System i

ネットワーキング
QoS (Quality of Service)

バージョン 6 リリース 1

System i

ネットワーキング
QoS (Quality of Service)

バージョン 6 リリース 1

お願い

本書および本書で紹介する製品をご使用になる前に、 79 ページの『特記事項』に記載されている情報をお読みください。

本書は、IBM i5/OS (プロダクト番号 5761-SS1) のバージョン 6、リリース 1、モディフィケーション 0 に適用されます。また、改訂版で断りがない限り、それ以降のすべてのリリースおよびモディフィケーションにも適用されます。 このバージョンは、すべての RISC モデルで稼働するとは限りません。また CISC モデルでは稼働しません。

IBM 発行のマニュアルに関する情報のページ

http://www.ibm.com/jp/manuals/

こちらから、日本語版および英語版のオンライン・ライブラリーをご利用いただけます。また、マニュアルに関するご意見やご感想を、上記ページよりお送りください。今後の参考にさせていただきます。

(URL は、変更になる場合があります)

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原　典： System i
Networking
Quality of service
Version 6 Release 1

発　行： 日本アイ・ビー・エム株式会社

担　当： ナショナル・ランゲージ・サポート

第1刷 2008.2

この文書では、平成明朝体™W3、平成明朝体™W7、平成明朝体™W9、平成角ゴシック体™W3、平成角ゴシック体™W5、および平成角ゴシック体™W7を使用しています。この(書体*)は、(財) 日本規格協会と使用契約を締結し使用しているものです。フォントとして無断複製することは禁止されています。

注* 平成明朝体™W3、平成明朝体™W7、平成明朝体™W9、平成角ゴシック体™W3、平成角ゴシック体™W5、平成角ゴシック体™W7

目次

Quality of Service

i5/OS® Quality of Service (QoS) ソリューションを使用すると、TCP/IP アプリケーションのネットワーク優先順位と帯域幅を要求するポリシーがネットワーク全体で使用可能になります。

ネットワークのすべてのトラフィックは等しく優先順位を与えられます。クリティカルではないブラウザー・トラフィックもクリティカルなビジネス・アプリケーションと同じくらい重要と見なされます。最高経営責任者 (CEO) が、オーディオ・ビデオ・アプリケーションを使用してプレゼンテーションを行なおうとしている場合、IP パケットの優先順位が重要な問題です。プレゼンテーションの間、このアプリケーションが他のアプリケーションより優れたパフォーマンスを得られることが肝心です。

マルチメディアなど、予測可能で信頼できる結果が必要なアプリケーションを送信する場合、パケットの優先順位が重要です。 QoS ポリシーは、パケットの優先順位を管理することができ、また、システムから発信されるデータの制限、接続要求の管理、およびシステム・ロードの制御が可能です。侵入検知ポリシーを活動化するためには、QoS サーバーが稼働状態でなければなりません。

Quality of Service の PDF ファイル

本書の PDF ファイルを表示および印刷することができます。

本書の PDF 版を表示またはダウンロードするには、「QoS (Quality of Service)」を選択します。

PDF ファイルの保管

表示用または印刷用の PDF をワークステーションに保管するには、次のようにします。

1. ご使用のブラウザーで該当の PDF リンクを右クリックする。
2. PDF をローカルで保管するオプションをクリックする。
3. PDF を保管するディレクトリーを指定する。
4. 「**保存**」をクリックする。

Adobe Reader のダウンロード

PDF を表示または印刷するには、システムに Adobe® Reader がインストールされている必要があります。

Adobe Web サイト (www.adobe.com/products/acrobat/readstep.html) から、無償コピーをダウンロードできます。

関連資料

76 ページの『Quality of Service の関連情報』

Quality of Service の Request For Comments、IBM® Redbooks® 資料、およびその他の Information Center トピック・コレクションには、Quality of Service トピック・コレクションに関連する情報が記載されています。以下の PDF ファイルのいずれも表示または印刷できます。

概念

QoS (Quality of Service) を使用する前に、基本的な用語および QoS の概念を理解する必要があります。これらの概念は、サービスがお客様のニーズに合っているかどうかを判別する上で役立ちます。

QoS を実行するには、System i™ ナビゲーター のウィザードを使用してポリシーを構成します。 ポリシーとは、アクションを指定する規則のセットです。ポリシーは、基本的には、(指定した) どのクライアント、アプリケーション、およびスケジュールが特定のサービスを受けるかを提示しています。 以下のポリシー・タイプを構成できます。

- 差異化サービス (DiffServ)
- 統合サービス (IntServ)
- インバウンド許可

DiffServ と *IntServ* はアウトバウンド帯域幅ポリシーと見なされます。アウトバウンド・ポリシーは、ネットワークから発信されるデータを制限し、システム負荷の制御に役立ちます。 アウトバウンド・ポリシー内に設定した速度により、システム内で制限されるデータと制限されないデータの種類、および制限の方法が制御されます。 アウトバウンド・ポリシーの両方のタイプでは、インターネット・サービス・プロバイダー (ISP) とのサービス・レベル・アグリーメント (SLA) が必要となることがあります。

インバウンド許可ポリシー は、外部の送信元からネットワークに着信する接続要求を制御します。 インバウンド・ポリシーは ISP からのサービス・レベルに依存しません。 どちらのポリシーを使用するかを決定するためには、QoS を使用する理由と、システムの役割を検討してください。

QoS を実行するための最も重要な部分の 1 つは、システム自体です。 QoS 概念を理解するだけでなく、それらの概念においてオペレーティング・システムが果たす役割も認識する必要があります。i5/OS オペレーティング・システムは、クライアントまたはサーバーとしてのみ機能します。ルーターの役割は果たせません。例えば、クライアントとして機能するオペレーティング・システムは、DiffServ ポリシーを使用して、他のシステムへの情報要求がネットワーク内で高い優先順位を持つようにすることができます。サーバーとして機能するオペレーティング・システムは、インバウンド許可ポリシーを使用して、サーバーが受け入れる Uniform Resource Identifier (URI) 要求を制限することができます。

関連概念

55 ページの『サービス・レベル・アグリーメント』
このトピックでは、QoS (Quality of Service) インプリメンテーションに影響を及ぼす可能性があるサービス・レベル・アグリーメント (SLA) の重要な特徴のいくつかを指摘します。 QoS とは、つまりネットワーク・パフォーマンスを意味します。プライベート・ネットワークの外部でネットワーク優先順位を受け取るには、インターネット・サービス・プロバイダー (ISP) との SLA を保持する必要が生じる場合があります。

関連資料

76 ページの『Quality of Service の関連情報』
Quality of Service の Request For Comments、IBM Redbooks 資料、およびその他の Information Center トピック・コレクションには、Quality of Service トピック・コレクションに関連する情報が記載されています。以下の PDF ファイルのいずれも表示または印刷できます。

DiffServ

これは、オペレーティング・システムで作成できるアウトバウンド帯域幅ポリシーの第 1 のタイプです。DiffServ はトラフィックをクラスに分割します。 DiffServ ポリシーをインプリメントするには、ネットワーク・トラフィックの分類方法とさまざまなクラスの処理方法を決定する必要があります。

関連概念

27 ページの『QoS sendmsg() API 拡張機能』
sendmsg() 機能は、接続ソケットまたは非接続ソケットを通して、データ、補助データ、またはそれらの組み合わせを送信するために使用されます。

11 ページの『トークン・バケットおよび帯域幅の限界』
トークン・バケット限界と帯域幅限界はともにパフォーマンス制限として知られています。これらのパフォーマンス制限によって、アウトバウンド帯域幅ポリシー (IntServ および DiffServ の両方) 内でのパケットの送達が保証されます。

14 ページの『サービス・クラス』
DiffServ ポリシーまたはインバウンド許可ポリシーを作成するときは、サービス・クラスも作成して使用します。

31 ページの『シナリオ: ブラウザー・トラフィックの制限』
QoS (Quality of Service) を使用して、トラフィック・パフォーマンスを制御することができます。 ネットワーク内でのアプリケーションのパフォーマンスを制限または拡張するには、DiffServ ポリシーを使用します。

36 ページの『シナリオ: 安全で予測可能な結果 (VPN と QoS)』
VPN (仮想プライベート・ネットワーク) を使用している場合でも、Quality of Service (QoS) ポリシーを作成できます。

関連資料

16 ページの『コード・ポイントを使用した PHB (ホップごとの転送優先順位付け) の割り当て』
Quality of Service (QoS) は、業界推奨コード・ポイントを使用して、トラフィックに PHB (ホップごとの転送優先順位付け) を割り当てます。

58 ページの『ウィザードを使用した QoS の構成』
Quality of Service (QoS) ポリシーを構成するには、System i ナビゲーター にある QoS ウィザードを使用してください。

関連情報

ご使用の HTTP サーバー (Apache 付き) のアドレスおよびポートの管理

優先順位付けされたクラス: ネットワーク・トラフィックの分類方法

DiffServ はトラフィックをクラスとして識別します。 最も一般的なクラスは、クライアント IP アドレス、アプリケーション・ポート、サーバー・タイプ、プロトコル、ローカル IP アドレス、およびスケジュールを使用して定義されます。同じクラスに分類されたトラフィックは、すべて同等に扱われます。

より拡張された分類を行うために、種々のレベルのサービスを幾つかの i5/OS アプリケーションに設定するためのアプリケーション・データを指定することができます。アプリケーション・データの使用はオプションですが、細分されたレベルでの分類が必要な場合に役立ちます。 アプリケーション・データには、アプリケーション・トークンまたは Uniform Resource Identifier (URI) という 2 つのタイプがあります。トラフィックがポリシーで指定したトークンまたは URI に一致すると、そのポリシーがアウトバウンド応答に適用されます。したがって、DiffServ ポリシーで指定した優先順位にかかわりなくアウトバウンド・トラフィックが実現します。

DiffServ ポリシーでのアプリケーション・トークンの使用

アプリケーション・データを使用すると、ポリシーは、アプリケーションから sendmsg() アプリケーション・プログラミング・インターフェース (API) を通してオペレーティング・システムに渡された特定のパラメーター (トークンおよび優先順位) に応答する設定になります。この設定はオプションです。アウトバウンド・ポリシーにこのレベルの細分度が必要でない場合は、ウィザードで「**すべてのトークン (All tokens)**」を選択してください。アプリケーションのトークンおよび優先順位と、アウトバウンド・ポリシーに設定された特定のトークンおよび優先順位を一致させることもできます。ポリシーには、アプリケーション・データを設定するためのトークンと優先順位という 2 つの部分があります。

- アプリケーション・トークンの概念

アプリケーション・トークン は、定義されたリソースを表現できる文字ストリング (myFTP など) です。 Quality of Service (QoS) ポリシーに指定したトークンは、アウトバウンド・アプリケーションが提供するトークンと突き合わせされます。アプリケーションは sendmsg() API を通してトークン値を提供します。 2 つのトークンが一致すると、アプリケーション・トラフィックは DiffServ ポリシーに組み込まれます。

DiffServ ポリシーでアプリケーション・トークンを使用するには、次のようにします。

1. QoS 構成ウィンドウで「**DiffServ**」を右マウス・ボタンでクリックし、「**新規ポリシー (New Policy)**」を選択します。ウィザードを開始します。
2. 「サーバー・データ要求 (Server Data Request)」ページで、「**選択済みアプリケーション・トークン (Selected application token)**」を選択します。
3. 新しいトークンを作成するには、「**新規**」を選択します。「新規 URI」ウィンドウが開きます。
4. 「**名前 (Name)**」フィールドに、分かりやすいアプリケーション・トークン名を入力します。
5. 「**URI**」フィールドで、「**(/)**」を削除し、アプリケーション・トークン (最大 128 文字のストリング) を入力します。典型的な URI ではなく、例えば「myFTPapp」のようにします。

- アプリケーション優先順位の概念

  ポリシーに指定したアプリケーション*優先順位*は、アウトバウンド・アプリケーションが提供するアプリケーション優先順位と突き合わせされます。 アプリケーションは sendmsg() API を通して優先順位の値を提供します。 2 つの優先順位が一致すると、アプリケーション・トラフィックは DiffServ ポリシーに組み込まれます。 DiffServ ポリシーに定義されているすべてのトラフィックは、ポリシー全体に指定されている優先順位を引き続き受け取ります。

アプリケーション・トークンを指定する場合、この情報をオペレーティング・システムに提供するアプリケーションでは sendmsg() API の使用を明確にコード化しておく必要があります。 これはアプリケーション・プログラマーの役割です。アプリケーションの文書には有効な値 (トークンおよび優先順位) を記載し、QoS 管理者が DiffServ ポリシーを使用できるようにします。その場合、DiffServ ポリシーは、ポリシー内に設定されたトークンに一致するトラフィックにそのポリシーの優先順位と分類を適用します。ポリシーに設定された値に一致する値がアプリケーションにない場合は、アプリケーションを更新するか、または DiffServ ポリシーに別のアプリケーション・データ・パラメーターを使用することが必要になります。

DiffServ ポリシーでの URI の使用

DiffServ ポリシーの作成では、『DiffServ ポリシーでのアプリケーション・トークンの使用』の項のように、ウィザードを使用してシステム・データ情報を設定できます。ウィザードのフィールドにはアプリケーション・トークンを指定するようにプロンプトが出されますが、代わりに相対 URI を指定できます。この指定もオプションです。アウトバウンド・ポリシーにこのレベルの細分度が必要でない場合は、ウィザードで「**すべてのトークン (All tokens)**」を選択してください。アウトバウンド・ポリシーに設定された特定の URI を突き合わせることができます。

相対 URI は、実際には絶対 URI のサブセットです (旧絶対 URL と類似)。http://www.ibm.com/software の例について考慮してみます。*http://www.ibm.com/software* セグメントは、絶対 URI と見なされます。*/software* セグメントは、相対 URI です。すべての相対 URI 値は、1 個のスラッシュ (**/**) で始まっていなければなりません。以下のセグメントは、有効な相対 URI の例です。

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

URI を使用する DiffServ ポリシーをセットアップする前に、URI に割り当てるアプリケーション・ポートを、Apache Web サーバー構成で Fast Response Cache Accelerator (FRCA) 用に使用可能になっている Listen ディレクティブに一致させる必要があります。ご使用の HTTP サーバーのポートを変更または表示するには、『Manage addresses and ports for HTTP Server (powered by Apache)』  を参照してください。

FRCA は、アウトバウンド HTTP 応答ごとに URI を識別します。アウトバウンド応答に関連した URI が、各 DiffServ ポリシーで定義されている URI と比較されます。 FRCA で識別された URI に最もよく一致するトークン・ストリング (URI) を持つ最初のポリシーが、その URI へのすべての応答に適用されます。

関連概念

27 ページの『QoS sendmsg() API 拡張機能』
sendmsg() 機能は、接続ソケットまたは非接続ソケットを通して、データ、補助データ、またはそれらの組み合わせを送信するために使用されます。

優先順位の設定: クラスの処理方法

トラフィックが分類された後、DiffServ ではトラフィックを処理する方法を定義するためにホップごとの転送優先順位付けも必要です。

オペレーティング・システムは、IP ヘッダー内のビットを使用して、IP パケットのサービス・レベルを識別します。 ルーターとスイッチは、IP ヘッダーの TOS オクテット・フィールドの PHB (ホップごとの転送優先順位付け) 情報に基づいてリソースを割り振ります。 TOS オクテット・フィールドは、Request for Comments (RFC) 1349 および OS/400® V5R1 オペレーティング・システムで再定義されました。 *PHB (ホップごとの転送優先順位付け)* は、パケットがネットワーク・ノードで受け取る転送動作です。PHB は、コード・ポイント と呼ばれる 16 進値で表されます。システムまたはネットワークの他の部分 (ルーターなど) のいずれかの場所で、パケットのマーク付けを行なえます。パケットが要求されたサービスを保持するためには、すべてのネットワーク・ノードが DiffServ 使用可能でなくてはなりません。つまり、ネットワーク装置が PHB を実施できなくてはなりません。 PHB (ホップごとの転送優先順位付け) 処理を実施するには、ネットワーク・ノードは、待ち行列スケジューリングおよびアウトバウンド優先順位管理を利用できなくてはなりません。 DiffServ 使用可能の意味についての詳細は、 6 ページの『トラフィック・コンディショナー』を参照してください。

パケットが、DiffServ 使用可能でないルーターまたはスイッチを通過すると、そのパケットはそのルーターにおけるサービス・レベルを失います。その結果、パケットは依然として処理可能ですが、予期しない遅延が生じることがあります。 システムでは、定義済みの PHB (ホップごとの転送優先順位付け) コード・ポイントを使用するか、独自のコード・ポイントを定義できます。 プライベート・ネットワークの外側での使用を目的として、独自のコード・ポイントを作成してはなりません。割り当てるコード・ポイントがわからない場合は、 16 ページの『コード・ポイントを使用した PHB (ホップごとの転送優先順位付け) の割り当て』を参照してください。

IntServ とは異なり、DiffServ トラフィックの場合、予約またはフローごとの処理は必要ありません。同じクラスに分類されたすべてのトラフィックは、同等に扱われます。

DiffServ は、システムから発信されるトラフィックを絞り込むためにも使用されます。つまり、システムは実際に DiffServ を利用してパフォーマンスを制限します。 重要度の低いアプリケーションを制限することで、主幹業務のアプリケーションを最初にプライベート・ネットワークから送り出すことが可能になります。このポリシーのサービス・クラスを作成するとき、システムでさまざまな限界を設定するように指示さ

れます。 パフォーマンス制限には、トークン・バケット・サイズ、ピーク速度限界、平均速度限界などがあります。 System i ナビゲーター の Quality of Service (QoS) 機能内のヘルプ・トピックに、これらの限界に関する詳しい情報があります。

トラフィック・コンディショナー

QoS (Quality of Service) ポリシーを使用するには、ネットワーク装置 (ルーターやスイッチなど) にトラフィック・コンディショナーの機能が備わっている必要があります。トラフィック・コンディショナーは、分類子、計量機能、マーカー、シェイパー、およびドロッパーを表します。

ネットワーク装置にすべてのトラフィック・コンディショナーが装備されていると、その装置は DiffServ 使用可能であると見なされます。

注: これらのハードウェア要件は、System i 製品に固有のものではありません。システムは外部ハードウェアを制御できないので、これらの用語は QoS インターフェースでは使用されていません。 プライベート・ネットワークの外部では、ハードウェアは QoS の一般要件を処理する能力を持つ必要があります。特定の装置の資料を調べて、その装置が DiffServ 要件を処理できることを確認してください。また、ポリシーをインプリメントする前に、QoS の一般概念と前提条件を調べてください。

次の図は、トラフィック・コンディショナーの作用を論理的に表したものです。

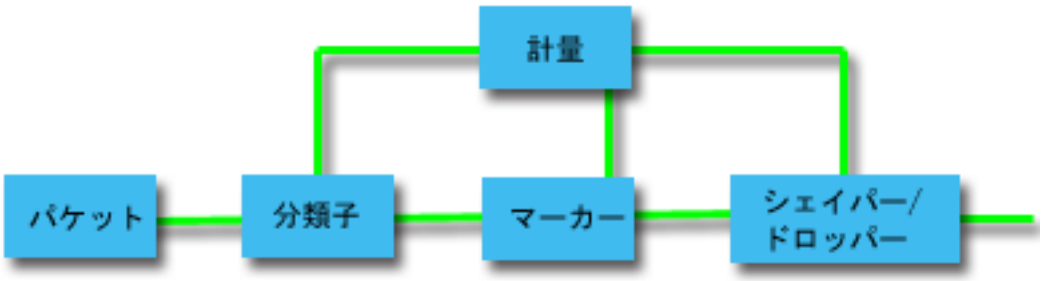


図 1. トラフィック・コンディショナー

各トラフィック・コンディショナーについて、詳しく説明します。

分類子 パケット分類子は、パケットの IP ヘッダーの内容に基づいてトラフィック・ストリームの中からパケットを選択します。i5/OS オペレーティング・システムは、2 つのタイプの分類子を定義しています。 動作集合は、排他的に DiffServ コード・ポイントに基づいてパケットを分類します。複数フィールド分類子は、1 つ以上のヘッダー・フィールド (ソース・アドレス、宛先アドレス、DiffServ フィールド、プロトコル ID、ソース・ポート、URI、サーバー・タイプ、宛先ポート番号など) の組み合わせの値に基づいてパケットを選択します。

計量機能
トラフィック計量機能は、分類子によって転送される IP パケットがトラフィックの IP ヘッダー・プロファイルに対応しているかどうかを判定します。 IP ヘッダー内の情報は、このトラフィックの QoS ポリシーの中に設定した値によって決定します。 計量機能は、アクションを起動するために情報を他の調整機能に渡します。アクションは、(それがプロファイル内パケットか、プロファイル外パケットかに関係なく) それぞれのパケットごとに起動されます。

マーカー

パケット・マーカーは、DiffServ フィールドを設定します。マーカーは、単一のコード・ポイントか、または PHB の選択に使用するコード・ポイント・セットへのすべてのパケットにマーク付けを行うように構成することができます。

シェイパー

シェイパーは、トラフィック・ストリームをトラフィック・プロファイルに準拠させるためにそのトラフィック・ストリーム内のいくつかのパケットまたはすべてのパケットを遅らせます。シェイパーのバッファー・サイズは限られているので、遅延パケットを保持するためのスペースがないとルーターによりパケットが廃棄される場合があります。

ドロッパー

ドロッパーは、トラフィック・ストリーム内のいくつかのパケットまたはすべてのパケットを廃棄します。これは、ストリームをトラフィック・プロファイルに準拠させるために行なわれます。

関連概念

57 ページの『ネットワークのハードウェアおよびソフトウェア』
ネットワーク内部の装置とネットワーク外部の他の装置の能力は、Quality of Service (QoS) の結果に非常に大きく影響します。

IntServ

作成できるアウトバウンド帯域幅ポリシーの第 2 のタイプは、IntServ ポリシーです。 IntServ によって、IP アプリケーションは、ReSerVation Protocol (RSVP) と QoS API を使用して帯域幅を要求し予約することができます。

IntServ ポリシーでは、RSVP および Resource Reservation Setup Protocol API (RAPI) (または qtoq ソケット API) を使用して、エンドツーエンド接続を保証します。 これは、指定できる最高水準のサービスですが、最も複雑なサービスでもあります。

IntServ は、トラフィック送達時間を処理し、特定のトラフィックに特別な処理命令を割り当てます。IntServ ポリシーは、データ転送を保証する手段としてはまだ比較的費用のかかる方法なので、IntServ ポリシーについては慎重であることが大切です。ただし、リソースのオーバー・プロビジョニング (バンド幅過供給) は、IntServ よりもさらに費用がかかる場合があります。

IntServ は、データを送信する前に特定のポリシー用にリソースを予約します。データ転送の前にルーターに信号が送られ、ネットワークが実際にポリシーに基づいて (エンドツーエンド) データ転送に同意し管理します。ポリシーとは、アクションを指定する規則のセットです。ポリシーは、基本的には許可制御リストです。帯域幅要求は、クライアントからの予約に入ります。パスの中のすべてのルーターが要求側クライアントからの要件を応諾する場合は、その要求はシステムおよび IntServ ポリシーに届きます。 要求が、ポリシーで定義された限度内にある場合は、QoS サーバーは RSVP 接続を許可し、アプリケーションの帯域幅を無視します。 RSVP と RAPI API、または RSVP と qtoq QoS ソケット API を使用して、リソースの予約を行います。

トラフィックが通過する各ノードには、RSVP を使用する能力が備わっている必要があります。 ルーターは、パケット・スケジューラー、パケット分類子および許可制御というトラフィック制御機能を通じて QoS を提供します。このトラフィック制御を実行する能力があることを、しばしば RSVP 使用可能であるといいます。つまり、IntServ ポリシーをインプリメントする場合の最も重要な課題は、ネットワークでリソースを制御可能および予測可能にすることです。予測可能な結果を得るためには、ネットワークのすべてのノードが RSVP 使用可能になる必要があります。例えば、トラフィックは、どのパスに RSVP 使用可能ルーターがあるかに基づいてではなく、リソースに基づいて経路指定されます。 RSVP 使用可能でないルーターが混在すると、予測不可能なパフォーマンス上の問題が発生する場合があります。接続は続行されま

すが、アプリケーションが要求するパフォーマンスは、そのルーターによって保証されません。次の図は、IntServ 機能が論理的にどのように動作するかを示しています。

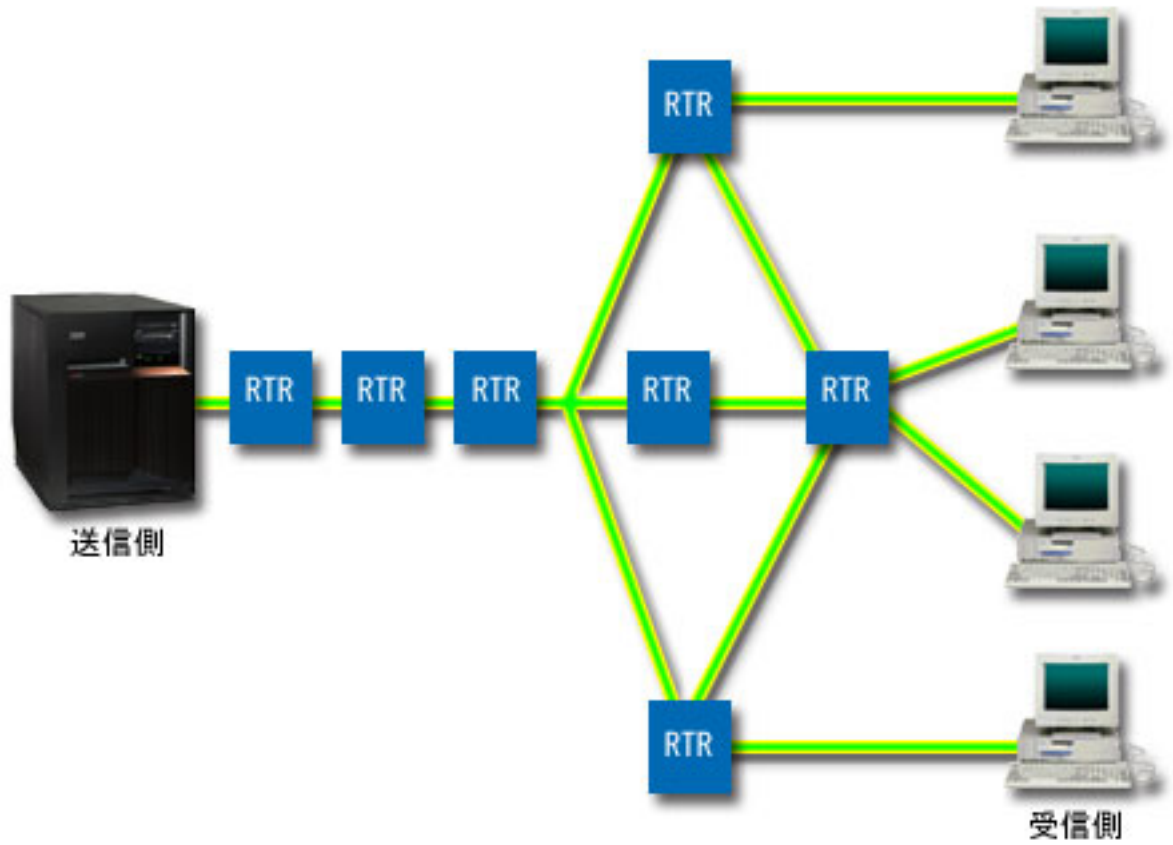


図 2. クライアントとサーバーの間の RSVP パス

上図で送信側として表示されているサーバー上の RSVP 使用可能アプリケーションが、クライアントまたは受信側からの接続要求を検出します。それに応じて、アプリケーションはクライアントに対して PATH コマンドを発行します。 このコマンドは RAPI API または qtoq QoS ソケット API を使用して発行します。このコマンドにはルーター (RTR) IP アドレス情報が入っています。 PATH コマンドには、サーバー上の使用可能なリソースとパスに存在するルーターの情報、およびサーバーとクライアントの間の経路情報が含まれます。次に、クライアント上の RSVP 使用可能アプリケーションは、ネットワーク・リソースが割り振られたことをサーバーに知らせるためにネットワーク・パスを介して RESV コマンドを戻します。このコマンドは、PATH コマンドからのルーター情報に基づいて予約を行います。サーバーとパスに存在するすべてのルーターが、RSVP 接続用にリソースを予約します。サーバーが RESV コマンドを受け付けると、アプリケーションはクライアントへのデータ送信を開始します。データは、予約と同じ経路で送信されます。これは、ポリシーの実施を成功させるためには、この予約を実行するルーター能力がいかに重要であるかを示しています。

IntServ は、HTTP のように、短期間の RSVP 接続には向きません。 ただし、もちろんこれは自由裁量です。ご自分のネットワークにとって、なにが最善かを判断してください。どの領域とアプリケーションにパフォーマンスの問題があり、QoS が必要かを考えてください。 IntServ ポリシーで使用するどのアプリケ

