nemôžete kontrolovať spracovanie premávky sieťovým hardvérom. Mimo vašej súkromnej siete potrebujete SLA na garantovanie priority pre triedu služby alebo rezerváciu prostriedkov.

Prečo treba mať SLA?
Vaše politiky a rezervácie sú dobré iba tak ako najslabšia linka. To znamená, že politiky QoS umožňujú aplikáciám prijímať prioritu prostredníctvom siete. Predsa len, ak niektorý uzol nachádzajúci sa niekde na ceste medzi klientom a serverom nedokáže vykonať ľubovoľnú z charakteristík riadenia premávky opísaných v témach o diferencovanej alebo integrovanej službe, s vašimi politikami sa nebude manipulovať tak, ako si predstavujete. Ak vaša SLA neposkytne dostatok zdrojov, ani najlepšie politiky vám nepomôžu riešiť problém preťaženej siete.

To taktiež zahŕňa zmluvy medzi ISP. Medzi doménami musí každý ISP súhlasiť s podporou požiadaviek kvality služieb. Ich vzájomné fungovanie by mohlo spôsobiť určité problémy.

Uistite sa, že poznáte úroveň služieb, ktorú v skutočnosti dostávate. Zmluvy o úprave prevádzky presne určujú, ako sa prevádzka spracúva, ktorá je zrušená, označená, smerovaná, alebo opakovane prenášaná. Kľúčové dôvody na poskytovanie kvality služieb zahŕňajú kontrolu oneskorenia, časovej nestability, šírky pásma, straty paketov, dostupnosti a priepustnosti. Vaše zmluvy o službách musia byť schopné dať vašim politikám, o čo požiadajú. Overte, či dostávate taký objem služieb, aký potrebujete. Ak nie, možno plytváte svojimi zdrojmi. Napríklad ak žiadate o rezervovanie 500kbps pre IP telefóniu, no vaša aplikácia potrebuje iba 20kbps, asi platíte navyše bez toho, aby ste o tom dostali správu od vášho ISP.

Poznámka: Politiky QoS vám umožňujú realizovať úrovne služieb s vašim ISP, čo môže znížiť cenu sieťovej služby. Napríklad váš ISP vám môže garantovať určitú finančnú sadzbu, ak nepresiahnete úroveň dohodnutej šírky pásma. Alebo si môžete rozložiť používanie politík, počas dňa použijete len časť ″x″ zo šírky pásma a počas noci časť ″y″ zo šírky pásma a dohodnete rýchlosť prenosu údajov pre každú takúto časť. Znovu, ak presiahnete šírku pásma, ISP bude vyžadovať vyššiu platbu. ISP bude vyžadovať dohodnutie sa na určitej úrovni služby a bude chcieť mať možnosť sledovať vami používanú šírku pásma.

Sieťový hardvér a softvér

Kapacita vašich interných zariadení a zariadení mimo vašej siete má na výsledky QoS obrovský vplyv.

Aplikácie
Politiky integrovaných služieb vyžadujú povolené RSVP. Pretože aplikácie iSeries (TM) teraz nepodporujú RSVP, musíte im povoliť používať protokol RSVP. Ak chcete povoliť vaše aplikácie, musíte napísať špeciálne programy za použitia API Resource Reservation Setup Protocol (RAPI) alebo API qtoq QoS soketov. Tieto programy umožnia vašim aplikáciám používať RSVP. Viac informácií nájdete v RSVP protokol a QoS API.

Sieťové uzly
Smerovače, prepínače a dokonca vaše vlastné servery musia mať schopnosť používať kvalitu služieb. Ak chcete používať diferencované politiky služieb, vaše zariadenie musí byť umožnené diferencovanými službami. Znamená to, že sieťový uzol musí byť schopný zoradiť, merať, označiť, upraviť a zrušiť IP pakety. Viac podrobných informácií o upravovačoch premávky (triediť, merať, označiť, upraviť a zrušiť) nájdete v téme Upravovače premávky.

Ak chcete použiť politiky integrovaných služieb, musí mať vaše zariadenie povolené RSVP. Znamená to, že sieťové uzly musia byť taktiež schopné podporovať RSVP protokol. Podrobnejšie informácie o RSVP protokole nájdete v téme RSVP.

Konfigurácia QoS

Po tom, ako vytvoríte plán pre QoS, vytvoríte vaše politiky QoS použitím sprievodcov v rámci programu iSeries™ Navigator. Sprievodcovia vykonajú vynikajúcu prácu tým, že vás prevedú cez konfiguráciu.

Po nakonfigurovaní vašich politík môžete použiť konfiguračné objekty v iSeries Navigator na úpravu vašej konfigurácie politiky. Konfiguračné objekty sú rozličné kusy, alebo časti tvoriace politiku. Keď otvoríte kvalitu služieb v iSeries Navigator, existujú zložky označené klientmi, aplikáciami, plánmi, politikami, triedami služieb, správaniami vykonávanými po skokoch a URI. Tieto objekty vám umožňujú vytvoriť politiku. Ak chcete sprístupniť viac informácií o objektoch, pozrite si Prehľadnú pomoc kvality služby v programe iSeries Navigator.

Konfigurovať QoS použitím sprievodcov
Použite tieto inštrukcie o tom, ako pristupovať k QoS sprievodcom.

Konfigurácia adresárového servera
Tieto informácie použite v prípade, ak plánujete exportovať údaje vašej politiky do adresárového servera. Sprievodca vám umožní určiť, ktorý adresárový server môžete použiť.

V prípade potreby použiť rozhrania API QoS
V závislosti od typu politiky, ktorú ste si zvolili vytvoriť, budete možno musieť použiť API QoS na realizáciu danej politiky.

Povoliť politiky QoS
Aby politiky nadobudli účinnosť, musia byť povolené. Ak ste použili sprievodcov, server vám automaticky povolí politiky. Ak ste však zmenili politiku použitím objektov konfigurácie, budete musieť dynamicky aktualizovať server pred tým, ako sa politiky stanú aktívne. Pred ich aktiváciou však dozrite na prekrývajúce sa politiky, ktoré možno spôsobujú problémy. Pozrite si Poradie politík QoS, kde o tom nájdete viac informácií.

Konfigurovať QoS pomocou sprievodcov

Na konfigurovanie politík kvality služieb musíte použiť sprievodcov QoS, ktorí sa nachádzajú v iSeries(TM) Navigator. Tu je zoznam sprievodcov a ich funkcie:

Sprievodca úvodnou konfiguráciou
Sprievodca vám umožňuje nastaviť špecifickú konfiguráciu servera a informácie adresárového servera.

Sprievodca novou politikou IntServ
Nový sprievodca politikou IntServ vám umožňuje vytvoriť politiku integrovaných služieb. Táto politika povoľuje, alebo zamieta požiadavky RSVP, ktoré nepriamo riadia šírku pásma servera. Ohraničenia výkonu politiky (ktoré určujete vy) rozhodujú, či môže server zvládnuť požadovanú šírku pásma prichádzajúcu z klientskej aplikácie RSVP. Budete potrebovať smerovače a aplikácie podporujúce RSVP, ak chcete realizovať politiky integrovaných služieb vytvorených v tomto sprievodcovi.

Poznámka: Skôr, než nastavíte politiku integrovaných služieb, musíte napísať svoju vlastnú aplikáciu, ktorá používa protokol RSVP. Viac informácií nájdete v časti Rozhrania API QoS.

Sprievodca novou politikou DiffServ
Tento sprievodca vám umožňuje odlíšiť a priradiť prioritu premávke TCP/IP. Budete schopný odlíšiť premávku vytvorením politík. V rámci politiky priraďujete úrovne služieb odchádzajúcej premávke na základe adresy IP zdroja/cieľa, portov, aplikácií a klientov. Vo V5R3 môžu vaše aplikácie iSeries prijímať úrovne služby na základe viac špecifických informácií aplikácie. Viac informácií nájdete v koncepte diferencovaných služieb pred vytvorením tejto politiky.

Sprievodca novou triedou služby
Sprievodcu novou triedou služby použite na nastavenie značkovania paketov smerovačmi a prepínačmi v sieti. Tiež určuje hranice výkonu premávky odchádzajúcej z vašej siete. Triedy služieb použijete v spojení s politikou diferencovaných služieb a politikou povolenia vstupu.

Sprievodca politikou povolenia vstupu
Sprievodcu politikou povolenia vstupu použite na obmedzenie pripojení prichádzajúcich do vášho servera. Prístup

môžete obmedziť podľa adresy TCP/IP, aplikácie, lokálneho rozhrania, alebo URI. Toto umožňuje administrátorovi systému riadiť prístup k vášmu serveru od špecifických klientov, špecifických aplikácii servera alebo podľa URI. Navyše môžete zvýšiť výkon servera.

> **Poznámka:** Predtým, ako nastavíte politiku vstupu používajúcu URI skontrolujte, či port aplikácie priradený pre URI zodpovedá direktíve 'Listen' povolenej pre FRCA v konfigurácii webového servera Apache Web Server. Keď chcete zmeniť alebo si pozrieť port pre váš http server, pozrite si túto tému: Manažovanie adries a portov pre váš HTTP server (podporovaný Apache).

Keď sa rozhodnete, aký typ politiky chcete vytvoriť, môžete ju konfigurovať pomocou príslušného z hore uvedených sprievodcov. Informácie o začatí konfigurácie politiky nájdete v téme Prístup k sprievodcom QoS v iSeries Navigator.

