System i

Spájanie počítačov prostredníctvom sietí Kvalita služby

Verzia 6, vydanie 1

System i

Spájanie počítačov prostredníctvom sietí Kvalita služby

Verzia 6, vydanie 1

Poznámka

Pred použitím týchto informácií a produktu, ktorý podporujú, si prečítajte informácie v časti “Právne informácie”, na strane 67.

Toto vydanie sa vzťahuje na verziu 6, vydanie 1, modifikácia 0 systému IBM i5/OS (číslo produktu 5761-SS1) a na všetky následné vydania a modifikácie, pokiaľ nie je v nových vydaniach uvedené inak. Táto verzia sa nedá spustiť na počítačoch s redukovanou inštrukčnou sadou (RISC), ani na modeloch CISC.

Obsah

Kvalita služby

Riešenie i5/OS kvality služieb (QoS) dovoľuje, aby si politiky vyžiadali prioritu a šírku pásma v sieti pre sieťové aplikácie TCP/IP.

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

Priorita paketov je pre vás významná, ak odosielate aplikácie, ktoré potrebujú predvídateľné a spoľahlivé výsledky, ako napríklad multimédiá. Politiky QoS dokážu riadiť prioritu paketov a tiež obmedziť údaje odchádzajúce z vášho systému, spravovať požiadavky na pripojenie a riadiť záťaž systému. Aby bolo možné aktivovať politiku detekcie narušenia bezpečnosti systému, server QoS musí byť spustený.

PDF súbor pre kvalitu služieb

Tieto informácie môžete zobraziť alebo vytlačiť ako súbor PDF.

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

Uloženie súborov PDF

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

1. Pravým tlačidlom myši kliknite na odkaz PDF vo vašom prehliadači.
2. Kliknite na voľbu, ktorá ukladá dokument PDF lokálne.
3. Navigujte k adresáru, do ktorého chcete uložiť dokument PDF.
4. Kliknite na **Uložiť**.

Stiahnutie programu Adobe Reader

Na zobrazenie a tlač týchto PDF súborov musíte mať nainštalovaný Adobe Reader. Voľne dostupnú verziu tohto programu si môžete stiahnuť na stránkach Adobe (www.adobe.com/products/acrobat/readstep.html)  .

Súvisiaci odkaz

“Informácie súvisiace s kvalitou služieb” na strane 65

Dokumenty Request for Comments, publikácie IBM Redbooks a ďalšie témy informačného centra obsahujú ďalšie informácie súvisiace s témami kvality služieb. Súbory PDF môžete zobraziť alebo stiahnuť.

Základné pojmy

Skôr ako začnete používať kvalitu služieb (QoS), potrebujete porozumieť základným pojmom a konceptom QoS. Pomôže vám to zistiť, či služba spĺňa vaše potreby.

Aby ste mohli realizovať QoS, nakonfigurujte politiky pomocou sprievodcov v System i Navigator. *Politika* je sada pravidiel, ktorá určuje akciu. Politika v zásade určuje, ktorý klient, aplikácia či plán (ktorý označíte) musí prijať určitú službu. Konfigurovať môžete nasledujúce typy politík:

- Diferencovaná služba
- Integrovaná služba
- Povolenie vstupu

Diferencovaná služba a *integrovaná služba* sa považujú za politiky výstupnej šírky pásma. Výstupné politiky obmedzujú údaje opúšťajúce vašu sieť a pomáhajú riadiť záťaž systému. Rýchlosti, ktoré nastavíte pre výstupnú politiku, riadia, ktoré údaje budú a ktoré nebudú v systéme obmedzené, a akým spôsobom. Oba typy výstupnej politiky môžu vyžadovať zmluvu o dohodnutej úrovni poskytovanej služby (SLA) s vaším poskytovateľom internetových služieb (ISP).

Politiky *povolenia vstupu* riadia požiadavky na pripojenie, ktoré do vašej siete prichádzajú z externých zdrojov. Vstupné politiky nie sú závislé od úrovne služieb poskytovanej vašim ISP. Aby ste určili, ktorú politiku potrebujete použiť, zvážte dôvody, prečo chcete použiť QoS a posúďte úlohu vášho systému.

Jeden z najdôležitejších prvkov realizovania QoS je samotný operačný systém. Potrebujete nielen rozumieť konceptom QoS, ale musíte tiež poznať úlohu, akú v koncepcii QoS zohráva váš operačný systém. Operačný systém i5/OS môže fungovať len ako klient alebo server, no nie ako smerovač. Napríklad váš operačný systém, fungujúci ako klient, môže použiť rôzne politiky diferencovaných služieb, aby zaistil, že požiadavky na informácie iných systémov dostanú v sieti vyššiu prioritu. Operačný systém fungujúci ako server môže použiť politiku povolenia vstupu a obmedziť požiadavky URI (Uniform Resource Identifier) prijaté serverom.

Súvisiace koncepty

“Dohodnutá úroveň poskytovaných služieb” na strane 48
Táto téma sa venuje niektorým dôležitým aspektom dohodnutej úrovne poskytovaných služieb (SLA), ktoré môžu vplývať na implementáciu kvality služieb (QoS). QoS je sieťové riešenie. Ak chcete získať sieťovú prioritu mimo vašej súkromnej siete, pravdepodobne potrebujete s vaším poskytovateľom internetových služieb (ISP) uzavrieť zmluvu o dohodnutej úrovni poskytovaných služieb.

Súvisiaci odkaz

“Informácie súvisiace s kvalitou služieb” na strane 65
Dokumenty Request for Comments, publikácie IBM Redbooks a ďalšie témy informačného centra obsahujú ďalšie informácie súvisiace s témami kvality služieb. Súbory PDF môžete zobraziť alebo stiahnuť.

Diferencované služby

Toto je prvý typ politiky výstupnej šírky pásma, ktorú môžete vytvoriť vo vašom operačnom systéme. Diferencovaná služba rozdeľuje vašu premávku do tried. Ak chcete uplatňovať politiku diferencovanej služby, musíte určiť, ako chcete klasifikovať vašu sieťovú prevádzku a ako chcete zaobchádzať s jednotlivými triedami.

Súvisiace koncepty

“Rozšírenia API QoS sendmsg()” na strane 22
Funkcia sendmsg() sa používa na odoslanie údajov, pre podporné údaje, prípadne oboje prostredníctvom pripojeného alebo nepripojeného soketu.

“Limity bloku tokenov a šírky pásma” na strane 9
Limity pre blok tokenov a šírku pásma sú známe pod pojmom limity pre výkon. Tieto výkonové limity pomáhajú garantovať doručovanie paketov v politikách výstupnej šírky pásma u integrovanej rovnako ako diferencovanej služby.

“Trieda služby” na strane 12
Pri vytváraní politiky diferencovaných služieb alebo politiky povolenia vstupu taktiež vytvárate a používate triedu služby.

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

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

Súvisiaci odkaz

“Použitie kódových bodov na priradenie správania typu per-hop” na strane 14
Kvalita služieb (QoS) používa ponúknuté kódové body na priradenie správania typu per-hop komunikačnej prevádzke.

“Konfigurácia QoS pomocou sprievodcov” na strane 50
Ak chcete konfigurovať politiky kvality služieb (QoS), musíte použiť sprievodcov QoS, ktorí sa nachádzajú v System i Navigator.

Súvisiace informácie

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

Prioritné triedy: Klasifikácia komunikácie po sieti

Diferencovaná služba klasifikuje prevádzku do tried. Najbežnejšie triedy sú definované prostredníctvom klientskych adries IP, aplikačných portov, typov serverov, protokolov, lokálnych adries IP a rozvrhov. Všetka prevádzka, spadajúca do rovnakej triedy, sa spracúva rovnako.

Keď chcete dosiahnuť podrobnejšiu klasifikáciu, môžete pre niektoré vaše aplikácie i5/OS určiť aplikačné údaje a nastaviť rôzne úrovne služieb. Aplikačné údaje nemusíte použiť, môžu však byť užitočné, keď chcete vytvoriť klasifikáciu na nižšej úrovni. Existujú dva typy aplikačných údajov: token aplikácie a URI (jednotný identifikátor prostriedku). Keď prenášané údaje vyhovujú tokenu alebo URI, ktoré ste zadali v politike, na výstupnú odpoveď sa použije táto politika, čím výstupnej prevádzke poskytnete tú prioritu, ktorá je určená v politike diferencovanej služby.

Použitie tokenu aplikácie s politikami diferencovaných služieb

Použitie aplikačných údajov umožňuje politike reagovať na špecifické parametre (token a prioritu), ktoré aplikácia odovzdá operačnému systému prostredníctvom aplikačného programovacieho rozhrania (API) sendmsg(). Táto voľba je voliteľná. Ak nepotrebujete takúto úroveň granularity vo vašich politikách výstupu, v sprievodcovi vyberte **Všetky tokeny**. Token a prioritu aplikácie môžete zviazať s konkrétnym tokenom a prioritou, ktoré sú nastavené vo výstupnej politike. V politike sú dve miesta, kde môžete nastaviť aplikačné údaje: token a priorita.

- Čo je token aplikácie?

  Token aplikácie je znakový reťazec, ktorý reprezentuje definovaný prostriedok, napríklad myFTP. Token, ktorý zadáte v politike kvality služby (QoS), sa porovná s tokenom, ktorý poskytne daná aplikácia pre odchádzajúcu komunikáciu. Aplikáciu tento token poskytuje prostredníctvom API sendmsg(). Ak sú tokeny rovnaké, premávka aplikácie sa zahrnie do politiky diferencovaných služieb.

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

  1. V okne konfigurácie QoS kliknite pravým tlačidlom na **DiffServ** a vyberte **Nová politika**. Spustite sprievodcu.
  2. Na stránke Server Data Request zvoľte **Vybratý token aplikácie**.
  3. Ak chcete vytvoriť nový token, kliknite na **Nový**. Otvorí sa okno Nové URI.
  4. V poli **Názov** zadajte zmysluplný názov pre token aplikácie.
  5. V poli **URI** vymažte (/) a zadajte token aplikácie (reťazec nie dlhší ako 128 znakov). Napríklad, skôr myFTPapp než typický identifikátor URI.
- Čo je priorita aplikácie?

  Priorita aplikácie, ktorú zadáte, sa porovná s prioritou aplikácie, ktorú poskytne výstupná aplikácia. Aplikáciu túto prioritu poskytuje prostredníctvom API sendmsg(). Ak sú priority rovnaké, premávka aplikácie sa zahrnie do politiky diferencovaných služieb. Celá premávka definovaná v politike diferencovaných služieb bude stále prijímať prioritu udelenú celej politike.

Keď zadáte token aplikácie ako typ aplikačných údajov, potom aplikácia, ktorá tieto informácie poskytuje operačnému systému, musí byť špeciálne naprogramovaná na použitie API rozhrania sendmsg(). Toto realizuje aplikačný programátor. Platné hodnoty (token a priorita), ktoré administrátor QoS použije v politike diferencovanej služby, by mali byť uvedené v dokumentácii k aplikácii. Politika diferencovanej služby potom na komunikáciu, ktorá zodpovedá symbolu zadanému v politike, použije svoju vlastnú prioritu a klasifikáciu. Ak aplikácia nemá hodnoty zodpovedajúce hodnotám nastaveným v politike, musíte buď aktualizovať aplikáciu alebo pre politiku diferencovanej služby použiť iné parametre aplikačných údajov.

Použitie URI s politikami diferencovaných služieb

Keď vytvárate politiku diferencovanej služby, sprievodca vám umožní nastaviť systémové údaje, ako opisuje časť ″Použitie tokenu aplikácie s politikami diferencovaných služieb″. Aj keď polia v sprievodcovi od vás požadujú symbol aplikácie, môžete do nich namiesto neho zadať relatívny identifikátor URI. Znovu, toto je voliteľné. Ak nepotrebujete takúto úroveň granularity vo vašich politikách výstupu, v sprievodcovi vyberte **Všetky tokeny**. Môžete stanoviť špecifické URI nastavené vo výstupnej politike.

Relatívne URI je v skutočnosti podsada absolútneho URI (podobné starému absolútnemu URL). Pozrite si tento príklad: http://www.ibm.com/software. *http://www.ibm.com/software* segment sa považuje za absolútne URI. Segment */software* je relatívne URI. Všetky relatívne URI hodnoty musia začať s jednou lomkou (/). Nasledovné segmenty sú platnými príkladmi relatívnych identifikátorov URI:

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

Skôr, než nastavíte politiku diferencovanej služby, ktorá používa identifikátory URI, musíte sa postarať o to, aby aplikačný port priradený tomuto URI zodpovedal inštrukcii Listen povolenej v konfigurácii webového servera Apache pre fast response cache (FRCA). Ak chcete zmeniť alebo zobraziť port pre váš HTTP server, pozrite si časť Správa adries a portov vášho HTTP servera (s nainštalovaným webovým serverom Apache) .

FRCA identifikuje URI pre každú odchádzajúcu odozvu HTTP. Porovná URI súvisiace s odchádzajúcou odpoveďou s URI definovaným v každej politike diferencovaných služieb. Prvá politika s reťazcom tokenu (URI), ktorá najlepšie vyhovuje URI, ktoré identifikovala FRCA, sa použije na všetky odpovede pre dané URI.

Súvisiace koncepty

“Rozšírenia API QoS sendmsg()” na strane 22
Funkcia sendmsg() sa používa na odoslanie údajov, pre podporné údaje, prípadne oboje prostredníctvom pripojeného alebo nepripojeného soketu.

Nastavenie priorít: Ako zaobchádzať s triedami

Po klasifikovaní prevádzky musíte určiť aj správanie per-hop pre diferencovanú službu a zadefinovať tak, ako sa má spracovať prevádzka.

Operačný systém používa bity v hlavičke IP na identifikáciu úrovne služieb IP paketu. Smerovače a prepínače alokujú svoje prostriedky na základe informácií skokového správania v oktetovom poli typu služby v záhlaví IP. Typ oktetového poľa typu služby bol nanovo definovaný v dokumente Request for Comments (RFC) 1349 a v operačnom systéme OS/400 V5R1. *Správanie per-hop* je smerovacie správanie, ktoré paket prijme v uzle siete. Reprezentuje ho hodnota, ktorú poznáme pod názvom *kódový bod*. Pakety môžu byť označené buď v operačnom systéme alebo v iných častiach siete, napríklad v smerovači. Aby si paket uchoval požadovanú službu, každý sieťový uzol musí vedieť o diferencovanej službe. To znamená, že zariadenie musí byť schopné presadiť správania vykonávané po skokoch. Aby sieťový uzol mohol presadzovať spracovávanie podľa skokového správania, musí byť tento sieťový uzol schopný používať plánovanie frontu a riadenie priorít odchádzajúcej komunikácie. Pozrite si “Udržiavače prevádzky” na strane 5, kde zistíte viac o tom, čo znamená vedieť o diferencovanej službe.

Ak váš paket prejde cez smerovač alebo prepínač, ktorý si nie je vedomý diferencovanej služby, paket v takomto smerovači stratí svoju úroveň služby. Bude spracovaný, môže sa však oneskoriť. Na vašom systéme môžete použiť preddefinované kódové body správania per-hop, alebo môžete zadefinovať svoje vlastné kódové body. Vlastné kódové body nemôžete vytvoriť mimo vašej súkromnej siete. Ak neviete, ktoré kódové body máte priradiť, pozrite si “Použitie kódových bodov na priradenie správania typu per-hop” na strane 14.

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

Diferencovaná služba sa používa aj na obmedzenie prevádzky odchádzajúcej zo systému. Znamená to, že váš systém skutočne používa diferencovanú službu na obmedzenie výkonu. Obmedzovanie menej kritickej aplikácie umožňuje kľúčovým aplikáciám, aby opustili vašu privátnu sieť najskôr. Keď pre túto politiku vytvárate triedu služieb, ste vyzvaný nastaviť rôzne limity na vašom systéme. Medzi ohraničenia výkonu patrí veľkosť bloku tokenov, limit maximálnej rýchlosti a limit priemernej rýchlosti. Podrobnejšie informácie o týchto ohraničeniach nájdete v témach pomoci kvality služieb (QoS) v System i Navigator.

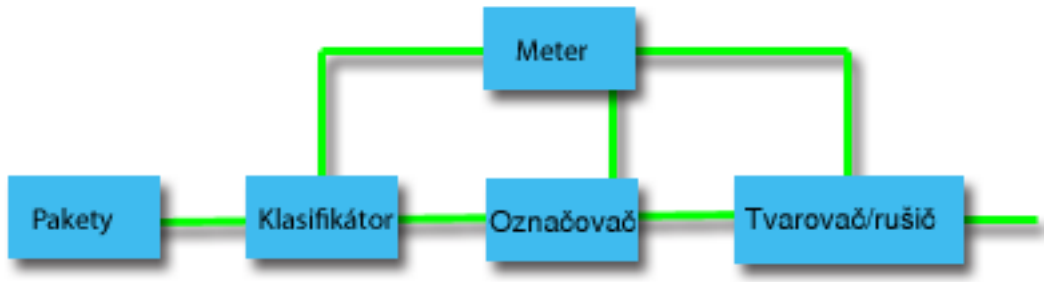
Udržiavače prevádzky

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

Ak má sieťové zariadenie všetky upravovače prevádzky, označuje sa ako vedomé si diferencovaných služieb.

Poznámka: Tieto hardvérové požiadavky nie sú špecifické pre produkty System i. Tieto výrazy, použité v rozhraní QoS, nemôžete vidieť, pretože systém nedokáže riadiť externý hardvér. Mimo súkromnej siete musí mať hardvér schopnosť spracúvať všeobecné požiadavky QoS. Pozrite sa do manuálov konkrétnych zariadení a uistite, že vaše zariadenia vyhovujú požiadavkám diferencovanej služby. Pred implementáciou politík by ste si mali preštudovať všeobecné pojmy, koncepty a nevyhnutné predpoklady QoS.

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



Obrázok 1. Upravovače prevádzky

Nasledujúce informácie podrobne opisujú jednotlivé upravovače prevádzky:

Klasifikátory

Klasifikátory paketov vyberajú pakety v toku prevádzky na základe obsahu v IP hlavičke paketu. Operačný systém i5/OS definuje dva typy klasifikátorov. Agregát správania triedi pakety výlučne podľa kódového bodu diferencovaných služieb. Viacpoľový klasifikátor vyberá pakety na základe hodnoty kombinácie jedného alebo viacerých polí hlavičky, napríklad zdrojovej adresy, cieľovej adresy, poľa Diferencované služby, ID protokolu, zdrojového portu, jednotného identifikátora prostriedku (URI), typu servera a čísla cieľového portu.

Merače

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

Značkovače

Značkovače paketov nastavujú pole Diferencované služby. Značkovač môžete nakonfigurovať tak, aby všetky pakety označil jedným kódovým bodom alebo skupinou kódových bodov, ktorá sa používa na výber správania typu per-hop.

Tvarovače

Tvarovače oneskoria niektoré, alebo všetky pakety v toku premávky, aby zosúladili tok s profilom premávky. Tvarovač má obmedzenú veľkosť vyrovnávacej pamäte a smerovače môžu pakety vymazať, ak na uchovávanie oneskorených paketov nie je dosť miesta.

Prerušovače

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

Súvisiace koncepty

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

Integrované služby

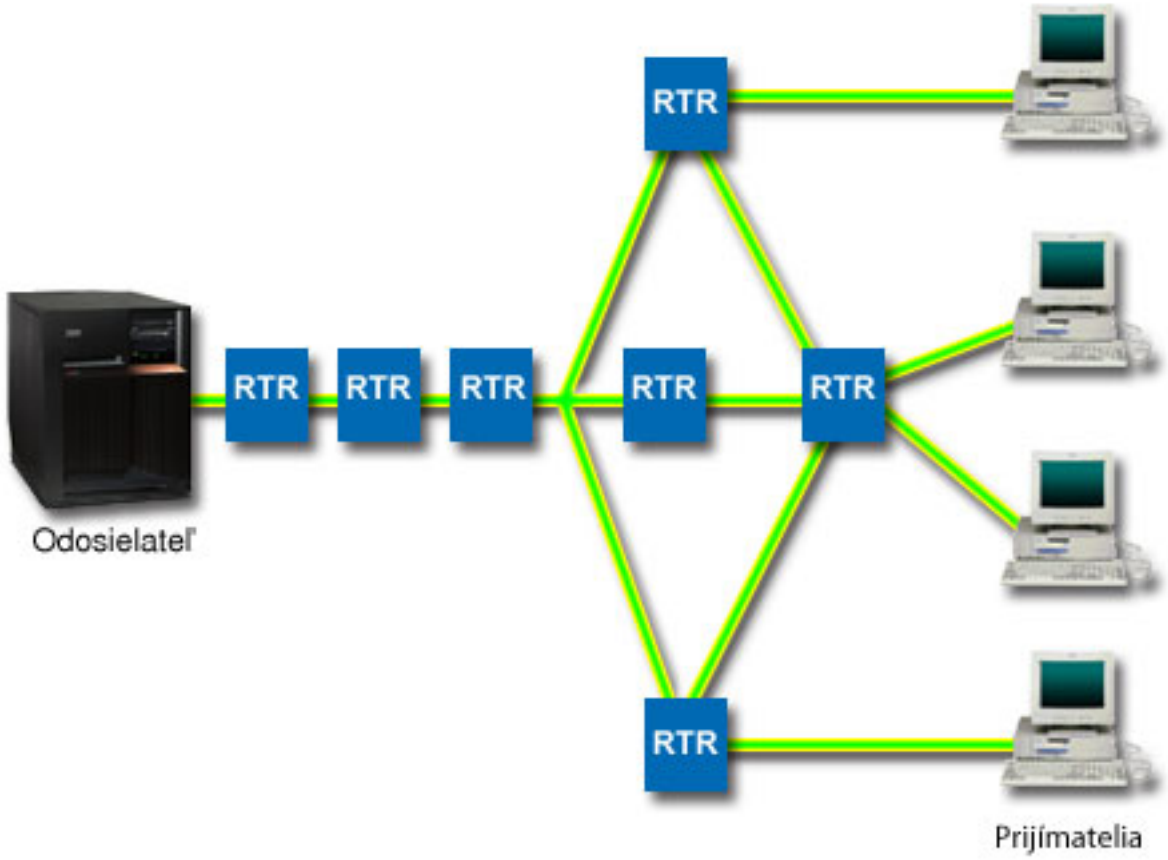
Druhý typ politiky výstupnej šírky pásma, ktorú môžete vytvoriť vo vašom operačnom systéme, je politika integrovanej služby. Integrovaná služba poskytuje IP aplikáciám schopnosť požadovať a vyhradiť si frekvenčné pásmo pomocou protokolu ReSerVation Protocol (RSVP) a aplikačných programových rozhraní kvality služby (QoS).

Politiky integrovaných služieb používajú protokol RSVP a API rozhranie Resource Reservation Setup Protocol API (RAPI) (alebo API rozhranie soketu qtoq) na garanciu komplexného pripojenia. Ide o najvyššiu úroveň služby, ktorú môžete stanoviť; súčasne je to aj najzložitejšia služba.

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

Pred odoslaním údajov integrovaná služba rezervuje prostriedky pre príslušnú politiku. Smerovače dostávajú signály pred dátovým prenosom a sieť v skutočnosti schvaľuje a riadi (koniec-ku-koncu) dátový prenos na základe politiky. *Politika* je sada pravidiel, ktorá určuje akciu. V skutočnosti to je kontrolný zoznam prijatia. Požiadavka šírky pásma prichádza v rezervácii od klienta. Ak všetky smerovače po ceste súhlasia s požiadavkami, ktoré prichádzajú od klienta, požiadavka sa dostane do systému a do politiky integrovanej služby. Ak požiadavka spadá do obmedzení definovaných politikou, QoS server udelí povolenie pre RSVP pripojenie a potom vyhradí šírku pásma pre aplikáciu. Rezervácia sa vykoná prostredníctvom protokolu RSVP a API rozhrania RAPI, alebo prostredníctvom protokolu RSVP a API rozhraní soketov qtoq QoS.

Každý uzol, cez ktorý prechádza vaša prevádzka, musí byť schopný používať protokol RSVP. Smerovače poskytujú QoS prostredníctvom nasledovných funkcií riadenia komunikačnej prevádzky: plánovač paketov, klasifikátor paketov a riadenie príjmu. Schopnosť vykonávať túto kontrolu premávky sa často označuje ako podporujúce RSVP. Následne je najdôležitejšia časť implementácie politík integrovaných služieb schopná kontrolovať a predpovedať zdroje vo vašej sieti. Aby sa získali predpovedateľné údaje, každý uzol v sieti musí podporovať RSVP. Napríklad, ak je vaša premávka smerovaná na základe prostriedkov, poznačte si, ktoré cesty majú smerovače podporujúce RSVP. Prechodové smerovače, ktoré nemajú povolený protokol RSVP, môžu spôsobiť nepredvídateľné prevádzkové problémy. Pripojenie je aj tak uskutočnené, ale výkon požadovaný aplikáciou nie je zaručený smerovačom. Nasledujúca schéma ukazuje, ako funkcia integrovanej služby logicky pracuje.



Obrázok 2. RSVP cesta medzi klientom a serverom

Aplikácia na serveri podporujúca RSVP, na predchádzajúcom obrázku zobrazená ako odosielateľ, zachytí požiadavku na pripojenie od klientov alebo prijímateľov. Ako odpoveď vydá príkaz PATH pre klienta. Tento príkaz bude zadaný cez API rozhrania RAPI alebo API rozhrania soketov qtoq QoS, pričom obsahuje informácie o IP adrese smerovača (RTR). Príkaz PATH obsahuje informácie o dostupných prostriedkoch na serveri a o smerovačoch v ceste, a tiež informácie o komunikačnej ceste medzi serverom a klientom. Aplikácia podporujúca RSVP na klientovi potom pošle príkaz RESV späť po sieti, aby informovala server, že boli vyhradené sieťové prostriedky. Tento príkaz vykonáva rezerváciu na základe informácií smerovača z príkazu PATH. Server a všetky smerovače pozdĺž cesty rezervujú zdroje pre RSVP pripojenie. Keď server prijme príkaz RESV, aplikácia začne prenášať dáta na klienta. Dáta sú prenášané pozdĺž rovnakej cesty, ako rezervácia. Opäť to dokazuje dôležitosť schopnosti smerovačov vykonávať rezervácie pre úspešnosť vašich politík.

Integrovaná služba nie je určená pre krátkodobé RSVP pripojenia, napríklad HTTP. Samozrejme záleží na vašom uvážení. Len vy môžete rozhodnúť, čo je pre vašu sieť najlepšie. Zvážte, ktoré oblasti a aplikácie majú problémy s výkonom a potrebovali by QoS. Aplikácie používané v politike integrovanej služby musia byť schopné použiť protokol RSVP. Zo začiatku váš operačný systém i5/OS nemá k dispozícii žiadne aplikácie podporujúce RSVP, preto mu musíte takúto aplikáciu poskytnúť.