ーションも、RSVP を使用できなくてはなりません。 最初は、ご使用の i5/OS オペレーティング・システムに RSVP 使用可能アプリケーションがないため、RSVP を使用できるアプリケーションを作成する必要があります。

パケットが到着し、ネットワークから出ようとすると、オペレーティング・システムは、パケットを送信するためのリソースがあるかどうかを判断します。この受け入れは、トークン・バケット内のスペース量によって決まります。トークン・バケット内の受け入れ用のスペース (ビット数)、帯域幅限界、トークン速度限界、およびシステムで許可する最大接続数は、手動で設定します。これらの値はパフォーマンス制限値と呼ばれます。パケットが制限内に収まるようだと、そのパケットはプロファイルに準拠しているので送信されます。 IntServ では、各接続には独自のトークン・バケットが与えられます。

DiffServ マーク付けを使用した IntServ

ネットワーク全体が RSVP 接続を保証できるかどうか不確実な場合も、IntServ ポリシーを作成できます。ネットワーク・リソースが RSVP を使用できない場合は、接続は保証されません。この場合、ポリシーにコード・ポイントを適用する必要があります。通常、このコード・ポイントは DiffServ ポリシー内で使用され、トラフィックにサービス・クラスを割り当てます。 接続が保証されない場合でも、このコード・ポイントは接続になんらかの優先順位を与えようと試みます。

関連概念

18 ページの『Quality of Service API』
このトピックには、プロトコルと API に関する情報、および ReSerVation Protocol (RSVP) で使用可能なルーターに関する要件が記載されています。Quality of Service (QoS) API には、RAPI API、qtoq ソケット API、sendmsg() API、およびモニター API が含まれています。

12 ページの『DiffServ マーク付けのある IntServ』
IntServ ポリシーの中で DiffServ マーク付けを使用して、混合環境で送信されるパケットの優先順位を維持することができます。

44 ページの『シナリオ: 予測可能な B2B トラフィック』
予測可能な送達が必要で、引き続き予約を要求したい場合は、IntServ ポリシーも使用します。 この例では、負荷制御サービスを使用します。

48 ページの『シナリオ: 専用送達 (IP テレフォニー)』
専用送達が必要で、予約を要求したい場合は、IntServ ポリシーを使用します。作成する IntServ ポリシーには、2 つのタイプ (保証サービスと負荷制御サービス) があります。 この例では、保証サービスが使用されています。

トラフィック制御機能

トラフィック制御機能は、IntServ にのみ適用されますが、System i 製品に固有のものではありません。

サーバーは外部ハードウェアを制御できないので、これらの用語は Quality of Service (QoS) インターフェースでは使用されていません。 プライベート・ネットワークの外部では、ハードウェアは QoS の一般要件を処理する能力を持つ必要があります。 IntServ ポリシーの一般ルーター要件を以下のセクションで説明します。 また、ポリシーをインプリメントする前に、QoS の一般概念と前提条件を調べることもお勧めします。

予測可能な結果を得るためには、トラフィック・パスに ReSerVation Protocol (RSVP) 使用可能ハードウェアを設置する必要があります。 ルーターには、RSVP を使用するためのある特定のトラフィック制御機能が必要です。 この、あるトラフィック制御機能がある状態を、しばしば RSVP 使用可能である、または QoS 使用可能である、といいます。 システムの役割はクライアントまたはサーバーのいずれかであること

を覚えておいてください。 現時点では、サーバーをルーターとして使用することはできません。 ネットワーク装置の資料で、QoS 要件が処理できるかどうか調べてください。

トラフィック制御機能には、次のものがあります。

パケット・スケジューラー
パケット・スケジューラーは、IP ヘッダー内の情報に基づいて転送されるパケットを管理します。パケット・スケジューラーにより、パケットは、ポリシーの中に設定したパラメーターに従って送達されます。 スケジューラーは、パケットがキューイングされるポイントにインプリメントされます。

パケット分類子
パケット分類子は、IP フローのどのパケットが IP ヘッダー情報に基づいてある特定のサービス・レベルを受けるかを識別します。それぞれの着信パケットは、分類子によって特定のクラスにマップされます。同じクラスに分類されたすべてのパケットは、同じ処理を受けます。このサービス・レベルは、ポリシーの中に設定した情報に基づきます。

許可制御
許可制御には、ルーターが、新規フロー用に要求された QoS を受け入れる十分な経路指定リソースがあるかどうかを判断する時に使用する、決定アルゴリズムが組み込まれています。 十分なリソースがないと、新規のフローは拒否されます。フローが受け入れられると、ルーターは、要求された QoS を予約するためにパケット分類子とスケジューラーを割り当てます。許可制御は、予約パス沿いに存在する各ルーターで行われます。

関連概念

18 ページの『Quality of Service API』
このトピックには、プロトコルと API に関する情報、および ReSerVation Protocol (RSVP) で使用可能なルーターに関する要件が記載されています。Quality of Service (QoS) API には、RAPI API、qtoq ソケット API、sendmsg() API、およびモニター API が含まれています。

関連資料

76 ページの『Quality of Service の関連情報』
Quality of Service の Request For Comments、IBM Redbooks 資料、およびその他の Information Center トピック・コレクションには、Quality of Service トピック・コレクションに関連する情報が記載されています。以下の PDF ファイルのいずれも表示または印刷できます。

IntServ タイプ

IntServ には、負荷制御サービスと保証サービスの 2 つのタイプがあります。

負荷制御

負荷制御サービスは、混雑したネットワークによる影響を大きく受けるアプリケーション (例えば、リアルタイム・アプリケーション) をサポートします。 このようなアプリケーションは、少量の脱落や遅延も許容しなければなりません。アプリケーションが負荷制御サービスを使用する場合、ネットワーク負荷が増えてもそのパフォーマンスには影響しません。トラフィックには、負荷が少ない状況でのネットワークの正常なトラフィックが受けられるサービスに類似したサービスが提供されます。

ルーターは、負荷制御サービスが十分な帯域幅およびパケット処理リソースを確実に受け取るようにする必要があります。 このためには、ルーターは、IntServ をサポートする Quality of Service (QoS) 使用可能でなければなりません。 ルーターの仕様をチェックして、トラフィック制御機能を通じて QoS を提供するかどうかを調べる必要があります。トラフィック制御は、次の要素、すなわち、パケット・スケジューラー、パケット分類子、および許可制御から構成されます。

保証サービス

保証サービスは、パケットが指定の送達時間内で確実に到着するようにします。 保証サービスを必要とするアプリケーションには、ストリーミング・テクノロジーを使用するビデオおよびオーディオのブロードキャスト・システムが含まれます。保証サービスは、パケットが指定時間以上は遅れないように最大キューイング遅延を制御します。 パケットのパス沿いにあるルーターはすべて、送達を保証するための ReSerVation Protocol (RSVP) 機能を備えていなければなりません。 トークン・バケット限界および帯域幅限界を割り当てると、保証サービスを定義することになります。保証サービスは、TCP を使用するアプリケーションにのみ適用できます。

関連概念

44 ページの『シナリオ: 予測可能な B2B トラフィック』
予測可能な送達が必要で、引き続き予約を要求したい場合は、IntServ ポリシーも使用します。 この例では、負荷制御サービスを使用します。

48 ページの『シナリオ: 専用送達 (IP テレフォニー)』
専用送達が必要で、予約を要求したい場合は、IntServ ポリシーを使用します。作成する IntServ ポリシーには、2 つのタイプ (保証サービスと負荷制御サービス) があります。 この例では、保証サービスが使用されています。

トークン・バケットおよび帯域幅の限界

トークン・バケット限界と帯域幅限界はともにパフォーマンス制限として知られています。これらのパフォーマンス制限によって、アウトバウンド帯域幅ポリシー (IntServ および DiffServ の両方) 内でのパケットの送達が保証されます。

トークン・バケット・サイズ

*トークン・バケット・サイズ*は、システムが任意の時点に処理できる情報量を決定します。 システムがネットワークからデータを送り出す速度よりアプリケーションがシステムに情報を送る速度が速い場合、バッファーがいっぱいになります。 この限界を超えるデータ・パケットはアウト・オブ・プロファイルとして処理されます。 IntServ ポリシーはこの規則の例外です。 IntServ ポリシーでは「制限しない」を選択でき、ReSerVation Protocol (RSVP) 接続要求が可能になります。 他のすべてのポリシーでは、プロファイル外トラフィックの処理方法を決定できます。最大トークン・バケット・サイズは 1 GB です。

トークン速度限界

トークン速度限界 は、長期データ転送速度またはネットワーク内に許容されるビット/秒の数を指定します。Quality of Service (QoS) ポリシーは要求された帯域幅を調べ、それとこのポリシーの速度およびフロー限界を比較します。 要求が、システムが限界を超える原因となる場合、システムは要求を否認します。トークン速度限界は、IntServ ポリシー内の許可制御のみに使用されます。 この値の範囲は 10 kbps から 1 Gbps です。この値を「制限しない」に設定することもできます。速度に「制限しない」を割り当てた場合には、使用可能なリソースを制限する必要があります。

ヒント: 設定する限界を決めるために、モニターを実行することができます。ネットワーク上のほとんどのデータ・トラフィックを収集するために、集約トークン速度限界の大きさを十分にとったポリシーを作成します。 次に、このポリシーでデータ収集を開始します。現在のネットワーク統計のモニターに関するシナリオには、ご使用のアプリケーションおよびネットワークが現在使用する合計速度を収集する 1 つの方法が示されています。これらの結果を使用して、限界を適切に削減することができます。

特定のデータ収集ではなくリアルタイム・モニター・データを表示するには、モニターを開いてください。モニターにはすべてのアクティブ・ポリシーに関するリアルタイム統計が表示されます。

関連概念

2 ページの『DiffServ』
これは、オペレーティング・システムで作成できるアウトバウンド帯域幅ポリシーの第 1 のタイプです。DiffServ はトラフィックをクラスに分割します。 DiffServ ポリシーをインプリメントするには、ネットワーク・トラフィックの分類方法とさまざまなクラスの処理方法を決定する必要があります。

52 ページの『シナリオ: 現在のネットワーク統計のモニター』
ウィザードの中で、個々のネットワーク要件に基づくパフォーマンス制限を設定する必要があります。

DiffServ マーク付けのある IntServ

IntServ ポリシーの中で DiffServ マーク付けを使用して、混合環境で送信されるパケットの優先順位を維持することができます。

IntServ 予約はサポートしないが、DiffServ をサポートするさまざまなルーターを IntServ 予約が通過する場合、混合環境が生じます。トラフィックは、さまざまな異なるドメイン、サービス・レベル・アグリーメント (SLA)、および、さまざまな機能を持つ装置を通過するので、常に意図するサービスを得られるとは限りません。

この潜在的な問題を減少させるために、DiffServ マーク付けを IntServ ポリシーに付加することができます。ポリシーが、ReSerVation Protocol (RSVP) を使用できないルーターを行き交っても、ポリシーはいくらかの優先順位を保持します。追加するマーク付けは、*PHB (ホップごとの転送優先順位付け)* といいます。

非信号送出

マーク付けの使用に加えて、新しい「非信号送出」機能を使用することもできます。 API の「非信号送出」バージョンであるこの機能を選択した場合は、オペレーティング・システムに RSVP 規則がロードされるようにするアプリケーションを作成できるようになります。このアプリケーションでは、TCP/IP 会話のサーバー側アプリケーションを RSVP 使用可能にするだけで済みます。RSVP 信号送出方式は、クライアント・サイドのために自動的に実行されます。これにより、クライアント・サイドが RSVP を使用できない場合でも、アプリケーションの RSVP 接続が可能になります。

「非信号送出」機能は、IntServ ポリシー内に指定します。「非信号送出」機能を指定するには、以下のステップを実行します。

1. System i ナビゲーター で、**「ユーザーのシステム」** → **「ネットワーク」** → **「IP ポリシー」**の順に展開します。
2. **「Quality of Service」**を右マウス・ボタンでクリックし、**「構成」**を選択します。
3. **「アウトバウンド帯域幅ポリシー」** → **「IntServ」**を展開します。
4. 必要な IntServ ポリシー名を右マウス・ボタンでクリックして、**「プロパティー」**を選択します。「IntServ プロパティー」ウィンドウが開きます。
5. **「トラフィック管理」**タブを選択して、信号送出を使用不可または使用可能にします。このダイアログではスケジュール、クライアント、アプリケーション、およびトラフィック管理を編集できます。

関連概念

14 ページの『サービス・クラス』
DiffServ ポリシーまたはインバウンド許可ポリシーを作成するときは、サービス・クラスも作成して使用します。

7 ページの『IntServ』
作成できるアウトバウンド帯域幅ポリシーの第 2 のタイプは、IntServ ポリシーです。 IntServ によって、IP アプリケーションは、ReSerVation Protocol (RSVP) と QoS API を使用して帯域幅を要求し予約することができます。

インバウンド許可ポリシー

インバウンド許可ポリシーは、ネットワークに着信する接続要求を制御します。

インバウンド許可ポリシーは、システムに接続しようとするトラフィックを制限するために使用されます。アクセスは、クライアント、Uniform Resource Identifier (URI)、アプリケーション、またはシステムのローカル・インターフェースにより制限できます。さらに、インバウンド・トラフィックにサービス・クラスを適用して、システムのパフォーマンスを強化することができます。 このポリシーは、System i ナビゲーター のインバウンド許可ウィザードを使用して定義します。

インバウンド・ポリシーには、さらに知っておかねばならない 3 つのコンポーネントがあります。それらは、トラフィックを制限する URI、サービス・クラスで定義されている接続率、および正常な接続の順序を制御する優先待ち行列です。詳しくは、『URI』、 14 ページの『接続率』、および 14 ページの『優先待ち行列の重み』を参照してください。

URI

Web サーバーに接続する HTTP トラフィックを制限するために、インバウンド・ポリシーの使用を考慮する必要があります。この環境では、インバウンド許可ポリシーを作成して、特定の URI のトラフィックを制限する必要があります。 URI 要求率は、サーバーを過負荷から保護するのに役立つソリューションの一部です。サーバーが受け入れる URI 要求を制限するために、アプリケーション・レベルの情報に基づいて、許可制御を適用する特定の URI を指定します。業界では、これを、優先順位を設定するために URI を使用するヘッダー・ベースの接続制御とも呼んでいます。

URI を指定することにより、パケット・ヘッダーだけでなくコンテンツもインバウンド・ポリシーで検査することができます。検査されるコンテンツは URI 名です。 i5/OS オペレーティング・システムでは相対 URI 名 (例えば、 `/products/clothing`) を使用できます。

相対 URI

相対 URI は、実際には絶対 URI のサブセットです (旧絶対 URL と類似)。 http://www.ibm.com/software の例について考慮してみます。*http://www.ibm.com/software* セグメントは、絶対 URI と見なされます。*/software* セグメントは、相対 URI です。すべての相対 URI 値は、1 個のスラッシュ (**/**) で始まっていなければなりません。以下のセグメントは、有効な相対 URI の例です。

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

注:

- URI を使用する場合、プロトコルには TCP を指定しなければなりません。また、ポートおよび IP アドレスは、HTTP サーバーに構成したポートおよび IP アドレスと一致しなければなりません。通常はポート 80 です。
- URI を指定するには暗黙のワイルドカードがあります。例えば /software は、software ディレクトリー内のすべてを含んでいます。
- URI には * は使用しないでください。これは有効な文字ではありません。

- URI 情報は、インバウンド・ポリシーまたは DiffServ (アウトバウンド) ポリシーで使用できます。

URI を使用するインバウンド・ポリシーをセットアップする前に、URI に割り当てるアプリケーション・ポートを、Apache Web サーバー構成で Fast Response Cache Accelerator (FRCA) 用に使用可能になっている Listen ディレクティブに一致させる必要があります。ご使用の HTTP サーバーのポートを変更または表示するには、トピック『Manage addresses and ports for your HTTP server (powered by Apache)』を参照してください。

接続率

インバウンド許可ポリシーの一部として、サービス・クラスも選択する必要があります。このサービス・クラスは、システムが受け入れる接続を制限するために、許可制御として機能する接続速度を定義します。

接続率は、作成するポリシーで定義される秒当たりの平均接続数および瞬間最大接続数を基にして、新規パケットの受け入れまたは否認を制限します。これらの接続制限の内容は平均率およびバースト限界からなり、System i ナビゲーター のウィザードで入力します。着信接続要求がオペレーティング・システムに到着すると、システムはパケット・ヘッダー情報を分析して、このトラフィックがポリシー内で定義されているかどうかを判別します。システムは、この情報を接続制限プロファイルと対比して検証します。パケットがポリシー限界内である場合は、そのパケットは待ち行列に入れられます。

上記の情報を使用して、インバウンド許可ウィザードを完了します。 System i ナビゲーター では、ヘルプを使用して、ポリシーの作成時に同様の情報を参照できます。

優先待ち行列の重み

このインバウンド制御の一部として、接続要求がポリシーに評価された後で、処理される優先順位を指定することができます。優先待ち行列に重みを割り当てることにより、接続要求が着信した後の待ち行列の応答時間を制御することになります。待ち行列に入れられた場合、接続は待ち行列優先順位 (高、中、低、またはベストエフォート) の順に処理されます。 割り当てる重みがわからない場合は、デフォルト値を使用してください。すべての重みの和は 100 です。例えば、すべての優先順位を 25 と指定した場合、すべての待ち行列が同等に処理されます。 仮に、高 (50)、中 (30)、低 (15)、ベストエフォート (5) の重みを指定したとします。受け入れられる接続の比率は次のようになります。

- 高優先度の接続 50%
- 中優先度の接続 30%
- 低優先度の接続 15%
- ベストエフォート優先度の接続 5%

関連概念

『サービス・クラス』
DiffServ ポリシーまたはインバウンド許可ポリシーを作成するときは、サービス・クラスも作成して使用します。

18 ページの『平均接続率およびバースト限界』
接続率およびバースト限界は、速度限界です。これらの速度限界は、システムに入ろうとするインバウンド接続を制限するのに役立ちます。 速度限界はインバウンド許可ポリシーで使用するサービス・クラスに設定します。

サービス・クラス

DiffServ ポリシーまたはインバウンド許可ポリシーを作成するときは、サービス・クラスも作成して使用します。

DiffServ ポリシーとインバウンド許可ポリシーでは、サービス・クラスを使用してトラフィックをクラスに分類します。 このクラス分けのほとんどはハードウェアで行なわれますが、トラフィックのクラス分け方法とトラフィックが受け取る優先順位は、ユーザーが制御します。

QoS (Quality of Service) を実行する際、最初にポリシーを定義します。 ポリシーで、だれが、なにを、どこで、いつ、といった詳細を決定します。次にサービス・クラスをポリシーに割り当てます。サービス・クラスは個別に定義するので、ポリシーが再利用できます。サービス・クラスを定義する際、そのクラスをアウトバウンド・ポリシー、インバウンド・ポリシー、またはこの両方のポリシー・タイプに適用できるかどうかを指定します。両方 (アウトバウンドとインバウンド) を選択した場合は、DiffServ ポリシーとインバウンド許可ポリシーがそのサービス・クラスを使用できます。

サービス・クラス内での設定値は、そのサービス・クラスがインバウンド・ポリシー、アウトバウンド・ポリシー、または両方のポリシー・タイプに使用されるかどうかに依存します。サービス・クラスを作成する際、次のような要件があります。

コード・ポイント・マーク付け

QoS は、トラフィックに対して、業界推奨のコード・ポイントを使用した PHB (ホップごとの転送優先順位付け) の割り当てを行います。ルーターとスイッチは、これらのコード・ポイントを使用してトラフィックに優先順位レベルを与えます。ご使用のシステムは、ルーターとして動作していないので、これらのコード・ポイントを使用できません。 ネットワークの個別のニーズに基づいて、使用するコード・ポイントを決める必要があります。最も重要なアプリケーションはどれか、どのポリシーに高い優先順位を割り当てるかについて、考慮してください。最も重要なことは、マーク付けと一貫性を持たせることです。それによって、期待した結果が得られます。 これらのコード・ポイントは、トラフィックのさまざまなクラスを区別する上でキーとなります。

トラフィック計量

QoS は、速度制御限界を利用して、ネットワークを通るトラフィックを制限します。これらの制限を設けるには、トークン・バケット・サイズ、ピーク速度限界、および平均速度限界を設定します。これらの特定値の詳細については、11 ページの『トークン・バケットおよび帯域幅の限界』を参照してください。

プロファイル外トラフィック

サービス・クラスの最後の分担は、プロファイル外処理です。速度制御限界を割り当てる際に、トラフィックを制限する値を設定します。 トラフィックが制限値を超えると、そのパケットはプロファイル外と見なされます。システムは、サービス・クラス内のこの情報から、UDP トラフィックを廃棄して TCP 輻輳 (ふくそう) ウィンドウを縮小するか、シェイピング (遅延) するか、またはプロファイル外パケットを再マーク付けするかを判断します。

UDP パケットの廃棄または TCP 輻輳 (ふくそう) ウィンドウの縮小 : プロファイル外パケットの廃棄と調整を決定した場合は、UDP パケットは廃棄されます。 しかし、TCP 輻輳 (ふくそう) ウィンドウが縮小されるので、データ速度はトークン・バケット速度に合わせられます。 任意の時点でネットワークに送り出せるパケットの数が減少し、輻輳 (ふくそう) が緩和されます。

遅延 (シェイピング): プロファイル外パケットを遅延させると、これらのパケットは定義された処理特性に適合するようにシェイピングされます。

DiffServ コード・ポイントによる再マーク付け: コード・ポイントでプロファイル外パケットを再マーク付けすると、それらのパケットには新しいコード・ポイントが割り当てられます。 パケットは処理特性に適合するように絞り込まれるのではなく、再マーク付けされるだけです。 ウィザードでこの処理指示を割り当てる時、「ヘルプ」をクリックして詳しい情報をご確認ください。

優先順位

各種のインバウンド許可制御ポリシーを使用して、システムとの接続の優先順位付けを行うことが

できます。 これにより、システムが完了した接続を処理する順序を定義できます。選択できる優先順位は、高、中、低、またはベストエフォートです。

関連概念

12 ページの『DiffServ マーク付けのある IntServ』
IntServ ポリシーの中で DiffServ マーク付けを使用して、混合環境で送信されるパケットの優先順位を維持することができます。

13 ページの『インバウンド許可ポリシー』
インバウンド許可ポリシーは、ネットワークに着信する接続要求を制御します。

2 ページの『DiffServ』
これは、オペレーティング・システムで作成できるアウトバウンド帯域幅ポリシーの第 1 のタイプです。DiffServ はトラフィックをクラスに分割します。 DiffServ ポリシーをインプリメントするには、ネットワーク・トラフィックの分類方法とさまざまなクラスの処理方法を決定する必要があります。

関連資料

『コード・ポイントを使用した PHB (ホップごとの転送優先順位付け) の割り当て』
Quality of Service (QoS) は、業界推奨コード・ポイントを使用して、トラフィックに PHB (ホップごとの転送優先順位付け) を割り当てます。

コード・ポイントを使用した PHB (ホップごとの転送優先順位付け) の割り当て

Quality of Service (QoS) は、業界推奨コード・ポイントを使用して、トラフィックに PHB (ホップごとの転送優先順位付け) を割り当てます。

サービス・クラス・ウィザードを使用して、ポリシーに PHB (ホップごとの転送優先順位付け) を割り当てる必要があります。 ネットワークの個別のニーズに基づいて、使用するコード・ポイントを決める必要があります。 どのコード・ポイント・スキームを自分の環境で使用するかを決定できるのは、自分のみです。最も重要なアプリケーションはどれか、どのポリシーに高い優先順位を割り当てるかについて、考慮してください。最も重要なことは、マーク付けと一貫性を持たせることです。それによって、期待した結果が得られます。重要度が同じであるポリシーでは同じコード・ポイントを使用して、これらのポリシーの結果に一貫性を持たせることができます。割り当てるコード・ポイントがわからない場合は、試行錯誤手法を行います。 テスト・ポリシーを作成し、これらのポリシーをモニターし、必要に応じて調整することができます。

次のセクションの表に、業界標準に基づいて推奨されているコード・ポイントを示します。 ほとんどのインターネット・サービス・プロバイダー (ISP) は業界標準のコード・ポイントをサポートしており、ご使用の ISP がこれらのコード・ポイントをサポートしているかどうかを調べることができます。 複数のドメインにわたり、すべての ISP は QoS 要求のサポートに合意していなくてはなりません。サービス・レベル・アグリーメント (SLA) は、ポリシーに、そのポリシーが要求するものを提供できなくてはなりません。現在、必要な量のサービスを受けているかを確認してください。受けていない場合は、リソースを無駄にしている可能性があります。 QoS ポリシーでは、ISP とサービス・レベルを折衝することが可能であり、その結果ネットワーク・サービス・コストが削減されることがあります。 また、独自のコード・ポイントを作成することもできますが、外部での使用はお勧めしません。独自のコード・ポイントはテスト環境で使用するのが最良です。

優先転送

優先転送は PHB (ホップごとの転送優先順位付け) のタイプの 1 つです。 優先転送は、主にネットワークにおける保証サービスの提供に使用されます。優先転送は、ネットワーク全体にわたって帯域幅を保証することで、脱落およびジッターの少ないエンドツーエンド・サービスをトラフィックに提供します。パケットが送信される前に予約が行なわれます。主な目的は、遅延を防ぎ、パケットを適時に送信することです。

表 1. 推奨コード・ポイント: 優先転送

優先転送
101110

注: 優先転送処理は通常はコストが高いので、この PHB (ホップごとの転送優先順位付け) の常用はお勧めしません。

クラス・セレクター

クラス・セレクター・コード・ポイントは、PHB のもう 1 つのタイプです。クラスは 7 つあります。クラス 0 はパケットに最低優先順位を与え、クラス 7 はクラス・セレクターのコード・ポイント値の範囲内で、パケットに最高の優先順位を与えます。これは PHB の最も一般的なものです。なぜなら、ほとんどのルーターは既に類似したコード・ポイントを使用しています。

表 2. 推奨コード・ポイント: クラス・セレクター

クラス・セレクター
クラス 0 - 000000
クラス 1 - 001000
クラス 2 - 010000
クラス 3 - 011000
クラス 4 - 100000
クラス 5 - 101000
クラス 6 - 110000
クラス 7 - 111000

保証転送

保証転送は、4 つの PHB クラスにわかれており、各クラスに廃棄優先順位 (低、中、高) があります。廃棄優先順位によって、パケットの廃棄の可能性が決まります。各クラスには、それぞれ独自の帯域幅仕様があります。「クラス 1、高」の場合、ポリシーには最低優先順位が与えられ、「クラス 4、低」の場合はポリシーに最高優先順位が与えられます。 廃棄レベルが「低」とは、このポリシーの中のパケットは、この特定のクラス・レベルで廃棄される可能性が最も低いという意味です。

表 3. 推奨コード・ポイント: 保証転送

保証転送
保証転送、クラス 1、低 - 001010
保証転送、クラス 1、中 - 001100
保証転送、クラス 1、高 - 001110
保証転送、クラス 2、低 - 010010
保証転送、クラス 2、中 - 010100
保証転送、クラス 2、高 - 010110
保証転送、クラス 3、低 - 011010
保証転送、クラス 3、中 - 011100
保証転送、クラス 3、高 - 011110
保証転送、クラス 4、低 - 100010

表 3. 推奨コード・ポイント: 保証転送 (続き)

保証転送
保証転送、クラス 4、中 - 100100
保証転送、クラス 4、高 - 100110

関連概念

2 ページの『DiffServ』
これは、オペレーティング・システムで作成できるアウトバウンド帯域幅ポリシーの第 1 のタイプです。DiffServ はトラフィックをクラスに分割します。 DiffServ ポリシーをインプリメントするには、ネットワーク・トラフィックの分類方法とさまざまなクラスの処理方法を決定する必要があります。

14 ページの『サービス・クラス』
DiffServ ポリシーまたはインバウンド許可ポリシーを作成するときは、サービス・クラスも作成して使用します。

平均接続率およびバースト限界

接続率およびバースト限界は、速度限界です。これらの速度限界は、システムに入ろうとするインバウンド接続を制限するのに役立ちます。 速度限界はインバウンド許可ポリシーで使用するサービス・クラスに設定します。

接続バースト率

バースト限界により、接続バーストを保持するバッファー容量が決定されます。 接続バーストは、システムが処理できるより速い速度で、あるいは許可したい速度より速い速度でシステムに入ることです。バースト内の接続数が、設定した接続バースト限界を超えた場合には、それ以上の接続は廃棄されます。

平均接続率

平均接続率は、システム内で許可された受け入れられた Uniform Resource Identifier (URI) 要求の、新規に確立された接続または率の限界を指定します。 設定した限界をシステムが超える原因となる要求は、システムにより否認されます。 平均接続要求限界は、毎秒ごとの接続で測られます。

ヒント: 設定する限界を決めるために、モニターを実行することができます。現在のネットワーク統計のモニターに関するシナリオには、システム上を移動する大部分のデータの収集に役立つサンプル・ポリシーが記載されています。 これらの結果を使用して、適切な限界に調整することができます。