Sprístupniť sprievodcu QoS v programe iSeries Navigator

Ak chcete pristupovať k QoS sprievodcom a vytvoriť novú politiku, nasledujte tieto kroky:

1. V programe iSeries™ Navigator rozviňte váš server —> **Sieť—> Politiky IP**.
2. Pravým tlačidlom kliknite na **Kvalita služby** a kliknite na **Konfigurácia**.
   Poznámka: Sprievodca úvodnou konfiguráciou sa spustí za týchto podmienok:
   - Po prvý krát používate QoS grafické užívateľské rozhranie (GUI) na tomto systéme.
   - Chcete manuálne odstrániť všetky staršie konfiguračné informácie a znova naštartovať. Stáva sa to, len ak je QoS rozhranie už otvorené.
3. Dokončite **sprievodcu Počiatočnou konfiguráciou**. Ak sa Sprievodca úvodnou konfiguráciou nespustí, preskočte na krok 4.
4. Vyberte **Politiky**. Pravým tlačidlom kliknite na **IntServ**, **DiffServ** alebo **Povolenie vstupu**.
5. Vyberte **Nová politika**.

Konfigurovať adresárový server

Konfigurácie politík QoS sa dajú exportovať do adresárového servera LDAP. Toto umožňuje jednoduchšie manažovanie vašich riešení QoS. Namiesto konfigurácie politík QoS na všetkých serveroch môžete konfiguračné údaje uložiť na lokálnom adresárovom serveri na zdieľanie pre viacero systémov. Ak po prvý krát konfigurujete kvalitu servisu na vašom serveri, objaví sa sprievodca Počiatočnou konfiguráciou. Tento sprievodca vás vyzve ku konfigurácii adresárového servera.

Ak chcete konfigurovať adresárový server, budete sa musieť rozhodnúť, alebo poznať nasledujúce informácie:

- Názov adresárového servera
- Určiť rozlišovací názov (DN) ako referenciu do politík QoS
- Určiť používanie alebo nepoužívanie bezpečnosti SSL s vaším adresárovým serverom LDAP
- Určiť používanie alebo nepoužívanie kľúčových slov, ktoré urýchľujú vyhľadávanie vašich politík v adresárovom serveri.

Poznámka: V súčasnosti Kerberos nemôže byť konfigurovaný ako autentifikačná metóda, ktorú QoS server použije na prístup k adresáru.

Ak chcete spravovať LDAP adresárový server, musíte mať jednu z nasledujúcich sád oprávnení:

- *ALLOBJ oprávnenie a *IOSYSCFG oprávnenie

- *JOBCTL oprávnenie a objektové oprávnenie k príkazom Ukončiť TCP/IP (ENDTCP), Spustiť TCP/IP (STRTCP), Spustiť TCP/IP server (STRTCPSVR) a Ukončiť TCP/IP server (ENDTCPSVR).
- *AUDIT oprávnenie na konfiguráciu OS/400(R) bezpečnostného auditovania.

Ak používate program iSeries™ Navigator, budete mať prístup k predvolenej Schéme QoS. Aktuálny súbor schémy je umiestnený vo vašom serveri v /QIBM/UserData/OS400/DirSrv. Avšak, ak používate iný editor, ako iSeries Navigator budete musieť importovať LDIF súbor popísaný nižšie. Rovnako môžete importovať tento súbor, ak po úprave chcete znovu načítať pôvodný štandardný súbor.

QoS schéma

Sada pravidiel nazývaná schéma existujúca, aby určovala, aké typy LDAP objektov sú platné pre QoS server. Schéma obsahuje pravidlá potrebné pre QoS. Ak však používaný LDAP server nie je iSeries server, tieto pravidlá musia byť importované na LDAP server. Deje sa tak so súborom LDIF (LDAP Data Interchange Format). Použite webovú stránku iSeries LDAP

na stiahnutie súboru LDIF. Tento súbor nájdete v ľavej časti okna **Kategórie —> Politiky TCP/IP**. Vzorovú QoS schému nájdete v LDAP koncepty.

Poradie politík QoS

Vždy, keď máte dve politiky, ktoré sa prekrývajú, je dôležité fyzické poradie vašich politík v iSeries(™) Navigator. Prekrývajúce sa politiky predstavujú dve politiky používajúce rovnakého klienta, aplikáciu, plán, lokálnu adresu IP, URI, údaje servera, kódový bod alebo protokol. Politiky na obrazovke iSeries Navigator sú usporiadané v zozname. Priorita politiky závisí od poradia politík v tomto zozname. Ak chcete, aby mala jedna politika prioritu pred inou, musí sa politika s vyššou prioritou nachádzať v zozname vyššie.

Na zistenie, či sa politika prekrýva s inou politikou, postupujte podľa týchto inštrukcií:

1. V programe iSeries Navigator, rozviňte váš server —> **Sieť—> Politiky IP**.
2. Kliknite pravým tlačidlom na **Kvalita služieb**.
3. Zvoľte **Konfigurácia**.
4. Označte príslušný adresár politík.
5. Kliknite pravým tlačidlom na názov politiky, ktorá má združené prekrývajúce sa politiky. Prekrývajúce sa politiky majú pred sebou ikonu, ktorá indikuje prekrývanie.
6. Vyberte **Zobraziť prekrývanie**. Zobrazí sa panel Prekrývanie politík.

Na zmenu poradia politiky na obrazovke použite nasledujúce kroky:

- Označte politiku a použite šípky hore a dole na obrazovke na zmenu poradia politík.
- Kliknite pravým tlačidlom na názov politiky a zvoľte **Presunúť vyššie** alebo **Presunúť nižšie**.
- Aktualizujte server QoS. Môžete použiť tlačidlo Aktualizovať server na lište nástrojov, alebo si pozrite Pomoc úloh QoS, kde nájdete podrobnejšie inštrukcie.

Spravovanie QoS

Po spustení a spravení vašich politík QoS aktívnymi budete musieť najskôr vykonať aktualizácie. Vaše politiky budete spravovať nasledujúcim spôsobom:

Sprístupniť pomoc pre úlohu QoS v programe iSeries Navigator
Pravdepodobne ste zaznamenali, že táto téma odkazuje na pomoc pre úlohu QoS v programe iSeries™ Navigator pomerne často. Ak si nie ste istý, ako sa tam dostať, prezrite si tieto inštrukcie.

Zálohovanie politík QoS
Vaše politiky môžete zálohovať, aby ste sa chránili proti strate súborov.

Kopírovanie existujúcej politiky
Môžete skopírovať existujúcu politiku podobnú politike, ktorú chcete vytvoriť.

Dynamicky aktualizovať politiky
Politiky môžete dynamicky aktualizovať počas behu vášho servera. Použite *Aktualizovať server QoS* v pomoci pre úlohu QoS pre program iSeries Navigator pre postupné pokyny.

Upravovanie politík QoS
Vo vašich existujúcich politikách môžete meniť parametre.

Upraviť vlastnosti konfigurácie QoS
Môžete zmeniť vlastnosti vašej konfigurácie kvality servisu. Tieto vlastnosti zahŕňajú nastavenia pre konfigurácie adresárového servera, žurnálovanie a automatické spúšťanie servera. Použite *Upraviť QoS vlastnosti* v QoS úlohová pomoc iSeries Navigator kvôli inštrukciám krok za krokom.

Povoliť politiky QoS
Ak používate sprievodcov, politika je automaticky povolená. Aj tak však musíte server aktualizovať pre politiku, aby povolenie nadobudlo účinnosť. Skontrolujte, či je povolené QoS a aktualizujte server. Nezabudnite na manuálnu kontrolu v prípade výskytu chýb. Napríklad skontrolujte, či sú vaše politiky v správnom poradí. Ak chcete viac informácií o poradí politík, pozrite si Poradie QoS politík. Inak použite *Povoliť QoS politiky* v QoS úlohová pomoc iSeries Navigator kvôli inštrukciám krok za krokom.

Monitorovanie politík QoS
Pri spravovaní vašich politík môžete chcieť analyzovať QoS monitor, aby ste overili, že politiky pracujú, ako zamýšľate.

Zobraziť prekrývajúce sa politiky QoS
Prezeraním prekrývajúcich sa politík môžete určiť, kde dosahujete iné výsledky, ako ste očakávali. Môžete skontrolovať akékoľvek viditeľné prekrývanie medzi politikami, ktoré by mohlo spôsobovať problémy. Tieto prekrytia budete chcieť vidieť nielen pred aktiváciou a testovaním, ale aj pred tlačením a zálohovaním. Je to užitočný spôsob, ako minimalizovať, alebo odstrániť chyby pred testovaním. Ak chcete zobraziť prekrývajúce sa politiky QoS, pozrite si Usporiadať politiky QoS.

Sprístupniť Pomoc pre QoS v programe iSeries Navigator

Na sprístupnenie pomoci pre kvalitu služby musíte použiť program iSeries™ Navigator:

1. V programe iSeries Navigator, rozviňte váš server —> **Sieť—> Politiky IP**.
2. Pravým tlačidlom kliknite na **Kvalita služby** a kliknite na **Konfigurácia**.
3. Z ponukovej lišty kliknite na **Pomoc —> Témy pomoci**. Na vašej obrazovke sa otvorí okno s pomocou pre úlohu.

Zálohovať QoS politiky

Zálohovanie vašich konfiguračných súborov je vždy dobrý nápad. Vaše politiky sa dajú uložiť lokálne alebo sa dajú exportovať do adresárového servera. Konkrétne musíte zálohovať tento adresár integrovaného súborového systému: QIBM/UserData/OS400/QOS/ETC, QIBM/UserData/OS400/QOS/TEMP a QIBM/UserData/OS400/QOS/USR. Tiež musíte zálohovať vášho zverejňovacieho agenta adresárového servera pre server QoS. Publikačný agent obsahuje názov adresárového servera, charakteristický názov (DN) pre QoS server, port použitý na prístup k adresárovému serveru a autentifikačné informácie. V prípade straty vám potom vaše zálohy ušetria čas a prácu potrebnú na znovuvytvorenie vašich politík úplne od začiatku. Toto sú všeobecné tipy, ktoré môžete použiť na zabezpečenie toho, že budete mať jednoduchý spôsob, ako nahradiť stratené súbory:

1. **Použiť zálohovacie a obnovovacie programy integrovaného súborového systému**
   Použite odkaz na knihu Záloha a obnova viditeľnú dolu.

