CA Application Delivery Analysis

ユーザ ガイド

10.1

ca technologies

CA Technologies 製品リファレンス

このマニュアルが参照している CA Technologies の製品は以下のとおりです。

- CA Application Delivery Analysis
- CA GigaStor
- CA GigaStor コネクタ
- CA Multi-Port Monitor
- CA Performance Center
- CA NetQoS Performance Center
- CA Standard Monitor
- CA Virtual Systems Monitor

CA への連絡先

テクニカル サポートの詳細については、弊社テクニカル サポートの Web サイト（http://www.ca.com/jp/support/）をご覧ください。

目次

第 1 章: Application Delivery Analysis へようこそ

このセクションには、以下のトピックが含まれています。

はじめに

CA Application Delivery Analysis は、CA Performance Center（CA PC）および CA NetQoS Performance Center （CA NPC）内のエンド ツー エンドのパフォーマンス監視モジュールで、デスクトップまたはサーバのエージェントなしでアプリケーション レスポンス時間を追跡および測定します。 エンド ツーエンド パフォーマンス監視により、以下を行うことができます。

- ネットワークがエンド ユーザに提供しているサービスの品質を測定できます。
- ネットワーク上で発生しているすべての現象の最もわかりやすい全体像を把握できます。

CA Application Delivery Analysis は、ネットワークからデータ センターに送信され、再びデータ センターから送信される TCP アプリケーション パケットを監視し、ネットワーク ラウンドトリップ時間、サーバ レスポンス時間、データ転送時間およびその他多数のデータを測定することができます。

管理コンソール はアプリケーション、ネットワークおよびサーバ遅延コンポーネントにレスポンス時間を分け、すばやくネットワーク パフォーマンスのボトルネックをトラブルシューティングしてアプリケーションのパフォーマンスを維持することを可能にします。 自動プロセスは、すべての TCP/IP ユーザ トランザクションのアプリケーション パフォーマンスを測定し、分析します。 次に、このプロセスは、しきい値とレスポンス時間を比較し、問題を発生と同時に自動的に調査します。［ネットワーク］グループと［操作］グループには、すばやくパフォーマンスの問題を解決するための重要な診断データが表示されるようになりました。

また、正式の OLA（運用レベル契約）が取り交わされていなくても、CA Application Delivery Analysis は、内部ユーザと外部サービス プロバイダに一貫するサービス品質メトリック セットを取得できるように、可用性およびアプリケーション パフォーマンスを監視します。

パフォーマンスの測定

エンドツーエンド パフォーマンスを監視するために、管理コンソール は以下を使用します。

- ベースラインまたは平均。これは 管理コンソール によって計算され、ネットワークの過去の標準的なパフォーマンスを参照できるようにします。 ベースラインは、特定期間のアプリケーションとサーバの組み合わせのパフォーマンスを過去のパフォーマンスの平均と比較するために使用します。 ベースラインを超えた場合でも、問題が発生しているとは限りません。
- *しきい値*。これは、パフォーマンスが受け入れ可能な限界を超えたことを 管理コンソール に通知します。 管理コンソール のデフォルトしきい値は、管理コンソール 管理者がパーセンタイル ベースの値（感度ファクタ）またはミリ秒値に調整できます。 パフォーマンスしきい値を超えると、管理コンソール がインシデントを作成します。 管理コンソール 管理者は、アクションとインシデント レスポンスの通知を作成して、問題の原因を識別できるようにします。

しきい値とベースラインを比較することによって、しきい値と過去の加重平均を比較し、キャパシティ計画にこの情報を使用することができます。管理コンソール は、しきい値を使用して、データを評価します。 しきい値違反は、既存の問題があるか、新しい問題が潜んでいることを示します。

ベースライン

ベースラインは過去のパフォーマンスの標準です。 管理コンソール は自動的に 1 時間ごとのベースラインを計算し、1 日の各時間、曜日および日付の各期間中、1 時間ごとのベースラインを調整します。 ベースラインがシステムの変更に正しく適合するように、先週のアクティビティに対して最も重い重みが加えられます。 これらのベースラインは、業務サイクルへの影響度を反映するよう、非常に詳細に設定されます。組み合わせ（メトリック、ネットワーク、サーバ、アプリケーション）ごとに、1 日の各時間ごとにその計算値が表示されます。 ベースラインを使用することで、そのときに期待されるパフォーマンスと実際のパフォーマンスを対照できるようになり、このため、「標準」の定義にコンテキストが提供されます。

管理コンソール は、特定のネットワーク - サーバ - アプリケーションの組み合わせに対して、10 のベースライン化されたメトリックごとにベースラインを計算します。 これは、ベースラインの平均値は算出しません。 そのため、レポートには、集約のベースラインは表示されません。 管理コンソール のパフォーマンス詳細グラフには、ベースライン情報が表示されます。 これは、ベースラインを使用してしきい値を決定することはありません。

グラフでベースラインを表示するには、ネットワーク、サーバ、アプリケーションおよびベースライン化されたメトリックを選択します。 サマリ グラフにはベースラインは含まれません。 ［操作］ページのパフォーマンス グラフには、現在のパフォーマンスと標準値を比較できる、プロットされたベースライン値が表示されます。 ［管理］ページの［パフォーマンス スコアカード］では、ベースライン値が表形式で表示されます。

［グラフ設定］ページでベースラインを有効にすると、管理コンソール は［操作］の［メトリック詳細］ビューにベースラインを表示します。

しきい値、インシデントおよびインシデント レスポンス

*しきい値*は受け入れ可能なパフォーマンスの上限です。 しきい値は以下の理由で重要です。

- 管理コンソール はしきい値によってデータを評価できます。
- しきい値は、インシデント作成、それに対するインシデント レスポンス、および適時のトラブルシューティングおよび問題解決を可能にする調査で役に立ちます。

しきい値はアプリケーションごとにデフォルトで存在します。 管理コンソール 管理者は、ネットワークおよびサーバのパフォーマンスのしきい値を設定します。メトリックごとに、マイナー（黄色）しきい値、メジャー（オレンジ）しきい値、およびパフォーマンス低下を表示するのに必要な最小の観測数を定義します。

管理コンソール はデフォルトしきい値を計算します。 しきい値の計算には、ベースラインは使用されません、しきい値とベースラインは同じデータから別々に計算されます。 管理者は、パフォーマンス変更に対するしきい値の感度を増減することができます。

しきい値を超えると、管理コンソール はインシデントを作成し、設定されているインシデント レスポンスを起動します。ネットワーク、サーバ、アプリケーションまたは 監視デバイス インシデント タイプごとに、インシデント レスポンスを設定することができます。 管理コンソール には、各インシデント タイプのデフォルト インシデント レスポンスが用意されています。

管理コンソール 管理者は、指定された期間に到達または違反する各しきい値に対するアクションと通知を設定できます。 管理者は、指定するインシデント レスポンスに対するアクションまたは通知を、以下の状況で行われるように指定できます。

- パフォーマンスがマイナーしきい値に到達したか超えたとき
- パフォーマンスがメジャーしきい値に到達したか超えたとき

管理コンソール は、各条件に対してインシデントをオープンします。 条件に対してアクションが存在する場合は、管理コンソール はそのアクションを自動的に起動します。

インシデント、インシデント レスポンスおよびアクションに関する以下の詳細を覚えておいてください。

- しきい値を超えると、管理コンソール はインシデントを作成します。
- 以下の条件が満たされない限り、インシデントはアクションを自動トリガしません。
  - ネットワーク、サーバ、アプリケーションまたは 監視デバイス に対して適切なインシデント レスポンスが関連付けられている。 この関連付けは、インシデント レスポンスを作成する際に設定します。
  - 関連するインシデント レスポンスにアクションが関連付けられている。デフォルト インシデント レスポンスにはアクションが関連付けられていません。
  - 違反が最小の重大度および期間条件を超えている。
- インシデントにアクションがなくてもかまいません。
- インシデントのないアクションを起動することは可能です。インシデントと関連付けられたアクションは調査と呼ばれ、手動で起動することも、スケジュールすることもできます。

インシデントおよびインシデント レスポンスは、以下の点でトラブルシューティングに役立ちます。

- 問題が発生したとき、インシデントに条件のレコードが保持されている。
- インシデント レスポンスでは、問題が発生したときに、問題のトラブルシューティングに役立つ情報が自動的に収集されるため、MTTR（Mean Time to Repair）が短縮されます。

インシデント レスポンスには、アクションが含まれないか、1 つ以上のアクションが含まれます。 アクションは、通知または自動調査にすることができます。 作成できるインシデント レスポンスのタイプの詳細については、「管理者ガイド」を参照してください。

調査

問題の解決に役立つ十分な情報がインシデント レスポンスで収集されない場合は、さらにその問題をトラブルシューティングするための詳細を収集するために、即時調査またはスケジュールされた調査を起動できます。調査は、しきい値違反の原因に関する診断情報を収集するために 管理コンソール が実行するアクションです。管理コンソール ユーザ アカウントには、調査の実行権限がある、関連する役割を設定する必要があります。

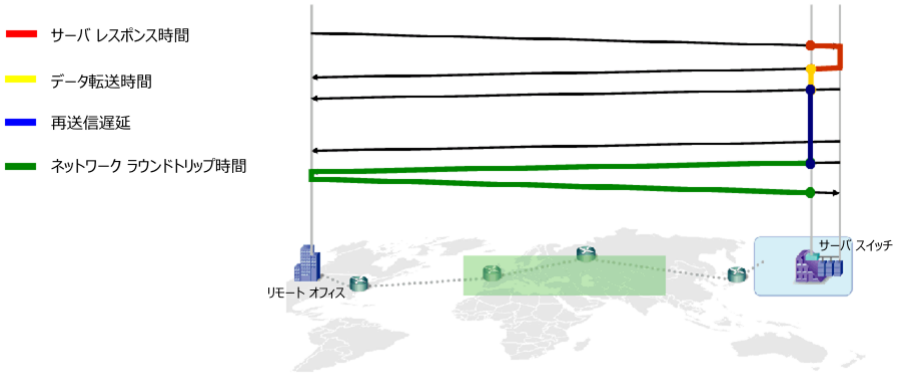
調査では、以下のいずれかのアクションを実行することができます。

- アプリケーション接続時間
- パケット キャプチャ
- ping レスポンス時間
- SNMP サーバ クエリ
- SNMP ルータ クエリ
- ICMP トレース ルート
- TCP トレース ルート

管理コンソール 管理者は、調査できる SNMP コミュニティを設定する必要があることに注意してください。 詳細については、「*管理者ガイド*」を参照してください。

レスポンス時間

管理コンソール には、レスポンス時間の測定値が表示されます。これは、5 分間隔で平均され、以下を含みます。



注：これらのレスポンス時間の定義は、WAN 向けに最適化されたトランザクションでは異なります。

サーバ レスポンス時間

サーバがクライアント要求に対する初期レスポンスを送信するのにかかる時間、またはサーバの初期「思考時間」。サーバ レスポンス時間の増加は、通常以下のことを示しています。

- CPU、メモリ、ディスクまたは I/O などサーバ リソースの不足
- アプリケーションの設計に問題がある

データ転送時間

レスポンス全体（最初のパケットから最終パケットまで）を送信するのにかかった時間。 TCP ウィンドウに収容しきれない大量のデータを送信する場合は、［データ転送時間］から初期サーバ レスポンス時間を除外し、ネットワーク ラウンドトリップ時間のみを含めます。

再送信遅延

元のパケット送信から最後の重複するパケット送信までに経過した時間。管理コンソール は再送信パケット数に対してだけではなく観測を通した平均としての再送信遅延をレポートします。10 個で 1 セットの 1 つのパケットが 300 ミリ秒の再送信時間を必要とする場合、再送信遅延は 30 ミリ秒（300 ミリ秒/10 パケット）としてレポートされます。

ネットワーク ラウンドトリップ時間

パケットがネットワーク上をクライアントからサーバおよびサーバからクライアントの両方向に移動するのにかかる時間。

合計トランザクション時間

永続的な TCP 接続において TCP トランザクションまたはデータ要求を完了するのにかかる時間。

実効ラウンドトリップ時間

ネットワーク ラウンドトリップ時間と再送信によって発生した遅延の合計。

主要な概念

管理コンソール が収集しレポートするデータを理解し使用するには、いくつかの重要な概念および用語に精通する必要があります。

このセクションのトピックでは、新しいユーザにはなじみがない大部分の製品用語だけでなく、いくつかの業界標準用語についても説明します。

集約

集約は、比較レポートをわかりやすくするために作成する、アプリケーション、サーバまたはネットワークのグループです。 ［エンジニアリング］ページでは、管理コンソール は集約を 1 つのエンティティとして扱います。 ［操作］ページと［インシデント］ページでは、集約の各メンバのデータが個別に表示されます。

集約の例は、リモート オフィスを構成する個別のクライアント サブネットにおけるパフォーマンス メトリックを 管理コンソール が分析するリモート オフィスの、IP サブネットのグループです。 比較を可能にするために各リモート オフィスの集約を作成するのは、よいやり方です。

可用性

5 分期間中にユーザがアプリケーションまたはサーバにアクセスできた場合、管理コンソール はサーバまたはアプリケーションを使用可能として分類します。 管理コンソール はパッシブ データの観測を通じてサーバおよびアプリケーション ポート レベルで可用性メトリックを追跡します。ユーザ トラフィックが観測されないとき、管理コンソール は 5 分ごとにアクティブな要求を作成することにより可用性を確認します。

可用性監視を有効にしている場合、管理コンソール は、サーバとアプリケーションの組み合わせの可用性を追跡します。 管理コンソール はネットワークの可用性を追跡しません。

先頭に表示

管理コンソール は、［操作］レポート ページのリストの先頭にパフォーマンスが最も低いサーバやアプリケーションを表示します。 これらのページには、パフォーマンスが最も低いネットワーク、サーバおよびアプリケーションのパフォーマンス メトリックが表示されます。

監視デバイス

監視デバイス は、TCP セッションのレスポンス時間を監視します。管理コンソール はいくつかのタイプの 監視デバイス をサポートしています。

データ ポイント

デフォルトでは、管理コンソール は、データ ポイントを作成するために、事前設定された間隔におけるデータを平均します。 データを平均するために使用される間隔ごとに、管理コンソール は代表的データ ポイントを算定し、グラフまたはテーブルにこのデータを表示します。 すべてのグラフおよびテーブルには、各データ ポイントを算定するために使用された期間がレポートされます。

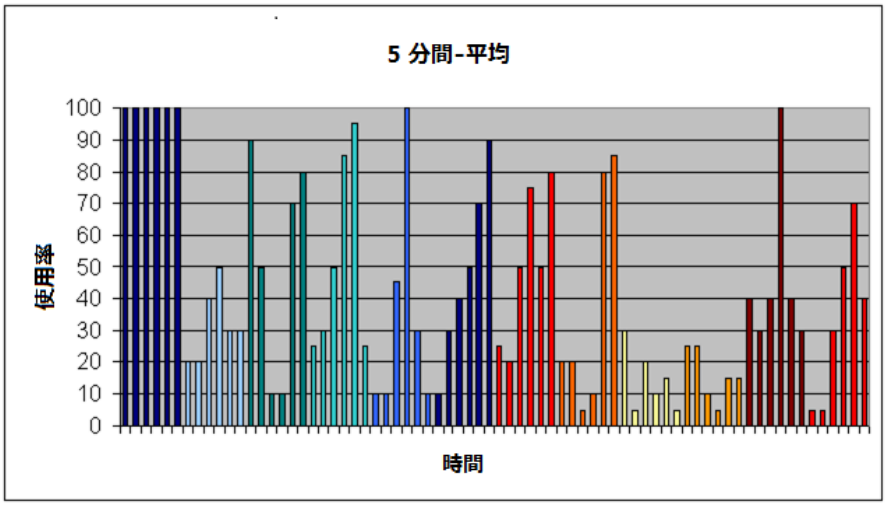
以下のテーブルにおいて、間隔を使用しているビューに対して、管理コンソール は以下の間隔を使用してデータを平均します。

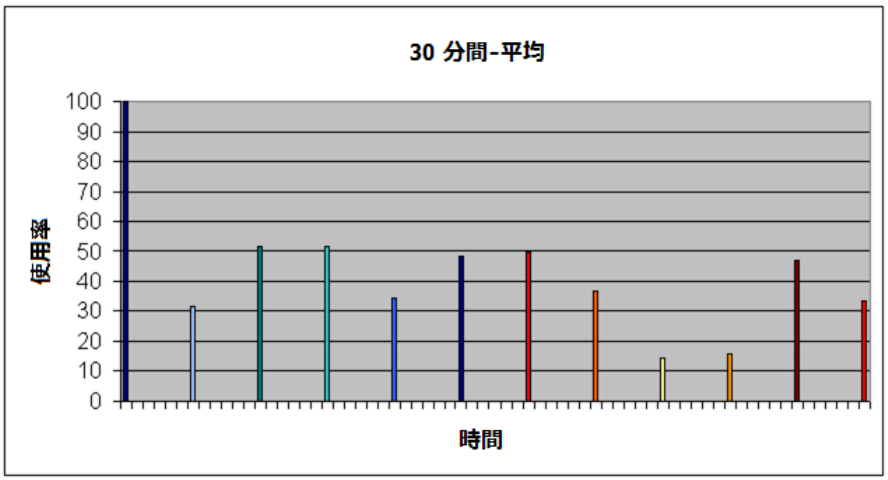
期間	間隔
過去 1 時間	5 分
過去 8 時間	5 分
昨日	15 分
先週	1 時間
先月	6 時間

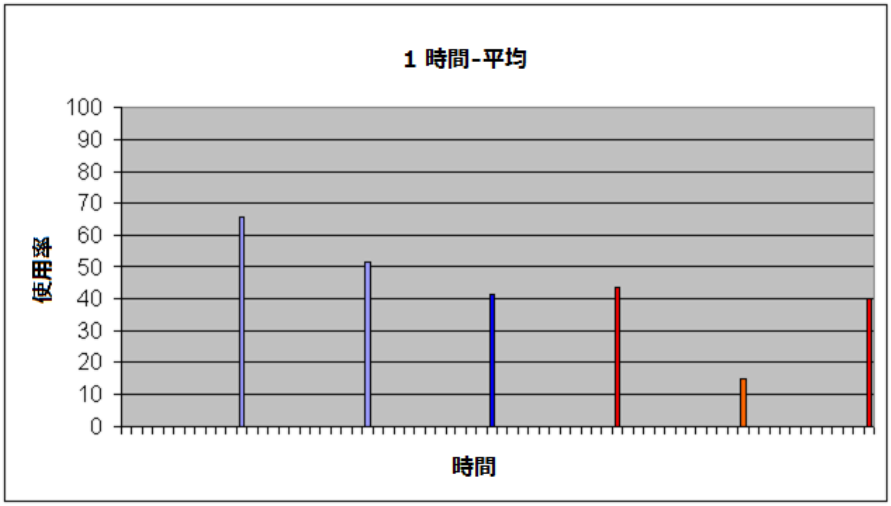
データ ポイントのレポートを以下のように設定します。

- 特定の問題を分析するには、短めの平均間隔を使用します。
- 一定時間にわたるパターンやトレンドを検出するには、長めの平均間隔を使用します。

以下のビューは、平均間隔が 5 分から 1 時間に増加したときに、詳細なデータ ポイントが曲線に移行していき、トレンドおよびパターンを識別できるようになる様子を示しています。







インシデント

インシデントは、管理コンソール が、パフォーマンスが定義済みのしきい値に到達したか、または超えたことを検出したときに作成する情報レコードです。 メトリック上昇の原因となったイベントを決定するには、インシデントを分析することをお勧めします。 管理コンソール は、［インシデント］ページで割り当てられたケース番号によってインシデントをレポートします。

管理コンソール が CA PC または CA NPC に登録されている場合、管理コンソール はそのインシデント ステータスを CA PC または CA NPC 内のイベントと同期します。

管理コンソール は、5 分データをユーザが保存するように設定した期間だけ、インシデント レコードを保存します。

インシデント レスポンス

インシデント レスポンスを使用すると、問題が発生したときにトラブルシューティングし、平均修復時間を短縮して、ビジネス クリティカルなアプリケーション、サーバおよびネットワークにインシデント レスポンスを割り当てることができます。 インシデント レスポンスは以下を行います。

- ユーザのチームにパフォーマンスの低下を知らせます。
- 問題を積極的に調査し、パフォーマンス低下の根本的原因を特定するのに役立つ追加情報を収集します。

デフォルトでは、管理コンソール はインシデント レスポンスを自動的に開始しません。

調査

インシデント原因の詳細を収集するための調査アクションは、手動で起動することも、スケジュールすることもできます。

保守スケジュール

保守スケジュールは、監視されるすべてのサーバと関連付けることができます。 以下のルールが保守スケジュールに適用されます。

- 保守期間中、管理コンソール は、データベース内のそのサーバのデータ ポイントおよびインシデントにフラグを設定し、レポートにそれらを含めません。
- 保守スケジュールを変更した場合でも、過去のデータは改訂されません。
- 管理コンソール は保守期間中でもサーバのパフォーマンスについてレポートしますが、OLA レポートの保守期間中に発生したパフォーマンス低下や少ない観測数に対してはインシデントをオープンしません。
- 保守スケジュールの終了または開始時、管理コンソール はオープンしているインシデントをクローズして、現在の保守状況を反映するために新規インシデントを作成します。

メトリック

メトリックは、5 分のレポート期間にわたって、特定のサーバおよびネットワーク上の特定のアプリケーションについて 管理コンソール が測定するパラメータです。 管理コンソール は、またメトリックの平均値を使用して、5 分期間中に確認された観測数を記録します。

管理コンソール は以下のメトリックをレポートします。

- バイト ボリューム
- 接続セットアップ時間
- データ転送速度 （ビット/秒） （サーバ間）。パケット別（サーバ間）
- データ ボリューム （バイト） （サーバ間）。パケット別（サーバ間）
- パケット ボリューム
- パーセンタイル スループット
- 1 ユーザあたりのコンポジット レート
- 再送信遅延
- TCP/IP セッション数 - 完了
- TCP/IP セッション数 - オープン
- TCP/IP セッション数 - 期限切れ
- TCP/IP セッション時間
- ユーザ
- ユーザ Goodput

ユーザは、これらのメトリックのしきい値を設定できません。また、管理コンソール は、これらのメトリックに関するインシデントを作成しません。しきい値を設定できるメトリックは、*相対メトリック*と呼ばれます。管理コンソール は相対メトリックについてもレポートします。

ネットワーク タイプ

類似の機能およびパフォーマンス期待値を持つネットワークをグループ化するのに使用されるネットワークです。 ネットワーク タイプを使用して、レポート、インシデント レスポンス生成、またはサービス レベル監視を実行するためにユーザの企業を編成します。たとえば、以下のようなネットワーク タイプがあります。

- 帯域幅によるグループ化 - 128K、T1、LAN
- 場所によるグループ化 - 中西部、本社

デフォルトのネットワーク タイプを使用することも、カスタム タイプを作成することもできます。

通知

通知は、インシデント レスポンスと関連付けられる一種のアクションです。 通知は、指定された期間においてしきい値に到達したか超えたことをユーザまたはコンピュータに知らせます。

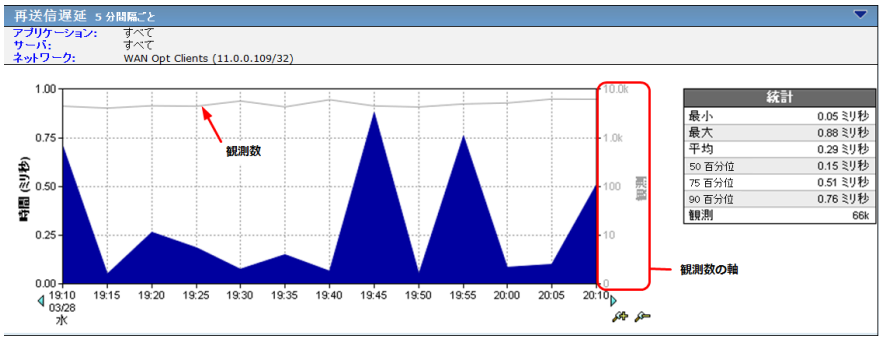
通知は、以下のいずれかになります。

- 特定のユーザに送信される電子メール メッセージ
- サードパーティ監視プラットフォームなどの受信側に送信される SNMP トラップ

観測数

観測数は、指定された間隔中に発生した監視対象の TCP トランザクションの数です。 観測数は、メトリック測定が行われた回数です。 各メトリックが調査をトリガする最小観測数を指定し、意味のあるトラフィック量が存在しない場合に通知が回避されるようにします。

観測数はグレーの線として 管理コンソール ビュー内に表示されます。 右側の軸は、観測数を示し、指数関数的で、ビューにおけるカウントが変動していることを示します。



観測数は使用率を示します。観測数が多いほど、アプリケーション、サーバまたはネットワークは頻繁に使用されています。

観測数を使用して、イベントの重要性を決定します。 観測数が多いことは、イベントが多くのユーザ、アプリケーションまたはサーバに影響している可能性があることを示します。 サーバの観測数がサーバ接続時間の増加と同時に減少する場合、このサーバ接続時間の増加はバックアップなど別の操作がサーバ上で実行されていることを示している可能性があります。

パーセンタイル

*パーセンタイル*は、5 分のデータ ポイントのコレクションからのパーセント計算です。管理コンソール はパーセンタイル データを保存し、そのデータをレポートで使用します。

メトリックの評価

5 分のレポート間隔中に十分な観測数が確認され、アプリケーション、サーバ、ネットワークおよび 5 分期間のすべての組み合わせにしきい値がある場合、管理コンソール はメトリックを正常、マイナー（黄色）またはメジャー（オレンジ）として評価します。 観測数が不十分か、またはしきい値がない場合は、管理コンソール はメトリックを未評価として分類します。

相対メトリック

*相対メトリック*は、しきい値を関連付けているメトリックです。このしきい値は、管理コンソール 管理者が設定できます。 管理コンソール は、しきい値を超えたときにインシデントをオープンし、5 分期間における相対メトリック パラメータの平均測定値を計算して、ベースラインをレポートします。

以下のセクションで説明するメトリックは、そこで説明されているアイテムに関連しています。たとえば、ネットワーク ラウンドトリップ時間は、ネットワークに関連しています。

ネットワーク メトリック

ネットワーク メトリックはネットワーク パフォーマンスに関連しています。

メトリック	説明
ネットワーク ラウンドトリップ時間	パケットがネットワークをトラバースするのにかかる時間。
ネットワーク接続時間	クライアントがサーバの接続確認応答コードを確認するのにかかる時間です。遅延は、通常ネットワーク遅延によって引き起こされます。
実効ラウンドトリップ時間	ネットワーク ラウンドトリップ時間と再送信によって発生した遅延の合計。
パケット ロスの割合	データ全体に対する再送信されたデータの比率、監視されているネットワークにおいて失われたデータの割合、および 1 秒あたりのパケット内の消失率。 ［QoS］ビューの要素です。

サーバ メトリック

サーバ メトリックはサーバのパフォーマンスに関連しています。

メトリック	説明
サーバ レスポンス時間	サーバが要求への応答を開始するまでにかかる時間。
サーバ接続時間	サーバが初期クライアント接続要求を確認するまでにかかる時間。
拒否されたセッション	3 方向ハンドシェーク中にサーバによって明示的に拒否された接続要求。［未対応の TCP/IP セッション リクエスト］ビューの要素です。
無応答セッション	接続要求が送信されたが、サーバが応答しなかったセッション。［未対応の TCP/IP セッション リクエスト］ビューの要素です。

結合メトリックについて

結合メトリックは、アプリケーションのパフォーマンスに関連しており、サーバ メトリックおよびネットワーク メトリックの両方から構成されます。

メトリック	説明
データ転送時間	レスポンス全体（レスポンス内の最初のパケットから最終パケットまで）を送信するのにかかった時間。 TCP ウィンドウに収容しきれない大量のデータを送信する場合は、［データ転送時間］から初期サーバ レスポンス時間を除外し、ネットワーク ラウンドトリップ時間のみを含めます。
トランザクション時間	クライアントがリクエスト（パケット レベルまたはトランザクション レベル）を送信した瞬間から、クライアントがレスポンスの最後のパケットを受信するときまでに経過した時間。管理コンソール は、［エンジニアリング］ページの［レスポンス時間構成: 平均］サマリ ビュー内にこのタイプのレスポンス時間データを表示します。

相対メトリックにはしきい値を設定できます。管理コンソール は、5 分期間における相対メトリック パラメータの平均測定値を計算して、ベースラインをレポートします。

注: メトリック定義は WAN 向けに最適化されたトランザクションでは異なります。

レポート間隔

管理コンソール レポートのデフォルトのレポート間隔を以下に示します。

- 8 時間までのレポートについては 5 分
- 8 時間超、24 時間までのレポートについては 15 分
- 1 日超、7 日までのレポートについては 1 時間
- 7 日超、1 か月までのレポートについては 6 時間

カスタムのタイムフレームを作成する際には、以下の値からレポート間隔を選択します。

- 5 分
- 15 分
- 30 分
- 1 時間
- 1 日

8 時間未満の期間において最も長い間隔のデータをレポートに表示するには、5 分間隔を使用します。1 か月を超えるレポート期間があるときは、1 日間隔を使用します。

長いレポート期間に対して短い間隔を選択すると、データ ポイント数のために、ビューが見づらくトレンドを把握するのが難しくなると共に、管理コンソール がビューを生成するのに長時間かかる可能性があります。

サンプル間隔

管理コンソール レポートに対するデフォルトのサンプリング間隔を以下に示します。

- 8 時間レポートについては 5 分
- 日単位レポートについては 15 分
- 週単位レポートについては 1 時間
- 月単位レポートについては 6 時間

OLA（運用レベル契約）

OLM（Operational Level Management）には、ビジネスの優先度に従って受け入れ可能なコストですべての IT ユーザに適切なレベルのサービスが提供されるようにする手順が含まれます。 管理コンソール で OLA（運用レベル契約）を設定および監視することで、サービス レベルが満たされているかどうかを判定できます。 ［管理］ページで OLA レポートを参照します。

通常、以下のパフォーマンス メトリックに関する OLA を設定します。

- サーバ レスポンス時間。これは、データ センターのパフォーマンスを測定します。
- ネットワーク ラウンドトリップ時間。これは、ネットワーク インフラストラクチャのパフォーマンスを測定します。
- トランザクション時間。これは、ユーザのアプリケーションの操作性をキャプチャします。

しきい値タイプ

管理コンソール は、パーセンタイルと感度設定を使用してデータ サンプル内のすべてのメトリックを分類し、自動的に最近のパフォーマンスからしきい値を計算します。

しきい値を変更するには、感度設定を調整するか、または、割合またはミリ秒の値を設定します。

しきい値タイプ	説明
なし	（オフ）管理コンソール にすべてのデータを［*未評価*］と評価させます。管理コンソール は、［なし］のしきい値を持ったメトリックにはインシデントを作成しません。
感度	（動的）このタイプのしきい値を設定するには、パーセント値を使用します。管理コンソール は、しきい値を計算するために使用する式に因子としてこのパーセント値を自動的に入れます。感度設定を 200 にすると、75 パーセンタイルまでのトラフィック測定がマイナー（黄色）またはメジャー（オレンジ）と評価されます。 感度設定を低くすると、しきい値が高くなるため、インシデントが少なくなります。
ミリ秒	（静的）このタイプのしきい値は、100 などの特定の静的な値に設定します。