特定のデータ収集ではなくリアルタイム・モニター・データを表示するには、モニターを開いてください。モニターにはすべてのアクティブ・ポリシーに関するリアルタイム統計が表示されます。

関連概念

13 ページの『インバウンド許可ポリシー』
インバウンド許可ポリシーは、ネットワークに着信する接続要求を制御します。

52 ページの『シナリオ: 現在のネットワーク統計のモニター』
ウィザードの中で、個々のネットワーク要件に基づくパフォーマンス制限を設定する必要があります。

Quality of Service API

このトピックには、プロトコルと API に関する情報、および ReSerVation Protocol (RSVP) で使用可能なルーターに関する要件が記載されています。Quality of Service (QoS) API には、RAPI API、qtoq ソケット API、sendmsg() API、およびモニター API が含まれています。

大部分の QoS ポリシーでは API の使用が必要です。以下の API は、DiffServ ポリシーまたは IntServ ポリシーと組み合わせて使用できます。さらに、QoS モニターと共に使用される多数の API があります。

- 『IntServ API』
- 『DiffServ API』
- 20 ページの『モニター API』

IntServ API

RSVP は、RAPI API または qtoq QoS ソケット API と共に IntServ の予約を行います。トラフィックが通過する各ノードには、RSVP を使用する能力が備わっている必要があります。この IntServ ポリシーを実行する能力があることを、しばしば RSVP 使用可能 であるといいます。 トラフィック制御機能を使用して、RSVP を使用するにはどのルーター機能が必要であるかを判断することができます。

RSVP は、トラフィックのパスに存在するすべてのネットワーク・ノードでの RSVP 予約の作成に使用されます。 RSVP プロトコルは、要求されたサービスをポリシーに提供する期間中、この予約を保持します。 予約は、この対話でデータが必要とする処理と帯域幅を定義します。 ネットワーク・ノードは、予約で定義されているデータ処理を実行します。

RSVP は単純なプロトコルであり、予約は (受信側から) 一方向でのみ行われます。オーディオ/ビデオ会議などのより複雑な接続の場合は、送信側のそれぞれが受信側でもあります。この場合、それぞれの側で 2 つの RSVP セッションをセットアップする必要があります。

RSVP 使用可能ルーターに加えて、IntServ を使用するためには RSVP 使用可能アプリケーションも必要です。最初はシステムに RSVP 使用可能アプリケーションがないので、RAPI API または qtoq QoS ソケット API を使用してアプリケーションを作成する必要があります。これらの API により、アプリケーションは RSVP を使用できるようになります。 詳しい説明が必要な場合は、これらのモデル、その操作、およびメッセージ処理に関する多数の資料がありますので、それらを参照してください。RSVP およびインターネット RFC 2205 の内容についての理解を深める必要があります。

qtoq ソケット API

qtoq QoS ソケット API を使用して、システム上で RSVP を使用するのに必要な作業を単純化できるようになりました。 qtoq ソケット API は RAPI API を呼び出して、より複雑なタスクの一部を実行します。qtoq ソケット API は、RAPI API ほど柔軟ではありませんが、少ない負荷で同じ機能を提供します。 API の「非信号送出方式」バージョンにより、下記のアプリケーションを作成することができます。

- システム上に RSVP 規則をロードするアプリケーション。
- TCP/IP 会話のサーバー側アプリケーションを RSVP 使用可能にするだけのアプリケーション。

RSVP 信号送出方式は、クライアント・サイドのために自動的に実行されます。

コネクション型またはコネクションレスの qtoq QoS ソケットを使用するアプリケーションまたはプロトコルの典型的な QoS API フローについては、『QoS API コネクション型機能フロー』または『QoS API コネクションレス機能フロー』を参照してください。

DiffServ API

注: sendmsg() API は、特定のアプリケーション・トークンを定義する特定の DiffServ ポリシーに使用されます。 DiffServ ポリシーを作成するときは、(オプションで) アプリケーション特性 (トークンおよ

び優先順位) を指定できます。 これは拡張ポリシー定義であり、使用しない場合はこの API を無視することができます。ただし、ルーターおよびネットワーク・パスにあるその他のシステムは DiffServ 使用可能である必要があります。

DiffServ ポリシーでアプリケーション・トークンを使用することに決めた場合、この情報を提供するアプリケーションでは sendmsg() API の使用を明確にコード化しておく必要があります。 これはアプリケーション・プログラマーの役割です。アプリケーションの文書には有効な値 (トークンおよび優先順位) を記載し、QoS 管理者が DiffServ ポリシーに使用できるようにします。 その場合、DiffServ ポリシーは、ポリシー内に設定されたトークンに一致するトラフィックにそのポリシーの優先順位と分類を適用します。 ポリシーに設定された値に一致する値がアプリケーションにない場合は、アプリケーションを変更するか、または DiffServ ポリシーに別のアプリケーション・データ・パラメーターを使用することが必要になります。

以下に、アプリケーション・トークンおよびアプリケーション優先順位の 2 つのシステム・データ・パラメーターについて簡単に説明します。

アプリケーション・トークンの概念

アプリケーション・トークンは、定義済みリソースを表す Uniform Resource Identifier (URI) です。 QoS ポリシーに指定したトークンは、アウトバウンド・アプリケーションが提供するトークンと突き合わせされます。 アプリケーションは sendmsg() API を使用してトークン値を提供します。 2 つのトークンが一致すると、アプリケーション・トラフィックは DiffServ ポリシーに組み込まれます。

アプリケーション優先順位の概念

ポリシーに指定したアプリケーション優先順位は、アウトバウンド・アプリケーションが提供するアプリケーション優先順位と突き合わせされます。アプリケーションは sendmsg() API を使用して優先順位の値を提供します。 2 つの優先順位が一致すると、アプリケーション・トラフィックは DiffServ ポリシーに組み込まれます。 DiffServ ポリシーに定義されているすべてのトラフィックは、ポリシー全体に指定されている優先順位を引き続き受け取ります。

DiffServ ポリシー・タイプについて詳しくは、2 ページの『DiffServ』 を参照してください。

モニター API

RSVP (Resource Reservation Setup Protocol) API には、モニター API が含まれています。モニターに適用される API は、その名称に monitor というワードを含んでいます。 例: *QgyOpenListQoSMonitorData*。以下に、それぞれのモニター API について簡単に説明します。

- QgyOpenListQoSMonitorData (QoS モニター・データ・リストのオープン) は、QoS サービスに関連した情報を収集します。
- QtoqDeleteQoSMonitorData (QoS モニター・データの削除) は、収集された QoS モニター・データの 1 つ以上のセットを削除します。
- QtoqEndQoSMonitor (QoS モニターの終了) は、QoS サービスに関連した情報の収集を停止します。
- QtoqListSavedQoSMonitorData (保管済み QoS モニター・データのリスト) は、前に保管されたすべての収集済みモニター・データのリストを戻します。
- QtoqSaveQoSMonitorData (QoS モニター・データの保管) は、収集された QoS モニター・データのコピーを、将来の使用のために保管します。
- QtoqStartQoSMonitor (QoS モニターの開始) は、QoS サービスに関連した情報を収集します。

関連概念

7 ページの『IntServ』
作成できるアウトバウンド帯域幅ポリシーの第 2 のタイプは、IntServ ポリシーです。 IntServ によって、IP アプリケーションは、ReSerVation Protocol (RSVP) と QoS API を使用して帯域幅を要求し予約することができます。

9 ページの『トラフィック制御機能』
トラフィック制御機能は、IntServ にのみ適用されますが、System i 製品に固有のものではありません。

44 ページの『シナリオ: 予測可能な B2B トラフィック』
予測可能な送達が必要で、引き続き予約を要求したい場合は、IntServ ポリシーも使用します。 この例では、負荷制御サービスを使用します。

57 ページの『ネットワークのハードウェアおよびソフトウェア』
ネットワーク内部の装置とネットワーク外部の他の装置の能力は、Quality of Service (QoS) の結果に非常に大きく影響します。

関連資料

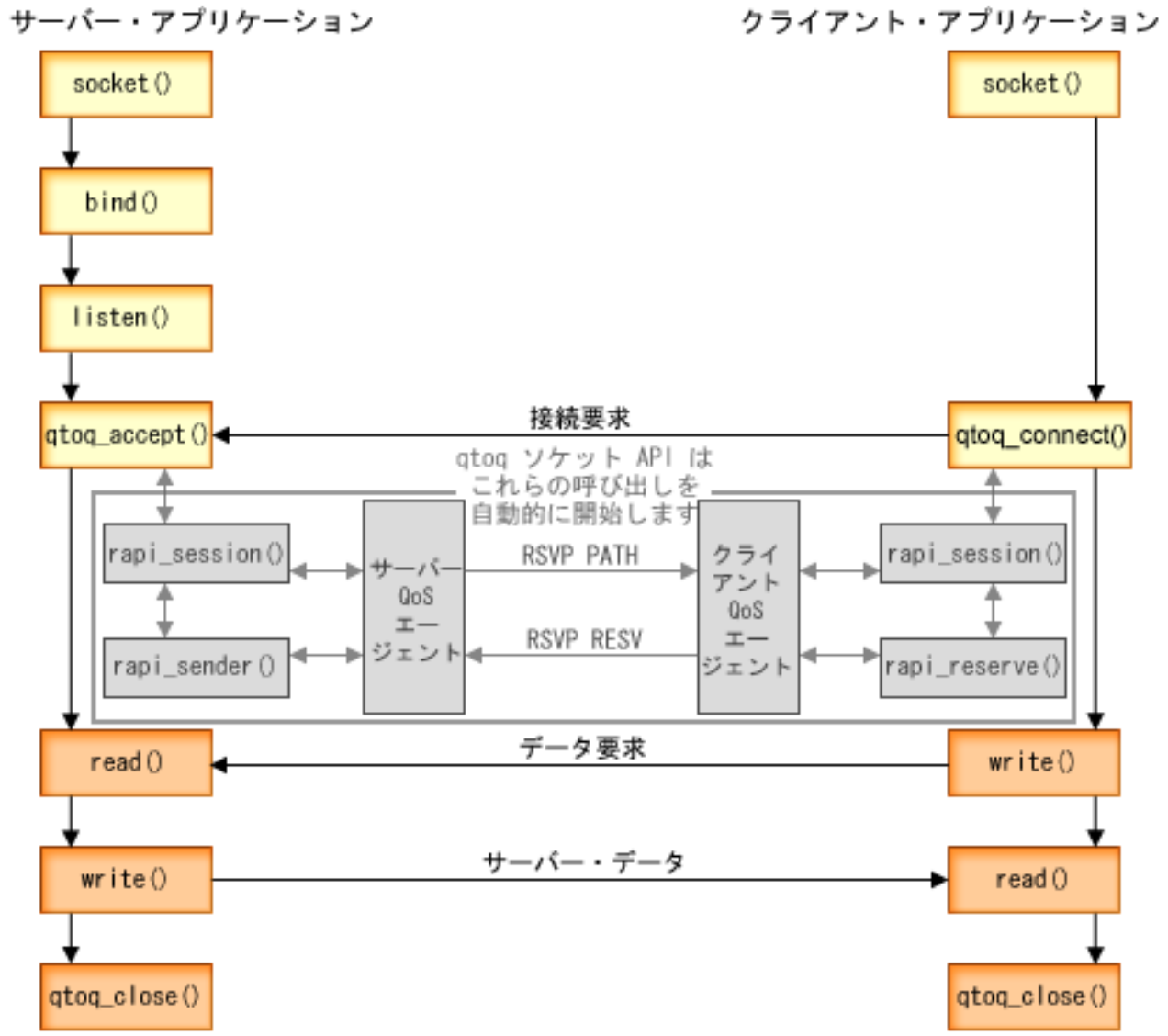
Resource Reservation Setup Protocol API

58 ページの『ウィザードを使用した QoS の構成』
Quality of Service (QoS) ポリシーを構成するには、System i ナビゲーター にある QoS ウィザードを使用してください。

QoS API コネクション型機能フロー

このトピックの中のサーバーとクライアントの例では、コネクション型機能フロー用に書かれた qtoq QoS (Quality of Service) ソケット API を示します。

ReSerVation Protocol (RSVP) の始動を要求するコネクション型フローのために、QoS 使用可能 API 関数が呼び出されると、その他の関数も開始されます。これらの追加の関数により、クライアントおよびサーバー上の QoS エージェントは、クライアントとサーバーとの間のデータ・フローのための RSVP をセットアップします。



イベントの qtoq フロー: 次のソケット呼び出し手順では、上図について説明しています。 また、コネクション型設計でのサーバー・アプリケーションとクライアント・アプリケーション間の関係についても説明しています。これらは基本ソケット API を修正したものです。

サーバー側

「非信号送出方式」とマーク付けされた規則に関する qtoq_accept() API

1. アプリケーションは socket() 関数を呼び出し、ソケット記述子を取得します。
2. アプリケーションは listen() を呼び出し、どの接続を待つのかを示します。
3. アプリケーションは qtoq_accept() を呼び出し、クライアントからの接続要求を待ちます。
4. API は rapi_session() API を呼び出します。正常に行われると、QoS セッション ID が割り当てられます。
5. API は標準 accept() 関数を呼び出し、クライアントの接続要求を待ちます。

6. 接続要求が受信されると、要求された規則に関して許可制御が行われます。規則は TCP/IP スタックに送られます。この規則は、有効である場合は、その結果とセッション ID と一緒に呼び出し側アプリケーションに戻されます。
7. サーバーとクライアントのアプリケーションは、要求されたデータ転送を実行します。
8. アプリケーションは qtoq_close() 関数を呼び出し、ソケットをクローズして規則をアンロードします。
9. QoS サーバーは、その規則を QoS マネージャーから削除し、QoS セッションを削除し、さらに必要とされる他のアクションをすべて実行します。

通常の RSVP 信号送出方式による qtoq_accept()

1. アプリケーションは socket() 関数を呼び出し、ソケット記述子を取得します。
2. アプリケーションは listen() を呼び出し、どの接続を待つのかを示します。
3. アプリケーションは qtoq_accept() を呼び出し、クライアントからの接続要求を待ちます。
4. 接続要求が届くと、rapi_session() API が呼び出されます。この API が、この接続に関する QoS サーバーとのセッションを作成し、呼び出し元に戻されることになる QoS セッション ID を取得します。
5. rapi_sender() API が呼び出され、QoS サーバーから PATH メッセージを送り、 QoS サーバーにクライアントからの RESV メッセージが必要であること知らせます。
6. rapi_getfd() API が呼び出され、 QoS イベント・メッセージを待つためにアプリケーションが使用する記述子を取得します。
7. 受け入れ記述子および QoS 記述子は、アプリケーションに戻されます。
8. QoS サーバーは、RESV メッセージが受信されるのを待ちます。メッセージが受信されると、QoS サーバーは、QoS マネージャーを使用して適切な規則をロードし、アプリケーションにメッセージを送信します (アプリケーションが qtoq_accept() API 呼び出しに関する通知を要求した場合)。
9. QoS サーバーは、確立されたセッションへの最新表示の提供を継続します。
10. アプリケーションは、この接続の完了時に qtoq_close() を呼び出します。
11. QoS サーバーは、その規則を QoS マネージャーから削除し、QoS セッションを削除し、さらに必要とされる他のアクションをすべて実行します。

クライアント・サイド

通常の RSVP 信号送出方式による qtoq_connect()

1. アプリケーションは socket() 関数を呼び出し、ソケット記述子を取得します。
2. アプリケーションは、qtoq_connect() 関数を呼び出して、接続を望んでいることをサーバーに通知します。
3. qtoq_connect() 関数は、この接続に関する QoS サーバーとのセッションを作成するために、rapi_session() API を呼び出します。
4. QoS サーバーは、要求された接続からの PATH コマンドを待つためにプライム状態になります。
5. rapi_getfd() API が呼び出され、 QoS メッセージを待つためにアプリケーションが使用する QoS 記述子を取得します。
6. connect() 関数が呼び出されます。 connect() の結果および QoS 記述子は、アプリケーションに戻されます。
7. QoS サーバーは、PATH メッセージが受信されるのを待ちます。メッセージが受信されると、QoS サーバーは、アプリケーション・サーバー・マシン上の QoS サーバーに対する RESV メッセージで応答します。

8. アプリケーションが通知を要求した場合は、QoS サーバーは、QoS 記述子を使用してアプリケーションに通知を送ります。
9. QoS サーバーは、確立されたセッションへの最新表示の提供を継続します。
10. アプリケーションは、この接続の完了時に qtoq_close() を呼び出します。
11. QoS サーバーは QoS セッションをクローズし、他の必要なアクションをすべて実行します。

「非信号送出方式」とマーク付けされた規則に関する qtoq_connect() API

この要求はクライアント・サイドでは無効です。この場合はクライアントからの応答が不要であるためです。

関連資料

qtoq_accept() -- QoS ソケット接続 API の受け入れ

qtoq_close() -- QoS ソケット接続 API のクローズ

rapi_session() -- RAPI セッションの作成

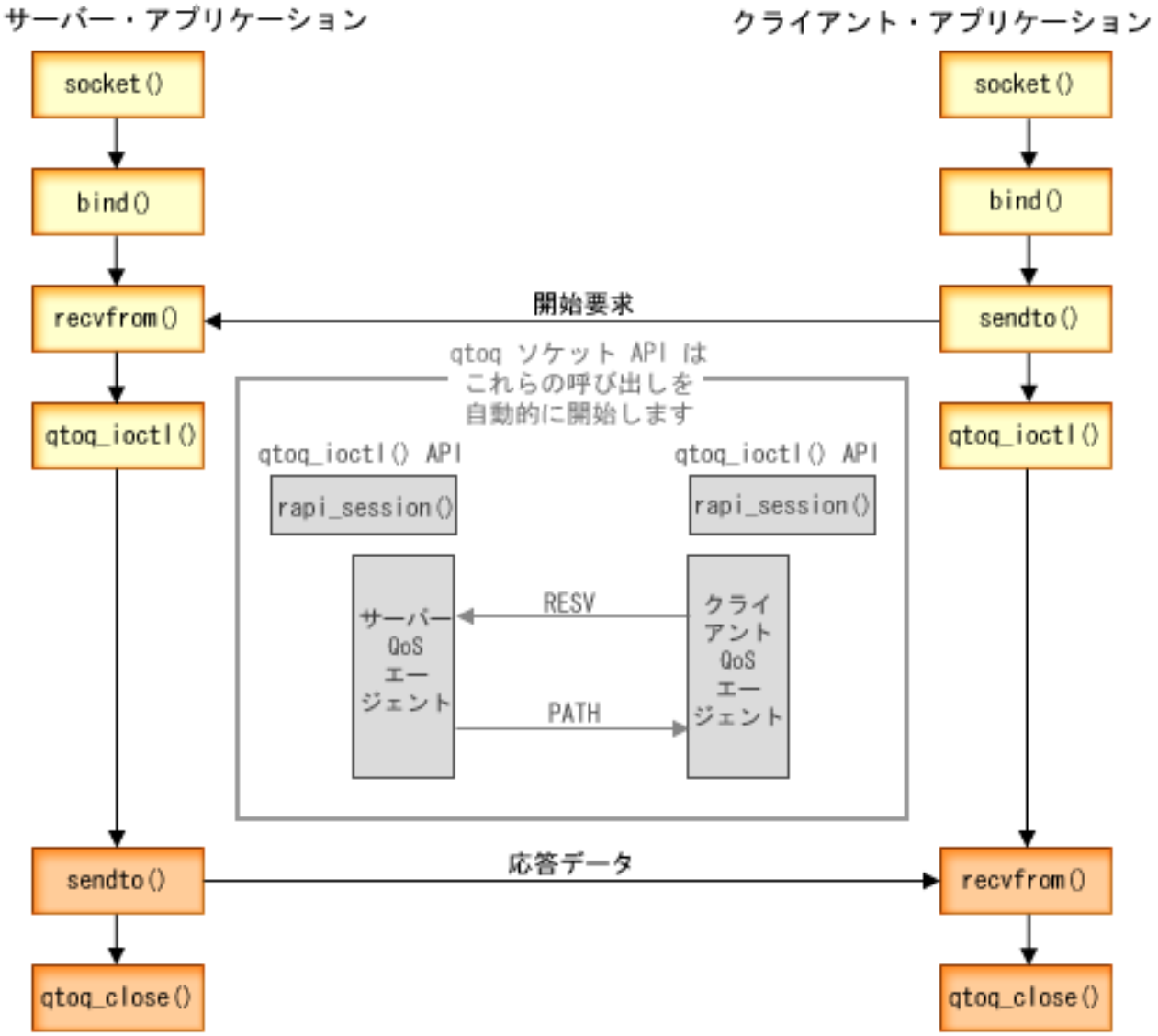
rapi_sender() -- RAPI 送信側の識別

rapi_getfd() -- 待機する記述子の取得

qtoq_connect() -- QoS ソケット接続 API の作成

QoS API コネクションレス機能フロー

QoS 使用可能 API 関数が、ReSerVation Protocol (RSVP) を開始するように要求するコネクションレス・フローのために呼び出されると、その他の関数も開始されます。 これらの追加の関数により、クライアントおよびサーバー上の QoS エージェントは、クライアントとサーバーとの間のデータ・フローのための RSVP をセットアップします。



イベントの qtoq フロー: 次のソケット呼び出し手順では、上図について説明しています。 また、コネクションレス設計でのサーバー・アプリケーションとクライアント・アプリケーション間の関係についても説明しています。これらは基本ソケット API を修正したものです。

サーバー側

「非信号送出方式」とマーク付けされた規則に関する qtoq_ioctl() API

1. qtoq_ioctl() API は、要求された規則に関して許可制御を実行するように求めるメッセージを QoS サーバーに送信します。
2. この規則が受け入れ可能な場合は、規則がロードされるように要求する QoS サーバーへのメッセージを送信する関数を呼び出します。
3. QoS サーバーは、この要求の成否を示す状況を呼び出し元に戻します。
4. アプリケーションが接続の使用を完了した時点で、アプリケーションは接続をクローズするために qtoq_close() 関数を呼び出します。

5. QoS サーバーは、その規則を QoS マネージャーから削除し、QoS セッションを削除し、さらに必要とされる他のアクションをすべて実行します。

通常の RSVP 信号送出方式による qtoq_ioctl() API

1. qtoq_ioctl() API は、要求された接続に関して許可制御を要求するメッセージを QoS サーバーに送信します。
2. QoS サーバーは、rapi_session() を呼び出して、その規則に応じてセッションをセットアップするように要求し、呼び出し元に戻される QoS セッション ID を取得します。
3. また、rapi_sender() を呼び出して、クライアントに PATH メッセージを送り返します。
4. 次に rapi_getfd() を呼び出して、QoS のイベントを待つためにファイル記述子を取得します。
5. QoS サーバーは、記述子 select()、QoS セッション ID、および状況を呼び出し元に戻します。
6. QoS サーバーは、RESV メッセージの受信時に規則をロードします。
7. アプリケーションは、この接続の完了時に qtoq_close() を発行します。
8. QoS サーバーは、その規則を QoS マネージャーから削除し、QoS セッションを削除し、さらに必要とされる他のアクションをすべて実行します。

クライアント・サイド

通常の RSVP 信号送出方式による qtoq_ioctl() API

1. qtoq_ioctl() API は、rapi_session() を呼び出して、セッションをこの接続に応じてセットアップするように要求します。 rapi_session() 関数は、この接続に関する許可制御を要求します。 この接続がクライアント・サイドで拒否されるのは、クライアント用に構成済みの規則が存在し、その規則がこの時点で活動状態ではない場合だけです。この関数は、渡される QoS セッション ID をアプリケーションに戻します。
2. rapi_getfd() を呼び出して、QoS のイベントを待つためにファイル記述子を取得します。
3. qtoq_ioctl() は呼び出し元に戻り、記述子およびセッション ID を待ちます。
4. QoS サーバーは、PATH メッセージが受信されるのを待ちます。 PATH メッセージが受信されると、QoS サーバーは、RESV メッセージで応答してから、セッション記述子を使用してアプリケーションにイベントが生じたことを信号送出します。
5. QoS サーバーは、確立されたセッションへの最新表示の提供を継続します。
6. このクライアント・コードでは、この接続の完了時に qtoq_close() を呼び出します。

「非信号送出方式」とマーク付けされた規則に関する qtoq_ioctl() API

この要求はクライアント・サイドでは無効です。この場合はクライアントからの応答が不要であるためです。

関連資料

qtoq_close() -- QoS ソケット接続 API のクローズ

rapi_session() -- RAPI セッションの作成

rapi_sender() -- RAPI 送信側の識別

rapi_getfd() -- 待機する記述子の取得

qtoq_ioctl() -- QoS ソケット制御オプション API の設定

QoS sendmsg() API 拡張機能

sendmsg() 機能は、接続ソケットまたは非接続ソケットを通して、データ、補助データ、またはそれらの組み合わせを送信するために使用されます。

sendmsg() API により、QoS (Quality of Service) 分類データが使用できます。 QoS ポリシーでは、この機能を使用して、発信または着信 TCP/IP トラフィックについて細分度のより高い分類レベルを定義します。QoS ポリシーでは、IP 層に適用される補助データ・タイプを特定的に使用します。使用されるメッセージ・タイプは IP_QOS_CLASSIFICATION_DATA です。アプリケーションではこの補助データを使用して、特定の TCP 接続のトラフィックの属性を定義できます。アプリケーションが渡す属性が QoS ポリシーに定義されている属性と一致する場合は、TCP トラフィックはそのポリシーにより制限されます。

IP_QOS_CLASSIFICATION_DATA 構造を初期設定するには、以下の情報を使用します。

- ip_qos_version: 構造のバージョンを示します。これは定数 *IP_QOS_CURRENT_VERSION* を使用して入力します。
- ip_qos_classification_scope: 接続レベルの有効範囲 (定数 *IP_QOS_CONNECTION_LEVEL* を使用) またはメッセージ・レベルの有効範囲 (定数 *IP_QOS_MESSAGE_LEVEL*) を指定します。

  接続レベルの有効範囲は、このメッセージの分類によって取得された QoS サービス・レベルが、分類データを持つ次の sendmsg() 呼び出しまでに送信される以後のすべてのメッセージに影響を及ぼすことを示します。メッセージ・レベルの有効範囲は、割り当てられた QoS サービス・レベルが、この sendmsg() 呼び出しに含まれているメッセージ・データのみに使用されることを示します。 QoS 分類データなしで送信される将来のデータは、前の接続レベル QoS 割り当てを継承します (sendmsg() による最後の接続レベル分類から、または接続確立時にオリジナルの TCP 接続分類から)。
- ip_qos_classification_type: この指定は、受け渡される分類データのタイプを示します。アプリケーションでは、アプリケーション定義のトークン、アプリケーション指定の優先順位、またはトークンと優先順位の両方の受け渡しを選択できます。 3 番目のオプションを選択する場合、選択する 2 つの分類タイプは論理和として指定する必要があります。以下のタイプを指定できます。
  - アプリケーション定義のトークン分類。 1 つのタイプを指定してください。2 つ以上のタイプを指定すると、結果は予測不能になります。
    - IP_SET_QOSLEVEL_W_APPL_TOKEN_ASCII : これは分類データが ASCII 形式の文字ストリングであることを示します。このオプションを指定する場合、アプリケーション・トークンを ip_qos_appl_token フィールドで受け渡す必要があります。

      注: アプリケーションが分類データ用の数値を渡す必要がある場合は、最初に印刷可能な ASCII 形式に変換する必要があります。指定するストリングは大文字小文字混合で指定することができ、指定されたとおりの形式で比較のために使用されます。
    - IP_SET_QOSLEVEL_W_APPL_TOKEN_EBCDIC : 上記と同じですが、ストリングは EBCDIC 形式です。

      注: このオプションより IP_SET_QOSLEVEL_W_APPL_TOKEN_ASCII の方がいくらか便利です。ポリシーで指定されたアプリケーション・データが TCP/IP スタックの中に ASCII 形式で保管されるので、sendmsg() 要求が出されるたびにアプリケーション定義のトークンを変換する必要がありません。
  - アプリケーション定義の優先順位分類。 1 つのタイプを指定してください。複数の優先順位タイプを指定すると、結果は予測不能になります。
    - IP_SET_QOSLEVEL_EXPIDITED: 優先転送の優先順位が要求されることを示します。
    - IP_SET_QOSLEVEL_HIGH: 高優先順位が要求されることを示します。
    - IP_SET_QOSLEVEL_MEDIUM: 中優先順位が要求されることを示します。

- IP_SET_QOSLEVEL_LOW: 低優先順位が要求されることを示します。
- IP_SET_QOSLEVEL_BEST_EFFORT: ベストエフォート優先順位が要求されることを示します。

– ip_qos_appl_token_len: ip_qos_appl_token の長さを指定します。
– ip_qos_appl_token: ip_qos_classification_type フィールドのすぐ後に続く仮想フィールドです。アプリケーション分類トークン・ストリング。分類タイプに指定した IP_SET_QOSLEVEL_W_APPL_TOKEN_xxxx のフレーバーに応じて、ASCII 形式または EBCDIC 形式になります。 このフィールドは、アプリケーション定義のトークンを指定した場合にのみ参照されます。このストリングは 128 バイトを超えてはなりません。大きいサイズを指定した場合、最初の 128 バイトだけが使用されます。また、ストリングの長さは、cmsg_len に指定された値に基づいて計算されます (cmsg_len - sizeof(cmsghdr) - sizeof(ip_qos_classification_data))。この計算される長さには、ヌル終了文字は含まれません。