Ako pakety prichádzajú a pokúšajú sa odísť z vašej siete, operačný systém určuje, či má dosť prostriedkov na odoslanie paketu. Toto prijatie je určené množstvom miesta v bloku symbolu. Ručne nastavte počet bitov povolených pre váš blok tokenov, nastavte limity šírky pásma a rýchlosti tokenov a nastavte maximálny povolený počet pripojení vo vašom systéme. Týmto hodnotám sa hovorí výkonové limity. Pokiaľ pakety splnia tieto limity, budú odoslané. V integrovaných službách má každé pripojenie vyhradené svoj vlastný blok symbolu.

Integrovaná služba, využívajúca diferencované označenia služieb

Ak si nie ste istý, či celá sieť dokáže garantovať RSVP pripojenie, i tak môžete vytvoriť politiku integrovanej služby. Ak však sieťové prostriedky nedokážu použiť RSVP, pripojenie nemôže byť garantované. V takejto situácii budete možno chcieť v politike použiť kódový bod. Kódový bod sa obvykle používa v politikách diferencovaných služieb na priradenie triedy služieb prevádzke. Aj keď pripojenie nemôže byť garantované, tento kódový bod sa pokúsi získať pre pripojenie určitú prioritu.

Súvisiace koncepty

"API rozhrania kvality služieb" na strane 16
Táto téma obsahuje informácie o protokoloch a rozhraniach API, a tiež požiadavky na smerovač, ktorý je povolený pre protokol ReSerVation (RSVP). Medzi rozhrania API kvality služieb (QoS) patrí API rozhranie RAPI, API rozhranie soketu qtoq, sendmsg() a API rozhrania monitora.

"Integrovaná služba, využívajúca označenia diferencovaných služieb" na strane 10
V politike integrovanej služby môžete použiť označenia diferencovaných služieb, aby ste zachovali prioritu paketov prenášaných v zmiešanom prostredí.

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

"Scenár: Dedikované doručenie (IP telefónia)" na strane 41
Ak potrebujete vyhradené doručenie a chcete vyžadovať rezerváciu, použijete politiku integrovaných služieb. Môžete vytvoriť dva typy politík integrovaných služieb: garantované a s riadeným zaťažením. V tomto príklade sa používa garantovaná služba.

Funkcia kontroly premávky

Funkcie riadenia prevádzky sa vzťahujú len na integrovanú službu a nie sú špecifické pre produkty System i.

Tieto výrazy, použité v rozhraní kvality služieb (QoS), nemôžete vidieť, pretože server nedokáže riadiť externý hardvér. Mimo súkromnej siete musí mať hardvér schopnosť spracúvať všeobecné požiadavky QoS. Všeobecné požiadavky na smerovač pre politiky integrovaných služieb sú popísané v nasledujúcej časti. Pred implementáciou politík vám odporúčame preštudovať si všeobecné pojmy, koncepty a nevyhnutné predpoklady QoS.

Aby ste dosiahli predvídateľné výsledky, v celej ceste prevádzky potrebujete mať hardvér, ktorý je povolený pre ReSerVation Protocol (RSVP). Smerovače musia mať určité funkcie na riadenie prevádzky, aby mohli používať RSVP. Označuje sa to ako povolené pre RSVP alebo povolené pre QoS. Pamätajte na to, že rola vášho operačného systému je buď klient alebo server. V tomto prípade ho nie je možné použiť ako smerovač. V príručkách k vašim sieťovým zariadeniam si overte, či dokážu spracovať požiadavky QoS.

Funkcie riadenia prevádzky obsahujú tieto funkcie:

Plánovač paketov
Plánovač paketov spravuje posielanie paketov ďalej v závislosti na informáciách v hlavičke IP. Plánovač paketov zaručuje, aby doručenie paketov zodpovedalo parametrom, ktoré ste nastavili vo vašej politike. Plánovač vstupuje do platnosti tam, kde sa pakety zoraďujú vo fronte.

Triedič paketov
Triedič paketov na základe informácií v IP hlavičke identifikuje, ktorý paket z IP toku získa vyššiu úroveň služby. Každý prichádzajúci paket je triedičom zaradený do príznačnej triedy. So všetkými paketmi, ktoré sú zaradené v tej istej triede, sa zaobchádza rovnako. Táto úroveň služby vychádza z informácií, ktoré zadáte v politike.

Riadenie vstupu
Riadenie vstupu obsahuje rozhodovací algoritmus, pomocou ktorého smerovač určuje, či je k dispozícii dostatok smerovacích prostriedkov na prijatie požadovanej QoS pre nový tok. Ak nie je dostatok prostriedkov, je nový tok zamietnutý. Ak je tok akceptovaný, vyhradí smerovač požadovaný QoS priradením plánovača a triediča paketov. Kontrola vstupu sa na každom smerovači objavuje zároveň s cestou rezervovania.

Súvisiace koncepty

“API rozhrania kvality služieb” na strane 16
Táto téma obsahuje informácie o protokoloch a rozhraniach API, a tiež požiadavky na smerovač, ktorý je povolený pre protokol ReSerVation (RSVP). Medzi rozhrania API kvality služieb (QoS) patrí API rozhranie RAPI, API rozhranie soketu qtoq, sendmsg() a API rozhrania monitora.

Súvisiaci odkaz

“Informácie súvisiace s kvalitou služieb” na strane 65
Dokumenty Request for Comments, publikácie IBM Redbooks a ďalšie témy informačného centra obsahujú ďalšie informácie súvisiace s témami kvality služieb. Súbory PDF môžete zobraziť alebo stiahnuť.

Typy integrovaných služieb

Sú dva typy integrovaných služieb: riadené zaťaženie a garantovaná služba.

Riadené zaťaženie

Služba riadeného zaťaženia podporuje aplikácie, ktoré sú veľmi citlivé na preplnené siete, napríklad aplikácie bežiace v reálnom čase. Aplikácie musia tiež tolerovať malé množstvá strát a oneskorenia. Ak aplikácia používa službu riadeného zaťaženia, jej výkon nebude trpieť zvýšením zaťaženia siete. Premávku bude poskytovať služba, ktorá pripomína normálnu premávku v sieti za menej náročných podmienok.

Smerovače musia zaistiť, aby služba riadeného zaťaženia získala primeranú šírku pásma a prostriedky na spracovanie paketov. Na to potrebujú, aby boli povolené pre kvalitu služieb (QoS) s podporou integrovaných služieb. Musíte skontrolovať špecifikáciu smerovača a zistiť, či QoS poskytuje prostredníctvom funkcie riadenia prevádzky. Riadenie prevádzky pozostáva z nasledujúcich komponentov: rozvrhový program paketov, klasifikátor paketov a riadenie prístupu.

Garantovaná služba

Garantovaná služba zaručuje, že pakety dorazia v stanovenej lehote. Aplikácie, ktoré potrebujú garantovanú službu, zahŕňajú systémy video a audio vysielania, ktoré používajú technológie vysielania na internete. Garantovaná služba riadi maximálne oneskorenie pri radení do frontu, aby sa pakety nezdržali viac než stanovuje lehota. Každý smerovač v ceste paketu musí poskytovať schopnosti RSVP (ReSerVation Protocol), aby zaručil dodanie. Keď priraďujete limity bloku tokenov a limity šírky pásma, definujete garantovanú službu. Garantovaná služba sa dá použiť iba v prípade aplikácií využívajúcich TCP.

Súvisiace koncepty

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

“Scenár: Dedikované doručenie (IP telefónia)” na strane 41
Ak potrebujete vyhradené doručenie a chcete vyžadovať rezerváciu, použijete politiku integrovaných služieb. Môžete vytvoriť dva typy politík integrovaných služieb: garantované a s riadeným zaťažením. V tomto príklade sa používa garantovaná služba.

Limity bloku tokenov a šírky pásma

Limity pre blok tokenov a šírku pásma sú známe pod pojmom limity pre výkon. Tieto výkonové limity pomáhajú garantovať doručovanie paketov v politikách výstupnej šírky pásma u integrovanej rovnako ako diferencovanej služby.

Veľkosť bloku tokenov

Veľkosť bloku tokenov určuje množstvo informácií, ktoré váš systém dokáže spracovať v danom čase. Keď nejaká aplikácia odosiela systémové informácie rýchlejšie, než ich systém dokáže odoslať von zo siete, vyrovnávacia pamäť sa zaplní. So všetkými dátovými paketmi presahujúcimi túto hranicu sa zaobchádza ako s paketmi mimo profilu. Politiky integrovaných služieb sú pre toto pravidlo výnimkou. Môžete zvoliť možnosť Neobmedziť, ktorá povoľuje požiadavky na pripojenia cez ReSerVation Protocol (RSVP). Pre všetky ostatné politiky môžete určiť spôsob spracovania premávky mimo profilu. Maximálna veľkosť bloku tokenov je 1 GB.

Limit rýchlosti tokenov

Limit rýchlosti tokenov určuje dlhodobú prenosovú rýchlosť alebo počet bitov za sekundu, ktoré môžu vstúpiť do siete. Politika kvality služieb (QoS) sa pozrie na požadovanú šírku pásma a porovná ju s limitmi pre rýchlosť a tok pre danú politiku. Ak požiadavka spôsobí, že systém prekročí svoj limit, systém ju odmietne. Limit rýchlosti tokenov sa používa iba na riadenie vstupu v rámci politík integrovaných služieb. Jeho hodnota môže byť od 10 Kb/s do 1 Gb/s. Môžete tiež nastaviť možnosť Neobmedziť. Ak pre rýchlosť nastavíte Neobmedziť, vytvoríte hranicu pre dostupné prostriedky.

Tip: Ak chcete určiť, aké limity sa majú nastaviť, mohli by ste zapnúť monitor. Vytvorte politiku s limitom agregovanej rýchlosti tokenov, ktorý je dosť veľký na to, aby zhromaždil väčšinu prenášaných údajov vo vašej sieti. Potom spustite zhromažďovanie údajov na tejto politike. Scenár monitorovania aktuálnej štatistiky o sieťach ukazuje jeden spôsob, ako zhromaždiť celkové rýchlosti, ktoré vaša aplikácia a sieť momentálne používajú. Prostredníctvom týchto výsledkov môžete limity náležite znížiť.

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

Súvisiace koncepty

"Diferencované služby" na strane 2
Toto je prvý typ politiky výstupnej šírky pásma, ktorú môžete vytvoriť vo vašom operačnom systéme. Diferencovaná služba rozdeľuje vašu premávku do tried. Ak chcete uplatňovať politiku diferencovanej služby, musíte určiť, ako chcete klasifikovať vašu sieťovú prevádzku a ako chcete zaobchádzať s jednotlivými triedami.

"Scenár: Monitorovanie aktuálnej sieťovej štatistiky" na strane 45
V sprievodcoch potrebujete nastaviť výkonové limity, založené na jednotlivých sieťových požiadavkách.

Integrovaná služba, využívajúca označenia diferencovaných služieb

V politike integrovanej služby môžete použiť označenia diferencovaných služieb, aby ste zachovali prioritu paketov prenášaných v zmiešanom prostredí.

Zmiešané prostredie nastane vtedy, keď sa rezervácia integrovanej služby presúva cez rôzne smerovače, ktoré nepodporujú rezervácie integrovanej služby, avšak samu integrovanú službu podporujú. Keďže vaša komunikácia prechádza rôznymi doménami s rôznymi zmluvami o dohodnutej úrovni poskytovanej služby a s rôznymi hardvérovými danosťami, môže sa stať, že nie vždy dostanete požadovanú službu.

Aby ste zmiernili tento problém, k vašej politike integrovaných služieb môžete pripojiť značku diferencovanej služby. Ak aj politika prejde smerovačom, ktorý nedokáže použiť protokol RSVP (ReSerVation Protocol), naďalej si uchová určité priority. Toto pridané označenie sa nazýva *správanie typu per-hop*.

Funkcia ″bez signalizácie″

Okrem týchto označení môžete tiež použiť funkciu bez signalizácie. Keď zvolíte túto funkciu, bezsignálové verzie API rozhraní vám umožnia napísať aplikáciu, ktorá spôsobí, že sa do operačného systému načíta RSVP pravidlo. Aplikácia vyžaduje, len aby aplikácia zabezpečujúca konverzáciu TCP/IP na strane servera podporovala RSVP. Na strane klienta sa signalizácia RSVP vykoná automaticky. Takto sa pre danú aplikáciu vytvorí spojenie prostredníctvom protokolu RSVP dokonca aj vtedy, ak na strane klienta nie je možné použiť protokol RSVP.

Funkcia bez signalizácie sa špecifikuje v politike integrovanej služby. Ak chcete zadať ″bez signalizácie″, postupujte podľa nasledovných pokynov:

1. V System i Navigator rozviňte položky ***váš systém*** → **Network** → **IP Policies**.
2. Pravým tlačidlom myši kliknite na **Quality of Service** a kliknite na **Configuration**.
3. Rozviňte **Outbound Bandwidth Policies** → **IntServ**.
4. Pravým tlačidlom myši kliknite na názov politiky integrovanej služby a vyberte **Properties**. Otvorí sa okno vlastností IntServ.
5. Zvoľte kartu **Traffic Management** a potom signalizáciu buď zakážte alebo povoľte. Takisto tam môžete upravovať rozvrh, klienta, aplikácie a manažment prevádzky.

Súvisiace koncepty

"Trieda služby" na strane 12
Pri vytváraní politiky diferencovaných služieb alebo politiky povolenia vstupu taktiež vytvárate a používate triedu služby.

"Integrované služby" na strane 6
Druhý typ politiky výstupnej šírky pásma, ktorú môžete vytvoriť vo vašom operačnom systéme, je politika integrovanej služby. Integrovaná služba poskytuje IP aplikáciám schopnosť požadovať a vyhradiť si frekvenčné pásmo pomocou protokolu ReSerVation Protocol (RSVP) a aplikačných programových rozhraní kvality služby (QoS).

Politika povolenia vstupu

Politika povolenia vstupu riadi požiadavky na pripojenie do vášho systému.

Vstupná politika sa používa na obmedzenie prevádzky, ktorá sa snaží pripojiť do vášho systému. Vstup môžete obmedziť na základe klienta, jednotného identifikátora prostriedku (URI), aplikácie alebo lokálneho rozhrania na vašom systéme. Navyše môžete zlepšiť výkon systému tým, že na vstupnú prevádzku použijete triedu služieb. Túto politiku zadefinujete pomocou sprievodcu povolením vstupu v System i Navigator.

Tri komponenty vstupnej politiky vyžadujú podrobnejšie informácie. Sú to URI na obmedzenie premávky, rýchlosti pripojenia definované v triede služby a prioritné fronty na zoradenie úspešných pripojení. Bližšie informácie nájdete v častiach "URI", "Počet pripojení" na strane 12 a "Vážené prioritné fronty" na strane 12.

URI

Uvážte použitie politiky vstupu na obmedzenie premávky HTTP pripájajúcej sa k vášmu webovému serveru. V takejto situácii môžete vytvoriť politiku prijímania prichádzajúcej komunikácie, ktorá komunikačnú prevádzku obmedzuje len pre konkrétne identifikátory URI. Rýchlosť požiadaviek o URI je súčasť riešenia, pomáhajúca chrániť servery pred ich možným zahltením. Určenie špecifických identifikátorov URI použije riadiace prvky vstupu, vychádzajúce z informácií o úrovni aplikácie, na obmedzenie požiadaviek na URI, akceptovaných serverom. Označuje sa to tiež ako riadenie pripojení na základe hlavičky, ktoré nastavuje priority pomocou identifikátorov URI.

Špecifikovanie URI umožní politike vstupu preskúmať aj obsah, nie len hlavičky paketov. Preskúmaným obsahom je názov URI. V prípade operačného systému i5/OS môžete použiť relatívny názov URI (napríklad /products/clothing).

Relatívny identifikátor URI

Relatívne URI je v skutočnosti podsada absolútneho URI (podobné starému absolútnemu URL). Pozrite si tento príklad: http://www.ibm.com/software. *http://www.ibm.com/software* segment sa považuje za absolútne URI. Segment */software* je relatívne URI. Všetky relatívne URI hodnoty musia začať s jedným lomítkom (/). Nasledovné segmenty sú platnými príkladmi relatívnych identifikátorov URI:

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

Poznámky:

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

Skôr, než nastavíte politiku pre prichádzajúcu komunikáciu, ktorá používa identifikátory URI, musíte sa postarať o to, aby aplikačný port priradený tomuto URI zodpovedal inštrukcii Listen povolenej v konfigurácii webového servera Apache pre Fast Response Cache Accelerator (FRCA). Ak chcete zmeniť alebo zobraziť port pre váš HTTP server, pozrite si časť Správa adries a portov vášho HTTP servera (s nainštalovaným webovým serverom Apache).

Počet pripojení

Súčasťou politiky povolenia vstupu je aj to, že musíte vybrať triedu služby. Táto trieda služieb definuje rýchlosť pripojení, ktorá slúži ako riadenie vstupu na obmedzenie pripojení akceptovaných systémom.

Rýchlosť pripojenia obmedzuje prijatie alebo odmietnutie nového paketu na základe priemerného počtu pripojení za sekundu a maximálneho počtu okamžitých pripojení, ktoré sú zadefinované vo vytvorenej politike. Tieto obmedzenia pripojenia tvorí limit priemernej rýchlosti a nárazový limit (prah zahltenia pripojenia), ktoré zadáte prostredníctvom sprievodcov System i Navigator. Keď požiadavka na vstupné pripojenie dorazí do operačného systému, systém zanalyzuje informácie v hlavičke paketu a určí, či je táto prevádzka zadefinovaná v politike. Systém overuje tieto informácie voči profilu obmedzení pripojenia. Ak sa paket nachádza vnútri medzných hodnôt, uloží sa do frontu.

Vyššie uvedené informácie použite po dokončení Sprievodcu povolenia vstupu. V System i Navigator môžete pri dokončovaní politiky použiť aj súvisiaci systém pomoci a zobraziť podobné informácie.

Vážené prioritné fronty

Ako súčasť riadenia vstupu môžete špecifikovať prioritu, v ktorej sa budú požiadavky o pripojenie spracúvať po vyhodnotení pomocou politík. Priradením váhy prioritnému frontu v skutočnosti riadite dobu odozvy frontu po príchode pripojenia. Ak je pripojenie zaradené do frontu, jeho spracovanie sa riadi poradím priority frontu (vysoká, stredná, nízka, prijateľná). Ak si nie ste istý, ktorú váhu máte priradiť, použite predvolené hodnoty. Súčet všetkých váh sa musí rovnať 100. Ak je napríklad pre všetky priority zadaná hodnota 25, systém bude so všetkými frontmi zaobchádzať rovnako. Predpokladajme, že zadáte nasledovné váhy: vysoká (50), stredná (30), nízka (15) a prijateľná (5). Akceptované pripojenia potom zahrňujú:

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

Súvisiace koncepty

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

"Priemerný počet okamžitých pripojení a prah zahltenia pripojenia" na strane 15
Počet okamžitých pripojení a prah zahltenia predstavujú limity pre pripojenie. Tieto limity pomáhajú obmedziť vstupné pripojenia, ktoré sa snažia vstúpiť do vášho systému. Limity pripojení sa nastavujú v triede služby, ktorá sa používa v politike povolenia vstupu.

Trieda služby

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

Politiky diferencovaných služieb a politiky povolenia vstupu zoskupujú prevádzku do tried služieb. Napriek tomu, že veľa z tohto sa uskutočňuje prostredníctvom hardvéru, vy riadite spôsob, akým sa premávka zoskupuje a akú prioritu musí premávka prijať.

Keď chcete uplatňovať kvalitu služieb (QoS), najskôr definujete politiky. Politiky určujú kto, čo, kde a kedy. Potom musíte priradiť triedu služby vašej politike. Triedy služby sú definované oddelene a politiky ich môžu používať

opakovane. Pri definovaní triedy služby špecifikujete, či je ju možné aplikovať na politiku vstupu, výstupu alebo obidva typy politík. Ak si vyberiete poslednú voľbu (vstup aj výstup), potom danú triedu služby môže používať politika diferencovaných služieb aj politika povolenia vstupu.

Nastavenia v rámci triedy služby závisia od toho, či sa trieda služby používa pre politiku prichádzajúcej komunikácie, odchádzajúcej komunikácie alebo pre obidva typy politík. Keď vytvárate triedu služby, môžete sa stretnúť s nasledovnými požiadavkami:

Označovanie kódového bodu

QoS pomocou navrhnutých kódových bodov priraďuje prevádzke správanie typu per-hop. Smerovače a prepínače používajú tieto kódové body na priradenie úrovne priority premávke. Váš systém tieto kódové body nemôže použiť, pretože nefunguje ako smerovač. Musíte stanoviť, ktoré kódové body sa majú použiť, a to na základe individuálnych potrieb vašej siete. Uvážte, ktoré aplikácie sú pre vás najdôležitejšie a ktorým politikám treba priradiť vyššiu prioritu. Najdôležitejšie je, aby boli konzistentné s vašimi označeniami, aby ste dosiahli výsledky, ktoré očakávate. Tieto kódové body predstavujú kľúčovú časť pri rozlišovaní rôznych tried prevádzky.

Meranie komunikačnej prevádzky

Na obmedzovanie komunikačnej prevádzky vo vašej sieti využíva QoS limity riadenia rýchlosti. Tieto limity sú dané nastavením veľkosti bloku tokenov, limitu špičkovej rýchlosti a limitu priemernej rýchlosti. Bližšie informácie o týchto špecifických hodnotách nájdete v časti “Limity bloku tokenov a šírky pásma” na strane 9.

Mimoprofilová komunikácia

Konečná časť triedy služieb je spracúvanie mimo profilu. Keď priradíte limity pre riadenie rýchlosti, nastavením hodnôt obmedzíte premávku. Keď premávka presiahne tieto obmedzenia, pakety sa považujú za mimo profilu. Informácie v triede služby informujú systém, či má prerušiť UDP prevádzku a zredukovať okno preťaženia TCP, tvarovať alebo preznačiť pakety mimo profilu.

Prerušenie UDP paketov alebo zredukovanie okna preťaženia TCP: Keď sa rozhodnete prerušiť a prispôsobiť pakty mimo profilu, UDP pakety budú prerušené. Okno preťaženia TCP sa však zredukuje, aby prenosová rýchlosť zodpovedala rýchlosti blokov tokenov. Počet paketov, ktoré sa v danom čase dajú poslať do siete, sa zníži a preťaženie sa zredukuje.

Oneskorenie (tvarovanie): Ak oneskoríte pakety mimo profilu, vytvarujú sa tak, aby vyhovovali vami zadefinovanej charakteristike spracovania.

Preznačiť kódovým bodom DiffServ: Ak pakety mimo profil preznačíte kódovým bodom, bude im priradený nový kódový bod. Pakety nebudú preformované, aby vyhoveli vašej charakteristike spracovania, len sa preznačia. Keď priradíte tieto inštrukcie spracovania v sprievodcovi, kliknite na Pomoc pre špecifickejšie informácie.

Priorita

Môžete stanoviť priority pre pripojenia k vášmu systému, a to pomocou politík riadenia povolenia vstupu. Môžete tak zadefinovať poradie, v ktorom bude váš systém spracúvať dokončené pripojenia. Môžete si zvoliť medzi vysokou, strednou, nízkou alebo prijateľnou prioritou.

Súvisiace koncepty

“Integrovaná služba, využívajúca označenia diferencovaných služieb” na strane 10
V politike integrovanej služby môžete použiť označenia diferencovaných služieb, aby ste zachovali prioritu paketov prenášaných v zmiešanom prostredí.

“Politika povolenia vstupu” na strane 11
Politika povolenia vstupu riadi požiadavky na pripojenie do vášho systému.

“Diferencované služby” na strane 2
Toto je prvý typ politiky výstupnej šírky pásma, ktorú môžete vytvoriť vo vašom operačnom systéme. Diferencovaná služba rozdeľuje vašu premávku do tried. Ak chcete uplatňovať politiku diferencovanej služby, musíte určiť, ako chcete klasifikovať vašu sieťovú prevádzku a ako chcete zaobchádzať s jednotlivými triedami.

Súvisiaci odkaz

Použitie kódových bodov na priradenie správania typu per-hop

Kvalita služieb (QoS) používa ponúknuté kódové body na priradenie správania typu per-hop komunikačnej prevádzke.

V sprievodcovi triedou služieb potrebujete vašej politike priradiť správanie typu per-hop. Musíte stanoviť, ktoré kódové body sa majú použiť, a to na základe individuálnych potrieb vašej siete. Iba vy môžete rozhodnúť, aké schémy kódových bodov majú zmysel pre vaše prostredie. Musíte uvážiť, ktoré aplikácie sú pre vás najdôležitejšie a ktorým politikám možno treba priradiť vyššiu prioritu. Najdôležitejšou vecou je, aby boli konzistentné s vašimi označeniami, aby ste dosiahli výsledky, ktoré očakávate. Napríklad politikám majúcim rovnakú dôležitosť môžete priradiť podobné kódové body, čím dosiahnete konzistentné výsledky pre tieto politiky. Ak si nie ste istý, ktoré kódové body máte priradiť, použite metódu pokusu a omylu. Môžete vytvoriť testovacie politiky, môžete monitorovať tieto politiky a primerane spraviť potrebné úpravy.

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

Urýchlené postupovanie

Urýchlené postupovanie je jedným typom správania typu per-hop. Používa sa hlavne na poskytovanie garantovanej služby medzi sieťami. Zrýchlené postupovanie dáva prevádzke nízkostratovú, stabilnú, komplexnú službu medzi dvomi koncami tým, že garantuje šírku pásma medzi sieťami. Rezervácia sa vykoná pred odoslaním paketu. Hlavným cieľom je zabrániť oneskoreniu a doručiť paket včas.

Tabuľka 1. Navrhované kódové body: Urýchlené postupovanie

Urýchlené postupovanie
101110

Poznámka: Zaobchádzanie poskytujúce urýchlené postupovanie je obvykle veľmi nákladné, preto sa toto správanie typu per-hop neodporúča používať bežne.

Selektor triedy

Kódové body selektora triedy predstavujú iný typ správania. Existuje sedem tried. Trieda 0 dáva paketom najnižšiu prioritu a Trieda 7 dáva paketom najvyššiu prioritu v rámci hodnôt kódových bodov selektora triedy. Je to najbežnejšia skupina správaní pri skokoch, lebo väčšina smerovačov už používa podobné kódové body.

Tabuľka 2. Navrhované kódové body: Selektor triedy

Selektor triedy
Trieda 0 - 000000
Trieda 1 - 001000
Trieda 2 - 010000
Trieda 3 - 011000
Trieda 4 - 100000
Trieda 5 - 101000

Tabuľka 2. Navrhované kódové body: Selektor triedy (pokračovanie)

Selektor triedy
Trieda 6 - 110000
Trieda 7 - 111000

Zaistené postupovanie

Zaistené postupovanie je rozdelené do štyroch tried správania per-hop, každá z nich má nízku, strednú alebo vysokú úroveň precedensu zrušenia. Úroveň precedensu zrušenia určuje pravdepodobnosť zrušenia paketov. Každá trieda má vlastnú špecifikáciu šírky pásma. Trieda 1, vysoké, poskytuje politike najnižšiu prioritu a Trieda 4, nízke, poskytuje politike najvyššiu prioritu. Nízka úroveň zrušenia znamená, že pakety v tejto politike majú najnižšiu šancu byť zrušené v tejto konkrétnej úrovni triedy.