2. **Vytlačiť politiky**
   Výtlačky môžete uložiť kamkoľvek, kde budú s najväčšou pravdepodobnosťou bezpečné a znovu zadajte informácie podľa potreby.
3. **Kopírovať informácie na disk**
   Kopírovanie má v porovnaní s vytlačením výhodu: odpadá potreba znovu zadávať manuálne informácie existujúce elektronicky. Táto voľba vám poskytuje priamočiaru metódu na prenášanie informácií z jedného zdroja online k inému zdroju.

   Poznámka: Váš server iSeries(TM) kopíruje informácie na systémový disk, nie na disketu. Súbory pravidiel sú v QIBM/UserData/OS400/QOS/ETC ako aj v rámci charakteristického názvu v adresárovom serveri, ktorý ste nakonfigurovali, nie na PC. Môžete chcieť použiť metódu ochrany disku, ako spôsob zálohy na ochranu dát, ktoré sú uložené na systémovom disku.

Pri použití iSeries servera si musíte naplánovať stratégiu zálohovania a obnovy. Zobrazte dokument Záloha a obnova

, kde nájdete viac informácií.

Skopírovať existujúcu politiku

Môžete zistiť, že máte niekoľko politík, ktoré sú si navzájom veľmi podobné. Nevytvárajte ich však všetky od základu, ale urobte si kópie pôvodnej politiky a potom upravte jej časti, ktoré sa líšia od pôvodnej. V iSeries(TM) Navigator sa táto funkcia QoS nazýva *Nová založená na*. Použite program iSeries Navigator, ak chcete sprístupniť dialógové okno QoS, ktoré vám umožňuje uskutočniť kopírovanie politík.

Ak chcete vytvoriť kópiu existujúcej politiky, postupujte podľa krokov opísaných v téme **Vytvoriť novú politiku založenú na existujúcej politike** v pomoci programu iSeries Navigator.

Predtým ako vaše politiky nadobudnú účinnosť, musíte ich povoliť spustením servera QoS alebo vykonaním aktualizácie dynamického servera. Pred ich aktiváciou však dozrite na prekrývajúce sa politiky, ktoré možno spôsobujú problémy. Pozrite si Poradie politík QoS, kde o tom nájdete viac informácií.

Upravovanie politík QoS

Pri zmene vašich potrieb musíte upraviť vaše politiky, aby ste zabezpečili, že stále dostávate vhodný výkon. Pred aktiváciou musíte opraviť všetky chyby a vykonať všetky nutné zmeny vo vašich politikách. Je to najlepší spôsob, ako predísť komplikáciám s výsledkami vašej politiky.

Po konfigurácii vašich politík môžete použiť objekty konfigurácie v programe iSeries™ Navigator na upravenie konfigurácie politiky. Konfiguračné objekty sú rozličné kusy, alebo časti tvoriace politiku. Keď otvoríte kvalitu služieb v iSeries Navigator, existujú zložky označené klientmi, aplikáciami, plánmi, politikami, triedami služieb, správaniami vykonávanými po skokoch a URI. Tieto objekty vám umožňujú upraviť politiku.

Ak chcete upraviť politiku v programe iSeries Navigator, vykonajte kroky opísané na strane **Úprava politiky QoS** v pomoci pre program iSeries Navigator.

Monitorovanie QoS

Monitor môžete použiť na analýzu svojej prevádzky IP cez server. Pomáha určiť, kde sa vo vašej sieti objavuje preťaženie. Je to užitočné nielen počas plánovania QoS, ale aj ako nástroj na odstraňovanie problémov. Monitor QoS vám pomôže v monitorovaní siete, aby ste podľa potreby mohli prispôsobiť vaše politiky. Ak chcete monitorovať všetky aktívne politiky, z okna konfigurácie servera QoS vyberte **Server—>Monitor**. Ak pravým tlačidlom kliknete na niektorú politiku a vyberiete **Monitorovať**, monitor zobrazí len informácie pre túto politiku.

Politiky monitora môžete použiť nasledovne:

- **Ak chcete zobraziť údaje v reálnom čase pre aktívne politiky**
  Ak spustíte monitor, údaje v reálnom čase sa vždy zobrazia pre aktívne politiky. Nemusíte spúšťať zhromažďovanie údajov.
- **Ak chcete zhromažďovať a uchovávať údaje počas istej doby**
  Ak chcete uložiť výsledky monitora, musíte spustiť zhromažďovanie údajov QoS. Monitor bude pokračovať v zhromažďovaní, až kým ho nezastavíte. Zatvorením okna monitora zhromažďovanie nezastavíte. Tiež môžete zmeniť vlastnosti, ktoré monitor používa pri zhromažďovaní údajov. V okne monitora QoS zvýraznite *Monitor QoS* a vyberte *Súbor—>Vlastnosti*, aby ste zmenili vaše voľby. Viac informácií nájdete v online pomoci.

  Ak je spustené zhromažďovanie údajov QoS a vlastnosti monitora sa zmenia, potom vykonajte tieto kroky, aby ste sa uistili, že sa zmeny prejavia v zhromažďovaní údajov.

  1. Zastavte zhromažďovanie údajov QoS.
  2. Zmeňte vlastnosti monitora.
     a. V okne Monitor kliknite na **Monitor QoS**.
     b. Vyberte **Súbor—>Vlastnosti**.
     c. Zmeňte vlastnosti monitora a kliknite na tlačidlo **OK**.
  3. Aktualizujte server QoS.
  4. Spustite zhromažďovanie údajov QoS.

Výstup monitora
Výstupné informácie, ktoré dostávate, závisia od typu politiky, ktorú monitorujete. Spomeňte si na typy politík: DiffServ, IntServ (Riadená záťaž), IntServ (Garantované) a Povolenie vstupu. Vyhodnocované polia závisia od typu politiky. Najzaujímavejšími hodnotami sú hodnoty, ktoré ukazujú meranie. Namiesto daných definícií sa merajú tieto polia: akceptované požiadavky, aktívne pripojenie, služby pripojení, rýchlosti pripojení, zrušené požiadavky, pakety v profile, bity v profile, bity mimo profilu, celkovo bitov, celkovo paketov a celkovo požiadaviek.

Čítaním informácií z vyššie uvedených meraných polí si môžete utvoriť vhodný obraz o tom, či vaša sieťová prevádzka vyhovuje vašim politikám. Nižšie uvedené opisy použite na získanie detailnejších informácií o výstupnom poli monitora pre každý typ politiky. Pozrite si ktorýkoľvek zo scenárov QoS pre získanie príkladu na spôsob použitia monitora spolu s politikami QoS.

- Politiky diferencovaných služieb (Pozrite 50)
- Politiky integrovaných služieb (riadené zavedenie) (Pozrite 51)
- Politiky integrovaných služieb (garantované) (Pozrite 52)
- Politiky povolenia vstupu (Pozrite 52)

Politiky diferencovaných služieb

Pole	Popis
Názov politiky	Názov, ktorý ste priradili tejto politike.
Protokol	UDP, TCP, ALL
Limit priemernej rýchlosti tokenov	Priemerná rýchlosť symbolov, povolená touto politikou v každom smerovači a serveri po celej dĺžke trasy.
Limit hĺbky symbolu	Maximálna veľkosť vyrovnávacej pamäte symbolov, povolená touto politikou v každom smerovači a serveri po celej dĺžke trasy.
Limit vrcholu rýchlosti symbolov	Maximálna rýchlosť, povolená týmto pripojením.
Pakety v profile	Počet prenesených IP paketov, ktoré sa hodia do parametrov tejto politiky.
Bity v profile	Počet prenesených bitov, ktoré sa hodia do parametrov tejto politiky.

Pole	Popis
Bity mimo profilu	Počet prenesených bitov, ktoré presahujú parametre tejto politiky.
Počet bitov	Meraný počet bitov, povolený týmto pripojením.
Aktívne pripojenia	Celkový počet aktívnych pripojení.
Profil prevádzky	Typ podmieňovania paketov, použitého na paketoch mimo profilu. Formát môže zahŕňať: • Preznačenie • Tvarovanie • Zrušenie
Bitov spolu	Počet prenesených bitov, použitých touto politikou od času, keď bola spustená, do momentu ich zhromaždenia monitorom.
Kódový bod v profile	Ak je paket preznačený s novým kódovým bodom, toto je kódový bod, ktorý budú IP pakety používať, ak budú vhodné v rámci parametrov tejto politiky.
Kódový bod mimo profilu	Ak je paket preznačený s novým kódovým bodom, toto je kódový bod, ktorý budú IP pakety používať, ak sa budú vymykať z rámca parametrov tejto politiky.
Rozsah cieľových adries	Rozsah adries, ktorý určuje cieľový bod paketu (riadeného touto politikou).
Spolu paketov	Počet prenesených paketov, použitých touto politikou od času, keď bola spustená, do momentu ich zhromaždenia monitorom.
Rozsah zdrojových portov	Rozsah zdrojových portov, ktorý určuje, ktoré aplikácie bude riadiť táto politika.

Politiky integrovaných služieb (riadená záťaž)

Poznámka: Politiky IntServ sa v monitore nezobrazujú pokiaľ sú aplikácie spustené a sú zriadené rezervácie. Ak vaše politiky IntServ majú viac ako jednu rezerváciu, v monitore uvidíte viac položiek.