関連概念

2 ページの『DiffServ』
これは、オペレーティング・システムで作成できるアウトバウンド帯域幅ポリシーの第 1 のタイプです。DiffServ はトラフィックをクラスに分割します。 DiffServ ポリシーをインプリメントするには、ネットワーク・トラフィックの分類方法とさまざまなクラスの処理方法を決定する必要があります。

3 ページの『優先順位付けされたクラス: ネットワーク・トラフィックの分類方法』
DiffServ はトラフィックをクラスとして識別します。 最も一般的なクラスは、クライアント IP アドレス、アプリケーション・ポート、サーバー・タイプ、プロトコル、ローカル IP アドレス、およびスケジュールを使用して定義されます。同じクラスに分類されたトラフィックは、すべて同等に扱われます。

関連資料

Sendmsg() API - ソケットによるメッセージの送信

ディレクトリー・サーバー

ポリシーをディレクトリー・サーバーにエクスポートすることができます。 Lightweight Directory Access Protocol (LDAP) の概念と構成、および QoS (Quality of Service) スキーマについて調べるには、このトピックをお読みください。

LDAP バージョン 3 を使用すると、ディレクトリー・サーバーにポリシーをエクスポートできるようになりました。

ディレクトリー・サーバーの使用法

QoS ポリシーをディレクトリー・サーバーにエクスポートすると、ポリシーの管理が容易になります。ディレクトリー・サーバーを使用するには、3 つの方法があります。

- 1 つのローカル・ディレクトリー・サーバーに構成データを保管して、多くのシステムで共用することができます。
- 1 つのシステムで構成データの構成と保管を行い、そのシステムだけで使用することができます (共用はしません)。
- 他のシステム用のデータを保持するディレクトリー・サーバーに構成データを置くことができます。ただし、構成データがそれらの他のシステムと共用されるわけではありません。これによって、単一ロケーションを使用していくつかのシステムのデータをバックアップおよび保管することができます。

ローカル・システムのみに保管する場合の利点

QoS ポリシーをローカル・システムに保管するのはそれほど複雑ではありません。ポリシーをローカルで使用すると、多くの利点があります。

- 複雑な LDAP 構成を必要としないユーザーは、それを行わずに済みます。
- LDAP への書き込みは最高速の方法ではないので、パフォーマンスが向上します。
- 異なるシステム間での構成の複写が簡単になります。1 つのシステムから別のシステムへファイルをコピーできます。 1 次マシンまたは 2 次マシンがないので、個別のシステム上で各ポリシーを直接に調整できます。

LDAP リソース

ポリシーを LDAP サーバーにエクスポートすることに決めた場合、続行する前に LDAP の概念とディレクトリー構造について知っておく必要があります。 System i ナビゲーターの QoS 機能を使用して、QoS ポリシーで使用されるディレクトリー・サーバーを構成することができます。

関連概念

IBM Tivoli Directory Server for i5/OS (LDAP)

60 ページの『ディレクトリー・サーバーの構成』

Quality of Service (QoS) ポリシー構成は、QoS ソリューションを簡単に管理できるように Lightweight Directory Access Protocol (LDAP) ディレクトリー・サーバーにエクスポートすることができます。

キーワード

ディレクトリー・サーバーを構成する場合、キーワードを各 Quality of Service (QoS) 構成に関連付けるかどうかを決める必要があります。

キーワード・フィールドはオプションであり、無視することができます。

QoS 初期構成ウィザードでディレクトリー・サーバーを構成できます。構成するサーバーが 1 次システムか 2 次システムかを指定できます。すべての QoS ポリシーを維持するサーバーは、1 次システムと呼ばれます。

1 次システムによって作成された構成を識別するのに、キーワードを使用します。キーワードは、1 次システムで作成されますが、実際には、2 次システムのためのものです。キーワードによって、2 次システムは、1 次システムで作成された構成をロードおよび使用することができます。 以下の記述では、各システムでキーワードを使用する方法について説明されています。

キーワードと 1 次システム

キーワードは、1 次システムによって作成および維持される QoS 構成と関連付けられます。これらは、2 次システムが 1 次システムで作成された構成を識別できるよう使用されます。

キーワードと 2 次システム

2 次システムは、キーワードを使用して構成を検索します。2 次システムは、1 次システムによって作成された構成をロードおよび使用します。 2 次システムを構成する時に、特定のキーワードを選択することができます。選択したキーワードによっては、2 次システムはその選択したキーワードと関連した構成をロードします。これによって、2 次システムは複数の 1 次システムによって作成された複数の構成をロードすることができます。

System i ナビゲーター でディレクトリー・サーバーの構成を開始する場合は、具体的な説明に関して QoS タスクのヘルプを使用してください。

関連概念

『識別名』
ディレクトリーの一部を管理する場合、識別名 (DN) またはキーワード (選択した場合) を参照します。

60 ページの『ディレクトリー・サーバーの構成』
Quality of Service (QoS) ポリシー構成は、QoS ソリューションを簡単に管理できるように Lightweight Directory Access Protocol (LDAP) ディレクトリー・サーバーにエクスポートすることができます。

識別名

ディレクトリーの一部を管理する場合、識別名 (DN) またはキーワード (選択した場合) を参照します。

Quality of Service (QoS) 初期構成ウィザード内でディレクトリー・サーバーを構成する場合は、DN を指定します。 DN は、通常、項目自体の名前と、ディレクトリー内のその項目より上のオブジェクト (逆の順序で) から構成されます。サーバーは、DN より下にあるディレクトリーのすべてのオブジェクトにアクセスすることができます。例えば、LDAP サーバーには、下図に示すようなディレクトリー構造が含まれます。

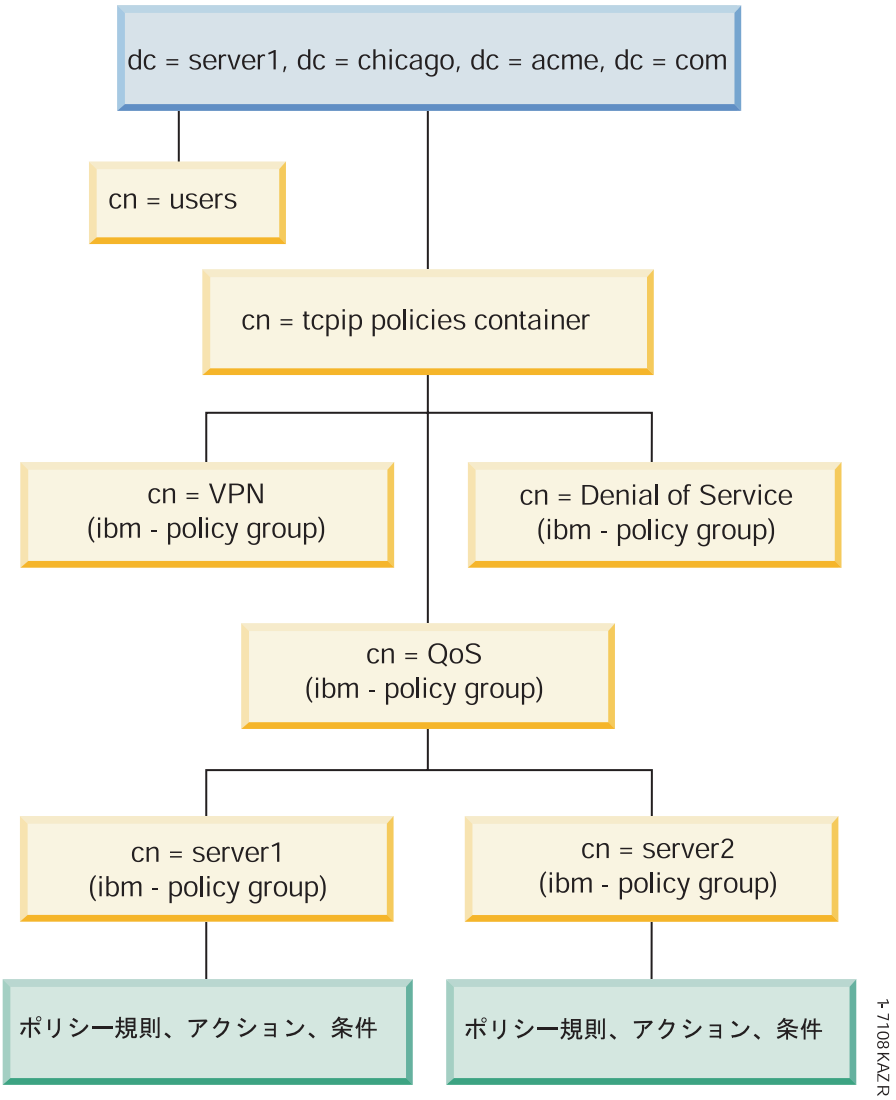


図 3. QoS ディレクトリー構造の例

一番上の Server1 (dc=server1,dc=chicago,dc=acme,dc=com) は、ディレクトリー・サーバーが常駐するサーバーです。その他のサーバー (例えば、cn=QoS または cn=tcpip policies) には、QoS の各サーバーが常駐します。そのため、cn=server1 では、デフォルトの DN は `cn=server1,cn=QoS,cn=tcpip policies, dc=server1,dc=chicago,dc=acme,dc=com` になります。 cn=server2 では、デフォルトの DN は `cn=server2,cn=QoS,cn=tcpip policies,dc=server1,dc=chicago,dc=acme,dc=com` になります。

ディレクトリーを管理する場合は、DN 内の cn または dc などを適切なサーバーに変更することが重要です。 DN のストリングは通常、スクロールしなくては表示できないほど長くなるので、 DN を編集するときには特に注意が必要です。

関連概念

29 ページの『キーワード』
ディレクトリー・サーバーを構成する場合、キーワードを各 Quality of Service (QoS) 構成に関連付けるかどうかを決める必要があります。

60 ページの『ディレクトリー・サーバーの構成』
Quality of Service (QoS) ポリシー構成は、QoS ソリューションを簡単に管理できるように Lightweight Directory Access Protocol (LDAP) ディレクトリー・サーバーにエクスポートすることができます。

関連資料

76 ページの『Quality of Service の関連情報』
Quality of Service の Request For Comments、IBM Redbooks 資料、およびその他の Information Center トピック・コレクションには、Quality of Service トピック・コレクションに関連する情報が記載されています。以下の PDF ファイルのいずれも表示または印刷できます。

シナリオ: Quality of Service ポリシー

以下の QoS (Quality of Service) ポリシー・シナリオは、QoS が必要な理由およびポリシーとサービス・クラスの作成方法を理解するのに役立ちます。

QoS について学ぶ最善の方法の 1 つは、ネットワーク全体図の中で機能がどのように動作するかを確認することです。以下の基本例は、QoS ポリシーを使用する理由を示すとともに、ポリシーおよびサービス・クラスを作成するステップの指示を含んでいます。

注: IP アドレスと図は架空のものであり、例示目的でのみ使用されています。

関連概念

72 ページの『システム・トランザクションのモニター』
QoS (Quality of Service) モニターを使用して、QoS ポリシーが意図したとおりに機能しているか確認することができます。QoS モニターは、QoS の計画フェーズとトラブルシューティング・フェーズで役に立ちます。

関連資料

64 ページの『QoS のモニター』
Quality of Service (QoS) モニターを利用して、システムで IP トラフィックを分析できます。

シナリオ: ブラウザー・トラフィックの制限

QoS (Quality of Service) を使用して、トラフィック・パフォーマンスを制御することができます。 ネットワーク内でのアプリケーションのパフォーマンスを制限または拡張するには、DiffServ ポリシーを使用します。

状態

会社では、金曜日にユーザー向け業務設計 (UCD) グループからのブラウザー・トラフィックのレベルが高くなることを経験しています。このトラフィックは、毎週金曜日、会計アプリケーション処理のために良好なパフォーマンスを必要としている、会計部門の妨げとなっています。そこで、UCD グループからのブラウザー・トラフィックを制限することに決めました。次の図は、このシナリオでのネットワーク・セットアップを示しています。

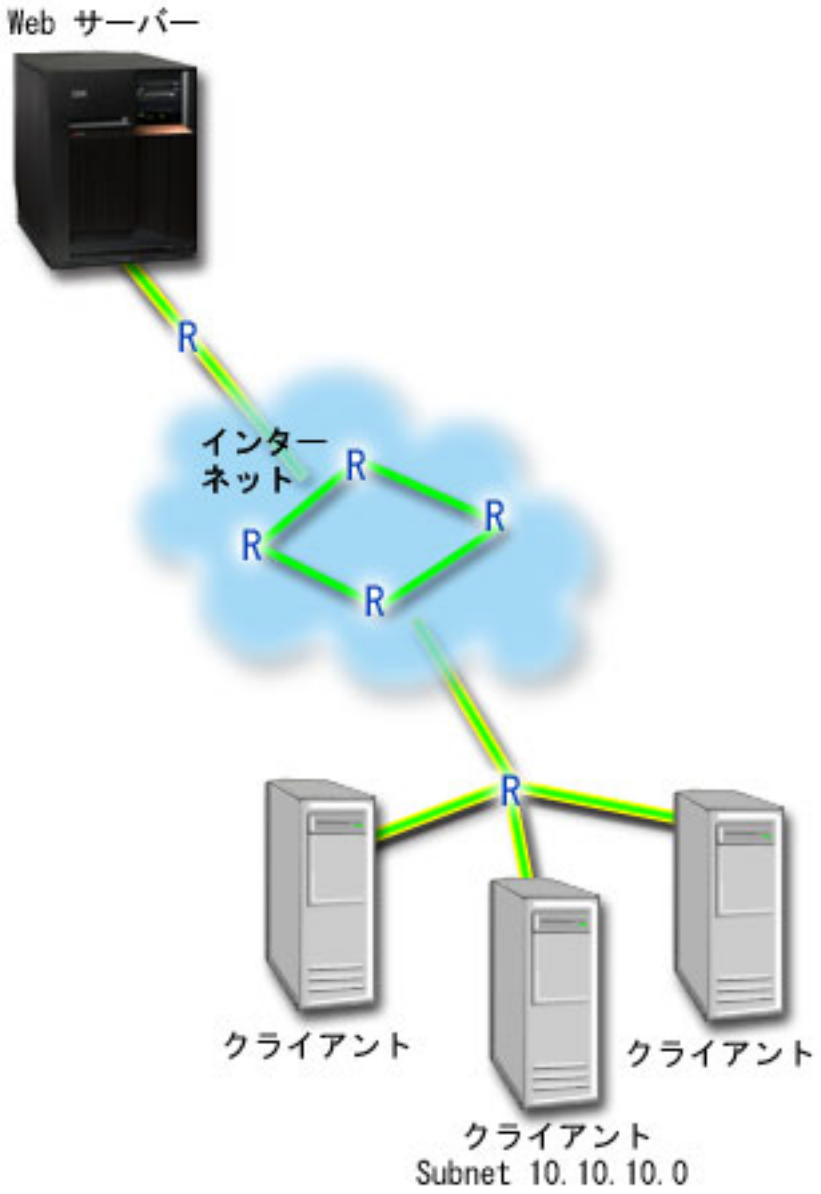


図 4. 図 1. クライアントへのブラウザー・トラフィックを制限している Web サーバー

目的

ネットワークからのブラウザー・トラフィックを制限するために、DiffServ ポリシーを作成することができます。 DiffServ ポリシーはトラフィックをクラスに分割します。 このポリシーの中のすべてのトラフィックにコード・ポイントが割り当てられます。このコード・ポイントはルーターに、トラフィックの処理方法

を知らせます。このシナリオでは、ポリシーには低いコード・ポイント値が割り当てられ、ネットワークのブラウザー・トラフィックへの優先順位付けに影響を与えています。

前提条件および前提事項

- ポリシーが要求された優先順位を受け取ることができるように、インターネット・サービス・プロバイダー (ISP) とサービス・レベル・アグリーメント (SLA) を交わしているとします。システム上で作成する QoS ポリシーでは、トラフィックが (ポリシー内で) ネットワーク全体での優先順位を受け取るようにするものとします。 QoS ポリシーでは優先順位が保証されているわけではなく、これは SLA に依存します。 QoS ポリシーの利点を有効に利用すれば、一部のサービス・レベルおよび速度について折衝が可能になります。
- DiffServ ポリシーでは、ネットワーク・パスに DiffServ 使用可能なルーターがあることが必要です。ほとんどのルーターは DiffServ 使用可能ではありません。

構成

前提条件のステップを確認したら、DiffServ ポリシーの作成準備は完了です。

関連概念

55 ページの『サービス・レベル・アグリーメント』
このトピックでは、QoS (Quality of Service) インプリメンテーションに影響を及ぼす可能性があるサービス・レベル・アグリーメント (SLA) の重要な特徴のいくつかを指摘します。 QoS とは、つまりネットワーク・パフォーマンスを意味します。プライベート・ネットワークの外部でネットワーク優先順位を受け取るには、インターネット・サービス・プロバイダー (ISP) との SLA を保持する必要が生じる場合があります。

2 ページの『DiffServ』
これは、オペレーティング・システムで作成できるアウトバウンド帯域幅ポリシーの第 1 のタイプです。DiffServ はトラフィックをクラスに分割します。 DiffServ ポリシーをインプリメントするには、ネットワーク・トラフィックの分類方法とさまざまなクラスの処理方法を決定する必要があります。

関連資料

64 ページの『QoS のモニター』
Quality of Service (QoS) モニターを利用して、システムで IP トラフィックを分析できます。

シナリオ詳細: DiffServ ポリシーの作成

このトピックには、システム上での DiffServ ポリシーの構成に関する情報が記載されています。

1. System i ナビゲーター で、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**IP ポリシー**」の順に展開します。
2. 「**Quality of Service**」を右マウス・ボタンでクリックし、「**構成**」を選択して、Quality of Service (QoS) インターフェースを開きます。
3. QoS インターフェースで DiffServ ポリシー・タイプを右マウス・ボタンでクリックし、「**新規ポリシー**」を選択して、ウィザードを開きます。
4. 「ウェルカム」ページを読んでから、「**次へ**」をクリックして、「名前」ページへ進みます。
5. 「**名前**」フィールドに「UCD」と入力します。オプションとして、このポリシーの意図を説明する記述を入力することもできます。「**次へ**」をクリックします。
6. 「クライアント」ページで、「**特定の 1 つまたは複数のアドレス**」を選択し、「**新規**」をクリックして、クライアントを定義します。
7. 「新規クライアント」ウィンドウで、以下の情報を入力し、「**OK**」をクリックします。
   - **名前**: UCD_Client

- **IP アドレスおよびマスク**: 10.10.10.0 / 24

「**OK**」をクリックすると、ポリシー・ウィザードに戻ります。 前に作成されたクライアントがある場合は、それらをクリアして、関連するクライアントだけが選択されていることを確認します。

8. 「サーバー・データ要求 (Server Data Request)」ページで、「**任意のトークン (Any token)**」と「**すべての優先順位 (All priorities)**」が選択されていることを確認し、「**次へ**」をクリックします。
9. 「アプリケーション」ページで、「**特定のポート、ポート範囲、またはサーバー・タイプ (Specific port, range of ports, or server type)**」を選択し、「**新規**」をクリックします。
10. 「新規アプリケーション」ウィンドウで、以下の情報を入力し、「**OK**」をクリックして、ウィザードに戻ります。
    - **名前**: HTTP
    - **ポート**: 80
11. 「アプリケーション」ページで、「**プロトコル**」を選択し、「**TCP**」が選択されていることを確認します。「**次へ**」をクリックします。
12. 「ローカル IP アドレス」ページで、「**すべての IP アドレス**」が選択されていることを確認し、「**次へ**」をクリックします。
13. 「DiffServ クラス」ページで、「**新規**」をクリックし、パフォーマンス特性を定義します。「新規サービス・クラス (New Class of Service)」ウィザードが開きます。
14. 「ウェルカム」ページを読んでから、「**次へ**」をクリックします。
15. 「名前」ページで、「UCD_service」と入力します。オプションとして、このポリシーの意図を説明する記述を入力することができます。「**次へ**」をクリックします。
16. 「サービス・タイプ (Type of Service)」ページで、「**アウトバウンドのみ (Outbound only)**」を選択し、「**次へ**」をクリックします。このサービス・クラスはアウトバウンド・ポリシーのみに使用されます。
17. 「アウトバウンド DiffServ コード・ポイントのマーク付け」ページで、「**Class 4**」を選択し、「**次へ**」をクリックします。 PHB (ホップごとの転送優先順位付け) は、このトラフィックがルーターおよびネットワーク上の他のシステムからどんなパフォーマンスを受けるかを決定します。 インターフェースに関連したヘルプを使用して判断に役立ててください。
18. 「アウトバウンド・トラフィック計量の実行」ページで、「**はい**」が選択されていることを確認し、「**次へ**」をクリックします。
19. 「アウトバウンド速度制御限界」ページで、以下の情報を入力し、「**次へ**」をクリックします。
    - **トークン・バケット・サイズ**: 100 K ビット
    - **平均速度限界**: 512 K ビット/秒
    - **ピーク速度限界**: 1 M ビット/秒
20. 「アウトバウンド・プロファイル外トラフィック」ページで、「**UDP パケットの廃棄または TCP 輻輳 (ふくそう) ウィンドウの縮小 (Drop UDP packets or reduce TCP congestion window)**」を選択し、「**次へ**」をクリックします。
21. このサービス・クラスの要約情報を検討します。情報が正しい場合は、「**完了**」をクリックして、サービス・クラスを作成します。「**完了**」をクリックした後、ポリシー・ウィザードに戻って、サービス・クラスを選択します。 「**次へ**」をクリックします。
22. 「スケジュール」ページで、「**選択されたスケジュールの間アクティブ**」を選択し、「**新規**」をクリックします。
23. 「新規スケジュール」ウィンドウで、以下の情報を入力し、「**OK**」をクリックします。
    - **名前**: UCD_schedule

- **時刻**: 24 時間アクティブ
- **曜日**: 金曜日

24. 「**次へ**」をクリックして、ポリシーの要約を表示します。情報が正しければ「**完了**」をクリックします。「QoS サーバー構成」ウィンドウの右側のペインに新しいポリシーがリストされます。

シナリオ詳細: QoS サーバーの開始または更新

このトピックには、QoS サーバーの開始または更新に関する情報が記載されています。

「Quality of Service (QoS) サーバー構成」ウィンドウで、「**サーバー**」 → 「**開始**」または「**サーバー**」 → 「**更新**」を選択します。

シナリオ詳細: ポリシーが動作していることを確認する

ポリシーが構成したとおりに動作していることを検証するには、モニターを使用する必要があります。

1. 「Quality of Service (QoS) 構成」ウィンドウで、「**サーバー**」 → 「**モニター**」を選択します。 「QoS モニター」ウィンドウが開きます。
2. 「DiffServ」ポリシー・タイプ・フォルダーを選択します。すべての DiffServ ポリシーが表示されます。 リストから「**UCD**」を選択します。

   最も注意を払う必要のあるフィールドは、トラフィックからデータを取得するフィールドです。合計ビット数、プロファイル中のビット数およびプロファイル中のパケット数の各フィールドを必ずチェックしてください。プロファイル外ビット数は、トラフィックが、構成されたポリシー値を超えた場合に示されます。 DiffServ ポリシーの中のプロファイル外の数は、(UDP パケットの場合) 廃棄されるビット数を表します。 TCP の場合は、プロファイル外の数は、トークン・バケット速度を超えてネットワークに送信されるビット数を表します。 TCP パケットの場合、ビットは廃棄されません。プロファイル中のパケット数は、(パケットが発信してから現在のモニター出力に至るまでの間) このポリシーによって制御されたパケットの数を示します。

   「**平均速度限界**」フィールドにどのような値を割り当てるかということも重要です。パケットがこの制限値を超えると、システムはそれらのパケットの廃棄を開始します。 その結果、プロファイル外ビット数が増加します。 これは、ポリシーが、構成したとおりに動作していることを表しています。すべてのモニター・フィールドについては、64 ページの『QoS のモニター』を参照してください。

   注: 正しい結果はポリシーがアクティブな場合にのみ得られます。 ポリシー内で指定したスケジュールを確認してください。

シナリオ詳細: プロパティーの変更

モニターの結果を調べた後、期待どおりの結果が得られるようにポリシーまたはサービス・クラス・プロパティーを変更できます。

ポリシーで作成した任意の値を変更するには、以下のステップを実行します。

1. 「Quality of Service (QoS) サーバー構成」ウィンドウで、「**DiffServ**」フォルダーを選択します。右側のペインのリストから「**UCD** 」を右マウス・ボタンでクリックし、「**プロパティー**」を選択して、ポリシーを編集します。「プロパティー」ウィンドウが開き、一般ポリシーを制御する値が示されます。
2. 該当する値を指定してください。
3. サービス・クラスを編集するには、「**サービス・クラス**」フォルダーを選択します。右側のペインのリストから「**UCD_service**」を右マウス・ボタンでクリックし、「**プロパティー**」を選択して、サービス・クラスを編集します。「QoS プロパティー」ウィンドウが開き、トラフィック管理を制御する値が示されます。

4. 該当する値を指定してください。
5. 「QoS サーバー構成」ウィンドウで、「**サーバー**」 → 「**更新**」 を選択し、変更を受け入れます。

シナリオ: 安全で予測可能な結果 (VPN と QoS)

VPN (仮想プライベート・ネットワーク) を使用している場合でも、Quality of Service (QoS) ポリシーを作成できます。

状態

VPN を介して接続を行っているパートナーがおり、主幹業務データのセキュリティーと予測可能な e-business フローを実現できるように VPN のもとで QoS を実行したいと考えています。 QoS 構成は、一方向にのみ送信されます。従って、オーディオまたはビデオ・アプリケーションがある場合は、接続の両端でそのアプリケーション用に QoS を設定する必要があります。

図は、ホスト間 VPN 接続されているサーバーとクライアントを表しています。それぞれの R は、トラフィックのパスに存在する DiffServ 使用可能ルーターを表します。図からわかるように、QoS ポリシーは一方向にのみ流れます。

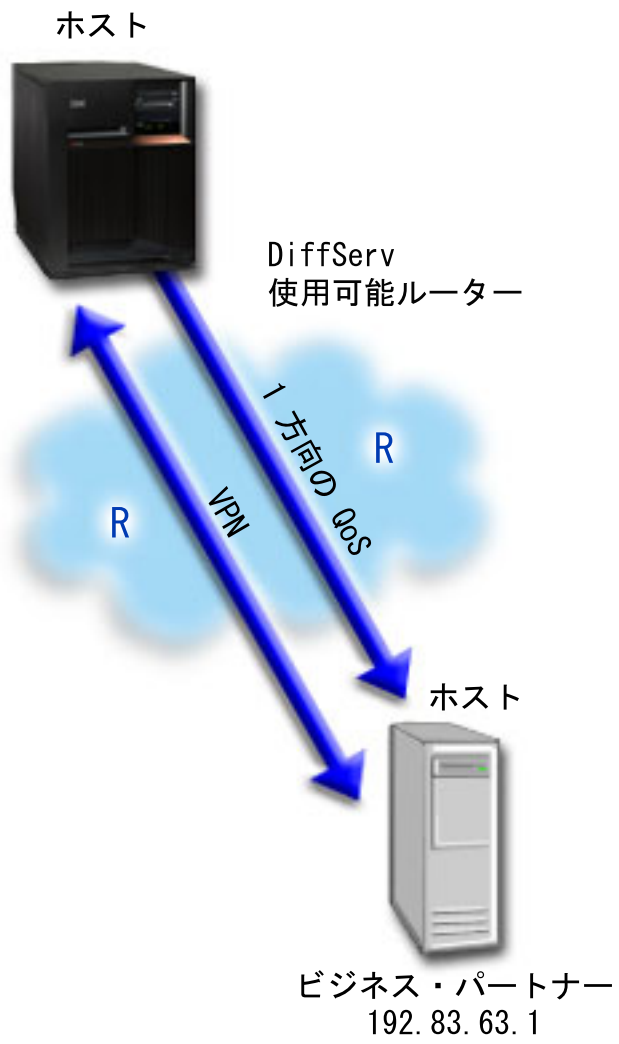


図 5. QoS DiffServ ポリシーを使用したホスト間 VPN 接続

目的

保護だけでなく、この接続の優先順位も確立するために、VPN と QoS を使用します。 最初に、ホスト間 VPN 接続をセットアップします。 VPN 接続の保護を確立後、QoS ポリシーをセットアップすることができます。 DiffServ ポリシーを作成します。このポリシーには高優先転送コード・ポイント値が割り当てられ、ネットワークでの主幹業務トラフィックの優先順位付けに影響を与えています。