Tabuľka 3. Navrhované kódové body: Zaistené postupovanie

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

Súvisiace koncepty

"Diferencované služby" na strane 2
Toto je prvý typ politiky výstupnej šírky pásma, ktorú môžete vytvoriť vo vašom operačnom systéme. Diferencovaná služba rozdeľuje vašu premávku do tried. Ak chcete uplatňovať politiku diferencovanej služby, musíte určiť, ako chcete klasifikovať vašu sieťovú prevádzku a ako chcete zaobchádzať s jednotlivými triedami.

"Trieda služby" na strane 12
Pri vytváraní politiky diferencovaných služieb alebo politiky povolenia vstupu taktiež vytvárate a používate triedu služby.

Priemerný počet okamžitých pripojení a prah zahltenia pripojenia

Počet okamžitých pripojení a prah zahltenia predstavujú limity pre pripojenie. Tieto limity pomáhajú obmedziť vstupné pripojenia, ktoré sa snažia vstúpiť do vášho systému. Limity pripojení sa nastavujú v triede služby, ktorá sa používa v politike povolenia vstupu.

Nárazová rýchlosť pripojenia

Nárazová rýchlosť pripojenia určuje kapacitu vyrovnávacej pamäte, ktorá udržiava pripojenia v nárazoch. Pripojenia v nárazoch môžu do systému vstupovať rýchlejšie, než ich dokáže zvládnuť, alebo než chcete dovoliť. Ak počet pripojení v náraze prekročí nastavenú úroveň nárazu pripojenia, potom sú dodatočné spojenia zrušené.

Priemerný počet okamžitých pripojení

Priemerný počet okamžitých pripojení určuje limit pre novo vytvorené pripojenia alebo počet prijatých požiadaviek URI (Uniform Resource Identifier), povolených v systéme. Ak požiadavka spôsobí, že systém prekročí nastavený limit, systém ju odmietne. Limit pre priemerný počet okamžitých pripojení sa meria v pripojeniach za sekundu.

Tip: Ak chcete zistiť, aké limity máte nastaviť, môžete spustiť monitor. Scenár monitorovania aktuálnej štatistiky o sieťach obsahuje ukážkovú politiku, ktorá vám pomôže zhromaždiť väčšinu informácií prechádzajúcich vašim systémom. Použitím týchto výsledkov môžete limity okamžite nastaviť.

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

Súvisiace koncepty

"Politika povolenia vstupu" na strane 11
Politika povolenia vstupu riadi požiadavky na pripojenie do vášho systému.

"Scenár: Monitorovanie aktuálnej sieťovej štatistiky" na strane 45
V sprievodcoch potrebujete nastaviť výkonové limity, založené na jednotlivých sieťových požiadavkách.

API rozhrania kvality služieb

Táto téma obsahuje informácie o protokoloch a rozhraniach API, a tiež požiadavky na smerovač, ktorý je povolený pre protokol ReSerVation (RSVP). Medzi rozhrania API kvality služieb (QoS) patrí API rozhranie RAPI, API rozhranie soketu qtoq, sendmsg() a API rozhrania monitora.

Väčšina politík QoS vyžaduje používanie rozhrania API. Tieto rozhrania API sa môžu použiť v spojitosti buď s politikou diferencovaných služieb alebo politikou integrovaných služieb. Okrem toho je k dispozícii veľký počet rozhraní API, použiteľných s monitorom QoS:

- "Rozhrania API integrovaných služieb"
- "Rozhrania API diferencovaných služieb" na strane 17
- "Rozhrania API monitora" na strane 17

Rozhrania API integrovaných služieb

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

Protokol RSVP sa používa na vytvorenie rezervácie RSVP vo všetkých sieťových uzloch na ceste vašej premávky. Uchováva túto rezerváciu dostatočne dlho na to, aby bolo možné poskytnúť služby vyžadované vašou politikou. Rezervácia definuje spôsob zaobchádzania a šírku pásma, ktoré potrebujú údaje v tejto konverzácii. Sieťové uzly poskytujú spôsob zaobchádzania s údajmi, ktorý je definovaný v rezervácii.

RSVP je jednoduchý protokol v tých rezerváciách, ktoré sú vytvorené iba v jednom smere (od prijímača). Pre komplexnejšie pripojenia, ako sú audio- a videokonferencie, je každý odosielateľ súčasne prijímateľom. V tomto prípade musíte nastaviť dve relácie RSVP pre každú stranu.

Okrem smerovačov, podporujúcich RSVP, musíte mať na používanie integrovaných služieb aj aplikácie, ktoré podporujú RSVP. Keďže systém na začiatku nemá žiadne aplikácie podporujúce RSVP, musíte takúto aplikáciu napísať pomocou RAPI API alebo API rozhrania soketu qtoq QoS. Tým povolíte použitie protokolu RSVP aplikáciami. Ak máte záujem o hlbšie vysvetlenie, existuje veľa zdrojov, ktoré vysvetľujú tieto modely, ich fungovanie a spracovanie správ. Potrebujete dôkladne rozumieť protokolu RSVP a obsahu internetového štandardu RFC 2205.

Rozhrania API qtoq soketu

Pomocou API rozhraní soketu qtoq QoS si môžete zjednodušiť prácu spojenú s používaním protokolu RSVP v systéme. Rozhrania API qtoq soketov volajú rozhrania API RAPI a vykonávajú niektoré zo zložitejších úloh. Rozhrania API qtoq soketov nie sú také flexibilné ako rozhrania API RAPI, ale poskytujú rovnaké funkcie pri menšej námahe. Verzie bez signalizácie rozhraní API vám dovoľujú zapísať tieto aplikácie:

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

Signalizácia protokolu RSVP sa deje automaticky pre stranu klienta.

Pozrite si časti Funkčný tok rozhrania API QoS orientovaný na spojenie alebo Funkčný tok rozhrania API QoS bez pripojenia, kde nájdete bežný tok rozhrania API QoS pre aplikáciu alebo protokol, ktorý používa sokety qtoq QoS orientované na spojenie alebo bez pripojenia.

Rozhrania API diferencovaných služieb

Poznámka: API rozhranie sendmsg() sa používa pre určité politiky diferencovaných služieb, ktoré definujú špecifický token aplikácie. Pri vytváraní politiky diferencovanej služby môžete (voliteľne) poskytnúť charakteristiku aplikácie (token a prioritu). Ide o pokročilú definíciu politiky, a ak ju nepoužijete, toto rozhranie API môžete vynechať. Majte však na pamäti, že smerovače a ďalšie systémy v sieti i tak budú musieť byť informované o diferencovanej službe.

Ak sa rozhodnete v politike diferencovanej služby použiť token aplikácie, potom aplikácia, ktorá tieto informácie poskytuje, musí byť špeciálne naprogramovaná na použitie API rozhrania sendmsg(). Toto realizuje aplikačný programátor. Platné hodnoty (token a priorita), ktoré administrátor QoS použije v politike diferencovanej služby, musia byť uvedené v dokumentácii k aplikácii. Politika diferencovanej služby potom na komunikáciu, ktorá zodpovedá tokenu zadanému v politike, použije svoju vlastnú prioritu a klasifikáciu. Ak aplikácia nemá hodnoty zodpovedajúce hodnotám nastaveným v politike, musíte buď aktualizovať aplikáciu, alebo pre politiku diferencovanej služby použiť iné parametre aplikačných údajov.

Nasledujúce informácie stručne popisujú parametre systémových údajov: token aplikácie a prioritu aplikácie.

Čo je token aplikácie?

Token aplikácie je jednotný identifikátor prostriedku (URI), ktorý reprezentuje definovaný zdroj. Token, ktorý zadáte v politike QoS, sa porovná s tokenom, ktorý poskytne aplikácia pre odchádzajúcu komunikáciu. Aplikácia tento token poskytuje prostredníctvom API rozhrania sendmsg(). Ak sú tokeny rovnaké, premávka aplikácie sa zahrnie do politiky diferencovaných služieb.

Čo je priorita aplikácie?

Vami zadaná priorita aplikácie sa porovná s prioritou aplikácie poskytnutou vonkajšou aplikáciou. Aplikácia túto prioritu poskytuje prostredníctvom API rozhrania sendmsg(). Ak sú priority rovnaké, premávka aplikácie sa zahrnie do politiky diferencovaných služieb. Celá prevádzka definovaná v politike diferencovaných služieb bude naďalej prijímať prioritu udelenú celej politike.

Bližšie informácie o type politiky diferencovanej služby nájdete v časti “Diferencované služby” na strane 2.

Rozhrania API monitora

Rozhrania API protokolu Resource Reservation Setup Protocol zahŕňajú rozhrania API monitora. Rozhrania API, ktoré sa týkajú monitora, majú vo svojom názve slovo monitor. Napríklad *QgyOpenListQoSMonitorData*. Nasledujúci zoznam stručne opisuje každé API monitora:

- QgyOpenListQoSMonitorData (Open List of QoS Monitor Data) zhromažďuje informácie súvisiace so službami QoS.

- QtoqDeleteQoSMonitorData (Delete QoS Monitor Data) vymaže jednu alebo viac sád zhromaždených údajov monitora QoS.
- QtoqEndQoSMonitor (End QoS Monitor) zastaví získavanie informácií súvisiacich so službami QoS.
- QtoqListSavedQoSMonitorData (List Saved QoS Monitor Data) vráti zoznam všetkých predtým zozbieraných a uložených údajov monitora.
- QtoqSaveQoSMonitorData (Save QoS Monitor Data) uloží kópiu zhromaždených údajov monitora QoS pre budúce použitie.
- QtoqStartQoSMonitor (Start QoS Monitor) zhromaždí informácie súvisiace so službami QoS.

Súvisiace koncepty

"Integrované služby" na strane 6
Druhý typ politiky výstupnej šírky pásma, ktorú môžete vytvoriť vo vašom operačnom systéme, je politika integrovanej služby. Integrovaná služba poskytuje IP aplikáciám schopnosť požadovať a vyhradiť si frekvenčné pásmo pomocou protokolu ReSerVation Protocol (RSVP) a aplikačných programových rozhraní kvality služby (QoS).

"Funkcia kontroly premávky" na strane 8
Funkcie riadenia prevádzky sa vzťahujú len na integrovanú službu a nie sú špecifické pre produkty System i.

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

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

Súvisiaci odkaz

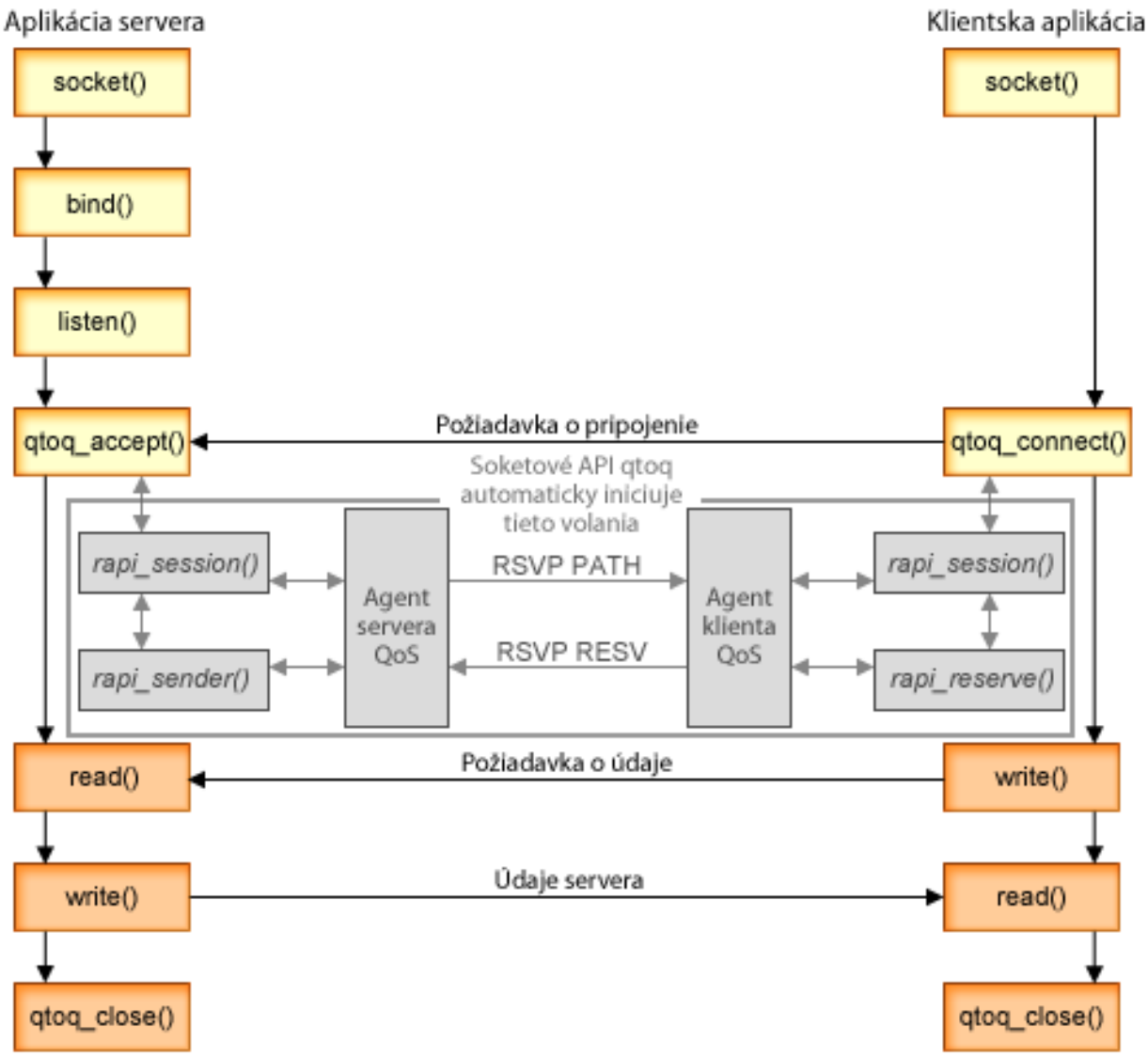
Rozhrania API protokolu Resource Reservation Setup Protocol

"Konfigurácia QoS pomocou sprievodcov" na strane 50
Ak chcete konfigurovať politiky kvality služieb (QoS), musíte použiť sprievodcov QoS, ktorí sa nachádzajú v System i Navigator.

Funkčný tok rozhrania API QoS orientovaný na spojenie

Príklady servera a klienta ilustrujú API rozhrania soketu qtoq kvality služieb (QoS), ktoré sú napísané pre funkčný tok orientovaný na spojenie.

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



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

Serverová strana

Rozhranie qtoq_accept() API pre pravidlo neoznačené signalizáciou

1. Aplikácia volá funkciu socket(), aby získala deskriptor soketu.
2. Aplikácia volá listen(), aby špecifikovala, na ktoré pripojenia čaká.
3. Aplikácia volá qtoq_accept(), aby čakala na klientsku požiadavku na pripojenie.
4. API volá rapi_session() API. Ak je úspešné, priradí sa ID relácie QoS.
5. API volá štandardnú funkciu accept(), aby čakala na klientsku požiadavku na pripojenie.
6. Keď je prijatá požiadavka o pripojenie, v požadovanom pravidle sa vykoná riadenie prístupu. Pravidlo sa odošle do zásobníka TCP/IP. Ak je pravidlo platné, vráti sa volajúcej aplikácii s výsledkami a s ID relácie.
7. Aplikácie pre server a pre klienta vykonávajú požadovaný prenos údajov.
8. Aplikácia volá funkciu qtoq_close(), aby sa zatvoril soket a uvoľnilo pravidlo.

9. Server QoS vymaže pravidlo zo správcu QoS, vymaže reláciu QoS a vykoná všetky ďalšie potrebné akcie.

rozhranie qtoq_accept() API s normálnou signalizáciou RSVP

1. Aplikácia volá funkciu socket(), aby získala deskriptor soketu.
2. Aplikácia volá listen(), aby špecifikovala, na ktoré pripojenia čaká.
3. Aplikácia volá qtoq_accept(), aby čakala na klientsku požiadavku na pripojenie.
4. Keď príde požiadavka na pripojenie, je volané API rapi_session(), aby sa vytvorila relácia so serverom QoS pre toto pripojenie a získalo sa ID relácie QoS, ktoré sa vráti volajúcej aplikácii.
5. Volá sa API rapi_sender(), aby sa iniciovala správa PATH zo servera QoS a aby bol server QoS informovaný, že musí očakávať správu RESV od klienta.
6. API rozhranie rapi_getfd() je volané, aby sa získal deskriptor, ktorý používajú aplikácie na čakanie na správy o udalostiach QoS.
7. Deskriptor akceptácie a deskriptor QoS sú vrátené do aplikácie.
8. Server QoS čaká na prijatie novej správy RESV. Keď je správa prijatá, server načíta príslušné pravidlo s manažérom QoS a odošle správu aplikácii, ak si vyžiadala notifikáciu o volaní rozhrania API qtoq_accept().
9. Server QoS pokračuje v poskytovaní obnovení pre vytvorenú reláciu.
10. Aplikácia volá qtoq_close(), keď sa spojenie dokončí.
11. Server QoS vymaže pravidlo zo správcu QoS, vymaže reláciu QoS a vykoná všetky ďalšie potrebné akcie.

Klientska strana

Rozhranie qtoq_connect() API s normálnou signalizáciou RSVP

1. Aplikácia volá funkciu socket(), aby získala deskriptor soketu.
2. Aplikácia volá funkciu qtoq_connect(), aby informovala serverovú aplikáciu, že chce vytvoriť pripojenie.
3. Funkcia qtoq_connect() volá rozhranie API rapi_session(), aby sa vytvorila relácia so serverom QoS pre toto pripojenie.
4. Server QoS je informovaný, aby čakal na príkaz PATH z požadovaného pripojenia.
5. API rozhranie rapi_getfd() je volané, aby sa získal deskriptor QoS, ktorý používajú aplikácie na čakanie na správ QoS.
6. Je volaná funkcia connect(). Výsledky funkcie connect() a deskriptora QoS sa vrátia aplikácii.
7. Server QoS čaká na prijatie správy PATH. Keď je prijatá správa, odpovedá odoslaním správy RESV do servera QoS v počítači servera aplikácie.
8. Ak aplikácia požiadala o oznámenie, server QoS odošle oznámenie aplikácii prostredníctvom deskriptora QoS.
9. Server QoS pokračuje v poskytovaní obnovení pre vytvorenú reláciu.
10. Aplikácia volá qtoq_close(), keď je spojenie dokončené.
11. Server QoS zatvorí reláciu QoS a vykoná všetky ďalšie potrebné akcie.

Rozhranie qtoq_connect() API pre pravidlo neoznačené signalizáciou

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

Súvisiaci odkaz

qtoq_accept()--Prijať API pripojenia soketov QoS

qtoq_close()--Zatvoriť API pripojenia soketov QoS

rapi_session()--Vytvoriť reláciu RAPI

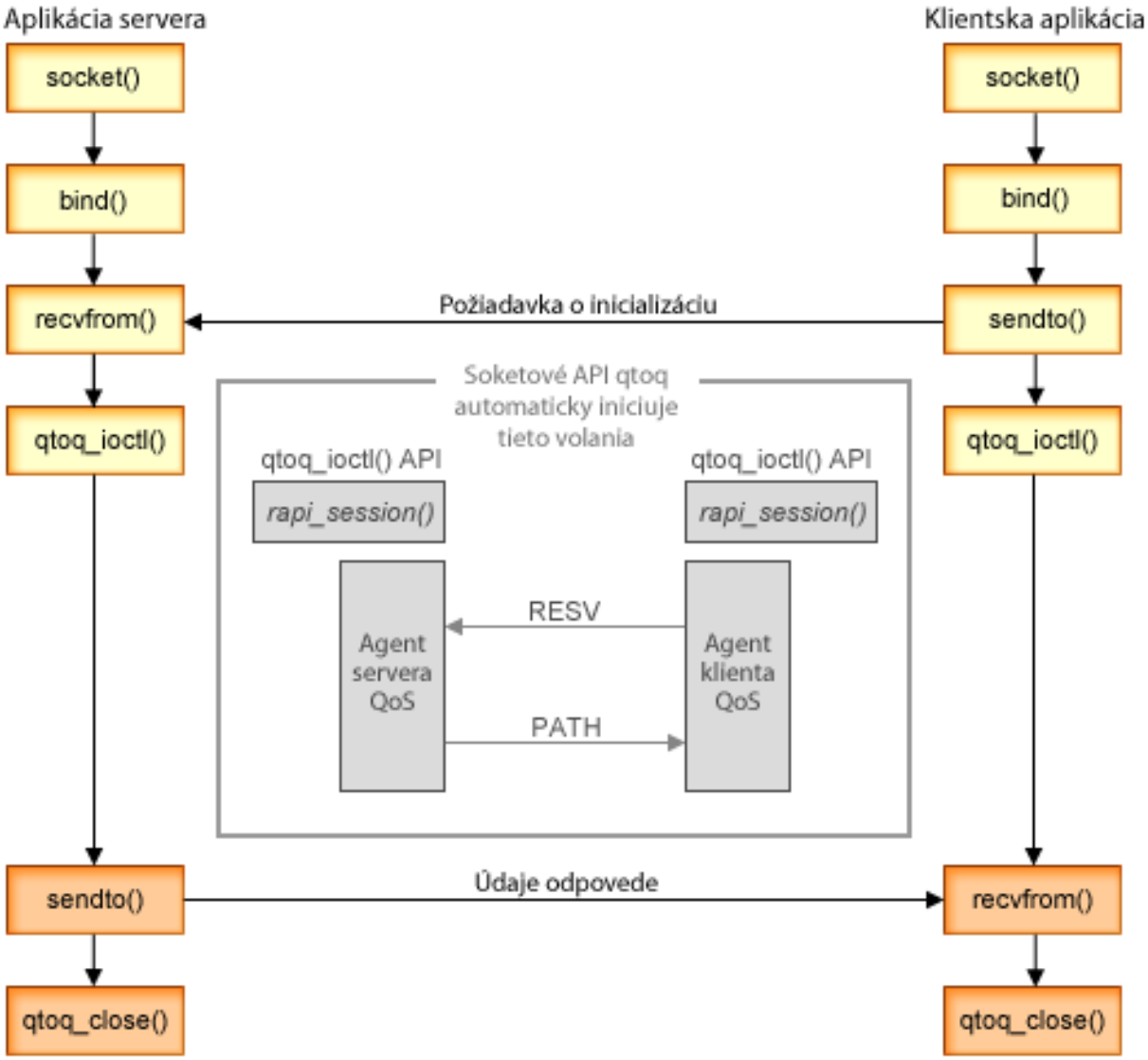
rapi_sender()--Identifikovať odosielateľa RAPI

rapi_getfd()--Získať deskriptor, na ktorý sa má čakať

qtoq_connect()--Vytvoriť API pripojenia soketov QoS

Funkčný tok rozhrania API QoS bez pripojenia

Keď sú volané funkcie rozhrania API, povolené pre QoS, pre tok bez spojenia, ktorý vyžaduje, aby bol spustený protokol ReSerVation Protocol (RSVP), spustia sa doplnkové funkcie. Tieto funkcie spôsobia, že QoS agenti na klientovi a serveri nastavia RSVP pre tok údajov medzi klientom a serverom.



Tok udalostí qtoq: Nasledujúca postupnosť soketových volaní poskytuje popis k obrázku. Taktiež popisuje vzťah medzi serverom a klientskou aplikáciou v dizajne bez pripojenia. Toto sú modifikácie základných soketových API.

Serverová strana

qtoq_ioctl() Rozhranie API pre pravidlo neoznačené signalizáciou

1. API rozhranie qtoq_ioctl() odošle správu serveru QoS so žiadosťou, aby vykonal riadenie vstupu na požadovanom pravidle.
2. Ak je pravidlo akceptovateľné, volá funkciu, ktorá odosiela správu na server QoS a žiada ho o zavedenie pravidla.
3. Server QoS potom volajúcemu vráti stav udávajúci úspech alebo zlyhanie požiadavky.
4. Keď aplikácia dokončí používanie pripojenia, zavolá funkciu qtoq_close(), ktorá pripojenie ukončí.

5. Server QoS vymaže pravidlo zo správcu QoS, vymaže reláciu QoS a vykoná všetky ďalšie potrebné akcie.

Rozhranie qtoq_ioctl() API s normálnou signalizáciou RSVP

1. API rozhranie qtoq_ioctl() odošle správu serveru QoS, požadujúcu riadenie vstupu pre požadované pripojenie.
2. Server QoS volá rapi_session() s požiadavkou, aby bola pre pravidlo vytvorená relácia a aby sa získalo ID relácie QoS, ktoré sa má vrátiť volajúcemu.
3. Volá rapi_sender() na iniciovanie správy PATH späť klientovi.
4. Potom zavolá rapi_getfd() na získanie deskriptora, aby sa čakalo na udalosti QoS.
5. Server QoS vráti deskriptor select(), ID relácie QoS a stav volajúcemu.
6. Server QoS načítava pravidlo, keď je prijatá správa RESV.
7. Aplikácia zadá qtoq_close(), keď sa spojenie dokončí.
8. Server QoS vymaže pravidlo zo správcu QoS, vymaže reláciu QoS a vykoná akúkoľvek ďalšiu potrebnú akciu.

Klientska strana

Rozhranie qtoq_ioctl() API s normálnou signalizáciou RSVP

1. API rozhranie qtoq_ioctl() volá rapi_session() s požiadavkou, aby sa pre pripojenie vytvorila relácia. Funkcia rapi_session() požaduje riadenie vstupu pre pripojenie. Pripojenie bude na klientskej strane odmietnuté, iba ak je na nej nakonfigurované pravidlo pre klienta a nie je momentálne aktívne. Táto funkcia vracia ID relácie QoS, ktoré je vrátené späť do aplikácie.
2. Zavolá rapi_getfd() na získanie deskriptora, aby sa čakalo na udalosti QoS.
3. qtoq_ioctl() sa vráti späť volajúcemu s deskriptorom a ID relácie.
4. Server QoS čaká na prijatie správy PATH. Keď je prijatá správa o ceste, odpovedá správou RESV a potom signalizuje aplikácii, že udalosť nastala prostredníctvom deskriptora relácie.
5. Server QoS pokračuje v poskytovaní obnovení pre vytvorenú reláciu.
6. Klientsky kód volá qtoq_close(), keď sa spojenie dokončí.

Rozhranie qtoq_ioctl() API pre pravidlo označené žiadna signalizácia

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

Súvisiaci odkaz

qtoq_close()--Zatvoriť API pripojenia soketov QoS

rapi_session()--Vytvoriť reláciu RAPI

rapi_sender()--Identifikovať odosielateľa RAPI

rapi_getfd()--Získať deskriptor, na ktorý sa má čakať

qtoq_ioctl()--Nastaviť API volieb riadenia soketov QoS

Rozšírenia API QoS sendmsg()

Funkcia sendmsg() sa používa na odoslanie údajov, pre podporné údaje, prípadne oboje prostredníctvom pripojeného alebo nepripojeného soketu.