スループット

管理コンソール は、転送されたバイト数を経過時間で除算して、スループットを計算します。 管理コンソール は TCP トランザクションごとにこの計算を実行します。 転送されたバイト数は、合計バイト数でなくサーバからのバイト数です。 スループット計算は、大きなトランザクションの場合にのみ、適切な測定値になります。

タイムフレーム

管理コンソール 内のビューを設定するには、レポート ページ上の［設定］にある［タイムフレーム］メニューを使用します。 管理コンソール は、現在の時刻で終了する時間間隔のデータを表示します。 今日以外の終了日を持つ間隔を指定するには、［カスタム］を選択します。

管理コンソールへのログイン

管理コンソール の使用を開始するには、サーバ名または IP アドレスを使用してコンソールをホストするサーバにアクセスします。次に例を示します。

`http://<IPAddress>`

管理コンソール は、Microsoft Internet Explorer バージョン 7 または 8、および Mozilla Firefox 3.6 での表示用に設計されていて、Adobe Flash Player を必要とします。 ログイン情報については、管理コンソール 管理者にお問い合わせください。

バージョン情報の表示

管理コンソール のバージョンおよびリビジョン情報を表示するには、メニュー バー上の［バージョン情報］をクリックします。

- バージョン : 管理コンソール のインストール バージョン、インストール日時、HASP 期限日時、および設定に関する情報を表示します。 製品ドキュメントへのリンクも表示されます。
- 修正履歴 : インストール バージョンおよびインストール時期の履歴がリスト表示されます。
- CA PC および CA NPC : データ ソースとして CA PC または CA NPC に登録されている場合、CA PC または CA NPC サーバのアドレスおよび製品バージョン番号を示します。

ナビゲーションに関するヒント

管理コンソール のインターフェースに精通するにあたり、以下のヒントを覚えておいてください。

- 管理コンソール でレポート ページおよびビューを表示するときは、青いフォントのネットワーク、アプリケーション、メトリック、インシデントおよび他のリスト表示されたアイテムをクリックしてレポートに移動し、詳細情報を表示します。
- この記号が表示されているすべての情報ボックスにリンクがないかどうかを注意し、あればクリックします。 管理コンソール は、情報ボックスを使用して、手順を案内し、詳細を入力するようにユーザに求めます。
- レポートで青いアイテムをクリックしたり情報を表示および検討した後は、［設定］領域の［クリア］をクリックして、概要レベルのデータまたはページに戻ります。

- 役に立つツールヒント情報を参照するには、コントロールやビューの部分などのアイテム上でマウスを保持します。 ビューにあるインターフェースを表すバー上でマウスを保持して、ルータ、説明および速度などインターフェースに関する詳細を表示します。
- レポート ページまたはビューを印刷、電子メール送信したり、またはスプレッドシートに保存したりして、情報を共有します。 レポート全体ページを印刷、電子メール送信、またはエクスポートするには、レポート ページの最上部のボタンを使用します。 ビューを印刷、電子メール送信、またはエクスポートするには、ビューの最上部の青い歯車型メニュー（ ）を使用します。
- 昇順または降順にデータを並べ替えるには、列見出しをクリックしてソート順を変更します。
- CA Performance Center または CA NetQoS Performance Center にデータソースとして 管理コンソール を追加した場合は、管理コンソール の右上隅の NPC リンクをクリックすると、管理コンソール から連係する Performance Center にアクセスできます。CA Performance Center または CA NetQoS Performance Center を使用する詳細については、CA Performance Center または CA NetQoS Performance Center のドキュメントを参照してください。

第 2 章: 管理コンソールの使用

AITempty

このセクションには、以下のトピックが含まれています。

シングル サインオン

シングル サインオンは、CA PC、CA NPC、および CA Application Delivery Analysis を含むサポート対象のすべてのデータ ソースで使用される認証スキームです。 ユーザが CA PC または CA NPC に一度認証されたら、そのユーザはその後サインインすることなしに CA PC、CA NPC、および登録されているデータ ソースを移動できます。

シングル サインオンは自動的にインストールされます。 連係している CA PC または CA NPC へのリンクは、管理コンソール の右上隅に表示されます。

ユーザのプロファイルの編集

ユーザ プロファイルの編集は、たとえばローカル タイム ゾーンを指定するために使用されます。 CA PC または CA NPC にデータ ソースとして登録されている場合、変更は 5 分以内に自動的に同期されます。

次の手順に従ってください：

1. メニュー バー上の自身のユーザ名をクリックします。

   ［ユーザのプロファイル］ページが表示されます。

2. 以下の情報を変更します。

   パスワード

   新しいパスワードを入力します。

   パスワードの確認

   パスワードを再入力します。

   電子メール アドレス

   電子メール アドレスを入力します。

   Time Zone

   ローカル タイム ゾーンを選択します。管理コンソール は、このタイム ゾーンにレポート データをオフセットします。デフォルトのタイム ゾーンは CST6CDT です。これは中央標準時の期間はグリニッジ標準時マイナス 6 時間、中部夏時間の期間はグリニッジ標準時マイナス 5 時間です。 可能な限りタイム ゾーンの Etc バージョンではなく、特定のタイム ゾーンを使用します。これは、Etc バージョンは夏時間を考慮しておらず、またオフセットは予想の反対となるからです。つまり Etc/GMT+4 はグリニッジ標準時（GMT）から 4 時間進んでいるのではなく、4 時間遅れています。

   ホーム ページ

   管理コンソール にアクセスするときに表示するデフォルト ページを選択します。

3. ［適用］をクリックし、［OK］をクリックします。

収集されたデータ、レポート ページ、およびビュー

パフォーマンスの問題がネットワーク インフラストラクチャ、サーバ、またはアプリケーションのために発生しているかどうかを判別するには、管理コンソール レポートを使用します。 管理コンソール は、以下の変数の組み合わせを使用してレポートを生成します。

- ネットワーク
- サーバ
- アプリケーション
- タイムフレーム
- メトリック

分析するデータがわかっている場合は、必要な情報を表示するレポートを容易に生成できます。

管理コンソール によって、以下のテーブルにリスト表示されたエレメントの 1 つまたは組み合わせにパフォーマンスの問題を特定できます。

エレメント	パフォーマンスの問題のあり得る発生源
ネットワーク インフラストラクチャ	遅延の原因： ■ 回線 ■ トラフィックの輻輳 ■ ルータ ■ スイッチ
サーバ インフラストラクチャ	遅延の原因： ■ CPU 処理 ■ メモリ I/O ■ ディスク読み取り/書き込み数
アプリケーション アーキテクチャ	送信対象としての多数の小型パケットに大きなデータ要求を書き込んだため。

以下の方法を使用して 管理コンソール データを確認して分析し、パフォーマンス問題の発生源を特定します。

1. パフォーマンス マップやアプリケーション詳細表示を使用して、パフォーマンス上の問題を示しているアプリケーションを特定します。
2. パフォーマンス問題を引き起こしているレスポンス時間の構成要素を特定します。レスポンス時間コンポーネント ビューの色は、レスポンス時間全体を構成する各構成要素を識別します。
3. ［トラフィック］、［セッション数］、［トレンド］、［レスポンス サイズ］、［QoS］、［統計］ページを調べ、パフォーマンス上の問題に関与している要因を調査します。

   パフォーマンス問題の検出および解決の詳細については、「トラブルシューティング (P. 159)」を参照してください。

レポート ページのナビゲーション

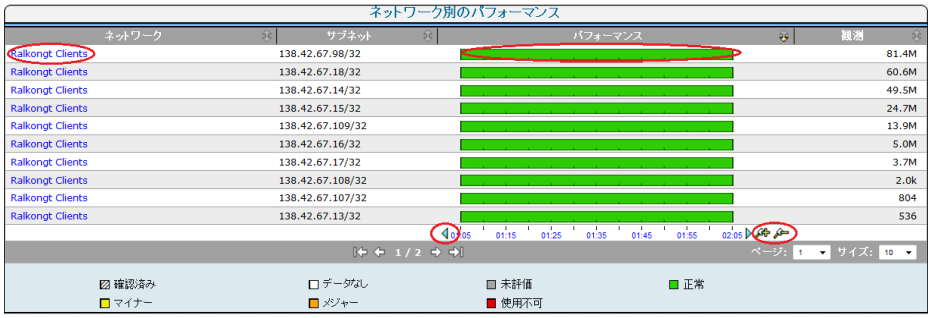
タブ ページは、IT 部門内の職務上の役割に相当します。 たとえば、［エンジニアリング］ページでは、［ネットワーク別のパフォーマンス］レポート ページをはじめとする、ネットワーク エンジニアが担当するデータが含まれるレポートに、迅速にアクセスできます。タブ ページはそれぞれ、トラブルシューティング、最適化用のトレンドの研究、サマリ レポートの表示を簡単に行うなど、異なる目的に合う方法でデータを表示します。

［表示項目］メニューでビューを選択するか、またはレポートに移動します。ビューまたはレポートに表示するタイムフレーム、選択したメトリック、アプリケーション、サーバ、およびネットワークを変更するには、［操作］、［インシデント］、［管理］、［エンジニアリング］、または［最適化］ビューおよびレポート ページの［設定］をクリックします。

レポート ページ上でデータをフィルタするには	参照
概要レポートの詳細情報に移動します。	レポートへの移動 (P. 39)
［表示項目］メニューでビューを選択します。	［表示項目］メニューのナビゲーション (P. 40)
［設定］をクリックして、ビューの設定を変更します。	レポート設定の変更 (P. 41)

レポートへの移動

操作レポートの詳細情報にアクセスするには、以下のサンプルのパフォーマンス レポートに示すように、レポートおよび他のエレメントの中のユーザ インターフェースのリンクをクリックします。

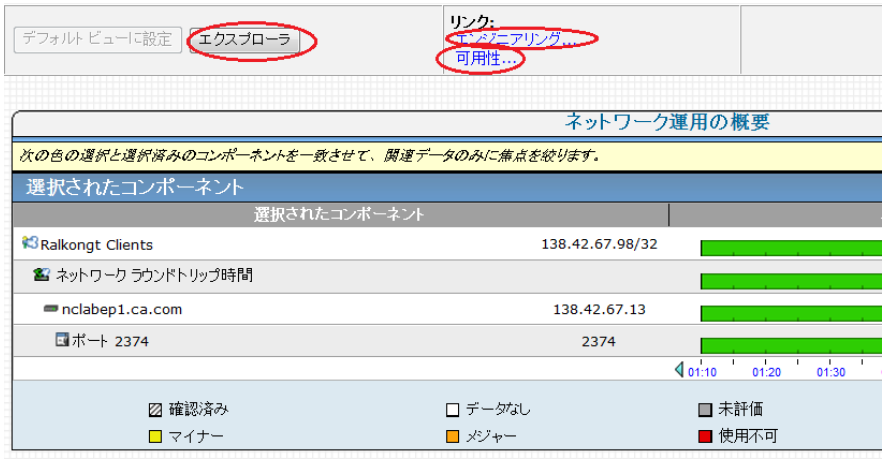


パフォーマンス レポートで、以下の手順に従って詳細情報を表示します。

- ネットワークの選択コンポーネントを表示するには、ネットワークをクリックします。
- タイムラインを後方または前方に移動するには、タイムライン上の矢印をクリックします。
- ズームインする（タイムフレームを絞り込む）かズームアウトする（タイムフレームを拡大する）には、拡大鏡をクリックします。

また、関連するレポートへのリンクをクリックすることもできます。 次に例を示します。

- ［エクスプローラ］をクリックすると、関連するメトリック詳細レポートが表示されます。
- ［エンジニアリング］をクリックすると、選択されているコンポーネントのコンポーネント レポートが表示されます。
- ［可用性］をクリックすると、可用性レポートが表示されます。



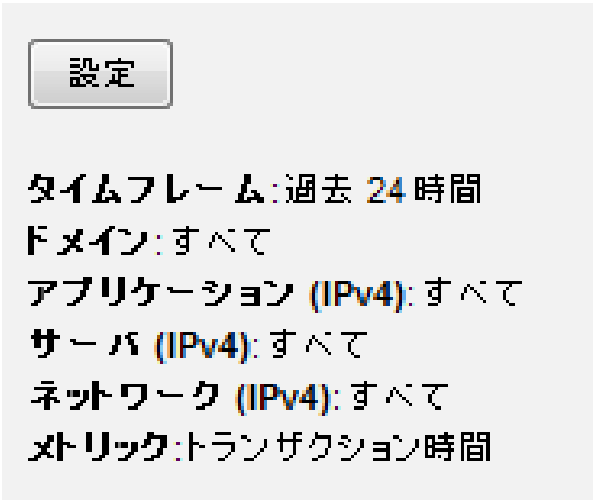
［表示項目］メニューのナビゲーション

管理コンソール の上部の 6 つのタブは職務上の役割に相当します。 タブはそれぞれ、トラブルシューティング、最適化用のトレンドの研究、サマリ レポートの表示を簡単に行うなど、異なる目的に合う方法でデータを表示します。

各タブの［表示項目］メニューでは、ページ上のデータのビューを変更できます。 ［操作］ページの［表示項目］メニューでは、ネットワーク、サーバ、またはアプリケーション ビューのデータ概要を表示できます。

レポート設定の変更

管理コンソールは、各レポート ページの上部の［設定］ボタンの下に、現在のページおよびレポートの設定を表示します。 以下の例では、管理コンソールは、191.168.1.0 ネットワーク上のすべてのアプリケーションおよびサーバの過去 1 時間のデータを表示し、ビューとレポートにすべての相対メトリックを含めます。



レポート設定を変更するには、［設定］ボタンをクリックします。

タイムフレーム

リストから目的のタイムフレームをクリックし、定期保守中に収集されたデータを含めるかどうかを選択します。 選択したタイムフレームに応じて、現在の時刻とレポートの最新データの間にギャップが発生する可能性があります。 たとえば、タイムフレームを 1 週間に設定すると、レポート間隔は 60 分になるため、最大 55 分のギャップが確認される場合があります。

- 8 時間以下に設定すると、間隔が 5 分で表示されます。
- 16 時間以下に設定すると、間隔が 10 分で表示されます。
- 24 時間以下に設定すると、間隔が 15 分で表示されます。
- 1 週間以下に設定すると、間隔が 60 分で表示されます。
- 1 か月以下に設定すると、間隔が 6 時間で表示されます。

メトリック

必要なメトリックまたはメトリックのグループを選択する場合にクリックします。 たとえば、［インシデント］ページから、［すべてのサーバ メトリック］または特定のサーバ メトリックを選択できます。

アプリケーション、サーバ、ネットワークの組み合わせ

必要なアプリケーション、サーバ、およびネットワークの組み合わせを選択します。

- アプリケーション、サーバまたはネットワークの選択内容をクリアするには［X］ボタンをクリックします。次に、別の選択を行います。
- グループフィルタを CA PC または CA NPC からアプリケーション、サーバ、およびネットワークに適用するには、［すべてのグループを選択］をクリックします。 グループ フィルタを上書きするには、［X］ボタンをクリックします。次に、必要なアプリケーション、サーバまたはネットワークをクリックします。
- アプリケーション、サーバまたはネットワークを検索するには、目的の名前を入力し、［検索］をクリックします。
- 重複した IP トラフィックを分離するようにドメインを作成している場合は、目的のドメインを選択します。 この選択により、当該のドメインに一致するサーバおよびネットワークのリストのみが表示されます。 デフォルトでは、［デフォルト ドメイン］がすべてのサーバおよびネットワークに適用されます。

CA Multi-Port Monitor を使用した詳細へのドリル

管理コンソール は、CA Observer Expert などでセッション分析用のパケットのエクスポートを可能にすると共に、セッション レベルの可視性を実現するように、CA Multi-Port Monitor と統合されています。

管理コンソール の［操作］、［インシデント］、または［エンジニアリング］タブで、時間枠、ネットワーク、サーバおよびアプリケーション設定を含む現在のレポート コンテキストが、CA Multi-Port Monitor 内のドリルダウン ビューに適用されます。

5 分精度を持ったネットワーク レベルで TCP セッションを分析する CA Standard Monitor と異なり、CA Multi-Port Monitor は、1 分精度のサーバと特定のクライアントの間の TCP セッションを分析できます。 さらに、CA Multi-Port Monitor を使用すると、TCP および非 TCP トラフィックなど、CA Multi-Port Monitor によって観測されているすべてのトラフィックのトラフィック ボリュームを分析できます。

管理コンソール レポートから CA Multi-Port Monitor 内のデフォルト分析に至るトラブルシューティング パスをたどる場合は、手始めに 1 時間などの比較的狭い時間枠を 管理コンソール レポート設定で選択することをお勧めします。単一のネットワーク、サーバまたはアプリケーションにデータを限定するなど、レポートに適用するすべてのフィルタリングは、CA Multi-Port Monitor でデフォルト ビューをドリルダウンした後もそのまま残り、トラブルシューティング作業をネットワークの適切な領域に絞り込むことができます。

次の手順に従ってください:

1. ［操作］、［インシデント］または［エンジニアリング］タブ内の［設定］をクリックします。

   ［設定］ダイアログ ボックスが表示されます。

2. レポート設定を設定して、［OK］をクリックします。

   ドリルダウンによりサーバ トラフィックを観測する論理ポートが自動的に選択されるようにするには、特定のサーバが選択されるように管理コンソール のレポート設定を設定する必要があります。

3. ［セッション分析］をクリックします。

   ［セッション分析］ボタンが無効な場合は、CA Multi-Port Monitor で監視されるサーバを選択するようにレポート設定を設定します。

CA Multi-Port Monitor が表示する分析メニューには、レポート設定のコンテキストに基づいてレスポンス時間メトリックが表示されます。

分析メニューの使用の詳細については、CA Multi-Port Monitor 製品ドキュメントを参照してください。

ヒント： すべてのサーバを表示するようにレポート設定を設定した場合に、CA Multi-Port Monitor に複数の論理ポートが設定されていると、［セッション分析］ダイアログ ボックスにより、分析するサーバ トラフィックを観測する論理ポートを選択するように求められます。 適切な論理ポートを選択し、［OK］をクリックして CA Multi-Port Monitor を開始します。

グラフからテーブルへのレポート形式の変更

グラフからテーブルまたは詳細なテーブルに、またはテーブルをグラフに、レポート形式を変更できます。 また、グラフからより大きなグラフに一部のレポート ページを変更することもできます。

次の手順に従ってください:

1. ［エンジニアリング］ページをクリックします。
2. グラフの右上隅の青い歯車型メニュー（ ）をクリックし、［テーブル］をクリックします。

   注: 表示形式として［より大きなグラフ］を選択できるグラフがあります。
3. 管理コンソール は、表形式でビューを表示します。 グラフ ビューに戻るには、青い歯車型メニュー（ ）をクリックし、［グラフ］をクリックします。

レポート ページおよびビューのデータの解釈

十分な観測数があり、アプリケーション、サーバ、ネットワークおよび 5 分期間のすべての組み合わせにしきい値がある場合、管理コンソール は以下の評価の 1 つを使用して、メトリックを分類します。

確認済み

管理コンソール ユーザがインシデントを確認したことを示します。ユーザがインシデントを確認すると、管理コンソール は、インシデントに含まれるデータを[確認済み]としてマークします。管理コンソール では、確認済みのインシデントに含まれる将来のデータは、自動的に［確認済み］としてマークされます。

データなし

使用可能なデータがないことを示します。

未評価

未評価のパフォーマンス評価は、管理コンソール［操作］ページでグレーの重大度状態によって示され、しきい値を設定するには過去のデータが不十分である（正味 2 営業日分のデータが必要）ことを意味するか、または、観測数が少なかったために、設定された最小の観測しきい値を超える観測がなかったことを意味します。

標準

メトリック値がゼロとマイナーしきい値の間にあることを示します。

マイナー

メトリック値がマイナーしきい値を超えたことを示します。

メジャー

メトリック値がメジャーしきい値を超えたことを示します。

使用不可

サーバ上のアプリケーションが実行されていない（使用不可である）ことを示します。 この評価は、［設定］で［すべてのサーバ メトリック］をクリックすると表示されます。 この評価は、管理コンソール 管理者がサーバを割り当てたユーザ定義のアプリケーションにのみ適用可能です。

第 3 章: 操作ページの使用

このセクションには、以下のトピックが含まれています。

操作レポート ページの使用

パフォーマンス問題を調査し、トラブルシューティングするには、［操作］ページを使用します。 *パフォーマンス マップ*ページでは、上部から、パフォーマンスの低い順にネットワーク、サーバ、およびアプリケーションが表示されます。 これらのアイテムをクリックすると、レポートの焦点が絞られます。

通常、エンド ユーザは、Operations Center およびサポート チームに以下のパフォーマンス問題をレポートします。

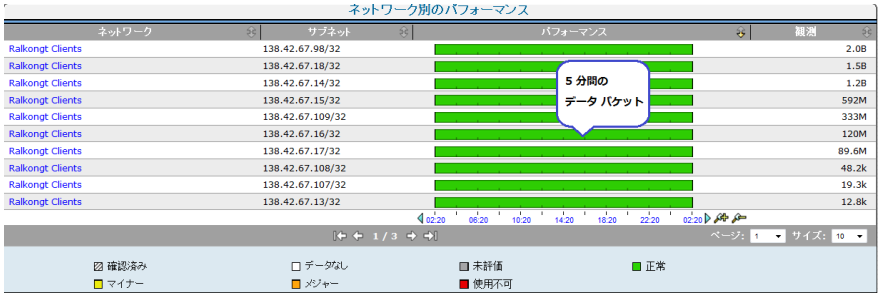
- アプリケーションのパフォーマンス問題
- ネットワークのパフォーマンス問題
- サーバのパフォーマンス問題

パフォーマンス マップは、パフォーマンス問題に関して以下のデータを収集します。

- パフォーマンス問題が発生しているアプリケーションとサーバの名前
- ユーザの場所および IP アドレス、ネットワークを識別するローカルまたはリモートのオフィスの場所
- パフォーマンス問題が最初に発生した時間
- パフォーマンス問題の履歴および再発有無
- この問題に関連する他のパフォーマンス問題

［操作］ページでは、パフォーマンス エレメント全体と定義されたしきい値を比較する色分けされた横の棒グラフとして、ネットワーク、サーバまたはアプリケーション別にパフォーマンス マップが表示されます。 色分けはデータの評価に対応します。

パフォーマンス バー上の間隔は、5 分期間の平均値を表します。

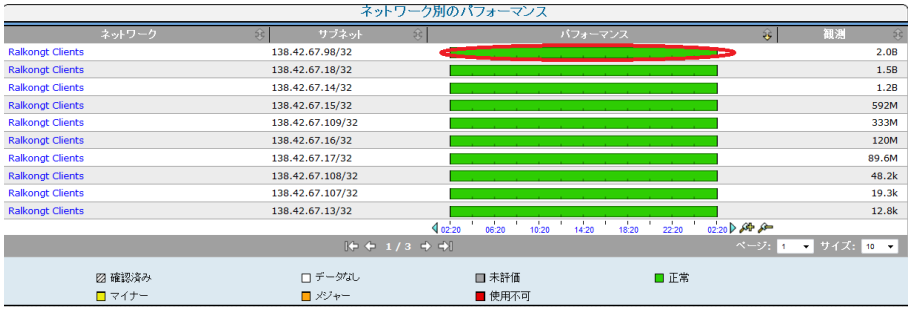


詳細:

レポート ページの電子メール送信 (P. 157)
レポート ページの印刷 (P. 157)
レポート設定の変更 (P. 41)
レポートのファイルへのエクスポート (P. 155)
操作レポート ページのナビゲート (P. 49)

操作レポート ページのナビゲート

パフォーマンス低下に関連するネットワーク、サーバ、およびアプリケーションを表示するには、ビューの上部に表示されているパフォーマンスが最も低いコンポーネントの 1 つをクリックします。



たとえば、ユーザが NetQoS LAN ネットワークのパフォーマンス バーをクリックすると、管理コンソール は、ネットワーク メトリックだけでなく、影響を受けたサーバおよびアプリケーションも表示します。 マイナーのネットワーク パフォーマンス低下に影響されていないサーバおよびアプリケーションを表示するには、［無関連］リンクをクリックして展開します。 ［無関連］フォルダには、［正常］と評価されたコンポーネント、［未評価］のコンポーネント、またはデータがないコンポーネントが含まれます。

管理コンソール はこのタイプを示すためにコンポーネントの前にアイコンを表示することに注意してください。 以下のアイコンは、コンポーネントのステータスを示していません。

アイコン	説明
	ネットワーク

アイコン	説明
	サーバ
	アプリケーション

コンポーネントの詳細の表示

コンポーネントの詳細を表示して、パフォーマンスの問題を調査します。詳細には、［関連するメトリック］、［影響を受けたメトリック］および［影響を受けたユーザ］が含まれます。

次の手順に従ってください:

1. ［操作］ページをクリックします。
2. ［表示項目］メニュー下の［エクスプローラ］をクリックします。
3. パフォーマンスを調査してパフォーマンスのしきい値を変更するには、以下のタブをクリックします。

関連するメトリック

このタブには、問題に関連する他のメトリックが表示されます。このタブの情報を使用して、問題を診断できます。 各メトリックのグラフには以下が表示されます。

- メトリックの関連する統計または平均。 統計には最小値、最大値、加重平均、50 番目、75 番目、90 番目のパーセンタイル、観測数があります。 平均は、サーバ間のバイト数またはパケット数です。
- ベースライン パフォーマンス。これは、実際のデータと比較するのに使用できます。

影響を受けたメトリック

このタブには、問題の影響を受けた他のメトリックが表示されます。 各メトリックのグラフには以下が表示されます。

- メトリックの関連する統計または平均。 統計には最小値、最大値、加重平均、50 番目、75 番目、90 番目のパーセンタイル、観測数があります。 平均は、サーバ間のバイト数またはパケット数です。
- ベースライン パフォーマンス。これは、実際のデータと比較できます。
- ユーザが前後の時間にスクロールできるようにする左右両方向の矢印。
- ビューをセンタリングできるようにするグリッド。

影響を受けたユーザ

このタブには、パフォーマンス問題の影響を受けたユーザが表示されます。 タブには、ユーザごとに IP アドレス、サブネット マスク、およびホスト名が表示されます。

しきい値の編集

このタブでは、パフォーマンス評価を定義するしきい値を編集できます。 しきい値の設定の詳細については、「*管理者ガイド*」を参照してください。

ベースラインの表示

ベースラインを使用して、パフォーマンス状態が正常かどうかを判断できます。 管理コンソール によるベースラインの計算には、以下のパラメータが組み込まれます。これらのパラメータを設定するには、関連するデータベース パラメータを設定します。

パラメータ	デフォルト	データベース パラメータ	説明
過去の日数要因	7	maxDaysBack	ベースラインの算出に使用する過去の日数の最大値。 デフォルトは前週の 7 日間です。
過去の週数要因	12	maxWeeksBack	曜日のベースラインの算出に使用する過去の週数の最大値。 デフォルトは前四半期の週数です。
過去の月数要因	6	maxMonthsBack	日付のベースラインの算出に使用する過去の月数の最大値。

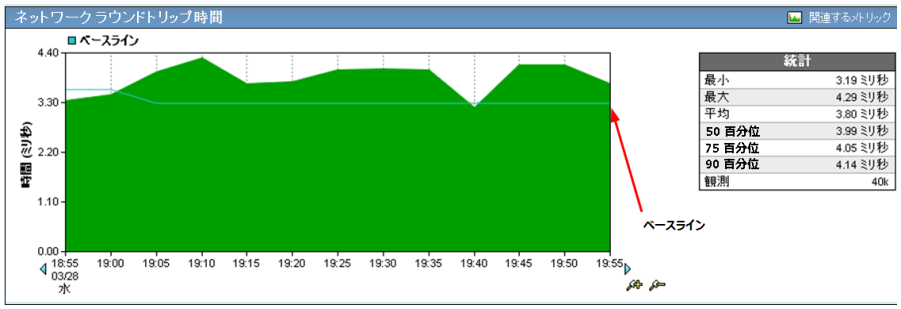
次の手順に従ってください:

1. ［操作］ページをクリックします。
2. ネットワーク、サーバまたはアプリケーションをクリックします。
3. 選択内容をメトリック、ネットワーク、アプリケーションまたはサーバに絞り込みます。
4. ［表示項目］メニュー下の［エクスプローラ］をクリックします。

   ［操作： メトリック詳細］ページが表示されます。
5. ［グラフ設定］をクリックします。

   ［グラフ設定］が表示されます。
6. 一次軸を設定します。
   a. ［メトリックとベースライン］をクリックします
   b. ［表示］ボックスからベースラインを選択します。
   c. ［OK］をクリックします。

   詳細ビューに、選択されたベースラインが表示されます。



コンポーネントのインシデントの表示

［インシデント］ページに、インシデント番号、ターゲット、アプリケーション、重大度、時間、および期間がリスト表示されます。

次の手順に従ってください:

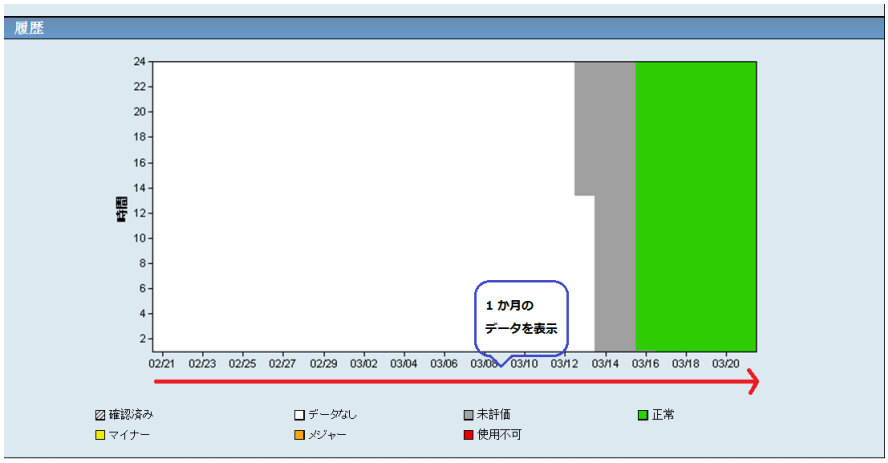
1. ［操作］ページをクリックします。
2. インシデントを表示するネットワーク、サーバまたはアプリケーションのパフォーマンス バーをクリックします。
3. 選択したコンポーネントの［インシデント］ページを表示するには、［表示項目］メニュー内の［インシデント］をクリックします。

コンポーネントの履歴データの表示

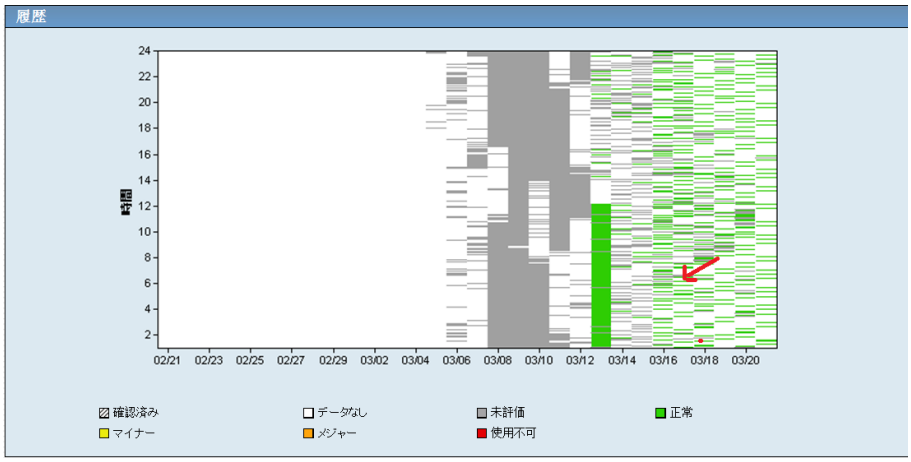
時系列でパフォーマンスの挙動を分析するには、ネットワーク、サーバまたはアプリケーションの履歴データを表示します。

