IBM Systems - iSeries

Spájanie počítačov prostredníctvom sietí Kvalita služby

Verzia 5, vydanie 4

IBM Systems - iSeries

Spájanie počítačov prostredníctvom sietí Kvalita služby

Verzia 5, vydanie 4

Poznámka

Skôr, ako tieto informácie a produkt, na ktorého podporu sú určené, použijete, prečítajte si informácie v časti “Právne informácie”, na strane 67.

Piate vydanie (február 2006)

Pokiaľ v novších vydaniach tejto publikácie nebude uvedené inak, toto vydanie sa vzťahuje na verziu 5, vydanie 4, modifikáciu 0 systému IBM i5/OS (produktové číslo 5722-SS1) a na všetky neskoršie vydania a modifikácie. Táto verzia sa nedá spustiť na počítačoch s redukovanou inštrukčnou sadou (RISC), ani na modeloch CISC.

Obsah

Kvalita služby

Riešenie kvality služby (QoS) systému iSeries umožňuje politikám požadovať pre aplikácie TCP/IP sieťovú prioritu a šírku pásma v celej sieti.

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.

Priorita paketov je pre vás významná, ak odosielate aplikácie, ktoré potrebujú predvídateľné a spoľahlivé výsledky, ako napríklad multimédiá. Politiky QoS na serveri iSeries môžu okrem iného limitovať údaje, ktoré opúšťajú váš server, riadiť požiadavky na pripojenie a spravovať zaťaženie servera. Aby bolo možné aktivovať politiku detekcie narušenia bezpečnosti systému, server QoS musí byť spustený.

Je dôležité pochopiť QoS pred tým, ako začnete konfigurovať politiky.

Čo je nové vo V5R4

Nová funkcia zistenia narušenia

Vo V5R4 server kvality služieb (QoS) poskytuje schopnosti zistenia narušenia prostredníctvom politiky zistenia narušenia. Na aktivovanie tejto novej politiky musí byť spustený server QoS. Ak budete používať politiku zistenia narušenia QoS, môžete zistiť narušenia, vytvoriť auditovacie záznamy a odosielať správy na indikovanie možného pokusu o narušenie. Viac informácií nájdete vo funkcii zistenia narušenia.

Ako sa dá zistiť čo je nové alebo zmenené

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.

Ak chcete nájsť ďalšie informácie o tom, čo je v tomto vydaní nové alebo zmenené pozrite si Poznámky pre užívateľov.

Vytlačiteľný formát PDF

Použite ho na zobrazenie a vytlačenie týchto informácií vo formáte PDF .

Na zobrazenie alebo načítanie verzie PDF tohto dokumentu vyberte Kvalitu služieb (okolo 525 KB).

Uloženie súborov PDF

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

1. Vo svojom prehliadači kliknite pravým tlačidlom na dokument PDF (kliknite pravým tlačidlom na odkaz hore).
2. Kliknite na voľbu, ktorá ukladá dokument PDF lokálne.
3. Navigujte k adresáru, do ktorého chcete uložiť dokument PDF.
4. Kliknite na **Uložiť**.

Stiahnutie programu Adobe Reader

Ak chcete zobraziť alebo tlačiť tieto dokumenty PDF, musíte mať vo svojom systéme nainštalovaný program Adobe Reader. Voľná kópia sa dá stiahnuť na webovej stránke spoločnosti Adobe

(www.adobe.com/products/acrobat/readstep.html) .

Základné pojmy

Ak ste prvýkrát v kontakte s kvalitou služieb (QoS), môžete si prečítať niekoľko základných pojmov QoS. Toto vám dá prehľad o tom, ako QoS pracuje a ako spolupracujú funkcie QoS.

Predtým ako sa pokúsite spraviť QoS, odporúča sa, aby ste preskúmali tému a uistili sa, že táto služba naplní vaše potreby. Výrazy QoS sa dajú nájsť v početných zdrojoch, takže v tejto téme sa bude písať len o základnej terminológii.

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

- Diferenčný servis
- Integrovaná služba
- Povolenie vstupu

Diferencovaná služba a *integrovaná služba* sa považujú za politiky výstupu 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. Obidva typy politík výstupu môžu vyžadovať dohodu o úrovni služieb (SLA) s vaším poskytovateľom internetových služieb (ISP).

Politiky *vstupu* riadia požiadavky o spojenie prichádzajúce do vašej siete z vonkajšieho zdroja. Politiky vstupu nie sú závislé na úrovni služieb od vášho ISP. Pri rozhodovaní, ktorú politiku budete používať, zhodnoťte dôvody, prečo chcete používať QoS a zvážte rolu vášho servera iSeries.

Jednou z najdôležitejších častí realizácie QoS je samotný server. Nielenže musíte rozumieť základným pojmom QoS, ale musíte si tiež uvedomovať rolu, ktorú hrá váš server v týchto základných pojmoch. Server iSeries sa môže správať ako klient alebo ako server, nie ako smerovač. Napríklad server iSeries, ktorý sa správa ako klient môže používať politiky diferencovaných služieb, aby zabezpečil, že požiadavky smerujúce do iných serverov dostanú v sieti vyššiu prioritu. Server iSeries, ktorý sa správa ako server môže používať politiku vstupu na obmedzenie požiadaviek identifikátora Uniform Resource Identifier (URI) akceptovaných serverom.

Súvisiace koncepty

“Dohoda úrovne služieb” na strane 48
Táto téma poukazuje na niektoré dôležité aspekty dohody úrovne služieb (SLA), ktoré by mohli ovplyvniť vašu implementáciu kvality služieb (QoS).

Súvisiaci odkaz

“Informácie týkajúce sa QoS” na strane 65
Sú tu uvedené publikácie IBM Redbooks (vo formáte PDF), webové stránky, a témy informačného centra, ktoré sa týkajú témy kvality služieb (QoS). Je možné prezerať alebo tlačiť všetky súbory vo formáte PDF.

Diferenčný servis

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.

Súvisiace koncepty

“Rozšírenia API QoS sendmsg()” na strane 22
Funkcia sendmsg() sa používa na odosielanie údajov, pomocných údajov, prípadne oboch, prostredníctvom pripojeného alebo nepripojeného soketu.

"Limity bloku tokenov a šírky pásma" na strane 9
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.

"Trieda služby" na strane 13
Pri vytváraní politiky diferencovaných služieb alebo politiky povolenia vstupu taktiež vytvárate a používate triedu služby.

"Scenár: Obmedzenie prevádzky prehliadača" na strane 27
Kvalitu služieb (QoS) môžete využiť pri riadení výkonu komunikačnej prevádzky. Použite politiku diferencovaných služieb buď na obmedzenie, alebo rozšírenie výkonu aplikácie v rámci vašej siete.

"Scenár: Bezpečné a predpovedateľné výsledky (VPN a QoS)" na strane 31
Aj vtedy, ak používate virtuálnu súkromnú sieť (VPN), môžete vytvárať politiky kvality služby (QoS). Tento príklad vám ukazuje spoločné použitie oboch.

Súvisiaci odkaz

"Na priradenie správaní per-hop používajte kódové body." na strane 14
Kvalita servisu (QoS) používa odporúčané kódové body na priradenie správaní per-hop do premávky.

"Konfigurácia QoS pomocou sprievodcov" na strane 50
Ak chcete konfigurovať politiky kvality služieb (QoS) musíte použiť sprievodcov QoS umiestnených v aplikácii iSeries Navigator.

Súvisiace informácie

Správa adries a portov vášho HTTP servera (s nainštalovaným webovým serverom Apache)

Prioritné triedy: Ako sa klasifikuje komunikácia po sieti

Diferencovaná služba identifikuje komunikačnú prevádzku vo forme *tried*. Najbežnejšie triedy sú definované prostredníctvom klientskych adries IP, aplikačných portov, typov serverov, protokolov, lokálnych adries IP a rozvrhov. Celá premávka zodpovedajúca rovnakej triede je spracovaná rovnako.

Pri rozšírenej klasifikácii môžete špecifikovať údaje servera a nastaviť tak pre niektoré z vašich aplikácií iSeries rôzne úrovne služby. Použitie údajov servera je nepovinné, avšak ak chcete klasifikovať na nižšej úrovni, môže byť užitočné. Údaje servera sa zakladajú na dvoch typoch aplikačných údajov: *symbole aplikácie* alebo identifikátore prostriedkov *Uniform Resource Identifier (URI)*. Ak komunikácia zodpovedajúca symbolu alebo identifikátoru URI, ktorý ste v politike špecifikovali, použije sa táto politika pri odchádzajúcich odozvách, čím sa vlastne vytvára odchádzajúca komunikácia bez ohľadu na to, aká priorita je v politike diferencovanej služby zadaná.

Využitie symbolu aplikácie v politikách diferencovanej služby

Používanie aplikačných údajov danej politike diktuje, aby reagovala na konkrétne parametre (symbol a prioritu), ktoré aplikácia prostredníctvom aplikačného programového rozhrania sendmsg() prenáša na server. Táto voľba je voliteľná. Ak nepotrebujete takúto úroveň granularity vo vašich politikách výstupu, v sprievodcovi vyberte **Všetky tokeny**. Ak chcete, môžete symbol a prioritu niektorej aplikácie priradiť ku konkrétnej množine symbolov a priorít v politike odchádzajúcich komunikácie. 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. Symbol, ktorý zadáte v politike kvality služby (QoS),sa porovná so symbolom, ktorý poskytne daná aplikácia pre odchádzajúcu komunikáciu. Aplikácia poskytuje hodnotu tokenu prostredníctvom sendmsg() API. Ak sú tokeny rovnaké, premávka aplikácie sa zahrnie do politiky diferencovaných služieb.

  Ak chcete v politike diferencovanej služby použiť symbol aplikácie, postupujte podľa týchto pokynov:

  1. V okne konfigurácie QoS kliknite pravým tlačidlom na **DiffServ** a vyberte **Nová politika**. Spustite sprievodcu.
  2. Na stránke Server Data Request zvoľte **Vybratý token aplikácie**.
  3. Ak chcete vytvoriť nový token, kliknite na **Nový**. Objaví sa okno New 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, skôr myFTPapp než typický identifikátor 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 zadávate symbol aplikácie ako typ aplikačného údaja, aplikácia, ktorá tieto informácie serveru poskytuje, musí byť kódovaná špecificky tak, aby používala aplikačné programové rozhranie sendmsg(). Toto realizuje aplikačný programátor. Dokumentácia aplikácie musí poskytnúť platné hodnoty (tokeny a priority), ktoré administrátor QoS použije v politike diferencovaných služieb. Politika diferencovanej služby potom na komunikáciu, ktorá zodpovedá symbolu zadanému v politike, použije svoju vlastnú prioritu a klasifikáciu. Ak aplikácia neobsahuje hodnoty, ktoré by zodpovedali hodnotám nastaveným v politike, musíte buď aplikáciu aktualizovať, alebo pre danú politiku diferencovanej služby použiť iné parametre aplikačných údajov.

Využitie identifikátora URI v politikách diferencovanej služby

Keď vytvárate politiku diferencovanej služby, sprievodca vám umožňuje zadať údaje o serveri, ako sa o tom pojednáva v časti “Využitie symbolu aplikácie v politikách diferencovanej služby”. Aj keď polia v sprievodcovi od vás požadujú symbol aplikácie, môžete do nich namiesto neho zadať relatívny identifikátor URI. Znovu, toto je voliteľné. Ak nepotrebujete takúto úroveň granularity vo vašich politikách výstupu, v sprievodcovi vyberte **Všetky tokeny**. Ak chcete, môžete v politike odchádzajúcej komunikácie označiť konkrétnu množinu identifikátorov 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 jednou lomkou (/). Nasledovné segmenty sú platnými príkladmi relatívnych identifikátorov URI:

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

Pred nastavením diferencovanej servisnej politiky, ktorá používa URL, musíte zabezpečiť, že aplikačný port, vyhradený pre URI, sa musí zhodovať s Načúvacou direktívou, aktivovanou pre FRCA (Fast Response Cache Accelerator) v konfigurácii webového servera Apache. Ak chcete zmeniť alebo vidieť port vášho HTTP servera, pozrite si časť Manage addresses and ports for your HTTP server (powered by Apache).

FRCA identifikuje URI pre každú odchádzajúcu odozvu 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.

Súvisiace koncepty

“Rozšírenia API QoS sendmsg()” na strane 22
Funkcia sendmsg() sa používa na odosielanie údajov, pomocných údajov, prípadne oboch, prostredníctvom pripojeného alebo nepripojeného soketu.

Priority nastavenia: Ako zaobchádzať s triedami

Keď je už komunikačná prevádzka klasifikovaná, diferencovaná služba tiež vyžaduje, aby skokové správanie zadefinovalo spôsob spracúvania komunikácie.

Server používa bajty v IP hlavičke na identifikáciu servisnej úrovne IP paketu. Smerovače a prepínače alokujú svoje prostriedky na základe informácií skokového správania v oktetovom poli typu služby v záhlaví IP. Typ oktetového poľa typu služby bol nanovo definovaný v dokumente Request for Comments (RFC) 1349 a v operačnom systéme OS/400 V5R1. Skokové správanie je správanie posielania ďalej, ktoré získava paket v sieťovom uzle. Reprezentuje ho hodnota, ktorú poznáme pod názvom *kódový bod*. Pakety sa môžu označovať buď na serveri alebo v iných častiach siete, napríklad v smerovači. 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. Aby sieťový uzol mohol presadzovať spracovávanie podľa skokového správania, musí byť tento sieťový uzol schopný

používať plánovanie frontu a riadenie priorít odchádzajúcej komunikácie. Pozrite si tému “Udržiavače prevádzky”, kde nájdete bližšie informácie o význame výrazu ″DiffServ-aware″.

Ak váš paket prechádza cez smerovač alebo prepínač, ktorý nie je typu DiffServ, paket v ňom stratí svoju úroveň služby. Paket sa síce spracováva, no jeho spracovávanie sa môže neočakávane zdržať. Na vašom serveri iSeries môžete využívať preddefinované kódové body skokového správania alebo si môžete zadefinovať svoj vlastný kódový bod. Neodporúča sa, aby ste si vytvárali vaše vlastné kódové body pre používanie mimo vašej privátnej sieti. Ak neviete, ktoré kódové body máte priradiť, pozrite sa do témy “Na priradenie správaní per-hop používajte kódové body.” na strane 14.

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 na obmedzenie výkonu skutočne využíva diferencovanú službu. 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. Výkonové limity sú dané veľkosťou pamäťového bloku symbolov, ohraničením špičkovej rýchlosti a limitom priemernej rýchlosti. Bližšie informácie o týchto limitoch nájdete v pomocných témach funkcie kvalita služby (QoS) programu iSeries Navigator.

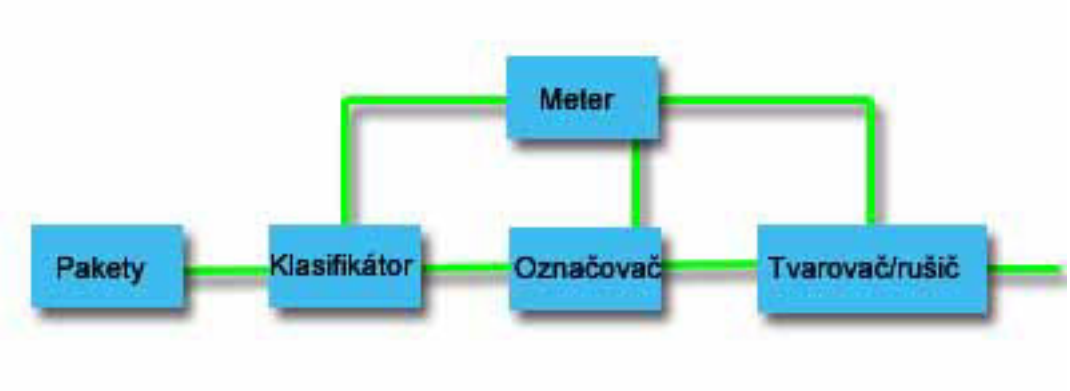
Udržiavače prevádzky

Ak si želáte využiť politiky kvality služby (QoS), vaše sieťové zariadenia (napríklad smerovače a prepínače) musia disponovať spôsobilosťou pre upravovače komunikačnej prevádzky. Upravovačmi komunikačnej prevádzky sú klasifikátory, merače, značkovače, tvarovače a prerušovače.

Ak má sieťové zariadenie všetky tieto upravovače komunikačnej prevádzky, potom sa považuje za *DiffServ-aware*, t.j. také, ktoré podporuje diferencovanú službu.

Poznámka: Tieto hardvérové požiadavky nie sú špecifické len pre servery iSeries. Tieto pojmy neuvidíte použité v rozhraní QoS, pretože server neumožňuje riadiť externý hardvér. Mimo súkromnej siete musí mať hardvér schopnosť spracúvať všeobecné požiadavky QoS. Pozrite sa do manuálov konkrétnych zariadení a uistite, že vaše zariadenia vyhovujú požiadavkám diferencovanej služby. 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 1. Udržiavače prevádzky

Nasledujúce informácie popisujú každý z udržiavačov premávky podrobnejšie.

Klasifikátory

Klasifikátory paketov vyberajú pakety v toku komunikačnej prevádzky podľa obsahu jeho IP záhlavia. Server iSeries definuje dva typy klasifikátorov. Súhrnné správanie (BA) klasifikuje pakety výlučne na základe

kódového bodu diferencovaných služieb. Viacpoľový (MF) klasifikátor vyberá pakety podľa hodnoty kombinácie jedného alebo viacerých polí záhlavia, napríklad podľa zdrojovej adresy, adresy určenia, poľa diferencovaných služieb, ID protokolu, zdrojového portu, identifikátora Uniform Resource Identifier (URI), typu servera a čísel 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.

Značkovače

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 obmedzenú veľkosť vyrovnávacej pamäte a smerovače môžu pakety vymazať, ak na uchovávanie oneskorených paketov nie je dosť miesta.

Prerušovače

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

Súvisiace koncepty

"Sieťový hardvér a softvér" na strane 49
Schopnosti vašich interných zariadení a ďalších zariadení mimo vašej siete majú mimoriadne veľký vplyv na výsledky kvality služby (QoS).

Integrovaná služba

Druhý typ politiky šírky pásma pre prístup smerom von, ktorý môžete vytvoriť, je politika integrovaných služieb. Integrovaná služba poskytuje IP aplikáciám schopnosť požadovať a vyhradiť si frekvenčné pásmo pomocou protokolu ReSerVation Protocol (RSVP) a aplikačných programových rozhraní kvality služby (QoS).

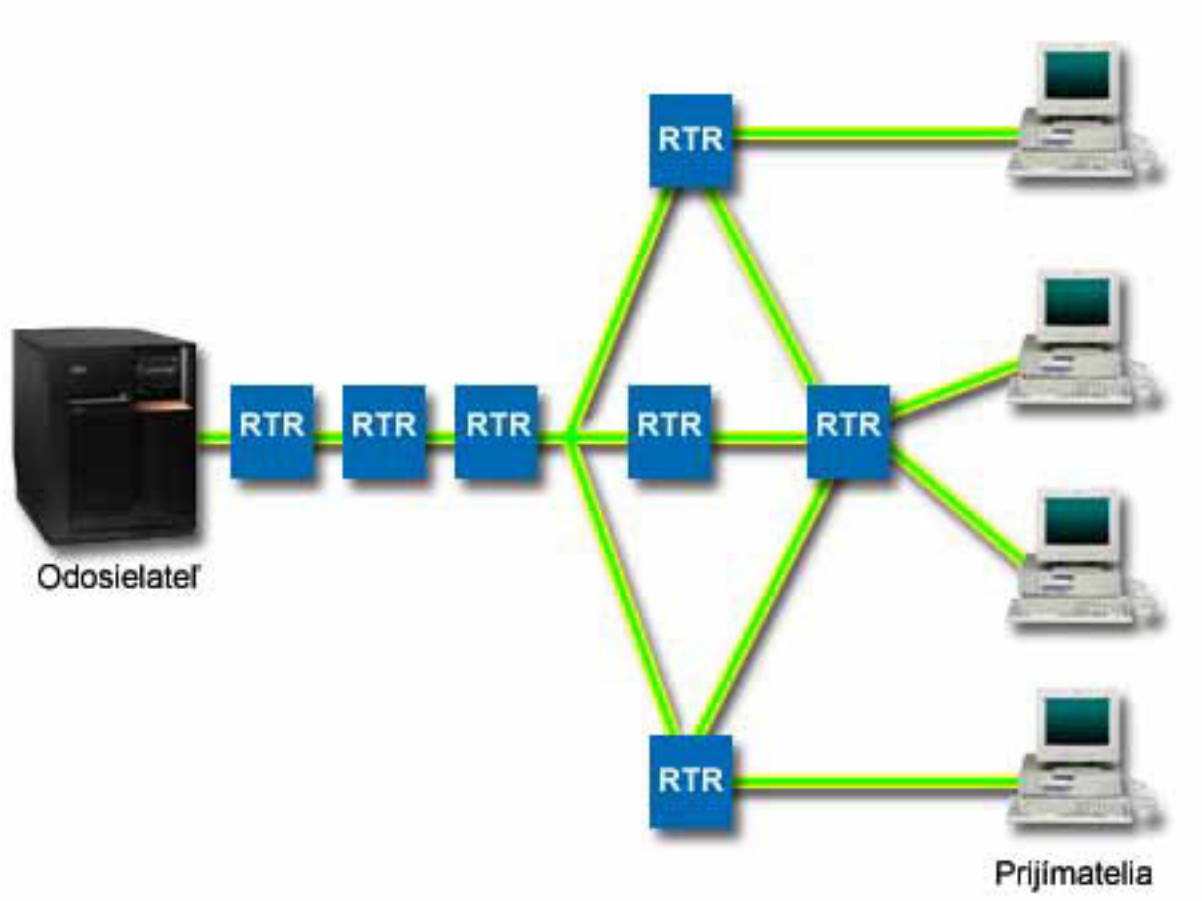
Politiky integrovanej služby využívajú protokol RSVP a aplikačné programové rozhranie Resource Reservation Setup Protocol (RAPI) (alebo API soketu qtoq) na zaručenie spojenia typu koniec-koniec. Toto je najvyššia úroveň služby, ktorú môžete určiť; je ale aj najkomplexnejšia.