API rozhranie sendmsg() umožňuje klasifikačné údaje kvality služieb (QoS). Politiky QoS používajú túto funkciu na definovanie jemnejšej úrovne klasifikácie pre odchádzajúcu alebo prichádzajúcu premávku TCP/IP. Konkrétne používajú podporné údaje, ktoré sa aplikujú do vrstvy IP. Používaný typ správy je IP_QOS_CLASSIFICATION_DATA. Tieto podporné údaje môže aplikácia použiť na definovanie atribútov pre premávku v konkrétnom pripojení TCP. Ak aplikáciou odovzdané atribúty zodpovedajú atribútom definovaným v politike QoS, potom politika QoS obmedzí premávku TCP.

Nasledovné informácie použite pri inicializácii štruktúry IP_QOS_CLASSIFICATION_DATA:

- ip_qos_version: Označuje verziu štruktúry. Túto položku je treba vyplniť pomocou konštanty *IP_QOS_CURRENT_VERSION*.

- ip_qos_classification_scope: Špecifikuje rozsah úrovne pripojenia (použite konštantu *IP_QOS_CONNECTION_LEVEL*) alebo rozsah úrovne správy (konštanta *IP_QOS_MESSAGE_LEVEL*).

  Rozsah na úrovni pripojenia udáva, že úroveň služby QoS, získaná prostredníctvom klasifikácie tejto správy, zostane účinná pre všetky ďalšie odoslané správy až do nasledujúceho volania sendmsg(), ktoré obsahuje klasifikačné údaje. Rozsah na úrovni správ udáva, že priradená úroveň služby QoS sa použije len pre údaje správy z tohto volania sendmsg(). Údaje odoslané v budúcnosti bez klasifikačných údajov QoS zdedia predchádzajúce priradenie úrovne pripojenia QoS (z poslednej klasifikácie na úrovni pripojenia cez API rozhranie sendmsg() alebo z pôvodnej klasifikácie pripojenia TCP počas vytvárania pripojenia).
- ip_qos_classification_type: Táto špecifikácia určuje typ odovzdávaných údajov klasifikácie. Aplikácia si môže zvoliť medzi odovzdaním tokenu definovaného aplikáciou, priority špecifikovanej aplikáciou alebo medzi odovzdaním obidvoch možností, aj tokenu aj priority. Ak sa zvolí posledná z týchto možností, teda aj symbol aj priorita, typy klasifikácií musia byť logicky oddelené operátorom OR. Dajú sa špecifikovať nasledujúce typy:
  - Klasifikácia tokenu definovaného aplikáciou. Musí byť zadaný iba jediný typ; ak je zadaných viac typov (dva a viac), výsledok nemožno predvídať.
    - IP_SET_QOSLEVEL_W_APPL_TOKEN_ASCII : Toto označuje, že údaje klasifikácie sú znakový reťazec vo formáte ASCII. Ak je zadaná táto možnosť, symbol aplikácie je treba presunúť do poľa ip_qos_appl_token.

      Poznámka: Ak aplikácia musí pre klasifikačné údaje posielať numerické hodnoty, musí ich najskôr skonvertovať do formátu ASCII vhodného na tlač. Zadaný reťazec môže obsahovať veľké aj malé písmená a udáva sa v presnej forme pre potreby budúceho porovnania.
    - IP_SET_QOSLEVEL_W_APPL_TOKEN_EBCDIC : Označuje to isté ako voľba uvedená vyššie okrem toho, že reťazec je vo formáte EBCDIC.

      Poznámka: Voľba IP_SET_QOSLEVEL_W_APPL_TOKEN_ASCII je o niečo vhodnejšia, pretože aplikačné údaje zadané v politike sa uložia vo formáte ASCII do zásobníka TCP/IP, čím sa eliminuje potreba prekladať token zadefinovaný aplikáciou pri každej požiadavke sendmsg().
  - Klasifikácia priority definovanej aplikáciou. Musí byť zadaný iba jediný typ; ak je zadaných viac typov priority, výsledky nemožno predvídať.
    - IP_SET_QOSLEVEL_EXPIDITED: Udáva, že sa vyžaduje urýchlená priorita.
    - IP_SET_QOSLEVEL_HIGH: Udáva, že sa vyžaduje vysoká priorita.
    - IP_SET_QOSLEVEL_MEDIUM: Udáva, že sa vyžaduje stredná priorita.
    - IP_SET_QOSLEVEL_LOW: Udáva, že sa vyžaduje nízka priorita.
    - IP_SET_QOSLEVEL_EFFORT: Udáva, že sa vyžaduje prijateľná priorita.
  - ip_qos_appl_token_len: dĺžka tokenu ip_qos_appl_token.
  - ip_qos_appl_token: Toto virtuálne pole nasleduje ihneď za poľom ip_qos_classification_type. Reťazec tokenu na klasifikáciu aplikácie vo formáte ASCII alebo EBCDIC podľa toho, aká koncovka je zadaná v IP_SET_QOSLEVEL_W_APPL_TOKEN_xxxx pre daný klasifikačný typ. Toto pole je referencované len v prípade špecifikácie tokenu definovaného aplikáciou. Nezabudnite, že dĺžka tohto poľa nesmie presiahnuť 128 bajtov. Aj je zadaná väčšia dĺžka, použije sa iba prvých 128 bajtov. Nezabudnite, že dĺžka reťazca sa určuje na základe hodnoty špecifikovanej pre cmsg_len (cmsg_len - sizeof(cmsghdr) - sizeof(ip_qos_classification_data)). Táto vypočítaná dĺžka nesmie obsahovať žiadne ukončujúce nulové znaky.

Súvisiace koncepty

“Diferencované služby” na strane 2
Toto je prvý typ politiky výstupnej šírky pásma, ktorú môžete vytvoriť vo vašom operačnom systéme. Diferencovaná služba rozdeľuje vašu premávku do tried. Ak chcete uplatňovať politiku diferencovanej služby, musíte určiť, ako chcete klasifikovať vašu sieťovú prevádzku a ako chcete zaobchádzať s jednotlivými triedami.

“Prioritné triedy: Klasifikácia komunikácie po sieti” na strane 3
Diferencovaná služba klasifikuje prevádzku do tried. Najbežnejšie triedy sú definované prostredníctvom klientskych adries IP, aplikačných portov, typov serverov, protokolov, lokálnych adries IP a rozvrhov. Všetka prevádzka, spadajúca do rovnakej triedy, sa spracúva rovnako.

Súvisiaci odkaz

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

Adresárový server

Svoje politiky môžete vyexportovať na adresárový server. Prečítajte si túto tému so základnými pojmami a konfiguráciou protokolu LDAP (Lightweight Directory Access Protocol) a pozrite si schému kvality služieb (QoS).

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

Ako používať adresárový server

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

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

Výhody ukladania výlučne na váš lokálny systém

Ukladanie politík QoS na váš lokálny systém nie je také zložité. Existuje niekoľko výhod používania politík lokálne:

- Eliminuje sa zložitosť konfigurácie LDAP pre užívateľov, ktorí to nepotrebujú.
- Zvyšuje sa výkonnosť, pretože zapisovanie do LDAP nie je najrýchlejšou metódou.
- Budete môcť ľahšie zduplikovať konfiguráciu na iný systém. Môžete kopírovať súbor z jedného systému do druhého. Keďže tu neexistuje primárny alebo sekundárny počítač, každú politiku môžete prispôsobiť presne na mieru konkrétnemu systému.

Prostriedky protokolu LDAP

Ak sa rozhodnete exportovať vaše politiky do servera LDAP, najskôr sa musíte oboznámiť s konceptmi LDAP a so štruktúrami adresárov. V rámci funkcie QoS v System i Navigator môžete nakonfigurovať adresárový server, ktorý sa použije s vašou politikou QoS.

Súvisiace koncepty

IBM Tivoli Directory Server for i5/OS (LDAP)

“Konfigurácia adresárového servera” na strane 51
Konfigurácie politík kvality služieb (QoS) môžete exportovať do adresárového servera LDAP, vďaka ktorému sa riešenie QoS ľahšie spravuje.

Kľúčové slová

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

Polia kľúčových slov sú nepovinné a možno ich ignorovať.

Adresárový server si môžete nakonfigurovať pomocou sprievodcu QoS Initial Configuration. Môžete upresniť aj to, či má byť server, ktorý konfigurujete, primárnym alebo sekundárnym systémom. Server, na ktorom uchovávate všetky vaše politiky QoS, sa označuje ako primárny systém.

Na identifikáciu konfigurácií vytvorených primárnym systémom sa používajú kľúčové slová. Hoci sú vytvorené na primárnom systéme kľúčové slová sú skutočne užitočné na sekundárnom systéme. Umožňujú sekundárnym systémom načítať a používať konfigurácie vytvorené primárnym systémom. Nasledovné opisy vysvetľujú spôsoby používania kľúčových slov v každom systéme.

Kľúčové slová a primárne systémy

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

Kľúčové slová a sekundárne systémy

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

Pri konfigurácii adresárového servera v System i Navigator môžete použiť pomoc k úlohám QoS, ktorá obsahuje špecifické inštrukcie.

Súvisiace koncepty

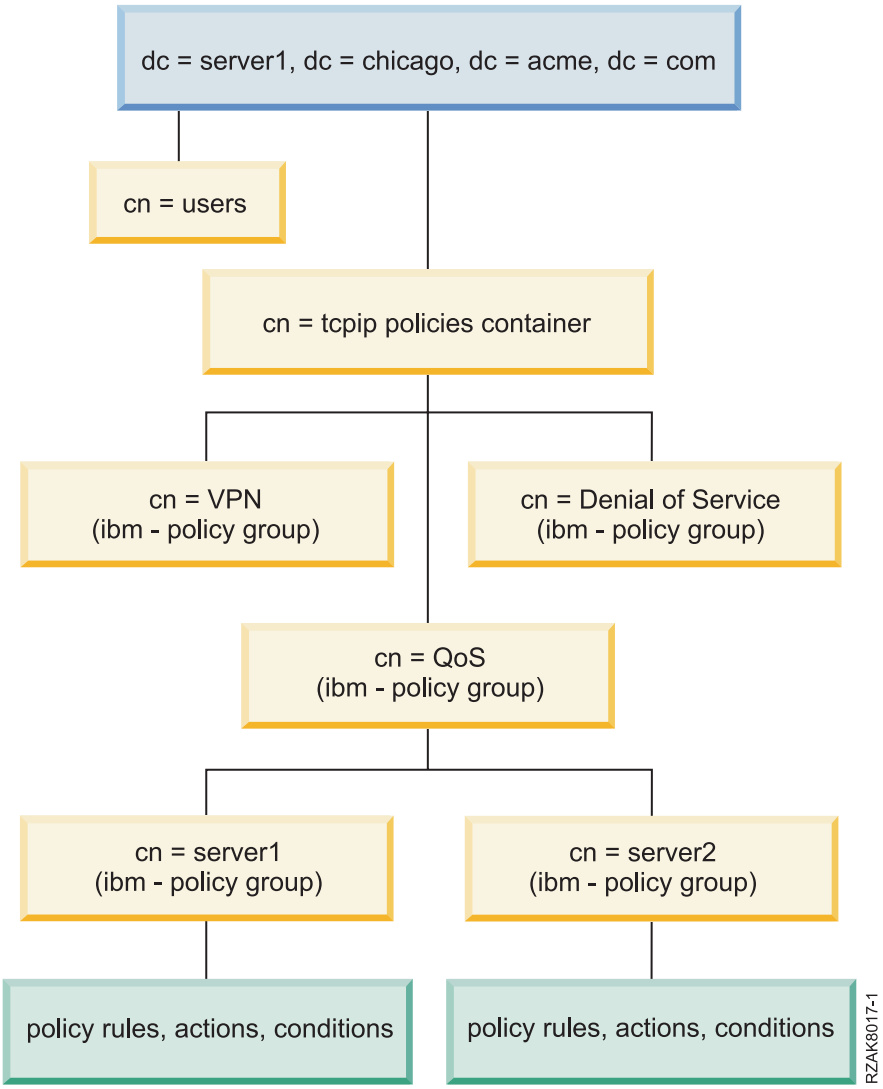
"Rozlišovací názov"
Keď chcete spravovať časť vášho adresára, odkazujete na charakteristický názov (DN) alebo na kľúčové slovo (ak ho zvolíte).

"Konfigurácia adresárového servera" na strane 51
Konfigurácie politík kvality služieb (QoS) môžete exportovať do adresárového servera LDAP, vďaka ktorému sa riešenie QoS ľahšie spravuje.

Rozlišovací názov

Keď chcete spravovať časť vášho adresára, odkazujete na charakteristický názov (DN) alebo na kľúčové slovo (ak ho zvolíte).

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



Obrázok 3. Vzorová adresárová štruktúra QoS

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

Pri spravovaní adresára je dôležité, aby ste v DN zmenili príslušný server, napríklad cn alebo dc. Buďte opatrný pri upravovaní DN, hlavne kvôli tomu, že reťazec je zvyčajne príliš dlhý, aby sa zobrazil bez pretáčania.

Súvisiace koncepty

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

“Konfigurácia adresárového servera” na strane 51
Konfigurácie politík kvality služieb (QoS) môžete exportovať do adresárového servera LDAP, vďaka ktorému sa riešenie QoS ľahšie spravuje.

Súvisiaci odkaz

"Informácie súvisiace s kvalitou služieb" na strane 65
Dokumenty Request for Comments, publikácie IBM Redbooks a ďalšie témy informačného centra obsahujú ďalšie informácie súvisiace s témami kvality služieb. Súbory PDF môžete zobraziť alebo stiahnuť.

Scenáre: Politiky kvality služieb

Tieto scenáre politík kvality služieb (QoS) vám pomôžu pochopiť, prečo potrebujete QoS a ako môžete vytvoriť politiky a triedy služieb.

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

Poznámka: IP adresy a diagramy sú vymyslené a majú len ilustratívny charakter.

Súvisiace koncepty

"Monitorovanie systémových transakcií" na strane 61
Pomocou monitora kvality služieb (QoS) si môžete overiť, či politiky QoS fungujú podľa vašej predstavy. Monitor QoS vám môže pomôcť v plánovacej fáze a vo fáze odstraňovania problémov QoS.

Súvisiaci odkaz

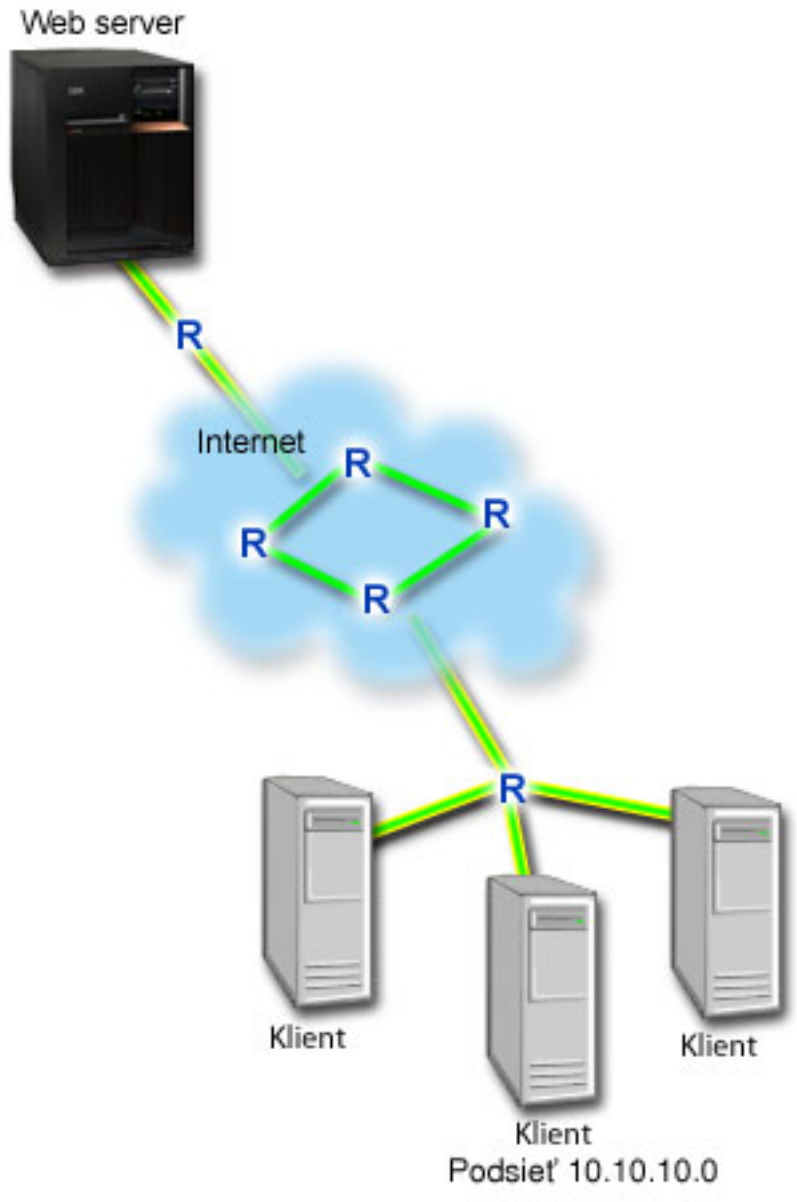
"Monitorovanie QoS" na strane 55
Pomocou monitora kvality služieb (QoS) môžete analyzovať IP prevádzku vo vašom systéme.

Scenár: Obmedzenie prevádzky prehliadača

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

Situácia

Vaša spoločnosť máva vždy v piatok veľmi rušnú komunikáciu s dizajnérskou skupinou, a táto komunikácia prebieha cez webové prehliadače. Táto premávka interferovala s účtovným oddelením, ktoré taktiež požaduje dobrý výkon od ich účtovných aplikácií počas piatkov. Rozhodnete sa obmedziť premávku prehliadačov z UCD skupiny. Nasledujúca schéma ilustruje nastavenie siete v tomto scenári.



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

Ciele

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

Nevyhnutné podmienky a predpoklady

- S vašim poskytovateľom internetových služieb máte zmluvu o dohodnutej úrovni poskytovaných služieb (SLA), ktorá má zaručiť, aby politiky získali požadovanú prioritu. V systéme vytvorená politika QoS umožňuje, aby prevádzka (stanovená v politike) získala v sieti určitú prioritu. Táto politika QoS nezaručuje prioritu a je závislá od vašej zmluvy o úrovni služieb. V skutočnosti vám používanie politík QoS môže pomôcť vyjednať určité dohodnuté úrovne služieb a prenosové rýchlosti.

- Politiky diferencovaných služieb vyžadujú, aby si smerovače v celej sieťovej ceste boli vedomé diferencovaných služieb. Väčšina smerovačov si nie je vedomá diferencovaných služieb.

Konfigurácia

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

Súvisiace koncepty

"Dohodnutá úroveň poskytovaných služieb" na strane 48
Táto téma sa venuje niektorým dôležitým aspektom dohodnutej úrovne poskytovaných služieb (SLA), ktoré môžu vplývať na implementáciu kvality služieb (QoS). QoS je sieťové riešenie. Ak chcete získať sieťovú prioritu mimo vašej súkromnej siete, pravdepodobne potrebujete s vaším poskytovateľom internetových služieb (ISP) uzavrieť zmluvu o dohodnutej úrovni poskytovaných služieb.

"Diferencované služby" na strane 2
Toto je prvý typ politiky výstupnej šírky pásma, ktorú môžete vytvoriť vo vašom operačnom systéme. Diferencovaná služba rozdeľuje vašu premávku do tried. Ak chcete uplatňovať politiku diferencovanej služby, musíte určiť, ako chcete klasifikovať vašu sieťovú prevádzku a ako chcete zaobchádzať s jednotlivými triedami.

Súvisiaci odkaz

"Monitorovanie QoS" na strane 55
Pomocou monitora kvality služieb (QoS) môžete analyzovať IP prevádzku vo vašom systéme.

Podrobnosti scenára: Vytvorenie politiky diferencovaných služieb

Táto téma obsahuje informácie o konfigurácii politiky diferencovanej služby na systéme.

1. V System i Navigator rozviňte položky ***váš systém*** → **Network** → **IP Policies**.
2. Kliknite pravým tlačidlom na **Quality of Service** a vyberte **Configuration** na otvorenie rozhrania kvality služieb (QoS).
3. V rozhraní QoS pravým tlačidlom kliknite na typ politiky DiffServ a vyberte **New Policy**, aby ste spustili sprievodcu.
4. Prečítajte si Uvítaciu stránku a kliknite na tlačidlo **Next**, aby ste sa dostali na stránku Name.
5. V poli **Name** zadajte UCD. Tiež môžete voliteľne zadať opis na lepšie zapamätanie si účelu tejto politiky. Kliknite na tlačidlo **Next**.
6. Na stránke Clients vyberte **Specific address or addresses** a kliknite na **New** a definujte vášho klienta.
7. V okne New Client zadajte nasledujúce informácie a kliknite na tlačidlo **OK**:
   - **Názov**: UCD_Client
   - **IP adresa a maska**: 10.10.10.0 / 24

   Po kliknutí na **OK** sa vrátite späť do sprievodcu politikami. Ak ste predtým vytvorili nejakých klientov, zrušte ich označenie a overte si, či sú vybratí iba relevantní klienti.
8. Na stránke Požiadavka o údaje servera skontrolujte, či sú vybraté voľby **Any token** a **All priorities** a kliknite na tlačidlo **Next**.
9. Na stránke Applications vyberte **Specific port, range of ports, or server type** a kliknite na **New**.
10. V okne New application zadajte nasledujúce informácie a kliknite na tlačidlo **OK** na návrat do sprievodcu:
    - **Názov**: HTTP
    - **Port**: 80
11. Na stránke Applications vyberte **Protocol** a skontrolujte, či je vybraté **TCP**. Kliknite na tlačidlo **Next**.
12. Na stránke Local IP address skontrolujte, či sú vybraté **All IP addresses** a kliknite na tlačidlo **Next**.
13. Na stránke Differentiated Class of Service kliknite na **New**, aby ste zadefinovali charakteristiky výkonu. Otvorí sa sprievodca pre novú triedu služieb.
14. Prečítajte si Uvítaciu stránku a kliknite na tlačidlo **Next**.
15. Na stránke Name zadajte UCD_service. Tiež môžete voliteľne zadať opis na lepšie zapamätanie si účelu tejto politiky. Kliknite na tlačidlo **Next**.

16. Na stránke Type of Service vyberte **Outbound only** a kliknite na tlačidlo **Next**. Táto trieda služby sa použije len pre politiky výstupu.
17. Na strane Outbound DiffServ Codepoint Marking vyberte **Class 4** a kliknite na **Next**. Správanie typu per-hop určuje, aký výkon získa táto prevádzka od smerovačov a iných systémov v sieti. Pri rozhodovaní vám pomôže systém pomoci umiestnený v rozhraní.
18. Na stránke Perform Outbound Traffic Metering skontrolujte, či je vybraté **Yes** a kliknite na tlačidlo **Next**.
19. Na stránke Outbound Rate Control Limits zadajte nasledujúce informácie a kliknite na tlačidlo **Next**:
    - **Veľkosť bloku tokenov**: 100 kilobitov
    - **Limit priemernej rýchlosti**: 512 kilobitov za sekundu
    - **Limit špičkovej rýchlosti**: 1 megabit za sekundu
20. Na stránke Outbound Out-of-Profile Traffic vyberte **Drop UDP packets or reduce TCP congestion window** a kliknite na tlačidlo **Next**.
21. Skontrolujte súhrnné informácie pre triedu služieb. Ak sú správne, kliknite na tlačidlo **Finish** na vytvorenie triedy služby. Po kliknutí na **Finish** sa vrátite späť do sprievodcu politikami. Bude vybratá vaša trieda služieb. Kliknite na tlačidlo **Next**.
22. Na stránke Schedule vyberte **Active during selected schedule** a kliknite na tlačidlo **New**.
23. V okne Add New Schedule zadajte nasledujúce informácie a kliknite na tlačidlo **OK**:
    - **Názov**: UCD_schedule
    - **Denný čas**: Aktívny 24 hodín
    - **Deň v týždni**: Piatok
24. Kliknutím na **Next** zobrazíte súhrnný prehľad politiky. Ak sú informácie správne, kliknite na tlačidlo **Finish**. V okne konfigurácie servera QoS sa v pravej časti okna zobrazí nová politika.

Podrobnosti scenára: Spustenie alebo aktualizovanie servera QoS

Táto téma obsahuje informácie o spustení alebo aktualizovaní servera QoS.

V okne Quality of Service (QoS) Server Configuration vyberte **Server → Start** alebo **Server → Update**.

Podrobnosti scenára: Overenie funkčnosti politiky

Pomocou monitora skontrolujte, či sa sieťová prevádzka správa podľa toho, ako ste ju nakonfigurovali.

1. V okne Konfigurácia kvality služieb (QoS) vyberte **Server → Monitor**. Otvorí sa okno Monitor QoS.
2. Vyberte zložku s typom politiky DiffServ. Zobrazia sa všetky politiky diferencovaných služieb. Zo zoznamu vyberte **UCD**.

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

   Hodnota, ktorú priradíte poľu **Limit priemernej rýchlosti**, je tiež dôležitá. Keď pakety prekročia túto hranicu, systém ich začne ukončovať. V dôsledku toho sa zvýši počet bitov mimo profilu. To vám naznačí, že politika sa správa tak, ako ste ju nakonfigurovali. Popis všetkých polí monitorov nájdete v časti “Monitorovanie QoS” na strane 55.

   Poznámka: Pamätajte, že výsledky sú správne len vtedy, keď je politika aktívna. Skontrolujte plán, ktorý ste špecifikovali v rámci politiky.

Podrobnosti scenára: Zmena vlastností

Keď sa pozriete na výsledky monitora, môžete zmeniť ľubovoľné vlastnosti politiky alebo triedy služieb, aby ste dosiahli očakávané výsledky.

Ak chcete zmeniť nejaké hodnoty, ktoré ste vytvorili v politike, postupujte podľa týchto krokov:

1. V okne Konfigurácia servera kvality služieb (QoS) vyberte adresár **DiffServ**. V zozname v pravej časti okna pravým tlačidlom kliknite na **UCD** a vyberte **Properties**, aby ste upravili politiku. Otvorí sa okno vlastností s hodnotami, ktoré riadia všeobecnú politiku.
2. Zadajte príslušné hodnoty.
3. Ak chcete upraviť triedu služby, vyberte zložku **Classes of service**. V zozname v pravej časti okna pravým tlačidlom kliknite na **UCD_service** a vyberte **Properties**, aby ste upravili triedu služby. Otvorí sa okno vlastností QoS s hodnotami, ktoré riadia prevádzku.
4. Zadajte príslušné hodnoty.
5. V okne konfigurácie servera QoS vyberte **Server → Update** na akceptovanie zmien.

