System i

Netzwerkbetrieb
Quality of Service (QoS)

Version 6 Release 1

System i

Netzwerkbetrieb
Quality of Service (QoS)

Version 6 Release 1

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen", auf Seite 77 gelesen werden.

Sechste Ausgabe (Februar 2008)

Diese Ausgabe betrifft Version 6, Release 1, Modifikation 0 von IBM i5/OS (Produktnummer 5761-SS1) und alle nachfolgenden Releases, soweit keine anderen Angaben in neuen Ausgaben vorliegen. Diese Version kann nicht auf allen RISC-Modellen (Reduced Instruction Set Computer) ausgeführt werden. Auf CISC-Modellen ist sie nicht ausführbar.

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM System i Networking, Quality of service,
herausgegeben von International Business Machines Corporation, USA

Herausgegeben von:
SW TSC Germany
Kst. 2877
Februar 2008

Inhaltsverzeichnis

Quality of Service (QoS)

Dank der QoS-Lösung (Quality of Service - Qualität des Service) für i5/OS können die Richtlinien Netzwerkpriorität und Bandbreite für TCP/IP-Anwendungen im gesamten Netzwerk anfordern.

Dem gesamten Datenaustausch im Netzwerk ist die gleiche Priorität zugeordnet. Der nicht kritische Browserdatenaustausch wird als ebenso wichtig wie geschäftskritische Anwendungen bewertet. Die Priorität von IP-Paketen kann jedoch - beispielsweise bei Präsentationen, die unter Verwendung einer Audio-/Videoanwendung erfolgen - zu einem wesentlichen Aspekt werden. In diesem Fall ist es wichtig, dass die Anwendung während der Präsentation einen größeren Durchsatz erhält als andere Anwendungen.

Die Paketpriorität ist wichtig, wenn Sie Anwendungen senden wollen, die vorhersehbare und zuverlässige Ergebnisse benötigen (z. B. Multimedia). Die QoS-Richtlinien verwalten die Paketpriorität, begrenzen die Daten, die das System verlassen, verwalten Verbindungsanforderungen und steuern die Systemauslastung. Der QoS-Server muss aktiv sein, damit die Richtlinie für die Erkennung von unbefugtem Zugriff aktiviert werden kann.

PDF-Datei für QoS

Sie können eine PDF-Datei der vorliegenden Informationen anzeigen und drucken.

Um die PDF-Version des vorliegenden Dokuments anzuzeigen oder herunterzuladen, wählen Sie QoS (Quality of Service) aus (ca. 525 KB).

PDF-Dateien speichern

So können Sie eine PDF-Datei zum Anzeigen oder Drucken auf Ihrer Workstation speichern:

1. Klicken Sie mit der rechten Maustaste auf den PDF-Link in Ihrem Browser.
2. Klicken Sie auf die Option, mit der die PDF lokal gespeichert werden kann.
3. Navigieren Sie zu dem Verzeichnis, in dem Sie die PDF speichern wollen.
4. Klicken Sie auf **Speichern**.

Adobe Reader herunterladen

Damit diese PDF-Dateien angezeigt oder gedruckt werden können, muss auf Ihrem System der Adobe Reader installiert sein. Auf der Adobe-Website (www.adobe.com/products/acrobat/readstep.html) können Sie eine kostenlose Kopie dieses Programms herunterladen.

Zugehörige Verweise

„Referenzinformationen zu QoS" auf Seite 75
RFCs (Request for Comments) für QoS, IBM Redbooks und andere Themensammlungen im Information Center enthalten Informationen, die sich auf die QoS-Themensammlung beziehen. Sie können alle PDF-Dateien anzeigen oder drucken.

Konzepte

Bevor Sie QoS (Quality of Service - Qualität des Service) verwenden, müssen Sie die Basisterminologie erlernen und sich über die QoS-Konzepte informieren. Mit Hilfe dieser Konzepte können Sie feststellen, ob der Service Ihren Anforderungen entspricht.

Zur Ausführung von QoS müssen Sie mit den Assistenten in System i Navigator Richtlinien konfigurieren. Eine *Richtlinie* ist eine Gruppe von Regeln, die eine Aktion definieren. Sie besagt im Wesentlichen, dass ein Client, eine Anwendung und ein Zeitplan (von Ihnen definiert) einen bestimmten Service erhalten sollen. Sie können letztlich die folgenden Typen von Richtlinien konfigurieren:

- Differenzierte Services
- Integrierte Services
- Ankommende Daten

Die Richtlinien für *differenzierte Services* und für *integrierte Services* werden als Richtlinien für die Bandbreite abgehender Daten betrachtet. Richtlinien für abgehende Daten begrenzen den Datenaustausch, der das Netzwerk verlässt, und helfen Ihnen dabei, die Systemauslastung zu steuern. Mit den Geschwindigkeiten, die Sie in einer Richtlinie für abgehende Daten festlegen, steuern Sie, welche Daten innerhalb des Systems eingeschränkt bzw. nicht eingeschränkt werden sollen und auf welche Weise dies umgesetzt wird. Beide Richtlinientypen für abgehende Daten machen unter Umständen ein Service-Level-Agreement (SLA) mit Ihrem Internet-Service-Provider (ISP) erforderlich.

Richtlinien für *ankommende Daten* steuern die Verbindungsanforderungen, die aus externen Quellen stammen und in Ihrem Netzwerk eintreffen. Diese Richtlinien sind nicht von einer Servicestufe des ISP abhängig. Welche Richtlinie Sie verwenden müssen, können Sie feststellen, indem Sie Ihre Gründe für die gewünschte Verwendung von QoS auswerten und den Aufgabenbereich des Systems berücksichtigen.

Einer der wichtigsten Bestandteile beim Einsatz von QoS ist das Betriebssystem selbst. Sie müssen nicht nur die QoS-Konzepte kennen, sondern außerdem den Aufgabenbereich berücksichtigen, den das Betriebssystem in diesen Konzepten übernimmt. Das Betriebssystem i5/OS kann nur als Client oder als Server, aber nicht als Router eingesetzt werden. Das Betriebssystem, das als Client agiert, kann beispielsweise durch Richtlinien für differenzierte Services sicherstellen, dass Informationsanforderungen an andere Systeme im Netzwerk eine höhere Priorität erhalten. Wird ein Betriebssystem als Server eingesetzt, können mit einer Richtlinie für ankommende Daten die URI-Anforderungen (Uniform-Resource-Identifier) begrenzt werden, die der Server akzeptiert.

Zugehörige Konzepte

„Service-Level-Agreement" auf Seite 55
Dieses Thema stellt einige wichtige Aspekte eines Service-Level-Agreements (SLA) heraus, die sich auf Ihre QoS-Implementierung auswirken können. QoS ist eine Lösung für Netzwerke. Um auch außerhalb Ihres privaten Netzwerks Priorität zu erhalten, benötigen Sie möglicherweise ein Service-Level-Agreement (SLA) mit Ihrem ISP (Internet Service Provider).

Zugehörige Verweise

„Referenzinformationen zu QoS" auf Seite 75
RFCs (Request for Comments) für QoS, IBM Redbooks und andere Themensammlungen im Information Center enthalten Informationen, die sich auf die QoS-Themensammlung beziehen. Sie können alle PDF-Dateien anzeigen oder drucken.

Differenzierte Services

Dies ist der erste Typ einer Richtlinie für die Bandbreite abgehender Daten, den Sie auf dem Betriebssystem erstellen können. Die differenzierten Services unterteilen den Datenaustausch im Netzwerk in unterschiedliche Klassen. Wenn Sie eine Richtlinie für differenzierte Services einsetzen wollen, müssen Sie festlegen, wie der Datenaustausch im Netzwerk klassifiziert werden soll und wie die unterschiedlichen Klassen zu behandeln sind.

Zugehörige Konzepte

„QoS-Erweiterungen der API sendmsg()" auf Seite 27
Die Funktion sendmsg() wird zum Senden von Daten und/oder von Hilfsdaten über einen verbundenen oder nicht verbundenen Socket verwendet.

„Grenzwerte für Token-Puffer und Bandbreite" auf Seite 11
Grenzwerte für Token-Puffer und Bandbreite werden unter dem Begriff "Leistungsgrenzen" zusam-

mengefasst. Mit solchen Leistungsgrenzen kann die Paketübermittlung in Richtlinien für die Bandbreite abgehender Daten (sowohl für integrierte Services als auch für differenzierte Services) garantiert werden.

„Serviceklasse" auf Seite 14
Beim Erstellen einer Richtlinie für differenzierte Services oder für ankommende Daten erstellen und verwenden Sie ebenfalls eine Serviceklasse.

„Szenario: Browserdatenaustausch begrenzen" auf Seite 32
Mit QoS können Sie das Leistungsverhalten für den Datenaustausch steuern. Durch den Einsatz einer Richtlinie für differenzierte Services können Sie die Leistung einer Anwendung in Ihrem Netzwerk entweder einschränken oder erweitern.

„Szenario: Sichere und vorhersehbare Ergebnisse (VPN und QoS)" auf Seite 36
Auch wenn Sie ein VPN (Virtual Private Network - virtuelles privates Netzwerk) verwenden, können Sie QoS-Richtlinien erstellen.

Zugehörige Verweise

„Pro-Hop-Verhalten mit Codepunkten zuordnen" auf Seite 16
QoS verwendet die empfohlenen Codepunkte, um einem Datenaustausch ein Pro-Hop-Verhalten zuzuordnen.

„QoS mit Assistenten konfigurieren" auf Seite 58
Zur Konfiguration von QoS-Richtlinien müssen Sie die QoS-Assistenten in System i Navigator verwenden.

Zugehörige Informationen

Adressen und Ports für den HTTP-Server (auf Apache-Basis) verwalten

Klassen mit Priorität: Vorgehensweise zur Klassifizierung von Datenaustausch im Netzwerk

Die differenzierten Services unterteilen den Datenaustausch in unterschiedliche Klassen. Die gängigsten Klassen werden unter Verwendung von Client-IP-Adressen, Anwendungsports, Servertypen, Protokollen, lokalen IP-Adressen und Zeitplänen definiert. Der gesamte Datenaustausch, der derselben Klasse entspricht, wird gleich behandelt.

Um eine erweiterte Klassifizierung zu ermöglichen, können Sie durch die Angabe von Anwendungsdaten unterschiedliche Servicestufen für einige i5/OS-Anwendungen erhalten. Die Verwendung von Anwendungsdaten ist optional, kann jedoch hilfreich sein, wenn Sie eine differenzierte Klassifizierung vornehmen möchten. Es gibt zwei unterschiedliche Typen von Anwendungsdaten, nämlich entweder Anwendungstoken oder Uniform-Resource-Identifier (URI). Falls der Datenaustausch dem in der Richtlinie angegebenen Token oder URI entspricht, wird die Richtlinie auf die abgehende Antwort angewendet. Auf diese Weise wird dem abgehenden Datenaustausch diejenige Priorität erteilt, die in der Richtlinie für differenzierte Services angegeben ist.

Anwendungstoken bei Richtlinien für differenzierte Services verwenden

Die Verwendung von Anwendungsdaten ermöglicht der Richtlinie, auf bestimmte Parameter (Token und Priorität) zu reagieren, die von der Anwendung über die Anwendungsprogrammierschnittstelle sendmsg() an das Betriebssystem übergeben werden. Diese Einstellung ist optional. Wenn Sie dieses Differenzierungsniveau in Ihren Richtlinien für abgehende Daten nicht benötigen, wählen Sie im Assistenten die Option **Alle Token** aus. Sollen das Token und die Priorität einer Anwendung mit einem spezifischen Token und einer spezifischen Priorität übereinstimmen, die in der Richtlinie für abgehende Daten definiert sind, können Sie dies festlegen. Die Richtlinie enthält zwei Bestandteile zum Festlegen der Anwendungsdaten, nämlich das Token und die Priorität.

- Anwendungstoken - Beschreibung

  Ein *Anwendungstoken* ist eine beliebige Zeichenfolge, die eine definierte Ressource repräsentieren kann (z. B. `myFTP`). Das von Ihnen in der QoS-Richtlinie angegebene Token wird mit dem Token abgeglichen, das durch die Anwendung für abgehende Daten bereitgestellt wird. Die Anwendung stellt den Token-

wert über die API sendmsg() zur Verfügung. Wenn die Token übereinstimmen, wird der Datenaustausch der Anwendung in die Richtlinie für differenzierte Services aufgenommen.

So verwenden Sie ein Anwendungstoken in einer Richtlinie für differenzierte Services:

1. Klicken Sie im Fenster "Konfiguration des QoS-Servers" mit der rechten Maustaste auf **DiffServ**, und wählen Sie die Option **Neue Richtlinie** aus. Starten Sie den Assistenten.
2. Wählen Sie auf der Seite "Serverdatenanforderung" die Option **Ausgewähltes Anwendungstoken** aus.
3. Um ein neues Token zu erstellen, klicken Sie auf **Neu**. Das Fenster "Neuer URI" wird aufgerufen.
4. Geben Sie im Feld **Name** einen aussagekräftigen Namen für das Anwendungstoken ein.
5. Löschen Sie im Feld **URI** die Zeichen (/), und geben Sie das Anwendungstoken in Form einer Zeichenfolge mit maximal 128 Zeichen Länge ein. Geben Sie beispielsweise anstelle eines herkömmlichen URIs die Zeichenfolge myFTPapp ein.

- Anwendungspriorität - Beschreibung

  Die von Ihnen angegebene *Anwendungspriorität* wird mit der Anwendungspriorität abgeglichen, die durch die Anwendung für abgehende Daten bereitgestellt wird. Die Anwendung stellt den Prioritätswert mittels der API sendmsg() zur Verfügung. Wenn die Prioritäten übereinstimmen, wird der Datenaustausch der Anwendung in die Richtlinie für differenzierte Services aufgenommen. Der gesamte Datenaustausch, der in der Richtlinie für differenzierte Services definiert ist, erhält weiterhin die Priorität, die der gesamten Richtlinie zugewiesen ist.

Wenn Sie ein Anwendungstoken als Anwendungsdatentyp angeben, muss die Anwendung, die diese Informationen für das Betriebssystem bereitstellt, speziell für die Verwendung der API sendmsg() codiert sein. Vorgenommen wird dies durch den Anwendungsprogrammierer. Die Dokumentation der Anwendung sollte gültige Werte (Token und Priorität) angeben, die vom QoS-Administrator in der DiffServ-Richtlinie verwendet werden. Die Richtlinie für differenzierte Services wendet dann ihre eigene Priorität und Klassifizierung auf den Datenaustausch an, der dem in der Richtlinie festgelegten Token entspricht. Falls die Anwendung keine Werte enthält, die den in der Richtlinie festgelegten Werten entsprechen, müssen Sie entweder die Anwendung aktualisieren oder in der Richtlinie für differenzierte Services andere Parameter für die Anwendungsdaten verwenden.

URI bei Richtlinien für differenzierte Services verwenden

Beim Erstellen einer Richtlinie für differenzierte Services können Sie im Assistenten Systemdateninformationen festlegen (siehe Abschnitt "Anwendungstoken bei Richtlinien für differenzierte Services verwenden"). Die Felder im Assistenten fordern zwar die Eingabe eines Anwendungstokens an, aber Sie können stattdessen auch einen relativen URI angeben. Diese Einstellung ist, wie schon erwähnt, optional. Wenn Sie dieses Differenzierungsniveau in Ihren Richtlinien für abgehende Daten nicht benötigen, wählen Sie im Assistenten die Option **Alle Token** aus. Sie können eine Übereinstimmung mit einem in der Richtlinie für abgehende Daten festgelegten bestimmten URI angeben.

Der relative URI ist eigentlich eine Untergruppe eines absoluten URIs (ähnlich dem früheren absoluten URL). Nehmen wir beispielsweise die Angabe "http://www.ibm.com/software". Das Segment *http://www.ibm.com/software* gilt als absoluter URI. Das Segment */software* ist der relative URI. Alle relativen URI-Werte müssen mit einem Schrägstrich (/) beginnen. Die folgenden Segmente sind Beispiele für gültige relative URIs:

- /markt/lebensmittel#D5
- /software
- /markt/lebensmittel?q=gruen

Bevor Sie eine Richtlinie für differenzierte Services definieren, die URIs verwendet, müssen Sie sicherstellen, dass der Anwendungsport, der für den URI zugeordnet wird, der für FRCA (Fast Response Cache Accelerator) aktivierten Anweisung "listen" in der Konfiguration des Apache-Webservers entspricht.

Unter Adressen und Ports für den HTTP-Server (auf Apache-Basis) verwalten  ist erläutert, wie Sie den Port für Ihren HTTP-Server anzeigen oder ändern können.

FRCA stellt den URI für jede abgehende HTTP-Antwort fest. Diese Funktion vergleicht den URI der abgehenden Antwort mit den URIs, die in den Richtlinien für differenzierte Services definiert sind. Die erste Richtlinie mit einer Tokenzeichenfolge (URI), die dem durch FRCA festgestellten URI am meisten entspricht, wird auf alle Antworten für den URI angewendet.

Zugehörige Konzepte

„QoS-Erweiterungen der API sendmsg()" auf Seite 27
Die Funktion sendmsg() wird zum Senden von Daten und/oder von Hilfsdaten über einen verbundenen oder nicht verbundenen Socket verwendet.

Prioritäten definieren: Klassen verarbeiten

Nach der Klassifizierung des Datenaustausches benötigen die differenzierten Services außerdem ein Pro-Hop-Verhalten. Dieses definiert, wie der Datenaustausch zu verarbeiten ist.

Das Betriebssystem stellt die Servicestufe eines IP-Pakets anhand der Bit im IP-Header fest. Router und Switches ordnen ihre Ressourcen basierend auf den Informationen für das Pro-Hop-Verhalten zu, die im Feld für das Servicetypoktett (Type of Service = TOS) des IP-Headers angegeben sind. Das Feld für das Servicetypoktett wurde im Dokument "Request for Comments (RFC) 1349" und in V5R1 des Betriebssystems OS/400 erneut definiert. Ein *Pro-Hop-Verhalten* ist das Weiterleitungsverhalten, das einem Paket an einem Netzwerkknoten zugewiesen wird. Es wird durch einen Wert dargestellt, der als *Codepunkt* bezeichnet wird. Pakete können entweder auf dem Betriebssystem oder an anderen Stellen des Netzwerks (z. B. einem Router) markiert werden. Damit ein Paket den angeforderten Service beibehält, muss jeder Netzwerkknoten Angaben für differenzierte Services (DiffServ) erkennen können. Dies bedeutet, dass die Netzwerkeinheiten in der Lage sein müssen, das jeweilige Pro-Hop-Verhalten durchzusetzen. Um die Verarbeitung des Pro-Hop-Verhaltens durchzusetzen, muss ein Netzwerkknoten die Zeitplanung für Warteschlangen und die Prioritätsverwaltung für abgehende Daten verwenden können. Unter „Bedingungsfunktionen für den Datenaustausch" können Sie weitere Informationen zur Erkennung von DiffServ-Angaben nachlesen.

Falls Ihr Paket einen Router oder Switch passiert, der DiffServ-Angaben nicht erkennen kann, verliert das Paket an diesem Router seine Servicestufe. Das Paket wird zwar verarbeitet, erfährt jedoch möglicherweise eine unerwartete Verzögerung. Auf dem System können Sie die vordefinierten Codepunkte für das Pro-Hop-Verhalten verwenden oder aber eigene Codepunkte definieren. Die Erstellung eigener Codepunkte für die Verwendung außerhalb des privaten Netzwerkes ist nicht zu empfehlen. Wenn Sie nicht genau wissen, welche Codepunkte zuzuordnen sind, finden Sie unter „Pro-Hop-Verhalten mit Codepunkten zuordnen" auf Seite 16 weitere Informationen.

Anders als bei den integrierten Services ist für den Datenaustausch der differenzierten Services eine Reservierung oder datenflussspezifische Verarbeitung nicht erforderlich. Der gesamte Datenaustausch in derselben Klasse wird gleich behandelt.

Die differenzierten Services werden außerdem eingesetzt, um den Datenaustausch zu drosseln, der ein System verlässt. Dies bedeutet, dass Ihr System die differenzierten Services eigentlich zur Durchsatzbegrenzung einsetzt. Durch die Begrenzung einer weniger wichtigen Anwendung kann eine unternehmenskritische Anwendung das private Netzwerk als Erste verlassen. Wenn Sie für diese Richtlinie eine Serviceklasse erstellen, werden Sie aufgefordert, unterschiedliche Grenzwerte auf dem System festzulegen. Zu den Leistungsgrenzwerten gehören die Größe des Tokenpuffers, der Grenzwert für die Spitzengeschwindigkeit und der Grenzwert für die Durchschnittsgeschwindigkeit. Die Hilfethemen der QoS-Funktion von System i Navigator enthalten spezifischere Informationen zu diesen Grenzwerten.

Bedingungsfunktionen für den Datenaustausch

Damit QoS-Richtlinien verwendet werden können, müssen die Netzwerkeinheiten (wie beispielsweise Router und Switches) in der Lage sein, Bedingungsfunktionen für den Datenaustausch zu verarbeiten.

Bedingungsfunktionen für den Datenaustausch sind Klassifizierungsfunktionen, Messfunktionen, Markierungsfunktionen, Anpassungsfunktionen und Löschfunktionen.

Verfügt eine Netzwerkeinheit über alle Bedingungsfunktionen für den Datenaustausch, kann sie DiffServ-Angaben erkennen und ist somit DiffServ-fähig.

Anmerkung: Hierbei handelt es sich nicht um System i-spezifische Hardwarevoraussetzungen. In der QoS-Schnittstelle werden diese Elemente nicht angezeigt, da das System externe Hardware nicht steuern kann. Außerhalb eines privaten Netzwerks muss die Hardware in der Lage sein, allgemeine QoS-Anforderungen zu verarbeiten. In den Handbüchern zu den spezifischen Netzwerkeinheiten können Sie feststellen, ob diese Einheiten die Voraussetzungen für differenzierte Services erfüllen. Sie sollten die allgemeinen QoS-Konzepte und -Voraussetzungen prüfen, bevor Richtlinien implementiert werden.

Die folgende Abbildung zeigt in einer logischen Darstellung, wie die Bedingungsfunktionen für den Datenaustausch arbeiten:

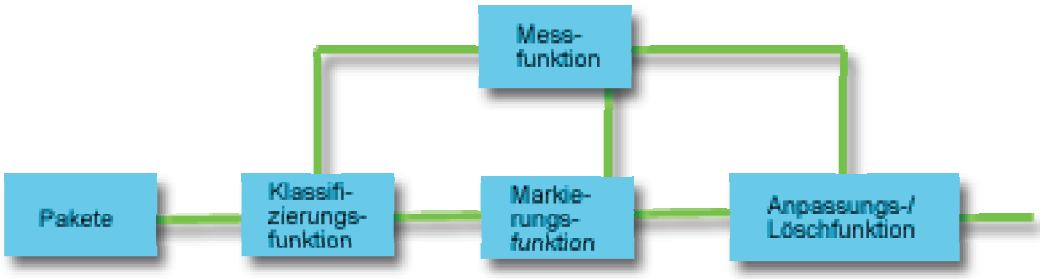


Abbildung 1. Bedingungsfunktionen für den Datenaustausch

Die folgenden Informationen beschreiben die einzelnen Bedingungsfunktionen für den Datenaustausch im Detail:

Klassifizierungsfunktionen
Klassifizierungsfunktionen für Pakete wählen Pakete in einem Datenaustauschstrom anhand des Inhalts im IP-Header des Pakets aus. Das Betriebssystem i5/OS definiert zwei Typen von Klassifizierungsfunktionen. Die Klassifizierungsfunktion des Typs ″Behavior Aggregate″ (Gesamtverhalten) klassifiziert Pakete ausschließlich anhand des Codepunktes für die differenzierten Services. Die Klassifizierungsfunktion des Typs ″Multi-Field″ (Mehrfeld) wählt Pakete anhand der Wertekombination aus einem oder mehreren Headerfeldern aus. Zu diesen Feldern gehören die Quellenadresse, die Zieladresse, das Feld für die differenzierten Services, die Protokoll-ID, der Ausgangsport, der URI, der Servertyp und die Zielportnummer.

Messfunktionen
Die Funktionen für die Datenaustauschmessung bewerten, ob die IP-Pakete, die durch die Klassifizierungsfunktion weitergeleitet wurden, dem IP-Headerprofil des Datenaustausches entsprechen. Die Informationen im IP-Header werden anhand der Werte bestimmt, die Sie in der QoS-Richtlinie für diesen Datenaustausch festlegen. Eine Messfunktion übergibt Informationen an andere Bedingungsfunktionen, um eine Aktion auszulösen. Die Aktion wird für jedes Paket ausgelöst, unabhängig davon, ob es der Profildefinition entspricht oder von dieser abweicht.

Markierungsfunktionen
Paketmarkierungsfunktionen legen das Feld für die differenzierten Services fest. Die

Markierungsfunktion kann so konfiguriert werden, dass alle Pakete mit einem einzelnen Codepunkt oder mit einer Gruppe von Codepunkten zur Auswahl eines Pro-Hop-Verhaltens markiert werden.

Anpassungsfunktionen
Anpassungsfunktionen verzögern einige oder alle Pakete in einem Datenaustauschstrom, um den Datenstrom an das Datenaustauschprofil anzugleichen. Die Puffergröße einer Anpassungsfunktion ist begrenzt. Router können Pakete löschen, wenn nicht genügend Speicherplatz zur Aufnahme der verzögerten Pakete vorhanden ist.

Löschfunktionen
Löschfunktionen löschen einige oder alle Pakete in einem Datenaustauschstrom. Dies geschieht, um den Datenstrom an das Datenaustauschprofil anzugleichen.

Zugehörige Konzepte

„Netzwerkhardware und -software" auf Seite 57
Das Leistungsspektrum Ihrer internen Ausstattung und der Einheiten außerhalb des Netzwerks hat beträchtliche Auswirkungen auf die QoS-Ergebnisse.

Integrierte Services

Der zweite Typ einer Richtlinie für die Bandbreite abgehender Daten, den Sie erstellen können, ist eine Richtlinie für integrierte Services. Die integrierten Services bieten IP-Anwendungen die Möglichkeit, unter Verwendung des RSVP-Protokolls (ReSerVation Protocol) und der APIs für QoS Bandbreite anzufordern und zu reservieren.

Die Richtlinien für integrierte Services verwenden das RSVP und die RAPI-API (oder die qtoc-Socket-API), um eine durchgängige Verbindung zu garantieren. Dies ist die höchste Servicestufe, die Sie zuordnen können. Es handelt sich allerdings auch um den komplexeste Service.

Mit den integrierten Services können Sie die Zeit für die Datenaustauschübermittlung beeinflussen und einem bestimmten Datenaustausch spezielle Verarbeitungsanweisungen zuordnen. Der Einsatz von Richtlinien für integrierte Services sollte jedoch unbedingt gut überlegt erfolgen, da die Garantierung des Datenaustausches noch immer relativ teuer ist. Andererseits kann eine übermäßige Bereitstellung von Ressourcen sogar noch teurer sein.

Die integrierten Services reservieren Ressourcen für eine bestimmte Richtlinie, bevor die Daten gesendet werden. Die Router erhalten vor der Datenübertragung ein entsprechendes Signal, und das Netzwerk akzeptiert und verwaltet den Datenaustausch (von Endpunkt zu Endpunkt) auf der Basis einer Richtlinie. Eine *Richtlinie* ist eine Gruppe von Regeln, die eine Aktion definieren. Im Grunde genommen handelt es sich um eine Liste für die Zugangssteuerung. Die Bandbreitenanforderung erfolgt in Form einer Reservierung durch den Client. Wenn alle Router im Pfad die Voraussetzungen des anfordernden Clients akzeptieren, wird die Anforderung an das System und die Richtlinie für integrierte Services weitergeleitet. Falls die Anforderung die Grenzwerte, die in der Richtlinie definiert sind, nicht überschreitet, erteilt der QoS-Server die Berechtigung für die RSVP-Verbindung und reserviert anschließend die Bandbreite für die Anwendung. Die Reservierung wird unter Verwendung des RSVP und der RAPI-API oder der qtoc-Socket-APIs für QoS vorgenommen.

Jeder Knoten, den der Datenaustausch passiert, muss RSVP verwenden können. Router stellen QoS über die folgenden Funktionen zur Datenaustauschsteuerung bereit: Paketscheduler, Paketklassifizierung und Zugangssteuerung. Die Fähigkeit zur Ausführung dieser Datenaustauschsteuerung wird häufig als RSVP-Fähigkeit bezeichnet. Infolgedessen ist die Möglichkeit, die Ressourcen im Netzwerk zu steuern und vorherzusehen, der wichtigste Bestandteil bei der Implementierung von Richtlinien für integrierte Services. Um vorhersehbare Ergebnisse erzielen zu können, muss jeder Knoten im Netzwerk RSVP-fähig sein. Beispiel: Ihr Datenaustausch wird basierend auf Ressourcen weitergeleitet und nicht auf der Basis von Pfaden, die RSVP-fähige Router enthalten. Wenn nun der Datenaustausch Router passiert, die nicht RSVP-fähig sind, kann dies zu unvorhersehbaren Durchsatzproblemen führen. Die Verbindung wird zwar hergestellt, aber die von der Anwendung angeforderte Leistung kann durch diesen Router nicht garan-

tiert werden. Die folgende Abbildung zeigt die logische Funktionsweise der integrierten Services.

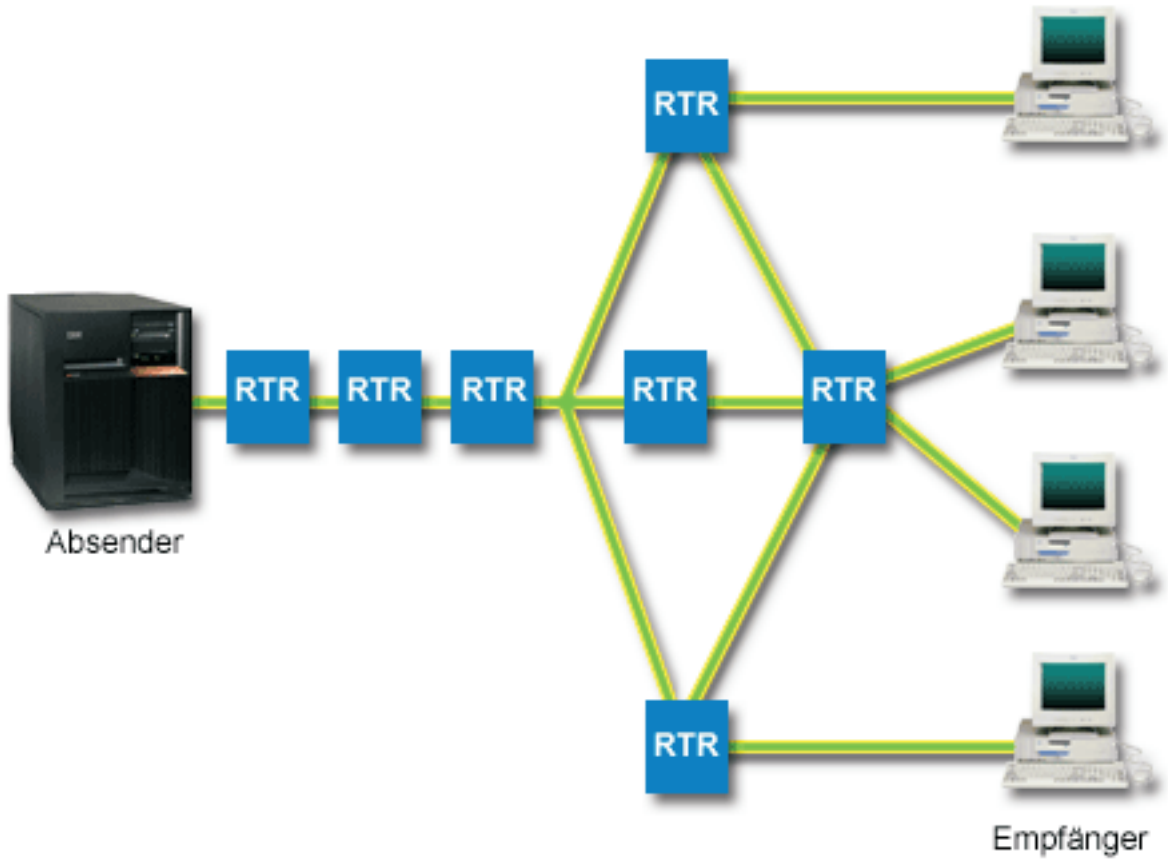


Abbildung 2. RSVP-Pfad zwischen Client und Server

Die RSVP-fähige Anwendung auf dem Server in der Abbildung oben stellt eine von den Clients oder den Empfängern ausgehende Verbindungsanforderung fest. Als Reaktion gibt die Anwendung einen Befehl PATH an den Client aus. Dieser Befehl wird mit der RAPI-API oder den qtoc-Socket-APIs von QoS abgesetzt und enthält Informationen zur IP-Adresse des Routers (RTR). Ein Befehl PATH enthält Informationen zu den verfügbaren Ressourcen auf dem Server und den im Pfad vorhandenen Routern sowie Informationen zu den Routen zwischen dem Server und dem Client. Die RSVP-fähige Anwendung auf dem Client sendet anschließend einen Befehl RESV zusammen mit dem Netzwerkpfad zurück und signalisiert dem Server auf diese Weise, dass die Netzwerkressourcen zugeordnet wurden. Dieser Befehl nimmt die Reservierung anhand der Routerinformationen aus dem Befehl PATH vor. Der Server und alle Router im Pfad reservieren die Ressourcen für die RSVP-Verbindung. Sobald der Server den Befehl RESV empfängt, beginnt die Anwendung mit der Übertragung von Daten an den Client. Die Daten werden über den gleichen Pfad wie die Reservierung übertragen. Dies macht noch einmal deutlich, wie wichtig es für den erfolgreichen Einsatz von Richtlinien ist, dass die Router diese Reservierung vornehmen können.

Integrierte Services sind nicht für kurzfristige RSVP-Verbindungen wie HTTP gedacht. Natürlich liegt dies in Ihrem eigenen Ermessen. Nur Sie wissen, welche Lösung für Ihr Netzwerk am besten geeignet ist. Zu berücksichtigen ist hierbei, bei welchen Anwendungen und in welchen Bereichen Leistungsprobleme auftreten und QoS erforderlich ist. Anwendungen, die in einer Richtlinie für integrierte Services eingesetzt werden, müssen RSVP verwenden können. Anfangs verfügt das Betriebssystem i5/OS über keine RSVP-fähigen Anwendungen. Sie müssen daher die Anwendung bereitstellen, um RSVP verwenden zu können.

Sobald Pakete eintreffen und versuchen, das Netzwerk zu verlassen, ermittelt das Betriebssystem, ob die Ressourcen für das Senden der Pakete verfügbar sind. Grundlage dieser Entscheidung ist der Umfang des Speicherplatzes im Tokenpuffer. Die Anzahl der im Tokenpuffer zulässigen Bit, Bandbreitengrenzen, Grenzwerte für die Tokengeschwindigkeit und die maximal zulässige Anzahl von Verbindungen auf dem System werden von Ihnen manuell definiert. Diese Werte werden als Leistungsgrenzwerte bezeichnet. Falls das Paket die Grenzwerte nicht überschreitet, gelten die Pakete als konform und werden gesendet. Bei den integrierten Services erhält jede Verbindung einen eigenen Tokenpuffer.

Integrierte Services mit DiffServ-Markierungen

Wenn Sie nicht genau wissen, ob eine RSVP-Verbindung im gesamten Netzwerk garantiert werden kann, können Sie dennoch eine Richtlinie für integrierte Services erstellen. Falls die Netzwerkressourcen RSVP nicht verwenden können, kann die Verbindung nicht garantiert werden. In einer solchen Situation kann es günstig sein, einen Codepunkt auf die Richtlinie anzuwenden. Dieser Codepunkt wird normalerweise in Richtlinien für differenzierte Services eingesetzt, um dem Datenaustausch eine Serviceklasse zuzuweisen. Auch wenn die Verbindung nicht garantiert wird, versucht dieser Codepunkt, der Verbindung gewisse Prioritäten zu erteilen.

Zugehörige Konzepte

„APIs für QoS" auf Seite 18
Dieses Thema enthält Informationen über Protokolle, APIs und die Voraussetzungen für einen Router, der RSVP (ReSerVation Protocol) verwenden kann, also RSVP-fähig ist. Zu den APIs für QoS gehören die RAPI-API, die qtoq-Socket-API, die API sendmsg() und die monitor-APIs.

„Szenario: Vorhersehbarer B2B-Datenaustausch" auf Seite 44
Wenn Sie eine vorhersehbare Übermittlung benötigen und dennoch eine Reservierung anfordern müssen, können Sie natürlich auch eine Richtlinie für integrierte Services verwenden. Dieses Beispiel verwendet einen Service des Typs ″Gesteuertes Laden″.