前提条件および前提事項

- ポリシーが要求された優先順位を受け取ることができるように、インターネット・サービス・プロバイダー (ISP) とサービス・レベル・アグリーメント (SLA) を交わしているとします。システム上で作成する QoS ポリシーでは、トラフィックが (ポリシー内で) ネットワーク全体での優先順位を受け取るようにするものとします。 ただし、これは保証されているわけではなく、SLA に依存します。 QoS ポリシーの利点を有効に利用すれば、一部のサービス・レベルおよび速度について折衝が可能になります。 詳しくは SLA リンクを参照してください。
- DiffServ ポリシーでは、ネットワーク・パスに DiffServ 使用可能なルーターがあることが必要です。ほとんどのルーターは DiffServ 使用可能です。

構成

前提条件のステップを確認したら、DiffServ ポリシーの作成準備は完了です。

関連概念

55 ページの『サービス・レベル・アグリーメント』
このトピックでは、QoS (Quality of Service) インプリメンテーションに影響を及ぼす可能性があるサービス・レベル・アグリーメント (SLA) の重要な特徴のいくつかを指摘します。 QoS とは、つまりネットワーク・パフォーマンスを意味します。プライベート・ネットワークの外部でネットワーク優先順位を受け取るには、インターネット・サービス・プロバイダー (ISP) との SLA を保持する必要が生じる場合があります。

2 ページの『DiffServ』
これは、オペレーティング・システムで作成できるアウトバウンド帯域幅ポリシーの第 1 のタイプです。DiffServ はトラフィックをクラスに分割します。 DiffServ ポリシーをインプリメントするには、ネットワーク・トラフィックの分類方法とさまざまなクラスの処理方法を決定する必要があります。

関連資料

64 ページの『QoS のモニター』
Quality of Service (QoS) モニターを利用して、システムで IP トラフィックを分析できます。

シナリオ詳細: ホスト間 VPN 接続のセットアップ

このトピックには、ホスト間 VPN 接続のセットアップに関する情報が記載されています。

シナリオ: 基本的な企業間接続は、VPN を構成する時に役立つので参照してください。

シナリオ詳細: DiffServ ポリシーの作成

このトピックには、DiffServ ポリシーの作成に関する情報が記載されています。

1. System i ナビゲーター で、**「ユーザーのシステム」** → **「ネットワーク」** → **「IP ポリシー」**の順に展開します。
2. 「**Quality of Service**」を右マウス・ボタンでクリックし、「**構成**」を選択して、「Quality of Service (QoS) サーバー構成」ウィンドウを開きます。
3. 「QoS サーバー構成」ウィンドウで、DiffServ を右マウス・ボタンでクリックし、**「新規ポリシー」**を選択して、ウィザードを開きます。
4. 「ウェルカム」ページを読んでから、「**次へ**」をクリックして、「**名前**」ページへ進みます。
5. 「**名前**」フィールドに「VPN」と入力し、「**次へ**」をクリックします。オプションとして、このポリシーの意図を説明する記述を入力することができます。
6. 「クライアント」ページで、「**特定の 1 つまたは複数のアドレス**」を選択し、「**新規**」をクリックして、クライアントを定義します。
7. 「新規クライアント」ウィンドウで、以下の情報を入力します。
   - **名前**: VPN_Client
   - **IP アドレス**: 192.83.63.1
   - 「**OK**」をクリックしてクライアントを作成し、DiffServ ウィザードに戻ります。

   「OK」をクリックすると、ポリシー・ウィザードに戻ります。 前に作成したクライアントがある場合は、それらをクリックして、関連するクライアントだけが選択されていることを確認します。
8. 「サーバー・データ要求 (Server Data Request)」ページで、**「任意のトークン (Any token)」**と**「すべての優先順位 (All priorities)」**が選択されていることを確認します。

9. 「アプリケーション」ページで、「**すべてのポート**」と「**すべて**」が選択されていることを確認します。
10. 「**次へ**」をクリックします。
11. 「ローカル IP アドレス」ページで、デフォルト値を受け入れて、「**次へ**」をクリックします。
12. 「DiffServ クラス」ページで、「**新規**」をクリックし、パフォーマンス特性を定義します。「新規サービス・クラス (New Class of Service)」ウィザードが開きます。
13. 「ウェルカム」ページを読んでから、「**次へ**」をクリックします。
14. 「名前」ページで、「EF_VPN」と入力します。
15. 「サービス・タイプ (Type of Service)」ページで、「**アウトバウンドのみ (Outbound only)**」を選択し、「**次へ**」をクリックします。このサービス・クラスはアウトバウンド・ポリシーのみに使用されます。
16. 「アウトバウンド DiffServ コード・ポイントのマーク付け」ページで、「**Class 3**」を選択します。PHB (ホップごとの転送優先順位付け) は、このトラフィックがルーターおよびネットワーク上の他のシステムからどんなパフォーマンスを受けるかを決定します。インターフェースに関連したヘルプを使用して判断に役立ててください。
17. 「アウトバウンド・トラフィック計量の実行」ページで、「**はい**」が選択されていることを確認し、「**次へ**」をクリックします。
18. 「アウトバウンド速度制御限界」ページで、以下の情報を入力し、「**次へ**」をクリックします。
    - **トークン・バケット・サイズ**: 100 K ビット
    - **平均速度限界**: 64 M ビット/秒
    - **ピーク速度限界**: 制限しない
19. 「アウトバウンド・プロファイル外トラフィック」ページで、「**UDP パケットの廃棄または TCP 輻輳 (ふくそう) ウィンドウの縮小 (Drop UDP packets or reduce TCP congestion window)**」を選択し、「**次へ**」をクリックします。
20. 「クラス - 要約」ページを検討し、「**完了**」をクリックして、ポリシー・ウィザードに戻ります。
21. 「DiffServ クラス」ページで、「**EF_VPN**」が選択されていることを確認し、「**次へ**」をクリックします。
22. 「スケジュール」ページで、「**選択されたスケジュールの間アクティブ**」を選択し、「**新規**」をクリックします。
23. 「新規スケジュール」ウィンドウで、以下の情報を入力し、「**OK**」をクリックします。
    - **名前**: FirstShift
    - **時刻**: 特定時間にアクティブ、午前 9 時から午後 5 時を追加
    - **曜日**: 特定日にアクティブ、月曜日から金曜日を選択
24. 「スケジュール」ページで、「**次へ**」をクリックします。
25. 要約情報を検討します。情報が正しい場合は、「**完了**」をクリックして、ポリシーを作成します。「QoS サーバー構成」ウィンドウに、システムで作成されたすべてのポリシーがリストされます。 ウィザードの完了後は、右側のペインにポリシーがリストされます。

シナリオ詳細: QoS サーバーの開始または更新

このトピックには、QoS サーバーの開始または更新に関する情報が記載されています。

「Quality of Service (QoS) サーバー構成」ウィンドウで、「**サーバー**」 → 「**開始**」または「**サーバー**」 → 「**更新**」を選択します。

シナリオ詳細: ポリシーが動作していることを確認する

ポリシーが構成したとおりに動作していることを検証するには、モニターを使用する必要があります。

1. 「Quality of Service (QoS) サーバー構成」ウィンドウで、「**サーバー**」 → 「**モニター**」を選択します。 「QoS モニター」ウィンドウが開きます。
2. 「DiffServ」ポリシー・タイプを選択します。 すべての DiffServ ポリシーが表示されます。

   例 1 と同様に、最も注意を払う必要のあるフィールドは、トラフィックからデータを取得するフィールドです。合計ビット数、プロファイル中のビット数、およびプロファイル外パケット数の各フィールドがあります。 プロファイル外ビット数は、トラフィックが、構成されたポリシー値を超えた場合に示されます。プロファイル中のパケット数は、このポリシーによって制御されたパケットの数を示します。平均速度限界のフィールドにどのような値を割り当てるかが、非常に重要です。 TCP パケットがこの制限を超えると、TCP 輻輳 (ふくそう) ウィンドウが縮小されてプロファイル外パケットを待ち行列に書き込めるようになるまで、それらの TCP パケットがネットワークに送り出されます。その結果、プロファイル外ビット数が増加します。 このポリシーがブラウザー・トラフィックの制限のシナリオと異なる点は、パケットが VPN プロトコルの使用により保護されていることです。図からわかるように、QoS は VPN 接続のもとで機能します。すべてのモニター・フィールドについては、64 ページの『QoS のモニター』を参照してください。

   注: 正しい結果はポリシーがアクティブな場合にのみ得られます。 ポリシー内で指定したスケジュールを確認してください。

シナリオ詳細: プロパティーの変更

モニターの結果を調べた後、期待どおりの結果が得られるようにポリシーまたはサービス・クラス・プロパティーを変更できます。

1. 「Quality of Service (QoS) サーバー構成」ウィンドウで、「**DiffServ**」フォルダーを選択します。右側のペインのリストから「**VPN**」を右マウス・ボタンでクリックし、「**プロパティー**」を選択して、ポリシーを編集します。「プロパティー」ウィンドウが開き、一般ポリシーを制御する値が示されます。
2. 該当する値を指定してください。
3. サービス・クラスを編集するには、「**サービス・クラス**」フォルダーを選択します。右側のペインのリストから「**EF_VPN**」を右マウス・ボタンでクリックし、「**プロパティー**」を選択して、サービス・クラスを編集します。「QoS プロパティー」ウィンドウが開き、トラフィック管理を制御する値が示されます。
4. 該当する値を指定してください。
5. 「QoS サーバー構成」ウィンドウで、「**サーバー**」 → 「**更新**」 を選択し、変更を受け入れます。

シナリオ: インバウンド接続の制限

ユーザーのシステムに対してなされるインバウンド接続要求を制御する必要がある場合には、インバウンド許可ポリシーを使用します。

状態

ネットワークに入ってくるクライアント要求により、Web サーバーのリソースが過負荷になっています。ローカル・インターフェース 192.168.1.1 上の Web サーバーへの着信 HTTP トラフィックを減らすように求められています。 Quality of Service (QoS) は、システムに対する接続属性 (例えば、IP アドレス) に基づいて、受け入れられるインバウンド接続試行を制限するのに役立ちます。 そのために、受け入れられるインバウンド接続の数を制限するインバウンド許可ポリシーをインプリメントすることに決めました。

次の図は、ユーザーの会社とクライアントの会社を示したものです。この QoS ポリシーでは、一方向のトラフィックの流れしか制御することができません。

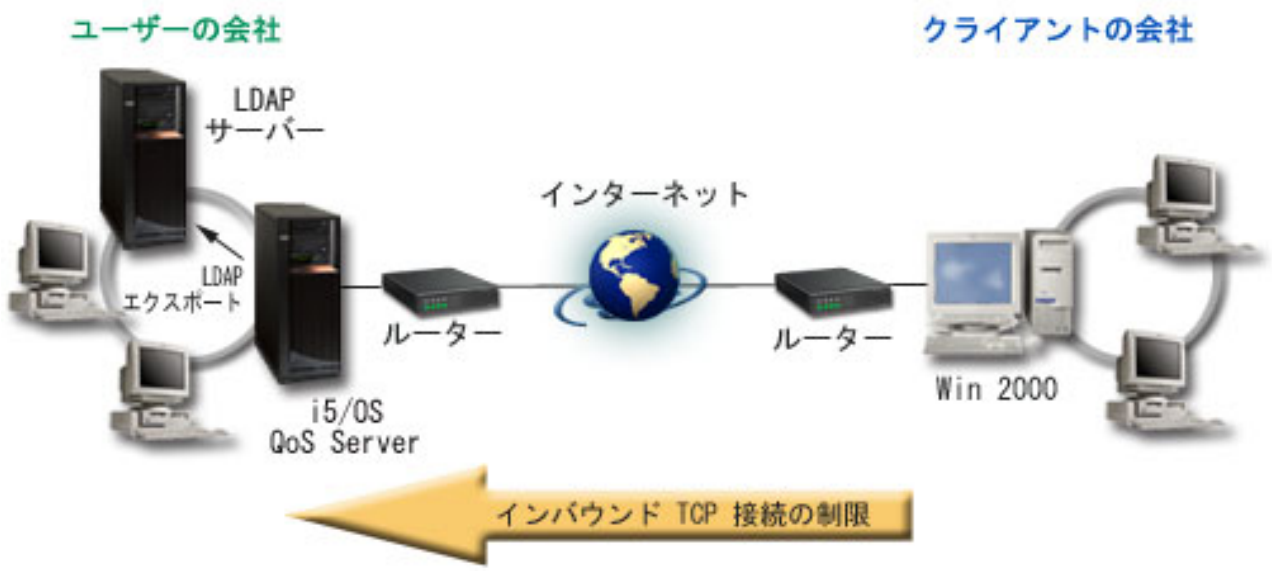


図 6. インバウンド TCP 接続の制限

目的

インバウンド・ポリシーを構成するには、ローカル・インターフェースまたは特定のアプリケーションのどちらへのトラフィックを制限するか、また特定のクライアントからのトラフィックを制限するかどうかを決める必要があります。この場合、クライアントの会社からローカル・インターフェース 192.168.1.1 上のポート 80 (HTTP プロトコル) への接続試行を制限するポリシーを作成する必要があります。

構成

これらのトピックは、インバウンド許可ポリシーを作成する方法を示します。

関連資料

64 ページの『QoS のモニター』
Quality of Service (QoS) モニターを利用して、システムで IP トラフィックを分析できます。

シナリオ詳細: インバウンド許可ポリシーの作成

このトピックには、システム上でのインバウンド許可ポリシーの作成に関する情報が記載されています。

1. System i ナビゲーター で、**「ユーザーのシステム」** → **「ネットワーク」** → **「IP ポリシー」**の順に展開します。
2. **「Quality of Service」**を右マウス・ボタンでクリックし、**「構成」**を選択して、「Quality of Service (QoS) サーバー構成」ウィンドウを開きます。
3. 「QoS サーバー構成」ウィンドウで、**「インバウンド許可ポリシー」**を右マウス・ボタンでクリックし、**「新規ポリシー」**を選択して、ウィザードを開きます。
4. 「ウェルカム」ページを読んでから、**「次へ」**をクリックします。
5. **「名前」**フィールドに「Restrict_TheirCo」と入力し、**「次へ」**をクリックします。オプションとして、このポリシーの意図を説明する記述を入力することができます。

6. 「クライアント」ページで、「**特定の 1 つまたは複数のアドレス**」を選択し、「**新規**」をクリックして、クライアントを定義します。
7. 「新規クライアント」ウィンドウで、以下の情報を入力します。
   - **名前**: Their_Co
   - **IP アドレスの範囲**: 10.1.1.1 - 10.1.1.10
   - 「**OK**」をクリックしてクライアントを作成し、ポリシー・ウィザードに戻ります。

   「**OK**」をクリックすると、ポリシー・ウィザードに戻ります。前に作成したクライアントがある場合は、それらをクリアして、関連するクライアントだけが選択されていることを確認します。
8. 「URI」ページで、「**すべての URI**」が選択されていることを確認し、「**次へ**」をクリックします。
9. 「アプリケーション」ページで、「**特定のポート、ポート範囲、またはサーバー・タイプ (Specific port, range of ports, or server type)**」を選択し、「**新規**」をクリックします。
10. 「新規アプリケーション」ウィンドウで、以下の情報を入力し、「**OK**」をクリックして、ウィザードに戻ります。
    - **名前**: HTTP
    - **ポート**: 80
11. 「**次へ**」をクリックして、「コード・ポイント (Codepoint)」ページへ進みます。
12. 「コード・ポイント (Codepoint)」ページで、「**すべてのコード・ポイント (All codepoints)**」が選択されていることを確認し、「**次へ**」をクリックします。
13. 「ローカル IP アドレス」ページで、「**IP アドレス**」を選択し、ローカル・システムへの要求に使用されるインターフェースを選択します。この例では、192.168.1.1 を使用します。
14. 「サービス・クラス (Class of Service)」ページで、「**新規**」をクリックし、パフォーマンス特性を定義します。「新規サービス・クラス (New Class of Service)」ウィザードが開きます。
15. 「ウェルカム」ページを読んでから、「**次へ**」をクリックします。
16. 「名前」ページで、「**inbound**」と入力し、「**次へ**」をクリックします。オプションとして、このサービス・クラスの意図を説明する記述を入力することができます。
17. 「サービス・タイプ (Type of Service)」ページで、「**インバウンドのみ (Inbound only)**」を選択します。このサービス・クラスはインバウンド・ポリシーのみに使用されます。
18. 「インバウンド限界」ページで、以下の情報を入力し、「**次へ**」をクリックします。
    - **平均接続率**: 50/秒
    - **接続バースト限界**: 50 接続
    - **優先順位**: 中
19. 「**完了**」をクリックして、ポリシー・ウィザードに戻ります。
20. 「サービス・クラス (Class of service)」ページで、作成したサービス・クラスが選択されていることを確認し、「**次へ**」をクリックします。
21. 「スケジュール」ページで、「**選択されたスケジュールの間アクティブ**」を選択し、「**新規**」をクリックします。
22. 「新規スケジュール」ウィンドウで、以下の情報を入力し、「**OK**」をクリックします。
    - **名前**: FirstShift
    - **時刻**: 特定時間にアクティブ、午前 9 時から午後 5 時を追加
    - **曜日**: 特定日にアクティブ、月曜日から金曜日を選択
23. 「スケジュール」ページで、「**次へ**」をクリックします。

24. 要約情報を検討します。情報が正しい場合は、「**完了**」をクリックして、ポリシーを作成します。「QoS サーバー構成」に、システムで作成されたすべてのポリシーがリストされます。 ウィザードの完了後は、右側のペインにポリシーがリストされます。

    これで、システムでのインバウンド許可ポリシーの構成が完了しました。次のステップは、サーバーを開始または更新することです。

シナリオ詳細: QoS サーバーの開始または更新

このトピックには、QoS サーバーの開始または更新に関する情報が記載されています。

「Quality of Service (QoS) サーバー構成」ウィンドウで、「**サーバー**」 → 「**開始**」または「**サーバー**」 → 「**更新**」を選択します。

シナリオ詳細: ポリシーが動作していることを確認する

このトピックには、モニターを使用してポリシーが構成したとおりに動作していることを検証する方法が記載されています。

1. 「Quality of Service (QoS) 構成」ウィンドウで、「**サーバー**」 → 「**モニター**」を選択します。「QoS モニター」ウィンドウが開きます。
2. インバウンド許可ポリシー・タイプを選択します。 すべてのインバウンド許可ポリシーが表示されます。リストから「**Restrict_TheirCo**」を選択します。

   すべての測定値フィールド (例えば、受け入れられた要求数、廃棄された要求数、合計要求数、接続率など) を必ず検査してください。廃棄された要求数は、トラフィックが、構成されたポリシー値を超えた場合に示されます。受け入れられた要求数は、(そのパケットが発信してから現在のモニター出力に至るまでの間) このポリシーによって制御されたビット数を示します。

   「**平均接続要求率**」フィールドにどのような値を割り当てるかということも重要です。パケットがこの制限値を超えると、システムはそれらのパケットの廃棄を開始します。 その結果、廃棄された要求数が増加します。 これは、ポリシーが、構成したとおりに動作していることを表しています。 すべてのモニター・フィールドについては、64 ページの『QoS のモニター』を参照してください。

   注: 正しい結果はポリシーがアクティブな場合にのみ得られます。 ポリシー内で指定したスケジュールを確認してください。

シナリオ詳細: プロパティーの変更

モニターの結果を調べた後、期待どおりの結果が得られるようにポリシーまたはサービス・クラス・プロパティーを変更できます。

1. 「Quality of Service (QoS) サーバー構成」ウィンドウで、「**インバウンド許可ポリシー**」フォルダーを選択します。 右側のペインのリストから「**Restrict_TheirCo**」を右マウス・ボタンでクリックし、「**プロパティー**」を選択して、ポリシーを編集します。「プロパティー」ウィンドウが開き、一般ポリシーを制御する値が示されます。
2. 該当する値を変更してください。
3. サービス・クラスを編集するには、「**サービス・クラス**」フォルダーを選択します。右側のペインのリストから「**インバウンド**」を右マウス・ボタンでクリックし、「**プロパティー**」を選択して、サービス・クラスを編集します。「QoS プロパティー」ウィンドウが開き、トラフィック管理を制御する値が示されます。
4. 該当する値を指定してください。
5. 「QoS サーバー構成」ウィンドウで、「**サーバー**」 → 「**更新**」 を選択し、変更を受け入れます。

シナリオ: 予測可能な B2B トラフィック

予測可能な送達が必要で、引き続き予約を要求したい場合は、IntServ ポリシーも使用します。 この例では、負荷制御サービスを使用します。

状態

販売部門から、ネットワーク・トラフィックが期待通りには機能していないことが報告されています。会社の i5/OS オペレーティング・システムは、予測可能なオンデマンド・ビジネス・サービスを必要とする企業間 (B2B) 環境に置かれています。 お客様に予測可能なトランザクションを提供する必要があります。 1 日で最も忙しい時間帯 (午前 10 時から午後 4 時) に受注アプリケーション用としてより高い Quality of Service (QoS) を販売課に提供したいと考えています。.

下記の図では、販売チームはプライベート・ネットワーク内に存在します。 B2B クライアントへのトラフィック・パス沿いの ReSerVation Protocol (RSVP) 使用可能ルーターがあります。それぞれの R は、トラフィック・パス沿いのルーターを表しています。

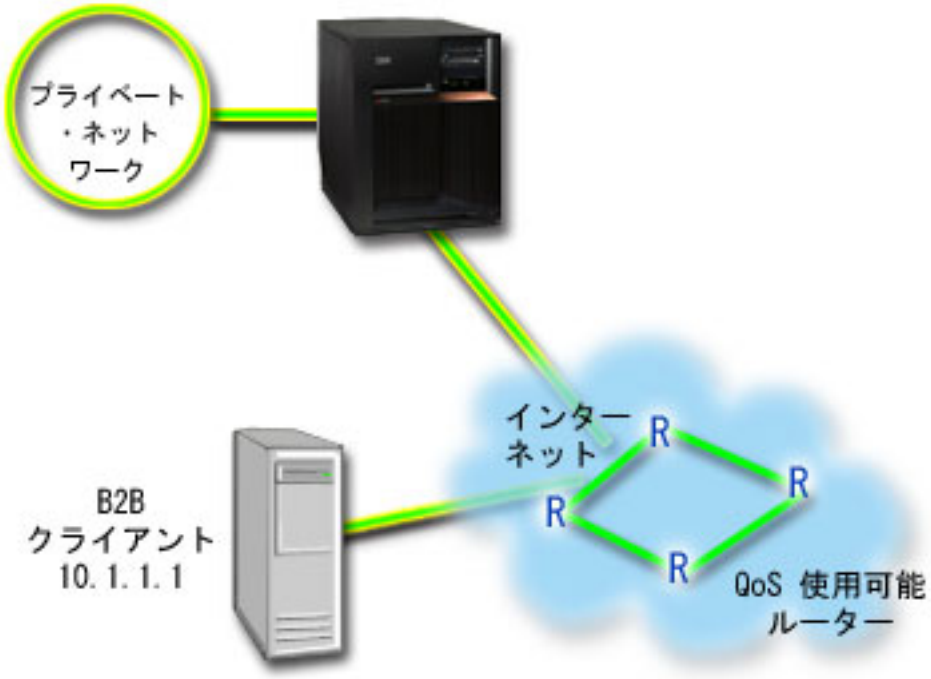


図 7. RSVP 使用可能ルーターを使用した B2B クライアントへの IntServ ポリシー

目的

負荷制御サービスは、混雑したネットワークによる影響を大きく受けるけれども少量の脱落や遅延を許容するアプリケーションをサポートします。 アプリケーションが負荷制御サービスを使用する場合、ネットワーク負荷が増えてもそのパフォーマンスには影響しません。トラフィックには、負荷が少ない状況でのネットワークの正常なトラフィックが受けられるサービスに類似したサービスが提供されます。 この特定のアプリケーションは少量の遅延を許容するので、負荷制御サービスを利用する IntServ ポリシーを使用することに決めました。

IntServ ポリシーを使用する場合、トラフィック・パス沿いにあるルーターも RSVP 使用可能でなくてはなりません。

前提条件および前提事項

IntServ ポリシーは高機能のポリシーであり、大量のリソースを必要とすることがあります。 IntServ ポリシーには以下の前提条件が必要です。

- **RSVP 使用可能アプリケーション**

  現在、ご使用のシステムには RSVP 使用可能アプリケーションがないため、ユーザー自身の RSVP 使用可能アプリケーションを作成する必要があります。 ユーザー自身のアプリケーションを作成するには、 RSVP API または qtoq QoS ソケット API を使用してください。

- **ネットワーク・パスに配備された RSVP 使用可能ルーターおよびシステム**

  QoS とは、つまりネットワーク・パフォーマンスを意味します。ネットワーク全体に RSVP 機能があるかどうか不確実な場合も、IntServ ポリシーを作成し、マーク付けを使用してそのポリシーに一定の優先順位を与えることができます。ただし、優先順位の保証はありません。

- **サービス・レベル・アグリーメント**

  ポリシーが要求された優先順位を受け取ることができるように、インターネット・サービス・プロバイダー (ISP) とサービス・レベル・アグリーメント (SLA) を交わしているとします。 システム上で作成する QoS ポリシーでは、トラフィックが (ポリシー内で) ネットワーク全体での優先順位を受け取るようにするものとします。 QoS ポリシーでは優先順位が保証されているわけではなく、これは SLA に依存します。 QoS ポリシーの利点を有効に利用すれば、一部のサービス・レベルおよび速度について折衝が可能になります。

  注: プライベート・ネットワーク内では、SLA は必要ありません。

構成

前提条件のステップを確認したら、IntServ ポリシーの作成準備は完了です。

関連概念

10 ページの『IntServ タイプ』
IntServ には、負荷制御サービスと保証サービスの 2 つのタイプがあります。

7 ページの『IntServ』
作成できるアウトバウンド帯域幅ポリシーの第 2 のタイプは、IntServ ポリシーです。 IntServ によって、IP アプリケーションは、ReSerVation Protocol (RSVP) と QoS API を使用して帯域幅を要求し予約することができます。

18 ページの『Quality of Service API』
このトピックには、プロトコルと API に関する情報、および ReSerVation Protocol (RSVP) で使用可能なルーターに関する要件が記載されています。Quality of Service (QoS) API には、RAPI API、qtoq ソケット API、sendmsg() API、およびモニター API が含まれています。

55 ページの『サービス・レベル・アグリーメント』
このトピックでは、QoS (Quality of Service) インプリメンテーションに影響を及ぼす可能性があるサービス・レベル・アグリーメント (SLA) の重要な特徴のいくつかを指摘します。 QoS とは、つまりネットワーク・パフォーマンスを意味します。プライベート・ネットワークの外部でネットワーク優先順位を受け取るには、インターネット・サービス・プロバイダー (ISP) との SLA を保持する必要が生じる場合があります。

関連資料

64 ページの『QoS のモニター』
Quality of Service (QoS) モニターを利用して、システムで IP トラフィックを分析できます。

シナリオ詳細: IntServ ポリシーの作成

このトピックには、システム上での IntServ ポリシーの作成に関する情報が記載されています。

1. System i ナビゲーター で、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**IP ポリシー**」の順に展開します。
2. 「**Quality of Service**」を右マウス・ボタンでクリックし、「**構成**」を選択して、「Quality of Service (QoS) サーバー構成」ウィンドウを開きます。
3. 「QoS サーバー構成」ウィンドウで、IntServ ポリシー・タイプを右マウス・ボタンでクリックし、「**新規ポリシー**」を選択して、ウィザードを開きます。
4. 「ウェルカム」ページを読んでから、「**次へ**」をクリックして、「**名前**」ページへ進みます。
5. 「**名前**」フィールドに「B2B_CL」と入力し、「**次へ**」をクリックします。オプションとして、このポリシーの意図を説明する記述を入力することができます。
6. 「クライアント」ページで、「**特定の 1 つまたは複数のアドレス**」を選択し、「**新規**」をクリックして、クライアントを定義します。
7. 「新規クライアント」ウィンドウで、以下の情報を入力します。
   - **名前**: CL_client
   - **IP アドレス**: 10.1.1.1
   - 「**OK**」をクリックしてクライアントを作成し、ポリシー・ウィザードに戻ります。

   「**OK**」をクリックすると、ポリシー・ウィザードに戻ります。前に作成されたクライアントがある場合は、それらをクリアして、関連するクライアントだけが選択されていることを確認します。
8. 「新規アプリケーション」ウィンドウで、以下の情報を入力し、「**OK**」をクリックして、ウィザードに戻ります。
   - **名前**: business_app
   - **ポートの範囲**: 7000-8000
9. 「アプリケーション」ページで、「**プロトコル**」を選択し、「**TCP**」が選択されていることを確認します。「**次へ**」をクリックします。