Scenár: Bezpečné a predpovedateľné výsledky (VPN a QoS)

Aj vtedy, ak používate virtuálnu súkromnú sieť (VPN), môžete vytvárať politiky kvality služby (QoS).

Situácia

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

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

Obrázok 5. Pripojenie typu hostiteľ-hostiteľ v rámci virtuálnej súkromnej siete s použitím politiky diferencovanej služby QoS.

Ciele

Pomocou VPN a QoS môžete vytvoriť nielen ochranu, ale aj prioritu pre toto pripojenie. Najprv nakonfigurujte pripojenie VPN medzi dvomi hostiteľmi. Keď ste už zaistili ochranu svojho VPN pripojenia, môžete si nastaviť aj politiku QoS. Môžete vytvoriť politiku diferencovaných služieb. Tejto politike môže byť priradená vysoká hodnota kódového bodu urýchleného napredovania, čo bude mať vplyv na spôsob, akým bude sieť stanovovať priority najdôležitejšej komunikačnej prevádzky.

Nevyhnutné podmienky a predpoklady

- S vašim poskytovateľom internetových služieb máte zmluvu o dohodnutej úrovni poskytovaných služieb (SLA), ktorá má zaručiť, aby politiky získali požadovanú prioritu. V systéme vytvorená politika QoS umožňuje, aby prevádzka (stanovená v politike) získala v sieti určitú prioritu. Nezaručuje to a je závislá na vašom SLA. V skutočnosti vám používanie politík QoS môže pomôcť vyjednať určité dohodnuté úrovne služieb a prenosové rýchlosti. Ak chcete zistiť viac, použite odkaz SLA.
- Politiky diferencovaných služieb vyžadujú v celej sieťovej ceste smerovače podporujúce diferencované služby. Väčšina smerovačov dokáže podporovať diferencované služby.

Konfigurácia

Keď ste skontrolovali všetky predbežné požiadavky, môžete vytvoriť politiku diferencovanej služby.

Súvisiace koncepty

“Dohodnutá úroveň poskytovaných služieb” na strane 48
Táto téma sa venuje niektorým dôležitým aspektom dohodnutej úrovne poskytovaných služieb (SLA), ktoré môžu vplývať na implementáciu kvality služieb (QoS). QoS je sieťové riešenie. Ak chcete získať sieťovú prioritu mimo vašej súkromnej siete, pravdepodobne potrebujete s vaším poskytovateľom internetových služieb (ISP) uzavrieť zmluvu o dohodnutej úrovni poskytovaných služieb.

“Diferencované služby” na strane 2
Toto je prvý typ politiky výstupnej šírky pásma, ktorú môžete vytvoriť vo vašom operačnom systéme. Diferencovaná služba rozdeľuje vašu premávku do tried. Ak chcete uplatňovať politiku diferencovanej služby, musíte určiť, ako chcete klasifikovať vašu sieťovú prevádzku a ako chcete zaobchádzať s jednotlivými triedami.

Súvisiaci odkaz

“Monitorovanie QoS” na strane 55
Pomocou monitora kvality služieb (QoS) môžete analyzovať IP prevádzku vo vašom systéme.

Podrobnosti scenára: Nastavenie pripojenia VPN medzi dvomi hostiteľmi

Táto téma obsahuje informácie o nastavení pripojení VPN medzi dvomi hostiteľmi.

Pri konfigurácii VPN vám pomôže téma Scenár: Základné prepojenie dvoch firiem.

Podrobnosti scenára: Vytvorenie politiky diferencovaných služieb

Táto téma obsahuje informácie o vytvorení politiky diferencovanej služby.

1. V System i Navigator rozviňte položky ***váš systém*** → **Network** → **IP Policies**.
2. Kliknite pravým tlačidlom na **Quality of Service** a vyberte **Configuration** na otvorenie okna Quality of Service Server Configuration.
3. V okne konfigurácie servera QoS pravým tlačidlom kliknite na IntServ a vyberte **New Policy**, aby ste spustili sprievodcu.
4. Prečítajte si uvítaciu stránku a kliknite na tlačidlo **Next**, aby ste sa dostali na stránku **Name**.
5. V poli **Name** zadajte VPN a kliknite na tlačidlo **Next**. Tiež môžete voliteľne zadať opis na lepšie zapamätanie si účelu tejto politiky.
6. Na stránke Clients vyberte **Specific address or addresses** a kliknite na **New** a definujte vášho klienta.
7. V okne New client zadajte nasledujúce informácie:
   - **Názov**: VPN_Client
   - **Adresa IP**: 192.83.63.1
   - Kliknite na tlačidlo **OK**, aby ste vytvorili klienta a zároveň sa vrátili späť do sprievodcu diferencovanou službou.

   Po kliknutí na **OK** sa vrátite späť do sprievodcu politikami. Ak ste predtým vytvorili nejakých klientov, kliknite na nich a overte si, či sú vybratí iba relevantní klienti.
8. Na stránke Server Data Request skontrolujte, či je vybraté **Any token** a **All priorities**.
9. Na stránke Applications skontrolujte, či sú vybraté **All ports** a **All**.
10. Kliknite na tlačidlo **Next**.
11. Na stránke Local IP Address použite predvolenú hodnotu a kliknite na **Next**.
12. Na stránke Differentiated Class of Service kliknite na **New**, aby ste zadefinovali charakteristiky výkonu. Otvorí sa sprievodca pre novú triedu služieb.
13. Prečítajte si Uvítaciu stránku a kliknite na tlačidlo **Next**.
14. Na stránke Name zadajte EF_VPN.
15. Na stránke Type of Service vyberte **Outbound only** a kliknite na tlačidlo **Next**. Táto trieda služby sa použije len pre politiky výstupu.

16. Na stránke Outbound DiffServ Codepoint Marking zvoľte **Class 3**. Správanie typu per-hop určuje, aký výkon získa táto prevádzka od smerovačov a iných systémov v sieti. Pri rozhodovaní vám pomôže systém pomoci umiestnený v rozhraní.
17. Na stránke Perform Outbound Traffic Metering skontrolujte, či je vybraté **Yes** a kliknite na tlačidlo **Next**.
18. Na stránke Outbound Rate Control Limits zadajte nasledujúce informácie a kliknite na tlačidlo **Next**:
    - **Veľkosť bloku tokenov**: 100 kilobitov
    - **Limit priemernej rýchlosti**: 64 megabitov za sekundu
    - **Limit špičkovej rýchlosti**: Neobmedziť
19. Na stránke Outbound Out-of-Profile Traffic vyberte **Drop UDP packets or reduce TCP congestion window** a kliknite na tlačidlo **Next**.
20. Pozrite si súhrnnú stránku triedy služieb a kliknite na tlačidlo **Finish**, aby ste sa vrátili do sprievodcu politikou.
21. Na stránke Differentiated Class of Service skontrolujte, či je vybraté **EF_VPN** a kliknite na tlačidlo **Next**.
22. Na stránke Schedule vyberte **Active during selected schedule** a kliknite na tlačidlo **New**.
23. V okne Add New Schedule zadajte nasledujúce informácie a kliknite na tlačidlo **OK**:
    - **Názov**: FirstShift
    - **Denný čas**: Aktívny v konkrétnych časoch a pridajte 9:00 až 17:00.
    - **Deň v týždni**: Aktívny v špecifické dni a vyberte pondelok až piatok.
24. Na stránke Schedule kliknite na tlačidlo **Next**.
25. Pozrite si súhrnné informácie. Ak sú správne, kliknite na tlačidlo **Finish**, aby sa vytvorila politika. Okno konfigurácie servera QoS v zozname zobrazí všetky politiky vytvorené v systéme. Po ukončení sprievodcu sa politika zobrazí v pravej časti okna.

Podrobnosti scenára: Spustenie alebo aktualizovanie servera QoS

Táto téma obsahuje informácie o spustení alebo aktualizovaní servera QoS.

V okne Quality of Service (QoS) Server Configuration vyberte **Server → Start** alebo **Server → Update**.

Podrobnosti scenára: Overenie funkčnosti politiky

Pomocou monitora skontrolujte, či sa sieťová prevádzka správa tak, ako ste ju nakonfigurovali.

1. V okne Konfigurácia servera kvality služieb (QoS) vyberte **Server → Monitor**. Otvorí sa okno Monitor QoS.
2. Vyberte typ politiky diferencovaných služieb. Zobrazia sa všetky politiky diferencovaných služieb.

   Podobne, ako v príklade 1, najzaujímavejšie polia sú polia, ktoré získavajú svoje dáta z vašej premávky. Tieto polia zahrňujú všetky bity, bity v profile a pakety mimo profilu. Bity mimo profilu označujú, že premávka presiahla nakonfigurované hodnoty politiky. Pakety v profile označujú počet paketov, ktoré táto politika manažuje. Je veľmi dôležité, aké hodnoty priradíte poľu priemernej úrovni obmedzenia. Keď pakety TCP prekročia tento limit, budú sa posielať do siete, kým okno preťaženia TCP neklesne na front paketov mimo profil. V dôsledku toho sa zvýši počet bitov mimo profilu. Rozdiel medzi touto politikou a scenárom obmedzenia premávky prehliadača je v tom, že tu sú pakety chránené pomocou protokolu VPN. Ako vidíte QoS pracuje s VPN pripojením. Popis všetkých polí monitorov nájdete v časti “Monitorovanie QoS” na strane 55.

   Poznámka: Pamätajte, že výsledky sú správne len vtedy, keď je politika aktívna. Skontrolujte plán, ktorý ste špecifikovali v rámci politiky.

Podrobnosti scenára: Zmena vlastností

Keď sa pozriete na výsledky monitora, môžete zmeniť ľubovoľné vlastnosti politiky alebo triedy služieb, aby ste dosiahli očakávané výsledky.

1. V okne Konfigurácia servera kvality služieb (QoS) vyberte adresár **DiffServ**. V zozname v pravej časti okna pravým tlačidlom kliknite na **VPN** a vyberte **Properties**, aby ste upravili politiku. Otvorí sa okno vlastností s hodnotami, ktoré riadia všeobecnú politiku.
2. Zadajte príslušné hodnoty.

3. Ak chcete upraviť triedu služby, vyberte zložku **Classes of service**. V zozname v pravej časti okna pravým tlačidlom kliknite na **EF_VPN** a vyberte **Properties**, aby ste upravili triedu služby. Otvorí sa okno vlastností QoS s hodnotami, ktoré riadia prevádzku.
4. Zadajte príslušné hodnoty.
5. V okne konfigurácie servera QoS vyberte **Server → Update** na akceptovanie zmien.

Scenár: Obmedzenie vstupných pripojení

Ak potrebujete mať pod kontrolou požiadavky na vstupné pripojenia do vášho systému, použite politiku povolenia vstupu.

Situácia

Vaše prostriedky webového servera sú preťažené požiadavkami od klientov vstupujúcimi do vašej siete. Musíte spomaliť prichádzajúcu premávku HTTP do vášho webového servera na lokálnom rozhraní 192.168.1.1. Kvalita služby (QoS) vám pomôže obmedziť počet akceptovaných pokusov o vstupné pripojenie, a to na základe atribútov pripojení (napríklad IP adresy) pre váš systém. Dosiahnete to prostredníctvom politiky povolenia vstupu, ktorá obmedzuje počet akceptovaných vstupných pripojení.

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

Obrázok 6. Obmedzenie prichádzajúcich pripojení TCP

Ciele

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

Konfigurácia

Tieto témy zobrazujú spôsob, ako vytvoriť prichádzajúce politiku prístupu.

Súvisiaci odkaz

"Monitorovanie QoS" na strane 55
Pomocou monitora kvality služieb (QoS) môžete analyzovať IP prevádzku vo vašom systéme.

Podrobnosti scenára: Vytvorenie politiky povolenia vstupu

Táto téma obsahuje informácie o vytvorení politiky povolenia vstupu na systéme.

1. V System i Navigator rozviňte položky ***váš systém*** → **Network** → **IP Policies**.
2. Kliknite pravým tlačidlom na **Quality of Service** a vyberte **Configuration** na otvorenie okna Quality of Service Server Configuration.
3. V okne konfigurácie servera QoS pravým tlačidlom kliknite na **Inbound Admission Policies** a vyberte **New Policy**, aby ste spustili sprievodcu.
4. Prečítajte si Uvítaciu stránku a kliknite na tlačidlo **Next**.
5. V poli **Name** zadajte Restrict_TheirCo a kliknite na tlačidlo **Next**. Tiež môžete voliteľne zadať opis na lepšie zapamätanie si účelu tejto politiky.
6. Na stránke Clients vyberte **Specific address or addresses** a kliknite na **New** a definujte vášho klienta.
7. V okne New client zadajte nasledujúce informácie:
   - **Názov**: Their_Co
   - **Rozsah adries IP**: 10.1.1.1 až 10.1.1.10
   - Kliknite na tlačidlo **OK**, aby ste vytvorili klienta a zároveň sa vrátili späť do sprievodcu politikou.

   Po kliknutí na **OK** sa vrátite späť do sprievodcu politikami. Ak ste predtým vytvorili nejakých klientov, zrušte ich označenie a overte si, či sú vybratí iba relevantní klienti.
8. Na stránke Uniform Resource Identifier (URI) skontrolujte, či je vybratá možnosť **Any URI** a kliknite na **Next**.
9. Na stránke Applications vyberte **Specific port, range of ports, or server type** a kliknite na **New**.
10. V okne New Application zadajte nasledujúce informácie a kliknite na tlačidlo **OK** na návrat do sprievodcu:
    - **Názov**: HTTP
    - **Port**: 80
11. Kliknite na tlačidlo **Next** a otvorte stránku Codepoint.
12. Na stránke Codepoint skontrolujte, či je vybraté **All codepoints** a kliknite na tlačidlo **Next**.
13. Na stránke Local IP Address vyberte **IP address** a vyberte rozhranie, na ktoré prichádzajú požiadavky do vášho lokálneho systému. V tomto príklade je to adresa 192.168.1.1.
14. Na stránke Class of Service kliknite na **New**, aby ste zadefinovali charakteristiky výkonu. Otvorí sa sprievodca pre novú triedu služieb.
15. Prečítajte si Uvítaciu stránku a kliknite na tlačidlo **Next**.
16. Na stránke Name zadajte **inbound** a kliknite na tlačidlo **Next**. Tiež môžete voliteľne pridať opis na lepšie zapamätanie si účelu tejto triedy služby.
17. Na stránke Type of Service vyberte **Inbound only**. Táto trieda služby sa použije len pre politiky vstupu.
18. Na stránke Inbound Limits zadajte nasledujúce informácie a kliknite na tlačidlo **Next**:
    - **Priemerný počet okamžitých pripojení**: 50 za sekundu
    - **Nárazový limit pripojení**: 50 pripojení
    - **Priorita**: Stredná
19. Kliknite na tlačidlo **Finish**, aby ste sa vrátili do sprievodcu politikou.
20. Na stránke Class of service skontrolujte, či je vybratá trieda služby, ktorú ste práve vytvorili a kliknite na tlačidlo **Next**.
21. Na stránke Schedule vyberte **Active during selected schedule** a kliknite na tlačidlo **New**.
22. V okne New Schedule zadajte nasledujúce informácie a kliknite na tlačidlo **OK**:
    - **Názov**: FirstShift
    - **Denný čas**: Aktívny v konkrétnych časoch a pridajte 9:00 až 17:00.
    - **Deň v týždni**: Aktívny v špecifické dni a vyberte pondelok až piatok.

23. Na stránke Schedules kliknite na tlačidlo **Next**.
24. Pozrite si súhrnné informácie. Ak sú správne, kliknutím na **Finish** vytvorte politiku. Konfigurácia servera QoS vypíše všetky politiky vytvorené na systéme. Po ukončení sprievodcu sa politika zobrazí v pravej časti okna.

    Dokončili ste konfiguráciu politiky povolenia vstupu. Nasledujúci krok je spustenie alebo aktualizácia servera.

Podrobnosti scenára: Spustenie alebo aktualizovanie servera QoS

Táto téma obsahuje informácie o spustení alebo aktualizovaní servera QoS.

V okne Quality of Service (QoS) Server Configuration vyberte **Server → Start** alebo **Server → Update**.

Podrobnosti scenára: Overenie funkčnosti vašej politiky

Táto téma obsahuje informácie o použití monitora, aby ste si overili, či vaša politika funguje tak, ako ste ju nakonfigurovali.

1. V okne Konfigurácia kvality služieb (QoS) vyberte **Server → Monitor**. Otvorí sa okno Monitor QoS.
2. Vyberte typ politiky povolenie vstupu. Zobrazia sa všetky politiky povolenia vstupu. Zo zoznamu vyberte **Restrict_TheirCo**.

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

   Hodnota, ktorú priradíte poľu **Average Connection Request Rate**, je tiež dôležitá. Keď pakety prekročia túto hranicu, systém ich začne ukončovať. V dôsledku toho sa zvýši počet ukončených požiadaviek. To vám naznačí, že politika sa správa tak, ako bola nakonfigurovaná. Popis všetkých polí monitorov nájdete v časti “Monitorovanie QoS” na strane 55.

   Poznámka: Pamätajte, že výsledky sú správne len vtedy, keď je politika aktívna. Skontrolujte plán, ktorý ste špecifikovali v rámci politiky.

Podrobnosti scenára: Zmena vlastností

Keď sa pozriete na výsledky monitora, môžete zmeniť ľubovoľné vlastnosti politiky alebo triedy služieb, aby ste dosiahli očakávané výsledky.

1. V okne Konfigurácia servera kvality služieb (QoS) vyberte adresár **Vstup**. V zozname v pravej časti okna pravým tlačidlom kliknite na **Restrict_TheirCo** a vyberte **Properties**, aby ste upravili politiku. Otvorí sa okno vlastností s hodnotami, ktoré riadia všeobecnú politiku.
2. Zmeňte príslušné hodnoty.
3. Ak chcete upraviť triedu služby, vyberte zložku **Classes of service**. V zozname v pravej časti okna pravým tlačidlom kliknite na **inbound** a vyberte **Properties**, aby ste upravili triedu služby. Otvorí sa okno vlastností QoS s hodnotami, ktoré riadia prevádzku.
4. Zadajte príslušné hodnoty.
5. V okne konfigurácie servera QoS vyberte **Server → Update** na akceptovanie zmien.

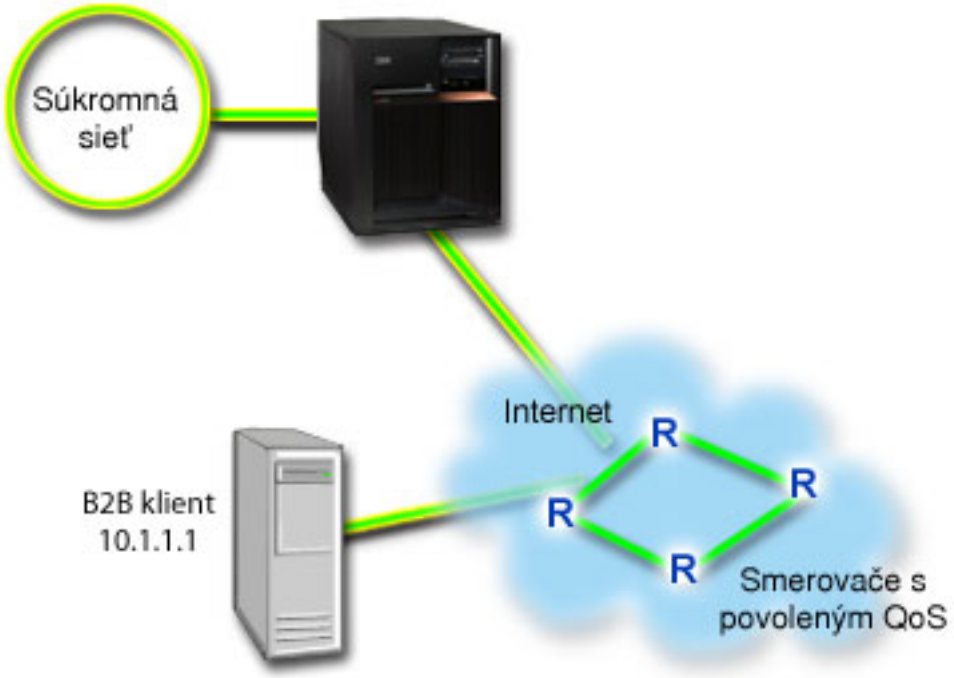
Scenár: Predvídateľná prevádzka B2B

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

Situácia

Oddelenie predaja nahlásilo, že sieťová prevádzka nefunguje tak, ako očakávali. Operačný systém i5/OS vo vašej firme sa nachádza v prostredí business-to-business (B2B), ktoré vyžaduje predvídateľné služby on-demand. Potrebujete poskytovať predpovedateľné transakcie vašim zákazníkom. Odbytovej jednotke chcete teda pre jeho objednávkovú aplikáciu počas najrušnejších hodín dňa (medzi 1O.00 a 16.OO h) poskytnúť vyššiu kvalitu služby (QoS).

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



Obrázok 7. Politika integrovaných služieb ku klientovi B2B prostredníctvom smerovačov podporujúcich protokol RSVP

Ciele

Služba riadeného zaťaženia podporuje aplikácie, ktoré sú veľmi citlivé na preťažené siete, ale dokážu zniesť malé straty alebo oneskorenie. Ak aplikácia používa službu riadeného zaťaženia, jej výkon nebude trpieť zvýšením zaťaženia siete. Premávku bude poskytovať služba, ktorá pripomína normálnu premávku v sieti za menej náročných podmienok. Pretože konkrétne táto aplikácia je voči určitému oneskoreniu tolerantná, rozhodnete sa použiť politiku integrovaných služieb pomocou služby riadeného zaťaženia.

Politiky integrovaných služieb tiež vyžadujú, aby smerovače v celej komunikačnej ceste podporovali RSVP.

Nevyhnutné podmienky a predpoklady

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

- **Aplikácie podporujúce RSVP**

  Pretože váš systém neobsahuje žiadne aplikácie podporujúce RSVP, musíte si napísať vlastné. Ak si chcete napísať svoje vlastné aplikácie, použite aplikačné programové rozhranie RSVP, aplikačné programové rozhrania soketu qtoq QoS alebo aplikačné programové rozhrania integrovaných služieb.
- **Smerovače a systémy v sieťovej ceste, podporujúce RSVP**

  QoS je sieťové riešenie. Ak si nie ste istý, či má celá sieť schopnosti podporujúce RSVP, i tak môžete vytvoriť politiku integrovanej služby a priradiť jej určitú prioritu pomocou označenia; túto prioritu však nemožno garantovať.
- **Dohodnutá úroveň poskytovaných služieb**

  S vašim poskytovateľom internetových služieb máte zmluvu o dohodnutej úrovni poskytovaných služieb (SLA), ktorá má zaručiť, aby politiky získali požadovanú prioritu. V systéme vytvorená politika QoS umožňuje, aby

prevádzka (stanovená v politike) získala v sieti určitú prioritu. Táto politika QoS nezaručuje prioritu a je závislá od vašej zmluvy o úrovni služieb. V skutočnosti vám používanie politík QoS môže pomôcť vyjednať určité dohodnuté úrovne služieb a prenosové rýchlosti.

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

Konfigurácia

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

Súvisiace koncepty

"Typy integrovaných služieb" na strane 9
Sú dva typy integrovaných služieb: riadené zaťaženie a garantovaná služba.

"Integrované služby" na strane 6
Druhý typ politiky výstupnej šírky pásma, ktorú môžete vytvoriť vo vašom operačnom systéme, je politika integrovanej služby. Integrovaná služba poskytuje IP aplikáciám schopnosť požadovať a vyhradiť si frekvenčné pásmo pomocou protokolu ReSerVation Protocol (RSVP) a aplikačných programových rozhraní kvality služby (QoS).

"API rozhrania kvality služieb" na strane 16
Táto téma obsahuje informácie o protokoloch a rozhraniach API, a tiež požiadavky na smerovač, ktorý je povolený pre protokol ReSerVation (RSVP). Medzi rozhrania API kvality služieb (QoS) patrí API rozhranie RAPI, API rozhranie soketu qtoq, sendmsg() a API rozhrania monitora.

"Dohodnutá úroveň poskytovaných služieb" na strane 48
Táto téma sa venuje niektorým dôležitým aspektom dohodnutej úrovne poskytovaných služieb (SLA), ktoré môžu vplývať na implementáciu kvality služieb (QoS). QoS je sieťové riešenie. Ak chcete získať sieťovú prioritu mimo vašej súkromnej siete, pravdepodobne potrebujete s vaším poskytovateľom internetových služieb (ISP) uzavrieť zmluvu o dohodnutej úrovni poskytovaných služieb.

Súvisiaci odkaz

"Monitorovanie QoS" na strane 55
Pomocou monitora kvality služieb (QoS) môžete analyzovať IP prevádzku vo vašom systéme.

Podrobnosti scenára: Vytvorenie politiky integrovaných služieb

Táto téma obsahuje informácie o vytvorení politiky integrovanej služby na systéme.

1. V System i Navigator rozviňte položky ***váš systém*** → **Network** → **IP Policies**.
2. Kliknite pravým tlačidlom na **Quality of Service** a vyberte **Configuration** na otvorenie okna Quality of Service Server Configuration.
3. V okne konfigurácie servera QoS pravým tlačidlom kliknite na typ politiky IntServ a vyberte **New Policy**, aby ste spustili sprievodcu.
4. Prečítajte si Uvítaciu stránku a kliknite na tlačidlo **Next**, aby ste sa dostali na stránku **Name**.
5. V poli **Name** zadajte B2B_CL a kliknite na tlačidlo **Next**. Tiež môžete voliteľne zadať opis na lepšie zapamätanie si účelu tejto politiky.
6. Na stránke Clients vyberte **Specific address or addresses** a kliknite na **New** a definujte vášho klienta.
7. V okne New Client zadajte nasledujúce informácie:
   - **Názov**: CL_client
   - **Adresa IP**: 10.1.1.1
   - Kliknite na tlačidlo **OK**, aby ste vytvorili klienta a zároveň sa vrátili späť do sprievodcu politikou.