„Szenario: Dedizierte Übermittlung (IP-Telefonie)" auf Seite 48
Wenn Sie eine dedizierte Übermittlung benötigen und eine Reservierung anfordern wollen, verwenden Sie eine Richtlinie für integrierte Services. Sie können zwei unterschiedliche Typen von Richtlinien für integrierte Services erstellen, nämlich ″Garantiert″ und ″Gesteuertes Laden″. In diesem Beispiel wird ein Service des Typs ″Garantiert″ verwendet.

Funktionen zur Datenaustauschsteuerung

Die Funktionen zur Datenaustauschsteuerung können nur auf integrierte Services angewendet werden und sind nicht System i-spezifisch.

In der QoS-Schnittstelle werden diese Elemente nicht angezeigt, da der Server externe Hardware nicht steuern kann. Außerhalb eines privaten Netzwerks muss die Hardware in der Lage sein, allgemeine QoS-Anforderungen zu verarbeiten. Die allgemeinen Routervoraussetzungen für Richtlinien für integrierte Services werden im folgenden Abschnitt erläutert. Es empfiehlt sich, die allgemeinen QoS-Konzepte und -Voraussetzungen zu prüfen, bevor die Richtlinien implementiert werden.

Um die vorhersehbaren Ergebnisse erzielen zu können, muss die Hardware im Pfad für den Datenaustausch RSVP-fähig sein. Router müssen mit bestimmten Funktionen zur Datenaustauschsteuerung ausgestattet sein, damit RSVP verwendet werden kann. Dies wird häufig als RSVP-Fähigkeit oder QoS-Fähigkeit bezeichnet. Bitte berücksichtigen Sie, dass das Betriebssystem entweder als Client oder als Server fungiert. Seine Verwendung als Router ist zu diesem Zeitpunkt nicht möglich. In den Handbüchern Ihrer Netzwerkeinheiten können Sie feststellen, ob die QoS-Voraussetzungen erfüllt werden.

Zu den Funktionen für die Datenaustauschsteuerung gehören:

Paketscheduler

Ein Paketscheduler verwaltet die Paketweiterleitung anhand der Informationen im IP-Header. Er stellt sicher, dass die Paketübermittlung den Parametern entspricht, die Sie in der Richtlinie definiert haben. Der Scheduler wird an der Stelle implementiert, an der die Pakete in eine Warteschlange gestellt werden.

Paketklassifizierung

Die Funktion zur Paketklassifizierung stellt (anhand der Informationen im IP-Header) fest, welche Pakete eines IP-Datenflusses eine bestimmte Servicestufe erhalten. Jedes ankommende Paket wird durch die Klassifizierungsfunktion einer spezifischen Klasse zugeordnet. Alle Pakete, die für dieselbe Klasse klassifiziert wurden, werden gleich behandelt. Diese Servicestufe basiert auf den Informationen, die Sie in der Richtlinie angeben.

Zugangssteuerung

Die Zugangssteuerung enthält den Entscheidungsalgorithmus, mit dessen Hilfe ein Router feststellt, ob genügend Weiterleitungsressourcen vorhanden sind, um die angeforderte QoS für einen neuen Datenfluss zu akzeptieren. Wenn nicht genügend Ressourcen vorhanden sind, wird der neue Datenfluss zurückgewiesen. Wird der Datenfluss akzeptiert, ordnet der Router die Paketklassifizierung und den Paketscheduler zu, um die angeforderte QoS zu reservieren. Die Zugangssteuerung findet in jedem Router des Reservierungspfades statt.

Zugehörige Konzepte

„APIs für QoS" auf Seite 18
Dieses Thema enthält Informationen über Protokolle, APIs und die Voraussetzungen für einen Router, der RSVP (ReSerVation Protocol) verwenden kann, also RSVP-fähig ist. Zu den APIs für QoS gehören die RAPI-API, die qtoq-Socket-API, die API sendmsg() und die monitor-APIs.

Zugehörige Verweise

„Referenzinformationen zu QoS" auf Seite 75
RFCs (Request for Comments) für QoS, IBM Redbooks und andere Themensammlungen im Information Center enthalten Informationen, die sich auf die QoS-Themensammlung beziehen. Sie können alle PDF-Dateien anzeigen oder drucken.

Typen von integrierten Services

Es gibt zwei Typen von integrierten Services: gesteuertes Laden und garantierter Service.

Gesteuertes Laden

Ein Service des Typs ″Gesteuertes Laden″ unterstützt Anwendungen, die sehr empfindlich auf Netzwerküberlastungen reagieren (z. B. Echtzeitanwendungen). Anwendungen müssen außerdem geringe Verluste und Verzögerungen tolerieren. Wenn eine Anwendung einen Service des Typs ″Gesteuertes Laden″ verwendet, leidet ihr Leistungsverhalten nicht unter einer Zunahme der Netzwerkauslastung. Dem Datenaustausch wird ein Service bereitgestellt, der etwa dem normalen Datenaustausch in einem Netzwerk mit normalen Bedingungen entspricht.

Router müssen sicherstellen, dass der Service des Typs ″Gesteuertes Laden″ eine angemessene Bandbreite und die entsprechenden Ressourcen für die Paketverarbeitung erhält. Hierzu müssen die Router QoS-fähig sein und integrierte Services unterstützten. In den Spezifikationen des Routers können Sie prüfen, ob der Router QoS über eine Funktion zur Datenaustauschsteuerung bereitstellt. Die Datenaustauschsteuerung besteht aus den folgenden Komponenten: Paketscheduler, Paketklassifizierung und Zugangssteuerung.

Garantiert

Der Service ″Garantiert″ stellt sicher, dass Pakete innerhalb einer bestimmten Zustellfrist beim Empfänger ankommen. Zu den Anwendungen, die den Service ″Garantiert″ benötigen, gehören Rundesendesysteme für Video- und Audiodaten, die mit Streamingtechnologien arbeiten. Ein Service des Typs ″Garantiert″ steuert die maximale Verzögerung für die Warteschlange, damit die Pakete nicht über einen bestimmten Zeitraum hinaus verzögert werden. Jeder Router im Pfad des Pakets muss RSVP-fähig sein, damit die Zustellung sichergestellt werden kann. Wenn Sie die Grenzwerte für Token-Puffer und Bandbreite zuordnen, definieren Sie einen Service ″Garantiert″. Die Verwendung des Services ″Garantiert″ ist nur bei Anwendungen gültig, die TCP verwenden.

Zugehörige Konzepte

„Szenario: Vorhersehbarer B2B-Datenaustausch" auf Seite 44
Wenn Sie eine vorhersehbare Übermittlung benötigen und dennoch eine Reservierung anfordern müssen, können Sie natürlich auch eine Richtlinie für integrierte Services verwenden. Dieses Beispiel verwendet einen Service des Typs "Gesteuertes Laden".

„Szenario: Dedizierte Übermittlung (IP-Telefonie)" auf Seite 48
Wenn Sie eine dedizierte Übermittlung benötigen und eine Reservierung anfordern wollen, verwenden Sie eine Richtlinie für integrierte Services. Sie können zwei unterschiedliche Typen von Richtlinien für integrierte Services erstellen, nämlich "Garantiert" und "Gesteuertes Laden". In diesem Beispiel wird ein Service des Typs "Garantiert" verwendet.

Grenzwerte für Token-Puffer und Bandbreite

Grenzwerte für Token-Puffer und Bandbreite werden unter dem Begriff "Leistungsgrenzen" zusammengefasst. Mit solchen Leistungsgrenzen kann die Paketübermittlung in Richtlinien für die Bandbreite abgehender Daten (sowohl für integrierte Services als auch für differenzierte Services) garantiert werden.

Größe des Token-Puffers

Die *Größe des Token-Puffers* bestimmt, wie viele Informationen Ihr System zu einem bestimmten Zeitpunkt verarbeiten kann. Wenn eine Anwendung Daten schneller an das System sendet, als dieses sie aus dem Netzwerk heraussenden kann, füllt sich der Puffer. Alle Datenpakete, die diesen Grenzwert überschreiten, werden als Datenpakete behandelt, die von der Profildefinition abweichen. Von dieser Regel ausgenommen sind Richtlinien für integrierte Services. Sie können auswählen, dass `keine Begrenzung` gelten soll. In diesem Fall ist eine RSVP-Verbindungsanforderung zulässig. Bei allen anderen Richtlinien können Sie bestimmen, wie Datenaustausch, der von der Profildefinition abweicht, behandelt werden soll. Die maximale Größe für den Tokenpuffer beträgt 1 GB.

Grenze für Tokengeschwindigkeit

Die *Grenze für Tokengeschwindigkeit* gibt die langfristige Übertragungsgeschwindigkeit an, also die in einem Netzwerk zulässige Anzahl der Bit pro Sekunde. Die QoS-Richtlinie vergleicht die angeforderte Bandbreite mit den Grenzwerten für Geschwindigkeit und Datenfluss, die in der Richtlinie festgelegt sind. Wenn die Anforderung dazu führt, dass das System seine Grenzwerte überschreitet, weist es die Anforderung zurück. Die Grenze für die Tokengeschwindigkeit wird nur in Richtlinien für integrierte Services zur Zugangssteuerung verwendet. Dieser Wert kann zwischen 10 Kb/s und 1 Gb/s variieren. Sie können für diesen Wert aber auch die Einstellung `Keine Begrenzung` festlegen. Wenn Sie die Einstellung `Keine Begrenzung` für die Geschwindigkeit auswählen, wird der Grenzwert durch die verfügbaren Ressourcen bestimmt.

Tipp: Es ist unter Umständen sinnvoll, eine Überwachung auszuführen, um die festzulegenden Grenzwerte zu ermitteln. Erstellen Sie eine Richtlinie, deren Grenzwert für die Tokendurchschnittsgeschwindigkeit ausreichend hoch ist, um den Großteil des Datenverkehrs im Netzwerk erfassen zu können. Anschließend starten Sie die Datenerfassung für diese Richtlinie. Das Szenario für die Überwachung der aktuellen Netzwerkstatistik stellt eine Methode für die Erfassung der Gesamtgeschwindigkeiten vor, die gegenwärtig von der Anwendung und dem Netzwerk verwendet werden. Anhand dieser Ergebnisse können Sie die Grenzwerte entsprechend herabsetzen.

Wenn Sie anstelle einer bestimmten Datenerfassung eine Echtzeitüberwachung ansehen wollen, müssen Sie einfach nur die Überwachung öffnen. Die Überwachung stellt eine Echtzeitstatistik für alle aktiven Richtlinien zur Verfügung.

Zugehörige Konzepte

„Differenzierte Services" auf Seite 2
Dies ist der erste Typ einer Richtlinie für die Bandbreite abgehender Daten, den Sie auf dem Betriebssystem erstellen können. Die differenzierten Services unterteilen den Datenaustausch im Netzwerk in

unterschiedliche Klassen. Wenn Sie eine Richtlinie für differenzierte Services einsetzen wollen, müssen Sie festlegen, wie der Datenaustausch im Netzwerk klassifiziert werden soll und wie die unterschiedlichen Klassen zu behandeln sind.

„Szenario: Aktuelle Netzwerkstatistik überwachen" auf Seite 52
Sie müssen die Leistungsgrenzwerte, die auf einzelnen Netzwerkvoraussetzungen basieren, innerhalb der Assistenten festlegen.

Integrierte Services mit DiffServ-Markierungen

Durch DiffServ-Markierungen in einer Richtlinie für integrierte Services können Sie die Priorität der Pakete verwalten, die in einer heterogenen Umgebung gesendet werden.

Eine heterogene Umgebung entsteht, wenn eine Reservierung von integrierten Services unterschiedliche Router passiert, die solche Reservierungen nicht unterstützen, jedoch eine Unterstützung für differenzierte Services bieten. Da Ihr Datenaustausch verschiedene Domänen, Service-Level-Agreements und Einheitenfunktionalitäten passiert, erhalten Sie nicht in allen Fällen den gewünschten Service.

Um dieses potenzielle Problem abzuschwächen, können Sie Ihrer Richtlinie für integrierte Services eine DiffServ-Markierung zuordnen. Falls eine Richtlinie einen Router passiert, der das RSVP-Protokoll nicht verwenden kann, behält Ihre Richtlinie dann gewisse Prioritäten bei. Die von Ihnen hinzugefügte Markierung wird als *Pro-Hop-Verhalten* bezeichnet.

Signal senden inaktivieren

Neben der Verwendung von Markierungen können Sie außerdem die Funktion "Signal senden inaktivieren" verwenden. Wenn Sie diese Funktion auswählen, können Sie mit den gleichlautenden Versionen der APIs eine Anwendung schreiben, die das Laden einer RSVP-Regel im Betriebssystem veranlasst. Bei der Anwendung muss nur die serverseitige Anwendung des TCP/IP-Dialogs RSVP-fähig sein. Die RSVP-Signalsendung erfolgt für die Clientseite automatisch. Dies erstellt die RSVP-Verbindung für die Anwendung auch dann, wenn die Clientseite RSVP nicht verwenden kann.

Die Funktion "Signal senden inaktivieren" wird in der Richtlinie für integrierte Services angegeben. So können Sie angeben, dass die Funktion "Signal senden inaktivieren" verwendet werden soll:

1. Erweitern Sie in System i Navigator ***Ihr System*** → **Netzwerk** → **IP-Richtlinien**.
2. Klicken Sie mit der rechten Maustaste auf **Quality of Service**, und wählen Sie die Option **Konfiguration** aus.
3. Erweitern Sie die Einträge **Richtlinien für Bandbreite abgehender Daten** → **IntServ**.
4. Klicken Sie mit der rechten Maustaste auf den Namen der gewünschten Richtlinie für integrierte Services, und wählen Sie die Option **Eigenschaften** aus. Das Fenster mit den IntServ-Eigenschaften wird aufgerufen.
5. Wählen Sie die Indexzunge **Datenaustauschverwaltung** aus, um das Senden von Signalen zu inaktivieren oder zu aktivieren. Hier können Sie außerdem den Zeitplan, den Client, die Anwendungen und die Datenaustauschverwaltung bearbeiten.

Zugehörige Konzepte

„Serviceklasse" auf Seite 14
Beim Erstellen einer Richtlinie für differenzierte Services oder für ankommende Daten erstellen und verwenden Sie ebenfalls eine Serviceklasse.

Richtlinien für ankommende Daten

Mit den Richtlinien für ankommende Daten werden die Verbindungsanforderungen gesteuert, die in Ihrem Netzwerk eintreffen.

Mit einer Richtlinie für ankommende Daten wird der Datenaustausch begrenzt, der versucht, eine Verbindung zum System herzustellen. Sie können den Zugriff nach Client, URI, Anwendung oder lokaler Schnittstelle auf dem System einschränken. Außerdem können Sie die Systemleistung heraufsetzen,

indem Sie eine Serviceklasse auf den ankommenden Datenaustausch anwenden. Eine solche Richtlinie wird mit dem Assistenten für Richtlinien für ankommende Daten in System i Navigator definiert.

Es gibt drei Komponenten einer Richtlinie für ankommende Daten, die genauer erläutert werden müssen. Hierzu gehören die URIs für die Begrenzung des Datenaustausches, die in einer Serviceklasse definierten Verbindungsgeschwindigkeiten sowie die Prioritätswarteschlangen zur Anforderung von erfolgreichen Verbindungen. Weitere Informationen finden Sie unter „URI", „Verbindungsgeschwindigkeit" auf Seite 14 und „Prioritätswarteschlangen mit Wertigkeit" auf Seite 14.

URI

Wenn Sie den HTTP-Datenaustausch, der Verbindungen zu Ihrem Webserver herstellt, begrenzen wollen, können Sie zu diesem Zweck eine Richtlinie für ankommende Daten verwenden. Beispielsweise könnten Sie in diesem Fall eine Richtlinie für ankommende Daten erstellen, die den Datenaustausch für einen spezifischen URI einschränkt. Die URI-Anforderungsgeschwindigkeit ist Bestandteil einer Lösung für den Schutz von Servern gegen Überlastung. Die Angabe spezifischer URIs führt zur Anwendung von Zugangssteuerungen, die auf Informationen auf Anwendungsebene basieren und die vom Server akzeptierten URI-Anforderungen begrenzen. Branchenintern wird dies auch als headerbasierte Steuerung von Verbindungen bezeichnet, bei der URIs zum Festlegen von Prioritäten verwendet werden.

Bei der Angabe eines URIs kann die Richtlinie für ankommende Daten nicht nur die Paketheader, sondern den gesamten Inhalt untersuchen. Der untersuchte Inhalt ist ein URI-Name. Für das Betriebssystem i5/OS können Sie den relativen URI-Namen verwenden (z. B. `/produkte/bekleidung`).

Relativer URI

Der *relative URI* ist eigentlich eine Untergruppe eines absoluten URIs (ähnlich dem früheren absoluten URL). Nehmen wir beispielsweise die Angabe "http://www.ibm.com/software". Das Segment *http://www.ibm.com/software* gilt als absoluter URI. Das Segment */software* ist der relative URI. Alle relativen URI-Werte müssen mit einem Schrägstrich (/) beginnen. Die folgenden Segmente sind Beispiele für gültige relative URIs:

- /markt/lebensmittel#D5
- /software
- /markt/lebensmittel?q=gruen

Hinweise:

- Bei Verwendung eines URIs müssen Sie das Protokoll mit TCP angeben. Außerdem müssen der Port und die IP-Adresse mit dem Port und der IP-Adresse identisch sein, die für Ihren HTTP-Server konfiguriert sind. Normalerweise ist dies Port 80.
- Bei der Angabe eines URIs gibt es ein implizites Platzhalterzeichen. Die Angabe "/software" schließt beispielsweise alles im Verzeichnis "software" ein.
- Verwenden Sie im URI keinen Stern (*). Dieses Zeichen ist ungültig.
- URI-Informationen können sowohl in Richtlinien für ankommende Daten als auch in Richtlinien für differenzierte Services (für abgehende Daten) verwendet werden.

Bevor Sie eine Richtlinie für ankommende Daten definieren, die URIs verwendet, müssen Sie sicherstellen, dass der dem URI zugeordnete Anwendungsport der Anweisung "listen" (= Empfangsbereit) entspricht, die für FRCA (Fast Response Cache Accelerator) in der Konfiguration des Apache-Webservers aktiviert ist. Unter Adressen und Ports für den HTTP-Server (auf Apache-Basis) verwalten ist erläutert, wie Sie den Port für Ihren HTTP-Server anzeigen oder ändern können.

Verbindungsgeschwindigkeit

In einer Richtlinie für ankommende Daten müssen Sie ebenfalls eine Serviceklasse auswählen. Diese Serviceklasse definiert die Verbindungsgeschwindigkeiten, die als Zugangssteuerung dienen und die vom System akzeptierten Verbindungen begrenzen.

Die Grenzwerte für Verbindungsgeschwindigkeiten legen die in der erstellten Richtlinie definierte durchschnittliche Anzahl von Verbindungen pro Sekunde und die maximale Anzahl gleichzeitiger Verbindungen zu Grunde, um ein neues Paket zu akzeptieren bzw. zurückzuweisen. Zu diesen Grenzwerten für Verbindungen gehören ein Grenzwert für die Durchschnittsgeschwindigkeit und eine Burstrate, die Sie über die Assistenten von System i Navigator eingeben. Sobald eingehende Verbindungsanforderungen das System erreichen, ermittelt das System anhand der Angaben im Paketheader, ob dieser Datenaustausch in einer Richtlinie definiert ist. Das System gleicht diese Informationen mit dem Profil für die Verbindungsgrenzwerte ab. Wenn das Paket innerhalb der Grenzwerte der Richtlinien liegt, wird es in die Warteschlange gestellt.

Verwenden Sie die obigen Informationen beim Durcharbeiten des Assistenten für Richtlinien für ankommende Daten. In System i Navigator können Sie beim Erstellen der Richtlinie auch den zugeordneten Hilfetext hinzuziehen, der ähnliche Informationen enthält.

Prioritätswarteschlangen mit Wertigkeit

Im Rahmen der Steuerung von ankommenden Daten können Sie die Priorität definieren, in der die Verbindungsanforderungen verarbeitet werden sollen, nachdem sie von den Richtlinien ausgewertet wurden. Wenn Sie einer Prioritätswarteschlange eine Wertigkeit zuordnen, steuern Sie damit eigentlich die Antwortzeit der Warteschlange, nachdem eine Verbindung eintroffen ist. Falls die Verbindung in die Warteschlange gestellt wird, wird sie in der Reihenfolge der Warteschlangenpriorität (″Hoch″, ″Mittel″, ″Niedrig″ oder ″Bester Versuch″) verarbeitet. Wenn Sie sich nicht sicher sind, welche Wertigkeiten zuzuordnen sind, verwenden Sie die Standardwerte. Die Summe aller Wertigkeiten muss 100 sein. Beispiel: Wenn Sie für alle Prioritäten den Wert 25 angeben, werden alle Warteschlangen gleich behandelt. Geben Sie aber die Wertigkeiten mit ″Hoch″ (50), ″Mittel″ (30), ″Niedrig″ (15) und ″Bester Versuch″ (5) an, enthalten die akzeptierten Verbindungen Folgendes:

- 50% Verbindungen mit hoher Priorität
- 30 % Verbindungen mit mittlerer Priorität
- 15% Verbindungen mit niedriger Priorität
- 5% Verbindungen mit der Priorität ″Bester Versuch″

Zugehörige Konzepte

„Serviceklasse”
Beim Erstellen einer Richtlinie für differenzierte Services oder für ankommende Daten erstellen und verwenden Sie ebenfalls eine Serviceklasse.

„Grenzwerte für Durchschnittsverbindungsgeschwindigkeit und Burstrate” auf Seite 18
Grenzwerte für die Verbindungsgeschwindigkeit und die Burstrate sind Grenzwerte. Diese Grenzwerte für die Geschwindigkeit ermöglichen die Begrenzung von eingehenden Verbindungen, die auf dem System eintreffen. Grenzwerte für Geschwindigkeiten werden in einer Serviceklasse festgelegt, die zusammen mit Richtlinien für ankommende Daten verwendet wird.

Serviceklasse

Beim Erstellen einer Richtlinie für differenzierte Services oder für ankommende Daten erstellen und verwenden Sie ebenfalls eine Serviceklasse.

Richtlinien für differenzierte Services und Richtlinien für ankommende Daten teilen den Datenaustausch mit Hilfe einer Serviceklasse in Klassen ein. Auch wenn der größte Teil dieses Vorgangs über die Hardware erfolgt, können Sie steuern, wie der Datenaustausch gruppiert wird und welche Priorität der Datenaustausch erhalten soll.

Zur Ausführung von QoS müssen Sie zunächst Richtlinien definieren. Die Richtlinien legen Herkunft, Typ, Position und Zeitpunkt der Daten fest. Anschließend müssen Sie Ihrer Richtlinie eine Serviceklasse zuordnen. Serviceklassen werden separat definiert und können von anderen Richtlinien wiederverwendet werden. Beim Definieren einer Serviceklasse geben Sie an, ob sie auf Richtlinien für abgehende Daten und/oder auf Richtlinien für ankommende Daten angewendet werden kann. Wenn Sie beide Möglichkeiten auswählen (abgehende und ankommende Daten), kann diese Serviceklasse von einer Richtlinie für differenzierte Services und einer Richtlinie für ankommende Daten verwendet werden.

Die Einstellungen in der Serviceklasse sind davon abhängig, ob sie für ankommende Daten, für abgehende Daten oder für beide Richtlinientypen verwendet wird. Bei der Erstellung einer Serviceklasse stellen Sie möglicherweise die folgenden Anforderungen fest:

Codepunktmarkierung
QoS verwendet die empfohlenen Codepunkte, um einem Datenaustausch ein Pro-Hop-Verhalten zuzuordnen. Router und Switches verwenden diese Codepunkte, um dem Datenaustausch Prioritätsstufen zuzuweisen. Ihr System kann diese Codepunkte nicht nutzen, da es nicht als Router agiert. Ausgehend von den spezifischen Anforderungen in Ihrem Netzwerk müssen Sie ermitteln, welche Codepunkte zu verwenden sind. Berücksichtigen Sie hierbei, welche Anwendungen am wichtigsten sind und welchen Richtlinien eine höhere Priorität zugeordnet werden muss. Am wichtigsten ist hierbei die Konsistenz der Markierungen, damit Sie die erwarteten Ergebnisse erzielen. Die Codepunkte sind ein essenzieller Aspekt bei der Differenzierung der unterschiedlichen Datenaustauschklassen.

Datenaustauschmessung
QoS verwendet Grenzwerte für die Geschwindigkeitssteuerung, um den Datenaustausch in Netzwerk einzuschränken. Diese Grenzwerte werden durch das Festlegen der folgenden Werte definiert: Größe des Tokenpuffers, Grenzwert für die Spitzengeschwindigkeit und Grenzwert für die Durchschnittsgeschwindigkeit. Weitere Informationen zu diesen spezifischen Werten finden Sie unter „Grenzwerte für Token-Puffer und Bandbreite" auf Seite 11.

Von Profildefinition abweichender Datenaustausch
Der letzte Bestandteil einer Serviceklasse ist die Verarbeitung des von der Profildefinition abweichenden Datenaustausches. Wenn Sie die Grenzwerte für die Geschwindigkeitssteuerung zuordnen, legen Sie Werte für die Einschränkung des Datenaustausches fest. Sobald der Datenaustausch diese Einschränkungen überschreitet, gelten die Pakete als von der Profildefinition abweichend. Die Informationen in einer Serviceklasse teilen dem System mit, ob UDP-Datenaustausch gelöscht und das TCP-Überlastungsfenster verkleinert werden soll bzw. ob von der Profildefinition abweichende Pakete angepasst oder erneut markiert werden sollen.

UDP-Pakete löschen oder TCP-Überlastungsfenster verkleinern: Wenn Sie beschließen, dass von der Profildefinition abweichende Pakete gelöscht und angepasst werden sollen, werden die UDP-Pakete gelöscht. Das TCP-Überlastungsfenster wird jedoch verkleinert, so dass die Datengeschwindigkeit der Geschwindigkeit des Tokenpuffers entspricht. Die Anzahl der Pakete, die zu einem bestimmten Zeitpunkt in das Netzwerk gesendet werden können, wird reduziert, und die Überlastung wird verringert.

Verzögern (Anpassen): Wenn Sie Pakete, die von der Profildefinition abweichen, verzögern, werden die Pakete so angepasst, dass sie den von Ihnen definierten Verarbeitungsmerkmalen entsprechen.

Mit DiffServ-Codepunkt erneut markieren: Wenn Sie Pakete, die von der Profildefinition abweichen, mit einem Codepunkt erneut markieren, wird den Paketen ein neuer Codepunkt zugeordnet. Die Pakete werden nicht gedrosselt, um die Anforderungen der Verarbeitungsmerkmale zu erfüllen, sondern nur erneut markiert. Weitere spezifische Informationen erhalten Sie, wenn Sie beim Zuordnen dieser Verarbeitungsanweisungen im Assistenten auf "Hilfe" klicken.

Priorität
Sie können für die Verbindungen, die zu Ihrem System hergestellt werden, durch verschiedene Richtlinien für ankommende Daten Prioritäten vergeben. Auf diese Weise können Sie die Reihen-

folge festlegen, in der hergestellte Verbindungen von Ihrem System bearbeitet werden. Zur Auswahl stehen die Optionen ″Hoch″, ″Mittel″, ″Niedrig″ oder ″Bester Versuch″.

Zugehörige Konzepte

„Integrierte Services mit DiffServ-Markierungen” auf Seite 12
Durch DiffServ-Markierungen in einer Richtlinie für integrierte Services können Sie die Priorität der Pakete verwalten, die in einer heterogenen Umgebung gesendet werden.

„Richtlinien für ankommende Daten” auf Seite 12
Mit den Richtlinien für ankommende Daten werden die Verbindungsanforderungen gesteuert, die in Ihrem Netzwerk eintreffen.

„Differenzierte Services” auf Seite 2
Dies ist der erste Typ einer Richtlinie für die Bandbreite abgehender Daten, den Sie auf dem Betriebssystem erstellen können. Die differenzierten Services unterteilen den Datenaustausch im Netzwerk in unterschiedliche Klassen. Wenn Sie eine Richtlinie für differenzierte Services einsetzen wollen, müssen Sie festlegen, wie der Datenaustausch im Netzwerk klassifiziert werden soll und wie die unterschiedlichen Klassen zu behandeln sind.

Pro-Hop-Verhalten mit Codepunkten zuordnen

QoS verwendet die empfohlenen Codepunkte, um einem Datenaustausch ein Pro-Hop-Verhalten zuzuordnen.

Im Assistenten für Serviceklassen müssen Sie Ihrer Richtlinie ein Pro-Hop-Verhalten zuordnen. Ausgehend von den spezifischen Anforderungen in Ihrem Netzwerk müssen Sie ermitteln, welche Codepunkte zu verwenden sind. Nur Sie selbst können entscheiden, welche Codepunktschemata in Ihrer Umgebung sinnvoll sind. Hierbei müssen Sie berücksichtigen, welche Anwendungen am wichtigsten sind und welchen Richtlinien eine höhere Priorität zugeordnet werden sollte. Am wichtigsten ist hierbei die Konsistenz der Markierungen, damit Sie die erwarteten Ergebnisse erzielen. Richtlinien mit einer ähnlichen Wichtigkeit könnten beispielsweise ähnliche Codepunkte verwenden, damit für diese Richtlinien konsistente Ergebnisse erzielt werden. Wenn Sie nicht genau wissen, welcher Codepunkt zugeordnet werden sollte, müssen Sie unter Umständen etwas experimentieren. Sie können hierzu Testrichtlinien erstellen, diese Richtlinien überwachen und entsprechende Anpassungen vornehmen.

Die Tabellen in den folgenden Abschnitten enthalten die empfohlenen, auf Branchenstandards basierenden Codepunkte. Die meisten Internet-Service-Provider (ISP) unterstützten die standardisierten Codepunkte. Sie können prüfen, ob Ihr ISP diese Codepunkte unterstützt. Wenn die Übertragung über mehrere Domänen hinweg erfolgt, muss jeder ISP der Unterstützung von QoS-Anforderungen zustimmen. Ihre Servicevereinbarungen müssen Ihren Richtlinien die angeforderten Bedingungen zur Verfügung stellen können. Überprüfen Sie, ob Sie den Service im benötigten Umfang erhalten. Falls nicht, werden Ressourcen möglicherweise vergeblich aufgewendet. Bei Verwendung von QoS-Richtlinien können Sie mit Ihrem ISP Servicestufen vereinbaren, die unter Umständen die Kosten für den Netzwerkdienst reduzieren. Sie können auch eigene Codepunkte erstellen. Wird eine externe Verwendung angestrebt, ist dies jedoch nicht zu empfehlen. Ihre eigenen Codepunkte testen Sie am besten in einer Testumgebung.

Beschleunigte Weiterleitung (Expedited Forwarding - EF)

Die beschleunigte Weiterleitung (Expedited forwarding - EF) ist ein bestimmter Typ von Pro-Hop-Verhalten. Er wird hauptsächlich eingesetzt, um einen Service in einem Netzwerk zu garantieren. Die beschleunigte Weiterleitung stellt für den Datenaustausch einen Endpunkt-zu-Endpunkt-Service mit geringen Verlusten und einer geringen Abweichung zur Verfügung, indem die Brandbreite über Netzwerke hinweg garantiert wird. Die Reservierung wird vor dem Senden des Pakets vorgenommen. Hauptziel dieses Typs ist die Vermeidung von Verzögerungen und die rechtzeitige Übermittlung des Pakets.

Tabelle 1. Empfohlene Codepunkte: Beschleunigte Weiterleitung

Beschleunigte Weiterleitung (Expedited Forwarding - EF)
101110

Anmerkung: Eine EF-Verarbeitung ist in der Regel mit hohen Kosten verbunden. Dieses Pro-Hop-Verhalten sollte daher nicht als Standardverfahren verwendet werden.

Klassenselektor

Codepunkte für Klassenselektoren sind ein weiterer Verhaltenstyp. Es gibt insgesamt sieben Klassen. Klasse 0 weist Paketen die niedrigste Priorität zu, Klasse 7 erteilt Paketen die höchste Priorität innerhalb der Codepunktwerte für Klassenselektoren. Diese Gruppe von Pro-Hop-Verhalten wird am häufigsten verwendet, da die meisten Router bereits ähnliche Codepunkte verwenden.

Tabelle 2. Empfohlene Codepunkte: Klassenselektor

Klassenselektor
Klasse 0 - 000000
Klasse 1 - 001000
Klasse 2 - 010000
Klasse 3 - 011000
Klasse 4 - 100000
Klasse 5 - 101000
Klasse 6 - 110000
Klasse 7 - 111000

Garantierte Weiterleitung (Assured Forwarding - AF)

Die garantierte Weiterleitung (Assured Forwarding - AF) wird in vier Klassen von Pro-Hop-Verhalten unterteilt, die jeweils mit einer niedrigen, mittleren oder hohen Löschpriorität versehen sind. Die Stufe der Löschpriorität bestimmt, wie wahrscheinlich es ist, dass die Pakete gelöscht werden. Den Klassen ist jeweils eine eigene Bandbreitenspezifikation zugeordnet. Klasse 1 (Hoch) weist der Richtlinie die niedrigste Priorität zu, Klasse 4 (Niedrig) weist der Richtlinie die höchste Priorität zu. Eine niedrige Löschpriorität bedeutet, dass die Pakete in dieser Richtlinie auf dieser bestimmten Klassenstufe mit der geringsten Wahrscheinlichkeit gelöscht werden.

Tabelle 3. Empfohlene Codepunkte: Garantierte Weiterleitung

Garantierte Weiterleitung (Assured Forwarding - AF)
AF-Klasse 1, Niedrig - 001010
AF-Klasse 1, Mittel - 001100
AF-Klasse 1, Hoch 001110
AF-Klasse 2, Niedrig - 010010
AF-Klasse 2, Mittel - 010100
AF-Klasse 2, Hoch - 010110
AF-Klasse 3, Niedrig - 011010
AF-Klasse 3, Mittel - 011100
AF-Klasse 3, Hoch - 011110
AF-Klasse 4, Niedrig - 100010
AF-Klasse 4, Mittel - 100100
AF-Klasse 4, Hoch - 100110

Zugehörige Konzepte

„Differenzierte Services" auf Seite 2
Dies ist der erste Typ einer Richtlinie für die Bandbreite abgehender Daten, den Sie auf dem Betriebssystem erstellen können. Die differenzierten Services unterteilen den Datenaustausch im Netzwerk in unterschiedliche Klassen. Wenn Sie eine Richtlinie für differenzierte Services einsetzen wollen, müssen Sie festlegen, wie der Datenaustausch im Netzwerk klassifiziert werden soll und wie die unterschiedlichen Klassen zu behandeln sind.

Grenzwerte für Durchschnittsverbindungsgeschwindigkeit und Burstrate

Grenzwerte für die Verbindungsgeschwindigkeit und die Burstrate sind Grenzwerte. Diese Grenzwerte für die Geschwindigkeit ermöglichen die Begrenzung von eingehenden Verbindungen, die auf dem System eintreffen. Grenzwerte für Geschwindigkeiten werden in einer Serviceklasse festgelegt, die zusammen mit Richtlinien für ankommende Daten verwendet wird.

Burstrate der Verbindung

Die Größe der Burstrate bestimmt die Kapazität des Puffers, der Datenüberhänge von Verbindungen aufnimmt. Datenüberhänge von Verbindungen können unter Umständen schneller auf dem System eintreffen, als dieses sie verarbeiten kann oder als es von Ihnen gewünscht wird. Wenn die Anzahl der Verbindungen in einem Überhang den von Ihnen festgelegten Burstgrenzwert für Verbindungen überschreitet, werden die weiteren Verbindungen gelöscht.

Durchschnittsverbindungsgeschwindigkeit

Die Durchschnittsverbindungsgeschwindigkeit gibt den Grenzwert für neu hergestellte Verbindungen oder für die Geschwindigkeit von akzeptierten URI-Anforderungen an, die für ein System zulässig sind. Wenn eine Anforderung dazu führt, dass das System die festgelegten Grenzwerte überschreitet, weist das System die Anforderung zurück. Der Grenzwert für die durchschnittliche Verbindungsanforderung wird in Verbindungen pro Sekunde gemessen.

Tipp: Sie können eine Überwachung ausführen, um die festzulegenden Grenzwerte zu ermitteln. Das Szenario für die Überwachung der aktuellen Netzwerkstatistik enthält eine Beispielrichtlinie, mit deren Hilfe Sie die meisten der über das System ausgetauschten Daten erfassen können. Anhand dieser Ergebnisse können Sie die Grenzwerte entsprechend anpassen.