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 trase súhlasia s požiadavkami prichádzajúcimi od klienta, požiadavka sa dostáva na server a do politiky IntServ. Ak požiadavka spadá do obmedzení definovaných politikou, QoS server udelí povolenie pre RSVP pripojenie a potom vyhradí šírku pásma pre aplikáciu. Rezervácia sa vykonáva pomocou protokolu RSVP a aplikačného programového rozhrania RAPI alebo pomocou protokolu RSVP a aplikačných programových rozhraní soketov QoS.

Každý uzol, cez ktorý prechádza vaša prevádzka, musí mať schopnosť používať protokol RSVP. Smerovače poskytujú QoS prostredníctvom nasledovných funkcií riadenia komunikačnej prevádzky: plánovač paketov, klasifikátor paketov a riadenie príjmu. 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. Prechodové

smerovače, ktoré nemajú povolený protokol RSVP, môžu spôsobiť nepredvídateľné prevádzkové problémy. Pripojenie je aj tak uskutočnené, ale výkon požadovaný aplikáciou nie je zaručený smerovačom. Nasledujúca schéma ukazuje, ako funkcia integrovanej služby logicky pracuje.



Obrázok 2. Trasa 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 dostupných prostriedkoch na serveri a smerovačoch na trase ako aj informácie o trase 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 problémy s výkonom a potrebovali by QoS. 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.

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.

Týmto hodnotám sa hovorí výkonové limity. Ak sú tieto pakety stále v medziach limitov servera, sú tieto pakety vyhovujúce a odošlú sa. V integrovaných službách má každé pripojenie vyhradené svoj vlastný blok symbolu.

Integrovaná služba, využívajúca diferencované označenia služieb

Ak si nie ste istý, či môže celá sieť garantovať pripojenie RSVP, môžete vytvoriť politiku integrovaných služieb. Ak však sieťové prostriedky nemôžu použiť protokol RSVP, spojenie nie je možné zaručiť. V takejto situácii budete možno chcieť v politike použiť 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.

Súvisiace koncepty

"Rozhrania API QoS" na strane 16
Túto tému si môžete prečítať, aby ste sa získali informácie o protokoloch, rozhraniach API a požiadavkách pre smerovač, ktorý je povolený pre protokol ReSerVation Protocol (RSVP). Aktuálne rozhrania kvality služieb (QoS) API zahŕňajú rozhrania API RAPI, rozhranie API qtoq soketu, rozhranie sendmsg() API a rozhrania monitor API.

"Integrovaná služba, využívajúca diferencované označenia služieb" na strane 10
Ak chcete zachovať prioritu paketov odoslaných v zmiešanom prostredí, použite v politike integrovanej služby označenia diferencovanej služby.

"Scenár: Predvídateľná prevádzka B2B" na strane 37
Ak potrebujete predpovedateľné doručenie a zároveň potrebujete vyžadovať rezerváciu, použijete taktiež politiku integrovaných služieb. Tento príklad ilustruje službu riadeného zaťaženia.

"Scenár: Dedikované doručenie (IP telefónia)" na strane 41
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.

Funkcia kontroly premávky

Funkcie riadenia premávky sa používajú len na integrovanú službu a nie sú charakteristické pre aplikáciu iSeries.

Tieto výrazy neuvidíte v rozhraní kvality služieb (QoS), pretože tento server nedokáže riadiť externý hardvér. Mimo súkromnej siete musí mať hardvér schopnosť spracúvať všeobecné požiadavky QoS. O požiadavkách na všeobecný smerovač pre politiky IntServ sa píše v nasledujúcej časti. Odporúča sa, aby ste preskúmali všeobecné základné pojmy QoS a nevyhnutné podmienky pred implementáciou politík.

Na získanie predvídateľných výsledkov potrebujete mať hardvér, ktorý je povolený protokolom ReSerVation Protocol (RSVP) na ceste premávky. Smerovače musia mať isté funkcie na riadenie premávky, aby mohli používať protokol RSVP. Často sa na ne odkazuje ako na *RSVP-povolené* alebo *QoS-povolené*. 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 zahŕňať nasledujúce funkcie:

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 triediča paketov. Kontrola vstupu sa na každom smerovači objavuje zároveň s cestou rezervovania.

Súvisiace koncepty

"Rozhrania API QoS" na strane 16
Túto tému si môžete prečítať, aby ste sa získali informácie o protokoloch, rozhraniach API a požiadavkách pre smerovač, ktorý je povolený pre protokol ReSerVation Protocol (RSVP). Aktuálne rozhrania kvality služieb (QoS) API zahŕňajú rozhrania API RAPI, rozhranie API qtoq soketu, rozhranie sendmsg() API a rozhrania monitor API.

Súvisiaci odkaz

"Informácie týkajúce sa QoS" na strane 65
Sú tu uvedené publikácie IBM Redbooks (vo formáte PDF), webové stránky, a témy informačného centra, ktoré sa týkajú témy kvality služieb (QoS). Je možné prezerať alebo tlačiť všetky súbory vo formáte PDF.

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 tolerovať malé množstvá strát a oneskorenia. 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. Ak tak chcete urobiť musia byť povolené kvalitou služieb (QoS) s podporou pre integrované služby. Budete musieť skontrolovať špecifikácie smerovačov, aby ste zistili, či poskytujú QoS prostredníctvom funkcie riadenia premávky. 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 na ceste paketu musí poskytnúť schopnosti protokolu ReSerVation Protocol (RSVP) na zaistenie doručenia. Keď priraďujete limity bloku tokenov a limity šírky pásma, definujete garantovanú službu. Garantovaná služba sa dá použiť len na aplikácie používajúce protokol TCP.

Súvisiace koncepty

"Scenár: Predvídateľná prevádzka B2B" na strane 37
Ak potrebujete predpovedateľné doručenie a zároveň potrebujete vyžadovať rezerváciu, použijete taktiež politiku integrovaných služieb. Tento príklad ilustruje službu riadeného zaťaženia.

"Scenár: Dedikované doručenie (IP telefónia)" na strane 41
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.

Limity bloku tokenov a šírky 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 vybrať neobmedzovať, čo povolí požiadavku o pripojenie na protokol ReSerVation Protocol (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 kvality služieb(QoS) sa pozerá na 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 môže byť v rozsahu od 10 Kbps do 1 Gbps. Môžete ju tiež nastaviť na neobmedzovať. Ak pre rýchlosť nastavíte Neobmedziť, vytvoríte hranicu pre dostupné prostriedky.

Tip: Ak chcete určiť, aké limity sa majú nastaviť, mohli by ste zapnúť 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. Scenár o monitorovaní aktuálnej štatistiky o sieťach ukazuje jeden spôsob, ako zhromaždiť všetky rýchlosti, ktoré vaša aplikácia a sieť momentálne používajú. 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.

Súvisiace koncepty

“Diferenčný servis” na strane 2
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.

“Scenár: Monitorovanie aktuálnych sieťových štatistík” na strane 45
Sprievodcovia vás vyzvú, aby ste nastavili výkonové limity. Nie je možné odporúčať nijaké konkrétne hodnoty, pretože tie sa zakladajú na individuálnych požiadavkách konkrétnych sietí.

Integrovaná služba, využívajúca diferencované označenia služieb

Ak chcete zachovať prioritu paketov odoslaných v zmiešanom prostredí, použite v politike integrovanej služby označenia diferencovanej služby.

Zmiešané prostredie nastane vtedy, keď sa rezervácia integrovanej služby presúva cez rôzne smerovače, ktoré nepodporujú rezervácie integrovanej služby, avšak samu integrovanú službu podporujú. Pretože vaša komunikácia prechádza cez rozličné domény, zmluvy o úrovni služieb a rôzne schopnosti zariadení, nemusíte vždy dostať presne tú službu, ktorú by ste chceli.

Aby ste zmiernili tento potenciálny problém, vašej politike integrovaných služieb môžete pripojiť značku diferencovanej služby. Aj v prípade, že politika prechádza cez smerovač, ktorý nemôže použiť protokol ReSerVation Protocol (RSVP), vaša politika si istú prioritu predsa len zachová. Označenie, ktoré pridávate, sa nazýva správanie pri skoku.

Funkcia signálu "no"

Okrem používania označení môžete využiť aj funkciu *no-signal*. Ak si zvolíte túto funkciu, ″no-signal″ verzie aplikačných programových rozhraní vám umožnia napísať aplikáciu, ktorá sa postará o zavedenie pravidla RSVP do servera a vyžaduje iba to, aby aplikácia TCP/IP komunikácie na strane servera podporovala RSVP. Na strane klienta sa signalizácia RSVP vykoná automaticky. Takto sa pre danú aplikáciu vytvorí spojenie prostredníctvom protokolu RSVP dokonca aj vtedy, ak na strane klienta nie je možné použiť protokol RSVP.

Funkcia no-signal sa špecifikuje v politike integrovanej služby. Ak chcete zadať funkciu ″no signal″, postupujte podľa nasledovných pokynov:

1. V prostredí iSeries Navigator, rozviňte → **Sieť → Politiky IP** pre váš server.
2. Pravým tlačidlom myši kliknite na **Kvalita služby** a zvoľte **Konfigurácia**.
3. Rozviňte **Výstupné politiky šírky pásma → IntServ**.
4. Pravým tlačidlom kliknite na požadovaný názov politiky IntServ a vyberte **Vlastnosti**. Otvorí sa okno vlastností IntServ.
5. Zvoľte kartu **Manažment prevádzky** a potom signalizáciu buď zakážte alebo povoľte. Takisto tam môžete upravovať rozvrh, klienta, aplikácie a manažment prevádzky.

Súvisiace koncepty

"Trieda služby" na strane 13
Pri vytváraní politiky diferencovaných služieb alebo politiky povolenia vstupu taktiež vytvárate a používate triedu služby.

"Integrovaná služba" na strane 6
Druhý typ politiky šírky pásma pre prístup smerom von, ktorý môžete vytvoriť, je politika integrovaných služieb. Integrovaná služba poskytuje IP aplikáciám schopnosť požadovať a vyhradiť si frekvenčné pásmo pomocou protokolu ReSerVation Protocol (RSVP) a aplikačných programových rozhraní kvality služby (QoS).

Politika povolenia vstupu

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

Politika pre prichádzajúcu komunikáciu sa používa na obmedzenie komunikácie, ktorá sa pokúša o pripojenie k vášmu serveru. Prístup môžete obmedzovať podľa klienta, jednotného identifikátora URI, aplikácie alebo podľa lokálneho rozhrania vášho servera iSeries. Okrem toho môžete výkon servera zvýšiť tak, že na prichádzajúcu komunikáciu budete aplikovať triedy služby. Túto politiku definujete prostredníctvom sprievodcu pre príjem prichádzajúcej komunikácie 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. Bližšie informácie nájdete v častiach " URI ", " Počet pripojení " na strane 12 a "Vážené prioritné fronty" na strane 12.

URI

Uvážte použitie politiky vstupu na obmedzenie premávky HTTP pripájajúcej sa k vášmu webovému serveru. V takejto situácii môžete vytvoriť politiku prijímania prichádzajúcej komunikácie, ktorá komunikačnú prevádzku obmedzuje len pre konkrétne identifikátory 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. Odborne sa to nazýva aj *riadením požiadaviek na pripojenie podľa záhlavia*, čo je metóda, ktorá na nastavovanie priorít využíva identifikátory URI.

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

Relatívny identifikátor 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 (/). Nasledovné segmenty sú platnými príkladmi relatívnych identifikátorov URI:

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

Poznámky:

1. 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.
2. Pri zadávaní URI sa používa implicitný zástupný znak. Napríklad zadaním /software zahrniete všetko vnútri adresára software.
3. V URI nepoužívajte znak *. Tento znak nie je platný.
4. Informácie o URI sa dajú použiť buď v politikách vstupu, alebo v (výstupnej) politike diferencovaných služieb.

Skôr, než nastavíte politiku pre prichádzajúcu komunikáciu, ktorá používa identifikátory URI, musíte sa postarať o to, aby aplikačný port priradený tomuto URI zodpovedal inštrukcii Listen povolenej v konfigurácii webového servera Apache pre Fast Response Cache Accelerator (FRCA). Ak chcete zmeniť alebo vidieť port vášho HTTP servera, pozrite si časť Manage addresses and ports for your HTTP server (powered by Apache).

Počet pripojení

Súčasťou politiky povolenia vstupu je aj to, že musíte vybrať triedu služby. Táto trieda služby definuje rýchlosti pripojenia, ktoré pôsobia ako riadenie príjmu a obmedzujú tak pripojenia, ktoré server prijíma.

Limity rýchlostí pripojenia prijmú alebo odmietnu nový paket podľa priemerného počtu pripojení za sekundu a maximálneho počtu okamžitých pripojení definovaných v politike, ktorú vytvárate. Tieto limity pripojení pozostávajú z priemerného počtu okamžitých pripojení a tzv. ″burst limitu″ (prahu zahltenia pripojenia), ktorých zadanie od vás sprievodcovia v programe iSeries navigator budú požadovať. 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. V programe iSeries Navigator môžete použiť tiež asociovanú pomoc, kde pri dokončovaní politiky nájdete podobné informácie.

Vážené 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. Ak je napríklad pre všetky priority zadaná hodnota 25, potom sa so všetkými frontmi zaobchádza rovnako. Predpokladajme, že zadáte nasledovné váhy: vysoká (50), stredná (30), nízka (15) a ″pri najlepšej vôli″ (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

Súvisiace koncepty

“Trieda služby” na strane 13
Pri vytváraní politiky diferencovaných služieb alebo politiky povolenia vstupu taktiež vytvárate a používate triedu služby.

“Priemerný počet okamžitých pripojení a tzv. ″burst limit″ (prah zahltenia pripojenia)” na strane 15
Priemerný počet okamžitých pripojení a tzv. ″burst limit″ (prah zahltenia pripojenia) sú dovedna známe pod spoločným názvom *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.

Trieda služby

Pri vytváraní politiky diferencovaných služieb alebo politiky povolenia vstupu taktiež vytvárate a používate triedu služby.

Politiky diferencovanej služby a politiky prijímania prichádzajúcej komunikácie používajú na zoskupovanie komunikácie do tried triedu služby. Napriek tomu, že veľa z tohto sa uskutočňuje prostredníctvom hardvéru, vy riadite spôsob, akým sa premávka zoskupuje a akú prioritu musí premávka prijať.

Keď vykonávate kvalitu služby (QoS), najskôr si zadefinujete politiky. Politiky určujú kto, čo, kde a kedy. Potom musíte priradiť triedu služby vašej politike. Triedy služby sú definované oddelene a politiky ich môžu používať opakovane. 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 od toho, či sa trieda služby používa pre politiku prichádzajúcej komunikácie, odchádzajúcej komunikácie alebo pre obidva typy politík. Keď vytvárate triedu služby, môžete sa stretnúť s nasledovnými požiadavkami:

Označovanie kódového bodu
QoS používa na priraďovanie skokových správaní komunikácii odporúčané kódové body. Smerovače a prepínače používajú tieto kódové body na priradenie úrovne priority premávke. Váš server nemôže tieto kódové body používať, pretože sa nespráva ako smerovač. Musíte stanoviť, ktoré kódové body sa majú použiť, a to na základe individuálnych potrieb vašej siete. 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 komunikačnej prevádzky
Na obmedzovanie komunikačnej prevádzky vo vašej sieti využíva QoS limity riadenia rýchlosti. Tieto limity sú dané nastavením veľkosti bloku tokenov, limitu špičkovej rýchlosti a limitu priemernej rýchlosti. Bližšie informácie o týchto špecifických hodnotách nájdete v časti “Limity bloku tokenov a šírky pásma” na strane 9.

Mimoprofilová komunikácia
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. Okno zahltenia TCP je však zmenšené, aby rýchlosť údajov zodpovedala rýchlosti pamäťového bloku symbolov. 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.

Súvisiace koncepty

“Integrovaná služba, využívajúca diferencované označenia služieb” na strane 10
Ak chcete zachovať prioritu paketov odoslaných v zmiešanom prostredí, použite v politike integrovanej služby označenia diferencovanej služby.

“Politika povolenia vstupu” na strane 11
Politika povolenia vstupu sa používa na riadenie požiadaviek o pripojenie prichádzajúcich do vašej siete.

“Diferenčný servis” na strane 2
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.

Súvisiaci odkaz

“Na priradenie správaní per-hop používajte kódové body.”
Kvalita servisu (QoS) používa odporúčané kódové body na priradenie správaní per-hop do premávky.

Na priradenie správaní per-hop používajte kódové body.

Kvalita servisu (QoS) používa odporúčané kódové body na priradenie správaní per-hop do premávky.

V sprievodcovi triedy služby musíte priradiť skokové správanie pre vašu politiku. Musíte určiť, ktoré kódové body sa majú používať na základe toho, aké individuálne potreby má vaša sieť. 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. Môžete vytvoriť testovacie politiky, môžete monitorovať tieto politiky a primerane spraviť potrebné úpravy.

Tabuľky v nasledujúcich častiach zobrazujú navrhované kódové body, ktoré vychádzajú z priemyselných štandardov. Väčšina poskytovateľov internetových služieb (ISP) podporuje kódové body vychádzajúce z priemyselných štandardov a vy si môžete overiť, či váš ISP tieto kódové body podporuje. Naprieč doménami musí každý ISP súhlasiť s podporou požiadaviek QoS. Vaše zmluvy o službách musia byť schopné dať vašim politikám, o čo požiadajú. Overte, či dostávate taký objem služieb, aký potrebujete. Ak to tak nie je, je možné, že plytváte svojimi prostriedkami. Politiky QoS vám umožňujú vyjednávať s vaším ISP o úrovniach služieb, čo môže znížiť náklady na sieťové služby. Môžete si tiež vytvoriť vlastné kódové body; neodporúčajú sa však na externé použitie. Vaše vlastné kódové body sa môžu najlepšie použiť v testovacom prostredí.

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.

Tabuľka 1. Odporúčané kódové body: Urýchlené postupovanie

Urýchlené postupovanie
101110

Poznámka: Zvyčajne sa s prijatím spracovania urýchleného postupovania viažu vysoké náklady, a preto sa toto správanie per-hop neodporúča používať pravidelne.

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.

Tabuľka 2. Odporúčané kódové body: Trieda selektora

Trieda selektora
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

Zaistené postupovanie je rozdelené do štyroch tried správania per-hop, každá z nich 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 znamená, že pakety v tejto politike majú najnižšiu šancu byť zrušené v tejto konkrétnej úrovni triedy.

Tabuľka 3. Odporúčané kódové body: Zaistené postupovanie

Zaistené postupovanie
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

Súvisiace koncepty

“Diferenčný servis” na strane 2
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.

“Trieda služby” na strane 13
Pri vytváraní politiky diferencovaných služieb alebo politiky povolenia vstupu taktiež vytvárate a používate triedu služby.

Priemerný počet okamžitých pripojení a tzv. ″burst limit″ (prah zahltenia pripojenia)

Priemerný počet okamžitých pripojení a tzv. ″burst limit″ (prah zahltenia pripojenia) sú dovedna známe pod spoločným názvom *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.

Nárazová rýchlosť pripojenia

Veľkosť maximálnej rýchlosti pripojenia určuje kapacitu pamäťového bloku, ktorá uchováva maximálne rýchlosti pripojení. Nárazy pripojení môžu vstupovať do servera rýchlejšie, než ich server dokáže spracovávať, prípadne rýchlejšie, než by ste vy sami chceli. Ak počet pripojení v náraze prekročí nastavenú úroveň nárazu pripojenia, potom sú dodatočné spojenia zrušené.

Priemerný počet okamžitých pripojení

Priemerný počet okamžitých pripojení udáva limit počtu nových nadviazaných pripojení alebo okamžitý počet prichádzajúcich požiadaviek identifikátorov URI, ktoré môže server prijať. Ak by požiadavka zapríčinila presiahnutie vami nastavených limitov, server požiadavku zamietne. Obmedzenie požiadavky priemerného pripojenia sa meria v pripojeniach za sekundu.

Tip: Ak chcete zistiť, aké limity máte nastaviť, môžete spustiť monitor. Scenár monitorovania aktuálnych štatistických údajov siete obsahuje ukážku politiky, ktorá vám môže pomôcť zhromaždiť väčšinu údajov, ktoré prechádzajú cez váš server. Použitím týchto výsledkov môžete limity okamžite nastaviť.

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

Súvisiace koncepty

“Politika povolenia vstupu” na strane 11
Politika povolenia vstupu sa používa na riadenie požiadaviek o pripojenie prichádzajúcich do vašej siete.

“Scenár: Monitorovanie aktuálnych sieťových štatistík” na strane 45
Sprievodcovia vás vyzvú, aby ste nastavili výkonové limity. Nie je možné odporúčať nijaké konkrétne hodnoty, pretože tie sa zakladajú na individuálnych požiadavkách konkrétnych sietí.

Rozhrania API QoS

Túto tému si môžete prečítať, aby ste sa získali informácie o protokoloch, rozhraniach API a požiadavkách pre smerovač, ktorý je povolený pre protokol ReSerVation Protocol (RSVP). Aktuálne rozhrania kvality služieb (QoS) API zahŕňajú rozhrania API RAPI, rozhranie API qtoq soketu, rozhranie sendmsg() API a rozhrania monitor API.

Väčšina politík QoS vyžaduje používanie rozhrania API. Tieto rozhrania API sa môžu použiť v spojitosti buď s politikou diferencovaných služieb alebo politikou integrovaných služieb. Existuje tiež istý počet rozhraní API, ktoré sa dajú použiť s Monitorom QoS.

- “Rozhrania API integrovaných služieb”
- “Rozhrania API diferencovaných služieb” na strane 17
- “Rozhrania API monitora” na strane 18

Rozhrania API integrovaných služieb

Protokol RSVP spolu s rozhraniami API RAPI alebo rozhraniami API qtoq QoS soketov vykoná vašu rezerváciu integrovaných služieb. Každý uzol, cez ktorý prechádza vaša premávka musí mať schopnosť používať protokol RSVP. Na schopnosť vykonať politiky integrovaných služieb sa často odkazuje ako na *RSVP-umožnené*. Funkcie riadenia premávky sa môžu použiť na určenie toho, ktoré funkcie smerovača sú potrebné na použitie protokolu RSVP.