Pole	Popis
Názov politiky	Názov, ktorý ste priradili tejto politike.
Protokol	UDP alebo TCP
Cieľová adresa	Rozsah adries, ktorý určuje cieľový bod paketu (riadeného touto politikou).
Limit priemernej rýchlosti tokenov	Priemerná rýchlosť symbolov, povolená touto politikou v každom smerovači a serveri po celej dĺžke trasy pripojenia.
Limit hĺbky symbolu	Maximálna veľkosť vyrovnávacej pamäte symbolov, povolená touto politikou v každom smerovači a serveri po celej dĺžke trasy pripojenia.
Limit vrcholu rýchlosti symbolov	Maximálna rýchlosť, povolená týmto pripojením.
Spolu paketov	Počet prenesených paketov, použitých touto politikou od času, keď bola spustená, do momentu ich zhromaždenia monitorom.
Bity mimo profilu	Počet prenesených bitov, ktoré presahujú parametre tejto politiky.
Bitov spolu	Počet prenesených bitov, použitých touto politikou od času, keď bola spustená, do momentu ich zhromaždenia monitorom.
Počet bitov	Meraný počet bitov, povolený týmto pripojením.

Pole	Popis
Bity v profile	Počet prenesených bitov, ktoré sa hodia do parametrov tejto politiky.
Maximálna veľkosť paketu	Maximálna povolená veľkosť paketu, riadeného touto politikou.
Minimálna odoberaná jednotka	Najmenší počet bitov, ktorý bude odstránený z bloku symbolov. Napríklad ak vaša minimálna odoberaná jednotka je 100 bitov, pakety pod 100 bitov sa odstránia na 100 bitoch.
Pakety v profile	Počet prenesených IP paketov, ktoré sa hodia do parametrov tejto politiky.
Rozsah zdrojových portov	Rozsah zdrojových portov, ktorý určuje, ktoré aplikácie bude riadiť táto politika.

Politiky integrovaných služieb (garantované)

Poznámka: Politiky IntServ sa v monitore nezobrazujú pokiaľ sú aplikácie spustené a sú zriadené rezervácie. Ak vaše politiky IntServ majú viac ako jednu rezerváciu, v monitore uvidíte viac položiek.

Pole	Popis
Názov politiky	Názov, ktorý ste priradili tejto politike.
Protokol	UDP alebo TCP
Cieľová adresa	Rozsah adries, ktorý určuje cieľový bod paketu (riadeného touto politikou).
Limit priemernej rýchlosti tokenov	Maximálna rýchlosť symbolov, povolená touto politikou v každom smerovači a serveri po celej dĺžke trasy pripojenia.
Limit hĺbky symbolu	Maximálna veľkosť vyrovnávacej pamäte symbolov, povolená touto politikou v každom smerovači a serveri po celej dĺžke trasy pripojenia.
Limit vrcholu rýchlosti symbolov	Maximálna rýchlosť, povolená týmto pripojením.
Spolu paketov	Počet prenesených paketov, použitých touto politikou od času, keď bola spustená, do momentu ich zhromaždenia monitorom.
Bitov spolu	Počet prenesených bitov, použitých touto politikou od času, keď bola spustená, do momentu ich zhromaždenia monitorom.
Bity mimo profilu	Počet prenesených bitov, ktoré presahujú parametre tejto politiky.
Garantovaná rýchlosť	Garantovaná rýchlosť v bitoch za sekundu.
Bity v profile	Počet prenesených bitov, ktoré sa hodia do parametrov tejto politiky.
Maximálna veľkosť paketu	Maximálna povolená veľkosť paketu, riadeného touto politikou.
Minimálna odoberaná jednotka	Najmenší počet bitov, ktorý bude odstránený z bloku symbolov. Napríklad ak vaša minimálna odoberaná jednotka je 100 bitov, pakety pod 100 bitov sa odstránia na 100 bitoch.
Pakety v profile	Počet prenesených IP paketov, ktoré sa hodia do parametrov tejto politiky.
Trvanie omeškania	Rozdiel (v sekundách) medzi vyžadovaným a získaným oneskorením.
Rozsah zdrojových portov	Rozsah zdrojových portov, ktorý určuje, ktoré aplikácie bude riadiť táto politika.

Politiky povolenia vstupu

Pole	Popis
Názov politiky	Názov, ktorý ste priradili tejto politike.
Počet pripojení	Počet akceptovaných požiadaviek na pripojenie za sekundu.
Požiadaviek spolu	Celkový počet požiadaviek na pripojenie, odoslaných na tento server.
Akceptované požiadavky	Celkový počet požiadaviek na pripojenie, akceptovaných týmto serverom.
Zrušené požiadavky	Celkový počet požiadaviek, zrušených týmto serverom.
Limit priemerného počtu pripojení	Povoliteľný priemerný počet prijatých nových pripojení na pripojenie za sekundu.
Nárazový limit pripojení	Maximálny počet nových požiadaviek na pripojenie, akceptovaných súčasne.
Limit vrcholu rýchlosti pripojenia	Maximálna povoliteľná úroveň, na ktorej bude server akceptovať pripojenia zo siete
Priorita	Priorita, priradená každému pravidlu, zavedenému do Manažéra QoS.
Priorita vo fronte	Priorita, priradená prichádzajúcim pripojeniam, uloženým do načúvacieho frontu.
Rozsah cieľových portov	Rozsah portov alebo port, na ktorý je na vašom serveri smerovaná prevádzka.
Adresa rozhrania	IP adresa systémového rozhrania, ktoré sa má monitorovať.
Rozsah zdrojových adries	Rozsah IP adries klientov, odosielajúcich požiadavky na váš server.
URI	Identita preverovaného URI.

Odstránenie problémov QoS

V tejto téme nájdete informácie o odstraňovaní problémov s QoS.

Sledovanie komunikácií
Váš server poskytuje sledovanie komunikácií na zbieranie údajov o vašej komunikačnej linke, akou je rozhranie lokálnej siete (LAN), alebo rozšírenej siete (WAN). Bežný užívateľ nemusí chápať úplný rozsah sledovaných údajov. Vy však môžete použiť záznamy zo sledovania pri rozhodovaní, či medzi dvoma bodmi v sieti došlo k výmene údajov. Viac informácií nájdete v časti sledovanie komunikácií v téme Odstraňovanie problémov s TCP/IP.

Povoliť QoS v serveri
Prvú vec, ktorú treba skontrolovať, ak sa server QoS nespustí, je zistiť, či je QoS v serveri povolené. Keď svoje politiky konfigurujete po prvý raz, Sprievodca úvodnou konfiguráciou povolí QoS v serveri automaticky. Predsa len, ak bola táto hodnota menená z akéhokoľvek dôvodu, server sa nespustí.

Ak chcete skontrolovať, či je QoS povolené v serveri, vykonajte tieto kroky:

1. V iSeries(TM) Navigator rozviňte váš server —> **Sieť—> Politiky IP**.
2. Kliknite pravým tlačidlom na **Kvalita služieb** a zvoľte **Konfigurácia**.
3. Po zobrazení rozhrania QoS pravým tlačidlom kliknite na **QoS** a vyberte **Vlastnosti**.
4. Na strane vlastností QoS skontrolujte, či je vybraté **Povoliť QoS**.

Žurnálovanie politík QoS
Vaša funkcia kvality servera obsahuje aj vlastnosť zaznamenávania. Môžete ju použiť na zaznamenávanie politík IP, ktoré sú na vašom server pridané, odstránené, alebo zmenené. Toto vám umožňuje ladiť a náhodne kontrolovať vaše politiky a overovať si, že fungujú tak, ako ste to zamýšľali.

Protokolovať politiky QoS
Ak zistíte, že máte problémy so serverom, možno budete chcieť analyzovať protokoly úloh.

Monitorovanie serverových transakcií
Monitor QoS predstavuje prvý bod pre vyhľadanie a vyriešenie vašich problémov s QoS. Zaznamenáva a umožňuje vám prezerať informácie o výkone QoS.

Sledovanie aplikácií TCP
Na protokolovanie niekoľkých úrovní serverových akcií použite príkaz trace. Môže to pomôcť, ak sa pokúšate určiť problémy s politikami QoS.

Poradie politík QoS
Poradie, v akom sú politiky v súbore zoradené, je pre úspech implementácie QoS veľmi dôležité.

Žurnálovať QoS politiky

QoS zahŕňa žurnálovaciu funkciu. Žurnálovanie vám umožňuje sledovať akcie QoS politiky, ako kedy a bola politika pridaná, odstránená, alebo zmenená. Vytvára protokol akcií politiky pokiaľ máte žurnálovanie nastavené na ON. Pomáha vám to odladiť a zbadať, kde politiky nepracujú podľa predstáv. Napríklad nastavíte politiku tak, aby bola spustená od 9:00 - 16:00. Potom môžete skontrolovať protokol žurnálu, ak chcete zistiť, či bola politika naozaj pridaná o 9:00 a odstránená o 16:00.

Ak je žurnálovanie zapnuté, žurnálové vstupy sú generované kedykoľvek je politika pridaná, odstránená, alebo modifikovaná. Pomocou týchto žurnálov vytvoríte všeobecný súbor na serveri iSeries(TM). Potom môžete použiť informácie zaznamenané v žurnáloch vášho systému na určenie toho, ako sa systém používa. Môže vám to pomôcť pri rozhodovaní zmeniť rôzne aspekty vašich politík.

Buďte selektívny pri výbere vecí na žurnálovanie. Žurnálovanie môže veľmi zaťažovať vaše systémové zdroje. Ak chcete spustiť, alebo zastaviť žurnálovanie použite iSeries Navigator. Ak chcete vidieť protokoly žurnálov, musíte použiť rozhranie založené na znakoch.