Wenn Sie anstelle einer bestimmten Datenerfassung eine Echtzeitüberwachung ansehen wollen, öffnen Sie die Überwachung. Die Überwachung stellt eine Echtzeitstatistik für alle aktiven Richtlinien zur Verfügung.

Zugehörige Konzepte

„Richtlinien für ankommende Daten" auf Seite 12
Mit den Richtlinien für ankommende Daten werden die Verbindungsanforderungen gesteuert, die in Ihrem Netzwerk eintreffen.

„Szenario: Aktuelle Netzwerkstatistik überwachen" auf Seite 52
Sie müssen die Leistungsgrenzwerte, die auf einzelnen Netzwerkvoraussetzungen basieren, innerhalb der Assistenten festlegen.

APIs für QoS

Dieses Thema enthält Informationen über Protokolle, APIs und die Voraussetzungen für einen Router, der RSVP (ReSerVation Protocol) verwenden kann, also RSVP-fähig ist. Zu den APIs für QoS gehören die RAPI-API, die qtoq-Socket-API, die API sendmsg() und die monitor-APIs.

Die meisten QoS-Richtlinien erfordern die Verwendung einer API. Die folgenden APIs können zusammen mit Richtlinien für differenzierte Services oder für integrierte Services verwendet werden. Außerdem gibt es eine Reihe von APIs, die bei der QoS-Überwachung verwendet werden können:

- „APIs für integrierte Services " auf Seite 19

- „APIs für differenzierte Services ”
- „APIs für Überwachung ” auf Seite 20

APIs für integrierte Services

RSVP führt, gemeinsam mit den RAPI-APIs oder den qtoc-Socket-APIs für QoS, die Reservierung für die integrierten Services aus. Jeder Knoten, den der Datenaustausch passiert, muss RSVP verwenden können. Die Fähigkeit zur Ausführung von Richtlinien für integrierte Services wird häufig als RSVP-Fähigkeit bezeichnet. Mit den Funktionen zur Datenaustauschsteuerung können Sie ermitteln, welche Routerfunktionen für die Verwendung von RSVP erforderlich sind.

Mit RSVP wird eine RSVP-Reservierung auf allen Netzwerkknoten im Pfad des Datenaustausches erstellt. Diese Reservierung wird lange genug beibehalten, damit die angeforderten Services der Richtlinien bereitgestellt werden. Die Reservierung definiert die Verarbeitung und die Bandbreite, die für die Daten in diesem Dialog erforderlich sind. Die Netzwerkknoten stellen die in der Reservierung definierte Datenverarbeitung bereit.

RSVP ist insofern ein einfaches Protokoll, als Reservierungen nur in einer Richtung (vom Empfänger ausgehend) vorgenommen werden. Bei komplexeren Verbindungen, wie beispielsweise Audio- und Videokonferenzen, ist jeder Absender gleichzeitig auch Empfänger. In einem solchen Fall müssen Sie für jede Seite zwei RSVP-Sitzungen einrichten.

Neben RSVP-fähigen Routern benötigen Sie RSVP-fähige Anwendungen, um integrierte Services verwenden zu können. Da das System anfangs nicht über RSVP-fähige Anwendungen verfügt, müssen Sie die Anwendung mit der RAPI-API oder den qtoq-Socket-APIs für QoS schreiben. Dann können die Anwendungen RSVP verwenden. Wenn Sie eine umfassende Erläuterung wünschen, gibt es viele Informationsquellen, in denen diese Modelle, ihre Funktionsweise und die Nachrichtenbehandlung erklärt werden. Fundierte Kenntnisse über RSVP und den Inhalt des Internet-RFC 2205 sind erforderlich.

qtoq-Socket-APIs

Dank der qtoq-Socket-APIs für QoS können Sie den Aufwand verringern, der mit der Verwendung von RSVP auf dem System verbunden ist. Die qtoq-Socket-APIs rufen die RAPI-APIs auf und führen einige der komplexeren Tasks aus. Die qtoq-Socket-APIs sind nicht so flexibel wie die RAPI-APIs, bieten jedoch bei geringerem Aufwand die gleichen Funktionen. Mit den API-Versionen des Typs ″No Signal″ (= ohne Signal) können Sie die folgenden Anwendungen schreiben:

- Anwendungen, die eine RSVP-Regel auf das System laden
- Anwendungen, bei denen nur die serverseitige Anwendung (des TCP/IP-Dialogs) RSVP-fähig sein muss

Die RSVP-Signalsendung erfolgt für die Clientseite automatisch.

Ein typischer Funktionsablauf der API für QoS bei einer Anwendung oder einem Protokoll, die bzw. das verbindungsorientierte oder verbindungslose qtoc-Sockets für QoS verwendet, ist unter Verbindungsorientierter Funktionsablauf der APIs für QoS bzw. Verbindungsloser Funktionsablauf der APIs für QoS dargestellt.

APIs für differenzierte Services

Anmerkung: Die API sendmsg() wird für bestimmte Richtlinien für differenzierte Services verwendet, die ein spezifisches Anwendungstoken definieren. Beim Erstellen einer Richtlinie für differenzierte Services können Sie (optional) Anwendungskenndaten (Token und Priorität) angeben. Hierbei handelt es sich um eine erweiterte Richtliniendefinition. Wenn sie nicht verwendet wird, kann diese API ignoriert werden. Bedenken Sie jedoch, dass diese Router und andere Systeme im Netzwerk auf jeden Fall DiffServ-fähig sein müssen.

Wenn Sie in einer Richtlinie für differenzierte Services ein Anwendungstoken verwenden wollen, muss die Anwendung, die diese Informationen bereitstellt, speziell für die Verwendung der API sendmsg() codiert sein. Vorgenommen wird dies durch den Anwendungsprogrammierer. Die Dokumentation der Anwendung muss gültige Werte (Token und Priorität) angeben, die vom QoS-Administrator in der Richtlinie für differenzierte Services verwendet werden. Die Richtlinie für differenzierte Services wendet dann ihre eigene Priorität und Klassifizierung auf den Datenaustausch an, der dem in der Richtlinie festgelegten Token entspricht. Falls die Anwendung keine Werte enthält, die den in der Richtlinie festgelegten Werten entsprechen, muss entweder die Anwendung geändert werden oder Sie müssen in der Richtlinie für differenzierte Services andere Parameter für die Anwendungsdaten verwenden.

Die folgenden Informationen liefern eine Kurzbeschreibung der Parameter für das Anwendungstoken und die Anwendungspriorität der Systemdaten.

Anwendungstoken - Beschreibung

Ein *Anwendungstoken* ist ein URI (Uniform-Resource-Identifier), der eine definierte Ressource repräsentiert. Das von Ihnen in der QoS-Richtlinie angegebene Token wird mit dem Token abgeglichen, das durch die Anwendung für abgehende Daten bereitgestellt wird. Die Anwendung stellt den Tokenwert über die API sendmsg() zur Verfügung. Wenn die Token übereinstimmen, wird der Datenaustausch der Anwendung in die Richtlinie für differenzierte Services aufgenommen.

Anwendungspriorität - Beschreibung

Die von Ihnen angegebene Anwendungspriorität wird mit der Anwendungspriorität abgeglichen, die durch die Anwendung für abgehende Daten bereitgestellt wird. Die Anwendung stellt den Prioritätswert mittels der API sendmsg() zur Verfügung. Wenn die Prioritäten übereinstimmen, wird der Datenaustausch der Anwendung in die Richtlinie für differenzierte Services aufgenommen. Der gesamte Datenaustausch, der in der Richtlinie für differenzierte Services definiert ist, erhält weiterhin die Priorität, die der gesamten Richtlinie zugewiesen ist.

Weitere Informationen zum Richtlinientyp für differenzierte Services finden Sie unter „Differenzierte Services” auf Seite 2.

APIs für Überwachung

Die APIs für die Überwachung gehören zu den RSVP-APIs. Die APIs, die für die Überwachung verwendet werden können, enthalten in ihrem Namen die Angabe "monitor". (Beispiel: *QgyOpenListQoSMonitorData*). Die folgende Liste enthält eine kurze Beschreibung der einzelnen APIs für die Überwachung:

- Die API QgyOpenListQoSMonitorData (Liste der QoS-Überwachungsdaten öffnen) erfasst Informationen, die mit QoS-Services zusammenhängen.
- Die API QtoqDeleteQoSMonitorData (QoS-Überwachungsdaten löschen) löscht eine oder mehrere Gruppen von erfassten QoS-Überwachungsdaten.
- Die API QtoqEndQoSMonitor (QoS-Überwachung beenden) stoppt die Erfassung von Informationen für QoS-Services.
- Die API QtoqListSavedQoSMonitorData (Gespeicherte QoS-Überwachungsdaten auflisten) gibt eine Liste mit allen erfassten Überwachungsdaten zurück, die zuvor gespeichert wurden.
- Die API QtoqSaveQoSMonitorData (QoS-Überwachungsdaten speichern) speichert eine Kopie der erfassten QoS-Überwachungsdaten für eine spätere Verwendung.
- Die API QtoqStartQoSMonitor (QoS-Überwachung starten) erfasst Informationen für QoS-Services.

Zugehörige Konzepte

„Integrierte Services” auf Seite 7
Der zweite Typ einer Richtlinie für die Bandbreite abgehender Daten, den Sie erstellen können, ist

eine Richtlinie für integrierte Services. Die integrierten Services bieten IP-Anwendungen die Möglichkeit, unter Verwendung des RSVP-Protokolls (ReSerVation Protocol) und der APIs für QoS Bandbreite anzufordern und zu reservieren.

„Funktionen zur Datenaustauschsteuerung" auf Seite 9
Die Funktionen zur Datenaustauschsteuerung können nur auf integrierte Services angewendet werden und sind nicht System i-spezifisch.

„Szenario: Vorhersehbarer B2B-Datenaustausch" auf Seite 44
Wenn Sie eine vorhersehbare Übermittlung benötigen und dennoch eine Reservierung anfordern müssen, können Sie natürlich auch eine Richtlinie für integrierte Services verwenden. Dieses Beispiel verwendet einen Service des Typs ″Gesteuertes Laden″.

„Netzwerkhardware und -software" auf Seite 57
Das Leistungsspektrum Ihrer internen Ausstattung und der Einheiten außerhalb des Netzwerks hat beträchtliche Auswirkungen auf die QoS-Ergebnisse.

Zugehörige Verweise

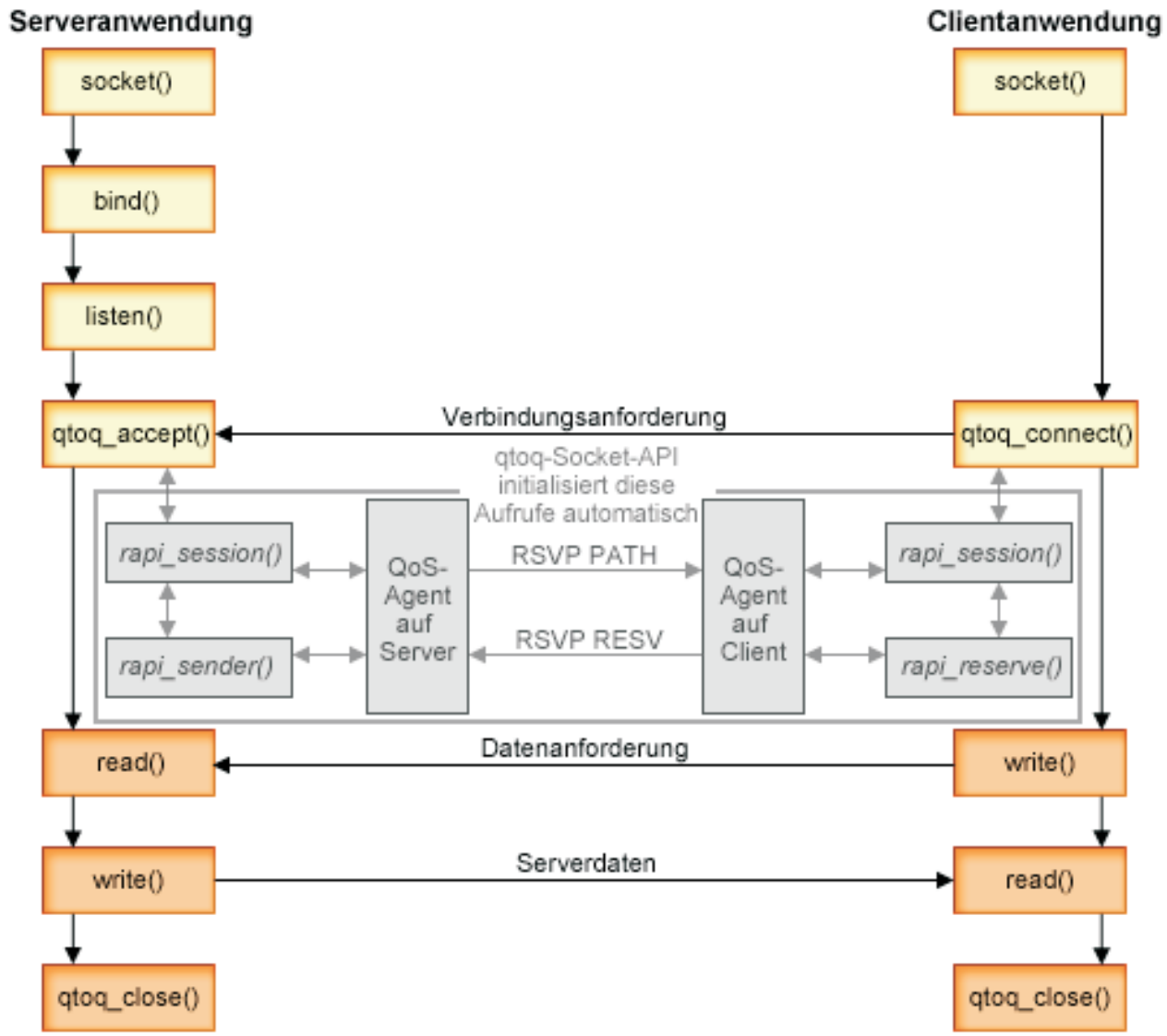
Resource Reservation Setup Protocol APIs

„QoS mit Assistenten konfigurieren" auf Seite 58
Zur Konfiguration von QoS-Richtlinien müssen Sie die QoS-Assistenten in System i Navigator verwenden.

Verbindungsorientierter Funktionsablauf der APIs für QoS

Die Server- und Clientbeispiele veranschaulichen die qtoc-Socket-APIs für QoS, die für einen verbindungsorientierten Funktionsablauf geschrieben sind.

Wenn die Funktionen der QoS-fähigen API für einen verbindungsorientierten Funktionsablauf aufgerufen werden, der eine Initialisierung von RSVP erforderlich macht, werden zusätzliche Funktionen initialisiert. Diese Funktionen bewirken, dass die QoS-Agenten auf dem Client und dem Server RSVP für den Datenfluss zwischen dem Client und dem Server einrichten.



qtoq-Ereignisablauf: Die nachstehende Folge von Socketaufrufen beschreibt die Abbildung. Außerdem wird die Beziehung zwischen der Server- und der Clientanwendung in einem verbindungsorientierten Konzept erläutert. Es handelt sich hierbei um Bearbeitungen der Socket-Basis-APIs.

Serverseite

API qtoq_accept() für eine mit ″no signaling″ (= ohne Signalsendung) markierte Regel

1. Die Anwendung ruft die Funktion socket() auf, um einen Socketdeskriptor abzurufen.
2. Die Anwendung ruft listen() auf, um die Verbindungen anzugeben, auf die gewartet wird.
3. Die Anwendung ruft qtoq_accept() auf, um auf eine Verbindungsanforderung des Clients zu warten.
4. Die API ruft die API rapi_session() auf. Bei erfolgreicher Ausführung wird eine QoS-Sitzungs-ID zugeordnet.
5. Die API ruft die Standardfunktion accept() auf, um auf die Verbindungsanforderung eines Clients zu warten.
6. Sobald die Verbindungsanforderung empfangen wurde, wird die Zugangssteuerung für die angeforderte Regel ausgeführt. Die Regel wird an den TCP/IP-Stack gesendet. Sofern sie gültig ist, wird die Regel mit den Ergebnissen und der Sitzungs-ID an die aufrufende Anwendung zurückgegeben.

7. Die Anwendungen für den Server und den Client führen die angeforderten Datenübertragungen aus.
8. Die Anwendung ruft die Funktion qtoq_close() auf, um den Socket zu schließen und die Regel zu entladen.
9. Der QoS-Server löscht die Regel aus dem QoS-Manager, löscht die QoS-Sitzung und führt ggfs. noch erforderliche Aktionen aus.

API qtoq_accept() mit normaler RSVP-Signalsendung

1. Die Anwendung ruft die Funktion socket() auf, um einen Socketdeskriptor abzurufen.
2. Die Anwendung ruft listen() auf, um die Verbindungen anzugeben, auf die gewartet wird.
3. Die Anwendung ruft qtoq_accept() auf, um auf eine Verbindungsanforderung des Clients zu warten.
4. Sobald eine Verbindungsanforderung eintrifft, wird die API rapi_session() aufgerufen, um für diese Verbindung eine Sitzung mit dem QoS-Server zu erstellen und die QoS-Sitzungs-ID abzurufen, die an die aufrufende Anwendung zurückgegeben wird.
5. Die API rapi_sender() wird aufgerufen, um eine Nachricht PATH vom QoS-Server zu initialisieren und den QoS-Server zu informieren, dass eine Nachricht RESV vom Client erwartet werden muss.
6. Die API rapi_getfd() wird aufgerufen, um den Deskriptor abzurufen, mit dem die Anwendungen auf QoS-Ereignisnachrichten warten.
7. Der Deskriptor für das Akzeptieren und der QoS-Deskriptor werden an die Anwendung zurückgegeben.
8. Der QoS-Server wartet auf den Empfang der Nachricht RESV. Sobald die Nachricht empfangen wurde, lädt der Server die entsprechende Regel mit dem QoS-Manager und sendet eine Nachricht an die Anwendung, wenn die Anwendung im Aufruf der API qtoq_accept() eine Benachrichtigung angefordert hatte.
9. Der QoS-Server wird weiterhin ausgeführt, um Aktualisierungen für die aufgebaute Sitzung bereitzustellen.
10. Die Anwendung ruft qtoq_close() auf, wenn die Verbindung beendet wird.
11. Der QoS-Server löscht die Regel aus dem QoS-Manager, löscht die QoS-Sitzung und führt ggfs. noch erforderliche Aktionen aus.

Clientseite

API qtoq_connect() mit normaler RSVP-Signalsendung

1. Die Anwendung ruft die Funktion socket() auf, um einen Socketdeskriptor abzurufen.
2. Die Anwendung ruft die Funktion qtoq_connect() auf, um die Serveranwendung darüber zu informieren, dass eine Verbindung hergestellt werden soll.
3. Die Funktion qtoq_connect() ruft die API rapi_session() auf, um für diese Verbindung eine Sitzung mit dem QoS-Server zu erstellen.
4. Der QoS-Server wird darauf vorbereitet, den Befehl PATH von der anfordernden Verbindung zu erwarten.
5. Die API rapi_getfd() wird aufgerufen, um den QoS-Deskriptor abzurufen, mit dem die Anwendungen auf QoS-Nachrichten warten.
6. Die Funktion connect() wird aufgerufen. Die Ergebnisse der Funktion connect() und des QoS-Deskriptors werden an die Anwendung zurückgegeben.
7. Der QoS-Server wartet auf den Empfang der Nachricht PATH. Sobald die Nachricht empfangen wurde, antwortet der Server mit einer Nachricht RESV an den QoS-Server auf der Servermaschine der Anwendung.
8. Falls die Anwendung eine Benachrichtigung angefordert hatte, sendet der QoS-Server die Benachrichtigung über den QoS-Deskriptor an die Anwendung.
9. Der QoS-Server wird weiterhin ausgeführt, um Aktualisierungen für die aufgebaute Sitzung bereitzustellen.

10. Die Anwendung ruft qtoq_close() auf, wenn die Verbindung beendet wird.
11. Der QoS-Server schließt die QoS-Sitzung und führt alle ggfs. noch erforderlichen Aktionen aus.

API qtoq_connect() für eine mit ″no signaling″ (= ohne Signalsendung) markierte Regel

Diese Anforderung ist auf der Clientseite ungültig, da vom Client in diesem Fall keine Antwort benötigt wird.

Zugehörige Verweise

qtoq_accept()--Accept QoS Sockets Connection API

qtoq_close()--Close QoS Sockets Connection API

rapi_session()--Create a RAPI session

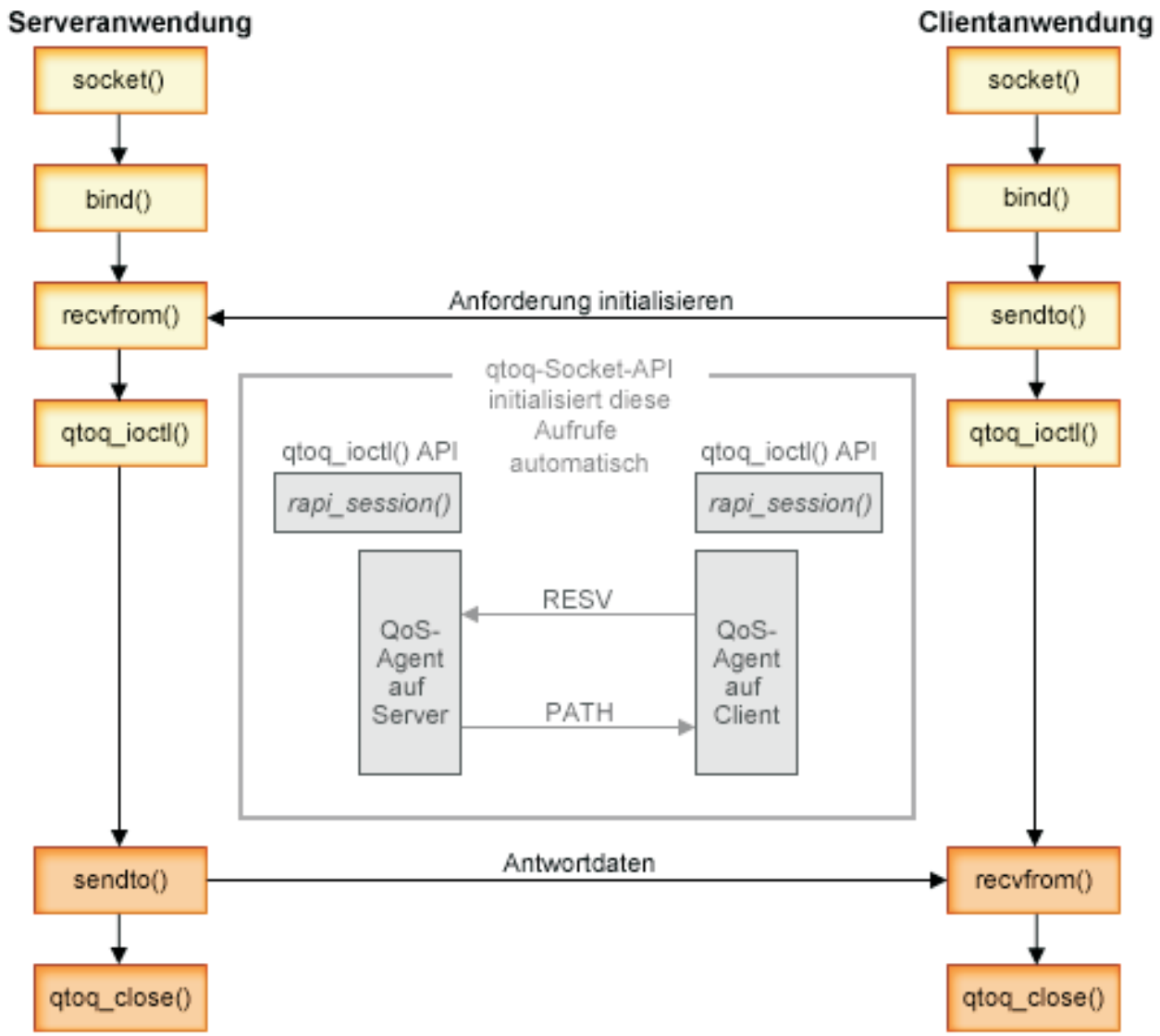
rapi_sender()--Identify a RAPI sender

rapi_getfd()--Get descriptor to wait on

qtoq_connect()--Make QoS Sockets Connection API

Verbindungsloser Funktionsablauf der APIs für QoS

Wenn die Funktionen der QoS-fähigen API für einen verbindungslosen Funktionsablauf aufgerufen werden, der eine Initialisierung von RSVP erforderlich macht, werden zusätzliche Funktionen initialisiert. Diese Funktionen bewirken, dass die QoS-Agenten auf dem Client und dem Server RSVP für den Datenfluss zwischen dem Client und dem Server einrichten.



qtoq-Ereignisablauf: Die nachstehende Folge von Socketaufrufen beschreibt die Abbildung. Außerdem wird die Beziehung zwischen der Server- und der Clientanwendung in einem verbindungslosen Konzept erläutert. Es handelt sich hierbei um Bearbeitungen der Socket-Basis-APIs.

Serverseite

API qtoq_ioctl() für eine mit ″no signaling″ (= ohne Signalsendung) markierte Regel

1. Die API qtoq_ioctl() sendet eine Nachricht an den QoS-Server, in der die Ausführung der Zugangssteuerung für die angeforderte Regel angefordert wird.
2. Wenn die Regel akzeptiert werden kann, wird eine Funktion aufgerufen, die eine Nachricht an den QoS-Server sendet, in der das Laden der Regel angefordert wird.
3. Der QoS-Server gibt den Status an die aufrufende Anwendung zurück, um die erfolgreiche Ausführung oder das Fehlschlagen der Anforderung anzugeben.
4. Sobald die Anwendung die Verwendung der Verbindung beendet hat, ruft sie die Funktion qtoq_close() auf, um die Verbindung zu schließen.

5. Der QoS-Server löscht die Regel aus dem QoS-Manager, löscht die QoS-Sitzung und führt ggfs. noch erforderliche Aktionen aus.

API qtoq_ioctl() mit normaler RSVP-Signalsendung

1. Die API qtoq_ioctl() sendet eine Nachricht an den QoS-Server, in der die Zugangssteuerung für die angeforderte Verbindung angefordert wird.
2. Der QoS-Server ruft die API rapi_session() auf, um das Einrichten einer Sitzung für die Regel anzufordern und die QoS-Sitzungs-ID abzurufen, die an die aufrufende Anwendung zurückgegeben wird.
3. Die API rapi_sender() wird aufgerufen, um eine Antwortnachricht PATH an den Client zu initialisieren.
4. Anschließend wird die API rapi_getfd() aufgerufen, um einen Dateideskriptor abzurufen und auf QoS-Ereignisse zu warten.
5. Der QoS-Server gibt den Deskriptor select(), die QoS-Sitzungs-ID und den Status an die aufrufende Anwendung zurück.
6. Der QoS-Server lädt die Regel, sobald die Nachricht RESV empfangen wurde.
7. Die Anwendung gibt qtoq_close() aus, wenn die Verbindung beendet wird.
8. Der QoS-Server löscht die Regel aus dem QoS-Manager, löscht die QoS-Sitzung und führt ggfs. noch erforderliche Aktionen aus.

Clientseite

API qtoq_ioctl() mit normaler RSVP-Signalsendung

1. Die API qtoq_ioctl() ruft rapi_session() auf, um das Einrichten einer Sitzung für die Verbindung anzufordern. Die Funktion rapi_session() fordert die Zugangssteuerung für die Verbindung an. Die Verbindung wird auf der Clientseite nur dann zurückgewiesen, wenn es eine konfigurierte Regel für den Client gibt, die zu diesem Zeitpunkt nicht aktiv ist. Diese Funktion gibt die QoS-Sitzungs-ID zurück, die wieder an die Anwendung übergeben wird.
2. Die API rapi_getfd() wird aufgerufen, um einen Dateideskriptor abzurufen und auf QoS-Ereignisse zu warten.
3. qtoq_ioctl() wird mit der Sitzungs-ID an die aufrufende Anwendung zurückgegeben und gibt an, dass auf den Deskriptor gewartet wird.
4. Der QoS-Server wartet auf den Empfang der Nachricht PATH. Sobald die Nachricht PATH empfangen wurde, antwortet der Server mit der Nachricht RESV und teilt anschließend der Anwendung über den Sitzungsdeskriptor mit, dass das Ereignis eingetreten ist.
5. Der QoS-Server wird weiterhin ausgeführt, um Aktualisierungen für die aufgebaute Sitzung bereitzustellen.
6. Der Client-Code ruft qtoq_close() auf, wenn die Verbindung beendet wird.

API qtoq_ioctl() für eine mit ″no signaling″ (= ohne Signalsendung) markierte Regel

Diese Anforderung ist auf der Clientseite ungültig, da vom Client in diesem Fall keine Antwort benötigt wird.

Zugehörige Verweise

qtoq_close()--Close QoS Sockets Connection API

rapi_session()--Create a RAPI session

rapi_sender()--Identify a RAPI sender

rapi_getfd()--Get descriptor to wait on

qtoq_ioctl()--Set QoS Sockets Control Options API

QoS-Erweiterungen der API sendmsg()

Die Funktion sendmsg() wird zum Senden von Daten und/oder von Hilfsdaten über einen verbundenen oder nicht verbundenen Socket verwendet.

Die API sendmsg() lässt QoS-Klassifizierungsdaten zu. QoS-Richtlinien verwenden diese Funktion, um eine differenziertere Klassifizierungsstufe für abgehenden oder ankommenden TCP/IP-Datenaustausch zu definieren. Sie verwenden insbesondere Hilfsdatentypen, die auf die IP-Schicht angewendet werden. Der verwendete Nachrichtentyp ist `IP_QOS_CLASSIFICATION_DATA`. Diese Hilfsdaten können durch die Anwendung verwendet werden, um Attribute für den Datenaustausch in einer bestimmten TCP-Verbindung zu definieren. Falls die von der Anwendung übergebenen Attribute mit den in der QoS-Richtlinie definierten Attributen übereinstimmen, wird der TCP-Datenaustausch durch die Richtlinie eingeschränkt.

Mit den folgenden Informationen können Sie die Struktur `IP_QOS_CLASSIFICATION_DATA` initialisieren:

- `ip_qos_version`: Gibt die Version der Struktur an. Dies muss unter Verwendung der Konstanten *IP_QOS_CURRENT_VERSION* ausgefüllt werden.
- `ip_qos_classification_scope`: Gibt einen Bereich für die Verbindungsebene (mit der Konstante *IP_QOS_CONNECTION_LEVEL*) oder einen Bereich für die Nachrichtenebene (mit der Konstante *IP_QOS_MESSAGE_LEVEL*) an.

  Der Bereich für die Verbindungsebene gibt an, dass die über die Klassifizierung dieser Nachricht erhaltene QoS-Servicestufe für alle anschließend gesendeten Nachrichten bis zum nächsten Aufruf von sendmsg() mit QoS-Klassifizierungsdaten wirksam ist. Der Bereich für die Nachrichtenebene gibt an, dass die zugeordnete QoS-Servicestufe nur für die Nachrichtendaten verwendet wird, die in diesem Aufruf von sendmsg() enthalten sind. Daten, die anschließend ohne QoS-Klassifizierungsdaten gesendet werden, übernehmen die QoS-Zuordnung der vorherigen Verbindungsebene (also aus der letzten Klassifizierung der Verbindungsebene über die API sendmsg()) oder aus der ursprünglichen Klassifizierung der TCP-Verbindung während des Verbindungsaufbaus).
- `ip_qos_classification_type`: Diese Spezifikation gibt den Typ der übergebenen Klassifizierungsdaten an. Eine Anwendung kann auswählen, ob ein anwendungsdefiniertes Token, eine anwendungsdefinierte Priorität oder ein Token und eine Priorität übergeben wird. Bei Auswahl der letzteren Möglichkeit müssen die beiden ausgewählten Klassifizierungstypen durch ein logisches OR verbunden werden. Die folgenden Typen können angegeben werden:
  - Anwendungsdefinierte Tokenklassifikation: Es muss ein einzelner Typ angegeben werden. Bei Angabe mehrerer Typen können die Ergebnisse nicht vorhergesehen werden.
    - `IP_SET_QOSLEVEL_W_APPL_TOKEN_ASCII`: Gibt an, dass die Klassifizierungsdaten eine Zeichenfolge im ASCII-Format sind. Bei Angabe dieser Option muss das Anwendungstoken im Feld ip_qos_appl_token übergeben werden.

      Anmerkung: Falls die Anwendung numerische Werte für die Klassifizierungsdaten übergeben muss, müssen diese Werte zuvor in ein druckbares ASCII-Format konvertiert werden. Die angegebene Zeichenfolge kann Groß-/Kleinschreibung enthalten und wird bei Vergleichen exakt im angegebenen Format verwendet.
    - `IP_SET_QOSLEVEL_W_APPL_TOKEN_EBCDIC`: Für diese Spezifikation gelten dieselben Bedingungen wie für die vorausgehende Spezifikation, mit der Ausnahme, dass die Zeichenfolge im EBCDIC-Format steht.

      Anmerkung: Das Leistungsverhalten ist bei `IP_SET_QOSLEVEL_W_APPL_TOKEN_ASCII` etwas besser als bei dieser Option, da die in der Richtlinie angegebenen Anwendungsdaten innerhalb des TCP/IP-Stacks im ASCII-Format gespeichert werden und somit eine Umsetzung des anwendungsdefinierten Tokens in jeder Anforderung sendmsg() überflüssig ist.
  - Anwendungsdefinierte Prioritätsklassifikation: Es muss ein einzelner Typ angegeben werden. Bei Angabe mehrerer Prioritätstypen können die Ergebnisse nicht vorhergesehen werden.
    - `IP_SET_QOSLEVEL_EXPIDITED`: Gibt an, dass eine beschleunigte Priorität angefordert wird.

- IP_SET_QOSLEVEL_HIGH: Gibt an, dass eine hohe Priorität angefordert wird.
- IP_SET_QOSLEVEL_MEDIUM: Gibt an, dass eine mittlere Priorität angefordert wird.
- IP_SET_QOSLEVEL_LOW: Gibt an, dass eine niedrige Priorität angefordert wird.
- IP_SET_QOSLEVEL_BEST_EFFORT: Gibt an, dass eine Priorität des Typs "Bester Versuch" angefordert wird.

– ip_qos_appl_token_len: Die Länge des angegebenen Feldes ip_qos_appl_token.

– ip_qos_appl_token: Dieses virtuelle Feld folgt unmittelbar auf das Feld ip_qos_classification_type. Es enthält die Zeichenfolge für das Klassifizierungstoken der Anwendung entweder im ASCII- oder im EBCDIC-Format (abhängig davon, welcher Wert von IP_SET_QOSLEVEL_W_APPL_TOKEN_xxxx für den Klassifizierungstyp angegeben ist). Auf dieses Feld wird nur dann verwiesen, wenn ein anwendungsdefinierter Tokentyp angegeben wird. Bitte beachten Sie, dass diese Zeichenfolge nicht länger als 128 Byte sein darf. Wenn eine größere Länge angegeben wird, werden nur die ersten 128 Byte verwendet. Außerdem ist zu beachten, dass die Länge der Zeichenfolge anhand des Wertes ermittelt wird, der für cmsg_len (cmsg_len - sizeof(cmsghdr) - sizeof(ip_qos_classification_data)) angegeben wurde. Diese berechnete Länge darf keine Nullabschlusszeichen enthalten.

Zugehörige Konzepte

„Differenzierte Services" auf Seite 2
Dies ist der erste Typ einer Richtlinie für die Bandbreite abgehender Daten, den Sie auf dem Betriebssystem erstellen können. Die differenzierten Services unterteilen den Datenaustausch im Netzwerk in unterschiedliche Klassen. Wenn Sie eine Richtlinie für differenzierte Services einsetzen wollen, müssen Sie festlegen, wie der Datenaustausch im Netzwerk klassifiziert werden soll und wie die unterschiedlichen Klassen zu behandeln sind.

„Klassen mit Priorität: Vorgehensweise zur Klassifizierung von Datenaustausch im Netzwerk" auf Seite 3
Die differenzierten Services unterteilen den Datenaustausch in unterschiedliche Klassen. Die gängigsten Klassen werden unter Verwendung von Client-IP-Adressen, Anwendungsports, Servertypen, Protokollen, lokalen IP-Adressen und Zeitplänen definiert. Der gesamte Datenaustausch, der derselben Klasse entspricht, wird gleich behandelt.

Zugehörige Verweise

API Sendmsg() - Nachricht über Socket senden

Directory-Server

Sie können Ihre Richtlinien auf einen Directory-Server exportieren. Dieses Thema beschreibt die Konzepte und die Konfiguration von LDAP (Lightweight Directory Access Protocol) sowie das QoS-Schema.

