IBM Systems - iSeries

Lucru în reţea
QoS (Quality of Service)

Versiunea 5 Ediţia 4

IBM Systems - iSeries

Lucru în reţea
QoS (Quality of Service)

Versiunea 5 Ediţia 4

Notă

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

Ediţia a cincea (Februarie 2006)

Această ediţie se aplică versiunii 5, ediţia 4, modificarea 0 a IBM i5/OS (număr produs 5722-SS1) şi tuturor ediţiilor şi modificărilor ulterioare, până când se indică altceva în ediţiile noi. Această versiune nu rulează pe toate modelele RISC şi nici pe modelele CISC.

Cuprins

Calitatea serviciului

Soluţia iSeries de QoS permite politicilor să ceară reţelei prioritate şi lăţime de bandă pentru aplicaţiile TCP/IP.

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 îngrijorătoare. Este critic ca, în timpul prezentării, această aplicaţie să primească o performanţă mai mare 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 de pe serverul iSeries pot de asemenea să limiteze datele care ies din serverul dumneavoastră, să gestioneze cererile de conexiuni şi să controleze sarcina serverului. Serverul QoS trebuie să fie activ pentru a activa politica de detectare a intruziunilor.

Este important de înţeles QoS înainte de a începe să configuraţi politicile.

Ce este nou pentru V5R4

Funcţie nouă pentru detectarea intruziunilor

Pentru V5R4, serverul QoS furnizează capabilităţi de detectare a intruziunilor printr-o politică de detectare a intruziunilor. Pentru a activa această nouă politică, serverul QoS trebuie să ruleze. Folosind politica de detectare a intruziunilor QoS, puteţi detecta intruziuni, crea înregistrări de auditare şi gestiona mesaje care indică o posibilă încercare de intruziune. Pentru informaţii suplimentare consultaţi Funcţia de detectare a intruziunilor.

Cum puteţi vedea ce este nou sau modificat

Pentru a vă ajuta să vedeţi unde au fost făcute modificări tehnice, aceste informaţii folosesc:

- Imaginea » pentru a marca unde încep informaţiile noi sau modificate.
- Imaginea « pentru a marca unde se termină informaţiile noi sau modificate.

Pentru a găsi alte informaţii despre ce este nou sau modificat în această ediţie, vedeţi Memo către utilizatori.

PDF tipăribil

Folosiţi aceasta pentru a vizualiza sau pentru a tipări un 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 PDF în browser (faceţi clic dreapta pe legătura de mai sus).
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 de Adobe Reader pentru a vizualiza sau tipări aceste PDF-uri. Puteţi descărca gratis o copie de la situl Web Adobe (www.adobe.com/products/acrobat/readstep.html) .

Concepte

Dacă sunteţi nou în ceea ce priveşte QoS, puteţi citi câteva concepte de bază QoS.Aceasta vă va oferi o privire generală asupra modului de funcţionare al QoS şi despre cum funcţionează împreună funcţiile QoS.

Înainte de a încerca să faceţi QoS, se recomandă insistent să cercetaţi subiectul şi să vă asiguraţi că serviciul acesta vă va satisface nevoile. Termenii QoS pot fi găsiţi în surse multiple, astfel încât acest subiect va trata doar ceea ce este elementar.

Pentru QoS, veţi configura politici folosind vrăjitori în Navigatorul iSeries. O *politică* este un set de reguli care desemnează o acţiune. Politica exprimă, în fond, care client, aplicaţie şi programare (pe care dumneavoastră o desemnaţi) trebuie să primească un anumit serviciu. Puteţi, în cele din urmă, să configuraţi trei tipuri de politică:

- Servicii diferenţiate
- Servicii integrate
- Admitere intrare

Serviciile diferenţiate şi *serviciile integrate* sunt considerate politici de lăţime de bandă ieşire. Politicile de ieşire limitează datele ce părăsesc reţeaua dumneavoastră şi vă ajută să controlaţi încărcarea serverului. Ratele pe care le-aţi setat în politica de ieşire controlează cum şi ce date sunt sau nu limitate în server. Amândouă politicile de ieşire necesită un SLA cu ISP-ul dumneavoastră.

Politicile admitere intrare controlează cererile de conexiune care intră în reţeaua dumneavoastră dintr-o sursă externă. Politicile de intrare nu sunt dependente de nivelul de serviciu de la ISP-ul dumneavoastră. Pentru a decide ce politică trebuie să folosiţi, evaluaţi motivele pentru care doriţi să folosiţi QoS şi luaţi în considerare rolul serverului dumneavoastră iSeries.

Una din părţile cele mai importante ce au grijă de QoS este însuşi serverul dumneavoastră. Dumneavoastră trebuie nu numai să înţelegeţi conceptele QoS, dar trebuie şi să fiţi conştient de rolul pe care-l joacă serverul dumneavoastră pentru aceste noţiuni. Serverul iSeries poate juca doar rolul unui client sau al unui server, nu al unui ruter. De exemplu, un server iSeries ce acţionează ca un client, poate utiliza politici de servicii diferenţiate pentru a se asigura că cererilor de informaţii pentru alte servere le este acordată o prioritate mai mare prin reţea. Un server iSeries ce acţionează ca un server, poate utiliza o politică de admitere intrare pentru a limita cererile URI acceptate de server.

Concepte înrudite

“Acord la nivel de serviciu” la pagina 48
Această secţiune punctează unele din aspectele importante ale acordului SLA (service-level agreement), care pot afecta implementarea QoS.

Referinţe înrudite

“Informaţii înrudite pentru QoS” la pagina 65
Listate mai jos sunt IBM Redbooks (în format PDF), site-uri Web şi subiectele Centrului de informare legate de subiectul QoS. Puteţi citi sau tipări oricare din PDF-uri.

Servicii diferenţiate

Acesta este primul tip de politică de lăţime de bandă de ieşire pe care o puteţi crea pe server. Serviciile diferenţiate împart traficul dumneavoastră pe clase. Pentru a avea grijă de politicile de servicii diferenţiate, trebuie să determinaţi cum doriţi să vă clasificaţi traficul din reţea şi cum manipulaţi clasele diferite.

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 garantarea livrării pachetelor în politici de lăţime de bandă de ieşire, atât servicii integrate cât şi diferenţiate.

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

"Scenariu: Limitarea traficului de browser" la pagina 27
Puteţi utiliza calitatea serviciilor (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. Acest exemplu le arată pe cele două fiind folosite împreună.

Referinţe înrudite

"Folosirea punctelor de cod pentru alocarea unui comportament per hop" la pagina 14
Calitatea serviciului (QoS - Quality of service) foloseşte următoarele puncte de cod pentru a aloca comportamente per-hop traficului.

"Configurarea QoS cu vrăjitori" la pagina 50
Pentru a configura politicile QoS, trebuie să folosiţi vrăjitorii QoS din Navigatorul iSeries.

Informaţii înrudite

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

Clase prioritare: Cum să clasificaţi traficul de reţea

Serviciul diferenţiat identifică traficul pe *clase*. Cele mai comune clase sunt definite utilizând adrese IP client, porturi de aplicaţie, tipuri de servere, protocoale, adrese locale IP şi planificări. Întreg traficul ce concordă aceleaşi clase este tratat la fel.

Pentru clasificări mai avansate, unele din aplicaţiile dumneavoastră iSeries TM pot primi niveluri diferite de serviciu prin specificarea datelor de server. Folosirea datelor de server este opţională, dar poate fi de ajutor când doriţi să faceţi clasificare la un nivel mai scăzut. Datele de server se bazează pe tipuri de date de aplicaţie: *jeton aplicaţie* sau *URI*. Dacă traficul se potriveşte jetonului sau URI-ului pe care îl specificaţi în politică, politica va fi aplicată la răspunsul de ieşire, prin aceasta dându-se traficului la ieşire ce prioritate este specificată în politica de servicii diferenţiate.

Folosirea jetonului de aplicaţie cu politici de servicii diferenţiate

Folosirea datelor aplicaţie va spune politicii să răspundă parametrilor specifici (jeton şi prioritate) înaintaţi de aplicaţie serverului prin API-ul sendmsg(). Această setare este opţională. Dacă nu aveţi nevoie de acest nivel de granularitate în politicile dumneavoastră de ieşire, selectaţi în vrăjitor **Toate jetoanele**. Puteţi să potriviţi un jeton şi o prioritate unei aplicaţii cu un jeton şi o prioritate specifice setate în politica de ieşire, daca doriţi. În politică, există două părţi de setare a datelor aplicaţie, ce includ jetonul şi prioritatea.

- Ce este un jeton aplicaţie?

  Un jeton aplicaţie este orice şir de caractere ce poate reprezenta o sursă definită, precum myFTP. Jetonul pe care îl specificaţi în politica QoS este comparat cu jetonul furnizat de aplicaţia de ieşire. Aplicaţia 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 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 aplicaţie selectat**.
  3. Pentru a crea un jeton nou, apăsaţi **Nou**. Apare 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 aplicaţie specificată de dumneavoastră este comparată cu prioritatea aplicaţiei furnizată de aplicaţia de ieşire. Aplicaţia furnizează valoarea priorităţii folosind 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 jetonul aplicaţie ca tip de date aplicaţie, aplicaţia ce furnizează această informaţie serverului trebuie să fie codificată specific pentru a folosi API-ul sendmsg(). Aceasta se realizează de către programatorul aplicaţiei. Documentaţia aplicaţiei trebuie să furnizeze valori valide (jeton şi prioritate), pe care le va utiliza administratorul QoS în politica 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 valorilor setate în politică, se va modifica aplicaţia sau va trebui să folosiţi parametrii diferiţi de date aplicaţie pentru politica de servicii diferenţiate.

Folosirea unui URI cu politici de servicii diferenţiate

Când creaţi politica de servicii diferenţiate, vrăjitorul vă permite să setaţi informaţiile de date server, aşa cum s-a discutat în secţiunea “Folosirea jetonului aplicaţie cu politici de servicii diferenţiate.”. Chiar dacă acele câmpuri din vrăjitor vă promptează pentru un jeton 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 de ieşire, selectaţi în vrăjitor **Toate jetoanele**. Puteţi potrivi un set URI specific în politica externă, dacă vreţi.

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 URL-uri, trebuie să vă asiguraţi că portul de aplicaţie asignat pentru URI se potriveşte cu directiva Listen activată pentru Fast Response Cache Accelerator (FRCA) în configuraţia serverului de Web Apache. Pentru a schimba sau vizualiza portul pentru serverul dumneavoastră HTTP , consultaţi Gestionare adrese şi porturi pentru serverul dumneavoastră HTTP (motorizat de Apache).

FRCA va identifica URI-ul pentru fiecare răspuns HTTP de ieşire. 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 URI-ului 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 este clasificat traficul, serviciile diferenţiate solicită, de asemenea, un comportament per-hop (PHB) pentru a defini modul în care să manipuleze traficul.

Serverul utilizează biţi în antetul IP pentru a identifica nivelul serviciului 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. Tipul serviciu câmp de octeţi a fost redefinit în sistemele de operare V5R1, în Cererea de comentarii (Request for Comments - RFC) 1349 OS/400 Un comportament per-hop este comportamentul de expediere pe care îl primeşte un pachet la un nod de reţea. Se reprezintă printr-o valoare cunoscută ca *punct de cod*. Pachetele pot fi marcate fie la server fie la alte părţi alte reţelei, cum ar fi un ruter. Pentru ca un pachet să reţină serviciul solicitat, fiecare nod de reţea trebuie să fie conştient de serviciile diferenţiate (DiffServ). 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 de ieşire. Citiţi pagina “Condiţionări de trafic” pentru informaţii suplimentare despre ce înseamnă să recunoască Diffserv.

Dacă pachetul dumneavoastră trece printr-un ruter sau switch care nu recunoaşte DiffServ, va pierde nivelurile sale de serviciu în acel ruter. Pachetul este încă manipulat, dar poate experimenta o întârziere neaşteptată. Pe serverul dumneavoastră iSeries puteţi folosi puncte de cod per-hop predefinite sau puteţi defini propriul dumneavoastră punct de cod. Nu este recomandat să vă creaţi propriile puncte de cod pentru a fi folosite în afara reţelei dumneavoastră private. Dacă nu ştiţi ce puncte de cod să alocaţi, revedeţi subiectul “Folosirea punctelor de cod pentru alocarea unui 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.

Serviciile diferenţiate pot fi folosite, de asemenea, pentru a încetini traficul ce părăseşte un server. Aceasta înseamnă că serverul dumneavoastră iSeries foloseşte într-adevăr serviciile 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 servicii pentru această politică, sunteţi întrebat să setaţi diverse limite pe serverul dumneavoastră. Limitele de performanţă sunt includ dimensiunea găleată a jetonului, limita ratei de vârf şi limita ratei medii. Subiectele de ajutor din funcţia QoS a Navigatorului iSeries vă dă mai multe informaţii specifice 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.

În cazul în care echipamentele de reţea au toate condiţionările de trafic, sunt considerate *capabile-DiffServ*.

Notă: Aceste cerinţe de hardware nu sunt specifice pentru iSeries. Nu veţi întâlni aceşti termeni în interfaţa QoS pentru că serverul 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 recomandat de asemenea să cercetaţi concepte QoS generale şi cerinţe preliminare înainte de a implementa politicile.

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

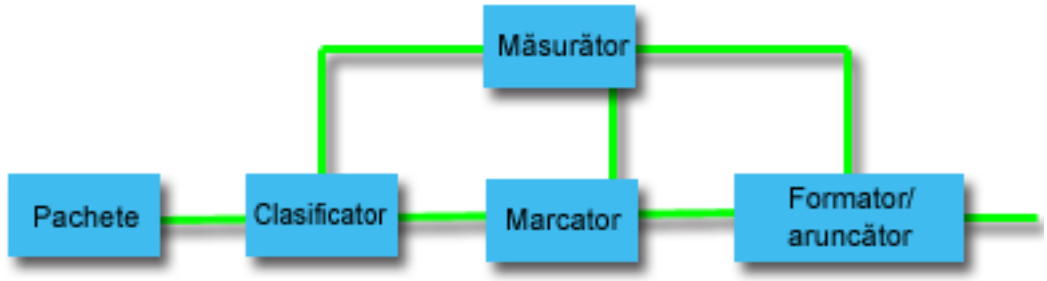


Figura 1. Condiţionări de trafic

Următoarele informaţii descriu fiecare condiţionare de trafic mai amănunţit.

Clasificatori

Clasificatorii de pachet selectează pachete într-un şir de trafic, bazându-se pe conţinutul din antetul lor IP. Serverul iSeries defineşte două tipuri de clasificatori. Colecţia comportamentală clasifică pachete bazându-se exclusiv pe punctul de cod de servicii diferenţiate. Clasificatorul MF (multi-field) selectează pachete, pe baza

valorii unei combinaţii de unul sau mai multe câmpuri antet, cum ar fi adresa sursă, adresa destinaţie, câmpurile de serviciu diferenţiat, ID-ul de protocol, portul sursă, URI, tipul server şi numerele de 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 sunt determinate 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 pachete setează câmpul de servicii diferenţiate (DS). Marcatorul poate fi configurat să marcheze toate pachetele la un singur punct de cod sau la un set de puncte de cod folosite la selectarea unui 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 lăţime de bandă de ieşire pe care o 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 servicii integrate folosesc protocolul RSVP şi API-ul RAPI (sau API-ul socket qtoq) pentru a garanta o conexiune capăt-la-capăt. Acesta este cel mai înalt nivel de serviciu pe care îl puteţi desemna; totuşi, este şi cel mai complex.

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 admisie. Cererea de lăţime de bandă vine într-o rezervare de la client. Dacă toate ruterele din cale sunt de acord cu cererile venind de la client, cererea ajunge la server şi la politica IntServ. 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 este efectuată folosind protocolul RSVP şi API-ul RAPI sau protocolul RSVP şi API-urile de socket-uri QoS qtoq.

Fiecare nod pe care traficul îl parcurge trebuie să poată folosi protocolul RSVP. Ruterele oferă calitate a serviciilor de-a lungul următoarelor funcţii de control de trafic : planificator pachet, clasificator pachet şi control al admisiei. 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.

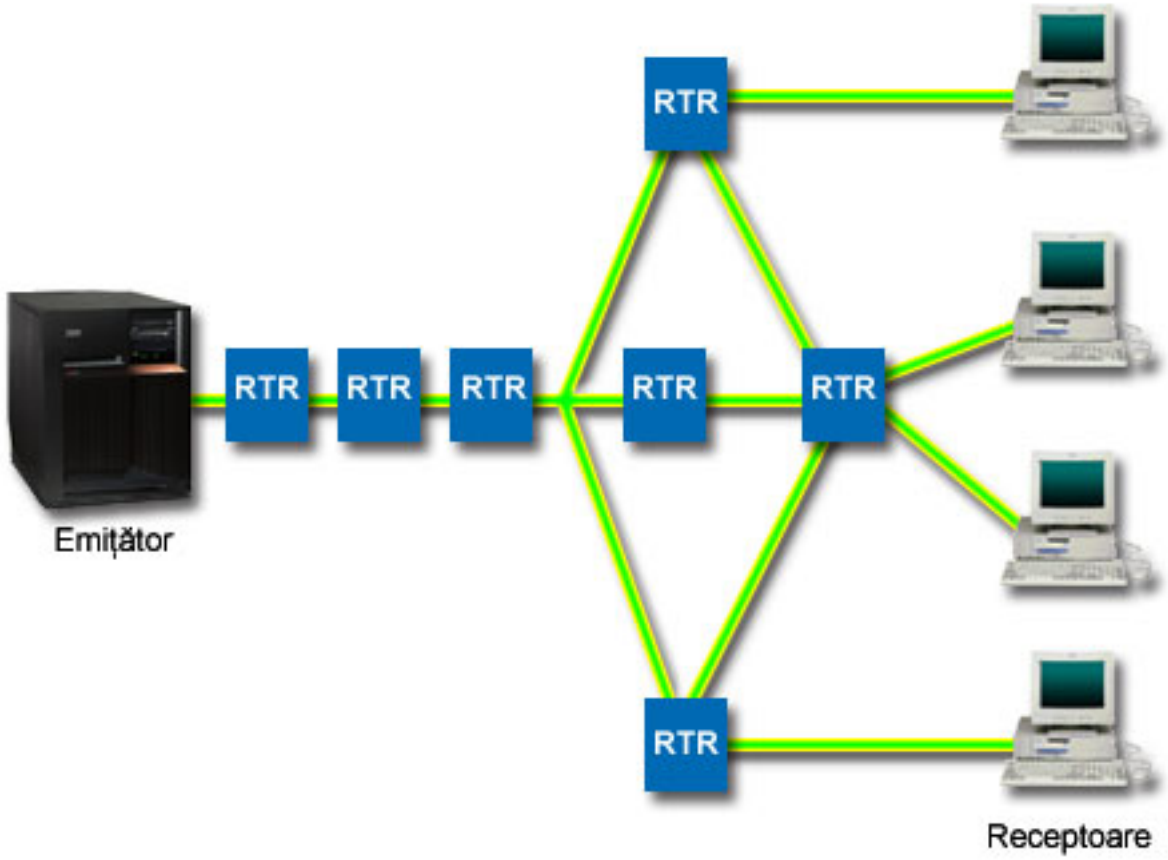


Figura 2. Calea RSVP dintre client şi server.