   注: IntServ ポリシー用に選択するアプリケーションは、Resource Reservation Setup Protocol (RAPI) API または qtoq ソケット API を使用するように作成されている必要があります。これらの API は、ReSerVation Protocol (RSVP) と共に、ネットワークでの IntServ の予約を行います。これらの API を使用しない場合は、アプリケーションは優先順位付けおよび保証を受け取りません。また、このポリシーは、アプリケーションがネットワークを使用して優先順位を受け取ることを可能にしますが、保証はしないことを理解しておくことが大切です。予約を保証するためには、トラフィックのパスに配備されたすべてのルーターとシステムも RSVP を使用する必要があります。エンドツーエンドの予約は、ネットワーク全体の状態に依存します。
10. 「ローカル IP アドレス」ページで、デフォルト値を受け入れて、「**次へ**」をクリックします。
11. 「IntServ のタイプ (Integrated Services Type)」ページで、「**制御負荷 (Controlled load)**」を選択し、「**次へ**」をクリックします。
12. 「IntServ のマーク付け」ページで、「**いいえ。PHB を割り当てません**」を選択し、「**次へ**」をクリックします。
13. 「IntServ パフォーマンス限界」ページで、以下の情報を入力し、「**次へ**」をクリックします。
    - **フローの最大数**: 5
    - **トークン速度限界 (R)**: 制限しない
    - **トークン・バケット・サイズ**: 100 K ビット

- **トークン速度限界 (R)**: 25 M ビット/秒

14. 「スケジュール」ページで、「**選択されたスケジュールの間アクティブ**」を選択し、「**新規**」をクリックします。
15. 「新規スケジュール」ページで、以下の情報を入力し、「**OK**」をクリックします。
    - **名前**: primetime
    - **時刻**: 特定時間にアクティブ、午前 10 時から午後 4 時を追加
    - **曜日**: 特定日にアクティブ、月曜日から金曜日を選択
16. 「スケジュール」ページで、「**次へ**」をクリックします。
17. 要約情報を検討します。 情報が正しい場合は、「**完了**」をクリックして、ポリシーを作成します。メイン QoS インターフェースに、システム上で作成されたすべてのポリシーがリストされます。 ウィザードの完了後は、右側のペインにポリシーがリストされます。

これで、システムでの IntServ ポリシーの構成が完了しました。次のステップは、サーバーを開始または更新することです。

シナリオ詳細: QoS サーバーの開始または更新

このトピックには、QoS サーバーの開始または更新に関する情報が記載されています。

「Quality of Service (QoS) サーバー構成」ウィンドウで、「**サーバー**」 → 「**開始**」または「**サーバー**」 → 「**更新**」を選択します。

シナリオ詳細: ポリシーが動作していることを確認する

このトピックには、モニターを使用してポリシーが構成したとおりに動作していることを検証する方法が記載されています。

1. 「Quality of Service (QoS) サーバー構成」ウィンドウで、「**サーバー**」 → 「**モニター**」を選択します。 「QoS モニター」ウィンドウが開きます。
2. IntServ ポリシー・タイプを選択します。すべての IntServ ポリシーが表示されます。

   最も注意を払う必要のあるフィールドは、トラフィックからデータを取得するフィールドです。 合計ビット数、プロファイル中のビット数およびプロファイル中のパケット数の各フィールドを必ずチェックしてください。プロファイル外ビット数は、この IntServ ポリシーの要件を満たすために他のトラフィックを遅らせるか、または廃棄することを示します。モニター・フィールドの詳細は、64 ページの『QoS のモニター』を参照してください。

   注: 正しい結果はポリシーがアクティブな場合にのみ得られます。 ポリシー内で指定したスケジュールを確認してください。また、モニターには、アプリケーションが実行された後にのみ IntServ ポリシーが表示されます。 モニターを実行する前に ReSerVation Protocol (RSVP) 予約を設定する必要があります。

シナリオ詳細: プロパティーの変更

モニターの結果を調べた後、期待どおりの結果が得られるようにポリシーのプロパティーを変更できます。

1. 「Quality of Service (QoS) サーバー構成」ウィンドウで、「**IntServ**」フォルダーを選択します。右側のペインのリストから「**B2B_CL**」を右マウス・ボタンでクリックし、「**プロパティー**」を選択して、ポリシーを編集します。「プロパティー」ウィンドウが開き、一般ポリシーを制御する値が示されます。
2. 該当する値を指定してください。
3. 「QoS サーバー構成」ウィンドウで、「**サーバー**」 → 「**更新**」 を選択し、変更を受け入れます。

シナリオ: 専用送達 (IP テレフォニー)

専用送達が必要で、予約を要求したい場合は、IntServ ポリシーを使用します。作成する IntServ ポリシーには、2 つのタイプ (保証サービスと負荷制御サービス) があります。 この例では、保証サービスが使用されています。

状態

会社の最高経営責任者 (CEO) は、午後 1 時から 2 時の間、地域のクライアントにライブ・ブロードキャストを提供したいと考えています。ブロードキャスト中に中断が起こらないように IP テレフォニーに保証された帯域幅を用意する必要があります。このシナリオでは、アプリケーションはサーバーに常駐させます。

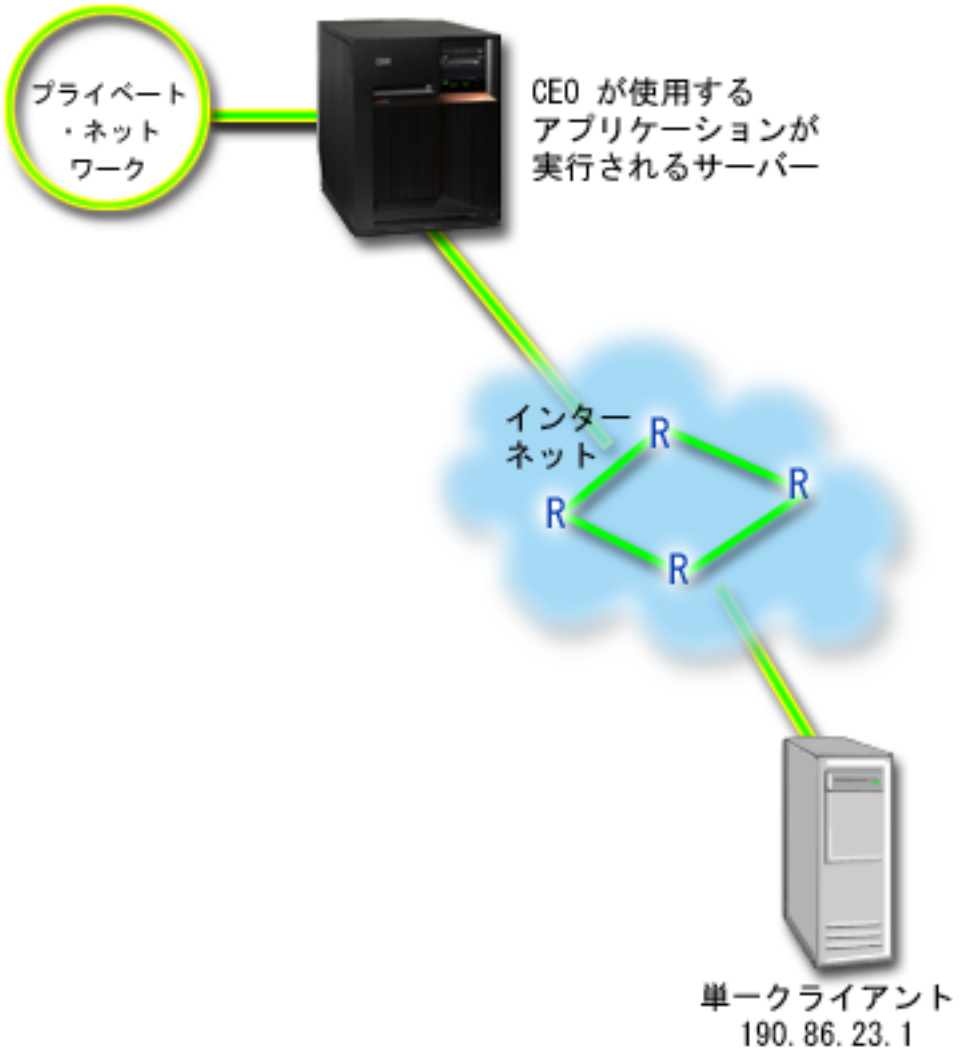


図 8. IntServ ポリシーによって保証された CEO からクライアントへのプレゼンテーション

目的

CEO が使用しているアプリケーションはスムーズで中断されない転送を必要とするので、保証された IntServ ポリシーを使用することに決めました。保証サービスは、パケットが指定時間以上は遅れないように最大キューイング遅延を制御します。

前提条件および前提事項

IntServ ポリシーは高機能のポリシーであり、大量のリソースを必要とすることがあります。 IntServ ポリシーには以下の前提条件が必要です。

- **RSVP 使用可能なアプリケーション**

  現在、ご使用のシステムには RSVP 使用可能アプリケーションがないため、ユーザー自身の RSVP 使用可能アプリケーションを作成する必要があります。 ユーザー自身のアプリケーションを作成するには、 ReSerVation Protocol (RAPI) API または qtoq Quality of Service (QoS) ソケット API を使用してください。 詳しくは 18 ページの『Quality of Service API』で IntServ API の説明を参照してください。

- **ネットワーク・パスに配備された RSVP 使用可能ルーターおよびシステム**

  QoS とは、つまりネットワーク・パフォーマンスを意味します。ネットワーク全体に RSVP 機能があるかどうか不確実な場合も、IntServ ポリシーを作成し、マーク付けを使用してそのポリシーに一定の優先順位を与えることができます。ただし、優先順位の保証はありません。

- **サービス・レベル・アグリーメント**

  ポリシーが要求された優先順位を受け取ることができるように、インターネット・サービス・プロバイダー (ISP) とサービス・レベル・アグリーメント (SLA) を交わしているとします。 システム上で作成する QoS ポリシーでは、トラフィックが (ポリシー内で) ネットワーク全体での優先順位を受け取るようにするものとします。 QoS ポリシーでは優先順位が保証されているわけではなく、これは SLA に依存します。 QoS ポリシーの利点を有効に利用すれば、一部のサービス・レベルおよび速度について折衝が可能になります。

構成

前提条件のステップを確認したら、IntServ ポリシーの作成準備は完了です。

関連概念

10 ページの『IntServ タイプ』
IntServ には、負荷制御サービスと保証サービスの 2 つのタイプがあります。

7 ページの『IntServ』
作成できるアウトバウンド帯域幅ポリシーの第 2 のタイプは、IntServ ポリシーです。 IntServ によって、IP アプリケーションは、ReSerVation Protocol (RSVP) と QoS API を使用して帯域幅を要求し予約することができます。

55 ページの『サービス・レベル・アグリーメント』
このトピックでは、QoS (Quality of Service) インプリメンテーションに影響を及ぼす可能性があるサービス・レベル・アグリーメント (SLA) の重要な特徴のいくつかを指摘します。 QoS とは、つまりネットワーク・パフォーマンスを意味します。プライベート・ネットワークの外部でネットワーク優先順位を受け取るには、インターネット・サービス・プロバイダー (ISP) との SLA を保持する必要が生じる場合があります。

関連資料

64 ページの『QoS のモニター』
Quality of Service (QoS) モニターを利用して、システムで IP トラフィックを分析できます。

シナリオ詳細: IntServ ポリシーの作成

このトピックには、システム上での IntServ ポリシーの作成に関する情報が記載されています。

1. System i ナビゲーター で、**「ユーザーのシステム」** → **「ネットワーク」** → **「IP ポリシー」**の順に展開します。
2. 「**Quality of Service**」を右マウス・ボタンでクリックし、「**構成**」を選択して、「Quality of Service (QoS) サーバー構成」ウィンドウを開きます。
3. 「QoS サーバー構成」ウィンドウで、IntServ ポリシー・タイプを右マウス・ボタンでクリックし、「**新規ポリシー**」を選択して、ウィザードを開きます。
4. 「ウェルカム」ページを読んでから、「**次へ**」をクリックして、「**名前**」ページへ進みます。
5. 「**名前**」フィールドに「CEO_guaranteed」と入力し、「**次へ**」をクリックします。オプションとして、このポリシーの意図を説明する記述を入力することができます。
6. 「クライアント」ページで、「**特定の 1 つまたは複数のアドレス**」を選択し、「**新規**」をクリックして、クライアントを定義します。
7. 「新規クライアント」ウィンドウで、以下の情報を入力します。
   - **名前**: Branch1
   - **IP アドレス**: 190.86.23.1
   - 「**OK**」をクリックしてクライアントを作成し、IntServ ウィザードに戻ります。

   「OK」をクリックすると、ポリシー・ウィザードに戻ります。前に作成されたクライアントがある場合は、それらをクリアして、関連するクライアントだけが選択されていることを確認します。「アプリケーション」ページで、「**特定のポート、ポート範囲、またはサーバー・タイプ (Specific port, range of ports, or server type)**」を選択し、「**新規**」をクリックします。
8. 「新規アプリケーション」ウィンドウで、以下の情報を入力し、「**OK**」をクリックして、ウィザードに戻ります。
   - **名前**: IP telephony
   - **ポート**: 2427
9. 「アプリケーション」ページで、「**プロトコル**」を選択し、「**TCP**」が選択されていることを確認します。「**次へ**」をクリックします。

   注: IntServ ポリシー用に選択するアプリケーションは、Resource Reservation Setup Protocol (RAPI) API または qtoq ソケット API を使用するように作成されている必要があります。これらの API は、ReSerVation Protocol (RSVP) と共に、ネットワークでの IntServ の予約を行います。これらの API を使用しない場合は、アプリケーションは優先順位付けおよび保証を受け取りません。また、このポリシーは、アプリケーションがネットワークを使用して優先順位を受け取ることを可能にしますが、保証はしないことを理解しておくことが大切です。予約を保証するためには、トラフィックのパスに配備されたすべてのルーターとサーバーも RSVP を使用する必要があります。 エンドツーエンドの予約は、ネットワーク全体の状態に依存します。
10. 「ローカル IP アドレス」ページで、デフォルト値「**すべての IP アドレス**」を受け入れます。
11. 「IntServ のタイプ (Integrated Services Type)」ページで、「**保証サービス (Guaranteed)**」を選択し、「**次へ**」をクリックします。
12. 「IntServ のマーク付け」ページで、「**いいえ。PHB を割り当てません**」を選択し、「**次へ**」をクリックします。
13. 「IntServ パフォーマンス限界」ページで、以下の情報を入力し、「**次へ**」をクリックします。
   - **フローの最大数**: 1
   - **集約帯域幅限界 (R) (Aggregate bandwidth limit (R))**: 制限しない
   - **トークン・バケット・サイズ**: 100 K ビット

- **帯域幅限界 (R) (Bandwidth limit (R))**: 16 M ビット/秒

14. 「スケジュール」ページで、「**選択されたスケジュールの間アクティブ**」を選択し、「**新規**」をクリックします。
15. 「新規スケジュール」ページで、以下の情報を入力し、「**OK**」をクリックします。
    - **名前**: one_hour
    - **時刻**: 特定時間にアクティブ、午後 1 時から 2 時を追加
    - **曜日**: 特定日にアクティブ、月曜日を選択
16. 「スケジュール」ページで、「**次へ**」をクリックします。
17. 要約情報を検討します。 情報が正しい場合は、「**完了**」をクリックして、ポリシーを作成します。「QoS サーバー構成」メイン・ウィンドウに、サーバーで作成されたすべてのポリシーがリストされます。ウィザードの完了後は、右側のペインにポリシーがリストされます。

これで、システムでの IntServ ポリシーの構成が完了しました。次のステップは、サーバーを開始または更新することです。

シナリオ詳細: QoS サーバーの開始または更新

このトピックには、QoS サーバーの開始または更新に関する情報が記載されています。

「Quality of Service (QoS) サーバー構成」ウィンドウで、「**サーバー**」 → 「**開始**」または「**サーバー**」 → 「**更新**」を選択します。

シナリオ詳細: ポリシーが動作していることを確認する

このトピックには、モニターを使用してポリシーが構成したとおりに動作していることを検証する方法が記載されています。

1. 「Quality of Service (QoS) サーバー構成」ウィンドウで、「**サーバー**」 → 「**モニター**」を選択します。「QoS モニター」ウィンドウが開きます。
2. IntServ ポリシー・タイプ・フォルダーを選択します。すべての IntServ ポリシーが表示されます。

   最も注意を払う必要のあるフィールドは、トラフィックからデータを取得する測定フィールドです。合計ビット数、プロファイル中のビット数およびプロファイル中のパケット数の各フィールドがあります。プロファイル外ビット数は、この IntServ ポリシーの要件を満たすために他のトラフィックを遅らせるか、または廃棄することを示します。 すべてのモニター・フィールドについては、64 ページの『QoS のモニター』を参照してください。

   注: 正しい結果はポリシーがアクティブな場合に得られます。ポリシー内で指定したスケジュールを確認してください。また、モニターには、アプリケーションが実行された後にのみ IntServ ポリシーが表示されます。 モニターを実行する前に ReSerVation Protocol (RSVP) 予約を設定する必要があります。

シナリオ詳細: プロパティーの変更

モニターの結果を調べた後、期待どおりの結果が得られるようにポリシーのプロパティーを変更できます。

1. 「Quality of Service (QoS) サーバー構成」ウィンドウで、「**IntServ**」フォルダーを選択します。右側のペインのリストから「**CEO_guaranteed**」を右マウス・ボタンでクリックし、「**プロパティー**」を選択して、ポリシーを編集します。「プロパティー」ウィンドウが開き、一般ポリシーを制御する値が示されます。
2. 該当する値を指定してください。
3. 「QoS サーバー構成」ウィンドウで、「**サーバー**」 → 「**更新**」 を選択し、変更を受け入れます。

シナリオ: 現在のネットワーク統計のモニター

ウィザードの中で、個々のネットワーク要件に基づくパフォーマンス制限を設定する必要があります。

目的

この制限値を設定するためには、現在のネットワーク・パフォーマンスについてよく理解しておく必要があります。 Quality of Service (QoS) ポリシーの構成を試みているということは、現在のネットワーク要件について十分に認識しているものと想定されます。正確な速度限界 (例えば、トークン・バケット速度) を判断する場合に、どの速度限界を設定すべきかをより良く判断できるように、システム上のすべてのトラフィックをモニターすることができます。

ソリューション

制限値 (最大値ではない) を含まず、かつすべてのインターフェースおよびすべての IP アドレスに適用される、許容範囲の広い DiffServ ポリシーを作成してください。 QoS モニターを使用して、このポリシーに関するデータを記録します。

関連概念

11 ページの『トークン・バケットおよび帯域幅の限界』
トークン・バケット限界と帯域幅限界はともにパフォーマンス制限として知られています。これらのパフォーマンス制限によって、アウトバウンド帯域幅ポリシー (IntServ および DiffServ の両方) 内でのパケットの送達が保証されます。

18 ページの『平均接続率およびバースト限界』
接続率およびバースト限界は、速度限界です。これらの速度限界は、システムに入ろうとするインバウンド接続を制限するのに役立ちます。 速度限界はインバウンド許可ポリシーで使用するサービス・クラスに設定します。

関連資料

64 ページの『QoS のモニター』
Quality of Service (QoS) モニターを利用して、システムで IP トラフィックを分析できます。

シナリオ詳細: System i ナビゲーター での QoS のオープン

このトピックには、System i ナビゲーター 内で QoS を開く方法が記載されています。

1. System i ナビゲーター で、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**IP ポリシー**」の順に展開します。
2. 「**Quality of Service**」を右マウス・ボタンでクリックし、「**構成**」を選択します。
3. 「**アウトバウンド帯域幅ポリシー**」を展開します。
4. 「**DiffServ**」を右マウス・ボタンでクリックし、「**新規ポリシー (New Policy)**」を選択します。「新規 DiffServ ポリシー」ウィザードが開きます。

シナリオ詳細: DiffServ ポリシーの作成

ネットワークに入るほとんどのトラフィックを収集するのにポリシー Network を呼び出します。すべての IP アドレス、すべてのポート、すべてのローカル IP アドレス、およびすべての時刻 (適宜) を使用します。

ウィザードでは、次の設定値を使用します。

名前: Network (任意の名前を割り当てられる)
クライアント: すべての IP アドレス
アプリケーション: すべてのポート
プロトコル: すべて
スケジュール: 常にアクティブ

System i ナビゲーター が、システムに作成されたすべての DiffServ ポリシーをリストします。

シナリオ詳細: 新規のサービス・クラスの完成

ウィザードを進んで行くと、PHB (ホップごとの転送優先順位付け)、パフォーマンス制限、およびプロファイル外トラフィックの処理を割り当てるように指示されます。 これは、サービス・クラスの中で定義されます。可能な限り多くのトラフィック・フローを許容するための特に大きな値を選択します。

実際は、サービス・クラスが、このトラフィックがルーターから受け取るパフォーマンス・レベルを決定します。このトラフィックがより高いサービスを受けることを示すように、サービス・クラスに Unlimited という名前を付けます。System i ナビゲーター が、サーバーに定義されたすべてのサービス・クラスをリストします。

シナリオ詳細: ポリシーをモニターする

モニターを使用して、トラフィックが、ポリシーの中で構成したとおりに動作しているかを検証することができます。

1. 特定のポリシー・フォルダー (DiffServ、IntServ、インバウンド許可) を選択します。
2. モニターするポリシーを右マウス・ボタンでクリックし、「**モニター**」を選択します。

次の図は、上記で設定したポリシーに関して考えられるモニター出力をリストしたものです。

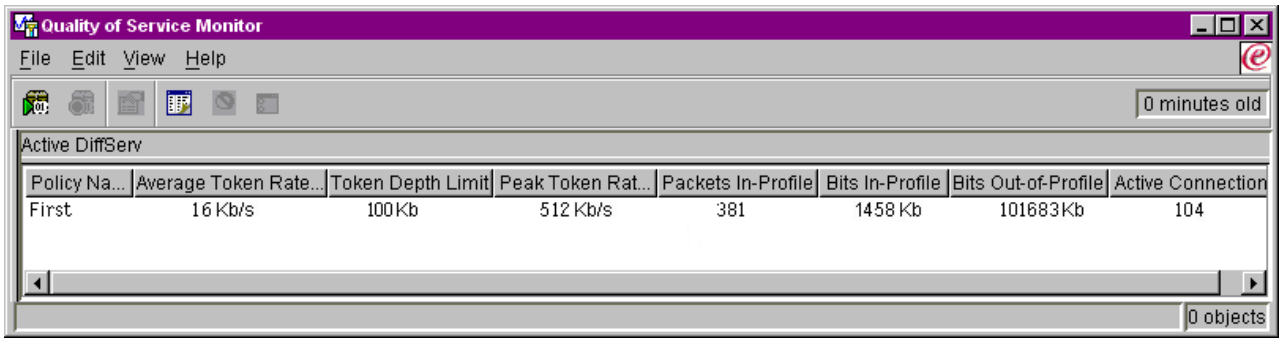


図 9. Quality of Service (QoS) モニター

トラフィックからデータを取得するフィールドを探してください。合計ビット数、プロファイル中のビット数、プロファイル中のパケット数、およびプロファイル外ビット数の各フィールドを必ずチェックしてください。プロファイル外ビット数は、トラフィックが、構成されたポリシー値を超えた場合に示されます。DiffServ ポリシーの中のプロファイル外の数は、廃棄されるバイト数を表します。プロファイル中のパケット数は、(そのパケットが発信してから現在のモニター出力に至るまでの間) このポリシーによって制御されたバイト数を示します。

「**平均トークン速度限界**」フィールドにどのような値を割り当てるかということも重要です。パケットがこの制限値を超えると、システムはそれらのパケットの廃棄を開始します。 その結果、プロファイル外ビット数が増加します。 これは、ポリシーが、構成したとおりに動作していることを表しています。 プロファイル外ビット数を変更するには、パフォーマンス制限を調整する必要があります。 すべてのモニター・フィールドについては、 64 ページの『QoS のモニター』を参照してください。

シナリオ詳細: 値の変更

モニターした後、前に選択した任意の値を変更することができます。 このポリシーで作成したサービス・クラス名を右マウス・ボタンでクリックします。「**プロパティー**」を選択すると、トラフィックの制御値が表示された「QoS プロパティー」ウィンドウが開きます。

シナリオ詳細: ポリシーを再度モニターする

表示された結果を見てから、「推測とチェック」方式を使用して、ネットワークのニーズに合う最適の制限を見つけます。

Quality of Service の計画

Quality of Service (QoS) を達成するための最も重要なステップは計画です。期待どおりの結果を得るためには、ネットワーク装置とモニター・ネットワーク・トラフィックを確認する必要があります。

このトピックでは、計画アドバイザーについても説明します。『QoS 計画アドバイザー』には、計画フェーズでご自分で確認する必要のある基本的な質問事項が記載されています。アドバイザーに加えて、QoS を構成する前に次のサブトピックも考慮してください。

ネットワーク・パフォーマンスに関する考慮事項

QoS とは、つまりネットワーク・パフォーマンスを意味します。 QoS の使用を考える主な理由は、既にネットワーク輻輳 (ふくそう) とパケット・ロスを経験しているから、という場合がほとんどです。ポリシーをインプリメントする前に、QoS モニターを使用して IP トラフィックの現在のパフォーマンス・レベルを検証する必要があります。このモニター結果から、どこで輻輳 (ふくそう) が発生しているかを判断できます。

関連概念

72 ページの『システム・トランザクションのモニター』
QoS (Quality of Service) モニターを使用して、QoS ポリシーが意図したとおりに機能しているか確認することができます。QoS モニターは、QoS の計画フェーズとトラブルシューティング・フェーズで役に立ちます。

58 ページの『Quality of Service の構成』
QoS (Quality of Service) の計画を立てた後で、System i ナビゲーター のウィザードを使用して QoS ポリシーを作成します。このトピックでは、DiffServ ポリシー、IntServ ポリシー、およびインバウンド許可ポリシーの作成方法を説明します。

権限要件

Quality of Service (QoS) ポリシーには、ネットワークに関する機密情報が含まれることがあります。したがって、QoS 管理権限は、必要な場合にのみ付与してください。

QoS ポリシーおよびオプションで Lightweight Directory Access Protocol (LDAP) ディレクトリー・サーバーを構成するためには、下記の権限が必要になります。

ディレクトリー・サーバーを管理するための権限の付与

QoS 管理者には、*ALLOBJ 権限と *IOSYSCFG 権限が必要です。代替権限については、『ディレクトリー・サーバーの構成』を参照してください。

TCP/IP サーバーを開始するための権限の付与

STRTCPSVR および ENDTCPSVR コマンドに対するオブジェクト権限を付与するには、以下のステップにしたがってください。

1. **STRTCPSVR**: コマンド行で GRTOBJAUT OBJ (QSYS/STRTCPSVR) OBJTYPE (*CMD) USER (ADMINPROFILE) AUT (*USE) を入力し、ADMINPROFILE に対する管理者のプロファイルの名前を置き換えて、「Enter」キーを押します。
2. **ENDTCPSVR**: コマンド行で GRTOBJAUT OBJ (QSYS/ENDTCPSVR) OBJTYPE (*CMD) USER (ADMINPROFILE) AUT (*USE) を入力し、ADMINPROFILE に対する管理者のプロファイルの名前を置き換えて、「Enter」キーを押します。

全オブジェクト許可およびシステム構成権限の付与

QoS を構成するユーザーは機密保護担当者アクセス権を持つことをお勧めします。全オブジェクト許可およびシステム構成権限を付与するには、以下のステップにしたがってください。

1. System i ナビゲーター で、**「ユーザーのシステム」** → **「ユーザーおよびグループ」**を展開します。
2. **「すべてのユーザー」**をダブルクリックします。
3. 管理者のユーザー・プロファイルを右クリックして、**「プロパティー」**を選択します。
4. 「プロパティー」ウィンドウで、**「機能」**をクリックします。
5. 「機能」ページで、**「すべてのオブジェクト・アクセス」および「システム構成」**を選択します。
6. **「OK」**をクリックして、「機能」ページをクローズします。
7. **「OK」**をクリックして、「プロパティー」ウィンドウをクローズします。

システム要件

Quality of Service (QoS) は、オペレーティング・システムの統合化の一部です。

以下の処理を完了させておく必要があります。

1. IBM TCP/IP Connectivity Utilities for i5/OS (5761-TC1) をインストールします。
2. System i ナビゲーター をご使用の PC にインストールします。 System i Access のインストール中に、必ず「ネットワーキング」コンポーネントをインストールしてください。 Quality of Service は、「ネットワーキング」フォルダーの中の「IP ポリシー」下にあります。

   関連概念

   System i Navigator 入門

   関連資料

   76 ページの『Quality of Service の関連情報』

   Quality of Service の Request For Comments、IBM Redbooks 資料、およびその他の Information Center トピック・コレクションには、Quality of Service トピック・コレクションに関連する情報が記載されています。以下の PDF ファイルのいずれも表示または印刷できます。

サービス・レベル・アグリーメント

このトピックでは、QoS (Quality of Service) インプリメンテーションに影響を及ぼす可能性があるサービス・レベル・アグリーメント (SLA) の重要な特徴のいくつかを指摘します。 QoS とは、つまりネットワーク・パフォーマンスを意味します。プライベート・ネットワークの外部でネットワーク優先順位を受け取るには、インターネット・サービス・プロバイダー (ISP) との SLA を保持する必要が生じる場合があります。