Ak chcete spustiť, alebo zastaviť žurnálovanie, urobte nasledovné:

1. V iSeries Navigator rozviňte váš server —> **Sieť—> IP Politiky**.
2. Kliknite pravým tlačidlom na **Kvalita služieb** a vyberte **Konfigurácia**.
3. Kliknite pravým tlačidlom na **QoS** a vyberte **Vlastnosti**.

4. Vyberte rámček **Spustiť žurnálovanie**, ak chcete spustiť žurnálovanie.
5. Zrušte výber **Spustiť žurnálovanie**, ak chcete vypnúť žurnálovanie.

Pozor: Ak je už server spustený pred ukončením horeuvedených krokov, musíte zastaviť a reštartovať server. Len čo bolo žurnálovanie zapnuté, existujú dva spôsoby, ako ho aktivovať. Môžete zastaviť a reštartovať server, alebo vykonať aktualizáciu servera. Oba spôsoby znovu prečítajú súbor policy.conf a budú hľadať žurnálovací atribút.

Prezeranie žurnálových záznamov na monitore

Ak chcete vidieť tieto žurnálové záznamy na obrazovke, urobte nasledovné:

1. V príkazovom riadku na iSeries serveri zadajte: DSPJRN JRN(QUSRSYS/QQOS). Vyberte **Voľba 5** na žurnálovom zázname, ktorý chcete vidieť.

Prezeranie žurnálových záznamov prostredníctvom výstupného súboru

Ak by ste chceli prezerať žurnálové záznamy formátované do jedného adresára, prezrite si súbor MODEL.OUT v adresári QUSRSYS. Skopírovaním žurnálových vstupov do výstupného súboru môžete jednoducho prezerať záznamy za použitia dotazovacích pomocných programov, ako Query/400, alebo SQL. Rovnako môžete napísať vaše vlastné HLL programy na spracúvanie záznamov vo výstupných súboroch.

Ak chcete skopírovať QoS žurnálové záznamy do výstupného súboru poskytnutého systémom:

1. Vytvorte kópiu výstupného súboru poskytnutého systémom QSYS/QATOQQOS do užívateľskej knižnice. Môžete tak urobiť za použitia príkazu CRTDUPOBJ (Create Duplicate Object). Nasleduje príklad príkazu CRTDUPOBJ:
   CRTDUPOBJ OBJ(QADSPJR4) FROMLIB(Qsys) OBJTYPE(*FILE) TOLIB(userlib) NEWOBj(userfile)
2. Použite príkaz DSPJRN (Display Journal) na skopírovanie záznamov zo žurnálu QUSRSYS/QQOS do výstupného súboru vytvoreného v predošlom kroku. Ak sa pokúsite skopírovať DSPJRN do neexistujúceho výstupného súboru, systém pre vás súbor vytvorí, ale tento súbor nebude obsahovať správne opisy polí.
   a. DSPJRN JRN(QUSRSYS/QQOS) JRNCDE((M)) ENTTYP(MP) CMTCYCID(*ALL) OUTPUT(*OUTFILE) OUTFILFMT(*TYPE4) OUTFILE(userlib/userfile)
   b. DSPF FILE(userlib/userfile)

Zaprotokolovať úlohy servera QoS

Keď narazíte na problémy s politikami QoS, analyzujte protokoly úloh servera iSeries™. Protokol úlohy obsahuje chybové hlásenia a ďalšie informácie týkajúce sa QoS.

V podsystéme QSYSWRK beží iba jedna úloha QoS - QTOQSRVR. Staršie a aktuálne protokoly úlohy servera QoS si môžete pozrieť cez iSeries Navigator.

Protokol zobrazte nasledujúcim spôsobom:

1. Rozviňte **Sieť** a kliknite na **Politiky IP**.
2. Kliknite pravým tlačidlom na **Kvalita služieb**.
3. Vyberte **Diagnostické nástroje —>Protokol servera QoS**.

Otvorí sa okno, ktoré vám umožní pracovať s úlohou.

Nasledujúci zoznam zobrazuje názvy najdôležitejších úloh, spolu so stručným vysvetlením, na čo sa úloha používa:

QTCP
Ide o základnú úlohu, ktorá spúšťa všetky rozhrania TCP/IP. Ak máte zásadné problémy s TCP/IP všeobecne, analyzujte protokol úlohy QTCPIP.

QTOQSRVR
Táto úloha je základnou úlohou QoS, ktorá vám poskytne informácie o protokole, špecifické pre QoS. Spustite (pracovný súbor v odkladacej oblasti) WRKSPLF QTCP a vyhľadajte protokol QTOQSRVR.

Ak chcete skontrolovať, či náhodou pracovný súbor v odkladacej oblasti neobsahuje chybu, vykonajte tieto kroky:

1. Z rozhrania príkazového riadka zadajte **WRKSPLF QTCP** a stlačte Enter.
2. Otvorí sa okno Pracovať so všetkými súbormi v odkladacej oblasti. V stĺpci Užívateľské údaje vyhľadajte QTOQSRVR, kde nájdete chyby, ktoré sa špecificky týkajú servera QoS.
3. Na riadku, ktorý chcete zobraziť, zvoľte **Voľba 5**. Prečítajte si tieto informácie a poznamenajte si ID správy, ktorá vysvetľuje problém. Napríklad TCP920C.
4. Dvakrát stlačte **F3** na návrat do hlavnej ponuky.
5. Z rozhrania príkazového riadka zadajte **WRKMSGF** a stlačte **Enter**.
6. Na obrazovke Pracovať so súborom správ zadajte nasledujúcu informáciu a stlačte **Enter**.
   Súbor správ: QTCPMSG
   Knižnica: *LIBL
7. Na obrazovke Pracovať so súborom správ zvoľte **voľbu 5** na zobrazenie súboru správ, ktorý si chcete pozrieť, a stlačte **Enter**.
8. Na obrazovke Zobraziť popisy správ zadajte nasledujúce informácie:
   Nastavte sa na: Zadajte vaše ID správy od čísla 3 vyššie a stlačte Enter. Napríklad TCP920C.
9. Vyberte **Voľba 5** pre vyžadované ID správy a stlačte kláves **Enter**.
10. Na obrazovke Zvoľte podrobnosti správy na zobrazenie vyberte 30 (Všetky predchádzajúce) a stlačte **Enter**.
11. Objaví sa podrobný popis správy.

Monitorovanie serverových transakcií

Monitor QoS vám môže pomôcť v plánovacej fáze a vo fáze odstraňovania problémov QoS.

Monitor môžete použiť na analýzu prevádzky IP cez server. To vám pomáha určiť, kde sa vo vašej sieti objavuje preťaženie. Monitor QoS vám pomôže v monitorovaní siete, aby ste podľa potreby mohli prispôsobiť vaše politiky.

Plánovanie a údržba výkonu
Najnáročnejšie pri implementácii QoS je určiť, aké limity výkonu sa majú nastaviť vo vašich politikách. Neexistuje žiadne konkrétne odporúčanie, pretože každá sieť je iná. Ak chcete zistiť, aké hodnoty sú pre vás najvhodnejšie, môžete ešte pred spustením akýchkoľvek politík použiť monitor.

Vytvorte politiku diferencovaných služieb bez použitia merania, ktoré identifikuje správanie vašej sieťovej prevádzky. Aktivujte túto politiku a spustite monitor. Výsledky monitora vám prípadne pomôžu optimalizovať politiky s vašimi špecifickými potrebami. Pozrite si vzorovú monitorovaciu politiku, ktorá identifikuje, ako sa správa vaša aktuálna prevádzka.

Odstraňovanie problémov s výkonom
Monitor môžete použiť na odstránenie problémov. Prostredníctvom výstupu monitora môžete zistiť, či sa dodržiavajú parametre, ktoré ste určili politike. Ak sa vaše politiky zobrazujú v monitore, ale neovplyvňujú premávku, skontrolujte nasledujúce:

- Ak politika filtruje na základe URI, skontrolujte, či je povolené FRCA a je správne nakonfigurované. Predtým, ako nastavíte politiku vstupu používajúcu URI skontrolujte, či port aplikácie priradený pre URI zodpovedá direktíve 'Listen' povolenej pre FRCA v konfigurácii webového servera Apache Web Server. Ak chcete zmeniť alebo zobraziť port pre váš server HTTP, pozrite si túto tému: Manažovať adresy a porty pre váš server HTTP (založený na Apache).
- Skontrolujte plán politiky. Možno budete chcieť zistiť výsledky počas neaktívnej doby politiky.
- Skontrolujte, či je číslo portu správne.
- Skontrolujte, či adresa IP správna.

Príklady výstupov monitora nájdete medzi Scenármi QoS, alebo si pozrite polia monitora v monitoringu.

Monitorovanie aktuálnych štatistík siete

Cieľ

V rámci sprievodcov budete vyzvaný zadať limity výkonu. Sú to však hodnoty, ktoré sa neodporúčajú, pretože sú založené na individuálnych potrebách sietí. Na nastavenie týchto limitov musíte reálne poznať aktuálny výkon vašej siete. Keďže sa pokúšate konfigurovať politiky kvality služieb, pravdepodobne už máte vhodnú predstavu o aktuálnych potrebách vašej siete. Ak chcete určiť presné limity rýchlosti, ako rýchlosť tokenov, môžete monitorovať všetku premávku vo vašom serveri, aby ste mohli lepšie určiť limity rýchlosti na nastavenie.

Riešenie

Vytvorte veľmi všeobecnú politiku diferencovanej služby, ktorá neobsahuje obmedzenia (žiadne maximálne hodnoty) a používa sa na všetky rozhrania a všetky IP adresy. Použite monitor QoS na záznam údajov z tejto politiky.