Aplicaţia RSVP-activat pe server detectează o cerere de conexiune de la un client. Ca răspuns, aplicaţia serverului lansează o comandă PATH la client. Această comandă este lansată folosind API-uri RAPI sau API-uri socket QoS qtoq şi conţine informaţii de adrese IP ale ruterelor. O comandă PATH conţine informaţii despre resursele disponibile pe server şi ruterele din cale, precum şi informaţii de rută între server şi client. Aplicaţia RSVP-activată pe client trimite apoi o comandă RESV înapoi pe calea reţelei 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.

Serviciile integrate nu înseamnă un termen prescurtat pentru conexiuni RSVP, cum este 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 serviciilor. Aplicaţiile folosite într-o politică de servicii integrate trebuie să fie capabile să folosească protocolul RSVP. Momentan, serverul nu are aplicaţii RSVP-activate, deci va trebui să scrieţi aplicaţia care să folosească RSVP.

PE măsură ce pachetele sosesc şi încearcă să părăsească reţeaua dumneavoastră, serverul dumneavoastră determină dacă are resursele necesare pentru a trimite pachetul. Această acceptare este determinată de cantitatea de spaţiu din găleata jeton. Dumneavoastră setaţi manual numărul de biţi permişi în găleata jetonului şi limitele de lăţime de bană, limitele de rată a jetonului şi numărul maxim de conexiuni permise de server. Aceste valori sunt referite ca limite de

performanţă. Dacă pachetele rămân în limitele serverului, pachetele se conformează şi sunt trimise în afară. În serviciile integrate, fiecărei conexiuni îi este acordată propria găleată de jetoane.

Servicii integrate folosind marcaje de servicii diferenţiate

Dacă nu sunteţi sigur că întreaga reţea poate garanta conexiuni RSVP, puteţi totuşi crea o politică de servicii integrate. Totuşi, dacă resursele reţelei nu pot folosi protocolul RSVP, conexiunea nu poate fi garantată. În această situaţie, poate doriţi să aplicaţi un punct de cod politicii. Acest punct de cod este folosit uzual în politici de serviciu diferenţiat pentru a a o clasă de serviciu traficului. Deşi conexiunea nu este garantată, acest punct de cod va încerca să dea conexiunii prioritate.

Concepte înrudite

"API-uri QoS" la pagina 16
Puteţi citi acest subiect pentru a învăţa despre protocoale, API-uri şi cerinţe pentru un ruter care este activat pentru protocolul ReSerVation (RSVP). Actualul API QoS include API-ul RAPI, API-ul qtoq socket, API-ul sendmsg() şi API-ul monitor.

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

"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. Sunt două tipuri de politici de servicii integrate de creat: încărcare garantată şi controlată. În acest exemplu, este folosit serviciul garantat.

Funcţii de control al traficului

Funcţiile de control al traficului se aplică numai serviciilor integrate şi nu sunt specifice serverului iSeries.

Nu veţi întâlni aceşti termeni în interfaţa QoS pentru că serverul nu poate controla hardware extern. În afara unei reţele private, hardware-ul trebuie să aibă abilitatea de a trata cerinţe QoS generale. Cererile generale pentru ruter pentru politicile IntServ sunt discutate în secţiunea următoare. Este recomandat să cercetaţi concepte QoS generale şi cerinţe preliminare înainte de a implementa politicile.

Pentru a obţine rezultate previzibile, trebuie să aveţi hardware RSVP-activat de-a lungul căii traficului. Ruterele trebuie să aibă anumite funcţii de control al traficului pentru a folosi protocolul RSVP. Acesta este deseori referit ca fiind *RSVP-activat* sau *QoS-activat*. Amintiţi-vă că rolul serverului dumneavoastră este de client sau de server. Nu poate fi folosit în acest moment ca ruter. Verificaţi cu manualele dumneavoastră de echipament de reţea, pentru a controla dacă pot face faţă cererilor QoS.

Funcţiile de control al traficului pot include următoarele funcţii:

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

Clasificator pachet
Clasificatorul de pachet identifică care pachete dintr-un flux IP vor primi un anumit nivel de servicii bazat ,din nou, pe informaţiile de antet 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 furnizate în politica dumneavoastră.

Control admitere
Controlul de admitere conţine algoritmul de decizie pe care îl foloseşte un ruter pentru a determina dacă există destule resurse de rutare pentru a accepta QoS 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 QoS" la pagina 16
Puteţi citi acest subiect pentru a învăţa despre protocoale, API-uri şi cerinţe pentru un ruter care este activat pentru protocolul ReSerVation (RSVP). Actualul API QoS include API-ul RAPI, API-ul qtoq socket, API-ul sendmsg() şi API-ul monitor.

Referinţe înrudite

"Informaţii înrudite pentru QoS" la pagina 65
Listate mai jos sunt IBM Redbooks (în format PDF), site-uri Web şi subiectele Centrului de informare legate de subiectul QoS. Puteţi citi sau tipări oricare din PDF-uri.

Tipuri de servicii integrate

Există două tipuri de servicii integrate: încărcare controlată şi garantată.

Încărcare controlată

Serviciul de încărcare controlată suportă aplicaţii care sunt foarte sensibile la reţele congestionate, cum ar fi 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 va fi furnizat asemănător serviciului cu trafic normal într-o reţea sub condiţii uşoare.

Ruterele trebuie să se asigure că serviciul de încărcare controlat primeşte lăţime de bandă adecvată şi resurse de procesare de pachete. Pentru a face asta, ele trebuie să fie QoS-activate cu suport pentru Servicii integrate. Va trebui să verificaţi specificaţiile ruterelor pentru a vedea dacă oferă QoS printr-o funcţie de control a traficului. Controlul traficului constă din următoarele componente: planificator de pachet, clasificator de pachet şi control de admisie.

Serviciu garantat

Serviciul garantat asigură sosirea pachetelor într-un interval de timp stabilit. Aplicaţiile care necesită serviciu garantat includ sisteme de difuzare video şi audio care folosesc tehnologii de înşirare. Serviciul garantat controlează întârzierea maximă a cozii, astfel că pachetele nu vor fi întârziate peste o anumită durată de timp. Fiecare ruter de-a lungul căii pachetului furnizează capacităţi RSVP pentru a asigura livrarea. Când alocaţi limite de găleată jeton şi limite de lăţime de bandă, definiţi serviciul dumneavoastră garantat. Serviciul garantat poate fi aplicat numai aplicaţiilor folosind protocolul 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. Sunt două tipuri de politici de servicii integrate de creat: 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 garantarea livrării pachetelor în politici de lăţime de bandă de ieşire, atât servicii integrate cât şi diferenţiate.

Dimensiune găleată jeton

Dimensiunea găleţii jeton determină cantitatea de informaţie pe care o poate procesa serverul dumneavoastră la orice moment cerut. Dacă o aplicaţie trimite informaţii serverului dumneavoastră mai repede decât serverul 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 limitare, ceea ce vă va permite o cerere de conexiune RSVP. 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 specifică rata datei pe termen lung sau numărul de biţi pe secundă permişi într-o reţea. Politica QoS se uită la lăţimea de bandă cerută şi o compară cu limitele de rată şi de flux pentru această politică. Dacă cererea determină serverul să-şi depăşească limitele, serverul refuză cererea. Limita ratei de jeton este folosită doar pentru control de admisie în politici de servicii integrate. Această valoare poate varia între 10 Kbps şi 1 Gbps. Puteţi se asemenea seta aceasta la nu limita. 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 de rată jeton adunată destul de mare să colecteze majoritatea traficului de date din 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 lăţime de bandă de ieşire pe care o puteţi crea pe server. Serviciile diferenţiate împart traficul dumneavoastră pe clase. Pentru a avea grijă de politicile de servicii diferenţiate, trebuie să determinaţi cum doriţi să vă clasificaţi traficul din reţea şi cum manipulaţi clasele diferite.

“Scenariu: Monitorizarea statisticilor curente de reţea” la pagina 45
În vrăjitori sunteţi rugat să setaţi limite de performanţă. Acestea sunt valori care nu pot fi recomandate, deoarece sunt bazate pe cerinţe de reţea individuale.

Servicii integrate folosind marcaje de servicii diferenţiate

Folosire marcaje de servicii diferenţiate într-o politică de servicii integrate pentru a menţine prioritatea pachetelor trimise într-un mediu amestecat.

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, înţelegeri de nivel de servicii şi capacităţi de echipamente, s-ar putea să nu primiţi mereu serviciul pe care îl doriţi.

Pentru a ajuta la rezolvarea acestei potenţiale probleme, puteţi ataşa un marcaj de serviciu diferenţiat la politica de servicii integrate. În eventualitatea în care o politică traversează un ruter care nu poate folosi protocolul RSVP, politica dumneavoastră va mai menţine ceva prioritate. Marcajul pe care îl adăugaţi este numit un comportament per-hop.

Fără semnalizare

În plus faţă de folosirea marcajelor, după cum este descris mai sus, puteţi folosi de asemenea funcţia *fără semnalizare*. Atunci când este selectată, versiunea ″fără semnalizare″ a API-urilor vă va permite să scrieţi o aplicaţie care face ca o regulă RSVP să fie încărcată pe server şi cere doar ca partea aplicaţiei corespunzătoare serverului 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 admitere intrare, realizaţi următorii paşi:

1. În Navigatorul iSeries, expandaţi serverul dumneavoastră → **Reţea → Politici IP**.
2. Faceţi clic dreapta **Calitatea serviciului** şi selectaţi **Configurare**.
3. Expandaţi **Politici lăţime de bandă de ieşire → IntServ**.

4. Faceţi clic dreapta pe numele politicii IntServ corespunzătoare 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 servicii diferenţiate sau o politică de admitere intrare, creaţi, de asemenea şi folosiţi o clasă de serviciu.

“Servicii integrate” la pagina 6
Al doilea tip de politică de lăţime de bandă de ieşire pe care o 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 admitere intrare

Politica de admitere intrare este folosită pentru a controla cererile de conexiune care vin în reţeaua dumneavoastră.

Politica de intrare este folosită pentru a restricţiona traficul care încearcă să se conecteze la serverul dumneavoastră. Pe serverul iSeries, puteţi restricţiona accesul după client, URI, aplicaţie sau interfaţă locală. În plus, puteţi îmbunătăţi performanţa serverului prin aplicarea unei clase a serviciului traficului de intrare. Definiţi această politică prin vrăjitorul de admitere intrare din Navigatorul iSeries.

Există trei componente ale unei politici de intrare care necesită informaţii suplimentare. Acestea includ URI pentru restricţionarea traficului, rate de conexiune 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 de intrare pentru a restricţiona traficul HTTP care se conectează la serverul dumneavoastră Web. În aceste circumstanţe puteţi crea o politică de admitere intrare 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 URI-urilor specifice va aplica control al intrărilor pe baza informaţiilor la nivel de aplicaţie, pentru a limita cererile URI acceptate de server. În industrie este referit ca şi *control cerere de conexiune bazată pe antet*, care foloseşte URI-uri pentru a seta priorităţi.

Specificarea unui URI permite politicii de intrare să examineze conţinutul, nu doar antetul pachetelor. Conţinutul examinat este un nume URI. Pentru iSeries, puteţi folosi numele URI relative (de exemplu, **/produse/haine**). Exemplele de mai jos descriu URI-ul înrudit.

URI înrudit

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

Note:

1. 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.

2. Există un caracter de înlocuire implicit atunci când specificaţi un URI. De exemplu, /software va include orice se află în directorul software.
3. Nu folosiţi un * în URI. Acesta nu este un caracter valid.
4. Informaţiile URI pot fi folosite la politicile de intrare sau de serviciu diferenţiat (politici de ieşire).

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 schimba sau vizualiza portul pentru serverul dumneavoastră HTTP, consultaţi Gestionare adrese şi porturi pentru serverul dumneavoastră HTTP (motorizat de Apache).

Rată de conexiune

Ca parte a politicii de admitere intrare, trebuie să selectaţi o clasă a serviciului. Această clasă a serviciului defineşte ratele de conexiune care funcţionează drept control al admisiei pentru a limita conexiunile acceptate de server.

Rata de conexiune limitează acceptarea sau respingerea unui pachet nou pe baza numărului mediu de conexiuni pe secundă şi a numărului maxim de conexiuni instantanee definite în politica pe care o creaţi. Aceste limitări de conexiuni constau din rata medie şi limita în rafală , pe care vrăjitorii din Navigatorul iSeries vă vor cere să le introduceţi. Atunci când o cerere de conexiune de intrare ajunge la server, acesta analizează informaţiile din antetul pachetului pentru a determina dacă traficul 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 admitere intrare. În Navigatorul iSeries, puteţi să folosiţi de asemenea ajutorul asociat pentru a vă referi la informaţii similare pe măsură ce completaţi politica.

Cozi de prioritate cu pondere

Ca parte al controlului traficului de intrare, puteţi specifica prioritatea în care sunt tratate cererile de conexiune după ce au fost evaluate ce politici. Prin asignarea unui ponderi la o coadă de prioritate, controlaţi timpul de răspuns al cozii după sosirea unei conexiuni. Dacă se află în coadă, conexiunea ca fi tratată în ordinea priorităţii cozii (high, medium, low sau best effort). 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 se specifică 25 pentru toate priorităţile, atunci toate cozile sunt tratate egal. Să presupunem că specificaţi următoarele ponderi: High (50), Medium (30), Low (15) şi Best effort (5). Conexiunile acceptate includ:

- 50% conexiuni de prioritate high
- 30 % conexiuni de prioritate medium
- 15% conexiuni de prioritate low
- 5% conexiuni de prioritate best effort

Concepte înrudite

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

“Rata medie de conexiune şi limite în rafală” la pagina 15
Ratele de conexiune şi limite în rafală sunt cunoscute împreună ca *limite de rată*. Aceste limite de rate restricţionează conexiunile de intrare încercând să între în server. Limitele de rate sunt un set de clase de serviciu folosite cu politici de admitere intrare.

Clasa serviciului

Când creaţi o politică servicii diferenţiate sau o politică de admitere intrare, creaţi, de asemenea şi folosiţi o clasă de serviciu.

Politicile de servicii diferenţiate şi politicile de admitere trafic de intrare folosesc o clasă de serviciu 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.

În timp ce realizaţi QoS, mai întâi veţi defini 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 de intrare, de ieşire sau ambelor. Dacă selectaţi ambele (de intrare şi de ieşire), atunci o politică de serviciu diferenţiat şi o politică de admitere intrare 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
: Calitatea serviciului (Quality of service - QoS) foloseşte următoarele puncte de cod pentru a aloca comportamente per-hop traficului. Ruterele şi switch-urile folosesc aceste puncte de cod pentru a da traficului niveluri de prioritate. Serverul dumneavoastră nu poate folosi aceste puncte de cod din moment ce 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. Cel mai important lucru este să fiţi consecvent cu marcajele astfel încât să obţineţi rezultatele aşteptate. Aceste puncte de cod vor fi o parte 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. Atunci când alocaţi limitele de control de mai sus, setaţi valori pentru a restricţiona traficul. Când traficul depăşeşte aceste restricţii, pachetele sunt considerate în-afara-profilului. Informaţiile din clasa serviciului spun serverului dacă să renunţe la traficul UDP şi să reducă fereastra de congestionare TCP, să remodeleze sau să marcheze pachetele din afara profilului.

  Renunţarea la pachetele UDP şi reducerea ferestrei de congestionare TCP: Dacă decideţi să renunţaţi sau să ajustaţi pachetele din afara profilului, pachetele UDP sunt abandonate. Totuşi, fereastra de congestionare TCP este redusă astfel încât rata de transfer a datelor este conformă cu rata găleţii jeton. Numărul de pachete care pot fi trimise în reţea la orice moment dat de timp scade şi rezultatul este că se reduce congestia.

  Întârziere (modelare): Dacă întârziaţi pachetele în-afara-profilului, acestea sunt modificate pentru a se conforma cu caracteristicile de tratare definite de dumneavoastră.

  Re-marcare cu punct de cod DiffServ: În cazul în care remarcaţi pachetele în-afara-profilului cu un punct de cod, le sunt reasignate un alt punct de cod. Pachetele nu sunt modificate pentru a se conforma caracteristicilor dumneavoastră de tratare, ci doar remarcate. Când alocaţi aceste instrucţiuni de tratare în vrăjitor, apăsaţi Ajutor pentru mai multe informaţii.

Prioritate
: Puteţi da priorităţi conexiunilor făcute la serverul dumneavoastră prin politici de control admitere ale traficului de intrare. Aceasta vă permite să definiţi ordinea în care conexiunile terminate sunt tratate de server. Puteţi alege priorităţi înalte, medii, joase sau cel mai bun efort.

