System i

Lucru în reţea
QoS (Quality of Service)

Versiunea 6 Ediţia 1

System i

Lucru în reţea
QoS (Quality of Service)

Versiunea 6 Ediţia 1

Notă

Înainte de a folosi aceste informaţii şi produsul pe care îl suportă, citiţi informaţiile din “Observaţii”, la pagina 67.

Această ediţie se aplică versiunii 6, ediţia 1, modificarea 0 a IBM i5/OS (număr de produs 5761-SS1) şi tuturor ediţiilor şi modificărilor care vor urma până când nu se indică altfel în ediţii noi. Această versiune nu rulează pe toate modelele RISC şi nici pe modelele CISC.

Cuprins

Calitatea serviciului

Soluţia QoS din i5/OS permite politicilor să ceară prioritate în reţea şi lungime de bandă pentru aplicaţii TCP/IP în toată reţeaua.

Tot traficul din reţea primeşte prioritate egală. Traficul de browser necritic este considerat la fel de important ca şi aplicaţiile de afaceri critice. Dacă directorul dumneavoastră executiv (CEO) face o prezentare folosind o aplicaţie audio/video, prioritatea pachetului IP devine o problemă. Este critic ca, în timpul prezentării, această aplicaţie să primească performanţe mai bune decât alte aplicaţii.

Prioritatea de pachet vă este importantă dacă trimiteţi aplicaţii care necesită rezultate previzibile şi pe care să vă puteţi baza, cum este multimedia. Politicile QoS pot gestiona priorităţi de pachet şi de asemenea pot limita datele care ies din sistem, gestiona cererile de conexiune şi pot controla încărcarea sistemului. Serverul QoS trebuie să fie activ pentru a activa politica de detectare a intruziunilor.

Fişierul PDF pentru Calitatea serviciului (QoS)

Puteţi vizualiza şi tipări un fişier PDF cu aceste informaţii.

Pentru a vedea sau a descărca o versiune PDF, selectaţi Calitate servicii (aproximativ 525 KB).

Salvarea fişierelor PDF

Pentru a salva un PDF pe staţia de lucru pentru vizualizare sau tipărire:

1. Faceţi clic dreapta pe legătura PDF din browser-ul dumneavoastră.
2. Faceţi clic pe opţiunea care salvează fişierul PDF local.
3. Navigaţi până la directorul unde vreţi să salvaţi fişierul PDF.
4. Faceţi clic pe **Salvare**.

Descărcarea programului Adobe Reader

Aveţi nevoie ca Adobe Reader să fie instalat în sistemul dumneavoastră pentru a vizualiza sau tipări aceste PDF-uri.

Puteţi descărca o copie gratuită de pe situl web Adobe (www.adobe.com/products/acrobat/readstep.html) .

Referinţe înrudite

"Informaţii înrudite pentru Calitatea serviciului" la pagina 65

RFC-uri QoS, publicaţii IBM Redbooks, şi alte colecţii de subiecte din centrul de informare conţin informaţii care sunt înrudite cu colecţia de subiecte Calitatea serviciului. Puteţi vedea sau tipări oricare din fişierele PDF.

Concepte

Înainte de a folosi QoS, este nevoie să învăţaţi terminologia de bază şi conceptele QoS. Aceste concepte vă ajută să determinaţi dacă serviciul vă întâlneşte nevoile.

Pentru a realiza QoS, configuraţi politici cu ajutorul vrăjitorilor în Navigator System i. O *politică* este un set de reguli care desemnează o acţiune. Politica, în mod fundamental, specifică ce client, aplicaţie şi planificare (pe care le desemnaţi) trebuie să primească un anumit serviciu. Puteţi configura următoarele tipuri de politici:

- Servicii diferenţiate
- Servicii integrate
- Acces inbound

Serviciile diferenţiate şi *serviciile integrate* sunt considerate politici de lăţime de bandă ieşire. Politicile outbound limitează datele care părăsesc reţeaua şi ajută la controlarea încărcării sistemului. Ratele pe care le setaţi în cadrul unei politici outbound controlează cum şi care date sunt sau nu limitate în sistem. Ambele tipuri de politici outbound ar putea avea nevoie de un SLA (service level agreement) cu ISP-ul (Internet service provider) dumneavoastră.

Politicile *Acces inbound* controlează cererile de conexiune care ajung în reţeaua dumneavoastră de la unele surse din afară. Politicile inbound nu sunt dependente de un nivel de serviciu de la ISP-ul dumneavoastră. Pentru a vă decide de ce politică aveţi nevoie să folosiţi, evaluaţi motivele pentru care doriţi să folosiţi QoS şi consideraţi rolul sistemului dumneavoastră.

Unul din cele mai importante părţi ale realizării QoS este însuşi sistemul de operare. Nu este nevoie doar să înţelegeţi conceptele QoS, ci de asemenea să fiţi conştienţi de rolul pe care sistemul dumneavoastră de operare îl joacă în aceste concepte. Sistemul de operare i5/OS poate fi doar un client sau un server, nu poate fi un ruter. De exemplu, sistemul dumneavoastră de operare care are rolul de client poate folosi politici de servicii diferenţiate pentru a asigura că cererile de informaţii către alte sisteme au o prioritate mai înaltă în reţea. Sistemul dumneavoastră de operare cu rolul de server poate folosi o politică de acces inbound pentru a limita cererile acceptate de URI (Uniform Resource Identifier) de către server.

Concepte înrudite

“Acord la nivel de serviciu” la pagina 48
Acest subiect scoate în evidenţă unele din aspectele importante ale unui SLA (service level agreement) care ar putea afecta implementarea QoS-ului dumneavoastră. QoS este o soluţie de reţea. Pentru a obţine prioritate de reţea în afara reţelei dumneavoastră private, aţi putea avea nevoie de un SLA cu ISP-ul (Internet service provider) dumneavoastră.

Referinţe înrudite

“Informaţii înrudite pentru Calitatea serviciului” la pagina 65
RFC-uri QoS, publicaţii IBM Redbooks, şi alte colecţii de subiecte din centrul de informare conţin informaţii care sunt înrudite cu colecţia de subiecte Calitatea serviciului. Puteţi vedea sau tipări oricare din fişierele PDF.

Servicii diferenţiate

Acesta este primul tip de politică de lungime de bandă outbound pe care o puteţi crea pe sistemul dumneavoastră de operare. Serviciile diferenţiate împart traficul dumneavoastră pe clase. Pentru a realiza o politică de serviciu diferenţiat, este necesar să determinaţi cum doriţi să clasificaţi traficul dumneavoastră de reţea şi cum să trataţi diferitele clase.

Concepte înrudite

“Extensii ale API-ului QoS sendmsg()” la pagina 22
Funcţia sendmsg() este folosită pentru a trimite date, date auxiliare sau o combinaţie a acestora printr-un socket conectat sau neconectat.

“Limite găleată jeton şi lăţime de bandă” la pagina 9
Limitele găleţii jeton şi ale lăţimii de undă sunt cunoscute împreună ca limite de performanţă. Aceste limite de performanţă ajută la garantarea livrării pachetelor în politici de lăţime de bandă ieşire, servicii integrate şi diferenţiate.

“Clasa serviciului” la pagina 12
Când creaţi o politică de servicii diferenţiate sau o politică de acces inbound, creaţi, de asemenea şi folosiţi o clasă de serviciu.

“Scenariu: Limitare trafic browser” la pagina 27
Puteţi utiliza calitatea serviciului (QoS) pentru a controla performanţa traficului. Folosiţi o politică de servicii diferenţiate pentru a limita sau a extinde performanţa unei aplicaţii în reţea.

“Scenariu: Rezultate sigure şi predictibile (VPN şi QoS)” la pagina 31
Dacă folosiţi o reţea privată virtuală (VPN), puteţi crea şi politici de calitatea serviciilor.

Referinţe înrudite

“Utilizarea punctelor de cod pentru a asigna comportament per-hop” la pagina 14
QoS (Quality of service) foloseşte punctele de cod sugerate pentru a asigna comportamente per-hop traficului.

“Configurarea QoS cu vrăjitori” la pagina 50
Pentru a configura politici QoS (quality of service), este necesar să folosiţi vrăjitorii QoS aflaţi în Navigator System i.

Informaţii înrudite

Gestionarea adreselor şi porturilor pentru serverul HTTP (motorizat de Apache).

Clase prioritare: Cum să clasificaţi traficul de reţea

Serviciul diferenţiat identifică traficul de reţea drept clase. Cele mai comune clase sunt definite utilizând adrese IP client, porturi de aplicaţie, tipuri de servere, protocoale, adrese locale IP şi planificări. Tot traficul care este în concordanţă cu aceeaşi clasă este tratat în mod egal.

Pentru o clasificare mai avansată, puteţi specifica datele aplicaţiei pentru a seta niveluri diferite de serviciu pentru unele dintre aplicaţiile dumneavoastră i5/OS. Folosirea datelor de aplicaţie este opţională, dar ar putea fi de folos când doriţi să clasificaţi la un nivel mai jos. Sunt două tipuri de date de aplicaţie: jeton de aplicaţie sau URI (Uniform Resource Identifier). Dacă traficul se potriveşte cu jetonul sau URI-ul pe care l-aţi specificat în politică, politica se aplică răspunsului outbound, astfel se dă traficului outbound orice prioritate este specificată în politica de servicii diferenţiate.

Folosirea jetonului de aplicaţie cu politicile de servicii diferenţiate

Foloisrea datelor de aplicaţiei permite politicii să răspundă la parametrul specific (jeton sau prioritate) transmis de aplicaţie către sistemul de operare prin API-ul sendmsg(). Această setare este opţională. Dacă nu aveţi nevoie de acest nivel de granularitate în politicile dumneavoastră outbound, selectaţi în vrăjitor **Toate jetoanele**. Puteţi potrivi jetonul şi prioritatea unei aplicaţii cu un anumit jeton şi prioritate ce sunt setate în politica outbound. În politică, sunt două părţi pentru a seta datele aplicaţiei: jetonul şi prioritatea.

- Ce este un jeton de aplicaţie?

  Un *jeton de aplicaţie* este un şir de caractere care poate reprezenta o resursă definită, cum este myFTP. Jetonul pe care îl specificaţi în politica QoS este comparat cu jetonul furnizat de aplicaţia outbound. Aplicaţie furnizează valoarea jetonului prin API-ul sendmsg(). Dacă jetoanele se potrivesc, traficul aplicaţiei este inclus în politica de servicii diferenţiate.

  Pentru a utiliza un jeton de aplicaţie într-o politică de servicii diferenţiată, urmaţi aceşti paşi:

  1. Din fereastra de configurare QoS, faceţi clic dreapta **DiffServ** şi selectaţi **Politică nouă** . Porniţi vrăjitorul.
  2. Pe pagina Cerere de date server, selectaţi **Jeton de aplicaţie selectat**.
  3. Pentru a crea un jeton nou, apăsaţi **Nou**. Se deschide fereastra URI nou.
  4. În câmpul **Nume**, introduceţi un nume semnificativ pentru jetonul aplicaţie.
  5. În câmpul **URI**, ştergeţi (/) şi introduceţi jetonul aplicaţie (un şir de nu mai mult de 128 de caractere). De exemplu, myFTPapp, în loc de URI-ul tipic.
- Ce este o prioritate aplicaţie?

  Prioritatea aplicaţiei pe care o specificaţi este comparată cu prioritatea de aplicaţie furnizată de aplicaţia outbound. Aplicaţia furnizează valoarea de prioritate prin API-ul sendmsg(). Dacă priorităţile se potrivesc, traficul aplicaţiei este inclus în politica de servicii diferenţiate. Tot traficul definit în politica de servicii diferenţiate va primi în continuare prioritatea dată întregii politici.

Când specificaţi un jeton de aplicaţie ca tipul de date al aplicaţiei, aplicaţia care furnizează aceste informaţii sistemului de operare trebuie să fie codată în mod specific pentru a folosi API-ul sendmsg() API. Aceasta se realizează de către programatorul aplicaţiei. Documentaţia aplicaţiei ar trebui să furnizeze valori valide (jeton şi prioritate) pe care administratorul QoS le foloseşte în cadrul politicii de servicii diferenţiate. Politica de servicii diferenţiate aplică atunci prioritatea ei proprie şi clasificarea sa traficului care se potriveşte cu jetonul setat în politică. Dacă aplicaţia nu are valori care se potrivesc cu valorile setate în politică, este necesar fie să actualizaţi aplicaţia sau să folosiţi parametri de date aplicaţie diferiţi pentru politica de servicii diferenţiate.

Folosirea unui URI cu politici de servicii diferenţiate

Când creaţi o politică de servicii diferenţiate, vrăjitorul vă permite să setaţi informaţii de date sistem, aşa cum s-a discutat în secţiunea ″Folosire jeton de aplicaţie cu politici de servicii diferenţiate″. Chiar dacă acele câmpuri din vrăjitor vă promptează pentru un jeton de aplicaţie, puteţi specifica în locul lui un URI relativ. Iar, această acţiune este opţională. Dacă nu aveţi nevoie de acest nivel de granularitate în politicile dumneavoastră outbound, selectaţi în vrăjitor **Toate jetoanele**. Puteţi potrivi un URI specific setat în politica outbound.

URI-ul înrudit este de fapt un subset al unui URI absolut (similar URI-ului absolut vechi). Consideraţi acest exemplu: http://www.ibm.com/software. Segmentul *http://www.ibm.com/software* este considerat URI-ul absolut. Segmentul */software* este URI-ul înrudit. Toate valorile de URI-uri înrudite trebuie să înceapă cu un slash înainte (/). Următoarele segmente sunt exemple de URI-uri înrudite valide:

- /piaţă/zarzavaturi#D5
- /software
- /piaţă/zarzavaturi?q=verde

Înainte de a seta o politică de servicii diferenţiate care foloseşte URI-uri, trebuie să vă asiguraţi că portul de aplicaţie asignat URI-ului se potriveşte cu directiva Listen activată pentru FRCA (fast response cache accelerator) în configuraţia Apache Web Server. Pentru a modifica sau vizualiza portul serverului dumneavoastră HTTP,

consultaţiGestionare adrese şi porturi pentru Server HTTP (motorizat de Apache)  .

FRCA va identifica URI-ul pentru fiecare răspuns HTTP outbound. El compară URI-ul în legătură cu răspunsul ieşire cu URI-ul definit în fiecare politică de servicii diferenţiate. Prima politică cu un şir jeton (URI) care se potriveşte cel mai bine cu URI-ul identificat de FRCA este aplicată tuturor răspunsurilor pentru URI.

Concepte înrudite

“Extensii ale API-ului QoS sendmsg()” la pagina 22
Funcţia sendmsg() este folosită pentru a trimite date, date auxiliare sau o combinaţie a acestora printr-un socket conectat sau neconectat.

Setarea priorităţilor: Cum se manipulează clasele

După ce traficul este clasificat, serviciul diferenţiat necesită de asemenea un comportament per-hop pentru a defini cum să fie tratat traficul.

Sistemul de operare foloseşte biţi în antetul IP pentru a identifica un nivel de serviciu al unui pachet IP. Ruterele şi switch-urile alocă resursele lor pe baza informaţiilor per-hop din câmpul tip de octet serviciu al antetului (TOS) IP. Câmpul octet Tip serviciu a fost redefinit în sistemele de operare V5R1, în RFC (Request for Comments) 1349 şi în sistemul de operare OS/400 Un *comportament per-hop* este comportamentul de înaintare pe care un pachet îl primeşte la un nod al reţelei. Este reprezentat printr-o valoare cunoscută ca *punct de cod*. Pachetele pot fi marcate fie la sistemul de operare, fie în alte părţi ale reţelei, cum ar fi un ruter. Pentru ca un pachet să reţină serviciul cerut, fiecare nod al reţelei trebuie să poată recunoaşte Servicii diferenţiate. Astfel, echipamentul trebuie să poată impune comportamente per-hop. Pentru a impune tratament de comportament per-hop, nodul de reţea trebuie să poată utiliza planificarea cozii şi gestionarea priorităţii outbound. Consultaţi “Condiţionări de trafic” la pagina 5 pentru informaţii suplimentare despre ce înseamnă a putea recunoaşte Servicii diferenţiate.

Dacă pachetul dumneavoastră trece printr-un ruter sau switch care nu poate recunoaşte Servicii diferenţiate, acesta va pierde nivelul de serviciu la acel ruter. Pachetul mai este tratat, dar ar putea suferi o întârziere neaşteptată. În sistemul dumneavoastră, puteţi folosi punctele de cod de comportament per-hop predefinite sau vă puteţi defini propriile puncte de cod. Se poate să nu puteţi crea propriile puncte de cod pentru a fi utilizate în afara reţelei private. Dacă nu ştiţi ce puncte de cod să alocaţi, consultaţi “Utilizarea punctelor de cod pentru a asigna comportament per-hop” la pagina 14.

Nu precum serviciile integrate, traficul de servicii diferenţiate nu cere o rezervare sau un comportament per-flux. Tot traficul situat în aceeaşi clasă este tratat în mod egal.

Serviciul diferenţiat este folosit de asemenea pentru a accelera traficul care iese din sistem. Aceasta înseamnă că sistemul dumneavoastră foloseşte servicii diferenţiate pentru a limita performanţa. Limitarea unei aplicaţii mai puţin critice permite unei aplicaţii critice să iasă prima din reţeaua dumneavoastră privată. Când creaţi o clasă de serviciu pentru această politică, sunteţi rugat să setaţi diverse limite în sistemul dumneavoastră. Limitele de performanţă includ dimensiuni de găleţi pentru jetoane, limite pentru rate de vârf şi limite de rate medii. Subiectele de ajutor din funcţia QoS (quality of service) Navigator System i vă oferă informaţii mai detaliate despre aceste limite.

Condiţionări de trafic

Pentru a utiliza politici QoS, echipamentele de reţea (precum ruterele şi switch-urile) trebuie sa fie capabile de condiţionare de trafic. Condiţionatoarele de trafic se referă la utilitare de tip clasifier, meter, marker, shaper şi dropper.

Dacă echipamentul de reţea are toate condiţionările de trafic, atunci se consideră că recunoaşte Serviciile diferenţiate.

Notă: Aceste cerinţe hardware nu sunt specifice produselor System i. Nu puteţi vedea aceşti termeni folosiţi în interfaţa QoS, deoarece sistemul nu poate controla hardware extern. În afara unei reţele private, hardware-ul trebuie să aibă abilitatea de a trata cerinţe QoS generale. Verificaţi manualele specifice echipamentelor pentru a vă asigura că pot trata cerinţe de serviciu diferenţiat. Este nevoie să studiaţi cu atenţie conceptele generale QoS şi cerinţele preliminare înainte de a implementa politicile.

Următoarea figură arată o reprezentare logică despre cum lucrează condiţionările de trafic.

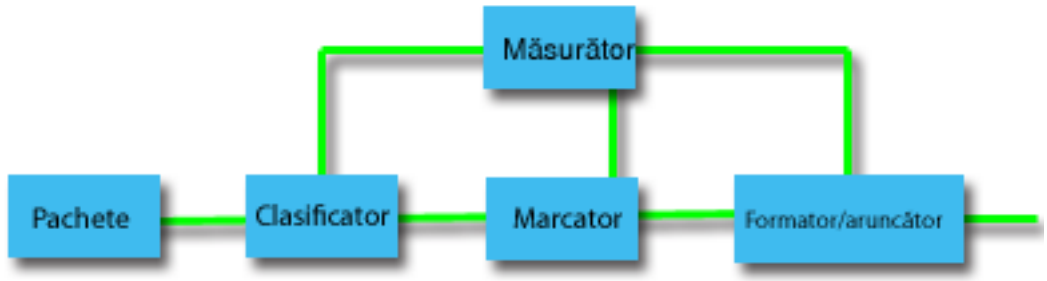


Figura 1. Condiţionări de trafic

Următoarele informaţii descriu fiecare condiţionare de trafic cu detalii suplimentare:

Clasificatori

Clasificatorii de pachete selectează pachete din fluxul de trafic, pe baza conţinutului din antetul IP al pachetului. Sistemul de operare i5/OS defineşte două tipuri de clasificatori. Agregarea comportamentală clasifică pachetele exclusiv pe baza punctului de cod Servicii diferenţiate. Clasificatorul pe mai multe câmpuri selectează pachete pe baza valorii combinaţiei unuia sau mai multor câmpuri antet, cum sunt adresa sursă, adresa destinaţie, câmpul Serviciu Diferenţiat, ID protocol, port sursă, URI (Uniform Resource Identifier), tip server şi număr port destinaţie.

Măsurători

Măsurătorii de trafic măsoară dacă pachetele IP, trimise de către clasificator, corespund profilului de antet IP al traficului. Informaţiile din antetul IP este determinată de valorile pe care le setaţi în politica QoS pentru acest trafic. Un măsurător transmite informaţiile la alte funcţii condiţionale pentru a declanşa o acţiune. Acţiunea este declanşată pentru fiecare pachet, indiferent dacă este în-profil sau în-afara-profilului.

Marcatori

Marcatorii de pachet setează câmpul Servicii diferenţiate. Marcatorul poate fi configurat pentru a marca toate pachetele la un singur punct de cod sau la un set de puncte de cod care este folosit pentru a selecta un comportament per-hop.

Formatori

Formatorii întârzie unele sau toate pachetele într-un flux de trafic pentru a conforma fluxul cu profilul de trafic. Un formator are o dimensiune a buffer-ului finită şi ruterele pot renunţa la pachete în cazul în care nu există suficient spaţiu pentru a păstra pachetele întârziate.

Aruncători

Aruncătorii renunţă la unele sau toate pachetele într-un flux de trafic. Aceasta se întâmplă pentru a aduce fluxul în concordanţă cu profilul de trafic.

Concepte înrudite

"Hardware şi software de reţea" la pagina 49
Capacităţile echipamentului dumneavoastră intern şi cele ale altor echipamente din afara reţelei au efecte enorme asupra rezultatelor QoS.

Servicii integrate

Al doilea tip de politică de lungime de bandă outbound pe care îl puteţi crea este o politică de servicii integrate. Serviciile integrate furnizează pentru aplicaţiile IP capacitatea de a cere şi a rezerva lăţime de bandă prin utilizarea protocolului RSVP şi a API-urilor QoS.

Politicile de servicii integrate folosesc RSVP şi RAPI (Resource Reservation Setup Protocol API) (sau API-ul socket-ului qtoq) pentru a garanta o conexiune capăt-la-capăt. Acesta este cel mai înalt nivel de serviciu pe care îl puteţi desemna; totuşi, este de asemenea şi cel mai complex serviciu.

Serviciile integrate se ocupă de timpii de furnizare ai traficului şi cu asignarea pentru un anumit trafic a anumitor instrucţiuni speciale de manupulare. Este important să fiţi conservatori cu politicile de servicii integrate deoarece este relativ scumpă garantarea transferului de date. Totuşi, asigurarea cu mai multe resurse poate fi chiar mai scumpă.

Serviciile integrate rezervă resurse pentru o anumită politică înainte ca datele să fie trimise. Ruterele sunt anunţate înainte ca transferul de date şi reţeaua să fie de fapt de acord cu şi să gestioneze (capăt-la-capăt) transferul de date bazat pe o politică. O *politică* este un set de reguli care desemnează o acţiune. Este de fapt o listă de control de acces. Cererea de lăţime de bandă vine într-o rezervare de la client. Dacă toate ruterele de pe cale îndeplinesc cerinţele emise de client, cererea ajunge la sistem şi la politica de servicii integrate. Dacă cererea cade între limitele definite de politică, serverul QoS acordă permisiune pentru conexiunea RSVP şi apoi va seta lăţimea de bandă pentru aplicaţie. Rezervarea se realizează prin folosirea RSVP şi API RAPI şi API-urile socket-ului QoS qtoq.

Fiecare nod prin care trece traficul dumneavoastră trebuie să aibă abilitatea de a folosi RSVP. Ruterele oferă calitatea serviciului (QoS) de-a lungul următoarelor funcţii de control de trafic : planificator pachet, clasificator pachet şi control al accesului. Abilitatea de a realiza acest control de trafic este de multe ori referit ca fiind RSVP-activat. Ca rezultat, cea mai importantă parte a implementării politicilor de servicii integrate este să fie capabile să controleze şi să prevadă resursele din reţea. Pentru a obţine rezultate previzibile, fiecare nod din reţea trebuie să fie activat pentru RSVP. De exemplu, traficul dumneavoastră este rutat pe baza resurselor şi nu pe baza căilor care au rutere activate pentru RSVP. Traversarea ruterelor care nu sunt RSVP-activate poate cauza probleme de performanţă imprevizibile. Conexiunea este totuşi făcută, dar performanţa pe care o cere aplicaţia nu este garantată de către ruter. Următoarea figură arată cum funcţionează logic funcţia de servicii integrate.

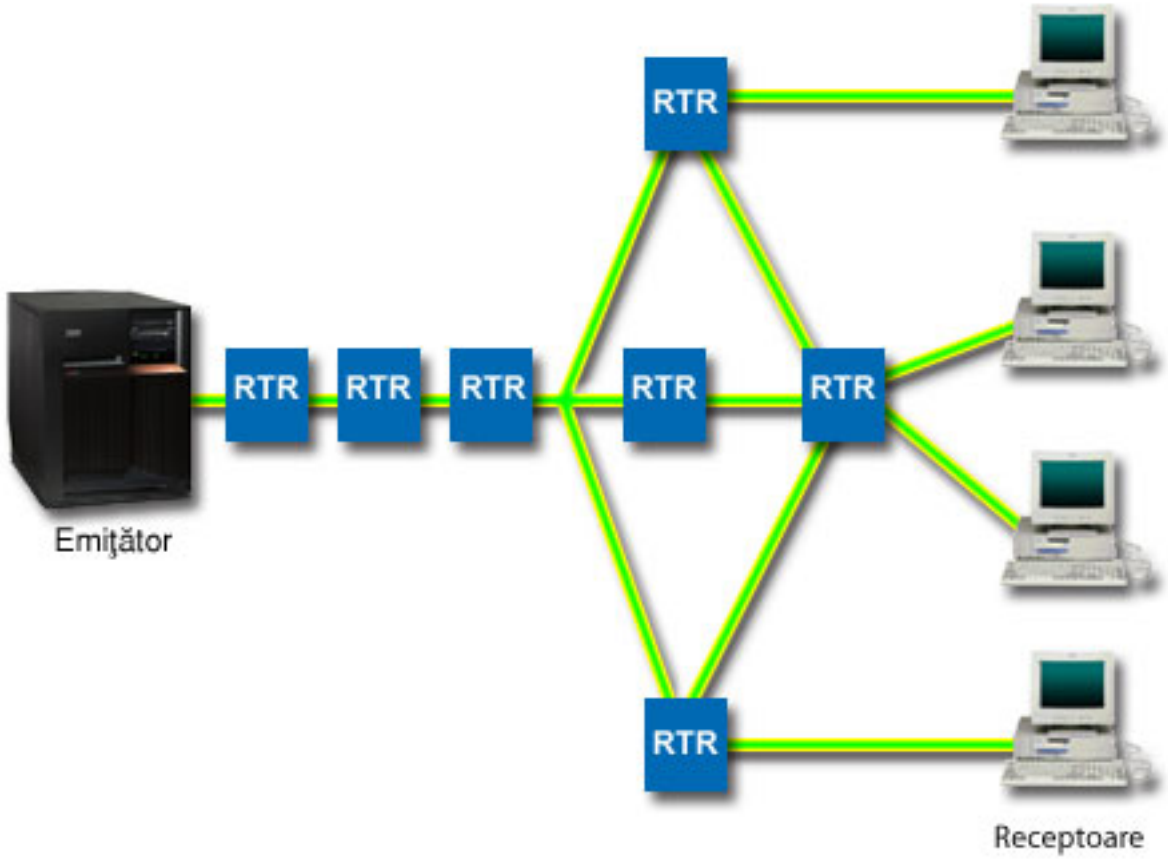


Figura 2. Cale RSVP între client şi server

Aplicaţia RSVP-activată de pe server, afişată în figura precedentă ca expeditor, detectează o cerere de conexiune de la clienţi sau de la receptori. În răspuns, aplicaţia emite o comandă PATH către client. Această comandă este emisă prin folosirea API-urilor RAPI sau API-urilor socket-ului QoS qtoq şi conţine informaţii de adresă IP RTR (ruter). O comandă PATH conţine informaţii despre resursele disponibile pe server şi pe ruterele de-a lungul căii, cât şi informaţia rutei dintre server şi client. Aplicaţia RSVP-actviată de la client apoi trimite înapoi de-a lungul căii reţelei o comandă RESV pentru a semnaliza serverului că resursele de reţea au fost alocate. Această comandă face rezervarea, bazată pe informaţiile de ruter din comanda PATH. Serverul şi toate ruterele din cale rezervă resurse pentru conexiunea RSVP. Când serverul primeşte comanda RESV, aplicaţia începe să transmită date la client. Datele sunt transmise pe aceeaşi rută ca şi rezervarea. Din nou, aceasta arată cât de importante sunt abilităţile ruterelor de a realiza această rezervare pentru succesul politicilor dumneavoastră.

Serviciul integrat nu este conceput pentru conexiuni RSVP pe termen scurt, ca HTTP. Desigur că rămâne la discreţia dumneavoastră. Doar dumneavoastră puteţi decide ce este mai bine pentru reţea. Luaţi în considerare care zone şi aplicaţii au probleme de performanţă şi au nevoie de calitatea serviciului. Aplicaţiile utilizate într-o politică de servicii integrate trebuie să fie capabile să folosească RSVP. Iniţial, sistemul dumneavoastră de operare i5/OS nu are aplicaţiile RSVP-activate, astfel este nevoie să vă asiguraţi că aplicaţia foloseşte RSVP.

În timp ce pachetele sosesc şi încearcă să vă părăsească reţeaua, sistemul dumneavoastră de operare determină dacă are resursele necesare pentru a trimite pachetul. Această acceptare este determinată de cantitatea de spaţiu din găleata jeton. Manual setaţi numărul de biţi permişi în găleata de jetoane, orice limită de lungime de bandă, setaţi limite de rată jetoane şi numărul maxim de conexiuni permise de sistemul dumneavoastră. Aceste valori sunt referite ca limite de performanţă. Dacă pachetele rămân între limite, pachetele sunt în concordanţă şi sunt transmise afară. În serviciile integrate, fiecărei conexiuni îi este acordată propria găleată de jetoane.

Servicii integrate folosind marcaje de servicii diferenţiate

Dacă nu sunteţi sigur dacă întreaga reţea poate garanta o conexiune RSVP, încă mai puteţi crea o politică de servicii integrate. Dacă resursele din reţea nu pot folosi RSVP, conexiunea nu poate fi garantată. În această situaţie, poate doriţi să aplicaţi un punct de cod politicii. Acest punct de cod este folosit în mod obişnuit în politicile de servicii diferenţiate de dat o clasă de servicii traficului. Chiar dacă conexiunea nu este garantată, acest punct de cod va încerca să dea conexiunii unele priorităţi.

Concepte înrudite

"API-uri Calitatea serviciului" la pagina 16
Acest subiect conţine informaţii despre protocoale şi API-uri şi conţine cerinţele pentru un ruter care este activat pentru RSVP (ReSerVation Protocol). API-urile QoS (Quality of Service) includ API-ul RAPI, API-ul qtoq socket, API-ul sendmsg() şi API-urile monitor.

"Servicii integrate folosind marcaje de servicii diferenţiate" la pagina 10
Puteţi folosi marcaje de servicii diferenţiate într-o politică de servicii integrate pentru a menţine prioritatea pachetelor trimise într-un mediu mixt.

"Scenariu: Trafic B2B predictibil" la pagina 37
Dacă aveţi nevoie de livrare predictibilă şi încă doriţi să cereţi o rezervare, folosiţi tot o politică de servicii integrate. Acest exemplu foloseşte un serviciu de încărcare controlat.

"Scenariu: Livrarea dedicată (telefonie IP)" la pagina 41
Dacă aveţi nevoie de livrare dedicată şi doriţi să cereţi o rezervare, folosiţi o politică de servicii integrate. Există două tipuri de politici de servicii integrate ce pot fi create: încărcare garantată şi controlată. În acest exemplu, este folosit serviciul garantat.