Protokol RSVP sa používa na vytvorenie rezervácie RSVP vo všetkých sieťových uzloch na ceste vašej premávky. 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. Keďže server iSeries momentálne nemá žiadne aplikácie RSVP-povolené budete musieť zapísať aplikácie používajúce rozhrania API RAPI alebo rozhrania API qtoq QoS soketov. 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 soketu

Môžete použiť rozhrania API qtoq QoS soketov na zjednodušenie práce vyžadovanej na použitie protokolu RSVP v systéme iSeries. Rozhrania API qtoq soketov volajú rozhrania API RAPI a vykonávajú niektoré zo zložitejších úloh. Rozhrania API qtoq soketov nie sú také flexibilné ako rozhrania API RAPI, ale poskytujú rovnaké funkcie pri menšej námahe. Verzie bez signalizácie rozhraní API vám dovoľujú zapísať tieto aplikácie:

- Aplikáciu, ktorá zavedie pravidlo protokolu RSVP do servera.
- Aplikáciu, ktorá vyžaduje len aplikáciu strany servera (konverzácie protokolu TCP/IP), aby bola RSVP-povolená.

Signalizácia protokolu RSVP sa deje automaticky pre stranu klienta.

Typický tok rozhrania API QoS pre aplikáciu/protokol používajúci sokety QoS qtoq orientované na spojenie alebo bez spojenia nájdete na stránke funkčného toku rozhrania API QoS orientovaného na spojenie alebo na stránke funkčného toku rozhrania API QoS bez spojenia.

Rozhrania API diferencovaných služieb

Poznámka: Rozhranie API sendmsg() sa používa na isté politiky diferencovaných služieb, ktoré definujú špecifický token aplikácie. Keď vytvoríte politiku diferencovaných služieb, môžete (voliteľne) poskytnúť charakteristiky aplikácie (token a priorita). Toto je rozšírená definícia politiky, a v prípade, že sa nepoužije, toto rozhranie API sa môže ignorovať. Nezabudnite však, že smerovače a iné servery v sieti stále musia vedieť o diferencovanej službe.

Ak sa rozhodnete používať token aplikácie v politike diferencovaných služieb, aplikácia poskytujúca tieto informácie musí byť špecificky kódovaná na použitie rozhrania API 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 sa zhodujú s hodnotami nastavenými v politike, musí sa zmeniť buď aplikácia, alebo musíte použiť odlišné parametre údajov o aplikácii pre politiku diferencovaných služieb.

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

Čo je token aplikácie?

Token aplikácie je identifikátor Uniform Resource Identifier (URI), ktorý reprezentuje definovaný zdroj. 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.

Viac informácií o type politiky DiffServ nájdete v časti “Diferenčný servis” na strane 2.

Rozhrania API monitora

Rozhrania API protokolu Resource Reservation Setup Protocol zahŕňajú rozhrania API monitora. Rozhrania API, ktoré sa používajú na monitor budú mať v názve slovo *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.

Súvisiace koncepty

“Integrovaná služba” na strane 6
Druhý typ politiky šírky pásma pre prístup smerom von, ktorý môžete vytvoriť, je politika integrovaných služieb. Integrovaná služba poskytuje IP aplikáciám schopnosť požadovať a vyhradiť si frekvenčné pásmo pomocou protokolu ReSerVation Protocol (RSVP) a aplikačných programových rozhraní kvality služby (QoS).

“Funkcia kontroly premávky” na strane 8
Funkcie riadenia premávky sa používajú len na integrovanú službu a nie sú charakteristické pre aplikáciu iSeries.

“Scenár: Predvídateľná prevádzka B2B” na strane 37
Ak potrebujete predpovedateľné doručenie a zároveň potrebujete vyžadovať rezerváciu, použijete taktiež politiku integrovaných služieb. Tento príklad ilustruje službu riadeného zaťaženia.

“Sieťový hardvér a softvér” na strane 49
Schopnosti vašich interných zariadení a ďalších zariadení mimo vašej siete majú mimoriadne veľký vplyv na výsledky kvality služby (QoS).

Súvisiaci odkaz

Aplikačné programové rozhranie (API) RAPI

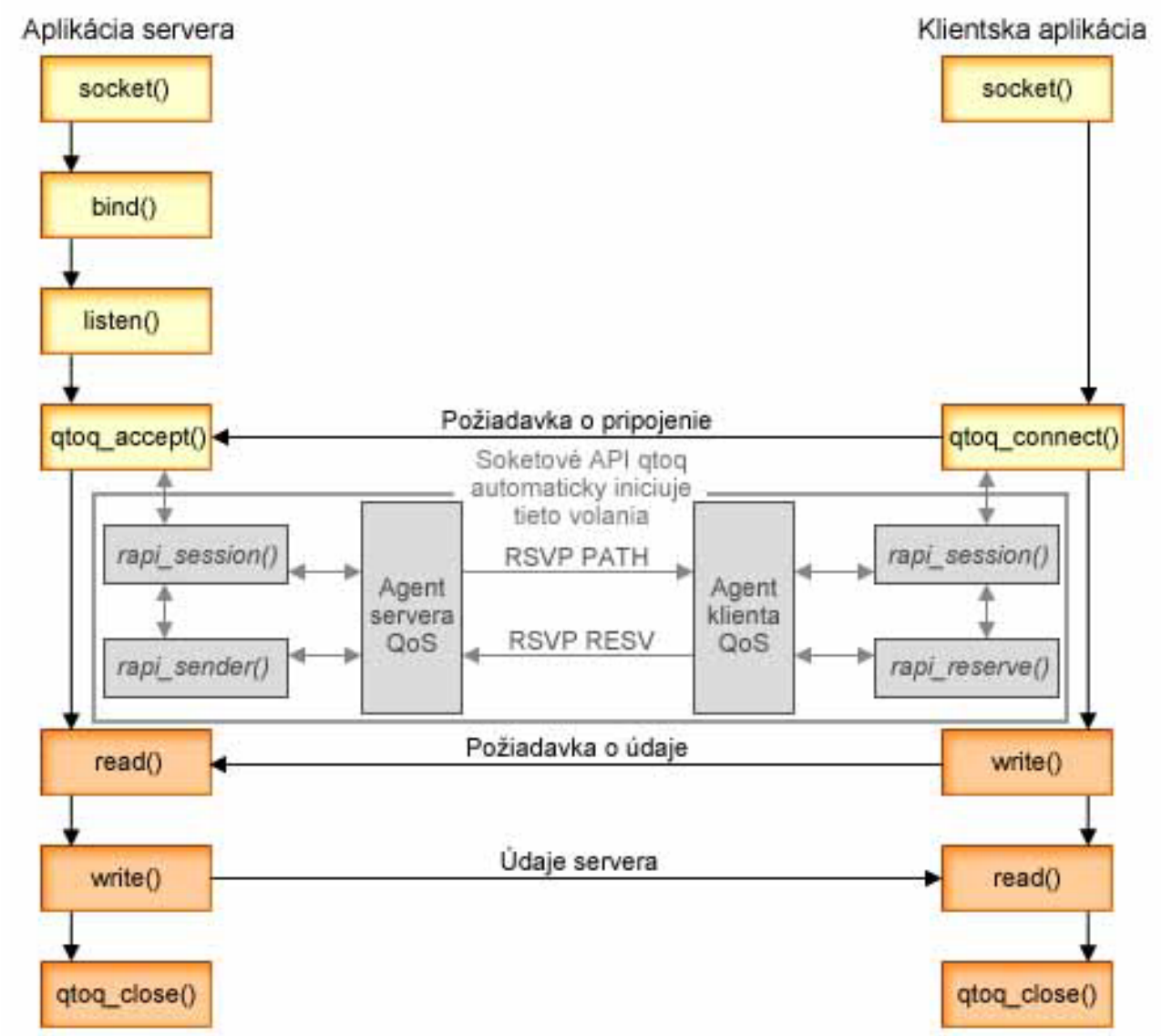
“Konfigurácia QoS pomocou sprievodcov” na strane 50
Ak chcete konfigurovať politiky kvality služieb (QoS) musíte použiť sprievodcov QoS umiestnených v aplikácii iSeries Navigator.

Funkčný tok rozhrania API QoS orientovaný na spojenie

Príklady servera a klienta v tejto téme ilustrujú rozhrania API qtoq kvality služieb (QoS) soketu zapísané pre funkčný tok orientovaný na spojenie.

Nasledujúca číslica ilustruje vzťah klienta/servera funkcií soketu qtoq povolené pre rozhrania API QoS pre protokol orientovaný na spojenie, ako je napríklad protokol Transmission Control Protocol (TCP).

Keď sú volané funkcie rozhrania API povolené QoS do toku orientovaného na spojenie vyžadujúceho, aby bol spustený protokol ReSerVation Protocol (RSVP), doplnkové funkcie sú spustené. Tieto funkcie spôsobujú, že agenti QoS na klientovi a serveri nastavia protokol RSVP pre tok údajov medzi klientom a serverom.



tok udalostí qtoq: Táto postupnosť soketových volaní poskytuje popis číslice. Taktiež popisuje vzťah medzi serverom a klientskou aplikáciou v dizajne, orientovanom na pripojenie. Toto sú modifikácie základných soketových rozhraní API.

Serverová strana

Rozhranie qtoq_accept() API pre pravidlo neoznačené signalizáciou

1. Aplikácia volá funkciu socket() na získanie deskriptora soketu.
2. Aplikácia volá listen() na zadanie, na aké pripojenie bude čakať.
3. Aplikácia volá qtoq_accept() na počkanie na požiadavku o pripojenie od klienta.
4. API volá rozhranie API rapi_session() a v prípade úspechu je priradené ID relácie QoS.
5. API volá štandardnú funkciu accept() na počkanie na klientsku požiadavku o pripojenie.
6. Keď je prijatá požiadavka o pripojenie, v požadovanom pravidle sa vykoná riadenie prístupu. Pravidlo je poslané do zásobníka protokolu TCP/IP a ak je platné, pravidlo sa vráti do volajúcej aplikácie s výsledkami a ID relácie.
7. Aplikácie pre server a pre klienta vykonávajú požadovaný prenos údajov.
8. Aplikácia volá funkciu qtoq_close() na zatvorenie soketu a uvoľnenie pravidla.
9. Server QoS vymaže pravidlo zo správcu QoS, vymaže reláciu QoS a vykoná všetky ďalšie potrebné akcie.

rozhranie qtoq_accept() API 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 volá funkciu qtoq_accept() na počkanie na požiadavku o pripojenie od klienta.
4. Keď príde požiadavka o pripojenie, rozhranie rapi_session() API je zavolané na vytvorenie relácie so serverom QoS pre toto spojenie a na získanie ID relácie QoS, ktorá je vrátená volajúcemu počítaču.
5. Rozhranie rapi_sender() API je zavolané na spustenie správy PATH zo servera QoS a na informovanie servera QoS, že musí očakávať správu RESV od klienta.
6. Rozhranie rapi_getfd() API je zavolané na získanie deskriptora, ktorý používajú aplikácie, keď čakajú na správy o udalostiach QoS.
7. Deskriptor akceptácie a deskriptor QoS sú vrátené do aplikácie.
8. Server QoS čaká na prijatie novej správy RESV. Keď je správa prijatá, server zavedie primerané pravidlo so správcom QoS a odošle správu aplikácii, ak aplikácia požiadala o oznámenie o volaní do rozhrania qtoq_accept() API.
9. Server QoS pokračuje v poskytovaní obnovení pre vytvorenú reláciu.
10. Aplikácia volá funkciu qtoq_close(), keď je pripojenie dokončené.
11. Server QoS vymaže pravidlo zo správcu QoS, vymaže reláciu QoS a vykoná všetky ďalšie potrebné akcie.

Klientska strana

Rozhranie qtoq_connect() API s normálnou signalizáciou RSVP

1. Aplikácia volá funkciu socket() na získanie deskriptora soketu.
2. Aplikácia volá funkciu qtoq_connect() na informovanie serverovej aplikácie, že chce naviazať spojenie.
3. Funkcia qtoq_connect() volá rozhranie rapi_session() API na vytvorenie relácie so serverom QoS pre toto pripojenie.
4. Server QoS je informovaný, aby čakal na príkaz PATH z požadovaného pripojenia.
5. Rozhranie rapi_getfd() API je zavolané na získanie deskriptora QoS, ktorý používajú aplikácie na počkanie 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 prijatá správa, odpovedá odoslaním správy RESV do servera QoS v počítači servera aplikácie.
8. Ak aplikácia požiadala o oznámenie, server QoS odošle oznámenie aplikácii prostredníctvom deskriptora QoS.
9. Server QoS pokračuje v poskytovaní obnovení pre vytvorenú reláciu.
10. Aplikácia volá funkciu qtoq_close(), keď je dokončené pripojenie.
11. Server QoS zatvorí reláciu QoS a vykoná všetky ďalšie potrebné akcie.

Rozhranie qtoq_connect() API pre pravidlo neoznačené signalizáciou

Táto požiadavka nie je platná pre klientsku stranu, pretože v tomto prípade nie je vyžadovaná odpoveď od klienta.

Súvisiaci odkaz

qtoq_accept() API

qtoq_close() API

rapi_session() API

rapi_sender() API

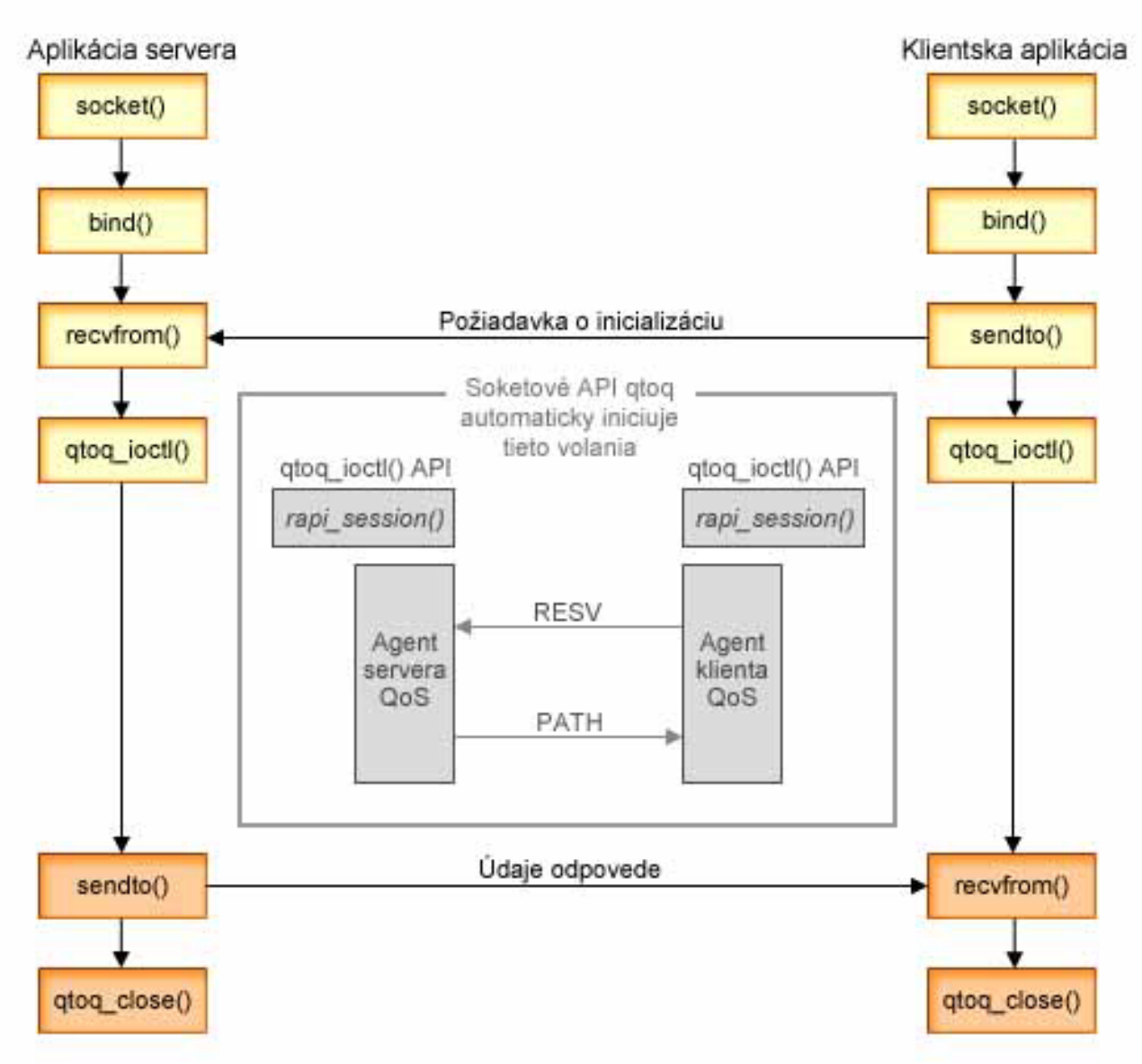
rapi_getfd() API

qtoq_connect() API

Funkčný tok rozhrania API QoS bez pripojenia

Príklady servera a klienta v tejto téme ilustrujú rozhrania API qtoq kvality služieb (QoS) soketu zapísané pre tok bez pripojenia.

Keď sú funkcie rozhrania API povolené QoS volané do toku bez pripojenia a vyžadujú, aby bol protokol ReSerVation Protocol (RSVP) spustený, doplnkové funkcie sú spustené. Tieto funkcie spôsobujú, že agenti QoS na klientovi a serveri nastavia protokol RSVP pre tok údajov medzi klientom a serverom.



tok udalostí qtoq: Táto postupnosť soketových volaní poskytuje popis číslic. Taktiež popisuje vzťah medzi serverom a klientskou aplikáciou v dizajne bez pripojenia. Toto sú modifikácie základných soketových API.

Serverová strana

qtoq_ioctl() Rozhranie API pre pravidlo neoznačené signalizáciou

1. Rozhranie qtoq_ioctl() API odošle správu do servera QoS, v ktorom ho žiada vykonať riadenie prístupu v požadovanom pravidle.
2. Ak je pravidlo akceptovateľné, volá funkciu, ktorá odosiela správu na server QoS a žiada ho o zavedenie pravidla.

3. Server QoS potom vráti stav volajúcemu počítaču indikujúci úspech alebo zlyhanie požiadavky.
4. Keď aplikácia prestala používať pripojenie, zavolá funkciu qtoq_close() na zatvorenie pripojenia.
5. Server QoS vymaže pravidlo zo Správcu QoS, vymaže reláciu QoS a vykoná všetky ďalšie potrebné akcie.

Rozhranie qtoq_ioctl() API s normálnou signalizáciou RSVP

1. Rozhranie qtoq_ioctl() API odošle správu do servera QoS, v ktorom ho žiada o riadenie prístupu pre žiadané spojenie.
2. Server QoS zavolá funkciu rapi_session() na požiadanie o naviazanie relácie pre pravidlo a aby sa ID relácie QoS vrátilo do volajúceho počítača.
3. Zavolá funkciu rapi_sender() na spustenie správy PATH späť ku klientovi.
4. Potom zavolá funkciu rapi_getfd() na získanie súborového deskriptora, aby počkal na udalosti QoS.
5. Server QoS vráti vybraný deskriptor(), ID relácie QoS a stav do volajúceho počítača.
6. Server QoS načítava pravidlo, keď je prijatá správa RESV.
7. Aplikácia zadá qtoq_close(), keď je spojenie naviazané.
8. Server QoS vymaže pravidlo zo Správcu QoS, vymaže reláciu QoS a vykoná všetky ďalšie potrebné akcie.

Klientska strana

qtoq_ioctl() API s normálnou signalizáciou RSVP

1. Rozhranie qtoq_ioctl() API zavolá funkciu rapi_session(), aby požiadalo o naviazanie relácie pre spojenie. 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. Zavolá funkciu rapi_getfd() na získanie súborového deskriptora, aby počkala na udalosti QoS.
3. Funkcia qtoq_ioctl() sa vráti do volajúceho počítača s počkaním na deskriptor a ID relácie.
4. Server QoS čaká na prijatie správy PATH. Keď je prijatá správa o ceste, odpovedá správou RESV a potom signalizuje aplikácii, že udalosť nastala prostredníctvom deskriptora relácie.
5. Server QoS pokračuje v poskytovaní obnovení pre vytvorenú reláciu.
6. Kód klienta zavolá funkciu qtoq_close(), keď je spojenie dokončené.

Rozhranie qtoq_ioctl() API pre pravidlo označené žiadna signalizácia

Táto žiadosť nie je platná pre klientsku stranu, pretože v tomto prípade nie je vyžadovaná odpoveď od klienta.

Súvisiaci odkaz

qtoq_close() API

rapi_session() API

rapi_sender() API

rapi_getfd() API

qtoq_ioctl() API

Rozšírenia API QoS sendmsg()

Funkcia sendmsg() sa používa na odosielanie údajov, pomocných údajov, prípadne oboch, prostredníctvom pripojeného alebo nepripojeného soketu.

Aplikačné programové rozhranie sendmsg() berie klasifikačné údaje kvality služby (QoS) do úvahy. 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.

Nasledovné informácie použite pri inicializácii štruktúry IP_QOS_CLASSIFICATION_DATA:

- ip_qos_version: Označuje verziu štruktúry. Túto položku je treba vyplniť pomocou konštanty *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 úrovní spojenia indikuje, že úroveň služby QoS získaná prostredníctvom klasifikácie tejto správy zostane v platnosti aj pre všetky ďalšie správy, ktoré budú odoslané až do najbližšej sendmsg() s klasifikačnými údajmi QoS. Rozsah úrovne správy označuje, že sa použije len priradená úroveň služby QoS pre údaje správy zahrnuté v tomto volaní funkcie sendmsg(). Budúce údaje, ktoré sa odošlú bez klasifikačných údajov QoS, zdedia predchádzajúce určenie úrovne spojenia QoS (z poslednej klasifikácie úrovne spojenia prostredníctvom sendmsg() alebo z pôvodnej klasifikácie spojenia TCP počas nadväzovania spojenia).
- 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 zvolí posledná z týchto možností, teda aj symbol aj priorita, typy klasifikácií musia byť logicky oddelené operátorom OR. Dajú sa špecifikovať nasledujúce typy:
  - Klasifikácia tokenu definovaného aplikáciou. Musí byť zadaný iba jediný typ; ak je zadaných viac typov (dva a viac), výsledok nemožno predvídať.
    - IP_SET_QOSLEVEL_W_APPL_TOKEN_ASCII : Toto označuje, že údaje klasifikácie sú znakový reťazec vo formáte ASCII. Ak je zadaná táto možnosť, symbol aplikácie je treba presunúť do poľa ip_qos_appl_token.