Die QoS-Richtlinienkonfiguration kann unter Verwendung von LDAP Version 3 auf einen Directory-Server exportiert werden.

Verwendung eines Directory-Servers

Wenn Sie QoS-Richtlinien auf einen Directory-Server exportieren, ist die Verwaltung der Richtlinien einfacher. Es gibt drei Möglichkeiten für die Verwendung eines Directory-Servers:

- Die Konfigurationsdaten können auf einem lokalen Directory-Server gespeichert und von vielen Systemen gemeinsam benutzt werden.
- Die Konfigurationsdaten können auf nur einem System konfiguriert, gespeichert und verwendet (also nicht gemeinsam benutzt) werden.
- Die Konfigurationsdaten können sich auf einem Directory-Server befinden, der Daten für andere Systeme speichert, jedoch nicht von diesen anderen Systemen gemeinsam benutzt wird. Hierdurch können Sie eine einzige Position zum Sichern und Speichern von Daten für mehrere Systeme verwenden.

Vorteile der ausschließlichen Speicherung auf dem lokalen System

Die Speicherung von QoS-Richtlinien auf einem lokalen System ist weniger komplex. Die lokale Verwendung von Richtlinien bietet eine Reihe von Vorteilen:

- Die Komplexität der LDAP-Konfiguration wird für Benutzer, die sie nicht benötigen, aufgehoben.
- Die Leistung wird verbessert, da das Schreiben auf LDAP keine besonders schnelle Methode ist.
- Das Duplizieren einer Konfiguration zwischen verschiedenen Systemen ist einfacher. Sie können die Datei von einem System auf ein anderes System kopieren. Da es kein primäres oder sekundäres System gibt, können Sie alle Richtlinien direkt auf den einzelnen Systemen anpassen.

LDAP-Ressourcen

Wenn Sie beschließen, Ihre Richtlinien auf einen LDAP-Server zu exportieren, müssen Sie zuvor die Konzepte und Verzeichnisstrukturen von LDAP kennen. In der QoS-Funktion von System i Navigator können Sie einen Directory-Server konfigurieren, der zusammen mit der QoS-Richtlinie verwendet wird.

Zugehörige Konzepte

IBM Tivoli Directory Server for i5/OS (LDAP)

„Directory-Server konfigurieren" auf Seite 60
QoS-Richtlinienkonfigurationen können auf einen LDAP-Directory-Server (LDAP - Lightweight Directory Access Protocol) exportiert werden, was eine einfachere Verwaltung Ihrer QoS-Lösung zur Folge hat.

Schlüsselwörter

Wenn Sie Ihren Directory-Server konfigurieren, müssen Sie festlegen, ob jeder QoS-Konfiguration Schlüsselwörter zugeordnet werden sollen.

Die Schlüsselwortfelder sind optional und können ignoriert werden.

Im Assistenten für die QoS-Erstkonfiguration können Sie einen Directory-Server konfigurieren. Sie können angeben, ob der konfigurierte Server ein primäres System oder ein sekundäres System ist. Der Server, auf dem Sie alle Ihre QoS-Richtlinien verwalten, wird als primäres System bezeichnet.

Mit Schlüsselwörtern werden die Konfigurationen gekennzeichnet, die durch primäre Systeme erstellt wurden. Obwohl sie auf dem primären System erstellt werden, dienen Schlüsselwörter eigentlich dem sekundären System. Mit ihrer Hilfe können sekundäre Systeme die Konfigurationen laden und verwenden, die durch ein primäres System erstellt wurden. Die folgenden Beschreibungen erläutern, wie Schlüsselwörter auf dem jeweiligen System eingesetzt werden.

Schlüsselwörter und primäre Systeme
: Die Schlüsselwörter werden QoS-Konfigurationen zugeordnet, die durch ein primäres System erstellt und verwaltet werden. Anhand der Schlüsselwörter können sekundäre Systeme erkennen, dass eine Konfiguration durch ein primäres System erstellt wurde.

Schlüsselwörter und sekundäre Systeme
: Sekundäre Systeme verwenden Schlüsselwörter, um nach Konfigurationen suchen zu können. Das sekundäre System lädt und verwendet Konfigurationen, die durch ein primäres System erstellt wurden. Wenn Sie ein sekundäres System konfigurieren, können Sie spezifische Schlüsselwörter auswählen. Abhängig vom ausgewähltem Schlüsselwort lädt das sekundäre System alle Konfigurationen, die dem ausgewählten Schlüsselwort zugeordnet sind. Auf diese Weise kann das sekundäre System mehrere Konfigurationen laden, die von unterschiedlichen primären Systemen erstellt wurden.

Wenn Sie mit der Konfiguration des Directory-Servers in System i Navigator beginnen, finden Sie in der QoS-Taskhilfe spezifische Anweisungen.

Zugehörige Konzepte

„Registrierter Name"
Wenn Sie einen Teil Ihres Verzeichnisses verwalten wollen, verwenden Sie hierzu entweder einen registrierten Namen oder (bei Auswahl) ein Schlüsselwort.

„Directory-Server konfigurieren" auf Seite 60
QoS-Richtlinienkonfigurationen können auf einen LDAP-Directory-Server (LDAP - Lightweight Directory Access Protocol) exportiert werden, was eine einfachere Verwaltung Ihrer QoS-Lösung zur Folge hat.

Registrierter Name

Wenn Sie einen Teil Ihres Verzeichnisses verwalten wollen, verwenden Sie hierzu entweder einen registrierten Namen oder (bei Auswahl) ein Schlüsselwort.

Den registrierten Namen geben Sie an, wenn Sie den Directory-Server im Assistenten für die QoS-Erstkonfiguration konfigurieren. Registrierte Namen bestehen in der Regel aus dem Namen für den Eintrag selbst sowie aus den Objekten, die im Verzeichnis über dem Eintrag angeordnet sind (die Objekte werden von oben nach unten angegeben). Der Server kann auf alle Objekte im Verzeichnis zugreifen, die unterhalb des registrierten Namens stehen. Angenommen, der LDAP-Server enthält beispielsweise die in der folgenden Abbildung dargestellte Verzeichnisstruktur:

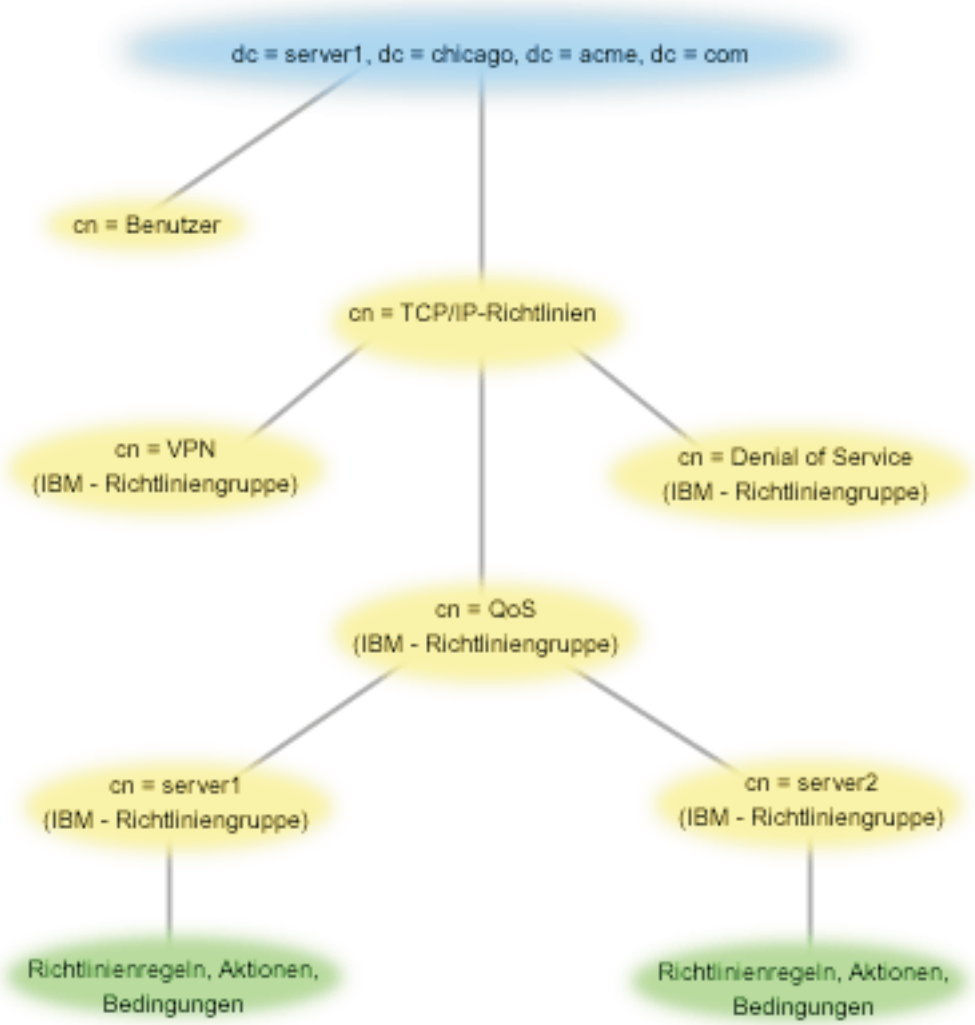


Abbildung 3. Beispiel für QoS-Verzeichnisstruktur

Der übergeordnete Server1 (dc=server1,dc=chicago,dc=acme,dc=com) ist der Server, auf dem sich der Directory-Server befindet. Auf den anderen Servern (z. B. cn=QoS oder cn=TCPIP-Richtlinien) befinden sich die QoS-Server. Auf cn=server1 lautet der Standardwerte für den registrierten Namen demzufolge `cn=server1,cn=QoS,cn=TCPIP-Richtlinien,dc=server1,dc=chicago,dc=acme,dc=com.` Auf cn=server2 lautet der Standardwert für den registrierten Namen `cn=server2,cn=QoS,cn=TCPIP-Richtlinien,dc=server1,dc=chicago,dc=acme,dc=com.`

Bei der Verwaltung Ihres Verzeichnisses ist es wichtig, dass der richtige Server im registrierten Namen geändert wird, beispielsweise cn oder dc. Bei der Bearbeitung des registrierten Namens ist Vorsicht geboten, insbesondere deshalb, weil die Zeichenfolge normalerweise so lang ist, dass sie nicht ohne Blättern angezeigt werden kann.

Zugehörige Konzepte

„Schlüsselwörter" auf Seite 29
Wenn Sie Ihren Directory-Server konfigurieren, müssen Sie festlegen, ob jeder QoS-Konfiguration Schlüsselwörter zugeordnet werden sollen.

„Directory-Server konfigurieren” auf Seite 60
QoS-Richtlinienkonfigurationen können auf einen LDAP-Directory-Server (LDAP - Lightweight Directory Access Protocol) exportiert werden, was eine einfachere Verwaltung Ihrer QoS-Lösung zur Folge hat.

Zugehörige Verweise

„Referenzinformationen zu QoS” auf Seite 75
RFCs (Request for Comments) für QoS, IBM Redbooks und andere Themensammlungen im Information Center enthalten Informationen, die sich auf die QoS-Themensammlung beziehen. Sie können alle PDF-Dateien anzeigen oder drucken.

Szenarien: QoS-Richtlinien

Die Szenarien für QoS-Richtlinien in diesem Abschnitt veranschaulichen, aus welchem Grund Sie QoS benötigen und auf welche Weise Sie Richtlinien und Serviceklassen erstellen.

Eine der besten Möglichkeiten für die Erläuterung von QoS ist die Betrachtung seiner Funktionsweise im Gesamtentwurf des Netzwerks. Die folgenden Basisbeispiele veranschaulichen den Grund für die Verwendung von QoS-Richtlinien und bieten außerdem einige schrittweise Anweisungen für die Erstellung der Richtlinien und Serviceklassen.

Anmerkung: Die IP-Adressen und Abbildungen sind fiktiv und werden nur zur Veranschaulichung verwendet.

Zugehörige Konzepte

„Systemtransaktionen überwachen” auf Seite 71
Mit der QoS-Überwachung können Sie überprüfen, ob die QoS-Richtlinien die gewünschte Wirkung haben. Die QoS-Überwachung hilft Ihnen in der Planungsphase und bei der Fehlerbehebung für QoS.

Zugehörige Verweise

„QoS überwachen” auf Seite 63
Mit der QoS-Überwachung können Sie den IP-Datenaustausch auf dem System analysieren.

Szenario: Browserdatenaustausch begrenzen

Mit QoS können Sie das Leistungsverhalten für den Datenaustausch steuern. Durch den Einsatz einer Richtlinie für differenzierte Services können Sie die Leistung einer Anwendung in Ihrem Netzwerk entweder einschränken oder erweitern.

Situation

Sie haben festgestellt, dass in Ihrem Unternehmen an Freitagen ein hohes Aufkommen von Browserdatenaustausch in der Gruppe für das benutzerorientierte Design (BOD) herrscht. Dieser Datenaustausch überschneidet sich mit dem der Buchhaltungsabteilung, die für ihre Buchhaltungsanwendungen an Freitagen ebenfalls ein gutes Leistungsverhalten benötigt. Daher beschließen Sie, den Browserdatenaustausch der Gruppe BOD einzuschränken. Die folgende Abbildung veranschaulicht den Netzwerkplan in diesem Szenario.

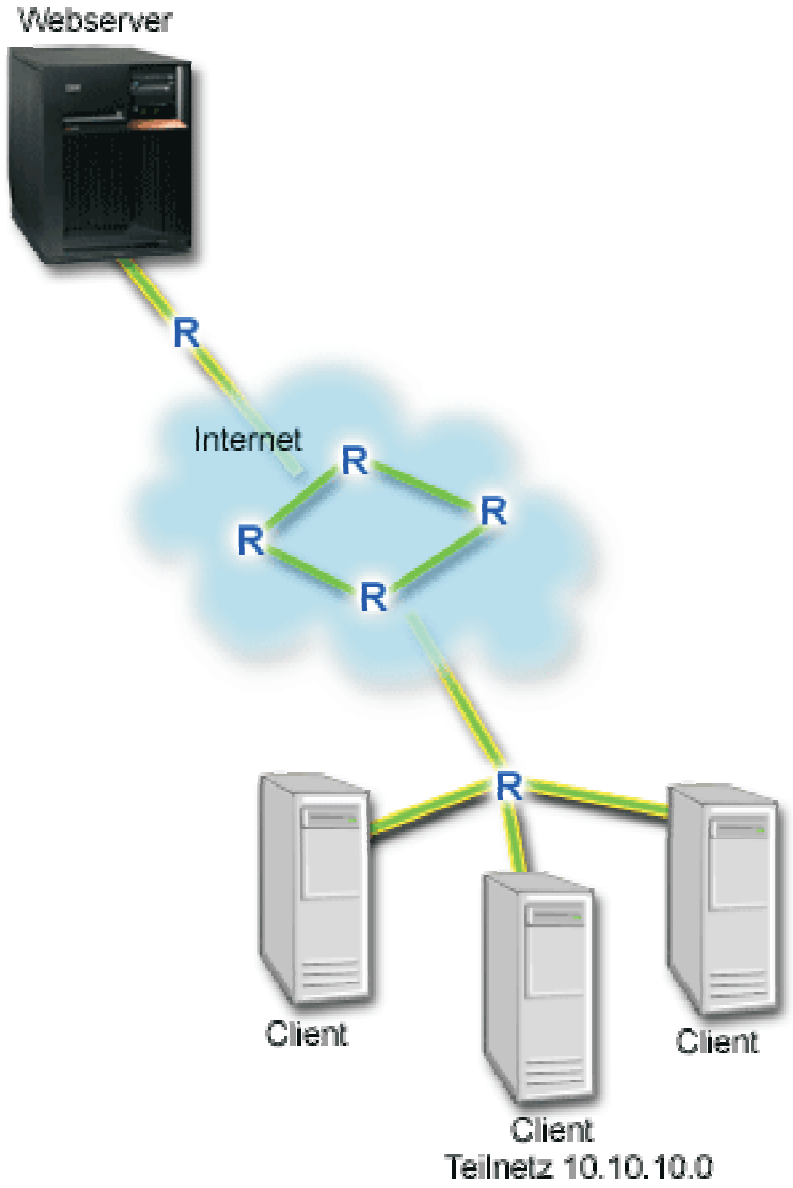


Abbildung 4. Begrenzung des Browserdatenaustausches an einen Client über den Webserver

Zielsetzungen

Um den Browserdatenaustausch zu begrenzen, der Ihr Netzwerk verlässt, können Sie eine Richtlinie für differenzierte Services erstellen. Eine Richtlinie für differenzierte Services unterteilt den Datenaustausch im Netzwerk in unterschiedliche Klassen. Dem gesamten Datenaustausch in dieser Richtlinie wird ein Codepunkt zugeordnet. Dieser Codepunkt teilt den Routern mit, wie der Datenaustausch behandelt werden soll. In diesem Szenario kann der Richtlinie ein niedriger Codepunktwert zugeordnet werden, um die Prioritätenvergabe für Browserdatenaustausch im Netzwerk zu beeinflussen.

Voraussetzungen und Annahmen

- Sie haben mit Ihrem ISP (Internet Service Provider) ein Service-Level-Agreement (SLA) geschlossen, um sicherzustellen, dass die Richtlinien die angeforderte Priorität erhalten. Die QoS-Richtlinie, die Sie auf dem System erstellen, ermöglicht es, dass der (in der Richtlinie angegebene) Datenaustausch im Netz-

werk eine Priorität erhält. Die QoS-Richtlinie garantiert die Priorität nicht und ist vom SLA abhängig. Tatsächlich haben Sie beim Einsatz von QoS-Richtlinien die Möglichkeit, bestimmte Servicestufen und Geschwindigkeiten zu vereinbaren.

- Richtlinien für differenzierte Services benötigen DiffServ-fähige Router im Netzwerkpfad. Die meisten Router sind DiffServ-fähig.

Konfiguration

Nachdem Sie die Voraussetzungen geprüft haben, können Sie jetzt die Richtlinie für differenzierte Services erstellen:

Zugehörige Konzepte

„Service-Level-Agreement" auf Seite 55
Dieses Thema stellt einige wichtige Aspekte eines Service-Level-Agreements (SLA) heraus, die sich auf Ihre QoS-Implementierung auswirken können. QoS ist eine Lösung für Netzwerke. Um auch außerhalb Ihres privaten Netzwerks Priorität zu erhalten, benötigen Sie möglicherweise ein Service-Level-Agreement (SLA) mit Ihrem ISP (Internet Service Provider).

„Differenzierte Services" auf Seite 2
Dies ist der erste Typ einer Richtlinie für die Bandbreite abgehender Daten, den Sie auf dem Betriebssystem erstellen können. Die differenzierten Services unterteilen den Datenaustausch im Netzwerk in unterschiedliche Klassen. Wenn Sie eine Richtlinie für differenzierte Services einsetzen wollen, müssen Sie festlegen, wie der Datenaustausch im Netzwerk klassifiziert werden soll und wie die unterschiedlichen Klassen zu behandeln sind.

Zugehörige Verweise

„QoS überwachen" auf Seite 63
Mit der QoS-Überwachung können Sie den IP-Datenaustausch auf dem System analysieren.

Szenariodetails: Richtlinie für differenzierte Services erstellen

Dieses Thema enthält Informationen zum Konfigurieren der Richtlinie für differenzierte Services auf dem System.

1. Erweitern Sie in System i Navigator *Ihr System* → **Netzwerk** → **IP-Richtlinien**.
2. Klicken Sie mit der rechten Maustaste auf **Quality of Service**, und wählen Sie die Option **Konfiguration** aus, um die QoS-Schnittstelle zu öffnen.
3. Klicken Sie in der QoS-Schnittstelle mit der rechten Maustaste auf den Richtlinientyp "DiffServ", und wählen Sie die Option **Neue Richtlinie** aus, um den Assistenten zu öffnen.
4. Lesen Sie die Angaben auf der Startseite des Assistenten, und klicken Sie auf **Weiter**, um die Seite "Name" aufzurufen.
5. Geben Sie im Feld **Name** den Wert `BOD` an. Auf Wunsch können Sie außerdem eine Beschreibung eingeben, die den Zweck dieser Richtlinie kenntlich macht. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite "Clients" die Option **Bestimmte Adresse oder Adressen** aus, und klicken Sie auf **Neu**, um Ihren Client zu definieren.
7. Geben Sie im Fenster "Neuer Client" die folgenden Informationen ein, und klicken Sie auf **OK**:
   - **Name**: `UCD_Client`
   - **IP-Adresse und Maske**: `10.10.10.0 / 24`

   Nachdem Sie auf **OK** geklickt haben, werden Sie zum Assistenten für Richtlinien zurückgeführt. Wenn Sie zuvor Clients erstellt haben, wählen Sie die Clients ab, und vergewissern Sie sich, dass nur relevante Clients ausgewählt sind.
8. Prüfen Sie auf der Seite "Serverdatenanforderung", dass die Einstellungen **Beliebiges Token** und **Alle Prioritäten** ausgewählt sind, und klicken Sie auf **Weiter**.
9. Wählen Sie auf der Seite "Anwendungen" die Einstellung **Bestimmter Port, Portbereich oder Servertyp** aus, und klicken Sie auf **Neu**.

10. Geben Sie im Fenster ″Neue Anwendung″ die folgenden Informationen ein, und klicken Sie auf **OK**, um zum Assistenten zurückzukehren:
    - **Name**: HTTP
    - **Port**: 80
11. Wählen Sie auf der Seite ″Anwendungen″ die Einstellung **Protokoll** aus, und vergewissern Sie sich, dass **TCP** ausgewählt ist. Klicken Sie auf **Weiter**.
12. Prüfen Sie, ob auf der Seite ″Lokale IP-Adresse″ die Einstellung **Alle IP-Adressen** ausgewählt ist, und klicken Sie auf **Weiter**.
13. Klicken Sie auf der Seite ″DiffServ-Serviceklasse″ auf **Neu**, um die Leistungskenndaten zu definieren. Der Assistent ″Neue Serviceklasse″ wird aufgerufen.
14. Lesen Sie die Angaben auf der Startseite des Assistenten, und klicken Sie auf **Weiter**.
15. Geben Sie auf der Seite ″Name″ den Wert BOD-Service ein. Auf Wunsch können Sie eine Beschreibung eingeben, die den Zweck dieser Richtlinie kenntlich macht. Klicken Sie auf **Weiter**.
16. Wählen Sie auf der Seite ″Servicetyp″ die Einstellung **Nur abgehend** aus, und klicken Sie auf **Weiter**. Diese Serviceklasse wird nur bei Richtlinien für abgehende Daten verwendet.
17. Wählen Sie auf der Seite ″DiffServ-Codepunktmarkierung für abgehende Daten″ die Einstellung **Klasse 4** aus, und klicken Sie auf **Weiter**. Die Leistung, die dieser Datenaustausch von Routern und anderen Systemen im Netzwerk zugewiesen bekommt, wird durch ein Pro-Hop-Verhalten bestimmt. Wenn Sie Unterstützung bei der Festlegung dieses Verhaltens benötigen, ziehen Sie den Hilfetext hinzu, der der Schnittstelle zugeordnet ist.
18. Prüfen Sie auf der Seite ″Abgehenden Datenaustausch messen″, ob die Einstellung **Ja** ausgewählt ist, und klicken Sie auf **Weiter**.
19. Geben Sie auf der Seite ″Grenzwerte für Geschwindigkeitssteuerung für abgehende Daten″ die folgenden Informationen ein, und klicken Sie auf **Weiter**:
    - **Größe des Token-Puffers**: 100 Kilobit
    - **Grenzwert für Durchschnittsgeschwindigkeit**: 512 Kilobit pro Sekunde
    - **Grenzwert für Spitzengeschwindigkeit**: 1 Megabit pro Sekunde
20. Wählen Sie auf der Seite ″Von Profildefinition abweichender, abgehender Datenaustausch″ die Einstellung **UDP-Pakete löschen oder TCP-Überlastungsfenster verkleinern** aus, und klicken Sie auf **Weiter**.
21. Prüfen Sie in der Zusammenfassung die Übersichtsdaten für die Serviceklasse. Wenn die Daten den gewünschten Einstellungen entsprechen, klicken Sie auf **Fertig stellen**, um die Serviceklasse zu erstellen. Nach dem Klicken auf **Fertig stellen** werden Sie zum Assistenten für Richtlinien zurückgeführt, und die Serviceklasse ist ausgewählt. Klicken Sie auf **Weiter**.
22. Wählen Sie auf der Seite ″Zeitplan″ die Einstellung **Aktiv während des ausgewählten Zeitplans** aus, und klicken Sie auf **Neu**.
23. Geben Sie im Fenster ″Neuen Zeitplan hinzufügen″ die folgenden Informationen ein, und klicken Sie auf **OK**:
    - **Name**: BOD-Zeitplan
    - **Tageszeit**: 24 Stunden aktiv
    - **Wochentag**: Freitag
24. Klicken Sie auf **Weiter**, um eine Zusammenfassung der Richtlinie anzuzeigen. Wenn die Angaben den gewünschten Einstellungen entsprechen, klicken Sie auf **Fertig stellen**. Im Fenster ″Konfiguration des QoS-Servers″ wird die neue Richtlinie nun im rechten Fensterbereich aufgelistet.

Szenariodetails: QoS-Server starten oder aktualisieren

Dieses Thema enthält Informationen zum Starten bzw. Aktualisieren des QoS-Servers.

Wählen Sie im Fenster ″Konfiguration des QoS-Servers″ die Optionen **Server → Starten** oder **Server → Aktualisieren** aus.

Szenariodetails: Prüfen, ob die Richtlinie funktioniert

Sie müssen anhand der Überwachung prüfen, ob die Richtlinie das konfigurierte Verhalten aufweist.

1. Wählen Sie im Fenster für die QoS-Konfiguration die Optionen **Server → Überwachen** aus. Das Fenster ″QoS-Überwachung″ wird aufgerufen.
2. Wählen Sie den Ordner für den Richtlinientyp ″DiffServ″ aus. In diesem Ordner werden alle DiffServ-Richtlinien angezeigt. Wählen Sie in der Liste den Eintrag **BOD** aus.

   Die wichtigsten Felder in diesem Zusammenhang sind diejenigen Felder, die ihre Daten aus dem Datenaustausch erhalten. Achten Sie besonders auf die Angaben in den Feldern ″Bits insgesamt″, ″Bits gemäß Profildefinition″ und ″Pakete gemäß Profildefinition″. Das Feld ″Von Profildefinition abweichende Bits″ signalisiert, ob der Datenaustausch die konfigurierten Richtlinienwerte überschreitet. In einer Richtlinie für differenzierte Services gibt die Anzahl für die Abweichung von der Profildefinition (bei UDP-Paketen) die Anzahl der gelöschten Bit an. Bei TCP gibt die Anzahl für die Abweichung von der Profildefinition an, wie viele Bit die Geschwindigkeit des Tokenpuffers überschreiten und in das Netzwerk gesendet werden. Bei TCP-Paketen werden Bit nie gelöscht. Die Anzahl der Pakete gemäß Profildefinition gibt an, wie viele Pakete durch diese Richtlinie gesteuert werden (von dem Zeitpunkt, an dem das Paket gestartet wurde, bis zur aktuellen Ausgabe der Überwachung).

   Auch der Wert, den Sie dem Feld **Grenzwert für Durchschnittsgeschwindigkeit** zuordnen, ist von Bedeutung. Sobald Pakete diesen Grenzwert überschreiten, beginnt das System mit dem Löschen der Pakete. Infolgedessen steigt der Wert für ″Von Profildefinition abweichende Bits″ an. Dies zeigt, dass die Richtlinie das gewünschte und konfigurierte Verhalten aufweist. Eine Beschreibung aller Felder in der Überwachung finden Sie unter „QoS überwachen” auf Seite 63.

   Anmerkung: Denken Sie daran, dass die Ergebnisse nur dann genau sind, wenn die Richtlinie aktiv ist. Prüfen Sie in diesem Zusammenhang den Zeitplan, der in der Richtlinie angegeben ist.

Szenariodetails: Eigenschaften ändern

Nachdem Sie die Ergebnisse der Überwachung geprüft haben, können Sie die Eigenschaften der Richtlinie oder der Serviceklasse ändern, um die erwarteten Ergebnisse zu erzielen.

So können Sie jeden Wert ändern, den Sie in der Richtlinie erstellt haben:

1. Wählen Sie im Fenster ″Konfiguration des QoS-Servers″ den Ordner **DiffServ** aus. Klicken Sie mit der rechten Maustaste in der Liste des rechten Fensterbereiches auf **BOD**, und wählen Sie die Option **Eigenschaften** aus, um die Richtlinie zu bearbeiten. Daraufhin wird ein Fenster ″Eigenschaften″ angezeigt. Es enthält die Werte, die die gesamte Richtlinie steuern.
2. Geben Sie die entsprechenden Werte an.
3. Um die Serviceklasse zu bearbeiten, wählen Sie den Ordner **Serviceklassen** aus. Klicken Sie mit der rechten Maustaste in der Liste des rechten Fensterbereiches auf **BOD-Service**, und wählen Sie die Option **Eigenschaften** aus, um die Serviceklasse zu bearbeiten. Daraufhin wird ein Fenster ″Eigenschaften″ für die Serviceklasse angezeigt. Es enthält die Werte, mit denen die Datenaustauschverwaltung gesteuert wird.
4. Geben Sie die entsprechenden Werte an.
5. Wählen Sie im Fenster ″Konfiguration des QoS-Servers″ die Optionen **Server → Aktualisieren** aus, um die Änderungen zu übernehmen.

Szenario: Sichere und vorhersehbare Ergebnisse (VPN und QoS)

Auch wenn Sie ein VPN (Virtual Private Network - virtuelles privates Netzwerk) verwenden, können Sie QoS-Richtlinien erstellen.

Situation

Einer Ihrer Partner verwendet eine Verbindung über ein VPN (Virtual Private Network - virtuelles privates Netzwerk). Sie möchten nun das VPN mit QoS kombinieren, um für die unternehmenskritischen

Daten Sicherheit und einen vorhersehbaren e-business-Ablauf zu gewährleisten. Die QoS-Konfiguration wird jeweils nur in einer Richtung ausgeführt. Wenn Sie eine Audio- oder eine Videoanwendung einsetzen, müssen Sie QoS daher auf beiden Seiten der Verbindung für die Anwendung einrichten.

Die Abbildung zeigt den Server und den Client in einer Host-zu-Host-Verbindung des VPN. Jedes R steht für einen DiffServ-fähigen Router im Pfad des Datenaustausches. In der Abbildung ist erkennbar, dass QoS-Richtlinien nur in einer Richtung ausgeführt werden.

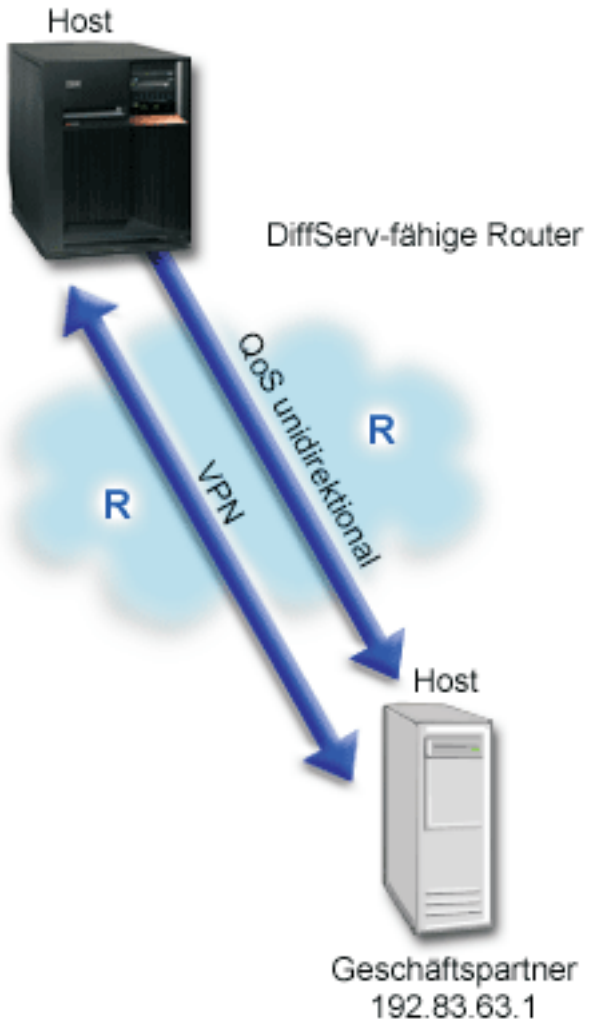


Abbildung 5. Host-zu-Host-Verbindung im VPN mit QoS-Richtlinie für differenzierte Services

Zielsetzungen

Durch die Kombination von VPN und QoS können Sie nicht nur einen Schutz, sondern auch eine Priorität für diese Verbindung einrichten. Zunächst konfigurieren Sie eine Host-zu-Host-Verbindung im VPN. Nachdem Sie den Schutz für die VPN-Verbindung eingerichtet haben, können Sie die QoS-Richtlinie definieren. Sie könnten beispielsweise eine Richtlinie für differenzierte Services erstellen. Dieser Richtlinie kann ein hoher Codepunktwert für die beschleunigte Weiterleitung zugeordnet werden, um die Prioritätenvergabe im Netzwerk für den unternehmenskritischen Datenaustausch zu beeinflussen.

Voraussetzungen und Annahmen

- Sie haben mit Ihrem ISP (Internet Service Provider) ein Service-Level-Agreement (SLA) geschlossen, um sicherzustellen, dass die Richtlinien die angeforderte Priorität erhalten. Die QoS-Richtlinie, die Sie auf dem System erstellen, ermöglicht es, dass der (in der Richtlinie angegebene) Datenaustausch im Netzwerk eine Priorität erhält. Die Priorität wird nicht garantiert und ist vom SLA abhängig. Tatsächlich haben Sie beim Einsatz von QoS-Richtlinien die Möglichkeit, bestimmte Servicestufen und Geschwindigkeiten zu vereinbaren. Weitere Informationen erhalten Sie nach Auswahl des Links zum Thema über Service-Level-Agreements.
- Richtlinien für differenzierte Services benötigen DiffServ-fähige Router im Netzwerkpfad. Die meisten Router sind DiffServ-fähig.

Konfiguration

Nachdem Sie die Voraussetzungen geprüft haben, können Sie jetzt die Richtlinie für differenzierte Services erstellen.

Zugehörige Konzepte

„Service-Level-Agreement" auf Seite 55
Dieses Thema stellt einige wichtige Aspekte eines Service-Level-Agreements (SLA) heraus, die sich auf Ihre QoS-Implementierung auswirken können. QoS ist eine Lösung für Netzwerke. Um auch außerhalb Ihres privaten Netzwerks Priorität zu erhalten, benötigen Sie möglicherweise ein Service-Level-Agreement (SLA) mit Ihrem ISP (Internet Service Provider).

„Differenzierte Services" auf Seite 2
Dies ist der erste Typ einer Richtlinie für die Bandbreite abgehender Daten, den Sie auf dem Betriebssystem erstellen können. Die differenzierten Services unterteilen den Datenaustausch im Netzwerk in unterschiedliche Klassen. Wenn Sie eine Richtlinie für differenzierte Services einsetzen wollen, müssen Sie festlegen, wie der Datenaustausch im Netzwerk klassifiziert werden soll und wie die unterschiedlichen Klassen zu behandeln sind.

Zugehörige Verweise

„QoS überwachen" auf Seite 63
Mit der QoS-Überwachung können Sie den IP-Datenaustausch auf dem System analysieren.

Szenariodetails: Host-zu-Host-Verbindung im VPN einrichten

Dieses Thema enthält Informationen zum Einrichten von Host-zu-Host-Verbindungen im VPN.

Informationen, die Ihnen bei der VPN-Konfiguration helfen, finden Sie unter Scenario: Basic business to business connection.

Szenariodetails: Richtlinie für differenzierte Services erstellen

Dieses Thema enthält Informationen zum Erstellen der Richtlinie für differenzierte Services.