Concepte înrudite

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

“Politici de admitere intrare” la pagina 11
Politica de admitere intrare este folosită pentru a controla cererile de conexiune care vin în reţeaua dumneavoastră.

“Servicii diferenţiate” la pagina 2
Acesta este primul tip de politică de lăţime de bandă de ieşire pe care o puteţi crea pe server. Serviciile diferenţiate împart traficul dumneavoastră pe clase. Pentru a avea grijă de politicile de servicii diferenţiate, trebuie să determinaţi cum doriţi să vă clasificaţi traficul din reţea şi cum manipulaţi clasele diferite.

Referinţe înrudite

“Folosirea punctelor de cod pentru alocarea unui comportament per hop”
Calitatea serviciului (QoS - Quality of service) foloseşte următoarele puncte de cod pentru a aloca comportamente per-hop traficului.

Folosirea punctelor de cod pentru alocarea unui comportament per hop

Calitatea serviciului (QoS - Quality of service) foloseşte următoarele puncte de cod pentru a aloca comportamente per-hop traficului.

În vrăjitorul Clasa de serviciu, va trebui să alocaţi un comportament per-hop politicii dumneavoastră. Trebuie să determinaţi care puncte de cod se vor folosi pentru nevoile individuale ale reţelei dumneavoastră. 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.

Tabelul de mai jos afişează punctele de cod recomandate, ce se bazează pe standardele 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 serviciilor. 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 nivelurile de serviciu cu ISP-ul dumneavoastră, care este posibil să micşoreze costurile de serviciu pentru 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

Trimiterea expeditivă este unul din tipurile 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 recomandate: Trimitere expeditivă

Trimitere expeditivă
101110

Notă: Există un cost tipic mare asociat cu comportamentul de trimitere expeditivă, aşa că nu se recomandă să utilizaţi acest comportament per-hop în mod obişnuit.

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 recomandate: Trimitere expeditivă

Selector de clasă
Clasa 0 - 000000
Clasa 1 - 001000
Clasa 2 - 010000
Clasa 3 - 011000
Clasa 4 - 100000
Clasa 5 - 101000
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, Înaltă dă politicii cea mai mică prioritate şi Clasa 4, joasă 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 recomandate: Trimitere expeditivă

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 lăţime de bandă de ieşire pe care o puteţi crea pe server. Serviciile diferenţiate împart traficul dumneavoastră pe clase. Pentru a avea grijă de politicile de servicii diferenţiate, trebuie să determinaţi cum doriţi să vă clasificaţi traficul din reţea şi cum manipulaţi clasele diferite.

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

Rata medie de conexiune şi limite în rafală

Ratele de conexiune şi limite în rafală sunt cunoscute împreună ca *limite de rată*. Aceste limite de rate restricţionează conexiunile de intrare încercând să între în server. Limitele de rate sunt un set de clase de serviciu folosite cu politici de admitere intrare.

Rată în rafală a conexiunii

Dimensiunea ratei în rafală determină capacitatea bufferului, care reţine rafalele conexiunii. Rafalele de conexiune pot intra în server la o rată mai mare decât acesta le poate manipula sau pe care aţi dori să o permiteţi. Dacă numărul de conexiuni într-o rafală depăşeşte rata de rafală a conexiunii pe care aţi setat-o, atunci conexiunile suplimentare sunt ignorate.

Rată de conexiune medie

Rata de conexiune medie specifică limita de conexiuni nou stabilite sau rata de cereri URI acceptate permise într-un server. Dacă o cerere face ca serverul să depăşească limitele pe care le-aţi setat, atunci serverul nu permite conexiunea. Limita cererii de conexiune medie este măsurată în conexiuni pe secundă.

Indiciu: Pentru a determina ce limite sunt setate, aţi putea dori să rulaţi monitorizarea. Scenariul despre monitorizarea statisticilor de reţea curente conţin un exemplu de politică care vă va ajuta să colectaţi majoritatea datelor care trec prin serverul dumneavoastră. Folosind aceste rezultate, puteţi regla corespunzător limitele.

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

Concepte înrudite

“Politici de admitere intrare” la pagina 11
Politica de admitere intrare este folosită pentru a controla cererile de conexiune care vin în reţeaua dumneavoastră.

“Scenariu: Monitorizarea statisticilor curente de reţea” la pagina 45
În vrăjitori sunteţi rugat să setaţi limite de performanţă. Acestea sunt valori care nu pot fi recomandate, deoarece sunt bazate pe cerinţe de reţea individuale.

API-uri QoS

Puteţi citi acest subiect pentru a învăţa despre protocoale, API-uri şi cerinţe pentru un ruter care este activat pentru protocolul ReSerVation (RSVP). Actualul API QoS include API-ul RAPI, API-ul qtoq socket, API-ul sendmsg() şi API-ul 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 pentru a folosi monitorul QoS.

- “ API-uri servicii integrate ”
- “ API-uri servicii diferenţiate ” la pagina 17
- “API-ul monitor” la pagina 18

API-uri servicii integrate

Protocolul de rezervare a resurselor (RSVP) împreună cu API-urile RAPI sau API-urile socket 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 aceste politici de servicii integrate este de multe ori referit ca fiind *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. Menţine rezervarea atât timp cât să serviciile cerute de politicile dumneavoastră. Rezervarea defineşte tratarea şi lăţimea de bandă pe care le vor necesita datele din această conversaţie. Fiecare nod de reţea este de acord să furnizeze tratarea de date definită în rezervare.

RSVP este un protocol simplu în care rezervările 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 serverul iSeries nu are în prezent nici o aplicaţie RSVP-activată, va trebui să scrieţi aplicaţiile folosind API-ul RAPI sau API-urile pentru socket-uri QoS qtoq. Asta va permite aplicaţiilor să folosească protocolul RSVP. Dacă doriţi o explicaţie în profunzime, există mai multe surse care explică aceste modele, operaţiile lor şi tratarea mesajului. Trebuie să înţelegeţi în ansamblu protocolul RSVP şi conţinutul RFC 2205.

API-urile socket-uri qtoq

Puteţi acum folosi API-urile socket QoS pentru a simplifica lucrul necesar folosirii protocolului RSVP pe sistemul iSeries. API-urile socket qtoq apelează API-urile RAPI şi realizează unele dintre cele mai dificile operaţii. API-urile socket 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 va încărca o regulă RSVP pe server.
- 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 pagina Fluxul funcţional orientat pe conexiune API QoS sau pagina Flux funcţional fără conexiune API QoS pentru fluxul tipic API QoS pentru o aplicaţie/protocol folosind socket-uri QoS qtoq orientat pe conexiune sau fără conexiune.

API-uri servicii diferenţiate

Notă: API-ul sendmsg() este folosită pentru anumite politici de servicii diferenţiate care definesc un jeton particular aplicaţie. Când creaţi o politică servicii diferenţiate, puteţi furniza (opţional) caracteristici de aplicaţie (jeton şi prioritate). Aceasta este o definiţie de politică avansată şi, dacă nu este folosită, acest API poate fi ignorat. Oricum, amintiţi-vă că ruterele şi alte servere din reţea au încă nevoie să fie conştiente de servicii diferenţiate.

Când vă hotărâţi să folosiţi un jeton aplicaţie, aplicaţia ce furnizează această informaţie trebuie să fie codificată propriu pentru a folosi API sendmsg(). Aceasta se realizează de către programatorul aplicaţiei. Documentaţia aplicaţiei trebuie să furnizeze valori valide (jeton şi prioritate), pe care le va utiliza administratorul QoS în politica de servicii diferenţiate. Politica de servicii diferenţiate aplică atunci prioritatea ei proprie şi clasificarea sa traficului, ce se potriveşte jetonului setat în politică. Dacă aplicaţia nu are valori care se potrivesc valorilor setate în politică, se va modifica aplicaţia sau va trebui să folosiţi parametrii diferiţi de date aplicaţie pentru politica de servicii diferenţiate.

Următoarele informaţii descriu pe scurt parametrii datelor din server: jetonul aplicaţie şi prioritatea aplicaţie.

Ce este un jeton aplicaţie?

Un *jeton aplicaţie* este un URI care reprezintă o resursă definită. Jetonul pe care îl specificaţi în politica QoS este comparat cu jetonul furnizat de aplicaţia de ieşire. Aplicaţia furnizează valoarea jetonului prin API 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 de ieşire. Aplicaţia furnizează valoarea priorităţii folosind API 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.

Pentru informaţii detaliate asupra tipului de politică DiffServ, consultaţi “Servicii diferenţiate” la pagina 2.

API-ul monitor

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

- QgyOpenListQoSMonitorData (Open List of QoS Monitor Data) strânge informaţii referitoare la servicii QoS.
- QtoqDeleteQoSMonitorData (Delete QoS Monitor Data) şterge unul sau mai multe seturi de date monitor QoS colectate.
- QtoqEndQoSMonitor (End QoS Monitor) opreşte strângerea informaţiilor de la serviciile QoS.
- QtoqListSavedQoSMonitorData (List Saved QoS Monitor Data) returnează o listă de date monitor colectate, care a fost salvată anterior.
- QtoqSaveQoSMonitorData (Save QoS Monitor Data) salvează o copie a datelor monitor QoS colectate pentru viitoarea folosire.
- QtoqStartQoSMonitor (Start QoS Monitor) strânge servicii înrudite cu serviciile QoS.

Concepte înrudite

“Servicii integrate” la pagina 6
Al doilea tip de politică de lăţime de bandă de ieşire pe care o 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 numai serviciilor integrate şi nu sunt specifice serverului iSeries.

“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-ul RAPI

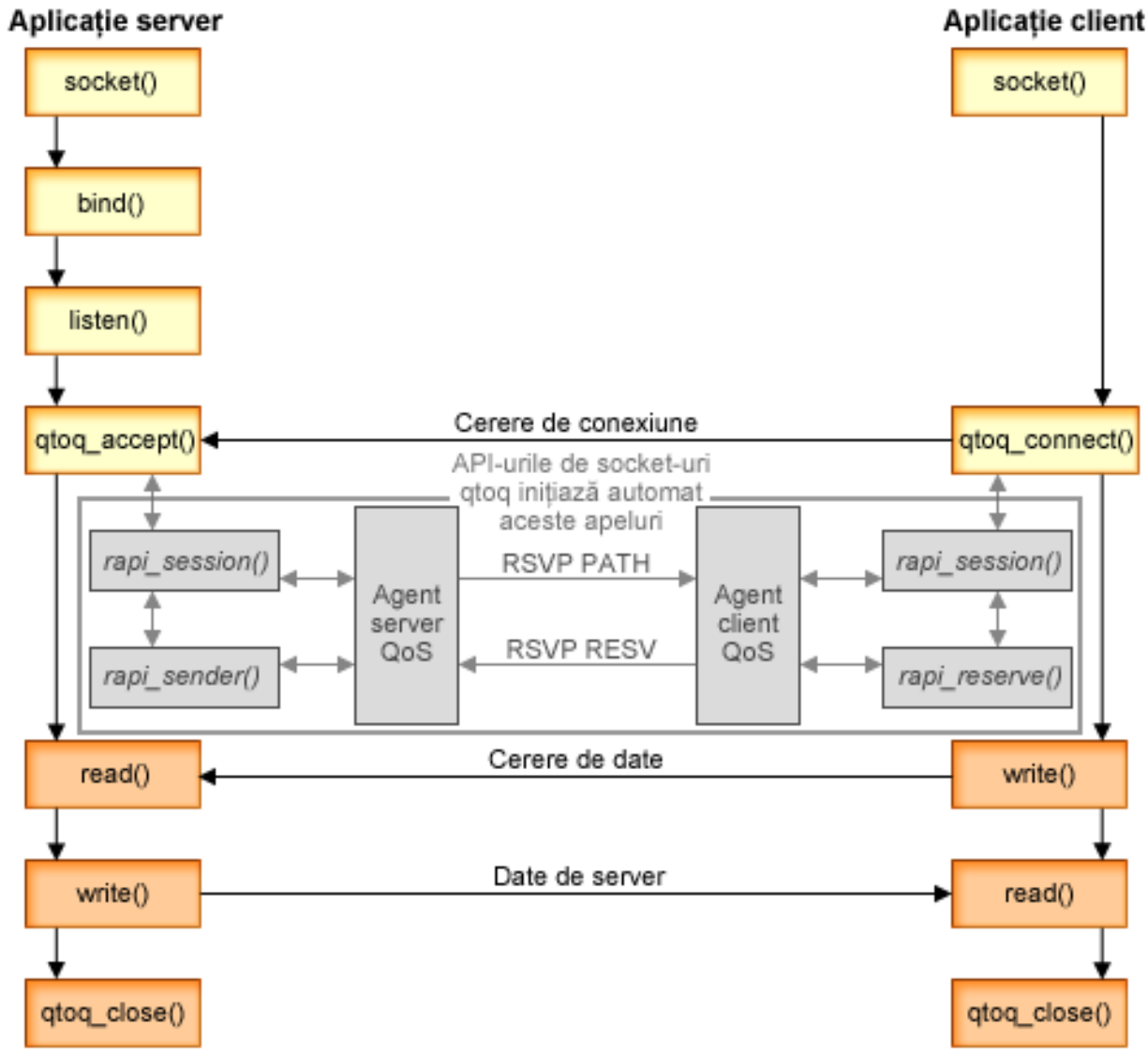
“Configurarea QoS cu vrăjitori” la pagina 50
Pentru a configura politicile QoS, trebuie să folosiţi vrăjitorii QoS din Navigatorul iSeries.

Flux funcţional orientat pe conexiune API QoS

Exemplele server şi client din acest subiect ilustrează calitatea socket-urilor API qtoq QoS scrise pentru un flux funcţional orientat pe conexiune.

Următoarea figură ilustrează relaţia client/server a funcţiilor socket-uri qtoq activate pentru API-urile QoS pentru un protocol orientat pe conexiune precum TCP (Transmission Control Protocol).

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 cauzează agenţii QoS pe client şi server să seteze protocolul RSVP pentru fluxul de date între client şi server.



flux qtoq de evenimente: Următoarea secvenţă de apelări de socket furnizează o descriere a graficului. 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 primi un descriptor de socket.
2. Aplicaţia apelează listen() pentru a specifica ce conexiuni va aştepta.
3. Aplicaţia apelează qtoq_accept() pentru a aştepta o cerere de conexiune de la client.
4. API-ul apelează rapi_session() şi dacă este cu succes, va fi alocat un ID de sesiune QoS.
5. API-ul apelează funcţia standard accept() pentru a aştepta cererea de conexiune a unui client.
6. Când este primită cererea de conexiune, este realizat controlul admisiei pe regula cerută. Regula este trimisă la stiva TCP/IP, iar dacă este validă, se întoarce la aplicaţia apelantă cu rezultatele şi sesiunea ID.
7. Aplicaţiile pentru server şi client realizează transferurile cerute de date.
8. Aplicaţia va apela funcţia qtoq_close() pentru a închide socket-ul şi 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 primi un descriptor de socket.
2. Aplicaţia apelează listen() pentru a specifica ce conexiuni va aştepta.
3. Aplicaţia apelează qtoq_accept() pentru a aştepta o cerere de conexiune de la client.
4. Când soseşte o cerere de conexiune în rapi_session() API va fi apelat pentru a crea o sesiune cu serverul QoS pentru această conexiune şi va obţine ID-ul sesiune QoS care va fi întors la apelant.
5. API-ul rapi_sender() va fi apelat să iniţieze un mesaj PATH de la serverul QoS şi să informeze serverul QoS să se aştepte la un mesaj RESV de la client.
6. API-ul rapi_getfd() este apelat să primească descriptorul pe care aplicaţiile îl folosesc pentru a aştepta mesaje de eveniment QoS.
7. Descriptorul de acceptare şi descriptorul QoS sunt întorşi la aplicaţie.
8. Serverul QoS aşteaptă mesajul RESV să fie primit. Când este primit mesajul va încărca regula potrivită cu gestionarul QoS şi va trimite un mesaj unei aplicaţii, dacă aplicaţia cere notificare la apelarea API-ului qtoq_accept().
9. Serverul QoS continuă să furnizeze reîmprospătări pentru sesiunea stabilită.
10. Aplicaţia apelează qtoq_close() când conexiunea s-a terminat.
11. Serverul QoS va şterge regula din managerul 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 primi un descriptor de socket.
2. Această aplicaţie apelează funcţia qtoq_connect() pentru a informa aplicaţia server că doreşte să facă conexiunea.
3. Funcţia qtoq_connect() apelează API-ul rapi_session() pentru a crea o sesiune cu server 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 să primească descriptorul QoS pe care aplicaţiile îl folosesc pentru a aştepta mesaje QoS.
6. Este apelată funcţia connect(). Rezultatele connect() şi ale descriptorului QoS sunt întoarse la aplicaţie.
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 s-a terminat.
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

API qtoq_accept()

API qtoq_close()

API rapi_session()

API rapi_sender()