Funcţii de control al traficului

Funcţiile de control al traficului se aplică doar serviciilor integrate şi nu sunt specifice produselor System i.

Nu puteţi vedea aceşti termeni folosiţi în interfaţa QoS (quality of service), deoarece serverul nu poate controla hardware extern. În afara unei reţele private, hardware-ul are nevoie să aibă abilitatea de a trata cerinţe QoS generale. Cerinţele generale de ruter pentru politici de servicii integrate sunt discutate în secţiunea următoare. Se recomandă studierea cu atenţie a conceptelor generale QoS şi a cerinţelor preliminare înainte de a implementa politicile.

Pentru a obţine rezultatele previzibile, este nevoie să aveţi hardware-ul care este activat de RSVP (ReSerVation Protocol) de-a lungul căii traficului. Ruterele trebuie să aibă anumite funcţii de control trafic pentru a folosi RSVP. Acesta este deseori referit ca fiind RSVP-activat sau QoS-activat. Ţineţi minte că rolul sistemului dumneavoastră de operare este fie de client sau de server. Nu poate fi folosit în acest moment ca ruter. Consultaţi manualele echipamentelor dumneavoastră de reţea pentru a verifica dacă acestea pot trata cerinţele QoS.

Funcţiile de control al traficului includ următoarele funcţii:

Planificator pachet
Planificatorul de pachet gestionează expedierea pachetului pe baza informaţiilor din antetul IP. Planificatorul de pachet asigură că livrarea pachetului corespunde parametrilor pe care îi setaţi în politica dumneavoastră. Planificatorul este implementat în punctul unde pachetele sunt puse în coadă.

Clasificator pachet
Clasificatorul de pachet identifică care pachete ale unui flux IP primesc un anumit nivel de serviciu pe baza informaţiilor din antetul IP. Fiecare pachet care intră este mapat de către clasificator într-o anumită clasă. Toate pachetele care sunt clasificate în aceeaşi clasă primesc acelaşi tratament. Acest nivel de serviciu se bazează pe informaţiile pe care le furnizaţi în politica dumneavoastră.

Control admitere
Controlul admitere conţine algoritmul de decizie pe care un ruter în foloseşte pentru a determina dacă sunt destule resurse de rutare pentru a accepta QoS-ul cerut pentru un nou flux. Dacă nu sunt destule resurse, noul flux este refuzat. Dacă fluxul este acceptat, ruterul alocă clasificatorul de pachet şi planificatorul pentru a rezerva QoS cerut. Controlul de admitere apare în fiecare ruter de-a lungul căii de rezervare.

Concepte înrudite

"API-uri Calitatea serviciului" la pagina 16
Acest subiect conţine informaţii despre protocoale şi API-uri şi conţine cerinţele pentru un ruter care este activat pentru RSVP (ReSerVation Protocol). API-urile QoS (Quality of Service) includ API-ul RAPI, API-ul qtoq socket, API-ul sendmsg() şi API-urile monitor.

Referinţe înrudite

"Informaţii înrudite pentru Calitatea serviciului" la pagina 65
RFC-uri QoS, publicaţii IBM Redbooks, şi alte colecţii de subiecte din centrul de informare conţin informaţii care sunt înrudite cu colecţia de subiecte Calitatea serviciului. Puteţi vedea sau tipări oricare din fişierele PDF.

Tipuri de servicii integrate

Există două tipuri de servicii integrate: încărcare controlată şi serviciu garantat.

Încărcare controlată

Serviciu cu încărcare controlată suportă aplicaţiile care sunt uşor sensibile la reţele congestionate, cum sunt aplicaţiile în timp real. Aplicaţiile trebuie să fie şi tolerante la mici cantităţi de pierderi sau întârzieri. Dacă o aplicaţie foloseşte serviciul de încărcare controlată, performanţa sa nu va suferi la creşterile de încărcare a reţelei. Traficul este prevăzut cu serviciu asemănător unui trafic normal într-o reţea în condiţii uşoare.

Ruterele trebuie să asigure că serviciile cu încărcare controlată primesc o lăţime de bandă corespunzătoare şi resurse de procesare pachet. Pentru a face asta, este nevoie să fiţi QoS-activat cu suport pentru servicii integrate. Este nevoie să verificaţi specificaţiile ruterului pentru a vedea dacă furnizează QoS printr-o funcţie de control trafic. Controlul traficului constă din următoarele componente: planificator de pachet, clasificator de pachet şi control de acces.

Serviciu garantat

Serviciu garantat asigură că pachetul ajunge într-un timp desemnat de livrare. Aplicaţiile care necesită serviciu garantat includ sisteme de difuzare video şi audio care folosesc tehnologii de înşirare. Serviciu garantat controlează întârzierea maximă de punere în coadă astfel încât pachetele nu sunt întârziate peste o durată desemnată de timp. Fiecare ruter de-a lungul căii pachetului trebui să ofere capabilităţi RSVP (ReSerVation Protocol) pentru a asigura livrarea. Când alocaţi limite de găleată jeton şi limite de lăţime de bandă, definiţi serviciul dumneavoastră garantat. Serviciu garantat poate fi aplicat doar aplicaţiilor care folosesc TCP.

Concepte înrudite

"Scenariu: Trafic B2B predictibil" la pagina 37
Dacă aveţi nevoie de livrare predictibilă şi încă doriţi să cereţi o rezervare, folosiţi tot o politică de servicii integrate. Acest exemplu foloseşte un serviciu de încărcare controlat.

"Scenariu: Livrarea dedicată (telefonie IP)" la pagina 41
Dacă aveţi nevoie de livrare dedicată şi doriţi să cereţi o rezervare, folosiţi o politică de servicii integrate. Există două tipuri de politici de servicii integrate ce pot fi create: încărcare garantată şi controlată. În acest exemplu, este folosit serviciul garantat.

Limite găleată jeton şi lăţime de bandă

Limitele găleţii jeton şi ale lăţimii de undă sunt cunoscute împreună ca limite de performanţă. Aceste limite de performanţă ajută la garantarea livrării pachetelor în politici de lăţime de bandă ieşire, servicii integrate şi diferenţiate.

Dimensiune găleată jeton

Dimensiunea găleată jeton determină cantitatea de informaţii pe care sistemul dumneavoastră o poate procesa la orice moment de timp. Dacă o aplicaţie trimite sistemului dumneavoastră informaţi mai repede decât sistemul poate trimite datele în afara reţelei, buffer-ul se umple. Orice pachete de date care depăşesc această limită sunt tratate ca afară-din-profil. Politicile serviciilor integrate sunt excepţia de la această regulă. Puteţi selecta fără limită, ceea ce dă permisiune unei cereri de conexiune RSVP (ReSerVation Protocol). Pentru toate celelalte politici, puteţi determina modul în care veţi manevra traficul afară-din-profil. Dimensiunea maximă a găleţii de jetoane este de 1 GB.

Limita ratei jetonului

Limita ratei jetonului specifică rata de date pe termen lung sau numărul de biţi pe secundă permişi într-o reţea. Politica QoS (quality of service) se uită la lungimea de bandă cerută şi o compară cu rata şi limitele de flux pentru această politică. Dacă cererea face ca sistemul să îşi depăşească limitele, sistemul refuză cererea. Limita ratei jetonului este folosită doar pentru control admitere în cadrul politicilor de servicii integrate. Această valoare poate varia între 10 kbps şi 1 Gbps. De asemenea puteţi seta această valoare la fără limită. Când alocaţi ratei fără limită, transformaţi resursele disponibile în limită.

Indiciu: Pentru a determina ce limite sunt setate, aţi putea dori să rulaţi monitorizarea. Creaţi o politică cu o limită a ratei agregate de jetoane destul de mare pentru a colecta majoritatea traficului de date de pe reţea. Apoi porniţi colecţionarea de date în această politică. Scenariul despre monitorizare statistici curente de reţea pentru o modalitate de a colecta ratele totale pentru aplicaţia dumneavoastră şi utilizarea curentă a reţelei. Folosind aceste rezultate, puteţi reduce corespunzător limitele.

Pentru a vedea datele curente ale monitorului în locul unei colecţii particulare de date, doar deschideţi monitorul. Monitorul dă statistici în timp-real pe toate politicile active.

Concepte înrudite

“Servicii diferenţiate” la pagina 2
Acesta este primul tip de politică de lungime de bandă outbound pe care o puteţi crea pe sistemul dumneavoastră de operare. Serviciile diferenţiate împart traficul dumneavoastră pe clase. Pentru a realiza o politică de serviciu diferenţiat, este necesar să determinaţi cum doriţi să clasificaţi traficul dumneavoastră de reţea şi cum să trataţi diferitele clase.

“Scenariu: Monitorizarea statisticilor curente de reţea” la pagina 45
În cadrul vrăjitorilor, este nevoie să setaţi limitele de performanţă care sunt bazate pe cerinţe individuale de reţea.

Servicii integrate folosind marcaje de servicii diferenţiate

Puteţi folosi marcaje de servicii diferenţiate într-o politică de servicii integrate pentru a menţine prioritatea pachetelor trimise într-un mediu mixt.

Un mediu mixt apare atunci când o rezervare de serviciu integrat trece prin diferite rutere care nu suportă rezervare de servicii integrate, dar suportă servicii diferenţiate. Deoarece traficul trece prin diferite domenii, acorduri la nivel de serviciu şi capabilităţi de echipament, s-ar putea să nu primiţi mereu serviciul dorit.

Pentru a ajuta la rezolvarea acestei potenţiale probleme, puteţi ataşa un marcaj de serviciu diferenţiat la politica de servicii integrate. Dacă o politică traversează un ruter care nu poate folosi RSVP (ReSerVation Protocol), politica dumneavoastră mai păstrează unele priorităţi. Marcajul pe care îl adăugaţi se numeşte *comportament per-hop*.

Fără semnalizare

În plus la utilizarea marcajelor, puteţi folosi funcţia fără semnalizare. Când selectaţi această funcţie, versiunile fără semnalizare ale API-urilor vă permit să scrieţi o aplicaţie care duce la încărcarea unei reguli RSVP pe sistemul de operare. Aplicaţia necesită doar ca aplicaţia părţii server a conversaţiei TCP/IP să fie RSVP-activată. Semnalizarea RSVP este făcută automat în numele părţii client. Aceasta creează conexiunea RSVP pentru aplicaţie chiar dacă partea client nu poate folosi protocolul RSVP.

Funcţia ″Fără semnalizare″ este specificată în politica de servicii integrate. Pentru a crea politica de acces inbound, realizaţi următorii paşi:

1. În Navigator System i, expandaţi ***sistemul dumneavoastră*** → **Reţea** → **Politici IP**.
2. Faceţi clic dreapta **Calitatea serviciului** şi selectaţi **Configurare**.
3. Expandaţi **Politici lăţime de bandă outbound** → **IntServ**.
4. Faceţi clic dreapta pe numele politicii de servicii integrate cerute şi selectaţi **Proprietăţi**. Se deschide fereastra Proprietăţi linie IntServ.

5. Selectaţi fişa **Gestionarea traficului** pentru a dezactiva sau a activa semnalizarea. Tot aici editaţi planificatorul, clientul, aplicaţiile şi gestionarea traficului.

Concepte înrudite

"Clasa serviciului" la pagina 12
Când creaţi o politică de servicii diferenţiate sau o politică de acces inbound, creaţi, de asemenea şi folosiţi o clasă de serviciu.

"Servicii integrate" la pagina 6
Al doilea tip de politică de lungime de bandă outbound pe care îl puteţi crea este o politică de servicii integrate. Serviciile integrate furnizează pentru aplicaţiile IP capacitatea de a cere şi a rezerva lăţime de bandă prin utilizarea protocolului RSVP şi a API-urilor QoS.

Politici de acces inbound

Politica de acces inbound este folosită pentru a controla cererile de conexiuni care sosesc în reţeaua dumneavoastră.

Politica inbound este folosită pentru a restricţiona traficul care încearcă să se conecteze la sistemul dumneavoastră. Puteţi restricţiona accesul la sistemul dumneavoastră după client, URI (Uniform Resource Identifier), aplicaţie sau interfaţă locală. În plus, puteţi îmbunătăţi performanţa sistemului prin aplicarea unei clase de servicii traficului inbound. Această politică se defineşte prin intermediul vrăjitorului Acces inbound din Navigator System i.

Există trei componente la o politică inbound care necesită mai multe informaţii. Acestea includ URI-uri cărora să li se restricţioneze traficul, ratele conexiunilor definite în clasa serviciului şi cozi de prioritate pentru ordonarea cu succes a conexiunilor. Pentru informaţii suplimentare vedeţi "URI", "Rată de conexiune" la pagina 12 şi "Cozi de prioritate cu pondere" la pagina 12.

URI

Puteţi lua în considerare folosirea unei politici inbound pentru a restricţiona traficul HTTP care se conectează la serverul dumneavoastră Web. În aceste circumstanţe puteţi crea o politică de acces inbound care restricţionează traficul după un anumit URI. Rata de cerere URI este o parte a unei soluţii pentru a ajuta la protejarea serverelor împotriva supraîncărcării. Desemnarea de URI-uri specifice aplică control de admitere, pe baza informaţiilor de nivel-aplicaţie, pentru a limita cererile de URI acceptate de către server. În industrie, aceasta se numeşte şi control conexiune pe baza antetului, care foloseşte URI-uri pentru a seta priorităţi.

Specificarea unui URI permite politicii inbound să examineze conţinutul, nu doar antetul pachetelor. Conţinutul examinat este un nume URI. Pentru sistemul de operare i5/OS, puteţi folosi numele URI relativ (de exemplu, /products/clothing).

URI înrudit

URI-ul relativ este de fapt un subset al unui URI absolut (similar vechiului URL absolut). Consideraţi acest exemplu: http://www.ibm.com/software. Segmentul *http://www.ibm.com/software* este considerat URI-ul absolut. Segmentul */software* este URI-ul înrudit. Toate valorile de URI-uri înrudite trebuie să înceapă cu un slash înainte (/). Următoarele segmente sunt exemple de URI-uri înrudite valide:

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

Note:

- La folosirea unui URI, trebuie să specificaţi protocolul ca TCP. În plus, portul şi adresa IP trebuie să se potrivească cu portul şi adresa configurate pentru serverul HTTP. Acesta este de obicei portul 80.
- Există un caracter de înlocuire implicit atunci când specificaţi un URI. De exemplu, /software include orice din directorul software.
- Nu folosiţi un * în URI. Acesta nu este un caracter valid.

- Informaţiile URI pot fi folosite la politicile inbound sau de serviciu diferenţiat (politici outbound).

Înainte de a seta o politică de servicii diferenţiate care utilizează URI-uri, trebuie să vă asiguraţi de faptul că portul aplicaţiei alocat pentru URI se potriveşte directivei ″Ascultare″ activată pentru FRCA în configurarea web serverului Apache. Pentru a modifica sau vizualiza portul serverului dumneavoastră HTTP, consultaţi Gestionare adrese şi porturi pentru server HTTP (motorizat de Apache).

Rată de conexiune

Ca parte a politicii de acces inbound, trebuie să selectaţi o clasă a serviciului. Această clasă de servicii defineşte rate de conexiune care au rol de control acces pentru a limita conexiunile acceptate de sistem.

Ratele de conexiune limitează acceptarea sau respingerea unui nou pachet, pe baza numărului mediu de conexiuni pe secundă şi numărului maxim de conexiuni instantanee definite în politica creată de dumneavoastră. Aceste limite de conexiune constau dintr-o rată medie şi o limită de rafală, pe care le introduceţi prin intermediul vrăjitorilor Navigator System i. Când cererile de conexiune de intrare ajung la sistemul de operare, sistemul analizează informaţiile din antetul pachetului pentru a determina dacă acest trafic este definit într-o politică. Sistemul verifică aceste informaţii cu profilul limite de conexiune. Dacă pachetul este în limitele politicii, este plasat într-o coadă.

Folosiţi informaţiile de mai sus pe măsură ce realizaţi vrăjitorul de acces inbound. În Navigator System i, puteţi de asemenea folosi Ajutorul asociat pentru a vedea informaţii similare în timp ce completaţi politica.

Cozi de prioritate cu pondere

Ca parte a controlului traficului inbound, puteţi specifica prioritatea în care sunt tratate cererile de conexiune după ce au fost evaluate de politici. Prin asignarea unui ponderi la o coadă de prioritate, controlaţi timpul de răspuns al cozii după sosirea unei conexiuni. Dacă este pus în coadă, conexiunea este tratată în ordinea cozii de priorităţi (înaltă, medie, joasă sau cel mai bun efort). Dacă nu sunteţi siguri pe ponderile pe care să le alocaţi, folosiţi-le pe cele implicite. Suma tuturor ponderilor trebuie să fie egală cu 100. De exemplu, dacă 25 este specificat pentru toate priorităţile, atunci toate cozile sunt tratate la fel. Să presupunem că specificaţi următoarele ponderi: High (50), Medium (30), Low (15) şi Best effort (5). Conexiunile acceptate includ:

- 50% conexiuni de prioritate înaltă
- 30 % conexiuni de prioritate medie
- j15% conexiuni de prioritate joasă
- 5% conexiuni de prioritate cel mai bun efort

Concepte înrudite

“Clasa serviciului”
Când creaţi o politică de servicii diferenţiate sau o politică de acces inbound, creaţi, de asemenea şi folosiţi o clasă de serviciu.

“Rata medie de conexiuni şi limitele pentru rafală” la pagina 15
Ratele de conexiuni şi limitele pentru rafală sunt limite de rată. Aceste limite de rată ajută la restricţionarea conexiunilor inbound care încearcă să intre pe serverul dumneavoastră. Limitele de rate sunt setate într-o clasă de serviciu care este folosită cu politici de acces inbound.

Clasa serviciului

Când creaţi o politică de servicii diferenţiate sau o politică de acces inbound, creaţi, de asemenea şi folosiţi o clasă de serviciu.

Politicile de servicii diferenţiate şi politicile de acces inbound folosesc o clasă de servicii pentru a grupa traficul în clase. Deşi aceasta se realizează în cea mai mare parte prin hardware, controlaţi modul de grupare al traficului şi prioritatea primită de trafic.

Când realizaţi QoS (quality of service), mai întâi definiţi politici. Politicile determină cine, ce, unde şi când. Apoi trebuie să alocaţi o clasă de servicii la politică. Clasele de servicii sunt definite separat şi pot fi reutilizate de politici.

Atunci când definiţi clasa de serviciu, specificaţi dacă aceasta poate fi aplicată tipului de politică inbound, outbound sau ambelor. Dacă selectaţi ambele (inbound şi outbound), atunci o politică de serviciu diferenţiat şi o politică de acces inbound pot folosi acea clasă de serviciu.

Setările din clasa de serviciu depind de setarea clasei de serviciu la intrare, ieşire sau ambele. Atunci când creaţi clasa de serviciu, puteţi întâlni următoarele cerinţe:

Marcarea punctului de cod

QoS foloseşte punctele de cod sugerate pentru a atribui comportamente per-hop traficului. Ruterele şi switch-urile folosesc aceste puncte de cod pentru a da traficului niveluri de prioritate. Sistemul dumneavoastră nu poate folosi aceste puncte de cod, deoarece nu se comportă ca un ruter. Trebuie să determinaţi care puncte de cod se vor folosi pentru nevoile individuale ale reţelei dumneavoastră. Luaţi în considerare ce aplicaţii sunt cele mai importante pentru dumneavoastră şi ce politici trebuie să primească prioritatea cea mai înaltă. Lucrul cel mai important este să fiţi consistent cu marcatorii dumneavoastră astfel încât să obţineţi rezultatele dorite. Aceste puncte de cod sunt o componentă cheie a diferenţierii diferitelor clase de trafic.

Măsurarea traficului

Calitatea serviciului (QoS) foloseşte limite de control pentru a restricţiona traficul prin reţeaua dumneavoastră. Aceste limite sunt puse setând dimensiunea găleată a jetonului, limita ratei de vârf şi limita ratei medii. Vedeţi “Limite găleată jeton şi lăţime de bandă” la pagina 9 pentru mai multe informaţii despre aceste valori specifice.

Trafic în afara profilului

În porţiunea finală a unei clase de servicii este tratarea în-afara-profilului. Când atribuiţi limitele de control rată, setaţi valori pentru a restricţiona traficul. Când traficul depăşeşte aceste restricţii, pachetele sunt considerate în-afara-profilului. Informaţiile dintr-o clasă de servicii îi spune sistemului dacă să renunţă la traficul UDP şi să reducă fereastra de congestionare TCP, să ordoneze sau să marcheze din nou pachetele în-afara-profilului.

Abandonarea pachetelor UDP sau reducerea ferestrei de congestionare TCP: Dacă decideţi să renunţaţi şi să ajustaţi pachetele în-afara-profilului, se renunţă la pachetele UDP. Totuşi, fereastră de congestionare TCP este redusă astfel încât rata de date se conformează cu rata de găleată jeton. Numărul de pachete care poate fi trimis în reţea la un anumit moment de timp scade şi congestia se reduce.

Întârziere (ordonare): Dacă întârziaţi pachetele în-afara-profilului, acestea sunt ordonate pentru a se conforma caracteristicilor de tratare definite de dumneavoastră.

Re-marcare cu punctul de cod DiffServ: Dacă re-marcaţi pachete în-afara-profilului cu un punct de cod, acestora le este realocat un nou punct de cod. Pachetele nu sunt accelerate pentru a îndeplini caracteristicile dumneavoastră de tratare, doar re-marcate. Când alocaţi aceste instrucţiuni de tratare în vrăjitor, apăsaţi Ajutor pentru mai multe informaţii.

Prioritate

Puteţi stabili priorităţi pentru conexiunile care sunt făcute către sistemul dumneavoastră prin diferite politici de control a admiterilor de intrări. Aceasta vă permite să definiţi ordinea în care conexiunile complete sunt tratate de către sistemul dumneavoastră. Puteţi alege priorităţi înalte, medii, joase sau cel mai bun efort.

Concepte înrudite

“Servicii integrate folosind marcaje de servicii diferenţiate” la pagina 10
Puteţi folosi marcaje de servicii diferenţiate într-o politică de servicii integrate pentru a menţine prioritatea pachetelor trimise într-un mediu mixt.

“Politici de acces inbound” la pagina 11
Politica de acces inbound este folosită pentru a controla cererile de conexiuni care sosesc în reţeaua dumneavoastră.

“Servicii diferenţiate” la pagina 2
Acesta este primul tip de politică de lungime de bandă outbound pe care o puteţi crea pe sistemul dumneavoastră de operare. Serviciile diferenţiate împart traficul dumneavoastră pe clase. Pentru a realiza o politică de serviciu diferenţiat, este necesar să determinaţi cum doriţi să clasificaţi traficul dumneavoastră de reţea şi cum să trataţi diferitele clase.

Referinţe înrudite

Utilizarea punctelor de cod pentru a asigna comportament per-hop

QoS (Quality of service) foloseşte punctele de cod sugerate pentru a asigna comportamente per-hop traficului.

În vrăjitorul Clasă de servicii, aveţi nevoie să asignaţi un comportament per-hop politicii dumneavoastră. Trebuie să determinaţi ce puncte de cod să folosiţi pe baza cerinţelor individuale de reţea. Doar dumneavoastră puteţi decide care scheme de puncte de cod au sens pentru mediul dumneavoastră. Trebuie să luaţi în considerare ce aplicaţii sunt cele mai importante pentru dumneavoastră şi ce politici pot fi alocate cu o prioritate mai înaltă. Cel mai important lucru este să fiţi perseverent cu marcajele astfel încât să obţineţi rezultatele aşteptate. De exemplu, politicile care au aceeaşi importanţă utilizează puncte de cod similare astfel încât dumneavoastră primiţi rezultate consistente pentru acele politici. Dacă sunteţi nesigur ce punct de cod să alocaţi, utilizaţi urma şi eroarea. Creaţi politici de test, monitorizaţi-le şi faceţi corecţiile corespunzătoare.

Tabelele din secţiunea următoare afişează punctele de cod sugerate bazate pe standarde industriale. Majoritatea furnizorilor de internet suportă punctele de cod standard ale industriei şi puteţi verifica daca furnizorul dumneavoastră suportă aceste puncte de cod. Între domenii, fiecare ISP trebuie să fie de acord să ajute cererile de calitatea serviciului. Înţelegerile de servicii trebuie să poată da politicilor ceea ce acestea cer. Verificaţi dacă primiţi serviciile de care aveţi nevoie. Dacă nu, v-aţi putea cheltui resursele. Politicile QoS vă permit să negociaţi niveluri de servicii cu ISP-ul dumneavoastră, care poate duce la scăderea costurilor de servicii reţea. Puteţi, de asemenea, să creaţi propriile dumneavoastră puncte de cod; oricum, nu se recomandă pentru utilizare externă. Punctul de cod propriu poate fi cel mai bine utilizat într-un mediu de testare.

Trimitere expeditivă

Trimitere expeditivă este un tip de comportament per-hop. Este în principal folosit pentru a furniza servicii garantate de-a lungul reţelei. Trimiterea expeditivă dă traficului un serviciu cu pierderi mici, sigur, cap la cap garantând lăţime de bandă de-a lungul reţelei. Rezervarea este făcută înainte ca pachetul să fie trimis. Scopul principal este evitarea întârzierii şi livrarea pachetului pe bază de timp.

Tabela 1. Puncte de cod sugerate: Trimitere expeditivă

Trimitere expeditivă
101110

Notă: Există de obicei un cost mare pentru a primi tratament de trimitere expeditivă, astfel că nu este recomandată folosirea acestui comportament per-hop în mod regulat.

Selector de clasă

Punctele de cod selector de clasă sunt alt tip de comportament. Sunt şapte clase. Clasa 0 dă pachetelor prioritatea cea mai joasă şi clasa 7 dă pachetelor prioritatea cea mai înaltă din cadrul valorilor punctelor de cod selectoare de clase. Acesta este cel mai obişnuit grup de comportamente per-hop, deoarece majoritatea ruterelor folosesc deja puncte de cod similare.

Tabela 2. Puncte de cod sugerate: Selector de clasă

Selector de clasă
Clasa 0 - 000000
Clasa 1 - 001000
Clasa 2 - 010000
Clasa 3 - 011000
Clasa 4 - 100000
Clasa 5 - 101000

Tabela 2. Puncte de cod sugerate: Selector de clasă (continuare)

Selector de clasă
Clasa 6 - 110000
Clasa 7 - 111000

Trimitere asigurată

Trimiterea asigurată este împărţită în patru clase de comportament per-hop, care fiecare au niveluri de precedare a aruncării de jos, mediu sau înalt. Un nivel de precedare a aruncării determină cât de posibil este ca pachetele să fie aruncate. Fiecare clasă are specificaţiile proprii de lăţime de bandă. Clasa 1, înalt dă politicii cea mai mică prioritate şi Clasa 4, jos dă politicii cea mai înaltă prioritate. Un nivel scăzut de abandon înseamnă că pachetele din această politică au cea mai scăzută modificare a abandonului în acest nivel particular de clasă.

Tabela 3. Puncte de cod sugerate: Trimitere asigurată

Trimitere asigurată
Expediere asigurată, Clasa 1, Jos - 001010
Expediere asigurată, Clasa 1, Mediu - 001100
Expediere asigurată, Clasa 1, Înalt- 001110
Expediere asigurată, Clasa 2, Jos - 010010
Expediere asigurată, Clasa 2, Mediu - 010100
Expediere asigurată, Clasa 2, Înalt - 010110
Expediere asigurată, Clasa 3, Jos - 011010
Expediere asigurată, Clasa 3, Mediu - 011100
Expediere asigurată, Clasa 3, Înalt - 011110
Expediere asigurată, Clasa 4, Jos - 100010
Expediere asigurată, Clasa 4, Mediu - 100100
Expediere asigurată, Clasa 4, Înalt - 100110

Concepte înrudite

"Servicii diferenţiate" la pagina 2
Acesta este primul tip de politică de lungime de bandă outbound pe care o puteţi crea pe sistemul dumneavoastră de operare. Serviciile diferenţiate împart traficul dumneavoastră pe clase. Pentru a realiza o politică de serviciu diferenţiat, este necesar să determinaţi cum doriţi să clasificaţi traficul dumneavoastră de reţea şi cum să trataţi diferitele clase.

"Clasa serviciului" la pagina 12
Când creaţi o politică de servicii diferenţiate sau o politică de acces inbound, creaţi, de asemenea şi folosiţi o clasă de serviciu.

Rata medie de conexiuni şi limitele pentru rafală

Ratele de conexiuni şi limitele pentru rafală sunt limite de rată. Aceste limite de rată ajută la restricţionarea conexiunilor inbound care încearcă să intre pe serverul dumneavoastră. Limitele de rate sunt setate într-o clasă de serviciu care este folosită cu politici de acces inbound.

Rată rafale de conexiuni (burst)

Mărimea ratei determină capacitatea buffer-ului care reţine rafalele de conexiuni. Rafalele de conexiuni ar putea intra în sistem la o rată mai mare decât poate suporta sau decât vreţi să permiteţi dumneavoastră. Dacă numărul de conexiuni într-o rafală depăşeşte rata de rafală de conexiuni pe care aţi setat-o, atunci conexiunile suplimentare sunt ignorate.

Rată medie de conexiuni

Rata medie de conexiuni specifică limita de conexiuni noi stabilite sau rata de cereri acceptate de URI-uri (Uniform Resource Identifier) permise în sistem. Dacă o cerere face ca sistemul să depăşească limitele setate, sistemul refuză cererea. Limita medie de cereri de conexiuni este măsurată în conexiuni pe secundă.

Indiciu: Pentru a determina ce limite sunt setate, aţi putea dori să rulaţi monitorizarea. Scenariul despre monitorizare statistici curente de reţea conţine un exemplu de politică care v-ar putea ajuta să colectaţi mare parte din datele care trec prin sistemul dumneavoastră. Folosind aceste rezultate, puteţi regla corespunzător limitele.

Pentru a vedea date de monitorizare în timp real în locul unei anumte colecţii de date, deschideţi monitorul. Monitorul dă statistici în timp-real pe toate politicile active.

Concepte înrudite

"Politici de acces inbound" la pagina 11
Politica de acces inbound este folosită pentru a controla cererile de conexiuni care sosesc în reţeaua dumneavoastră.

"Scenariu: Monitorizarea statisticilor curente de reţea" la pagina 45
În cadrul vrăjitorilor, este nevoie să setaţi limitele de performanţă care sunt bazate pe cerinţe individuale de reţea.

API-uri Calitatea serviciului

Acest subiect conţine informaţii despre protocoale şi API-uri şi conţine cerinţele pentru un ruter care este activat pentru RSVP (ReSerVation Protocol). API-urile QoS (Quality of Service) includ API-ul RAPI, API-ul qtoq socket, API-ul sendmsg() şi API-urile monitor.

Majoritatea politicilor QoS necesită utilizarea unui API. Următoarele API-uri pot fi folosite în legătură atât cu politici de servicii diferenţiate cât şi de servicii integrate. Există de asemenea un număr de API-uri folosite cu monitorizarea QoS:

- "API-uri servicii integrate"
- "API-uri servicii diferenţiate" la pagina 17
- "API-ul monitor" la pagina 17

API-uri servicii integrate

Protocolul de rezervare a resurselor (RSVP) împreună cu API-urile RAPI sau API-urile socket-ului QoS qtoq vă vor realiza rezervarea de servicii integrate. Fiecare nod pe care traficul îl parcurge trebuie să poată folosi protocolul RSVP. Abilitatea de a realiza politici de servicii integrate este deseori numită RSVP-activat. Funcţiile de control de trafic pot fi folosite pentru a determina care funcţii de sunt necesare pentru a folosi RSVP.

Protocolul RSVP este utilizat la crearea unei rezervări RSVP în toate nodurilor reţelei de-a lungul căii traficului. Acesta menţine această rezervare destul de mult încât să furnizeze politicii dumneavoastră serviciile cerute. Rezervarea defineşte modul de tratare şi lungimea de bandă de care datele din această conversaţie au nevoie. Nodurile de reţea furnizează datele de tratare care sunt definite în rezervare.