Krok 1: Otvorte QoS v iSeries(TM) Navigator.

1. V programe iSeries Navigator, rozviňte váš server —> **Sieť—> Politiky IP**
2. Kliknite pravým tlačidlom na **Kvalita služieb** a zvoľte **Konfigurácia**.
3. Rozviňte **Politiky šírky výstupného pásma**.
4. Kliknite pravým tlačidlom na **DiffServ** a zvoľte **Nová politika**. Zobrazí sa Sprievodca novou politikou QoS.

Krok 2: Vytvorte politiku diferencovanej služby

Keďže chcete zbierať väčšinu prevádzky, vstupujúcu do vašej siete, mohli by ste politiku nazývať **Sieť**. Použite všetky IP adresy, všetky porty, všetky lokálne IP adresy a všetky časy (ak je to vhodné). Počas prechodu sprievodcom použite nasledujúce nastavenia:

Názov = Sieť (akýkoľvek názov)
Klient = Všetky IP adresy
Aplikácia = Všetky porty
Protokol = Všetky protokoly
Plán = Všetky časy

iSeries Navigator zobrazí všetky politiky diferencovaných služieb, vytvorené na vašom serveri.

Krok 3: Dokončite novú triedu služieb

Počas dokončovania sprievodcu sa od vás bude vyžadovať priradenie skokového správania, limitov pre výkon a spôsobu riadenia premávky mimo profilu. To sa definuje v triede služieb. Zvoľte extrémne veľké hodnoty, aby ste umožnili tok takej prevádzky, aká je len možná.

Triedy služieb v skutočnosti určujú výkonové úrovne, ktoré táto prevádzka prijíma zo smerovača. Vašu triedu služby môžete nazvať **Neobmedzená**, aby ste označili, že táto premávka prijme vyššiu úroveň služby. iSeries Navigator zobrazuje všetky triedy služieb, vytvorené na vašom serveri.

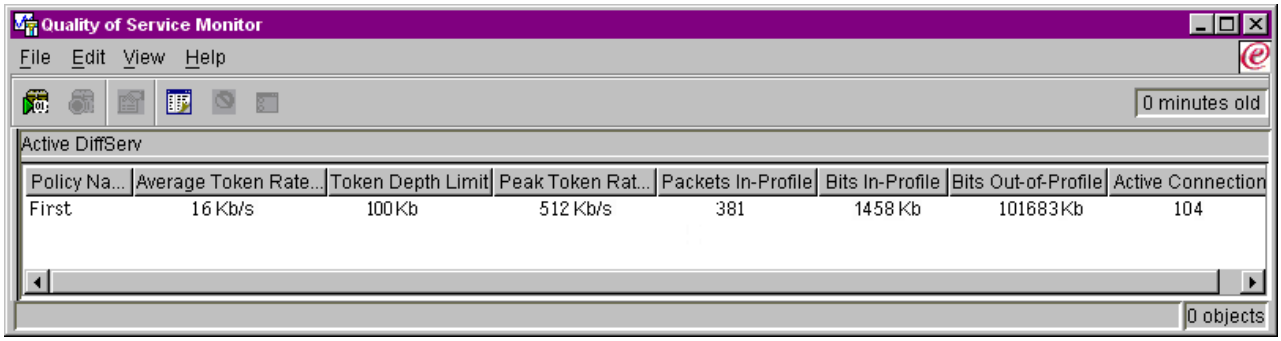
Krok 4: Monitorujte vašu politiku

Ak si chcete overiť, že prevádzka sa správa tak, ako ste to nakonfigurovali v politike, použite monitor.

1. Vyberte konkrétnu zložku politík (DiffServ, IntServ, Povolenie vstupu).
2. Kliknite pravým tlačidlom na politiku, ktorú chcete monitorovať a zvoľte **Monitorovať**.

Nižšie je zoznam možných výstupov monitora pre politiku, nastavenú vyššie.

Obrázok 14. Monitor kvality služby.



Vyhľadajte polia, ktoré získavajú svoje údaje z vašej prevádzky. Skontrolujte polia celkových bitov, bitov v profile, paketov v profile a bitov mimo profilu. Bity mimo profilu označujú, že premávka presiahla nakonfigurované hodnoty politiky. V politike diferencovanej služby číslo mimo profilu indikuje počet stratených bajtov. Pakety v profile indikujú počet bitov, riadených touto politikou (od momentu, keď bol paket spustený, po súčasný výstup monitora).

Záleží aj na tom, aké hodnoty priradíte poľu limitu priemernej rýchlosti symbolu. Keď pakety prekročia tento limit, server ich začne rušiť. Ako následok sa zvýši počet bitov mimo profilu. To vám ukazuje, že sa politika správa tak, ako ste ju nakonfigurovali. Na zmenu počtu bitov mimo profilu musíte prispôsobiť vaše limity výkonu. Kvôli popisu všetkých polí monitora si pozrite časť monitor.

Krok 5: zmeniť hodnoty v prípade potreby
Po spustení monitorovania môžete zmeniť ľubovoľné z hodnôt, ktoré ste predtým vybrali. Pravým tlačidlom kliknite na názov triedy služby, ktorý ste v tejto politike vytvorili. Ak si vyberiete **Vlastnosti**, zobrazí sa dialógové okno Vlastnosti QoS s hodnotami, prostredníctvom ktorých riadite vašu premávku.

Krok 6: Opakujte monitorovanie politiky
Po prezretí výsledkov použite metódu ″pokus a omyl″ na nájdenie najlepších hodnôt pre potreby vašej siete.

Sledovanie aplikácií TCP

Sledovanie QoS použite na prácu s funkciami sledovania a na zobrazenie aktuálneho pamäťového bloku sledovania. Ak chcete spustiť sledovanie v serveri, vykonajte jedno z nasledujúceho:

- Napíšte TRCTCPAPP z rozhrania pre príkazový riadok.

Tu je príklad výberu sledovania, ktoré má byť vykonané:

```
Aplikácia TCP/IP.............> *QOS
Nastavenie sledovania........> *ON
Maximálna pamäť sledovania...> *APP
Akcia plného sledovania......> *WRAP
Zoznam argumentov............> 'lvl=4'
Typ sledovania QoS...........> *ALL
```

Nasledujúca tabuľka predstavuje možné parametre, ktoré môžu byť použité pri sledovaní. Ak sa vám v znakovom prostredí možnosti nezobrazia, musíte ich zadať príkazom. Napríklad , TRCTCPAPP APP(*QOS) MAXSTG(1000) TRCFULL(*STOPTRC) ARGLIST('l=4 c=i').

Nastavenie	Voľby
Aplikácia TCP/IP	QOS
Nastavenie voľby Sledovať	*ON, *OFF, *END, *CHK
Maximálny úložný priestor pre sledovanie (Pozrite 59) (MAXSTG)	1-16000, *APP
Akcia Úplné sledovanie (Pozrite 59) (TRCFULL)	*WRAP, *STOPTRC
Zoznam argumentov (Pozrite 59) (ARGLIST)	Úrovne: 'lvl=1', 'lvl=2', 'lvl=3', 'lvl=4' Obsah: 'c=a', 'c=i', 'c=d' , 'c=m'
Typ sledovania QoS	*ALL

Ak potrebujete pomoc pri interpretácii výsledkov sledovania, pozrite si Čítanie výsledkov sledovania. Stránka s výsledkami sledovania obsahuje príklady výsledkov s poznámkami, ktoré vám môžu pomôcť pri interpretácii. Funkciu TRCTCPAPP typicky používa servis, preto ak máte problémy pri interpretácii výstupu, kontaktujte predstaviteľa servisu.

Maximálny úložný priestor pre sledovanie

1-16000
Toto je maximálna veľkosť pamäte vyhradenej pre údaje o sledovaní. Keď je táto veľkosť dosiahnutá, sledovanie sa buď zastaví, alebo zbalí. Predvolená veľkosť sú 4MB. Ak chcete zadať túto predvolenú veľkosť, zadajte *APP.

***APP**
Toto je predvolená možnosť. Podľa nej má aplikácia použiť predvolenú veľkosť sledovania. Predvolená veľkosť sledovania pre server QoS sú 4MB.

Akcia Úplné sledovanie

***WRAP**
Keď sledovanie dosiahne maximálnu povolenú veľkosť diskového priestoru (veľkosť vyrovnávacej pamäte sledovania), zbalí informácie o sledovaní. Zbalenie umožní systému prepísať v súbore staršie informácie, takže môžete pokračovať v zaznamenávaní informácií o sledovaní. Ak nevyberiete túto možnosť, pri naplnení disku sa zastaví sledovanie.

***STOPTRC**
Keď systém dosiahne maximálnu veľkosť disku, zastaví zbieranie informácií.

Zoznam argumentov

Určuje, ktoré chybové úrovne a obsah budú protokolované. Pre príkaz TRCTCPAPP sú povolené dva argumenty: úroveň sledovania a sledovaný obsah. Keď ich zadáte, uistite sa, že sú všetky atribúty zahrnuté v jednotlivých úvodzovkách. Napríklad TRCTCPAPP 'l=4 c=a'

Poznámka: Úrovne protokolovania zahŕňaju aj všetky nižšie úrovne. To znamená, že ak zadáte úroveň protokolovania, automaticky ste vybrali aj všetky predošlé úrovne. Ak napríklad zadáte úroveň 3, sú do nej automaticky zahrnuté aj úrovne 1 a 2. Pri typickom sledovaní sa odporúča zadať 'l=4'. **Úrovne sledovania**

Úroveň 1: Systémové chyby (SYSERR)
Protokolovanie chýb, ktoré sa objavia pri systémových operáciách. Ak sa objaví takáto chyba, server QoS nemôže pokračovať. Takáto systémová chyba sa napríklad môže objaviť, ak sa blížite k hraniciam systémovej pamäte, alebo ak systém nemôže komunikovať s TCP/IP. Toto je predvolená úroveň.