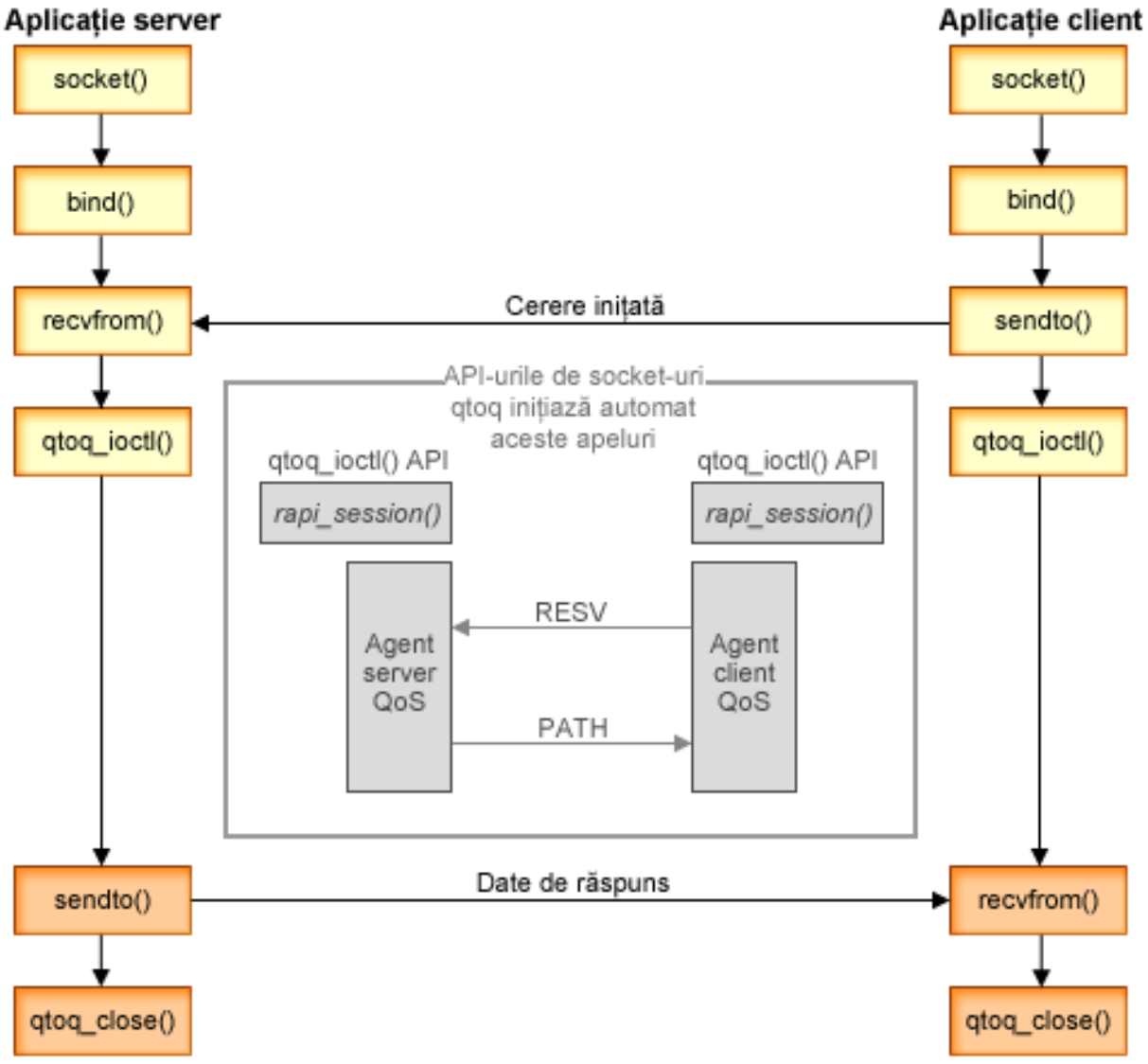
API rapi_getfd()

API qtoq_connect()

Flux funcţional fără conexiune API QoS

Exemplele server şi client din acest subiect ilustrează calitatea socket-urilor API qtoq QoS scrise pentru un flux funcţional orientat pe conexiune.

Când funcţiile API activate QoS sunt apelate pentru un flux fără conexiune care cere ca RSVP să fie iniţiat, sunt iniţiate funcţii în plus. Aceste funcţii cauzează agenţii QoS pe client şi server să seteze protocolul RSVP pentru fluxul de date între client şi server.



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

Parte a serverului

qtoq_ioctl() pentru o regulă marcată "Fără semnalizare"

1. Trimite un mesaj la serverul QoS cerându-i să realizeze control de admisie pe regula cerută.
2. Dacă regula este acceptată, apelează o funcţie care trimite un mesaj la serverul QoS cerând ca regula să fie încărcată.

3. Serverul QoS întoarce apoi starea la apelant indicând succesul sau eşuarea cererii.
4. Când aplicaţia a terminat folosirea conexiunii, apelează funcţia qtoq_close() pentru a închide conexiunea.
5. Serverul QoS va şterge regula din gestionarul QoS, sesiunea QoS şi va realiza orice altă acţiune este necesară.

qtoq_ioctl() cu semnalizare normală RSVP

1. Trimite un mesaj la serverul QoS cerându-i să realizeze control de admisie pe regula cerută.
2. Apelează rapi_session() pentru a cere setarea unei sesiuni pentru regulă şi pentru a face ca ID-ul sesiunii QoS să fie întors apelantului.
3. Apelează rapi_sender() pentru a iniţia un mesaj PATH înapoi la client.
4. Apelează apoi rapi_getfd() pentru a face descriptorul de fişiere să aştepte evenimente QoS.
5. Serverul QoS returnează select() de descriptor, ID-ul sesiunii QoS şi starea la apelant.
6. Serverul QoS încarcă regula când este primit mesajul RESV.
7. Aplicaţia apelează qtoq_close() când conexiunea este terminată.
8. Serverul QoS va şterge regula din gestionarul QoS, sesiunea QoS şi va realiza orice altă acţiune este necesară.

Partea clientului

qtoq_ioctl() cu semnalizare normală RSVP

1. qtoq_ioctl() apelează rapi_session() pentru a cere setarea unei conexiuni. Funcţia rapi_session() cere controlul admisiei 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. Apelează apoi rapi_getfd() pentru a face descriptorul de fişiere să aştepte evenimente QoS.
3. qtoq_ioctl() se întoarce la apelant cu aşteptarea pe descriptor şi pe sesiunea ID.
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. Aplicaţia apelează qtoq_close() când conexiunea este terminată.

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

API qtoq_close()

API rapi_session()

API rapi_sender()

API rapi_getfd()

API qtoq_ioctl()

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() permite date de clasificare QoS. 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 nivel de conexiune indică faptul că nivelul de servicii QoS obţinut prin clasificarea acestui mesaj va rămâne în efect pentru toate mesajele următoare trimise până la următoarea funcţie sendmsg() cu date QoS de clasificare. Domeniul de nivel mesaj indică faptul nivelul de serviciu QoS asignat va fi folosit doar pentru datele mesajului incluse în acest apel sendmsg(). Datele următoare trimise fără date de clasificare QoS vor moşteni asignarea anteriorului nivelul de conexiune QoS (de la ultima clasificare Nivel conexiune prin sendmsg() sau de la clasificarea originală a conexiunii TCP din 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. De asemenea, şirul specificat poate conţine litere mici şi mari şi va fi folosit în formatul exact specificat în scopul comparării.
    - 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 se comportă mai bine decât această opţiune pentru că datele specificate în politică sunt salvate în format ASCII în stiva TCP/IP, eliminând în acest fel nevoia de translatare a jetonului definit de aplicaţie la 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 cererea de prioritate de tip Expedited
    - IP_SET_QOSLEVEL_HIGH: Indică cererea de prioritate de tip High
    - IP_SET_QOSLEVEL_MEDIUM: Indică cererea de prioritate de tip Medium
    - IP_SET_QOSLEVEL_LOW: Indică cererea de prioritate de tip Low
    - IP_SET_QOSLEVEL_BEST_EFFORT: Indică cererea de prioritate de tip Best Effort
  - ip_qos_appl_token_len: lungimea ip_qos_appl_token.
  - ip_qos_appl_token: Acest ″câmp virtual″ urmează imediat după câmpul ip_qos_classification_type. Jetonul de clasificare al aplicaţiei în format ASCII sau EBCDIC în funcţie de IP_SET_QOSLEVEL_W_APPL_TOKEN_xxxx 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 lăţime de bandă de ieşire pe care o puteţi crea pe server. Serviciile diferenţiate împart traficul dumneavoastră pe clase. Pentru a avea grijă de politicile de servicii diferenţiate, trebuie să determinaţi cum doriţi să vă clasificaţi traficul din reţea şi cum manipulaţi clasele diferite.

"Clase prioritare: Cum să clasificaţi traficul de reţea" la pagina 3
Serviciul diferenţiat identifică traficul pe *clase*. Cele mai comune clase sunt definite utilizând adrese IP client, porturi de aplicaţie, tipuri de servere, protocoale, adrese locale IP şi planificări. Întreg traficul ce concordă aceleaşi clase este tratat la fel.

Referinţe înrudite

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

Server director

Puteţi alege să exportaţi politicile dumneavoastră unui server director. Vedeţi acest subiect pentru a afla avantajele utilizării sau neutilizării unui server director, a conceptelor şi configuraţiei LDAP, cât şi ale schemei QoS.

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

Avantajele folosirii unui server 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.

Avantajele salvării exclusiv pe serverul local

Salvarea politicilor QoS pe serverul local nu este aşa 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.
- Este mai uşor să se copieze o configuraţie între diferite sisteme iSeries. Puteţi copia fişierul de pe un sistem pe altul. Din moment ce nu există o maşină primară sau secundară, puteţi configura fiecare politică direct pe un anumit server.

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 interiorul funcţiei QoS din Navigatorul iSeries, puteţi configura un server director care este folosit cu politica dumneavoastră QoS.

Concepte înrudite

IBM Directory Server pentru iSeries (LDAP)

“Configurare server de directoare” la pagina 52
Configurările de politici QoS pot fi exportate la un server director LDAP.

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. Următoarele informaţii vor ajuta la explicarea conceptului de cuvânt cheie şi de ce aţi putea dori să folosiţi cuvinte cheie.

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 se află politicile dumneavoastră QoS este cunoscut ca sistemul primar.

Cuvintele cheie sunt folosite la identificarea configuraţiilor create de sisteme principale. Deşi create de sisteme principale, cuvintele cheie sunt de fapt spre beneficiul sistemelor secundare. Ele permit sistemelor secundare încărcarea şi utilizarea configuraţiilor create de un sistem principal. 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 create de un sistem principal. 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 directoare în Navigatorul iSeries, folosiţi ajutorul de task-uri QoS pentru anumite instrucţiuni.

Concepte înrudite

"Nume distinct"
Când doriţi să gestionaţi o parte a directorului dumneavoastră, vă referiţi la *Nume distinct* sau (dacă alegeţi) la un cuvânt cheie.

"Configurare server de directoare" la pagina 52
Configurările de politici QoS pot fi exportate la un server director LDAP.

Nume distinct

Când doriţi să gestionaţi o parte a directorului dumneavoastră, vă referiţi la *Nume distinct* 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:

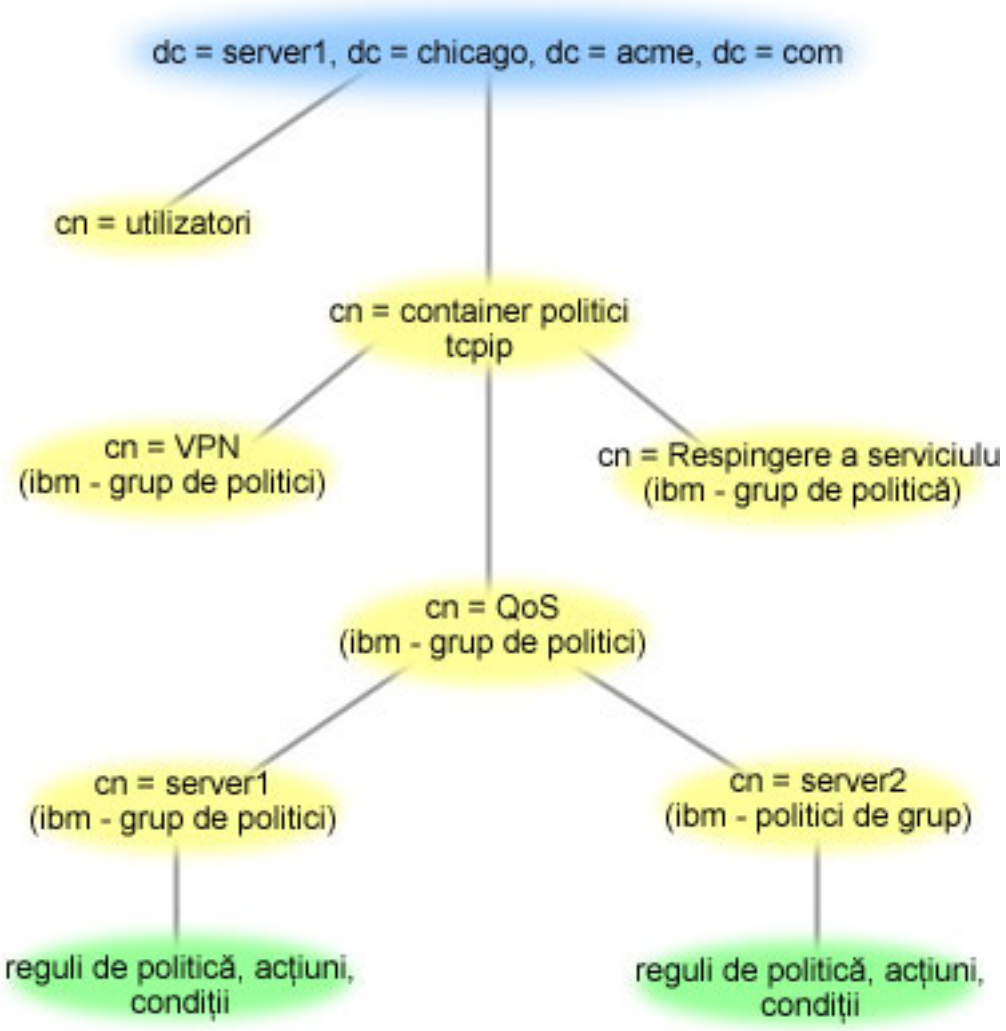


Figura 3. Exemplu de structură de directoare QoS

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 modificaţi serverul corespunzător în 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 directoare” la pagina 52
Configurările de politici QoS pot fi exportate la un server director LDAP.

Referinţe înrudite

"Informaţii înrudite pentru QoS" la pagina 65
Listate mai jos sunt IBM Redbooks (în format PDF), site-uri Web şi subiectele Centrului de informare legate de subiectul QoS. Puteţi citi sau tipări oricare din PDF-uri.

Scenarii

Aceste scenarii de politicii de QoS vă pot ajuta să înţelegeţi de ce şi cum să folosiţi QoS.

Una dintre cele mai bune căi de a învăţa despre calitatea serviciilor 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 pentru exemplificare.

Concepte înrudite

"Monitorizarea tranzacţiilor server" la pagina 62
Cu monitorizarea QoS puteţi să verificaţi că politicile QoS funcţionează aşa cum doriţi dumneavoastră ca ele să funcţioneze.

Referinţe înrudite

"Monitorizarea QoS" la pagina 55
Puteţi folosi monitorizarea la analizarea traficului IP prin server.

Scenariu: Limitarea traficului de browser

Puteţi utiliza calitatea serviciilor (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.

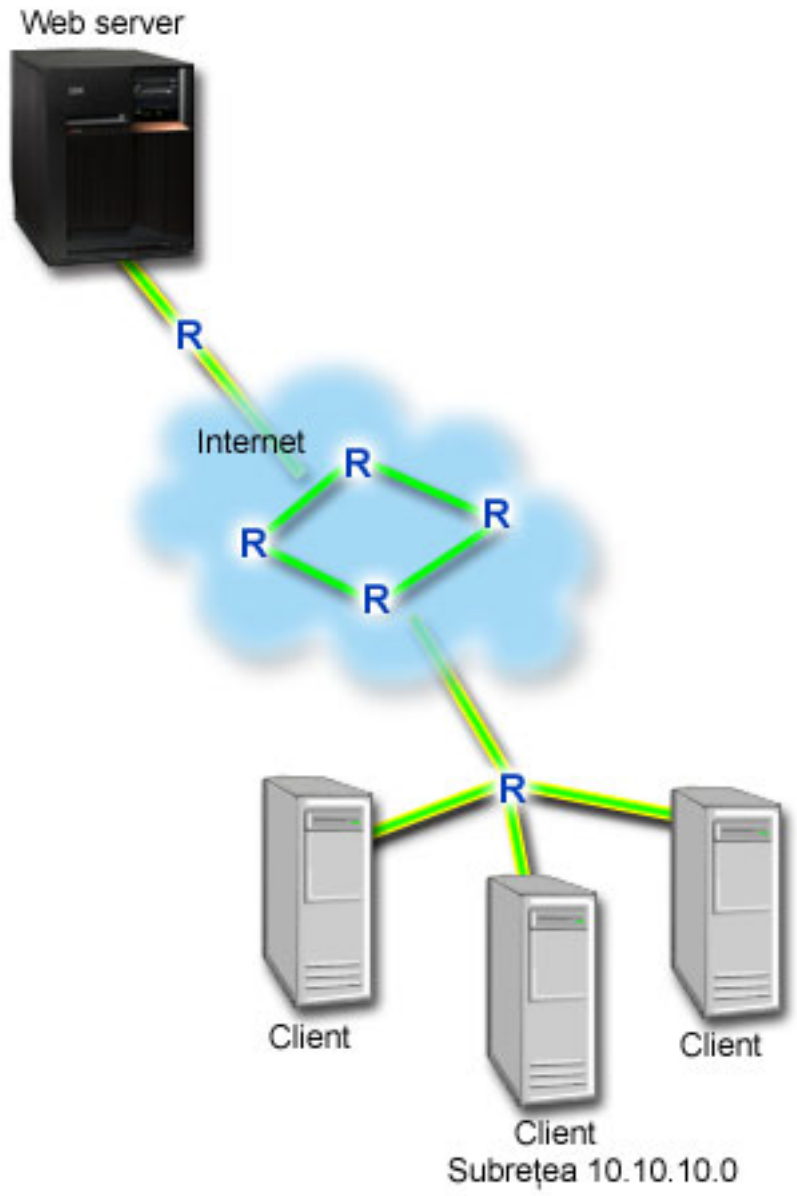


Figura 4. Serverul Web de limitare a traficului browser pentru un client

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 Acord de nivel serviciu (SLA - service-level agreement) cu ISP-ul dumneavoastră pentru a vă asigura că politicile primesc prioritatea cerută. Politica QoS pe care o creaţi pe serverul iSeries activează traficul (în politică) pentru a primi prioritate prin reţea. Politica QoS nu garantează aceasta şi este dependentă de SLA-ul dumneavoastră. De fapt, profitarea de politicile QoS vă poate da un mijloc de a negocia anumite niveluri şi rate de serviciu.
- Politicile de servicii diferenţiate cer rutere conştiente DiffServ de-a lungul căii de reţea. Majoritatea ruterelor recunosc DiffServ.