RSVP este un protocol simplu în acele rezervări care sunt făcute doar într-o direcţie (de la receptor). Pentru conexiuni mai complexe, cum sunt conferinţele audio şi video, fiecare emiţător este şi un receptor. În acest caz, trebuie să setaţi două sesiuni pentru fiecare parte.

Adiţional ruterelor dumneavoastră RSVP-activate, trebuie să aveţi aplicaţii RSVP-activate pentru a folosi serviciile integrate. Deoarece sistemul nu are iniţial nici o aplicaţie RSVP-activată, este nevoie să vă scrieţi aplicaţiile folosind API-ul RAPI sau API-urile socket-ului QoS qtoq. Astfel se dă posibilitatea aplicaţiilor să folosească RSVP-ul. Dacă doriţi o explicaţie mai detaliată, multe surse explică aceste modele, operaţiile lor şi tratarea mesajelor. Aveţi nevoie de o înţelegere amănunţită a RSVP-ului şi a conţinutului Internet RFC 2205.

API-urile socket-uri qtoq

Puteţi folosi API-urile socket-ului QoS qtoq pentru a simplifica munca necesară folosirii RSVP în sistem. API-urile socket-ului qtoq apelează API-urile RAPI şi realizează unele dintre cele mai dificile operaţii. API-urile socket-ului qtoq nu sunt la fel de flexibile ca şi API-urile RAPI, dar oferă aceleaşi funcţii cu mai puţin efort. Versiunile ″Fără semnalizare″ ale API-urilor vă permit să scrieţi următoarele aplicaţii:

- O aplicaţie care încarcă o regulă RSVP în sistem.
- O aplicaţie care necesită doar ca aplicaţia din partea serverului (a conversaţiei TCP/IP) să fie RSVP-activată.

Semnalizarea RSVP este făcută automat în numele părţii client.

Consultaţi Flux funcţional orientat pe conexiune API QoS sau Flux funcţional fără conexiune API QoS pentru flux obişnuit API QoS al unei aplicaţii sau protocol care foloseşte socket-uri QoS qtoq orientate pe conexiune sau fără conexiune.

API-uri servicii diferenţiate

Notă: API-ul sendmsg() este folosit pentru anumite politici de servicii diferenţiate care definesc un anumit jeton de aplicaţie. Când creaţi o politică de servicii diferenţiate, puteţi (opţional) furniza caracteristici de aplicaţie (jeton sau prioritate). Aceasta este o definire avansată de politică, iar dacă nu este folosită, acest API poate fi ignorat. Totuşi, ţineţi minte că ruterele şi alte sisteme de-a lungul reţelei încă mai au nevoie să poată recunoaşte servicii diferenţiate.

Dacă vă decideţi să folosiţi un jeton de aplicaţie într-o politică de servicii diferenţiate, aplicaţia care furnizează aceste informaţii trebuie să fie codată în mod specific pentru folosirea API-ului sendmsg(). Aceasta se realizează de către programatorul aplicaţiei. Documentaţia aplicaţiei trebuie să furnizeze valori valide (jeton şi prioritate) pe care administratorul QoS le foloseşte în politica de servicii diferenţiate. Politica de servicii diferenţiate îşi aplică apoi propria prioritate şi clasificare traficului care se potriveşte cu jetonul setat în politică. Dacă aplicaţia nu are valori care să se potrivească cu cele setate în politică, fie aplicaţia necesită modificări fie este nevoie să folosiţi alţi parametrii datelor aplicaţie pentru politica de servicii diferenţiate.

Următoarele informaţii descriu pe scurt parametrii datelor de sistem: jeton de aplicaţie şi prioritate aplicaţie.

Ce este un jeton de aplicaţie?

Un *jeton de aplicaţie* este un URI care reprezintă o resursă definită. Jetonul pe care îl specificaţi în politica QoS este comparată cu jetonul furnizat de aplicaţia outbound. Aplicaţia furnizează valoarea jetonului prin folosirea API-ului sendmsg(). Dacă jetoanele se potrivesc, traficul aplicaţiei este inclus în politica de servicii diferenţiate.

Ce este o prioritate aplicaţie?

Prioritatea aplicaţie specificată de dumneavoastră este comparată cu prioritatea aplicaţiei furnizată de aplicaţia outbound. Aplicaţia furnizează valoarea priorităţii prin folosirea API-ului sendmsg(). Dacă priorităţile se potrivesc, traficul aplicaţiei este inclus în politica de servicii diferenţiate. Tot traficul definit în politica de servicii diferenţiate încă mai primeşte prioritatea dată întregii politici.

Pentru informaţii suplimentare despre tipul de politică de servicii diferenţiate, consultaţi “Servicii diferenţiate” la pagina 2.

API-ul monitor

API-urile Resource Reservation Setup Protocol includ API-urile monitor. API-urile care se aplică monitorizării au cuvântul monitor în titlu. De exemplu, *QgyOpenListQoSMonitorData*. Următoarea listă descrie pe scurt fiecare API monitor:

- QgyOpenListQoSMonitorData (Open List of QoS Monitor Data) adună informaţii înrudite cu serviciile QoS.
- QtoqDeleteQoSMonitorData (Delete QoS Monitor Data) şterge unul sau mai multe seturi de date colectate de monitorizarea QoS.

- QtoqEndQoSMonitor (End QoS Monitor) opreşte adunarea de informaţii înrudite cu serviciile QoS.
- QtoqListSavedQoSMonitorData (List Saved QoS Monitor Data) returnează o listă cu toate datele de monitorizare colectate care au fost salvate anterior.
- QtoqSaveQoSMonitorData (Save QoS Monitor Data) salează o copie a datelor de monitorizare QoS colectate pentru o viitoare utilizare.
- QtoqStartQoSMonitor (Start QoS Monitor) adună informaţii înrudite cu servicii QoS.

Concepte înrudite

"Servicii integrate" la pagina 6
Al doilea tip de politică de lungime de bandă outbound pe care îl puteţi crea este o politică de servicii integrate. Serviciile integrate furnizează pentru aplicaţiile IP capacitatea de a cere şi a rezerva lăţime de bandă prin utilizarea protocolului RSVP şi a API-urilor QoS.

"Funcţii de control al traficului" la pagina 8
Funcţiile de control al traficului se aplică doar serviciilor integrate şi nu sunt specifice produselor System i.

"Scenariu: Trafic B2B predictibil" la pagina 37
Dacă aveţi nevoie de livrare predictibilă şi încă doriţi să cereţi o rezervare, folosiţi tot o politică de servicii integrate. Acest exemplu foloseşte un serviciu de încărcare controlat.

"Hardware şi software de reţea" la pagina 49
Capacităţile echipamentului dumneavoastră intern şi cele ale altor echipamente din afara reţelei au efecte enorme asupra rezultatelor QoS.

Referinţe înrudite

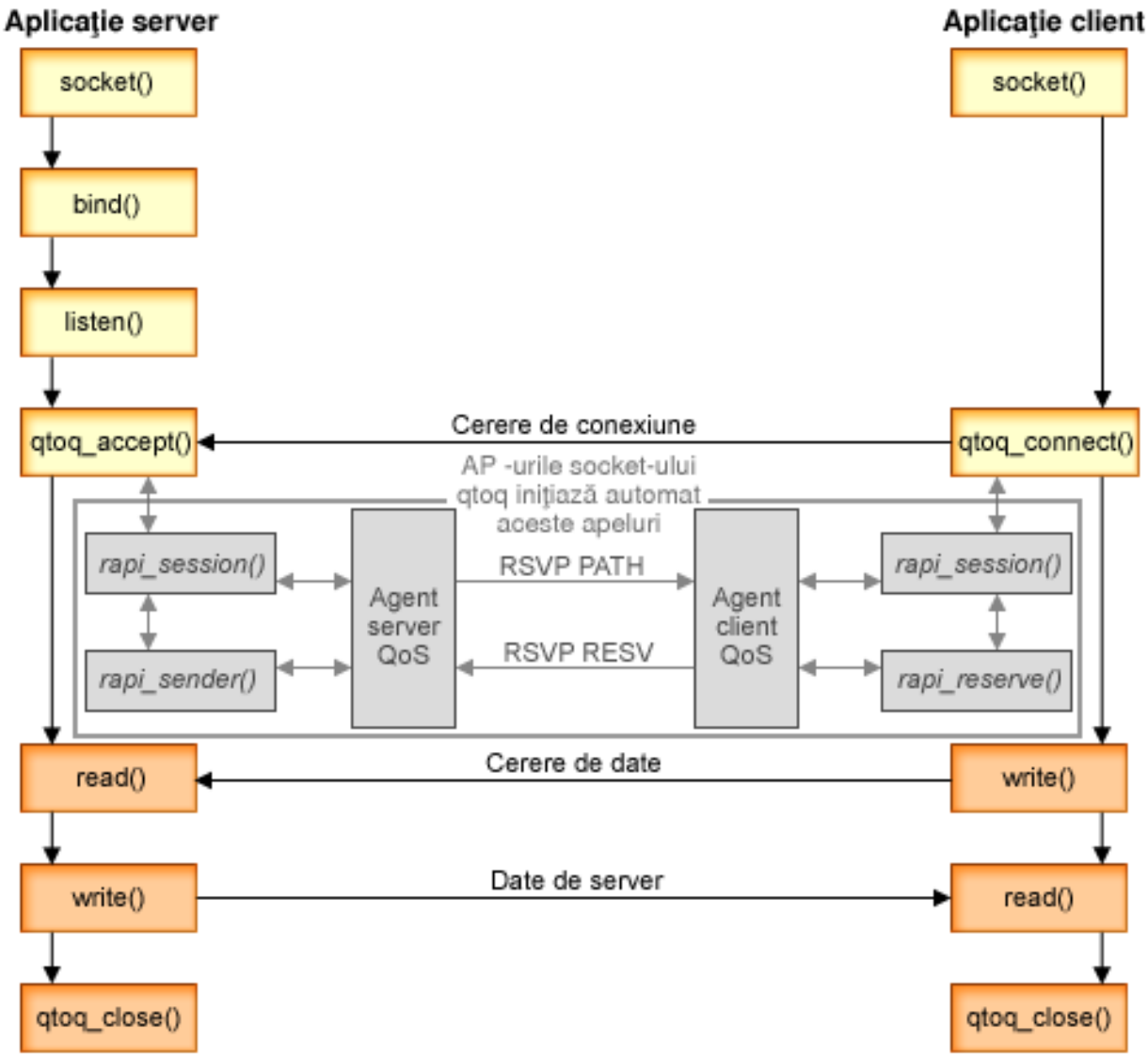
API-uri pentru setare a protocolului de rezervare resurse

"Configurarea QoS cu vrăjitori" la pagina 50
Pentru a configura politici QoS (quality of service), este necesar să folosiţi vrăjitorii QoS aflaţi în Navigator System i.

Flux funcţional orientat pe conexiune API QoS

Exemplele de server şi client ilustrează API-uri socket-ului QoS qtoq care au fost scrise pentru un flux funcţional orientat pe conexiune.

Când funcţiile API activate QoS sunt apelate pentru un flux orientat pe conexiune care cere ca RSVP să fie iniţiat, sunt iniţiate funcţii în plus. Aceste funcţii fac ca agenţii QoS de la server şi client să seteze RSVP-ul pentru fluxul de date dintre client şi server.



flux qtoq de evenimente: Următoarea secvenţă de apelări socket oferă o descriere a figurii. Descrie şi relaţia dintre aplicaţia de server şi client într-o proiecţie orientată pe conexiune. Acestea sunt modificări ale API-urilor socket de bază.

Parte a serverului

qtoq_accept() pentru o regulă marcată ″Fără semnalizare″

1. Aplicaţia apelează funcţia socket() pentru a obţine un descriptor de socket.
2. Aplicaţia apelează listen() pentru a specifica care sunt conexiunile pe care le aşteaptă.
3. Aplicaţia apelează qtoq_accept() pentru a aştepta o cerere de conexiune de la client.
4. API-ul apelează API-ul rapi_session(). Dacă are succes, un ID de sesiune QoS este asignat.
5. API-ul apelează funcţia standard accept() pentru a aştepta o cerere de conexiune a unui client.
6. Când este primită cererea de conexiune, este realizat controlul accesului pe regula cerută. Regula este trimisă stivei TCP/IP. Dacă este validă, regula se întoarce la aplicaţia apelantă cu rezultatele şi ID-ul sesiunii.
7. Aplicaţiile pentru server şi client realizează transferurile cerute de date.
8. Aplicaţia apelează funcţia qtoq_close() pentru a închide socket-ul şi pentru a descărca regula.

9. Serverul QoS va şterge regula din gestionarul QoS, sesiunea QoS şi va realiza orice acţiuni sunt necesare.

toq_accept() cu semnalizare normală RSVP

1. Aplicaţia apelează funcţia socket() pentru a obţine un descriptor de socket.
2. Aplicaţia apelează listen() pentru a specifica conexiunile pe care le aşteaptă.
3. Aplicaţia apelează qtoq_accept() pentru a aştepta o cerere de conexiune de la client.
4. Când o cerere de conexiune soseşte, API-ul rapi_session() este apelat pentru a crea o sesiune cu serverul QoS pentru această conexiune şi pentru a obţine ID-ul sesiunii QoS, care este returnat apelantului.
5. API-ul rapi_sender() este apelat pentru a iniţia un mesaj PATH de pe serverul QoS şi pentru a informa serverul QoS că trebuie să aştepte un mesaj RESV de la client.
6. API-ul rapi_getfd() este apelat pentru a obţine descriptorul pe care aplicaţiile îl folosesc pentru a aştepta pentru mesaje de evenimente QoS.
7. Descriptorul de acceptare şi descriptorul QoS sunt întorşi la aplicaţie.
8. Serverul QoS aşteaptă mesajul RESV să fie primit. Când mesajul este primit, serverul încarcă regula corespunzătoare cu managerul QoS şi trimite un mesaj aplicaţiei dacă aplicaţia a cerut notificare pentru apel API-uluiqtoq_accept().
9. Serverul QoS continuă să furnizeze reîmprospătări pentru sesiunea stabilită.
10. Aplicaţia apelează qtoq_close() când conexiunea este finalizată.
11. Serverul QoS va şterge regula din gestionarul QoS, sesiunea QoS şi va realiza orice acţiuni sunt necesare.

Partea client

API-ul qtoq_connect() cu semnalizare normală RSVP

1. Aplicaţia apelează funcţia socket() pentru a obţine un descriptor de socket.
2. Aplicaţia apelează funcţia qtoq_connect() pentru a informa aplicaţia de la server că doreşte să se realizeze o conexiune.
3. Funcţia qtoq_connect() apelează API-ul rapi_session() pentru a crea o sesiune cu serverul QoS pentru această conexiune.
4. Serverul QoS va trebui să aştepte întâi comanda PATH de la conexiunea cerută.
5. API-ul rapi_getfd() este apelat pentru a obţine descriptorul QoS pe care aplicaţiile îl folosesc pentru a aştepta mesaje QoS.
6. Funcţia connect() este apelată. Rezultatul de la connect() şi descriptorul QoS sunt returnate aplicaţiei.
7. Serverul QoS aşteaptă ca mesajul PATH să fie primit. Când este primit mesajul, va răspunde cu un mesaj RESV pentru serverul QoS de pe maşina server de aplicaţii.
8. Dacă aplicaţia a cerut notificare, serverul QoS va trimite notificarea la aplicaţie prin descriptorul QoS.
9. Serverul QoS continuă să furnizeze reîmprospătări pentru sesiunea stabilită.
10. Aplicaţia apelează qtoq_close() când conexiunea este finalizată.
11. Serverul QoS va închide sesiunea QoS şi va realiza orice alte acţiuni sunt necesare.

API-ul qtoq_connect() pentru o regulă marcată cu 'fără semnalizare'

Această cerere nu este validă pentru partea client, din moment ce nu se cere, în acest caz, nici un răspuns de la client.

Referinţe înrudite

qtoq_accept()--Acceptă API cu conexiune la socket-uri QoS

qtoq_close()--Închide API cu conexiune la socket-uri QoS

rapi_session()--Crearea unei sesiuni RAPI

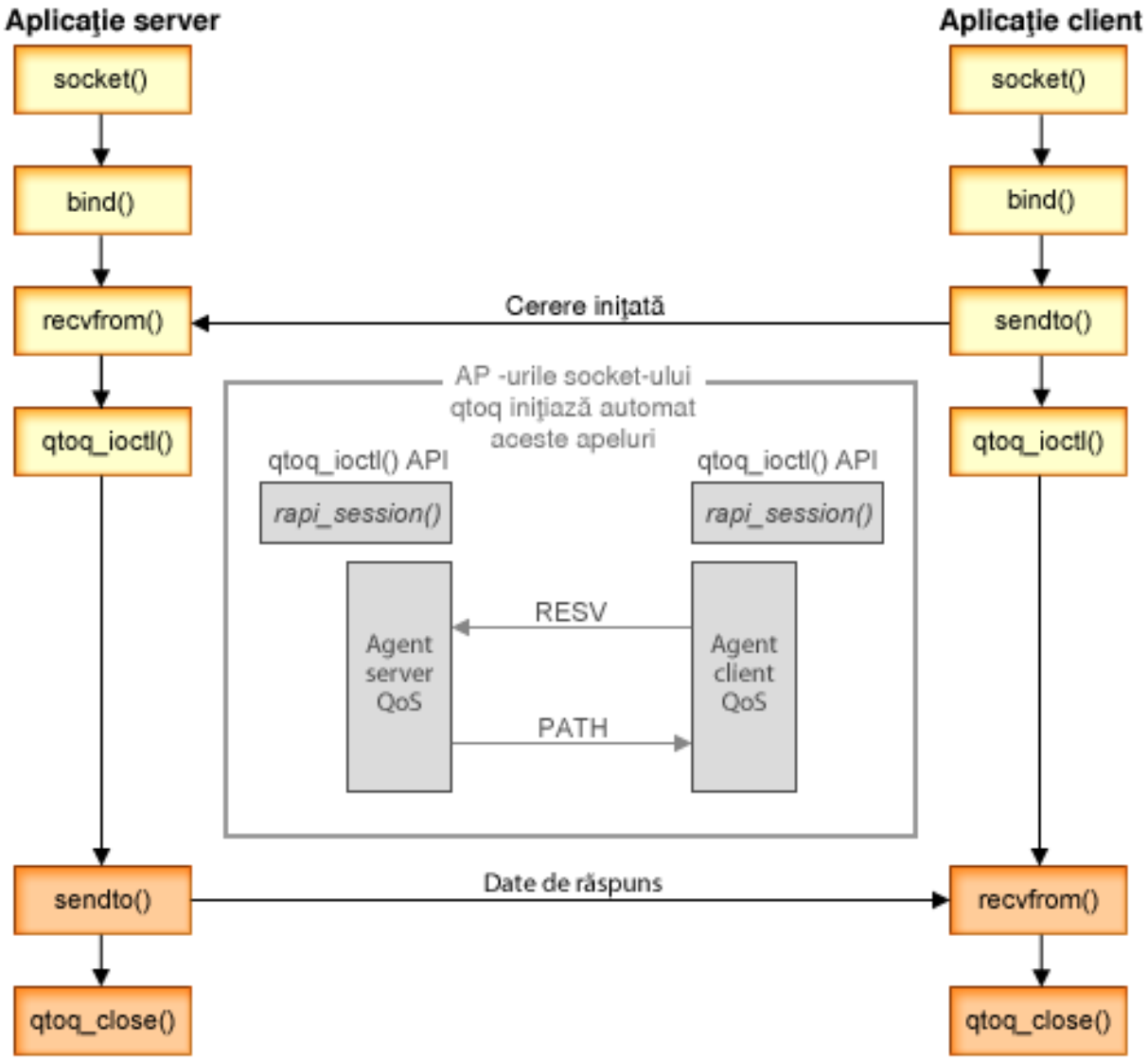
rapi_sender()--Identificarea unui expeditor RAPI

rapi_getfd()--Face ca descriptorul să însoţească pe

qtoq_connect()--Face API cu conexiune la socket-uri QoS

Flux funcţional fără conexiune API QoS

Când sunt apelate funcţiile API-ului QoS-activat pentru un flux fără conexiune care necesită ca RSVP (ReSerVation Protocol) să fie iniţiat, funcţii suplimentare sunt iniţiate. Aceste funcţii fac ca agenţii QoS de la client şi server să seteze RSVP pentru fluxul de date dintre clietn şi server.



Flux qtoq de evenimente: Următoarea secvenţă de apelări socket oferă o descriere a figurii. Descrie şi relaţia dintre aplicaţiile de server şi client într-un proiect fără conexiune. Acestea sunt modificări ale API-urilor socket de bază.

Parte server

qtoq_ioctl() pentru o regulă marcată ″Fără semnalizare″

1. API-ul qtoq_ioctl() trimite un mesaj către serverul QoS, cerându-i să realizeze un control de admitere asupra regulii cerute.
2. Dacă regula este acceptată, apelează o funcţie care trimite un mesaj la serverul QoS cerând ca regula să fie încărcată.
3. Serverul QoS returnează apoi starea către apelant indicând succesul sau eşecul cererii.

4. Când aplicaţia a terminat de folosit conexiunea, apelează funcţia qtoq_close() pentru a închide conexiunea.
5. Serverul QoS şterge regula din mangerul QoS, şterge sesiunea QoS şi realizează orice altă acţiune este necesară.

qtoq_ioctl() cu semnalizare normală RSVP

1. API-ul qtoq_ioctl() trimite mesaje către serverul QoS, cerând control de admitere pentru conexiunea cerută.
2. Serverul QoS apelează rapi_session() pentru a cere pornirea unei sesiunii pentru regulă şi returnarea ID-ului sesiunii QoS către apelant.
3. Acesta apelează rapi_sender() pentru a iniţia un mesaj PATH înapoi la client.
4. Acesta apoi apelează rapi_getfd() pentru a face ca descriptorul de fişier să aştepte evenimente QoS.
5. Serverul QoS returnează apelantului descriptorul select(), ID-ul de sesiune QoS şi starea.
6. Serverul QoS încarcă regula când este primit mesajul RESV.
7. Aplicaţia emite o qtoq_close() când conexiunea este finalizată.
8. Serverul QoS şterge regula din managerul QoS, şterge sesiunea QoS şi realizează orice altă acţiune necesară.

Partea clientului

qtoq_ioctl() cu semnalizare normală RSVP

1. API-ul qtoq_ioctl() apelează rapi_session() pentru a cere setarea unei sesiunii pentru conexiune. Funcţia rapi_session() cere control de admitere pentru conexiune. Conexiunea va refuzată doar de partea clientului dacă este o regulă configurată pentru client şi nu este activă în acest moment. Această funcţie întoarce ID-ul de sesiune QoS care este transmisă înapoi la aplicaţie.
2. Aceasta apelează rapi_getfd() pentru a face ca descriptorul de fişier să aştepte evenimente QoS.
3. qtoq_ioctl() se întoarce la apelant cu aşteptarea descriptorului şi ID-ul sesiunii.
4. Serverul QoS aşteaptă ca mesajul PATH să fie primit. Când este primit mesajul de cale, va răspunde cu mesajul RESV şi apoi va semnaliza aplicaţiei că s-a produs evenimentul prin descriptorul sesiunii.
5. Serverul QoS continuă să furnizeze reîmprospătări pentru sesiunea stabilită.
6. Codul client apelează qtoq_close() la finalizarea conexiunii.

qtoq_ioctl() pentru o regulă marcată ″Fără semnalizare″

Această cerere nu este validă pentru o parte de client, din moment ce nu se cere, în acest caz, nici un răspuns de la client.

Referinţe înrudite

qtoq_close()--Închide API cu conexiune la socket-uri QoS

rapi_session()--Crearea unei sesiuni RAPI

rapi_sender()--Identificarea unui expeditor RAPI

rapi_getfd()--Face ca descriptorul să însoţească pe

qtoq_ioctl()--Setare API opţiuni pentru control socket-uri QoS

Extensii ale API-ului QoS sendmsg()

Funcţia sendmsg() este folosită pentru a trimite date, date auxiliare sau o combinaţie a acestora printr-un socket conectat sau neconectat.

API-ul sendmsg() are permisiune pentru date de clasificare QoS (quality of service - Calitatea serviciului). Politicile QoS folosesc această funcţie pentru a defini un nivel de clasificare mai granular pentru traficul TCP/IP. Folosesc în special tipuri de date auxiliare care se aplică nivelului IP. Tipul de mesaj folosit este IP_QOS_CLASSIFICATION_DATA. Aceste date auxiliare pot fi folosite de către aplicaţie pentru a defini atribute pentru trafic într-o anumită conexiune TCP. În cazul în care atributele transmise de către aplicaţie se potrivesc cu atributele definite în politica QoS, atunci traficul TCP este restricţionat de către politică.

Folosiţi informaţiile de mai jos pentru a iniţializa structura IP_QOS_CLASSIFICATION_DATA:

- ip_qos_version: Indică versiunea structurii. Aceasta trebuie să fie completată folosind constanta *IP_QOS_CURRENT_VERSION*.
- ip_qos_classification_scope: Specifică un domeniu de nivel de conexiune (folosiţi constanta *IP_QOS_CONNECTION_LEVEL*) sau un domeniu de nivel mesaj (constanta *IP_QOS_MESSAGE_LEVEL*).

  Domeniul de nivel de conexiune indică faptul că nivelul de serviciu QoS obţinut prin intermediul clasificării acestui mesaj are efect şi pentru toate mesajele care urmează până la următoarea apelare sendmsg() care are date de clasificare. Domeniul de nivel mesaj indică faptul că nivelul de serviciu QoS asignat să fie folosit doar pentru mesajul de date inclus în această apelare a sendmsg(). Viitoare date trimise fără clasificare QoS de date moşteneşte nivelul de conexiune QoS asignat anterior (de la ultima clasificare de nivel de conexiune prin API-ul sendmsg() sau de la clasificarea originală a conexiunii TCP în timpul stabilirii conexiunii).
- ip_qos_classification_type: Această clasificare indică tipul datelor clasificate. O aplicaţie poate alege să trimită un jeton definit pentru aplicaţie, o prioritate sau ambele. Dacă este selectată ultima opţiune, cele două tipuri de clasificare selectate trebuie legate prin 'OR'. Pot fi specificate următoarele tipuri:
  - Clasificare pe bază de jeton definit de aplicaţie. Trebuie specificat un singur tip; în cazul în care se specifică mai mult de unul, rezultatele sunt imprevizibile.
    - IP_SET_QOSLEVEL_W_APPL_TOKEN_ASCII : Aceasta indică faptul că datele de clasificare sunt şiruri de caractere în format ASCII. La specificarea acestei opţiuni, jetonul de aplicaţie trebuie transmis în câmpul ip_qos_appl_token.

      Notă: În cazul în care aplicaţia trebuie să transmită valori numerice pentru datele de clasificare, trebuie să le convertească mai întâi în format ASCII tipăribil. Şirul specificat poate fi în format mixt şi este folosit exact în formatul specificat din motive de comparaţie.
    - IP_SET_QOSLEVEL_W_APPL_TOKEN_EBCDIC : La fel ca mai sus cu excepţia faptului că şirul este în format EBCDIC.

      Notă: IP_SET_QOSLEVEL_W_APPL_TOKEN_ASCII are performanţe ceva mai bune decât această opţiune deoarece datele aplicaţiei specificate în politică sunt salvate în format ASCII în interiorul stivei TCP/IP, astfel se elimină nevoia de a translata jetonul definit pentru aplicaţie pentru fiecare cerere sendmsg().
  - Clasificare a priorităţilor definite de aplicaţie. Trebuie specificat un singur tip, în cazul în care se specifică mai multe tipuri; rezultatele sunt imprevizibile.
    - IP_SET_QOSLEVEL_EXPIDITED: Indică faptul că se cere prioritate Urgenţă.
    - IP_SET_QOSLEVEL_HIGH: Indică faptul că se cere prioritate Înaltă.
    - IP_SET_QOSLEVEL_MEDIUM: Indică faptul că se cere prioritate Medie.
    - IP_SET_QOSLEVEL_LOW: Indică faptul că se cere prioritate joasă.
    - IP_SET_QOSLEVEL_BEST_EFFORT: Indică faptul că se cere prioritate Cel mai bun efort.
  - ip_qos_appl_token_len: lungimea ip_qos_appl_token.
  - ip_qos_appl_token: Acest câmp virtual urmează imediat câmpul ip_qos_classification_type. Şirul jeton de clasificare aplicaţie în format ASCII sau EBCDIC în funcţie de ce tip de IP_SET_QOSLEVEL_W_APPL_TOKEN_xxxx este specificat pentru tipul de clasificare. Acest câmp este referenţiat doar când este specificat un tip de jeton definit de aplicaţie. Acest şir nu trebuie să depăşească 128 de octeţi. În cazul în care se specifică o dimensiune mai mare, vor fi folosiţi doar primii 128 de octeţi. De asemenea, lungimea şirului este determinată pe baza valorii specificate pentru ' cmsg_len (cmsg_len - sizeof(cmsghdr) - sizeof(ip_qos_classification_data)). Această lungime calculată nu trebuie să includă caractere terminate cu null.

Concepte înrudite

"Servicii diferenţiate" la pagina 2
Acesta este primul tip de politică de lungime de bandă outbound pe care o puteţi crea pe sistemul dumneavoastră de operare. Serviciile diferenţiate împart traficul dumneavoastră pe clase. Pentru a realiza o politică de serviciu diferenţiat, este necesar să determinaţi cum doriţi să clasificaţi traficul dumneavoastră de reţea şi cum să trataţi diferitele clase.

"Clase prioritare: Cum să clasificaţi traficul de reţea" la pagina 3
Serviciul diferenţiat identifică traficul de reţea drept clase. Cele mai comune clase sunt definite utilizând adrese IP client, porturi de aplicaţie, tipuri de servere, protocoale, adrese locale IP şi planificări. Tot traficul care este în concordanţă cu aceeaşi clasă este tratat în mod egal.

Referinţe înrudite

API Sendmsg() - Trimiterea unui mesaj printr-un socket

Server director

Puteţi alege să exportaţi politicile dumneavoastră unui server director. Citiţi acest subiect pentru a vedea conceptele şi configuraţia LDAP (Lightweight Directory Access Protocol) cât şi schema QoS (quality of service).

Configurarea politicii QoS poate fi exportată pe un server director, folosind cel mai nou protocol LDAP, versiunea 3.

Cum se foloseşte un server de director

Exportarea politicilor QoS pe un server director face gestionarea politicilor dumneavoastră mai uşoară. Există trei moduri de folosire a serverului director:

- Datele de configurare pot fi stocate într-un server director local partajat între mai multe sisteme.
- Datele de configurare pot fi configurate, stocate şi folosite doar de un sistem (nepartajate).
- Datele de configurare pot să se afle pe un server director care ţine datele pentru alte sisteme dar nu este partajat între aceste sisteme. Aceasta permite să folosiţi o singură locaţie pentru salvarea datelor pentru mai multe sisteme.

Avantaje la salvarea exclusivă pe sistemul dumneavoastră local

Salvarea politicilor QoS în sistemul dumneavoastră local nu este atât de complexă. Există un număr de avantaje pentru folosirea locală a politicilor:

- Se elimină complexitatea configurării LDAP pentru utilizatorii care nu au nevoie de acesta.
- Se îmbunătăţeşte performanţa, din moment ce scrierea în LDAP nu este cea mai rapidă metodă.
- Duplicaţi mai uşor o configuraţie între diferite sisteme. Puteţi copia fişierul de pe un sistem pe altul. Deoarece nu există o maşină primară sau secundară, puteţi configura fiecare politică direct pe sistemele individuale.

Resurse LDAP

Dacă decideţi să exportaţi politicile dumneavoastră pe un server LDAP, trebuie să fiţi familiarizat cu conceptele LDAP şi cu structura de director înainte de a continua. În funcţia QoS din Navigator System i, puteţi configura un server de director care este folosit cu politica dumneavoastră QoS.

Concepte înrudite

IBM Tivoli Directory Server pentru i5/OS (LDAP)

"Configurare server de director" la pagina 52
Configuraţiile de politici QoS (Quality of service) pot fi exportate către un serve de director LDAP (Lightweight Directory Access Protocol), ceea ce face ca soluţiile dumneavoastră QoS să fie mai uşor de gestionat.