SLA が必要な場合

SLA は、プライベート・ネットワークの外部で優先順位を必要とするポリシーを使用する場合にのみ必要です。 システムから発信されるトラフィックを制御するためにアウトバウンド・ポリシーを使用する場合は、サービス保証は必要ありません。例えば、システム上で、あるアプリケーションに別のアプリケーションより高い優先順位を与えるポリシーを作成できます。 システムはこの優先順位を認識しますが、システムの外部ではこの優先順位はまったく認識されません。 プライベート・ネットワークにおいて、コード・ポイントのマーク付け (アウトバウンド・ポリシーにサービス・レベルを与えるために使用される) を認識するようにルーターを構成する場合、ルーターはプライベート・ネットワークでの優先順位を与えます。しかし、トラフィックがプライベート・ネットワークから出る場合、保証はまったくありません。 SLA がないと、ネットワーク・ハードウェアによるトラフィックの処理を制御できません。 プライベート・ネットワークの外部では、サービス・クラスの優先順位またはリソース予約を保証するために SLA が必要です。

SLA が必要な理由

ポリシーと予約は、最も弱いリンクの能力に合わせて機能します。つまり、QoS ポリシーにより、アプリケーションはネットワークでの優先順位を受け取ることができます。 しかし、クライアントとサーバーの間に存在する、あるノードが、DiffServ または IntServ のトピックで説明されているトラフィック処理特性のいずれかを実行できない場合、ポリシーは意図したとおりに処理されません。 SLA によって十分なリソースが使用可能でないと、最高のポリシーであってもネットワークの輻輳 (ふくそう) 問題を解決できません。

これは、ISP 間の合意にもかかわります。複数のドメインにわたり、すべての ISP は QoS 要求のサポートに合意していなくてはなりません。相互運用性が問題を引き起こす可能性もあります。

必ず、実際に受けているサービス・レベルを確認してください。 トラフィック調整アグリーメントは、特にトラフィックの処理方法 (廃棄、マーク付け、シェイピング、または再送) に関する合意です。 QoS を提供する主な理由は、待ち時間、ジッター、帯域幅、パケット・ロス、可用性、およびスループットにかかわっています。サービス・レベル・アグリーメント (SLA) は、ポリシーに、そのポリシーが要求するものを提供できなくてはなりません。現在、必要な量のサービスを受けているかを確認してください。受けていない場合は、リソースを無駄にしている可能性があります。例えば、IP 電話用に 500 kbps の予約を要求しても、アプリケーションは 20 kbps しか必要としない場合、ISP からは通知がなくても余分な料金を支払っている可能性があります。

注: QoS ポリシーでは、ISP とサービス・レベルを折衝することが可能であり、その結果ネットワーク・サービス・コストが削減されることがあります。 例えば、ユーザーが合意された帯域幅レベルを超えない場合、ISP は一定の金額を保証することがあります。あるいは、QoS ポリシーの使用により、昼間は帯域幅のうち ″x″ に相当する分だけを使用し、夜間は ″y″ に相当する分だけを使用し、時間フレーム別の料金に合意することができます。また、帯域幅を超えた場合は、ISP は追加料金を請求する場合があります。 ISP は一定のサービス・レベルに同意する必要があり、ユーザーが使用する帯域幅を追跡する能力を持っている必要があります。

関連概念

1 ページの『概念』

QoS (Quality of Service) を使用する前に、基本的な用語および QoS の概念を理解する必要があります。これらの概念は、サービスがお客様のニーズに合っているかどうかを判別する上で役立ちます。

31 ページの『シナリオ: ブラウザー・トラフィックの制限』
QoS (Quality of Service) を使用して、トラフィック・パフォーマンスを制御することができます。 ネットワーク内でのアプリケーションのパフォーマンスを制限または拡張するには、DiffServ ポリシーを使用します。

36 ページの『シナリオ: 安全で予測可能な結果 (VPN と QoS)』
VPN (仮想プライベート・ネットワーク) を使用している場合でも、Quality of Service (QoS) ポリシーを作成できます。

44 ページの『シナリオ: 予測可能な B2B トラフィック』
予測可能な送達が必要で、引き続き予約を要求したい場合は、IntServ ポリシーも使用します。 この例では、負荷制御サービスを使用します。

48 ページの『シナリオ: 専用送達 (IP テレフォニー)』
専用送達が必要で、予約を要求したい場合は、IntServ ポリシーを使用します。作成する IntServ ポリシーには、2 つのタイプ (保証サービスと負荷制御サービス) があります。 この例では、保証サービスが使用されています。

ネットワークのハードウェアおよびソフトウェア

ネットワーク内部の装置とネットワーク外部の他の装置の能力は、Quality of Service (QoS) の結果に非常に大きく影響します。

アプリケーション

IntServ ポリシーには、ReSerVation Protocol (RSVP) で使用可能にされるアプリケーションが必要です。 i5/OS アプリケーションは、最初は RSVP が使用できないので、それらのアプリケーションが RSVP を使用できるようにする必要があります。このためには、RSVP API または qtoq QoS ソケット API を利用して特別なプログラムを作成する必要があります。 このプログラムによって、アプリケーションは RSVP を使用できるようになります。

ネットワーク・ノード

ルーター、スイッチ、さらにはご使用のシステムにいたるまで、QoS を使用する能力をもっている必要があります。 DiffServ ポリシーを使用するには、装置が DiffServ 使用可能でなくてはなりません。 つまり、ネットワーク・ノードには、IP パケット (トラフィック・コンディショナー) の分類、計量、マーク付け、シェイピング、および廃棄を行う能力が必要です。

IntServ ポリシーを使用するには、装置が RSVP 使用可能でなくてはなりません。つまり、ネットワーク・ノードが RSVP もサポートできなくてはなりません。

関連概念

18 ページの『Quality of Service API』
このトピックには、プロトコルと API に関する情報、および ReSerVation Protocol (RSVP) で使用可能なルーターに関する要件が記載されています。Quality of Service (QoS) API には、RAPI API、qtoq ソケット API、sendmsg() API、およびモニター API が含まれています。

6 ページの『トラフィック・コンディショナー』
QoS (Quality of Service) ポリシーを使用するには、ネットワーク装置 (ルーターやスイッチなど) にトラフィック・コンディショナーの機能が備わっている必要があります。トラフィック・コンディショナーは、分類子、計量機能、マーカー、シェイパー、およびドロッパーを表します。

Quality of Service の構成

QoS (Quality of Service) の計画を立てた後で、System i ナビゲーター のウィザードを使用して QoS ポリシーを作成します。このトピックでは、DiffServ ポリシー、IntServ ポリシー、およびインバウンド許可ポリシーの作成方法を説明します。

これらのウィザードから出される指示に従うことで、構成をスムーズに行うことができます。

ポリシーを構成した後は、System i ナビゲーター の構成オブジェクトを使用してポリシー構成を編集できます。 構成オブジェクトは、ポリシーを構成しているさまざまな部分のことです。 System i ナビゲーター で Quality of Service を開くと、クライアント、アプリケーション、スケジュール、ポリシー、サービス・クラス、PHB (ホップごとの転送優先順位付け)、および Uniform Resource Identifiers (URI) のラベルが付いたフォルダーがあります。 これらのオブジェクトを使用してポリシーを作成できます。これらのオブジェクトの詳細は、System i ナビゲーター の Quality of Service の概要のヘルプを参照してください。

QoS ポリシーを使用可能にする

ポリシーを有効にするには、その前にそのポリシーを使用可能にしなくてはなりません。ウィザードを使用すると、システムは自動的にポリシーを使用可能にします。 ただし、構成オブジェクトを使用してポリシーを変更した場合、ポリシーを活動状態にするにはシステムを動的に更新する必要があります。 ポリシーを使用可能にする前に、問題の原因となる重複ポリシーがないかを確認してください。

関連概念

54 ページの『Quality of Service の計画』
Quality of Service (QoS) を達成するための最も重要なステップは計画です。期待どおりの結果を得るためには、ネットワーク装置とモニター・ネットワーク・トラフィックを確認する必要があります。

System i Navigator 入門

関連タスク

61 ページの『QoS ポリシーの順序付け』
重複する 2 つのポリシーがある場合は、System i ナビゲーター におけるポリシーの物理的な順序が重要です。

関連資料

62 ページの『Quality of Service の管理』
以下の手順を使用して、QoS (Quality of Service) の既存のプロパティーおよびポリシーを管理することができます。

ウィザードを使用した QoS の構成

Quality of Service (QoS) ポリシーを構成するには、System i ナビゲーター にある QoS ウィザードを使用してください。

各種ウィザードとその機能について説明します。

「初期構成」ウィザード
このウィザードでは、システム固有の構成およびディレクトリー・サーバー情報をセットアップすることができます。

「新規 IntServ ポリシー」ウィザード
「新規 IntServ ポリシー」ウィザードでは、IntServ ポリシーを作成することができます。このポリシーは、ReSerVation Protocol (RSVP) 要求を承認または否認し、間接的にサーバーの帯域幅を制御します。 ポリシー・パフォーマンスの制限 (ユーザーが設定する) により、システムがクライアン

トの RSVP アプリケーションから取り入れられる要求された帯域幅を処理できるかどうかが決まります。このウィザードで作成された IntServ ポリシーを実行するには、RSVP 作動可能ルーターおよびアプリケーションが必要です。

注: IntServ ポリシーをセットアップする前に、RSVP を使用するためのユーザー自身のアプリケーションを作成する必要があります。

「新規 DiffServ ポリシー」ウィザード
このウィザードでは、TCP/IP トラフィックを差異化し、優先順位を TCP/IP トラフィックに割り当てることができます。 ポリシーを作成することでトラフィックを差異化できるようになります。ポリシー内で、ソース/宛先 IP アドレス、ポート、アプリケーション、およびクライアントに基づいて、発信トラフィックにサービス・レベルを割り当てます。 i5/OS アプリケーションはさらに具体的なアプリケーション情報に基づいたサービス・レベルを受け取ることができます。

「新規サービス・クラス」ウィザード
ネットワーク内のルーターおよびスイッチで使用されるパケット・マーク付けを設定するには、この「サービス・クラス」ウィザードを利用します。 このウィザードでは、ネットワークを出るトラフィックにパフォーマンス制限も割り当てます。サービス・クラスは、DiffServ ポリシーおよびインバウンド許可ポリシーと共に使用します。

「新規インバウンド許可ポリシー」ウィザード
「インバウンド許可」ウィザードを使用して、システムに対して行われる接続を制限します。アクセスは、TCP/IP アドレス、アプリケーション、ローカル・インターフェース、または Uniform Resource Identifier (URI) により制限することができます。これにより、システム管理者は、特定のクライアント、特定のシステム・アプリケーションからサーバーへのアクセスを制御することができます。 さらに、システムのパフォーマンスを向上させることができます。

注: URI を使用するインバウンド・ポリシーをセットアップする前に、URI に割り当てるアプリケーション・ポートを、Apache Web サーバー構成で Fast Response Cache Accelerator (FRCA) 用に使用可能になっている Listen ディレクティブに一致させる必要があります。

作成するポリシーのタイプを決めた後で、上記の適切なウィザードでポリシーを構成することができます。

System i ナビゲーター 内での QoS ウィザードへのアクセス

以下の手順に従って、QoS ウィザードにアクセスし、System i ナビゲーター 内でポリシーを作成することができます。

QoS ウィザードにアクセスし、新規ポリシーを作成するには、次の手順に従ってください。

1. System i ナビゲーター で、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**IP ポリシー**」の順に展開します。
2. 「**Quality of Service**」を右マウス・ボタンでクリックし、「**構成**」をクリックします。

   注: 以下の場合には、初期構成ウィザードが表示されます。
   - これが、このシステムで初めて QoS グラフィカル・ユーザー・インターフェース (GUI) を使用しようとしている場合。
   - 以前の構成情報を手動で除去し、やり直したい場合。これは QoS インターフェースが既にオープンされている場合にのみ生じます。
3. 初期構成ウィザードの手順を完了させます。初期構成ウィザードが表示されない場合は、ステップ 4 に進みます。

4. 「**ポリシー**」を選択します。「**IntServ**」、「**DiffServ**」、または「**インバウンド許可ポリシー**」を右マウス・ボタンでクリックします。
5. 「**新規ポリシー (New Policy)**」を選択します。

関連概念

18 ページの『Quality of Service API』
このトピックには、プロトコルと API に関する情報、および ReSerVation Protocol (RSVP) で使用可能なルーターに関する要件が記載されています。Quality of Service (QoS) API には、RAPI API、qtoq ソケット API、sendmsg() API、およびモニター API が含まれています。

2 ページの『DiffServ』
これは、オペレーティング・システムで作成できるアウトバウンド帯域幅ポリシーの第 1 のタイプです。DiffServ はトラフィックをクラスに分割します。 DiffServ ポリシーをインプリメントするには、ネットワーク・トラフィックの分類方法とさまざまなクラスの処理方法を決定する必要があります。

関連情報

ご使用の HTTP サーバー (Apache 付き) のアドレスおよびポートの管理

ディレクトリー・サーバーの構成

Quality of Service (QoS) ポリシー構成は、QoS ソリューションを簡単に管理できるように Lightweight Directory Access Protocol (LDAP) ディレクトリー・サーバーにエクスポートすることができます。

すべてのシステムで QoS ポリシーを構成する代わりに、1 つのローカル・ディレクトリー・サーバーで構成データを保管して、たくさんのシステムで共用することができます。 システム上に QoS を最初に構成するときに、初期構成ウィザードが開きます。このウィザードは、ディレクトリー・サーバーを構成するようにプロンプトを出します。

ディレクトリー・サーバーを構成するためには、下記の情報を決定するかまたは認識しておく必要があります。

- ディレクトリー・サーバー名を認識する。
- QoS ポリシーを参照するための識別名 (DN) を決定する。
- LDAP ディレクトリー・サーバーで Secure Sockets Layer (SSL) セキュリティーを使用するかどうかを決定する。
- ディレクトリー・サーバー上でのポリシーの検索を改善するためにキーワードを使用するかどうかを決定する。

注: 現在、QoS サーバーがディレクトリーにアクセスするために使用する認証方式として、Kerberos を構成することはできません。

LDAP ディレクトリー・サーバーを管理するには、下記のいずれかの権限セットを保持する必要があります。

- *ALLOBJ 権限と *IOSYSCFG 権限
- *JOBCTL 権限と TCP/IP 終了 (ENDTCP)、TCP/IP 開始 (STRTCP)、TCP/IP サーバー開始 (STRTCPSVR)、TCP/IP サーバー終了 (ENDTCPSVR) の各コマンドに対するオブジェクト権限
- i5/OS セキュリティー監査を構成するための *AUDIT 権限

System i ナビゲーターを使用している場合は、デフォルトの QoS スキーマにアクセスできます。 実際のスキーマ・ファイルはシステムの `/QIBM/UserData/OS400/DirSrv` にあります。ただし、System i ナビゲーター 以外のエディターを使用している場合は、次のセクションで説明する LDAP データ交換形式 (LDIF)

ファイルをインポートする必要があります。編集後に、元のデフォルト・ファイルを再ロードしたい場合にも、LDIF ファイルをインポートすることができます。

QoS スキーマ

スキーマ と呼ばれる規則セットは、どのタイプの LDAP オブジェクトが QoS サーバーに対して有効であるかを指定するためのものです。 スキーマには、QoS に必要な規則が含まれています。使用する LDAP サーバーが System i プラットフォームでない場合は、これらの規則を LDAP サーバーにインポートする必要があります。 このインポートは LDAP データ交換形式 (LDIF) ファイルを使用して行われます。 LDAP Web ページを使用して、LDIF ファイルをダウンロードします。 このファイルを見つけるには、左側のペインで「**Categories**」 → 「**TCP/IP Policies**」の順に展開します。

関連概念

28 ページの『ディレクトリー・サーバー』
ポリシーをディレクトリー・サーバーにエクスポートすることができます。 Lightweight Directory Access Protocol (LDAP) の概念と構成、および QoS (Quality of Service) スキーマについて調べるには、このトピックをお読みください。

30 ページの『識別名』
ディレクトリーの一部を管理する場合、識別名 (DN) またはキーワード (選択した場合) を参照します。

IBM Tivoli Directory Server for i5/OS (LDAP)

ディレクトリー・サーバーでの SSL およびトランスポート層セキュリティーの使用可能化

29 ページの『キーワード』
ディレクトリー・サーバーを構成する場合、キーワードを各 Quality of Service (QoS) 構成に関連付けるかどうかを決める必要があります。

関連情報

IBM LDAP ディレクトリー・スキーマ

QoS ポリシーの順序付け

重複する 2 つのポリシーがある場合は、System i ナビゲーター におけるポリシーの物理的な順序が重要です。

重複ポリシーとは、同じクライアント、アプリケーション、スケジュール、ローカル IP アドレス、Uniform Resource Identifier (URI)、サーバー・データ、コード・ポイント、またはプロトコルを使用する 2 つのポリシーです。 ポリシーは、System i ナビゲーター 画面で順序付きリスト形式で表示されます。 ポリシーの優先順位は、このリストのポリシーの順序に依存します。あるポリシーの優先順位を別のポリシーより高くしたい場合、その優先順位が高い方のポリシーがリストでは先に表示されなくてはなりません。

あるポリシーが別のポリシーと重複しているかどうかを判断するには、次の手順に従ってください。

1. System i ナビゲーター で、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**IP ポリシー**」の順に展開します。
2. 「**Quality of Service**」を右マウス・ボタンでクリックします。
3. 「**構成**」を選択します。
4. 「**特定のポリシー**」フォルダーを選択します。
5. 関連した重複ポリシーがあるポリシーの名前を右マウス・ボタンでクリックします。重複したポリシーの場合、重複を示すアイコンが前にあります。

6. 「**オーバーラップの表示**」を選択します。「オーバーラップするポリシー」ウィンドウが開きます。

パネル上のポリシー順序の変更は、次の方法で行います。

- ポリシーを強調表示して、ウィンドウの上矢印および下矢印を使用してポリシー順序を変更します。
- ポリシー名を右マウス・ボタン・クリックし、「**上に移動**」または「**下に移動**」を選択します。
- Quality of Service (QoS) サーバーを更新します。ツールバーの「**サーバー更新**」ボタンを使用するか、または詳細について『QoS ヘルプ』を参照してください。

関連概念

58 ページの『Quality of Service の構成』
QoS (Quality of Service) の計画を立てた後で、System i ナビゲーター のウィザードを使用して QoS ポリシーを作成します。このトピックでは、DiffServ ポリシー、IntServ ポリシー、およびインバウンド許可ポリシーの作成方法を説明します。

63 ページの『既存ポリシーのコピー』
スクラッチからすべてのポリシーを作成するのではなく、元のポリシーのコピーを作成し、元のポリシーとは異なるポリシーのセクションを編集することもできます。

69 ページの『Quality of Service のトラブルシューティング』
QoS (Quality of Service) は、QoS に関する問題のトラブルシューティングを行ういくつかの方法を提供します。

関連タスク

『System i ナビゲーター での QoS ヘルプへのアクセス』
System i ナビゲーター を使用して、QoS (Quality of Service) ヘルプにアクセスできます。

Quality of Service の管理

以下の手順を使用して、QoS (Quality of Service) の既存のプロパティーおよびポリシーを管理することができます。

ポリシーの編集、使用可能化、表示、およびその他のポリシー管理技法を使用するための実際のタスク、さらに、システムを通過する IP トラフィックの分析に役立つ QoS モニターおよびデータ収集機能の使用方法の説明があります。

関連概念

58 ページの『Quality of Service の構成』
QoS (Quality of Service) の計画を立てた後で、System i ナビゲーター のウィザードを使用して QoS ポリシーを作成します。このトピックでは、DiffServ ポリシー、IntServ ポリシー、およびインバウンド許可ポリシーの作成方法を説明します。

System i ナビゲーター での QoS ヘルプへのアクセス

System i ナビゲーター を使用して、QoS (Quality of Service) ヘルプにアクセスできます。

1. System i ナビゲーター で、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**IP ポリシー**」の順に展開します。
2. 「**Quality of Service**」を右マウス・ボタンでクリックし、「**構成**」をクリックします。
3. メニュー・バーで「**ヘルプ**」 → 「**ヘルプ・トピック**」をクリックします。 画面にタスク・ヘルプ・ウィンドウが表示されます。

関連タスク

61 ページの『QoS ポリシーの順序付け』
重複する 2 つのポリシーがある場合は、System i ナビゲーター におけるポリシーの物理的な順序が重要です。

QoS ポリシーのバックアップ

システム障害または電力損失の場合にポリシーを再作成する必要が生じないようにするために QoS (Quality of Service) ポリシーをバックアップする必要があります。

ポリシーはローカルに保管することができます。また、ディレクトリー・サーバーにエクスポートすることもできます。特に、統合ファイル・システム・ディレクトリー QIBM/UserData/OS400/QOS/ETC、QIBM/UserData/OS400/QOS/TEMP、および QIBM/UserData/OS400/QOS/USR のバックアップをとってください。 QoS サーバーに関するディレクトリー・サーバー公表エージェントのバックアップもとる必要があります。この公表エージェントには、ディレクトリー・サーバー名、QoS サーバーの識別名 (DN)、ディレクトリー・サーバーへのアクセスに使用されるポート、および認証情報が含まれています。ファイルが破損した場合、バックアップがあれば、最初からポリシーを再作成するのに要する時間と作業が省略できます。破損ファイルの置き換えに簡単に利用できる、一般的なヒントを次に示します。

1. **統合ファイル・システムのバックアップおよび回復プログラムを利用する。**

   「*バックアップおよび回復*」ブックには、統合ファイル・システムからのバックアップの実施についての説明があります。
2. **ポリシーを印刷しておく。**

   印刷出力を、最も安全だと考えられる場所に保管し、必要に応じてその情報を再入力します。
3. **情報をディスクにコピーする。**

   コピーは、情報が電子的に存在するという点で、手作業で情報を再入力しなければならない印刷出力よりも利点があります。コピーは、1 つのオンライン・ソースから別のオンライン・ソースに情報をトランスポートする直接的な手段です。

注: システムは、情報をディスケットではなくシステム・ディスクにコピーします。 ルール・ファイルは、QIBM/UserData/OS400/QOS/ETC の中、ならびにユーザーが構成したディレクトリー・サーバーの識別名の中にあります (PC 上ではない)。 システム・ディスクに保管されているデータを保護するためのバックアップ手段として、ディスク保護という方法を使用できます。

System i 製品を使用する場合、バックアップおよび回復の方針を計画する必要があります。

関連情報

システムのバックアップ

既存ポリシーのコピー

スクラッチからすべてのポリシーを作成するのではなく、元のポリシーのコピーを作成し、元のポリシーとは異なるポリシーのセクションを編集することもできます。

System i ナビゲーターでは、この QoS (Quality of Service) 機能は *New based on (既存のものを基にした新規作成)* と呼ばれます。 ポリシーのコピーを行うことができる QoS ウィンドウにアクセスするには、System i ナビゲーター を使用する必要があります。

既存ポリシーのコピーを作成するには、System i ナビゲーター ヘルプの「**既存ポリシーを基にしたポリシーの作成**」の中の手順に従ってください。

ポリシーを有効にするには、その前に、QoS サーバーを始動するかまたはサーバーの動的更新を実行して、そのポリシーを使用可能にする必要があります。ポリシーを使用可能にする前に、問題の原因となる重複ポリシーがないかを確認してください。

関連タスク

61 ページの『QoS ポリシーの順序付け』
重複する 2 つのポリシーがある場合は、System i ナビゲーター におけるポリシーの物理的な順序が重要です。

QoS ポリシーの編集

ニーズの変更に伴い、引き続き適切なパフォーマンスを得られるようにポリシーを編集する必要があります。

活動化の前に、エラーは訂正し、ポリシーに必要な変更を加えてください。予期しないポリシー結果を生み出さないようにするには、これが最善の方法です。

ポリシーを構成した後は、System i ナビゲーター の構成オブジェクトを使用してポリシー構成を編集できます。 構成オブジェクトは、ポリシーを構成しているさまざまな部分のことです。 System i ナビゲーター で Quality of Service を開くと、クライアント、アプリケーション、スケジュール、ポリシー、サービス・クラス、PHB (ホップごとの転送優先順位付け)、および Uniform Resource Identifier (URI) のラベルが付いたフォルダーがあります。 これらのオブジェクトを使用してポリシーを編集できます。

System i ナビゲーター でポリシーを編集するには、System i ナビゲーター のヘルプの「Quality of Service (QoS) ポリシーの編集」内の手順に従ってください。

QoS のモニター

Quality of Service (QoS) モニターを利用して、システムで IP トラフィックを分析できます。

QoS モニターは、ネットワーク内のどこで輻輳 (ふくそう) が発生しているかを判断するのに役立ちます。QoS の計画時に役立つだけでなく、トラブルシューティング・ツールとして役立てることができます。QoS モニターを使用することで、必要に応じてポリシーを調整できるようにネットワークをモニターし続けることができます。 すべてのアクティブ・ポリシーをモニターするには、「QoS サーバー構成」ウィンドウから「**サーバー**」 → 「**モニター**」を選択します。単一のポリシーを右マウス・ボタンでクリックし、「**モニター**」を選択すると、モニターはその 1 つのポリシーの情報のみを表示します。

モニター・ポリシーは次のように使用することができます。

- **アクティブ・ポリシーのリアルタイム・データを表示するには**

  モニターをオープンすると、常にアクティブ・ポリシーに関するリアルタイム・データが表示されます。データ収集を開始する必要はありません。

- **一定期間のデータを収集して保管するには**

  モニター結果を保管するには、QoS データ収集を開始する必要があります。モニターは、ユーザーが収集を停止するまで、データの収集を続けます。 モニター・ウィンドウを閉じても、データ収集は停止しません。また、データ収集中にモニターが使用するプロパティーを変更することもできます。「QoS モニター」ウィンドウで、「**QoS モニター**」を強調表示し、「**ファイル**」**-->**「**プロパティー**」を選択して、オプションを変更します。 詳しくはオンライン・ヘルプを参照してください。

  QoS データ収集をオンにし、モニター・プロパティーを変更する場合は、以下のステップを実行して、変更内容がデータ収集に確実に反映されたことを確認する必要があります。

1. QoS データ収集を停止します。
2. モニター・プロパティーを変更します。
   a. 「モニター」ウィンドウで、「**QoS モニター**」をクリックします。
   b. 「**ファイル**」 → 「**プロパティー**」を選択します。
   c. モニター・プロパティーを変更し、「**OK**」をクリックします。
3. QoS サーバーを更新します。
4. QoS データ収集を開始します。

モニター出力

受け取る出力情報は、モニターしているポリシーのタイプによって異なります。 ポリシー・タイプには、DiffServ、IntServ (負荷制御サービス)、IntServ (保証サービス)、およびインバウンド許可があります。評価するフィールドは、このポリシー・タイプに依存します。最も注意するべき値は、測定値です。次のフィールドは、与えられた定義ではなく測定された値です。すなわち、受け入れられた要求、アクティブ接続、接続サービス、接続率、廃棄された要求、プロファイル中のパケット数、プロファイル中のビット数、プロファイル外ビット数、合計ビット数、合計パケット数、および合計要求数です。

上記の測定フィールドの情報を確認することで、ネットワーク・トラフィックがどのくらいポリシーに合致しているかということがわかります。ポリシー・タイプごとのモニター出力フィールドの詳細については、以下の説明を参照してください。 QoS ポリシーと共にモニターを使用する方法の例については、『QoS のシナリオ』のいずれかの例を参照してください。

DiffServ ポリシー

表 4. DiffServ ポリシー

フィールド	説明
ポリシー名	このポリシーに割り当てた名前。
プロトコル	UDP、TCP、ALL。
平均トークン速度限界	フロー・パスに存在する各ルーターおよびシステムにおいて、このポリシーが許可する平均トークン速度。
トークンの深さ限界	フロー・パスに存在する各ルーターおよびシステムにおいて、このポリシーが許可する最大トークン・バッファー・サイズ。
ピーク・トークン速度限界	この接続で許可される最大速度。
プロファイル中のパケット数	このポリシーのパラメーター値内に収まる、送信 IP パケット数。
プロファイル中のビット数	このポリシーのパラメーター値内に収まる、送信ビット数。
プロファイル外ビット数	このポリシーのパラメーター値を超えた、送信ビット数。
ビット・レート	この接続で許可されるビットの測定数値。
アクティブ接続	アクティブな接続の合計数。

表 4. DiffServ ポリシー (続き)

フィールド	説明
トラフィック・プロファイル	アウト・オブ・プロファイル・パケットに使用されるパケット調整のタイプ。フォーマットでは、次の調整方法を指定できます。 • 再マーク付け • シェイピング • 廃棄
合計ビット数	このポリシーが始動されてからモニター収集までの間に、ポリシーによって使用された送信ビット数。
プロファイル中のコード・ポイント	パケットに新規のコード・ポイントが付いていて、IP パケットがこのポリシーのパラメーター値内に収まっている場合、それらの IP パケットはこのコード・ポイントを使用します。
プロファイル外コード・ポイント	パケットに新規のコード・ポイントが付いているが、IP パケットがポリシーのパラメーター値を超えている場合、それらの IP パケットはこのコード・ポイントを使用します。
宛先アドレス範囲 (Destination address range)	パケットの (このポリシーによって制御される) 宛先ポイントを判断するアドレス範囲。
合計パケット数	このポリシーが始動されてからモニター収集までの間に、ポリシーによって送信されたパケット数。
送信元ポート範囲 (Source port range)	このポリシーによって制御されるアプリケーションを判別する、送信元ポートの範囲。