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
Această secţiune punctează unele din aspectele importante ale acordului SLA (service-level agreement), care pot afecta implementarea QoS.

"Servicii diferenţiate" la pagina 2
Acesta este primul tip de politică de lăţime de bandă de ieşire pe care o puteţi crea pe server. Serviciile diferenţiate împart traficul dumneavoastră pe clase. Pentru a avea grijă de politicile de servicii diferenţiate, trebuie să determinaţi cum doriţi să vă clasificaţi traficul din reţea şi cum manipulaţi clasele diferite.

Referinţe înrudite

"Monitorizarea QoS" la pagina 55
Puteţi folosi monitorizarea la analizarea traficului IP prin server.

Detaliile scenariului: Crearea politicii de servicii diferenţiate

1. În Navigator iSeries, expandaţi iSeries A → **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 faceţi clic pe OK, vă întoarceţi la vrăjitorul politică. Dacă aţi creat înainte clienţi, deselectaţi-i şi verificaţi dacă doar clienţii relevanţi sunt selectaţi.
8. Pe pagina Cerere de date server, verificaţi că **Orice jeton** şi **Toate prioritățile** 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. Apăsaţi **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. Apare vrăjitorul Noua clasă de serviciu.
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. Apăsaţi **Următorul**.
16. În pagina Tipul de serviciu, selectaţi **Doar ieşire** şi faceţi clic pe **Următorul**. Această clasă de servicii va fi utilizată numai pentru politici de ieşire.
17. În pagina Marcaj de punct de cod DiffServ ieşire, selectaţi **Clasa 4** şi faceţi clic pe **Următorul**. Un comportament per-hop determină ce performanţă va primi acest trafic de la ruter-ele şi alte servere din reţea. Folosiţi Ajutorul asociat interfeţei pentru a vă asista în decizia dumneavoastră.
18. În pagina Realizare măsurare a traficului de ieşire, verificaţi dacă este selectat **Da**şi apăsaţi **Următorul**.
19. În pagina Limite de control al ratei de ieşire, introduceţi următoarele informaţii şi faceţi clic pe **Următorult**:

- **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. Revedeţi Informaţia de sumar a clasei de serviciu. Dacă este corect, faceţi clic pe **Terminare** pentru a crea clasa de serviciu. După ce faceţi clic pe Sfârşit, vă întoarceţi la vrăjitorul politică şi va fi selectată clasa dumneavoastră de serviciu. Faceţi clic pe Următorul.
22. În pagina Planificare, selectaţi Activare în timpul programării selectate şi faceţi clic pe 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. Faceţi clic mai departe pentru a vedea sumarul politicii. Dacă corespunde, faceţi clic pe **Terminare**. În fereastra Configurare server QoS, puteţi vedea noua politică listată în panoul din dreapta.

Dacă terminaţi acum configurarea politicii de servicii diferenţiate pe iSeries A. Următorul pas este să porniţi sau să actualizaţi serverul.

Detaliile scenariului: Pornire sau actualizare a serverului QoS

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

Detaliile scenariului: Folosiţi monitorul pentru a verifica dacă funcţionează politica dumneavoastră.

Pentru a verifica dacă politica se comportă după cum aţi configurat-o, urmaţi următorii paşi:

1. În fereastra de configurare server QoS, selectaţi **Server → Monitor**. Fereastra Monitor QoS apare.
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 alocată câmpului limită a ratei medii este şi ea importantă. Când pachetele depăşesc această limită serverul va începe să le arunce. Ca rezultat, vor creşte biţii în-afara-profilului. Aceasta arată că politica se comportă după cum a fost configurată să se comporte. Consultaţi “Monitorizarea QoS” la pagina 55 pentru o descriere a tuturor câmpurilor de monitorizare.

   Notă: Amintiţi-vă că rezultatele vor fi corecte numai când este activă politica. Verificaţi programarea pe care aţi specificat-o în politică.

Detaliile scenariului: Modificare proprietăţi (dacă este nevoie)

După ce aţi văzut rezultatele din monitor, puteţi modifica orice politică sau proprietăţi de clasă de servicii pentru a ajuta realizarea rezultatelor pe care le aşteptaţi.

Puteţi modifica orice valori pe care le-aţi creat în politică urmând următorii 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 pagină Proprietăţi apare cu valori 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 **serviciu_UCD** din lista din panoul din dreapta şi selectaţi **Proprietăţi** pentru a edita clasa de serviciu.O fereastră Proprietăţi QoS apare cu valori care controlează gestiunea traficului.
4. Modificare a valorilor 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. Acest exemplu le arată pe cele două fiind folosite împreună.

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. De aceea, dacă aveţi o aplicaţie audio/video, trebuie 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.

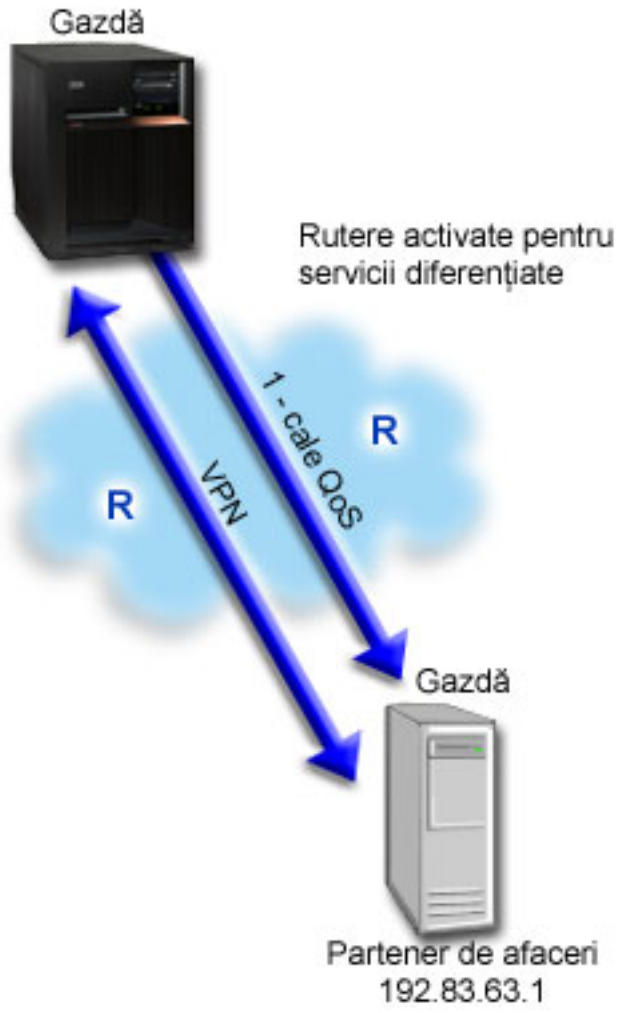


Figura 5. Conexiune gazdă-la-gazdă folosind o politică diferenţiată de servicii

Obiective

Este posibil să folosiţi VPN şi QoS pentru a stabili nu numai o protecţie, dar şi prioritate pentru această conexiune. 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) cu ISP-ul dumneavoastră pentru a vă asigura că politicile primesc prioritatea cerută. Politica QoS pe care o creaţi pe serverul iSeries activează traficul (în politică) pentru a primi prioritate prin reţea. Nu garantează aceasta şi este dependent de SLA-ul dumneavoastră. De fapt, profitarea de politicile QoS vă poate da un mijloc de a negocia anumite niveluri şi rate de serviciu. Folosiţi trimiterea la acordul de nivel de serviciu pentru a afla mai multe detalii.
- Politicile de servicii diferenţiate cer rutere care recunosc DiffServ de-a lungul căii de reţea. Majoritatea ruterelor recunosc DiffServ.

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
Această secţiune punctează unele din aspectele importante ale acordului SLA (service-level agreement), care pot afecta implementarea QoS.

"Servicii diferenţiate" la pagina 2
Acesta este primul tip de politică de lăţime de bandă de ieşire pe care o puteţi crea pe server. Serviciile diferenţiate împart traficul dumneavoastră pe clase. Pentru a avea grijă de politicile de servicii diferenţiate, trebuie să determinaţi cum doriţi să vă clasificaţi traficul din reţea şi cum manipulaţi clasele diferite.

Referinţe înrudite

"Monitorizarea QoS" la pagina 55
Puteţi folosi monitorizarea la analizarea traficului IP prin server.

Detaliile scenariului: Setarea unei conexiuni VPN gazdă-la-gazdă

Consultaţi exemplul Conexiune VPN gazdă-la-gazdă,pentru a vă ajuta cu configurarea VPN.

Detaliile scenariului: Crearea politicii de servicii diferenţiate

1. În Navigatorul iSeries, expandaţi iSeries A → **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 faceţi clic pe OK, vă întoarceţi la vrăjitorul politică. Dacă aţi creat înainte clienţi, deselectaţi-i şi verificaţi dacă doar clienţii relevanţi sunt selectaţi.
8. Pe pagina Cerere de date server, verificaţi că **Orice jeton** şi **Toate priorităţile** 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. Apare vrăjitorul Noua clasă de serviciu.
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 va fi utilizată numai pentru politici de ieşire.
16. În pagina Marcaj punct de cod DiffServ de ieşire, selectaţi **Clasa 3**. Un comportament per-hop determină ce performanţă va primi acest trafic de la ruter-ele şi alte servere din reţea. Folosiţi Ajutorul asociat interfeţei pentru a vă asista în decizia dumneavoastră.
17. În pagina Realizare măsurătoare a traficului de ieşire, verificaţi dacă este selectat **Da**şi faceţi clic pe **Următorul**.
18. În pagina Limite de control al ratei de ieşire, 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. Revedeţi pagina de sumar Clasa de serviciu şi faceţi clic pe **Terminare** 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
    - **Momentul zilei**: Activare la momente specifice şi adăugare 9:00 a.m. la 5:00 p.m.
    - **Ziua din săptămână**: Activare la o anumită zi şi selectare de luni până vineri.
24. În pagina Programare, faceţi clic pe **Următorul**.
25. Revedeţi informaţia de sumar. Dacă este corect, faceţi clic pe **Terminare** pentru a crea politica. Fereastra Configurare server QoS listează toate politicile create pe server. După ce aţi finalizat vrăjitorul, politica este listată în panoul drept.

Terminaţi acum configurarea politicii de servicii diferenţiate pe iSeries A. Următorul pas este să porniţi sau să actualizaţi serverul.

Detaliile scenariului: Pornire sau actualizare a serverului QoS

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

Detaliile scenariului: Folosiţi monitorul pentru a verifica dacă funcţionează politica dumneavoastră.

Pentru a verifica dacă politica se comportă după cum aţi configurat-o, urmaţi următorii paşi:

1. În fereastra de configurare server QoS, selectaţi **Server → Monitor**. Fereastra Monitor QoS apare.
2. Selectaţi tipul politică DiffServ. Acesta afişează toate politicile DiffServ.

   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, vor creşte biţii în-afara-profilului. 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: Amintiţi-vă că rezultatele vor fi corecte numai când este activă politica. Verificaţi programarea pe care aţi specificat-o în politică.

Detaliile scenariului: Modificare proprietăţi (dacă este nevoie)

După ce aţi văzut rezultatele din monitor, puteţi modifica orice politică sau proprietăţi de clasă de servicii pentru a ajuta realizarea rezultatelor pe care le aşteptaţi.

Pentru a edita clasa de servicii după ce aţi creat-o, urmaţi următorii paşi:

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 casetă dialog Proprietăţi apare cu valori 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 **EF_VPN** din lista din panoul din dreapta şi selectaţi **Proprietăţi** pentru a edita clasa de serviciu.O casetă dialog Proprietăţi QoS apare cu valori care controlează gestiunea traficului.
4. Modificare a valorilor corespunzătoare.
5. Din fereastra Configurare server QoS, selectaţi **Server → Actualizare** pentru a accepta schimbările.

Scenariu: Limitarea conexiunilor de intrare

Dacă trebuie să controlaţi cererile de conexiuni de intrare făcute la server, folosiţi o politică de admitere a intrării.

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 vă poate ajuta să restricţionaţi încercările de conectare de intrare , pe baza atributelor conexiunii (de exemplu, adresa IP) la serverul dumneavoastră. Pentru a realiza aceasta, vă decideţi să faceţi o politică de admitere intrare, care va restricţiona numărul de conexiuni acceptate.

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

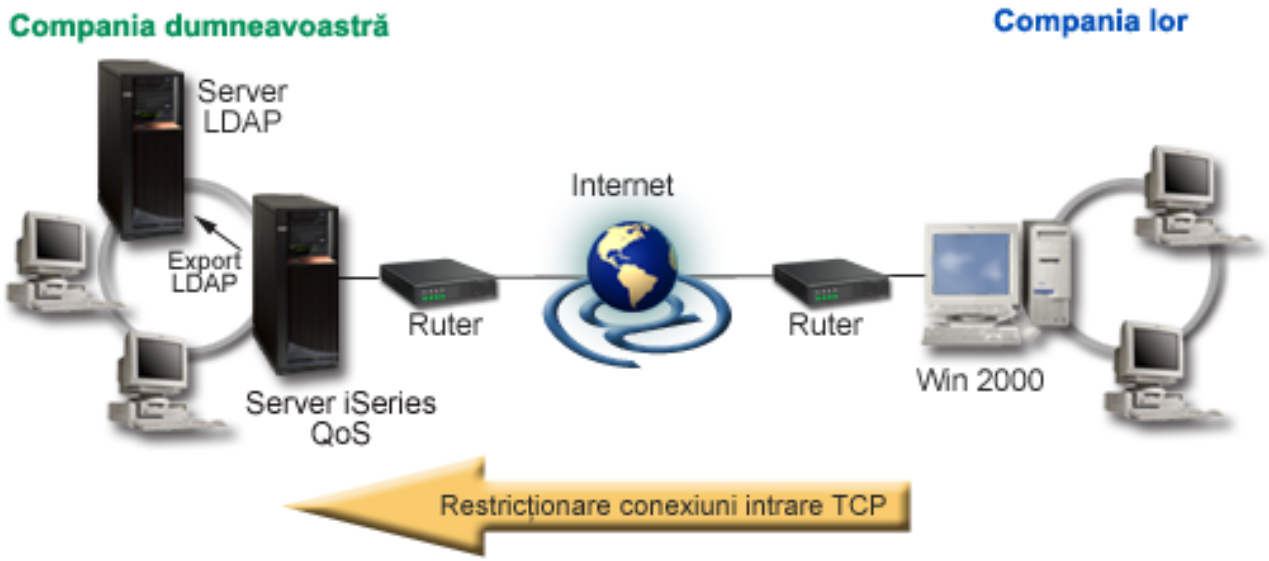


Figura 6. Restricţionare conexiuni intrare TCP

Obiective

Pentru a configura o politică de intrare, 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 la analizarea traficului IP prin server.

Detaliile scenariului: Crearea politicii de admitere intrare

1. În Navigator iSeries, expandaţi iSeries A → **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 admitere intrare** 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 politică. Dacă aţi creat înainte clienţi, deselectaţi-i şi verificaţi dacă doar clienţii relevanţi sunt selectaţi.
8. În pagina URI, verificaţi că este selectat **Orice URI** şi apăsaţi **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 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. Apare vrăjitorul Noua clasă de serviciu.
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 de intrare.
18. În pagina Limite de intrare, introduceţi următoarele informaţii şi faceţi clic pe **Următorul**:
    - Rata medie de conexiune: 50 pe secundă
    - Limita rafalei conexiune: 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
    - Momentul zilei: Activare la momente specifice şi adăugare 9:00 la 5:00.
    - Ziua din săptămână: Activare la anumite zile şi selectare Luni până Vineri.
23. În pagina Programare, apăsaţi **Următorul**.

24. Revedeţi informaţia de sumar. Dacă este corect, faceţi clic pe **Terminare** pentru a crea politica. Fereastra Configurare server QoS listează toate politicile create pe server. După ce aţi finalizat vrăjitorul, politica este listată în panoul drept.

    Dacă terminaţi acum configurarea politicii de servicii diferenţiate pe iSeries A. Următorul pas este să porniţi sau să actualizaţi serverul.

Detaliile scenariului: Pornire sau actualizare a serverului QoS

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

Detaliile scenariului: Folosiţi monitorul pentru a verifica dacă funcţionează politica dumneavoastră.

Pentru a verifica dacă politica se comportă după cum aţi configurat-o, urmaţi următorii paşi:

1. În fereastra de configurare server QoS, selectaţi **Server → Monitor**. Fereastra Monitor QoS apare.
2. Selectaţi tipul politică admitere intrare. Acesta va afişa toate politicile de Admitere intrare. 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 alocată câmpului rată de cerere de conexiune medie este şi ea importantă. Când pachetele depăşesc această limită serverul va începe să le arunce. Ca rezultat, vor creşte cererile aruncate. Aceasta arată că politica se comportă după cum a fost configurată să se comporte. Consultaţi secţiunea “Monitorizarea QoS” la pagina 55 pentru o descriere a tuturor câmpurilor de monitorizare.

   Notă: Amintiţi-vă că rezultatele vor fi corecte numai când este activă politica. Verificaţi programarea pe care aţi specificat-o în politică.

Detaliile scenariului: Modificare proprietăţi (dacă este nevoie)

După ce aţi văzut rezultatele din monitor, puteţi modifica orice politică sau proprietăţi de clasă de servicii pentru a ajuta realizarea rezultatelor pe care le aşteptaţi.

1. În fereastra Configurare server QoS, selectaţi folderul **Admiteri de intrare**. Faceţi clic dreapta pe **Restrict_TheirCot** din lista din panoul din dreapta şi selectaţi **Proprietăţi** pentru a edita politica.O pagină Proprietăţi apare cu valori 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 apare cu valori care controlează gestiunea traficului.
4. Modificare a valorilor 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 probleme precum faptul că traficul în reţea nu se realizează aşa cum ei se aşteptau. Serverul iSeries al companiei se află într-un mediu B2B (business-to-business), care necesită servicii de afaceri previzibile 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.