1. Erweitern Sie in System i Navigator ***Ihr System*** → **Netzwerk** → **IP-Richtlinien**.
2. Klicken Sie mit der rechten Maustaste auf **Quality of Service**, und wählen Sie die Option **Konfiguration** aus, um das Fenster "Konfiguration des QoS-Servers" zu öffnen.
3. Klicken Sie im Fenster "Konfiguration des QoS-Servers" mit der rechten Maustaste auf "DiffServ", und wählen Sie die Option **Neue Richtlinie** aus, um den Assistenten zu öffnen.
4. Lesen Sie die Angaben auf der Startseite des Assistenten, und klicken Sie auf **Weiter**, um die Seite **Name** aufzurufen.
5. Geben Sie im Feld **Name** den Wert `VPN` an, und klicken Sie auf **Weiter**. Auf Wunsch können Sie eine Beschreibung eingeben, die den Zweck dieser Richtlinie kenntlich macht.
6. Wählen Sie auf der Seite "Clients" die Option **Bestimmte Adresse oder Adressen** aus, und klicken Sie auf **Neu**, um Ihren Client zu definieren.
7. Geben Sie im Fenster "Neuer Client" die folgenden Informationen ein:
   - **Name**: VPN-Client

- **IP-Adresse**: 192.83.63.1
- Klicken Sie auf **OK**, um den Client zu erstellen und zum Assistenten für differenzierte Services zurückzukehren.

Nachdem Sie auf **OK** geklickt haben, werden Sie zum Assistenten für Richtlinien zurückgeführt. Wenn Sie zuvor Clients erstellt haben, klicken Sie auf die Clients, und vergewissern Sie sich, dass nur relevante Clients ausgewählt sind.

8. Prüfen Sie auf der Seite "Serverdatenanforderung", dass die Einstellungen **Beliebiges Token** und **Alle Prioritäten** ausgewählt sind.
9. Prüfen Sie auf der Seite "Anwendungen", ob die Einstellungen **Alle Ports** und **Alle** ausgewählt sind.
10. Klicken Sie auf **Weiter**.
11. Übernehmen Sie auf der Seite "Lokale IP-Adresse" den Standardwert, und klicken Sie auf **Weiter**.
12. Klicken Sie auf der Seite "DiffServ-Serviceklasse" auf **Neu**, um die Leistungskenndaten zu definieren. Der Assistent "Neue Serviceklasse" wird aufgerufen.
13. Lesen Sie die Angaben auf der Startseite des Assistenten, und klicken Sie auf **Weiter**.
14. Geben Sie auf der Seite "Name" den Wert `EF-VPN` ein.
15. Wählen Sie auf der Seite "Servicetyp" die Einstellung **Nur abgehend** aus, und klicken Sie auf **Weiter**. Diese Serviceklasse wird nur bei Richtlinien für abgehende Daten verwendet.
16. Wählen Sie auf der Seite "DiffServ-Codepunktmarkierung für abgehende Daten" die Einstellung **Klasse 3** aus. Die Leistung, die dieser Datenaustausch von Routern und anderen Systemen im Netzwerk zugewiesen bekommt, wird durch ein Pro-Hop-Verhalten bestimmt. Wenn Sie Unterstützung bei der Festlegung dieses Verhaltens benötigen, ziehen Sie den Hilfetext hinzu, der der Schnittstelle zugeordnet ist.
17. Prüfen Sie auf der Seite "Abgehenden Datenaustausch messen", ob die Einstellung **Ja** ausgewählt ist, und klicken Sie auf **Weiter**.
18. Geben Sie auf der Seite "Grenzwerte für Geschwindigkeitssteuerung für abgehende Daten" die folgenden Informationen ein, und klicken Sie auf **Weiter**:
    - **Größe des Token-Puffers**: 100 Kilobit
    - **Grenzwert für Durchschnittsgeschwindigkeit**: 64 Megabit pro Sekunde
    - **Grenzwert für Spitzengeschwindigkeit**: Keine Begrenzung
19. Wählen Sie auf der Seite "Von Profildefinition abweichender, abgehender Datenaustausch" die Einstellung **UDP-Pakete löschen oder TCP-Überlastungsfenster verkleinern** aus, und klicken Sie auf **Weiter**.
20. Sehen Sie sich die Angaben auf der Seite "Serviceklasse - Zusammenfassung" an, und klicken Sie auf **Fertig stellen**, um zum Assistenten für Richtlinien zurückzukehren.
21. Prüfen Sie auf der Seite "DiffServ-Serviceklasse", ob **EF-VPN** ausgewählt ist, und klicken Sie auf **Weiter**.
22. Wählen Sie auf der Seite "Zeitplan" die Einstellung **Aktiv während des ausgewählten Zeitplans** aus, und klicken Sie auf **Neu**.
23. Geben Sie im Fenster "Neuen Zeitplan hinzufügen" die folgenden Informationen ein, und klicken Sie auf **OK**:
    - **Name**: Erste_Schicht
    - **Tageszeit**: Zu bestimmten Zeiten aktiv (fügen Sie 9.00 Uhr bis 17.00 Uhr hinzu)
    - **Wochentag**: An bestimmten Tagen aktiv (wählen Sie Montag bis Freitag aus)
24. Klicken Sie auf der Seite "Zeitplan" auf **Weiter**.
25. Sehen Sie sich die Übersichtsdaten an. Wenn die Daten den gewünschten Einstellungen entsprechen, klicken Sie auf **Fertig stellen**, um die Richtlinie zu erstellen. Das Fenster "Konfiguration des QoS-Servers" enthält eine Liste mit allen auf dem System erstellten Richtlinien. Nachdem Sie den Assistenten beendet haben, wird die Richtlinie im rechten Fensterbereich angezeigt.

Szenariodetails: QoS-Server starten oder aktualisieren

Dieses Thema enthält Informationen zum Starten bzw. Aktualisieren des QoS-Servers.

Wählen Sie im Fenster ″Konfiguration des QoS-Servers″ die Optionen **Server → Starten** oder **Server → Aktualisieren** aus.

Szenariodetails: Prüfen, ob die Richtlinie funktioniert

Sie müssen anhand der Überwachung prüfen, ob die Richtlinie das konfigurierte Verhalten aufweist.

1. Wählen Sie im Fenster ″Konfiguration des QoS-Servers″ die Optionen **Server → Überwachen** aus. Das Fenster ″QoS-Überwachung″ wird aufgerufen.
2. Wählen Sie den Richtlinientyp für differenzierte Services aus. Damit werden alle Richtlinien für differenzierte Services angezeigt.

   Ähnlich wie bei dem ersten Beispiel sind die wichtigsten Felder in diesem Zusammenhang diejenigen Felder, die ihre Daten aus dem Datenaustausch erhalten. Achten Sie besonders auf die Angaben in den Feldern ″Bits insgesamt″, ″Bits gemäß Profildefinition″ und ″Von Profildefinition abweichende Pakete″. Das Feld ″Von Profildefinition abweichende Bits″ signalisiert, ob der Datenaustausch die konfigurierten Richtlinienwerte überschreitet. Die Anzahl der Pakete gemäß Profildefinition gibt an, wie viele Pakete durch diese Richtlinie gesteuert werden. Auch der Wert, den Sie dem Feld ″Grenzwert für Durchschnittsgeschwindigkeit″ zuordnen, ist von Bedeutung. Wenn TCP-Pakete diesen Grenzwert überschreiten, werden sie solange in das Netzwerk gesendet, bis das TCP-Überlastungsfenster verkleinert werden kann, um Pakete, die von der Profildefinition abweichen, in eine Warteschlange zu stellen. Infolgedessen steigt der Wert für ″Von Profildefinition abweichende Bits″ an. Der Unterschied zwischen dieser Richtlinie und dem Szenario ″Datenaustausch des Browser begrenzen″ besteht darin, dass die Pakete in diesem Beispiel unter Verwendung des VPN-Protokolls geschützt werden. QoS kann somit in Kombination mit einer VPN-Verbindung verwendet werden. Eine Beschreibung aller Felder in der Überwachung finden Sie unter „QoS überwachen” auf Seite 63.

   Anmerkung: Denken Sie daran, dass die Ergebnisse nur dann genau sind, wenn die Richtlinie aktiv ist. Prüfen Sie in diesem Zusammenhang den Zeitplan, der in der Richtlinie angegeben ist.

Szenariodetails: Eigenschaften ändern

Nachdem Sie die Ergebnisse der Überwachung geprüft haben, können Sie die Eigenschaften der Richtlinie oder der Serviceklasse ändern, um die erwarteten Ergebnisse zu erzielen.

1. Wählen Sie im Fenster ″Konfiguration des QoS-Servers″ den Ordner **DiffServ** aus. Klicken Sie mit der rechten Maustaste in der Liste des rechten Fensterbereiches auf **VPN**, und wählen Sie die Option **Eigenschaften** aus, um die Richtlinie zu bearbeiten. Daraufhin wird ein Fenster ″Eigenschaften″ angezeigt. Es enthält die Werte, die die gesamte Richtlinie steuern.
2. Geben Sie die entsprechenden Werte an.
3. Um die Serviceklasse zu bearbeiten, wählen Sie den Ordner **Serviceklassen** aus. Klicken Sie mit der rechten Maustaste in der Liste des rechten Fensterbereiches auf **EF-VPN**, und wählen Sie die Option **Eigenschaften** aus, um die Serviceklasse zu bearbeiten. Daraufhin wird ein Fenster ″Eigenschaften″ für die Serviceklasse angezeigt. Es enthält die Werte, mit denen die Datenaustauschverwaltung gesteuert wird.
4. Geben Sie die entsprechenden Werte an.
5. Wählen Sie im Fenster ″Konfiguration des QoS-Servers″ die Optionen **Server → Aktualisieren** aus, um die Änderungen zu übernehmen.

Szenario: Eingehende Verbindungen begrenzen

Falls Sie die eingehenden Verbindungsanforderungen an Ihr System steuern müssen, verwenden Sie eine Richtlinie für ankommende Daten.

Situation

Die Ressourcen Ihres Webservers sind aufgrund von Clientanforderungen, die in Ihrem Netzwerk eintreffen, überlastet. Sie werden gebeten, den ankommenden HTTP-Datenaustausch für den Webserver auf der lokalen Schnittstelle 192.168.1.1 zu verlangsamen. QoS hilft Ihnen dabei, die akzeptierten Anforderungen eingehender Verbindungen anhand der Verbindungsattribute (z. B. IP-Adresse) auf dem System zu begrenzen. Zu diesem Zweck definieren Sie eine Richtlinie für ankommende Daten, in der die Anzahl der akzeptierten eingehenden Verbindungen begrenzt wird.

Die Abbildung zeigt ein Unternehmen und ein Kundenunternehmen. Diese QoS-Richtlinie kann den Fluss des Datenaustausches nur in einer Richtung steuern.

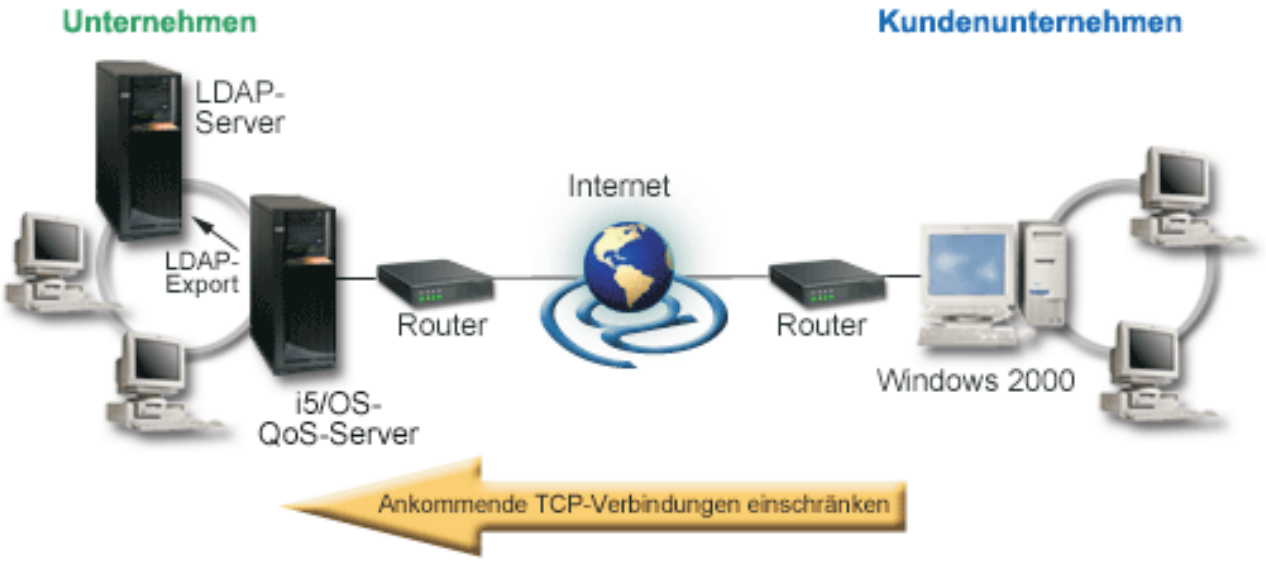


Abbildung 6. Ankommende TCP-Verbindungen einschränken

Zielsetzungen

Um eine Richtlinie für ankommende Daten zu konfigurieren, müssen Sie festlegen, ob Sie den Datenaustausch für eine lokale Schnittstelle oder für eine spezifische Anwendung einschränken wollen und ob Sie den Datenaustausch von einem bestimmten Client begrenzen wollen. In diesem Fall können Sie eine Richtlinie erstellen, die Verbindungsversuche von "Fremdunternehmen" zu Port 80 (HTTP-Protokoll) auf der lokalen Schnittstelle 192.168.1.1 einschränkt.

Konfiguration

Die folgenden Themen erläutern, wie Sie eine Richtlinie für ankommende Daten erstellen.

Zugehörige Verweise

„QoS überwachen" auf Seite 63
Mit der QoS-Überwachung können Sie den IP-Datenaustausch auf dem System analysieren.

Szenariodetails: Richtlinie für ankommende Daten erstellen

Dieses Thema enthält Informationen zum Erstellen der Richtlinie für ankommende Daten auf dem System.

1. Erweitern Sie in System i Navigator ***Ihr System*** → **Netzwerk** → **IP-Richtlinien**.
2. Klicken Sie mit der rechten Maustaste auf **Quality of Service**, und wählen Sie die Option **Konfiguration** aus, um das Fenster "Konfiguration des QoS-Servers" zu öffnen.

3. Klicken Sie im Fenster ″Konfiguration des QoS-Servers″ mit der rechten Maustaste auf **Richtlinien für ankommende Daten**, und wählen Sie die Option **Neue Richtlinie** aus, um den Assistenten zu öffnen.
4. Lesen Sie die Angaben auf der Startseite des Assistenten, und klicken Sie auf **Weiter**.
5. Geben Sie im Feld **Name** den Wert `Fremdunternehmen_einschränken` an, und klicken Sie auf **Weiter**. Auf Wunsch können Sie eine Beschreibung eingeben, die den Zweck dieser Richtlinie kenntlich macht.
6. Wählen Sie auf der Seite ″Clients″ die Option **Bestimmte Adresse oder Adressen** aus, und klicken Sie auf **Neu**, um Ihren Client zu definieren.
7. Geben Sie im Fenster ″Neuer Client″ die folgenden Informationen ein:
   - **Name**: Fremdunternehmen
   - **IP-Adressenbereich**: 10.1.1.1 bis 10.1.1.10
   - Klicken Sie auf **OK**, um den Client zu erstellen und zum Assistenten für Richtlinien zurückzukehren.

   Nachdem Sie auf **OK** geklickt haben, werden Sie zum Assistenten für Richtlinien zurückgeführt. Wenn Sie zuvor Clients erstellt hatten, wählen Sie die Clients ab, und vergewissern Sie sich, dass nur relevante Clients ausgewählt sind.
8. Prüfen Sie auf der Seite ″URI″, ob die Einstellung **Beliebiger URI** ausgewählt ist, und klicken Sie auf **Weiter**.
9. Wählen Sie auf der Seite ″Anwendungen″ die Einstellung **Bestimmter Port, Portbereich oder Servertyp** aus, und klicken Sie auf **Neu**.
10. Geben Sie im Fenster ″Neue Anwendung″ die folgenden Informationen ein, und klicken Sie auf **OK**, um zum Assistenten zurückzukehren:
    - **Name**: HTTP
    - **Port**: 80
11. Klicken Sie auf **Weiter**, um die Seite ″Codepunkt″ aufzurufen.
12. Prüfen Sie auf der Seite ″Codepunkt″, ob die Einstellung **Alle Codepunkte** ausgewählt ist, und klicken Sie auf **Weiter**.
13. Wählen Sie auf der Seite ″Lokale IP-Adresse″ die Einstellung **IP-Adresse** aus, und wählen Sie eine Schnittstelle aus, an die die Anforderungen für Ihr lokales System gesendet werden. In diesem Beispiel wird der Wert ″192.168.1.1″ verwendet.
14. Klicken Sie auf der Seite ″Serviceklasse″ auf **Neu**, um die Leistungskenndaten zu definieren. Der Assistent ″Neue Serviceklasse″ wird aufgerufen.
15. Lesen Sie die Angaben auf der Startseite des Assistenten, und klicken Sie auf **Weiter**.
16. Geben Sie auf der Seite ″Name″ den Wert **Ankommend** ein, und klicken Sie auf **Weiter**. Auf Wunsch können Sie eine Beschreibung eingeben, die den Zweck dieser Serviceklasse kenntlich macht.
17. Wählen Sie auf der Seite ″Servicetyp″ die Einstellung **Nur ankommend** aus. Diese Serviceklasse wird nur bei Richtlinien für ankommende Daten verwendet.
18. Geben Sie auf der Seite ″Grenzwerte für eingehende Verbindungen″ die folgenden Informationen ein, und klicken Sie auf **Weiter**:
    - **Durchschnittsverbindungsgeschwindigkeit**: 50 pro Sekunde
    - **Burstgrenzwert der Verbindungen**: 50 Verbindungen
    - **Priorität**: Mittel
19. Klicken Sie auf **Fertig stellen**, um zum Assistenten für Richtlinien zurückzukehren.
20. Prüfen Sie auf der Seite ″Serviceklasse″, ob die soeben erstellte Serviceklasse ausgewählt ist, und klicken Sie auf **Weiter**.
21. Wählen Sie auf der Seite ″Zeitplan″ die Einstellung **Aktiv während des ausgewählten Zeitplans** aus, und klicken Sie auf **Neu**.

22. Geben Sie im Fenster ″Neuen Zeitplan hinzufügen″ die folgenden Informationen ein, und klicken Sie auf **OK**:
    - **Name**: Erste_Schicht
    - **Tageszeit**: Zu bestimmten Zeiten aktiv (fügen Sie 9.00 Uhr bis 17.00 Uhr hinzu)
    - **Wochentag**: An bestimmten Tagen aktiv (wählen Sie Montag bis Freitag aus)
23. Klicken Sie auf der Seite ″Zeitpläne″ auf **Weiter**.
24. Sehen Sie sich die Übersichtsdaten an. Wenn die Daten den gewünschten Einstellungen entsprechen, klicken Sie auf **Fertig stellen**, um die Richtlinie zu erstellen. Das Fenster ″Konfiguration des QoS-Servers″ enthält eine Liste mit allen auf dem System erstellten Richtlinien. Nachdem Sie den Assistenten beendet haben, wird die Richtlinie im rechten Fensterbereich angezeigt.

    Die Konfiguration der Richtlinie für ankommende Daten auf dem System ist beendet. Als Nächstes müssen Sie den Server starten oder aktualisieren.

Szenariodetails: QoS-Server starten oder aktualisieren

Dieses Thema enthält Informationen zum Starten bzw. Aktualisieren des QoS-Servers.

Wählen Sie im Fenster ″Konfiguration des QoS-Servers″ die Optionen **Server → Starten** oder **Server → Aktualisieren** aus.

Szenariodetails: Prüfen, ob die Richtlinie funktioniert

Dieses Thema enthält Information darüber, wie Sie mit der Überwachung prüfen, ob die Richtlinie das konfigurierte Verhalten aufweist.

1. Wählen Sie im Fenster für die QoS-Konfiguration die Optionen **Server → Überwachen** aus. Das Fenster ″QoS-Überwachung″ wird aufgerufen.
2. Wählen Sie den Richtlinientyp ″Ankommend″ aus. Hierdurch werden alle Richtlinien für ankommende Daten angezeigt. Wählen Sie in der Liste den Eintrag **Fremdunternehmen_einschränken** aus.

   Bitte prüfen Sie unbedingt alle Felder mit Messangaben (z. B. akzeptierte Anforderungen, gelöschte Anforderungen, Anforderungen insgesamt und Verbindungsgeschwindigkeit). Das Feld ″Gelöschte Anforderungen″ signalisiert, ob der Datenaustausch die konfigurierten Richtlinienwerte überschreitet. Die akzeptierten Verbindungen geben an, wie viele Bit durch diese Richtlinie gesteuert werden (von dem Zeitpunkt, an dem das Paket gestartet wurde, bis zur aktuellen Ausgabe der Überwachung).

   Auch der Wert, den Sie dem Feld **Grenze für Durchschnittsanforderungsgeschwindigkeit** zuordnen, ist von Bedeutung. Sobald Pakete diesen Grenzwert überschreiten, beginnt das System mit dem Löschen der Pakete. Infolgedessen steigt der Wert für ″Gelöschte Anforderungen″ an. Dies zeigt, dass die Richtlinie das gewünschte und konfigurierte Verhalten aufweist. Eine Beschreibung aller Felder in der Überwachung finden Sie unter „QoS überwachen″ auf Seite 63.

   Anmerkung: Denken Sie daran, dass die Ergebnisse nur dann genau sind, wenn die Richtlinie aktiv ist. Prüfen Sie in diesem Zusammenhang den Zeitplan, der in der Richtlinie angegeben ist.

Szenariodetails: Eigenschaften ändern

Nachdem Sie die Ergebnisse der Überwachung geprüft haben, können Sie die Eigenschaften der Richtlinie oder der Serviceklasse ändern, um die erwarteten Ergebnisse zu erzielen.

1. Wählen Sie im Fenster ″Konfiguration des QoS-Servers″ den Ordner **Ankommende Daten** aus. Klicken Sie mit der rechten Maustaste in der Liste des rechten Fensterbereiches auf **Fremdunternehmen_einschränken**, und wählen Sie die Option **Eigenschaften** aus, um die Richtlinie zu bearbeiten. Daraufhin wird ein Fenster ″Eigenschaften″ angezeigt. Es enthält die Werte, die die gesamte Richtlinie steuern.
2. Hier können Sie die entsprechenden Werte ändern.
3. Um die Serviceklasse zu bearbeiten, wählen Sie den Ordner **Serviceklassen** aus. Klicken Sie mit der rechten Maustaste in der Liste des rechten Fensterbereiches auf **Ankommend**, und wählen Sie die

Option **Eigenschaften** aus, um die Serviceklasse zu bearbeiten. Daraufhin wird ein Fenster "Eigenschaften" für die Serviceklasse angezeigt. Es enthält die Werte, mit denen die Datenaustauschverwaltung gesteuert wird.

4. Geben Sie die entsprechenden Werte an.
5. Wählen Sie im Fenster "Konfiguration des QoS-Servers" die Optionen **Server** → **Aktualisieren** aus, um die Änderungen zu übernehmen.

Szenario: Vorhersehbarer B2B-Datenaustausch

Wenn Sie eine vorhersehbare Übermittlung benötigen und dennoch eine Reservierung anfordern müssen, können Sie natürlich auch eine Richtlinie für integrierte Services verwenden. Dieses Beispiel verwendet einen Service des Typs "Gesteuertes Laden".

Situation

Die Verkaufsabteilung hat mitgeteilt, dass der Datenaustausch im Netzwerk nicht erwartungsgemäß ausgeführt wird. Das Betriebssystem i5/OS Ihres Unternehmens befindet sich in einer B2B-Umgebung, die einen vorhersehbaren Service für das On Demand Business erfordert. Sie müssen für Ihre Kunden vorhersehbare Transaktionen zur Verfügung stellen. Sie wollen der Verkaufsabteilung eine höhere Qualität des Service für die Bestellanwendung zuweisen, die während der Tageszeiten mit den meisten Aktivitäten gültig ist (zwischen 10.00 Uhr und 16.00 Uhr).

In der folgenden Abbildung befindet sich die Verkaufsabteilung im privaten Netzwerk. Im Pfad für den Datenaustausch mit dem B2B-Client gibt es RSVP-fähige Router. Jedes `R` steht für einen Router im Pfad des Datenaustausches.

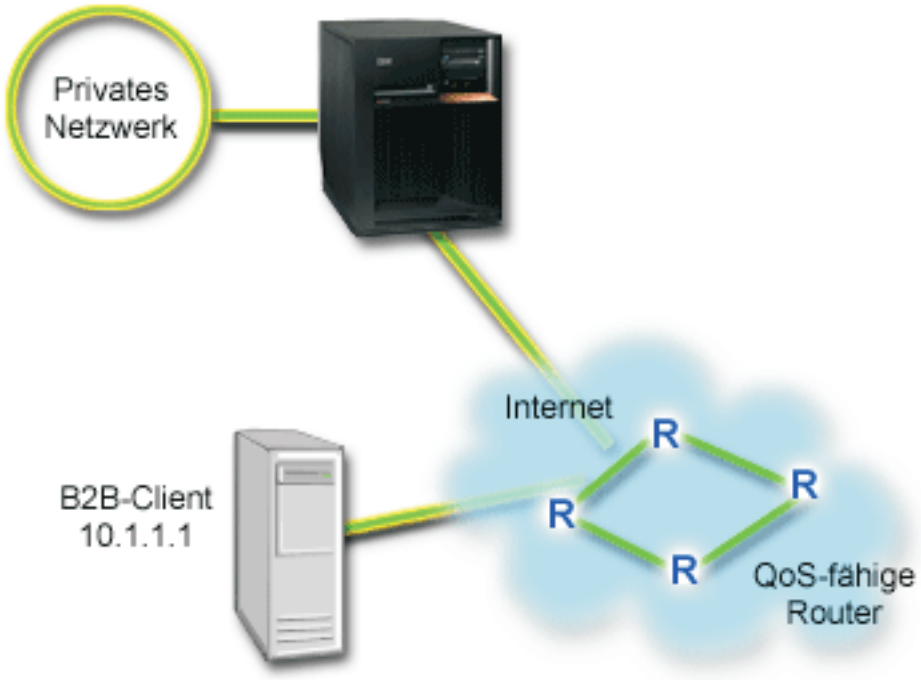


Abbildung 7. Richtlinie für integrierte Services bei einem B2B-Client unter Verwendung von RSVP-fähigen Routern

Zielsetzungen

Ein Service des Typs "Gesteuertes Laden" unterstützt Anwendungen, die sehr empfindlich auf Netzwerküberlastungen reagieren, aber trotzdem leichte Verzögerungen und Datenverluste tolerieren. Wenn eine

Anwendung einen Service des Typs ″Gesteuertes Laden″ verwendet, leidet ihr Leistungsverhalten nicht unter einer Zunahme der Netzwerkauslastung. Dem Datenaustausch wird ein Service bereitgestellt, der etwa dem normalen Datenaustausch in einem Netzwerk mit normalen Bedingungen entspricht. Da diese spezifische Anwendung eine gewisse Verzögerung toleriert, beschließen Sie, eine Richtlinie für integrierte Services zu verwenden, die einen Service des Typs ″Gesteuertes Laden″ einsetzt.

Richtlinien für integrierte Services setzen voraus, dass die Router im Pfad des Datenaustausches RSVP-fähig sind.

Voraussetzungen und Annahmen

Eine Richtlinie für integrierte Services ist eine erweiterte Richtlinie, die substanzielle Ressourcen erfordern kann. Richtlinien für integrierte Services setzen Folgendes voraus:

- **RSVP-fähige Anwendungen**

  Da Ihr System nicht über RSVP-fähige Anwendungen verfügt, müssen Sie eigene RSVP-fähige Anwendungen schreiben. Zum Schreiben von eigenen Anwendungen verwenden Sie die RAPI-API, die qtoq-Socket-APIs für QoS oder die APIs für integrierte Services.
- **RSVP-fähige Router und Systeme im Netzwerkpfad**

  QoS ist eine Lösung für Netzwerke. Auch wenn Sie sich nicht sicher sind, ob das gesamte Netzwerk RSVP-fähig ist, können Sie eine Richtlinie für integrierte Services erstellen und dann eine Markierung verwenden, um der Richtlinie eine bestimmte Priorität zuzuweisen. Die Priorität kann jedoch nicht garantiert werden.
- **Service-Level-Agreement**

  Sie haben mit Ihrem ISP (Internet Service Provider) ein Service-Level-Agreement (SLA) geschlossen, um sicherzustellen, dass die Richtlinien die angeforderte Priorität erhalten. Die QoS-Richtlinie, die Sie auf dem System erstellen, ermöglicht es, dass der (in der Richtlinie angegebene) Datenaustausch im Netzwerk eine Priorität erhält. Die QoS-Richtlinie garantiert die Priorität nicht und ist vom SLA abhängig. Tatsächlich haben Sie beim Einsatz von QoS-Richtlinien die Möglichkeit, bestimmte Servicestufen und Geschwindigkeiten zu vereinbaren.

  Anmerkung: Wenn Sie in einem privaten Netzwerk arbeiten, ist ein SLA nicht erforderlich.

Konfiguration

Nachdem Sie die Voraussetzungen geprüft haben, können Sie jetzt die Richtlinie für integrierte Services erstellen.

Zugehörige Konzepte

„Typen von integrierten Services” auf Seite 10
Es gibt zwei Typen von integrierten Services: gesteuertes Laden und garantierter Service.

„Integrierte Services” auf Seite 7
Der zweite Typ einer Richtlinie für die Bandbreite abgehender Daten, den Sie erstellen können, ist eine Richtlinie für integrierte Services. Die integrierten Services bieten IP-Anwendungen die Möglichkeit, unter Verwendung des RSVP-Protokolls (ReSerVation Protocol) und der APIs für QoS Bandbreite anzufordern und zu reservieren.

„APIs für QoS” auf Seite 18
Dieses Thema enthält Informationen über Protokolle, APIs und die Voraussetzungen für einen Router, der RSVP (ReSerVation Protocol) verwenden kann, also RSVP-fähig ist. Zu den APIs für QoS gehören die RAPI-API, die qtoq-Socket-API, die API sendmsg() und die monitor-APIs.

„Service-Level-Agreement” auf Seite 55
Dieses Thema stellt einige wichtige Aspekte eines Service-Level-Agreements (SLA) heraus, die sich auf Ihre QoS-Implementierung auswirken können. QoS ist eine Lösung für Netzwerke. Um auch außerhalb Ihres privaten Netzwerks Priorität zu erhalten, benötigen Sie möglicherweise ein Service-Level-Agreement (SLA) mit Ihrem ISP (Internet Service Provider).

Zugehörige Verweise

„QoS überwachen" auf Seite 63
Mit der QoS-Überwachung können Sie den IP-Datenaustausch auf dem System analysieren.

Szenariodetails: Richtlinie für integrierte Services erstellen

Dieses Thema enthält Informationen zum Erstellen der Richtlinie für integrierte Services auf dem System.

1. Erweitern Sie in System i Navigator ***Ihr System*** → **Netzwerk** → **IP-Richtlinien**.
2. Klicken Sie mit der rechten Maustaste auf **Quality of Service**, und wählen Sie die Option **Konfiguration** aus, um das Fenster "Konfiguration des QoS-Servers" zu öffnen.
3. Klicken Sie im Fenster "Konfiguration des QoS-Servers" mit der rechten Maustaste auf den Richtlinientyp "IntServ", und wählen Sie die Option **Neue Richtlinie** aus, um den Assistenten zu öffnen.
4. Lesen Sie die Angaben auf der Startseite des Assistenten, und klicken Sie auf **Weiter**, um die Seite **Name** aufzurufen.
5. Geben Sie im Feld **Name** den Wert `B2B-CL` ein, und klicken Sie auf **Weiter**. Auf Wunsch können Sie eine Beschreibung eingeben, die den Zweck dieser Richtlinie kenntlich macht.
6. Wählen Sie auf der Seite "Clients" die Option **Bestimmte Adresse oder Adressen** aus, und klicken Sie auf **Neu**, um Ihren Client zu definieren.
7. Geben Sie im Fenster "Neuer Client" die folgenden Informationen ein:
   - **Name**: CL-Client
   - **IP-Adresse**: 10.1.1.1
   - Klicken Sie auf **OK**, um den Client zu erstellen und zum Assistenten für Richtlinien zurückzukehren.

   Nachdem Sie auf **OK** geklickt haben, werden Sie zum Assistenten für Richtlinien zurückgeführt. Wenn Sie zuvor Clients erstellt haben, wählen Sie die Clients ab, und vergewissern Sie sich, dass nur relevante Clients ausgewählt sind.
8. Geben Sie im Fenster "Neue Anwendung" die folgenden Informationen ein, und klicken Sie auf **OK**, um zum Assistenten zurückzukehren:
   - **Name**: Geschäftsanwendung
   - **Portbereich**: 7000-8000
9. Wählen Sie auf der Seite "Anwendungen" die Einstellung **Protokoll** aus, und vergewissern Sie sich, dass **TCP** ausgewählt ist. Klicken Sie auf **Weiter**.

   Anmerkung: Die Anwendung, die Sie für eine Richtlinie für integrierte Services auswählen, muss für die Verwendung der RAPI-API oder der qtoc-Socket-APIs geschrieben worden sein. Zusammen mit RSVP führen diese APIs die Reservierung für die integrierten Services im Netzwerk aus. Wenn Sie diese APIs nicht verwenden, erhält die Anwendung keine Priorität oder Garantie. Außerdem muss beachtet werden, dass diese Richtlinie Ihre Anwendungen zwar in die Lage versetzt, im Netzwerk eine Priorität zu erhalten, dies jedoch nicht garantieren kann. Alle Router und Systeme im Pfad des Datenaustausches müssen ebenfalls RSVP verwenden, damit eine Reservierung garantiert werden kann. Eine durchgängige Reservierung ist von der Teilnahme im gesamten Netzwerk abhängig.
10. Übernehmen Sie auf der Seite "Lokale IP-Adresse" den Standardwert, und klicken Sie auf **Weiter**.
11. Wählen Sie auf der Seite "Typ der integrierten Services" die Einstellung **Gesteuertes Laden** aus, und klicken Sie auf **Weiter**.
12. Wählen Sie auf der Seite "Markierung für integrierte Services" die Einstellung **Nein, kein Pro-Hop-Verhalten zuordnen** aus, und klicken Sie auf **Weiter**.
13. Geben Sie auf der Seite "Leistungsgrenzen für integrierte Services" die folgenden Informationen ein, und klicken Sie auf **Weiter**:
    - **Maximale Anzahl Datenflüsse**: 5

- **Grenze für Token-Geschwindigkeit (R)**: Keine Begrenzung
- **Größe des Token-Puffers**: 100 Kilobit
- **Grenze für Token-Geschwindigkeit (R)**: 25 Megabit pro Sekunde

14. Wählen Sie auf der Seite ″Zeitplan″ die Einstellung **Aktiv während des ausgewählten Zeitplans** aus, und klicken Sie auf **Neu**.
15. Geben Sie auf der Seite ″Neuen Zeitplan hinzufügen″ die folgenden Informationen ein, und klicken Sie auf **OK**:
    - **Name**: Hauptzeit
    - **Tageszeit**: Zu bestimmten Zeiten aktiv (fügen Sie 10.00 Uhr bis 16.00 Uhr hinzu)
    - **Wochentag**: An bestimmten Tagen aktiv (wählen Sie Montag bis Freitag aus)
16. Klicken Sie auf der Seite ″Zeitpläne″ auf **Weiter**.
17. Prüfen Sie die Übersichtsdaten. Wenn die Daten den gewünschten Einstellungen entsprechen, klicken Sie auf **Fertig stellen**, um die Richtlinie zu erstellen. Die QoS-Hauptschnittstelle enthält eine Liste mit auf dem System erstellten Richtlinien. Nachdem Sie den Assistenten beendet haben, wird die Richtlinie im rechten Fensterbereich angezeigt.

Die Konfiguration der Richtlinie für integrierte Services auf dem System ist beendet. Als Nächstes müssen Sie den Server starten oder aktualisieren.

Szenariodetails: QoS-Server starten oder aktualisieren

Dieses Thema enthält Informationen zum Starten bzw. Aktualisieren des QoS-Servers.

Wählen Sie im Fenster ″Konfiguration des QoS-Servers″ die Optionen **Server → Starten** oder **Server → Aktualisieren** aus.

Szenariodetails: Prüfen, ob die Richtlinie funktioniert

Dieses Thema enthält Information darüber, wie Sie mit der Überwachung prüfen, ob die Richtlinie das konfigurierte Verhalten aufweist.

1. Wählen Sie im Fenster ″Konfiguration des QoS-Servers″ die Optionen **Server → Überwachen** aus. Das Fenster ″QoS-Überwachung″ wird aufgerufen.
2. Wählen Sie den Richtlinientyp für integrierte Services aus. Damit werden alle Richtlinien für integrierte Services angezeigt.