Cuvinte cheie

Atunci când configuraţi serverul de directoare, va trebui să determinaţi dacă să asociaţi cuvinte cheie fiecărei configuraţii QoS.

Câmpurile cuvânt cheie sunt opţionale şi pot fi ignorate.

În vrăjitorul Configurare iniţială QoS, puteţi configura serverul de directoare. Puteţi specifica dacă serverul pe care îl configuraţi este un sistem primar sau un sistem secundar. Serverul pe care vă păstraţi toate politicile QoS este cunoscut ca sistemul primar.

Cuvintele cheie sunt folosite pentru a identifica configuraţiile create de către sistemele primare. Deşi create de sisteme principale, cuvintele cheie sunt de fapt spre beneficiul sistemelor secundare. Acestea permit sistemelor secundare să încarce şi să folosească configuraţiile create de un sistem primar. Descrierile de mai jos vor ajuta explicarea folosirii cuvintelor cheie în fiecare sistem.

Cuvinte cheie şi sisteme principale
Cuvintele cheie sunt asociate configuraţiilor QoS create şi menţinute de un sistem principal. Ele sunt folosite pentru ca sistemele secundare să poată identifica o configuraţie creată de un sistem principal.

Cuvinte cheie şi sisteme secundare
Sistemele secundare folosesc cuvinte cheie pentru a căuta configuraţii. Sistemul secundar încarcă şi foloseşte configuraţii care sunt create de un sistem primar. Când configuraţi un sistem secundar, puteţi selecta anumite cuvinte cheie. Depinzând de cuvântul cheie selectat, sistemul secundar încarcă orice configuraţii asociate cu cuvântul cheie selectat. Aceasta permite sistemului secundar să încarce configuraţii create de mai multe sisteme principale.

Când începeţi să configuraţi serverul de director în Navigator System i, folosiţi taskul QoS Ajutor pentru instrucţiuni specifice.

Concepte înrudite

"Nume distinct"
Când doriţi să gestionaţi o parte a directorului dumneavoastră, vă referiţi la DN (distinguished name - nume distinctiv) sau (dacă alegeţi) la un cuvânt cheie.

"Configurare server de director" la pagina 52
Configuraţiile de politici QoS (Quality of service) pot fi exportate către un serve de director LDAP (Lightweight Directory Access Protocol), ceea ce face ca soluţiile dumneavoastră QoS să fie mai uşor de gestionat.

Nume distinct

Când doriţi să gestionaţi o parte a directorului dumneavoastră, vă referiţi la DN (distinguished name - nume distinctiv) sau (dacă alegeţi) la un cuvânt cheie.

Specificaţi DN-ul când configuraţi serverul director în vrăjitorul Configurare iniţială QoS. DN-urile sunt alcătuite, în mod obişnuit, din chiar numele intrării, cât şi din obiectele (de la vârf la bază) de deasupra intrării în director. Serverul poate accesa toate obiectele în director care sunt mai jos de DN. De exemplu, să zicem că serverul LDAP conţine structura de directoare din figura următoare:

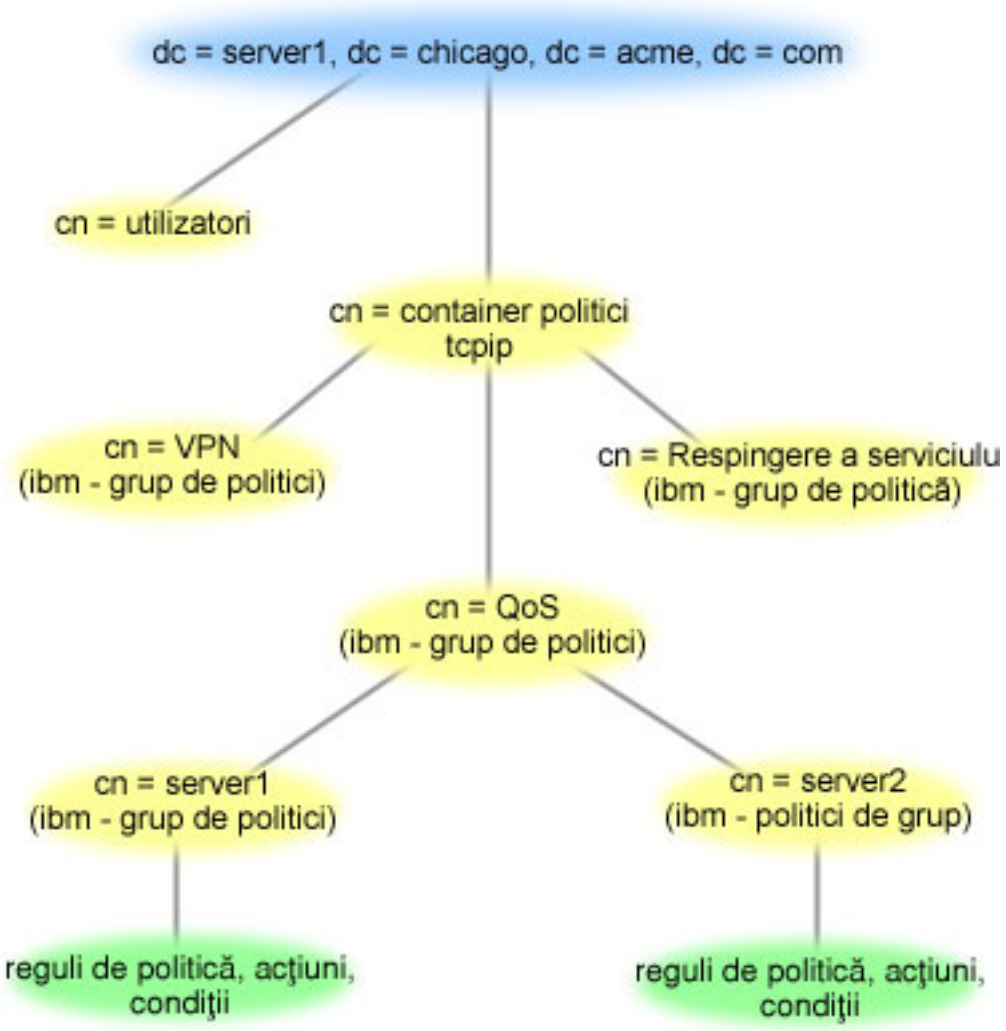


Figura 3. Exemplu de structură de directoare QoS

Server1 de sus (dc=server1, dc=chicago, dc=acme, dc=com) este serverul pe care se află serverul de directoare. Celelalte servere, cum sunt politicile cn=QoS sau cn=tcpip se află unde se află şi serverele QoS. Aşa că pe cn=server1 DN-ul implicit citeşte cn=server1, cn=QoS, cn=tcpip policies, dc=server1, dc=chicago, dc=acme, dc=com. Pe cn=server2 DN-ul implicit este cn=server2, cn=QoS, cn=tcpip policies, dc=server1, dc=chicago, dc=acme, dc=com.

Când vă gestionaţi directorul, este important să vă modificaţi serverul sorespunzător din DN, cum ar fi cn sau dc. Fiţi atent când editaţi DN-ul, mai ales pentru faptul că şirul este, de obicei, prea lung pentru a fi afişat fără derulare.

Concepte înrudite

“Cuvinte cheie” la pagina 24
Atunci când configuraţi serverul de directoare, va trebui să determinaţi dacă să asociaţi cuvinte cheie fiecărei configuraţii QoS.

“Configurare server de director” la pagina 52
Configuraţiile de politici QoS (Quality of service) pot fi exportate către un serve de director LDAP (Lightweight Directory Access Protocol), ceea ce face ca soluţiile dumneavoastră QoS să fie mai uşor de gestionat.

Referinţe înrudite

"Informaţii înrudite pentru Calitatea serviciului" la pagina 65
RFC-uri QoS, publicaţii IBM Redbooks, şi alte colecţii de subiecte din centrul de informare conţin informaţii care sunt înrudite cu colecţia de subiecte Calitatea serviciului. Puteţi vedea sau tipări oricare din fişierele PDF.

Scenarii: Politici QoS

Aceste scenarii de politici QoS (quality of service) vă pot ajuta să înţelegeţi de ce aveţi nevoie de QoS şi cum să creaţi politici şi clase de servicii.

Una dintre cele mai bune căi de a învăţa despre calitatea serviciului este a vedea cum lucrează funcţia într-o privire de ansamblu asupra reţelei. Exemplele următoare vă arată de ce este nevoie să folosiţi politici de QoS şi furnizează de asemenea anumiţi paşi cu instrucţiuni pentru crearea politicilor şi a claselor de serviciu.

Notă: Adresele IP şi diagramele sunt fictive şi sunt folosite doar ca exemple.

Concepte înrudite

"Monitorizare tranzacţii de sistem" la pagina 62
Cu monitorizarea QoS puteţi să verificaţi că politicile QoS funcţionează aşa cum doriţi dumneavoastră ca ele să funcţioneze. Monitorizarea QoS vă poate ajuta în faza de plănuire şi în faza de depanare a QoS.

Referinţe înrudite

"Monitorizarea QoS" la pagina 55
Puteţi folosi monitorizarea QoS (quality of service) pentru a analiza traficul dumneavoastră IP prin sistem.

Scenariu: Limitare trafic browser

Puteţi utiliza calitatea serviciului (QoS) pentru a controla performanţa traficului. Folosiţi o politică de servicii diferenţiate pentru a limita sau a extinde performanţa unei aplicaţii în reţea.

Situaţie

Compania dumneavoastră s-a confruntat cu niveluri înalte de trafic browser de la grupul de proiectare centrată pe utilizator (UCD), vinerea. Acest trafic interferează cu departamentul de contabilitate, care necesită şi el o bună performanţă pentru aplicaţiile de contabilitate vinerea. Decideţi să limitaţi traficul de browser de la grupul UCD. Următoarea figură ilustrează setarea reţelei în acest scenariu.

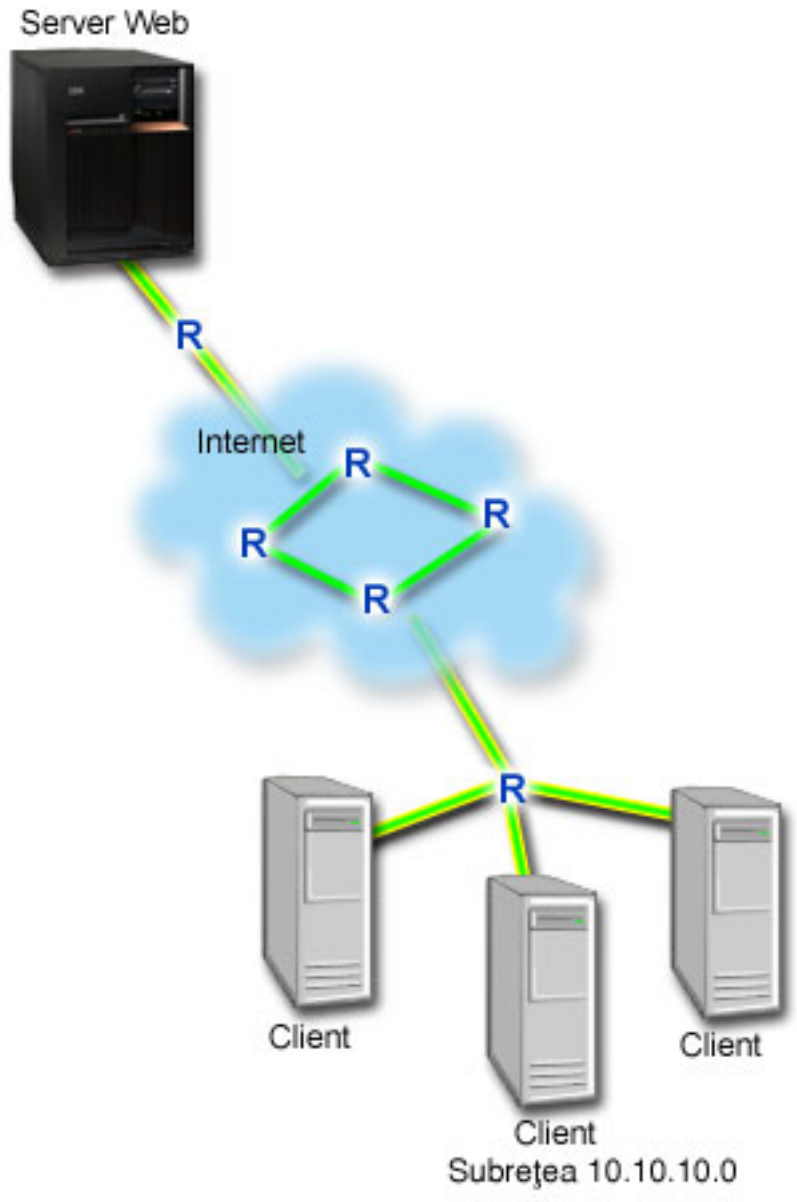


Figura 4. Serverul Web de limitare a traficului browser pentru un client

Obiective

Pentru a limita traficul browser în afara reţelei dumneavoastră, este posibil să creaţi o politică de servicii diferenţiate. O politică de servicii diferenţiate împarte traficul în clase. Tot traficul în această politică este alocat unui punct de cod. Acest punct de cod spune ruterelor cum să trateze traficul. În acest scenariu, politicii trebuie să-i fie alocată o valoare scăzută a punctului de cod pentru a afecta modul în care reţeaua favorizează traficul browser.

Cerinţe preliminare şi presupuneri

- Aveţi un SLA (service level agreement) cu ISP-ul (Internet service provider) dumneavoastră pentru a vă asigura că politicile primesc prioritatea cerută. Politica QoS pe care o creaţi pe sistem permite traficului (din politică) să primească prioritate în întreaga reţea. Politica QoS nu garantează aceasta şi este dependentă de SLA-ul dumneavoastră. De fapt, profitând de politicile QoS ar putea să vă ofere un avantaj în negocierea anumitor niveluri de servicii şi de rate.

- Politicile de servicii diferenţiate necesită ca ruterele să poată recunoaşte Servicii diferenţiate de-a lungul căii reţelei. Majoritatea ruterelor nu pot recunoaşte Servicii diferenţiate.

Configurare

După ce verificaţi paşii de pre-cereri, sunteţi pregătit să creaţi politica de servicii diferenţiate.

Concepte înrudite

"Acord la nivel de serviciu" la pagina 48
Acest subiect scoate în evidenţă unele din aspectele importante ale unui SLA (service level agreement) care ar putea afecta implementarea QoS-ului dumneavoastră. QoS este o soluţie de reţea. Pentru a obţine prioritate de reţea în afara reţelei dumneavoastră private, aţi putea avea nevoie de un SLA cu ISP-ul (Internet service provider) dumneavoastră.

"Servicii diferenţiate" la pagina 2
Acesta este primul tip de politică de lungime de bandă outbound pe care o puteţi crea pe sistemul dumneavoastră de operare. Serviciile diferenţiate împart traficul dumneavoastră pe clase. Pentru a realiza o politică de serviciu diferenţiat, este necesar să determinaţi cum doriţi să clasificaţi traficul dumneavoastră de reţea şi cum să trataţi diferitele clase.

Referinţe înrudite

"Monitorizarea QoS" la pagina 55
Puteţi folosi monitorizarea QoS (quality of service) pentru a analiza traficul dumneavoastră IP prin sistem.

Detalii scenariu: Crearea politicii de servicii diferenţiate

Acest subiect conţine informaţii despre configurarea unei politici de servicii diferenţiate în sistem.

1. În Navigator System i, expandaţi ***sistemul dumneavoastră*** → **Reţea** → **Politici IP**.
2. Faceţi clic dreapta pe **Calitatea serviciului** şi selectaţi **Configuraţie** pentru a deschide interfaţa QoS.
3. Pe interfaţa QoS, faceţi clic dreapta pe tipul de politică DiffServ şi selectaţi **Politică nouă** pentru a deschide vrăjitorul.
4. Citiţi pagina Bun venit şi faceţi clic pe **Următorul** pentru a merge la pagina Nume.
5. În câmpul **Nume**, introduceţi UCD. Opţional, puteţi introduce o descriere pentru a vă ajuta să vă amintiţi intenţia acestei politici. Faceţi clic pe **Următorul**.
6. Pe pagina Clienţi, selectaţi **Adresa sau adresele specifice** şi faceţi clic pe **Nou** pentru a vă defini clientul.
7. În fereastra Client nou, introduceţi următoarele informaţii şi apăsaţi **OK**:
   - **Nume**: UCD_Client
   - **Adresă IP şi mască**: 10.10.10.0 / 24

   După ce apăsaţi **OK**, vă întoarceţi la vrăjitorul de politică. Dacă aveţi clienţi creaţi anterior, ştergeţi-i şi verificaţi că doar clienţii relevanţi sunt selectaţi.
8. Pe pagina Cerere de date server, verificaţi că **Orice jeton** şi **Toate priorităţile** sunt selectate şi faceţi clic pe **Următorul**
9. În pagina Aplicaţii, selectaţi **Portul specific, intervalul de porturi sau tipul serverului** şi faceţi clic pe **Nou**.
10. În fereastra Aplicaţie nouă, introduceţi următoarele informaţii şi faceţi clic pe **OK** pentru a vă întoarce la vrăjitor:
    - **Nume**: HTTP
    - **Port**: 80
11. În pagina Aplicaţii, selectaţi **Protocol** şi verificaţi că **TCP** este selectat. Faceţi clic pe **Următorul**.
12. În pagina Adresă locală IP, verificaţi că **Toate adresele IP** este selectat şi faceţi clic pe **Următorul**.
13. În pagina Clasă diferenţiată de serviciu, faceţi clic pe **Nou** pentru a defini caracteristicile performanţă. Se deschide vrăjitorul Nouă clasă de servicii.
14. Citiţi pagina Bun venit şi apăsaţi **Următorul**.
15. În pagina Nume, introduceţi serviciu_UCD. Opţional, puteţi introduce o descriere pentru a vă ajuta să vă amintiţi intenţia acestei politici. Faceţi clic pe **Următorul**.

16. În pagina Tipul de serviciu, selectaţi **Doar ieşire** şi faceţi clic pe **Următorul**. Această clasă de servicii este folosită doar pentru politici outbound.
17. În pagina Marcaj de punct de cod DiffServ ieşire, selectaţi **Clasa 4** şi faceţi clic pe **Următorul**. Un comportament per-hop determină ce performanţe primeşte acest trafic de la rutere şi alte sisteme din reţea. Folosiţi Ajutorul asociat interfeţei pentru a vă ajuta în luarea deciziei.
18. În pagina Realizare măsurare a traficului outbound, verificaţi dacă este selectat **Da** şi apăsaţi **Următorul**.
19. În pagina Limite de control al ratei outbound, introduceţi următoarele informaţii şi faceţi clic pe **Următorul**:
    - **Dimensiunea găleţii de jeton**: 100 kilobiţi
    - **Limita ratei medii**: 512 kilobiţi pe secundă
    - **Limita ratei de vârf**: 1 megabit pe secundă
20. În pagina Trafic ieşire în-afara-profilului, selectaţi **Abandonare pachete UDP sau reducere a ferestrei de congestie TCP** şi faceţi clic pe **Următorul**.
21. Examinaţi informaţiile din rezumat ale clasei de servicii. Dacă este corect, faceţi clic pe **Sfârşit** pentru a crea clasa de serviciu. După ce faceţi clic pe **Sfârşit**, vă întoarceţi la vrăjitorul de politică şi clasa dumneavoastră de servicii este selectată. Faceţi clic pe **Următorul**.
22. În pagina Planificare, selectaţi **Activare în timpul programării selectate** şi apăsaţi **Nou** .
23. În fereastra Client nou, introduceţi următoarele informaţii şi apăsaţi **OK**:
    - **Nume**: Programare_UCD
    - **Moment al zilei**: Activare 24 de ore
    - **Ziua săptămânii**: Vineri
24. Apăsaţi **următor** pentru a vizualiza un rezumat al politicii. Dacă corespunde, faceţi clic pe **Sfârşit**. În fereastra Configurare server QoS, puteţi vedea noua politică listată în panoul din dreapta.

Detalii scenariu: Pornirea sau actualizarea serverului QoS

Acest subiect conţine informaţii despre pornirea sau actualizarea serverului QoS.

În fereastra Configuraţie server QoS (Quality of Service), selectaţi **Server → Pornire** sau **Server → Actualizare**.

Detalii scenariu: Verificarea că politica funcţionează

Este nevoie de o monitorizare pentru a verifica dacă politica funcţionează aşa cum aţi configurat-o.

1. În fereastra Configuraţie QoS (Quality of Service), selectaţi **Server → Monitorizare**. Fereastra Monitorizare QoS se deschide.
2. Selectaţi fişierul tip politică DiffServ. Acesta afişează toate politicile DiffServ. Selectaţi **UCD** din listă.

   Cele mai interesante câmpuri sunt câmpurile care îşi obţin datele din trafic. Asiguraţi-vă că verificaţi câmpurile total biţi, biţi în profil şi pachete în profil. Biţii în-afara-profilului indică când traficul depăşeşte valorile politică configurată. În politica servicii diferenţiate, numărul în-afara-profilului (pentru pachete UDP) indică numărul de biţi ce sunt abandonaţi. Pentru TCP, numărul în-afara-profilului indică numărul de biţi ce depăşesc rata găleată a jetonului, care sunt trimişi în reţea. Biţii nu sunt abandonaţi niciodată la pachetele TCP. Pachetele în-profil indică numărul de pachete controlate de această politică (de la momentul în care pachetul a fost pornit la ieşirea monitorului prezent).

   Valoarea pe care o alocaţi câmpului **Limită rată medie** este de asemenea importantă. Când pachetele depăşesc această limită, sistemul începe să renunţe la ele. Ca rezultat, biţii în-afara-profilului cresc. Aceasta vă arată că politica se comportă aşa cum aţi configurat-o să funcţioneze. Consultaţi “Monitorizarea QoS” la pagina 55 pentru o descriere a tuturor câmpurilor de monitorizare.

   Notă: Ţineţi minte că rezultatele sunt exacte doar când politica este activă. Verificaţi programarea pe care aţi specificat-o în politică.

Detalii scenariu: Modificarea proprietăţilor

După consultarea rezultatelor de la monitorizare, puteţi modifica proprietăţile oricărei politici sau clase de servicii pentru a ajunge la rezultatele dorite.

Pentru a modifica oricare din valorile pe care le-aţi creat în politică, urmaţi aceşti paşi:

1. În fereastra Configurare server QoS, selectaţi folderul **DiffServ**. Faceţi clic dreapta pe **UCD** din lista din panoul din dreapta şi selectaţi **Proprietăţi** pentru a edita politica. O fereastră Proprietăţi se deschide cu valorile care controlează politica generală.
2. Specificaţi valorile corespunzătoare.
3. Pentru a edita clasa de serviciu, selectaţi fişierul **Clase de serviciu** . Faceţi clic dreapta pe **serviciu_UCD** din lista din panoul din dreapta şi selectaţi **Proprietăţi** pentru a edita clasa de serviciu. O fereastră Proprietăţi QoS se deschide cu valorile care controlează gestionarea traficului.
4. Specificaţi valorile corespunzătoare.
5. Din fereastra Configurare server QoS, selectaţi **Server → Actualizare** pentru a accepta schimbările.

Scenariu: Rezultate sigure şi predictibile (VPN şi QoS)

Dacă folosiţi o reţea privată virtuală (VPN), puteţi crea şi politici de calitatea serviciilor.

Situaţie

Dumneavoastră aveţi un partener de afaceri conectat prin VPN şi doriţi să combinaţi VPN şi QoS pentru a furniza securitate şi flux previzibil e-business pentru date de misiune critică. Configuraţia QoS călătoreşte într-o singură direcţie. Prin urmare, aveţi o aplicaţie audio sau video, este nevoie să stabiliţi QoS pentru aplicaţie de ambele părţi ale conexiunii.

Ilustraţia arată serverul şi clientul într-o conectare VPN gazdă-la-gazdă. Fiecare R reprezintă rutere activate pe serviciu diferenţiate de-a lungul căii traficului. După cum vedeţi, politicile QoS merg într-o singură direcţie.

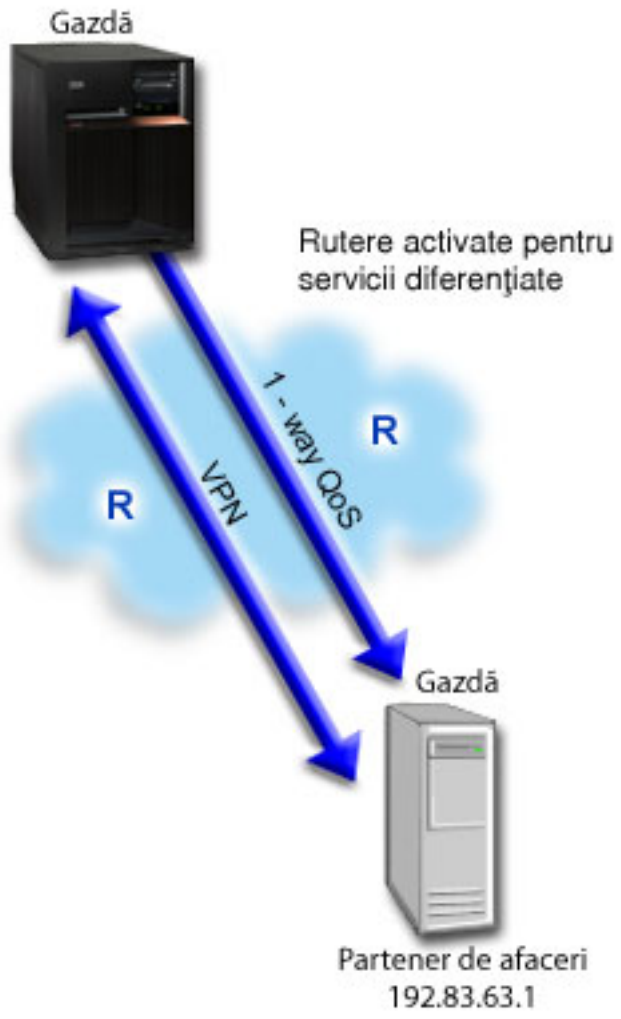


Figura 5. Conexiune gazdă-la-gazdă folosind o politică diferenţiată de servicii

Obiective

Aţi putea folosi VPN şi QoS pentru a stabili nu doar protecţie, cât şi prioritatea acestei conexiuni. Prima dată, setaţi o conexiune gazdă-la-gazdă VPN. Odată ce aveţi protecţia conexiunii VPN, puteţi seta politica QoS. Puteţi crea o politică de servicii diferenţiate. Acestei politici îi poate fi alocată o valoare mare a punctului de cod pentru a afecta modul în care reţeaua favorizează traficul misiune critică.

Cerinţe preliminare şi presupuneri

- Aveţi un SLA (service level agreement - acord la nivel de serviciu) cu ISP-ul (Internet service provider - furnizor de servicii internet) dumneavoastră pentru a vă asigura că politicile primesc prioritatea cerută. Politica QoS pe care o creaţi pe sistem permite traficului (din politică) să primească prioritate în întreaga reţea. Nu garantează aceasta şi este dependent de SLA-ul dumneavoastră. De fapt, profitând de politicile QoS ar putea să vă ofere un avantaj în negocierea anumitor niveluri de servicii şi de rate. Folosiţi legătura SLA pentru a afla mai multe.
- Politicile de servicii diferenţiate necesită rutere Servicii diferenţiate-activate de-a lungul căii reţelei. Majoritatea ruterelor sunt capabile Servicii diferenţiate.

Configurare

După ce verificaţi paşii de cerinţe preliminare, sunteţi gata să creaţi politica de Servicii diferenţiate.

Concepte înrudite

"Acord la nivel de serviciu" la pagina 48
Acest subiect scoate în evidenţă unele din aspectele importante ale unui SLA (service level agreement) care ar putea afecta implementarea QoS-ului dumneavoastră. QoS este o soluţie de reţea. Pentru a obţine prioritate de reţea în afara reţelei dumneavoastră private, aţi putea avea nevoie de un SLA cu ISP-ul (Internet service provider) dumneavoastră.

"Servicii diferenţiate" la pagina 2
Acesta este primul tip de politică de lungime de bandă outbound pe care o puteţi crea pe sistemul dumneavoastră de operare. Serviciile diferenţiate împart traficul dumneavoastră pe clase. Pentru a realiza o politică de serviciu diferenţiat, este necesar să determinaţi cum doriţi să clasificaţi traficul dumneavoastră de reţea şi cum să trataţi diferitele clase.

Referinţe înrudite

"Monitorizarea QoS" la pagina 55
Puteţi folosi monitorizarea QoS (quality of service) pentru a analiza traficul dumneavoastră IP prin sistem.

Detalii scenariu: Setarea unei conexiuni VPN gazdă-la-gazdă

Acest subiect conţine informaţii despre setarea unei conexiuni VPN gazdă-la-gazdă.

Consultaţi Scenariu: Conexiune elementară afacere la afacere, pentru a vă asista la configurarea VPN.

Detalii scenariu: Crearea politicii de servicii diferenţiate

Acest subiect conţine informaţii despre crearea politicii de servicii diferenţiate.

1. În Navigator System i, expandaţi ***sistemul dumneavoastră*** → **Reţea** → **Politici IP**.
2. Faceţi clic dreapta pe **Calitatea serviciului** şi selectaţi **Configuraţie** pentru a deschide interfaţa QoS.
3. În fereastra Configurare server QoS, faceţi clic dreapta pe DiffServ şi selectaţi **Politică nouă** pentru a deschide vrăjitorul.
4. Citiţi pagina Bun venit şi faceţi clic pe **Următorul** pentru a merge la pagina **Nume**.
5. În câmpul **Nume**, introduceţi VPN şi faceţi clic **Următorul**. Opţional, puteţi introduce o descriere pentru a vă ajuta să vă amintiţi intenţia acestei politici.
6. Pe pagina Clienţi, selectaţi **Adresa sau adresele specifice** şi faceţi clic pe **Nou** pentru a vă defini clientul.
7. În fereastra client nou, introduceţi următoarele informaţii:
   - **Nume**: Client_VPN
   - **adresa IP**: 192.83.63.1
   - Faceţi clic pe **OK** pentru a crea clientul şi a vă întoarce la vrăjitorul servicii diferenţiate.

   După ce apăsaţi **OK**, vă întoarceţi la vrăjitorul de politică. Dacă anterior aţi creat clienţi, faceţi clic pe aceştia şi verificaţi că sunt selectaţi doar clienţii relevanţi.
8. Pe pagina Cerere de date server, verificaţi că **Orice jeton** şi **Toate prioritățile** sunt selectate.
9. În pagina Aplicaţii, verificaţi că **Toate porturile** şi **Totul** sunt selectate.
10. Apăsaţi **Următorul**.
11. În pagina Adresă locală IP, se acceptă valoarea implicită şi se face clic pe **Următorul**.
12. În pagina Clasă diferenţiată de serviciu, faceţi clic pe **Nou** pentru a defini caracteristicile performanţă. Se deschide vrăjitorul Nouă clasă de servicii.
13. Citiţi pagina Bun venit şi apăsaţi **Următorul**.
14. În pagina Nume, introduceţi EF_VPN
15. În pagina Tipul de serviciu, selectaţi **Doar ieşire** şi faceţi clic pe **Următorul**. Această clasă de servicii este folosită doar pentru politici outbound.