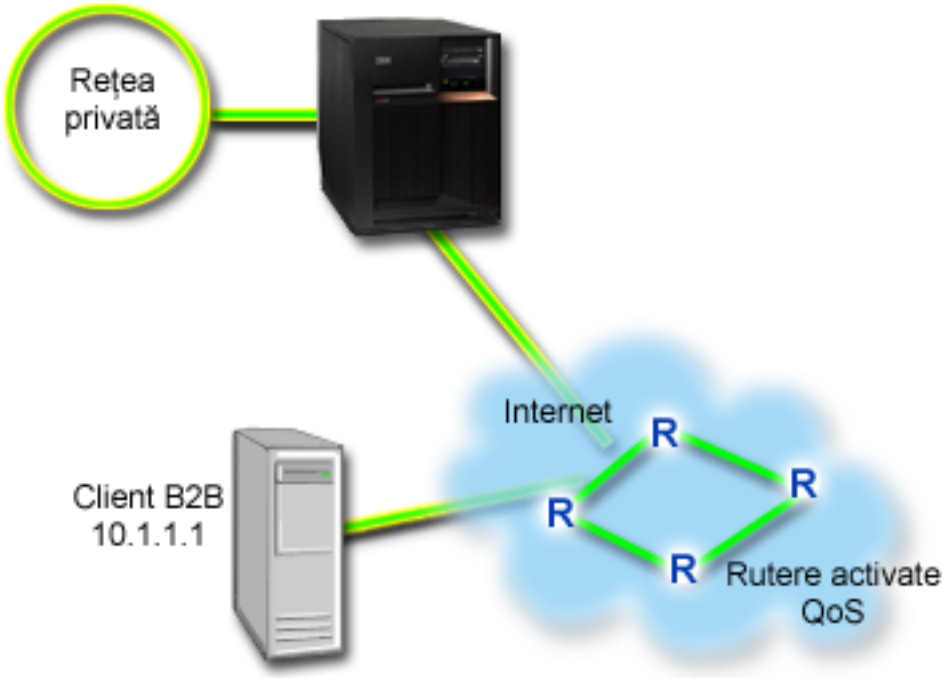


Figura 7. Politică de servicii integrate la un client B2B folosind rutere RSVP-activate.

Obiective

Serviciul de încărcare controlată suportă aplicaţii care sunt foarte sensibile la reţele congestionate, dar sunt încă 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 va fi furnizat asemănător serviciului cu trafic normal într-o reţea sub 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 şi ca de-a lungul căii traficului ruterele să fie RSVP-activate.

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 serverul nu are aplicaţii RSVP-activate, trebuie să 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.
- **Ruterele şi serverele RSVP-activate şi serverele de-a lungul căii de reţea**

  QoS este o soluţie de reţea. Dacă sunteţi nesigur dacă întreaga reţea are capacităţi RSVP, puteţi încă crea o politică de servicii integrate şi să folosiţi un marcaj pentru a da acesteia o prioritate; oricum, prioritatea nu poate fi garantată.
- **Acord la nivel de serviciu**

  Aveţi un SLA (service-level agreement) cu ISP-ul dumneavoastră pentru a vă asigura că politicile primesc prioritatea cerută. Politica QoS pe care o creaţi pe serverul iSeries activează traficul (în politică) pentru a primi prioritate prin

reţea. Politica QoS nu garantează aceasta şi este dependentă de SLA-ul dumneavoastră. De fapt, beneficiind de politicile QoS vă oferă un mijloc de a negocia anumite niveluri şi rate de serviciu. Folosiţi trimiterea la acordul de nivel de serviciu pentru a afla mai multe detalii.

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 garantată.

"Servicii integrate" la pagina 6
Al doilea tip de politică de lăţime de bandă de ieşire pe care o 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 QoS" la pagina 16
Puteţi citi acest subiect pentru a învăţa despre protocoale, API-uri şi cerinţe pentru un ruter care este activat pentru protocolul ReSerVation (RSVP). Actualul API QoS include API-ul RAPI, API-ul qtoq socket, API-ul sendmsg() şi API-ul monitor.

"Acord la nivel de serviciu" la pagina 48
Această secţiune punctează unele din aspectele importante ale acordului SLA (service-level agreement), care pot afecta implementarea QoS.

Referinţe înrudite

"Monitorizarea QoS" la pagina 55
Puteţi folosi monitorizarea la analizarea traficului IP prin server.

Detaliile scenariului: Crearea politicii de servicii integrate

1. În Navigatorul iSeries, expandaţi iSeries A → **Reţea** → **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 politică. Dacă aţi creat înainte clienţi, deselectaţi-i şi verificaţi dacă 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 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 ruter-ele şi serverele de-a lungul căii traficului, trebuie să folosească, de asemenea, protocolul RSVP 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
    - **Momentul zilei**: Activare la momente specifice şi adăugare 10:00 a.m. la 4:00 p.m.
    - **Ziua din săptămână**: Activare la o anumită zi şi selectare de luni până vineri.
16. În pagina Programare, apăsaţi **Următorul**.
17. Revedeţi informaţia de sumar. Dacă este corect, faceţi clic pe **Terminare** pentru a crea politica. Interfaţa principală QoS listează toate politicile create pe server. După ce aţi completat vrăjitorul, politica este listată în panoul drept.

Terminaţi acum configurarea politicii de servicii diferenţiate pe iSeries A. Următorul pas este să porniţi sau să actualizaţi serverul.

Detaliile scenariului: Pornire sau actualizare a serverului QoS

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

Detaliile scenariului: Folosiţi monitorul pentru a verifica dacă funcţionează politica dumneavoastră.

Pentru a verifica dacă politica se comportă după cum aţi configurat-o, urmaţi următorii paşi:

1. În fereastra configurare server QoS, selectaţi **Server → Monitor**. Fereastra Monitor QoS apare.
2. Selectaţi tipul politică IntServ. Acesta afişează toate politicile IntServ.

   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 câmpurilor de monitorizare, consultaţi secţiunea “Monitorizarea QoS” la pagina 55.

   Notă: Amintiţi-vă că rezultatele vor fi corecte numai când este activă politica.Verificaţi programarea pe care aţi specificat-o în politică. De asemenea, monitorul arată numai politicile IntServ după ce aplicaţiile rulează. O rezervare RSVP trebuie să fie stabilită înainte de monitorizare.

Detaliile scenariului: Modificare proprietăţi (dacă este nevoie)

După ce aţi văzut rezultatele din monitor, puteţi modifica orice proprietăţi de politică pentru a ajuta realizarea rezultatelor pe care le aşteptaţi.

După ce aţi creat această politică, puteţi modifica valorile pe care le-aţi creat înainte cu vrăjitorul.

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 apare cu valorile care controlează politica generală.
2. Modificare a valorilor 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. Sunt două tipuri de politici de servicii integrate de creat: încărcare garantată şi controlată. În acest exemplu, este folosit serviciul garantat.

Situaţie

Directorul executiv (CEO - chief executive officer) al companiei dumneavoastră este pe cale să lanseze o difuzare în direct pentru un client aflat în cealaltă parte a ţării, între 1:00 p.m.- 2:00 p.m. Dumneavoastră trebuie să asiguraţi ca telefonia IP să garanteze lăţimea de bandă, astfel încât să nu apară întreruperi în timpul difuzării. În acest scenariu, aplicaţia se află pe server.

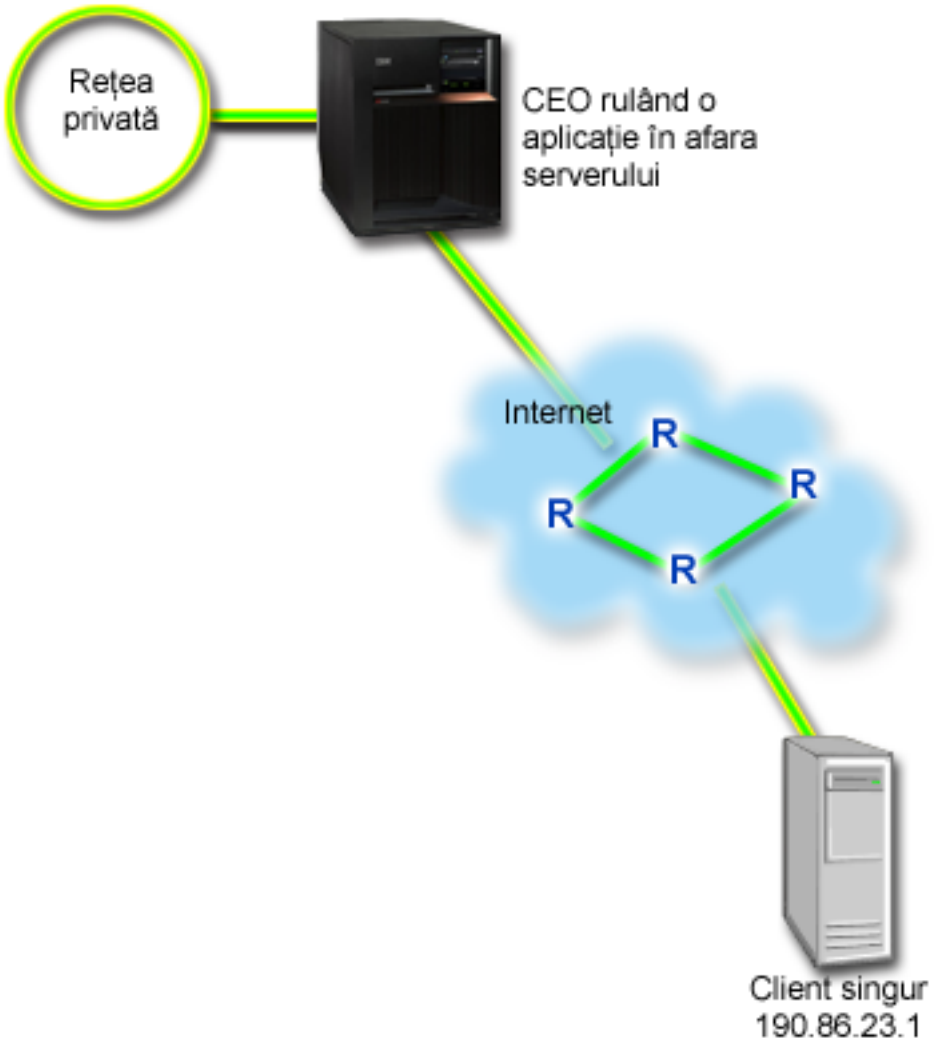


Figura 8. Prezentarea CEO pentru un client, garantată de o politică de servicii integrate.

Obiective

Deoarece aplicaţia pe care CEO-ul dumneavoastră o foloseşte necesită un transfer uniform, neîntrerupt, decideţi să folosiţi o politică de servicii integrate garantată. Serviciul garantat controlează întârzierea maximă a cozii, astfel că pachetele nu vor fi întârziate peste 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 serverul nu are aplicaţii activate RSVP, trebuie să scrieţi propriile aplicaţii RSVP-activate. Pentru a scrie propriile dumneavoastră aplicaţii, folosiţi API-ul RAPI (ReSerVation Protocol) sau APi-urile socket-ului QoS qtoq. Pentru informaţii suplimentare, vedeţi “API-uri QoS” la pagina 16 şi căutaţi API-urile servicii integrate.
- **Ruterele şi serverele RSVP-activate de-a lungul căii de reţea**

  QoS este o soluţie de reţea. Dacă sunteţi nesigur dacă întreaga reţea are capacităţi RSVP, puteţi crea, încă o politică de servicii integrate şi folosiţi un marcaj pentru a da acesteia o prioritate; oricum, prioritatea nu poate fi garantată.
- **Acord la nivel de serviciu**

Aveţi un Acord de nivel serviciu (SLA - service-level agreement) cu ISP-ul dumneavoastră pentru a vă asigura că politicile primesc prioritatea cerută. Politica QoS pe care o creaţi pe serverul iSeries activează traficul (în politică) pentru a primi prioritate prin reţea. Politica QoS nu garantează aceasta şi este dependentă de SLA-ul dumneavoastră. De fapt, profitarea de politicile QoS vă poate da un mijloc de a negocia anumite niveluri şi rate de serviciu. Folosiţi trimiterea la acordul de nivel de serviciu pentru a afla mai multe detalii.

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 garantată.

"Servicii integrate" la pagina 6
Al doilea tip de politică de lăţime de bandă de ieşire pe care o 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
Această secţiune punctează unele din aspectele importante ale acordului SLA (service-level agreement), care pot afecta implementarea QoS.

Referinţe înrudite

"Monitorizarea QoS" la pagina 55
Puteţi folosi monitorizarea la analizarea traficului IP prin server.

Detaliile scenariului: Crearea politicii de servicii integrate

1. În Navigatorul iSeries, expandaţi iSeries A → **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 aţi creat înainte clienţi, deselectaţi-i şi verificaţi dacă 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 ruter-ele şi serverele de-a lungul căii traficului, trebuie să folosească, de asemenea, protocolul RSVP 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
    - **Momentul zilei**: Activare la momente specifice şi adăugare 1:00 p.m. la 2:00 p.m.
    - **Ziua din săptămână**: Activare la o anumită zi şi selectare Luni.
16. În pagina Programare, faceţi clic pe **Următorul**.
17. Revedeţi informaţia de sumar. Dacă este corect, faceţi clic pe **Terminare** 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.

Terminaţi acum configurarea politicii de servicii diferenţiate pe iSeries A. Următorul pas este să porniţi sau să actualizaţi serverul.

Detaliile scenariului: Pornire sau actualizare a serverului QoS

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

Detaliile scenariului: Folosiţi monitorul pentru a verifica dacă funcţionează politica dumneavoastră.

Pentru a verifica dacă politica se comportă după cum aţi configurat-o, urmaţi următorii paşi:

1. În fereastra de configurare server QoS, selectaţi **Server → Monitor**. Fereastra Monitor QoS apare.
2. Selectaţi fişierul tip politică IntServ. Acesta afişează toate politicile IntServ.

   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: Amintiţi-vă că rezultatele vor fi corecte numai când este activă politica. Verificaţi programarea pe care aţi specificat-o în politică. De asemenea, monitorul arată numai politicile IntServ după ce aplicaţiile rulează. O rezervare RSVP trebuie să fie stabilită înainte de monitorizare.

Detaliile scenariului: Modificare proprietăţi (dacă este nevoie)

După ce aţi văzut rezultatele din monitor, puteţi modifica orice proprietăţi de politică pentru a ajuta realizarea rezultatelor pe care le aşteptaţi.

După ce aţi văzut rezultatele monitor pentru această politică, puteţi modifica valorile pe care le-aţi creat înainte cu vrăjitorul.

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 apare cu valorile care controlează politica generală.

2. Modificare a valorilor corespunzătoare.
3. Din fereastra Configurare server QoS, selectaţi **Server → Actualizare** pentru a accepta schimbările.

Scenariu: Monitorizarea statisticilor curente de reţea

În vrăjitori sunteţi rugat să setaţi limite de performanţă. Acestea sunt valori care nu pot fi recomandate, deoarece sunt bazate pe cerinţe de reţea individuale.

Obiective

Pentru a seta aceste limite, trebuie să înţelegeţi într-adevăr performanţa actuală a reţelei dumneavoastră. Deoarece încercaţi să configuraţi politicile de calitate a serviciilor, probabil aveţi deja o idee despre cerinţele curente ale reţelei. Pentru a determina cu exactitate limitele de rată, cum ar fi rata găleţii jeton, aţi putea dori să monitorizaţi tot traficul de pe server încât să puteţi determina mai bine ce limite de rate să setaţi.

Soluţie

Creaţi o politică de service diferenţiat foarte cuprinzătoare care să nu conţină restricţii (fără valori maxime) şi să fie aplicată 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 garantarea livrării pachetelor în politici de lăţime de bandă de ieşire, atât servicii integrate cât şi diferenţiate.

“Rata medie de conexiune şi limite în rafală” la pagina 15
Ratele de conexiune şi limite în rafală sunt cunoscute împreună ca *limite de rată*. Aceste limite de rate restricţionează conexiunile de intrare încercând să între în server. Limitele de rate sunt un set de clase de serviciu folosite cu politici de admitere intrare.

Referinţe înrudite

“Monitorizarea QoS” la pagina 55
Puteţi folosi monitorizarea la analizarea traficului IP prin server.

Detaliile scenariului: Deschideţi QoS în Navigatorul iSeries

1. În Navigatorul iSeries, expandaţi serverul dumneavoastră **→ Reţea → Politici IP**.
2. Faceţi clic dreapta **Calitatea serviciului** şi selectaţi **Configurare**.
3. Expandaţi **Politici lăţime de bandă de ieşire**.
4. Faceţi clic dreapta pe **DiffServ** şi selectaţi **Politică nouă** . Apare noul vrăjitor de politică QoS.

Detaliile scenariului: Crearea politicii de servicii diferenţiate

Deoarece doriţi să colectaţi majoritatea intrărilor de trafic din reţeaua dumneavoastră, aţi putea apela la politica **Reţea**. Folosiţi toate adresele IP, toate porturile, toate adresele IP locale şi toţi timpii (dacă sunt potriviţi). Folosiţi următoarele setări de-a lungul vrăjitorului:

Nume = Reţea (poate fi orice nume alocat)**Client** = Toate adresele IP**Aplicaţie** = Toate porturile**Protocol** = Toate protocoal

Navigatorul iSeries listează toate politicile de servicii diferenţiate create pe server.

Detaliile scenariului: Crearea unei noi clase de servicii

În timp ce rulează vrăjitorul, sunteţi rugat să alocaţi un comportament per-hop, limite de performanţă şi tratarea traficului afară-din-profil. Aceasta este definită într-o clasă de servicii. Alegeţi valori foarte mari pentru a permite cât mai mult flux de trafic posibil.

Clasele de servicii determină chiar nivelurile de performanţă pe care acest trafic le primeşte de la un ruter. Este posibil să numiţi clasa dumneavoastră de serviciu **Nelimitată**, pentru a arăta că acest trafic primeşte un serviciu mai înalt. Navigatorul iSeries listează toate politicile de servicii diferenţiate create pe server.