次の手順に従ってください:

1. ［操作］ページをクリックします。
2. 履歴データを表示するネットワーク、サーバまたはアプリケーションのパフォーマンス バーをクリックします。
3. ［表示項目］メニュー内の［履歴］をクリックします。 グラフに、選択されたアイテムの前月データが表示されます。



4. グラフ内の特定のデータ ポイントをクリックして、その日時に対する［選択されたコンポーネント］ビューを表示します。



アプリケーションのパフォーマンス問題のトラブルシューティング

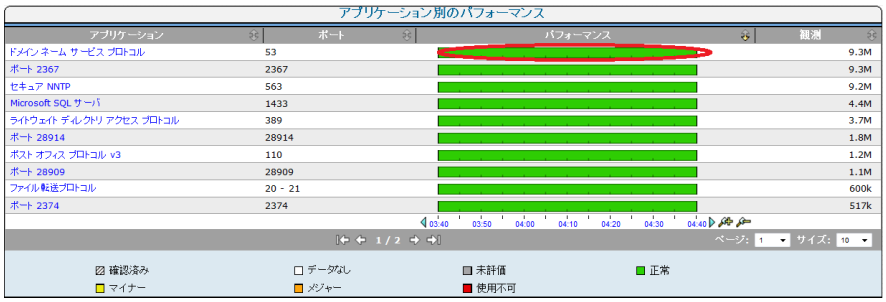
アプリケーションのパフォーマンス問題をトラブルシューティングするには、以下の手順を使用します。 ネットワークまたはサーバに関する問題を調査する場合にも、メトリック、ネットワークまたはサーバ別に限定するリンクをクリックすることで、この同じ手順を使用できます。

会社の本社のユーザが、アプリケーションのパフォーマンス問題をレポートしたとします。

次の手順に従ってください:

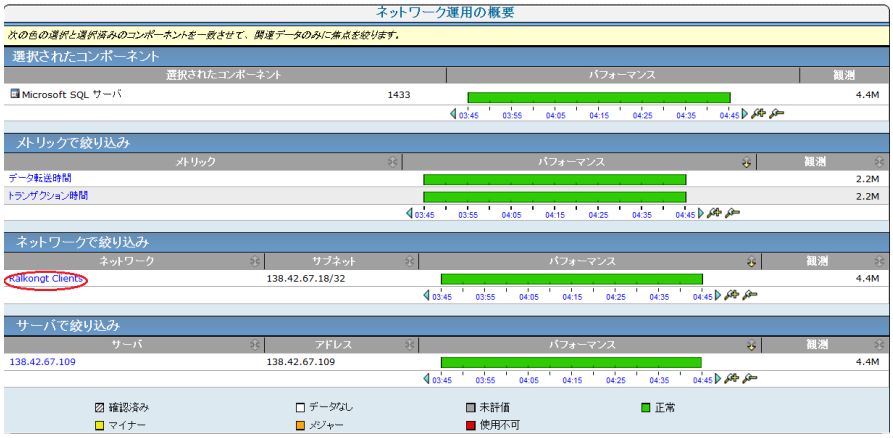
1. ［操作］ページをクリックします。
2. ［表示項目］メニューの［アプリケーション］をクリックします。
3. ［アプリケーション別のパフォーマンス］リストのトップに問題のアプリケーションが表示されたかどうかを確認します。

   アプリケーションがリストのトップに表示されない場合は、より大きなサイズ設定を選択します。アプリケーションがリストに表示されない場合は、管理コンソール がそのアプリケーションを監視していない可能性があります。
4. アプリケーションに関する詳細を表示するには、アプリケーション名の横のパフォーマンス バーをクリックします。



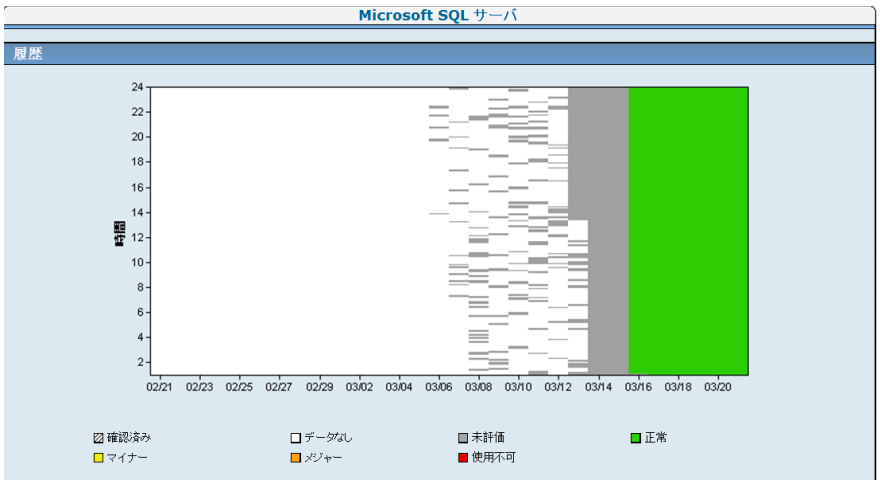
詳細ページには、問題に関連するデータへの移動に使用できる関連のメトリック、ネットワーク、およびサーバが表示されます。

5. （オプション）アプリケーションをホストするネットワークまたはサーバがわかっている場合は、該当するパフォーマンス バーをクリックしてデータの範囲を狭めます。



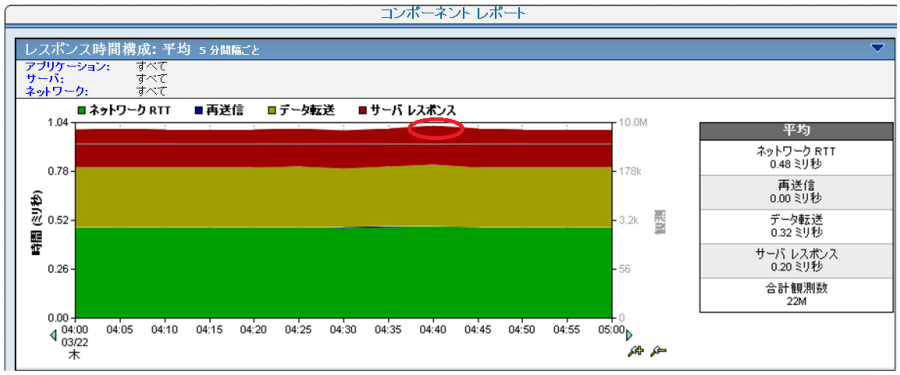
6. ［表示項目］メニュー内の［履歴］をクリックします。

7. ［履歴］ページのアプリケーション履歴を確認し、使用不可またはパフォーマンス低下の系統的なパターンを識別して確認します。



8. ［表示項目］メニューで［パフォーマンス］、［エクスプローラ］の順にクリックして、トラブルシューティングを開始します。
9. より徹底的なトラブルシューティングを実行するには、詳細ページの最上部の［エンジニアリング］リンクをクリックします。

10. レポートされた問題が発生した時間を正確に知るには、［コンポーネント レポート］ページの［レスポンス時間構成: 平均］ビューを確認します。



11. その時点でどのメトリックがパフォーマンス問題の大きな要因になっているかを識別します。 レスポンス時間の増加が発生したメトリックが

    - サーバ レスポンス時間（SRT）の場合は、サーバ レスポンス時間の増加 (P. 170)をトラブルシューティングします。
    - ネットワーク ラウンドトリップ時間（NRTT）の場合は、ネットワーク ラウンドトリップ時間（NRTT）の増加 (P. 176)をトラブルシューティングします。
    - 再送信遅延の場合は、ネットワーク ラウンドトリップ時間(NRTT)の増加 (P. 176)をトラブルシューティングします。
    - データ転送時間の場合は、データ転送時間の増加 (P. 181)をトラブルシューティングします。

メトリックで履歴タイムラインに関して受け入れ可能なパフォーマンスがレポートされた場合は、問題がユーザのコンピュータにある可能性があります。

第 4 章: インシデント ページの使用

このセクションには、以下のトピックが含まれています。

インシデント ページの使用

しきい値を超えるか、または OLA（運用レベル契約）が履行されないごとに、管理コンソールは、情報のレコードまたはインシデントを作成します。 管理コンソール管理者は、管理コンソールがより多くの情報を収集したりパフォーマンス問題について特定のユーザに通知したりするアクションを自動的に起動するインシデント レスポンスを設定することもできます。 インシデント レスポンスに問題解決に役立つ情報が不足している場合は、より多くのデータを収集するためのトラブルシューティング調査を設定することができます。

［インシデント］ページには、連番のインシデントがリスト表示されます。インシデント レポートには、関連するパフォーマンス低下の詳細と共に、24 時間の最大時間ウィンドウが表示されますが、必要な時間が含まれるようにシフトすることもできます。 インシデントのオープンおよびクローズはインシデント作成ルールに従うので、複数のインシデントが連続すると、長期間にわたってパフォーマンスが低下する可能性があります。

管理コンソールは 5 分データを保存する場合には、必ず履歴インシデント レコードを保存します。 5 分データの保存期間の変更の詳細については、「*管理者ガイド*」を参照してください。

インシデント、インシデント レスポンス、および調査

*インシデント*は、パフォーマンスしきい値を超えるときに作成される情報レコードです。 *しきい値*は、受け入れ可能なパフォーマンスの挙動の上限です。これは、すべてのアプリケーションに対してデフォルトで存在します。 管理者は、パフォーマンス変更に対するしきい値の感度を増減することができます。

しきい値を超えると、管理コンソール は、割り当て済みの連続するケース番号を付けてインシデントを作成し、それらのインシデントを［インシデント］ページにレポートします。 管理コンソール 管理者がインシデント レスポンスを設定していて、それらを違反対象のしきい値と関連付けている場合、管理コンソール は 1 つ以上の自動的なレスポンスを起動します。 問題解決に追加の情報が必要な場合は、その問題をトラブルシューティングする調査を起動することができます。

以下の条件に該当する場合は、管理コンソール はインシデントをクローズします。

- 受け入れ可能なパフォーマンスが 1 時間にわたって継続した場合。
- 問題のサーバが保守ウィンドウにある場合。
- 24 時間を経過したインシデント。 問題が解決しない場合、管理コンソール は新規インシデントをオープンします。

管理コンソール が CA PC または CA NPC に登録され、管理コンソール が新しいマイナーまたはメジャーの状態を検出した場合、管理コンソール はインシデントをオープンし、CA PC または CA NPC は対応するイベントをオープンします。

- 管理コンソール インシデントの原因となるマイナーまたはメジャーの状態が 1 時間正常なパフォーマンスを示すと、管理コンソール はそのインシデントをクローズし、CA PC または CA NPC は対応するインシデントをクリアします。 その後、マイナーまたはメジャーのインシデント状態が戻ると、管理コンソール は新規インシデントをオープンし、CA PC または CA NPC は対応するイベントをオープンします。
- 管理コンソール インシデントが 24 時間オープンのままであると、管理コンソール は、その状態に関係なく自動的にインシデントをクローズします。 マイナーまたはメジャーのインシデント状態が引き続き存在する場合、管理コンソール は新規インシデントをオープンし、CA PC または CA NPC は対応するイベントの数を増分します。 それ以外の場合、およそ 10 分の同期遅延の後、CA PC または CA NPC はイベントをクリアします。

管理コンソール がマイナーまたはメジャーのインシデント状態に対して［データなし］を正味 1 時間レポートした場合に、CA PC または CA NPC が、サーバがオフラインの状態で 管理コンソール インシデントと関連付けられたイベントをクリアできるようにするため、CA PC または CA NPC は対応するイベントをクリアします。 サーバが再びオンラインになった後で、管理コンソール が新しいマイナーまたはメジャーの状態を検出した場合、管理コンソール はインシデントをオープンし、CA PC または CA NPC は対応するイベントをオープンします。

CA PC または CA NPC では、ユーザが 管理コンソール インシデントに対応するイベントをクローズすると、管理コンソール 内のインシデント ステータスが［確認済み］に変わります。インシデントの状態が 1 時間の正常なパフォーマンスを示した後、管理コンソール は自動的にそのインシデントをクローズします。

インシデントの表示

管理コンソール は、［インシデント］ページではネットワーク、サーバおよびアプリケーションの連番のインシデントを表示し、［環境管理］ページでは 監視デバイス のインシデントを表示します。

インシデント レポートには、関連するパフォーマンス低下の詳細と共に、24 時間の最大時間ウィンドウが表示されます。 このウィンドウは、必要な時間が含まれるようにシフトできます。 インシデントのオープンおよびクローズはインシデント作成ルールに従うので、複数のインシデントが連続すると、連続する長期間にわたってパフォーマンスが低下する可能性があります。

CA PC または CA NPC に登録されている場合、管理コンソール はそのインシデントを登録済みの CA PC または CA NPC と同期します。

- 管理コンソール でインシデントを確認したら、対応するインシデントのイベント ステータスが CA PC または CA NPC で自動的に更新されます。
- 管理コンソール インシデントの結果であるイベントをイベント マネージャ内で確認すると、管理コンソール では、対応するインシデント ステータスが自動的に更新されます。

CA PC または CA NPC が 管理コンソール インシデントと同期する方法の詳細については、CA PC または CA NPC の製品ドキュメントを参照してください。

注: 5 分データが保存される場合には、必ず履歴インシデント レコードが保存されます。 保存期間は、［環境管理］ページで設定できます。

監視デバイス別のインシデントの表示

監視デバイス インシデントは［環境管理］ページに表示されます。

注: 監視デバイス インシデントを表示するには、ユーザ アカウントに管理者製品権限が必要です。 詳細については、「*管理者ガイド*」を参照してください。

ネットワーク、サーバ、またはアプリケーション別のインシデントの表示

5 分間隔でネットワーク、サーバ、またはアプリケーション メトリックの対応するしきい値を超えると、管理コンソール はネットワークまたはサーバのインシデントをオープンします。 たとえば、［データ転送時間］のしきい値を超えると、管理コンソール はアプリケーションに対してサーバまたはネットワークのインシデントを作成します。

次の手順に従ってください:

1. ［インシデント］ページをクリックしてインシデントのリストを表示します。
2. 目的のインシデントを表示する方法
    1. ［表示項目］メニュー内のオプションを選択し、対応するインシデントを表示します。
    2. 必要なインシデントを表示するために、［設定］をクリックして特定のタイムフレームやネットワークなどのような追加のフィルタ条件を指定します。
    3. インシデントのリストをフィルタするために、以下のオプションから選択します。

        インシデントの状態

        インシデントの状態または目的の状態を指定します。

        最小の重大度

        最小限必要なインシデント重大度と、インシデントの状態が最低限継続する必要がある時間の長さを指定します。[使用不可]が最も高い重大度であることに注意してください。

        表示順

        インシデントのリストの表示オプションを指定します。

インシデントに関連する調査の表示

次の手順に従ってください:

1. ［インシデント］ページをクリックします。
2. ［表示項目］メニュー内の［概要］をクリックします。

   インシデント リストが表示されます。
3. インシデントの詳細を表示するには、インシデント リスト内のリンクをクリックします。

   ［インシデントの詳細］ページが表示されます。
4. 2 番目の［表示項目］メニュー内の［調査］をクリックします。

   インシデントに関連する調査があれば表示されます。

インシデントの詳細の表示

インシデント リストを使用して、ネットワークまたはサーバのインシデント詳細にドリルダウンします。

次の手順に従ってください:

1. ［インシデント］ページをクリックします。
2. ページ上の［表示順］フィルタがインシデント数を表示するように設定されている場合、［インシデント数］列のパフォーマンス バーをクリックしてインシデントのリストを表示します。

   ユーザの選択内容に基づいて、インシデントのリストがフィルタされます。
3. インシデントの詳細を表示するには、インシデント番号をクリックします。

   ［インシデントの詳細］ページが表示されます。
4. メトリック、サーバおよびアプリケーションを選択して情報を限定します。

   管理コンソール は、インシデントの以下の情報をリスト表示します。

   数

   インシデントを識別する一意の数。

   ネットワーク

   ネットワーク関連インシデントの場合は、インシデントのネットワーク ソース。

   サーバ

   サーバ関連のインシデントの場合は、インシデントのサーバ ソース。

   重大度

   インシデントの色分けによる評価 (P. 45)。

   タイムフレーム

   インシデントの合計期間。

   調査

   関連する調査へのリンク。

   ステータス

［オープン］または［クローズ］。

選択されたコンポーネント

コンポーネントを選択して、データを絞り込むことができます。

パフォーマンス バー

問題が存在する箇所を示すために、色分けされたセグメントを使用しています。

観測

観測数。

インシデントの調査

［表示項目］メニューの下の［エクスプローラ］ボタンを使用して、関連するメトリック、影響を受けたメトリック、影響を受けたユーザを表示するか、またはしきい値を編集します。

次の手順に従ってください:

1. ［インシデント］ページをクリックします。
2. ［概要］、［アプリケーション］、［サーバ］または［ネットワーク］をクリックして、選択したコンポーネントのインシデントを表示します。
3. 選択したコンポーネントをクリックして、インシデントの詳細を表示します。

   ［エクスプローラ］ボタンが有効になります。
4. ［表示項目］メニュー下の［エクスプローラ］をクリックします。
5. ［エクスプローラ］ダイアログ ボックスが表示されます。以下の種類があります。

   [メトリック]タブ

   関連するメトリックを表示します。

   影響を受けたメトリック

   影響を受けたメトリックを表示します。

   影響を受けたユーザ

   指定されたタイムフレーム中にアプリケーションにアクセスしたクライアント IP アドレスのリストを表示します。

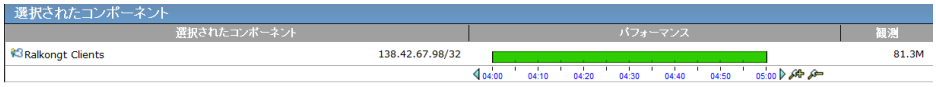
   しきい値の編集

   選択されたメトリックのパフォーマンスしきい値を編集します。

インシデントの確認

インシデントを確認すると、その優先度がレポート内で低下し、ユーザがそのインシデントを確認したことが示されます。 また、レポート内で確認済みのインシデントを未確認状態にすると、インシデントの優先度を上げることができます。

インシデントを確認すると、正時から正時に至るインシデントのライフタイム全体を確認する効果があります。 以下の例では、インシデント詳細ページでタイムラインにハッシュ マークが表示され、14:00 から 16:00 までの間にインシデント ステータスが「確認済み」であることを示しています。



次の手順に従ってください:

1. インシデントの詳細ページで［確認］をクリックします。
2. ［確認の確定］ページ上の以下のいずれかのオプションを選択し、［OK］をクリックします。
   - インシデントを確認状態にする： インシデントを確認済みとしてマークする場合は、このオプションを選択します。
   - インシデントを未確認状態にする： インシデントを未確認状態としてマークする場合は、このオプションを選択します。

インシデントの比較

［比較］ページを使用して、ネットワーク、サーバ、またはアプリケーション全体において、低下の兆候など関連がある可能性のあるパターンを検出します。 詳細を調査するには、特定のネットワーク、サーバまたはアプリケーションをクリックします。 また、関連する調査があるかどうかを確認するには、インシデントの詳細を表示します。

以下を比較します。

ネットワーク インシデント

インシデントに関連するネットワークのパフォーマンスを同様のネットワークに対して比較します。

サーバ インシデント

インシデントに関連するサーバのパフォーマンスを同様のサーバに対して比較します。

次の手順に従ってください:

1. ［インシデント］ページをクリックします。
2. ページ上の［表示順］フィルタがインシデント数を表示するように設定されている場合、［インシデント数］列のパフォーマンス バーをクリックしてインシデントのリストを表示します。

   ユーザの選択内容に基づいて、インシデントのリストがフィルタされます。
3. インシデントの詳細を表示するには、インシデント番号をクリックします。

   ［インシデントの詳細］ページが表示されます。
4. ［表示項目］メニューの［比較］をクリックし、選択されたネットワークまたはサーバのパフォーマンスを、指定されたタイムフレームにおけるすべてのネットワークまたはサーバに対して比較します。

インシデント履歴の表示

現在選択されているインシデントとターゲットが同じである、過去 30 日間に発生したインシデントを表示します。

次の手順に従ってください:

1. ［インシデント］ページをクリックします。
2. ページ上の［表示順］フィルタがインシデント数を表示するように設定されている場合、［インシデント数］列のパフォーマンス バーをクリックしてインシデントのリストを表示します。

   ユーザの選択内容に基づいて、インシデントのリストがフィルタされます。
3. インシデントの詳細を表示するには、インシデント番号をクリックします。

   ［インシデントの詳細］ページが表示されます。
4. ［表示項目］メニュー内の［履歴］をクリックします。

   ［インシデント履歴］リストが表示されます。
5. インシデント番号をクリックして詳細を表示します。

アプリケーション別のネットワーク インシデントおよびサーバ インシデントの表示

アプリケーション別のインシデント レポートは、アプリケーションのネットワーク インシデントとサーバ ンシデントをリスト表示します。

インシデント レポートの詳細には、関連するパフォーマンスの低下が表示され、24 時間の最大時間ウィンドウが設定されています。 このウィンドウは、必要な時間が含まれるようにシフトできます。 インシデントのオープンおよびクローズはインシデント作成ルールに従うので、複数のインシデントが連続すると、連続する長期間にわたってパフォーマンスが低下する可能性があります。

アプリケーション別のインシデント レポートに移動するには、［インシデント］ページで［アプリケーション］をクリックします。

サーバ インシデントの表示

［インシデント］ページには、アプリケーション別にサーバ インシデントがリスト表示されます。インシデント レポートには、関連するパフォーマンス低下の詳細と共に、24 時間の最大時間ウィンドウが表示されます。このウィンドウは、必要な時間が含まれるようにシフトできます。 インシデントのオープンおよびクローズはインシデント作成ルールに従うので、複数のインシデントが連続すると、連続する長期間にわたってパフォーマンスが低下する可能性があります。

［サーバ インシデント］ページに移動するには、［インシデント］ページで［サーバ］をクリックします。

アプリケーション別のネットワーク インシデントの表示

［インシデント］ページには、アプリケーション別にネットワーク インシデントがリスト表示されます。 インシデント レポートには、関連するパフォーマンス低下の詳細と共に、24 時間の最大時間ウィンドウが表示されます。 このウィンドウは、必要な時間が含まれるようにシフトできます。 インシデントのオープンおよびクローズはインシデント作成ルールに従うので、複数のインシデントが連続すると、連続する長期間にわたってパフォーマンスが低下する可能性があります。

［ネットワーク インシデント］ページに移動するには、［インシデント］ページで［ネットワーク］をクリックします。

調査レポートの使用

*調査*は、管理コンソール がインシデント レスポンスの一環として自動的に開始するアクションである場合もあれば、管理者製品権限を持ったユーザによって手動でスケジュールまたは起動されるアクションである場合もあります。 調査のタイプは以下のいずれかになります。

調査タイプ	説明
アプリケーション接続時間	サーバが接続確認応答コードで応答するのにかかる時間を含む、TCP/IP アプリケーション ポートへの接続にかかる時間を算定します。

調査タイプ	説明
パケット キャプチャ	問題が発生しているサーバ、アプリケーション ポート、およびネットワークのみのフィルタによるキャプチャを有効にして、調査します。
SNMP 経由のパフォーマンス	SNMP（簡易ネットワーク管理プロトコル）を使用して収集された、サーバまたはルータのパフォーマンス関連の情報を調査します。
ping レスポンス時間	TCP ping 要求を送信してから ping 応答を受信するまでにかかる時間を測定します。
ping レスポンス時間とパケット サイズの比較	さまざまなサイズの TCP ping 要求の ping 応答（データ パケット）を受信するのにかかる時間を測定します。 さまざまなパケット サイズでの接続不能および過度の遅延を追跡するのに役立ちます。
トレース ルート	遅延とルーティングの問題を検出するために、管理コンソール とエンド ポイントの間のパスおよびすべてのホップを記録します。

調査の表示

調査に関する詳細の表示、レポート設定の変更、または調査の削除を行うには、［調査レポート］を使用します。

次の手順に従ってください:

1. ［インシデント］ページをクリックします。
2. ［調査］をクリックします。

   ［調査レポート］ページが表示されます。
3. インシデントのリストをフィルタする場合は、［設定］をクリックします。
4. 調査結果の詳細を表示するには、タイムスタンプ リンクをクリックします。

調査の起動およびスケジュール

調査をすぐに起動するように設定するか、またはスケジュールした日時に起動するように設定します。

調査を手動で開始する場合は、ポップアップ ブロッカを無効にする必要があります。そうしないと、調査が実行できません。調査を実行しても、調査のステータスを示すポップアップが表示されない場合は、ポップアップ ブロッカがおそらくまだ有効になっているために、調査が実行されていません。

次の手順に従ってください:

1. ［インシデント］ページをクリックします。

   ［表示項目］メニュー内の［調査］をクリックします。
2. ［調査レポート］ページが表示されます。
3. ［表示項目］メニュー内の［起動］をクリックします。

   ［調査タイプ］ページが表示されます。
4. 以下のいずれかのタスクを実行して、調査を起動するか、またはスケジュールします。
   - すぐに起動する場合は、起動する調査タイプの横にある［起動］をクリックします。
   - スケジュールする場合は、スケジュールする調査タイプの横にある［スケジュール］をクリックします。

   選択した調査タイプに応じた［設定］ページが表示されます。 各［設定］ページの詳細については、後続のセクションを参照してください。

アプリケーション接続時間調査

アプリケーション接続時間調査は、サーバが接続確認応答コードで応答するのにかかる時間を含む、TCP/IP アプリケーション ポートへの接続にかかる時間を算定します。

この調査をスケジュールする場合は、通知用に指定するタイム ゾーンも、調査をスケジュールするために使用されます。

［アプリケーション接続時間］調査を起動またはスケジュールするには、以下の設定を指定します。

調査のターゲット

調査するターゲット タイプに基づいて、サーバなどのターゲットを指定します。ターゲットのグループを調査するには、［ターゲット タイプ］リストから［サーバの集約］を選択します。

調査オプション

以下のオプションを指定します。

調査元

調査を起動する 監視デバイス を指定します。サーバと通信できる監視デバイス か、または調査するデバイスを選択します。

アプリケーション

調査するアプリケーションを指定します。

サンプル

調査中に観測するデータ サンプルの数を 1 ～ 10 から選定します。サンプルは 1 つの統計的測定対象です。

タイムアウト（秒）

調査がアプリケーションのタイムアウトを記録するまでに経過する必要のある秒数を 1 ～ 10 から選定します。

通知オプション

調査結果について、指定された電子メール受信者に通知します。 調査は電子メール通知用に指定されたタイム ゾーンを使用してスケジュールされますので注意してください。

スケジュール

調査をスケジュールする場合にのみ、スケジュール オプションが表示されます。 調査を特定日付の特定時刻か、または週単位か月単位で実行するようにスケジュールします。

パケット キャプチャ調査

パケット キャプチャ調査は、問題が発生しているサーバ、アプリケーション ポート、およびネットワークのみをフィルタしてキャプチャします。

この調査をスケジュールする場合は、通知用に指定するタイム ゾーンも、調査をスケジュールするために使用されます。

［パケット キャプチャ］調査を起動またはスケジュールするには、以下の設定を指定します。

調査のターゲット

調査するサーバを指定します。

キャプチャ フィルタ

以下のオプションを指定します。

アプリケーション

キャプチャするアプリケーション トラフィックを指定します。ターゲット サーバ上のアプリケーション トラフィックをすべてキャプチャする場合は、［すべて］をクリックします。 カスタム ポート範囲を指定する場合は、［カスタム アプリケーション］をクリックし、開始および終了のポート番号を指定します。

ネットワーク

ターゲット アプリケーション トラフィックをキャプチャするクライアント ネットワークを指定します。

クライアント ネットワークをすべて指定する場合は［すべて］をクリックし、特定のネットワークを指定する場合は［特定のネットワーク］をクリックします。次に、［ネットワーク］リンクをクリックして、目的のネットワークを選択します。

調査オプション

以下のオプションを指定します。

キャプチャ期間

パケットをキャプチャする最大期間を 30 秒～ 30 分から選定します。

最大ファイル サイズ

パケット キャプチャ ファイルの最大サイズを 10MB ～ 100MB から選定します。

1 パケットあたりのバイト数

CA Standard Monitor でパケットをキャプチャするときに、パケット当たりキャプチャするバイト数を指定します。［ヘッダのみ］から 8192 バイトの間で選択します。［ヘッダのみ］では MAC（第 2 層）、IP（第 3 層）および TCP（第 4 層）のヘッダ情報がキャプチャされることに注意してください。

パケットが CA GigaStor または CA Multi-Port Monitor によってキャプチャされる場合、このオプションは適用不能です。

通知オプション

調査結果について、指定された電子メール受信者に通知します。 調査は電子メール通知用に指定されたタイム ゾーンを使用してスケジュールされますので注意してください。

スケジュール

調査をスケジュールする場合にのみ、スケジュール オプションが表示されます。 調査を特定日付の特定時刻か、または週単位か月単位で実行するようにスケジュールします。

SNMP 経由のパフォーマンス調査

*SNMP 経由のパフォーマンス調査*は、SNMP（簡易ネットワーク管理プロトコル）を使用して、パフォーマンス関連情報をサーバまたはルータに対してクエリします。

この調査をスケジュールする場合は、通知用に指定するタイム ゾーンも、調査をスケジュールするために使用されます。

［SNMP 経由のパフォーマンス］調査を起動またはスケジュールするには、以下の設定を指定します。

調査のターゲット

調査するターゲット タイプに基づいて、サーバなどのターゲットを指定します。ターゲットのグループを調査するには、［ターゲット タイプ］リストから［サーバの集約］を選択します。 パフォーマンス情報をルータに対して SNMP ポーリングするには、管理コンソール 管理者はネットワーク デバイスとしてルータを追加する必要があります。詳細については、「管理者ガイド」を参照してください。

調査オプション

以下のオプションを指定します。

調査元

調査を起動する 監視デバイス を指定します。サーバと通信できる監視デバイス か、または調査するデバイスを選択します。

サンプル期間（秒）

レートを計算するためにサンプル間に待機する時間の長さを 5 ～ 300 秒から選定します。

再試行

レスポンスを取得する試行数を 0 ～ 4 から選定します。

タイムアウト（秒）

管理コンソール によりサーバでタイムアウトと決定されるまでに経過している必要がある時間の長さを 1 ～ 30 秒から選定します。

通知オプション

調査結果について、指定された電子メール受信者に通知します。 調査は電子メール通知用に指定されたタイム ゾーンを使用してスケジュールされますので注意してください。

スケジュール

調査をスケジュールする場合にのみ、スケジュール オプションが表示されます。 調査を特定日付の特定時刻か、または週単位か月単位で実行するようにスケジュールします。

ping レスポンス時間調査

ping レスポンス時間調査は、TCP ping 要求を送信してから ping 応答を受信するまでにかかる時間を測定します。

この調査をスケジュールする場合は、通知用に指定するタイム ゾーンも、調査をスケジュールするために使用されます。

ping レスポンス時間調査を起動またはスケジュールするには、以下の設定を指定します。

調査のターゲット

調査するターゲット タイプに基づいて、サーバなどのターゲットを指定します。ターゲットのグループを調査するには、［ターゲット タイプ］リストから［サーバの集約］を選択します。