Úroveň 2: Chyby medzi objektmi (OBJERR)
Protokoluje chyby, ktoré sa objavia v kóde servera QoS. Objektová chyba sa môže napríklad objaviť ak sa serverová operácia stretne s neočakávanými výsledkami. Toto vo všeobecnosti predstavuje vážny stav, ktorý je treba nahlásiť servisu.

Úroveň 3: Špecifické udalosti (EVENT)
Zaznamenáva akékoľvek operácie servera QoS, ktoré sa vyskytnú. Napríklad príkazy a požiadavky o záznamy protokolu udalostí. Výsledky sú podobné, ako funkcia denníka QoS.

Úroveň 4: Správy sledovania (TRACE)
Sleduje všetky údaje prenášané zo servera QoS a na server QoS. Napríklad môžete toto vysoko-úrovňové sledovanie použiť na zaprotokolovanie všetkého, o čom si myslíte, že môže byť užitočné pri odstraňovaní problémov. Tieto informácie sú prospešné pri určovaní, kde sa problém objavil a ako ho reprodukovať.

Obsah sledovania

Poznámka: Môžete zadať len jeden typ obsahu. Ak neurčíte žiaden typ, bude (štandardne) sledovaný všetok obsah.

Obsah = Všetko (’c=a’)
Sleduje všetky funkcie servera QoS. Toto je predvolená hodnota.

Obsah = Intserv (’c=i’)
Sleduje len operácie IntServ. Túto možnosť použijete, ak hľadáte problém spojený s IntServ.

Obsah = Diffserv (’c=d’)
Sleduje len operácie DiffServ. Túto možnosť použijete, ak hľadáte problém spojený s DiffServ.

Obsah = Monitor (’c=m’)
Sleduje len monitorovacie operácie.

Ak chcete získať kompletnejšie informácie o príkaze TRCTCPAPP, pozrite si Opis príkazu TRCTCPAPP (Sledovať aplikáciu TCP/IP) v rámci témy Príkazy CL.

Prečítať výstup sledovania

Nejde tu o kompletnú diskusiu, ako čítať váš výstup zo sledovania. Vyzdvihuje však kľúčové udalosti, ktoré máte v informáciách zo sledovania hľadať.

V **politike integrovaných služieb** je najdôležitejším bodom zistenie prípadného zamietnutia pripojenia RSVP v prípade, že sa nenašla príslušná politika pre toto pripojenie. Tu je príklad správy o úspechu:

```
12/15 11:36:14 [336,80] TRCE :.......rpapi_getPolicyData: Našiel sa názov akcie vreStnl_kraMoNlCvreStnl pre tok
[sess=x.x.x.x:y:z:s, source=x.x.x.x:y]
```

Tu je príklad správy o neúspešnom pripojení integrovaných služieb:

```
12/15 11:36:14 [336,80] TRCE :.......rpapi_getPolicyData: Nenašiel sa názov akcie pre tok [sess=x.x.x.x:y]
```

Pre **politiku diferencovaných služieb** najdôležitejšie správy ukazujú, či server zaviedol pravidlo politiky alebo či nastala chyba v konfiguračnom súbore politiky.

Príklad:
01/11 14:07:52 [376,57] TRCE :.....KernelAddPolicyRule: Inštaluje sa pravidlo = timed_42ring.
01/11 14:07:52 [376,57] EVNT :.....create_tcp_resv: Žiadna hodnota v konfiguračnom súbore pre DiffServInProfilePeakRate, nastavené na 100000 00.
01/11 14:07:52 [376,57] TRCE :.....create_tcp_resv: Create resv - bRate: 537395 5722SS1 V5R1M0 010525 TRCTCPAPP Výstup RS004 Date-01/11/01 Čas-14:08:03 Strana-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

Taktiež môžete mať správy, ktoré ukazujú, že označenia v konfiguračnom súbore politiky boli nesprávne. Tu je niekoľko vzorových správ:

12/15 11:36:14 [336,80] TRCE :.....rpapi_getPolicyData: Neznámy atribút %s v politike služieb - ignoruje sa. 12/15 11:36:14 [336,80] TRCE :.....rpapi_getPolicyData: Neznámy atribút %s pri mapovaní priority - ignoruje sa.

Poznámka: Znak % je premennou, ktorá reprezentuje neznáme označenie.

Informácie týkajúce sa QoS

Existuje veľa ďalších zdrojov informácií o kvalite služby v priemysle. Prezrite si najnovšie RFC, biele stránky, Redbooks(TM) a iné zdroje, z ktorých získate všeobecné informácie o QoS. Tu je niekoľko z nich:

Dokumenty RFC (Requests for Comments) o QoS
Dokumenty RFC (Requests for Comments) sú napísané definície štandardov protokolov a navrhovaných štandardov používaných v sieti Internet. Nasledujúce RFC môžu pomôcť pri pochopení QoS a s ním súvisiacich funkcií:

RFC 1349
Tento RFC pojednáva o novej definícii poľa TOS v hlavičke IP paketu.

RFC 2205
Toto RFC vysvetľuje definíciu protokolu RSVP (Resource ReSerVation Protocol).

RFC 2210
Toto RFC vysvetľuje používanie RSVP spolu s Integrovanými službami IETF.

RFC 2474
Toto RFC vysvetľuje definíciu poľa diferencovaných služieb (poľa DS).

RFC 2475
Toto RFC vysvetľuje architektúru diferencovaných služieb.

Ak chcete zobraziť vyššie uvedené dokumenty RFC, pozrite si stránku RFC index search engine

umiestnenú na webovej lokalite RFC editor

. Vyhľadajte číslo dokumentu RFC, ktoré chcete zobraziť. Výsledky vyhľadávacieho mechanizmu zobrazia príslušný názov dokumentu RFC, autora, dátum a stav.

IBM(R) Redbooks

iSeries IP Networks: Dynamic!

Toto je najnovší redbook o budovaní sietí IP. Uvádza, ako navrhnúť samokonfigurujúcu sa sieť IP, odolnú voči chybám a s efektívnou prevádzkou. Ako doplnok k ďalším mnohým funkciám vysvetľuje teóriu QoS, ako aj jeho implementáciu v systéme iSeries. Tiež v nej nájdete viac scenárov s postupnými pokynmi na ich vyriešenie.

TCP/IP More Cool Things than Ever

Tento návod poskytuje vzorové scenáre, ktoré demonštrujú bežné riešenia s príkladmi konfigurácií. Informácie v tomto návode vám pomôžu naplánovať, nainštalovať, prispôsobiť, konfigurovať a opravovať TCP/IP na vašom serveri iSeries. Zatiaľ síce ešte neobsahuje Kvalitu služby, ale poskytuje informácie o adresárovom serveri LDAP.

TCP/IP Tutorial and Technical Overview

Tento návod poskytuje úvod, ako aj odkaz na sadu protokolov a aplikácií Transmission Control Protocol/Internet Protocol (TCP/IP). Nájdete kvalitu služieb v rámci *časti 3. Rozšírené koncepty a nové technológie* v kapitole 22.

Témy súvisiace s Informačným centrom iSeries

Adresárové služby (LDAP)
Pozrite si túto tému, aby ste získali základy, konfiguráciu a administráciu adresárového servera a pomoc pri odstraňovaní problémov. Téma adresárových služieb vám tiež poskytne ďalšie zdroje pre konfiguráciu vášho adresárového servera.

Príloha. Právne informácie

Tieto informácie boli vyvinuté pre produkty a služby ponúkané v USA.

IBM nemusí ponúkať produkty, služby alebo vlastnosti opisované v tomto dokumente v iných krajinách. Informácie o aktuálne dostupných produktoch a službách vo vašej krajine získate od predstaviteľa lokálnej pobočky IBM. Žiadny odkaz na produkt, program alebo službu IBM nie je myslený tak a ani neimplikuje, že sa môže používať len tento produkt, program alebo služba od IBM. Namiesto nich sa môže použiť ľubovoľný funkčne ekvivalentný produkt, program alebo služba, ktorá neporušuje intelektuálne vlastnícke právo IBM. Vyhodnotenie a kontrola činnosti produktu, programu alebo služby inej ako od IBM je však na zodpovednosti užívateľa.

IBM môže vlastniť patenty alebo nevybavené prihlášky patentov, týkajúce sa predmetu, popísaného v tomto dokumente. Získanie tohto dokumentu vám nedáva žiadnu licenciu na tieto patenty. Žiadosti o licencie môžete zasielať písomne na:

```
IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY  10504-1785
U.S.A.
```

Žiadosti o licencie týkajúce sa dvojbajtových (DBCS) informácií smerujte na oddelenie intelektuálneho vlastníctva IBM vo vašej krajine alebo ich pošlite písomne na:

```
IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan
```

Nasledujúci odsek sa netýka Veľkej Británie ani žiadnej inej krajiny, kde sú takéto vyhlásenia nezlučiteľné s lokálnym zákonom: SPOLOČNOSŤ INTERNATIONAL BUSINESS MACHINES POSKYTUJE TÚTO PUBLIKÁCIU ″TAK AKO JE″ BEZ ZÁRUKY AKÉHOKOĽVEK DRUHU, VYJADRENEJ ALEBO IMPLIKOVANEJ, VRÁTANE (ALE NEOBMEDZENE) IMPLIKOVANÝCH ZÁRUK NEPOŠKODENIA, PREDAJNOSTI ALEBO VHODNOSTI NA KONKRÉTNY ÚČEL. Niektoré štáty nedovoľujú zriecť sa vyjadrených alebo implikovaných záruk v určitých transakciách, preto sa vás toto vyhlásenie nemusí týkať.