   Po kliknutí na **OK** sa vrátite späť do sprievodcu politikami. Ak ste predtým vytvorili nejakých klientov, zrušte ich označenie a overte si, či sú vybratí iba relevantní klienti.
8. V okne New Application zadajte nasledujúce informácie a kliknite na tlačidlo **OK** na návrat do sprievodcu:
   - **Názov**: business_app
   - **Rozsah portov**: 7000-8000

9. Na stránke Applications vyberte **Protocol** a skontrolujte, či je vybraté **TCP**. Kliknite na tlačidlo **Next**.

   Poznámka: Aplikácia, ktorú vyberiete pre politiku integrovaných služieb musí byť zapísaná na používanie API protokolu Resource Reservation Setup Protocol (RAPI) alebo na API qtoq soketov. Spolu s protokolom ReSerVation Protocol (RSVP) vykonávajú tieto rozhrania API rezerváciu integrovaných služieb v sieti. Ak nevyužijete tieto rozhrania API, aplikácia neprijme žiadnu prioritu ani záruku. Tiež je dôležité uvedomiť si, že táto politika umožňuje vašim aplikáciám prijímať priority prostredníctvom siete, ale nedokáže to zaručiť. Všetky smerovače a systémy v ceste komunikačnej prevádzky musia tiež používať protokol RSVP na garantovanie rezervácie. Rezervácia medzi dvomi koncami závisí na súčinnosti celej siete.
10. Na stránke Local IP Address použite predvolenú hodnotu a kliknite na **Next**.
11. Na stránke Integrated Services Type vyberte **Controlled load** a kliknite na tlačidlo **Next**.
12. Na stránke Integrated Services Marking vyberte **No, do not assign a per-hop behavior** a kliknite na tlačidlo **Next**.
13. Na stránke Integrated Services Performance Limits zadajte nasledujúce informácie a kliknite na tlačidlo **Next**:
    - **Maximálny počet tokov**: 5
    - **Limit rýchlosti tokenov (R)**: Neobmedziť
    - **Veľkosť bloku tokenov**: 100 kilobitov
    - **Limit rýchlosti tokenov (R)**: 25 megabitov za sekundu
14. Na stránke Schedule vyberte **Active during selected schedule** a kliknite na tlačidlo **New**.
15. Na stránke New Schedule zadajte nasledujúce informácie a kliknite na tlačidlo **OK**:
    - **Názov**: primetime
    - **Denný čas**: Aktívny v konkrétnych časoch a pridajte 10:00 až 16:00.
    - **Deň v týždni**: Aktívny v špecifické dni a vyberte pondelok až piatok.
16. Na stránke Schedules kliknite na tlačidlo **Next**.
17. Skontrolujte súhrnné informácie. Ak sú správne, kliknite na tlačidlo **Finish**, aby sa vytvorila politika. Hlavné rozhranie QoS vypíše všetky politiky vytvorené na systéme. Po ukončení sprievodcu sa politika zobrazí v pravej časti okna.

Dokončili ste konfiguráciu politiky integrovanej služby. Nasledujúci krok je spustenie alebo aktualizácia servera.

Podrobnosti scenára: Spustenie alebo aktualizovanie servera QoS

Táto téma obsahuje informácie o spustení alebo aktualizovaní servera QoS.

V okne Quality of Service (QoS) Server Configuration vyberte **Server → Start** alebo **Server → Update**.

Podrobnosti scenára: Overenie funkčnosti politiky

Táto téma obsahuje informácie o použití monitora, aby ste si overili, či politika funguje tak, ako ste ju nakonfigurovali.

1. V okne Konfigurácia servera kvality služieb (QoS) vyberte **Server → Monitor**. Otvorí sa okno Monitor QoS.
2. Vyberte typ politiky integrovaných služieb. Zobrazia sa všetky politiky integrovaných služieb.

   Najzaujímavejšie polia sú polia, ktoré získavajú svoje dáta z vašej premávky. Nezabudnite skontrolovať polia celkový počet bitov, bity v profile a pakety v profile. Bity mimo profil označujú, že sa oneskoruje alebo ruší iná premávka, aby sa splnili požiadavky integrovanej politiky služieb. Podrobný popis polí monitora nájdete v “Monitorovanie QoS” na strane 55.

   Poznámka: Pamätajte, že výsledky sú správne len vtedy, keď je politika aktívna. Skontrolujte plán, ktorý ste špecifikovali v rámci politiky. Okrem toho, monitor ukazuje iba politiky integrovaných služieb po spustení aplikácií. Pred monitorovaním je potrebné vytvoriť rezerváciu protokolu ReSerVation Protocol (RSVP).

Podrobnosti scenára: Zmena vlastností

Keď sa pozriete na výsledky monitora, môžete zmeniť ľubovoľné vlastnosti politiky, aby ste dosiahli očakávané výsledky.

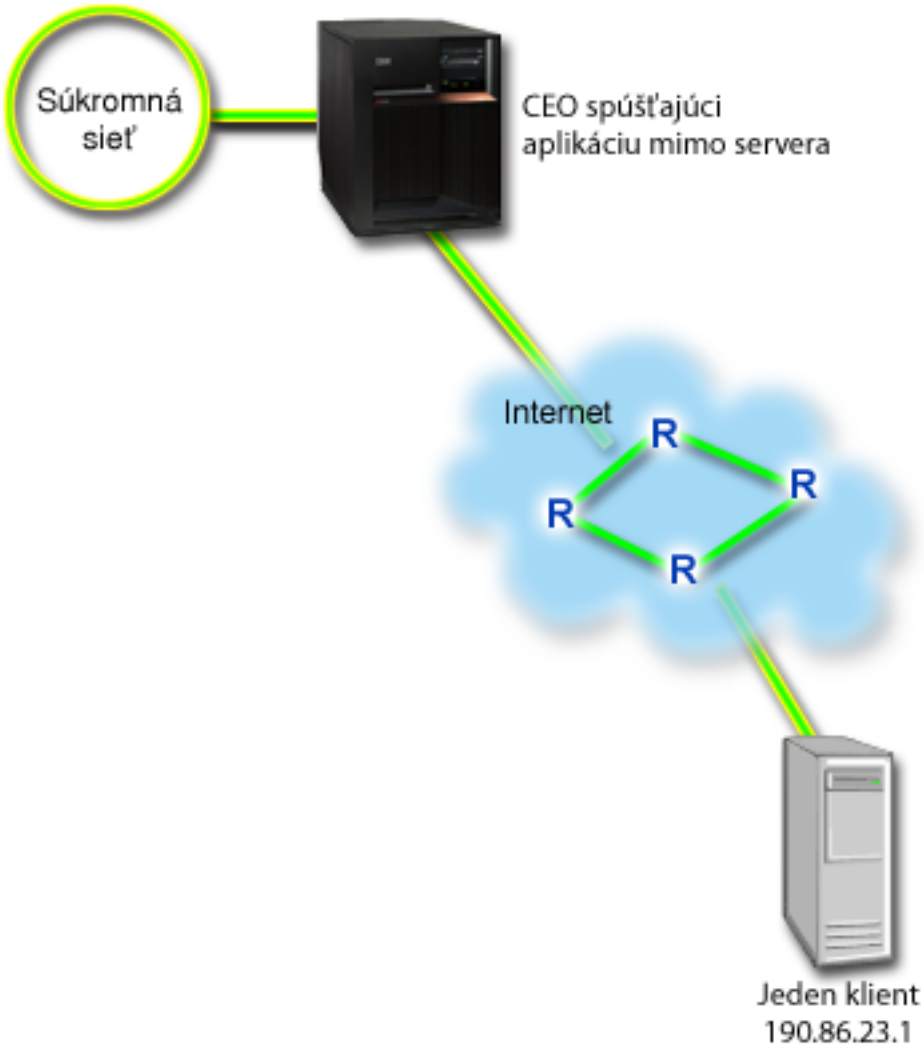
1. V okne Konfigurácia servera kvality služieb (QoS) vyberte adresár **IntServ**. V zozname v pravej časti okna pravým tlačidlom kliknite na **B2B_CL** a vyberte **Properties**, aby ste upravili politiku. Otvorí sa okno vlastností s hodnotami, ktoré riadia všeobecnú politiku.
2. Zadajte príslušné hodnoty.
3. V okne konfigurácie servera QoS vyberte **Server → Update** na akceptovanie zmien.

Scenár: Dedikované doručenie (IP telefónia)

Ak potrebujete vyhradené doručenie a chcete vyžadovať rezerváciu, použijete politiku integrovaných služieb. Môžete vytvoriť dva typy politík integrovaných služieb: garantované a s riadeným zaťažením. V tomto príklade sa používa garantovaná služba.

Situácia

Generálny riaditeľ vašej firmy sa ide v živom vysielaní spojiť s klientom, ktorý sa na nachádza v inom regióne, v čase medzi 13:00 a and 14:00. Musíte zabezpečiť garantovanú šírku pásma pre telefonické IP spojenie, aby počas spojenia nedošlo k prerušeniu. V tomto scenári je aplikácia umiestnená na serveri.



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

Ciele

Keďže aplikácia, ktorú sa riaditeľ chystá použiť, vyžaduje hladký a neprerušovaný prenos, rozhodli ste sa použiť politiku garantovanej integrovanej služby. Garantovaná služba riadi maximálne oneskorenie pri radení do frontu, aby sa pakety nezdržali viac než stanovuje lehota.

Nevyhnutné podmienky a predpoklady

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

- **Aplikácie podporujúce RSVP**

  Pretože váš systém neobsahuje žiadne aplikácie podporujúce RSVP, musíte si napísať vlastné. Ak si chcete napísať svoje vlastné aplikácie, použite aplikačné programové rozhranie protokolu ReSerVation alebo aplikačné programové rozhrania soketu qtoq QoS. Bližšie informácie nájdete v “API rozhrania kvality služieb” na strane 16 v časti venovanej rozhraniam API pre integrované služby.
- **Smerovače a systémy v sieťovej ceste, podporujúce RSVP**

  QoS je sieťové riešenie. Ak si nie ste istý, či má celá sieť schopnosti podporujúce RSVP, i tak môžete vytvoriť politiku integrovanej služby a priradiť jej určitú prioritu pomocou označenia; túto prioritu však nemožno garantovať.

- **Dohodnutá úroveň poskytovaných služieb**

  S vašim poskytovateľom internetových služieb máte zmluvu o dohodnutej úrovni poskytovaných služieb (SLA), ktorá má zaručiť, aby politiky získali požadovanú prioritu. V systéme vytvorená politika QoS umožňuje, aby prevádzka (stanovená v politike) získala v sieti určitú prioritu. Táto politika QoS nezaručuje prioritu a je závislá od vašej zmluvy o úrovni služieb. V skutočnosti vám používanie politík QoS môže pomôcť vyjednať určité dohodnuté úrovne služieb a prenosové rýchlosti.

Konfigurácia

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

Súvisiace koncepty

"Typy integrovaných služieb" na strane 9
Sú dva typy integrovaných služieb: riadené zaťaženie a garantovaná služba.

"Integrované služby" na strane 6
Druhý typ politiky výstupnej šírky pásma, ktorú môžete vytvoriť vo vašom operačnom systéme, je politika integrovanej služby. Integrovaná služba poskytuje IP aplikáciám schopnosť požadovať a vyhradiť si frekvenčné pásmo pomocou protokolu ReSerVation Protocol (RSVP) a aplikačných programových rozhraní kvality služby (QoS).

"Dohodnutá úroveň poskytovaných služieb" na strane 48
Táto téma sa venuje niektorým dôležitým aspektom dohodnutej úrovne poskytovaných služieb (SLA), ktoré môžu vplývať na implementáciu kvality služieb (QoS). QoS je sieťové riešenie. Ak chcete získať sieťovú prioritu mimo vašej súkromnej siete, pravdepodobne potrebujete s vaším poskytovateľom internetových služieb (ISP) uzavrieť zmluvu o dohodnutej úrovni poskytovaných služieb.

Súvisiaci odkaz

"Monitorovanie QoS" na strane 55
Pomocou monitora kvality služieb (QoS) môžete analyzovať IP prevádzku vo vašom systéme.

Podrobnosti scenára: Vytvorenie politiky integrovaných služieb

Táto téma obsahuje informácie o vytvorení politiky integrovanej služby na systéme.

1. V System i Navigator rozviňte položky ***váš systém*** → **Network** → **IP Policies**.
2. Kliknite pravým tlačidlom na **Quality of Service** a vyberte **Configuration** na otvorenie okna Quality of Service Server Configuration.
3. V okne konfigurácie servera QoS pravým tlačidlom kliknite na typ politiky IntServ a vyberte **New Policy**, aby ste spustili sprievodcu.
4. Prečítajte si Uvítaciu stránku a kliknite na tlačidlo **Next**, aby ste sa dostali na stránku **Name**.
5. V poli **Name** zadajte CEO_guaranteed a kliknite na tlačidlo **Next**. Tiež môžete voliteľne zadať opis na lepšie zapamätanie si účelu tejto politiky.
6. Na stránke Clients vyberte **Specific address or addresses** a kliknite na **New** a definujte vášho klienta.
7. V okne New Client zadajte nasledujúce informácie:
   - **Názov**: Branch1
   - **Adresa IP**: 190.86.23.1
   - Kliknite na tlačidlo **OK**, aby ste vytvorili klienta a zároveň sa vrátili späť do sprievodcu integrovanou službou.

   Po kliknutí na tlačidlo OK sa vrátite do sprievodcu politikou. Ak ste predtým vytvorili nejakých klientov, zrušte ich označenie a overte si, či sú vybratí iba relevantní klienti.Na stránke Applications vyberte **Specific port, range of ports, or server type** a kliknite na **New**.
8. V okne New Application zadajte nasledujúce informácie a kliknite na tlačidlo **OK** na návrat do sprievodcu:
   - **Názov**: Telefónia IP
   - **Port**: 2427
9. Na stránke Applications vyberte **Protocol** a skontrolujte, či je vybraté **TCP**. Kliknite na tlačidlo **Next**.

Poznámka: Aplikácia, ktorú vyberiete pre politiku integrovaných služieb musí byť zapísaná na používanie rozhrania API protokolu Resource Reservation Setup Protocol (RAPI) alebo rozhrania API qtoq soketov. Spolu s protokolom ReSerVation Protocol (RSVP) vykonávajú tieto rozhrania API rezerváciu integrovaných služieb v sieti. Ak nevyužijete tieto rozhrania API, aplikácia neprijme žiadnu prioritu alebo záruku. Tiež je dôležité uvedomiť si, že táto politika umožňuje vašim aplikáciám prijímať priority prostredníctvom siete, ale nedokáže to zaručiť. Všetky smerovače a servery v ceste komunikačnej prevádzky musia tiež používať protokol RSVP na garantovanie rezervácie. Rezervácia medzi dvomi koncami závisí na súčinnosti celej siete.

10. Na stránke Local IP Address použite predvolenú hodnotu **All IP addresses**.
11. Na stránke Integrated Services Type vyberte **Guaranteed** a kliknite na tlačidlo **Next**.
12. Na stránke Integrated Services Marking vyberte **No, do not assign a per-hop behavior** a kliknite na tlačidlo **Next**.
13. Na stránke Integrated Services Performance Limits zadajte nasledujúce informácie a kliknite na tlačidlo **Next**:
    - **Maximálny počet tokov**: 1
    - **Limit agregovanej šírky pásma (R)**: Neobmedziť
    - **Veľkosť bloku tokenov**: 100 kilobitov
    - **Limit šírky pásma (R)**: 16 megabitov za sekundu
14. Na stránke Schedule vyberte **Active during selected schedule** a kliknite na tlačidlo **New**.
15. Na stránke New Schedule zadajte nasledujúce informácie a kliknite na tlačidlo **OK**:
    - **Názov**: one_hour
    - **Denný čas**: Aktívny v konkrétnych časoch a pridajte 13:00 až 14:00.
    - **Deň v týždni**: Aktívny v špecifický deň a vyberte pondelok.
16. Na stránke Schedule kliknite na tlačidlo **Next**.
17. Skontrolujte súhrnné informácie. Ak sú správne, kliknite na tlačidlo **Finish**, aby sa vytvorila politika. Hlavné okno konfigurácie servera QoS v zozname zobrazí všetky politiky vytvorené v serveri. Po ukončení sprievodcu sa politika zobrazí v pravej časti okna.

Dokončili ste konfiguráciu politiky integrovanej služby. Nasledujúci krok je spustenie alebo aktualizácia servera.

Podrobnosti scenára: Spustenie alebo aktualizovanie servera QoS

Táto téma obsahuje informácie o spustení alebo aktualizovaní servera QoS.

V okne Quality of Service (QoS) Server Configuration vyberte **Server → Start** alebo **Server → Update**.

Podrobnosti scenára: Overenie funkčnosti politiky

Táto téma obsahuje informácie o použití monitora, aby ste si overili, či politika funguje tak, ako ste ju nakonfigurovali.

1. V okne Konfigurácia servera kvality služieb (QoS) vyberte **Server → Monitor**. Otvorí sa okno Monitor QoS.
2. Vyberte zložku typu politiky integrovaných služieb. Zobrazia sa všetky politiky integrovaných služieb.

   Najzaujímavejšie polia sú merané polia, ktoré získavajú svoje dáta z vašej premávky. Tieto polia zahrňujú všetky bity, bity v profile a pakety v profile. Bity mimo profilu indikujú, že ostatná premávka sa oneskoruje alebo, že neuspokojila požiadavky tejto politiky integrovaných služieb. Popis všetkých polí monitorov nájdete v časti “Monitorovanie QoS” na strane 55.

   Poznámka: Pamätajte, že výsledky sú správne, iba keď je politika aktívna. Skontrolujte plán, ktorý ste špecifikovali v rámci politiky. Okrem toho, monitor ukazuje iba politiky integrovaných služieb po spustení aplikácií. Pred monitorovaním je potrebné vytvoriť rezerváciu protokolu ReSerVation Protocol (RSVP).

Podrobnosti scenára: Zmena vlastností

Keď sa pozriete na výsledky monitora, môžete zmeniť ľubovoľné vlastnosti politiky, aby ste dosiahli očakávané výsledky.

1. V okne Konfigurácia servera kvality služieb (QoS) vyberte adresár **IntServ**. V zozname v pravej časti okna pravým tlačidlom kliknite na **CEO_guaranteed** a vyberte **Properties**, aby ste upravili politiku. Otvorí sa okno vlastností s hodnotami, ktoré riadia všeobecnú politiku.
2. Zadajte príslušné hodnoty.
3. V okne konfigurácie servera QoS vyberte **Server → Update** na akceptovanie zmien.

Scenár: Monitorovanie aktuálnej sieťovej štatistiky

V sprievodcoch potrebujete nastaviť výkonové limity, založené na jednotlivých sieťových požiadavkách.

Ciele

Na nastavenie týchto limitov musíte reálne poznať aktuálny výkon vašej siete. Keďže sa pokúšate konfigurovať politiky kvality služby (QoS), zrejme už máte jasnú predstavu o tom, aké sú aktuálne potreby vašej siete. Ak chcete presne určiť, aké rýchlostné limity máte nastaviť, napríklad rýchlosť bloku tokenov, môžete monitorovať celú prevádzku vo vašom systéme.

Riešenie

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

Súvisiace koncepty

"Limity bloku tokenov a šírky pásma" na strane 9
Limity pre blok tokenov a šírku pásma sú známe pod pojmom limity pre výkon. Tieto výkonové limity pomáhajú garantovať doručovanie paketov v politikách výstupnej šírky pásma u integrovanej rovnako ako diferencovanej služby.

"Priemerný počet okamžitých pripojení a prah zahltenia pripojenia" na strane 15
Počet okamžitých pripojení a prah zahltenia predstavujú limity pre pripojenie. Tieto limity pomáhajú obmedziť vstupné pripojenia, ktoré sa snažia vstúpiť do vášho systému. Limity pripojení sa nastavujú v triede služby, ktorá sa používa v politike povolenia vstupu.

Súvisiaci odkaz

"Monitorovanie QoS" na strane 55
Pomocou monitora kvality služieb (QoS) môžete analyzovať IP prevádzku vo vašom systéme.

Podrobnosti scenára: Otvorenie QoS v System i Navigator

Táto téma obsahuje informácie o tom, ako otvoríte QoS v rámci System i Navigator.

1. V System i Navigator rozviňte položky ***váš systém*** **→ Network → IP Policies**.
2. Pravým tlačidlom myši kliknite na **Quality of Service** a kliknite na **Configuration**.
3. Rozviňte **Outbound bandwidth policies**.
4. Kliknite pravým tlačidlom na **DiffServ** a zvoľte **New Policy**. Otvorí sa sprievodca pre novú politiku DiffServ.

Podrobnosti scenára: Vytvorenie politiky diferencovaných služieb

Keďže chcete zhromaždiť čo najviac prevádzky prichádzajúcej do vašej siete, môžete volať sieť politík. Použite všetky IP adresy, všetky porty, všetky lokálne IP adresy a všetky časy (ak je to vhodné).

Počas prechodu sprievodcom použite nasledujúce nastavenia:

```
Názov: Sieť (akýkoľvek názov, ktorý priradíte)
Klient : Všetky IP adresy
Aplikácia: Všetky porty
Protokol: Všetky protokoly
Plán: Všetky časy
```

System i Navigator vypíše všetky politiky diferencovaných služieb, vytvorené vo vašom systéme.

Podrobnosti scenára: Dokončenie novej triedy služieb

Sprievodca vás požiada, aby ste stanovili správanie per-hop, obmedzenia výkonu a spracovanie prevádzky nezapadajúcej do profilu. To sa definuje v triede služieb. Zvoľte čo najvyššie hodnoty, aby ste povolili čo najväčší možný objem prevádzky.

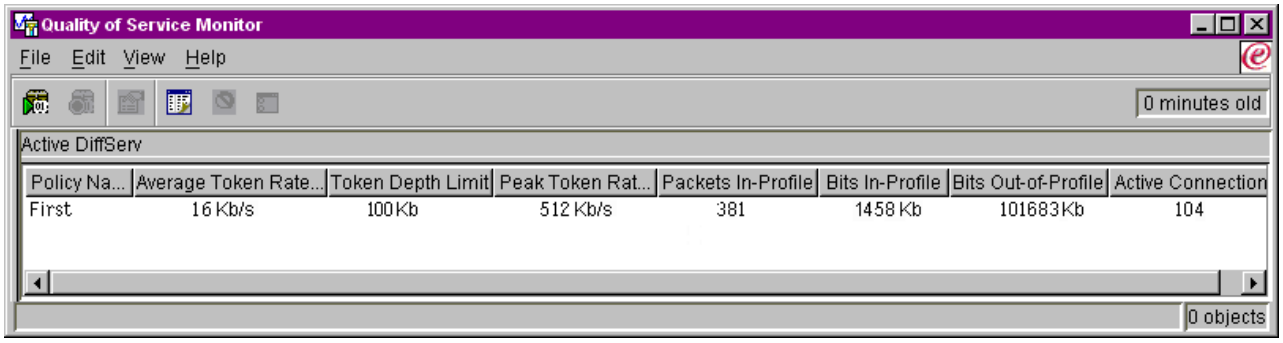
Triedy služieb v skutočnosti určujú výkonové úrovne, ktoré táto prevádzka prijíma zo smerovača. Vašu triedu služieb môžete nazvať neobmedzená, aby bolo jasné, že táto prevádzka má získať vyššiu úroveň služby. System i Navigator uvádza všetky triedy služieb, zadefinované vo vašom systéme.

Podrobnosti scenára: Monitorovanie politiky

Pomocou monitora môžete skontrolovať, či sa sieťová prevádzka správa podľa toho, ako ste ju nakonfigurovali v politike.

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

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



Obrázok 9. Monitor kvality služieb (QoS)

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

Hodnoty, ktoré priradíte poľu **Limit priemernej rýchlosti tokenov**, sú tiež dôležité. Keď pakety prekročia túto hranicu, systém ich začne ukončovať. V dôsledku toho sa zvýši počet bitov mimo profilu. To vám naznačí, že politika sa správa tak, ako bola nakonfigurovaná. Ak chcete zmeniť počet bitov mimo profilu, musíte tomu prispôsobiť limity výkonu. Popis všetkých polí monitorov nájdete v časti “Monitorovanie QoS” na strane 55.

Podrobnosti scenára: Zmena hodnôt

Po ukončení monitorovania môžete zmeniť ľubovoľné hodnoty, ktoré ste predtým vybrali. Pravým tlačidlom kliknite na názov triedy služby, ktorý ste v tejto politike vytvorili. Keď zvolíte **Properties**, otvorí sa okno vlastností QoS s hodnotami, ktoré riadia vašu prevádzku.

Podrobnosti scenára: Opakované monitorovanie politiky

Keď si pozriete výsledky, pomocou metódy pokusu a omylu nájdite najvhodnejšie ohraničenia, aké potrebujete pre svoju sieť.

Plánovanie kvality služieb

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

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

Zváženie výkonu siete

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

Súvisiace koncepty

"Monitorovanie systémových transakcií" na strane 61
Pomocou monitora kvality služieb (QoS) si môžete overiť, či politiky QoS fungujú podľa vašej predstavy. Monitor QoS vám môže pomôcť v plánovacej fáze a vo fáze odstraňovania problémov QoS.

"Konfigurácia kvality služieb" na strane 50
Keď si naplánujete kvalitu služieb (QoS), vytvorte si vlastné politiky QoS pomocou sprievodcov v System i Navigator. Tieto témy opisujú vytvorenie politík diferencovaných služieb, integrovaných služieb a povolenia vstupu.

Požiadavky na oprávnenia

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

Potrebné sú nasledujúce oprávnenia na to, aby ste mohli konfigurovať politiky QoS, a voliteľne adresárové servery LDAP (Lightweight Directory Access Protocol).

Poskytnutie oprávnení na správu adresárového servera

Administrátor QoS musí mať nasledovné oprávnenia: oprávnenie *ALLOBJ a *IOSYSCFG. Alternatívne oprávnenia nájdete v časti Konfigurácia adresárového servera.

Poskytnutie oprávnení na spustenie TCP/IP servera

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

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

Poskytnutie oprávnení na prístup a konfiguráciu systému všetkým objektom

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

1. V System i Navigator rozviňte položky ***váš systém*** → **Users and Groups**.
2. Dvakrát kliknite na **All users**.
3. Kliknite pravým tlačidlom na užívateľský profil administrátora a vyberte **Properties**.
4. V okne Vlastnosti kliknite na **Capabilities**.
5. Na stránke Capabilities vyberte **All object access and System configuration**.
6. Kliknite na **OK** a zatvorte stránku Capabilities.
7. Kliknite na **OK**. Okno Properties sa zatvorí.

Systémové požiadavky

Kvalita služieb (QoS) je integrovanou časťou operačného systému.

Musíte splniť tieto požiadavky:

1. Inštalovať IBM TCP/IP Connectivity Utilities for i5/OS (5761-TC1).
2. Nainštalujte System i Navigator na váš osobný počítač. Počas inštalácie System i Access nezabudnite nainštalovať komponent Networking. Kvalita služieb je umiestnená pod politikami IP v rámci adresára výstavby sietí.

Súvisiace koncepty

Zoznámenie s navigátorom pre System i

Súvisiaci odkaz

“Informácie súvisiace s kvalitou služieb” na strane 65
Dokumenty Request for Comments, publikácie IBM Redbooks a ďalšie témy informačného centra obsahujú ďalšie informácie súvisiace s témami kvality služieb. Súbory PDF môžete zobraziť alebo stiahnuť.

Dohodnutá úroveň poskytovaných služieb

Táto téma sa venuje niektorým dôležitým aspektom dohodnutej úrovne poskytovaných služieb (SLA), ktoré môžu vplývať na implementáciu kvality služieb (QoS). QoS je sieťové riešenie. Ak chcete získať sieťovú prioritu mimo vašej súkromnej siete, pravdepodobne potrebujete s vaším poskytovateľom internetových služieb (ISP) uzavrieť zmluvu o dohodnutej úrovni poskytovaných služieb.