      Poznámka: Ak aplikácia musí pre klasifikačné údaje posielať numerické hodnoty, musí ich najskôr skonvertovať do formátu ASCII vhodného na tlač. Nezabudnite, že špecifikovaný reťazec môže obsahovaťmalé 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: IP_SET_QOSLEVEL_W_APPL_TOKEN_ASCII funguje o poznanie lepšie ako táto možnosť, pretože aplikačné údaje zadané v politike sa ukladajú vo formáte ASCII vo vnútri zásobníka TCP/IP, čím sa eliminuje potreba prekladať symbol definovaný aplikáciou pri každej požiadavke sendmsg().
  - Klasifikácia priority definovanej aplikáciou. Musí byť zadaný iba jediný typ; ak je zadaných viac typov priority, výsledky nemožno predvídať.
    - 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. Aj je zadaná väčšia dĺžka, použije sa iba 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.

Súvisiace koncepty

“Diferenčný servis” na strane 2
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.

“Prioritné triedy: Ako sa klasifikuje komunikácia po sieti” na strane 3
Diferencovaná služba identifikuje komunikačnú prevádzku vo forme *tried*. Najbežnejšie triedy sú definované prostredníctvom klientskych adries IP, aplikačných portov, typov serverov, protokolov, lokálnych adries IP a rozvrhov. Celá premávka zodpovedajúca rovnakej triede je spracovaná rovnako.

Súvisiaci odkaz

Aplikačné programové rozhranie (API) Sendmsg() - Odoslanie správy cez soket

Adresárový server

Svoje politiky môžete vyexportovať na adresárový server. V tejto téme sa dočítate o výhodách používania alebo nepoužívania adresárového servera, o základných pojmoch a konfigurácii protokolu Lightweight Directory Access Protocol (LDAP), ako aj o schéme kvality služieb (QoS).

Konfiguráciu politiky QoS je možné na adresárový server exportovať pomocou verzie 3 protokolu LDAP.

Výhody používania adresárového servera

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

- Konfiguračné údaje sa môžu ukladať na jeden lokálny adresárový server tak, aby ich mohlo zdieľať mnoho systémov.
- Konfiguračné údaje sa môže konfigurovať, ukladať a môže ich používať iba jeden systém (nezdieľajú sa).
- Konfiguračné údaje sa môžu nachádzať na adresárovom serveri, na ktorom sa nachádzajú aj údaje iných systémov, avšak medzi týmito systémami sa údaje nezdieľajú. Toto vám umožňuje použiť jediné umiestnenie na zálohovanie a uloženie údajov pre niekoľko systémov.

Výhody ukladania výhradne na váš lokálny server

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.
- Zvyšuje sa výkonnosť, pretože zapisovanie do LDAP nie je najrýchlejšou metódou.
- Jednoduchšie je kopírovať konfiguráciu medzi rôznymi servermi iSeries. Môžete kopírovať súbor z jedného systému do druhého. Pretože tu neexistuje nijaký primárny a sekundárny počítač, môžete každú politiku prispôsobiť priamo jednotlivým serverom.

Prostriedky protokolu LDAP

Ak sa rozhodnete exportovať vaše politiky do servera LDAP, najskôr sa musíte oboznámiť s konceptmi LDAP a so štruktúrami adresárov. Adresárový server, ktorý používa vaša politika QoS, môžete konfigurovať v rámci funkcie QoS v programe iSeries Navigator .

Súvisiace koncepty

Adresárový server IBM pre iSeries (LDAP)

“Konfigurácia adresárového servera” na strane 51
Konfigurácie politík QoS sa dajú exportovať do adresárového servera LDAP.

Kľúčové slová

Keď konfigurujete svoj adresárový server, musíte sa rozhodnúť, či sa majú s každou konfiguráciou kvality služieb (QoS) asociovať kľúčové slová.

Polia kľúčových slov sú nepovinné a možno ich ignorovať. Nasledovné informácie vám pomôžu porozumieť koncepcii kľúčových slov a vysvetlia vám dôvod, pre ktorý ich možno budete chcieť použiť.

Adresárový server si môžete nakonfigurovať pomocou sprievodcu QoS Initial Configuration. Môžete upresniť aj to, či má byť server, ktorý konfigurujete, primárnym alebo sekundárnym systémom. 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. Nasledovné opisy vysvetľujú spôsoby používania kľúčových slov v každom systéme.

Kľúčové slová a primárne systémy
: Kľúčové slová sú priradené QoS konfiguráciám vytvoreným a udržiavaným primárnym systémom. Používajú sa na to, aby sekundárne systémy mohli identifikovať konfiguráciu, ktorú vytvoril primárny systém.

Kľúčové slová a sekundárne systémy
: 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 v programe iSeries Navigator začínate konfigurovať adresárový server, použite pomoc k úlohám QoS, kde nájdete presné pokyny.

Súvisiace koncepty

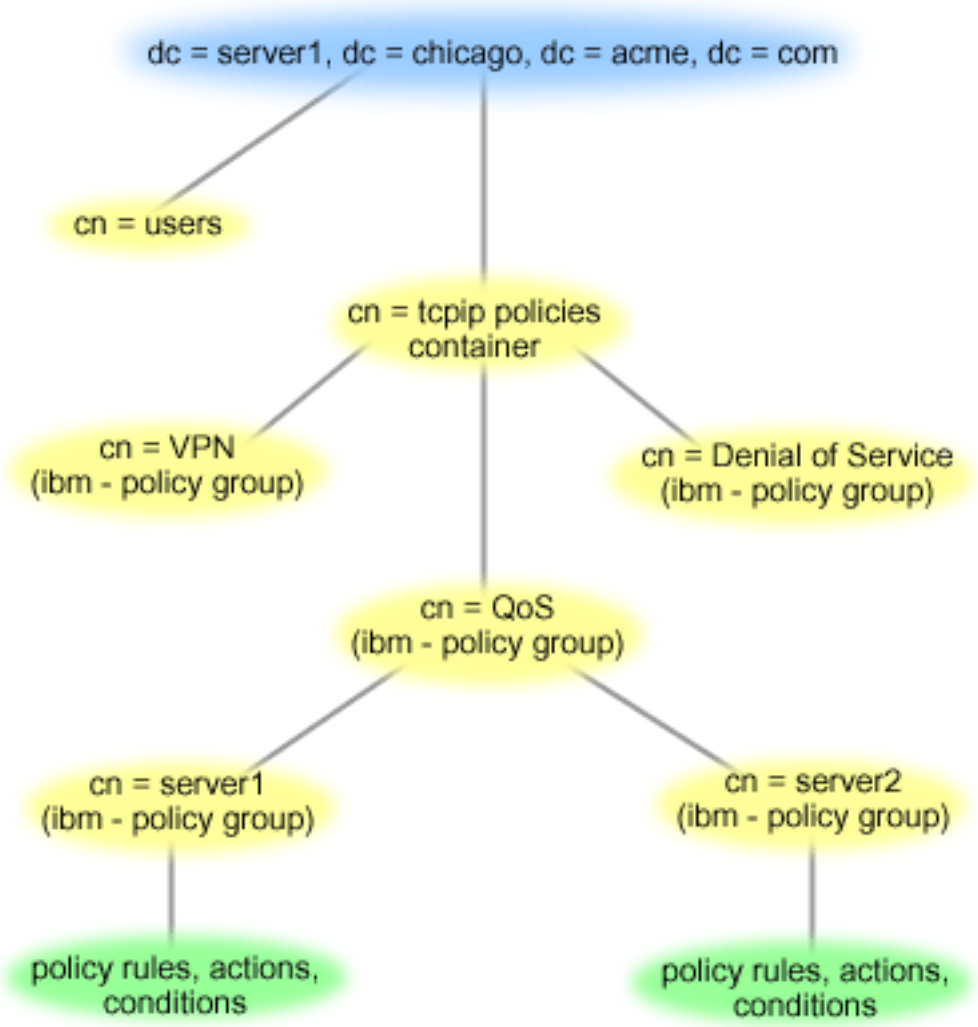
"Rozlišovací názov"
Keď chcete spravovať časť svojho adresára pozrite si *rozlišovací názov (DN)* alebo (ak sa rozhodnete) kľúčové slovo.

"Konfigurácia adresárového servera" na strane 51
Konfigurácie politík QoS sa dajú exportovať do adresárového servera LDAP.

Rozlišovací názov

Keď chcete spravovať časť svojho adresára pozrite si *rozlišovací názov (DN)* alebo (ak sa rozhodnete) kľúčové slovo.

DN zadajte, keď konfigurujete adresárový server v rámci sprievodcu Úvodnou konfiguráciou kvality služieb (QoS). DN sa zvyčajne skladá z názvu pre samotnú položku ako aj objektov (radených zhora nadol) nad položkou v adresári. Server môže sprístupniť všetky objekty v adresári, ktoré sú pod DN. Povedzme napríklad, že server LDAP obsahuje adresárovú štruktúru tak, ako je to zobrazené na nasledujúcom obrázku:



Obrázok 3. Vzorová adresárová štruktúra QoS

Server1 hore (dc=server1,dc=chicago,dc=acme,dc=com) je server, na ktorom sa nachádza adresárový server. Ostatné servery, napríklad politiky cn=QoS alebo cn=tcpip sú tam, kde sú uložené v pamäti servery QoS. Takže v cn=serveri1, je predvolený DN napísaný ako cn=server1,cn=QoS,cn=tcpip politiky,dc=server1,dc=chicago,dc=acme,dc=com. V cn=serverI2, sa predvolený DN píše ako cn=server2,cn=QoS,cn=tcpip politiky,dc=server1,dc=chicago,dc=acme,dc=com.

Pri riadení vášho adresára je dôležité zmeniť správny server v DN, ako je cn alebo dc. Buďte opatrný pri upravovaní DN, hlavne kvôli tomu, že reťazec je zvyčajne príliš dlhý, aby sa zobrazil bez pretáčania.

Súvisiace koncepty

“Kľúčové slová” na strane 24
Keď konfigurujete svoj adresárový server, musíte sa rozhodnúť, či sa majú s každou konfiguráciou kvality služieb (QoS) asociovať kľúčové slová.

“Konfigurácia adresárového servera” na strane 51
Konfigurácie politík QoS sa dajú exportovať do adresárového servera LDAP.

Súvisiaci odkaz

“Informácie týkajúce sa QoS” na strane 65
Sú tu uvedené publikácie IBM Redbooks (vo formáte PDF), webové stránky, a témy informačného centra, ktoré sa týkajú témy kvality služieb (QoS). Je možné prezerať alebo tlačiť všetky súbory vo formáte PDF.

Scenáre

Tieto scenáre politík kvality služby (QoS) vám môžu pomôcť porozumieť, prečo a ako treba QoS používať.

Jedným z najlepších spôsobov, akým sa možno o QoS niečo naučiť, je oboznámiť sa s fungovaním tejto funkcie na celkovom pôdoryse vašej siete. Nasledovné jednoduché príklady ilustrujú, prečo je treba politiky QoS používať; príklady tiež poskytujú určité návody na vytváranie politík a tried služby.

Poznámka: IP adresy a diagramy na obrázkoch sú vymyslené a slúžia iba na ilustračné účely.

Súvisiace koncepty

“Monitorovanie serverových transakcií” na strane 62
Pomocou monitora kvality služieb (QoS) si môžete overiť, či politiky QoS fungujú podľa vašej predstavy.

Súvisiaci odkaz

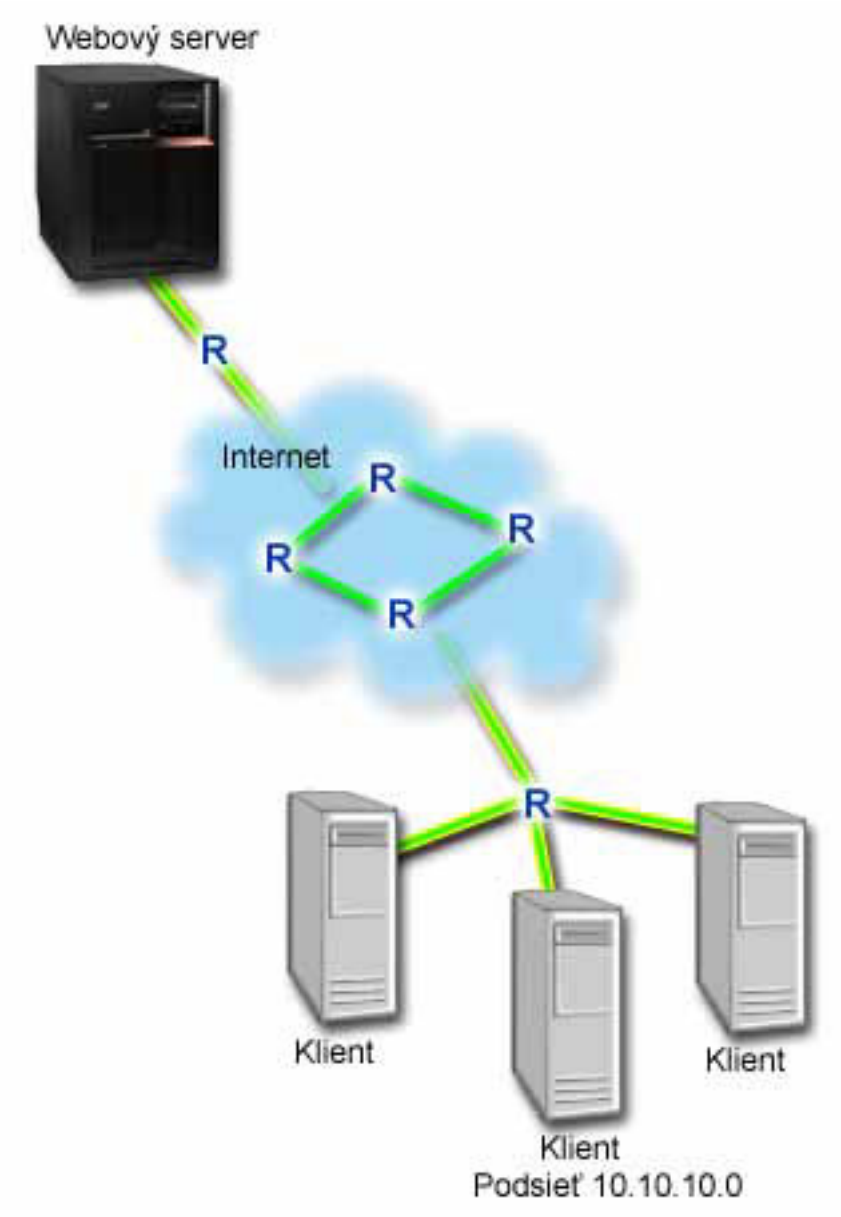
“Monitorovanie QoS” na strane 55
Monitor kvality služieb (QoS) môžete použiť na analýzu prevádzky IP cez server.

Scenár: Obmedzenie prevádzky prehliadača

Kvalitu služieb (QoS) môžete využiť pri riadení výkonu komunikačnej prevádzky. Použite politiku diferencovaných služieb buď na obmedzenie, alebo rozšírenie výkonu aplikácie v rámci vašej siete.

Situácia

Vaša spoločnosť máva vždy v piatok veľmi rušnú komunikáciu s dizajnérskou skupinou, a táto komunikácia prebieha cez webové prehliadače. 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.



Obrázok 4. Obmedzenie komunikácie s klientom cez webový prehliadač pomocou webového servera

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.

Nevyhnutné podmienky a predpoklady

- So svojím poskytovateľom internetových služieb máte uzavretú zmluvu o úrovni služieb (SLA), ktorá vám zabezpečuje, že tieto politiky budú mať požadovanú prioritu. Politika QoS, ktorú si vytvárate na serveri iSeries, umožňuje komunikácii (v politike) získať prioritu v celej sieti. Táto politika QoS nezaručuje prioritu a je závislá od vašej zmluvy o úrovni služieb. Využitie politík QoS vám vlastne môže poskytnúť isté ″páky″ pri dojednávaní určitých úrovní služieb a rýchlostí.

- Politiky diferencovaných služieb vyžadujú smerovače typu DiffServ pozdĺž sieťovej cesty. Väčšina smerovačov podporuje diferencovanú službu.

Konfigurácia

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

Súvisiace koncepty

"Dohoda úrovne služieb" na strane 48
Táto téma poukazuje na niektoré dôležité aspekty dohody úrovne služieb (SLA), ktoré by mohli ovplyvniť vašu implementáciu kvality služieb (QoS).

"Diferenčný servis" na strane 2
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.

Súvisiaci odkaz

"Monitorovanie QoS" na strane 55
Monitor kvality služieb (QoS) môžete použiť na analýzu prevádzky IP cez server.

Podrobnosti scenára: Vytvoriť politiku diferencovaných služieb

1. V aplikácii iSeries Navigator rozviňte iSeries A → **Sieť** → **Politiky IP**.
2. Kliknite pravým tlačidlom na **Kvalitu služieb** a vyberte **Konfiguráciu** na otvorenie rozhrania kvality služieb (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 okne Nový klient zadajte nasledujúce informácie a kliknite na tlačidlo **OK**:
   - **Názov**: UCD_Client
   - **IP adresa 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 okne Nová aplikácia zadajte nasledujúce informácie a kliknite na tlačidlo **OK** na návrat 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 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.

Práve ste ukončili konfiguráciu politiky diferencovaných služieb v aplikácii iSeries A. Nasledujúci krok je spustenie alebo aktualizácia servera.

Podrobnosti scenára: Spustiť alebo aktualizovať server QoS

V okne Konfigurácia servera kvality služieb (QoS) vyberte **Spustiť → server** alebo **Aktualizovať → server**.

Podrobnosti scenára: Použiť monitor na skontrolovanie, či vaša politika funguje

Na skontrolovanie, či vaša politika funguje tak, ako ste ju nakonfigurovali, aby fungovala podniknite tieto kroky:

1. V okne Konfigurácia kvality služieb (QoS) vyberte **Monitorovať → server**. 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 číslo mimo profilu indikuje počet bitov, ktoré presahujú rýchlosť sektoru tokena a 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).

   Dôležitá je aj hodnota, ktorú priradíte poľu ohraničenia priemernej rýchlosti. 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 monitorov nájdete v časti “Monitorovanie QoS” na strane 55.

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

Podrobnosti scenára: Zmeniť vlastnosti (v prípade potreby)

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 vytvorili v politike pomocou týchto krokov:

1. V okne Konfigurácia servera kvality služieb (QoS) vyberte adresár **DiffServ**. V zozname v pravej časti okna pravým tlačidlom kliknite na **UCD** a vyberte **Vlastnosti**, aby ste upravili politiku.Objaví sa okno Vlastnosti s hodnotami, ktoré riadia všeobecnú politiku.
2. 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.Objaví sa okno Vlastnosti QoS s hodnotami, ktoré upravujú riadenie premávky.
4. Zmeňte príslušné hodnoty.
5. Z okna Konfigurácia servera QoS vyberte **Aktualizovať → server** na akceptovanie svojich zmien.

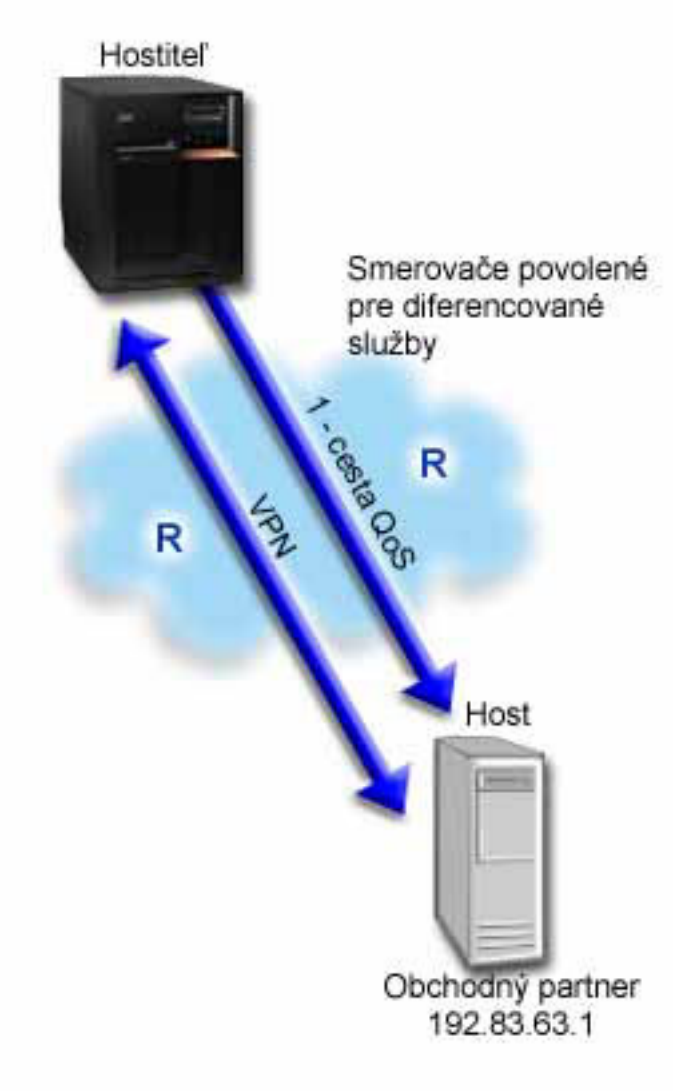
Scenár: Bezpečné a predpovedateľné výsledky (VPN a QoS)

Aj vtedy, ak používate virtuálnu súkromnú sieť (VPN), môžete vytvárať politiky kvality služby (QoS). Tento príklad vám ukazuje spoločné použitie oboch.

Situácia

Váš partner je pripojený prostredníctvom VPN a vy chcete skombinovať VPN a QoS, aby ste tak pre najdôležitejšie obchodné údaje zaistili bezpečnosť a predvídateľný tok. Konfigurácia QoS cestuje len jedným smerom. Preto, ak máte audio/video aplikáciu, potrebujete vytvoriť QoS pre aplikáciu na oboch stranách pripojenia.

Tento obrázok znázorňuje váš server a vášho klienta v pripojení typu hostiteľ-hostiteľ v rámci virtuálnej súkromnej siete. Každé R predstavuje diferencované službou umožnené smerovače pozdĺž cesty premávky. Ako vidíte QoS politiky tečú len v jednom smere.