IntServ (負荷制御サービス) ポリシー

IntServ ポリシーは、アプリケーションが実行され、予約が確立されるまでモニターに表示されません。IntServ ポリシーに複数の予約がある場合は、モニターに複数の項目が表示されます。

表 5. IntServ (負荷制御サービス) ポリシー

フィールド	説明
ポリシー名	このポリシーに割り当てた名前。
プロトコル	UDP または TCP。
宛先アドレス	パケットの (このポリシーによって制御される) 宛先ポイントを判断するアドレス範囲。
平均トークン速度限界	接続パスに存在する各ルーターおよびシステムにおいて、このポリシーが許可する平均トークン速度。
トークンの深さ限界	接続パスに存在する各ルーターおよびシステムにおいて、このポリシーが許可する最大トークン・バッファー・サイズ。
ピーク・トークン速度限界	この接続で許可される最大速度。
合計パケット数	このポリシーが始動されてからモニター収集までの間に、ポリシーによって送信されたパケット数。
プロファイル外ビット数	このポリシーのパラメーター値を超えた、送信ビット数。

表 5. IntServ (負荷制御サービス) ポリシー (続き)

フィールド	説明
合計ビット数	このポリシーが始動されてからモニター収集までの間に、ポリシーによって使用された送信ビット数。
ビット・レート	この接続で許可されるビットの測定数値。
プロファイル中のビット数	このポリシーのパラメーター値内に収まる、送信ビット数。
最大パケット・サイズ (Maximum packet size)	このポリシーによって制御される最大許容パケット・サイズ。
最小ポリス単位 (Minimum policed unit)	トークン・バケットから除去される最小ビット数。例えば、最小ポリス単位が 100 ビットの場合、100 ビット未満パケットも 100 ビットとして除去されます。
プロファイル中のパケット数	このポリシーのパラメーター値内に収まる、送信 IP パケット数。
送信元ポート範囲 (Source port range)	このポリシーによって制御されるアプリケーションを判別する、送信元ポートの範囲。

IntServ (保証) ポリシー

IntServ ポリシーは、アプリケーションが実行され、予約が確立されるまでモニターに表示されません。IntServ ポリシーに複数の予約がある場合は、モニターに複数の項目が表示されます。

表 6. IntServ (保証) ポリシー

フィールド	説明
ポリシー名	このポリシーに割り当てた名前。
プロトコル	UDP または TCP。
宛先アドレス	パケットの (このポリシーによって制御される) 宛先ポイントを判断するアドレス範囲。
平均トークン速度限界	接続パスに存在する各ルーターおよびシステムにおいて、このポリシーが許可する最大トークン速度。
トークンの深さ限界	接続パスに存在する各ルーターおよびシステムにおいて、このポリシーが許可する最大トークン・バッファー・サイズ。
ピーク・トークン速度限界	この接続で許可される最大速度。
合計パケット数	このポリシーが始動されてからモニター収集までの間に、ポリシーによって送信されたパケット数。
合計ビット数	このポリシーが始動されてからモニター収集までの間に、ポリシーによって使用された送信ビット数。
プロファイル外ビット数	このポリシーのパラメーター値を超えた、送信ビット数。
保証済み速度	保証された速度 (ビット/秒)。
プロファイル中のビット数	このポリシーのパラメーター値内に収まる、送信ビット数。
最大パケット・サイズ (Maximum packet size)	このポリシーによって制御される最大許容パケット・サイズ。

表 6. IntServ (保証) ポリシー (続き)

フィールド	説明
最小ポリス単位 (Minimum policed units)	トークン・バケットから除去される最小ビット数。例えば、最小ポリス単位が 100 ビットの場合、100 ビット未満パケットも 100 ビットとして除去されます。
プロファイル中のパケット数	このポリシーのパラメーター値内に収まる、送信 IP パケット数。
遊び期間 (Slack term)	必要な遅延と実際の遅延の差 (秒)。
送信元ポート範囲 (Source port range)	このポリシーによって制御されるアプリケーションを判別する、送信元ポートの範囲。

インバウンド許可ポリシー

表 7. インバウンド許可ポリシー

フィールド	説明
ポリシー名	このポリシーに割り当てた名前。
接続率	受け入れられる接続要求数 (毎秒)。
合計要求数	このシステムに対して行われる接続要求の合計数。
受け入れられた要求数	このシステムが受け入れた接続要求の合計数。
廃棄された要求数	このシステムによって廃棄された接続要求の合計数。
平均接続率限界 (Average connection rate limit)	許可される新規接続要求の平均許容数 (毎秒)。
接続バースト限界	並行して受け入れられた新規接続要求の最大数。
ピーク接続率限界	システムがネットワークからの接続を受け入れる最大許容速度。
優先順位	QoS マネージャーにロードされる各規則に割り当てられる優先順位。
待ち行列優先順位	listen 待ち行列に入れられる着信接続に割り当てられる優先順位。
宛先ポート範囲 (Destination port range)	システム上でトラフィックの宛先となるポート範囲またはポート。
インターフェース・アドレス (Interface address)	モニターされるシステム・インターフェースの IP アドレス。
送信元アドレス範囲 (Source address range)	システムに要求を送信するクライアントの IP アドレス範囲。
URI (Uniform Resource Identifier)	ポリシングされる URI の ID。

関連概念

31 ページの『シナリオ: ブラウザー・トラフィックの制限』
QoS (Quality of Service) を使用して、トラフィック・パフォーマンスを制御することができます。 ネットワーク内でのアプリケーションのパフォーマンスを制限または拡張するには、DiffServ ポリシーを使用します。

36 ページの『シナリオ: 安全で予測可能な結果 (VPN と QoS)』
VPN (仮想プライベート・ネットワーク) を使用している場合でも、Quality of Service (QoS) ポリシーを作成できます。

40 ページの『シナリオ: インバウンド接続の制限』
ユーザーのシステムに対してなされるインバウンド接続要求を制御する必要がある場合には、インバウンド許可ポリシーを使用します。

44 ページの『シナリオ: 予測可能な B2B トラフィック』
予測可能な送達が必要で、引き続き予約を要求したい場合は、IntServ ポリシーも使用します。 この例では、負荷制御サービスを使用します。

48 ページの『シナリオ: 専用送達 (IP テレフォニー)』
専用送達が必要で、予約を要求したい場合は、IntServ ポリシーを使用します。作成する IntServ ポリシーには、2 つのタイプ (保証サービスと負荷制御サービス) があります。 この例では、保証サービスが使用されています。

31 ページの『シナリオ: Quality of Service ポリシー』
以下の QoS (Quality of Service) ポリシー・シナリオは、QoS が必要な理由およびポリシーとサービス・クラスの作成方法を理解するのに役立ちます。

72 ページの『システム・トランザクションのモニター』
QoS (Quality of Service) モニターを使用して、QoS ポリシーが意図したとおりに機能しているか確認することができます。QoS モニターは、QoS の計画フェーズとトラブルシューティング・フェーズで役に立ちます。

52 ページの『シナリオ: 現在のネットワーク統計のモニター』
ウィザードの中で、個々のネットワーク要件に基づくパフォーマンス制限を設定する必要があります。

Quality of Service のトラブルシューティング

QoS (Quality of Service) は、QoS に関する問題のトラブルシューティングを行ういくつかの方法を提供します。

通信トレース

システムからは、ローカル・エリア・ネットワーク (LAN) または広域ネットワーク (WAN) インターフェースなどの通信回線上のデータを収集するための通信トレースが提供されます。 ユーザーは、一般的にトレース・データの内容全体を理解していない場合があります。 しかし、本書の読者であれば、トレース項目から 2 つの地点間のデータ交換が実際に行われたかどうかを判断できます。

システムでの QoS の使用可能化

QoS サーバーが始動しない場合、最初に、QoS がシステム上で使用可能であるかどうかを調べます。初めてポリシーを構成する場合は、初期構成ウィザードがシステム上の QoS を自動的に使用可能にします。ただし、この値が何らかの理由で変更された場合は、サーバーは始動しません。

QoS がシステム上で使用可能であるかどうか調べるには、次のステップを実行します。

1. System i ナビゲーター で、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**IP ポリシー**」の順に展開します。
2. 「**Quality of Service**」を右マウス・ボタンでクリックし、「**構成**」を選択します。
3. QoS インターフェースが表示されたら、「**QoS**」を右マウス・ボタンでクリックし、「**プロパティー**」を選択します。
4. 「QoS プロパティー (QoS properties)」ページで、「**QoS の使用可能化 (Enable QoS)**」を選択します。

関連概念

通信トレース

関連タスク

61 ページの『QoS ポリシーの順序付け』
重複する 2 つのポリシーがある場合は、System i ナビゲーター におけるポリシーの物理的な順序が重要です。

QoS ポリシーのジャーナル処理

Quality of Service (QoS) にはジャーナル処理機能が組み込まれています。 ジャーナル処理機能を利用して、ポリシーが追加、除去、または変更された場合に QoS ポリシーのアクションを追跡できます。

ジャーナル処理機能をオンに設定している場合、ポリシー・アクションのログが作成されます。このログは、ポリシーが期待どおり動作していない個所をデバッグしたりスポット・チェックするのに役立ちます。例えば、午前 9 時から午後 4 時に実行するようにポリシーを設定したとします。ジャーナル・ログをチェックして、ポリシーが実際に午前 9 時に追加され、午後 4 時に除去されたかどうか確認することができます。

ジャーナル処理がオンに設定されていると、ポリシーが追加、除去または変更されるたびにジャーナル項目が生成されます。こうしたジャーナルを使用して、システム上に一般ファイルを作成します。 これにより、システムのジャーナルに記録された情報からシステムの使用状況を判断することができます。これは、ポリシーのさまざまな局面の変更を決定する時に役立ちます。

ジャーナル処理する内容は慎重に選択してください。ジャーナル処理は、システム・リソースに多大な負担を与えます。ジャーナル処理の開始または停止には、System i ナビゲーター を使用します。 ジャーナル・ログを表示するには、文字ベースのインターフェースを使用してください。

ジャーナル処理の開始または停止は、次の手順で行ってください。

1. System i ナビゲーター で、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**IP ポリシー**」の順に展開します。
2. 「**Quality of Service**」を右マウス・ボタンでクリックし、「**構成**」を選択します。
3. 「**QoS**」を右マウス・ボタン・クリックし、「**プロパティー**」を選択します。
4. ジャーナル処理をオンにするには、「**ジャーナル処理の実行**」ボックスを選択します。
5. ジャーナル処理をオフにするには、ボックスをクリアします。

注: 上記の手順を終了する前に既にシステムが始動している場合は、システムを停止して再始動する必要があります。 ジャーナル処理をオンにしたら、2 つの方法のうちのいずれかを使用してジャーナル処理をアクティブにします。ジャーナル処理をアクティブにする方法の 1 つは、システムを停止して再始動することで、もう 1 つの方法はシステムを更新することです。 どちらかの方法を実行すると、サーバーが policy.conf ファイルの再読み取りをして、ジャーナル処理属性を探します。

モニターでのジャーナル項目の確認

このトピックには、モニターでのジャーナル項目の確認に関する情報が記載されています。

1. コマンド・プロンプトで、`DSPJRN JRN(QUSRSYS/QQOS)` コマンドを入力します。
2. 表示したいジャーナル項目に関して「オプション 5」を選択します。

出力ファイルでのジャーナル項目の確認

ジャーナル項目を 1 つのフォルダーにフォーマット設定して表示したい場合は、`QUSRSYS` ディレクトリー内の `MODEL.OUT` ファイルを見てください。ジャーナル項目を出力ファイルにコピーすれば、Query/400 や

構造化照会言語 (SQL) などの Query ユーティリティーを利用して簡単にジャーナル項目を確認できます。出力ファイル内の項目を処理する独自の高水準言語 (HLL) プログラムを作成することもできます。

Quality of Service (QoS) ジャーナル項目をシステムが提供する出力ファイルにコピーするには、次のステップを実行します。

1. ユーザー・ライブラリーの中に、システム提供の出力ファイル QSYS/QATOQQOS のコピーを作成します。このコピーは、複製オブジェクト作成 (CRTDUPOBJ) コマンドで作成できます。以下は、CRTDUPOBJ コマンドの例です。
   - CRTDUPOBJ OBJ(QADSPJR4) FROMLIB(Qsys) OBJTYPE(*FILE) TOLIB(*userlib*) NEWOBj(*userfile*)
2. ジャーナル表示 (DSPJRN) コマンドを使用して、QUSRSYS/QQOS ジャーナルから、前のステップで作成した出力ファイルに項目をコピーします。存在しない出力ファイルに DSPJRN をコピーしようとすると、システムはファイルを作成しますが、このファイルには適切なフィールド記述が含まれていません。
   - DSPJRN JRN(QUSRSYS/QQOS) JRNCDE((M)) ENTTYP(MP) CMTCYCID(*ALL) OUTPUT(*OUTFILE) OUTFILFMT(*TYPE4) OUTFILE(*userlib/userfile*)
   - DSPF FILE(*userlib/userfile*)

QoS サーバー・ジョブのロギング

Quality of Service (QoS) ポリシーに問題が生じた場合は、ジョブ・ログを分析してください。 ジョブ・ログには、エラー・メッセージおよび QoS に関連するその他の情報が入っています。

QoS ジョブ QTOQSRVR だけを、サブシステム QSYSWRK で実行することができます。 System i ナビゲーター で古い QoS サーバー・ジョブ・ログと現在の QoS サーバー・ジョブ・ログを見ることができます。

ログの表示は、次の手順で行います。

1. 「**ネットワーク**」を展開し、「**IP ポリシー**」をクリックします。
2. 「**Quality of Service**」を右マウス・ボタンでクリックします。
3. 「**診断ツール**」 → 「**QoS サーバー・ログ**」をクリックします。

ジョブに関する作業を行うウィンドウが開きます。

最も重要なジョブ名、およびそのジョブの用途の簡単な説明を、次に挙げます。

QTCP このジョブは、すべての TCP/IP インターフェースを始動する基本ジョブです。 TCP/IP に基本的な問題がある場合、通常は QTCPIP ジョブ・ログを分析してください。

QTOQSRVR
このジョブは、QoS のみのログ情報を提供する基本 QoS ジョブです。スプール・ファイルの処理 (WRKSPLF QTCP) コマンドを実行し、QTOQSRVR ログを探します。

作業用スプール・ファイルを検査してエラーを探す

スプール・ファイルを検査してエラーを探すには、下記のステップを実行してください。

1. コマンド行インターフェースで、`WRKSPLF QTCP` と入力し、Enter キーを押します。「すべてのスプール・ファイルの処理」パネルが表示されます。
2. 「ユーザー・データ」欄で、QoS サーバーに具体的に関係しているエラーを検出するために `QTOQSRVR` を探します。

3. 表示したい行で「**オプション 5**」を選択します。この情報を読み通して、問題について説明しているメッセージの ID を記録します。 例: TCP920C。
4. 「終了」キーを 2 回押してメインメニューに戻ります。
5. コマンド行インターフェースで、 WRKMSGF と入力し、Enter キーを押します。
6. 「メッセージ・ファイルの処理」パネルで、下記の情報を入力し、Enter キーを押します。

   メッセージ・ファイル: QTCPMSG
   ライブラリー: *LIBL
7. 「メッセージ・ファイルの処理」パネルで、確認したいメッセージ・ファイルを表示するために「**オプション 5**」を選択し、Enter キーを押します。
8. 「メッセージ記述表示」画面で、下記の情報を入力します。**位置指定**: *(上記の番号 3 からのメッセージ ID を入力し、Enter キーを押します。)*例: TCP920C。
9. 必要なメッセージ ID について「**オプション 5**」を選択し、Enter キーを押します。
10. 「表示するメッセージ明細の選択」画面で、 **30 (上記オプションのすべて)** を選択し、Enter キーを押します。

    メッセージの詳細記述が表示されます。

システム・トランザクションのモニター

QoS (Quality of Service) モニターを使用して、QoS ポリシーが意図したとおりに機能しているか確認することができます。QoS モニターは、QoS の計画フェーズとトラブルシューティング・フェーズで役に立ちます。

モニターを利用して、システムで IP トラフィックを分析できます。 これによって、ネットワーク内のどこで輻輳 (ふくそう) が発生しているかを判断できます。 QoS モニターを使用することで、必要に応じてポリシーを調整できるようにネットワークをモニターし続けることができます。

パフォーマンスの計画と保守

QoS のインプリメンテーションの最も難しい部分の 1 つは、ポリシーでどのようなパフォーマンス制限を設定するかの判断です。 1 つ 1 つのネットワークは異なるので、特定の勧告はありません。ご自身のポリシーにとって適切な値を判断するために、業務固有のポリシーを開始する前にモニターを使用することができます。

現在のネットワーク・トラフィックの動作を確認するためには、計量を選択しないで DiffServ ポリシーを作成してみてください。このポリシーを使用可能にして、モニターを始動します。このモニターの結果を利用して、特定のニーズに合うようにポリシーを調整することができます。現在のトラフィックの動作を確認するために『現在のネットワーク統計のモニター』を参照してください。

パフォーマンス上の問題のトラブルシューティング

問題のトラブルシューティングにもモニターを利用できます。モニター出力を利用して、ポリシーに割り当てたパラメーターが順守されているかを判断できます。ポリシーがモニターに現れるのにトラフィックをモニターしていないと思われる場合は、以下の検証を行います。

- URI を基にしたフィルター操作を行うポリシーの場合、FRCA が使用可能であり正しく構成されていることを確認します。 URI を使用するインバウンド・ポリシーをセットアップする前に、URI に割り当てるアプリケーション・ポートを、Apache Web サーバー構成で FRCA 用に使用可能になっている Listen ディレクティブに一致させる必要があります。
- ポリシー・スケジュールを検証します。非アクティブ時間内に結果を探し出せます。

- ポート番号が正しいかどうか検証します。
- IP アドレスが正しいかどうか検証します。

関連概念

54 ページの『Quality of Service の計画』
Quality of Service (QoS) を達成するための最も重要なステップは計画です。期待どおりの結果を得るためには、ネットワーク装置とモニター・ネットワーク・トラフィックを確認する必要があります。

31 ページの『シナリオ: Quality of Service ポリシー』
以下の QoS (Quality of Service) ポリシー・シナリオは、QoS が必要な理由およびポリシーとサービス・クラスの作成方法を理解するのに役立ちます。

関連資料

64 ページの『QoS のモニター』
Quality of Service (QoS) モニターを利用して、システムで IP トラフィックを分析できます。

関連情報

ご使用の HTTP サーバー (Apache 付き) のアドレスおよびポートの管理

TCP アプリケーションのトレース

トレース機能を使用する場合および現在のトレース・バッファーを表示する場合は、Quality of Service (Qos) トレースが使用できます。

システムでトレースを実行するには、コマンド行インターフェースで TRCTCPAPP (TCP/IP アプリケーションのトレース・コマンド) と入力します。

次に、トレース選択の入力例を挙げます。

```
TCP/IP 適用業務.....> *QOS
追跡オプションの設定値....> *ON
追跡用最大記憶域.....> *APP
追跡満杯処置.....> *WRAP
引数リスト.....> 'lvl=4'
QoS 追跡タイプ.....> *ALL
```

次の表は、トレースで使用可能なパラメーターを示しています。設定値が文字ベースのインターフェースに表示されない場合は、コマンドに設定値を入力する必要があります。 例えば、TRCTCPAPP APP(*QOS) MAXSTG(1000) TRCFULL(*STOPTRC) ARGLIST('l=4 c=i') と入力します。

設定	オプション
TCP/IP アプリケーション	QOS
追跡オプションの設定値	*ON、*OFF、*END、*CHK
追跡用最大記憶域	1 から 16000、*APP
追跡満杯処置 (TRCFULL)	*WRAP、*STOPTRC
引数リスト (ARGLIST)	レベル: 'lvl=1'、'lvl=2'、'lvl=3'、'lvl=4' 内容: 'c=a'、'c=i'、'c=d'、'c=m'
QoS 追跡タイプ	*ALL

追跡用最大記憶域

1-16000
トレース・データ用の最大記憶域サイズです。トレースは、このサイズに達すると停止するか、または折り返します。デフォルト・サイズは 4 MB です。 デフォルト・サイズを指定する場合は、*APP を選択します。

***APP** これはデフォルト・オプションです。アプリケーションに、デフォルトのトレース・サイズを使用するように指示します。 QoS サーバーのデフォルトのトレース・サイズは 4 MB です。

追跡満杯処置

***WRAP**
トレースが最大ディスク・スペース・サイズ (トレース・バッファー・サイズ) に達すると、トレース情報を折り返します。折り返しにより、ファイル内の最も古い情報が上書きされ、トレース情報の記録が継続されます。 折り返しを選択しない場合、ディスクが満杯になるとトレース操作は停止します。

***STOPTRC**
システムが最大ディスク・スペースに達すると、情報の収集は停止します。

引数リスト

引数リストは、ログに記録されているエラー・レベルおよび内容を指定します。TRCTCPAPP コマンドで使用できる引数は 2 つ (トレース・レベルとトレース内容) あります。トレース・レベルとトレース内容を指定する場合は、すべての属性が一組の単一引用符内に収まるようにしてください (例えば、`TRCTCPAPP 'l=4 c=a'`)。

注: ログ・レベルは包括的です。つまり、あるログ・レベルを選択すると、その前のすべてのログ・レベルも選択されます。例えば、レベル 3 を選択すると、レベル 1 とレベル 2 も自動的に選択されます。典型的なトレースでは、'l=4' を指定することをお勧めします。

トレース・レベル

レベル 1: システム・エラー (SYSERR)
システム操作において発生したエラーをログに記録します。このエラーが発生した場合、QoS サーバーの稼働を継続することはできません。例えば、システム・メモリーが不足している場合、システムが TCP/IP と通信できない場合などに、システム・エラーは発生します。これはデフォルト・レベルです。

レベル 2: オブジェクト間のエラー (OBJERR)
QoS サーバー・コード内で発生したエラーをログに記録します。例えば、あるシステム操作を実行して予期しない結果が生じた場合などに、オブジェクト・エラーが発生することがあります。これは、通常はサービスに報告しなければならない深刻な状態です。

レベル 3: 特定のイベント (EVENT)
行われたすべての QoS 操作をログに記録します。例えば、イベント・ログにはコマンドと要求が記録されます。結果は、QoS ジャーナル処理機能の結果に似ています。

レベル 4: メッセージのトレース (TRACE)
QoS サーバーとの間で転送されているすべてのデータをトレースします。例えば、問題のデバッグに役立つと思われるあらゆる情報のロギングに、このハイレベル・トレースを利用できます。このトレースの情報は、問題の発生個所および問題の再現方法を判断する時に役立ちます。

トレース内容

内容タイプを 1 つだけ指定してください。トレースする内容を指定しないと、(デフォルトにより) すべての内容がトレースされます。

Content = All ('c=a')
QoS サーバーの全機能をトレースします。これはデフォルト値です。

Content = Intserv ('c=i')
IntServ 操作のみをトレースします。問題が IntServ に関連していると判断した場合に、この内容タイプを使用します。

Content = Diffserv ('c=d')
DiffServ 操作のみをトレースします。問題が DiffServ に関連していると判断した場合に、この内容タイプを使用します。

Content = Monitor ('c=m')
モニター操作のみをトレースします。

トレース出力の解釈の際にヘルプが必要な場合は、トレース出力ページに関するトレース出力例をお読みください。トレース出力ページには、出力の意味の解釈に役立つ注記付きの出力例が含まれています。TRCTCPAPP 機能は、通常、保守サービスで使用します。出力の読み方に問題がある場合は、サービス技術員にお問い合わせください。

関連資料

TCP/IP アプリケーションのトレース (TRCTCPAPP)

例: トレース出力の読み方

ここでは、トレース出力の解読方法のすべてを説明しているわけではありませんが、トレース情報の中で検出する必要のある重要なキー・イベントを取り上げて説明します。

IntServ ポリシーの場合、留意する必要のある最も重要なイベントは、ReSerVation Protocol (RSVP) 接続が拒否された原因は、その接続に関するポリシーが見つからなかったことかどうか、ということです。 次に、正常に接続した場合のメッセージの例を挙げます。

```
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]
```

IntServ の接続が失敗した場合のメッセージの例を、次に示します。

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

DiffServ ポリシーの場合、最も重要なメッセージは、サーバーがポリシー規則をロードしたかどうか、もしくはポリシー構成ファイルでエラーが発生したかどうかを示しているメッセージです。

例:

```
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
```

ポリシー構成ファイル内のタグが間違っていることを示すメッセージが戻される場合もあります。以下にメッセージの例を挙げます。

```
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.
```

注: % 符号は、認識されないタグを表す変数です。

Quality of Service の関連情報

Quality of Service の Request For Comments、IBM Redbooks 資料、およびその他の Information Center トピック・コレクションには、Quality of Service トピック・コレクションに関連する情報が記載されています。以下の PDF ファイルのいずれも表示または印刷できます。

Quality of Service の Request For Comments

コメント要求 (RFC) とは、インターネットに使用されるプロトコル規格および提案規格の書面による定義です。次の RFC は、QoS および関連機能を理解するのに役立ちます。

- **RFC 1349.**

  この RFC は、IP パケット・ヘッダー内の TOS オクテット・フィールドの新規定義について説明しています。

- **RFC 2205.**

  この RFC は、ReSerVation Protocol (RSVP) の定義に関するものです。

- **RFC 2210.**

  この RFC は、Internet Engineering Task Force (IETF) IntServ における RSVP の使用に関するものです。

- **RFC 2474.**

  この RFC は、DiffServ フィールドの定義に関するものです。

- **RFC 2475.**

  この RFC は、DiffServ のアーキテクチャーに関するものです。

上記の RFC を表示するには、RFC Editor Web サイトにある RFC Index Search Engine にアクセスしてください。

IBM Redbooks

- IBM i5/OS IP Networks: Dynamic 。これには、自己構成、フォールト・トレラント、効率的に運用される IP ネットワークを設計する方法が示されています。他の多くの機能のほか、QoS の背後にある理論と、システムにおける実装について説明しています。 また、段階的な指示のあるシナリオが記載されています。

- V4 TCP/IP for AS/400®: More Cool Things Than Ever  。この資料には、構成例を用いて一般的なソリューションを具体的に説明するサンプル・シナリオが記載されています。この資料の中の情報は、システム上の TCP/IP の計画、インストール、調整、構成、およびトラブルシューティングに役立ちます。 この資料ではまだ QoS について具体的に取り上げてはいませんが、LDAP ディレクトリー・サーバーについて詳しく説明しています。

- TCP/IP Tutorial and Technical Overview  。この資料には、プロトコルおよびアプリケーションの一連の TCP/IP プロトコルの概要ならびに参照するものを示してあります。『*Part 3. Advanced concepts and new technologies*』の第 22 章にて QoS について説明しています。

その他の情報

- IBM Tivoli® Directory Server for i5/OS (LDAP)。 このトピックでは、ディレクトリー・サーバーの基本概念、構成、管理、およびトラブルシューティングについて説明しています。また、このトピックには、ディレクトリー・サーバーを構成するための追加のリソースも記載されています。
- 侵入検知。このトピックでは、TCP/IP ネットワークを介して入ってくる無許可のアクセス試行およびアタックに関する情報の収集について説明しています。セキュリティー管理者は、この種のアタックから i5/OS ネットワークを保護するために侵入検知機能が提供する監査レコードを分析することができます。

関連資料

1 ページの『Quality of Service の PDF ファイル』
本書の PDF ファイルを表示および印刷することができます。

付録. 特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒106-8711
東京都港区六本木 3-2-12
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

以下の保証は、国または地域の法律に沿わない場合は、適用されません。IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

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

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、IBM 機械コードのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。 IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物にも、次のように、著作権表示を入れていただく必要があります。

© (お客様の会社名) (西暦年). このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。 © Copyright IBM Corp. _年を入れる_. All rights reserved.

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

プログラミング・インターフェース情報

本書 (「ネットワーキング QoS (Quality of Service)」) には、プログラムを作成するユーザーが IBM i5/OS のサービスを使用するためのプログラミング・インターフェースが記述されています。

商標

以下は、International Business Machines Corporation の米国およびその他の国における商標です。

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

Adobe、Adobe ロゴ、PostScript、PostScript ロゴは、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

他の会社名、製品名およびサービス名等はそれぞれ各社の商標です。

使用条件

これらの資料は、以下の条件に同意していただける場合に限りご使用いただけます。

個人使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することはできません。

商業的使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。 ただし、IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態で提供され、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。

Printed in Japan

日本アイ・ビー・エム株式会社
〒106-8711　東京都港区六本木3-2-12