16. În pagina Marcare punct de cod DiffServ outbound, selectaţi **Clasa 3**. Un comportament per-hop determină ce performanţe va primi acest trafic de la rutere şi alte sisteme din reţea. Folosiţi Ajutorul asociat interfeţei pentru a vă ajuta în luarea deciziei.
17. În pagina Realizare măsurătoare a traficului outbound, verificaţi dacă este selectat **Da**şi faceţi clic pe **Următorul**.
18. În pagina Limite de control al ratei outbound, introduceţi următoarele informaţii şi faceţi clic pe **Următorul**:
    - **Dimensiunea găleţii de jeton**: 100 kilobiţi
    - **Limita ratei medii**: 64 megabiţi pe secundă
    - **Limita ratei jetonului de vârf**: Fără limită
19. În pagina Trafic ieşire în-afara-profilului, selectaţi **Abandonare pachete UDP sau reducere a ferestrei de congestie TCP** şi faceţi clic pe **Mai departe**.
20. Consultaţi pagina de rezumat Clasă de servicii şi apăsaţi **Sfârşit** pentru a vă întoarce la vrăjitorul de politică.
21. În pagina Clasă diferenţiată de serviciu, verificaţi că este selectat **EF_VPN** şi apăsaţi **Următorul**.
22. În pagina Planificare, selectaţi **Activare în timpul programării selectate** şi apăsaţi pe **Nou** .
23. În fereastra Client nou, introduceţi următoarele informaţii şi apăsaţi **OK**:
    - **Nume**: FirstShift
    - **Moment al zilei**: Activ la orele specificate şi adăugaţi de la 9:00 a.m. la 5:00 p.m..
    - **Ziua săptămânii**: Activ în zilele specificate şi selectaţi de Luni până Vineri
24. În pagina Programare, faceţi clic pe **Următorul**.
25. Examinaţi informaţiile din rezumat. Dacă este corect, faceţi clic pe **Sfârşit** pentru a crea politica. Fereastra Configuraţie server QoS listează toate politicile care sunt create în sistem. După ce aţi finalizat vrăjitorul, politica este listată în panoul drept.

Detalii scenariu: Pornirea sau actualizarea serverului QoS

Acest subiect conţine informaţii despre pornirea sau actualizarea serverului QoS.

În fereastra configurare server QoS, selectaţi **Server → Pornire** sau **Server → Actualizare**.

Detalii scenariu: Verificarea că politica funcţionează

Este nevoie de o monitorizare pentru a verifica dacă politica funcţionează aşa cum aţi configurat-o.

1. În fereastra Configuraţie server QoS (Quality of Service), selectaţi **Server → Monitorizare**. Se deschide fereastra Monitorizare QoS.
2. Selectaţi tipul de politică de servicii diferenţiate. Acesta afişează toate politicile de servicii diferenţiate.

   Similar exemplului 1, cele mai interesante câmpuri sunt câmpurile care îşi obţin datele din trafic. Aceste câmpuri includ biţii total, biţii în-profil şi câmpurile pachete în-profil. Biţii în-afara-profilului indică când traficul depăşeşte valorile politică configurată. Pachetele în-profil indică numărul de pachete controlate de această politică. Este foarte important ce valori alocaţi câmpului de limitare a ratei medii. Când pachetele TCP depăşesc această limită, ele sunt trimise în reţea, până fereastra de congestie TCP poate fi redusă la punerea în coadă a pachetelor în-afara-profilului. Ca rezultat, biţii în-afara-profilului cresc. Diferenţa dintre această politică şi scenariul Limitare traficului browser că pachetele de aici sunt protejate folosind protocolul VPN. După cum vedeţi, QoS lucrează cu o conexiune VPN. Consultaţi “Monitorizarea QoS” la pagina 55 pentru o descriere a tuturor câmpurilor de monitorizare.

   Notă: Ţineţi minte că rezultatele sunt exacte doar când politica este activă. Verificaţi programarea pe care aţi specificat-o în politică.

Detalii scenariu: Modificarea proprietăţilor

După consultarea rezultatelor de la monitorizare, puteţi modifica proprietăţile oricărei politici sau clase de servicii pentru a ajunge la rezultatele dorite.

1. În fereastra Configurare server QoS, selectaţi folderul **DiffServ**. Faceţi clic dreapta pe **VPN** din lista din panoul din dreapta şi selectaţi **Proprietăţi** pentru a edita politica. O fereastră Proprietăţi se deschide cu valorile care controlează politica generală.
2. Specificaţi valorile corespunzătoare.

3. Pentru a edita clasa de serviciu, selectaţi fişierul **Clase de serviciu** . Faceţi clic dreapta pe **EF_VPN** din lista din panoul din dreapta şi selectaţi **Proprietăţi** pentru a edita clasa de serviciu. O fereastră Proprietăţi QoS se deschide cu valorile care controlează gestionarea traficului.
4. Specificaţi valorile corespunzătoare.
5. Din fereastra Configurare server QoS, selectaţi **Server → Actualizare** pentru a accepta schimbările.

Scenariu: Limitarea conexiunilor inbound

Dacă aveţi nevoie de un control al cererilor de conexiuni inbound care sunt făcute către sistemul dumneavoastră, folosiţi o politică de acces inbound.

Situaţie

Resursele dumneavoastră de server Web sunt suprapuse de cererile clientului care intră în reţeaua dumneavoastră. Vi se cere să încetiniţi traficul ce intră în serverul dumneavoastră Web pe interfaţa locală 192.168.1.1 QoS (Quality of service) vă poate ajută să restricţionaţi încercările acceptate de conexiune inbound, pe baza atributelor de conexiune (de exemplu, adresă IP) către sistemul dumneavoastră. Pentru a realiza asta, vă decideţi să faceţi o politică de acces inbound, care restricţionează numărul de conexiuni acceptate inbound.

Ilustraţia arată compania dumneavoastră şi o companie client. Această politică QoS poate controla doar fluxul de trafic într-o singură direcţie.

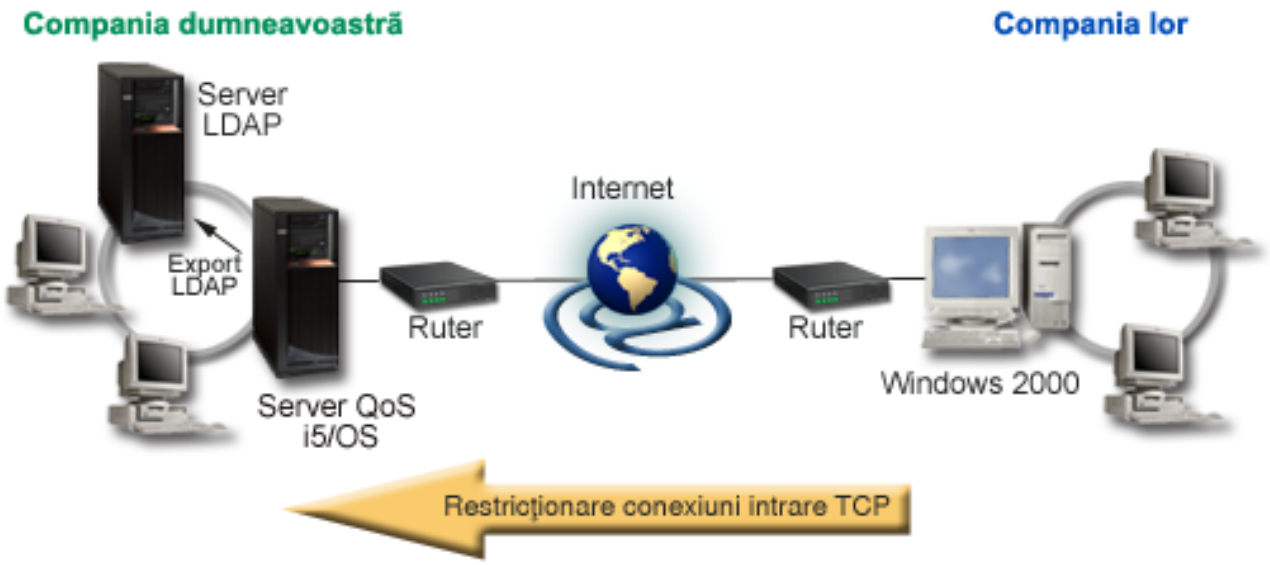


Figura 6. Restricţionare conexiuni intrare TCP

Obiective

Pentru a configura o politică inbound, trebuie să decideţi dacă restricţionaţi traficul pentru o interfaţă locală sau o aplicaţie particulară şi dacă îl restricţionaţi faţă de un anumit client. În acest caz, dumneavoastră doriţi să creaţi o politică care restricţionează încercări de conexiune de la Compania_lor către portul 80 (protocol HTTP) pe interfaţa dumneavoastră locală 192.168.1.1.

Configurare

Aceste subiecte arată cum se creează o politică de admitere interioară.

Referinţe înrudite

“Monitorizarea QoS” la pagina 55
Puteţi folosi monitorizarea QoS (quality of service) pentru a analiza traficul dumneavoastră IP prin sistem.

Detalii scenariu: Crearea politicii de acces inbound

Acest subiect conţine informaţii despre crearea unei politici de acces inbound în sistem.

1. În Navigator System i, expandaţi ***sistemul dumneavoastră*** → **Reţea** → **Politici IP**.
2. Faceţi clic dreapta pe **Calitatea serviciului** şi selectaţi **Configuraţie** pentru a deschide interfaţa QoS.
3. În fereastra Configurare server QoS, faceţi clic dreapta pe **Politici de acces inbound** selectaţi **Politică nouă** pentru a deschide vrăjitorul.
4. Citiţi pagina Bun venit şi apăsaţi **Următorul**.
5. În câmpul **Nume**, introduceţi Restrict_TheirCo şi faceţi clic **Următorul**. Opţional, puteţi introduce o descriere pentru a vă ajuta să vă amintiţi intenţia acestei politici.
6. Pe pagina Clienţi, selectaţi **Adresa sau adresele specifice** şi faceţi clic pe **Nou** pentru a vă defini clientul.
7. În fereastra client nou, introduceţi următoarele informaţii:
   - **Nume**: Their_Co
   - **Interval adresă IP**: 10.1.1.1 până la 10.1.1.10
   - Apăsaţi **OK** pentru a crea clientul şi a vă întoarce la vrăjitorul de politică.

   După ce faceţi clic pe **OK**, vă întoarceţi la vrăjitorul de politică. Dacă aţi avut clienţi creaţi anterior, ştergeţi-i şi verificaţi că doar clienţii relevanţi sunt selectaţi.
8. În pagina URI (Uniform Resource Identifier), verificaţi dacă **Orice URI** este selectat şi apăsaţi**Următor**.
9. În pagina Aplicaţii, selectaţi **Portul specific, intervalul de porturi sau tipul serverului** şi faceţi clic pe **Nou**.
10. În fereastra Aplicaţie nouă, introduceţi următoarele informaţii şi apăsaţi **OK** pentru a vă întoarce la vrăjitor:
    - **Nume**: HTTP
    - **Port**: 80
11. Apăsaţi **Următorul** pentru a deschide pagina Punct de cod.
12. În pagina Punct de cod, verificaţi că este selectat **Toate punctele cod** şi faceţi clic pe **Următorul**.
13. În pagina Adresă IP locală, selectaţi **adresă IP** şi selectaţi o interfaţă în care cererile sunt făcute către sistemul dumneavoastră local. În acest exemplu, folosiţi 192.168.1.1.
14. În pagina Clasă diferenţiată de serviciu, faceţi clic pe **Nou** pentru a defini caracteristicile performanţă. Se deschide vrăjitorul Nouă clasă de servicii.
15. Citiţi pagina Bun venit şi apăsaţi **Următorul**.
16. În pagina Nume, introduceţi **intrare** şi faceţi clic pe **Următorul**. Opţional, puteţi adăuga o descriere pentru a vă ajuta să vă amintiţi intenţia acestei clase de serviciu.
17. În pagina Tipul de serviciu, selectaţi **Doar intrare**. Această clasă de servicii va fi utilizată numai pentru politici inbound.
18. În pagina Limite inbound, introduceţi următoarele informaţii şi faceţi clic pe **Următorul**:
    - **Rata medie de conexiuni**: 50 pe secundă
    - **Limită rafală de conexiuni**: 50 conexiuni
    - **Prioritate**: Medie
19. Faceţi clic pe **Sfârşit** pentru a vă întoarce la vrăjitorul politică.
20. În pagina Clasă de serviciu, verificaţi faptul că este selectată clasa de serviciu pe care tocmai aţi creat-o şi apăsaţi **Mai departe**.
21. În pagina Planificare, selectaţi **Activare în timpul programării selectate** şi apăsaţi **Nou**.
22. În fereastra Client nou, introduceţi următoarele informaţii şi apăsaţi **OK**:
    - **Nume**: FirstShift
    - **Moment al zilei**: Activ la orele specificate şi adăugaţi de la 9:00 a.m. la 5:00 p.m..
    - **Ziua săptămânii**: Activ la zilele specificate şi selectaţi de Luni până Vineri.

23. În pagina Programare, apăsaţi **Următorul**.
24. Examinaţi informaţiile din rezumat. Dacă sunt exacte, apăsaţi **Sfârşit** pentru a crea politica. Configuraţie server QoS listează toate politicile care sunt create în sistem. După ce aţi finalizat vrăjitorul, politica este listată în panoul drept.

    Aţi terminate de configurat politica de acces inbound în sistemul dumneavoastră. Următorul pas este să porniţi sau să actualizaţi serverul.

Detalii scenariu: Pornirea sau actualizarea serverului QoS

Acest subiect conţine informaţii despre pornirea sau actualizarea serverului QoS.

În fereastra configurare server QoS, selectaţi **Server → Pornire** sau **Server → Actualizare**.

Detalii scenariu: Verificarea că politica funcţionează

Acest subiect conţine informaţii despre folosirea monitorizării pentru a verifica dacă politica funcţionează aşa cum aţi configurat-o să funcţioneze.

1. În fereastra Configuraţie QoS (Quality of Service), selectaţi **Server → Monitorizare**. Se deschide fereastra Monitorizare QoS.
2. Selectaţi tipul politică de acces inbound. Acesta afişează toate politicile de acces inbound. Selectaţi **Restrict_TheirCo** din listă.

   Asiguraţi-vă că verificaţi orice câmpuri măsurate, cum sunt cererile acceptate, cererile aruncate, cereri totale şi rata conexiunii. Cererile abandonate indică dacă traficul depăşeşte valorile politică configurată. Cererile acceptate indică numărul de biţi controlaţi de această politică (din momentul în care a fost pornit pachetul până la ieşirea de monitorizare actuală).

   Valoarea pe care o asignaţi câmpului **Rata medie cereri conexiune** este de asemenea importantă. Când pachetele depăşesc această limită, sistemul începe să renunţe la ele. Ca rezultat, cererile abandonate cresc. Aceasta vă arată că politica se comportă aşa cum aţi configurat-o. Consultaţi “Monitorizarea QoS” la pagina 55 pentru o descriere a tuturor câmpurilor de monitorizare.

   Notă: Ţineţi minte că rezultatele sunt exacte doar când politica este activă. Verificaţi programarea pe care aţi specificat-o în politică.

Detalii scenariu: Modificarea proprietăţilor

După consultarea rezultatelor de la monitorizare, puteţi modifica proprietăţile oricărei politici sau clase de servicii pentru a ajunge la rezultatele dorite.

1. În fereastra Configurare server QoS, selectaţi folderul **Acces inbound**. Faceţi clic dreapta pe **Restrict_TheirCot** din lista din panoul din dreapta şi selectaţi **Proprietăţi** pentru a edita politica. O fereastră Proprietăţi se deschide cu valorile care controlează politica generală.
2. Modificare a valorilor corespunzătoare.
3. Pentru a edita clasa de serviciu, selectaţi fişierul **Clase de serviciu** . Faceţi clic dreapta pe **intrare** din lista din panoul din dreapta şi selectaţi **Proprietăţi** pentru a edita clasa de serviciu. O fereastră Proprietăţi QoS se deschide cu valorile care controlează gestionarea traficului.
4. Specificaţi valorile corespunzătoare.
5. Din fereastra Configurare server QoS, selectaţi **Server → Actualizare** pentru a accepta schimbările.

Scenariu: Trafic B2B predictibil

Dacă aveţi nevoie de livrare predictibilă şi încă doriţi să cereţi o rezervare, folosiţi tot o politică de servicii integrate. Acest exemplu foloseşte un serviciu de încărcare controlat.

Situaţie

Departamentul de vânzări raportează că traficul din reţea nu se comportă după aşteptări. Sistemul de operare i5/OS al companiei dumneavoastră de operare se află într-un mediu B2B (business-to-business - afacere-la-afacere) care necesită servicii predictibile de afacere la cerere. Trebuie să furnizaţi tranzacţii predictibile clienţilor dumneavoastră.

Dumneavoastră doriţi să daţi unităţii vânzare o calitate mai înaltă a serviciilor pentru aplicaţiile lor de comandare în timpul celui mai aglomerat moment al zilei (între 10:00 a.m. şi 4:00 p.m.).

În ilustraţia de mai jos, echipa de vânzări este în reţeaua dumneavoastră privată. De-a lungul căii de trafic către un client B2B există rutere, recunoscute de protocolul ReSerVation (RSVP). Fiecare R reprezintă un ruter de-a lungul căii traficului.

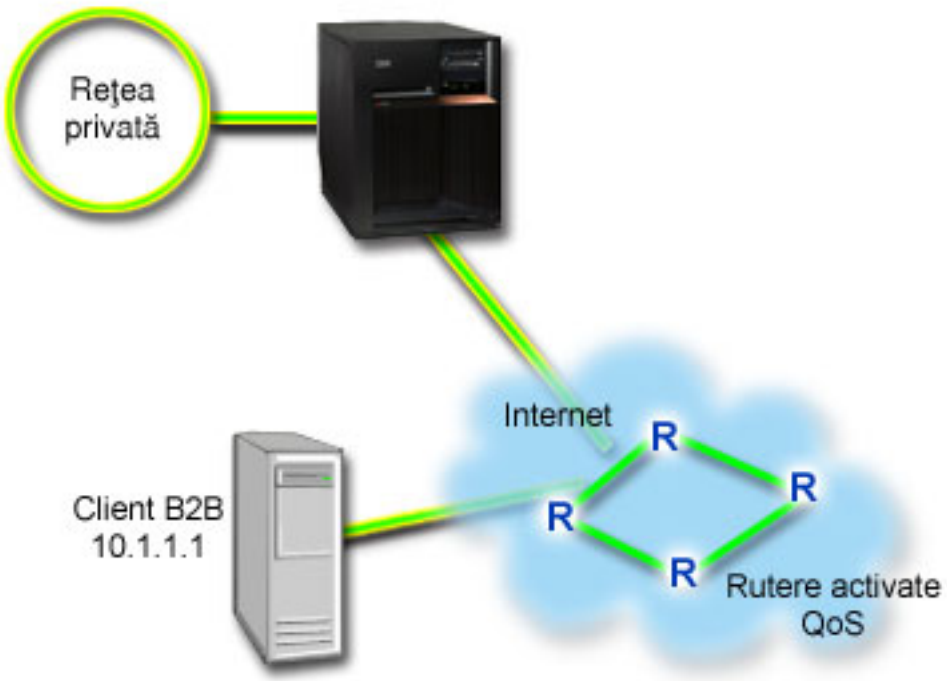


Figura 7. Politică de servicii integrate la un client B2B folosind rutere RSVP-activate.

Obiective

Serviciu cu încărcare controlată suportă aplicaţiile care sunt uşor sensibile la reţele congestionate, dar sunt încă tolerante la cantităţi mici de pierdere şi întârziere. Dacă o aplicaţie foloseşte serviciul de încărcare controlată, performanţa sa nu va suferi la creşterile de încărcare a reţelei. Traficul este prevăzut cu serviciu asemănător unui trafic normal într-o reţea în condiţii uşoare. Deoarece această aplicaţie tolerează unele întârzieri, decideţi să folosiţi o politică de servicii integrate folosind un serviciu de încărcare controlată.

Politicile de servicii integrate necesită de asemenea ca ruterele să fie RSVP-activate de-a lungul căii traficului.

Cerinţe preliminare şi presupuneri

O politică de servicii integrate este o politică avansată care nu poate cere resurse substanţiale. Politicile serviciilor integrate cer următoarele cerinţe preliminare:

- **Aplicaţii RSVP-activate**

  Deoarece sistemul dumneavoastră nu are nici o aplicaţie RSVP-activată, este nevoie să vă scrieţi propriile aplicaţii RSVP-activate. Pentru a scrie propriile dumneavoastră aplicaţii, folosiţi RAPI (RSVP API) sau API-urile socket-ului QoS qtoq sau API-urile serviciilor integrate.
- **Rutere şi sisteme RSVP-activate de-a lungul căii reţelei**

  QoS este o soluţie de reţea. Dacă nu sunteţi sigur că întreaga reţea are capabilităţi RSVP, încă mai puteţi crea o politică de servicii integrate şi să folosiţi o marcare pentru a-i da ceva prioritate; totuşi, prioritatea nu poate fi garantată.

- **Acord la nivel de serviciu**

  Aveţi un SLA (service level agreement - acord la nivel de serviciu) cu ISP-ul (Internet service provider - furnizor de servicii internet) dumneavoastră pentru a vă asigura că politicile primesc prioritatea cerută. Politicile QoS pe care le creaţi pe sistem permit traficului (în politică) să primească prioritate în întreaga reţea. Politica QoS nu garantează aceasta şi este dependentă de SLA-ul dumneavoastră. De fapt, profitând de politicile QoS vă poate oferi un avantaj în negocierea anumitor niveluri de servicii şi de rate.

  Notă: Dacă vă aflaţi într-o reţea privată, nu se cere un SLA.

Configurare

După ce verificaţi paşii de cerinţe preliminare, sunteţi pregătit să creaţi politica de servicii diferenţiate.

Concepte înrudite

"Tipuri de servicii integrate" la pagina 9
Există două tipuri de servicii integrate: încărcare controlată şi serviciu garantat.

"Servicii integrate" la pagina 6
Al doilea tip de politică de lungime de bandă outbound pe care îl puteţi crea este o politică de servicii integrate. Serviciile integrate furnizează pentru aplicaţiile IP capacitatea de a cere şi a rezerva lăţime de bandă prin utilizarea protocolului RSVP şi a API-urilor QoS.

"API-uri Calitatea serviciului" la pagina 16
Acest subiect conţine informaţii despre protocoale şi API-uri şi conţine cerinţele pentru un ruter care este activat pentru RSVP (ReSerVation Protocol). API-urile QoS (Quality of Service) includ API-ul RAPI, API-ul qtoq socket, API-ul sendmsg() şi API-urile monitor.

"Acord la nivel de serviciu" la pagina 48
Acest subiect scoate în evidenţă unele din aspectele importante ale unui SLA (service level agreement) care ar putea afecta implementarea QoS-ului dumneavoastră. QoS este o soluţie de reţea. Pentru a obţine prioritate de reţea în afara reţelei dumneavoastră private, aţi putea avea nevoie de un SLA cu ISP-ul (Internet service provider) dumneavoastră.

Referinţe înrudite

"Monitorizarea QoS" la pagina 55
Puteţi folosi monitorizarea QoS (quality of service) pentru a analiza traficul dumneavoastră IP prin sistem.

Detalii scenariu: Crearea politicii de servicii integrate

Acest subiect conţine informaţii despre crearea unei politici de servicii integrate în sistem.

1. În Navigator System i, expandaţi ***sistemul dumneavoastră*** → **Network** → **Politici IP**.
2. Faceţi clic dreapta pe **Calitatea serviciului** şi selectaţi **Configuraţie** pentru a deschide fereastra de configurare a serverului QoS.
3. În fereastra Configurare server QoS, faceţi clic dreapta pe tipul de politică IntServ şi selectaţi **Politică nouă** pentru a deschide vrăjitorul.
4. Citiţi pagina Bun venit şi faceţi clic pe **Următorul** pentru a merge la pagina **Nume**.
5. În câmpul **Nume**, introduceţi B2B_CL şi faceţi clic **Următorul**. Opţional, puteţi introduce o descriere pentru a vă ajuta să vă amintiţi intenţia acestei politici.
6. Pe pagina Clienţi, selectaţi **Adresa sau adresele specifice** şi faceţi clic pe **Nou** pentru a vă defini clientul.
7. În fereastra Client nou, introduceţi următoarele informaţii:
   - **Nume**: client_CL
   - **adresa IP**: 10.1.1.1
   - Apăsaţi **OK** pentru a crea clientul şi a vă întoarce la vrăjitorul de politică.

   După ce faceţi clic pe **OK**, vă întoarceţi la vrăjitorul de politică. Dacă aveţi clienţi creaţi anterior, ştergeţi-i şi verificaţi că doar clienţii relevanţi sunt selectaţi.
8. În fereastra Aplicaţie nouă, introduceţi următoarele informaţii şi apăsaţi **OK** pentru a vă întoarce la vrăjitor:
   - **Nume**: aplic_afacere

- **Intervalul de port**: 7000-8000

9. În pagina Aplicaţii, selectaţi **Protocol** şi verificaţi că **TCP** este selectat. Apăsaţi **Următorul**.

   Notă: Aplicaţia pe care o selectaţi pentru o politică de servicii integrate trebuie să fie scrisă pentru a utiliza API-ul RAPI sau API-ul socket-uri qtoq. Alături de protocolul de rezervare a resurselor (ReSerVation Protocol), aceste API-uri realizează rezervarea serviciilor integrate prin reţea. Dacă nu folosiţi aceste API-uri, aplicaţia nu va primi nici o garanţie sau prioritate. Este important, de asemenea, să observaţi că această politică activează aplicaţiile dumneavoastră pentru a primi prioritate prin reţea, dar nu o pot garanta. Toate ruterele şi sistemele de-a lungul căii traficului trebuie de asemenea să folosească RSVP-ul pentru a garanta o rezervare. O rezervare capăt-la-capăt este dependentă de participare prin reţea.

10. În pagina Adresă locală IP, se acceptă valoarea implicită şi se face clic pe **Următorul**.
11. În pagina Tipul serviciilor integrate, selectaţi **Încărcare controlată** şi faceţi clic pe **Următorul**.
12. În pagina Marcaj servicii integrate, selectaţi **Nu, nu alocaţi un comportament per-hop** şi faceţi clic pe **Următorul**.
13. În pagina Limite ale performanţei servicii integrate, introduceţi următoarele informaţii şi faceţi clic pe **Următorul**:
    - **Numărul maxim de fluxuri**: 5
    - **Limita ratei jetonului (R)**: Fără limită
    - **Dimensiunea găleţii de jeton**: 100 kilobiţi
    - **Limita ratei jetonului (R)**: 25 megabiţi pe secundă
14. În pagina Planificare, selectaţi **Activare în timpul programării selectate** şi apăsaţi **Nou** .
15. În pagina Programare nouă, introduceţi următoarele informaţii şi faceţi clic pe **OK**:
    - **Nume**: primetime
    - **Moment al zilei**: Activ la orele specificate şi adăugaţi de la 10:00 a.m. la 4:00 p.m..
    - **Ziua săptămânii**: Activ în zilele specificate şi selectaţi de Luni până Vineri.
16. În pagina Programare, apăsaţi **Următorul**.
17. Examinaţi informaţiile din rezumat. Dacă este corect, faceţi clic pe **Sfârşit** pentru a crea politica. Interfaţa principală QoS listează toate politicile care sunt create în sistem. După ce aţi completat vrăjitorul, politica este listată în panoul drept.

Aţi terminat configurarea politicii de servicii integrate în sistemul dumneavoastră. Următorul pas este să porniţi sau să actualizaţi serverul.

Detalii scenariu: Pornirea sau actualizarea serverului QoS

Acest subiect conţine informaţii despre pornirea sau actualizarea serverului QoS.

În fereastra configurare server QoS, selectaţi **Server → Pornire** sau **Server → Actualizare**.

Detalii scenariu: Verificarea că politica funcţionează

Acest subiect conţine informaţii despre folosirea monitorizării pentru a verifica dacă politica funcţionează aşa cum aţi configurat-o să funcţioneze.

1. În fereastra Configuraţie server QoS (Quality of Service), selectaţi **Server → Monitorizare**. Se deschide fereastra Monitorizare QoS.
2. Selectaţi tipul de politică de servicii integrate. Acesta afişează toate politicile de servicii integrate.

   Cele mai interesante câmpuri sunt câmpurile care îşi obţin datele din trafic. Asiguraţi-vă că verificaţi biţii total, biţii în-profil şi pachete în-profil. Biţii în-afara-profilului vor indică faptul că traficul intră în întârziere sau este abandonat pentru a satisface aceste cereri de politică de servicii integrate. Pentru o descriere completă a câmurilor monitorului, consultaţi “Monitorizarea QoS” la pagina 55.

Notă: Ţineţi minte că rezultatele sunt exacte doar când politica este activă. Verificaţi programarea pe care aţi specificat-o în politică. De asemenea, monitorizarea afişează politicile de servicii integrate doar după ce aplicaţiile rulează. O rezervare RSVP trebuie să fie stabilită înainte de monitorizare.

Detalii scenariu: Modificarea proprietăţilor

După examinarea rezultatelor monitorizării, puteţi modifica orice proprietăţi ale politicii pentru a ajunge la rezultatele dorite.

1. În fereastra Configurare server QoS, selectaţi folderul **IntServ**. Faceţi clic dreapta pe **B2B_CLt** din lista din panoul din dreapta şi selectaţi **Proprietăţi** pentru a edita politica. O fereastră Proprietăţi se deschide cu valorile care controlează politica generală.
2. Specificaţi valorile corespunzătoare.
3. Din fereastra Configurare server QoS, selectaţi **Server → Actualizare** pentru a accepta schimbările.

Scenariu: Livrarea dedicată (telefonie IP)

Dacă aveţi nevoie de livrare dedicată şi doriţi să cereţi o rezervare, folosiţi o politică de servicii integrate. Există două tipuri de politici de servicii integrate ce pot fi create: încărcare garantată şi controlată. În acest exemplu, este folosit serviciul garantat.

Situaţie

Directorul executiv al companiei dumneavoastră urmează să ţină o transmisie în direct către un client aflat în cealaltă parte a regiunii între 1:00 p.m. şi 2:00 p.m. Este nevoie să garantaţi ca telefonia IP să aibă o lăţime de bandă asigurată, astfel încât să nu existe întreruperi în timpul transmisiei. În acest scenariu, aplicaţia se află pe server.

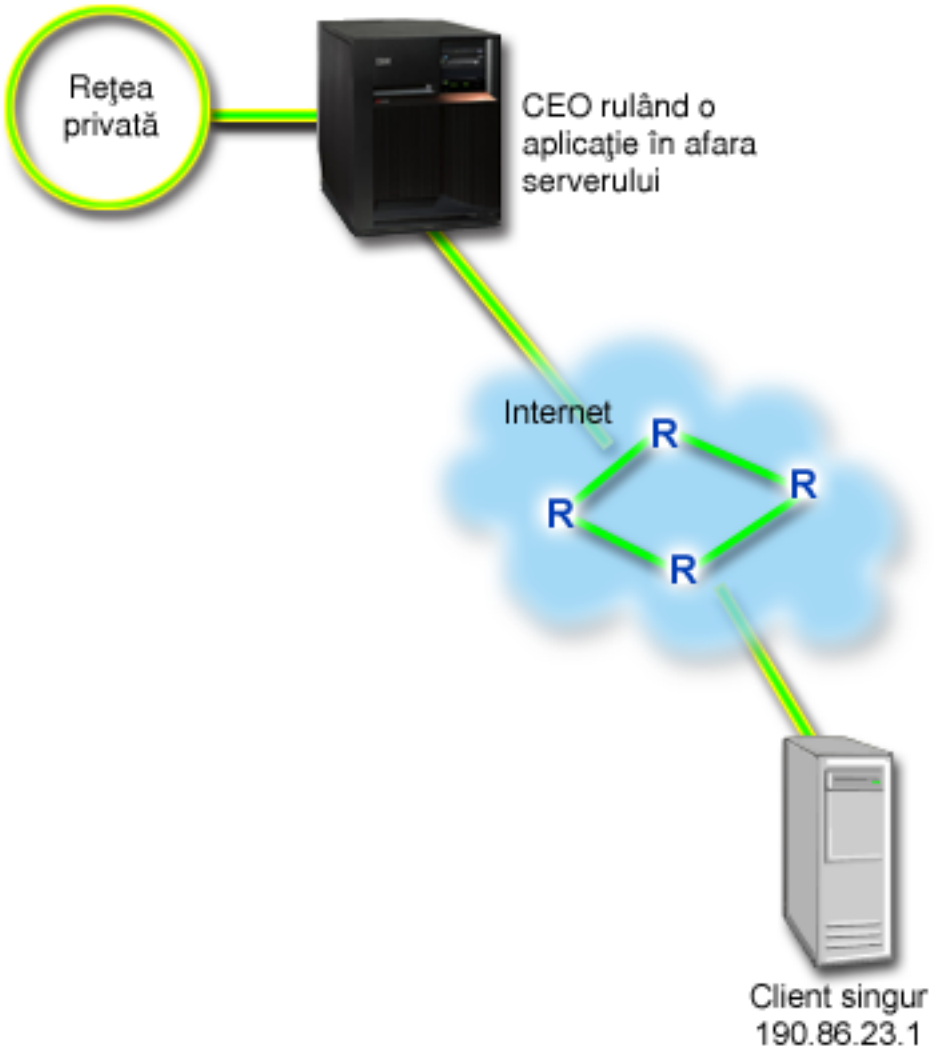


Figura 8. Prezentarea CEO pentru un client, garantată de o politică de servicii integrate.