Detaliile scenariului: Monitorizaţi-vă politica

Pentru a verifica dacă politica se comportă după cum aţi configurat-o, folosiţi monitorizarea.

1. Selectaţi fişerul specific Politici (DiffServ, IntServ, admitere intrare).
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.

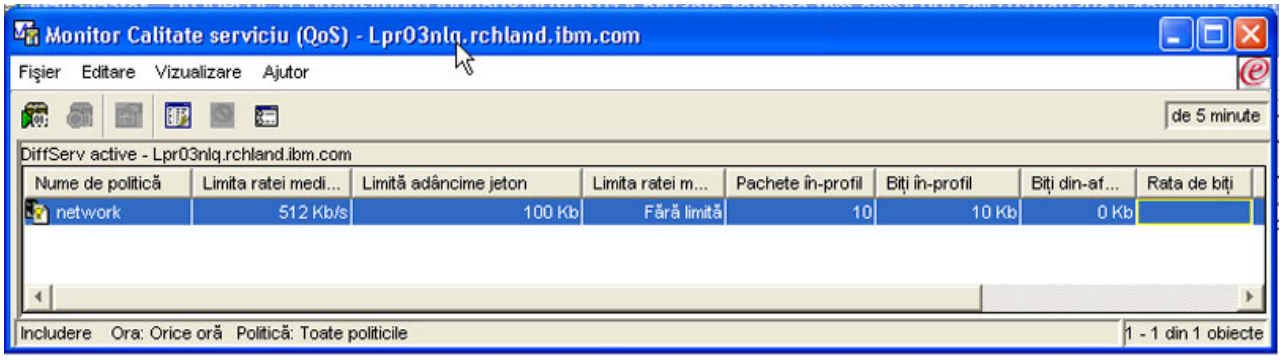


Figura 9. Monitorizare Calitatea serviciului (QoS - Quality of service)

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).

Este important şi ce valori alocaţi câmpului de limitare a ratei jeton medii. Când pachetele depăşesc această limită serverul va începe să le arunce. Ca rezultat, vor creşte biţii în-afara-profilului. Aceasta arată că politica se comportă după cum a fost configurată să se comporte. Pentru a modifica numărul de biţi în-afara-profilului, va trebui să ajustaţi limitele de performanţă. Monitorul QoS furnizează descrieri complete ale tuturor câmpurilor monitorizate.

Detaliile scenariului: modificarea valorilor când este nevoie

După monitorizarea dumneavoastră, puteţi modifica orice valori 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**, apare o fereastră Proprietăţi QoS cu valori ce controlează traficul dumneavoastră.

Detaliile scenariului: Monitorizaţi din nou politica

După vederea rezultatelor, folosiţi metoda ″ghicire şi verificare″ pentru a găsi cele mai bune limite pentru nevoile reţelei dumneavoastră.

Planificarea pentru QoS

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.

Considerare a performantei 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

"Monitorizarea tranzacţiilor server" la pagina 62
Cu monitorizarea QoS puteţi să verificaţi că politicile QoS funcţionează aşa cum doriţi dumneavoastră ca ele să funcţioneze.

"Configurarea QoS" la pagina 50
Puteţi utiliza acest subiect pentru a crea politici de servicii diferenţiate, politici de servicii integrate şi politici de admitere intrare.

Cerinţe de autorizare

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

Autorizările următoare sunt necesare înainte de a putea configura politicile QoS şi (opţional) serverele de directoare LDAP.

Acordarea autorizărilor necesare pentru a gestiona serverul de directoare.

Administratorul QoS are nevoie de următoarele autorizări: autorizarea *ALLOBJ şi *IOSYSCFG. Vedeţi Configurare server de directoare pentru autorizări alternative.

Acordare autorizare de pornire a serverului 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.

Acordaţi autorizări de accesare şi de configurare a sistemului tuturor obiectelor.

Este recomandat ca utilizatorii care vor configura QoS să aibă acces de responsabil cu securitatea. Pentru a acorda autorizări de accesare şi de configurare a sistemului tuturor obiectelor, urmaţi aceşti paşi:

1. În Navigatorul iSeries, expandaţi serverul 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 utilităţile de conectare TCP/IP (5722-TC1).
2. Instalaţi pe PC-ul dumneavoastră Navigatorul iSeries. Asiguraţi-vă că aţi instalat secţiunea Reţea în timpul instalării Accesului iSeries. Calitatea serviciului este localizată sub politici IP în Reţele.

   Concepte înrudite

   Navigator iSeries

   Referinţe înrudite

   “Informaţii înrudite pentru QoS” la pagina 65
   Listate mai jos sunt IBM Redbooks (în format PDF), site-uri Web şi subiectele Centrului de informare legate de subiectul QoS. Puteţi citi sau tipări oricare din PDF-uri.

Acord la nivel de serviciu

Această secţiune punctează unele din aspectele importante ale acordului SLA (service-level agreement), care pot afecta implementarea QoS.

QoS este o soluţie de reţea. Pentru a primi prioritate de reţea înafara reţelei dumneavoastră, aţi putea avea nevoie să aveţi un SLA cu ISP-ul dumneavoastră.

Când este necesar un SLA

Aveţi nevoie de un SLA, doar dacă politicile dumneavoastră au nevoie de prioritate în afara reţelei dumneavoastră private. Dacă folosiţi politici de ieşire pentru a încetini ieşirea traficului din serverul dumneavoastră, atunci nu este nevoie de nici o garanţie pentru serviciu. De exemplu, pe server, puteţi crea o politică ce dă unei aplicaţii prioritate mai înaltă decât altei aplicaţii. Serverul dumneavoastră recunoaşte această prioritate, dar orice din afara serverului este posibil să nu recunoască prioritatea. Dacă aveţi o reţea particulară şi configuraţi ruterele dumneavoastră pentru a recunoaşte marcajele punct de cod (utilizate pentru a da politicilor de ieşire un nivel de serviciu), atunci ruterele vor acorda prioritate prin reţeaua dumneavoastră privată. Oricum, dacă traficul părăseşte reţeaua dumneavoastră privată, nu există garanţii. Fără un SLA, dumneavoastră nu controlaţi cum hardware-ul de reţea va manevra traficul. În afara reţelei dumneavoastră private, vă va trebui un SLA pentru a garanta prioritatea pentru o clasă de serviciu sau rezervare de resursă.

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 activează aplicaţii pentru a primi 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 servicii pe care îl primiţi. 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 rezervarea a 500 Kbps pentru telefonie IP, dar aplicaţia dumneavoastră necesită doar 20 Kbps, puteţi să plătiţi în plus fără să fiţi înştiinţat de ISP-ul dumneavoastră.

Notă: Politicile QoS vă permit să negociaţi nivelurile de serviciu cu ISP-ul dumneavoastră, care este posibil să micşoreze costurile de serviciu pentru 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. ISP-ul va trebui să fie de acord cu un anumit nivel de serviciu şi sa aibă capacitatea să urmărească lăţimea de bandă pe care dumneavoastră o folosiţi.

Concepte înrudite

“Concepte” la pagina 2
Dacă sunteţi nou în ceea ce priveşte QoS, puteţi citi câteva concepte de bază QoS.Aceasta vă va oferi o privire generală asupra modului de funcţionare al QoS şi despre cum funcţionează împreună funcţiile QoS.

“Scenariu: Limitarea traficului de browser” la pagina 27
Puteţi utiliza calitatea serviciilor (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. Acest exemplu le arată pe cele două fiind folosite împreună.

“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. Sunt două tipuri de politici de servicii integrate de creat: 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 iSeries nu sunt în prezent RSVP-activate, trebuie să le activaţi pentru folosirea protocolului RSVP. Pentru a vă activa aplicaţiile, trebuie să scrieţi programe speciale folosind API-uri RSVP sau API-uri socket QoS qtoq. Aceste programe vor permite aplicaţiilor dumneavoastră să folosească.

Noduri de reţea

Ruterele, switch-urile şi chiar serverele dumneavoastră trebuie să aibă capacitatea de a folosi QoS. Pentru a folosi politici de servicii integrate, 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 QoS" la pagina 16
Puteţi citi acest subiect pentru a învăţa despre protocoale, API-uri şi cerinţe pentru un ruter care este activat pentru protocolul ReSerVation (RSVP). Actualul API QoS include API-ul RAPI, API-ul qtoq socket, API-ul sendmsg() şi API-ul 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.

Configurarea QoS

Puteţi utiliza acest subiect pentru a crea politici de servicii diferenţiate, politici de servicii integrate şi politici de admitere intrare.

După ce realizaţi planificarea QoS, puteţi să creaţi politicile QoS folosind vrăjitorii din Navigatorul iSeries. Vrăjitorii fac o treabă excelentă conducându-vă prin configurare.

După ce configuraţi politicile, puteţi folosi obiectele de configurare în Navigatorul iSeries pentru a vă edita configurarea de politici.Obiectele de configurare sunt piesele sau părţile diferite care fac o politică. Când deschideţi calitatea serviciilor în Navigatorul iSeries, sunt directoare etichetate clienţi, aplicaţii, planificări, politici, clase de servicii, comportamente per-hop şi URI-uri. Aceste obiecte vă permit să construiţi o politică. Pentru informaţii suplimentare despre obiecte, puteţi consulta Privire generală asupra Calităţii serviciilor din Navigatorul iSeries.

Activarea politicilor QoS

Înainte ca politicile să aibă efect, trebuie activate. Dacă aţi folosit vrăjitorii, serverul va activa automat politicile pentru dumneavoastră. Totuşi, dacă aţi modificat o politică folosind obiectele de configurare, va trebui să actualizaţi dinamic serverul înainte ca politicile să devină active. Înainte de activare, asiguraţi-vă că nu există politici suprapuse care pot cauza probleme.

Concepte înrudite

"Planificarea pentru QoS" 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.

Navigator iSeries

Operaţii înrudite

"Ordonarea politicilor QoS" la pagina 53
Ori de câte ori aveţi două politici ce se suprapun, contează ordinea fizică a politicilor în Navigatorul iSeries.

Referinţe înrudite

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

Configurarea QoS cu vrăjitori

Pentru a configura politicile QoS, trebuie să folosiţi vrăjitorii QoS din Navigatorul iSeries.

Aceasta este o listă a vrăjitorilor şi a funcţiilor lor:

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 admite sau refuză cereri RSVP, care controlează indirect lăţimea de bandă a serverului. Limitele de performanţă a

politicii (pe care le-aţi setat) decid dacă serverul poate manipula lăţimea de bandă cerută venind de la aplicaţia RSVP a clientului. Veţi avea nevoie de rutere şi aplicaţii RSVP pregătite să aibă grijă de politicile servicii integrate create în acest vrăjitor.

Notă: Înainte să setaţi o politică de servicii integrate trebuie să vă scrieţi propriile aplicaţii să folosească protocolul RSVP.

Vrăjitor politică nouă DiffServ
Acest vrăjitor vă permite să diferenţiaţi şi să alocaţi prioritate traficului TCP/IP. Veţi putea diferenţia traficul creând politici. Într-o politică, alocaţi niveluri de serviciu pentru ieşirea traficului bazat pe adrese IP sursă/destinaţie, porturi, aplicaţii şi chiar clienţi. În V5R3, aplicaţiile dumneavoastră iSeries pot primi niveluri de serviciu bazate pe mai multe informaţii aplicaţie specifică. Pentru informaţii suplimentare, citiţi noţiunea servicii diferenţiate înainte de a crea această politică.

Vrăjitorul Clasă nouă de serviciu
Folosiţi vrăjitorul clasă de serviciu pentru a seta pachetul de marcaje folosite de rutere şi switch-uri din reţele. Alocă şi limite de performanţă traficului care părăseşte reţeaua. Folosiţi clasa de servicii cu politică servicii diferenţiate şi o politică de admitere intrare.

Vrăjitorul admitere nouă intrare
Folosiţi vrăjitorul admitere intrare pentru a restricţiona conexiuni făcute de serverul 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 serverul dumneavoastră de la anumiţi clienţi, aplicaţii proprii de server sau de la URI. În plus, puteţi îmbunătăţi performanţa serverului.

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 aţi decis ce tip de politică să creaţi, puteţi configura politica în vrăjitorul corespunzător listat mai sus.

Accesaţi vrăjitorii QoS din Navigatorul iSeries

Pentru a accesa vrăjitorii QoS şi a crea o nouă politică în interiorul Navigatorului iSeries .

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

1. În Navigatorul iSeries, expandaţi serverul 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 **Inbound admission**.
5. Selectaţi **Politică nouă**.

Concepte înrudite

“API-uri QoS” la pagina 16
Puteţi citi acest subiect pentru a învăţa despre protocoale, API-uri şi cerinţe pentru un ruter care este activat pentru protocolul ReSerVation (RSVP). Actualul API QoS include API-ul RAPI, API-ul qtoq socket, API-ul sendmsg() şi API-ul monitor.

“Servicii diferenţiate” la pagina 2
Acesta este primul tip de politică de lăţime de bandă de ieşire pe care o puteţi crea pe server. Serviciile diferenţiate împart traficul dumneavoastră pe clase. Pentru a avea grijă de politicile de servicii diferenţiate, trebuie să determinaţi cum doriţi să vă clasificaţi traficul din reţea şi cum manipulaţi clasele diferite.

Informaţii înrudite

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

Configurare server de directoare

Configurările de politici QoS pot fi exportate la un server director LDAP.

Acesta vă poate face mai uşor de gestionat soluţia calitatea serviciilor (QoS). În loc să configuraţi politicile QoS pe toate serverele, puteţi stoca datele de configurare pe un server de directoare local pentru a fi împărţite mai multor sisteme. Când configuraţi pentru întâia oară calitatea serviciilor pe server, apare un vrăjitor de configurare iniţială. Acest vrăjitor vă va invita să configuraţi un server de directoare.

Pentru a configura serverul de directoare va trebui să decideţi sau să ştiţi următoarele informaţii:

- Nume server de directoare
- Determinaţi un nume distinctiv (distinguished name - DN) pentru a vă referi la politicile QoS
- Determinaţi dacă veţi folosi securitate SSL cu serverul dumneavoastră de directoare LDAP
- Determinaţi dacă veţi folosi cuvinte cheie pentru a îmbunătăţi căutarea politicilor dumneavoastră pe serverul de directoare.

Notă: Momentan, Kerberos nu poate fi configurat ca metodă de autentificare pe care serverul QoS o va folosi la accesarea directorului.

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 auditarea de securitate i5/OS

În cazul în care folosiţi Navigatorul iSeries, aveţi deja acces la schema implicită QoS.Fişierul schemă este localizat pe serverul dumneavoastră în /QIBM/UserData/OS400/DirSrv. Totuşi, dacă folosiţi alt editor decât Navigatorul iSeries, va trebui să importaţi fişierul LDIF descris în secţiunea următoare. Puteţi importa şi acest fişier dacă 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 un server QoS. Schema conţine regulile necesare pentru QoS. Dacă totuşi serverul LDAP folosit nu este un server iSeries, aceste reguli trebuie importate în serverul LDAP. Aceasta este făcută printr-un fişier LDIF (Format interschimbare de date LDAP). Folosiţi pagina de Web iSeries LDAP pentru a descărca fişierul LDIF. Veţi găsi acest fişier în **Categorii → Politici TCP/IP** pe panoul din stânga. Consultaţi Concepte LDAP pentru o schemă QoS exemplu.

Concepte înrudite

“Server director” la pagina 24
Puteţi alege să exportaţi politicile dumneavoastră unui server director. Vedeţi acest subiect pentru a afla avantajele utilizării sau neutilizării unui server director, a conceptelor şi configuraţiei LDAP, cât şi ale schemei QoS.

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

IBM Directory Server pentru iSeries (LDAP)

Securitate SSL cu serverul dumneavoastră de directoare LDAP

“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

Pagina Web iSeries LDAP

Ordonarea politicilor QoS

Ori de câte ori aveţi două politici ce se suprapun, contează ordinea fizică a politicilor în Navigatorul iSeries.

Politicile ce se suprapun sunt două politici care folosesc acelaşi client, aplicaţie, programare, adresă IP locală, URI, date de server, punct de cod sau protocol. Politicile pe ecranul Navigatorului iSeries 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 altă politică, urmaţi aceste instrucţiuni:

1. În Navigatorul iSeries, expandaţi serverul dumneavoastră → **Reţea → Politici IP**.
2. Faceţi clic dreapta **Calitatea serviciului**.
3. Selectaţi **Configurare**.
4. Selectaţi folderul Politici.
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**. Apare fereastra Suprapunere politici.

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

"Configurarea QoS" la pagina 50
Puteţi utiliza acest subiect pentru a crea politici de servicii diferenţiate, politici de servicii integrate şi politici de admitere intrare.

"Copierea unei politici existente" la pagina 54
Decât să creaţi toate politicile de la început, puteţi face copii după politicile originale şi pe urmă să editaţi secţiunile politicii care diferă de politica originală.

"Depanarea QoS" la pagina 59
QoS furnizează mai multe metode de depanare a problemelor QoS.

Operaţii înrudite

"Acces ajutorul QoS în Navigatorul iSeries" la pagina 54
Puteţi folosi Navigatorul iSeries pentru a accesa ajutorul Quality of Service (QoS).

Gestionaţi QoS

Puteţi folosi aceste proceduri pentru a gestiona proprietăţile şi politicile calitatea serviciilor (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 despre modul de folosire a monitorului QoS şi a colectării de date pentru a vă ajuta la analiza traficului IP prin server.

Concepte înrudite

"Configurarea QoS" la pagina 50
Puteţi utiliza acest subiect pentru a crea politici de servicii diferenţiate, politici de servicii integrate şi politici de admitere intrare.

Acces ajutorul QoS în Navigatorul iSeries

Puteţi folosi Navigatorul iSeries pentru a accesa ajutorul Quality of Service (QoS).