   Die wichtigsten Felder in diesem Zusammenhang sind diejenigen Felder, die ihre Daten aus dem Datenaustausch erhalten. Achten Sie besonders auf die Angaben in den Feldern ″Bits insgesamt″, ″Bits gemäß Profildefinition″ und ″Pakete gemäß Profildefinition″. Der Wert für ″Von Profildefinition abweichende Bits″ macht kenntlich, dass anderer Datenaustausch verzögert oder gelöscht wird, um die Anforderungen dieser Richtlinie für integrierte Services zu erfüllen. Eine vollständige Beschreibung der Felder für die Überwachung finden Sie unter „QoS überwachen” auf Seite 63.

   Anmerkung: Denken Sie daran, dass die Ergebnisse nur dann genau sind, wenn die Richtlinie aktiv ist. Prüfen Sie in diesem Zusammenhang den Zeitplan, der in der Richtlinie angegeben ist. Außerdem zeigt die Überwachung die Richtlinien für integrierte Services nur nach der Ausführung der Anwendungen an. Eine RSVP-Reservierung muss vor der Überwachung eingerichtet werden.

Szenariodetails: Eigenschaften ändern

Nachdem Sie die Ergebnisse der Überwachung geprüft haben, können Sie die Eigenschaften der Richtlinie ändern, um die erwarteten Ergebnisse zu erzielen.

1. Wählen Sie im Fenster ″Konfiguration des QoS-Servers″ den Ordner **IntServ** aus. Klicken Sie mit der rechten Maustaste in der Liste des rechten Fensterbereiches auf **B2B-CL**, und wählen Sie die Option **Eigenschaften** aus, um die Richtlinie zu bearbeiten. Daraufhin wird ein Fenster ″Eigenschaften″ angezeigt. Es enthält die Werte, die die gesamte Richtlinie steuern.
2. Geben Sie die entsprechenden Werte an.

3. Wählen Sie im Fenster ″Konfiguration des QoS-Servers″ die Optionen **Server → Aktualisieren** aus, um die Änderungen zu übernehmen.

Szenario: Dedizierte Übermittlung (IP-Telefonie)

Wenn Sie eine dedizierte Übermittlung benötigen und eine Reservierung anfordern wollen, verwenden Sie eine Richtlinie für integrierte Services. Sie können zwei unterschiedliche Typen von Richtlinien für integrierte Services erstellen, nämlich ″Garantiert″ und ″Gesteuertes Laden″. In diesem Beispiel wird ein Service des Typs ″Garantiert″ verwendet.

Situation

Der Geschäftsführer Ihres Unternehmens will zwischen 13.00 Uhr und 14.00 Uhr eine Livesendung an einen Kunden in der Region absetzen. Sie müssen sicherstellen, dass die IP-Telefonie eine garantierte Bandbreite hat, damit die Sendung nicht unterbrochen wird. In diesem Szenario befindet sich die Anwendung auf dem Server.

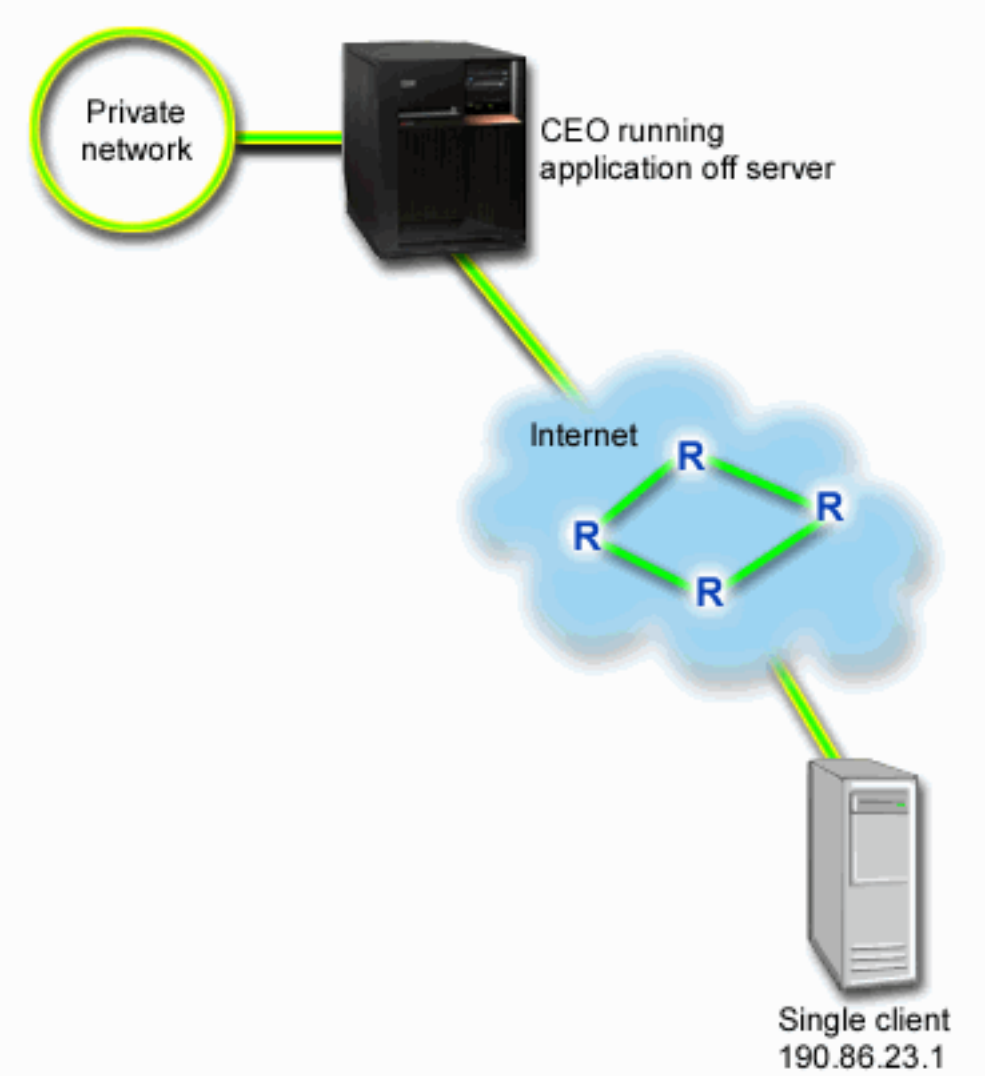


Abbildung 8. Garantierte Präsentation des Geschäftsführers für den Kunden durch Richtlinie für integrierte Services

Zielsetzungen

Da die von Ihrem Geschäftsführer verwendete Anwendung eine problemlose und ununterbrochene Übertragung erforderlich macht, beschließen Sie, eine Richtlinie für integrierte Services des Typs ″Garantiert″ zu verwenden. Ein Service des Typs ″Garantiert″ steuert die maximale Verzögerung für die Warteschlange, damit Pakete nicht über einen bestimmten Zeitraum hinaus verzögert werden.

Voraussetzungen und Annahmen

Eine Richtlinie für integrierte Services ist eine erweiterte Richtlinie, die substanzielle Ressourcen erfordern kann. Richtlinien für integrierte Services setzen Folgendes voraus:

- **RSVP-fähige Anwendungen**

  Da Ihr System nicht über RSVP-fähige Anwendungen verfügt, müssen Sie eigene RSVP-fähige Anwendungen schreiben. Zum Schreiben von eigenen Anwendungen verwenden Sie die RAPI-API (ReSerVation Reservation Setup Protocol) oder die qtoq-Socket-APIs für QoS. Weitere Informationen finden Sie unter „APIs für QoS″ auf Seite 18. Lesen Sie dort die Angaben zu den APIs für integrierte Services.
- **RSVP-fähige Router und Systeme im Netzwerkpfad**

  QoS ist eine Lösung für Netzwerke. Auch wenn Sie sich nicht sicher sind, ob das gesamte Netzwerk RSVP-fähig ist, können Sie eine Richtlinie für integrierte Services erstellen und dann eine Markierung verwenden, um der Richtlinie eine bestimmte Priorität zuzuweisen. Die Priorität kann jedoch nicht garantiert werden.
- **Service-Level-Agreement**

  Sie haben mit Ihrem ISP (Internet Service Provider) ein Service-Level-Agreement (SLA) geschlossen, um sicherzustellen, dass die Richtlinien die angeforderte Priorität erhalten. Die QoS-Richtlinie, die Sie auf dem System erstellen, ermöglicht es, dass der (in der Richtlinie angegebene) Datenaustausch im Netzwerk eine Priorität erhält. Die QoS-Richtlinie garantiert die Priorität nicht und ist vom SLA abhängig. Tatsächlich haben Sie beim Einsatz von QoS-Richtlinien die Möglichkeit, bestimmte Servicestufen und Geschwindigkeiten zu vereinbaren.

Konfiguration

Nachdem Sie die Voraussetzungen geprüft haben, können Sie jetzt die Richtlinie für integrierte Services erstellen.

Zugehörige Konzepte

„Typen von integrierten Services″ auf Seite 10
Es gibt zwei Typen von integrierten Services: gesteuertes Laden und garantierter Service.

„Integrierte Services″ auf Seite 7
Der zweite Typ einer Richtlinie für die Bandbreite abgehender Daten, den Sie erstellen können, ist eine Richtlinie für integrierte Services. Die integrierten Services bieten IP-Anwendungen die Möglichkeit, unter Verwendung des RSVP-Protokolls (ReSerVation Protocol) und der APIs für QoS Bandbreite anzufordern und zu reservieren.

„Service-Level-Agreement″ auf Seite 55
Dieses Thema stellt einige wichtige Aspekte eines Service-Level-Agreements (SLA) heraus, die sich auf Ihre QoS-Implementierung auswirken können. QoS ist eine Lösung für Netzwerke. Um auch außerhalb Ihres privaten Netzwerks Priorität zu erhalten, benötigen Sie möglicherweise ein Service-Level-Agreement (SLA) mit Ihrem ISP (Internet Service Provider).

Zugehörige Verweise

„QoS überwachen″ auf Seite 63
Mit der QoS-Überwachung können Sie den IP-Datenaustausch auf dem System analysieren.

Szenariodetails: Richtlinie für integrierte Services erstellen

Dieses Thema enthält Informationen zum Erstellen der Richtlinie für integrierte Services auf dem System.

1. Erweitern Sie in System i Navigator ***Ihr System*** → **Netzwerk** → **IP-Richtlinien**.

2. Klicken Sie mit der rechten Maustaste auf **Quality of Service**, und wählen Sie die Option **Konfiguration** aus, um das Fenster ″Konfiguration des QoS-Servers″ zu öffnen.
3. Klicken Sie im Fenster ″Konfiguration des QoS-Servers″ mit der rechten Maustaste auf den Richtlinientyp ″IntServ″, und wählen Sie die Option **Neue Richtlinie** aus, um den Assistenten zu öffnen.
4. Lesen Sie die Angaben auf der Startseite des Assistenten, und klicken Sie auf **Weiter**, um die Seite **Name** aufzurufen.
5. Geben Sie im Feld **Name** den Wert `Geschäftsführer` an, und klicken Sie auf **Weiter**. Auf Wunsch können Sie eine Beschreibung eingeben, die den Zweck dieser Richtlinie kenntlich macht.
6. Wählen Sie auf der Seite ″Clients″ die Option **Bestimmte Adresse oder Adressen** aus, und klicken Sie auf **Neu**, um Ihren Client zu definieren.
7. Geben Sie im Fenster ″Neuer Client″ die folgenden Informationen ein:
   - **Name**: Unternehmensbereich1
   - **IP-Adresse**: 190.86.23.1
   - Klicken Sie auf **OK**, um den Client zu erstellen und zum Assistenten für integrierte Services zurückzukehren.

   Nachdem Sie auf ″OK″ geklickt haben, werden Sie zum Assistenten für Richtlinien zurückgeführt. Wenn Sie zuvor Clients erstellt haben, wählen Sie die Clients ab, und vergewissern Sie sich, dass nur relevante Clients ausgewählt sind. Wählen Sie auf der Seite ″Anwendungen″ die Einstellung **Bestimmter Port, Portbereich oder Servertyp** aus, und klicken Sie auf **Neu**.
8. Geben Sie im Fenster ″Neue Anwendung″ die folgenden Informationen ein, und klicken Sie auf **OK**, um zum Assistenten zurückzukehren:
   - **Name**: IP-Telefonie
   - **Port**: 2427
9. Wählen Sie auf der Seite ″Anwendungen″ die Einstellung **Protokoll** aus, und vergewissern Sie sich, dass **TCP** ausgewählt ist. Klicken Sie auf **Weiter**.

   Anmerkung: Die Anwendung, die Sie für eine Richtlinie für integrierte Services auswählen, muss für die Verwendung der RAPI-API oder der qtoc-Socket-APIs geschrieben worden sein. Zusammen mit RSVP führen diese APIs die Reservierung für die integrierten Services im Netzwerk aus. Wenn Sie diese APIs nicht verwenden, erhält die Anwendung keine Priorität oder Garantie. Außerdem muss beachtet werden, dass diese Richtlinie Ihre Anwendungen zwar in die Lage versetzt, im Netzwerk eine Priorität zu erhalten, dies jedoch nicht garantieren kann. Alle Router und Server im Pfad des Datenaustausches müssen ebenfalls RSVP verwenden, damit eine Reservierung garantiert werden kann. Eine durchgängige Reservierung ist von der Teilnahme im gesamten Netzwerk abhängig.
10. Übernehmen Sie auf der Seite ″Lokale IP-Adresse″ den Standardwert **Alle IP-Adressen**.
11. Wählen Sie auf der Seite ″Typ der integrierten Services″ die Einstellung **Garantiert** aus, und klicken Sie auf **Weiter**.
12. Wählen Sie auf der Seite ″Markierung für integrierte Services″ die Einstellung **Nein, kein Pro-Hop-Verhalten zuordnen** aus, und klicken Sie auf **Weiter**.
13. Geben Sie auf der Seite ″Leistungsgrenzen für integrierte Services″ die folgenden Informationen ein, und klicken Sie auf **Weiter**:
   - **Maximale Anzahl Datenflüsse**: 1
   - **Grenzwert für kumulative Bandbreite (R)**: Keine Begrenzung
   - **Größe des Token-Puffers**: 100 Kilobit
   - **Grenzwerkt für Bandbreite (R)**: 16 Megabit pro Sekunde
14. Wählen Sie auf der Seite ″Zeitplan″ die Einstellung **Aktiv während des ausgewählten Zeitplans** aus, und klicken Sie auf **Neu**.

15. Geben Sie auf der Seite ″Neuen Zeitplan hinzufügen″ die folgenden Informationen ein, und klicken Sie auf **OK**:
    - **Name**: Einstündig
    - **Tageszeit**: Zu bestimmten Zeiten aktiv (fügen Sie 13.00 Uhr bis 14.00 Uhr hinzu)
    - **Wochentag**: An bestimmten Tagen aktiv (wählen Sie Montag aus)
16. Klicken Sie auf der Seite ″Zeitplan″ auf **Weiter**.
17. Prüfen Sie die Übersichtsdaten. Wenn die Daten den gewünschten Einstellungen entsprechen, klicken Sie auf **Fertig stellen**, um die Richtlinie zu erstellen. Das Hauptfenster ″Konfiguration des QoS-Servers″ enthält eine Liste mit allen auf dem Server erstellten Richtlinien. Nachdem Sie den Assistenten beendet haben, wird die Richtlinie im rechten Fensterbereich angezeigt.

Die Konfiguration der Richtlinie für integrierte Services auf dem System ist beendet. Als Nächstes müssen Sie den Server starten oder aktualisieren.

Szenariodetails: QoS-Server starten oder aktualisieren

Dieses Thema enthält Informationen zum Starten bzw. Aktualisieren des QoS-Servers.

Wählen Sie im Fenster ″Konfiguration des QoS-Servers″ die Optionen **Server → Starten** oder **Server → Aktualisieren** aus.

Szenariodetails: Prüfen, ob die Richtlinie funktioniert

Dieses Thema enthält Information darüber, wie Sie mit der Überwachung prüfen, ob die Richtlinie das konfigurierte Verhalten aufweist.

1. Wählen Sie im Fenster ″Konfiguration des QoS-Servers″ die Optionen **Server → Überwachen** aus. Das Fenster ″QoS-Überwachung″ wird aufgerufen.
2. Wählen Sie den Ordner zum Richtlinientyp für integrierte Services aus. In diesem Ordner werden alle Richtlinien für integrierte Services angezeigt.

   Die wichtigsten Felder in diesem Zusammenhang sind die Felder für Messwerte, die ihre Daten aus dem Datenaustausch erhalten. Achten Sie besonders auf die Angaben in den Feldern ″Bits insgesamt″, ″Bits gemäß Profildefinition″ und ″Pakete gemäß Profildefinition″. Der Wert für ″Von Profildefinition abweichende Bits″ macht kenntlich, dass anderer Datenaustausch verzögert oder gelöscht wird, um die Anforderungen dieser Richtlinie für integrierte Services zu erfüllen. Eine Beschreibung aller Felder in der Überwachung finden Sie unter „QoS überwachen” auf Seite 63.

   Anmerkung: Denken Sie daran, dass die Ergebnisse genau sind, wenn die Richtlinie aktiv ist. Prüfen Sie in diesem Zusammenhang den Zeitplan, der in der Richtlinie angegeben ist. Außerdem zeigt die Überwachung die Richtlinien für integrierte Services nur nach der Ausführung der Anwendungen an. Eine RSVP-Reservierung muss vor der Überwachung eingerichtet werden.

Szenariodetails: Eigenschaften ändern

Nachdem Sie die Ergebnisse der Überwachung geprüft haben, können Sie die Eigenschaften der Richtlinie ändern, um die erwarteten Ergebnisse zu erzielen.

1. Wählen Sie im Fenster ″Konfiguration des QoS-Servers″ den Ordner **IntServ** aus. Klicken Sie mit der rechten Maustaste in der Liste des rechten Fensterbereiches auf **Geschäftsführer**, und wählen Sie die Option **Eigenschaften** aus, um die Richtlinie zu bearbeiten. Daraufhin wird ein Fenster ″Eigenschaften″ angezeigt. Es enthält die Werte, die die gesamte Richtlinie steuern.
2. Geben Sie die entsprechenden Werte an.
3. Wählen Sie im Fenster ″Konfiguration des QoS-Servers″ die Optionen **Server → Aktualisieren** aus, um die Änderungen zu übernehmen.

Szenario: Aktuelle Netzwerkstatistik überwachen

Sie müssen die Leistungsgrenzwerte, die auf einzelnen Netzwerkvoraussetzungen basieren, innerhalb der Assistenten festlegen.

Zielsetzungen

Um diese Grenzwerte festlegen zu können, müssen Sie die aktuelle Leistungsfähigkeit des Netzwerkes kennen. Da Sie QoS-Richtlinien definieren wollen, haben Sie wahrscheinlich bereits eine genaue Vorstellung von den aktuellen Anforderungen an Ihr Netzwerk. Zur Bestimmung der exakten Grenzwerte für die Geschwindigkeit (z. B. Geschwindigkeit des Tokenpuffers) ist es sinnvoll, den gesamten Datenaustausch auf dem System zu überwachen. Auf diese Weise können Sie besser ermitteln, welche Grenzwerte für die Geschwindigkeit festgelegt werden sollten.

Lösung

Erstellen Sie eine sehr weit gefasste Richtlinie für differenzierte Services, die keine Einschränkungen (also keine Maximalwerte) enthält und auf alle Schnittstellen sowie alle IP-Adressen angewendet wird. Zeichnen Sie mit der QoS-Überwachung Daten über diese Richtlinie auf.

Zugehörige Konzepte

„Grenzwerte für Token-Puffer und Bandbreite" auf Seite 11
Grenzwerte für Token-Puffer und Bandbreite werden unter dem Begriff "Leistungsgrenzen" zusammengefasst. Mit solchen Leistungsgrenzen kann die Paketübermittlung in Richtlinien für die Bandbreite abgehender Daten (sowohl für integrierte Services als auch für differenzierte Services) garantiert werden.

„Grenzwerte für Durchschnittsverbindungsgeschwindigkeit und Burstrate" auf Seite 18
Grenzwerte für die Verbindungsgeschwindigkeit und die Burstrate sind Grenzwerte. Diese Grenzwerte für die Geschwindigkeit ermöglichen die Begrenzung von eingehenden Verbindungen, die auf dem System eintreffen. Grenzwerte für Geschwindigkeiten werden in einer Serviceklasse festgelegt, die zusammen mit Richtlinien für ankommende Daten verwendet wird.

Zugehörige Verweise

„QoS überwachen" auf Seite 63
Mit der QoS-Überwachung können Sie den IP-Datenaustausch auf dem System analysieren.

Szenariodetails: QoS in System i Navigator öffnen

Dieses Thema enthält Informationen zum Öffnen von QoS in System i Navigator.

1. Erweitern Sie in System i Navigator ***Ihr System*** → **Netzwerk** → **IP-Richtlinien**.
2. Klicken Sie mit der rechten Maustaste auf **Quality of Service**, und wählen Sie die Option **Konfiguration** aus.
3. Erweitern Sie **Richtlinien für Bandbreite abgehender Daten**.
4. Klicken Sie mit der rechten Maustaste auf **DiffServ**, und wählen Sie die Option **Neue Richtlinie** aus. Der Assistent für neue DiffServ-Richtlinie wird aufgerufen.

Szenariodetails: Richtlinie für differenzierte Services erstellen

Da Sie einen Großteil des Datenaustausches erfassen wollen, der in Ihrem Netzwerk eintrifft, könnten Sie die Richtlinie "Netzwerk" benennen. Verwenden Sie alle IP-Adressen, alle Ports, alle lokalen IP-Adressen und alle Zeiten (sofern anwendbar).

Verwenden Sie im Assistenten die folgenden Einstellungen:

```
Name: Netzwerk (Sie können jeden beliebigen Namen zuordnen)
Client: Alle IP-Adressen
Anwendung: Alle Ports
Protokoll: Alle Protokolle
Zeitplan: Alle Zeiten
```

System i Navigator listet alle Richtlinien für differenzierte Services auf, die auf Ihrem System erstellt wurden.

Szenariodetails: Neue Serviceklasse erstellen

Beim Durcharbeiten des Assistenten werden Sie aufgefordert, ein Pro-Hop-Verhalten, Leistungsgrenzwerte sowie eine Behandlung für den Datenaustausch anzugeben, der von der Profildefinition abweicht. Alle diese Angaben werden in einer Serviceklasse definiert. Wählen Sie extrem hohe Werte aus, um einen möglichst großen Teil des Datenflusses zuzulassen.

Serviceklassen bestimmen eigentlich die Leistungsstufen, die dieser Datenaustausch von einem Router erhält. Sie könnten Ihre Serviceklasse beispielsweise mit "Unbegrenzt" benennen und auf diese Weise kenntlich machen, dass dieser Datenaustausch einen höheren Service erhält. System i Navigator listet alle Serviceklassen auf, die auf Ihrem System erstellt wurden.

Szenariodetails: Richtlinie überwachen

Sie können mit der Überwachung prüfen, ob der Datenverkehr das in der Richtlinie konfigurierte Verhalten aufweist.

1. Wählen Sie den spezifischen Ordner für Richtlinien aus ("DiffServ", "IntServ" oder "Ankommende Daten").
2. Klicken Sie mit der rechten Maustaste auf die Richtlinie, die Sie überwachen wollen, und wählen Sie die Option **Überwachen** aus.

Die folgende Liste enthält die möglichen Ausgabedaten der Überwachung für die oben definierte Richtlinie.

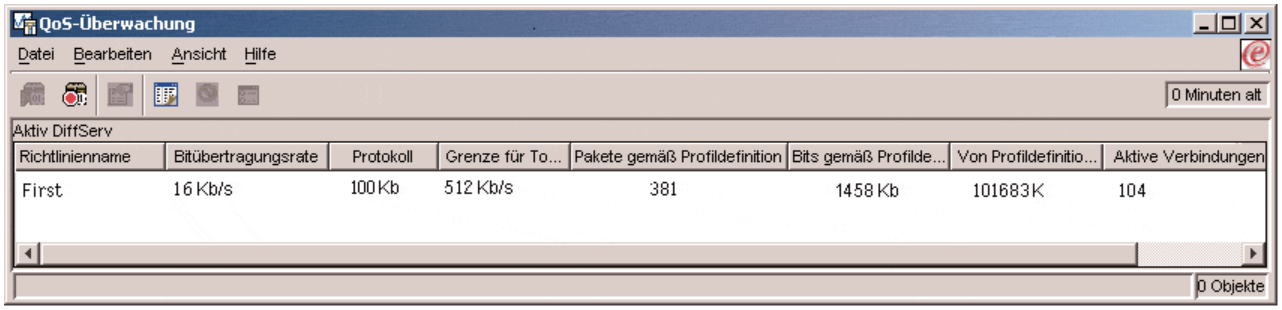


Abbildung 9. QoS-Überwachung

Suchen Sie nach den Feldern, die ihre Daten aus dem Datenaustausch erhalten. Achten Sie besonders auf die Angaben in den Feldern "Bits insgesamt", "Bits gemäß Profildefinition", "Pakete gemäß Profildefinition" und "Von Profildefinition abweichende Bits". Das Feld "Von Profildefinition abweichende Bits" signalisiert, ob der Datenaustausch die konfigurierten Richtlinienwerte überschreitet. In einer Richtlinie für differenzierte Services gibt die Anzahl für die Abweichung von der Profildefinition die Anzahl der gelöschten Byte an. Die Anzahl der Pakete gemäß Profildefinition gibt an, wie viele Byte durch diese Richtlinie gesteuert werden (von dem Zeitpunkt, an dem das Paket gestartet wurde, bis zur aktuellen Ausgabe der Überwachung).

Auch die Werte, die Sie dem Feld **Grenze für Token-Durchschnittsgeschwindigkeit** zuordnen, sind von Bedeutung. Sobald Pakete diesen Grenzwert überschreiten, beginnt das System mit dem Löschen der Pakete. Infolgedessen steigt der Wert für "Von Profildefinition abweichende Bits" an. Dies zeigt, dass die Richtlinie das gewünschte und konfigurierte Verhalten aufweist. Um den Wert für die von der Profildefinition abweichenden Bit zu ändern, müssen Sie lediglich die Leistungsgrenzwerte anpassen. Eine Beschreibung aller Felder in der Überwachung finden Sie unter „QoS überwachen" auf Seite 63.

Szenariodetails: Werte ändern

Nach der Überwachung können Sie jeden Wert, den Sie vorher ausgewählt hatten, ändern. Klicken Sie mit der rechten Maustaste auf den Namen der Serviceklasse, die Sie in dieser Richtlinie erstellt haben. Bei Auswahl von **Eigenschaften** wird ein Fenster mit den Eigenschaften für QoS angezeigt. Es enthält die Werte, die den Datenaustausch steuern.

Szenariodetails: Richtlinie erneut überwachen

Nach dem Anzeigen der Ergebnisse müssen Sie mit unterschiedlichen Werten experimentieren, um die besten Grenzwerte für Ihre Netzwerkumgebung herauszufinden.

QoS planen

Die Planung ist der wichtigste Schritt bei der Umsetzung von QoS. Um die gewünschten Ergebnisse erzielen zu können, müssen Sie Ihre Netzwerkeinheiten prüfen und den Datenaustausch im Netzwerk überwachen.

Dieses Thema enthält außerdem eine Advisorfunktion für die Planung. Die Advisorfunktion für die QoS-Planung führt Sie durch die grundlegenden Fragen, die Sie während der Planungsphase beantworten müssen. Neben der Advisorfunktion sollten Sie die folgenden Unterthemen lesen, bevor Sie QoS konfigurieren.

Netzwerkleistung bewerten

QoS wird immer im Hinblick auf die Netzwerkleistung eingesetzt. Die Hauptursache für die Verwendung von QoS besteht wahrscheinlich darin, dass bereits Netzwerküberlastungen und Paketverluste aufgetreten sind. Bevor Sie Ihre Richtlinien ausführen, empfiehlt es sich unter Umständen, die aktuellen Leistungsdaten des IP-Datenaustausches mit der QoS-Überwachung zu prüfen. Anhand der Ergebnisse können Sie feststellen, wo Engpässe vorhanden sind.

Zugehörige Konzepte

„Systemtransaktionen überwachen" auf Seite 71
Mit der QoS-Überwachung können Sie überprüfen, ob die QoS-Richtlinien die gewünschte Wirkung haben. Die QoS-Überwachung hilft Ihnen in der Planungsphase und bei der Fehlerbehebung für QoS.

„QoS konfigurieren" auf Seite 57
Nach der Planung von QoS erstellen Sie Ihre QoS-Richtlinien mit den Assistenten von System i Navigator. In diesem Thema wird beschrieben, wie Sie Richtlinien für differenzierte Services, Richtlinien für integrierte Services und Richtlinien für ankommende Daten erstellen.

Erforderliche Berechtigungen

QoS-Richtlinien enthalten unter Umständen schutzwürdige Informationen über Ihr Netzwerk. Daher darf die Berechtigung für die QoS-Verwaltung nur dann erteilt werden, wenn dies erforderlich ist.

Die folgenden Berechtigungen werden benötigt, damit QoS-Richtlinien und optional LDAP-Directory-Server (LDAP - Lightweight Directory Access Protocol) konfiguriert werden können.

Berechtigungen für die Verwaltung des Directory-Servers erteilen

Der QoS-Administrator benötigt die Berechtigungen `*ALLOBJ` und `*IOSYSCFG`. Informationen zu alternativen Berechtigungen finden Sie unter Directory-Server konfigurieren.

Berechtigung für das Starten des TCP/IP-Servers erteilen

So erteilen Sie eine Objektberechtigung für die Befehle STRTCPSVR (TCP/IP-Server starten) und ENDTCPSVR (TCP/IP-Server beenden):

1. **STRTCPSVR**: Geben Sie in der Befehlszeile den Befehl GRTOBJAUT OBJ (QSYS/STRTCPSVR) OBJTYPE (*CMD) USER (ADMINPROFILE) AUT (*USE) ein. Ersetzen Sie hierbei ADMINPROFILE durch den Namen des Profils Ihres Administrators, und drücken Sie die Eingabetaste.
2. **ENDTCPSVR**: Geben Sie in der Befehlszeile den Befehl GRTOBJAUT OBJ (QSYS/ENDTCPSVR) OBJTYPE (*CMD) USER (ADMINPROFILE) AUT (*USE) ein. Ersetzen Sie hierbei ADMINPROFILE durch den Namen des Profils Ihres Administrators, und drücken Sie die Eingabetaste.

Berechtigung für den Zugriff auf alle Objekte und die Systemkonfiguration erteilen

Für Benutzer, die QoS konfigurieren, empfiehlt sich die Berechtigung eines Sicherheitsbeauftragten. So erteilen Sie die Berechtigung für den Zugriff auf alle Objekte und für die Systemkonfiguration:

1. Erweitern Sie in System i Navigator *Ihr System* → **Benutzer und Gruppen**.
2. Doppelklicken Sie auf **Alle Benutzer**.
3. Klicken Sie mit der rechten Maustaste auf das Benutzerprofil des Administrators, und wählen Sie **Eigenschaften** aus.
4. Klicken Sie im Fenster ″Eigenschaften″ auf **Leistungsspektrum**.
5. Wählen Sie auf der Seite ″Leistungsspektrum″ die Option für **Zugriff auf alle Objekte und Systemkonfiguration** aus.
6. Klicken Sie auf **OK**, um die Seite ″Leistungsspektrum″ zu schließen.
7. Klicken Sie auf **OK**, um das Fenster ″Eigenschaften″ zu schließen.

Systemvoraussetzungen

QoS ist ein integrierter Bestandteil des Betriebssystems.

Die folgenden Voraussetzungen müssen erfüllt werden:

1. Das Programm IBM TCP/IP Connectivity Utilities for i5/OS (5761-TC1) muss installiert sein.
2. Auf dem PC muss System i Navigator installiert sein. Achten Sie darauf, dass die Komponente ″Netzwerk″ während der Installation von System i Access installiert wird. QoS finden Sie im Ordner ″Netzwerk″ unter ″IP-Richtlinien″.

   Zugehörige Konzepte

   System i Navigator - Einführung

   Zugehörige Verweise

   „Referenzinformationen zu QoS″ auf Seite 75
   RFCs (Request for Comments) für QoS, IBM Redbooks und andere Themensammlungen im Information Center enthalten Informationen, die sich auf die QoS-Themensammlung beziehen. Sie können alle PDF-Dateien anzeigen oder drucken.

Service-Level-Agreement

Dieses Thema stellt einige wichtige Aspekte eines Service-Level-Agreements (SLA) heraus, die sich auf Ihre QoS-Implementierung auswirken können. QoS ist eine Lösung für Netzwerke. Um auch außerhalb Ihres privaten Netzwerks Priorität zu erhalten, benötigen Sie möglicherweise ein Service-Level-Agreement (SLA) mit Ihrem ISP (Internet Service Provider).

Situationen für den Bedarf eines SLA

Sie benötigen ein SLA, wenn Ihre Richtlinie auch außerhalb Ihres privaten Netzwerks eine Priorität erhalten müssen. Falls Sie Richtlinien für abgehende Daten einsetzen, um den Datenaustausch zu steuern, der Ihr System verlässt, ist eine Servicegarantie nicht erforderlich. Beispielsweise können Sie auf dem System eine Richtlinie erstellen, die einer Anwendung eine höhere Priorität als einer anderen Anwendung erteilt. Ihr System erkennt diese Priorität, aber außerhalb des Systems wird die Priorität möglicherweise nicht erkannt. Falls Sie ein privates Netzwerk verwenden und Ihre Router so konfigurieren, dass Codepunkt-

markierungen erkannt werden (mit diesen Markierungen wird Richtlinien für abgehende Daten eine Servicestufe zugeordnet), räumen die Router die Priorität im privaten Netzwerk ein. Wenn der Datenaustausch jedoch das private Netzwerk verlässt, können keine Garantien gegeben werden. Ohne ein SLA sind Sie nicht in der Lage, die Behandlung des Datenaustausches durch die Netzwerkhardware zu steuern. Außerhalb Ihres privaten Netzwerks benötigen Sie ein SLA, um die Priorität für eine Serviceklasse oder eine Ressourcenreservierung garantieren zu können.

Gründe für den Bedarf eines SLA

Ihre Richtlinien und Reservierungen sind immer nur so gut wie die schwächste Verbindung. Dies bedeutet, dass QoS-Richtlinien die Anwendungen in die Lage versetzen, im Netzwerk eine Priorität zu erhalten. Wenn einer der Knoten zwischen dem Client und dem Server jedoch keines der Merkmale für die Behandlung des Datenaustausches verwenden kann, die in den Abschnitten zu den differenzierten Services bzw. den integrierten Services beschrieben sind, werden Ihre Richtlinien nicht wie von Ihnen beabsichtigt verarbeitet. Falls Ihr SLA Ihnen nicht genügend Ressourcen zur Verfügung stellt, kann auch die beste Richtlinie die Überlastungsprobleme des Netzwerks nicht lösen.

Dies bezieht auch Vereinbarungen zwischen ISPs ein. Wenn die Übertragung über mehrere Domänen hinweg erfolgt, muss jeder ISP der Unterstützung von QoS-Anforderungen zustimmen. Die Interoperabilität kann in diesem Zusammenhang einige Herausforderungen mit sich bringen.

Informieren Sie sich genau über die Servicestufe, die Sie gegenwärtig erhalten. Vereinbarungen über Bedingungen für den Datenaustausch legen insbesondere fest, wie der Datenaustausch behandelt wird, ob er also gelöscht, markiert, angepasst oder erneut übertragen wird. Zu den Hauptgründen für die Bereitstellung von QoS gehören die Steuerung von Latenz, Abweichungen, Bandbreite, Paketverlusten, Verfügbarkeit und Durchsatz. Ihre Servicevereinbarungen müssen Ihren Richtlinien die angeforderten Bedingungen zur Verfügung stellen können. Überprüfen Sie, ob Sie den Service im benötigten Umfang erhalten. Falls nicht, werden Ressourcen möglicherweise vergeblich aufgewendet. Wenn Sie beispielsweise die Reservierung von 500 Kb/s für die IP-Telefonie anfordern, Ihre Anwendung jedoch nur 20 Kb/s benötigt, zahlen Sie unter Umständen zu viel, ohne von Ihrem ISP darauf hingewiesen zu werden.

Anmerkung: Bei Verwendung von QoS-Richtlinien können Sie mit Ihrem ISP Servicestufen vereinbaren, die unter Umständen die Kosten für den Netzwerkdienst reduzieren. Beispielsweise könnte Ihr ISP Ihnen einen bestimmten Gebührensatz garantieren, wenn Sie eine bestimmte vereinbarte Bandbreitenstufe nicht überschreiten. Bei der Verwendung von QoS-Richtlinien ist es ebenfalls denkbar, dass Sie tagsüber einen bestimmten Bandbreitenumfang X, nachts jedoch einen Bandbreitenumfang Y nutzen und für jeden Zeitrahmen einen Gebührensatz vereinbaren. In diesem Fall könnte der ISP bei einer Überschreitung der Bandbreite Mehrkosten in Rechnung stellen. Der ISP muss einer bestimmten Servicestufe zustimmen und die von Ihnen verwendete Bandbreite überwachen können.