調査オプション

以下のオプションを指定します。

調査元

調査を起動する 監視デバイス を指定します。サーバと通信できる監視デバイス か、または調査するデバイスを選択します。

パケット サイズ

テスト パケットのバイトでのサイズを 32 ～ 8192 から選択します。

サンプル

調査中に観測するデータ サンプル数を 1 ～ 10 から選択します。サンプルはただ 1 つの統計的測定対象です。

タイムアウト（秒）

サーバでタイムアウトと決定されるまでに経過している必要がある秒数を 1 ～ 10 から選択します。

通知オプション

調査結果について、指定された電子メール受信者に通知します。 調査は電子メール通知用に指定されたタイム ゾーンを使用してスケジュールされますので注意してください。

スケジュール

調査をスケジュールする場合にのみ、スケジュール オプションが表示されます。 調査を特定日付の特定時刻か、または週単位か月単位で実行するようにスケジュールします。

ping レスポンス時間とパケット サイズの比較調査

ping レスポンス時間とパケット サイズの比較調査は、さまざまなサイズの TCP ping 要求（データ パケット）に対する ping 応答を受信するのにかかる時間を測定します。 さまざまなパケット サイズでの接続不能および過度の遅延を追跡するのに役立ちます。

ping レスポンス時間とパケット サイズの比較調査は、最小、最大、平均のパケット ラウンドトリップ時間に関するレポートを作成します。 他のタイプの調査と異なり、管理コンソール は、インシデントに対してこの調査を自動的に起動することはありません。

この調査をスケジュールする場合は、通知用に指定するタイム ゾーンも、調査をスケジュールするために使用されます。

ping レスポンス時間とパケット サイズの比較調査を起動またはスケジュールするには、以下の設定を指定します。

調査のターゲット

調査するターゲット タイプに基づいて、サーバなどのターゲットを指定します。ターゲットのグループを調査するには、［ターゲット タイプ］リストから［サーバの集約］を選択します。

調査オプション

以下のオプションを指定します。

調査元

調査を起動する 監視デバイス を指定します。サーバと通信できる監視デバイス か、または調査するデバイスを選択します。

最大パケット サイズ

調査するパケットの最大サイズを 512 ～ 8192 バイトから選択します。

サンプリング タイプ

パケット サイズをチェックするオプションを指定します。

- 連続。 指定した最大パケット サイズまでの全パケット サイズをチェックします。このオプションはより多くのサンプルを必要とします。
- 不連続。 パケット サイズの範囲がより小さい、より少数のサンプルの範囲をカバーします。

各サイズのサンプル

各サイズのサンプル数を 1 ～ 10 から選択します。

タイムアウト（秒）

サーバでタイムアウトと決定されるまでに経過している必要がある秒数を 1 ～ 10 から選択します。

通知オプション

調査結果について、指定された電子メール受信者に通知します。 調査は電子メール通知用に指定されたタイム ゾーンを使用してスケジュールされますので注意してください。

スケジュール

調査をスケジュールする場合にのみ、スケジュール オプションが表示されます。 調査を特定日付の特定時刻か、または週単位か月単位で実行するようにスケジュールします。

トレース ルート調査

トレース ルート調査は、遅延とルーティングの問題を検出するために、管理コンソール とエンド ポイントの間のパスおよびすべてのホップを記録します。

この調査をスケジュールする場合は、通知用に指定するタイム ゾーンも、調査をスケジュールするために使用されます。

トレース ルート調査を起動またはスケジュールするには、以下の設定を指定します。

調査のターゲット

調査するターゲット タイプに基づいて、サーバなどのターゲットを指定します。ターゲットのグループを調査するには、［ターゲット タイプ］リストから［サーバの集約］を選択します。

調査オプション

以下のオプションを指定します。

調査元

調査を起動する 監視デバイス を指定します。サーバと通信できる監視デバイス か、または調査するデバイスを選択します。

プロトコル

トレース ルート調査に使用するプロトコルを、ICMP または TCP のいずれかから選定します。 ICMP と指定された TCP ポートの間の traceroute のパフォーマンスが変動するただ 1 つの場合は、QoS が明示的に一方を他方より優先している場合です。 このような場合は、TCP （ネットワーク ルータによって真のアプリケーション トラフィックとしてもマークされている場合）を使用することをお勧めします。 ICMP は、セキュリティ上の理由でブロックされる可能性があるため、指定されたアーキテクチャ内を通過することを許可されている場合に限り、一般的に使用され、受け入れられています。

パケット サイズ

調査するパケットのサイズを 32 ～ 8192 バイトから選定します。

再試行

レスポンスを取得する試行数を 1 ～ 4 から選定します。

ルート検索

選択したターゲットに対して追加のルートを検索する試行数を 0 ～ 20 から選定します。

タイムアウト（秒）

サーバでタイムアウトと決定されるまでに経過している必要がある秒数を 1 ～ 10 から選定します。

SNMP を介したルータの調査

各ネットワーク デバイスに対してパフォーマンス詳細の SNMP クエリを実行するかどうか指定します。 管理コンソール へのネットワーク デバイスの追加の詳細については、「管理者ガイド」を参照してください。

通知オプション

調査結果について、指定された電子メール受信者に通知します。 調査は電子メール通知用に指定されたタイム ゾーンを使用してスケジュールされますので注意してください。

スケジュール

調査をスケジュールする場合にのみ、スケジュール オプションが表示されます。 調査を特定日付の特定時刻か、または週単位か月単位で実行するようにスケジュールします。

スケジュールされた調査の削除

手動でスケジュールされた調査の使用が終了した場合は、その調査を削除します。 スケジュールされた調査を削除しても、その調査レポートは削除されません。

次の手順に従ってください:

1. ［インシデント］ページをクリックします。
2. ［表示項目］メニュー内の［調査］、［起動］をクリックします。

   ［調査タイプ］ページが表示されます。
3. スケジュールされた調査を表示するには、調査タイプを展開します。
4. 削除対象となるスケジュールされた調査の横にある をクリックします。

   調査が削除されます。

第 5 章: 管理ページの使用

このセクションには、以下のトピックが含まれています。

はじめに

［管理］ページで［パフォーマンス スコアカード］および［OLA］（運用レベル契約）を表示して、時系列でのアプリケーション パフォーマンスを確認します。

OLA レポートは、パフォーマンス向上に注力するのに役立ちます。これらの領域を変更すると、OLA レポートの内容が改善されるのを確認することができます。

管理コンソール には、2 つのレベルの OLA レポートが含まれています。

- アプリケーション別に OLA コンプライアンスを要約するエグゼクティブ レポート
- 観測の OLA しきい値割合、結果および数に関する情報が含まれる詳細レポート

パフォーマンス スコアカードの使用

パフォーマンス スコアカードは、企業の毎月のアプリケーション パフォーマンスを示します。 管理コンソール は、以下の色分けを使用してパフォーマンスを評価します。

- 未評価（グレー）
- 正常（緑）
- マイナー（黄色）
- メジャー（オレンジ）

管理コンソール は、パフォーマンス評価を観測数の順に並べ替えます。

次の手順に従ってください:

1. ［管理］ページをクリックします。
2. ［表示項目］メニューの［パフォーマンス スコアカード］をクリックします。

   ［アプリケーション リスト］ページが表示されます。
3. （オプション）フィルタ オプションなどのレポート設定を変更する場合は、［設定］をクリックします。
4. 色分けされたパフォーマンス バーをクリックするか、または［アプリケーション リスト］内のアプリケーション名をクリックして、ネットワーク別のアプリケーション詳細の表示 (P. 90)を行います。

詳細情報:

レポート ページの電子メール送信 (P. 157)
レポート ページの印刷 (P. 157)
レポートのファイルへのエクスポート (P. 155)

時間別のアプリケーションの詳細の表示

次の手順に従ってください:

1. ［管理］ページをクリックします。
2. ［表示項目］メニュー上の［パフォーマンス スコアカード］をクリックします。

   ［アプリケーション リスト］ページが表示されます。
3. （オプション）フィルタ オプションなどのレポート設定を変更する場合は、［設定］をクリックします。
4. アプリケーション名またはパフォーマンスのリンクをクリックして、パフォーマンス詳細を表示します。
5. 3 番目の［表示項目］メニュー上の［時間］をクリックして、時間別にアプリケーションの詳細を表示します。
6. ［表示順］リスト内で［観測］または［割合］順での表示を選択します。
7. ［詳細］をクリックして、［エンジニアリング］ページの関連するコンポーネント レポートを表示します。

ネットワーク別のアプリケーションの詳細の表示

次の手順に従ってください:

1. ［管理］ページをクリックします。
2. ［表示項目］メニュー上の［パフォーマンス スコアカード］をクリックします。

   ［アプリケーション リスト］ページが表示されます。
3. （オプション）レポート設定を変更する場合は、［設定］をクリックします。
4. アプリケーション名またはパフォーマンスのリンクをクリックして、どのネットワークがそのピアと同じ方法で実行されていないかに関する詳細を取得します。
5. 3 番目の［表示項目］メニュー上の［ネットワーク］をクリックして、ネットワーク別にアプリケーションの詳細を表示します。
6. リストをフィルタする場合は、［表示順］リスト内のオプションをクリックします。
   - ネットワーク（パフォーマンスあり）
   - ネットワーク（平均あり）
   - ネットワーク タイプ（パフォーマンスあり）
   - ネットワーク タイプ（平均あり）
7. ［詳細］をクリックして、［エンジニアリング］ページのネットワーク別のパフォーマンス レポートを表示します。

サーバ別のアプリケーションの詳細の表示

次の手順に従ってください:

1. ［管理］ページをクリックします。
2. ［表示項目］メニュー上の［パフォーマンス スコアカード］をクリックします。
3. オプションでレポート設定を変更するには、［アプリケーション リスト］ページの［設定］をクリックします。
4. アプリケーション名またはパフォーマンスのリンクをクリックして、どのサーバがそのピアと同じ方法で実行されていないかに関する詳細を取得します。
5. 3 番目の［表示項目］メニュー上の［サーバ］をクリックして、サーバ別に詳細を表示します。
6. ［表示順］リストで、［サーバ（パフォーマンスあり）］または［サーバ（平均あり）］の表示を選択します。
7. ［詳細］をクリックして、［エンジニアリング］ページのサーバ別のパフォーマンス レポートを表示します。

運用レベル契約の使用

OLA（運用レベル契約）レポートは、ネットワークおよびアプリケーションのエンド ユーザが受けるサービスのパフォーマンスを追跡し、OLA 仕様が達成される頻度を示します。 パフォーマンス OLA と可用性 OLA レポートを参照することで、ユーザが体験した改善された点、利点および問題点を自分で確認および評価することが可能になります。

データを追跡し、OLA に違反している場所を識別するために時間、ネットワークまたはサーバ別に情報を表示するには、［環境管理］ページで設定する OLA 定義を使用します。 ネットワークが OLA を履行しているかどうかを迅速に測定できます。 履行していない場合は、［エンジニアリング］ページのリンクをクリックし、コンポーネント ビュー、パフォーマンス マップ、またはアプリケーションおよびサーバの可用性タイムライン レポートを表示して、問題の場所を特定します。 ［インシデント］ページを使用して、何がパフォーマンス問題を引き起こしているかを調査します。

管理コンソール 管理者は、パフォーマンス OLA と可用性 OLA を設定することができます。 OLA を設定するには、以下のガイドラインに従います。

- 管理コンソール 管理者は、パフォーマンス OLA を設定する場合、事前にネットワーク タイプを定義する必要があります。これは、パフォーマンス OLA が定義済みネットワーク タイプ別に適用されるためです。ネットワーク タイプの定義の詳細については、「*管理者ガイド*」を参照してください。
- 管理コンソール 管理者は、可用性 OLA を設定する場合、自分が OLA しきい値を設定しているアプリケーションおよびサーバに対して、可用性監視を事前に有効にする必要があります。 詳細については、「管理者ガイド」を参照してください。

運用レベル管理の説明

OLM （Operational Level Management： 運用レベル管理）には、ビジネスの優先度に従って受け入れ可能なコストですべての IT ユーザに適切なレベルのサービスが提供されるようにする、しっかりしたプロアクティブなメソドロジおよび手順が含まれます。 OLA（Operational Level Agreement： 運用レベル契約）レポートは、必要なサービス レベルが履行されているかどうかを明らかにします。

OLA は以下のメトリックに関して設定します。

- サーバ レスポンス時間。これは、データ センターのパフォーマンスを測定します。
- ネットワーク ラウンドトリップ時間。これは、ネットワーク インフラストラクチャのパフォーマンスを測定します。
- トランザクション時間。これは、アプリケーションのエンドツーエンド パフォーマンスをキャプチャします。

［管理］ページに以下のタイプのレポートが表示されます。

- パフォーマンス OLA レポート。これは、アプリケーションが OLA の目標を達成しているかどうかを示します。
- 可用性 OLA レポート。これは、アプリケーションの可用性の目標に対する大まかなコンプライアンス、履行度を示します。 このサマリ レポート内のリンクをクリックして、日単位および 1 時間ごとの詳細にアクセスすることができます。

効果的に OLA を導入するには、OLA の定義、コンプライアンスの監視、パフォーマンスの向上、および、OLA 向上およびパフォーマンス向上の意識を高めるための、低レベルの OLA の詳細化から成るプロセスを循環的に行う必要があります。

静的なしきい値に対する OLA を監視するには、管理コンソール を使用します。 営業時間中、ミッション クリティカルなアプリケーションの運用レベルへのコンプライアンスを監視できます。 管理コンソール 管理者が OLA を設定する際には、定期保守および他の計画された不定期の使用期間は OLA 監視から除外する必要があります。 OLA の設定の詳細については、「管理者ガイド」を参照してください。

OLA を監視するときは、ネットワーク メトリックからデータ センター メトリックを分けます。 すべてのメトリックがすべてのネットワークに対して意味があるとは限りません。たとえば、バックエンド アプリケーションでは、ネットワーク ラウンドトリップ時間を参照する必要はありません。OLA しきい値を選択して一時的な急上昇または急低下を除外する場合は、現在のネットワーク パフォーマンスの長期的なビューを使用します。OLA から特定のネットワーク タイプを除外するには、それらのネットワーク タイプを無効にします。

OLA レポートの表示

OLA レポートを表示するときは、意味のあるタイムフレームを指定します。以下のタイムフレームをお勧めします。

タイムフレーム	説明
日単位	詳細、短期のトラブルシューティング、IT 部門向け、技術的コンテンツ。
週単位	異常またはトレンドの追加詳細を含むサマリ。これも IT 部門向け。
月単位	ビジネス ユニットおよび経営管理のサマリ。
四半期単位	コンプライアンスを含む広範な運用レベル情報。計画への入力として使用される。

通常 OLA 違反は以下の領域の 1 つに起因すると考えることができます。

- 時間。つまり、特定の時刻または曜日
- ユーザ グループ。たとえば、VPN ユーザ ネットワーク
- サーバ。たとえば、Web サーバ 2 および 5

パフォーマンス詳細 OLA レポートの使用

パフォーマンス詳細 OLA レポートにはアプリケーション名、OLA 1 および 2 の結果、OLA 1 および 2 の割合、ならびに観測数が含まれます。パフォーマンス OLA を設定する前に、ネットワーク タイプを追加します。パフォーマンス OLA は定義済みのネットワーク タイプに適用されます。

パフォーマンス OLA リストの使用

パフォーマンス OLA リストには、管理コンソールによって監視されている現在のアプリケーションが表示され、先月のアプリケーションのコンプライアンス メトリックについての特定の評価を示します。

次の手順に従ってください:

1. ［管理］ページをクリックします。
2. ［表示項目］メニューの［パフォーマンス詳細 OLA］をクリックします。

   ［パフォーマンス OLA リスト］が表示されます。
3. そのパフォーマンス OLA の詳細を表示するには、アプリケーションをクリックします。

   OLA レポートでは、✔ はそのアプリケーションが設定済みのパフォーマンス OLA に適合していることを示し、❗ は適合していないことを示します。
4. アプリケーションが OLA に適合しない場合は赤い感嘆符が表示されます。 詳細情報を表示するには、以下の手順に従います。
   - 1 時間ごとの詳細を表示するには、アプリケーションの時間リンクをクリックします。
   - ［エンジニアリング］ページから使用可能な詳細レポートを表示するには、  をクリックします。
5. OLA のコンプライアンスの詳細をネットワークまたはネットワークタイプ別にフィルタするには、［表示順］をクリックします。

[パフォーマンス詳細 OLA]の[時間別]レポートの使用

次の手順に従ってください:

1. ［管理］ページをクリックします。
2. ［表示項目］メニューの［パフォーマンス詳細 OLA］をクリックします。

   ［パフォーマンス OLA リスト］が表示されます。
3. アプリケーションをクリックします。

   ［パフォーマンス詳細 OLA］の［時間別］レポートのデフォルト表示は先月の日単位表示です。 このレポートには、先月の毎日の結果が表示され、OLA 定義に対する違反が発生した日を明示します。
4. （オプション）毎時間に報告された特定の違反および観測データを表示する［1 時間ごとのビュー］に移動するには、アプリケーションの［日単位表示］内の個々のデータをクリックします。
5. アプリケーション データを表示する別のメトリックを選択するには、ページの最上部にある［設定］をクリックします。
6. コンポーネント レポートを参照するには  をクリックします。

[パフォーマンス詳細 OLA]の[ネットワーク別]レポートの使用

次の手順に従ってください:

1. ［管理］ページをクリックします。
2. ［表示項目］メニューの［パフォーマンス詳細 OLA］をクリックします。

   ［パフォーマンス OLA リスト］が表示されます。
3. アプリケーションをクリックします。
4. ［表示項目］メニューの［ネットワーク］をクリックします。

   ［パフォーマンス詳細 OLA］の［ネットワーク別］レポートでは、アプリケーションに対して設定されたしきい値に違反しているクライアントを迅速に特定できます。リストには、IP アドレスとサブネット マスク別に並べ替えられたクライアントの論理グループが表示されます。

   アプリケーションをトラブルシューティングするときにこのレポートを使用して、パフォーマンスの問題が発生したクライアントまたはクライアント グループに移動します。
5. ［表示順］ボックス内の［ネットワーク］または［ネットワーク タイプ］を選択します。

   レポートがリフレッシュされ、すべてのエントリの違反データが表示されます。
6. ネットワーク データを表示する別のメトリックを選択するには、ページ最上部の［設定］をクリックします。
7. ネットワーク別のパフォーマンス レポート表示するには、  をクリックします。

[パフォーマンス詳細 OLA]の[サーバ別]レポートの使用

次の手順に従ってください:

1. ［管理］ページをクリックします。
2. ［表示項目］メニューの［パフォーマンス詳細 OLA］をクリックします。

   ［パフォーマンス OLA リスト］が表示されます。
3. アプリケーションをクリックします。
4. ［表示項目］メニューの［サーバ］をクリックします。

   ［パフォーマンス詳細 OLA］の［サーバ別］レポートには、アプリケーション OLA に違反しているサーバが表示されます。このレポートを使用して、パフォーマンスの問題が発生したサーバ（複数可）に迅速に移動します。
5. サーバ データを表示する別のメトリックを選択するには、ページ最上部の［設定］をクリックします。
6. サーバ別のパフォーマンス レポート表示するには  をクリックします。

パフォーマンス エグゼクティブ OLA レポートの使用

パフォーマンス エグゼクティブ OLA レポートには、アプリケーション名とインジケータが表示され、コンプライアンスまたは違反が示されます。

パフォーマンス エグゼクティブ OLA リストの使用

パフォーマンス エグゼクティブ OLA レポートは、高レベル サマリ レポートで、最低限の詳細情報が提示されます。このレポートは、設定可能な OLA 条件に応じた OLA コンプライアンス ステータスに重きが置かれています。

次の手順に従ってください:

1. ［管理］ページをクリックします。
2. ［パフォーマンス エグゼクティブ OLA］をクリックします。

   ［パフォーマンス OLA エグゼクティブ リスト］が表示されます。

   このレポートでは、✔ は設定されたパフォーマンス OLA にアプリケーションが適合したことを示します。❗ は、適合しなかったことを示します。
3. 詳細を表示するには、アプリケーションをクリックします。

［パフォーマンス エグゼクティブ OLA］の［サマリ］の使用

［パフォーマンス エグゼクティブ OLA］の［サマリ］レポートは、特定のアプリケーションの高レベル サマリ レポートで、最低限の詳細情報が提示されます。 このレポートは、設定する OLA 条件に応じた OLA コンプライアンス ステータスに重きが置かれています。

次の手順に従ってください:

1. ［管理］ページをクリックします。
2. ［パフォーマンス エグゼクティブ OLA］をクリックします。

   ［パフォーマンス OLA エグゼクティブ リスト］が表示されます。

   このレポートでは、✔ は設定されたパフォーマンス OLA にアプリケーションが適合したことを示します。❗ は、適合しなかったことを示します。
3. サマリの詳細を表示するには、アプリケーションをクリックします。
4. 時間、ネットワークまたはサーバ別に OLA の結果を日単位表示で表示するには、  をクリックします。

可用性詳細 OLA レポートの使用

可用性 OLA を設定する前に、OLA のしきい値を設定するアプリケーションおよびサーバの可用性の監視を有効にします。

可用性 OLA リストの使用

可用性 OLA リストには、OLA 定義、実行中のアプリケーションとサーバ、時間の割合、およびそれらのアプリケーションおよびサーバが OLA 条件に適合しているかどうかについての特定の情報が表示されます。 ［可用性 OLA リスト］から、［可用性 OLA 定義］の［日単位表示］または［可用性 OLA 定義］の［サーバ別］レポートを表示して、OLA 条件を設定します。

可用性 OLA レポートに移動するには、［管理］ページで［可用性詳細 OLA］をクリックします。

OLA レポートでは、 はそのアプリケーションが設定済みの可用性 OLA に適合していることを示し、 は適合していないことを示しています。

可用性 OLA 定義の日単位表示

ユーザ定義済みアプリケーションの可用性 OLA を表示し管理します。

次の手順に従ってください:

1. ［管理］ページをクリックします。
2. ［表示項目］メニューの［可用性詳細 OLA］をクリックします。

   ［可用性 OLA リスト］が表示されます。
3. ［可用性 OLA 定義］の［日単位表示］を表示するには、アプリケーションのリンクをクリックします。 ［日単位表示］には、時間ごとのアプリケーション可用率とダウンタイム期間が表示されます。
4. 1 時間ごとの詳細を表示するには、アプリケーションの時間リンクをクリックします。
5. アプリケーションの可用性時系列レポートを表示するには、 をクリックします。

可用性 OLA 定義のサーバ別表示

次の手順に従ってください:

1. ［管理］ページをクリックします。
2. ［表示項目］メニューの［可用性詳細 OLA］をクリックします。

   ［可用性 OLA リスト］が表示されます。
3. ［可用性 OLA 定義］の［日単位表示］を表示するには、アプリケーションのリンクをクリックします。
4. ［表示項目］メニューの［サーバ］をクリックします。

   ［可用性 OLA 定義］の［サーバ別］レポートには、ダウンタイム継続時間を含め、サーバ別にアプリケーションの可用性が表示されます。
5. 可用性時系列レポートを表示するには、  をクリックします。

可用性エグゼクティブ OLA レポートの使用

可用性エグゼクティブ OLA レポートは、OLA 条件へのアプリケーションおよびサーバのコンプライアンスについての高レベル サマリを提供します。

可用性 OLA エグゼクティブ リストの使用

可用性 OLA エグゼクティブ リストは、動作中のアプリケーションとサーバが OLA 条件に適合しているかどうかを通知する高レベル サマリ レポートです。

［可用性 OLA エグゼクティブ リスト］に移動するには、［管理］ページ上で［可用性エグゼクティブ OLA］をクリックします。 OLA 定義のサマリ レポートを表示するには、アプリケーションのリンクをクリックします。

可用性 エグゼクティブ OLA のサマリ表示

次の手順に従ってください:

1. ［管理］ページをクリックします。
2. ［可用性エグゼクティブ OLA］をクリックします。

   ［可用性 OLA エグゼクティブ リスト］が表示されます。
3. ［可用性 OLA エグゼクティブ サマリ］を表示するには、サーバ リンクをクリックします。

   サマリにはサーバ可用率が表示されます。
4. サマリ レポートの［日単位表示］を表示するには、  をクリックします。

第 6 章: [エンジニアリング]ページの使用

［エンジニアリング］ページを使用して、設定されているネットワーク、サーバ、およびアプリケーションに関する詳細なパフォーマンス メトリックを表示およびレポートすることができます。 ［エンジニアリング］ページから使用可能なパフォーマンスや可用性に関するレポートを使用すると、ネットワーク上で最も低速なアプリケーションをすぐに特定できます。

このセクションには、以下のトピックが含まれています。

パフォーマンス マップの使用

パフォーマンス レポートのページは、デフォルトで［エンジニアリング］ページに表示されます。 パフォーマンス マップには、アプリケーションごとにトランザクション時間別に並べられた最も遅いネットワーク、サーバ、およびアプリケーションが水平棒グラフを使用して表示されます。その項目の詳細レポートを表示するには、グラフ内の項目をクリックします。

パフォーマンス レポートのナビゲート

［エンジニアリング］ページの［表示項目］メニューで、［パフォーマンス］をクリックしてからパフォーマンス レポートをクリックします。

ネットワーク

パフォーマンスが最低のネットワークの詳細と共にネットワーク マップ別のパフォーマンスが最上部に表示されます。パフォーマンス詳細レポートを表示するには、ネットワークをクリックします。

サーバ

パフォーマンスが最低のネットワークの詳細と共にサーバ マップ別のパフォーマンスが最上部に表示されます。 パフォーマンス詳細レポートを表示するには、サーバをクリックします。

アプリケーション

パフォーマンスが最低のネットワークの詳細と共にアプリケーション マップ別のパフォーマンスが最上部に表示されます。パフォーマンス詳細レポートを表示するには、アプリケーションをクリックします。

WAN に最適化されたアプリケーションの場合、ネットワーク セグメントを検索することにより最適化された各ネットワーク セグメントのパフォーマンスを表示できます。 管理コンソール はネットワーク セグメントをアプリケーション名に追加します。たとえば、SMTP [Client]、SMTP [WAN]、SMTP [Server] のようになります。

ヒント： 同じアプリケーションについて最適化されたパフォーマンス データと最適化されていないパフォーマンス データを分析する場合、データはデータ センターのローカル ユーザから送信されるため、最適化されていないアプリケーションのレスポンス時間のほうが速いことを覚えておいてください。

詳細:

レポート ページの電子メール送信 (P. 157)
レポート ページの印刷 (P. 157)
レポート設定の変更 (P. 41)
グラフからテーブルへのレポート形式の変更 (P. 44)
レポート ページの CSV ファイルへのエクスポート (P. 155)
表示の CSV ファイルへのエクスポート (P. 156)
表示の XML ファイルへのエクスポート (P. 156)
ネットワーク マップの使用 (P. 105)

ネットワーク マップの使用

ネットワーク マップでは、1 つのアプリケーション当たりのトランザクション時間に基づいて並べられ、最も遅いネットワークが示されます。ネットワークのパフォーマンス マップは、最も遅いネットワークの表示に水平棒グラフを使用します。

［ネットワーク別のパフォーマンス］マップを表示するには、［エンジニアリング］ページをクリックし、［表示項目］メニューで［パフォーマンス］-［ネットワーク］をクリックします。［ネットワーク別のパフォーマンス］レポートでネットワークをクリックすると、詳細レポートが表示されます。

ネットワークは、不定距離の回線によって接続された転送ポイントとバッファから構成されています。転送ポイントおよびバッファ内に輻輳が発生します。アプリケーションによってネットワークに多大な負荷がかかると、ユーザはパフォーマンスの低下に気づきます。

ネットワーク遅延

以下の等式でネットワーク遅延を数値化します。
［シリアル化遅延］ + ［キュー遅延］ + ［ルーティング/スイッチング遅延］ + ［距離遅延］ + ［プロトコル遅延］ = ネットワーク遅延

各項目の説明：

シリアル化遅延

一度に 1 フレームで 1 ビットを転送するのに必要な時間です。

キュー遅延

ネットワーク インターフェース上の転送までネットワーク バッファ内でフレームが待機する時間です。 キュー遅延は帯域幅/使用率の関数です。

ルーティング/スイッチング遅延

ネットワーク ノードがフレーム/パケットの次のホップを決定し、送信インターフェースへそのフレームを転送するのに必要な時間です。パス、ノード リソース、およびポリシー（ACL など）の切り替えによる影響を受ける可能性があります。

距離遅延

光学または電気的なシグナルが 2 つのエンド ポイント間のパスを移動する時間です。

プロトコル遅延

搬送波感知多重アクセス/衝突検出方式（レガシ イーサネットの CSMA/CA）および 搬送波感知多重アクセス/衝突回避方式（CSMA/CA)、および送信要求/受信準備完了（RTS/CTS、無線アクセス ポイント）、または最大 200 ミリ秒までの遅延確認応答（TCP）など、ネットワーク関連通信アルゴリズムによって引き起こされた遅延時間です。

レポートのワークフロー

次の手順に従ってください：

1. ［エンジニアリング］ページをクリックします。
2. ［表示項目］メニューの［パフォーマンス］、［ネットワーク］をクリックします。
3. ［ネットワーク別のパフォーマンス］テーブル内のネットワークをクリックします。
4. ［コンポーネント］をクリックし、ネットワーク ラウンドトリップ時間レポートと再送信遅延レポートなどのプライマリ インジケータを参照します。［セッション数］をクリックし、接続セットアップ時間レポートを確認します。
5. ［トラフィック］をクリックし、データ ボリュームおよびデータ転送速度のレポートを確認して、セカンダリ インジケータを表示します。［セッション数］をクリックし、TCP/IP セッション レポートを確認します。

サーバ マップの使用

サーバ マップでは、1 つのアプリケーション当たりのトランザクション時間によって並べられ、最も遅いサーバが示されます。 サーバのパフォーマンス マップは、最も遅いサーバの表示に水平棒グラフを使用します。

［サーバ別のパフォーマンス］マップを表示するには、［エンジニアリング］ページをクリックし、［表示項目］メニューで［パフォーマンス］-［サーバ］をクリックします。 ［サーバ別のパフォーマンス］レポートでサーバをクリックすると、詳細レポートが表示されます。

パフォーマンス インジケータ

サーバは以下のサブシステムから構成されます。

- CPU
- メモリ
- I/O （ネットワークとディスク）

アプリケーションによってサブシステムに多大な負荷がかかると、ユーザはパフォーマンスの低下に気づきます。

CPU 使用率の増加は多くのトランザクション、大きなクエリ、監視されているアプリケーションと無関係な他のプロセス、TCP チェックサム計算などを示唆している可能性があります。

メモリ使用率の増加はメモリ内に常駐する大きなデータ セット、ユーザ数またはセッション数の増加、プロセス数の増加、メモリが割り当てられていないこと（メモリ漏洩）などを示す場合があります。

I/O の増加は、ディスクまたはネットワークへのデータ書き込みの増加、ユーザ数またはセッション数、ディスク間のメモリ ページの増加などを示します。

レポートのワークフロー

次の手順に従ってください：

1. ［エンジニアリング］ページをクリックします。
2. ［表示項目］メニューの［パフォーマンス］、［サーバ］をクリックします。
3. ［サーバ別のパフォーマンス］テーブル内のサーバをクリックします。
4. ［コンポーネント］をクリックしサーバ レスポンス時間レポートを確認して、プライマリ インジケータを表示します。［セッション数］をクリックし、接続セットアップ時間レポートを確認します。
5. ［トラフィック］をクリックし、データ ボリュームおよびデータ転送速度のレポートを確認して、セカンダリ インジケータを表示します。［セッション数］をクリックし、未対応の TCP/IP セッション リクエスト レポートと TCP/IP セッション レポートを確認します。