Obiective

Deoarece aplicaţia folosită de către CEO-ul dumneavoastră utilizează un transfer fluent şi neîntrerupt, vă decideţi să folosiţi o politică de servicii integrate garantate. Serviciul garantat controlează întârzierea maximă de punere în coadă, astfel încât pachetele nu sunt întârziate mai mult de o anumită durată de timp.

Cerinţe preliminare şi presupuneri

O politică de servicii integrate este o politică avansată care nu poate cere resurse substanţiale. Politicile serviciilor integrate cer următoarele cerinţe preliminare:

- **Aplicaţii activate RSVP**

  Deoarece sistemul dumneavoastră nu are nici o aplicaţie cu RSVP-activat, este nevoie să vă scrieţi propriile aplicaţii cu RSVP-activat. Pentru a scrie propriile dumneavoastră aplicaţii, folosiţi API-ul RAPI (ReSerVation Protocol) sau APi-urile socket-ului QoS qtoq. Pentru informaţii suplimentare, consultaţi “API-uri Calitatea serviciului” la pagina 16 şi căutaţi API-urile pentru servicii integrate.
- **Rutere şi sisteme cu RSVP-activat de-a lungul căii reţelei**

QoS este o soluţie de reţea. Dacă nu sunteţi sigur că întreaga reţea are capabilităţi RSVP, încă mai puteţi crea o politică de servicii integrate şi să folosiţi o marcare pentru a-i da ceva prioritate; totuşi, prioritatea nu poate fi garantată.

- **Acord la nivel de serviciu**

  Aveţi un SLA (service level agreement - acord la nivel de serviciu) cu ISP-ul (Internet service provider - furnizor de servicii internet) dumneavoastră pentru a vă asigura că politicile primesc prioritatea cerută. Politicile QoS pe care le creaţi pe sistem permit traficului (în politică) să primească prioritate în întreaga reţea. Politica QoS nu garantează aceasta şi este dependentă de SLA-ul dumneavoastră. De fapt, profitând de politicile QoS vă poate oferi un avantaj în negocierea anumitor niveluri de servicii şi de rate.

Configurare

După ce verificaţi paşii de cerinţe preliminare, sunteţi pregătit să creaţi politica de servicii diferenţiate.

Concepte înrudite

“Tipuri de servicii integrate” la pagina 9
Există două tipuri de servicii integrate: încărcare controlată şi serviciu garantat.

“Servicii integrate” la pagina 6
Al doilea tip de politică de lungime de bandă outbound pe care îl puteţi crea este o politică de servicii integrate. Serviciile integrate furnizează pentru aplicaţiile IP capacitatea de a cere şi a rezerva lăţime de bandă prin utilizarea protocolului RSVP şi a API-urilor QoS.

“Acord la nivel de serviciu” la pagina 48
Acest subiect scoate în evidenţă unele din aspectele importante ale unui SLA (service level agreement) care ar putea afecta implementarea QoS-ului dumneavoastră. QoS este o soluţie de reţea. Pentru a obţine prioritate de reţea în afara reţelei dumneavoastră private, aţi putea avea nevoie de un SLA cu ISP-ul (Internet service provider) dumneavoastră.

Referinţe înrudite

“Monitorizarea QoS” la pagina 55
Puteţi folosi monitorizarea QoS (quality of service) pentru a analiza traficul dumneavoastră IP prin sistem.

Detalii scenariu: Crearea politicii de servicii integrate

Acest subiect conţine informaţii despre crearea unei politici de servicii integrate în sistem.

1. În Navigator System i, expandaţi ***sistemul dumneavoastră*** → **Reţea** → **Politici IP**.
2. Faceţi clic dreapta pe **Calitatea serviciului** şi selectaţi **Configuraţie** pentru a deschide interfaţa QoS.
3. În fereastra Configurare server QoS, faceţi clic dreapta pe tipul de politică IntServ şi selectaţi **Politică nouă** pentru a deschide vrăjitorul.
4. Citiţi pagina Bun venit şi faceţi clic pe **Următorul** pentru a merge la pagina **Nume**.
5. În câmpul **Nume**, introduceţi CEO_garantat şi faceţi clic **Următorul**. Opţional, puteţi introduce o descriere pentru a vă ajuta să vă amintiţi intenţia acestei politici.
6. Pe pagina Clienţi, selectaţi **Adresa sau adresele specifice** şi faceţi clic pe **Nou** pentru a vă defini clientul.
7. În fereastra Client nou, introduceţi următoarele informaţii:
   - **Nume**: Ramură1
   - **adresa IP**: 190.86.23.1
   - Faceţi clic pe **OK** pentru a crea clientul şi a vă întoarce la vrăjitorul servicii integrate.

   După ce faceţi clic pe OK, vă întoarceţi la vrăjitorul politică. Dacă aveţi clienţi creaţi anterior, ştergeţi-i şi verificaţi că doar clienţii relevanţi sunt selectaţi. În pagina Aplicaţii, selectaţi **Portul specific, intervalul de porturi sau tipul serverului** şi faceţi clic pe **Nou**.
8. În fereastra Aplicaţie nouă, introduceţi următoarele informaţii şi apăsaţi **OK** pentru a vă întoarce la vrăjitor:
   - **Nume**: telefonie IP
   - **Port**: 2427
9. În pagina Aplicaţii, selectaţi **Protocol** şi verificaţi că **TCP** este selectat. Apăsaţi **Următorul**.

Notă: Aplicaţia pe care o selectaţi pentru o politică de servicii integrate trebuie să fie scrisă pentru a utiliza API-ul RAPI şi API-ul socket-uri qtoq. Alături de protocolul de rezervare RSVP, aceste API-uri realizează rezervarea serviciilor integrate prin reţea. Dacă nu utilizaţi aceste API-uri, aplicaţia nu va primi nici o prioritate sau garantare. Este important, de asemenea, să observaţi că această politică activează aplicaţiile dumneavoastră pentru a primi prioritate prin reţea, dar nu o pot garanta. Toate ruterele şi serverele de-a lungul căii traficului trebuie de asemenea să folosească RSVP-ul pentru a garanta o rezervare. O rezervare capăt-la-capăt este dependentă de participare prin reţea.

10. În pagina Adresă locală IP, se acceptă valoarea implicită **Toate adresele IP**.
11. În pagina Tipul serviciilor integrate, selectaţi **Garantat** şi faceţi clic pe **Următorul**.
12. În pagina Marcaj servicii integrate, selectaţi **Nu, nu alocaţi un comportament per-hop** şi faceţi clic pe **Următorul**.
13. În pagina Limite ale performanţei servicii integrate, introduceţi următoarele informaţii şi faceţi clic pe **Următorul**:
    - **Numărul maxim de fluxuri**
    - **Limita agregată a lăţimii de bandă(R)**: Nu se limitează
    - **Dimensiunea găleţii de jeton**: 100 kilobiţi
    - **Limita lăţimii de bandă (R)**: 16 megabiţi pe secundă
14. În pagina Planificare, selectaţi **Activare în timpul programării selectate** şi apăsaţi **Nou** .
15. În pagina Programare nouă, introduceţi următoarele informaţii şi faceţi clic pe **OK**:
    - **Nume**: o_oră
    - **Moment al zilei**: Activ la orele specificate şi adăugaţi de la 1:00 p.m. la 2:00 p.m..
    - **Ziua săptămânii**: Activ în ziua specificată şi selectaţi Luni.
16. În pagina Programare, faceţi clic pe **Următorul**.
17. Examinaţi informaţiile din rezumat. Dacă este corect, faceţi clic pe **Sfârşit** pentru a crea politica. Fereastra principală Configurare server QoS listează toate politicile create pe server. După ce aţi completat vrăjitorul, politica este listată în panoul drept.

Aţi terminat configurarea politicii de servicii integrate în sistemul dumneavoastră. Următorul pas este să porniţi sau să actualizaţi serverul.

Detalii scenariu: Pornirea sau actualizarea serverului QoS

Acest subiect conţine informaţii despre pornirea sau actualizarea serverului QoS.

În fereastra configurare server QoS, selectaţi **Server → Pornire** sau **Server → Actualizare**.

Detalii scenariu: Verificarea că politica funcţionează

Acest subiect conţine informaţii despre folosirea monitorizării pentru a verifica dacă politica funcţionează aşa cum aţi configurat-o să funcţioneze.

1. În fereastra Configuraţie server QoS (Quality of Service), selectaţi **Server → Monitorizare**. Se deschide fereastra Monitorizare QoS.
2. Selectaţi folderul tip de politică de servicii integrate. Acesta afişează toate politicile de servicii integrate.

   Cele mai interesante câmpuri sunt câmpurile măsurate care îşi obţin datele din trafic. Aceste câmpuri includ biţii total, biţii în-profil şi pachete în-profil. Biţii în-afara-profilului indică faptul că traficul intră în întârziere sau este abandonat pentru a satisface aceste cereri de politică de servicii integrate. Consultaţi “Monitorizarea QoS” la pagina 55 pentru o descriere a tuturor câmpurilor de monitorizare.

   Notă: Ţineţi minte că rezultatele sunt exacte doar când politica este activă. Verificaţi programarea pe care aţi specificat-o în politică. De asemenea, monitorizarea afişează politicile de servicii integrate doar după ce aplicaţiile rulează. O rezervare RSVP trebuie să fie stabilită înainte de monitorizare.

Detalii scenariu: Modificarea proprietăţilor

După examinarea rezultatelor monitorizării, puteţi modifica orice proprietăţi ale politicii pentru a ajunge la rezultatele dorite.

1. În fereastra Configurare server QoS, selectaţi folderul **IntServ**. Faceţi clic dreapta pe **CEO_garantat** din lista din panoul din dreapta şi selectaţi **Proprietăţi** pentru a edita politica. O fereastră Proprietăţi se deschide cu valorile care controlează politica generală.
2. Specificaţi valorile corespunzătoare.
3. Din fereastra Configurare server QoS, selectaţi **Server → Actualizare** pentru a accepta schimbările.

Scenariu: Monitorizarea statisticilor curente de reţea

În cadrul vrăjitorilor, este nevoie să setaţi limitele de performanţă care sunt bazate pe cerinţe individuale de reţea.

Obiective

Pentru a seta aceste limite, trebuie să înţelegeţi într-adevăr performanţa actuală a reţelei dumneavoastră. Deoarece încercaţi să configuraţi politicile de calitatea serviciului, probabil aveţi deja o idee despre cerinţele curente ale reţelei. Pentru a determina limite de rate exacte, cum ar fi rate de găleată jeton, ar fi bine să monitorizaţi tot traficul din sistemul dumneavoastră astfel încât să puteţi determina mai bine ce limite de rate să setaţi.

Soluţie

Creaţi o politică de servicii diferenţiate foarte cuprinzătoare care nu conţine restricţii (fără valori maxime), şi se aplică tuturor interfeţelor şi adreselor IP. Folosiţi monitorizarea QoS pentru a înregistra date în această politică.

Concepte înrudite

"Limite găleată jeton şi lăţime de bandă" la pagina 9
Limitele găleţii jeton şi ale lăţimii de undă sunt cunoscute împreună ca limite de performanţă. Aceste limite de performanţă ajută la garantarea livrării pachetelor în politici de lăţime de bandă ieşire, servicii integrate şi diferenţiate.

"Rata medie de conexiuni şi limitele pentru rafală" la pagina 15
Ratele de conexiuni şi limitele pentru rafală sunt limite de rată. Aceste limite de rată ajută la restricţionarea conexiunilor inbound care încearcă să intre pe serverul dumneavoastră. Limitele de rate sunt setate într-o clasă de serviciu care este folosită cu politici de acces inbound.

Referinţe înrudite

"Monitorizarea QoS" la pagina 55
Puteţi folosi monitorizarea QoS (quality of service) pentru a analiza traficul dumneavoastră IP prin sistem.

Detalii scenariu: Deschiderea QoS în Navigator System i

Acest subiect conţine informaţii despre deschiderea QoS în Navigator System i.

1. În Navigator System i, expandaţi ***sistemul dumneavoastră* → Reţea → Politici IP**.
2. Faceţi clic dreapta **Calitatea serviciului** şi selectaţi **Configurare**.
3. Expandaţi **Politici lăţime de bandă outbound**.
4. Faceţi clic dreapta pe **DiffServ** şi selectaţi **Politică nouă** . Se deschide vrăjitorul Politică nouă DiffServ.

Detalii scenariu: Crearea unei politici de servicii diferenţiate

Deoarece doriţi să colectaţi majoritatea traficului care intră în reţeaua dumneavoastră, aţi putea apela politica reţelei. Utilizaţi toate adresele IP, toate porturile, toate adresele IP locale şi toate momentele (dacă este cazul).

Folosiţi următoarele setări de-a lungul vrăjitorului:

Nume: Reţea (poate fi orice nume pe care îl asignaţi)
Client: Toate adresele IP
Aplicaţie: Toate porturile
Protocol: Toate protocoalele
Planificare: Toate momentele

Navigator System i listează toate politicile de servicii diferenţiate create în sistemul dumneavoastră.

Detalii scenariu: Completarea unei noi clase de servicii

În timp ce completaţi un vrăjitor, sunteţi rugat să asignaţi un comportament per-hop, limite de performanţă şi tratare trafic în-afara-profilului. Aceasta este definită într-o clasă de servicii. Alegeţi valori extrem de mari pentru a permite un flux de trafic cât se poate de mare.

Clasele de servicii determină chiar nivelurile de performanţă pe care acest trafic le primeşte de la un ruter. Aţi putea să vă numiţi clasa de servicii nelimitat pentru a arăta că acest trafic primeşte un serviciu mai înalt. Navigator System i listează toate clasele de servicii definite în sistemul dumneavoastră.

Detalii scenariu: Monitorizarea politicii dumneavoastră

Puteţi folosi monitorizarea pentru a verifica dacă traficul se comportă aşa cum l-aţi configurat să funcţioneze în politică.

1. Selectaţi folderul de politică specific (DiffServ, IntServ, Acces inbound).
2. Faceţi clic dreapta pe politica pe care doriţi să o monitorizaţi şi selectaţi **Monitorizare**.

Mai jos este o listă de ieşiri de monitorizare posibile pentru setul de politici de mai sus.

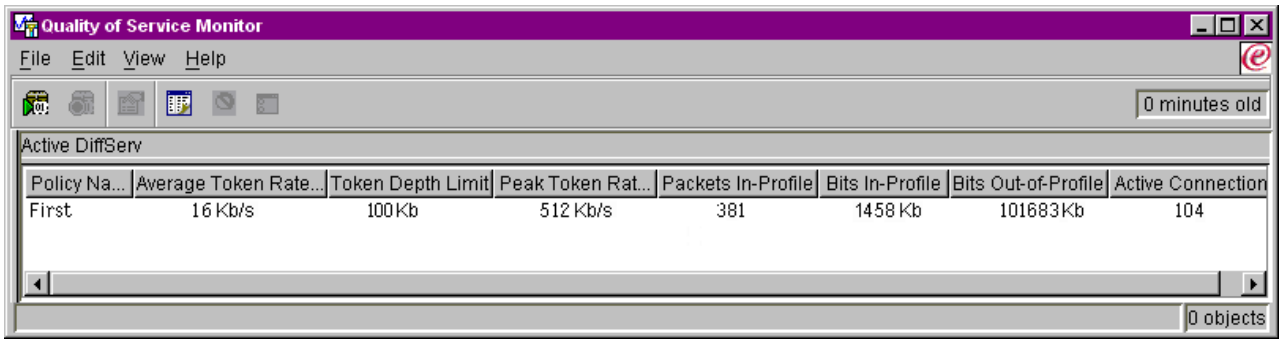


Figura 9. Monitorizare Calitatea serviciului (QoS - Quality of service)

Căutaţi câmpurile care îşi obţin datele din trafic. Asiguraţi-vă că verificaţi câmpurile biţi totali, biţi în profil, pachete în profil şi biţi în-afara-profilului. Biţii în-afara-profilului indică când traficul depăşeşte valorile politică configurată. Într-o politică de servicii diferenţiate, numărul în-afara-profilului indică numărul de biţi aruncaţi. Pachetele în profil indică numărul de biţi controlaţi de această politică (din momentul în care a fost pornit pachetul până la ieşirea de monitorizare actuală).

Valorile pe care le asignaţi câmpului **Limită rată medie jeton** sunt de asemenea importante. Când pachetele depăşesc această limită, sistemul începe să renunţe la ele. Ca rezultat, biţii în-afara-profilului cresc. Aceasta vă arată că politica se comportă aşa cum aţi configurat-o. Pentru a modifica cantitatea de biţi în-afara-profilului, este nevoie să ajustaţi limitele dumneavoastră de performanţă. Consultaţi “Monitorizarea QoS” la pagina 55 pentru o descriere a tuturor câmpurilor de monitorizare.

Detalii scenariu: Modificare valori

După ce monitorizaţi, puteţi modifica oricare din valorile pe care le-aţi selectat anterior. Faceţi clic dreapta pe numele clasă de serviciu pe care a-ţi creat-o în această politică. Când selectaţi **Proprietăţi**, o fereastră Proprietăţi QoS se deschide cu valorile care vă controlează traficul.

Detalii scenariu: Monitorizare din nou a politicii

După ce aţi văzut rezultatele, folosiţi metoda ghiceşte şi verifică pentru a găsi cele mai bune limite pentru nevoile reţelei dumneavoastră.

Planificarea pentru calitatea serviciului

Cel mai important pas pentru a realiza calitatea serviciilor este planificarea. Pentru a primi rezultatele aşteptate, trebuie să revedeţi echipamentul de reţea şi să monitorizaţi traficul de reţea.

Acest subiect oferă informaţii despre planificare. Consilierul de planificare QoS vă conduce prin întrebările de bază pe care trebuie să vi le puneţi în timpul fazei de planificare. În plus faţă de consilier, luaţi în considerare aceste subiecte înainte de configurarea QoS.

Luarea în considerare a performanţelor reţelei

QoS este doar despre performanţa reţelei. Acest motiv principal pentru care vă gândiţi la QoS este probabil pentru că deja aveţi congestionări de reţea şi pierderi de pachete. Înainte de a rezolva orice politică, este posibil să doriţi să folosiţi monitorul QoS pentru a verifica nivelurile curente de performanţă ale traficului dumneavoastră IP. Aceste rezultate vă ajută să determinaţi unde apare congestionarea.

Concepte înrudite

"Monitorizare tranzacţii de sistem" la pagina 62
Cu monitorizarea QoS puteţi să verificaţi că politicile QoS funcţionează aşa cum doriţi dumneavoastră ca ele să funcţioneze. Monitorizarea QoS vă poate ajuta în faza de plănuire şi în faza de depanare a QoS.

"Configurare Calitatea serviciului" la pagina 50
După planificarea QoS (quality of service - calitatea serviciului), vă creaţi politicile QoS cu ajutorul vrăjitorilor din Navigator System i. Această secţiune descrie cum să creaţi politici de servicii diferenţiate, politici de servicii integrate şi politici pentru accesul inbound.

Cerinţe de autorizare

Politicile de calitatea serviciului (QoS) pot conţine informaţii sensibile despre reţeaua dumneavoastră. De aceea, autorizarea de administrare QoS trebuie să fie acordată doar atunci când este necesar.

Următoarele autorizări sunt necesare înainte de a putea configura politici QoS, opţional servere de director LDAP (Lightweight Directory Access Protocol).

Acordare autorizări pentru a gestiona serverul de director

Administratorul QoS are nevoie de următoarele autorizări: autorizarea *ALLOBJ şi *IOSYSCFG. A se consulta Configurare server de director pentru autorizări alternative.

Acordare autorizări pentru a porni serverul TCP/IP

Pentru a acorda autorizare obiect comenzilor STRTCPSVR şi ENDTCPSVR, urmaţi aceşti paşi:

1. **STRTCPSVR**: În linia de comandă, scrieţi GRTOBJAUT OBJ (QSYS/STRTCPSVR) OBJTYPE (*CMD) USER (ADMINPROFILE) AUT (*USE), substituind numele profilului dumneavoastră de administrator cu ADMINPROFILE şi apăsaţi Enter.
2. **ENDTCPSVR**: În linia de comandă, scrieţi GRTOBJAUT OBJ (QSYS/ENDTCPSVR) OBJTYPE (*CMD) USER (ADMINPROFILE) AUT (*USE), substituind numele profilului dumneavoastră de administrator cu ADMINPROFILE şi apăsaţi Enter.

Acordare autorizări de accesare a tuturor obiectelor şi de configurare a sistemului

Se sugerează că utilizatorii care configurează QoS au acces de nivelul responsabilului cu securitatea. Pentru a acorda autorizări de accesare şi de configurare a sistemului tuturor obiectelor, urmaţi aceşti paşi:

1. În Navigator System i, expandaţi ***sistemul dumneavoastră*** → **Utilizatori şi grupuri**.
2. Faceţi clic dublu pe **Toţi utilizatorii**.
3. Faceţi clic dreapta pe profilul de utilizator al administratorului şi selectaţi **Proprietăţi**.

4. În fereastra Proprietaţi, apăsaţi **Capabilităţi**.
5. În pagina Capacităţi, selectaţi **Accesarea tuturor obiectelor şi configurarea sistemului**.
6. Faceţi clic **OK** pentru a închide pagina Capacităţi.
7. Apăsaţi **OK** pentru a închide fereastra Proprietăţi

Cerinţe de sistem

Calitatea serviciului (QoS) este o parte integrantă a sistemului de operare.

Trebuie să efectuaţi aceste cereri în întregime.

1. Instalaţi IBM TCP/IP Connectivity Utilities for i5/OS (5761-TC1).
2. Instalaţi Navigator System i pe PC-ul dumneavoastră. Asiguraţi-vă că instalaţi componenta Lucru în reţea în timpul instalării System i Access. Calitatea serviciului este localizată sub politici IP în Reţele.

   Concepte înrudite

   Să cunoaştem System i Navigator

   Referinţe înrudite

   "Informaţii înrudite pentru Calitatea serviciului" la pagina 65
   RFC-uri QoS, publicaţii IBM Redbooks, şi alte colecţii de subiecte din centrul de informare conţin informaţii care sunt înrudite cu colecţia de subiecte Calitatea serviciului. Puteţi vedea sau tipări oricare din fişierele PDF.

Acord la nivel de serviciu

Acest subiect scoate în evidenţă unele din aspectele importante ale unui SLA (service level agreement) care ar putea afecta implementarea QoS-ului dumneavoastră. QoS este o soluţie de reţea. Pentru a obţine prioritate de reţea în afara reţelei dumneavoastră private, aţi putea avea nevoie de un SLA cu ISP-ul (Internet service provider) dumneavoastră.

Când este necesar un SLA

Aveţi nevoie de un SLA doar dacă politicile dumneavoastră necesită prioritate în afara reţelei dumneavoastră private. Dacă folosiţi politici outbound pentru a controla traficul care vă părăseşte sistemul, atunci nu este nevoie de o garantare a serviciului. De exemplu, în sistem, puteţi crea o politică care dă unei aplicaţii o prioritate mai înaltă decât unei alte aplicaţii. Sistemul dumneavoastră recunoaşte această prioritate, dar orice în afara sistemului se poate să nu recunoască prioritatea. Dacă aveţi o reţea privată şi vă configuraţi ruterele să recunoască marcaje de puncte de cod (folosite pentru a da politicilor outbound un nivel de serviciu), atunci ruterele vor da prioritate prin reţeaua dumneavoastră privată. Oricum, dacă traficul părăseşte reţeaua dumneavoastră privată, nu există garanţii. Fără un SLA, nu puteţi controla cum hardware-ul din reţea tratează traficul. În afara reţelei dumneavoastră private, aveţi nevoie de un SLA pentru a garanta prioritatea unei clase de servicii sau rezervare de resurse.

De ce este necesar un SLA

Politicile şi rezervările dumneavoastră sunt doar atât de bune precum este cea mai slabă legătură. Aceasta înseamnă că politicile QoS permit aplicaţiilor să primească prioritate prin reţea. Oricum, dacă un nod oriunde între client şi server nu este capabil să realizeze orice caracteristici de manevrare a traficului discutate în subiectele de servicii diferenţiate sau integrate, politicile dumneavoastră nu vor fi manevrate aşa cum aţi intenţionat dumneavoastră. Dacă SLA-ul dumneavoastră nu vă lasă destule resurse, nici chiar cele mai bune politici nu vă vor ajuta la problema de congestionare a reţelei.

Asta implică şi acorduri de-a lungul ISP-urilor. Între domenii, fiecare ISP trebuie să fie de acord să ajute cererile QoS. Interoperabilitatea poate cauza nişte provocări.

Asiguraţi-vă că înţelegeţi nivelul de serviciu pe care îl primiţi de fapt. Acordurile de condiţionare a traficului se adresează în mod specific la modul de tratare al traficului, care este aruncat, marcat, configurat sau retransmis. Motivele cheie de a oferi QoS implică şi controlarea latenţei, neastâmpărului, lăţimii de bandă, pierderii de pachete şi disponibilităţii rezultatului. Înţelegerile de servicii trebuie să poată da politicilor ceea ce acestea cer. Verificaţi dacă

primiţi serviciile de care aveţi nevoie. Dacă nu, v-aţi putea cheltui resursele. De exemplu, dacă cereţi să rezervaţi 500 kbps pentru telefonie IP dar aplicaţie dumneavoastră necesită doar 20 kbps, s-ar putea să plătiţi în plus fără să fiţi anunţat de către ISP-ul dumneavoastră.

Notă: Politicile QoS vă permit să negociaţi nivelurile de servicii cu ISP-ul dumneavoastră care ar putea duce la scăderea costurilor serviciilor de reţea. De exemplu, ISP-ul dumneavoastră este posibil să fie capabil să vă garanteze o anumită rată monetară, dacă nu depăşiţi un nivel de lăţime de bandă asupra căruia v-aţi înţeles. Sau este posibil să realizaţi că folosind politici QoS, veţi folosi numai o cantitate ″x″ din lăţimea de bandă în timpul orelor de zi, o cantitate ″y″ a lăţimii de bandă noaptea şi să fiţi de acord pentru o rată a fiecărui segment de timp. Dar, dacă lăţimea de bandă este depăşită, ISP-ul probabil vă va taxa mai mult. Este nevoie ca ISP-ul să fie de acord cu un anumit nivel de serviciu şi să aibă abilitatea de a urmări lungimea de bandă pe care o folosiţi.

Concepte înrudite

“Concepte” la pagina 1
Înainte de a folosi QoS, este nevoie să învăţaţi terminologia de bază şi conceptele QoS. Aceste concepte vă ajută să determinaţi dacă serviciul vă întâlneşte nevoile.

“Scenariu: Limitare trafic browser” la pagina 27
Puteţi utiliza calitatea serviciului (QoS) pentru a controla performanţa traficului. Folosiţi o politică de servicii diferenţiate pentru a limita sau a extinde performanţa unei aplicaţii în reţea.

“Scenariu: Rezultate sigure şi predictibile (VPN şi QoS)” la pagina 31
Dacă folosiţi o reţea privată virtuală (VPN), puteţi crea şi politici de calitatea serviciilor.

“Scenariu: Trafic B2B predictibil” la pagina 37
Dacă aveţi nevoie de livrare predictibilă şi încă doriţi să cereţi o rezervare, folosiţi tot o politică de servicii integrate. Acest exemplu foloseşte un serviciu de încărcare controlat.

“Scenariu: Livrarea dedicată (telefonie IP)” la pagina 41
Dacă aveţi nevoie de livrare dedicată şi doriţi să cereţi o rezervare, folosiţi o politică de servicii integrate. Există două tipuri de politici de servicii integrate ce pot fi create: încărcare garantată şi controlată. În acest exemplu, este folosit serviciul garantat.

Hardware şi software de reţea

Capacităţile echipamentului dumneavoastră intern şi cele ale altor echipamente din afara reţelei au efecte enorme asupra rezultatelor QoS.

Aplicaţii

Politicile de servicii integrate necesită aplicaţii care sunt activate de către protocolul RSVP (ReSerVation Protocol). Deoarece aplicaţiile i5/OS nu sunt iniţial RSVP-activate, trebuie să le activaţi pentru a folosi RSVP. Pentru a vă activa aplicaţiile, este nevoie să scrieţi programe speciale cu ajutorul API-urilor RSVP sau API-urilor socket-ului QoS qtoq. Aceste programe permit aplicaţiilor dumneavoastră să folosească RSVP.

Noduri de reţea

Ruterele, switch-urile şi chiar şi sistemul dumneavoastră de operare trebuie să fie capabile să folosească QoS. Pentru a folosi politici de servicii diferenţiate, echipamentul dumneavoastră trebuie să fie activat pentru Servicii diferenţiate. Aceasta înseamnă că nodul de reţea trebuie să poată clasifica, măsura, marca, configura şi arunca pachete IP (condiţionări de trafic).

Pentru a folosi politici de servicii integrate, echipamentul dumneavoastră trebuie să fie RSVP-activat. Aceasta înseamnă că nodurile de reţea trebuie să poată să suporte şi RSVP.

Concepte înrudite

“API-uri Calitatea serviciului” la pagina 16
Acest subiect conţine informaţii despre protocoale şi API-uri şi conţine cerinţele pentru un ruter care este activat pentru RSVP (ReSerVation Protocol). API-urile QoS (Quality of Service) includ API-ul RAPI, API-ul qtoq socket, API-ul sendmsg() şi API-urile monitor.

"Condiţionări de trafic" la pagina 5
Pentru a utiliza politici QoS, echipamentele de reţea (precum ruterele şi switch-urile) trebuie sa fie capabile de condiţionare de trafic. Condiţionatoarele de trafic se referă la utilitare de tip clasifier, meter, marker, shaper şi dropper.

Configurare Calitatea serviciului

După planificarea QoS (quality of service - calitatea serviciului), vă creaţi politicile QoS cu ajutorul vrăjitorilor din Navigator System i. Această secţiune descrie cum să creaţi politici de servicii diferenţiate, politici de servicii integrate şi politici pentru accesul inbound.

Vrăjitorii fac o treabă bună în a vă ghida prin procesul de configurare.

După ce vă configuraţi politicile, puteţi folosi obiectele de configurare din Navigator System i pentru a vă edita configuraţia politicii. Obiectele de configurare sunt piesele sau părţile diferite care fac o politică. Când deschideţi calitatea serviciului în Navigator System i, sunt foldere etichetate clienţi, aplicaţii, planificări, politici, clase de servicii, comportamente per-hop şi URI-uri (Uniform Resource Identifiers). Aceste obiecte vă permit să construiţi o politică. Pentru informaţii suplimentare despre obiecte, puteţi consulta ajutorul privire generală asupra calitatea serviciului din Navigator System i.

Activarea politicilor QoS

Înainte ca politicile să aibă efect, trebuie activate. Puteţi folosi vrăjitorii, sistemul activează automat politicile pentru dumneavoastră. Totuşi, dacă schimbaţi o politică care foloseşte obiectele de configurare, este nevoie să actualizaţi dinamic sistemul înainte ca politicile să devină active. Înainte de activare, asiguraţi-vă că nu există politici suprapuse care pot cauza probleme.

Concepte înrudite

"Planificarea pentru calitatea serviciului" la pagina 47
Cel mai important pas pentru a realiza calitatea serviciilor este planificarea. Pentru a primi rezultatele aşteptate, trebuie să revedeţi echipamentul de reţea şi să monitorizaţi traficul de reţea.

Să cunoaştem System i Navigator

Operaţii înrudite

"Ordonarea politicilor QoS" la pagina 53
Dacă aveţi două politici care se suprapun, ordinea fizică a politicilor dumneavoastră în Navigator System i este importantă.