Obrázok 5. Pripojenie typu hostiteľ-hostiteľ v rámci virtuálnej súkromnej siete s použitím politiky diferencovanej služby 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. Keď ste už zaistili ochranu svojho VPN pripojenia, môžete si nastaviť aj politiku QoS. Môžete vytvoriť politiku diferencovaných služieb. Tejto politike môže byť priradená vysoká hodnota kódového bodu urýchleného napredovania, čo bude mať vplyv na spôsob, akým bude sieť stanovovať priority najdôležitejšej komunikačnej prevádzky.

Nevyhnutné podmienky a predpoklady

- So svojím poskytovateľom internetových služieb máte uzavretú zmluvu o úrovni služieb (SLA), ktorá vám zabezpečuje, že tieto politiky budú mať požadovanú prioritu. Politika QoS, ktorú si vytvárate na serveri iSeries, umožňuje komunikácii (v politike) získať prioritu v celej sieti. Nezaručuje to a je závislá na vašom SLA. Využitie politík QoS vám vlastne môže poskytnúť isté ″páky″ pri dojednávaní určitých úrovní služieb a rýchlostí. Viac informácií nájdete v témach týkajúcich sa zmluvy o úrovni služieb (použite príslušný odkaz).
- Politiky diferencovaných služieb vyžadujú smerovače typu DiffServ pozdĺž sieťovej cesty. Väčšina smerovačov podporuje diferencovanú službu.

Konfigurácia

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

Súvisiace koncepty

"Dohoda úrovne služieb" na strane 48
Táto téma poukazuje na niektoré dôležité aspekty dohody úrovne služieb (SLA), ktoré by mohli ovplyvniť vašu implementáciu kvality služieb (QoS).

"Diferenčný servis" na strane 2
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.

Súvisiaci odkaz

"Monitorovanie QoS" na strane 55
Monitor kvality služieb (QoS) môžete použiť na analýzu prevádzky IP cez server.

Podrobnosti scenára: Nakonfigurovať pripojenie VPN medzi dvomi hostiteľmi.

Pomoc pri konfigurácii VPN nájdete v príklade pripojenia VPN medzi dvoma hostiteľmi.

Podrobnosti scenára: Vytvoriť politiku diferencovaných služieb

1. V aplikácii iSeries Navigator rozviňte iSeries A → **Sieť** → **Politiky IP**.
2. Kliknite pravým tlačidlom na **Kvalitu služieb** a vyberte **Konfiguráciu** na otvorenie okna Konfigurácia servera kvality služieb (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 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 vytvorili predchádzajúcich klientov, zrušte túto voľbu a skontrolujte, či sú vybratí len príslušní klienti.
8. Na stránke Požiadavka o údaje servera skontrolujte, či je vybratý **Ľubovoľný token** a **Všetky vlastnosti**.
9. Na stránke Aplikácie skontrolujte, či sú vybraté **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 Diferencovanej triedy služieb skontrolujte, či je vybraté **EF_VPN** a kliknite na tlačidlo **Ďalej**.
22. Na stránke Naplánovať vyberte **Aktívny počas vybratého plánu** a kliknite na tlačidlo **Nový**.
23. V 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.

Práve ste ukončili konfiguráciu politiky diferencovaných služieb v aplikácii iSeries A. Nasledujúci krok je spustenie alebo aktualizácia servera.

Podrobnosti scenára: Spustiť alebo aktualizovať server QoS

V okne Konfigurácia servera kvality služieb (QoS) vyberte **Spustiť → server** alebo **Aktualizovať → server**.

Podrobnosti scenára: Použiť monitor na skontrolovanie, či vaša politika funguje

Na skontrolovanie, či vaša politika funguje tak, ako ste ju nakonfigurovali, aby fungovala podniknite tieto kroky:

1. V okne Konfigurácia servera kvality služieb (QoS) vyberte **Monitorovať → server**. 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 monitorov nájdete v “Monitorovanie QoS” na strane 55.

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

Podrobnosti scenára: Zmeniť vlastnosti (v prípade potreby)

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

Ak chcete upraviť triedu služieb po tom, ako ste ju vytvorili, podniknite tieto kroky:

1. V okne Konfigurácia servera kvality služieb (QoS) vyberte adresár **DiffServ**. V zozname v pravej časti okna pravým tlačidlom kliknite na **VPN** a vyberte **Vlastnosti**, aby ste upravili politiku. Dialógové okno Vlastnosti sa zobrazí s hodnotami, ktoré určujú všeobecnú politiku.
2. 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.Objaví sa dialógové okno Vlastnosti QoS s hodnotami, ktoré upravujú riadenie premávky.
4. Zmeňte príslušné hodnoty.
5. Z okna Konfigurácia servera QoS vyberte **Aktualizovať → server** na akceptovanie svojich zmien.

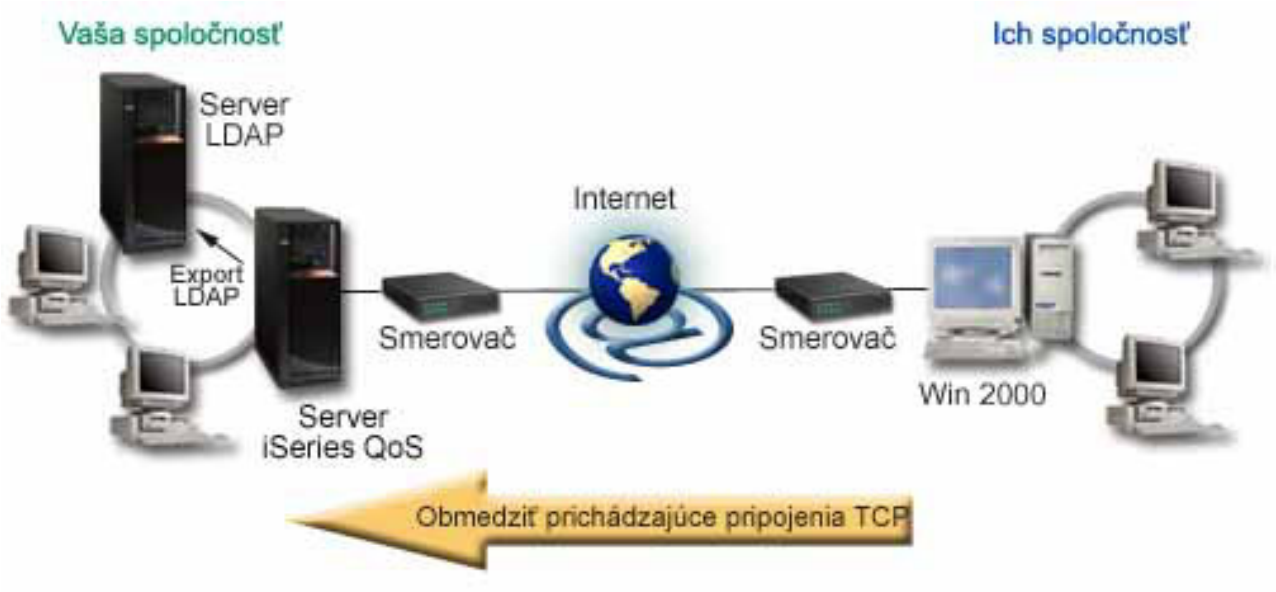
Scenár: Obmedzenie prichádzajúcich pripojení

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

Situácia

Vaše prostriedky webového servera sú preťažené požiadavkami od klientov vstupujúcimi do vašej siete. Musíte spomaliť prichádzajúcu premávku HTTP do vášho webového servera na lokálnom rozhraní 192.168.1.1. Kvalita služieb (QoS) vám môže pomôcť obmedziť prichádzajúce pokusy o pripojenie na základe atribútov pripojenia (napríklad IP adresa) do vášho servera. Aby ste toto dosiahli, rozhodnete sa spraviť politiku povolenia vstupu, ktorá obmedzí počet akceptovaných vstupných pripojení.

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



Obrázok 6. Obmedzenie prichádzajúcich pripojení TCP

Ciele

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

Tieto témy zobrazujú spôsob, ako vytvoriť prichádzajúce politiku prístupu.

Súvisiaci odkaz

“Monitorovanie QoS” na strane 55
Monitor kvality služieb (QoS) môžete použiť na analýzu prevádzky IP cez server.

Podrobnosti scenára: Vytvoriť politiku vstupu

1. V aplikácii iSeries Navigator rozviňte iSeries A → **Sieť** → **Politiky IP**.
2. Kliknite pravým tlačidlom na **Kvalitu služieb** a vyberte **Konfiguráciu** na otvorenie okna Konfigurácia servera kvality služieb (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 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 identifikátora Uniform Resource Identifier (URI) skontrolujte, či je vybratý **Ľubovoľný URI** a kliknite na tlačidlo **Ďalej**.
9. Na stránke Aplikácie vyberte **Špecifický port, rozsah portov alebo typ servera** a kliknite na **Nový**.
10. V okne Nová aplikácia zadajte nasledujúce informácie a kliknite na tlačidlo **OK** na návrat do sprievodcu:
    - **Názov**: HTTP
    - **Port**: 80
11. Kliknite na tlačidlo **Ďalej**, ak chcete ísť 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 Tried služieb 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 tlačidlo **Nový**.

22. V 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.

    Práve ste ukončili konfiguráciu politiky prichádzajúceho prístupu v aplikácii iSeries A. Nasledujúci krok je spustenie alebo aktualizácia servera.

Podrobnosti scenára: Spustiť alebo aktualizovať server QoS

V okne Konfigurácia servera kvality služieb (QoS) vyberte **Spustiť → server** alebo **Aktualizovať → server**.

Podrobnosti scenára: Použiť monitor na skontrolovanie, či vaša politika funguje

Na skontrolovanie, či vaša politika funguje tak, ako ste ju nakonfigurovali, aby fungovala podniknite tieto kroky:

1. V okne Konfigurácia kvality služieb (QoS) vyberte **Monitorovať → server**. 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).

   Dôležitá je aj hodnota, ktorú priradíte poľu priemernej rýchlosti požiadavky o spojenie. 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. Popis všetkých polí monitorov nájdete v časti “Monitorovanie QoS” na strane 55.

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

Podrobnosti scenára: Zmeniť vlastnosti (v prípade potreby)

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

1. V okne Konfigurácia servera kvality služieb (QoS) vyberte adresár **Vstup**. V zozname v pravej časti okna pravým tlačidlom kliknite na **Restrict_TheirCo** a vyberte **Vlastnosti**, aby ste upravili politiku.Objaví sa okno Vlastnosti s hodnotami, ktoré riadia všeobecnú politiku.
2. 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.Objaví sa okno Vlastnosti QoS s hodnotami, ktoré upravujú riadenie premávky.
4. Zmeňte príslušné hodnoty.
5. Z okna Konfigurácia servera QoS vyberte **Aktualizovať → server** na akceptovanie svojich zmien.

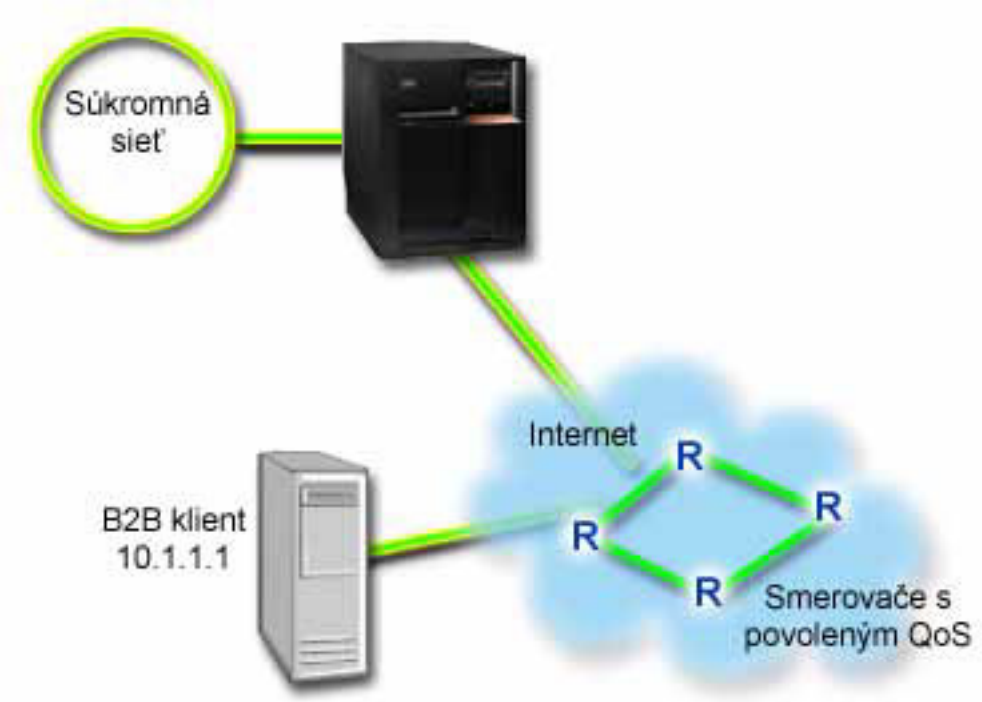
Scenár: Predvídateľná prevádzka B2B

Ak potrebujete predpovedateľné doručenie a zároveň potrebujete vyžadovať rezerváciu, použijete taktiež politiku integrovaných služieb. Tento príklad ilustruje službu riadeného zaťaženia.

Situácia

Odbytové oddelenie hlási problémy, že komunikácia po sieti nefunguje tak, ako očakávali. Server iSeries vašej spoločnosti je umiestnený v prostredí typu ″business-to-business″ (B2B), ktoré vyžaduje predvídateľné podnikové služby na požiadanie. Potrebujete poskytovať predpovedateľné transakcie vašim zákazníkom. Odbytovej jednotke chcete teda pre jeho objednávkovú aplikáciu počas najrušnejších hodín dňa (medzi 1O.00 a 16.OO h) poskytnúť vyššiu kvalitu služby (QoS).

Na nasledovnom obrázku sa odbytová skupina nachádza vo vašej privátnej sieti. Na komunikačnej trase ku klientovi B2B sú smerovače povolené protokolom ReSerVation Protocol (RSVP). Každé R predstavuje smerovač pozdĺž cesty premávky.



Obrázok 7. Politika integrovaných služieb ku klientovi B2B prostredníctvom smerovačov podporujúcich protokol 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 riadeného zaťaženia, jej výkon nebude trpieť zvýšením zaťaženia siete. Prevádzka bude zabezpečovaná službou, podobnou prevádzke v sieti za bežných okolností. Pretože konkrétne táto aplikácia je voči určitému oneskoreniu tolerantná, rozhodnete sa použiť politiku integrovaných služieb pomocou služby riadeného zaťaženia.

Politiky integrovaných služieb taktiež požadujú, aby boli pozdĺž cesty premávky smerovače s povoleným RSVP.

Nevyhnutné podmienky a predpoklady

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

- **Aplikácie podporujúce RSVP**

Pretože váš server nemá nijaké aplikácie s povoleným protokolom RSVP, musíte si napísať svoje vlastné aplikácie s povoleným protokolom RSVP. Ak si chcete napísať svoje vlastné aplikácie, použite aplikačné programové rozhranie RSVP, aplikačné programové rozhrania soketu qtoq QoS alebo aplikačné programové rozhrania integrovaných služieb.

- **Smerovače a servery podporujúce protokol RSVP na sieťovej trase**

  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.

- **Zmluva o úrovni služieb**

  So svojím poskytovateľom internetových služieb máte uzavretú zmluvu o úrovni služieb (SLA), ktorá vám zabezpečuje, že tieto politiky budú mať požadovanú prioritu. Politika QoS, ktorú si vytvárate na serveri iSeries, umožňuje komunikácii (v politike) získať prioritu v celej sieti. Táto politika QoS nezaručuje prioritu a je závislá od vašej zmluvy o úrovni služieb. Využitie politík QoS vám vlastne môže poskytnúť isté ″páky″ pri dojednávaní určitých úrovní služieb a cien. Viac informácií nájdete v témach týkajúcich sa zmluvy o úrovni služieb (použite príslušný odkaz).

  Poznámka: Ak pracujete v súkromnej sieti, zmluvu o úrovni služieb nepotrebujete.

Konfigurácia

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

Súvisiace koncepty

“Typy integrovaných služieb” na strane 9
Existujú dva typy integrovaných služieb: riadená záťaž a typ s garanciou.

“Integrovaná služba” na strane 6
Druhý typ politiky šírky pásma pre prístup smerom von, ktorý môžete vytvoriť, je politika integrovaných služieb. Integrovaná služba poskytuje IP aplikáciám schopnosť požadovať a vyhradiť si frekvenčné pásmo pomocou protokolu ReSerVation Protocol (RSVP) a aplikačných programových rozhraní kvality služby (QoS).

“Rozhrania API QoS” na strane 16
Túto tému si môžete prečítať, aby ste sa získali informácie o protokoloch, rozhraniach API a požiadavkách pre smerovač, ktorý je povolený pre protokol ReSerVation Protocol (RSVP). Aktuálne rozhrania kvality služieb (QoS) API zahŕňajú rozhrania API RAPI, rozhranie API qtoq soketu, rozhranie sendmsg() API a rozhrania monitor API.

“Dohoda úrovne služieb” na strane 48
Táto téma poukazuje na niektoré dôležité aspekty dohody úrovne služieb (SLA), ktoré by mohli ovplyvniť vašu implementáciu kvality služieb (QoS).

Súvisiaci odkaz

“Monitorovanie QoS” na strane 55
Monitor kvality služieb (QoS) môžete použiť na analýzu prevádzky IP cez server.

Podrobnosti scenára: Vytvoriť politiku integrovaných služieb

1. V aplikácii iSeries Navigator rozviňte iSeries A → **Sieť** → **Politiky IP**.
2. Kliknite pravým tlačidlom na **Kvalitu služieb** a vyberte **Konfiguráciu** na otvorenie okna Konfigurácia servera kvality služieb (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 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 vytvorili predchádzajúcich klientov, zrušte túto voľbu a skontrolujte, či sú vybratí len príslušní klienti.

8. V okne Nová aplikácia zadajte nasledujúce informácie a kliknite na tlačidlo **OK** na návrat 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 vyberiete pre politiku integrovaných služieb musí byť zapísaná na používanie API protokolu Resource Reservation Setup Protocol (RAPI) alebo na API qtoq soketov. Spolu s protokolom ReSerVation Protocol (RSVP) vykonávajú tieto rozhrania API rezerváciu integrovaných služieb v sieti. 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 tlačidlo **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. Hlavné rozhranie QoS uvádza všetky politiky vytvorené v serveri. Po ukončení sprievodcu sa politika zobrazí v pravej časti okna.

Práve ste ukončili konfiguráciu politiky integrovaných služieb v aplikácii iSeries A. Nasledujúci krok je spustenie alebo aktualizácia servera.

Podrobnosti scenára: Spustiť alebo aktualizovať server QoS

V okne Konfigurácia servera kvality služieb (QoS) vyberte **Spustiť → server** alebo **Aktualizovať → server**.

Podrobnosti scenára: Použiť monitor na skontrolovanie, či vaša politika funguje

Na skontrolovanie, či vaša politika funguje tak, ako ste ju nakonfigurovali, aby fungovala podniknite tieto kroky:

1. V okne Konfigurácia servera kvality služieb (QoS) vyberte **Monitorovať → server**. 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. Úplný popis polí monitorov nájdete v časti “Monitorovanie QoS” na strane 55.

Poznámka: Nezabudnite, že výsledky budú presné len, keď je politika aktívna. Skontrolujte plán, ktorý ste špecifikovali v rámci politiky. Okrem toho, monitor zobrazuje politiky IntServ až po spustení aplikácií. Pred monitorovaním je potrebné vytvoriť rezerváciu protokolu ReSerVation Protocol (RSVP).

Podrobnosti scenára: Zmeniť vlastnosti (v prípade potreby)

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.

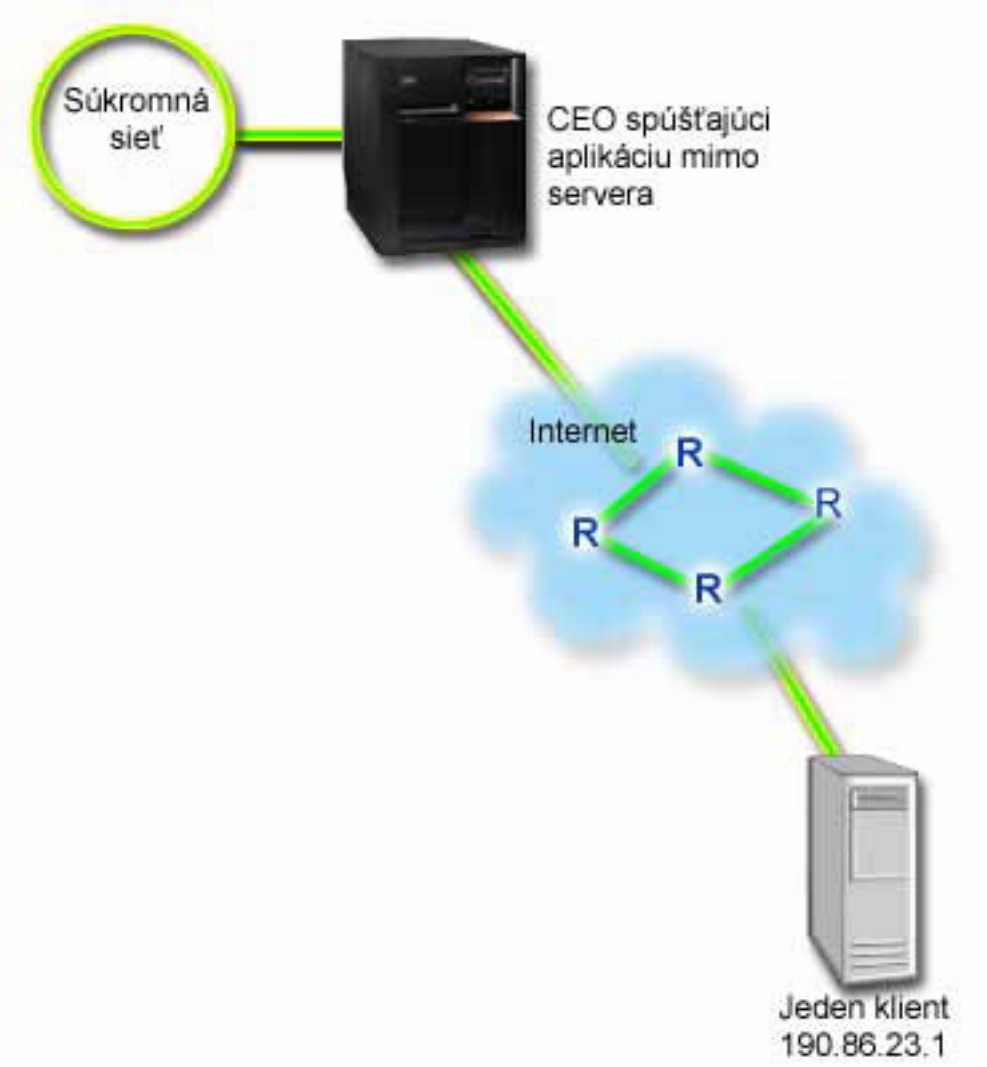
1. V okne Konfigurácia servera kvality služieb (QoS) vyberte adresár **IntServ**. V zozname v pravej časti okna pravým tlačidlom kliknite na **B2B_CL** a vyberte **Vlastnosti**, aby ste upravili politiku.Objaví sa okno Vlastnosti s hodnotami, ktoré riadia všeobecnú politiku.
2. Zmeňte príslušné hodnoty.
3. Z okna Konfigurácia servera QoS vyberte **Aktualizovať → server** na akceptovanie svojich zmien.