アプリケーション マップの使用

［エンジニアリング］ページの［アプリケーション別のパフォーマンス］マップは、最も遅いアプリケーションの表示に水平棒グラフを使用します。そのレポートには、サーバあたりの観測数が表示されます。 選択したアプリケーションの詳細レポートを表示するには、アプリケーション リンクをクリックします。

通常、アプリケーションは 2 つの部分から構成されます。

- サーバ（複数可）上で実行するデーモン
- ユーザのコンピュータ上で実行するクライアント

ネットワーク転送に最適化されていないアプリケーションはパフォーマンスの低下の原因となる場合があります。たとえば、ネットワーク間でデータを何度もやりとりしたり、永続的な TCP セッションではなく複数の連続 TCP セッションを開いたり、高レイテンシ WAN リンクに小さなアプリケーション/TCP ウィンドウ サイズを使用したりする場合があります。

次の手順に従ってください:

1. ［エンジニアリング］ページをクリックします。
2. ［表示項目］メニューの［パフォーマンス］、［アプリケーション］をクリックします。
3. ［アプリケーション別のパフォーマンス］テーブル内のアプリケーションをクリックします。
4. ［コンポーネント］をクリックしデータ転送時間レポートを確認して、プライマリ インジケータを表示します。 ［レスポンス サイズ］をクリックし、レスポンス サイズ別データ転送時間レポートを確認します。
5. ［トラフィック］をクリックし、データ ボリュームおよびデータ転送速度のレポートを確認して、セカンダリ インジケータを表示します。［セッション数］をクリックし、TCP/IP セッション レポートを確認します。

パフォーマンス詳細レポートの表示

［エンジニアリング］ページでは、管理コンソール は 5 分間のデータを使用してビューを作成し、そのデータを平均して以下のように 15 分間のデータを作成します。

- 5 分間データは最大 8 時間までレポートできます。
- 5 分間データは最大 24 時間までレポートできます。

次の手順に従ってください：

1. ［エンジニアリング］ページをクリックします。
2. ［表示項目］メニュー内の［パフォーマンス］をクリックし、次に以下をクリックします。
   - ネットワーク別のパフォーマンス マップを表示する場合は［ネットワーク］
   - サーバ別のパフォーマンス マップを表示する場合は［サーバ］
   - アプリケーション別のパフォーマンス マップを表示する場合は［アプリケーション］

   パフォーマンス マップが表示されます。
3. パフォーマンス マップ内のアイテムをクリックすると、その詳細レポートが表示されます。

   デフォルトでは、コンポーネント レポートが表示されます。
4. ［表示項目］メニューから、表示する詳細レポートを選択します。
   - コンポーネント レポート (P. 111)
   - トラフィック レポート (P. 119)
   - セッション レポート
   - レスポンス サイズ レポート (P. 126)
   - QoS レポート (P. 127)
   - 統計レポート (P. 132)
   - トレンド レポート (P. 134)

   各パフォーマンス詳細レポートには、その件名に関連する表示のコレクションがサマリ レポートと共に表示され、その下にコンポーネント表示が示されます。 詳細については、以下のセクションを参照してください。

コンポーネント レポートの使用

コンポーネント詳細レポートには、選択したアプリケーション、サーバ、およびネットワークごとにメトリックの詳細が表示されます。

ヒント： 特定のアプリケーション、サーバ、またはネットワークによって詳細レポートをフィルタするには、レポートの左上のリンクをクリックするか、または［設定］ボタンをクリックします。

レスポンス時間構成: 平均

レスポンス時間構成: 平均レポートには、合計時間を構成するコンポーネントで形成されたエンドツーエンドのレスポンス時間が表示されます。

- ネットワーク RTT： ネットワーク ラウンドトリップ時間
- 再送信： 再送信時間
- データ転送： データ転送時間
- サーバ レスポンス： サーバ レスポンス時間

このレポートには、レポート期間に観測された TCP トランザクションの数が表示されます。

トランザクションは、単一のリクエストおよび単一のサーバ レスポンス、1 つのデータ転送期間、1 つ以上の受信確認、および再送信されたパケットが原因となって観測された遅延です。

検索対象	考えられる事象
すべての値の漸増	ネットワーク トラフィックの標準的な経時的増加
測定値のスパイク	詳細調査すべき異常
レスポンス時間の他のコンポーネントが一定であるのに対し、1 つのコンポーネントが急増する	詳細調査すべき異常
ネットワーク ラウンドトリップ時間の増加にともなう観測数の増加	リンクの過大使用
高いデータ転送時間と低いネットワーク ラウンドトリップ時間	サーバの過度の使用
高い再送信遅延	パケット ロス

観測数の増加	アプリケーション使用の増加
観測数の増加と対応するサーバ レスポンス時間の増加	サーバの過負荷

サーバ レスポンス時間

サーバ レスポンス時間レポートには、クライアントによって行われたリクエストへの応答を開始するためにサーバが必要とする時間が表示されます。

ヒント： サーバ レスポンス時間データを表形式で表示した場合、テーブルの最下部の行には各列の平均/合計の統計が一覧表示されます。ただし、平均/合計の統計は平均値から計算されます。 たとえば、［最小］列の平均/合計値は、［最小］列の平均値ではなく、実際には［平均］列の値の最小値です。

この値はサーバ速度、アプリケーション設計、およびリクエストのボリュームによる影響を受ける可能性があります。

検索対象	考えられる事象
サーバ レスポンス時間が増大する一方で観測数も増加した場合は、同一期間中に以下の測定値の増加が見込まれる。 ■ データ ボリューム ■ データ転送時間 ■ 開いている TCP セッション	サーバの過負荷の明確な兆候です。
サーバ接続時間が増大する一方での観測数が減少	このサーバ上で実行中の他のアプリケーションが 管理コンソール によって監視されているかどうかを確認します。 監視されている場合、それらのアプリケーションのサーバ レスポンス時間の増加に対応する観測数の増加を確認し、サーバ上の原因となったアプリケーション プロセスを特定します。

検索対象	考えられる事象
サーバ上に監視対象アプリケーションがなく、観測数が減少する一方で、サーバ レスポンス時間が増加	別のアプリケーションがサーバ レスポンス時間に影響している場合があります。たとえば、サーバ上で実行中のバックアップ プログラムは、同時にアクティブになっているアプリケーションのレスポンス時間を増加させる可能性があります。 サーバ レスポンス時間の増加と観測数の減少のパターンを経時的に確認し、必要に応じて、他の運用チームと連絡をとるか、ネットワーク プロトコル アナライザを使用してサーバ上で実行中のどのアプリケーションがサーバ レスポンス時間の増加の原因となっているかを特定します。
高いサーバ レスポンス時間	サーバに関して以下の問題のいずれかがあります。 ■ 処理能力の不足 ■ 使用可能なメモリの不足 ■ 遅いハード ドライブ ■ ハング中のプロセス ■ NIC 設定の誤設定 ■ 大規模なクエリを使用するデータベース ルックアップなどの低品質のアプリケーションや低品質のインデックスの存在
サーバ レスポンス時間が絶えず変化する	大量のデータが定期的に発生しています。
アプリケーションがリクエストの受信直後に作業を開始したことを示すレスポンスを送信しているが、サーバ レスポンス時間が常に遅い	ユーザ操作性上の実際の遅延はデータ転送速度コンポーネントに現れます。

データ転送時間

データ転送時間レポートには、最初から最後のパケットまでを測定した、レスポンス全体の転送にかかる時間が表示されます。TCP ウィンドウに収容しきれない大量のデータを送信する場合は、［データ転送時間］から初期サーバ レスポンス時間を除外し、ネットワーク ラウンドトリップ時間のみを含めます。

この時間に影響する要因は、レスポンス サイズ、使用可能な帯域幅、距離によるネットワーク遅延、一部のサーバ処理、および往復数などの対話数、アプリケーションとネットワーク間の個々のパケット サイズです。

データ転送時間は、すべてのデータの配信に必要なネットワーク往復数および 1 往復あたりの遅延に関連します。

検索対象	考えられる事象
データ転送時間の増加	以下のいずれかの条件で発生します。 ■ アプリケーションの設計に問題がある。 ■ サーバが情報を連続的に送信できるほど TCP/IP 転送ウィンドウが大きくない。 データ転送時間の大幅な増加とデータ ボリュームとを相互に関連付け、その増加がネットワーク上で転送される大量のデータに起因するか、または問題がないかを判断します。
サブネット別のデータ転送時間における差異	その領域に使用可能な帯域幅の不足、特定の領域に必要な再送信数、およびアプリケーションの異なる使用法。

再送信遅延

再送信遅延は、再送信を必要とするパケットによって引き起こされたネットワーク ラウンドトリップ時間の追加的な遅延です。

表示されるデータは、1 つのトランザクションの実際の再送信時間ではなく、すべての観測の平均です。 再送信のない 4 つのトランザクションと、5 秒の再送信遅延のある 1 つのトランザクションの合計 5 つのトランザクションでは、1 秒の再送信遅延が表示されます。

管理コンソール は、監視デバイスのサーバに隣接する視点からネットワーク内の重複パケットを観測して再送信遅延を計算します。 監視デバイス は、ネットワーク パスに沿ったサーバからクライアントへの方向におけるデータ ロスにより、サーバによって再送信されたパケットを確認できます。 これらの観測は再送信遅延に含められます。 データ ロスがクライアントからサーバへの方向（たとえばサーバに到達する前のネットワーク パス内）で発生した場合、監視デバイス はそのようなパケット ロスを観測できないため、その遅延は再送信遅延メトリックには含められません。管理コンソール では、ネットワーク ラウンドトリップ時間メトリックでの再送信と関連するこの遅延が含められます。 これにはサーバ レスポンスおよびクライアント受信確認が含まれます。 未確認の再送信遅延によって引き起こされたクライアント受信確認の遅延は NRTT 値を増加させます。 このメトリックは、TCP の輻輳によるデータ転送時間の損失の影響を明らかにしません。

再送信は所定のセッションのトランザクション時間を短縮する可能性はありますが、パスを変更するか輻輳が増加しない限り、回線上のバイト速度はそのままです。

検索対象	考えられる事象
観測数の増加にともなう再送信遅延の増加	ネットワークは高い負荷を処理できない場合があります。バッファ割り当てまたはルーティング戦略の変更によって短期のスパイクが軽減される場合があります。

再送信遅延が一貫したパターンで変化する	領域へのリンクの問題。再送信が多い期間と他の情報源とを相互に関連付け、その時間帯にネットワーク上で他に何が発生しているかを特定します。特定のサブネットで、再送信遅延とネットワーク ラウンドトリップ時間の比率が他の領域よりも高いことが示されている場合、その領域へのリンクに問題がある場合があります。再送信のために過度の遅延が特定のネットワークに発生した疑いがある場合、問題のネットワークの再送信遅延を表示し、すべてのネットワークの平均再送信遅延と比較します。
ネットワークの再送信遅延がすべてのネットワークの平均よりも高い	無線環境では正常な動作です。
再送信遅延が一貫して高い	ネットワークが必要な負荷を搬送できないか、デバイスが誤動作している場合があります。
値が高い	ネットワークの輻輳、負荷分散の誤設定、パスまたはルートの重複、およびネットワーク エラー状態に起因するパケットのドロップ。

ネットワーク ラウンドトリップ時間

ネットワーク ラウンドトリップ時間は、ネットワーク上のサーバとクライアント間でのパケットの往復にかかる時間です（再送信による遅延を除く）。

この値を計算する場合は、アプリケーションとサーバの処理時間が除外されます。 管理コンソール は、接続セットアップ時間だけでなく、すべてのアプリケーション トラフィックの TCP 受信確認を調べてネットワーク ラウンドトリップ時間を継続的に改善し、最も正確なモデルを構築します。

キャリア遅延および NRTT 時間との比較のベースラインとしてのネットワーク接続時間の使用

検索対象	考えられる事象
観測数の増加と一致する NRTT の増加	クライアント ホストとサーバ間の帯域幅が、アプリケーションによって転送されているデータのボリュームには不十分です。観測数の増加に一致しない NRTT の増加は以下を示唆している場合があります。 ■ 別のアプリケーションがリモート クライアント ホストとアプリケーション サーバ間の使用可能な帯域幅を消費している。 ■ キャリアのネットワークが保護されているパスか別のパスに切り替えられている。 ■ いくつかのエラー状態がネットワーク内に存在する。
NRTT の増加をともなう観測数の増加	遅延増加の根本原因です。 データ、または TCP セッション、あるいはその両方に一致する増加があった場合、［データ ボリューム］および TCC セッションの表示を確認します。
NRTT の増加をともなう観測数の減少	監視デバイス とリモート クライアント間の他の観測対象アプリケーションが帯域幅の明白な減少が原因である場合があります。

検索対象	考えられる事象
同じ建物など、同一のオフィスの場所に存在するサブネットを比較した場合、本来は同じアプリケーションの NRTT の差異はわずかである必要があります。	10 ミリ秒よりも大きな差異は以下のいずれかが原因であると考えられます。 ■ LAN アーキテクチャの問題 ■ 正しく構成されていないスイッチまたは NIC ポートの設定 ■ ネットワーク内のエラー状態 ■ LAN 内の物理パス間の使用率の違い
サーバから不定距離にあるリモート オフィスのユーザと、サーバへの異なる WAN リンク上での操作で異なる遅延および NRTT が発生する	プロビジョニング済みの帯域幅、リンク使用パターン、およびアクセス テクノロジ(たとえば、ATM と IP VPN など)。

実効ネットワーク ラウンドトリップ時間

実効ラウンドトリップ時間は、ネットワーク ラウンドトリップ時間と、単一トランザクションの再送信によって引き起こされた遅延から構成されています。

これにはユーザが実際に経験する遅延が反映されるため、このメトリックは重要です。 管理者はこのメトリックにインシデントしきい値を設定し、再送信によるネットワークのパフォーマンスの低下を検出できます。

ネットワーク ラウンドトリップ時間および再送信遅延の両方が含まれているため、実効ラウンドトリップ時間のほうがネットワーク ラウンドトリップ時間よりもエンド ユーザが経験するネットワーク性能に近くなっています。 各コンポーネントが他方に関してどのように関与するかを確認するには、実効ラウンドトリップ時間と、ネットワーク ラウンドトリップ時間および再送信遅延とを比較します。

トラフィック レポート

［エンジニアリング］ページのネットワーク、サーバ、およびアプリケーションのトラフィック詳細レポートには、以下のメトリックが含まれます。

- レスポンス時間構成: 平均
- データ ボリューム（バイト）
- データ ボリューム（パケット）
- データ転送速度（ビット/秒）
- データ転送速度（パケット/秒）

ヒント： 特定のアプリケーション、サーバ、またはネットワークによって詳細レポートをフィルタするには、レポートの左上のリンクをクリックするか、または［設定］ボタンをクリックします。

レスポンス時間構成: 平均

レスポンス時間構成: 平均レポートには、合計時間を構成するコンポーネントで形成されたエンドツーエンドのレスポンス時間が表示されます。

- ネットワーク RTT： ネットワーク ラウンドトリップ時間
- 再送信： 再送信時間
- データ転送： データ転送時間
- サーバ レスポンス： サーバ レスポンス時間

このレポートには、レポート期間に観測された TCP トランザクションの数が表示されます。

トランザクションは、単一のリクエストおよび単一のサーバ レスポンス、1 つのデータ転送期間、1 つ以上の受信確認、および再送信されたパケットが原因となって観測された遅延です。

検索対象	考えられる事象
すべての値の漸増	ネットワーク トラフィックの標準的な経時的増加
測定値のスパイク	詳細調査すべき異常
レスポンス時間の他のコンポーネントが一定であるのに対し、1 つのコンポーネントが急増する	詳細調査すべき異常

ネットワーク ラウンドトリップ時間の増加にともなう観測数の増加	リンクの過大使用
高いデータ転送時間と低いネットワーク ラウンドトリップ時間	サーバの過度の使用
高い再送信遅延	パケット ロス
観測数の増加	アプリケーション使用の増加
観測数の増加と対応するサーバ レスポンス時間の増加	サーバの過負荷

データ ボリューム（バイト）

データ ボリューム（バイト）は、ネットワーク上で確認されたアプリケーション レイヤ バイトの総数を示します。

データ ボリュームのレポートは、高速のデータ転送速度の影響を明らかにする可能性があります。 非常に大きなデータ転送ボリュームがネットワーク ラウンドトリップ時間の上昇の原因であるかを調査します。

このレポートを使用して以下を行います。

- 過剰なトラフィックによって引き起こされたネットワーク上の異常を特定する。
- パフォーマンスの問題の原因として考えられるため、過剰トラフィックを除去する。
- 特定のアプリケーション、アプリケーション グループ、またはキャパシティ計画のネットワークのピーク使用率を決定する。

データ ボリューム（パケット）

［データ ボリューム （パケット）］は、監視対象のネットワーク上で確認されたパケットの総数を示します。 このレポートには、TCP 受信確認などのゼロ バイト パケットが含まれます。

この表示とデータ ボリュームの表示とを使用して、ネットワークを往来する平均パケット サイズを把握します。 小さなパケット サイズはサービス拒否攻撃を示唆する場合があるため、問題の領域や攻撃の特定に役立ちます。

データ転送速度（ビット/秒）

データ転送速度 （ビット/秒）には、指定された期間の 1 秒あたりのデータ転送速度がビット単位で表示されます（バイト/秒 × 8）。

この表示ではサーバに対するデータ トラフィックの速度が比較されているため、この表示を使用してサーバ上のキャパシティを計画します。

検索対象	考えられる事象
高速のビット レート	過負荷状態のサブネット
低速のビット レート	ネットワークまたはアプリケーションの問題

データ転送速度（パケット/秒）

データ転送速度（パケット/秒）には、指定された期間の 1 秒あたりのデータ転送速度がパケット単位で表示されます。

検索対象	考えられる事象
高速のパケット レート	負荷がかかったルータ、スイッチ、およびファイアウォールは過剰なパケット破棄の原因となります。
短期間の高速パケット レート	影響を受けたデバイスに十分なバッファ スペースを割り当てることにより緩和できます。 遅延を感知するアプリケーションに悪影響が及ぶ場合があるため、バッファ容量を増加させるときは注意が必要です。 バッファでの遅延よりも、音声パケットの破棄をお勧めします。
高速パケット レートの持続	デバイス容量をアップグレードする必要がある場合があります。
ルータ、スイッチ、およびファイアウォールの場合と同様に、監視デバイス はパケット レートが高い状態が短時間でも、その間にパケットを破棄する場合がある。	SPAN ポートがパケットをドロップした可能性があります。
異常に低速のパケット レート	ネットワークの問題。
低速のビット レートに伴って、パケット レートが高速になっている	セキュリティ攻撃。

セッション レポート

TCP/IP セッション レポートを使用して、無応答または拒否されたセッションに関連するアプリケーションおよびサーバの重大な問題や、一意のセッション数および一意のセッションの長さの一般的な調査を確認します。このレポートには、Web アプリケーションからの HTTP セッションは含まれません。

ヒント： 特定のアプリケーション、サーバ、またはネットワークによって詳細レポートをフィルタするには、レポートの左上のリンクをクリックするか、または［設定］ボタンをクリックします。

レスポンス時間構成: 平均

レスポンス時間構成: 平均レポートには、合計時間を構成するコンポーネントで形成されたエンドツーエンドのレスポンス時間が表示されます。

- ネットワーク RTT： ネットワーク ラウンドトリップ時間
- 再送信： 再送信時間
- データ転送： データ転送時間
- サーバ レスポンス： サーバ レスポンス時間

このレポートには、レポート期間に観測された TCP トランザクションの数が表示されます。

トランザクションは、単一のリクエストおよび単一のサーバ レスポンス、1 つのデータ転送期間、1 つ 以上の受信確認、および再送信されたパケットが原因となって観測された遅延です。

検索対象	考えられる事象
すべての値の漸増	ネットワーク トラフィックの標準的な経時的増加
測定値のスパイク	詳細調査すべき異常
レスポンス時間の他のコンポーネントが一定であるのに対し、1 つのコンポーネントが急増する	詳細調査すべき異常
ネットワーク ラウンドトリップ時間の増加にともなう観測数の増加	リンクの過大使用

高いデータ転送時間と低いネットワーク ラウンドトリップ時間	サーバの過度の使用
高い再送信遅延	パケット ロス
観測数の増加	アプリケーション使用の増加
観測数の増加と対応するサーバ レスポンス時間の増加	サーバの過負荷

接続セットアップ時間

接続セットアップ時間は、データ転送が開始される前に、クライアントとサーバとの間で TCP セッションを確立するために必要な時間です。 このビューのネットワーク コンポーネントは実効ラウンドトリップ時間とほとんど同じです。

接続セットアップ時間の 2 つのコンポーネントを別々に示します。

- サーバ接続時間（SCT）は、クライアントから受信する最初の SYN パケットからサーバが最初の SYN/ACK を送信するまでの時間です。
- ネットワーク接続時間（NCT）は、サーバから送信される SYN/ACK か 3 方向ハンドシェークを完了する ACK を受信するまでの時間です。

検索対象	考えられる事象
接続セットアップ時間が SCT や NCT よりも大幅に長い	サーバまたは LAN の問題が原因である可能性があります。 ■ 接続セットアップ時間をネットワーク ラウンドトリップ時間、再送信遅延、およびサーバ セットアップ時間と比較し、これらの表示が同様のパターンを示しているかどうかを判断します。 通常、接続セットアップ時間とネットワーク ラウンドトリップ時間は同時に増加しますが、直線的な増加ではありません。 ■ NRTT とデータ転送時間が増加し、接続セットアップ時間が一定のままである場合は、クライアントからサーバへの方向でのデータ ロスを示唆していることがあります。 データ ロスが疑われる場合は、クライアント ネットワーク上でスニファを使用して再送信数を表示し、確認できます。

検索対象	考えられる事象
接続セットアップ時間が SCT や NCT よりも大幅に長い	■ ネットワーク ラウンドトリップ時間のスパイクに関連する接続セットアップ時間のスパイクが発生した場合、トラフィック ボリュームの増加と帯域幅の不足、ネットワーク内のエラー、代替パスへのキャリア スイッチによる遅延の増加などにより、ネットワーク上で遅延が発生していることを示します。 ■ 接続セットアップ時間のスパイクのみの場合、CPU が過負荷状態になっているか TCP/IP セッション制限を超過しているために、サーバに負荷がかかっていることを示唆している可能性があります。

TCP/IP セッション

TCP/IP セッション レポートには、クライアントとサーバ間のユニークな接続の数が表示され、［オープン］、［完了］、および［期限切れ］の TCP/IP セッションが表示されます。

管理コンソール は 5 分間のモニタリング期間中に期限切れの TCP/IP セッションと完了した TCP/IP セッションを計算します。 オープン セッションはモニタリング期間の終了時にまだオープンしているセッションの数です。 オープン セッションは、後続のレポート間隔中に［期限切れ］または［完了］になる場合があります。 15 分以内にパケットを検出しなかった場合、管理コンソール はセッションを［期限切れ］に分類します。

検索対象	考えられる事象
複数の期限切れセッションが完了しない。	多くの期限切れセッションがオープンしたままになっていると、サーバがハングする可能性があります。 サーバがサポートできるのは、最大同時接続数のみです。

未対応の TCP/IP セッション リクエスト

未対応の TCP/IP セッション リクエストには、以下を含めて、クライアントとサーバ間で失敗した一意の接続の数が表示されます。

- 拒否されたセッション。 接続リクエストが 3 方向ハンドシェーク中にサーバによって明示的に拒否された場合、*拒否されたセッション*が発生します。
- 無応答セッション。 接続リクエストが送信されたときに*無応答セッション*が発生しても、サーバは応答しません。

検索対象	考えられる事象
多数の拒否されたセッション	1 つ以上のサーバが過負荷の状態になり始めました。 ■ サーバが通常のシステム リクエスト、または悪意のある攻撃により過度にビジーになっている可能性があります。 ■ サーバ上で実行中のアプリケーション ライセンスが、許可されている最大ユーザ数またはセッション数を超えた場合があります。

TCP/IP セッション時間

TCP/IP セッション時間は、各ユーザ セッションの長さを表示します。

検索対象	考えられる事象
同じユーザからの多くの短いセッション	アプリケーションが接続プールを活用している場合があります。
長いセッションがあり、トラフィックがほとんどない	アプリケーションがセッションを不必要に開いたままにしている場合があります。
サーバのピーク使用率が 1 週間、問題になっている	オープン セッション数の増加が過去数週間で増大し続けています。 次のセクションで説明する［トレンド］ビューを確認します。

レスポンス サイズ レポート

レスポンス時間は、転送されたレスポンスのサイズ別のデータ転送時間の測定値です。 接続セットアップ時間は含まれません。

さまざまなサイズのレスポンスの転送所要時間を比較すると、パフォーマンス上の問題がアプリケーションまたはネットワークと関連しているかどうかを確認できます。

ヒント： 特定のアプリケーション、サーバ、またはネットワークによって詳細レポートをフィルタするには、レポートの左上のリンクをクリックするか、または［設定］ボタンをクリックします。

レスポンス時間構成: 平均

この表示でアプリケーション レスポンス時間とネットワーク ラウンドトリップ時間が長く、トラフィック ビューでデータ ボリュームとデータ転送時間が大きいことが示された場合、レスポンス サイズがパフォーマンス低下の要因となっている可能性があります。 サーバ レスポンス時間が長い場合も、レスポンス サイズを確認する十分な根拠となり得ます。

詳細:

レスポンス時間構成: 平均 (P. 111)

レスポンス サイズ別データ転送時間

このレポートは、レスポンス サイズ別の平均データ転送時間を表示します。 通常、データ サイズが大きいと、転送時間が長くなります。

検索対象	考えられる事象
制限付きまたは特定のレスポンス サイズ	特定のトランザクション タイプは、エンドツーエンドのレスポンス時間を遅くします。
大型レスポンスのボリューム	「レスポンス サイズ別データ転送時間」ビューを使用して、ネットワーク上の遅延の原因となる可能性がある大型のレスポンスのボリュームを特定します。

検索対象	考えられる事象
このビューの各レスポンス サイズのグレーの観測数行は、各サイズのレスポンス数を示しています。	観測数は、少量のデータ転送で応答し、大規模なデータ転送を使用しないアプリケーションなど、アプリケーションの設計上の問題を示している可能性があります。

平均(大)データ転送時間

平均データ転送時間レポートは、サイズが小、中、大のレスポンスについて、レスポンス サイズ（KB）別の平均データ転送時間を表示します。

これらのビューで、以下を確認します。

- 1 つのレスポンス サイズのレスポンス時間の経時的な比較では、アプリケーション レスポンス時間の変化が返されたデータの量の変化によって引き起こされているかどうかが示されます。各レスポンス サイズのレスポンス時間が一定のままでもアプリケーションが遅くなる場合、その問題はユーザ動作の変化によって引き起こされている場合があります。たとえば、ユーザがより大きなオブジェクトをリクエストしている場合があります。グレーの観測行を使用して、各サイズ カテゴリに分類されるトランザクションの数を特定します。
- 相対レスポンス時間は、分析されるリクエストまたは転送されるレスポンスをアプリケーションが待機しているかどうかを示します。

QoS レポート

高トラフィック ボリュームと高データ転送速度が所定のレスポンス サイズの低速レスポンス時間と組み合わさると、サービス品質レポートの参照を促すメッセージが表示される場合があります。 このレポートでは、アプリケーションの特定のユーザについての詳細も［ユーザ］ビューに含まれています。

ヒント： 特定のアプリケーション、サーバ、またはネットワークによって詳細レポートをフィルタするには、レポートの左上のリンクをクリックするか、または［設定］ボタンをクリックします。

レスポンス時間構成: 平均

レスポンス時間構成: 平均レポートには、合計時間を構成するコンポーネントで形成されたエンドツーエンドのレスポンス時間が表示されます。

- ネットワーク RTT： ネットワーク ラウンドトリップ時間
- 再送信： 再送信時間
- データ転送： データ転送時間
- サーバ レスポンス： サーバ レスポンス時間

このレポートには、レポート期間に観測された TCP トランザクションの数が表示されます。

トランザクションは、単一のリクエストおよび単一のサーバ レスポンス、1 つのデータ転送期間、1 つ以上の受信確認、および再送信されたパケットが原因となって観測された遅延です。

検索対象	考えられる事象
すべての値の漸増	ネットワーク トラフィックの標準的な経時的増加
測定値のスパイク	詳細調査すべき異常
レスポンス時間の他のコンポーネントが一定であるのに対し、1 つのコンポーネントが急増する	詳細調査すべき異常
ネットワーク ラウンドトリップ時間の増加にともなう観測数の増加	リンクの過大使用
高いデータ転送時間と低いネットワーク ラウンドトリップ時間	サーバの過度の使用
高い再送信遅延	パケット ロス
観測数の増加	アプリケーション使用の増加
観測数の増加と対応するサーバ レスポンス時間の増加	サーバの過負荷

詳細:

レスポンス時間構成: 平均 (P. 111)

ユーザ

［ユーザ］ビューには、指定された期間における監視対象ネットワーク上の一意の IP アドレスまたはサブネット、あるいはその両方の数が表示されます。

サーバに同時にアクセスしているユーザが多数存在するかどうかを確認します。

パケット ロスの割合

［パケット ロスの割合］ビューには、監視対象ネットワーク上で損失したデータ の割合およびパケットでの毎秒のロス レートが表示されます。

監視デバイス は、サーバに隣接する位置からネットワーク内で再送信されたデータの合計データに対する割合を観測し、パケット ロスの割合を計算します。 監視デバイス は、ネットワーク パスにおけるサーバからクライアントへの方向でのデータ ロスにより、サーバによって再送信されたパケットを確認できます。 データ ロスがクライアントからサーバへの方向（たとえば、サーバに到達する前のネットワーク パス内）で発生した場合、監視デバイス はそのようなパケット ロスを観測できないため、その遅延は［パケット ロスの割合］には含まれません。

この表示内で以下を確認します。

検索対象	考えられる事象
1% を超える同時値。	高データ ロス。
このビューにはパケット ロスのみが表示され、データ テーブルにパケットおよびバイト ロスが表示されます。	パケット ロスによりデータが再送信され、それが原因で TCP でウィンドウ サイズが縮小し、そのために後続パケットの転送時間が低下します。 再送信されたパケットは、ネットワーク インフラストラクチャ上の負荷を増加させます。 再送信バイト数は、再送信データによって使用された帯域幅の量を示します。

ユーザ Goodput

［ユーザ Goodput］ビューは、クライアント操作性をキャプチャします。送信された良好なバイト数（再送信数を除く）を、この情報を送信するための所要時間で割った数が表示されます。

ユーザが Web からデータをダウンロードした場合、ファイルをダウンロードしているときにブラウザでスループットが計算されます。 スループットは転送されたバイト数をアクティビティの期間で割った数です。通常、このスループット値を使用してネットワーク接続の有効性を測定し、スループットから再送信バイト数を引いて計算したユーザ Goodput を表示します。これは、再送信バイト数はスループットを作為的に増大させるためです。

スループット測定値が 100 kbps でも、ダウンロードの半分が再送信から構成されている場合、ユーザ Goodput は 50 kbps となります。そのため、得られるメリットはスループットの半分のみとなります。