Pentru a accesa ajutorul QoS, trebuie să folosiţi Navigatorul iSeries:

1. În Navigatorul iSeries, expandaţi serverul 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
Ori de câte ori aveţi două politici ce se suprapun, contează ordinea fizică a politicilor în Navigatorul iSeries.

Politici QoS de rezervă

Ar trebui să faceţi o copie de rezervă a politicilor QoS pentru a elimina nevoia de a recrea politicile dumneavoastră în cazul unei întreruperi a serverului sau pană de curent.

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 eventualitatea unei pierderi, salvările dumneavoastră vă salvează timpul şi munca necesare pentru recrearea politicilor dumneavoastră 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 *Salvare de rezervă şi recuperare* furnizează instrucţiuni pentru a realiza copii de rezervă din sisteme integrate de fişiere.
2. **Tipăriţi politicile.**

   Puteţi stoca imprimatele oriunde este probabil să fie în siguranţă 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 iSeries copiază informaţiile pe discul sistemului, nu pe o dischetă. Fişierele cu reguli sunt în QIBM/UserData/OS400/QOS/ETC ca şi în numele distinctiv în serverul de directoare 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 server iSeries, trebuie să puneţi la punct o strategie de copiere de siguranţă şi de recuperare.

Informaţii înrudite

Salvare de rezervă şi recuperare

Copierea unei politici existente

Decât să creaţi toate politicile de la început, puteţi face copii după politicile originale şi pe urmă să editaţi secţiunile politicii care diferă de politica originală.

În Navigatorul iSeries, această funcţie QoS se numeşte *Nou bazat pe*. Trebuie să folosiţi Navigatorul iSeries pentru a accesa fereastra QoS care vă permite să realizaţi copierea politicilor.

Ca să creaţi o copie a unei politici existente, urmaţi paşii din **Crearea unei politici noi bazată pe o politică existentă** în ajutorul Navigatorului iSeries.

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
Ori de câte ori aveţi două politici ce se suprapun, contează ordinea fizică a politicilor în Navigatorul iSeries.

Editarea politicilor 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 configuraţi politicile, puteţi folosi obiectele de configurare în Navigatorul iSeries pentru a vă edita configurarea de politici. Obiectele de configurare sunt piesele sau părţile diferite care fac o politică. Când deschideţi calitatea serviciilor în Navigatorul iSeries, sunt foldere etichetate clienţi, aplicaţii, planificări, politici, clase de servicii, comportamente per-hop şi URI-uri. Aceste obiecte vă permit să editaţi o politică.

Pentru a edita o politică în Navigatorul iSeries, urmaţi paşii din pagina Editarea unei politici QoS din ajutorul Navigatorului iSeries.

Monitorizarea QoS

Puteţi folosi monitorizarea la analizarea traficului IP prin server.

Aceasta vă ajută să determinaţi unde apare congestionarea în reţea. Nu doar că este folositor în timpul planificării QoS, dar poate fi folositor şi ca unealtă de depanare. Monitorizarea QoS vă poate ajuta să continuaţi monitorizarea reţelei astfel încât să vă puteţi ajusta politicile după cum este necesar. Pentru a monitoriza toate politicile active, selectaţi **Server → Monitor** din fereastra Configurare server QoS. Dacă faceţi clic pe o singură politică şi selectaţi **Monitor**, monitor va afişa numai informaţiile 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 Monitor QoS, evidenţiaţi *monitor QoS* şi selectaţi *Fişier-->Proprietăţi* pentru a modifica opţiunile dumneavoastră. Folosiţi ajutorul online pentru informaţii suplimentare.

  Dacă este pornită colecţia de date QoS şi proprietăţile monitorului sunt modificate, atunci trebuie să realizaţi următorii paşi pentru a vă asigura că modificările sunt reflectate în colecţia de date.

  1. Oprire Colecţie de 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. Actualizaţi serverul QoS.
  4. Pornire Colecţie de date QoS.

Monitorizare ieşire

Informaţiile de ieşire pe care le primiţi depind de tipul politicii pe care o monitorizaţi. Amintiţi-vă tipurile de politici: DiffServ, IntServ (Încărcare controlată), IntServ (Garantat) şi Admitere intrare. 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, TOATE
Limită de rată jeton medie	Rata de jeton medie permisă de această politică în fiecare ruter şi server de-a lungul căii de flux.
Limită de adâncime jeton	Dimensiunea de buffer jeton maximă permisă de această politică în fiecare ruter şi server 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 port sursă care determină care aplicaţii sunt controlate de această politică.

Politici servicii integrate (sarcină controlată)

Politicile IntServ nu afişează în monitor până când aplicaţiile nu rulează şi rezervările s-au stabilit. Dacă politicile IntServ au mai mult de o rezervare, veţi vedea mai multe intrări în monitor.

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 server de-a lungul căii de conexiune.
Limită de adâncime jeton	Dimensiunea de buffer jeton maximă permisă de această politică în fiecare ruter şi server de-a lungul căii de conexiune.
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 vor fi înlăturaţi 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 port sursă care determină care aplicaţii sunt controlate de această politică.

Politici de servicii integrate (garantate)

Politicile IntServ nu afişează în monitor până când aplicaţiile nu rulează şi rezervările s-au stabilit. Dacă politicile IntServ au mai mult de o rezervare, veţi vedea mai multe intrări în monitor.

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	Rata de jeton maximă permisă de această politică în fiecare ruter şi server de-a lungul căii de conexiune.
Limită de adâncime jeton	Dimensiunea de buffer jeton maximă permisă de această politică în fiecare ruter şi server de-a lungul căii de conexiune.
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 vor fi înlăturaţi 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 port sursă care determină care aplicaţii sunt controlate de această politică.

Politici de admitere intrare

Tabela 7. Politici de admitere intrare

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 la acest server.
Cereri acceptate	Numărul total de cereri de conexiune acceptate de acest server.
Cereri aruncate	Numărul total de cereri aruncate de acest server.
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 admitere intrare (continuare)

Câmp	Descriere
Limită rată de conexiune de vârf	Rata permisă maximă la care serverul va accepta conexiuni de la reţea.
Prioritate	Prioritatea alocată fiecărei reguli încărcată în Managerul QoS.
Prioritate de coadă	Prioritatea alocată conexiunilor de intrare plasate în coada de ascultare.
Interval port destinaţie	Intervalul de port sau portul la care este destinat traficul pe server.
Adresă interfaţă	Adresă IP sau interfaţă de sistem monitorizată.
Interval adresă sursă	Intervalul de adresă IP a clienţilor care trimit cereri la server.
URI	Identitatea URI-ului este supravegheată.

Concepte înrudite

"Scenariu: Limitarea traficului de browser" la pagina 27
Puteţi utiliza calitatea serviciilor (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. Acest exemplu le arată pe cele două fiind folosite împreună.

"Scenariu: Limitarea conexiunilor de intrare" la pagina 35
Dacă trebuie să controlaţi cererile de conexiuni de intrare făcute la server, folosiţi o politică de admitere a intrării.

"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. Sunt două tipuri de politici de servicii integrate de creat: încărcare garantată şi controlată. În acest exemplu, este folosit serviciul garantat.

"Scenarii" la pagina 27
Aceste scenarii de politicii de QoS vă pot ajuta să înţelegeţi de ce şi cum să folosiţi QoS.

"Monitorizarea tranzacţiilor server" la pagina 62
Cu monitorizarea QoS puteţi să verificaţi că politicile QoS funcţionează aşa cum doriţi dumneavoastră ca ele să funcţioneze.

"Scenariu: Monitorizarea statisticilor curente de reţea" la pagina 45
În vrăjitori sunteţi rugat să setaţi limite de performanţă. Acestea sunt valori care nu pot fi recomandate, deoarece sunt bazate pe cerinţe de reţea individuale.

Depanarea QoS

QoS furnizează mai multe metode de depanare a problemelor QoS.

Urmărire de comunicaţii

Serverul dumneavoastră furnizează o urmărire de comunicaţii pentru a colecta datele dintr-o linie de comunicaţii, cum ar fi o interfaţă de reţea LAN sau o reţea WAN. 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.

Activare QoS pe server

Primul lucru care se verifică, dacă nu porneşte serverul QoS, este dacă QoS este activat pe server. Când configuraţi politicile pentru prima dată, vrăjitorul de Configurare iniţială activează automat QoS pe server. Oricum, dacă această valoare a fost modificată, din orice motiv, serverul nu va porni.

Pentru a verifica dacă QoS este activat pe server, faceţi următorii paşi:

1. În Navigatorul iSeries, expandaţi serverul dumneavoastră → **Reţea** → **Politici IP**.
2. Faceţi clic dreapta **Calitatea serviciului** şi selectaţi **Configurare**.
3. Când apare interfaţa QoS, 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
   Ori de câte ori aveţi două politici ce se suprapun, contează ordinea fizică a politicilor în Navigatorul iSeries.

Jurnal de politici QoS

QoS include o funcţie de jurnalizare. Jurnalizarea vă permite să urmăriţi acţiunile politicii QoS, cum ar fi când o politică este adăugată, înlăturată sau modificată.

Se creează un jurnal al acţiunilor politicii atâta timp cât aveţi jurnalizarea pornită. 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. Folosind aceste jurnale, creaţi un fişier general pe serverul iSeries. 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 Navigatorul iSeries. Pentru a vizualiza jurnalele, trebuie să folosiţi interfaţa pe bază de caractere.

Pentru a porni sau opri jurnalizarea, urmaţi aceşti paşi:

1. În NavigatoruliSeries, expandaţi serverul 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. Deselectaţi caseta Rulare jurnalizare pentru a opri jurnalizarea.

Notă: Dacă serverul este deja pornit înainte să efectuaţi paşii de mai sus, trebuie să vă opriţi şi să reporniţi serverul. Odată ce jurnalizarea a fost pornită există două căi de a o activa. Puteţi opri şi reporni serverul sau puteţi realiza o actualizare de server. Oricare din acestea va reciti fişierul policy.conf şi va căuta atributul de jurnalizare.

Vizualizarea intrărilor de jurnal pe monitor

Pentru a vizualiza istoricul, urmaţi aceşti paşi:

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 vizualizaţi.

Vizualizarea intrărilor de jurnal prin fişierul de ieşire

Dacă doriţi să vedeţi intrările de jurnal formatate într-un folder, vizualizaţi fişierul MODEL.OUT în directorul QUSRSYS . Copiind intrările de jurnal în fişierul de ieşire, puteţi vizualiza uşor intrările folosind utilităţi de coadă cum ar fi Query/400 sau SQL. Vă puteţi scrie şi propriul program HLL pentru a procesa intrările în fişierul de ieşire.

Pentru a copia intrările de jurnal QoS în fişierul de ieşire furnizat de sistem:

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*)

Istoric joburi server QoS

Atunci când întâlniţi probleme cu politicile dumneavoastră QoS, analizaţi istoricele de joburi ale iSeries. Istoricul de joburi conţine mesaje de eroare şi alte informaţii înrudite cu QoS.

Doar un singur job QoS, QTOQSRVR, rulează în subsistemul QSYSWRK. Puteţi vizualiza jurnalele de joburi de server QoS vechi şi actuale din Navigatorul iSeries.

Pentru a vizualiza istoricul, urmaţi aceşti 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.

Verifica fişierul spool pentru o eroare

Pentru verifica fişierul spool de 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 ecranul Lucru cu fişiere de mesaj, introduceţi următoarele informaţii şi apăsaţi Enter.

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

7. În ecranul Lucru cu fişiere de mesaj, selectaţi **opţiunea 5** pentru a afişa fişierul de mesaj pe care doriţi să-l vizualizaţi 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.

    Apare o descriere detaliată a mesajului.

Monitorizarea tranzacţiilor server

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 monitorizarea la analizarea traficului IP prin server. Aceasta vă ajută să determinaţi unde apare congestionarea în reţea. Monitorizarea QoS vă poate ajuta să continuaţi monitorizarea reţelei astfel încât să vă puteţi ajusta politicile după cum este necesar.

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 care sunt valorile potrivite pentru dumneavoastră, aţi putea dori să folosiţi monitorizarea chiar înainte de a porni orice politici 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 o politică de monitorizare exemplu care va identifica cum se comportă traficul actual.

Depanare probleme de performanţă

Puteţi folosi monitorizarea şi pentru a depana probleme. Utilizând ieşirea monitorizării, puteţi determina dacă parametrii alocaţi politicii sunt urmaţi. 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 de intrare 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.

Pentru nişte exemple de ieşiri de monitorizare, vizitaţi Scenarii QoS sau vizualizaţi toate câmpurile monitorizate în monitorizare.

Concepte înrudite

“Planificarea pentru QoS” 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” la pagina 27
Aceste scenarii de politicii de QoS vă pot ajuta să înţelegeţi de ce şi cum să folosiţi QoS.

Referinţe înrudite

“Monitorizarea QoS” la pagina 55
Puteţi folosi monitorizarea la analizarea traficului IP prin server.

Informaţii înrudite

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

Urmărirea aplicaţiilor TCP

Folosiţi urmărirea QoS pentru a lucra cu funcţiile de urmărire şi pentru a vizualiza buffer-ul urmărire curentă.

Pentru a rula urmărirea pe server, tastaţi TRCTCPAPP (comanda Trace TCP/IP Application) de la o interfaţă linie de comandă.

Acesta este un exemplu al selecţiei de urmărire de efectuat:

```
Aplicaţie TCP/IP ...........> *QOS
Setare opţiuni de urmărire.........> *ON
Memorie maximă 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 apare în interfaţa bazată pe 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 4MB. Pentru a specifica dimensiunea implicită, selectaţi *APP.

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

Urmărire întreaga acţiune

***WRAP**

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

***STOPTRC**

Opreşte colectarea informaţiilor când sistemul atinge spaţiul de disc maxim.

Liste de argumente

Specifică care niveluri de erori şi conţinuturi vor fi 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 urmărit, asiguraţi-vă că toate atributele sunt conţinute între o singură pereche 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, poate apare o eroare de obiect deoarece o operaţie de server a întâlnit un rezultat 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 IntServ. Folosiţi aceasta dacă determinaţi că problema este înrudită cu IntServ.

Conţinut = Diffserv ('c=d')
Urmăreşte doar operaţiile DiffServ. Folosiţi aceasta dacă determinaţi că problema este înrudită cu DiffServ.

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

Pagina de ieşire 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

Descriere comandă TRCTCPAPP (Trace TCP/IP Application)

Exemple: Citire ieşire urmărire

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 căutat este dacă conexiunea RSVP a fost refuzată, deoarece nu a fost găsită o politică pentru acea conexiune. 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*, cel mai important mesaj arată dacă serverul a încărcat o regulă de politică sau dacă a apărut o eroare în fişierul de configurare 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 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 QoS

Listate mai jos sunt IBM Redbooks (în format PDF), site-uri Web şi subiectele Centrului de informare legate de subiectul QoS. Puteţi citi sau tipări oricare din PDF-uri.

RFC-uri (Request for Comments) 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 Servicii integrate IETF.
- **RFC 2474.**

  Acest RFC explică definiţia pentru DS Field (Differentiated Services Field).
- **RFC 2475.**

  Acest RFC explică arhitectura serviciilor diferenţiate.

Pentru a vedea RFC-urile listate anterior, vizitaţi RFC Index Search Engine localizat pe situl Web RFC Editor .

IBM Redbooks

- iSeries IP Networks: Dynamic! (aproximativ 16 589 KB). Aceasta este cea mai recentă carte roşie de reţele IP. Vă arată cum să proiectaţi o reţea IP care se auto-configurează, este tolerantă la greşeală şi eficientă în operare. În plus faţă de multe funcţii, explică atât teoria din spatele QoS cât şi implementarea ei pe iSeries. Veţi găsi, de asemenea, mai multe scenarii cu instrucţiuni pas-cu-pas.
- TCP/IP Mai multe lucruri interesante decât niciodată (aproximativ 10 035 KB). Acest manual oferă scenarii exemplu care demonstrează soluţii comune cu configuraţii exemplu. Informaţiile din acest manual vă ajută să plănuiţi, instalaţi, modificaţi, configuraţi şi depanaţi TCP/IP pe serverul dumneavoastră iSeries. 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. Veţi găsi QoS *Partea 3. Concepte avansate şi tehnologii noi* sub Capitolul 22.

Alte informaţii

- Servicii de directoare (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 auditate pe care detectarea de intruziuni le pune la dispoziţie pentru a apăra reţeaua iSeries de astfel de atacuri.

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 repectării termenilor şi condiţiilor, iar în unele cazuri cu plata unor taxe.

Programul licenţiat descris în aceste informaţii şi toate materialele licenţiate disponibile pentru el sunt furnizate de către IBM conform termenilor din Contractul IBM cu Clientul, Contractul IBM International Program License Agreement, Contractul IBM de licenţă pentru Codul Maşină sau orice acord echivalent dintre 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 publicaţie Quality of Service (QoS) certifică Interfeţele de programare proiectate care permit clientului să scrie programe pentru a obţine serviciile IBM i5/OS.

Mărci comerciale

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

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

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 lucrări 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 publicaţii, nici să reproduceţi, să distribuiţi sau să afişaţi aceste publicaţii sau o porţiune a lor în afara întreprinderii dumneavoastră fără consimţământul explicit de la IBM.

În afara celor acordate expres prin această permisiune, nu se acordă nici o altă permisiune, licenţă sau drept, explicite sau implicite, pentru aceste publicaţii sau orice informaţii, date, software sau alte elemente pe care le conţin şi care reprezintă proprietate intelectuală.

IBM îşi păstrează dreptul de a retrage permisiunile acordate aici oricând, la discreţia sa, dacă folosirea publicaţiilor este în detrimentul intereselor sale sau, după cum este determinat de IBM sau dacă instrucţiunile de mai sus nu sunt urmate corespunzător.

Nu puteţi descărca, exporta sau reexporta aceste informaţii decât respectând integral legile şi reglementările în vigoare, precum şi legile şi reglementările din Statele Unite privind exportul.

IBM NU OFERĂ NICI O GARANŢIE CU PRIVIRE LA CONŢINUTUL ACESTOR PUBLICAŢII. PUBLICAŢIILE 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.