Zugehörige Konzepte

„Konzepte" auf Seite 1
Bevor Sie QoS (Quality of Service - Qualität des Service) verwenden, müssen Sie die Basisterminologie erlernen und sich über die QoS-Konzepte informieren. Mit Hilfe dieser Konzepte können Sie feststellen, ob der Service Ihren Anforderungen entspricht.

„Szenario: Browserdatenaustausch begrenzen" auf Seite 32
Mit QoS können Sie das Leistungsverhalten für den Datenaustausch steuern. Durch den Einsatz einer Richtlinie für differenzierte Services können Sie die Leistung einer Anwendung in Ihrem Netzwerk entweder einschränken oder erweitern.

„Szenario: Sichere und vorhersehbare Ergebnisse (VPN und QoS)" auf Seite 36
Auch wenn Sie ein VPN (Virtual Private Network - virtuelles privates Netzwerk) verwenden, können Sie QoS-Richtlinien erstellen.

„Szenario: Vorhersehbarer B2B-Datenaustausch" auf Seite 44
Wenn Sie eine vorhersehbare Übermittlung benötigen und dennoch eine Reservierung anfordern müs-

sen, können Sie natürlich auch eine Richtlinie für integrierte Services verwenden. Dieses Beispiel verwendet einen Service des Typs ″Gesteuertes Laden″.

„Szenario: Dedizierte Übermittlung (IP-Telefonie)” auf Seite 48
Wenn Sie eine dedizierte Übermittlung benötigen und eine Reservierung anfordern wollen, verwenden Sie eine Richtlinie für integrierte Services. Sie können zwei unterschiedliche Typen von Richtlinien für integrierte Services erstellen, nämlich ″Garantiert″ und ″Gesteuertes Laden″. In diesem Beispiel wird ein Service des Typs ″Garantiert″ verwendet.

Netzwerkhardware und -software

Das Leistungsspektrum Ihrer internen Ausstattung und der Einheiten außerhalb des Netzwerks hat beträchtliche Auswirkungen auf die QoS-Ergebnisse.

Anwendungen

Richtlinien für integrierte Services setzen Anwendungen voraus, die RSVP-fähig sind. Da die i5/OS-Anwendungen anfangs nicht RSVP-fähig sind, müssen Sie diese Anwendungen für die Verwendung von RSVP aktivieren. Zu diesem Zweck müssen Sie spezielle Programme unter Verwendung der RSVP-APIs oder der qtoc-Socket-APIs für QoS schreiben. Diese Programme ermöglichen Ihren Anwendungen die Verwendung von RSVP.

Netzwerkknoten

Router, Switches und sogar Ihre eigenen Betriebssysteme müssen in der Lage sein, QoS verwenden zu können. Damit Richtlinien für differenzierte Services eingesetzt werden können, müssen die Netzwerkeinheiten DiffServ-fähig sein. Dies bedeutet, dass ein Netzwerkknoten IP-Pakete klassifizieren, messen, markieren, anpassen und löschen können muss (Bedingungsfunktionen für den Datenaustausch).

Damit Richtlinien für integrierte Services eingesetzt werden können, müssen die Netzwerkeinheiten RSVP-fähig sein. Dies bedeutet, dass auch die Netzwerkknoten RSVP unterstützen müssen.

Zugehörige Konzepte

„APIs für QoS” auf Seite 18
Dieses Thema enthält Informationen über Protokolle, APIs und die Voraussetzungen für einen Router, der RSVP (ReSerVation Protocol) verwenden kann, also RSVP-fähig ist. Zu den APIs für QoS gehören die RAPI-API, die qtoq-Socket-API, die API sendmsg() und die monitor-APIs.

„Bedingungsfunktionen für den Datenaustausch” auf Seite 5
Damit QoS-Richtlinien verwendet werden können, müssen die Netzwerkeinheiten (wie beispielsweise Router und Switches) in der Lage sein, Bedingungsfunktionen für den Datenaustausch zu verarbeiten. Bedingungsfunktionen für den Datenaustausch sind Klassifizierungsfunktionen, Messfunktionen, Markierungsfunktionen, Anpassungsfunktionen und Löschfunktionen.

QoS konfigurieren

Nach der Planung von QoS erstellen Sie Ihre QoS-Richtlinien mit den Assistenten von System i Navigator. In diesem Thema wird beschrieben, wie Sie Richtlinien für differenzierte Services, Richtlinien für integrierte Services und Richtlinien für ankommende Daten erstellen.

Die Assistenten bieten eine hervorragende Führung durch den Konfigurationsprozess.

Nachdem Sie die Richtlinien konfiguriert haben, können Sie die Richtlinienkonfiguration mit Hilfe der Konfigurationsobjekte in System i Navigator bearbeiten. Die Konfigurationsobjekte sind die einzelnen Bestandteile, aus denen sich eine Richtlinie zusammensetzt. Wenn Sie die QoS-Komponente in System i Navigator öffnen, werden Ordner namens ″Clients″, ″Anwendungen″, ″Zeitpläne″, ″Richtlinien″, ″Service-

klassen", "Pro-Hop-Verhalten" und "URIs" angezeigt. Mit diesen Objekten können Sie eine Richtlinie erstellen. Ausführlichere Informationen zu den Objekten finden Sie im Hilfetext mit der Übersicht über QoS in System i Navigator.

QoS-Richtlinien aktivieren

Bevor Ihre Richtlinien wirksam werden können, müssen sie aktiviert werden. Wenn Sie die Assistenten verwenden, aktiviert das System die Richtlinien automatisch. Falls Sie jedoch eine Richtlinie ändern, die die Konfigurationsobjekte verwendet, müssen Sie das System dynamisch aktualisieren, damit die Richtlinien aktiv werden. Vor der Aktivierung sollten Sie unbedingt feststellen, ob überschneidende Richtlinien vorhanden sind, die Probleme verursachen könnten.

Zugehörige Konzepte

„QoS planen" auf Seite 54
Die Planung ist der wichtigste Schritt bei der Umsetzung von QoS. Um die gewünschten Ergebnisse erzielen zu können, müssen Sie Ihre Netzwerkeinheiten prüfen und den Datenaustausch im Netzwerk überwachen.

System i Navigator - Einführung

Zugehörige Verweise

„QoS verwalten" auf Seite 61
Mit den Prozeduren in diesem Thema können Sie vorhandene QoS-Eigenschaften und -Richtlinien verwalten.

QoS mit Assistenten konfigurieren

Zur Konfiguration von QoS-Richtlinien müssen Sie die QoS-Assistenten in System i Navigator verwenden.

Die folgende Liste enthält die einzelnen Assistenten und ihre jeweilige Funktion:

Assistent für Erstkonfiguration
Mit diesem Assistenten können Sie die systemspezifische Konfiguration sowie die Informationen zum Directory-Server definieren.

Assistent für neue IntServ-Richtlinie
Mit dem Assistenten für eine neue IntServ-Richtlinie können Sie eine Richtlinie für integrierte Services erstellen. Diese Richtlinie lässt RSVP-Anforderungen zu bzw. weist sie zurück und steuert somit indirekt die Bandbreite des Servers. Die (von Ihnen festgelegten) Leistungsgrenzen der Richtlinie bestimmen, ob das System die von der RSVP-Anwendung des Clients angeforderte Bandbreite verarbeiten kann. Um die in diesem Assistenten erstellten Richtlinien für integrierte Services auszuführen, müssen die Router und Anwendungen RSVP-fähig sein.

Anmerkung: Bevor Sie eine Richtlinie für integrierte Services definieren, müssen Sie eigene Anwendungen für die Verwendung von RSVP schreiben.

Assistent für neue DiffServ-Richtlinie
Mit diesem Assistenten können Sie TCP/IP-Datenaustausch differenzieren und ihm eine bestimmte Priorität zuweisen. Durch die Erstellung von Richtlinien können Sie Datenaustausch differenzieren. Innerhalb einer Richtlinie ordnen Sie dem abgehenden Datenaustausch bestimmte Servicestufen zu, die auf den IP-Adressen der Quelle/des Ziels, auf Ports, auf Anwendungen und sogar auf Clients basieren können. Die i5/OS-Anwendungen können Servicestufen aufgrund spezifischerer Anwendungsdaten erhalten.

Assistent für neue Serviceklasse
Mit dem Assistenten für Serviceklassen können Sie Paketmarkierungen festlegen, die durch Router und Switches innerhalb von Netzwerken verwendet werden. Außerdem können Sie mit die-

sem Assistenten Leistungsgrenzen für den Datenaustausch festlegen, der Ihr Netzwerk verlässt. Sie verwenden Serviceklassen in Richtlinien für differenzierte Services sowie in Richtlinien für ankommende Daten.

Assistent für neue Richtlinie für ankommende Daten
Mit dem Assistenten für Richtlinien für ankommende Daten können Sie die zu Ihrem System hergestellten Verbindungen einschränken. Sie können den Zugriff nach TCP/IP-Adressen, nach Anwendung, nach der lokalen Schnittstelle oder nach einem URI (Uniform-Resource-Identifier) einschränken. Auf diese Weise kann ein Systemadministrator den Zugriff auf Ihr System durch bestimmte Clients und bestimmte Serveranwendungen steuern. Außerdem kann die Systemleistung verbessert werden.

Anmerkung: Bevor Sie eine Richtlinie für ankommende Daten definieren, die URIs verwendet, müssen Sie sicherstellen, dass der dem URI zugeordnete Anwendungsport der Anweisung "listen" (= Empfangsbereit) entspricht, die für FRCA (Fast Response Cache Accelerator) in der Konfiguration des Apache-Webservers aktiviert ist.

Nachdem Sie entschieden haben, welchen Richtlinientyp Sie erstellen wollen, können Sie die Richtlinie mit dem entsprechenden Assistenten aus der oben angegebenen Liste konfigurieren.

In System i Navigator auf QoS-Assistenten zugreifen

Mit den folgenden Schritten können Sie auf die QoS-Assistenten zugreifen und in System i Navigator eine neue Richtlinie erstellen.

So können Sie auf die QoS-Assistenten zugreifen und eine neue Richtlinie erstellen:

1. Erweitern Sie in System i Navigator *Ihr System* → **Netzwerk** → **IP-Richtlinien**.
2. Klicken Sie mit der rechten Maustaste auf **Quality of Service**, und klicken Sie auf **Konfiguration**.

   Anmerkung: In den folgenden Situationen wird der Assistent für die Erstkonfiguration geöffnet:
   - Sie verwenden die QoS-GUI (Graphical User Interface - grafische Benutzerschnittstelle) auf diesem System zum ersten Mal.
   - Sie möchten alle Daten früherer Konfigurationen manuell entfernen und ganz neu erstellen. In diesem Fall wird der Assistent für die Erstkonfiguration nur dann aufgerufen, wenn die QoS-Schnittstelle bereits geöffnet ist.
3. Arbeiten Sie die Schritte im Assistenten für die Erstkonfiguration durch. Falls der Assistent für die Erstkonfiguration nicht geöffnet wird, fahren Sie mit Schritt 4 fort.
4. Wählen Sie **Richtlinien** aus. Klicken Sie mit der rechten Maustaste entweder auf **IntServ**, auf **DiffServ** oder auf **Ankommende Daten**.
5. Wählen Sie die Option **Neue Richtlinie** aus.

Zugehörige Konzepte

„APIs für QoS" auf Seite 18
Dieses Thema enthält Informationen über Protokolle, APIs und die Voraussetzungen für einen Router, der RSVP (ReSerVation Protocol) verwenden kann, also RSVP-fähig ist. Zu den APIs für QoS gehören die RAPI-API, die qtoq-Socket-API, die API sendmsg() und die monitor-APIs.

„Differenzierte Services" auf Seite 2
Dies ist der erste Typ einer Richtlinie für die Bandbreite abgehender Daten, den Sie auf dem Betriebssystem erstellen können. Die differenzierten Services unterteilen den Datenaustausch im Netzwerk in unterschiedliche Klassen. Wenn Sie eine Richtlinie für differenzierte Services einsetzen wollen, müssen Sie festlegen, wie der Datenaustausch im Netzwerk klassifiziert werden soll und wie die unterschiedlichen Klassen zu behandeln sind.

Zugehörige Informationen

Adressen und Ports für den HTTP-Server (auf Apache-Basis) verwalten

Directory-Server konfigurieren

QoS-Richtlinienkonfigurationen können auf einen LDAP-Directory-Server (LDAP - Lightweight Directory Access Protocol) exportiert werden, was eine einfachere Verwaltung Ihrer QoS-Lösung zur Folge hat.

Statt auf allen Systemen QoS-Richtlinien zu konfigurieren, können Sie die Konfigurationsdaten auf einem lokalen Directory-Server speichern und sie von vielen Systemen gemeinsam benutzen lassen. Wenn Sie QoS zum ersten Mal auf dem System konfigurieren, wird der Assistent für die Erstkonfiguration aufgerufen. Dieser Assistent fordert Sie auf, einen Directory-Server zu konfigurieren.

Zur Konfiguration des Directory-Servers müssen Sie Folgendes festlegen oder wissen:

- Sie müssen den Namen des Directory-Servers kennen.
- Bestimmen Sie einen registrierten Namen, auf den die QoS-Richtlinien verweisen können.
- Legen Sie fest, ob die SSL-Sicherheit (SSL - Secure Sockets Layer) mit dem LDAP-Directory-Server verwendet werden soll.
- Bestimmen Sie, ob die Suchen nach Ihren Richtlinien auf dem Directory-Server mit Hilfe von Schlüsselwörtern optimiert werden soll.

Anmerkung: Für den Zugriff des QoS-Servers auf das Verzeichnis kann Kerberos gegenwärtig nicht als Authentifizierungsmethode konfiguriert werden.

Zur Verwaltung des LDAP-Directory-Servers benötigen Sie eine der folgenden Berechtigungskombinationen:

- Berechtigungen *ALLOBJ und *IOSYSCFG
- Berechtigung *JOBCTL und Objektberechtigung für die Befehle ENDTCP (TCP/IP beenden), STRTCP (TCP/IP starten), STRTCPSVR (TCP/IP-Server starten) und ENDTCPSVR (TCP/IP-Server beenden)
- Berechtigung *AUDIT für die Konfiguration des i5/OS-Sicherheitsprotokolls

Wenn Sie mit System i Navigator arbeiten, können Sie bereits auf das QoS-Standardschema zugreifen. Die tatsächliche Schemadatei ist auf dem System im Verzeichnis `/QIBM/UserData/OS400/DirSrv` gespeichert. Falls Sie jedoch einen anderen Editor als System i Navigator verwenden, müssen Sie die im folgenden Abschnitt beschriebene LDIF-Datei (LDIF - LDAP Data Interchange Format) importieren. Sie können diese Datei außerdem importieren, wenn Sie nach der Bearbeitung die ursprüngliche Standarddatei erneut laden wollen.

QoS-Schema

Es gibt eine Gruppe von Regeln (ein so genanntes *Schema*), mit dem angegeben wird, welche Typen von LDAP-Objekten für den QoS-Server gültig sind. Das Schema enthält die erforderlichen Regeln für QoS. Falls es sich bei dem LDAP-Server nicht um eine System i-Plattform handelt, müssen diese Regeln auf dem LDAP-Server importiert werden. Dies erfolgt mit einer LDIF-Datei (LDAP Data Interchange Format - LDAP-Datenaustauschformat). Die LDIF-Datei können Sie auf der Webseite für LDAP herunterladen. Sie finden diese Datei im linken Teilfenster unter **Kategorien → TCP/IP-Richtlinien**.

Zugehörige Konzepte

„Directory-Server" auf Seite 28
Sie können Ihre Richtlinien auf einen Directory-Server exportieren. Dieses Thema beschreibt die Konzepte und die Konfiguration von LDAP (Lightweight Directory Access Protocol) sowie das QoS-Schema.

„Registrierter Name" auf Seite 30
Wenn Sie einen Teil Ihres Verzeichnisses verwalten wollen, verwenden Sie hierzu entweder einen registrierten Namen oder (bei Auswahl) ein Schlüsselwort.

IBM Tivoli Directory Server for i5/OS (LDAP)

Enabling SSL and Transport Layer Security on the Directory Server

„Schlüsselwörter" auf Seite 29
Wenn Sie Ihren Directory-Server konfigurieren, müssen Sie festlegen, ob jeder QoS-Konfiguration Schlüsselwörter zugeordnet werden sollen.

Zugehörige Informationen

IBM LDAP Directory Schema

QoS-Richtlinien anordnen

Die physische Reihenfolge der Richtlinien in System i Navigator ist immer dann wichtig, wenn sich zwei Richtlinien überschneiden.

Überschneidende Richtlinie verwenden dieselben Werte für Client, Anwendung, Zeitplan, lokale IP-Adresse, URI, Serverdaten, Codepunkt oder Protokoll. Die Richtlinien werden in System i Navigator als geordnete Liste angezeigt. Die Vorrangstellung der Richtlinien richtet sich nach der Reihenfolge der Richtlinien in dieser Liste. Wenn eine Richtlinie gegenüber einer anderen Richtlinie Priorität haben soll, muss die Richtlinie mit der höheren Priorität zuerst in der Liste erscheinen.

So ermitteln Sie, ob sich eine Richtlinie mit einer anderen Richtlinie überschneidet:

1. Erweitern Sie in System i Navigator *Ihr System* → **Netzwerk** → **IP-Richtlinien**.
2. Klicken Sie mit der rechten Maustaste auf **Quality of Service**.
3. Wählen Sie die Option **Konfiguration** aus.
4. Wählen Sie den Ordner für spezifische Richtlinien aus.
5. Klicken Sie mit der rechten Maustaste auf den Namen der Richtlinie, der überschneidende Richtlinien zugeordnet sind. Vor überschneidenden Richtlinien wird ein Symbol angezeigt, das auf diese Tatsache hinweist.
6. Wählen Sie die Option **Überschneidung anzeigen** aus. Das Fenster "Richtlinienüberschneidung" wird aufgerufen.

So können Sie die Reihenfolge der Richtlinien in der Anzeige ändern:

- Heben Sie die Richtlinie hervor, und ändern Sie ihre Position in der Liste mit dem Aufwärts- bzw. Abwärtspfeil im Fenster.
- Klicken Sie mit der rechten Maustaste auf den Namen der Richtlinie, und wählen Sie die Option **Nach oben** oder **Nach unten** aus.
- Aktualisieren Sie den QoS-Server. Hierzu können Sie die Schaltfläche **Server aktualisieren** in der Symbolleiste verwenden. Ausführlichere Anweisungen finden Sie in der QoS-Taskhilfe.

  Zugehörige Konzepte

  „Vorhandene Richtlinie kopieren" auf Seite 63
  Statt alle Richtlinien jeweils ganz neu zu erstellen, können Sie die Originalrichtlinie kopieren und dann die Abschnitte der Richtlinie bearbeiten, die vom Original abweichen.

  „Qos-Fehler beheben" auf Seite 68
  Für die Behebung von QoS-Fehlern bietet QoS mehrere Methoden.

  Zugehörige Tasks

  „Zugriff auf die QoS-Hilfe in System i Navigator" auf Seite 62
  Mit System i Navigator können Sie auf die QoS-Hilfe zugreifen.

QoS verwalten

Mit den Prozeduren in diesem Thema können Sie vorhandene QoS-Eigenschaften und -Richtlinien verwalten.

Die Themen erläutern, wo Sie die eigentlichen Tasks zum Bearbeiten, Aktivieren, Anzeigen und Verwenden weiterer Methoden zur Richtlinienverwaltung finden. Außerdem wird der Einsatz der QoS-Überwachung und die Funktion zur Datenerfassung erklärt, mit der Sie den IP-Datenaustausch über das System analysieren können.

Zugehörige Konzepte

„QoS konfigurieren" auf Seite 57
Nach der Planung von QoS erstellen Sie Ihre QoS-Richtlinien mit den Assistenten von System i Navigator. In diesem Thema wird beschrieben, wie Sie Richtlinien für differenzierte Services, Richtlinien für integrierte Services und Richtlinien für ankommende Daten erstellen.

Zugriff auf die QoS-Hilfe in System i Navigator

Mit System i Navigator können Sie auf die QoS-Hilfe zugreifen.

1. Erweitern Sie in System i Navigator ***Ihr System*** → **Netzwerk** → **IP-Richtlinien**.
2. Klicken Sie mit der rechten Maustaste auf **Quality of Service**, und klicken Sie auf **Konfiguration**.
3. Klicken Sie in der Menüleiste auf **Hilfe** → **Hilfethemen**. Daraufhin wird in der Anzeige das Fenster mit der Taskhilfe geöffnet.

Zugehörige Tasks

„QoS-Richtlinien anordnen" auf Seite 61
Die physische Reihenfolge der Richtlinien in System i Navigator ist immer dann wichtig, wenn sich zwei Richtlinien überschneiden.

QoS-Richtlinien sichern

Sie sollten Ihre QoS-Richtlinie sichern, damit Sie bei einem Systemausfall oder einem Spannungsverlust die Richtlinien nicht erneut erstellen müssen.

Ihre Richtlinien können lokal gespeichert oder auf einen Directory-Server exportiert werden. Sie müssen speziell die folgenden Verzeichnisse im Integrated File System sichern: `QIBM/UserData/OS400/QOS/ETC`, `QIBM/UserData/OS400/QOS/TEMP` und `QIBM/UserData/OS400/QOS/USR`. Außerdem müssen Sie den Publishing-Agenten des Directory-Servers für den QoS-Server sichern. Der Publishing-Agent enthält den Namen des Directory-Servers, den registrierten Namen für den QoS-Server, den Port für den Zugriff auf den Directory-Server und Authentifizierungsinformationen. Im Fall eines Datenverlustes ersparen Ihnen die Sicherungen die Zeit und den Aufwand, die mit der erneuten Erstellung der Richtlinien verbunden sind. Mit den folgenden Tipps können Sie sicherstellen, dass Sie verlorene Dateien auf einfache Weise ersetzen können:

1. **Programme des Integrated File System zur Sicherung und Wiederherstellung verwenden**

   Das Handbuch *Sicherung und Wiederherstellung* enthält Anweisungen zur Ausführung von Sicherungen in einem Integrated File System.
2. **Richtlinien drucken**

   Sie können die Druckausgaben an einem möglichst sicheren Ort archivieren und die Informationen bei Bedarf erneut eingeben.
3. **Informationen auf Datenträger kopieren**

   Das Kopieren hat gegenüber dem Ausdrucken einen Vorteil: Anstelle einer erneuten Eingabe sind die Informationen in elektronischer Form vorhanden. Auf diese Weise erhalten Sie eine schnelle Methode, um Daten von einer Onlinequelle an eine andere zu transportieren.

Anmerkung: Ihr System kopiert Informationen nicht auf Diskette, sondern auf eine Systemplatte. Die Regeldateien befinden sich - ebenso wie der registrierte Name im konfigurierten Directory-Server im Verzeichnis `QIBM/UserData/OS400/QOS/ETC`, nicht auf einem PC. Es kann sinnvoll sein, eine Plattenschutzmethode als Sicherungsmethode zu verwenden, um die auf der Systemplatte gespeicherten Daten zu schützen.

Bei Verwendung eines System i-Produkts müssen Sie eine Strategie für die Sicherung und Wiederherstellung planen.

Zugehörige Informationen

Sicherung des Systems

Vorhandene Richtlinie kopieren

Statt alle Richtlinien jeweils ganz neu zu erstellen, können Sie die Originalrichtlinie kopieren und dann die Abschnitte der Richtlinie bearbeiten, die vom Original abweichen.

In System i Navigator heißt diese QoS-Funktion *Neu basierend auf*. Sie müssen System i Navigator verwenden, um auf das QoS-Fenster zugreifen zu können, in dem Sie die Richtlinie kopieren.

Die Schritte zum Kopieren einer vorhandenen Richtlinie sind im Hilfetext von System i Navigator unter **Neue Richtlinie basierend auf einer vorhandenen Richtlinie erstellen** beschrieben.

Bevor Ihre Richtlinien wirksam werden können, müssen Sie sie aktivieren, indem Sie den QoS-Server starten oder eine dynamische Aktualisierung des Servers vornehmen. Vor der Aktivierung sollten Sie unbedingt feststellen, ob überschneidende Richtlinien vorhanden sind, die Probleme verursachen könnten.

Zugehörige Tasks

„QoS-Richtlinien anordnen" auf Seite 61
Die physische Reihenfolge der Richtlinien in System i Navigator ist immer dann wichtig, wenn sich zwei Richtlinien überschneiden.

QoS-Richtlinien bearbeiten

Wenn sich die Anforderungen ändern, müssen Sie Ihre Richtlinien bearbeiten, damit weiterhin die gewünschte Leistung erzielt wird.

Vor der Aktivierung müssen Sie versuchen, alle Fehler zu beheben, und die erforderlichen Änderungen an der Richtlinie vornehmen. Dies ist die beste Methode, um Komplikationen bei den Richtlinienergebnissen zu vermeiden.

Nachdem Sie die Richtlinien konfiguriert haben, können Sie die Richtlinienkonfiguration mit Hilfe der Konfigurationsobjekte in System i Navigator bearbeiten. Die Konfigurationsobjekte sind die einzelnen Bestandteile, aus denen sich eine Richtlinie zusammensetzt. Wenn Sie die QoS-Komponente in System i Navigator öffnen, werden Ordner namens ″Clients″, ″Anwendungen″, ″Zeitpläne″, ″Richtlinien″, ″Serviceklassen″, ″Pro-Hop-Verhalten″ und ″URI″ angezeigt. Mit diesen Objekten können Sie eine Richtlinie bearbeiten.

Die Schritte für die Bearbeitung einer Richtlinie in System i Navigator sind auf der Seite ″QoS-Richtlinie bearbeiten″ von System i Navigator beschrieben.

QoS überwachen

Mit der QoS-Überwachung können Sie den IP-Datenaustausch auf dem System analysieren.

Mit der QoS-Überwachung können Sie ermitteln, an welchen Stellen im Netzwerk eine Überlastung auftritt. Dies ist nicht nur bei der QoS-Planung hilfreich, sondern kann auch als Fehlerbehebungstool eingesetzt werden. Mit der QoS-Überwachung können Sie Ihr Netzwerk weiter überwachen und Ihre Richtlinien dann bei Bedarf anpassen. Zur Überwachung aller aktiven Richtlinien wählen Sie im Fenster ″Konfiguration des QoS-Servers″ die Optionen **Server → Überwachung** aus. Wenn Sie mit der rechten Maustaste auf eine Richtlinie klicken und die Option **Überwachen** auswählen, zeigt die Überwachung ausschließlich Informationen für diese Richtlinie an.

Die Überwachung von Richtlinien können Sie folgendermaßen einsetzen:

- **Echtzeitdaten über aktive Richtlinien anzeigen**

  Wenn Sie die Überwachung öffnen, werden immer Echtzeitdaten über aktive Richtlinien angezeigt. Zu diesem Zweck ist es nicht erforderlich, eine Datenerfassung zu starten.

- **Daten für einen bestimmten Zeitraum erfassen und speichern**

  Wenn Sie Überwachungsergebnisse speichern wollen, müssen Sie eine QoS-Datenerfassung starten. Die Überwachung erfasst so lange die Daten, bis Sie die Erfassung stoppen. Die Datenerfassung wird nicht durch das Schließen des Überwachungsfensters gestoppt. Sie können auch die Eigenschaften ändern, die von der Überwachung beim Erfassen der Daten verwendet werden. Heben Sie im Fenster ″QoS-Überwachung″ den Eintrag **QoS-Überwachung** hervor, und wählen Sie die Optionen **Datei -> Eigenschaften** aus, um die Optionen zu ändern. Zusätzliche Informationen finden Sie in der Onlinehilfe.

  Falls die QoS-Datenerfassung aktiviert ist und die Eigenschaften der Überwachung geändert werden, müssen Sie die folgenden Schritte ausführen, um sicherzustellen, dass die Änderungen bei der Datenerfassung berücksichtigt werden:

  1. Stoppen Sie die QoS-Datenerfassung.
  2. Ändern Sie die Eigenschaften der Überwachung.
     a. Klicken Sie im Fenster ″Überwachung″ auf **QoS-Überwachung**.
     b. Wählen Sie die Optionen **Datei** → **Eigenschaften** aus.
     c. Ändern Sie die Eigenschaften der Überwachung, und klicken Sie auf **OK**.
  3. Aktualisieren Sie den QoS-Server.
  4. Starten Sie die QoS-Datenerfassung.

Ausgabe überwachen

Die empfangenen Ausgabeinformationen sind vom Typ der Richtlinie abhängig, die überwacht wird. Wie bereits erläutert, gibt es die folgenden Richtlinientypen: differenzierter Service, integrierter Service (Gesteuertes Laden), integrierter Service (Garantiert) und Richtlinien für ankommende Daten. Die auszuwertenden Felder variieren je nach Richtlinientyp. Am interessantesten sind die Werte, die das Ergebnis einer Messung angeben. Die folgenden Felder werden nicht definiert, sondern gemessen: Akzeptierte Anforderungen, Aktive Verbindungen, Verbindungsservices, Verbindungsgeschwindigkeiten, Gelöschte Anforderungen, Pakete gemäß Profildefinition, Bits gemäß Profildefinition, Von Profildefinition abweichende Bits, Bits insgesamt, Pakete insgesamt und Anforderungen insgesamt.

Anhand der Informationen in den genannten Feldern mit Messwerten können Sie sich ein gutes Bild davon machen, inwieweit der Datenaustausch in Ihrem Netzwerk den Richtlinien entspricht. Die nachfolgenden Beschreibungen enthalten ausführliche Informationen zu den Ausgabefeldern der Überwachung für die einzelnen Richtlinientypen. Ein Beispiel für die Verwendung der Überwachung zusammen mit den QoS-Richtlinien finden Sie unter ″QoS-Szenarien″.

Richtlinien für differenzierte Services

Tabelle 4. Richtlinien für differenzierte Services

Feld	Beschreibung
Richtlinienname	Der Name, den Sie dieser Richtlinie zugeordnet haben.
Protokoll	UDP, TCP, ALLE.
Grenze für Token-Durchschnittsgeschwindigkeit	Die Token-Durchschnittsgeschwindigkeit, die durch diese Richtlinie bei jedem Router und System im Datenflusspfad zulässig ist.
Grenze für Token-Tiefe	Die maximale Größe des Tokenpuffers, die durch diese Richtlinie bei jedem Router und System im Datenflusspfad zulässig ist.

Tabelle 4. Richtlinien für differenzierte Services (Forts.)

Feld	Beschreibung
Grenze für Token-Spitzengeschwindigkeit	Die maximale Geschwindigkeit, die bei dieser Verbindung zulässig ist.
Pakete gemäß Profildefinition	Die Anzahl der übertragenen IP-Pakete, die den Parametern in dieser Richtlinie entsprechen.
Bits gemäß Profildefinition	Die Anzahl der übertragenen Bit, die den Parametern in dieser Richtlinie entsprechen.
Von Profildefinition abweichende Bits	Die Anzahl der übertragenen Bit, die die Parameter der Richtlinie überschreiten.
Bitübertragungsrate	Die gemessene Anzahl der Bit, die bei dieser Verbindung zulässig sind.
Aktive Verbindungen	Die Gesamtzahl der aktiven Verbindungen.
Datenaustauschprofil	Der Typ der Paketbedingungsfunktionen, die für von der Profildefinition abweichende Pakete verwendet wird. Das Format kann Folgendes enthalten: • Erneutes Markieren • Anpassen • Löschen
Bits insgesamt	Die Anzahl der übertragenen Bit, die durch diese Richtlinie vom Zeitpunkt ihres Starts bis zum Zeitpunkt der Überwachungserfassung verwendet wurden.
Codepunkt gemäß Profildefinition	Falls das Paket mit einem neuen Codepunkt erneut markiert wird, ist dies der Codepunkt, den IP-Pakete verwenden, wenn sie den Parametern dieser Richtlinie entsprechen.
Von Profildefinition abweichender Codepunkt	Falls das Paket mit einem neuen Codepunkt erneut markiert wird, ist dies der Codepunkt, den IP-Pakete verwenden, wenn sie die Parametern dieser Richtlinie überschreiten.
Zieladressenbereich	Der Adressenbereich, der den Zielpunkt der (durch diese Richtlinie gesteuerten) Pakete bestimmt.
Pakete insgesamt	Die Anzahl der Pakete, die durch diese Richtlinie vom Zeitpunkt ihres Starts bis zum Zeitpunkt der Überwachungserfassung übertragen wurden.
Ausgangs-Port-Bereich	Der Ausgangs-Port-Bereich, der bestimmt, welche Anwendungen durch diese Richtlinie gesteuert werden.

Richtlinien für integrierte Services (Gesteuertes Laden)

Richtlinien für integrierte Services werden nur dann in der Überwachung angezeigt, wenn die Anwendungen aktiv sind und die Reservierungen vorgenommen wurden. Wenn Ihre Richtlinien für integrierte Services mehrere Reservierungen enthalten, werden in der Überwachung mehrere Einträge angezeigt.

Tabelle 5. Richtlinien für integrierte Services (Gesteuertes Laden)

Feld	Beschreibung
Richtlinienname	Der Name, den Sie dieser Richtlinie zugeordnet haben.
Protokoll	UDP oder TCP.
Zieladresse	Der Adressenbereich, der den Zielpunkt der (durch diese Richtlinie gesteuerten) Pakete bestimmt.

Tabelle 5. Richtlinien für integrierte Services (Gesteuertes Laden) (Forts.)

Feld	Beschreibung
Grenze für Token-Durchschnittsgeschwindigkeit	Die Token-Durchschnittsgeschwindigkeit, die durch diese Richtlinie bei jedem Router und System im Verbindungspfad zulässig ist.
Grenze für Token-Tiefe	Die maximale Größe des Tokenpuffers, die durch diese Richtlinie bei jedem Router und System im Verbindungspfad zulässig ist.
Grenze für Token-Spitzengeschwindigkeit	Die maximale Geschwindigkeit, die bei dieser Verbindung zulässig ist.
Pakete insgesamt	Die Anzahl der Pakete, die durch diese Richtlinie vom Zeitpunkt ihres Starts bis zum Zeitpunkt der Überwachungserfassung übertragen wurden.
Von Profildefinition abweichende Bits	Die Anzahl der übertragenen Bit, die die Parameter der Richtlinie überschreiten.
Bits insgesamt	Die Anzahl der übertragenen Bit, die durch diese Richtlinie vom Zeitpunkt ihres Starts bis zum Zeitpunkt der Überwachungserfassung verwendet wurden.
Bitübertragungsrate	Die gemessene Anzahl der Bit, die bei dieser Verbindung zulässig sind.
Bits gemäß Profildefinition	Die Anzahl der übertragenen Bit, die den Parametern in dieser Richtlinie entsprechen.
Maximale Paketgröße	Die maximal zulässige Paketgröße, die durch diese Richtlinie gesteuert wird.
Mindesteinheit für Richtlinie	Die Mindestanzahl von Bit, die aus dem Tokenpuffer entfernt werden. Wenn Sie als Mindesteinheit für die Richtlinie 100 Bit verwenden, werden bei 100 Bit Pakete unter 100 Bit trotzdem entfernt.
Pakete gemäß Profildefinition	Die Anzahl der übertragenen IP-Pakete, die den Parametern in dieser Richtlinie entsprechen.
Ausgangs-Port-Bereich	Der Ausgangs-Port-Bereich, der bestimmt, welche Anwendungen durch diese Richtlinie gesteuert werden.

Richtlinien für integrierte Services (Garantiert)

Richtlinien für integrierte Services werden nur dann in der Überwachung angezeigt, wenn die Anwendungen aktiv sind und die Reservierungen vorgenommen wurden. Wenn Ihre Richtlinien für integrierte Services mehrere Reservierungen enthalten, werden in der Überwachung mehrere Einträge angezeigt.

Tabelle 6. Richtlinien für integrierte Services (Garantiert)

Feld	Beschreibung
Richtlinienname	Der Name, den Sie dieser Richtlinie zugeordnet haben.
Protokoll	UDP oder TCP.
Zieladresse	Der Adressenbereich, der den Zielpunkt der (durch diese Richtlinie gesteuerten) Pakete bestimmt.
Grenze für Token-Durchschnittsgeschwindigkeit	Die maximale Tokengeschwindigkeit, die durch diese Richtlinie bei jedem Router und System im Verbindungspfad zulässig ist.
Grenze für Token-Tiefe	Die maximale Größe des Tokenpuffers, die durch diese Richtlinie bei jedem Router und System im Verbindungspfad zulässig ist.

Tabelle 6. Richtlinien für integrierte Services (Garantiert) (Forts.)