Scenár: Dedikované 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.

Situácia

Generálny riaditeľ vašej spoločnosti sa chystá medzi 13.00 a 14.00 h uskutočniť on-line prezentáciu pre klienta na druhom konci krajiny. Musíte sa teda postarať o to, aby IP telefónia v danom čase mala zaručenú šírku pásma a aby počas prenosu nedochádzalo k prerušeniam. V tomto scenári je aplikácia umiestnená na serveri.



Obrázok 8. Prezentácia generálneho riaditeľa pre klienta zaručená politikou integrovanej služby

Ciele

Keďže aplikácia, ktorú váš generálny riaditeľ používa, vyžaduje neprerušovaný prenos, rozhodnete sa využiť politiku integrovanej služby so zárukou. Garantovaná služba riadi maximálne oneskorenie radenia, takže pakety nebudú oneskorené viac ako o určené množstvo času.

Nevyhnutné podmienky a predpoklady

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

- **Aplikácie podporujúce RSVP**

  Pretože váš server nemá nijaké aplikácie s povoleným protokolom RSVP, musíte si napísať svoje vlastné aplikácie s povoleným protokolom RSVP. Ak si chcete napísať svoje vlastné aplikácie, použite aplikačné programové rozhranie protokolu ReSerVation alebo aplikačné programové rozhrania soketu qtoq QoS. Bližšie informácie nájdete v časti “Rozhrania API QoS” na strane 16; nájdite si aplikačné programové rozhrania (API) pre integrovanú službu.
- **Smerovače a servery podporujúce protokol RSVP na sieťovej trase**

  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.

- **Zmluva o úrovni služieb**

  So svojím poskytovateľom internetových služieb máte uzavretú zmluvu o úrovni služieb (SLA), ktorá vám zabezpečuje, že tieto politiky budú mať požadovanú prioritu. Politika QoS, ktorú si vytvárate na serveri iSeries, umožňuje komunikácii (v politike) získať prioritu v celej sieti. Táto politika QoS nezaručuje prioritu a je závislá od vašej zmluvy o úrovni služieb. Využitie politík QoS vám vlastne môže poskytnúť isté ″páky″ pri dojednávaní určitých úrovní služieb a rýchlostí. Viac informácií nájdete v témach týkajúcich sa zmluvy o úrovni služieb (použite príslušný odkaz).

Konfigurácia

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

Súvisiace koncepty

“Typy integrovaných služieb” na strane 9
Existujú dva typy integrovaných služieb: riadená záťaž a typ s garanciou.

“Integrovaná služba” na strane 6
Druhý typ politiky šírky pásma pre prístup smerom von, ktorý môžete vytvoriť, je politika integrovaných služieb. Integrovaná služba poskytuje IP aplikáciám schopnosť požadovať a vyhradiť si frekvenčné pásmo pomocou protokolu ReSerVation Protocol (RSVP) a aplikačných programových rozhraní kvality služby (QoS).

“Dohoda úrovne služieb” na strane 48
Táto téma poukazuje na niektoré dôležité aspekty dohody úrovne služieb (SLA), ktoré by mohli ovplyvniť vašu implementáciu kvality služieb (QoS).

Súvisiaci odkaz

“Monitorovanie QoS” na strane 55
Monitor kvality služieb (QoS) môžete použiť na analýzu prevádzky IP cez server.

Podrobnosti scenára: Vytvoriť politiku integrovaných služieb

1. V aplikácii iSeries Navigator rozviňte iSeries A → **Sieť** → **Politiky IP**.
2. Kliknite pravým tlačidlom na **Kvalitu služieb** a vyberte **Konfiguráciu** na otvorenie okna Konfigurácia servera kvality služieb (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 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 vytvorili predchádzajúcich klientov, zrušte túto voľbu a skontrolujte, či sú vybratí len príslušní klienti. Na stránke Aplikácie vyberte **Špecifický port, rozsah portov alebo typ servera** a kliknite na **Nový**.
8. V okne Nová aplikácia zadajte nasledujúce informácie a kliknite na tlačidlo **OK** na návrat 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 vyberiete pre politiku integrovaných služieb musí byť zapísaná na používanie rozhrania API protokolu Resource Reservation Setup Protocol (RAPI) alebo rozhrania API qtoq

soketov. Spolu s protokolom ReSerVation Protocol (RSVP) vykonávajú tieto rozhrania API rezerváciu integrovaných služieb v sieti. 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 tlačidlo **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.

Práve ste ukončili konfiguráciu politiky integrovaných služieb v aplikácii iSeries A. Nasledujúci krok je spustenie alebo aktualizácia servera.

Podrobnosti scenára: Spustiť alebo aktualizovať server QoS

V okne Konfigurácia servera kvality služieb (QoS) vyberte **Spustiť → server** alebo **Aktualizovať → server**.

Podrobnosti scenára: Použiť monitor na skontrolovanie, či vaša politika funguje

Na skontrolovanie, či vaša politika funguje tak, ako ste ju nakonfigurovali, aby fungovala podniknite tieto kroky:

1. V okne Konfigurácia servera kvality služieb (QoS) vyberte **Monitorovať → server**. 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 profilu indikujú, že ostatná premávka sa oneskoruje alebo, že neuspokojila požiadavky tejto politiky integrovaných služieb. Popis všetkých polí monitorov nájdete v časti “Monitorovanie QoS” na strane 55.

   Poznámka: Nezabudnite, že výsledky budú presné len, keď je politika aktívna. Skontrolujte plán, ktorý ste špecifikovali v rámci politiky. Okrem toho, monitor zobrazuje politiky IntServ až po spustení aplikácií. Pred monitorovaním je potrebné vytvoriť rezerváciu protokolu ReSerVation Protocol (RSVP).

Podrobnosti scenára: Zmeniť vlastnosti (v prípade potreby)

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 Konfigurácia servera kvality služieb (QoS) vyberte adresár **IntServ**. V zozname v pravej časti okna pravým tlačidlom kliknite na **CEO_guaranteed** a vyberte **Vlastnosti**, aby ste upravili politiku.Objaví sa okno Vlastnosti s hodnotami, ktoré riadia všeobecnú politiku.
2. Zmeňte príslušné hodnoty.
3. Z okna Konfigurácia servera QoS vyberte **Aktualizovať → server** na akceptovanie svojich zmien.

Scenár: Monitorovanie aktuálnych sieťových štatistík

Sprievodcovia vás vyzvú, aby ste nastavili výkonové limity. Nie je možné odporúčať nijaké konkrétne hodnoty, pretože tie sa zakladajú na individuálnych požiadavkách konkrétnych sietí.

Ciele

Na nastavenie týchto limitov musíte reálne poznať aktuálny výkon vašej siete. Keďže sa pokúšate konfigurovať politiky kvality služby (QoS), zrejme už máte jasnú predstavu o tom, aké sú aktuálne potreby vašej siete. Ak chcete stanoviť presné limity rýchlostí, napríklad rýchlosť pamäťového bloku symbolov, môžete prípadne monitorovať celú komunikačnú prevádzku na vašom serveri. Takto môžete rýchlostné limity určiť spoľahlivejšie.

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.

Súvisiace koncepty

“Limity bloku tokenov a šírky pásma” na strane 9
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.

“Priemerný počet okamžitých pripojení a tzv. ″burst limit″ (prah zahltenia pripojenia)” na strane 15
Priemerný počet okamžitých pripojení a tzv. ″burst limit″ (prah zahltenia pripojenia) sú dovedna známe pod spoločným názvom *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.

Súvisiaci odkaz

“Monitorovanie QoS” na strane 55
Monitor kvality služieb (QoS) môžete použiť na analýzu prevádzky IP cez server.

Podrobnosti scenára: Otvoriť QoS v rámci aplikácie iSeries Navigator

1. V aplikácii iSeries Navigator, rozviňte svoj server → **Sieť → Politiky IP**.
2. Kliknite pravým tlačidlom na **Kvality služieb** a vyberte **Konfiguráciu**.
3. Rozviňte **Politiky šírky výstupného pásma**.
4. Kliknite pravým tlačidlom na **DiffServ** a zvoľte **Nová politika**. Objaví sa Nový sprievodca politikou kvality služieb (QoS).