ユーザ Goodput とスループットはアクティブな転送の期間中にのみ計算されます。 監視デバイス は、5 分間隔でトラフィック レートを平均します。 その時間の大半は自動で行われます。 ユーザ Goodput/スループットとトラフィック レートとの間に関係はほとんどありません。

以下のシナリオを検討し、この点を説明します。5 分間隔中で唯一の転送が 1 秒以内で再送信なしでダウンロードされた 50 KB のドキュメントである場合、これらのメトリックは以下を適用します。

- ユーザ Goodput とスループットは 400 kbps で、以下のように計算されます。

  50 KB * （8 ビット/バイト）/1 秒 = 400 kbps

- トラフィック レートは 1.3 kbps で、以下のように計算されます。

  50 KB * （8 ビット/バイト）/300 秒 = 1.3 kbps

重大なデータ転送がある場合のみ、ユーザ Goodput は有用で、対話型トランザクションではなく、大量の転送に使用されます。 スループットは、再転送されたパケットが含まれている場合を除き、ユーザ Goodput（データ転送時間で割ったバイト数）と同じ数式を使用して計算されます。 スループットは常にユーザ Goodput 以上になります。

検索対象	考えられる事象

検索対象	考えられる事象
ユーザ Goodput の低下	ネットワーク輻輳 トラフィックが転送されている場合に限り、ネットワーク メトリックとしてユーザ Goodput を使用します。 転送が低速だったか高速だったかにかかわらず、有用なバイトはほとんどない場合があります。
不良 Goodput	データ転送時間がサーバまたはアプリケーションのパフォーマンス不良によって阻害されます。

詳細:

スループット (P. 31)

1 ユーザあたりのコンポジット レート

［1 ユーザあたりのコンポジット レート］ビューには、転送済みのトラフィック量を時間間隔で割り、その間隔内のユニーク ユーザ数で割ったものが表示されます。

［1 ユーザあたりのコンポジット レート］ビューにはネットワーク上で使用されるアドレス空間の影響を受けます。 クラス A または B のアドレスの場合、［1 ユーザあたりのコンポジット レート］ビューには、個別のクライアントではなく、個別のサブネットの結果が表示されます。 クラス C アドレスの場合は、［1 ユーザあたりのコンポジット レート］ビューに各クライアントが反映されます。

この表示を使用して以下を行います。

- 新規ユーザのユーザ アプリケーションへの影響の予測に役立てます。
- 展開前のテストで、さまざまなネットワーク リンク上で予期されるアプリケーション 負荷を特定します。

統計レポート

［統計レポート］ページには、レスポンス時間における変動が表示されます。 影響度分析にこのレポート ページを使用します。 ［レスポンス時間構成: 平均］ビューには、合計レスポンス時間が表示されます。 ［レスポンス時間構成: 標準偏差］ビューには、レスポンス時間測定に存在する変動の量が表示されます。

ヒント： 特定のアプリケーション、サーバ、またはネットワークによって詳細レポートをフィルタするには、レポートの左上のリンクをクリックするか、または［設定］ボタンをクリックします。

レスポンス時間構成: 平均

レスポンス時間構成: 平均レポートには、合計時間を構成するコンポーネントで形成されたエンドツーエンドのレスポンス時間が表示されます。

- ネットワーク RTT： ネットワーク ラウンドトリップ時間
- 再送信： 再送信時間
- データ転送： データ転送時間
- サーバ レスポンス： サーバ レスポンス時間

このレポートには、レポート期間に観測された TCP トランザクションの数が表示されます。

トランザクションは、単一のリクエストおよび単一のサーバ レスポンス、1 つのデータ転送期間、1 つ 以上の受信確認、および再送信されたパケットが原因となって観測された遅延です。

検索対象	考えられる事象
すべての値の漸増	ネットワーク トラフィックの標準的な経時的増加
測定値のスパイク	詳細調査すべき異常
レスポンス時間の他のコンポーネントが一定であるのに対し、1 つのコンポーネントが急増する	詳細調査すべき異常
ネットワーク ラウンドトリップ時間の増加にともなう観測数の増加	リンクの過大使用

高いデータ転送時間と低いネットワーク ラウンドトリップ時間	サーバの過度の使用
高い再送信遅延	パケット ロス
観測数の増加	アプリケーション使用の増加
観測数の増加と対応するサーバ レスポンス時間の増加	サーバの過負荷

レスポンス時間構成: 標準偏差

レスポンス時間構成: 標準偏差メトリックは、レスポンス時間測定に存在する変動の量を数値化します。

検索対象	考えられる事象
すべてのユーザが同様に動作し（低い標準偏差）、変動の程度が時間と共に変化。	平均レスポンス時間が良好でも、標準偏差が高いアプリケーションの場合、かなりの数のユーザに対して劣悪なパフォーマンスを提供することになります。
標準偏差の規則的なパターン	アプリケーションの使用が経時的に変化またはクライアント ミックスが変化。ネットワークへのリンクにおける差異は、ネットワーク時間の標準偏差を引き上げる原因となる可能性があります。 使用可能なサンプルがわずかな場合、多くのデータポイントが使用可能であるときよりも差異が大きくなる傾向があります。
標準偏差が一貫して高い	重要な分析を行うには値が多様すぎます。たとえば、高速アプリケーションと低速アプリケーションを含むデータの比較では、アプリケーション間のユーザ操作性に大きな違いが出ます。 この場合、より有意味な結果となるように、データをアプリケーション別にフィルタします。標準偏差が一貫して高い場合も、アプリケーション動作における変動の度合いが高いことを意味します。

パーセンタイル

［エンジニアリング］ページの［サーバ レスポンス時間パーセンタイル］、［データ転送時間パーセンタイル］、［再送信遅延時間パーセンタイル］、および［ネットワーク ラウンドトリップ時間パーセンタイル］ビューを使用して、所定の問題によってトランザクションがどの程度の影響を受けたかを特定します。 ネットワークの問題が 90 番目のパーセンタイル ビューにのみ示されている場合、この問題は最も低速のトランザクションのみに限定されます。 問題が 75 番目または 50 番目のパーセンタイル 表示に示されている場合、その問題はトランザクションのより大きな部分を含んでいます。

数人のユーザが低速のアプリケーション レスポンスについて不平を言う場合がありまが、ほとんどのユーザのレスポンス時間は正常です。［ネットワーク ラウンドトリップ時間パーセンタイル］ビューでは、75 番目または 50 番目のパーセンタイル ラインよりもはるかに高い 90 番めのパーセンタイル ラインでこの状況を示す場合があります。 トランザクションの約 10% のパフォーマンスが劣悪であるのに対し、残りの 90% の結果が良好であることがわかります。 リモート サイトのユーザ、または特定のトランザクション タイプのユーザのパフォーマンスが劣悪であったと考えられます。

90 番目、75 番目、50 番目のパーセンタイル ラインが近接している場合、実行した場所や、トランザクションのタイプにかかわらず、ほとんどのユーザが大差なく、同じような結果となっていたと結論付けられます。

トレンド レポート

［エンジニアリング］ページの［トレンド］ビューには、特定の期間、平均エンドーツーエンド レスポンス時間データが表示されます。 レポート タイトルは、間隔の単位を示します。

ヒント： 特定のアプリケーション、サーバ、またはネットワークによって詳細レポートをフィルタするには、レポートの左上のリンクをクリックするか、または［設定］ボタンをクリックします。

トレンド レポート	間隔
1 時間のレスポンス時間構成: 平均	5 分
8 時間のレスポンス時間構成: 平均	5 分

トレンド レポート	間隔
日単位のレスポンス時間構成: 平均	15 分
週単位のレスポンス時間構成: 平均	1 時間
月単位のレスポンス時間構成: 平均	6 時間

これらのビューは以下のように使用します。

- 高データ転送速度および高ネットワーク ラウンドトリップ時間を調査する場合や、エンドツーエンドのレスポンス時間の変動について調査する場合、［トレンド レポート］ビューを参照してトラフィック ボリュームの急上昇を確認します。
- レスポンス時間の上昇を通じて輻輳のパターンを特定します。 定期的な輻輳か、永続的な輻輳か、突然の輻輳かを判断します。
- 以前のトラフィック トレンドからの大幅な変動を確認します。［トレンド］ビューは、ネットワーク使用率が高い期間の特定に役立ちます。
- 日単位データを他の曜日と比較するか、別の日についての観測数の比較方法を表示します。

可用性レポートの使用

管理コンソールは、タイム スライス中に観測した TCP トランザクションの成功、またはサーバ上のアプリケーション ポートへのリクエストに対する応答としてアプリケーション可用性を定義します。 管理コンソールは 5 分間隔でアプリケーション ポート レベルで情報を収集します。

管理コンソールは、観測した 5 分間隔の間に以下のいずれかの条件が発生した場合、可用性を疑問視します。

- 観測数が 10 未満
- 拒否されたセッション数が 10% 以上

必要に応じて、管理コンソールは以下の手順を実行して可用性を確認します。

1. 定義済みのアプリケーション ポート上で接続を試行し、アプリケーションをテストします。 ポート範囲によって定義されたアプリケーションについては、管理コンソールは範囲内の最初の 8 つのポート上で接続しようとします。
2. 管理コンソールがアプリケーションからのレスポンスを受信しない場合、そのアプリケーションは［使用不可］と評価されます。
3. オプションで、管理コンソールはサーバを ping し、ステータスを確認します。
   - サーバが ping リクエストの受信を確認した場合、管理コンソールはそのサーバを使用可能と見なします。
   - サーバが ping リクエストの受信を確認しなかった場合、管理コンソールはそのサーバを使用不可と見なします。
4. アプリケーションまたはサーバが使用不可の場合、管理コンソールはサーバ インシデントを開きます。

以下の 2 つのシナリオは異なる問題を示唆しています。

- アプリケーションは実行されていませんが、それをホストするサーバは実行されています。
- TCP ポートが、たとえば Web 用のポート 80 などのように、このアプリケーションのみに対してロックされている。

アプリケーションおよびサーバの可用性レポートの表示

次の手順に従ってください:

1. ［エンジニアリング］ページをクリックします。
2. ［表示項目］メニューの［可用性］をクリックします。

   アプリケーション可用性またはサーバの可用性レポートが表示されます。
3. 色分けされたパフォーマンス バーをクリックし、［時間］をクリックして可用性時系列レポートを表示します。
4. 矢印メニューをクリックし、［集約］を選択して、集約のみの可用性レポートを表示します。
5. 矢印メニューをクリックし、［テーブル］を選択して、表形式の可用性レポートを表示します。

詳細情報:

レポート ページの電子メール送信 (P. 157)
レポート ページの印刷 (P. 157)
レポート設定の変更 (P. 41)
レポート ページの CSV ファイルへのエクスポート (P. 155)
表示の CSV ファイルへのエクスポート (P. 156)

可用性時系列レポートの表示

次の手順に従ってください:

1. ［エンジニアリング］ページをクリックします。
2. ［表示項目］メニューの［可用性］をクリックします。

   アプリケーション可用性またはサーバの可用性レポートが表示されます。
3. アプリケーションまたはサーバのリンクをクリックします。
4. タイムライン サマリおよび可用性時系列レポートを表示するには、［表示項目］メニューの［時間］をクリックします。

可用性に関連するインシデントの表示

指定された期間中に報告されたインシデントを表示するには、［可用性レポート］ページ上で［関連するインシデント］をクリックします。 インシデント レポートには、可用性レポート期間中に報告されたインシデントが一覧表示されます。

詳細:

インシデント ページの使用 (P. 61)

リスト レポートの使用

［エンジニアリング］ページのリスト レポートには、管理コンソール によって監視されているネットワーク、サーバ、アプリケーションが表示されます。

リスト レポートについて

［エンジニアリング］ページで、ネットワーク、サーバおよびアプリケーションのリストを表示するには［リスト］をクリックします。 これらのリストから、特定のネットワーク、サーバまたはアプリケーションのパフォーマンス マップへ移動します。

ネットワーク、サーバおよびアプリケーションの表示

［エンジニアリング］ページから、ネットワーク、サーバ、またはアプリケーションのリストを表示します。 これらのリストから、選択したコンポーネントに固有のメトリックを表示する特定のネットワーク、サーバまたはアプリケーションのパフォーマンス マップのリンクをクリックします。

［エンジニアリング］ページで［リスト］をクリックした後、［ネットワーク］、［サーバ］、または［アプリケーション］をクリックしてレポートを表示します。

［ネットワーク リスト］、［サーバ リスト］または［アプリケーション リスト］で、マップへのリンクをクリックしてパフォーマンス レポートを表示します。

目的の操作	手順
アプリケーションまたはサーバに関連するネットワークのネットワーク別パフォーマンス レポートを表示する。	［サーバ リスト］または［アプリケーション リスト］ページで［マップ］列（使用可能な場合）の［ネットワーク］リンクをクリックします。
アプリケーションまたはネットワークに関連するサーバのサーバ別パフォーマンス レポートを表示する。	［ネットワーク リスト］または［アプリケーション リスト］ページで［マップ］列の［サーバ］リンクをクリックします。
サーバに関連するアプリケーションのアプリケーション別パフォーマンス レポートを表示する。	［ネットワーク リスト］または［サーバ リスト］ページで［マップ］列の［アプリケーション］リンクをクリックします。
集約のリスト レポートを表示する。	矢印メニューをクリックし、［集約］を選択します。

詳細:

レポート ページの電子メール送信 (P. 157)
レポート ページの印刷 (P. 157)
レポート ページの CSV ファイルへのエクスポート (P. 155)

第 7 章: [最適化]ページの使用

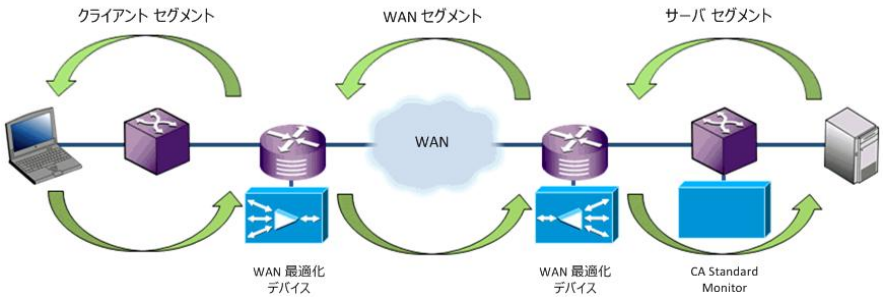
このセクションには、以下のトピックが含まれています。

最適化されたトランザクションについて

このセクションでは、Cisco WAAS または Riverbed Steelhead によって提供される、WAN で最適化されたトランザクションについて説明します。このセクションは、［最適化］ページの 管理コンソール レポートに表示される最適化されたトランザクションに関するデータを解釈するのに役立ちます。

WAN 最適化ソリューションは、WAN の両側にある最適化デバイスから構成されます。 WAN 最適化デバイスは、以下の 3 つのセグメントへ単一の TCP 接続を分割することで、クライアントとサーバ間の TCP 接続を最適化します。

- 先端の WAN 最適化デバイスへのクライアント
- WAN 最適化コア デバイスへの WAN 最適化エッジ デバイス
- サーバへの WAN 最適化コア デバイス



WAN 最適化データは、WAN 最適化ソリューションによって作成された、3 つの TCP セグメントに利用できます。 最適化されたアプリケーションとサーバとネットワークの単一の組み合わせの複数の監視ポイントから監視しているため、管理コンソール は 3 つのセグメントのそれぞれに個別のメトリックのセットを生成し、各セットを個別のアプリケーションとして扱います。 3 つのすべてのセグメントに沿ったアプリケーション動作は、ソースおよび宛先ポート、層全体にわたって同じままのアドレスを持つ 3 層アプリケーションに似ています。 管理コンソール の ［最適化］ページには、WAN に最適化されたトランザクションのデータが表示されます。

最適化されたトランザクションの監視

［エンジニアリング］ページでは、各ネットワーク セグメントに個別のアプリケーションを作成し、アプリケーション名にネットワーク セグメントを追加することによって、WAN に最適化されたアプリケーションが報告されます。それらのアプリケーションが存在する場合、管理コンソール レポートはセグメントを特定します。 各表示では、管理コンソール に以下の形式でアプリケーション名と関連セグメントが表示されます。

<ApplicationName> [**]

** はクライアント、サーバ、または WAN です。たとえば、以下のようになります。

HTTP [クライアント]

セグメント化されたアプリケーションからのトラフィックが収集されなかった場合、［**］ラベルは表示されません。

[最適化]ページの表示

管理コンソール が WAN ネットワーク セグメント上のアプリケーション トラフィックを監視する場合、［最適化］ページが表示されます。 ［最適化］ページを表示するには、［エンジニアリング］ページにアクセスできる役割が必要です。

［最適化］ページはクライアントの観点から最適化されたアプリケーション操作性を報告します。

［最適化］ページ上の設定パラメータは、以下の例外を除き、［エンジニアリング］ページと似ています。

- サーバの選択内容はデフォルトで[すべてのサーバ]に設定されます。サーバのフィルタリング オプションはありません。
- 使用可能なアプリケーションには WAN に最適化されたアプリケーションのみが含まれます。
- 使用可能なネットワークには、セグメント化されたアプリケーションがセグメント データを参照したネットワークのみが含まれます。
- 特定のメトリックやサンプリング間隔はフィルタできません。

最適化レポート ページのナビゲーション

［表示項目］メニューを使用して［最適化］レポート ページに移動します。 一方のレポートから、特定のアプリケーションのパフォーマンス詳細を参照するため、コンポーネント レポートにドリル インできます。

パフォーマンス

各クライアント セグメント アプリケーションに対してパフォーマンス マップを表示します。［最適化されたトランザクションのクライアント環境］ビューにはクライアントが体験する真の操作性が反映されます。 測定結果は、リモート Cisco WAE デバイス、またはリモート Steelhead アプライアンスを監視するリモート CA Standard Monitor から送信されます。

帯域幅縮小

WAN セグメント アプリケーションごとにボリューム メトリックを表示します。 ［帯域幅縮小］ビューは、最適化された WAN セグメントと、データ センターのサーバ セグメントまたはブランチのクライアント セグメントのいずれかの間の合計の帯域幅縮小バイト数を表示します。 ［合計バイト数］または［サーバからのバイト数］を比較することを選択できます。

Steelhead 環境でクライアント セグメントをレポートするには、CA Standard Monitor はブランチ Steelhead アプライアンスを監視する必要があります。

ヒント： デフォルトで現在のレポートを表示するには、［デフォルト ビューに設定］をクリックします。

最適化されたトランザクションのパフォーマンス詳細レポートの表示

［コンポーネント］レポートを使用して、最適化されたトランザクションのパフォーマンス詳細を表示し、WAN 最適化の効果を比較します。［最適化］ページから、特定のアプリケーションにドリル インして［コンポーネント］レポートを表示できます。

以下の表は、パフォーマンス詳細ビューおよびその派生元セグメントを示しています。

表示	表示されるアプリケーション セグメント	参照
レスポンス時間構成	クライアント	レスポンス時間構成: 平均 (P. 147)
サーバ レスポンス時間	サーバ	サーバ レスポンス時間 (P. 148)
ネットワーク ラウンドトリップ時間	WAN	ネットワーク ラウンドトリップ時間 (P. 149)
再送信遅延	WAN	再送信遅延 (P. 115)
パケット ロスの割合	WAN	パケット ロスの割合 (P. 117)
データ転送速度（ビット/秒）	WAN	データ転送速度（ビット/秒） (P. 151)
データ転送速度（パケット/秒）	WAN	データ転送速度（パケット/秒） (P. 151)
データ ボリューム（バイト）	WAN	データ ボリューム（バイト） (P. 151)
データ ボリューム（パケット）	WAN	データ ボリューム（パケット） (P. 151)

各表示では、管理コンソール に以下の形式でアプリケーション名と関連セグメントが表示されます。
<ApplicationName> [**]

 はクライアント、サーバ、または WAN です。

［コンポーネント］レポートは、最適化されたトランザクションに対するパフォーマンス詳細ビューを提供します。 このビューでは、5 分間のデータを平均して 15 分間データを生成します。以下を使用します。

- 最大 8 時間までのビューに 5 分間のデータを使用します。
- 最大 24 時間までのビューに 15 分間のデータを使用します。

詳細:

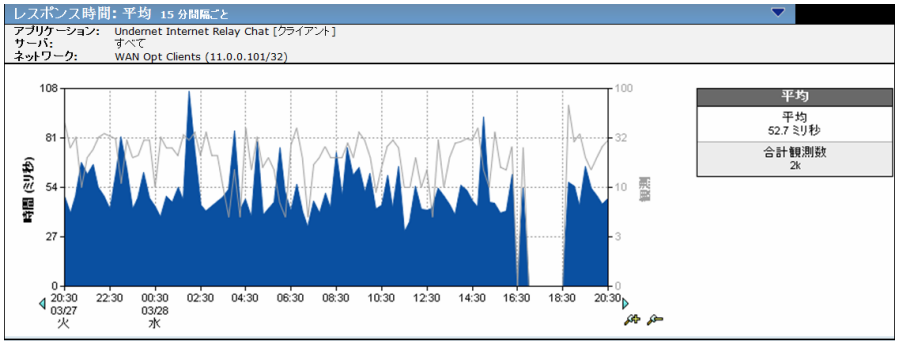
WAN 最適化の影響の比較 (P. 152)

レスポンス時間構成: 平均

［レスポンス時間構成: 平均］ビューには、クライアント アプリケーション セグメントのトランザクション時間が表示されます。 このビューには実際のクライアント操作性が反映されます。 測定結果は以下のものから送信されます。

- リモート Cisco WAE デバイス。
- ブランチ Steelhead アプライアンスを監視するリモート CA Standard Monitor。 CA Standard Monitor がブランチでクライアント セグメントを監視していない場合、該当するクライアント ネットワークのビューは空になります。

以下の例には、HTTP アプリケーションの WAN 最適化前後の影響が示されています。 このサブネットのユーザは、レスポンス時間の 25 倍の減少とトランザクションの 50 倍の増加に見舞われています。

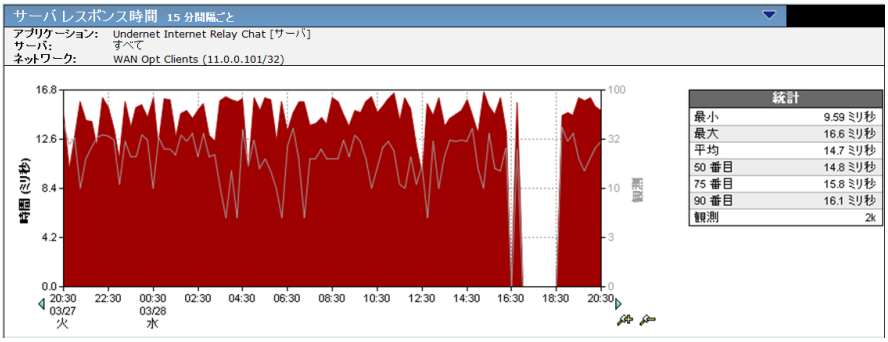


トランザクションは、単一のリクエストおよび単一のサーバ レスポンス、1 つのデータ転送期間、1 つ以上の受信確認、および再送信されたパケットが原因となって観測された遅延です。

サーバ レスポンス時間

［サーバ レスポンス時間］ビューには、サーバがアプリケーション リクエストに応答するのにかかる時間が表示されます。このビューには、サーバ セグメントのアプリケーションに関する情報が表示されます。 SPAN データが存在する場合、管理コンソール はそのデータを使用してこのセグメントに入力します。SPAN データがない場合、管理コンソール はデータ センターの WAN 最適化デバイスのサーバ側からの FlowAgent データを使用します。

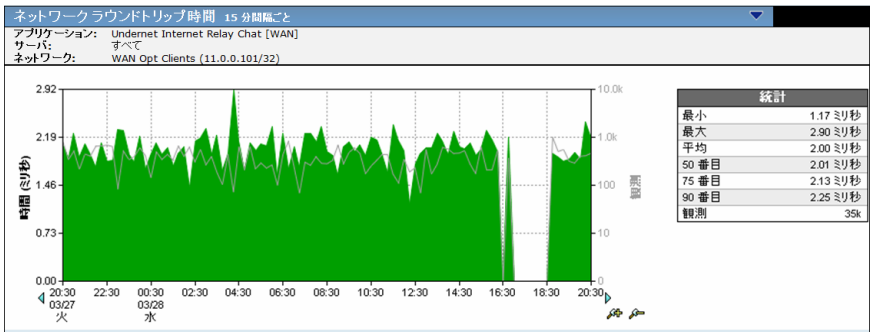
［レスポンス時間: 平均］ビューに付随する以下の表示例では、この HTTP アプリケーションのトランザクションで同様の 50 倍の増加が示され、サーバ レスポンス時間に目立った変更がない状態を示しています。



［レスポンス時間: 平均］ビューには、データ センター効率の大幅な改善が示されています。 ［サーバ レスポンス時間］ビューでは、クライアント側キャッシュがアクティブな場合は常に、データ センター オフロードのメリットを数値化します。サーバ レスポンス時間の値は、サーバ速度、アプリケーション設計およびリクエストのボリュームに影響される可能性があります。

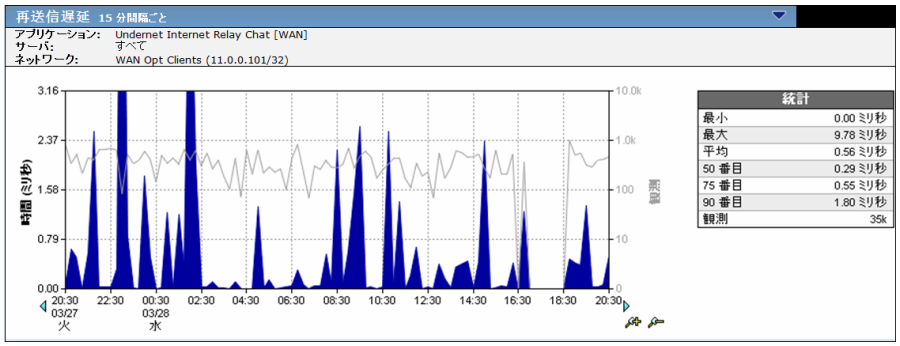
ネットワーク ラウンドトリップ時間

［ネットワーク ラウンドトリップ時間］ビューには、パケットがローカルとリモートの WAN 最適化デバイス間の往復全体にかかる時間から再送信によって発生する遅延を除いた時間が表示されます。 次の表示例では、WAN 最適化がアクティブにされた場合、キューイング遅延が削減または排除されたため、WAN 上のネットワーク ラウンドトリップ時間が大幅に改善されたことが示されています。



再送信遅延

再送信遅延は、再送信を必要とするパケットによって引き起こされたネットワーク ラウンドトリップ時間の追加的な遅延です。以下の表示例では、WAN 最適化がアクティブになると、この HTTP アプリケーションの WAN の上の再送信が停止することが示されています。



表示されたデータは、1 つのトランザクションの実際の再送信時間ではなく、すべての観測の平均です。たとえば、再送信のない 4 つのトランザクションと、5 秒の再送信遅延のある 1 つのトランザクションの合計 5 つのトランザクションでは、1 秒の再送信遅延が表示されます。

再送信遅延は、サーバに隣接する位置からネットワーク内の重複パケットを観測することによって計算されます。監視デバイス は、ネットワーク パスにおけるサーバからクライアントへの方向でのデータ ロスにより、サーバによって再送信されたパケットを確認できます。 これらの観測は再送信遅延に含まれます。 データ ロスがクライアントからサーバへの方向（たとえばサーバに到達する前のネットワーク パス内）で発生した場合、監視デバイス はそのようなパケット ロスを観測できないため、その遅延は再送信遅延メトリックには含まれません。

管理コンソール では、ネットワーク ラウンドトリップ時間メトリックにこの再送信遅延が含まれます。これにはサーバ レスポンスとクライアント受信確認が含まれるため、ネットワーク ラウンドトリップ時間の値を増加させるのは、未確認の再送信遅延によって引き起こされるクライアント受信確認の遅延です。 このメトリックは、TCP の輻輳によるデータ転送時間の損失の影響を明らかにしません。

再送信は所定のセッションのトランザクション時間を短縮する可能性はありますが、パスを変更するか輻輳が増加しない限り、回線上のバイト速度はそのままです。

パケット ロスの割合

［パケット ロスの割合］ビューには、監視対象ネットワーク上で損失したデータ の割合およびパケットでの毎秒のロス レートが表示されます。

監視デバイス は、サーバに隣接する位置からネットワーク内で再送信されたデータの合計データに対する割合を観測し、パケット ロスの割合を計算します。 監視デバイス は、ネットワーク パスにおけるサーバからクライアントへの方向でのデータ ロスにより、サーバによって再送信されたパケットを確認できます。 データ ロスがクライアントからサーバへの方向（たとえば、サーバに到達する前のネットワーク パス内）で発生した場合、監視デバイス はそのようなパケット ロスを観測できないため、その遅延は［パケット ロスの割合］には含まれません。

データ転送速度（ビット/秒）

［データ転送速度 （ビット/秒）］ビューには、指定された期間の WAN 上のビット/秒（バイト/秒 × 8）でデータ転送速度が表示されます。

データ転送速度（パケット/秒）

［データ転送速度 （パケット/秒）］ビューには、指定された期間の WAN 上のアプリケーションの 1 秒あたりのパケット数でデータ転送速度が表示されます。

データ ボリューム（バイト）

［データ ボリューム （バイト）］ビューには、ネットワーク上で確認されたアプリケーション レイヤ バイトの総数が表示されます。

データ ボリューム（パケット）

［データ ボリューム （パケット）］ビューには、監視対象ネットワーク上で確認されたパケットの総数が表示されます。 この表示では、TCP 受信確認などのゼロバイト パケットがカウントされます。

WAN 最適化の影響の比較

［コンポーネント］レポートを使用して、レスポンス時間およびボリューム メトリックに対する WAN 最適化の効果を比較します。管理コンソールは、自動的に期間を選択しません。 レスポンス時間の差異を比較するために WAN 最適化が開始または停止した場合、対応する期間を参照します。

WAN 最適化の効果を比較するには、特定のネットワーク上のアプリケーションについて［コンポーネント］レポートをフィルタします。

次の手順に従ってください:

1. ［最適化］ページから、［表示項目］メニューで［パフォーマンス］をクリックします。
2. ［設定］をクリックして必要なアプリケーションおよびネットワークを指定します。
3. ［OK］をクリックします。

   ［最適化されたトランザクションのクライアント環境］ビューはアプリケーションを表示します。
4. ［表示項目］メニューの［パフォーマンス］-［コンポーネント］をクリックします。
5. ［最適化の前後を表示］オプションをクリックします。

   コンポーネント レポートに、サーバ SPAN からの最適化されていないアプリケーション パフォーマンス データと、WAN に最適化されたパフォーマンス データの両方が表示されます。
6. レスポンス時差を比較するために WAN 最適化を開始または停止した場合は、左および右方向キーをクリックし、対応する期間を参照します。 管理コンソール は、自動的に期間を選択しません。

あふれトラフィックの検出

完全に最適化する必要がある組み合わせにあふれがあると（つまり、WAN 最適化デバイスがその瞬間に別のセッションを取得できないため、最適化するセッションが最適化されない）、あふれセッションの SPAN 測定は［サーバ］セグメントに移動します。

あふれセッションの測定は［クライアント］または［WAN］セグメントに影響しません。 あふれセッションおよび最適化セッションの測定が含まれていても、サーバ レスポンス時間 [サーバ] は正確です。［最適化］ページのすべてのメトリックは正確です。 100% ローカル ACK は取得しなくなっているため、ネットワーク ラウンドトリップ時間 [サーバ] は増加を示します。 あふれ測定によって、実際のネットワーク ラウンドトリップ時間がクライアントに示されます。 再送信遅延 [サーバ] およびパケット ロスの割合 [サーバ] も増加を示す場合があります。