Referinţe înrudite

"Gestionarea Calitatea serviciului (QoS)" la pagina 53
Puteţi folosi aceste proceduri pentru a gestiona proprietăţile şi politicile calitatea serviciului (QoS) existente.

Configurarea QoS cu vrăjitori

Pentru a configura politici QoS (quality of service), este necesar să folosiţi vrăjitorii QoS aflaţi în Navigator System i.

Aici este o listă a vrăjitorilor şi funcţiile acestora:

Vrăjitor configurare iniţială
Acest vrăjitor vă permite să setaţi configuraţii specifice sistemului şi informaţii de server de directoare.

Vrăjitor politică nouă IntServ
Vrăjitorul de politică IntServ nouă vă permite să creaţi o politică de servicii integrate. Această politică permite sau refuză o cerere RSVP (ReSerVation Protocol) care controlează indirect lăţimea de bandă a serverului. Limitele de performanţă ale politicii (pe care le setaţi) decid dacă sistemul poate trata lăţimea de bandă care vine de la aplicaţia RSVP a clientului. Aveţi nevoie de aplicaţii şi rutere RSVP-activate pentru a rula politicile de servicii integrate create în acest vărjitor.

Notă: Înainte de a seta o politică de servicii integrate, este necesar să vă scrieţi propriile aplicaţii pentru a folosi RSVP-ul.

Vrăjitorul Politică nouă DiffServ

Acest vrăjitor vă permite să diferenţiaţi şi să alocaţi prioritate traficului TCP/IP. Puteţi diferenţia traficul prin crearea politicilor. Într-o politică, asignaţi nivelul de serviciu traficului outbound pe baza adreselor IP sursă/destinaţie, porturi, aplicaţii, chiar şi clienţi. Aplicaţiile dumneavoastră i5/OS pot primi niveluri de serviciu bazate pe informaţii de aplicaţie mai detaliate.

Vrăjitorul Clasă nou de serviciu

Folosiţi vrăjitorul clasă de serviciu pentru a seta marcaje de pachete folosite de rutere şi switch-uri în reţele. Alocă şi limite de performanţă traficului care părăseşte reţeaua. Folosiţi clasa de servicii cu politică servicii diferenţiate şi o politică de acces inbound.

Vrăjitorul Acces inbound nouă

Folosiţi vrăjitorul Acces inbound pentru a restricţiona conexiunile făcute către sistemul dumneavoastră. Puteţi restricţiona accesul prin adresă TCP/IP, prin aplicaţie, prin interfeţe locale sau prin URI. Aceasta permite unui administrator de sistem să controleze accesul la sistemul dumneavoastră de la anumiţi clienţi şi aplicaţii server. În plus, puteţi îmbunătăţi performanţa sistemului.

Notă: Înainte de a seta o politică de servicii diferenţiate care utilizează URI-uri, trebuie să vă asiguraţi de faptul că portul aplicaţiei alocat pentru URI se potriveşte directivei ″Ascultare″ activată pentru FRCA în configurarea serverului Web Apache.

După ce vă decideţi ce tip de politică să creaţi, puteţi configura politica prin folosirea vrăjitorului corespunzător care este listat anterior.

Accesarea vrăjitorilor QoS din Navigator System i

Puteţi folosi aceşti paşi pentru a accesa vrăjitorii QoS şi crea o politică în Navigator System i.

Pentru a accesa vrăjitorii QoS şi a crea o nouă politică, urmaţi paşii:

1. În Navigator System i, expandaţi ***sistemul dumneavoastră*** → **Reţea** → **Politici IP**.
2. Faceţi clic dreapta **Quality of Service** şi apăsaţi **Configurare**.

   Notă: Se deschide vrăjitorul Configurare iniţială în condiţiile următoare:
   - Folosiţi pentru prima dată interfaţa grafică utilizator (GUI) pe acest sistem.
   - Doriţi să înlăturaţi manual informaţiile de configurare mai vechi şi să o luaţi de la capăt. Aceasta se întâmplă doar dacă interfaţa QoS este deja pornită.
3. Finalizaţi paşii din vrăjitorul Configurare iniţială. Dacă nu apare vrăjitorul Configurare iniţială, treceţi la pasul 4.
4. Selectaţi **Politici**. Faceţi clic dreapta pe **IntServ**, **DiffServ** sau **Acces inbound**.
5. Selectaţi **Politică nouă**.

Concepte înrudite

“API-uri Calitatea serviciului” la pagina 16
Acest subiect conţine informaţii despre protocoale şi API-uri şi conţine cerinţele pentru un ruter care este activat pentru RSVP (ReSerVation Protocol). API-urile QoS (Quality of Service) includ API-ul RAPI, API-ul qtoq socket, API-ul sendmsg() şi API-urile monitor.

“Servicii diferenţiate” la pagina 2
Acesta este primul tip de politică de lungime de bandă outbound pe care o puteţi crea pe sistemul dumneavoastră de operare. Serviciile diferenţiate împart traficul dumneavoastră pe clase. Pentru a realiza o politică de serviciu diferenţiat, este necesar să determinaţi cum doriţi să clasificaţi traficul dumneavoastră de reţea şi cum să trataţi diferitele clase.

Informaţii înrudite

Gestionarea adreselor şi porturilor pentru serverul HTTP (motorizat de Apache).

Configurare server de director

Configuraţiile de politici QoS (Quality of service) pot fi exportate către un serve de director LDAP (Lightweight Directory Access Protocol), ceea ce face ca soluţiile dumneavoastră QoS să fie mai uşor de gestionat.

În loc să configuraţi politici QoS pe toate sistemele dumneavoastră, puteţi stoca datele de configuraţie pe un server de director local pentru a fi distribuite între mai multe sisteme. Când configuraţi pentru prima dată QoS pe sistemul dumneavoastră, se deschide un vrăjitor Configuraţie iniţială. Acest vrăjitor vă întâmpină pentru a configura un server de director.

Pentru a configura serverul de director, este necesar să vă decideţi sau să cunoaşteţi următoarele informaţii:

- Ştiţi numele serverului de director
- Determinaţi un nume distinctiv (distinguished name - DN) pentru a vă referi la politicile QoS
- Determinaţi dacă să folosiţi securitate SSL (Secure Sockets Layer) cu serverul de director LDAP
- Determinaţi dacă veţi folosi cuvinte cheie pentru a îmbunătăţi căutarea politicilor dumneavoastră pe serverul de directoare.

Notă: În prezent, Kerberos nu poate fi configurat ca metoda de autentificare pe care serverul QoS o foloseşte pentru a accesa directorul.

Pentru a administra serverul de directoare LDAP, trebuie să aveţi unul din următoarele seturi de autorizări:

- autorizare *ALLOBJ şi autorizare *IOSYSCFG
- autorizare *JOBCTL şi autorizare obiect la comenzile Sfârşit TCP/IP (ENDTCP), Început TCP/IP (STRTCP), Pornire server TCP/IP (STRTCPSVR) şi Oprire server TCP/IP (ENDTCPSVR)
- autorizare *AUDIT pentru a configura securitatea de auditare i5/OS

Dacă folosiţi Navigator System i, aveţi deja acces la Schema QoS implicită. Fişierul schemă real se află în sistemul dumneavoastră la /QIBM/UserData/OS400/DirSrv. Totuşi, dacă folosiţi un editor altul decât Navigator System i, este nevoie să importaţi fişierul LDIF (LDAP Data Interchange Format) descris în secţiunea următoare. Puteţi de asemenea să importaţi acest fişier, după editare, doriţi să reîncărcaţi fişierul original implicit.

Schema QoS

Un set de reguli, numit *schemă*, există pentru a specifica ce tipuri de obiecte LDAP sunt valide pentru serverul QoS. Schema conţine regulile necesare pentru QoS. Dacă serverul LDAP utilizat nu este o platformă System i, aceste reguli trebuiesc importate pe serverul LDAP. Aceasta se face cu un fişier LDIF (LDAP Data Interchange Format). Folosiţi pagina web LDAP pentru a descărca fişierul LDIF. Puteţi găsi acest fişier în **Categories → TCP/IP Policies** pe panoul din stânga.

Concepte înrudite

“Server director” la pagina 24
Puteţi alege să exportaţi politicile dumneavoastră unui server director. Citiţi acest subiect pentru a vedea conceptele şi configuraţia LDAP (Lightweight Directory Access Protocol) cât şi schema QoS (quality of service).

“Nume distinct” la pagina 25
Când doriţi să gestionaţi o parte a directorului dumneavoastră, vă referiţi la DN (distinguished name - nume distinctiv) sau (dacă alegeţi) la un cuvânt cheie.

IBM Tivoli Directory Server pentru i5/OS (LDAP)

Activarea SSL şi TLS (Transport Layer Security) pe serverul de director

“Cuvinte cheie” la pagina 24
Atunci când configuraţi serverul de directoare, va trebui să determinaţi dacă să asociaţi cuvinte cheie fiecărei configuraţii QoS.

Informaţii înrudite

IBM LDAP Directory Schema

Ordonarea politicilor QoS

Dacă aveţi două politici care se suprapun, ordinea fizică a politicilor dumneavoastră în Navigator System i este importantă.

O suprapunere de politici reprezintă două politici care folosesc acelaşi client, aplicaţie, planificare, adresă IP locală, URI (Uniform Resource Identifier), date server, punct de cod sau protocol. Politicile din ecranul Navigator System i sunt într-o listă ordonată. Precedenţa politicii depinde de ordinea politicilor din listă. Dacă doriţi ca o politică să aibă prioritate în faţa alteia, politica cu prioritate mai înaltă trebuie să apară prima în listă.

Pentru a determina dacă o politică se suprapune cu o altă politică, urmaţi aceste instrucţiuni:

1. În Navigator System i, expandaţi ***sistemul dumneavoastră*** → **Reţea** → **Politici IP**.
2. Faceţi clic dreapta **Calitatea serviciului**.
3. Selectaţi **Configurare**.
4. Selectaţi folderul **Politici specifice**.
5. Faceţi clic dreapta pe numele politicii care are asociate politici de suprapunere. Politicile de suprapunere au o icoană în faţa lor pentru a indica suprapunerea.
6. Selectaţi **Arată suprapunerea**. Se deschide fereastra Suprapunere politică.

Pentru a modifica ordinea politicilor pe ecran, folosiţi următorii paşi:

- Evidenţiaţi politica şi folosiţi săgeţile jos şi sus pe ecran pentru a modifica ordinea politicii.
- Faceţi clic dreapta pe numele politicii şi selectaţi **Mută în sus** sau **Mută în jos**.
- Actualizaţi serverul QoS. Puteţi folosi butonul **Actualizare server** în bara de unelte sau consultaţi Ajutor operaţii QoS pentru instrucţiuni mai detaliate.

Concepte înrudite

"Configurare Calitatea serviciului" la pagina 50
După planificarea QoS (quality of service - calitatea serviciului), vă creaţi politicile QoS cu ajutorul vrăjitorilor din Navigator System i. Această secţiune descrie cum să creaţi politici de servicii diferenţiate, politici de servicii integrate şi politici pentru accesul inbound.

"Copierea unei politici existente" la pagina 54
Decât să vă creaţi toate politicile dumneavoastră de la început, puteţi face copii ale politicilor originale şi apoi să editaţi secţiunile politicilor care diferă de cele originale.

"Depanare calitatea serviciului (QoS)" la pagina 59
QoS furnizează mai multe metode de depanare a problemelor QoS.

Operaţii înrudite

"Accesarea ajutorului pentru QoS în Navigator System i" la pagina 54
Puteţi folosi Navigator System i pentru a accesa ajutorul pentru QoS (quality of service - calitatea serviciului).

Gestionarea Calitatea serviciului (QoS)

Puteţi folosi aceste proceduri pentru a gestiona proprietăţile şi politicile calitatea serviciului (QoS) existente.

Aceste articole vă spun unde anume să căutaţi taskuri pentru editarea, activarea, vizualizarea şi folosirea altor tehnici de gestionare a politicilor. Există de asemenea o explicaţie pentru cum să folosiţi monitorizarea QoS şi funcţia de colectare de date pentru a ajuta la analizarea traficului IP în sistem.

Concepte înrudite

"Configurare Calitatea serviciului" la pagina 50
După planificarea QoS (quality of service - calitatea serviciului), vă creaţi politicile QoS cu ajutorul vrăjitorilor din Navigator System i. Această secţiune descrie cum să creaţi politici de servicii diferenţiate, politici de servicii integrate şi politici pentru accesul inbound.

Accesarea ajutorului pentru QoS în Navigator System i

Puteţi folosi Navigator System i pentru a accesa ajutorul pentru QoS (quality of service - calitatea serviciului).

1. În Navigator System i, expandaţi ***sistemul dumneavoastră*** → **Reţea** → **Politici IP**.
2. Faceţi clic dreapta **Calitatea serviciului** şi apăsaţi **Configurare**.
3. Apăsaţi **Ajutor** → **Subiecte ajutor** în bara de meniuri. Aceasta va deschide fereastra de ajutor.

Operaţii înrudite

"Ordonarea politicilor QoS" la pagina 53
Dacă aveţi două politici care se suprapun, ordinea fizică a politicilor dumneavoastră în Navigator System i este importantă.

Salvarea de rezervă a politicilor QoS

Ar trebui să vă faceţi copii de rezervă a politicilor dumneavoastră QoS (quality of service - Calitatea serviciului) pentru a elimina nevoia de a vă crea din nou politicile în cazul unei întreruperi a sistemului sau a unor fluctuaţii de tensiune.

Politicile dumneavoastră pot fi stocate local sau exportate pe un server director. Trebuie mai ales să salvaţi următoarele directoare din sistemul de fişiere: QIBM/UserData/OS400/QOS/ETC, QIBM/UserData/OS400/QOS/TEMP şi QIBM/UserData/OS400/QOS/USR. Trebuie de asemenea să salvaţi agentul de publicare al serverului director pentru serverul QoS. Agentul de publicare conţine numele serverului de directoare, numele distinctiv (DN) pentru serverul QoS, portul folosit la accesarea serverului de directoare şi informaţii de autentificare. În cazul unor pierderi, salvările de rezervă vă pot scuti de timpul şi efortul necesar re-creării politicilor de la zero. Acestea sunt sugestii generale pe care le puteţi folosi pentru a vă asigura că aveţi un mijloc simplu de înlocuire a fişierelor pierdute:

1. **Folosiţi programe integrate de salvare şi recuperare a sistemelor de fişiere.**

   Cartea *Backup and recovery* furnizează instrucţiuni pentru a realiza copii de rezervă din sisteme integrate de fişiere.
2. **Tipăriţi politicile.**

   Puteţi stoca tipăririle oriunde ar fi mai ales pentru a fi siguri şi reintroduceţi informaţiile după cum este necesar.
3. **Copiaţi informaţiile pe un disc.**

   Copierea are un avantaj faţă de imprimate: în loc să le reintroduceţi manual, informaţiile există în format electronic. Furnizează a metodă directă pentru transportarea datelor de la o sursă online la alta.

Notă: Sistemul dumneavoastră copiază informaţii pe discul de sistem, nu pe o dischetă. Fişierele de reguli se află în QIBM/UserData/OS400/QOS/ETC cât şi în numele distinctiv din serverul de director pe care l-aţi configurat, nu pe un PC. Aţi putea dori să folosiţi o metodă de protecţie a discului ca un mijloc de copiere de siguranţă pentru a proteja datele care sunt stocate pe discul sistem.

Când folosiţi un produs System i, trebuie să vă stabiliţi o strategie de salvare de rezervă şi recuperare.

Informaţii înrudite

Salvarea de rezervă a sistemului dumneavoastră

Copierea unei politici existente

Decât să vă creaţi toate politicile dumneavoastră de la început, puteţi face copii ale politicilor originale şi apoi să editaţi secţiunile politicilor care diferă de cele originale.

În Navigator System i, această funcţie QoS (quality of service) se numeşte *Nou bazat pe*. Trebuie să folosiţi Navigator System i pentru a accesa fereastra QoS care vă permite să continuaţi cu copierea politicilor.

Pentru a crea o copie a unei politici existente, urmaţi paşii din **Crearea unei noi politici pe baza unei politici existente** din ajutorul Navigator System i.

Înainte ca politicile dumneavoastră să poată avea efect, trebuie să le activaţi prin pornirea serverului QoS sau realizând o actualizare dinamică de server. Înainte de activare, asiguraţi-vă că nu există politici suprapuse care pot cauza probleme.

Operaţii înrudite

"Ordonarea politicilor QoS" la pagina 53
Dacă aveţi două politici care se suprapun, ordinea fizică a politicilor dumneavoastră în Navigator System i este importantă.

Editare politici QoS

După cum vi se modifică nevoile, trebuie să vă editaţi politicile pentru a vă asigura că încă primiţi performanţa corespunzătoare.

Trebuie să încercaţi să corectaţi orice erori şi să efectuaţi modificările necesare pentru politicile dumneavoastră înainte de activare. Aceasta este cea mai bună cale de prevenire a complicaţiilor cu rezultatele politicilor.

După ce v-aţi configurat politicile, puteţi folosi obiectele de configurare din Navigator System i pentru a vă edita configuraţia politicii. Obiectele de configurare sunt piesele sau părţile diferite care fac o politică. Când deschideţi calitatea serviciului în Navigator System i, veţi întâlni foldere, clienţi etichetaţi, aplicaţii, planificări, clase de servicii, comportamente per-hop şi URI-uri (Uniform Resource Identifier). Aceste obiecte vă permit să editaţi o politică.

Pentru a edita o politică în Navigator System i, urmaţi paşii din pagina Editarea unei politici QoS (quality of service) din Ajutorul Navigator System i.

Monitorizarea QoS

Puteţi folosi monitorizarea QoS (quality of service) pentru a analiza traficul dumneavoastră IP prin sistem.

Monitorizarea QoS ajută la determinarea locului unde are loc o congestie în reţeaua dumneavoastră. Aceasta nu este folositoare doar în timpul planificarea QoS, poate fi de ajutor şi ca o unealtă de depanare. Monitorizarea QoS vă poate ajuta să continuaţi monitorizarea reţelei dumneavoastră astfel încât să vă puteţi ajusta politicile după nevoie. Pentru a monitoriza toate politicile active, selectaţi **Server → Monitor** din fereastra Configurare server QoS. Dacă faceţi clic dreapta pe o singură politică şi selectaţi **Monitorizare**, monitorizarea afişează informaţii doar pentru acea politică.

Puteţi utiliza politicile de monitorizare în următoarele feluri:

- **Pentru a vizualiza datele în timp-real pe politici active**

  Când deschideţi monitorul, datele în timp-real sunt întotdeauna afişate pe politici active. Nu este nevoie să începeţi colecţia de date.
- **Pentru a colecta şi salva datele pentru o perioadă de timp**

  Dacă doriţi să salvaţi rezultatele monitorizării, atunci trebuie să porniţi colectarea de date. Monitorul continuă să colecteze datele până când opriţi dumneavoastră colectarea. Închiderea ferestrei monitor nu opreşte colectarea de date. Puteţi, de asemenea, modifica proprietăţile pe care le foloseşte monitorul când colectează datele. În fereastra Monitorizare QoS, evidenţiaţi **Monitorizare QoS** şi selectaţi **Fişier-->Proprietăţi** pentru a vă modifica opţiunile. Folosiţi ajutorul online pentru informaţii suplimentare.

  Dacă se porneşte colectarea de date QoS şi proprietăţile de monitorizare sunt modificate, atunci este nevoie să faceţi următorii paşi pentru a vă asigura că modificările sunt reflectate în colectarea de date:

  1. Oprire colectare date QoS.
  2. Modificare proprietăţi monitor.
     a. În fereastra Monitor, faceţi clic pe **Monitor QoS**.
     b. Selectaţi **Fişier → Proprietăţi**.
     c. Modificaţi proprietăţile monitorului şi faceţi clic pe **OK**.
  3. Actualizare server QoS.
  4. Pornire colectare de date QoS.

Monitorizare ieşire

Informaţiile outbound pe care le primiţi depind de tipul de politică pe care o monitorizaţi. Ţineţi minte tipurile de politici: serviciu diferenţiat, serviciu integrat (Încărcare controlată), serviciu integrat (Garantat) şi acces inbound. Câmpurile de evaluat depind de tipul politicii. Cele mai interesante valori sunt valorile care arată o măsurare. Următoarele câmpuri sunt măsurate mai de grabă decât date ca definiţie: cereri acceptate, conexiuni active, servicii conexiune, rate de conexiune, cereri abandonate, pachete în-profil, biţi în-profil, biţi în-afara-profilului, biţi total, pachete total şi cereri total.

Citind informaţii din câmpurile măsurate de mai sus, vă puteţi forma o imagine bună despre cum se conformează traficul reţelei la politici. Folosiţi descrierile de mai jos pentru informaţii mai detaliate despre câmpul ieşire monitor pentru fiecare tip de politică. Vedeţi oricare din scenariile QoS ca exemplu despre cum se foloseşte un monitor cu politicile QoS.

Politici de servicii diferenţiate

Tabela 4. Politici de servicii diferenţiate

Câmp	**Descriere**
Nume politică	Numele alocat acestei politici.
Protocol	UDP, TCP, ALL.
Limită de rată jeton medie	Rata medie de jeton permisă de această politică în fiecare ruter şi sistem de-a lungul căii de flux.
Limită de adâncime jeton	Dimensiunea maximă a buffer-ului jeton permisă de această politică în fiecare ruter şi sistem de-a lungul căii de flux.
Limită de rată jeton de vârf	Rata maximă permisă de această conexiune.
Pachete în profil	Numărul de pachete IP transmise care se potriveşte cu parametrii acestei politici.
Biţi în profil	Numărul de biţi transmişi care se potriveşte cu parametrii acestei politici.
Biţi în-afara-profilului	Numărul de biţi transmişi care depăşeşte parametrii politicii.
Rată biţi	Numărul măsurat de biţi permis de această conexiune.
Conexiuni active	Numărul total de conexiuni active.
Profil trafic	Tipul de condiţionare de pachet folosit în pachete în-afara-profilului. Formatarea poate include: • Re-marcare • Configurare • Aruncare
Biţi totali	Numărul de biţi transmişi folosit de această politică din momentul în care a fost pornită până în momentul colecţiei de monitorizare.
Punct de cod în profil	Dacă pachetul este remarcat cu un nou punct de cod, acesta este punctul de cod pe care îl vor folosi pachetele IP dacă se vor potrivi cu parametrii acestei politici.
Punct de cod în-afara-profilului	Dacă pachetul este remarcat cu un nou punct de cod, acesta este punctul de cod pe care îl vor folosi pachetele IP dacă acestea depăşesc parametrii politicii.
Interval adresă de destinaţie	Intervalul de adresă care determină punctul de destinaţie al pachetului (controlat de această politică).
Pachet total	Numărul de pachete transmise de această politică din momentul în care a fost pornită până în momentul colecţiei de monitorizare.

Tabela 4. Politici de servicii diferenţiate (continuare)

Câmp	Descriere
Interval port sursă	Intervalul de porturi sursă care determină care aplicaţii sunt controlate de această politică.

Politici servicii integrate (sarcină controlată)

Politicile de servicii integrate nu sunt afişate în monitorizare decât când aplicaţiile rulează şi rezervările au fost stabilite. Dacă politicile dumneavoastră de servicii integrate au mai mult de o rezervare, veţi vedea mai multe intrări în monitorizare.

Tabela 5. Politici servicii integrate (sarcină controlată)

Câmp	Descriere
Nume politică	Numele alocat acestei politici.
Protocol	UDP sau TCP.
Adresă de destinaţie	Intervalul de adresă care determină punctul de destinaţie al pachetului (controlat de această politică).
Limită de rată jeton medie	Rata de jeton medie permisă de această politică în fiecare ruter şi sistem de-a lungul căii conexiunii.
Limită de adâncime jeton	Dimensiunea maximă a buffer-ului jeton permisă de această politică în fiecare ruter şi sistem de-a lungul căii conexiunii.
Limită de rată jeton de vârf	Rata maximă permisă de această conexiune.
Pachet total	Numărul de pachete transmise de această politică din momentul în care a fost pornită până în momentul colecţiei de monitorizare.
Biţi în-afara-profilului	Numărul de biţi transmişi care depăşeşte parametrii politicii.
Biţi totali	Numărul de biţi transmişi folosit de această politică din momentul în care a fost pornită până în momentul colecţiei de monitorizare.
Rată bit	Numărul măsurat de biţi permis de această conexiune.
Biţi în profil	Numărul de biţi transmişi care se potriveşte cu parametrii acestei politici.
Dimensiune de pachet maximă	Dimensiunea de pachet maximă permisă controlată de această politică.
Unitate de supraveghere minimă	Cel mai mic număr de biţi care este înlăturat din găleata jeton. De exemplu, dacă unitatea de supraveghere minimă este 100 biţi, pachetele sub 100 de biţi vor fi totuşi înlăturate la 100 de biţi.
Pachete în profil	Numărul de pachete IP transmise care se potriveşte cu parametrii acestei politici.
Interval port sursă	Intervalul de porturi sursă care determină care aplicaţii sunt controlate de această politică.

Politici de servicii integrate (garantate)

Politicile de servicii integrate nu sunt afişate în monitorizare decât când aplicaţiile rulează şi rezervările au fost stabilite. Dacă politicile dumneavoastră de servicii integrate au mai mult de o rezervare, veţi vedea mai multe intrări în monitorizare.

Tabela 6. Politici de servicii integrate (garantate)

Câmp	Descriere
Nume politică	Numele alocat acestei politici.
Protocol	UDP sau TCP.
Adresă de destinaţie	Intervalul de adresă care determină punctul de destinaţie al pachetului (controlat de această politică).
Limită de rată jeton medie	Dimensiunea maximă de rată jeton permisă de această politică în fiecare ruter şi sistem de-a lungul căii conexiunii.
Limită de adâncime jeton	Dimensiunea maximă a buffer-ului jeton permisă de această politică în fiecare ruter şi sistem de-a lungul căii conexiunii.
Limită de rată jeton de vârf	Rata maximă permisă de această conexiune.
Pachet total	Numărul de pachete transmise de această politică din momentul în care a fost pornită până în momentul colecţiei de monitorizare.
Biţi totali	Numărul de biţi transmişi folosit de această politică din momentul în care a fost pornită până în momentul colecţiei de monitorizare.
Biţi în-afara-profilului	Numărul de biţi transmişi care depăşeşte parametrii politicii.
Rată garantată	Rata garantată în biţi pe secundă.
Biţi în profil	Numărul de biţi transmişi care se potriveşte cu parametrii acestei politici.
Dimensiune de pachet maximă	Dimensiunea de pachet maximă permisă controlată de această politică.
Unităţi de supraveghere minime	Cel mai mic număr de biţi care este înlăturat din găleata jeton. De exemplu, dacă unitatea de supraveghere minimă este 100 biţi, pachetele sub 100 de biţi vor fi totuşi înlăturate la 100 de biţi.
Pachete în profil	Numărul de pachete IP transmise care se potriveşte cu parametrii acestei politici.
Termen lent	Diferenţa (în secunde) dintre întârzierea cerută şi întârzierea obţinută.
Interval port sursă	Intervalul de porturi sursă care determină care aplicaţii sunt controlate de această politică.

Politici de acces inbound

Tabela 7. Politici de acces inbound

Câmp	Descriere
Nume politică	Numele alocat acestei politici.
Rată de conexiune	Numărul de cereri de conexiune acceptate pe secundă.
Cereri totale	Numărul total de cereri de conexiune făcute către acest sistem.
Cereri acceptate	Numărul total de cereri de conexiune acceptat de acest sistem.
Cereri aruncate	Numărul total de cereri de conexiune refuzat de acest sistem.
Limită rată de conexiune medie	Numărul permis mediu de cereri de noi conexiuni admise pe secundă.
Limită de explozie a conexiunii	Numărul maxim de cereri de conexiune nouă acceptate momentan.

Tabela 7. Politici de acces inbound (continuare)

Câmp	Descriere
Limită rată de conexiune de vârf	Rata maximă permisibilă la care sistemul acceptă conexiuni din reţea.
Prioritate	Prioritatea alocată fiecărei reguli încărcată în Managerul QoS.
Prioritate de coadă	Prioritatea alocată conexiunilor inbound plasate în coada de ascultare.
Interval port destinaţie	Intervalul de porturi sau portul către care este destinat traficul în sistemul dumneavoastră.
Adresă interfaţă	Adresă IP sau interfaţă de sistem monitorizată.
Interval adresă sursă	Intervalul de adresă IP al clienţilor care trimit cereri către sistemul dumneavoastră.
URI	Identitatea URI-ului este supravegheată.

Concepte înrudite

"Scenariu: Limitare trafic browser" la pagina 27
Puteţi utiliza calitatea serviciului (QoS) pentru a controla performanţa traficului. Folosiţi o politică de servicii diferenţiate pentru a limita sau a extinde performanţa unei aplicaţii în reţea.

"Scenariu: Rezultate sigure şi predictibile (VPN şi QoS)" la pagina 31
Dacă folosiţi o reţea privată virtuală (VPN), puteţi crea şi politici de calitatea serviciilor.

"Scenariu: Limitarea conexiunilor inbound" la pagina 35
Dacă aveţi nevoie de un control al cererilor de conexiuni inbound care sunt făcute către sistemul dumneavoastră, folosiţi o politică de acces inbound.

"Scenariu: Trafic B2B predictibil" la pagina 37
Dacă aveţi nevoie de livrare predictibilă şi încă doriţi să cereţi o rezervare, folosiţi tot o politică de servicii integrate. Acest exemplu foloseşte un serviciu de încărcare controlat.

"Scenariu: Livrarea dedicată (telefonie IP)" la pagina 41
Dacă aveţi nevoie de livrare dedicată şi doriţi să cereţi o rezervare, folosiţi o politică de servicii integrate. Există două tipuri de politici de servicii integrate ce pot fi create: încărcare garantată şi controlată. În acest exemplu, este folosit serviciul garantat.

"Scenarii: Politici QoS" la pagina 27
Aceste scenarii de politici QoS (quality of service) vă pot ajuta să înţelegeţi de ce aveţi nevoie de QoS şi cum să creaţi politici şi clase de servicii.

"Monitorizare tranzacţii de sistem" la pagina 62
Cu monitorizarea QoS puteţi să verificaţi că politicile QoS funcţionează aşa cum doriţi dumneavoastră ca ele să funcţioneze. Monitorizarea QoS vă poate ajuta în faza de plănuire şi în faza de depanare a QoS.

"Scenariu: Monitorizarea statisticilor curente de reţea" la pagina 45
În cadrul vrăjitorilor, este nevoie să setaţi limitele de performanţă care sunt bazate pe cerinţe individuale de reţea.

Depanare calitatea serviciului (QoS)

QoS furnizează mai multe metode de depanare a problemelor QoS.

Urmărire de comunicaţii

Sistemul dumneavoastră furnizează o urmărire a comunicaţiei pentru a colecta date de pe o linie de comunicaţii, cum ar fi o interfaţă LAN (local area network) sau WAN (wide area network). Utilizatorul obişnuit s-ar putea să nu înţeleagă tot conţinutul datelor de urmărire. Totuşi, puteţi folosi intrările de urmărire pentru a determina dacă într-adevăr a avut loc un schimb de date între două puncte.

Activarea QoS în sistem

Dacă serverul QoS nu porneşte, mai întâi verificaţi QoS este activat în sistem. Când vă configuraţi politicile pentru prima dată, vrăjitorul Configurare iniţială activează automat QoS-ul în sistem. Oricum, dacă această valoare a fost modificată, din orice motiv, serverul nu va porni.

Pentru a verifica dacă QoS-ul este activat în sistem, urmaţi aceşti paşi:

1. În Navigator System i, expandaţi ***sistemul dumneavoastră*** → **Reţea** → **Politici IP**.
2. Faceţi clic dreapta **Calitatea serviciului** şi selectaţi **Configurare**.
3. Când interfaţa QoS este dezactivată, faceţi clic dreapta pe **QoS** şi selectaţi **Proprietăţi**.
4. În pagina proprietăţi QoS, verificaţi dacă este selectat **Activare QoS**.

   Concepte înrudite

   Urmărire de comunicaţii

   Operaţii înrudite

   "Ordonarea politicilor QoS" la pagina 53
   Dacă aveţi două politici care se suprapun, ordinea fizică a politicilor dumneavoastră în Navigator System i este importantă.