Kedy sa vyžaduje SLA

SLA potrebujete len prípade, ak vaše politiky vyžadujú prioritu mimo vašej súkromnej siete. Ak používate výstupné politiky na riadenie prevádzky, ktorá odchádza z vášho systému, nepotrebujete žiadnu garanciu služby. Napríklad môžete na systéme vytvoriť politiku, ktorá dáva jednej aplikácii vyššiu prioritu než inej aplikácii. Váš systém rozpozná túto prioritu, no iné systémy alebo zariadenia mimo vášho systému ju rozpoznať nemusia. Ak máte súkromnú sieť a nakonfigurujete smerovače tak, aby rozpoznali označenia kódových bodov (ktoré sa používajú na poskytnutie úrovne služby výstupným politikám), potom budú smerovače poskytovať prioritu prostredníctvom vašej súkromnej siete. Ak premávka opustí vašu súkromnú sieť, neexistujú už žiadne garancie. Bez SLA nemôžete riadiť, ako má sieťový hardvér zaobchádzať s prevádzkou. Mimo vašej súkromnej siete potrebujete zmluvu o SLA, aby ste garantovali prioritu pre triedu služieb alebo rezerváciu prostriedku.

Kedy sa vyžaduje SLA

Vaše politiky a rezervácie budú dobré iba tak, ako vaša najslabšia linka. Znamená to, že politiky QoS umožňujú aplikáciám prijímať prioritu v sieti. Ak však niektorý uzol, nachádzajúci sa niekde na ceste medzi klientom a serverom, nedokáže vykonať niektorú z charakteristík riadenia premávky opísaných v témach o diferencovanej alebo integrovanej službe, s vašimi politikami sa nebude zaobchádzať tak, ako si predstavujete. Ak vaša SLA neposkytne dostatok zdrojov, ani najlepšie politiky vám nepomôžu riešiť problém preťaženej siete.

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

Uistite sa, že plne rozumiete úrovni služby, ktorú reálne prijímate. Dohody formujúce premávku špecificky určujú ako sa narába s premávkou, čo sa ukončuje, označuje, formuje alebo opakovanie prenáša. Kľúčové dôvody na poskytnutie QoS zahŕňajú čakaciu dobu riadenia, nepokoj, šírku pásma, stratu paketov, dostupnosť a priepustnosť. Vaše zmluvy o službách musia byť schopné dať vašim politikám, o čo požiadajú. Overte, či dostávate taký objem služieb, aký potrebujete. Ak to tak nie je, je možné, že plytváte svojimi prostriedkami. Napríklad ak žiadate o rezervovanie 500 Kb/s na účely IP telefonovania, ale vaša aplikácia reálne potrebuje len 20 Kb/s, môže sa stať, že bude platiť navyše bez toho, aby vás ISP na to vopred upozornil.

Poznámka: Politiky QoS vám umožňujú vyjednať s ISP úrovne služieb, ktoré pomôžu znížiť vaše náklady na sieťové služby. Napríklad váš ISP vám môže garantovať určitú finančnú sadzbu, ak nepresiahnete úroveň

dohodnutej šírky pásma. Alebo si môžete rozložiť používanie politík, počas dňa použijete len časť ″x″ zo šírky pásma a počas noci časť ″y″ zo šírky pásma a dohodnete rýchlosť prenosu údajov pre každú takúto časť. Znovu, ak presiahnete šírku pásma, ISP bude vyžadovať vyššiu platbu. ISP musí súhlasiť s určitou úrovňou poskytovanej a musí byť schopný zaznamenávať, akú šírku pásma používate.

Súvisiace koncepty

“Základné pojmy” na strane 1
Skôr ako začnete používať kvalitu služieb (QoS), potrebujete porozumieť základným pojmom a konceptom QoS. Pomôže vám to zistiť, či služba spĺňa vaše potreby.

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

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

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

“Scenár: Dedikované doručenie (IP telefónia)” na strane 41
Ak potrebujete vyhradené doručenie a chcete vyžadovať rezerváciu, použijete politiku integrovaných služieb. Môžete vytvoriť dva typy politík integrovaných služieb: garantované a s riadeným zaťažením. V tomto príklade sa používa garantovaná služba.

Sieťový hardvér a softvér

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

Aplikácie

Politiky integrovanej služby vyžadujú aplikácie, ktoré povoľuje protokol RSVP. Pretože aplikácie i5/OS pôvodne nie sú povolené pre RSVP, musíte ich nastaviť na použitie RSVP. Urobíte to tak, že pomocou API rozhraní RSVP alebo API rozhraní soketu qtoq QoS napíšete špeciálne programy. Tieto programy umožnia aplikáciám používať protokol RSVP.

Sieťové uzly

Smerovače, prepínače a aj vaše operačné systémy musia byť schopné používať protokol QoS. Ak chcete použiť politiky diferencovaných služieb, vaše zariadenie musí byť povolené pre diferencované služby. To znamená, že sieťový uzol musí byť schopný klasifikovať, merať, označovať, tvarovať a prerušovať IP pakety (upravovače komunikačnej prevádzky).

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

Súvisiace koncepty

“API rozhrania kvality služieb” na strane 16
Táto téma obsahuje informácie o protokoloch a rozhraniach API, a tiež požiadavky na smerovač, ktorý je povolený pre protokol ReSerVation (RSVP). Medzi rozhrania API kvality služieb (QoS) patrí API rozhranie RAPI, API rozhranie soketu qtoq, sendmsg() a API rozhrania monitora.

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

Konfigurácia kvality služieb

Keď si naplánujete kvalitu služieb (QoS), vytvorte si vlastné politiky QoS pomocou sprievodcov v System i Navigator. Tieto témy opisujú vytvorenie politík diferencovaných služieb, integrovaných služieb a povolenia vstupu.

Sprievodcovia vás prevedú celou konfiguráciou.

Po nakonfigurovaní politík môžete použiť konfiguračné objekty v System i Navigator na úpravu konfigurácie vašej politiky. Konfiguračné objekty sú rozličné kusy, alebo časti tvoriace politiku. Keď otvoríte kvalitu služieb v System i Navigator, zobrazia sa zložky s označením klienti, aplikácie, plány, politiky, triedy služieb, správania per-hop a identifikátory URI (Uniform Resource Identifiers). Tieto objekty vám umožňujú vytvoriť politiku. Podrobnejšie informácie o týchto objektoch nájdete vo všeobecnej pomoci ku kvalite služieb v System i Navigator.

Povolenie politík QoS

Aby politiky nadobudli účinnosť, musia byť povolené. Ak použijete sprievodcov, systém politiky automaticky povolí za vás. Ak však zmeníte politiku, ktorá používa konfiguračné objekty, musíte dynamicky systém aktualizovať, aby sa politiky stali aktívnymi. Skôr, ako ich povolíte, nezabudnite skontrolovať, či sa niektoré navzájom neprekrývajú. To by mohlo spôsobiť problémy.

Súvisiace koncepty

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

Zoznámenie s navigátorom pre System i

Súvisiace úlohy

“Zoraďovanie politík QoS” na strane 52
Ak máte dve politiky, ktoré sa vzájomne prekrývajú, dôležité bude poradie vašich politík v System i Navigator.

Súvisiaci odkaz

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

Konfigurácia QoS pomocou sprievodcov

Ak chcete konfigurovať politiky kvality služieb (QoS), musíte použiť sprievodcov QoS, ktorí sa nachádzajú v System i Navigator.

Nasleduje zoznam sprievodcov a ich funkcií:

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

Sprievodca novou politikou IntServ
Sprievodca novou politikou IntServ vám umožňuje vytvoriť politiku integrovaných služieb. Táto politika prijíma alebo odmieta požiadavku RSVP (ReSerVation Protocol), ktorá nepriamo riadi šírku pásma servera. Limity výkonu politiky, ktoré nastavíte, určujú, či systém dokáže zvládnuť šírku pásma, požadovanú RSVP aplikáciou klienta. Na výkon politík integrovaných služieb, vytvorených pomocou tohto sprievodcu, potrebujete smerovače a aplikácie povolené pre RSVP.

Poznámka: Skôr ako nastavíte politiku integrovanej služby, musíte mať vlastné aplikácie, ktoré používajú protokol RSVP.

Sprievodca novou politikou DiffServ
Tento sprievodca vám umožňuje odlíšiť a priradiť prioritu premávke TCP/IP. Prevádzku môžete diferencovať vytvorením politík. V rámci politiky priradíte výstupnej prevádzke úrovne služieb na základe zdrojovej/cieľovej IP adresy, portu, aplikácie či klienta. Vaše i5/OS aplikácie môžu získať úrovne služieb na základe špecifickejších informácií o aplikácii.

Sprievodca novou triedou služieb

Pomocou sprievodcu novou triedou služieb nastavte označenia paketov, ktoré používajú sieťové smerovače a prepínače. Tiež môžete určiť hranice výkonu premávky odchádzajúcej z vašej siete. Triedy služieb použijete v spojení s politikou diferencovaných služieb a politikou povolenia vstupu.

Sprievodca novým povolením vstupu

Sprievodca novým povolením vstupu dokáže obmedziť vytvorené pripojenia k vášmu systému. Môžete obmedziť prístup adresou protokolu TCP/IP, aplikáciou, miestnym rozhraním alebo identifikátorom Uniform Resource Identifier (URI). Administrátor systému tak môže riadiť prístup k vášmu systému z konkrétnych klientov a serverových aplikácií. Navyše tak môžete zlepšiť výkon systému.

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

Keď určíte, aký typ politiky chcete vytvoriť, môžete politiku nakonfigurovať pomocou jedného z uvedených sprievodcov.

Prístup k sprievodcom QoS v System i Navigator

Pomocou tohto postupu môžete pristúpiť k sprievodcom QoS a vytvoriť politiku v System i Navigator.

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

1. V System i Navigator rozviňte položky ***váš systém*** → **Network** → **IP Policies**.
2. Pravým tlačidlom myši kliknite na **Quality of Service** a kliknite na **Configuration**.

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

Súvisiace koncepty

"API rozhrania kvality služieb" na strane 16
Táto téma obsahuje informácie o protokoloch a rozhraniach API, a tiež požiadavky na smerovač, ktorý je povolený pre protokol ReSerVation (RSVP). Medzi rozhrania API kvality služieb (QoS) patrí API rozhranie RAPI, API rozhranie soketu qtoq, sendmsg() a API rozhrania monitora.

"Diferencované služby" na strane 2
Toto je prvý typ politiky výstupnej šírky pásma, ktorú môžete vytvoriť vo vašom operačnom systéme. Diferencovaná služba rozdeľuje vašu premávku do tried. Ak chcete uplatňovať politiku diferencovanej služby, musíte určiť, ako chcete klasifikovať vašu sieťovú prevádzku a ako chcete zaobchádzať s jednotlivými triedami.

Súvisiace informácie

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

Konfigurácia adresárového servera

Konfigurácie politík kvality služieb (QoS) môžete exportovať do adresárového servera LDAP, vďaka ktorému sa riešenie QoS ľahšie spravuje.

Namiesto toho, aby ste politiky QoS konfigurovali na všetkých vašich systémoch, môžete konfiguračné údaje uložiť na jeden lokálny adresárový server, aby ich zdieľalo viacero systémov. Pri prvom konfigurovaní QoS na vašom systéme sa otvorí sprievodca úvodnou konfiguráciou. Sprievodca vás vyzve, aby ste nakonfigurovali adresárový server.

Pri konfigurácii adresárového servera musíte určiť nasledujúce informácie:

- Názov adresárového servera
- Zadajte charakteristický názov (DN), ktorým sa bude odkazovať na politiky QoS
- Určite, či chcete s vaším adresárovým serverom LDAP používať zabezpečenie SSL (Secure Sockets Layer)
- Rozhodnite, či sa majú na vylepšenie vyhľadávania vašich politík na adresárovom serveri používať kľúčové slová.

Poznámka: V súčasnosti nie je možné nakonfigurovať Kerberos ako autentifikačnú metódu pre prístup servera QoS k adresáru.

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

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

Ak používate System i Navigator, už máte prístup k predvolenej schéme QoS. Skutočný súbor schémy je umiestnený na vašom systéme v adresári /QIBM/UserData/OS400/DirSrv. Ak však používate iný editor než System i Navigator, musíte naimportovať súbor LDIF (LDAP Data Interchange Format) opísaný v nasledujúcej časti. Môžete tiež importovať tento súbor, ak chcete po úpravách znovu načítať pôvodný predvolený súbor.

Schéma QoS

Existuje sada pravidiel, označovaná ako *schéma*, ktorá určuje, aké typy LDAP objektov sú platné pre server QoS. Schéma obsahuje pravidlá potrebné pre QoS. Ak používaný server LDAP nie je na platforme System i, tieto pravidlá musíte na LDAP server naimportovať. Urobte tak pomocou súboru LDIF (LDAP Data Interchange Format). LDIF súbor si stiahnite z webových stránok LDAP. Súbor nájdete v ľavom podokne pod položkou **Categories → TCP/IP Policies**.

Súvisiace koncepty

“Adresárový server” na strane 24
Svoje politiky môžete vyexportovať na adresárový server. Prečítajte si túto tému so základnými pojmami a konfiguráciou protokolu LDAP (Lightweight Directory Access Protocol) a pozrite si schému kvality služieb (QoS).

“Rozlišovací názov” na strane 25
Keď chcete spravovať časť vášho adresára, odkazujete na charakteristický názov (DN) alebo na kľúčové slovo (ak ho zvolíte).

IBM Tivoli Directory Server for i5/OS (LDAP)

Povolenie SSL a zabezpečenia prenosovej vrstvy na adresárovom serveri

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

Súvisiace informácie

Schéma IBM adresára LDAP

Zoraďovanie politík QoS

Ak máte dve politiky, ktoré sa vzájomne prekrývajú, dôležité bude poradie vašich politík v System i Navigator.

Prekrývajúce sa politiky sú politiky, ktoré používajú rovnakého klienta, aplikáciu, plán, lokálnu IP adresu, URI (jednotný identifikátor prostriedku), serverové údaje, kódový bod alebo protokol. Politiky na obrazovke System i Navigator sú zoradené do zoznamu. Priorita politiky závisí od poradia politík v tomto zozname. Ak chcete, aby mala jedna politika prioritu pred inou, musí sa politika s vyššou prioritou nachádzať v zozname vyššie.

Ak chcete určiť, či sa politika prekrýva s inou politikou, postupujte takto:

1. V System i Navigator rozviňte položky ***váš systém*** → **Network** → **IP Policies**.
2. Kliknite pravým tlačidlom na **Kvalita služieb**.
3. Zvoľte **Configuration**.
4. Vyberte zložku **Specific Policies**.
5. Kliknite pravým tlačidlom na názov politiky, ktorá má združené prekrývajúce sa politiky. Prekrývajúce sa politiky majú pred sebou ikonu, ktorá indikuje prekrývanie.
6. Vyberte **Show Overlap**. Otvorí sa okno Policy Overlap.

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

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

Súvisiace koncepty

"Konfigurácia kvality služieb" na strane 50
Keď si naplánujete kvalitu služieb (QoS), vytvorte si vlastné politiky QoS pomocou sprievodcov v System i Navigator. Tieto témy opisujú vytvorenie politík diferencovaných služieb, integrovaných služieb a povolenia vstupu.

"Kopírovanie existujúcej politiky" na strane 54
Namiesto toho, aby ste všetky politiky vytvárali od základu, môžete urobiť kópie pôvodnej politiky a tieto potom upraviť.

"Odstraňovanie problémov s kvalitou služieb" na strane 59
Kvalita služieb (QoS) poskytuje niekoľko metód na odstraňovanie problémov QoS.

Súvisiace úlohy

"Prístup k pomoci QoS v System i Navigator"
Pomocou System i Navigator môžete pristúpiť k pomoci pre kvalitu služieb (QoS).

Správa kvality služieb

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

Tieto témy vám poskytujú informácie o tom, kde nájdete reálne úlohy ilustrujúce spôsoby upravovania, povoľovania, zobrazovania alebo iné techniky spravovania politík. Nájdete tu tiež vysvetlenie, ako používať funkciu QoS monitora a zberu údajov na analýzu vašej IP prevádzky v systéme.

Súvisiace koncepty

"Konfigurácia kvality služieb" na strane 50
Keď si naplánujete kvalitu služieb (QoS), vytvorte si vlastné politiky QoS pomocou sprievodcov v System i Navigator. Tieto témy opisujú vytvorenie politík diferencovaných služieb, integrovaných služieb a povolenia vstupu.

Prístup k pomoci QoS v System i Navigator

Pomocou System i Navigator môžete pristúpiť k pomoci pre kvalitu služieb (QoS).

1. V System i Navigator rozviňte položky ***váš systém*** → **Network** → **IP Policies**.
2. Pravým tlačidlom myši kliknite na **Quality of Service** a kliknite na **Configuration**.
3. V lište ponuky kliknite na **Help** → **Help topics**. Zobrazí sa okno s pomocou pre úlohu.

Súvisiace úlohy

"Zoraďovanie politík QoS" na strane 52
Ak máte dve politiky, ktoré sa vzájomne prekrývajú, dôležité bude poradie vašich politík v System i Navigator.

Zálohovanie politík QoS

Vaše politiky kvality služieb (QoS) by ste mali zálohovať, aby ste ich v prípade výpadku systému alebo napájania nemuseli vytvárať nanovo.

Vaše politiky sa dajú uložiť lokálne alebo sa dajú exportovať do adresárového servera. Konkrétne musíte zálohovať tento adresár integrovaného súborového systému: QIBM/UserData/OS400/QOS/ETC, QIBM/UserData/OS400/QOS/TEMP a QIBM/UserData/OS400/QOS/USR. Tiež musíte zálohovať vášho zverejňovacieho agenta adresárového servera pre server QoS. Publikačný agent obsahuje názov adresárového servera, charakteristický názov (DN) pre QoS server, port použitý na prístup k adresárovému serveru a autentifikačné informácie. V prípade straty vám zálohy ušetria čas a námahu spojenú s opätovným vytváraním politík od nuly. Toto sú všeobecné tipy, ktoré môžete použiť na zabezpečenie toho, že budete mať jednoduchý spôsob, ako nahradiť stratené súbory:

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

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

   Vytlačené politiky uložte na miesto, kde budú v bezpečí a pritom poruke.
3. **Skopírujte si tieto informácie na disk.**

   Kopírovanie má v porovnaní s vytlačením výhodu: odpadá potreba znovu zadávať manuálne informácie existujúce elektronicky. Táto voľba vám poskytuje priamočiaru metódu na prenášanie informácií z jedného zdroja online k inému zdroju.

Poznámka: Systém údaje skopíruje na systémový disk a nie na disketu. Súbory s pravidlami sa nachádzajú v QIBM/UserData/OS400/QOS/ETC a tiež pod jedinečným názvom v nakonfigurovanom adresárovom serveri, nie na osobnom počítači. Ako náhradný prostriedok na ochranu údajov uložených na systémovom disku môžete prípadne využiť niektorú z metód ochrany diskov.

Pri používaní produktu System i si musíte naplánovať stratégiu zálohovania a obnovy.

Súvisiace informácie

Zálohovanie systému

Kopírovanie existujúcej politiky

Namiesto toho, aby ste všetky politiky vytvárali od základu, môžete urobiť kópie pôvodnej politiky a tieto potom upraviť.

V System i Navigator sa táto funkcia kvality služieb (QoS) nazýva *Nové, založené na*. Musíte použiť System i Navigator, aby ste sa dostali do okna QoS, v ktorom môžete pokračovať ďalej v kopírovaní politík.

Ak chcete vytvoriť kópiu existujúcej politiky, postupujte podľa krokov uvedených v časti **Vytvoriť novú kópiu z existujúcej politiky** v pomoci k System i Navigator.

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

Súvisiace úlohy

“Zoraďovanie politík QoS” na strane 52
Ak máte dve politiky, ktoré sa vzájomne prekrývajú, dôležité bude poradie vašich politík v System i Navigator.

Upravovanie politík QoS

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

Pred aktiváciou musíte opraviť všetky chyby a vykonať všetky nutné zmeny vo vašich politikách. Je to najlepší spôsob, ako predísť komplikáciám s výsledkami vašej politiky.

Po nakonfigurovaní politík môžete použiť konfiguračné objekty v System i Navigator na úpravu konfigurácie vašej politiky. Konfiguračné objekty sú rozličné kusy, alebo časti tvoriace politiku. Keď otvoríte kvalitu služieb v System i Navigator, zobrazia sa zložky s označením klienti, aplikácie, plány, politiky, triedy služieb, správania per-hop a identifikátory URI (Uniform Resource Identifier). Tieto objekty vám umožňujú upraviť politiku.

Ak chcete upraviť politiku v System i Navigator, postupujte podľa krokov uvedených na stránke Upravovanie politiky kvality služieb (QoS) v rámci systému pomoci k System i Navigator.

Monitorovanie QoS

Pomocou monitora kvality služieb (QoS) môžete analyzovať IP prevádzku vo vašom systéme.

Monitor QoS vám pomôže určiť, kde sa vo vašej sieti objavuje preťaženie. Je užitočný nielen vo fáze plánovania QoS, ale tiež ako nástroj odstraňovania problémov. Monitor QoS neustále monitoruje vašu sieť, takže môžete prispôsobovať vaše politiky podľa aktuálnej potreby. Ak chcete monitorovať všetky aktívne politiky, vyberte položky **Server → Monitor** v okne Konfiguračný server QoS. Ak pravým tlačidlom myši kliknete na jednu politiku a zvolíte možnosť **Monitor**, monitor zobrazí informácie len k tejto politike.

Monitorovacie politiky môžete použiť nasledovnými spôsobmi:

- **Ak chcete zobraziť údaje o aktívnych politikách v reálnom čase**

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

  Ak chcete uložiť výsledky monitora, musíte spustiť zhromažďovanie údajov QoS. Monitor bude pokračovať v zhromažďovaní, až kým ho nezastavíte. Zatvorením okna monitora zhromažďovanie nezastavíte. Tiež môžete zmeniť vlastnosti, ktoré monitor používa pri zhromažďovaní údajov. V okne Monitor QoS vyznačte možnosť **QoS monitor** a zvoľte položky **Súbor-->Vlastnosti**, aby ste mohli zmeniť vaše voľby. Viac informácií nájdete v online pomoci.

  Keď je zapnutá funkcia zhromažďovania údajov QoS a zmeníte vlastnosti monitora, potom musíte vykonať nasledujúci postup, aby sa zmeny premietli do zhromažďovania údajov:

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

Výstup monitorovania

Výstupné informácie budú závisieť od typu monitorovanej politiky. Typy politík sú: diferencovaná služba, integrovaná služba (riadené zaťaženie), integrovaná služba (garantovaná) a povolenie vstupu. Vyhodnocované polia závisia od typu politiky. Najzaujímavejšími hodnotami sú hodnoty, ktoré ukazujú meranie. Bez toho, aby boli nejako presnejšie definované, sa merajú nasledovné polia: prijaté požiadavky, aktívne pripojenia, služby pripojení, rýchlosti pripojenia, odmietnuté požiadavky, vnútroprofilové pakety, vnútroprofilové bity, mimoprofilové bity, celkový počet bitov, celkový počet paketov a celkový počet požiadaviek.

Čítaním informácií z vyššie uvedených meraných polí si môžete utvoriť vhodný obraz o tom, či vaša sieťová prevádzka vyhovuje vašim politikám. Nižšie uvedené opisy použite na získanie detailnejších informácií o výstupnom poli monitora pre každý typ politiky. Ukážky spôsobov využitia monitorovania v politikách QoS nájdete v ktoromkoľvek scenári QoS.

Politiky diferencovanej služby

Tabuľka 4. Politiky diferencovanej služby

Pole	Popis
Názov politiky	Názov, ktorý ste priradili tejto politike.
Protokol	UDP, TCP, ALL.
Limit priemernej rýchlosti tokenov	Priemerná rýchlosť tokenov povolená v tejto politike v každom smerovači a systéme v komunikačnom toku.
Limit hĺbky symbolu	Maximálna veľkosť vyrovnávacej pamäte tokenov povolená v tejto politike v každom smerovači a systéme v komunikačnom toku.
Limit vrcholu rýchlosti symbolov	Maximálna rýchlosť, povolená týmto pripojením.
Pakety v profile	Počet prenesených IP paketov, ktoré sa hodia do parametrov tejto politiky.
Bity v profile	Počet prenesených bitov, ktoré sa hodia do parametrov tejto politiky.
Bity mimo profilu	Počet prenesených bitov, ktoré presahujú parametre tejto politiky.
Počet bitov	Meraný počet bitov, povolený týmto pripojením.
Aktívne pripojenia	Celkový počet aktívnych pripojení.
Profil prevádzky	Typ podmieňovania paketov, použitého na paketoch mimo profilu. Formát môže obsahovať: • Preznačenie • Tvarovanie • Zrušenie
Bitov spolu	Počet prenesených bitov, použitých touto politikou od času, keď bola spustená, do momentu ich zhromaždenia monitorom.
Kódový bod v profile	Ak je paket preznačený s novým kódovým bodom, toto je kódový bod, ktorý budú IP pakety používať, ak budú vhodné v rámci parametrov tejto politiky.
Kódový bod mimo profilu	Ak je paket preznačený s novým kódovým bodom, toto je kódový bod, ktorý budú IP pakety používať, ak sa budú vymykať z rámca parametrov tejto politiky.
Rozsah cieľových adries	Rozsah adries, ktorý určuje cieľový bod paketu (riadeného touto politikou).
Spolu paketov	Počet prenesených paketov, použitých touto politikou od času, keď bola spustená, do momentu ich zhromaždenia monitorom.
Rozsah zdrojových portov	Rozsah zdrojových portov, ktorý určuje, ktoré aplikácie bude riadiť táto politika.

Politiky integrovanej služby (riadený objem)

Politiky integrovaných služieb sa nezobrazia v monitore, kým nebudú spustené aplikácie a vytvorené rezervácie. Ak majú vaše politiky integrovaných služieb viac ako jednu rezerváciu, monitor zobrazí viac položiek.

Tabuľka 5. Politiky integrovanej služby (riadený objem)

Pole	Popis
Názov politiky	Názov, ktorý ste priradili tejto politike.
Protokol	UDP alebo TCP.