適切にサイズ設定された WAN 最適化展開では、本来あふれはほとんどないかまったくありません。 ネットワーク ラウンドトリップ時間 [サーバ] の負荷がほとんどない時間と負荷の大きい時間で一貫して差異がある場合は、あふれが生じる可能性があります。 そのソリューションは WAN 最適化展開の容量を増やすことです。 すべてのネットワークが増加を示している場合、データ センター WAN 最適化デバイスに十分な容量がない場合があります。 増加を示しているネットワークがごく少数の場合は、それらのブランチ WAN 最適化デバイスに十分な容量がない場合があります。

あふれのもう 1 つのヒントとして、［クライアント］セグメントよりも［サーバ］セグメントでより多くのセッションが報告されていることが挙げられます。 これは、少なくとも、いくつかの最適化が［サーバ］セグメントで報告されている組み合わせの最適化以外のセッションが、所属する親アプリケーションよりも多く［サーバ］セグメントに報告されている場合に発生します。

第 8 章: [レポート]ページおよび表示の情報の共有

このセクションには、以下のトピックが含まれています。

レポートのファイルへのエクスポート

レポートを CSV ファイルにエクスポートします。 レポート ページの特定の表示またはすべての表示からデータを CSV ファイルまたは XML ファイルにエクスポートできます。

レポート ページの CSV ファイルへのエクスポート

管理コンソール ページのすべての表示からデータを CSV ファイルにエクスポートします。 たとえば、［操作］ページから CSV ファイルにすべての表示データをエクスポートできます。

次の手順に従ってください:

1. レポート ページをクリックします。
2. ［エクスポート］をクリックします。

   ［ファイルのダウンロード］ダイアログ ボックスが表示されます。
3. CSV ファイルとしてレポートを保存すには［保存］を、CSV ファイルを表示するには［開く］をクリックします。

表示の CSV ファイルへのエクスポート

［エンジニアリング］ページの表示からデータを CSV ファイルにエクスポートします。

次の手順に従ってください:

1. ［エンジニアリング］ページをクリックします。
2. 必要な表示上の青い矢印 ⚙ メニューをクリックし、［CSV へエクスポート］を選択します。

   ［ファイルのダウンロード］ダイアログ ボックスが表示されます。
3. CSV ファイルとして表示を保存すには［保存］を、CSV ファイルを開くには［開く］をクリックします。

表示の XML ファイルへのエクスポート

［エンジニアリング］ページの表示からデータを XML ファイルにエクスポートします。

次の手順に従ってください:

1. ［エンジニアリング］ページをクリックします。
2. 対象のビューで青い矢印 ⚙ メニューをクリックし、［XML へエクスポート］を選択します。

   XML 形式のデータが表示されます。

レポート ページの電子メール送信

指定された受信者へ HTML 形式でレポート ページを電子メールで送信します。 レポート ページを電子メールで送信する場合、レポートをすぐに送信するか、または後で送信するようにスケジュールを設定することができます。

次の手順に従ってください:

1. レポート ページをクリックします。
2. ［電子メール］をクリックします。

   ［電子メール送信のプロパティ］が表示されます。
3. 以下の設定を指定して［OK］をクリックします。

   電子メールのプロパティ

   指定された電子メール受信者に通知します。 電子メール通知は指定したタイム ゾーンを使用してスケジュールが設定されます。

   スケジュール オプション

   通知のスケジュールを設定するように選択した場合にのみ、スケジューリング オプションが表示されます。 特定の日の特定の時刻に実行するように通知のスケジュールを設定するか、週単位または月単位で通知のスケジュールを設定します。

レポート ページの印刷

［印刷プレビュー］ボタンを使用して印刷するレポート ページをフォーマットしてから、Web ブラウザを使用してレポートを印刷します。

次の手順に従ってください:

1. レポート ページをクリックします。
2. ［印刷プレビュー］をクリックします。

   管理コンソール は、ブラウザ ウィンドウにレポート ページを表示します。
3. Web ブラウザを使用してレポート ページを印刷します。

第 9 章: トラブルシューティング

このセクションには、以下のトピックが含まれています。

概要

管理コンソール を使用して以下を行います。

- 企業ネットワーク上に配置されたアプリケーションのパフォーマンスを運用レベルのレポートで数値化する
- 事前事後分析により、計画または計画外の変更の影響を検証する
- エンドユーザの問題を自動的に特定し、原因を分離し、インシデント発生時に診断データを収集してパフォーマンス上の問題を迅速に解決する

パフォーマンス上の問題の原因は以下の 3 つの実装上のエレメントのいずれか、またはその組み合わせである可能性があります。

- ネットワーク インフラストラクチャ（回線、過密トラフィック、ルータ、およびスイッチによって引き起こされた遅延など）
- サーバ インフラストラクチャ（CPU 処理、メモリ I/O、またはディスクの読み書きなどによって引き起こされた遅延など）
- アプリケーション アーキテクチャ（たとえば、送信のための多数の小型パケットに大型のデータ リクエストを書き込むなど）

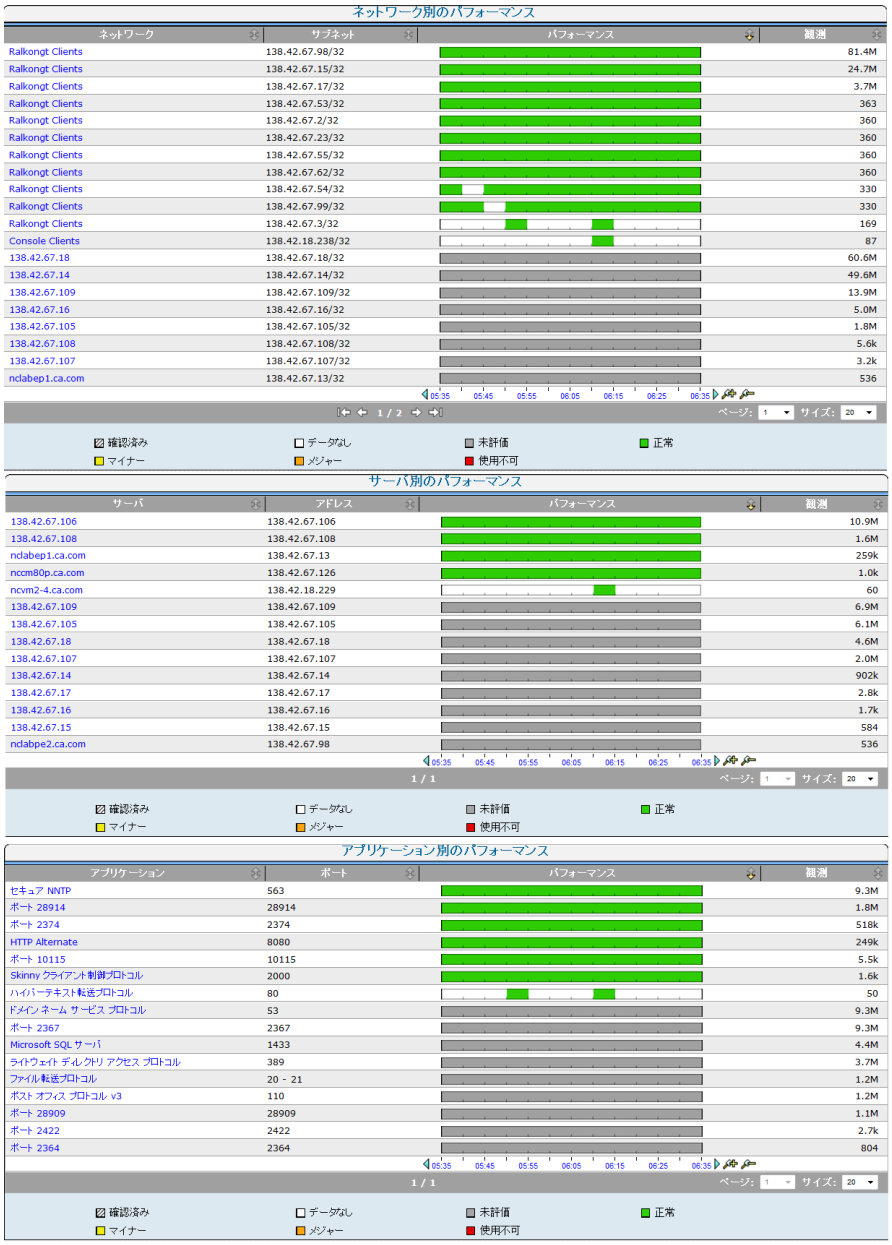
管理コンソール データを確認して分析する以下のメソッドを使用して、パフォーマンス上の問題の発生源を特定できます。

1. パフォーマンス マップやアプリケーション詳細表示を使用して、パフォーマンス上の問題を示しているアプリケーションを特定します。
2. パフォーマンス上の問題に関与した時間コンポーネントを分離します。レスポンス時間コンポーネント ビューの色は、レスポンス時間全体を構成する各構成要素を識別します。
3. ［トラフィック］、［セッション数］、［トレンド］、［レスポンス サイズ］、［QoS］、［統計］ページを調べ、パフォーマンス上の問題に関与している要因を調査します。

[操作]ページの使用

［操作］ページには、パフォーマンス エレメント全体をしきい値と比較する水平の棒グラフが表示されます。 パフォーマンスが最低の監視対象ネットワーク、サーバ、およびアプリケーションが、各表示に降順で一覧表示されます。

企業内の懸案領域を迅速に確認できます。



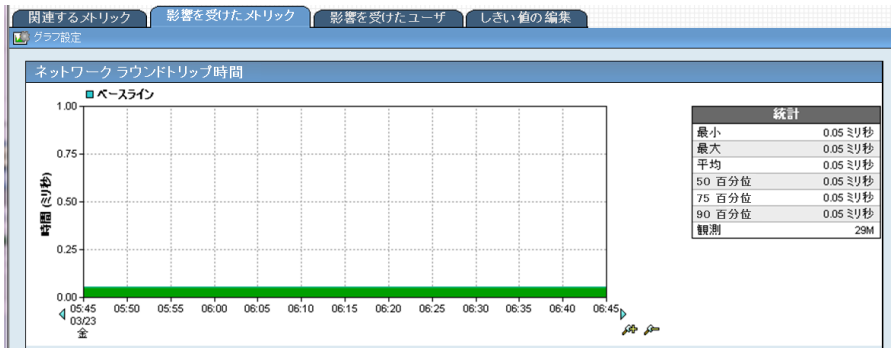
パフォーマンス上の問題に関与しているコンポーネントおよびメトリックを分離するには、その表示の最上部のパフォーマンスが最低の項目の 1 つをクリックします。

以下の例では、［ネットワーク別のパフォーマンス］ビューの最上部にあるシンガポール ネットワークが選択されています。 選択内容に焦点を当ててリフレッシュされた情報が表示されます。

このページでは、以下を確認できます。

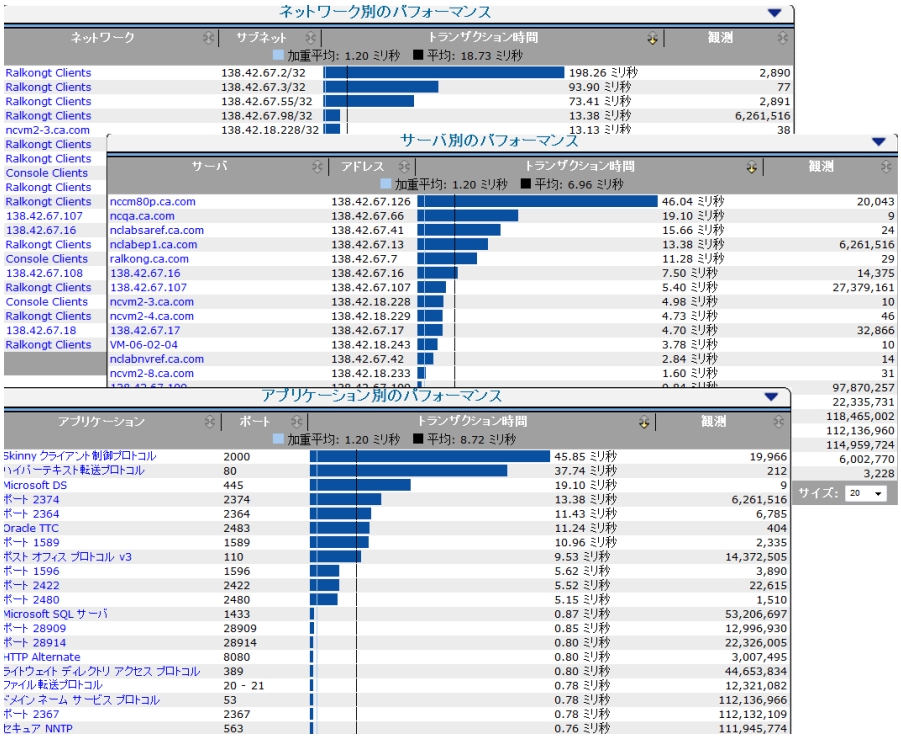
- 興味のあるメトリックおよび関連コンポーネント
- 影響を受けた項目を示すしきい値ベースの色パターン
- 選択したコンポーネントに一致するパフォーマンス パターン

パフォーマンスをさらに調査するには、一致するパフォーマンス プロファイルを選択してから［エクスプローラ］をクリックし、詳細を表示します。



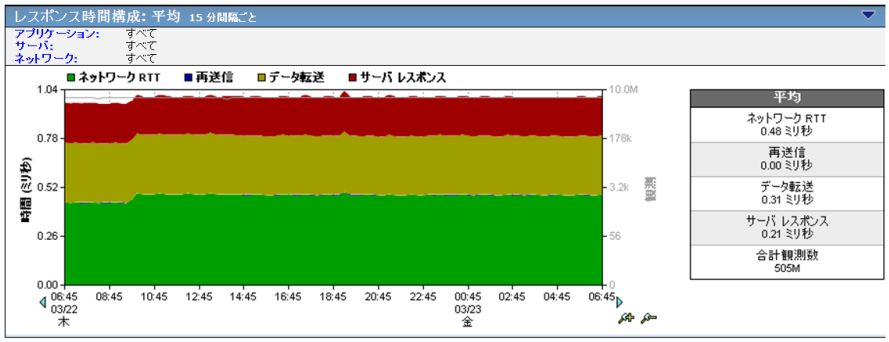
[エンジニアリング]ページの使用

パフォーマンス マップは [エンジニアリング] ページに表示されます。形式はさまざまなエレメントを比較する水平の棒グラフです。設定済みアプリケーションあたりの合計トランザクション時間が長い順（アプリケーション速度が遅い順）に、設定済みネットワークあたりのネットワーク ラウンドトリップ時間が長い順（ネットワーク速度が遅い順）に、設定済みサーバあたりのサーバ レスポンス時間が長い順（サーバ速度が遅い順）に、それぞれ上から表示されます。

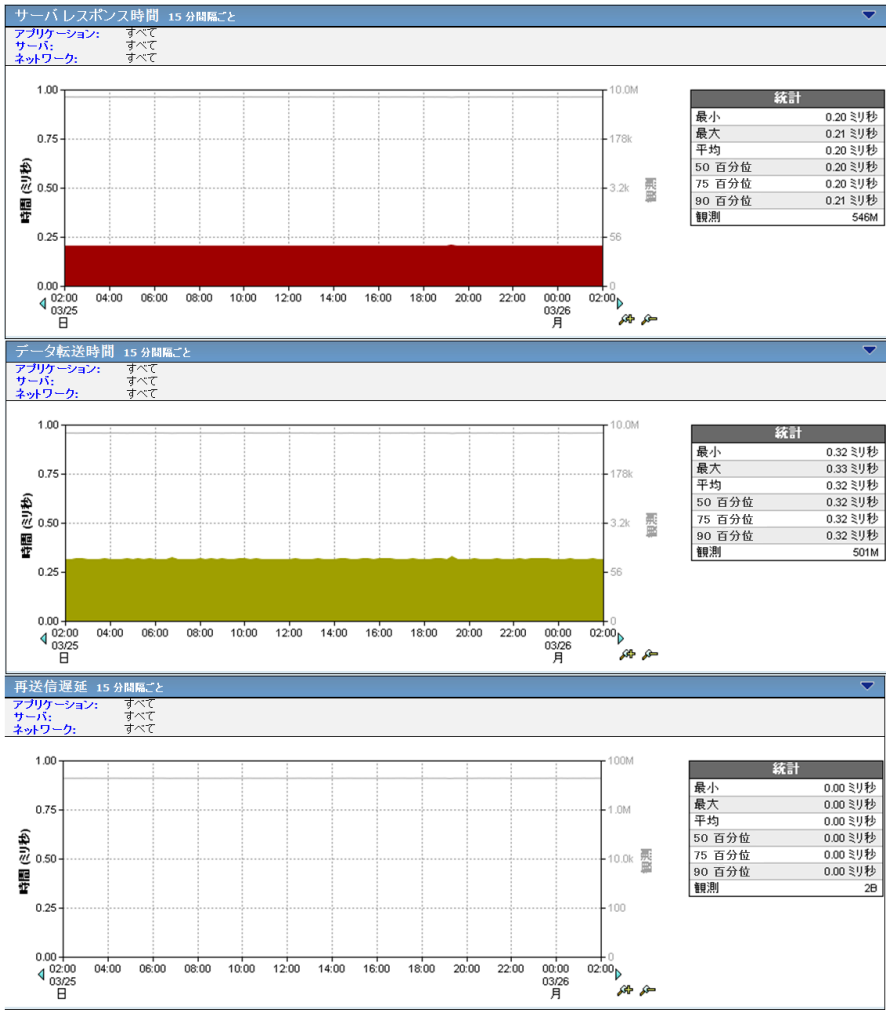


このビューに一覧表示されているいずれかの項目をクリックすると、パフォーマンス上の問題に関与するコンポーネントの時間を分離できます。ページがリフレッシュされ、選択内容に焦点を当てた詳細情報が表示されます。

以下の例では、［レスポンス時間構成: 平均］ビューが表示されます。



［レスポンス時間構成: 平均］ビューは下に並べられます。以下にその一部を示します。



重ねて表示されたコンポーネント表示を表示した場合、全体または何らかのスパイクで最も多くの部分を占める色を持つコンポーネントが、アプリケーションのパフォーマンス速度の低下にその時点で主に関与しています。

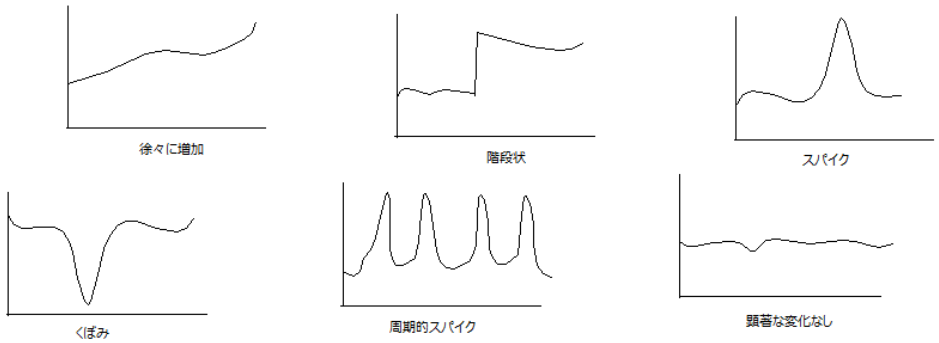
アプリケーション パフォーマンス全体の最大の遅延の一因となっているコンポーネントを特定し、個々のコンポーネント表示を下にスクロールして、パフォーマンス上の問題の範囲の調査を開始します。

以下の一般的なガイドラインに従い、パフォーマンス上の問題の範囲を調査します。

1. 合計トランザクション時間から始めます。
2. 重ねて表示された表示をドリル ダウンします。これには、15 分間隔のデータ ポイントで作成された日単位表示を使用します。 15 分間隔でパフォーマンス イベントを確認できない場合は、5 分間隔に落とします。
3. データ間隔が長い場合は、スパイク イベントを 5 分間隔の［過去 1 時間］または［8 時間］ビューで表示します。
4. 1 つのグラフで観測されたスパイクまたは色パターンを、他のメトリックで同時に発生した同様のスパイク、または低下、あるいは色パターンと相互に関連付けます。
5. 簡単に比較できるように、複数の Web セッションを開きます。また、［ズーム イン］機能と［ズーム アウト］機能を使用して、特定の時刻、特定の曜日、および月に関連する問題の大規模なパターンを見つけます。

一般的なトラブルシューティング

ネットワーク、サーバ、またはアプリケーションに関する問題の原因を絞り込むには、管理コンソール を使用します。 このセクションでは、一連のレポートに表示されたデータを解釈するために推奨されている方法を説明します。 以下の指標となるパターンに従ったメトリック表示の変化に注意してください。



メトリックのどのコンポーネントがこの変化を引き起こしているのかを確認するための調査を行います。

問題の原因の究明

1. ［操作］ページをクリックし、1 つ以上のコンポーネント（相対的なネットワーク、サーバ、アプリケーション）を選択し、［リンク: エンジニアリング］をクリックして、選択した内容が［エンジニアリング］ページに反映されていることを確認します。
2. ［表示項目］メニューの［コンポーネント］をクリックします。
3. コンポーネント レポートから調査を開始します。このレポートは、最上部が重ねて表示された、さまざまなレスポンス時間表示から構成され、それぞれがレスポンス時間全体にどのように関与しているかを示しています。コンポーネント レポートのコンポーネントは以下のとおりです。
   - レスポンス時間構成: 平均
   - サーバ レスポンス時間
   - データ転送時間
   - 再送信遅延
   - ネットワーク ラウンドトリップ時間
   - 実効ネットワーク ラウンドトリップ時間

   表示上のある時点で、表示の大半を占めるコンポーネントの色が、アプリケーションのレスポンス時間全体のほとんどの遅延の一因となっているコンポーネントであることを示しています。

   個別に検討します。

   - ［サーバ レスポンス時間］の値が高い場合は、サーバに問題がある可能性があります。
   - ［データ転送時間］の値が高い場合は、通常、アプリケーションがその問題の原因であることを示しています。
   - ［NRTT］または［再送信時間］の値が高い場合は、通常、ネットワークに問題があることを示しています。
4. コンポーネント レポートの最大の遅延に関与している、レスポンス時間のコンポーネントを特定した後、グラフのページを下にスクロールして、そのコンポーネント単独の表示を検討します。
5. 個々のコンポーネント表示では、問題が発生したときに記録された観測の数がわかります。観測の数は、問題の原因がサーバか、ネットワークかアプリケーションかを特定するのに役立ちます。

   何が「正常」であるかに関しての観測数は、以下の理解に役立ちます。

- イベントの重要性 -- 観測数が多いほど、分析中のアプリケーションのユーザへの多大な影響を示し、値が小さい場合はエンド ユーザへの影響力が限定されていた、またはその問題を分析するにはデータ ポイントが十分でなかった、あるいはその両方であることを示します。
- 対象アプリケーションの関連関与 -- 観測数が少ない場合は、分析中のアプリケーションがパフォーマンス イベントの原因でなかったことを示す場合があります。

6. 関連プロセスに従ってこれらの結果を確認し、根本的な問題領域がサーバか、ネットワークか、アプリケーションかを特定します。稀に、パフォーマンスの問題は、その原因として 2 つ以上の誘因が考えられる場合がありますが、これは異例です。

以下の可能性を検討します。

- 結果 1： 問題の原因がサーバ、ネットワーク、またはアプリケーションであることを示す肯定的な結果。 たとえば、サーバが問題だったことがデータに示されている。
- 結果 2： 問題の原因がネットワーク、サーバ、またはアプリケーションでなかったことを示す否定的な結果。 たとえば、ネットワークが問題でなかったことをデータが明白に示している。
- 結果 3： 問題の原因が最終的に残っていたネットワーク、サーバ、またはアプリケーションでなかったことを示す否定的な結果。 たとえば、アプリケーションが問題でなかったことをさらにデータが示している。

これらの結果は、サーバを原因と判定できないものの、ネットワークおよびアプリケーションは原因でないと判定できることを示しています。 このような 3 つの要素から成る結果により、根本原因を特定し、修正を進める確信を持つ場合があります。

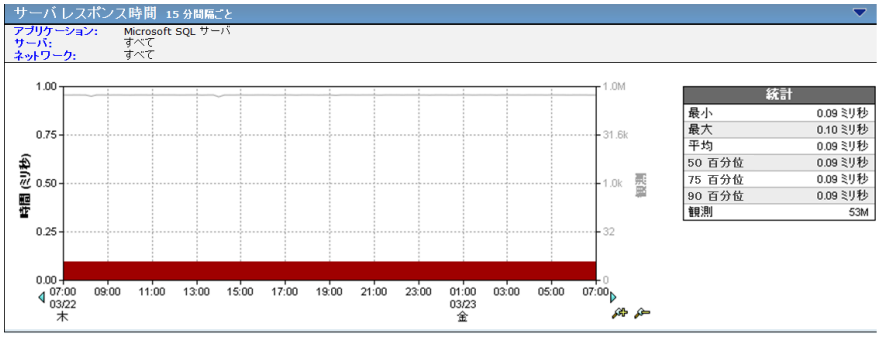
注: マウス カーソルをそのままの位置にするか、レスポンス時間コンポーネント ビューに着目し、下向き矢印キーでページを下方にスクロールして、下部のビューをマウス カーソルの下に表示させます。矢印キーでページの下方へ移動しても、マウス ポインタは画面の同じ位置に残るため、［コンポーネント］ビューの所定位置と、ページの下部にある表示とを同じ位置に簡単に並べることができます。

サーバ レスポンス時間の増加

サーバ レスポンス時間の増加は観測数に関連しています。増加も減少も、以下の分析で検討します。

サーバ レスポンス時間および観測数の増加

サーバ レスポンス時間および観測数の増加は、パフォーマンスの問題がサーバに関連していることを強く示唆しています。 この結論は、これを他の相対的なデータと相互に関連付けることによって裏付けられます。



サーバと関連付けられたパフォーマンスの問題は、データ センターとしての同じ建物内のユーザなどのローカル ネットワーク セットでも、WAN 接続上のユーザなどのリモート ネットワーク セットでも、すべてのネットワーク セットや集約にわたって確認できます。

サーバ レスポンス時間と観測数の両方が、パフォーマンスの問題が観測されたのと同じ時点でピークとなっている場合、同じ時点の以下のデータセットを確認します。

- トラフィック -- データ ボリュームおよびデータ転送速度

  データ ボリューム/転送速度が増加したかどうか確認します。 大量のデータをネットワークに書き込んでいる場合、サーバは通常以上に稼働します。 サーバ レスポンス時間の増加に一致するデータ ボリュームの異常な増加は、サーバが要求に応じきれていないことを示します。

- セッション -- 接続セットアップ時間、TCP/IP セッション、未対応の TCP/IP セッション リクエスト、TCP/IP セッション時間

  サーバ接続時間に同時増加があるかどうかを確認します。これがある場合、OS カーネルで新しいセッション リクエストへの応答にかかる時間が増加している可能性を示します。

  TCP/IP セッションの数が大幅に（たとえば 10%）増加したかどうか確認します。追加の TCP セッションおよび付随するアプリケーション リクエストは、サーバからより多くのリソースを必要とし、その処理能力に負担をかけます。

  未対応の TCP/IP リクエスト数に異常な増加があったかどうかを確認します。大幅な増加は、サーバのハードウェア リソースの負荷が過剰になっていることを顕著に示します。

- QoS -- ユーザ、パケット ロスの割合、ユーザ Goodput、1 ユーザあたりのコンポジットレート

  ユーザ数に大幅な増加があるかどうかを確認します。 ユーザの数の増加は、サーバ リソースにの需要を増加させます。 特定数のユーザがサーバ レスポンス時間を低下させる原因となったポイントは、サーバのアップグレード、または同様に設定されたサーバ間のアプリケーションの負荷分散についての今後に向けての次善策を講じるポイントと解釈できます。

- 統計 -- レスポンス時間構成: 標準偏差、サーバ レスポンス時間パーセンタイル、データ転送時間パーセンタイル、再送信遅延時間パーセンタイル、ネットワーク ラウンドトリップ時間パーセンタイル

サーバ レスポンス時間の標準偏差、パーセンタイル、またはその両方に増加があったかどうかを確認します。 これは、平均から大幅に離れた場所にある「周辺」データ ポイントで見受けられるような、一貫性がなく、散発的なサーバのパフォーマンスであることを示す可能性があり、サーバ ベースの問題であることを強く示しています。

サーバ レスポンス時間の増加と観測数の減少

サーバ レスポンス時間が増加し、観測数が減少している場合は、2 つのきわめて異なるイベントを示唆している可能性があります。

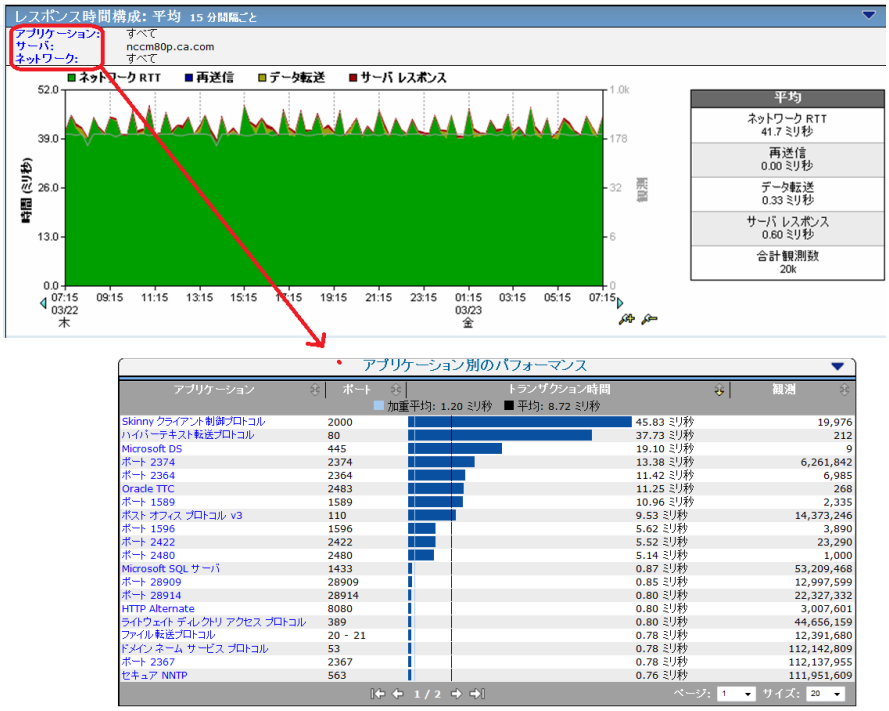
- サーバ上の別のアプリケーションが［サーバ レスポンス時間］を増加させています。 このアプリケーションは 管理コンソール によって監視される場合と監視されない場合があります。
- CPU、メモリ、または NIC のサーバは不安定なため、アプリケーション サービスは信頼できません。 これが原因で散発的なサービス ロストとなったり、最終的にはサービスが完全に停止する場合があります。

観測されたパフォーマンスの問題と同時に、サーバ レスポンス時間が急増する一方で、観測数が減少した場合は、以下の手順を実行し、パフォーマンスの低下の原因となったイベントを特定します。