Politici QoS de jurnalizare

QoS (Quality of service) include o funcţie de jurnalizare. Jurnalizarea vă permite să urmăriţi acţiunilie politicii QoS când o politică este adăugată, înlăturată sau modificată.

Jurnalizarea crează un istoric al acţiunilor politicilor când porniţi funcţia de jurnalizare. Aceasta vă ajută să depanaţi şi să verificaţi exact unde politicile nu operează cum ar trebui. De exemplu, setaţi o politică pentru a rula între 9:00 a.m. - 4:00 p.m. Puteţi vedea istoricul pentru a vedea dacă politica a fost într-adevăr adăugata la ora 9:00 a.m. şi ştearsă la ora 4:00 p.m.

Dacă este pornită jurnalizarea, intrările de jurnal sunt generate oricând o politică este adăugată, înlăturată sau modificată. Prin folosirea acestor jurnale, creaţi un fişier general în sistem. Puteţi apoi folosi informaţiile înregistrate în jurnalele sistemului pentru a determina cum este folosit sistemul. Aceasta vă poate ajuta să decideţi schimbarea diferitelor aspecte a politicilor dumneavoastră.

Fiţi selectiv în ceea ce alegeţi să jurnalizaţi. Jurnalizarea poate fi o povară grea pentru resursele sistemului. Pentru a porni sau opri jurnalizarea, folosiţi Navigator System i. Pentru a vedea înregistrările de jurnal, trebue să folosiţi interfaţa pe bază de caracter.

Pentru a porni sau opri jurnalizarea, urmaţi aceşti paşi:

1. În Navigator System i, expandaţi ***sistemul dumneavoastră*** → **Reţea** → **Politici IP**.
2. Faceţi clic dreapta **Calitatea serviciului** şi selectaţi **Configurare**.
3. Faceţi clic dreapta pe **QoS** şi selectaţi **Proprietăţi**.
4. Selectaţi caseta **Rulare jurnalizare** pentru a porni jurnalizarea.
5. Eliberaţi caseta pentru a opri jurnalizarea.

Notă: Dacă sistemul este deja pornit înainte de a finaliza paşi de mai sus, este nevoie să opriţi şi să reporniţi sistemul. Odată ce jurnalizarea a fost pornită există două căi de a o activa. Puteţi opri şi reporni sistemul sau să realizaţi o actualizare de sistem. Oricare ar fi metoda se reciteşte fişierul policy.conf şi se caută atributele de jurnalizare.

Vizualizarea intrărilor de jurnal pe monitor

Acest subiect conţine informaţii despre cum puteţi vizualiza intrările de jurnal pe monitor.

1. În linia de comandă a serverului iSeries introduceţi: DSPJRN JRN(QUSRSYS/QQOS).
2. Selectaţi Opţiunea 5 pe intrarea de jurnal pe care doriţi să o vedeţi.

Vizualizarea intrărilor din jurnal prin fişierul de ieşire

Dacă doriţi să vedeţi intrările din jurnal formatate într-un singur folder, vedeţi fişierul MODEL.OUT din directorul QUSRSYS. Prin copierea intrărilor din jurnal în fişierul de ieşire, puteţi vedea uşor intrările prin utilizarea utilităţilor de interogare cum ar fi Query/400 sau SQL (Structured Query Language). De asemenea puteţi să vă scrieţi propriile programe de HHL (high-level language - limbaj de nivel înalt) pentru a procesa intrările din fişierele de ieşire.

Pentru a copia intrările de jurnal QoS (quality of service) în fişierul de ieşiri livrat de sistem, urmaţi aceşti paşi:

1. Creaţi o copie a fişierului de ieşire furnizat de sistem QSYS/QATOQQOS într-o bibliotecă utilizator. Puteţi face aceasta utilizând comanda (CRTDUPOBJ) Creare obiect duplicat. Următorul şir este un exemplu al comenzii CRTDUPOBJ:
   - CRTDUPOBJ OBJ(QADSPJR4) FROMLIB(Qsys) OBJTYPE(*FILE) TOLIB(*userlib*) NEWOBj(*userfile*)
2. Folosiţi comanda Afişare jurnal (DSPJRN) pentru a copia intrările din jurnalul QUSRSYS/QQOS în fişierul de ieşire creat la pasul anterior. Dacă încercaţi să copiaţi DSPJRN într-un fişier de ieşire care nu există, sistemul ceează fişierul pentru dumneavoastră dar acest fişier nu conţine descrierile de câmp corecte.
   - DSPJRN JRN(QUSRSYS/QQOS) JRNCDE((M)) ENTTYP(MP) CMTCYCID(*ALL) OUTPUT(*OUTFILE) OUTFILFMT(*TYPE4) OUTFILE(*userlib*/*userfile*)
   - DSPF FILE(*userlib*/*userfile*)

Înregistrarea în istoric a joburilor de server QoS

Când întâmpinaţi probleme cu politicile dumneavoastră QoS (quality of service), analizaţi istoricul de joburi. Istoricul de joburi conţine mesaje de eroare şi alte informaţii înrudite cu QoS.

Doar un singur job QoS, QTOQSRVR, rulează în subsistemul QSYSWRK. Puteţi vedea istoricul de joburi server QoS vechi şi curent din Navigator System i.

Pentru a vedea istoricul, urmaţi aceşt paşi:

1. Expandaţi **Reţea** şi faceţi clic **Politici IP**.
2. Faceţi clic dreapta **Calitatea serviciului**.
3. Selectaţi **Unelte de diagnosticare → Istoric server QoS**.

Acesta deschide o fereastră care vă permite să lucraţi cu jobul.

Următoarea listă arată cele mai importante nume de joburi, alături de o scurtă explicaţie despre utilizarea lor:

QTCP Acest job este jobul de bază care porneşte toate interfeţele TCP/IP. Dacă aveţi probleme fundamentale cu TCP/IP în general, analizaţi istoricul de job QTCPIP.

QTOQSRVR
Acest job este jobul de bază care vă dă informaţiile de istoric specifice pentru QoS. Rulaţi comanda Work with Spooled File (WRKSPLF QTCP) şi căutaţi jurnalul QTOQSRVR.

Verificarea fişierului spool pentru erori

Pentru a verifica fişierul spool pentru o eroare, efectuaţi următorii paşi:

1. De la o interfaţă linie de comandă, introduceţi WRKSPLF QTCP şi apăsaţi Enter. Se deschide fereastra Lucru cu toate fişierele spool.
2. În coloana Date utilizator, căutaţi QTOQSRVR pentru a găsi erorile care privesc în special serverul QoS.
3. Selectaţi **opţiunea 5** în linia unde doriţi să se afişeze. Citiţi aceste informaţii şi înregistraţi ID-ul de mesaj care explică problema. De exemplu, TCP920C.
4. Apăsaţi Ieşire de două ori pentru a vă întoarce la meniul principal.
5. De la interfaţa linie de comandă, introduceţi WRKMSGF şi apăsaţi Enter.
6. În panoul Lucru cu Fişier Mesaj, introduceţi următoarele informaţii şi apăsaţi Enter:

```
Fişier mesaj: QTCPMSG
Bibliotecă: *LIBL
```

7. În panoul Lucru cu Fişier Mesaj, selectaţi **opţiunea 5** pentru a afişa fişierul de mesaje pe care doriţi să îl vedeţi şi apăsaţi Enter.
8. În ecranul Afişare descrieri mesaje, introduceţi următoarele informaţii: Poziţionare la: *Introduceţi ID-ul de mesaj de la numărul 3 de sus şi apăsaţi Enter.*. De exemplu, TCP920C.
9. Selectaţi **opţiunea 5** pe ID-ul mesajului corespunzător şi apăsaţi Enter.
10. În detaliile Selectare mesaj de afişat, selectaţi **30 (Toate de mai sus)** şi apăsaţi Enter.

    Se deschide o descriere detaliată a mesajului.

Monitorizare tranzacţii de sistem

Cu monitorizarea QoS puteţi să verificaţi că politicile QoS funcţionează aşa cum doriţi dumneavoastră ca ele să funcţioneze. Monitorizarea QoS vă poate ajuta în faza de plănuire şi în faza de depanare a QoS.

Puteţi folosi monitorul pentru a analiza traficul dumneavoastră IP prin sistem. Aceasta vă ajută să determinaţi unde apare congestionarea în reţea. Monitorizarea QoS vă poate ajuta să vă continuaţi monitorizarea reţelei astfel încât să puteţi ajusta politicile după nevoie.

Plănuirea şi menţinerea performanţei

Una dintre cele mai dificile părţi în implementarea QoS este determinarea a ce limite de performanţă să setaţi în politicile dumneavoastră. Nu există o recomandare specială deoarece fiecare reţea este diferită. Pentru a vă ajuta să determinaţi ce valori sunt bune pentru dumneavoastră, aţi putea folosi monitorizarea înainte de a porni orice politică cu specific de afaceri.

Încercaţi să creaţi o politică de servicii diferenţiate fără a selecta măsurarea a identifica cum se comportă traficul curent al reţelei. Activaţi politica şi porniţi monitorizarea. Rezultatele monitorizării vă pot ajuta să vă ajustaţi politicile la nevoile specifice. Consultaţi un exemplu de monitorizare politică care identifică cum se comportă traficul dumneavoastră curent.

Depanare probleme de performanţă

Puteţi folosi monitorizarea şi pentru a depana probleme. Prin folosirea rezultatelor de monitorizare, puteţi determina dacă parametrii pe care îi asignaţi unei politici sunt urmăriţi. Dacă politicile dumneavoastră apar în monitor, dar nu par să afecteze traficul, verificaţi următoarele:

- Dacă politica filtrează pe baza unui URI, verificaţi că FRCA este activat şi configurat corespunzător. Înainte de a seta o politică inbound care utilizează URI-uri, trebuie să vă asiguraţi de faptul că portul aplicaţiei alocat pentru URI se potriveşte directivei ″Ascultare″ activată pentru FRCA în configurarea serverului Web Apache.
- Verificaţi programarea politicii. Este posibil să căutaţi rezultatele în timpul unui timp inactiv.
- Verificaţi că numărul portului este corect.
- Verificaţi că adresa IP este corectă.

Concepte înrudite

“Planificarea pentru calitatea serviciului” la pagina 47
Cel mai important pas pentru a realiza calitatea serviciilor este planificarea. Pentru a primi rezultatele aşteptate, trebuie să revedeţi echipamentul de reţea şi să monitorizaţi traficul de reţea.

“Scenarii: Politici QoS” la pagina 27
Aceste scenarii de politici QoS (quality of service) vă pot ajuta să înţelegeţi de ce aveţi nevoie de QoS şi cum să creaţi politici şi clase de servicii.

Referinţe înrudite

“Monitorizarea QoS” la pagina 55
Puteţi folosi monitorizarea QoS (quality of service) pentru a analiza traficul dumneavoastră IP prin sistem.

Informaţii înrudite

Gestionarea adreselor şi porturilor pentru serverul HTTP (motorizat de Apache).

Urmărirea aplicaţiilor TCP

Puteţi folosi urmărirea QoS (quality of service) să lucreze cu funcţiile de urmărire şi pentru a vedea buffer-ul curent de urmărire.

Pentru a rula urmărirea în sistem, tastaţi TRCTCPAPP (comanda Trace TCP/IP Application - Urmărirea aplicaţie TCP/IP) de la o interfaţă linie de comandă.

Acesta este un exemplu al selecţiei de urmărire de efectuat:

```
Aplicaţie TCP/IP...................> *QOS
Setare opţiune urmărire.....................> *ON
Spaţiul maxim de memorare pentru urmărire....> *APP
Urmărire întreaga acţiune...................> *WRAP
Liste de argumente..........................> 'lvl=4'
Tipul de urmărire QoS.......................> *ALL
```

Următorul tabel introduce parametrii posibili de utilizat într-o urmărire. Dacă o setare nu este afişată în interfaţa pe bază de caractere, trebuie să o introduceţi într-o comandă. De exemplu, TRCTCPAPP APP(*QOS) MAXSTG(1000) TRCFULL(*STOPTRC) ARGLIST('l=4 c=i').

Setări	Opţiuni
Aplicaţie TCP/IP	QOS
Setare opţiune urmărire	*ON, *OFF, *END, *CHK
Spaţiul maxim de memorare pentru urmărire (MAXSTG)	1-16000, *APP
Urmărire întreaga acţiune (TRCFULL)	*WRAP, *STOPTRC
Liste de argumente (ARGLIST)	Niveluri: 'lvl=1', 'lvl=2', 'lvl=3', 'lvl=4' Content: 'c=a', 'c=i', 'c=d', 'c=m'
Tipul de urmărire QoS	*ALL

Spaţiul maxim de memorare pentru urmărire

1-16000

Aceasta este dimensiunea de memorie maximă pentru datele de urmărire. Urmărirea ori se opreşte ori este ascunsă când este atinsă dimensiunea. Dimensiunea implicită este 4 MB. Pentru a specifica dimensiunea implicită, selectaţi *APP.

***APP** Aceasta este opţiunea implicită. Spune aplicaţiei să îşi folosească dimensiunea de urmărire implicită. Dimensiunea implicită de urmărire pentru serverul QoS este 4 MB.

Urmărire întreaga acţiune

***WRAP**

Ascunde informaţiile de urmărire când urmărirea atinge spaţiul de disc maxim (dimensiunea buffer-ului de urmărire). Ascunderea permite sistemului să suprascrie cele mai vechi informaţii din fişier astfel încât să puteţi continua înregistrarea de informaţii de urmărire. Dacă nu selectaţi ascunderea, atunci operaţia de ascundere se opreşte când discul este plin.

***STOPTRC**

Opreşte colectarea de informaţii atunci când sistemul atinge spaţiul maxim de disc.

Liste de argumente

Listele de argumente specifică ce niveluri de erori şi conţinut sunt înregistrate în istoric. Sunt două argumente permise în comanda TRCTCPAPP : nivelul de urmărire şi conţinutul de urmărit. Când specificaţi nivelul de urmărire şi conţinutul de urmărire, asiguraţi-vă că toate atributele sunt conţinute într-un singur set de ghilimele, de exemplu TRCTCPAPP ’l=4 c=a’

Notă: Nivelurile de înregistrare sunt inclusive. Aceasta înseamnă că, atunci când selectaţi un nivel de înregistrare, toate nivelurile de înregistrare anterioare sunt şi ele selectate. De exemplu, dacă selectaţi nivelul 3, atunci nivelurile 1 şi 2 sunt automat incluse. Într-o urmărire tipică, se recomandă să specificaţi ’l=4’.

Niveluri de urmărire

Nivel 1: Erori de sistem (SYSERR)
Se înregistrează erorile care apar în operaţiile de sistem. Dacă această eroare apare, serverul QoS nu poate continua. De exemplu, poate apare o eroare de sistem dacă vi se termină memoria de sistem sau dacă sistemul dumneavoastră nu poate comunica cu TCP/IP. Acesta este nivelul implicit.

Nivel 2: Erori între obiecte (OBJERR)
Se înregistrează erorile care apar în codul de server QoS. De exemplu, o eroare de obiect poate apărea deoarece o operaţie de sistem întâlneşte un răspuns neaşteptat. Aceasta este, în general, o condiţie serioasă care trebuie raportată serviciului.

Nivel 3: Evenimente specifice (EVENT)
Înregistrează orice operaţie QoS care a apărut. De exemplu, un istoric eveniment înregistrează comenzi şi cereri. Rezultatele sunt similare funcţiei de jurnalizare QoS.

Nivel 4: Mesaje urmărire (TRACE)
Urmăreşte toate datele transferate la şi de la serverul QoS. De exemplu, ar trebui să folosiţi urmărirea aceasta de nivel înalt pentru înregistrarea în istoric a orice credeţi dumneavoastră că ar fi de ajutor pentru depanarea problemelor. Aceste informaţii sunt folositoare să determinaţi unde a apărut o problemă şi cum să reproduceţi problema.

Conţinut urmărire

Specificaţi doar un singur tip de conţinut. Dacă nu specificaţi ce conţinut să se urmărească, atunci (implicit) va fi urmărit tot conţinutul.

Conţinut = All (’c=a’)
Urmăreşte toate funcţiile serverului QoS. Aceasta este valoarea implicită.

Conţinut = Intserv (’c=i’)
Urmăreşte doar operaţiile serviciilor integrate. Folosiţi aceasta dacă se determină că problema este legată de serviciile integrate.

Conţinut = Diffserv (’c=d’)
Urmăreşte doar operaţiile serviciilor diferenţiate. Folosiţi aceasta dacă se determină că problema este legată de serviciile diferenţiate.

Conţinut = Monitor (’c=m’)
Urmăreşte doar operaţiile de monitorizare.

Pagina outbound a urmăririi conţine exemple de ieşiri cu comentarii pentru a vă ajuta să le interpretaţi înţelesul. Funcţia TRCTCPAPP este folosită, de obicei, de către serviciu,deci dacă aveţi probleme în a citi ieşirea, ar trebui să contactaţi reprezentanţii dumneavoastră de service.

Referinţe înrudite

TRCTCPAPP (Trace TCP/IP Application - Urmărire aplicaţie TCP/IP)

Exemple: Citirea ieşirii urmăririi

Aceasta nu este o discuţie atotcuprinzătoare despre cum să vă ieşirea urmăririi. Totuşi, subliniază evenimentele cheie de căutat în informaţiile de urmărire.

Într-o politică de servicii integrate, cel mai important eveniment de luat în considerare este dacă conexiunea RSVP (ReSerVation Protocol) a fost respinsă deoarece o politică pentru acea conexiune nu a fost găsită. Acesta este un exemplu a unui mesaj de succes:

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

Acesta este un exemplu al unui mesaj de conexiune de servicii integrate fără succes:

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

Pentru o politică de servicii diferenţiate, cele mai importante mesaje afişează dacă serverul a încărcat o regulă de politică sau dacă a apărut o eroare în fişierul de configuraţie al politicii.

```
Exemplu:
01/11 14:07:52 [376,57] TRCE :......KernelAddPolicyRule: Installing rule = timed_42ring.
01/11 14:07:52 [376,57] EVNT :.......create_tcp_resv: No value in config file for
DiffServInProfilePeakRate, defaulted to 100000 00.
01/11 14:07:52 [376,57] TRCE :.......create_tcp_resv: Create resv - bRate:
537395 5761SS1 V6R1M0 010525 TRCTCPAPP Output RS004 Date-01/11/07 Time-14:08:03 Page-6
01/11 14:07:52 [376,57] TRCE :.......create_tcp_resv: Create resv - bRate: 537395 5722SS1 V5R1M0
010525 TRCTCPAPP Output RS004 Date-01/11/01 Time-14:08:03 Page-6
01/11 14:07:52 [376,57] TRCE :.......create_tcp_resv: bDepth: 32768
01/11 14:07:52 [376,57] TRCE :.......create_tcp_resv: peakR: 10000000
01/11 14:07:52 [376,57] TRCE :.......create_tcp_resv: m: 128
01/11 14:07:52 [376,57] TRCE :.......create_tcp_resv: M: 41452
01/11 14:07:52 [376,57] TRCE :.......create_tcp_resv: mark(TOS): a0
01/11 14:07:52 [376,57] TRCE :.......create_tcp_resv: flags: 15
01/11 14:07:52 [376,57] TRCE :.......create_tcp_resv: flowspe.form = 1, QOS_FORMAT_DS = 1
```

Puteţi avea şi un mesaj care să arate că etichetele din fişierul de configurare al politicii au fost incorecte. Acestea sunt câteva exemple de mesaje:

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

Notă: Semnul % este o variabilă care reprezintă o etichetă necunoscută.

Informaţii înrudite pentru Calitatea serviciului

RFC-uri QoS, publicaţii IBM Redbooks, şi alte colecţii de subiecte din centrul de informare conţin informaţii care sunt înrudite cu colecţia de subiecte Calitatea serviciului. Puteţi vedea sau tipări oricare din fişierele PDF.

RFC-uri (Request for Comments) pentru QoS

RFC-urile (Requests for Comments) sunt definiţii scrise de standarde de protocoale şi standarde propuse folosite pentru Internet. RFC-urile ce urmează pot fi de ajutor pentru înţelegerea QoS şi a funcţiilor înrudite cu QoS:

- **RFC 1349.**

  Acest RFC discută noile definiţii ale tipului de serviciului câmp de octeţi într-un antet de pachet IP.
- **RFC 2205.**

  Acest RFC explică definiţia RSVP (Resource ReSerVation Protocol)
- **RFC 2210.**

  Acest RFC explică utilizarea RSVP cu serviciile integrate IETF (Internet Engineering Task Force).

- **RFC 2474.**

  Acest RFC explică definiţia Câmpului Servicii diferenţiate.
- **RFC 2475.**

  Acest RFC explică arhitectura serviciilor diferenţiate.

Pentru a vedea RFC-urile listate anterior, vizitaţi Motorul de căutare index RFC localizat în situl web Editor RFC .

IBM Redbooks

- IBM i5/OS IP Networks: Dynamic (about 16 589 KB). Vă arată cum să proiectaţi o reţea IP care se auto-configurează, este tolerantă la greşeală şi eficientă în operare. Pe lângă multe alte funcţii, explică atât teoria din spatele QoS cât şi implementarea ei în sistem. De asemenea puteţi găsi mai multe scenarii cu instrucţiuni pas-cu-pas.
- V4 TCP/IP for AS/400: More Cool Things Than Ever (aproximativ 10 035 KB). Acest manual oferă scenarii exemplu care demonstrează soluţii comune cu configuraţii exemplu. Informaţiile din acest manual vă ajută să planificaţi, instalaţi, adaptaţi, configuaţi şi depanaţi TCP/IP în sistemul dumneavoastră. Nu include încă în mod special Calitatea serviciului, dar trece prin informaţiile server director LDAP.
- TCP/IP Îndrumar şi privire generală tehnică (aproximativ 7885 KB). Acest manual oferă o introducere precum şi o referinţă la suita de protocoale şi aplicaţii TCP/IP. Puteţi găsi QoS în *Partea 3. Concepte avansate şi tehnologii noi* la Capitolul 22.

Alte informaţii

- IBM Tivoli Directory Server for i5/OS (LDAP). Vizualizaţi acest subiect pentru a obţine cunoştinţe de bază despre server de directoare, configurare, administrare şi depanare. Subiectul servicii de directoare vă va da şi resurse adiţionale pentru a vă configura serverul de directoare.
- Detectarea intruziunilor. Acest subiect discută despre adunarea de informaţii despre încercările de acces neautorizat şi atacuri venite pe reţeaua TCP/IP. Administratorii de securitate pot analiza înregistrările de auditare furnizate de detecţia de intruziune pentru a proteja reţeaua i5/OS de aceste tipuri de atacuri.

  Referinţe înrudite

  “Fişierul PDF pentru Calitatea serviciului (QoS)” la pagina 1
  Puteţi vizualiza şi tipări un fişier PDF cu aceste informaţii.

Anexa. Observaţii

Aceste informaţii au fost elaborate pentru produse şi servicii oferite în S.U.A.

Este posibil ca IBM să nu ofere în alte ţări produsele, serviciile sau caracteristicile discutate în acest document. Luaţi legătura cu reprezentantul IBM local pentru informaţii despre produsele şi serviciile disponibile în zona dumneavoastră. Referirea la un produs, program sau serviciu IBM nu înseamnă că se afirmă sau că se sugerează faptul că poate fi folosit numai acel produs, program sau serviciu IBM. Poate fi folosit în loc orice produs, program sau serviciu care este echivalent din punct de vedere funcţional şi care nu încalcă dreptul de proprietate intelectuală al IBM. Însă evaluarea şi verificarea modului în care funcţionează un produs, program sau serviciu non-IBM ţine de responsabilitatea utilizatorului.

IBM poate avea brevete sau aplicaţii în curs de brevetare care să acopere subiectele descrise în acest document. Furnizarea acestui document nu vă acordă nici o licenţă asupra acestor patente. Puteţi trimite întrebări cu privire la licenţe, în scris, la:

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

Pentru întrebări privind licenţa pentru informaţiile DBCS (double-byte character set), contactaţi departamentul de Proprietate intelectuală al IBM-ului din ţara dumneavoastră sau trimiteţi întrebările în scris la:

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

Următorul paragraf nu se aplică în cazul Marii Britanii sau al altor ţări unde asemenea prevederi sunt incompatibile cu legile locale: INTERNATIONAL BUSINESS MACHINES CORPORATION OFERĂ ACEASTĂ PUBLICAŢIE “CA ATARE” FĂRĂ NICI UN FEL DE GARANŢIE EXPLICITĂ SAU IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA GARANŢIILE IMPLICITE DE NEÎNCĂLCARE A UNOR DREPTURI SAU NORME, DE VANDABILITATE SAU DE POTRIVIRE CU UN ANUMIT SCOP. Unele state nu permit declinarea responsabilităţii pentru garanţiile exprese sau implicite în anumite tranzacţii şi de aceea este posibil ca aceste clauze să nu fie valabile în cazul dumneavoastră.

Aceste informaţii pot include inexactităţi tehnice sau erori tipografice. Se efectuează modificări periodice la informaţiile incluse aici; aceste modificări vor fi încorporate în noi ediţii ale publicaţiei. IBM poate aduce îmbunătăţiri şi/sau modificări produsului (produselor) şi/sau programului (programelor) descrise în această publicaţie în orice moment, fără notificare.

Referirile din aceste informaţii la adrese de site-uri Web non-IBM sunt făcute numai pentru a vă ajuta, fără ca prezenţa lor să însemne un gir acordat acestor site-uri Web. Materialele de pe site-urile Web respective nu fac parte din materialele pentru acest produs IBM, iar utilizarea acestor site-uri Web se face pe propriul risc.

IBM poate utiliza sau distribui oricare dintre informaţiile pe care le furnizaţi, în orice mod considerat adecvat, fără ca aceasta să implice vreo obligaţie faţă de dumneavoastră.

Posesorii de licenţe pentru acest program care doresc să aibă informaţii despre el în scopul de a permite: (I) schimbul de informaţii între programe create independent şi alte programe (inclusiv acesta) şi (II) utilizarea mutuală a informaţiilor care au fost schimbate, vor contacta:

IBM Corporation

Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
S.U.A.

Aceste informaţii pot fi disponibile cu condiţia respectării termenilor şi condiţiilor, iar în unele cazuri cu plata unor taxe.

Programul cu licenţă descris în acest document şi toate produsele cu licenţă disponibile pentru acesta sunt furnizate de către IBM sub termenii Contractului IBM cu Clientul, Contractului IBM de licenţa internaţională a programului, Contractului IBM de licenţă pentru cod maşină sau orice contract echivalent între noi.

Toate datele de performanţă din acest document au fost determinate într-un mediu controlat. De aceea, rezultatele obţinute în alte medii de funcţionare pot fi diferite. Unele măsurători s-ar putea să fi fost făcute pe sisteme la nivel de dezvoltare şi nu există nici o garanţie că aceste măsurători vor fi identice pe sistemele disponibile pe piaţă. Mai mult de atât, unele măsurători s-ar putea să fi fost estimate prin extrapolare. Rezultatele reale pot fi diferite. Utilizatorii acestui document trebuie să verifice datele aplicabile pentru mediul lor specific.

Toate declaraţiile privind direcţiile de viitor şi intenţiile IBM-ului pot fi schimbate sau se poate renunţa la ele, fără notificare prealabilă şi reprezintă doar scopuri şi obiective.

Informaţiile privind produsele non-IBM au fost obţinute de la furnizorii acestor produse, din anunţurile lor publicate sau din alte surse disponibile publicului. IBM nu a testat aceste produse şi nu poate confirma acurateţea performanţelor, compatibilitatea sau oricare alte pretenţii legate de produsele non-IBM. Întrebările legate de capacităţile produselor non-IBM le veţi adresa furnizorilor acestor produse.

Aceste informaţii conţin exemple de date şi rapoarte folosite în operaţiile comerciale de zi cu zi. Pentru a fi cât mai complete, exemplele includ nume de persoane, de companii, de mărci şi de produse. Toate aceste nume sunt fictive şi orice asemănare cu nume sau adrese folosite de o întreprindere reală este pură coincidenţă.

LICENŢĂ - COPYRIGHT:

Aceste informaţii cuprind exemple de programe de aplicaţie în limbaj sursă, care ilustrează tehnici de programare pe diverse platforme de operare. Puteţi copia, modifica şi distribui aceste programe-eşantion în orice formă fără necesitatea unei plăţi către IBM, în scopul dezvoltării, utilizării, marketingului sau distribuirii programelor de aplicaţie în concordanţă cu interfaţa de programare a aplicaţiei pentru platforma de operare pentru care sunt scrise programele-eşantion. Aceste exemple nu au fost testate complet în toate condiţiile. Prin urmare, IBM nu poate garanta sau sugera că aceste programe vor fi fiabile, practice sau funcţionale.

Fiecare copie sau orice porţiune din aceste exemple de program sau orice lucrare derivată din acestea trebuie să includă un anunţ de copyright de genul următor:

© (numele companiei dumneavoastră) (anul). Porţiuni din acest cod sunt derivate din Programe eşantion ale IBM Corp.
© Copyright IBM Corp. _introduceţi anul sau anii_. Toate drepturile rezervate.

Dacă vedeţi aceste informaţii folosind o copie electronică, fotografiile şi ilustraţiile color s-ar putea să nu apară.

Informaţii despre interfaţa de programare

Această publicare QoS documentează anumite Interfeţe de programare care permit clientului să scrie programe care obţin servicii de la IBM i5/OS.

Mărci comerciale

Următorii termeni sunt mărci comerciale ale International Business Machines Corporation în Statele Unite, în alte ţări sau ambele:

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

Adobe, logo-ul Adobe, PostScript şi logo-ul PostScript sunt fie mărci comerciale înregistrate fie mărci comerciale ale Adobe Systems Incorporated în Statele Unite, şi/sau alte ţări.

Alte nume de companii, produse sau servicii pot fi mărci comerciale sau mărci de serviciu ale altora.

Termenii şi condiţiile

Permisiunile pentru utilizarea acestor publicaţii sunt acordate în conformitate cu următorii termeni şi condiţii.

Utilizare personală: Puteţi reproduce aceste publicaţii pentru utilizarea personală, necomercială, cu condiţia ca toate anunţurile de proprietate să fie păstrate. Nu puteţi distribui, afişa sau realiza obiecte derivate din aceste publicaţii sau dintr-o porţiune a lor fără consimţământul explicit al IBM.

Utilizare comercială: Puteţi reproduce, distribui şi afişa aceste publicaţii doar în cadrul întreprinderii dumneavoastră, cu condiţia ca toate anunţurile de proprietate să fie păstrate. Nu puteţi să realizaţi lucrări derivate din aceste informaţii, nici să reproduceţi, să distribuiţi sau să afişaţi aceste informaţii sau o porţiune a lor în afara întreprinderii dumneavoastră fără consimţământul explicit al IBM.

Cu excepţia a ceea ce este acordat explicit prin această permisiune, nu sunt acordate alte permisiuni, licenţe sau drepturi, explicit sau implicit, pentru Publicaţii sau alte informaţii, date, software sau altă proprietate intelectuală conţină în acestea.

IBM îşi rezervă dreptul de a retrage permisiunile acordate aici oricând consideră că folosirea publicaţiilor este în detrimentul intereselor sale sau când personalul IBM constată că instrucţiunile de mai sus nu sunt urmate corespunzător.

Nu puteţi descărca, exporta sau reexporta aceste informaţii decât în deplină conformitate cu legile şi regulamentele aplicabile, inclusiv toate legile şi regulamentele de export ale Statelor Unite.

IBM NU ACORDĂ NICI O GARANŢIE PENTRU CONŢINUTUL ACESTOR PUBLICAŢII. ACESTE PUBLICAŢII SUNT FURNIZATE ″CA ATARE″, FĂRĂ NICI UN FEL DE GARANŢIE, EXPLICITĂ SAU IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA ELE, GARANŢIILE IMPLICITE DE VANDABILITATE, DE NEÎNCĂLCARE A UNOR DREPTURI SAU NORME ŞI DE POTRIVIRE PENTRU UN ANUMIT SCOP.

Tipărit în S.U.A.