Tieto informácie môžu obsahovať technické nepresnosti alebo typografické chyby. Tu uvádzané informácie sa periodicky menia; tieto zmeny budú začleňované do nových vydaní publikácie. IBM môže kedykoľvek bez ohlásenia spraviť zmeny a/alebo vylepšenia v produkte(och) a/alebo programe(och) opísanom v tejto publikácii.

Všetky odkazy v týchto informáciách na webové lokality iné ako od IBM sú poskytnuté len pre pohodlie a v žiadnom prípade neslúžia ako potvrdenie obsahu týchto webových lokalít. Materiály na týchto webových lokalitách nie sú časťou produktov IBM a použitie týchto webových lokalít je na vaše vlastné riziko.

IBM môže použiť alebo distribuovať všetky vami poskytnuté informácie ľubovoľným spôsobom bez toho, aby voči vám vznikli akékoľvek záväzky.

Vlastníci licencií na tento program, ktorí chcú o ňom získať informácie za účelom povolenia: (i) výmeny informácií medzi nezávisle vytvorenými programami a inými programami (vrátane tohto) a (ii) vzájomného použitia vymieňaných informácií by mali kontaktovať:

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

Takéto informácie môžu byť dostupné, môžu byť predmetom príslušných pojmov a podmienok a v niektorých prípadoch sú dostupné za poplatok.

Licenčný program opísaný v týchto informáciách a všetky preň dostupné licenčné materiály, poskytuje IBM podľa podmienok zmluvy IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code, alebo inej ekvivalentnej zmluvy medzi nami.

Všetky údaje o výkone, uvádzané v tomto dokumente boli získané v riadenom prostredí. Výsledky získané v iných prevádzkových prostrediach sa môžu podstatne odlišovať. Niektoré merania boli vykonané v systémoch vývojovej úrovne a nie je žiadna záruka, že tieto merania budú rovnaké vo všeobecne dostupných systémoch. Okrem toho, niektoré výsledky boli odhadnuté extrapoláciou. Skutočné výsledky sa môžu odlišovať. Užívatelia tohto dokumentu by si mali overiť použiteľnosť týchto údajov pre svoje špecifické prostredie.

Informácie o produktoch iných ako od IBM boli získané od poskytovateľov týchto produktov, z ich uverejnených oznámení alebo z iných, verejne dostupných zdrojov. IBM netestovala tieto produkty a nemôže potvrdiť presnosť ich výkonu, kompatibilitu ani žiadne iné tvrdenie týkajúce sa produktov iných ako od IBM. Otázky k schopnostiam produktov iných ako od IBM by ste mali adresovať poskytovateľom týchto produktov.

Všetky vyhlásenia týkajúce sa budúceho smerovania alebo úmyslov IBM sú predmetom zmeny alebo zrušenia bez ohlásenia a vyjadrujú len zámery a ciele.

Všetky ceny IBM sú navrhované predajné ceny stanovené spoločnosťou IBM, sú aktuálne a sú predmetom zmeny bez ohlásenia. Ceny dílerov môžu byť odlišné.

Tieto informácie slúžia len na plánovacie účely. Tu uvedené informácie sú predmetom zmeny pred sprístupnením opisovaných produktov.

Tieto informácie obsahujú príklady údajov a hlásení používaných v každodenných firemných operáciách. Kvôli ich čo najlepšej ilustrácii obsahujú tieto príklady mená osôb, názvy spoločností, pobočiek a produktov. Všetky tieto mená a názvy sú vymyslené a akákoľvek podobnosť s menami, názvami a adresami používanými skutočnými osobami a spoločnosťami je čisto náhodná.

LICENCIA NA AUTORSKÉ PRÁVA:

Tieto informácie obsahujú vzorové aplikačné programy v zdrojovom kóde, ktoré ilustrujú programovacie techniky v rôznych platformách. Tieto vzorové programy môžete kopírovať, upravovať a distribuovať v ľubovoľnej forme bez platenia poplatku spoločnosti IBM, za účelom vývoja, použitia, marketingu alebo distribúcie aplikačných programov vyhovujúcich aplikačnému programovému rozhraniu pre prevádzkovú platformu, pre ktorú sú napísané tieto vzorové programy. Tieto príklady neboli dôkladne otestované pri všetkých podmienkach. IBM preto nemôže garantovať alebo predpokladať spoľahlivosť, použiteľnosť ani funkciu týchto programov.

S VÝNIMKOU ZÁRUK VYPLÝVAJÚCICH ZO ZÁKONA, KTORÉ NEMOŽNO ODOPRIEŤ, IBM, JEJ VÝVOJÁRI PROGRAMOV A DODÁVATELIA NEDÁVAJÚ ŽIADNE VYJADRENÉ ANI PREDPOKLADANÉ ZÁRUKY ALEBO PODMIENKY, VRÁTANE ALEBO BEZ OBMEDZENIA LEN NA PREDPOKLADANÉ ZÁRUKY ALEBO PODMIENKY PREDAJNOSTI, VHODNOSTI NA URČITÝ ÚČEL A DODRŽIAVANIA AUTORSKÝCH PRÁV TÝKAJÚCICH SA PROGRAMU ALEBO TECHNICKEJ PODPORY, AK JE NEJAKÁ.

V ŽIADNOM PRÍPADE NIE SÚ IBM, JEJ VÝVOJÁRI PROGRAMOV ALEBO DODÁVATELIA ZODPOVEDNÍ ZA NIČ Z NASLEDUJÚCEHO, AJ KEĎ BOLI O TEJTO MOŽNOSTI INFORMOVANÍ:

1. STRATA ALEBO POŠKODENIE DÁT;
2. ZVLÁŠTNE, NÁHODNÉ ALEBO NEPRIAME ŠKODY, ALEBO ZA ŽIADNE EKONOMICKÉ NÁSLEDNÉ ŠKODY; ALEBO
3. UŠLÝ ZISK, STRATU OBCHODU, ZISKU, DOBRÉHO MENA ALEBO OČAKÁVANÝCH ÚSPOR.

NIEKTORÉ PRÁVNE SYSTÉMY NEUMOŽŇUJÚ VYLÚČENIE ALEBO OBMEDZENIE NÁHODNÝCH ČI NÁSLEDNÝCH ŠKÔD, TAKŽE VYŠŠIE UVEDENÉ VYLÚČENIE ALEBO OBMEDZENIE SA NA VÁS NEMUSÍ VZŤAHOVAŤ.

Každá kópia alebo časť týchto vzorových programov alebo odvodená práca musí obsahovať túto poznámku o autorských právach:

© (názov vašej spoločnosti) (rok). Časti tohto kódu sú odvodené od vzorových programov IBM Corp. © Copyright IBM Corp. _uveďte rok alebo roky_. Všetky práva vyhradené.

Ak si prezeráte elektronickú kópiu týchto informácií, nemusia byť zobrazené fotografie ani farebné ilustrácie.

Ochranné známky

Nasledujúce pojmy sú ochranné známky spoločnosti International Business Machines v USA, v iných krajinách alebo v oboch:
IBM
iSeries
Operating System/400
OS/400

Ostatné názvy spoločnosti, produktov alebo služieb môžu byť ochranné známky alebo značky služieb iných.

Podmienky preberania a tlače publikácií

Oprávnenia na použitie vami vybratých publikácií na prevzatie sú poskytované len pri vašom akceptovaní nasledujúcich pojmov a podmienok.

Osobné použitie: Tieto Publikácie môžete reprodukovať pre svoje osobné, nekomerčné použitie za podmienky zachovania všetkých informácií o autorských právach. Bez výslovného povolenia od IBM nemôžete distribuovať, zobrazovať ani odvádzať práce z týchto Publikácií ani žiadnej ich časti.

Komerčné použitie: Tieto publikácie môžete reprodukovať, distribuovať a zobrazovať výlučne vo vašej spoločnosti za podmienky zachovania všetkých informácií o autorských právach. Bez výslovného povolenia od IBM nemôžete odvádzať práce z týchto Publikácií ani reprodukovať, distribuovať a zobrazovať tieto Publikácie ani žiadne ich časti.

S výnimkou ako je uvedené v týchto informáciách, na Publikácie alebo ľubovoľné informácie, údaje, softvér alebo iné tu obsiahnuté intelektuálne vlastníctvo nemáte žiadne oprávnenia, licencie ani práva, vyjadrené ani implikované.

IBM si vyhradzuje právo odobrať tu uvedené oprávnenia vždy, podľa vlastného uváženia, keď použitie týchto publikácií škodí spoločnosti IBM, alebo ak IBM prehlási, že pokyny hore nie sú striktne dodržiavané.

Tieto informácie nemôžete prevziať ani exportovať okrem prípadu, ak to dovoľujú všetky aplikovateľné zákony a regulácie, vrátane všetkých zákonov a regulácií USA pre export. IBM SA NEZARUČUJE ZA OBSAH TÝCHTO PUBLIKÁCIÍ. PUBLIKÁCIE SÚ POSKYTNUTÉ ″TAK AKO SÚ″ BEZ ZÁRUKY AKÉHOKOĽVEK DRUHU, VYJADRENEJ ALEBO IMPLIKOVANEJ, VRÁTANE (ALE NEOBMEDZENE) IMPLIKOVANÝCH ZÁRUK PREDAJNOSTI A VHODNOSTI NA KONKRÉTNY ÚČEL.

Všetok materiál je vlastníctvom IBM Corporation.

Prevzatím alebo vytlačením publikácie z tejto lokality vyjadrujete váš súhlas s týmito pojmami a podmienkami.

Vytlačené v USA