Feld	Beschreibung
Grenze für Token-Spitzengeschwindigkeit	Die maximale Geschwindigkeit, die bei dieser Verbindung zulässig ist.
Pakete insgesamt	Die Anzahl der Pakete, die durch diese Richtlinie vom Zeitpunkt ihres Starts bis zum Zeitpunkt der Überwachungserfassung übertragen wurden.
Bits insgesamt	Die Anzahl der übertragenen Bit, die durch diese Richtlinie vom Zeitpunkt ihres Starts bis zum Zeitpunkt der Überwachungserfassung verwendet wurden.
Von Profildefinition abweichende Bits	Die Anzahl der übertragenen Bit, die die Parameter der Richtlinie überschreiten.
Garantierte Geschwindigkeit	Die garantierte Geschwindigkeit in Bit pro Sekunde.
Bits gemäß Profildefinition	Die Anzahl der übertragenen Bit, die den Parametern in dieser Richtlinie entsprechen.
Maximale Paketgröße	Die maximal zulässige Paketgröße, die durch diese Richtlinie gesteuert wird.
Mindesteinheit für Richtlinie	Die Mindestanzahl von Bit, die aus dem Tokenpuffer entfernt werden. Wenn Sie als Mindesteinheit für die Richtlinie 100 Bit verwenden, werden bei 100 Bit Pakete unter 100 Bit trotzdem entfernt.
Pakete gemäß Profildefinition	Die Anzahl der übertragenen IP-Pakete, die den Parametern in dieser Richtlinie entsprechen.
Pufferdifferenz	Die Differenz (in Sekunden) zwischen der erforderlichen Verzögerung und der erhaltenen Verzögerung.
Ausgangs-Port-Bereich	Der Ausgangs-Port-Bereich, der bestimmt, welche Anwendungen durch diese Richtlinie gesteuert werden.

Richtlinien für ankommende Daten

Tabelle 7. Richtlinien für ankommende Daten

Feld	Beschreibung
Richtlinienname	Der Name, den Sie dieser Richtlinie zugeordnet haben.
Verbindungsgeschwindigkeit	Die Anzahl der akzeptierten Verbindungsanforderungen pro Sekunde.
Anforderungen insgesamt	Die Gesamtzahl der an dieses System ausgegebenen Verbindungsanforderungen.
Akzeptierte Anforderungen	Die Gesamtzahl der von diesem System akzeptierten Verbindungsanforderungen.
Gelöschte Anforderungen	Die Gesamtzahl der von diesem System gelöschten Verbindungsanforderungen.
Durchschnittsverbindungsgeschwindigkeit	Die durchschnittlich zulässige Anzahl von neuen Verbindungsanforderungen, die pro Sekunde akzeptiert werden.
Burstgrenzwert der Verbindungen	Die maximale Anzahl neuer Verbindungsanforderungen, die gleichzeitig akzeptiert werden.
Grenze für Spitzenverbindungsgeschwindigkeit	Die maximal zulässige Geschwindigkeit, in der das System Verbindungen aus dem Netzwerk akzeptiert.
Priorität	Die Priorität, die der jeweils im QoS-Manager geladenen Regel zugeordnet ist.

Tabelle 7. Richtlinien für ankommende Daten (Forts.)

Feld	Beschreibung
Warteschlangenpriorität	Die Priorität, die eingehenden Verbindungen zugeordnet ist, die in die Warteschlange für die Empfangsbereitschaft gestellt wurden.
Ziel-Port-Bereich	Der Portbereich oder Port, an den der Datenaustausch auf dem System gesendet wird.
Schnittstellenadresse	Die IP-Adresse der überwachten Systemschnittstelle.
Quellenadressenbereich	Der IP-Adressenbereich der Clients, die Anforderungen an Ihr System senden.
URI	Die Identität des URIs, auf den die Richtlinie angewendet wird.

Zugehörige Konzepte

„Szenario: Browserdatenaustausch begrenzen" auf Seite 32
Mit QoS können Sie das Leistungsverhalten für den Datenaustausch steuern. Durch den Einsatz einer Richtlinie für differenzierte Services können Sie die Leistung einer Anwendung in Ihrem Netzwerk entweder einschränken oder erweitern.

„Szenario: Sichere und vorhersehbare Ergebnisse (VPN und QoS)" auf Seite 36
Auch wenn Sie ein VPN (Virtual Private Network - virtuelles privates Netzwerk) verwenden, können Sie QoS-Richtlinien erstellen.

„Szenario: Eingehende Verbindungen begrenzen" auf Seite 40
Falls Sie die eingehenden Verbindungsanforderungen an Ihr System steuern müssen, verwenden Sie eine Richtlinie für ankommende Daten.

„Szenario: Vorhersehbarer B2B-Datenaustausch" auf Seite 44
Wenn Sie eine vorhersehbare Übermittlung benötigen und dennoch eine Reservierung anfordern müssen, können Sie natürlich auch eine Richtlinie für integrierte Services verwenden. Dieses Beispiel verwendet einen Service des Typs ″Gesteuertes Laden″.

„Szenario: Dedizierte Übermittlung (IP-Telefonie)" auf Seite 48
Wenn Sie eine dedizierte Übermittlung benötigen und eine Reservierung anfordern wollen, verwenden Sie eine Richtlinie für integrierte Services. Sie können zwei unterschiedliche Typen von Richtlinien für integrierte Services erstellen, nämlich ″Garantiert″ und ″Gesteuertes Laden″. In diesem Beispiel wird ein Service des Typs ″Garantiert″ verwendet.

„Szenarien: QoS-Richtlinien" auf Seite 32
Die Szenarien für QoS-Richtlinien in diesem Abschnitt veranschaulichen, aus welchem Grund Sie QoS benötigen und auf welche Weise Sie Richtlinien und Serviceklassen erstellen.

„Systemtransaktionen überwachen" auf Seite 71
Mit der QoS-Überwachung können Sie überprüfen, ob die QoS-Richtlinien die gewünschte Wirkung haben. Die QoS-Überwachung hilft Ihnen in der Planungsphase und bei der Fehlerbehebung für QoS.

„Szenario: Aktuelle Netzwerkstatistik überwachen" auf Seite 52
Sie müssen die Leistungsgrenzwerte, die auf einzelnen Netzwerkvoraussetzungen basieren, innerhalb der Assistenten festlegen.

Qos-Fehler beheben

Für die Behebung von QoS-Fehlern bietet QoS mehrere Methoden.

Datenübertragungstrace

Ihr System bietet einen Datenübertragungstrace, mit dem Daten auf einer Übertragungsleitung wie beispielsweise einer LAN-Schnittstelle oder einer WAN-Schnittstelle erfasst werden können. Der Durchschnittsbenutzer versteht unter Umständen nicht den gesamten Inhalt der Tracedaten. Anhand der Trace-

einträge können Sie jedoch feststellen, ob zwischen zwei Punkten tatsächlich ein Datenaustausch stattgefunden hat.

QoS auf dem System aktivieren

Falls der QoS-Server nicht gestartet wird, müssen Sie als Erstes prüfen, ob QoS auf dem System aktiviert ist. Wenn Sie Ihre Richtlinien zum ersten Mal konfigurieren, aktiviert der Assistent für die Erstkonfiguration QoS automatisch auf dem System. Wurde dieser Wert jedoch zwischenzeitlich geändert, wird der Server nicht gestartet.

So prüfen Sie, ob QoS auf dem System aktiviert ist:

1. Erweitern Sie in System i Navigator *Ihr System* → **Netzwerk** → **IP-Richtlinien**.
2. Klicken Sie mit der rechten Maustaste auf **Quality of Service**, und wählen Sie die Option **Konfiguration** aus.
3. Sobald die QoS-Schnittstelle angezeigt wird, klicken Sie mit der rechten Maustaste auf **QoS**, und wählen Sie die Option **Eigenschaften** aus.
4. Prüfen Sie auf der Seite mit den Eigenschaften für QoS, ob die Einstellung **QoS aktivieren** ausgewählt ist.

Zugehörige Konzepte

Datenübertragungstrace

Zugehörige Tasks

„QoS-Richtlinien anordnen" auf Seite 61
Die physische Reihenfolge der Richtlinien in System i Navigator ist immer dann wichtig, wenn sich zwei Richtlinien überschneiden.

QoS-Richtlinien im Journaling aufzeichnen

QoS ist mit einer Journalingfunktion ausgestattet. Mit dem Journaling können Sie QoS-Richtlinienaktionen protokollieren, wenn eine Richtlinie hinzugefügt, entfernt oder geändert wird.

Wenn Sie die Journalingfunktion aktivieren, wird ein Protokoll der Richtlinienaktionen erstellt. Dies hilft Ihnen bei der Fehlerbehebung und Detailprüfung, wenn Richtlinien nicht erwartungsgemäß funktionieren. Beispiel: Sie haben für eine Richtlinie die Ausführung von 9.00 Uhr bis 16.00 Uhr definiert. Sie können im Journalprotokoll prüfen, ob die Richtlinie tatsächlich um 9.00 Uhr hinzugefügt und um 16.00 Uhr entfernt wurde.

Bei aktiviertem Journaling werden bei jedem Hinzufügen, Entfernen oder Ändern einer Richtlinie Journaleinträge hinzugefügt. Mit Hilfe dieser Journale können Sie auf dem System eine allgemeine Datei erstellen. Anschließend können Sie anhand der Informationen, die in den Journalen Ihres Systems aufgezeichnet wurden, ermitteln, wie das System verwendet wird. Auf diese Weise können Sie einfacher entscheiden, ob bestimmte Aspekte der Richtlinien geändert werden sollten.

Die Elemente, die im Journal aufgezeichnet werden sollen, müssen sorgfältig ausgewählt werden, denn das Journaling kann eine erhebliche Belastung für Ihre Systemressourcen darstellen. Zum Starten oder Stoppen des Journalings verwenden Sie System i Navigator. Zum Anzeigen der Journalprotokolle müssen Sie die zeichenorientierte Schnittstelle verwenden.

So können Sie das Journaling starten oder stoppen:

1. Erweitern Sie in System i Navigator *Ihr System* → **Netzwerk** → **IP-Richtlinien**.
2. Klicken Sie mit der rechten Maustaste auf **Quality of Service**, und wählen Sie die Option **Konfiguration** aus.
3. Klicken Sie mit der rechten Maustaste auf **QoS**, und wählen Sie **Eigenschaften** aus.
4. Wählen Sie das Feld **Journaling ausführen** aus, um das Journaling zu aktivieren.

5. Wählen Sie das Feld ab, um das Journaling zu inaktivieren.

Anmerkung: Falls das System bereits gestartet wurde, wenn Sie die obigen Schritte ausführen, müssen Sie das System stoppen und dann erneut starten. Nachdem die Option für die Ausführung des Journalings ausgewählt wurde, gibt es zwei Möglichkeiten, um das Journaling zu aktivieren. Sie können entweder das System stoppen und erneut starten oder aber eine Systemaktualisierung ausführen. Beide Aktionen lesen die Datei "policy.conf" erneut und suchen nach dem Attribut für das Journaling.

Journaleinträge anzeigen

Dieses Thema enthält Informationen darüber, wie Sie die Journaleinträge anzeigen.

1. Geben Sie an einer Eingabeaufforderung den Befehl `DSPJRN JRN(QUSRSYS/QQOS)` ein.
2. Wählen Sie Auswahl 5 für den Journaleintrag aus, den Sie anzeigen möchten.

Journaleinträge über Ausgabedatei anzeigen

Wenn Sie die Journaleinträge in einem Ordner formatiert anzeigen wollen, rufen Sie die Datei `MODEL.OUT` im Verzeichnis `QUSRSYS` auf. Durch das Kopieren der Journaleinträge in die Ausgabedatei können Sie die Einträge mit Abfragedienstprogrammen wie Query/400 oder SQL (Structured Query Language) problemlos anzeigen. Außerdem können Sie eigene HLL-Programme (HLL - High Level Language) für die Verarbeitung der Einträge in den Ausgabedateien schreiben.

So kopieren Sie die QoS-Journaleinträge in die vom System bereitgestellte Ausgabedatei:

1. Erstellen Sie in einer Benutzerbibliothek eine Kopie der vom System bereitgestellten Ausgabedatei QSYS/QATOQQOS. Hierzu können Sie den Befehl CRTDUPOBJ (Doppeltes Objekt erstellen) verwenden. Die folgende Zeichenfolge ist ein Beispiel für den Befehl CRTDUPOBJ:
   - CRTDUPOBJ OBJ(QADSPJR4) FROMLIB(Qsys) OBJTYPE(*FILE) TOLIB(*benutzerbibliothek*) NEWOBj-(*benutzerdatei*)
2. Kopieren Sie die Einträge mit dem Befehl DSPJRN (Journal anzeigen) aus dem Journal QUSRSYS/QQOS in die Ausgabedatei, die Sie im vorherigen Schritt erstellt haben. Falls Sie versuchen, die Einträge mit dem Befehl DSPJRN in eine nicht vorhandene Ausgabedatei zu kopieren, wird die Datei zwar vom System erstellt, enthält jedoch nicht die korrekten Feldbeschreibungen.
   - DSPJRN JRN(QUSRSYS/QQOS) JRNCDE((M)) ENTTYP(MP) CMTCYCID(*ALL) OUTPUT(*OUTFILE) OUTFILFMT(*TYPE4) OUTFILE(*benutzerbibliothek/benutzerdatei*)
   - DSPF FILE(*benutzerbibliothek/benutzerdatei*)

QoS-Server-Jobs protokollieren

Wenn Probleme mit den QoS-Richtlinien auftreten, sollten Sie die Jobprotokolle analysieren. Die Jobprotokolle enthalten Fehlernachrichten und andere QoS-bezogene Informationen.

Lediglich 1 QoS-Job (QTOQSRVR) wird im Subsystem QSYSWRK ausgeführt. Über System i Navigator können Sie die alten und die aktuellen Server-Jobprotokolle für QoS anzeigen.

So zeigen Sie das Protokoll an:

1. Erweitern Sie **Netzwerk**, und klicken Sie auf **IP-Richtlinien**.
2. Klicken Sie mit der rechten Maustaste auf **Quality of Service**.
3. Klicken Sie auf **Diagnosetools** → **QoS-Serverprotokoll**.

Daraufhin wird ein Fenster geöffnet, in dem Sie mit dem Job arbeiten können.

Die folgende Liste enthält die wichtigsten Jobnamen sowie eine kurze Erläuterung für den jeweiligen Verwendungszweck des Jobs:

QTCP Dieser Job ist der Basisjob, der alle TCP/IP-Schnittstellen startet. Wenn mit TCP/IP selbst grundlegende Probleme auftreten, sollten Sie das Jobprotokoll für QTCPIP analysieren.

QTOQSRVR

Dieser Job ist ein QoS-Basisjob, der spezifische Protokolldaten über QoS bereitstellt. Führen Sie den Befehl WRKSPLF QTCP (Mit Spooldatei arbeiten) aus, und suchen Sie nach dem Protokoll QTOQSRVR.

Spooldatei auf Fehler prüfen

So können Sie prüfen, ob die Spooldatei einen Fehler enthält:

1. Geben Sie in einer Befehlszeilenschnittstelle den Befehl `WRKSPLF QTCP` ein, und drücken Sie die Eingabetaste. Die Anzeige "Mit allen Spooldateien arbeiten" wird geöffnet.
2. Suchen Sie in der Spalte "Benutzerdaten" nach `QTOQSRVR`, um Fehler zu ermitteln, die speziell für den QoS-Server angegeben sind.
3. Wählen Sie **Auswahl 5** in der Zeile aus, die Sie anzeigen wollen. Lesen Sie die Informationen, und notieren Sie die Nachrichten-ID, die den Fehler erläutert (Beispiel: `TCP920C`).
4. Drücken Sie zwei Mal die Taste zum Verlassen, um zum Hauptmenü zurückzukehren.
5. Geben Sie in der Befehlszeilenschnittstelle den Befehl `WRKMSGF` ein, und drücken Sie die Eingabetaste.
6. Geben Sie in der Anzeige "Mit Nachrichtendatei arbeiten" die folgenden Informationen ein, und drücken Sie die Eingabetaste:

   ```
   Nachrichtendatei: QTCPMSG
   Bibliothek: *LIBL
   ```

7. Wählen Sie in der Anzeige "Mit Nachrichtendatei arbeiten" **Auswahl 5** aus, um die gewünschte Nachrichtendatei anzuzeigen, und drücken Sie die Eingabetaste.
8. Geben Sie in der Anzeige "Nachrichtenbeschreibungen anzeigen" die folgenden Informationen ein: `Listenanfang bei` - *Geben Sie die Nachrichten-ID aus Schritt 3 ein, und drücken Sie die Eingabetaste.* (Beispiel: `TCP920C`).
9. Wählen Sie Auswahl **5** für die gewünschte Nachrichten-ID aus, und drücken Sie die Eingabetaste.
10. Treffen Sie in der Anzeige "Anzuzeigende Nachrichtendetails auswählen" Auswahl **30** (für alles oben angegebene), und drücken Sie die Eingabetaste.

    Daraufhin wird eine detaillierte Beschreibung der Nachricht angezeigt.

Systemtransaktionen überwachen

Mit der QoS-Überwachung können Sie überprüfen, ob die QoS-Richtlinien die gewünschte Wirkung haben. Die QoS-Überwachung hilft Ihnen in der Planungsphase und bei der Fehlerbehebung für QoS.

Mit der Überwachung können Sie den IP-Datenaustausch auf dem System analysieren. Auf diese Weise können Sie ermitteln, an welchen Stellen im Netzwerk eine Überlastung auftritt. Mit der QoS-Überwachung können Sie Ihr Netzwerk weiter überwachen und Ihre Richtlinien dann bei Bedarf anpassen.

Leistung planen und verwalten

Einer der schwierigsten Aspekte bei der Implementierung von QoS ist die Bestimmung der Leistungsgrenzwerte, die in der Richtlinien festgelegt werden müssen. Hierfür gibt es keine generelle Empfehlung, da jedes Netzwerk anders ist. Um die passenden Werte für Ihre Umgebung zu ermitteln, können Sie die Überwachung vor dem Starten von unternehmensspezifischen Richtlinien einsetzen.

Versuchen Sie zunächst, eine Richtlinie für differenzierte Services ohne Auswahl von Messeinstellungen zu erstellen. Auf diese Weise können Sie feststellen, wie sich der Datenaustausch im Netzwerk gegenwärtig verhält. Aktivieren Sie diese Richtlinie, und starten Sie die Überwachung. Anhand der Überwachungsergebnisse können Sie Ihre Richtlinien an Ihre speziellen Anforderungen anpassen. In einer Beispielrichtlinie für die Überwachung sehen Sie, wie sich der Datenaustausch gegenwärtig verhält.

Leistungsprobleme lösen

Die Überwachung kann auch zur Fehlerbehebung eingesetzt werden. Anhand der Überwachungsausgabe können Sie feststellen, ob die Parameter, die Sie einer Richtlinie zuordnen, ordnungsgemäß befolgt werden. Falls Ihre Richtlinien in der Überwachung angezeigt werden, sich jedoch nicht auf den Datenaustausch auszuwirken scheinen, sollten Sie Folgendes prüfen:

- Wenn die Richtlinie basierend auf einem URI gefiltert wird, prüfen Sie, ob FRCA aktiviert ist und korrekt konfiguriert wurde. Bevor Sie eine Richtlinie für ankommende Daten definieren, die URIs verwendet, müssen Sie sicherstellen, dass der dem URI zugeordnete Anwendungsport der Anweisung "listen" (= Empfangsbereit) entspricht, die für FRCA in der Konfiguration des Apache-Web-Servers aktiviert ist.
- Prüfen Sie den Richtlinienzeitplan. Möglicherweise haben Sie während einer Inaktivitätszeit nach Ergebnissen gesucht.
- Prüfen Sie, ob die Portnummer richtig ist.
- Prüfen Sie, ob die IP-Adresse richtig ist.

Zugehörige Konzepte

„QoS planen" auf Seite 54
Die Planung ist der wichtigste Schritt bei der Umsetzung von QoS. Um die gewünschten Ergebnisse erzielen zu können, müssen Sie Ihre Netzwerkeinheiten prüfen und den Datenaustausch im Netzwerk überwachen.

„Szenarien: QoS-Richtlinien" auf Seite 32
Die Szenarien für QoS-Richtlinien in diesem Abschnitt veranschaulichen, aus welchem Grund Sie QoS benötigen und auf welche Weise Sie Richtlinien und Serviceklassen erstellen.

Zugehörige Verweise

„QoS überwachen" auf Seite 63
Mit der QoS-Überwachung können Sie den IP-Datenaustausch auf dem System analysieren.

Zugehörige Informationen

Adressen und Ports für den HTTP-Server (auf Apache-Basis) verwalten

Trace für TCP-Anwendungen durchführen

Mit dem QoS-Trace können Sie Tracefunktionen verwenden und den aktuellen Tracepuffer anzeigen.

Um den Trace auf dem System auszuführen, geben Sie den Befehl `TRCTCPAPP` (Trace für TCP/IP-Anwendung) in einer Befehlszeilenschnittstelle ein.

Hier ein Beispiel für die Auswahl der Traceoptionen:

```
TCP/IP-Anwendung.............> *QOS
Trace-Einstellung............> *ON
Maximaler Speicher für Trace.> *APP
Aktion bei voller Trace-Datei> *WRAP
Argumentenliste..............> 'lvl=4'
QoS-Trace-Art................> *ALL
```

Die folgende Tabelle enthält die möglichen Parameter, die in einem Trace verwendet werden können. Falls eine Einstellung in der zeichenorientierten Schnittstelle nicht angezeigt wird, müssen Sie zur Eingabe einen Befehl verwenden (z. B. `TRCTCPAPP APP(*QOS) MAXSTG(1000) TRCFULL(*STOPTRC) ARGLIST('l=4 c=i')`).

Einstellungen	Optionen
TCP/IP-Anwendung	QOS
Trace-Einstellung	*ON, *OFF, *END, *CHK
Maximaler Speicher für Trace (MAXSTG)	1-16000, *APP

Einstellungen	Optionen
Aktion bei voller Trace-Datei (TRCFULL)	*WRAP, *STOPTRC
Argumentenlisten (ARGLIST)	Stufen: 'lvl=1', 'lvl=2', 'lvl=3', 'lvl=4' Inhalt: 'c=a', 'c=i', 'c=d', 'c=m'
QoS-Trace-Art	*ALL

Maximaler Speicher für Trace

1-16000
Dies ist die maximale Speichergröße für die Tracedaten. Sobald dieser Wert erreicht wird, wird der Trace entweder gestoppt oder umgebrochen. Die Standardgröße beträgt 4 MB. Zur Angabe der Standardgröße wählen Sie die Einstellung *APP aus.

***APP** Dies ist die Standardeinstellung. Sie weist die Anwendung an, die Standardtracegröße zu verwenden. Die Standardtracegröße für den QoS-Server beträgt 4 MB.

Aktion bei voller Trace-Datei

***WRAP**
Bei dieser Einstellung werden die Traceinformationen umgebrochen, sobald der Trace den maximalen Plattenspeicherplatz (Tracepuffergröße) erreicht. Beim Umbrechen kann das System die ältesten Informationen in der Datei überschreiben, so dass Sie die Aufzeichnung der Traceinformationen fortsetzen können. Wenn Sie diese Einstellung nicht auswählen, wird die Traceoperation gestoppt, sobald der Speicherbereich belegt ist.

***STOPTRC**
Bei dieser Einstellung wird die Erfassung von Informationen gestoppt, sobald das System den maximalen Plattenspeicherplatz erreicht.

Argumentenlisten

Die Argumentenlisten geben die Fehlerkategorien und den Inhalt an, der protokolliert wird. Es gibt zwei Argumente, die im Befehl TRCTCPAPP zulässig sind: ein Argument für die Tracestufe und ein Argument für den Traceinhalt. Wenn Sie die Tracestufe und den Traceinhalt angeben, müssen Sie darauf achten, dass alle Attribute in einer gemeinsamen, durch Anführungszeichen eingeschlossenen Gruppe enthalten sind (z. B. `TRCTCPAPP 'l=4 c=a'`.

Anmerkung: Protokollstufen sind Inklusivangaben. Dies bedeutet, dass bei der Auswahl einer Protokollstufe alle untergeordneten Protokollstufen ebenfalls ausgewählt werden. Wenn Sie beispielsweise die Stufe 3 auswählen, werden die Stufen 1 und 2 automatisch ebenfalls berücksichtigt. Bei einem normalen Trace empfiehlt sich die Angabe 'l=4'.

Tracestufen

Stufe 1: Systemfehler (SYSERR)
Auf dieser Stufe werden Fehler protokolliert, die im Systembetrieb auftreten. Wenn ein solcher Fehler auftritt, kann der QoS-Server nicht fortgesetzt werden. Ein Systemfehler tritt beispielsweise dann auf, wenn nicht genügend Systemspeicher vorhanden ist oder das System keinen Kontakt zu TCP/IP herstellen kann. Dies ist die Standardstufe.

Stufe 2: Fehler zwischen Objekten (OBJERR)
Auf dieser Stufe werden Fehler protokolliert, die im QoS-Server-Code auftreten. Ein Objektfehler kann beispielsweise auftreten, weil eine Systemoperation ein unerwartetes Ergebnis feststellt. Dies ist in der Regel eine schwer wiegende Bedingung, die dem Kundendienst mitgeteilt werden muss.

Stufe 3: Spezifische Ereignisse (EVENT)
Auf dieser Stufe werden alle ausgeführten QoS-Operation protokolliert. Beispielsweise werden in einem Ereignisprotokoll Befehle und Anforderungen protokolliert. Die Ergebnisse dieser Protokollstufe ähneln denen der QoS-Journalingfunktion.

Stufe 4: Tracenachrichten (TRACE)
Auf dieser Stufe werden alle Daten protokolliert, die an den QoS-Server oder von diesem Server übertragen werden. Diesen Trace der höheren Ebene können Sie beispielsweise verwenden, um alle Daten zu protokollieren, das beim Debug hilfreich sein könnten. Mit diesen Angaben können Sie einfacher feststellen, wo ein Fehler aufgetreten ist und wie der Fehler erneut erzeugt werden kann.

Trace-Inhalt

Geben Sie nur einen Inhaltstyp an. Wenn Sie nicht angeben, für welchen Inhalt der Trace durchgeführt werden soll, wird der Trace (standardmäßig) für den gesamten Inhalt durchgeführt.

Inhalt = Alles ('c=a')
Bei dieser Angabe wird der Trace für alle Funktionen des QoS-Servers durchgeführt. Dies ist der Standardwert.

Inhalt = Intserv ('c=i')
Bei dieser Angabe wird der Trace nur für Operationen von integrierten Services durchgeführt. Verwenden Sie sie, wenn Sie feststellen wollen, ob es sich um ein Problem hinsichtlich eines integrierten Service handelt.

Inhalt = Diffserv ('c=d')
Bei dieser Angabe wird der Trace nur für Operationen von differenzierten Services durchgeführt. Verwenden Sie sie, wenn Sie feststellen wollen, ob es sich um ein Problem hinsichtlich eines differenzierten Service handelt.

Inhalt = Überwachung ('c=m')
Bei dieser Angabe wird der Trace nur für Überwachungsoperationen durchgeführt.

Wenn Sie Hilfe bei der Interpretation der Traceausgabe benötigen, ziehen Sie das Beispiel für die Traceausgabe auf der Seite "Traceausgabe" hinzu. Dort finden Sie eine Beispielausgabe mit Kommentaren, die Ihnen die Interpretation ihrer Bedeutung erleichtern. Die Funktion TRCTCPAPP wird normalerweise von der Unterstützung verwendet. Wenn im Zusammenhang mit der Ausgabe Verständnisprobleme auftreten, können Sie sich daher mit dem Kundendienst in Verbindung setzen.

Zugehörige Verweise

Trace TCP/IP Application (TRCTCPAPP)

Beispiel: Traceausgabe lesen

Diese Erläuterung der Traceausgabe ist keine Gesamtdarstellung. Sie enthält jedoch Angaben zu den wichtigsten Ereignissen, nach denen in den Traceinformationen gesucht werden sollte.

In einer Richtlinie für integrierte Services sollte insbesondere darauf geachtet werden, ob die RSVP-Verbindung zurückgewiesen wurde, weil keine Richtlinie für diese Verbindung gefunden wurde. Das folgende Beispiel zeigt eine Erfolgsnachricht:

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

Das nächste Beispiel zeigt eine Nachricht für einen erfolglosen Verbindungsversuch zu integrierten Services:

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

Bei einer Richtlinie für differenzierte Services sind diejenigen Nachrichten am wichtigsten, die angeben, ob der Server eine Richtlinienregel geladen hat oder ob in der Richtlinienkonfigurationsdatei ein Fehler aufgetreten ist:

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

Außerdem kann es Nachrichten geben, die angeben, dass die Tags in der Richtlinienkonfigurationsdatei nicht korrekt sind. Hier einige Beispielnachrichten:

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

Anmerkung: Das Zeichen % ist eine Variable, die für ein nicht erkanntes Tag steht.

Referenzinformationen zu QoS

RFCs (Request for Comments) für QoS, IBM Redbooks und andere Themensammlungen im Information Center enthalten Informationen, die sich auf die QoS-Themensammlung beziehen. Sie können alle PDF-Dateien anzeigen oder drucken.

RFCs für QoS

RFCs (Requests for Comments) sind geschriebene Definitionen von Protokollstandards und vorgeschlagenen Standards, die im Internet verwendet werden. Die folgenden RFCs enthalten hilfreiche Angaben für das Verständnis von QoS und seiner Funktionen:

- **RFC 1349:**

  Dieses RFC erläutert die neue Definition des Feldes für den Serviceoctetttyp (Type of Service Octet - TOS) in einem IP-Paketheader.
- **RFC 2205:**

  Dieses RFC erläutert die Definition von RSVP (ReSerVation Protocol).
- **RFC 2210:**

  Dieses RFC erläutert die Verwendung von RSVP mit IETF Integrated Services (IETF - Internet Engineering Task Force).
- **RFC 2474:**

  Dieses RFC erläutert die Definition des Feldes für differenzierte Services.
- **RFC 2475:**

  Dieses RFC erläutert die Architektur von differenzierten Services.

Zum Anzeigen der oben aufgeführten RFCs rufen Sie die Seite RFC Index Search Engine auf, die Sie über die Website RFC Editor erreichen.

IBM Redbooks

- IBM i5/OS IP Networks: Dynamic  (ca. 16 589 KB). Es erläutert den Entwurf eines IP-Netzwerks, das selbst-konfigurierend, fehlertolerant und effizient in der Ausführung ist. Neben vielen anderen Funktionen wird sowohl die Theorie als auch die Implementierung von QoS auf dem System erklärt. Außerdem gibt es weitere Szenarien mit schrittweisen Anleitungen.

- V4 TCP/IP for AS/400: More Cool Things Than Ever  (ca. 10 035 KB). Dieses Handbuch liefert Beispielszenarien, die allgemeine Lösungen durch Beispielkonfigurationen veranschaulichen. Anhand der Informationen in diesem Handbuch können Sie TCP/IP auf dem System planen, installieren, anpassen, konfigurieren und Fehler beheben. Es enthält zwar noch keine spezifischen Angaben zu QoS, liefert jedoch Informationen zum LDAP-Directory-Server.

- TCP/IP Tutorial and Technical Overview  (ca. 7.885 KB). Dieses Handbuch enthält eine Einführung sowie Referenzinformationen zur Protokoll- und Anwendungsgruppe von Transmission Control Protocol/Internet Protocol (TCP/IP). QoS wird in Kapitel 22 unter *Part 3. Advanced concepts and new technologies* behandelt.

Weitere Informationen

- IBM Tivoli Directory Server for i5/OS (LDAP). Dieses Thema enthält Grundinformationen zum Directory-Server sowie Angaben zur Konfiguration, zur Verwaltung und zur Fehlerbehebung. Außerdem finden Sie im Thema zu den Directory Services zusätzliche Ressourcen für die Konfiguration des Directory-Servers.
- Intrusion detection: Dieses Thema erläutert die Zusammenstellung von Informationen zu unberechtigten Zugriffsversuchen und Angriffen über das TCP/IP-Netzwerk. Durch eine Analyse der Protokolleinträge, die von der Funktion für die Erkennung von unbefugtem Zugriff bereitgestellt werden, können Sicherheitsadministratoren das i5/OS-Netzwerk vor solchen Angriffen schützen.

Zugehörige Verweise

„PDF-Datei für QoS" auf Seite 1
Sie können eine PDF-Datei der vorliegenden Informationen anzeigen und drucken.

Anhang. Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich.Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. An Stelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder andere Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Fremdprodukten, Fremdprogrammen und Fremdservices liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes
2, avenue Gambetta
92066 Paris La Defense
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen oder in Technical News Letters (TNLs) bekannt gegeben. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängig voneinander erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Europe, Middle East and Africa
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des im Dokument aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung bzw. der Allgemeinen Geschäftsbedingungen von IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete, der IBM Lizenzvereinbarung für Maschinencode oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer kontrollierten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können davon abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

Die oben genannten Erklärungen bezüglich der Produktstrategien und Absichtserklärungen von IBM stellen die gegenwärtige Absicht von IBM dar, unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufes. Sie sollen nur die Funktionen des Lizenzprogramms illustrieren; sie können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

COPYRIGHTLIZENZ:

Diese Veröffentlichung enthält Musteranwendungsprogramme, die in Quellensprache geschrieben sind. Sie dürfen diese Musterprogramme kostenlos kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, zu verwenden, zu vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle konform sind, für die diese Musterprogramme geschrieben werden. Diese Beispiele wurden nicht unter allen denkbaren Bedingungen getestet. Daher kann IBM die Zuverlässigkeit, Wartungsfreundlichkeit oder Funktion dieser Programme weder zusagen noch gewährleisten.

Kopien oder Teile der Musterprogramme bzw. daraus abgeleiteter Code müssen folgenden Copyrightvermerk beinhalten:

© (Name Ihrer Firma) (Jahr). Teile des vorliegenden Codes wurden aus Musterprogrammen der IBM Corp. abgeleitet. © Copyright IBM Corp. _Jahr/Jahre angeben_. Alle Rechte vorbehalten.

Informationen zu Programmierschnittstellen

In der vorliegenden Veröffentlichung werden vorgesehene Programmierschnittstellen dokumentiert, mit deren Hilfe Kunden Programme für den Zugriff auf die Services von IBM i5/OS schreiben können.

Marken

Folgende Namen sind Marken der IBM Corporation in den USA und/oder anderen Ländern:

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

Adobe, das Adobe-Logo, PostScript Document Format (PDF) und das PostScript-Logo sind Marken oder eingetragene Marken der Adobe Systems Incorporated in den USA und/oder anderen Ländern.

Weitere Unternehmens-, Produkt- oder Servicenamen können Marken anderer Hersteller sein.

Bedingungen

Die Berechtigungen zur Nutzung dieser Veröffentlichungen werden Ihnen auf der Basis der folgenden Bedingungen gewährt.

Persönliche Nutzung: Sie dürfen diese Veröffentlichungen für Ihre persönliche, nicht kommerzielle Nutzung unter der Voraussetzung vervielfältigen, dass alle Eigentumsvermerke erhalten bleiben. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM weder weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

Kommerzielle Nutzung: Sie dürfen diese Veröffentlichungen nur innerhalb Ihres Unternehmens und unter der Voraussetzung, dass alle Eigentumsvermerke erhalten bleiben, vervielfältigen, weitergeben und anzeigen. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM außerhalb Ihres Unternehmens weder vervielfältigen, weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

Abgesehen von den hier gewährten Berechtigungen erhalten Sie keine weiteren Berechtigungen, Lizenzen oder Rechte (veröffentlicht oder stillschweigend) in Bezug auf die Veröffentlichungen oder darin enthaltene Informationen, Daten, Software oder geistiges Eigentum.

IBM behält sich das Recht vor, die in diesem Dokument gewährten Berechtigungen nach eigenem Ermessen zurückzuziehen, wenn sich die Nutzung der Veröffentlichungen für IBM als nachteilig erweist oder wenn die obigen Nutzungsbestimmungen nicht genau befolgt werden.

Sie dürfen diese Informationen nur in Übereinstimmung mit allen anwendbaren Gesetzen und Verordnungen, einschließlich aller US-amerikanischen Exportgesetze und Verordnungen, herunterladen und exportieren.

IBM übernimmt keine Gewährleistung für den Inhalt dieser Veröffentlichungen. Diese Veröffentlichungen werden auf der Grundlage des gegenwärtigen Zustands (auf ″as-is″-Basis) und ohne eine ausdrückliche oder stillschweigende Gewährleistung für die Handelsüblichkeit, die Verwendungsfähigkeit oder die Freiheit der Rechte Dritter zur Verfügung gestellt.