Podrobnosti scenára: Vytvoriť politiku diferencovaných služieb

Keďže chcete zhromaždiť väčšinu premávky, ktorá vstupuje do vašej siete mohli by ste zavolať politiku **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 adresyAplikácia = Všetky porty
Protokol = Všetky protokolyPlán = Vždy
```

AplikáciaiSeries Navigator uvádza všetky politiky diferencovaných služieb vytvorených vo vašom serveri.

Podrobnosti scenára: Dokončiť 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.

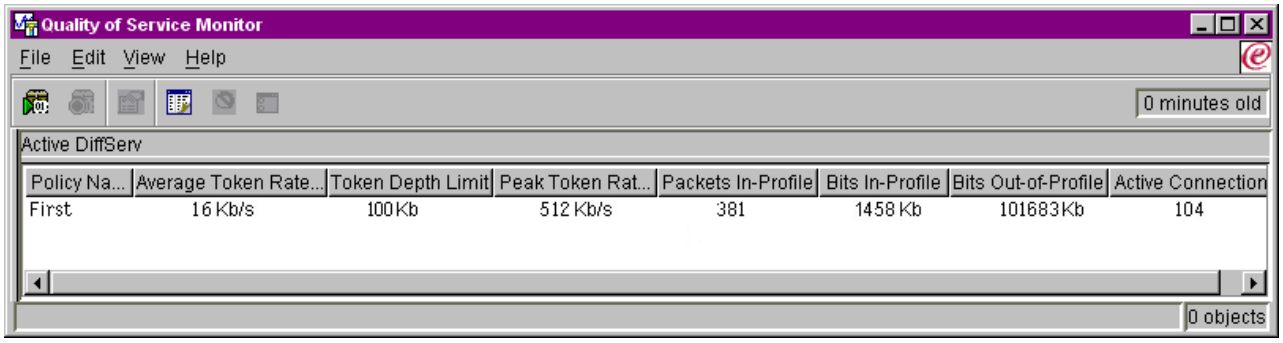
Triedy služieb v skutočnosti určujú výkonové úrovne, ktoré táto prevádzka prijíma zo smerovača. Vašu triedu služby môžete nazvať **Neobmedzená**, aby ste označili, že táto premávka prijme vyššiu úroveň služby. Aplikácia iSeries Navigator uvádza všetky triedy služieb definovaných vo vašom serveri.

Podrobnosti scenára: Monitorovať vlastnú 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**.

Táto číslica je zoznamom možného výstupu z monitora pre politiku zadanú vyššie.



Obrázok 9. Monitor kvality služieb (QoS)

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).

Dôležité je aj aké hodnoty priradíte poľu obmedzenia priemernej rýchlosti tokenu. 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. Monitor QoS poskytuje úplné popisy všetkých polí monitorov.

Podrobnosti scenára: Zmeniť hodnoty, keď je to potrebné

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. Keď vyberiete **Vlastnosti** objaví sa okno Vlastnosti QoS s hodnotami, ktoré riadia vašu premávku.

Podrobnosti scenára: Znovu monitorovať politiku

Po prezretí výsledkov použite metódu ″pokus a omyl″ na nájdenie najlepších hodnôt pre potreby vašej siete.

Plánovanie QoS

Najdôležitejší krok na splnenie kvality služieb (QoS) je plánovanie. Kvôli očakávaným výsledkom musíte posúdiť svoje sieťové zariadenia a monitorovať sieťovú prevádzku.

Táto téma zahŕňa aj poradcu plánovaním. Poradca plánovaním QoS vás prevedie cez základné otázky, ktoré si musíte položiť počas fázy plánovania. Ako dodatok k poradcovi si pred konfiguráciou QoS najprv prečítajte tieto podtémy.

Vezmite do úvahy výkon siete

QoS sa týka v skutočnosti výkonu siete. O QoS uvažujete zrejme preto, že začínate trpieť preťažením siete a strácaním paketov. Pred realizáciou ľubovoľnej politiky by ste mohli použiť monitor QoS na overenie svojich aktuálnych úrovní výkonu premávky IP. Tieto výsledky vám môžu pomôcť určiť, kde sa objavuje preťaženie.

Súvisiace koncepty

"Monitorovanie serverových transakcií" na strane 62
Pomocou monitora kvality služieb (QoS) si môžete overiť, či politiky QoS fungujú podľa vašej predstavy.

"Konfigurácia QoS" na strane 50
Túto tému môžete použiť pri vytváraní politík diferencovanej služby, politík integrovanej služby a politík prijímania prichádzajúcej komunikácie.

Požiadavky na oprávnenia

Politiky kvality služieb (QoS) môžu obsahovať citlivé informácie o vašej sieti. Preto je treba oprávnenia na správu QoS prideľovať len vtedy, keď je to nevyhnutné.

Skôr, ako môžete konfigurovať politiky QoS a prípadne aj adresárové servery LDAP, musíte mať nasledovné oprávnenia:

Prideľovanie oprávnení potrebných na správu adresárového servera

Administrátor QoS musí mať nasledovné oprávnenia: oprávnenie *ALLOBJ a *IOSYSCFG. Alternatívne oprávnenia nájdete v časti Configure directory server.

Prideľovanie oprávnení potrebných na spustenie servera TCP/IP

Ak chcete prideliť objektové oprávnenie príkazom STRTCPSVR a ENDTCPSVR, nasledujte tieto kroky:

1. **STRTCPSVR**: Do príkazového riadka napíšte GRTOBJAUT OBJ (QSYS/STRTCPSVR) OBJTYPE (*CMD) USER (ADMINPROFILE) AUT (*USE), za ADMINPROFILE dosaďte názov svojho vlastného administrátorského profilu a stlačte kláves Enter.
2. **ENDTCPSVR**: Do príkazového riadka napíšte GRTOBJAUT OBJ (QSYS/ENDTCPSVR) OBJTYPE (*CMD) USER (ADMINPROFILE) AUT (*USE), za ADMINPROFILE dosaďte názov svojho vlastného administrátorského profilu a stlačte kláves Enter.

Prideľovanie oprávnenia na prístup k všetkým objektom a oprávnenia na konfigurovanie systému

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 programe iSeries Navigator, rozviňte položku → **Užívatelia a skupiny** prislúchajúcu vášmu serveru.
2. Dvakrát kliknite na **Všetci užívatelia**.
3. Kliknite pravým tlačidlom na užívateľský profil administrátora a vyberte **Vlastnosti**.
4. V 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 **OK**; okno Vlastnosti sa zatvorí.

Systémové požiadavky

Kvalita služieb (QoS) je integrovanou časťou operačného systému.

Musíte splniť tieto požiadavky:

1. Inštalujte pomocné programy pripojiteľnosti protokolu TCP/IP (5722-TC1).
2. Inštalujte aplikáciu iSeries Navigator do vášho osobného počítača. Uistite sa, že komponent výstavby sietí nainštalujete počas inštalácie aplikácie iSeries Access. Kvalita služieb je umiestnená pod politikami IP v rámci adresára výstavby sietí.

Súvisiace koncepty

iSeries Navigator

Súvisiaci odkaz

"Informácie týkajúce sa QoS" na strane 65
Sú tu uvedené publikácie IBM Redbooks (vo formáte PDF), webové stránky, a témy informačného centra, ktoré sa týkajú témy kvality služieb (QoS). Je možné prezerať alebo tlačiť všetky súbory vo formáte PDF.

Dohoda úrovne služieb

Táto téma poukazuje na niektoré dôležité aspekty dohody úrovne služieb (SLA), ktoré by mohli ovplyvniť vašu implementáciu kvality služieb (QoS).

QoS je sieťové riešenie. Na prijatie priority siete mimo vašej súkromnej siete by ste mali mať SLA s vaším ISP.

Kedy sa vyžaduje SLA

SLA potrebujete len v prípade, ak vaše politiky vyžadovujú prioritu mimo vašej súkromnej siete. Ak používate politiky výstupu na spomalenie premávky odchádzajúcej z vášho servera, nevyžaduje sa žiadna garancia služby. V serveri môžete napríklad vytvoriť politiku, ktorá dáva jednej aplikácii vyššiu prioritu ako druhej. Váš server rozpoznáva túto prioritu, ale všetko mimo server túto prioritu rozpoznať nemusí. Ak máte súkromnú sieť a konfigurujete svoje smerovače na rozpoznanie značkovaní kódového bodu (použité na to, aby dali politikám výstupu úroveň služieb), potom im smerovače dajú prioritu vo vašej súkromnej sieti. 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.

Kedy sa vyžaduje 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. Naprieč doménami musí každý ISP súhlasiť s podporou požiadaviek QoS. Ich vzájomné fungovanie by mohlo spôsobiť určité problémy.

Uistite sa, že rozumiete úrovni služieb, ktorú skutočne prijímate. Dohody formujúce premávku špecificky určujú ako sa narába s premávkou, čo sa ukončuje, označuje, formuje alebo opakovanie prenáša. Kľúčové dôvody na poskytnutie QoS zahŕňajú čakaciu dobu riadenia, nepokoj, šírku pásma, stratu paketov, dostupnosť a priepustnosť. Vaše zmluvy o službách musia byť schopné dať vašim politikám, o čo požiadajú. Overte, či dostávate taký objem služieb, aký potrebujete. Ak to tak nie je, je možné, že plytváte svojimi prostriedkami. Napríklad ak požiadate o rezerváciu 500 Kbps pre telefóniu IP, ale vaša aplikácia potrebuje len 20 Kbps, môžete zaplatiť príplatok bez toho, aby ste dostali oznámenie od svojho ISP.

Poznámka: Politiky QoS vám umožňujú vyjednávať s vašim ISP o úrovniach služieb, čo môže znížiť náklady na sieťové 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 musieť súhlasiť s istou úrovňou služieb a mať schopnosť sledovať šírku pásma, ktoré používate.

Súvisiace koncepty

“Základné pojmy” na strane 2
Ak ste prvýkrát v kontakte s kvalitou služieb (QoS), môžete si prečítať niekoľko základných pojmov QoS. Toto vám dá prehľad o tom, ako QoS pracuje a ako spolupracujú funkcie QoS.

“Scenár: Obmedzenie prevádzky prehliadača” na strane 27
Kvalitu služieb (QoS) môžete využiť pri riadení výkonu komunikačnej prevádzky. Použite politiku diferencovaných služieb buď na obmedzenie, alebo rozšírenie výkonu aplikácie v rámci vašej siete.

“Scenár: Bezpečné a predpovedateľné výsledky (VPN a QoS)” na strane 31
Aj vtedy, ak používate virtuálnu súkromnú sieť (VPN), môžete vytvárať politiky kvality služby (QoS). Tento príklad vám ukazuje spoločné použitie oboch.

“Scenár: Predvídateľná prevádzka B2B” na strane 37
Ak potrebujete predpovedateľné doručenie a zároveň potrebujete vyžadovať rezerváciu, použijete taktiež politiku integrovaných služieb. Tento príklad ilustruje službu riadeného zaťaženia.

“Scenár: Dedikované doručenie (IP telefónia)” na strane 41
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.

Sieťový hardvér a softvér

Schopnosti vašich interných zariadení a ďalších zariadení mimo vašej siete majú mimoriadne veľký vplyv na výsledky kvality služby (QoS).

Aplikácie

Politiky integrovanej služby vyžadujú aplikácie, ktoré povoľuje protokol RSVP. Pretože aplikácie iSeries v súčasnosti protokol RSVP nepodporujú, musíte ich upraviť tak, aby mohli protokol RSVP používať. Ak to chcete urobiť, musíte si pomocou aplikačných programových rozhraní RSVP alebo aplikačných programových rozhraní soketov qtoq QoS napísať špeciálne programy. Tieto programy umožnia vašim aplikáciám používať RSVP.

Sieťové uzly

Smerovače, prepínače, ba dokonca aj vaše vlastné servery musia byť schopné používať QoS. Ak chcete použiť politiky integrovaných služieb, vaše zariadenia musia podporovať diferencovanú služby. To znamená, že sieťový uzol musí byť schopný klasifikovať, merať, označovať, tvarovať a prerušovať IP pakety (upravovače komunikačnej prevádzky).

Ak chcete použiť politiky integrovaných služieb, musí mať vaše zariadenie povolené RSVP. To znamená, že sieťové uzly tiež musia byť schopné podporovať protokol RSVP.

Súvisiace koncepty

“Rozhrania API QoS” na strane 16
Túto tému si môžete prečítať, aby ste sa získali informácie o protokoloch, rozhraniach API a požiadavkách pre smerovač, ktorý je povolený pre protokol ReSerVation Protocol (RSVP). Aktuálne rozhrania kvality služieb (QoS) API zahŕňajú rozhrania API RAPI, rozhranie API qtoq soketu, rozhranie sendmsg() API a rozhrania monitor API.

“Udržiavače prevádzky” na strane 5
Ak si želáte využiť politiky kvality služby (QoS), vaše sieťové zariadenia (napríklad smerovače a prepínače) musia disponovať spôsobilosťou pre upravovače komunikačnej prevádzky. Upravovačmi komunikačnej prevádzky sú klasifikátory, merače, značkovače, tvarovače a prerušovače.

Konfigurácia QoS

Túto tému môžete použiť pri vytváraní politík diferencovanej služby, politík integrovanej služby a politík prijímania prichádzajúcej komunikácie.

Keď si kvalitu služby (QoS) naplánujete, vytvorte si pomocou sprievodcov v programe iSeries Navigator svoje vlastné politiky QoS. Sprievodcovia vykonajú vynikajúcu prácu tým, že vás prevedú cez konfiguráciu.

Keď si svoje politiky nakonfigurujete, môžete na upravovanie konfigurácie svojich politík používať konfiguračné objekty programu iSeries Navigator. Konfiguračné objekty sú rozličné kusy, alebo časti tvoriace politiku. Keď si v programe iSeries Navigator otvoríte prostredie kvality služieb, nájdete tam adresáre označené ako klienty, aplikácie, rozvrhy, politiky, triedy služby, skokové správania a identifikátory URI. Tieto objekty vám umožňujú vytvoriť politiku. Bližšie informácie o týchto objektoch nájdete v prehľadnej pomoci ku kvalite služby v programeiSeries Navigator.

Povolenie politík QoS

Aby politiky nadobudli účinnosť, musia byť povolené. Ak ste pri ich vytváraní použili sprievodcov, server tieto politiky povolí automaticky. Ak ste však niektorú politiku zmenili pomocou konfiguračných objektov, musíte server najprv dynamicky aktualizovať - až potom začnú byť politiky aktívne. Skôr, ako ich povolíte, nezabudnite skontrolovať, či sa niektoré navzájom neprekrývajú. To by mohlo spôsobiť problémy.

Súvisiace koncepty

“Plánovanie QoS” na strane 46
Najdôležitejší krok na splnenie kvality služieb (QoS) je plánovanie. Kvôli očakávaným výsledkom musíte posúdiť svoje sieťové zariadenia a monitorovať sieťovú prevádzku.

iSeries Navigator

Súvisiace úlohy

“Poradie politík QoS” na strane 52
Vždy, keď máte dve politiky, ktoré sa prekrývajú, dôležité je fyzické poradie vašich politík v aplikácii iSeries Navigator.

Súvisiaci odkaz

“Spravovanie QoS” na strane 53
Tieto postupy môžete použiť na spravovanie už existujúcich vlastností a politík kvality služby (QoS).

Konfigurácia QoS pomocou sprievodcov

Ak chcete konfigurovať politiky kvality služieb (QoS) musíte použiť sprievodcov QoS umiestnených v aplikácii iSeries Navigator.

Tu je zoznam sprievodcov a ich funkcie:

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

Nový sprievodca politikou IntServ
Nový sprievodca politikou IntServ vám umožňuje vytvoriť politiku integrovaných služieb. Táto politika pripúšťa alebo zakazuje požiadavku protokolu ReSerVation Protocol (RSVP), ktorá nepriamo riadi 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: Predtým ako nastavíte politiku integrovaných služieb musíte zapísať vlastné aplikácie na používanie protokolu RSVP.

Nový sprievodca 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 do odchádzajúcej premávky na základe IP

adries zdroja/miesta určenia, portov, aplikácii a dokonca klientov. Vo V5R3 vaše aplikácie iSeries môžu prijať úrovne služieb na základe špecifickejších informácií o aplikáciách. Viac informácií nájdete v koncepte diferencovaných služieb pred vytvorením tejto politiky.

Sprievodca novou triedou služieb
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 novou politikou povolenia vstupu
Sprievodcu politikou povolenia vstupu použite na obmedzenie pripojení prichádzajúcich do vášho servera. Môžete obmedziť prístup adresou protokolu TCP/IP, aplikáciou, miestnym rozhraním alebo identifikátorom Uniform Resource Identifier (URI). Toto umožňuje administrátorovi systému riadiť prístup k vášmu serveru od špecifických klientov, špecifických aplikácii servera alebo podľa URI. Okrem toho môžete zvýšiť výkon servera.

Poznámka: Predtým ako nastavíte politiku vstupu, ktorá používa identifikátory URI, musíte zabezpečiť, aby port aplikácie priradený pre identifikátor URI vyhovoval načúvacej smernici povolenej pre akcelerátor Fast Response Cache Accelerator (FRCA) v konfigurácii Apache Web Server.

Po tom ako sa rozhodnete, ktorý typ politiky vytvoríte, môžete konfigurovať politiku prostredníctvom príslušného sprievodcu z predchádzajúceho zoznamu.

Pristúpte k sprievodcovi QoS v rámci aplikácie iSeries Navigator

Tieto kroky môžete používať na prístup k sprievodcom QoS a vytvoriť politiku v rámci aplikácie iSeries Navigator.

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

1. V aplikácii iSeries Navigator, rozviňte svoj server → **Sieť** → **Politiky IP**.
2. Kliknite pravým tlačidlom na **Kvalitu služieb** a kliknite na **Konfiguráciu**.

   Poznámka: Sprievodca úvodnou konfiguráciou sa otvára za týchto okolností:
   - Po prvý krát používate QoS grafické užívateľské rozhranie (GUI) na tomto systéme.
   - Chcete manuálne odstrániť všetky predchádzajúce informácie o konfigurácii a začať znovu. Stáva sa to, len ak je QoS rozhranie už otvorené.
3. Dokončite kroky v Sprievodcovi úvodnou konfiguráciou. Ak sa Sprievodca úvodnou konfiguráciou nespustí, preskočte na krok 4.
4. Vyberte **Politiky**. Kliknite pravým tlačidlom na **IntServ**, **DiffServ**, alebo **Povolenie vstupu**.
5. Vyberte **Nová politika**.

Súvisiace koncepty

"Rozhrania API QoS" na strane 16
Túto tému si môžete prečítať, aby ste sa získali informácie o protokoloch, rozhraniach API a požiadavkách pre smerovač, ktorý je povolený pre protokol ReSerVation Protocol (RSVP). Aktuálne rozhrania kvality služieb (QoS) API zahŕňajú rozhrania API RAPI, rozhranie API qtoq soketu, rozhranie sendmsg() API a rozhrania monitor API.

"Diferenčný servis" na strane 2
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.

Súvisiace informácie

Správa adries a portov vášho HTTP servera (s nainštalovaným webovým serverom Apache).

Konfigurácia adresárového servera

Konfigurácie politík QoS sa dajú exportovať do adresárového servera LDAP.

Takto sa vaše riešenie kvality služby (QoS) môže stať ľahšie ovládateľným. Namiesto konfigurácie politík QoS na všetkých serveroch môžete konfiguračné údaje uložiť na lokálnom adresárovom serveri na zdieľanie pre viacero systémov. Keď na svojom serveri konfigurujete QoS po prvý raz, objaví sa sprievodca Initial Configuration. Tento sprievodca vás vyzve ku konfigurácii adresárového servera.

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

- Názov adresárového servera
- Zadajte charakteristický názov (DN), ktorým sa bude odkazovať na politiky QoS
- Rozhodnite, či sa má na vašom adresárovom serveri LDAP používať bezpečnostná schéma SSL
- Rozhodnite, či sa majú na vylepšenie vyhľadávania vašich politík na adresárovom serveri používať kľúčové slová.

Poznámka: Kerberos aktuálne nie je možné nakonfigurovať ako autentifikačnú metódu, ktorú bude server QoS používať pri prístupe k adresáru.

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

- *ALLOBJ oprávnenie a *IOSYSCFG oprávnenie
- Oprávnenie a oprávnenie pre objekt *JOBCTL k príkazom End TCP/IP (ENDTCP), Start TCP/IP (STRTCP), Start TCP/IP Server (STRTCPSVR) a End TCP/IP Server (ENDTCPSVR)
- Oprávnenie *AUDIT na konfiguráciu bezpečnostného auditu i5/OS

Ak používate iSeries Navigator, prístup k predvolenej schéme QoS už budete mať. Aktuálny súbor schémy je umiestnený vo vašom serveri v /QIBM/UserData/OS400/DirSrv. Ak však používate iný editor než iSeries Navigator, budete musieť importovať súbor LDIF opísaný v nasledovnej časti. Rovnako môžete importovať tento súbor, ak po úprave chcete znovu načítať pôvodný štandardný súbor.

Schéma QoS

Množina pravidiel, ktorej sa hovorí *schéma*, slúži na špecifikáciu tých typov objektov LDAP, ktoré budú pre server QoS platnými objektmi. Schéma obsahuje pravidlá potrebné pre QoS. Ak sa však ako server LDAP používa iný server než iSeries, tieto pravidlá je treba do servera LDAP importovať. Deje sa tak so súborom LDIF (LDAP Data Interchange Format). Súbor LDIF si môžete stiahnuť z webovej stránky iSeries LDAP. Súbor nájdete v ľavej table pod odkazom **Categories → TCP/IP Policies**. Ukážkovú schému QoS nájdete v časti o základných pojmoch LDAP.

Súvisiace koncepty

“Adresárový server” na strane 24
Svoje politiky môžete vyexportovať na adresárový server. V tejto téme sa dočítate o výhodách používania alebo nepoužívania adresárového servera, o základných pojmoch a konfigurácii protokolu Lightweight Directory Access Protocol (LDAP), ako aj o schéme kvality služieb (QoS).

“Rozlišovací názov” na strane 25
Keď chcete spravovať časť svojho adresára pozrite si *rozlišovací názov (DN)* alebo (ak sa rozhodnete) kľúčové slovo.

Adresárový server IBM pre iSeries (LDAP)

Bezpečnostná schéma SSL na vašom adresárovom serveri LDAP

“Kľúčové slová” na strane 24
Keď konfigurujete svoj adresárový server, musíte sa rozhodnúť, či sa majú s každou konfiguráciou kvality služieb (QoS) asociovať kľúčové slová.

Súvisiace informácie

Webová stránka iSeries LDAP

Poradie politík QoS

Vždy, keď máte dve politiky, ktoré sa prekrývajú, dôležité je fyzické poradie vašich politík v aplikácii iSeries Navigator.

Prekrývajúce politiky sú dve politiky, ktoré používajú rovnakého klienta, aplikáciu, plán, miestnu IP adresu, identifikátor Uniform Resource Identifier (URI), údaje o serveri, kódový bod alebo protokol. Politiky na obrazovke aplikácie iSeries Navigator sú na usporiadanom 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 aplikácii iSeries Navigator, rozviňte svoj 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**. Objaví sa okno Prekrytie politík.

Ak chcete zmeniť poradie politík na paneli, použite tieto kroky:

- Zvýraznite politiku a použite šípka hore a dole na okne, aby ste zmenili poradenie politík.
- Kliknite pravým tlačidlom na názov politiky a zvoľte **Presunúť vyššie** alebo **Presunúť nižšie**.
- Aktualizujte server kvality služieb (QoS). Na lište nástrojov môžete použiť tlačidlo **Aktualizovať server** alebo si prezrite pomoc určenú pre úlohu QoS a nájdete podrobné inštrukcie.

Súvisiace koncepty

"Konfigurácia QoS" na strane 50
Túto tému môžete použiť pri vytváraní politík diferencovanej služby, politík integrovanej služby a politík prijímania prichádzajúcej komunikácie.

"Kopírovanie existujúcej politiky" na strane 54
Namiesto vytvárania všetkých svojich politík nanovo od začiatku si môžete urobiť kópiu, resp. kópie originálnej politiky a v nich upravovať jednotlivé sekcie, ktoré sa majú od pôvodnej politiky odlišovať.

"Odstránenie problémov QoS" na strane 59
Kvalita služieb (QoS) poskytuje niekoľko metód na odstraňovanie problémov QoS.

Súvisiace úlohy

"Prístup k pomoci o QoS v programe iSeries Navigator"
Na prístup k pomoci o kvalite služby (QoS) môžete použiť program iSeries Navigator.

Spravovanie QoS

Tieto postupy môžete použiť na spravovanie už existujúcich vlastností a politík kvality služby (QoS).

Tieto témy vám poskytujú informácie o tom, kde nájdete reálne úlohy ilustrujúce spôsoby upravovania, povoľovania, zobrazovania alebo iné techniky spravovania politík. Tiež tam nájdete vysvetlenie spôsobu používania monitora QoS a zhromažďovania údajov, čo vám pomôže pri analýze vašej premávky IP prechádzajúcej cez váš server.

Súvisiace koncepty

"Konfigurácia QoS" na strane 50
Túto tému môžete použiť pri vytváraní politík diferencovanej služby, politík integrovanej služby a politík prijímania prichádzajúcej komunikácie.

Prístup k pomoci o QoS v programe iSeries Navigator

Na prístup k pomoci o kvalite služby (QoS) môžete použiť program iSeries Navigator.

Ak chcete získať prístup k pomoci o QoS, musíte použiť program iSeries Navigator:

1. V prostredí iSeries Navigator, rozviňte → **Sieť** → **Politiky IP** pre váš server.
2. Pravým tlačidlom myši kliknite na **Kvalita služby** a kliknite na **Konfigurácia**.

3. V lište ponuky kliknite na **Pomoc → Témy pomoci**. Na obrazovke sa otvorí okno s pomocou pre úlohu.

Súvisiace úlohy

"Poradie politík QoS" na strane 52
Vždy, keď máte dve politiky, ktoré sa prekrývajú, dôležité je fyzické poradie vašich politík v aplikácii iSeries Navigator.

Zálohovanie politík QoS

Pre prípad poruchy na serveri alebo výpadku prúdu by ste si mali vytvoriť zálohy svojich politík kvality služby (QoS). Vyhnete sa tak prípadnej nevyhnutnosti vytvárať ich nanovo.

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 zálohy ušetria množstvo času a práce, ktorú by si vyžiadalo vytvorenie politík celkom odznova. Toto sú všeobecné tipy, ktoré môžete použiť na zabezpečenie toho, že budete mať jednoduchý spôsob, ako nahradiť stratené súbory:

1. **Použite programy na zálohovanie a obnovu integrovaných súborových systémov.**

   Pokyny pre zálohovanie integrovaných súborových systémov nájdete v knihe *Backup and recovery*.
2. **Politiky si vytlačte.**

   Výtlačky môžete uložiť kamkoľvek, kde budú s najväčšou pravdepodobnosťou bezpečné a znovu zadajte informácie podľa potreby.
3. **Skopírujte si tieto 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 systém iSeries 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. Ako náhradný prostriedok na ochranu údajov uložených na systémovom disku môžete prípadne využiť niektorú z metód ochrany diskov.

Pri používaní servera iSeries je treba stratégiu zálohovania a obnovy plánovať.

Súvisiace informácie

Zálohovanie a obnova

Kopírovanie existujúcej politiky

Namiesto vytvárania všetkých svojich politík nanovo od začiatku si môžete urobiť kópiu, resp. kópie originálnej politiky a v nich upravovať jednotlivé sekcie, ktoré sa majú od pôvodnej politiky odlišovať.

V programe iSeries Navigator sa táto funkcia kvality služby (QoS) nazýva *New based on*. Na prístup k oknu QoS, ktoré vám umožní kopírovať politiky, musíte použiť iSeries Navigator.

Ak chcete vytvoriť kópiu už existujúcej politiky, postupujte podľa pokynov v téme **Vytvorenie novej politiky založenej na existujúcej politike**, ktorú nájdete v pomoci k programu iSeries Navigator.

Predtým, než vaše politiky začnú fungovať, musíte ich zapnúť tak, že spustíte server QoS alebo vykonáte dynamickú aktualizáciu servera. Skôr, ako ich povolíte, nezabudnite skontrolovať, či sa niektoré navzájom neprekrývajú. Ak áno, mohlo by to spôsobiť problémy.

Súvisiace úlohy

“Poradie politík QoS” na strane 52
Vždy, keď máte dve politiky, ktoré sa prekrývajú, dôležité je fyzické poradie vašich politík v aplikácii iSeries Navigator.

Upravovanie politík QoS

Vaše potreby sa časom menia, takže ak chcete udržiavať výkonnosť v optimálnom stave, musíte upravovať aj svoje politiky.

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.

Keď si svoje politiky nakonfigurujete, môžete na upravovanie konfigurácie svojich politík používať konfiguračné objekty programu iSeries Navigator. Konfiguračné objekty sú rozličné kusy, alebo časti tvoriace politiku. Keď si v programe iSeries otvoríte prostredie kvality služieb, nájdete tam adresáre označené ako klienty, aplikácie, rozvrhy, politiky, triedy služby, skokové správania a identifikátory URI. Tieto objekty vám umožňujú upraviť politiku.

Ak chcete v programe iSeries Navigator upravovať politiku, postupujte podľa pokynov na stránke Editing a quality of service (QoS) policy v pomoci k programu iSeries Navigator.

Monitorovanie QoS

Monitor kvality služieb (QoS) môžete použiť na analýzu 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, v okne QoS Configuration Server zvoľte **Server → Monitor**. Ak pravým tlačidlom kliknete na niektorú politiku a vyberiete **Monitorovať**, monitor zobrazí len informácie pre túto politiku.

Monitorovacie politiky môžete použiť nasledovnými spôsobmi:

- **Ak si želáte zobraziť údaje o aktívnych politikách v reálnom čase**

  Ak spustíte monitor, údaje v reálnom čase sa vždy zobrazia pre aktívne politiky. Nemusíte spúšťať zhromažďovanie údajov.
- **Ak si želáte zhromaždiť a uložiť údaje za určitý časový úsek**

  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 zber údajov QoS zapnutý a vlastnosti monitorovania sa zmenia, potom musíte vykonať nasledovné kroky a zabezpečiť tak, že tieto zmeny sa prejavia aj v zbere údajov.

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

Výstup monitorovania

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. Bez toho, aby boli nejako presnejšie

definované, sa merajú nasledovné polia: prijaté požiadavky, aktívne pripojenia, služby pripojení, rýchlosti pripojenia, odmietnuté požiadavky, vnútroprofilové pakety, vnútroprofilové bity, mimoprofilové bity, celkový počet bitov, celkový počet paketov a celkový počet 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. Ukážky spôsobov využitia monitorovania v politikách QoS nájdete v ktoromkoľvek scenári QoS.

Politiky diferencovanej služby

Tabuľka 4. Politiky diferencovanej služby

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.
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 obsahovať: • 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 integrovanej služby (riadený objem)

Politiky IntServ za v monitore nezobrazujú, pokým sú aplikácie spustené a vyhradené rezervácie prostriedkov v platnosti. Ak vaše politiky IntServ majú viac ako jednu rezerváciu, v monitore uvidíte viac položiek.

Tabuľka 5. Politiky integrovanej služby (riadený objem)

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.
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 integrovanej služby (zaručenej)

Politiky IntServ za v monitore nezobrazujú, pokým sú aplikácie spustené a vyhradené rezervácie prostriedkov v platnosti. Ak vaše politiky IntServ majú viac ako jednu rezerváciu, v monitore uvidíte viac položiek.

Tabuľka 6. Politiky integrovanej služby (zaručenej)

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.

Tabuľka 6. Politiky integrovanej služby (zaručenej) (pokračovanie)

Pole	Popis
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 komunikácie smerom dnu

Tabuľka 7. Politiky povolenia komunikácie smerom dnu

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 prípustná rýchlosť, pri 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.

Tabuľka 7. Politiky povolenia komunikácie smerom dnu (pokračovanie)

Pole	Popis
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.
Identifikátor Uniform Resource Identifier (URI)	Identita preverovaného URI.

Súvisiace koncepty

"Scenár: Obmedzenie prevádzky prehliadača" na strane 27
Kvalitu služieb (QoS) môžete využiť pri riadení výkonu komunikačnej prevádzky. Použite politiku diferencovaných služieb buď na obmedzenie, alebo rozšírenie výkonu aplikácie v rámci vašej siete.

"Scenár: Bezpečné a predpovedateľné výsledky (VPN a QoS)" na strane 31
Aj vtedy, ak používate virtuálnu súkromnú sieť (VPN), môžete vytvárať politiky kvality služby (QoS). Tento príklad vám ukazuje spoločné použitie oboch.

"Scenár: Obmedzenie prichádzajúcich pripojení" na strane 35
Ak potrebujete kontrolovať požiadavky na prichádzajúce pripojenia uskutočnené na vašom serveri, použite politiku prijatia vstupov.

"Scenár: Predvídateľná prevádzka B2B" na strane 37
Ak potrebujete predpovedateľné doručenie a zároveň potrebujete vyžadovať rezerváciu, použijete taktiež politiku integrovaných služieb. Tento príklad ilustruje službu riadeného zaťaženia.

"Scenár: Dedikované doručenie (IP telefónia)" na strane 41
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.

"Scenáre" na strane 27
Tieto scenáre politík kvality služby (QoS) vám môžu pomôcť porozumieť, prečo a ako treba QoS používať.

"Monitorovanie serverových transakcií" na strane 62
Pomocou monitora kvality služieb (QoS) si môžete overiť, či politiky QoS fungujú podľa vašej predstavy.

"Scenár: Monitorovanie aktuálnych sieťových štatistík" na strane 45
Sprievodcovia vás vyzvú, aby ste nastavili výkonové limity. Nie je možné odporúčať nijaké konkrétne hodnoty, pretože tie sa zakladajú na individuálnych požiadavkách konkrétnych sietí.

Odstránenie problémov QoS

Kvalita služieb (QoS) poskytuje niekoľko metód na odstraňovanie problémov QoS.

Sledovanie komunikácie

Váš server poskytuje sledovanie komunikácií na zbieranie údajov o vašej komunikačnej linke, akou je rozhranie lokálnej siete (LAN), alebo rozšírenej siete (WAN). Priemerný užívateľ by nemusel porozumieť celému obsahu údajov o sledovaní. Vy však môžete použiť záznamy zo sledovania pri rozhodovaní, či medzi dvoma bodmi v sieti došlo k výmene údajov.

Povoliť QoS v serveri

Ak sa server QoS nespustí, prvú vec, ktorú musíte skontrolovať je, či je v serveri povolené QoS. Keď prvýkrát konfigurujete svoje politiky Sprievodca úvodnou konfiguráciou automaticky povolí v serveri QoS. 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 aplikácii iSeries Navigator, rozviňte svoj server → **Sieť** → **Politiky IP**.
2. Kliknite pravým tlačidlom na **Kvalitu služieb** a zvoľte **Konfiguráciu**.
3. Po zobrazení rozhrania QoS pravým tlačidlom kliknite na **QoS** a vyberte **Vlastnosti**.
4. Na strane vlastností QoS skontrolujte, či je vybraté **Povoliť QoS**.

Súvisiace koncepty

Sledovanie komunikácie

Súvisiace úlohy

"Poradie politík QoS" na strane 52
Vždy, keď máte dve politiky, ktoré sa prekrývajú, dôležité je fyzické poradie vašich politík v aplikácii iSeries Navigator.

Žurnálovanie politík QoS

Kvalita služieb (QoS) obsahuje aj funkciu žurnálovania. Žurnálovanie vám umožňuje sledovať činnosť politiky QoS - napríklad čas, kedy bola politika pridaná, odstránená alebo zmenená.

Žurnálovanie vytvára protokol činnosti politiky vtedy, ak máte túto funkciu zapnutú. Pomáha vám to odladiť a zbadať, kde politiky nepracujú podľa predstáv. Napríklad si nastavíte politiku tak, aby fungovala od 9.00 do 16.00 h. Potom si môžete v žurnálovom protokole overiť, či bola politika skutočne o 9.00 pridaná a o 16.00 odstránená.

Ak je žurnálovanie zapnuté, žurnálové vstupy sú generované kedykoľvek je politika pridaná, odstránená, alebo modifikovaná. Pri používaní žurnálu vytvárate na serveri iSeries obvyklý súbor. 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. Na spustenie alebo zastavenie žurnálovania používajte program iSeries Navigator. Ak chcete vidieť protokoly žurnálov, musíte použiť rozhranie založené na znakoch.

Ak chcete spustiť alebo zastaviť žurnálovanie, postupujte podľa týchto pokynov:

1. V programe iSeries Navigator, rozviňte položky → **Sieť** → **Politiky IP** prislúchajúce vášmu serveru.
2. Pravým tlačidlom myši kliknite na **Kvalita služby** a zvoľte **Konfigurácia**.
3. Kliknite pravým tlačidlom na **QoS** a vyberte **Vlastnosti**.
4. Vyberte rámček **Spustiť žurnálovanie**, ak chcete spustiť žurnálovanie.
5. Ak chcete žurnálovanie vypnúť, zaškrtnutie tohto políčka zrušte.

Poznámka: Ak bol server spustený ešte predtým, než ste ukončili horeuvedené kroky, musíte ho teraz zastaviť a reštartovať. Po zapnutí žurnálovania je možné ho aktivovať dvoma spôsobmi. Môžete zastaviť a reštartovať server, alebo vykonať aktualizáciu servera. Bez ohľadu na to, ktorý spôsob si vyberiete, server si najskôr prečíta súbor policy.conf a vyhľadá si atribút žurnálovania.

Zobraziť záznamy žurnálu na monitor

Na zobrazenie záznamov žurnálu postupujte podľa týchto krokov:

1. Pri výzve príkazu zadajte DSPJRN JRN(QUSRSYS/QQOS).
2. Vyberte voľbu 5 v zázname žurnálu, ktorý chcete zobraziť.

Zobraziť záznamy žurnálu 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 kopírovať záznamy žurnálu kvality služieb (QoS) 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). Nasledujúci reťazec je príkladom príkazu CRTDUPOBJ:
   - CRTDUPOBJ OBJ(QADSPJR4) FROMLIB(Qsys) OBJTYPE(*FILE) TOLIB(*userlib*) NEWOBj(*userfile*)
2. Použite príkaz Zobraziť žurnál (DSPJRN) na kopírovanie položiek zo žurnálu QUSRSYS/QQOS do výstupného súboru vytvoreného v predchádzajúcom kroku. Ak sa pokúsite kopírovať príkaz DSPJRN do výstupného súboru, ktorý neexistuje, systém vám vytvorí súbor, ale tento súbor neobsahuje správne popisy polí.
   - DSPJRN JRN(QUSRSYS/QQOS) JRNCDE((M)) ENTTYP(MP) CMTCYCID(*ALL) OUTPUT(*OUTFILE) OUTFILFMT(*TYPE4) OUTFILE(*userlib*/*userfile*)
   - DSPF FILE(*userlib*/*userfile*)

Protokolovanie úloh servera QoS

Ak sa pri využívaní politík vašej kvality služby (QoS) vyskytnú problémy, analyzujte protokoly úloh servera iSeries. Protokol úlohy obsahuje chybové hlásenia a ďalšie informácie týkajúce sa QoS.

V podsystéme QSYSWRK je spustená iba jedna úloha QoS, QTOQSRVR. Staré i aktuálne protokoly úloh servera QoS si môžete prezerať z prostredia programu iSeries Navigator.

Ak si chcete prezrieť protokol, postupujte podľa týchto pokynov:

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

Otvorí sa okno, prostredníctvom ktorého môžete s úlohou pracovať.

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 príkaz Work with Spooled File (WRKSPLF QTCP) a vyhľadajte protokol QTOQSRVR.

Vyhľadanie chyby v pracovnom spoolovom súbore

Ak chcete skontrolovať pracovný spoolový súbor a vyhľadať v ňom prípadnú chybu, postupujte podľa týchto pokynov:

1. V rozhraní príkazového riadka zadajte príkaz WRKSPLF QTCP a stlačte kláves Enter. Otvorí sa panel Work with All Spooled Files.
2. V stĺpci Užívateľské údaje vyhľadajte QTOQSRVR, kde nájdete chyby, ktoré sa špecificky týkajú servera QoS.
3. V riadku, ktorý chcete zobraziť, zvoľte **voľbu 5**. Prečítajte si tieto informácie a poznamenajte si ID správy, ktorá vysvetľuje problém. Napríklad TCP920C.
4. Dvakrát stlačte Exit. Vrátite sa tak do hlavnej ponuky.
5. V rozhraní príkazového riadka zadajte príkaz WRKMSGF a stlačte kláves Enter.
6. V paneli Work with Message File zadajte nasledovné informácie a stlačte kláves Enter.

   ```
   Súbor správ: QTCPMSG
   Knižnica: *LIBL
   ```
7. V paneli Work with Message File zvoľte **voľbu 5** a stlačte kláves Enter; zobrazí sa súbor správ, ktorý chcete vidieť.
8. V paneli Display Message Descriptions zadajte nasledovné informácie: Position to: *Zadajte ID svojej správy (musí byť vyššie ako 3) a stlačte kláves Enter*. Napríklad TCP920C.
9. Na požadovanom ID správy zvoľte **voľbu 5** a stlačte kláves Enter.

10. V paneli Select message details to display zvoľte **voľbu 30 (Všetky uvedené)** a stlačte kláves Enter.
    Objaví sa podrobný popis správy.

Monitorovanie serverových transakcií

Pomocou monitora kvality služieb (QoS) si môžete overiť, či politiky QoS fungujú podľa vašej predstavy.

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. Na pomoc pri určovaní hodnôt, ktoré sú pre vás najvhodnejšie, môžete monitor prípadne použiť ešte skôr, než vôbec spustíte akékoľvek konkrétne politiky.

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 ukážku politiky monitorovania, ktorá identifikuje správanie vašej aktuálnej komunikačnej prevádzky.

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 v monitore objavujú, avšak podľa všetkého komunikáciu nijako neovplyvňujú, preverte si situáciu nasledovným spôsobom:

- Ak je politikou filtrovanie podľa identifikátora Uniform Resource Identifier (URI), skontrolujte, či je povolený a správne nakonfigurovaný akcelerátor Fast Response Cache Accelerator (FRCA). Skôr, než nastavíte politiku pre prichádzajúcu komunikáciu, ktorá používa identifikátory URI, musíte sa postarať o to, aby aplikačný port priradený tomuto URI zodpovedal inštrukcii listen povolenej pre FRCA v konfigurácii webového servera Apache.
- Skontrolujte si rozvrh politiky. Je možné, že výsledky hľadáte v čase, keď politika nie je aktívna.
- Skontrolujte, či je správne číslo portu.
- Skontrolujte, či je správna IP adresa.

Niekoľko ukážok výstupov monitora nájdete v scenároch QoS, prípadne si pozrite všetky monitorovacie polia v monitorovaní.

Súvisiace koncepty

“Plánovanie QoS” na strane 46
Najdôležitejší krok na splnenie kvality služieb (QoS) je plánovanie. Kvôli očakávaným výsledkom musíte posúdiť svoje sieťové zariadenia a monitorovať sieťovú prevádzku.

“Scenáre” na strane 27
Tieto scenáre politík kvality služby (QoS) vám môžu pomôcť porozumieť, prečo a ako treba QoS používať.

Súvisiaci odkaz

“Monitorovanie QoS” na strane 55
Monitor kvality služieb (QoS) môžete použiť na analýzu prevádzky IP cez server.

Súvisiace informácie

Správa adries a portov vášho HTTP servera (s nainštalovaným webovým serverom Apache)

Sledovanie aplikácií TCP

Sledovanie kvality služieb (QoS) môžete použiť na prácu s funkciami sledovania a na zobrazenie aktuálnej vyrovnávacej pamäte sledovania.

Na spustenie sledovania v serveri napíšte TRCTCPAPP (príkaz Sledovať aplikáciu protokolu TCP/IP) z rozhrania príkazového riadka.

Tu je príklad výberu sledovania, ktoré má byť vykonané:

```
Aplikácia protokolu TCP/IP...........> *QOS
Nastavenie voľby sledovania.........> *ON
Maximálny úložný priestor na sledovanie....> *APP
Sledovať celú akciu.............> *WRAP
Zoznamy argumentov..............> 'lvl=4'
Typ sledovania QoS..............> *ALL
```

Nasledujúca tabuľka predstavuje možné parametre, ktoré môžu byť použité pri sledovaní. Ak sa nastavenie neobjaví v rozhraní založenom na znakoch, musíte ho zadať v príkaze. Napríklad , TRCTCPAPP APP(*QOS) MAXSTG(1000) TRCFULL(*STOPTRC) ARGLIST('l=4 c=i').

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

Maximálny úložný priestor na 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.

Sledovať celú akciu

***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.

Zoznamy 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 protokolov sú zahrnuté. 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. Systémová chyba sa môže napríklad objaviť, ak sa znižuje systémová pamäť alebo ak váš systém nedokáže komunikovať s protokolom TCP/IP. Toto je predvolená úroveň.

Úroveň 2: Chyby medzi objektmi (OBJERR)
Protokoluje chyby, ktoré sa objavia v kóde servera QoS. Chyba objektu sa môže napríklad objaviť, pretože serverová operácia zaznamená neočakávaný výsledok. 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 zo 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

Špecifikujte 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 potrebujete pomoc pri interpretácii výstupu sledovania, prečítajte si príklad výstupu sledovania na stránke výstupu sledovania, ktorá obsahuje vzorový výstup s komentármi, ktoré vám majú pomôcť interpretovať jeho význam. Funkciu TRCTCPAPP zvyčajne používa služba, tak ak máte problémy pri čítaní výstupu, mohli by ste kontaktovať svojho zástupcu pre služby.

Súvisiaci odkaz

Opis príkazu TRCTCPAPP (Trace TCP/IP Application)

Príklady: Prečítajte si 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 najdôležitejšou udalosťou, ktorej sa má venovať pozornosť tá, či bolo spojenie protokolu ReSerVation Protocol (RSVP) odmietnuté, pretože politika pre to spojenie nebola nájdená. Tu je príklad správy o úspechu:

```
12/15 11:36:14 [336,80] TRCE :.......rpapi_getPolicyData: Nájdený názov akcie vreStnl_kraMoNlCvreStnl for
flow[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: Neschopný nájsť 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: Installing rule = timed_42ring.
01/11 14:07:52 [376,57] EVNT :.......create_tcp_resv: Žiadna hodnota v konfiguračnom súbore pre DiffServInProfilePeakRat
01/11 14:07:52 [376,57] TRCE :.......create_tcp_resv: Create resv - bRate: 537395 5722SS1 V5R1M0 010525 TRCTCPAPP Výstup
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
```

Môžete mať aj správy ukazujúce, že tagy v súbore konfigurácie politiky boli nesprávne. Tu je niekoľko vzorových správ:

```
12/15 11:36:14 [336,80] TRCE :.......rpapi_getPolicyData: Neznámy atribúr %s v ServicePolicy-Ignoring.
12/15 11:36:14 [336,80] TRCE :.......rpapi_getPolicyData: Neznámy atribút %s v Priorite Ignorovanie mapovania.
```

Poznámka: Znamienko % je premenná, ktorá predstavuje nerozoznaný tag.

Informácie týkajúce sa QoS

Sú tu uvedené publikácie IBM Redbooks (vo formáte PDF), webové stránky, a témy informačného centra, ktoré sa týkajú témy kvality služieb (QoS). Je možné prezerať alebo tlačiť všetky súbory vo formáte PDF.

Požiadavka QoS o komentáre (RFCs)

Dokumenty RFC (Requests for Comments) sú napísané definície štandardov protokolov a navrhovaných štandardov používaných v sieti Internet. Tieto dokumenty RFC môžu byť užitočné na porozumenie QoS a jeho súvisiacich funkcií:

- **RFC 1349.**
  Toto RFC sa zaoberá novou definíciou typu oktetového poľa služieb v hlavičke paketu IP.
- **RFC 2205.**
  Toto RFC vysvetľuje definíciu protokolu ReSerVation Protocol (RSVP).
- **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.

Na prezeranie skôr uvedených dokumentov RFC navštívte odkaz RFC Index Search Engine umiestneného v odkaze RFC Editor webovej stránky.

IBM Redbooks

- iSeries Siete IP: Dynamické! (okolo 16 589 KB). Toto je najnovší redbook o budovaní sietí IP. Uvádza, ako navrhnúť samokonfigurujúcu sa sieť IP, odolnú voči chybám a s efektívnou prevádzkou. Okrem mnohých iných funkcií vysvetľuje teóriu QoS a jej implementáciu v aplikácii iSeries. Tiež v nej nájdete viac scenárov s postupnými pokynmi na ich vyriešenie.

- Protokol TCP/IP Viac skvelých vecí ako kedykoľvek doteraz (okolo 10 035 KB). Tento návod poskytuje vzorové scenáre, ktoré demonštrujú bežné riešenia s príkladmi konfigurácií. Informácie v tomto manuáli vám

pomáhajú plánovať, inštalovať, prispôsobiť, konfigurovať a odstraňovať problémy s protokolom TCP/IP vo vašom serveri iSeries. Ešte špecificky nezahŕňa QoS, ale prechádza cez informácie adresárového servera LDAP.

- Prehľad výukového programu a technických parametrov protokolu TCP/IP  (okolo 7885 KB). Tento návod poskytuje úvod, ako aj odkaz na sadu protokolov a aplikácií Transmission Control Protocol/Internet Protocol (TCP/IP). QoS nájdete v *časti 3. Rozšírené základné pojmy a nové technológie* v kapitole 22.

Ostatné informácie

- Adresárové služby (LDAP). Táto téma zahŕňa základné pojmy o adresárovom serveri, konfiguráciu, administráciu a odstraňovanie problémov. Téma adresárových služieb tiež poskytuje doplnkové prostriedky na konfiguráciu vášho adresárového servera.
- Zistenie narušenia. Táto téma sa zaoberá zhromažďovaním informácií o pokusoch neautorizovane pristúpiť a zaútočiť na sieť TCP/IP. Bezpečnostní správcovia môžu analyzovať auditovacie záznamy, ktoré poskytuje zistenie narušenia, aby zabezpečili sieť iSeries pred týmito typmi útokov.

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. Tým, že vám bol tento dokument poskytnutý, nezískavate na tieto patenty nijaké práva. 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 miestnym zákonom: SPOLOČNOSŤ INTERNATIONAL BUSINESS MACHINES POSKYTUJE TÚTO PUBLIKÁCIU "TAK AKO JE", BEZ AKÝCHKOĽVEK VÝSLOVNÝCH ALEBO MLČKY PREDPOKLADANÝCH ZÁRUK, VRÁTANE, ALE BEZ OBMEDZENIA NA ZÁRUKY NEPORUŠENIA PRÁV, PREDAJNOSTI ALEBO VHODNOSTI NA KONKRÉTNY ÚČEL. Niektoré štáty nepovoľujú zrieknutie sa výslovných ani mlčky predpokladaných záruk v určitých operáciách, preto sa na vás toto vyhlásenie nemusí vzťahovať.

Tento dokument môže obsahovať technické nepresnosti alebo tlačové chyby. Informácie uvedené v tomto dokumente podliehajú priebežným zmenám; tieto zmeny budú zapracované do nových vydaní. IBM môže kedykoľvek bez ohlásenia urobiť vylepšenia a/alebo zmeny v produktoch alebo programoch popísaných v tejto publikácii.

Akékoľvek odkazy v tejto publikácii na iné webové stránky, než stránky firmy IBM, sú poskytované len pre vaše pohodlie a v žiadnom prípade neslúžia ako súhlas s týmito webovými stránkami. Materiály, uvedené na týchto webových stránkach, nie sú súčasťou materiálov tohto produktu IBM a ich použitie je na vaše vlastné riziko.

Spoločnosť IBM môže ktorúkoľvek z vami poskytnutých informácií použiť alebo distribuovať spôsobom, ktorý považuje za správny, bez toho, aby jej z toho vyplynul akýkoľvek záväzok voči vám.

Držitelia licencií tohto programu, ktorí si želajú mať informácie o tomto programe kvôli povoleniu: (i) výmeny informácií medzi nezávisle vytvorenými programami a inými programami (vrátane tohto programu) a (ii) spoločného používania vymenených informácií by mali kontaktovať:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N

Rochester, MN 55901
U.S.A.

Takéto informácie môžu byť v niektorých prípadoch dostupné až po zaplatení príslušného poplatku.

Licenčný program spomínaný v tomto dokumente a všetky pre tento program dostupné licenčné materiály poskytuje spoločnosť IBM podľa podmienok zmluvy IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code alebo ľubovoľnej 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 na všeobecne dostupných systémoch. Okrem toho, niektoré výsledky boli odhadnuté extrapoláciou. Aktuálne výsledky môžu byť iné. Užívatelia tohto dokumentu by si mali overiť použiteľnosť týchto údajov pre svoje špecifické prostredie.

Všetky vyhlásenia týkajúce sa budúceho smerovania alebo zámerov spoločnosti IBM môžu byť zmenené alebo zrušené bez oznámenia a reprezentujú len ciele a zámery spoločnosti.

Informácie týkajúce sa produktov iných spoločností ako IBM boli získané od dodávateľov týchto produktov, z ich publikovaných oznámení alebo iných verejne prístupných zdrojov. Spoločnosť IBM tieto produkty netestovala a nemôže potvrdiť presnosť ich výkonu, kompatibilitu ani iné parametre týkajúce sa produktov nepochádzajúcich od IBM. Otázky o schopnostiach produktov nepochádzajúcich od IBM adresujte dodávateľom týchto produktov.

Tieto informácie obsahujú príklady údajov a hlásení používaných v každodenných obchodných operáciách. Kvôli čo najúplnejšiemu vysvetleniu obsahujú príklady konkrétne mená jednotlivcov, názvy spoločností, značiek a výrobkov. Všetky tieto názvy sú fiktívne a akákoľvek ich podobnosť s názvami a adresami používanými skutočným obchodným podnikom je úplne náhodná.

LICENCIA NA AUTORSKÉ PRÁVA:

Tieto informácie obsahujú vzorové aplikačné programy v zdrojovom jazyku, ktoré ilustrujú programovacie techniky na rozličných operačných platformách. Tieto vzorové programy môžete kopírovať, upravovať a distribuovať v akejkoľvek forme bez zaplatenia poplatkov spoločnosti IBM za účelom vývoja, používania, marketingu alebo distribuovania aplikačných programov, vyhovujúcich aplikačnému programovému rozhraniu pre operačnú platformu, pre ktorú boli tieto vzorové programy napísané. Tieto príklady neboli riadne testované za všetkých podmienok. Spoločnosť IBM preto nemôže zaručiť alebo potvrdiť spoľahlivosť, opraviteľnosť alebo fungovanie týchto programov.

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. _zadajte rok alebo roky_. Všetky práva vyhradené.

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

Informácia o programovom rozhraní

Táto publikácia nazvaná Kvalita služby dokumentuje plánované programové rozhrania, ktoré zákazníkovi umožnia za účelom získania služieb operačného systému IBM i5/OS písať vlastné programy.

Ochranné známky

Nasledujúce pojmy sú ochranné známky spoločnosti International Business Machines v USA alebo iných krajinách:

| IBM
| IBM (logo)
| iSeries
| i5/OS
| Redbooks

Ostatné názvy spoločnosti, produktov alebo služieb môžu byť ochrannými alebo servisnými známkami iných subjektov.

Podmienky

Povolenia na používanie týchto publikácií sa udeľujú za nasledovných podmienok.

Osobné použitie: Tieto publikácie môžete kopírovať len na svoje osobné nekomerčné použitie pod podmienkou, že dodržíte všetky oznámenia o vlastníckych právach. V žiadnom prípade nemôžete tieto publikácie ani žiadnu ich časť distribuovať, prezentovať alebo z nich vytvárať odvodené práce, bez výslovného súhlasu spoločnosti IBM.

Komerčné použitie: V rámci vášho podniku môžete kopírovať, distribuovať a prezentovať tieto publikácie len za predpokladu, že dodržíte všetky oznámenia o vlastníckych právach. V žiadnom prípade nemôžete tieto publikácie ani žiadnu ich časť distribuovať, prezentovať alebo z nich vytvárať odvodené práce mimo vášho podniku bez výslovného súhlasu spoločnosti IBM.

Okrem povolení výslovne vyjadrených v tomto dokumente, nie sú pre uvedené publikácie alebo informácie, údaje, softvér alebo iné duševné vlastníctvo v nich obsiahnuté, udelené žiadne iné výslovné alebo mlčky predpokladané povolenia, oprávnenia alebo práva.

Spoločnosť IBM si vyhradzuje právo vypovedať oprávnenia uvádzané v tomto dokumente kedykoľvek, ak usúdi, že používanie týchto publikácií poškodzuje jej záujmy alebo ak spoločnosť IBM zistí, že vyššie uvedené inštrukcie nie sú náležite 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 NEPOSKYTUJE ŽIADNU ZÁRUKU NA OBSAH TÝCHTO PUBLIKÁCIÍ. TIETO PUBLIKÁCIE SA POSKYTUJÚ ″TAK AKO SÚ″ BEZ AKÝCHKOĽVEK VÝSLOVNÝCH ALEBO MLČKY PREDPOKLADANÝCH ZÁRUK, VRÁTANE, ALE BEZ OBMEDZENIA NA ZÁRUKY NEPORUŠENIA PRÁV, PREDAJNOSTI ALEBO VHODNOSTI NA KONKRÉTNY ÚČEL.

Vytlačené v USA