Tabuľka 5. Politiky integrovanej služby (riadený objem) (pokračovanie)

Pole	Popis
Cieľová adresa	Rozsah adries, ktorý určuje cieľový bod paketu (riadeného touto politikou).
Limit priemernej rýchlosti tokenov	Priemerná rýchlosť tokenov povolená v tejto politike v každom smerovači a systéme v ceste pripojení.
Limit hĺbky symbolu	Maximálna veľkosť vyrovnávacej pamäte tokenov povolená v tejto politike v každom smerovači a systéme v ceste pripojení.
Limit vrcholu rýchlosti symbolov	Maximálna rýchlosť, povolená týmto pripojením.
Spolu paketov	Počet prenesených paketov, použitých touto politikou od času, keď bola spustená, do momentu ich zhromaždenia monitorom.
Bity mimo profilu	Počet prenesených bitov, ktoré presahujú parametre tejto politiky.
Bitov spolu	Počet prenesených bitov, použitých touto politikou od času, keď bola spustená, do momentu ich zhromaždenia monitorom.
Počet bitov	Meraný počet bitov, povolený týmto pripojením.
Bity v profile	Počet prenesených bitov, ktoré sa hodia do parametrov tejto politiky.
Maximálna veľkosť paketu	Maximálna povolená veľkosť paketu, riadeného touto politikou.
Minimálna odoberaná jednotka	Najmenší počet bitov, ktoré sa odstránia z bloku tokenov. Napríklad ak vaša minimálna odoberaná jednotka je 100 bitov, pakety pod 100 bitov sa odstránia na 100 bitoch.
Pakety v profile	Počet prenesených IP paketov, ktoré sa hodia do parametrov tejto politiky.
Rozsah zdrojových portov	Rozsah zdrojových portov, ktorý určuje, ktoré aplikácie bude riadiť táto politika.

Politiky integrovanej služby (zaručenej)

Politiky integrovaných služieb sa nezobrazia v monitore, kým nebudú spustené aplikácie a vytvorené rezervácie. Ak majú vaše politiky integrovaných služieb viac ako jednu rezerváciu, monitor zobrazí viac položiek.

Tabuľka 6. Politiky integrovanej služby (zaručenej)

Pole	Popis
Názov politiky	Názov, ktorý ste priradili tejto politike.
Protokol	UDP alebo TCP.
Cieľová adresa	Rozsah adries, ktorý určuje cieľový bod paketu (riadeného touto politikou).
Limit priemernej rýchlosti tokenov	Maximálna rýchlosť tokenov povolená v tejto politike v každom smerovači a systéme v ceste pripojení.
Limit hĺbky symbolu	Maximálna veľkosť vyrovnávacej pamäte tokenov povolená v tejto politike v každom smerovači a systéme v ceste pripojení.
Limit vrcholu rýchlosti symbolov	Maximálna rýchlosť, povolená týmto pripojením.
Spolu paketov	Počet prenesených paketov, použitých touto politikou od času, keď bola spustená, do momentu ich zhromaždenia monitorom.
Bitov spolu	Počet prenesených bitov, použitých touto politikou od času, keď bola spustená, do momentu ich zhromaždenia monitorom.

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

Pole	Popis
Bity mimo profilu	Počet prenesených bitov, ktoré presahujú parametre tejto politiky.
Garantovaná rýchlosť	Garantovaná rýchlosť v bitoch za sekundu.
Bity v profile	Počet prenesených bitov, ktoré sa hodia do parametrov tejto politiky.
Maximálna veľkosť paketu	Maximálna povolená veľkosť paketu, riadeného touto politikou.
Minimálna odoberaná jednotka	Najmenší počet bitov, ktoré sa odstránia z bloku tokenov. Napríklad ak vaša minimálna odoberaná jednotka je 100 bitov, pakety pod 100 bitov sa odstránia na 100 bitoch.
Pakety v profile	Počet prenesených IP paketov, ktoré sa hodia do parametrov tejto politiky.
Trvanie omeškania	Rozdiel (v sekundách) medzi vyžadovaným a získaným oneskorením.
Rozsah zdrojových portov	Rozsah zdrojových portov, ktorý určuje, ktoré aplikácie bude riadiť táto politika.

Politiky povolenia komunikácie smerom dnu

Tabuľka 7. Politiky povolenia komunikácie smerom dnu

Pole	Popis
Názov politiky	Názov, ktorý ste priradili tejto politike.
Počet pripojení	Počet akceptovaných požiadaviek na pripojenie za sekundu.
Požiadaviek spolu	Celkový počet požiadaviek na pripojenie k tomuto systému.
Akceptované požiadavky	Celkový počet požiadaviek na pripojenie, ktoré systém akceptoval.
Zrušené požiadavky	Celkový počet požiadaviek, ktoré systém prerušil.
Limit priemerného počtu pripojení	Povoliteľný priemerný počet prijatých nových pripojení na pripojenie za sekundu.
Nárazový limit pripojení	Maximálny počet nových požiadaviek na pripojenie, akceptovaných súčasne.
Limit vrcholu rýchlosti pripojenia	Maximálna povolená rýchlosť akceptovania požiadaviek zo siete.
Priorita	Priorita, priradená každému pravidlu, zavedenému do Manažéra QoS.
Priorita vo fronte	Priorita, priradená prichádzajúcim pripojeniam, uloženým do načúvacieho frontu.
Rozsah cieľových portov	Rozsah portov alebo port, kam je zacielená prevádzka na vašom systéme.
Adresa rozhrania	IP adresa systémového rozhrania, ktoré sa má monitorovať.
Rozsah zdrojových adries	Rozsah IP adries klientov odosielajúcich požiadavky do vášho systému.
Jednotný identifikátor prostriedku (URI)	Identita preverovaného URI.

Súvisiace koncepty

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

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

"Scenár: Obmedzenie vstupných pripojení" na strane 35
Ak potrebujete mať pod kontrolou požiadavky na vstupné pripojenia do vášho systému, použite politiku povolenia vstupu.

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

"Scenár: Dedikované doručenie (IP telefónia)" na strane 41
Ak potrebujete vyhradené doručenie a chcete vyžadovať rezerváciu, použijete politiku integrovaných služieb. Môžete vytvoriť dva typy politík integrovaných služieb: garantované a s riadeným zaťažením. V tomto príklade sa používa garantovaná služba.

"Scenáre: Politiky kvality služieb" na strane 27
Tieto scenáre politík kvality služieb (QoS) vám pomôžu pochopiť, prečo potrebujete QoS a ako môžete vytvoriť politiky a triedy služieb.

"Monitorovanie systémových transakcií" na strane 61
Pomocou monitora kvality služieb (QoS) si môžete overiť, či politiky QoS fungujú podľa vašej predstavy. Monitor QoS vám môže pomôcť v plánovacej fáze a vo fáze odstraňovania problémov QoS.

"Scenár: Monitorovanie aktuálnej sieťovej štatistiky" na strane 45
V sprievodcoch potrebujete nastaviť výkonové limity, založené na jednotlivých sieťových požiadavkách.

Odstraňovanie problémov s kvalitou služieb

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

Sledovanie komunikácie

Váš systém poskytuje funkciu sledovania komunikácie, ktorá zhromažďuje údaje na komunikačnej linke, napríklad v rozhraní lokálnej siete (LAN) alebo siete WAN. Priemerný užívateľ by nemusel porozumieť celému obsahu údajov o sledovaní. Vy však môžete použiť záznamy zo sledovania pri rozhodovaní, či medzi dvoma bodmi v sieti došlo k výmene údajov.

Povolenie QoS v systéme

Ak sa server QoS nespustí, najskôr skontrolujte, či je QoS na systéme povolené. Pri prvej konfigurácii politík sprievodca úvodnou konfiguráciou automaticky na systéme povolí QoS. Ak sa však táto hodnota z nejakého dôvodu zmenila, server sa nespustí.

Overte, či je QoS na systéme povolené:

1. V System i Navigator rozviňte položky ***váš systém*** → **Network** → **IP Policies**.
2. Kliknite pravým tlačidlom na **Quality of Service** a zvoľte **Configuration**.
3. Keď sa zobrazí rozhranie QoS, pravým tlačidlom myši kliknite na **QoS** a vyberte **Properties**.
4. Na strane vlastností QoS skontrolujte, či je vybraté **Enable QoS**.

Súvisiace koncepty

Sledovanie komunikácie

Súvisiace úlohy

"Zoraďovanie politík QoS" na strane 52
Ak máte dve politiky, ktoré sa vzájomne prekrývajú, dôležité bude poradie vašich politík v System i Navigator.

Politiky žurnálovania QoS

Kvalita služieb (QoS) obsahuje funkciu denníka. Denník vám umožňuje zaznamenávať akcie súvisiace s politikami QoS, keď pridáte, odstránite alebo zmeníte nejakú politiku.

Keď zapnete funkciu žurnálovania, vytvorí sa protokol akcií politík. Pomáha vám to odladiť a zbadať, kde politiky nepracujú podľa predstáv. Napríklad si nastavíte politiku tak, aby fungovala od 9.00 do 16.00 h. Potom si môžete v žurnálovom protokole overiť, či bola politika skutočne o 9.00 pridaná a o 16.00 odstránená.

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

Buďte selektívny pri výbere vecí na žurnálovanie. Žurnálovanie môže veľmi zaťažovať vaše systémové zdroje. Ak chcete spustiť alebo zastaviť žurnálovanie, použite System i Navigator. Ak si chcete prezerať žurnálové protokoly, musíte použiť znakové rozhranie.

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

1. V System i Navigator rozviňte položky ***váš systém*** → **Network** → **IP Policies**.
2. Pravým tlačidlom myši kliknite na **Quality of Service** a kliknite na **Configuration**.
3. Kliknite pravým tlačidlom na **QoS** a vyberte **Properties**.
4. Označte políčko **Run Journaling**, ak chcete spustiť žurnálovanie.
5. Ak chcete žurnálovanie vypnúť, zrušte označenie políčka.

Poznámka: Ak je systém spustený, skôr než dokončíte uvedené kroky, musíte ho zastaviť a znovu spustiť. Po zapnutí žurnálovania je možné ho aktivovať dvoma spôsobmi. Môžete systém zastaviť a znovu spustiť, alebo môžete vykonať aktualizáciu systému. V oboch prípadoch sa nanovo prečíta súbor policy.conf a vyhľadajú sa atribúty žurnálovania.

Zobrazenie položiek denníka

Táto téma obsahuje informácie o tom, ako zobrazíte položky denníka na monitore.

1. Pri výzve príkazu zadajte DSPJRN JRN(QUSRSYS/QQOS).
2. V položke denníka, ktorú chcete zobraziť, zvoľte voľbu 5.

Zobrazenie položiek denníka vo výstupnom súbore

Ak chcete zobraziť položky denníka tak, aby boli naformátované do jednej zložky, pozrite si súbor MODEL.OUT v adresári QUSRSYS. Skopírovaním položiek denníka do výstupného súboru ich môžete jednoducho zobraziť pomocou dotazovacích obslužných programov, napríklad Query/400 alebo Structured Query Language (SQL). Môžete tiež napísať vaše vlastné programy v jazyku HHL (high-level language) na spracovanie položiek vo výstupných súboroch.

Ak chcete záznam žurnálu kvality služieb (QoS) skopírovať do systémového výstupného súboru, postupujte podľa týchto krokov:

1. Vytvorte kópiu výstupného súboru poskytnutého systémom QSYS/QATOQQOS do užívateľskej knižnice. Môžete tak urobiť za použitia príkazu CRTDUPOBJ (Create Duplicate Object). Nasledujúci reťazec je príkladom príkazu CRTDUPOBJ:
   - CRTDUPOBJ OBJ(QADSPJR4) FROMLIB(Qsys) OBJTYPE(*FILE) TOLIB(*userlib*) NEWOBj(*userfile*)
2. Použite príkaz Zobraziť žurnál (DSPJRN) na kopírovanie položiek zo žurnálu QUSRSYS/QQOS do výstupného súboru vytvoreného v predchádzajúcom kroku. Ak sa pokúsite kopírovať príkaz DSPJRN do výstupného súboru, ktorý neexistuje, systém vám vytvorí súbor, ale tento súbor neobsahuje správne popisy polí.
   - DSPJRN JRN(QUSRSYS/QQOS) JRNCDE((M)) ENTTYP(MP) CMTCYCID(*ALL) OUTPUT(*OUTFILE) OUTFILFMT(*TYPE4) OUTFILE(*userlib*/*userfile*)
   - DSPF FILE(*userlib*/*userfile*)

Protokolovanie úloh servera QoS

Keď sa vyskytne problém s vašimi politikami kvality služieb (QoS), analyzujte protokoly úloh. Protokol úlohy obsahuje chybové hlásenia a ďalšie informácie týkajúce sa QoS.

V podsystéme QSYSWRK je spustená iba jedna úloha QoS, QTOQSRVR. Aktuálne aj staršie protokoly úloh servera QoS môžete zobraziť z System i Navigator.

Ak chcete zobraziť protokol, postupujte nasledovne:

1. Rozviňte **Network** a kliknite na **IP Policies**.
2. Kliknite pravým tlačidlom na **Quality of Service**.
3. Kliknite na **Diagnostic tools → QoS Server Log**.

Otvorí sa okno, prostredníctvom ktorého môžete s úlohou pracovať.

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

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

QTOQSRVR
Táto úloha je základnou úlohou QoS, ktorá vám poskytne informácie o protokole, špecifické pre QoS. Spustite príkaz Work with Spooled File (WRKSPLF QTCP) a vyhľadajte protokol QTOQSRVR.

Kontrola chýb v pracovnom spoolovom súbore

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

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

   ```
   Súbor správ: QTCPMSG
   Knižnica: *LIBL
   ```

7. Na paneli Práca so súborom správ vyberte **voľbu 5**, aby sa zobrazil požadovaný súbor správ, a stlačte kláves Enter.
8. V paneli Display Message Descriptions zadajte nasledovné informácie: Position to: *Zadajte ID svojej správy (musí byť vyššie ako 3) a stlačte kláves Enter*. Napríklad TCP920C.
9. Na požadovanom ID správy zvoľte **voľbu 5** a stlačte kláves Enter.
10. V paneli Select message details to display zvoľte **voľbu 30 (Všetky uvedené)** a stlačte kláves Enter.

    Otvorí sa podrobný popis správy.

Monitorovanie systémových transakcií

Pomocou monitora kvality služieb (QoS) si môžete overiť, či politiky QoS fungujú podľa vašej predstavy. Monitor QoS vám môže pomôcť v plánovacej fáze a vo fáze odstraňovania problémov QoS.

Pomocou monitora môžete analyzovať IP prevádzku vo vašom systéme. To vám pomáha určiť, kde sa vo vašej sieti objavuje preťaženie. Monitor QoS neustále monitoruje vašu sieť, takže môžete prispôsobovať vaše politiky podľa aktuálnej potreby.

Plánovanie a údržba výkonu

Najnáročnejšie pri implementácii QoS je určiť, aké limity výkonu sa majú nastaviť vo vašich politikách. Neexistuje žiadne konkrétne odporúčanie, pretože každá sieť je iná. Pred vytvorením špecifických podnikových politík môžete použiť monitor, aby ste určili najvhodnejšie hodnoty.

Vytvorte politiku diferencovaných služieb bez použitia merania, ktoré identifikuje správanie vašej sieťovej prevádzky. Aktivujte túto politiku a spustite monitor. Výsledky monitora vám prípadne pomôžu optimalizovať politiky s vašimi špecifickými potrebami. Pozrite si ukážku politiky monitora, ktorá identifikuje správanie aktuálnej prevádzky vo vašej sieti.

Odstraňovanie problémov s výkonom

Monitor môžete použiť na odstránenie problémov. Výstup z monitora vám pomôže určiť, či sa dodržujú parametre, ktoré ste priradili politike. Ak sa vaše politiky v monitore objavujú, avšak podľa všetkého komunikáciu nijako neovplyvňujú, preverte si situáciu nasledovným spôsobom:

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

Súvisiace koncepty

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

“Scenáre: Politiky kvality služieb” na strane 27
Tieto scenáre politík kvality služieb (QoS) vám pomôžu pochopiť, prečo potrebujete QoS a ako môžete vytvoriť politiky a triedy služieb.

Súvisiaci odkaz

“Monitorovanie QoS” na strane 55
Pomocou monitora kvality služieb (QoS) môžete analyzovať IP prevádzku vo vašom systéme.

Súvisiace informácie

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

Sledovanie aplikácií TCP

S kvalitou služieb (QoS) môžete použiť funkcie sledovania a zobraziť aktuálnu vyrovnávaciu pamäť sledovania.

Ak chcete na systéme spustiť sledovanie, do rozhrania príkazového riadka zadajte príkaz TRCTCPAPP (Trace TCP/IP Application).

Tu je príklad výberu sledovania, ktoré má byť vykonané:

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

Nasledujúca tabuľka predstavuje možné parametre, ktoré môžu byť použité pri sledovaní. Ak sa nejaké nastavenie nezobrazuje v znakovom rozhraní, musíte ho zadať v príkaze. Napríklad , TRCTCPAPP APP(*QOS)

MAXSTG(1000) TRCFULL(*STOPTRC) ARGLIST('l=4 c=i').

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

Maximálny úložný priestor na sledovanie

1-16000

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

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

Sledovať celú akciu

***WRAP**

Keď sledovanie dosiahne maximálnu povolenú veľkosť diskového priestoru (veľkosť vyrovnávacej pamäte sledovania), zbalí informácie o sledovaní. Zbalenie umožňuje systému prepísať najstaršie informácie v súbore, takže môžete naďalej zaznamenávať informácie o sledovaní. Ak nevyberiete túto možnosť, pri naplnení disku sa zastaví sledovanie.

***STOPTRC**

Zastaví zhromažďovanie informácií, keď systém dosiahne maximálny diskový priestor.

Zoznamy argumentov

Zoznamy argumentov udávajú, aká úroveň chýb a aký obsah sa bude protokolovať. Pre príkaz TRCTCPAPP sú povolené dva argumenty: úroveň sledovania a sledovaný obsah. Keď zadáte úroveň a obsah sledovania, skontrolujte, či sú všetky atribúty uzavreté v jednoduchých úvodzovkách, napríklad TRCTCPAPP 'l=4 c=a'

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

Úrovne sledovania

Úroveň 1: Systémové chyby (SYSERR)

Protokolovanie chýb, ktoré sa objavia pri systémových operáciách. Ak sa objaví takáto chyba, server QoS nemôže pokračovať. Systémová chyba sa môže napríklad objaviť, ak sa znižuje systémová pamäť alebo ak váš systém nedokáže komunikovať s protokolom TCP/IP. Toto je predvolená úroveň.

Úroveň 2: Chyby medzi objektmi (OBJERR)

Protokoluje chyby, ktoré sa objavia v kóde servera QoS. Napríklad sa mohla vyskytnúť chyba objektov, pretože systém zaznamenal neočakávané výsledky. Toto vo všeobecnosti predstavuje vážny stav, ktorý je treba nahlásiť servisu.

Úroveň 3: Špecifické udalosti (EVENT)

Zaznamenáva akékoľvek operácie servera QoS, ktoré sa vyskytnú. Napríklad príkazy a požiadavky o záznamy protokolu udalostí. Výsledky sú podobné, ako funkcia denníka QoS.

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

Obsah sledovania

Špecifikujte len jeden typ obsahu. Ak neurčíte žiaden typ, bude (štandardne) sledovaný všetok obsah.

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

Obsah = Intserv ('c=i')
Sleduje iba operácie integrovanej služby. Túto voľbu použite, ak ste určili, že problém súvisí s integrovanou službou.

Obsah = Diffserv ('c=d')
Sleduje iba operácie diferencovanej služby. Túto voľbu použite, ak ste určili, že problém súvisí s diferencovanou službou.

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

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

Súvisiaci odkaz

Sledovať TCP/IP aplikáciu (TRCTCPAPP)

Príklady: Čítanie výstupu sledovania

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

V politike integrovaných služieb je najdôležitejšie venovať pozornosť tomu, či nedošlo k odmietnutiu protokolu RSVP (ReSerVation Protocol), pretože sa nenašla politika pre dané pripojenie. Tu je príklad správy o úspechu:

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

Tu je príklad správy o neúspešnom pripojení integrovaných služieb:

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

V prípade politiky diferencovaných služieb najdôležitejšie správy ukazujú, či server zaviedol pravidlo politiky alebo či sa nevyskytla chyba v konfiguračnom súbore politiky.

```
Príklad:
01/11 14:07:52 [376,57] TRCE :......KernelAddPolicyRule: Installing rule = timed_42ring.
01/11 14:07:52 [376,57] EVNT :.......create_tcp_resv: Žiadna hodnota v konfiguračnom súbore pre DiffServInProfilePeakRate,
01/11 14:07:52 [376,57] TRCE :.......create_tcp_resv: Create resv - bRate:
537395 5761SS1 V6R1M0 010525 TRCTCPAPP Výstup RS004 Dátum-01/11/07 Čas-14:08:03 Strana-6
01/11 14:07:52 [376,57] TRCE :.......create_tcp_resv: Create resv - bRate: 537395 5722SS1 V5R1M0 010525 TRCTCPAPP Výstup RS
01/11 14:07:52 [376,57] TRCE :.......create_tcp_resv: bDepth: 32768
01/11 14:07:52 [376,57] TRCE :.......create_tcp_resv: peakR: 10000000
01/11 14:07:52 [376,57] TRCE :.......create_tcp_resv: m: 128
01/11 14:07:52 [376,57] TRCE :.......create_tcp_resv: M: 41452
```

```
01/11 14:07:52 [376,57] TRCE :.......create_tcp_resv: mark(TOS): a0
01/11 14:07:52 [376,57] TRCE :.......create_tcp_resv: flags: 15
01/11 14:07:52 [376,57] TRCE :.......create_tcp_resv: flowspe.form = 1, QOS_FORMAT_DS =1
```

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

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

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

Informácie súvisiace s kvalitou služieb

Dokumenty Request for Comments, publikácie IBM Redbooks a ďalšie témy informačného centra obsahujú ďalšie informácie súvisiace s témami kvality služieb. Súbory PDF môžete zobraziť alebo stiahnuť.

Dokumenty Request for Comments pre kvalitu služieb

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

- **RFC 1349.**
  Toto RFC sa zaoberá novou definíciou typu oktetového poľa služieb v hlavičke paketu IP.
- **RFC 2205.**
  Toto RFC vysvetľuje definíciu protokolu ReSerVation Protocol (RSVP).
- **RFC 2210.**
  Toto RFC objasňuje použitie protokolu RSVP s integrovanými službami Internet Engineering Task Force (IETF).
- **RFC 2474.**
  Toto RFC podáva definíciu poľa diferencovaných služieb.
- **RFC 2475.**
  Toto RFC vysvetľuje architektúru diferencovaných služieb.

Ak chcete zobraziť uvedené dokumenty RFC, použite RFC Index Search Engine , ktorý sa nachádza na stránkach RFC Editor .

Publikácie IBM Redbook

- IBM i5/OS IP Networks: Dynamické siete (cca 16 589 KB). Uvádza, ako navrhnúť samokonfigurujúcu sa sieť IP, odolnú voči chybám a s efektívnou prevádzkou. Okrem mnohých iných funkcií objasňuje teóriu v pozadí QoS a jej implementáciu do systému. Nájdete tu tiež ďalšie scenáre s podrobnými pokynmi.

- V4 TCP/IP for AS/400: More Cool Things Than Ever (cca 10 035 KB). Tento návod poskytuje vzorové scenáre, ktoré demonštrujú bežné riešenia s príkladmi konfigurácií. Informácie uvedené v tejto príručke vám pomôžu naplánovať, nainštalovať, prispôsobiť si, nakonfigurovať a riešiť problémy s TCP/IP na vašom systéme. Ešte špecificky nezahŕňa QoS, ale prechádza cez informácie adresárového servera LDAP.

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

Ostatné informácie

- IBM Tivoli Directory Server for i5/OS (LDAP). Táto téma zahŕňa základné pojmy o adresárovom serveri, konfiguráciu, administráciu a odstraňovanie problémov. Téma adresárových služieb tiež poskytuje doplnkové prostriedky na konfiguráciu vášho adresárového servera.
- Zistenie narušenia. Táto téma sa zaoberá zhromažďovaním informácií o pokusoch neautorizovane pristúpiť a zaútočiť na sieť TCP/IP. Bezpečnostní administrátori môžu analyzovať záznamy auditu, ktoré poskytuje funkcia zistenia narušenia, aby zabezpečili sieť i5/OS pred takýmito útokmi.

Súvisiaci odkaz

“PDF súbor pre kvalitu služieb” na strane 1
Tieto informácie môžete zobraziť alebo vytlačiť ako súbor PDF.

Príloha. Právne informácie

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

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

IBM môže vlastniť patenty alebo nevybavené prihlášky patentov, týkajúce sa predmetu, popísaného v tomto dokumente. Tým, že vám bol tento dokument poskytnutý, nezískavate na tieto patenty nijaké práva. Žiadosti o licencie môžete zasielať písomne na:

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

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

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

Nasledujúci odsek sa netýka Veľkej Británie ani žiadnej inej krajiny, kde sú takéto vyhlásenia nezlučiteľné s miestnym zákonom: SPOLOČNOSŤ INTERNATIONAL BUSINESS MACHINES POSKYTUJE TÚTO PUBLIKÁCIU "TAK AKO JE", BEZ AKÝCHKOĽVEK VÝSLOVNÝCH ALEBO MLČKY PREDPOKLADANÝCH ZÁRUK, VRÁTANE, ALE BEZ OBMEDZENIA NA ZÁRUKY NEPORUŠENIA PRÁV, PREDAJNOSTI ALEBO VHODNOSTI NA KONKRÉTNY ÚČEL. Niektoré štáty nepovoľujú zrieknutie sa výslovných ani mlčky predpokladaných záruk v určitých operáciách, preto sa na vás toto vyhlásenie nemusí vzťahovať.

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

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

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

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

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

Rochester, MN 55901
U.S.A.

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

Licenčný program opísaný v tomto dokumente a všetky dostupné licenčné materiály k nemu poskytuje spoločnosť IBM podľa podmienok uvedených v zmluvách IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code, prípadne v akejkoľvek inej ekvivalentnej zmluve medzi nami.

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

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

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

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

LICENCIA NA AUTORSKÉ PRÁVA:

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

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

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

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

Informácie o programovacom rozhraní

Tieto dokumenty publikácie Kvalita služieb boli zamýšľané pre programovacie rozhrania, ktoré zákazníkovi umožňujú písať programy na získanie služieb systému IBM i5/OS.

Ochranné známky

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

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

Adobe, logo Adob, PostScript a logo PostScript sú registrované ochranné známky alebo ochranné známky spoločnosti Adobe Systems Incorporated v USA a/alebo iných krajinách.

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

Pojmy a podmienky

Oprávnenia na používanie týchto publikácií sú predmetom nasledujúcich pojmov a podmienok.

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

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

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

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

Tieto informácie nemôžete prevziať ani exportovať okrem prípadu, ak to dovoľujú všetky aplikovateľné zákony a regulácie, vrátane všetkých zákonov a regulácií USA pre export.

SPOLOČNOSŤ IBM NERUČÍ ZA OBSAH TÝCHTO PUBLIKÁCIÍ. PUBLIKÁCIE SÚ POSKYTNUTÉ ″TAK AKO SÚ″ BEZ ZÁRUKY AKÉHOKOĽVEK DRUHU, VYJADRENEJ ALEBO IMPLIKOVANEJ, VRÁTANE (ALE NEOBMEDZENE) IMPLIKOVANÝCH ZÁRUK PREDAJNOSTI, NEPOŠKODENIA A VHODNOSTI NA KONKRÉTNY ÚČEL.

Vytlačené v USA