SRT のスパイクと観測数の減少の原因の究明

まず、サーバ上の別のアプリケーションがアクティブかどうかを判断します。

1. ［エンジニアリング］ページをクリックします。
2. 任意の［レスポンス時間］ビューから以下の設定を選択します。
   - アプリケーション -- すべて
   - サーバ -- サーバの名前を選択します。
   - ネットワーク セット -- すべて
3. このサーバによって監視されているすべてのアプリケーションを表示するには、［レスポンス時間構成］ビューのヘッダにある青いハイパーテキストのアプリケーションをクリックします。



別のアプリケーションが結果のパフォーマンス マップに表示された場合、以下の手順を繰り返し、パフォーマンスの問題の原因がそのアプリケーションかどうかを特定します。

特定のアプリケーションの観測数が、パフォーマンスの問題が報告されたのと同時に増加しているかどうかが重要です。

4. 他のアプリケーションが結果のパフォーマンス マップに表示されていない場合は、左向きの矢印を使用して［エンジニアリング］ページに戻ります。 水平メニューにある［トレンド］をクリックし、このパフォーマンス イベントが過去数週間および数か月にわたり何らかのパターンを示しているかを確認します。 パターンが表示される場合は、突出した反復日時の問題の特定の時間でプロトコル アナライザを使用し、問題の原因となったアプリケーションを特定します。

   サーバ上でプライマリ アプリケーションの問題を生じさせるアプリケーションの例は以下のとおりです。

   - 夜間に実行されたバックアップ
   - ウィルス対策ソフトウェアへのアップグレード
   - サーバ容量またはパフォーマンスを測定するために他のチームによって使用されるエージェント

   バックアップ処理は通常、バックアップ ソフトウェア エージェントを通じて定時にスケジュール設定されます。 そのため、［トレンド］ビューには、24 時間周期、24 時間おき、またはその他バックアップ スケジュールによる周期と同時にサーバ レスポンス時間の周期的なスパイクを示すパターンが表示されます。

   ウィルス対策定義へのアップグレードは、通常、週単位で、または「必要に応じて」緊急時に実行されます。 自動更新リリース スケジュールを決定するには、ウィルス対策ソフトウェア ベンダーまたはデスクトップ/セキュリティ チーム、あるいはその両方に相談してください。 アプリケーション開発チームがサードパーティ エージェントをインストールしたり、パフォーマンス エージェントをソフトウェアにエンコードする場合もあります。 変更通知を確認して、サーバ上のソフトウェアに加えられた変更がパフォーマンスの問題が始まる直前に行われたものかどうかを判断します。

サーバ/アプリケーション サービスの信頼性が失われたかどうかを判断します。

1. サーバ レスポンス時間が承認済みの値を超えた場合、管理コンソールにしきい値を設定して調査を開始します。 管理コンソール は、自動的に CPU やメモリ使用率などの関連情報を収集します。

2. サーバ システム ログの確認は、アプリケーションの安定性に影響している可能性のあるエラーやその他のイベントを明らかにできます。
3. サーバに面するスイッチ ポートおよびサーバ NIC を確認し、以下のテーブルから二重化および速度設定が正しく設定され、エラーがないようにします。

サーバ	スイッチ	結果
自動	自動	全二重、自動速度
自動	手動	半二重、手動速度
手動	自動	半二重、手動速度
手動 - 完全	手動 - 完全	全二重、手動速度（同じ速度、10 Mbps、100 Mbps、1000 Mbps が両端に設定されていると見なす）

ネットワーク ラウンドトリップ時間（NRTT）の増加

ネットワーク ラウンドトリップ時間は以下の等式によって定義できます。

```
NRTT = S_Delay + Q_Delay + R/SW_Delay + D_Delay + P_Delay
```

各項目の説明：

S_Delay

シリアル化遅延 - ［（フレーム サイズ × 8）/（アクセス速度］）

Q_Delay

キュー遅延 - 使用率および S_Delay に依存

R/SW_Delay

ルーティング/スイッチ遅延 - 通常 1 つのホップあたり 1 ミリ秒とほぼ同じ

D_Delay

距離遅延 - 移動すべき距離での伝達遅延 通常、ファイバの場合は 5ìs/km、銅の場合は 5.56ìs/km、衛星は 3.3ìs/km

P_Delay

プロトコル遅延 - 転送または上位レベル プロトコルによって追加された遅延

例： 共有イーサネットの CSMA/CD

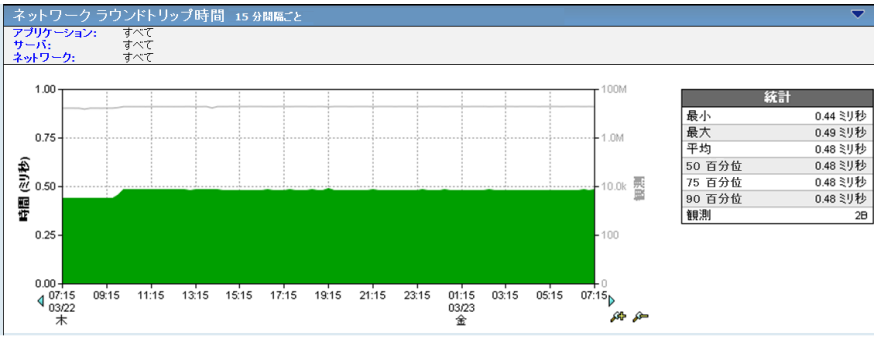
通常、アプリケーションと関連付けられた NRTT の増加は、前述の任意の変数の増加によって引き起こされます。 ただし、NRTT の増加の典型的な原因は、それらが通常発生する順番で一覧表示されます。

- 回線使用率の増加による Q_Delay の増加の結果の深いネットワーク キュー
- 距離的に長い保護/冗長パスへのキャリアまたはエンタプライズ フェールオーバーによる D_Delay の増加
- ネットワーク エラーによる R/SW_Delay の増加
- 低帯域幅の冗長パスへのエンタプライズ フェールオーバーによる S_Delay の増加

ネットワークの問題が単一リモートサイトに限定されているかどうかを特定するには、影響を受けたリモートサイトの NRTT のスパイクを、サーバからの距離、帯域幅、およびユーザ数に関して比較可能な他のサイトと対比し、比較します。 NRTT が複数のサイトで同時に増加または急増した場合、問題はキャリア関連である可能性があるか、ルーティング プロトコルの不安定さによって引き起こされた場合があります。

NRTT および観測数の増加

NRTT、および観測数の増加は、パフォーマンスの問題がネットワークのアプリケーション使用率に基づくものであることを強く示唆するインジケータです。 このインジケータの強さは、他の対応するデータ ポイントと相関させることで裏付け、問題の原因がネットワークであるという完璧な結果を構築することができます。



NRTT と観測数の両方が、パフォーマンスの問題が観測されたのと同じ時点でピークとなっている場合、同じ時点の以下のデータ セットを確認します。

- コンポーネント -- 再送信遅延

  再送信の長さが増加したかどうか確認します。 再送信は、ネットワーク キューが、空になるよりもはやい速度で充填され、パケット ドロップや関連 TCP の再送信を招くことを示します。

- セッション -- 接続セットアップ時間および TCP/IP セッション

  ネットワーク接続セットアップ時間に同時増加があるかどうかを確認します。 この増加は、ネットワーク内の事前に確立された他のセッションによって増加中のキューの深さにより、3 方向 TCP ハンドシェークがネットワーク上で遅延していることを示します。

  TCP/IP セッションの数が大幅に（10% を超えて）増加したかどうか確認します。 追加の TCP セッションおよび付随するアプリケーション データはより多くの帯域幅を必要とします。

- トラフィック -- データ ボリュームおよびデータ転送速度

  データ ボリューム/転送速度が増加したかどうか確認します。 ネットワーク上のよりデータ ボリュームが高くなると、キュー深さおよび関連する遅延を増加させます。 NRTT の増加に一致するデータ ボリュームの異常な増加は、サーバが要求に応じきれていないことを示します。

- QoS -- ユーザ

  ユーザ数に大幅な増加があるかどうかを確認します。 ネットワーク使用率の増加は、通常、ユーザ数の増加に一致します。 特定数のユーザが NRTT を低下させるポイントは、他の同様のサイトのネットワーク帯域幅をアップグレードするための今後に向けての次善策を講じるポイントと解釈できます。

- 統計 -- レスポンス時間構成 : 標準偏差、ネットワーク ラウンドトリップ時間パーセンタイル

  NRTT の標準偏差、パーセンタイル、またはその両方に増加があったかどうかを確認します。 この増加は、より多くの「周辺」データポイント（平均からかなり離れた距離にあるポイントなど）で証拠づけられる、ネットワークによる一貫性のない散発的なパフォーマンスを示し、ネットワーク ベースの問題であることを強く示唆します。

NRTT の増加と観測数の減少

NRTT が増加する一方で観測数が減少する場合は、2 つのきわめて異なるイベントを示唆している可能性があります。

- ネットワーク上の別のアプリケーションが NRTT の増加の原因となっています。 このアプリケーションは 管理コンソール によって監視される場合と監視されない場合があります。
- ネットワークの不安定さ（リンク障害、ルーティングの拡散、STP の拡散、キャリア フェールオーバー、その他のエラー）により、アプリケーション サービスの信頼性が低下しています。これが原因で散発的なサービス ロスとなったり、最終的にはサービスが完全に停止する場合があります。

パフォーマンスの問題が観察されたのと同時に NRTT が急増する一方で観察数が低下した場合は、以下のアクションを実行し、前述のどのイベントがパフォーマンスの低下の原因かを特定します。

パフォーマンスの低下原因の究明

ネットワーク上の別のアプリケーションがアクティブかどうかを判断します。

1. ［エンジニアリング］ページをクリックします。
2. 任意の［レスポンス時間］ビューから以下の設定を選択します。
   - アプリケーション -- すべて
   - サーバ -- すべて
   - ネットワーク セット - 以下のようなリモート サイト集約など、関連する集約
3. ［レスポンス時間構成］ビューで、このサーバ上の 管理コンソール によって監視されているすべてのアプリケーションを表示するには、青いハイパーテキストの[アプリケーション]リンクをクリックします。

   別のアプリケーションが結果のパフォーマンス マップに表示された場合、そのアプリケーションに対してこれらの手順を再度実行し、それがパフォーマンスの問題の原因かどうかを確認します。

   パフォーマンスの問題が報告されたのと同時に観測数が増加したかどうかが重要です。
4. 他のアプリケーションが結果のパフォーマンス マップに表示されていない場合は、左向きの矢印を使用してメインの［エンジニアリング］ページに戻ります。 水平メニューから［トレンド］を選択し、このパフォーマンス イベントが過去数週間および数か月にわたり何らかのパターンを示しているかを確認します。 パターンが表示される場合、NetFlow の履歴データ、IP アカウンティング、またはプロトコル アナライザを使用して、アプリケーションが問題の時間にネットワークを飽和させていたかどうかを特定します。 履歴データが使用可能でない場合、突出した反復日時の問題の時刻を手動で確認し、問題の発生源のアプリケーションを特定します。

   ネットワーク上でプライマリ アプリケーションの問題を生じさせるアプリケーションの例は以下のとおりです。
   - リモート サイト間のレプリケーションまたはバックアップ データ
   - サーバ間の大規模なファイル転送
   - サブレート WAN リンク（<T1）上で大量のデータをストリーミングしているユーザ

- 複数のサブレート WAN リンクにまたがるたウィルス対策ソフトウェアのアップグレード

ネットワークの信頼性が低下しているかの特定

1. サーバに面するスイッチ ポートおよびサーバ NIC を確認し、以下のテーブルから二重化および速度設定が正しく設定され（以下のテーブルを確認すること）、エラーがないようにします。

サーバ	スイッチ	結果
自動	自動	全二重、自動速度
自動	手動	半二重、手動速度
手動	自動	半二重、手動速度
手動 - 完全	手動 - 完全	全二重、手動速度（同じ速度が両端上で設定されると仮定）

2. NRTT が承認済みの値を超過したときに調査を開始するしきい値を 管理コンソール に設定し、設定上の問題またはネットワーク エラーのためにネットワークの信頼性が低下しているかどうかを特定します。 管理コンソール は、ルータおよびスイッチからの関連情報を自動的に収集します。
3. ルータおよびスイッチのログ、インターフェース エラー、変更レコードを確認し、ネットワークの安定性に影響を及ぼす、ルーティングの分岐や回線エラーなど、ネットワークのイベントを見つけます。

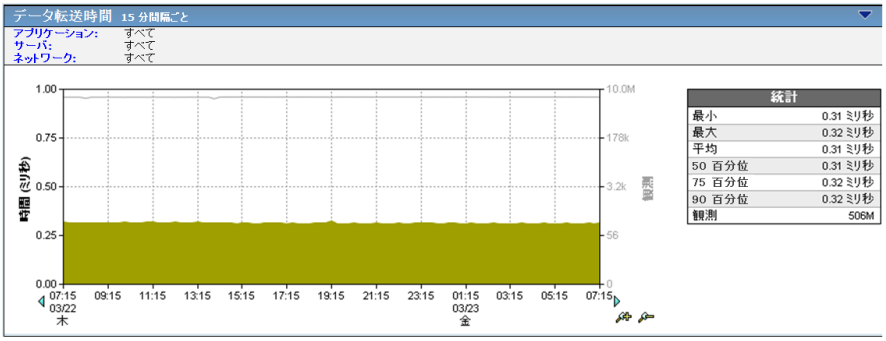
データ転送時間の増加

データ転送時間の増加は観測数に関連しています。増加も減少も、以下の分析で検討します。

データ転送時間および観測数の増加

データ転送時間および観測数の増加は、パフォーマンスの問題がアプリケーションに関連していることを示す良いインジケータです。

このインジケータの強さは、対応するデータ ポイントと相関させることで大幅に増強され、問題の原因がアプリケーションであるという完璧な結果を構築することができます。



アプリケーションと関連付けられたパフォーマンスの問題は、使用可能な帯域幅および距離によって引き起こされる遅延に応じてサイトごとに変わります。 同じサイトの一部のアプリケーション ユーザがアプリケーションのパフォーマンスについて不満を言うのは珍しくありません。 複数のアプリケーションにわたって照会し、データ転送時間のスパイクが、同じネットワーク パスを使用するアプリケーション、または同じサーバを起点とするアプリケーションに相関できるかどうかを確認します。 相関できる場合、その問題はネットワークまたはサーバ内にある場合があります。

データ転送時間の増加が単一のサーバ上の単一のアプリケーションに限定される場合、および観測されたパフォーマンス問題と、同じ時点の観測数の両方が急増する場合、その時間の以下のデータ セットを確認します。

- トラフィック -- データ ボリュームおよびデータ転送速度

  データ ボリューム/転送速度が増加したかどうかを確認します。 アプリケーションが低速の複数の WAN リンク、または距離的に遠くのサイトへ効率的に書き込んでいない場合があります。

- コンポーネント -- ネットワーク ラウンドトリップ時間、再送信遅延、サーバ レスポンス時間

  ボリュームが増加したときに NRTT と再送信遅延がほぼ一定のままだったかどうかを確認します。ネットワーク ラウンドトリップ時間がほぼ一定で許容範囲内であり、パケット ドロップがわずかである場合は、アプリケーションの問題を示唆しています。

  サーバ レスポンス時間が増加したかどうかを確認します。セッション数またはユーザ数、未対応の TCP セッション リクエスト、および NRTT の増加を伴わないサーバ レスポンス時間の増加は、問題がアプリケーションであることを示唆します。

- セッション -- 接続セットアップ時間、TCP/IP セッション、未対応の TCP/IP セッション

  サーバ接続セットアップ時間に同時増加があるかどうか確認します。このような増加は、OS カーネルが新しいセッション リクエストへの応答にかかった時間を増加させたことを示します。

  TCP/IP セッションの数が大幅に（10% を超えて）増加したかどうか確認します。追加の TCP セッションおよび付随するアプリケーション リクエストは、サーバからより多くのリソースを必要とし、その処理能力に負担をかけます。

未対応の TCP/IP リクエストが一定のままだったかどうか確認します（ゼロが最適）。アクティブ セッションの確立中に未対応の TCP リクエストがない場合は、サーバ リソースがユーザにとって使用可能だったことを示し、パフォーマンス問題とのサーバの関連性が軽減されます。

- QoS -- ユーザ

  パフォーマンス イベントその前後およびその最中に一定数のユーザがいたかどうかを確認します。パフォーマンス イベントの時間と同時にサーバに新規のユーザがいない場合は、絶対サーバ負荷が要因となる傾向があります。

- 統計 -- レスポンス時間構成： 標準偏差、データ転送時間パーセンタイル

  NRTT の付帯増加やサーバ レスポンス時間の大幅な増加なしに、データ転送時間またはパーセンタイルの標準偏差に増加あったかどうか確認します。このような増加は、より多くの「周辺」データポイント（平均からかなり離れた距離にあるポイントなど）で証拠づけられるアプリケーションによる一貫性のない散発的なパフォーマンスを示し、アプリケーション ベースの問題であることを示す良いインジケータです。

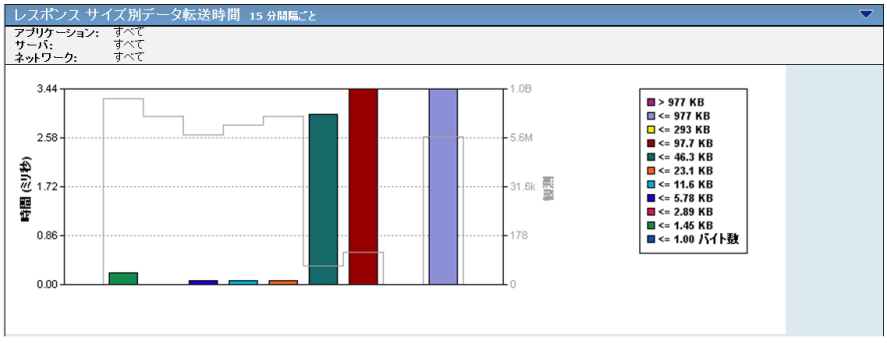
データ転送時間 = 0（ピンポン アプリケーション）

「ピンポン」アプリケーションは、ほとんどまたはすべてのリクエストに単一のパケットのレスポンスを送信します。これは、アプリケーションの問題です。 管理コンソール は、クライアント データ リクエストへの最初のアプリケーション レスポンスと関連付けられたタイム スタンプからクライアント データ リクエストに対する最後のアプリケーション レスポンスと関連付けられたタイム スタンプを引くことにより、データ転送時間を計算します。タイム スタンプが等しい場合、1 つのパケットのみがクライアント リクエストに応えてアプリケーションによって送信されたため、結果は 0 となり、クライアントが次のパケットをリクエストする前に、アプリケーション レイヤでこのパケットの受信を確認する必要があります。

トランザクション全体の完了に必要なデータ量が数十万から数百万バイトに達する場合、クライアントはパケットごとに 1 つ以上の NRTT が配信され、アプリケーションによって受領確認されるまで待機する必要があるため、これがアプリケーションにはスループットの大きな問題となる可能性があります。 クライアントが単一のリクエストでのすべてのデータを要求した場合、アプリケーションは、TCP のアクティブ ウィンドウで送信できるバイト数と同じバイト数を一度に複数パケットで送信して応答します。 これにより、データの転送に必要な往復数を大幅に減少させ、アプリケーションのパフォーマンスを引き上げます。

［データ転送時間］がゼロと等しい場合にこのシナリオを確認するには、次の手順に従います。

1. ［表示項目］メニューで、［レスポンス サイズ］をクリックします。
2. ［レスポンス サイズ別データ転送時間］ビューまでスクロールし、1.45 KB 未満のデータ転送（イーサネット フレームに基づく 1 つのセグメントまたはパケット）の数が以下のビューの最も顕著なバーであるかどうかを特定します。 これは、ほとんどのパケットに最低限のデータが含まれることを示します。



データ転送時間の増加と観測数の減少

データ転送時間が増加する一方で観察数が減少している場合は、通常、その問題はサーバまたはネットワークの問題と関連することを示唆しています。 サーバ レスポンス時間がデータ転送時間と共に増加した場合は、サーバ リソースおよびアプリケーション コードを確認します。

NRTT と再送信遅延がデータ転送時間と共に増加した場合は、問題のネットワーク セグメントを分離してから、ネットワーク パスと関連デバイスを確認します。

オペレーション

通常、エンド ユーザおよび企業経営者は、パフォーマンスの問題を以下の 3 つの方法のいずれかでオペレーション センターやサポート チームに報告します。

- アプリケーションにかかわるパフォーマンスの問題がある。
- ネットワークにかかわるパフォーマンスの問題がある。
- サーバにかかわるパフォーマンスの問題がある。

［操作］ページでは、シンプルかつ簡単な方法を使用して、パフォーマンスの問題のレポートを直接扱います。 パフォーマンスの問題が報告された場合、その問題を報告している担当者から以下の問題に関する情報を収集することが重要です。

- パフォーマンスの問題を示しているアプリケーションおよびサーバの名前
- エンド ユーザの場所または IP アドレス、あるいはその両方、ローカルまたはリモート オフィスの場所（エンドユーザやローカルまたはリモート オフィスのネットワークを特定するため）
- パフォーマンスの問題を最初に気付いた時刻、およびその問題が継続中かどうか
- パフォーマンスの問題の履歴 -- 再発しているように思うか -- 1 日に複数回か、他の日の同時刻か、常に月末か
- ユーザが関連がある可能性があると考える、他の低速なアプリケーションやサーバなどの他のパフォーマンスの問題。

例 1: アプリケーションに関するパフォーマンスの問題

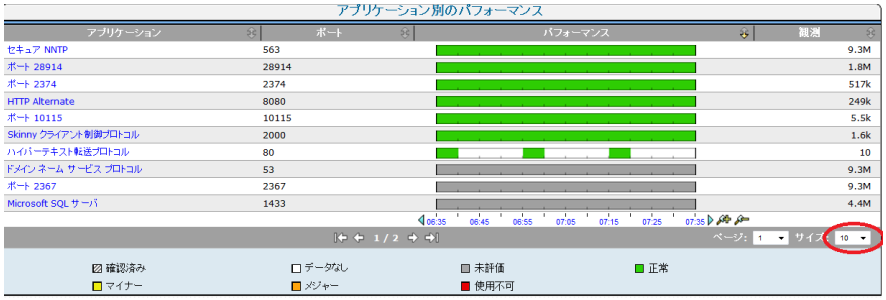
本社のユーザがアプリケーションに問題が発生していると報告しました。

アプローチ

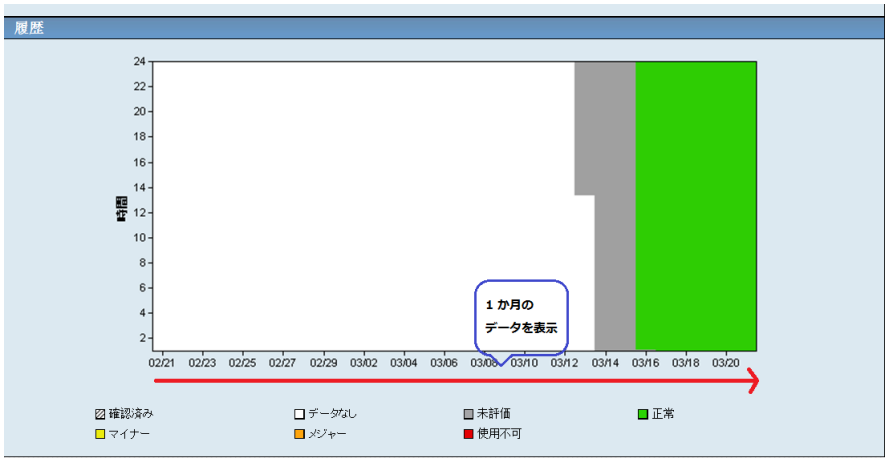
ユーザから問題に関する情報を収集し、トラブル チケットを作成します。

1. ［操作］ページをクリックします。
2. ［表示項目］メニューの［アプリケーション］をクリックします。

   ［アプリケーション別のパフォーマンス］ページが表示されます。
3. 報告されたアプリケーションがリストの上位に通知されているかどうかを特定します。 通常、上位 10 位以内に入っています。 そのアプリケーションが上位 10 位以内に表示されていない場合は、そのアプリケーションがリスト内に表示されるまで、［サイズ］の設定値を大きくしていきます。 そのアプリケーションがリストにない場合は、CA Application Delivery Analysis によって監視されていない場合があります。



4. アプリケーション名の右側にあるパフォーマンス バーをクリックし、詳細ページを表示します。詳細ページでネットワークまたはサーバのメトリックをクリックすると、データの範囲を絞り込むことができます。
5. ネットワークまたはサーバがわかっている場合は、適切なパフォーマンス バーを選択して範囲をさらに絞り込みます。
6. ［表示項目］メニューで、［履歴］をクリックします。
7. アプリケーションの履歴を確認し、使用不可状態やパフォーマンス低下の規則的なパターンを特定し、注意します。



8. ［表示項目］メニューで、［パフォーマンス］をクリックしてから［エクスプローラ］をクリックし、トラブルシューティングを開始することもできます。 また、ページ最上部の［リンク: エンジニアリング］をクリックすると、レスポンス時間コンポーネントの各遅延ページが表示され、徹底的なトラブルシューティングを実行できます。 ページ最上部のクエリ選択ボックスの選択したアプリケーション名、およびサーバまたはのネットワーク名に注目します。

9. ［レスポンス時間構成： 平均］ビューを確認し、報告された問題が発生した時間を正確に特定します。 その時点の最大関与コンポーネントを特定します。

   - サーバ レスポンス時間（SRT）がこの時点の大半を占めている場合は、サーバ レスポンス時間 (P. 170)の増加を確認します。
   - ネットワーク ラウンドトリップ時間（NRTT）または再送信遅延、あるいはその両方がこの時点の大半を占める場合は、「ネットワーク ラウンドトリップ時間（NRTT）の増加 (P. 176)」を確認します。
   - データ転送時間がこの時点の大半を占める場合は、データ転送時間の増加 (P. 181)を参照します。
   - すべてのコンポーネントが履歴の時系列について正常である場合は、ユーザのコンピュータに問題がある場合があります。

例 2: サーバに関するパフォーマンスの問題

本社のエンド ユーザが、サーバに問題が発生していると報告しました。

アプローチ

ユーザから問題に関する情報を収集し、トラブル チケットを作成します。

1. ［操作］ページをクリックします。
2. ページの中間までスクロールし、［サーバ別のパフォーマンス］ビューを確認します。
3. 報告されたサーバがリストの上位に通知されているかどうかを特定します。 通常、上位 10 位以内に入っています。 サーバが上位 10 位以内に表示されていない場合は、［設定］をクリックし、［サーバ リスト］からサーバを選択します。

4. サーバ名の右側にあるパフォーマンス バーを選択し、詳細ページを表示します。
5. ネットワークまたはアプリケーションがわかっている場合は、適切なパフォーマンス バーを選択して範囲を絞り込みます。
6. ［表示項目］メニューで、［履歴］をクリックします。
7. サーバの履歴を確認し、規則的なパターンを特定し、注意します。
8. ［表示項目］メニューで［パフォーマンス］をクリックし、［エクスプローラ］をクリックしてトラブルシューティングを開始することもできます。 また、ページ最上部の［リンク: エンジニアリング］をクリックすると、レスポンス時間コンポーネントの各遅延ページが表示され、徹底的なトラブルシューティングを実行できます。 ページ最上部のクエリ選択内容ボックス内の選択されたサーバ名、あるいはアプリケーション名またはネットワーク名に注目します。
9. 最初の表示である［レスポンス時間構成: 平均］ビューを確認し、問題が発生したと報告された表示の時刻を正確に特定します。 その時点の最大関与コンポーネントを特定します。
   - サーバ レスポンス時間（SRT）がこの時点の大半を占めている場合は、サーバ レスポンス時間 (P. 170)の増加を確認します。
   - ネットワーク ラウンドトリップ時間（NRTT）または再送信遅延、あるいはその両方がこの時点の大半を占める場合は、「ネットワーク ラウンドトリップ時間（NRTT）の増加 (P. 176)」を確認します。
   - データ転送時間がこの時点の大半を占める場合は、データ転送時間の増加 (P. 181)を参照します。
   - すべてのコンポーネントが履歴の時系列に関して正常である場合は、ユーザのコンピュータに問題がある場合があります。

例 3: ネットワークに関するパフォーマンスの問題

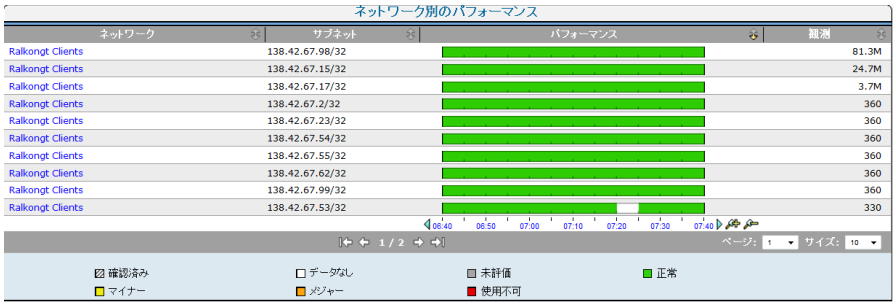
本社のエンド ユーザが、特定のネットワークに問題が発生していると報告しました。

アプローチ

ユーザから問題に関する情報を収集し、トラブル チケットを作成します。

1. ［操作］ページをクリックします。
2. ［表示項目］メニューの［ネットワーク］をクリックします。

   ［ネットワーク別のパフォーマンス］ビューが表示されます。
3. 報告されたネットワークがリストの上位 N 位に通知されているかどうかを特定します。そのネットワークが上位 N 位以内に表示されていない場合は、そのネットワークがリスト内に表示されるまで、［サイズ：］の設定値を大きくしていきます。 ネットワークがリスト内に表示されない場合は、CA Application Delivery Analysis によって監視されていない場合があります。



4. ネットワーク名の右側にあるパフォーマンス バーを選択し、詳細ページを表示します。 詳細ページでアプリケーションまたはサーバのメトリックをクリックすると、データの範囲を絞り込むことができます。
5. アプリケーションまたはサーバがわかっている場合は、適切なパフォーマンス バーを選択して範囲をさらに絞り込みます。
6. ［表示項目］メニューで、［履歴］をクリックします。
7. ネットワークの履歴を確認し、規則的なパターンまたはトレンドを特定し、注意します。
8. ページ最上部の［リンク： エンジニアリング］を選択し、レスポンス時間コンポーネントの各遅延ページを表示します。 ページ最上部のクエリ選択内容ボックス内の選択したネットワーク名、サーバまたはアプリケーション名に注目します。
9. 最初の表示である［レスポンス時間構成： 平均］ビューを確認し、問題が発生したと報告された表示の時刻を正確に特定します。 その時点の最大関与コンポーネントを特定します。
   - サーバ レスポンス時間（SRT）がこの時点の大半を占めている場合は、サーバ レスポンス時間および観測数の増加 (P. 170)を確認します。
   - ネットワーク ラウンドトリップ時間（NRTT）または再送信遅延、あるいはその両方がこの時点の大半を占める場合は、NRTT および観測数の増加 (P. 177)を確認します。
   - データ転送時間がこの時点の大半を占める場合は、データ転送時間および観測数の増加 (P. 182)を参照します。
   - すべてのコンポーネントが履歴の時系列に関して正常である場合は、ユーザのコンピュータに問題がある場合があります。

調査

以下の方法で調査を開始します。

- 調査を手動で開始する
- 調査のスケジュールを設定する
- 調査活動でインシデント レスポンスを作成します。この種の調査は、インシデント レスポンスが関連付けられている項目に対してインシデントがオープンしたときに、自動で開始されます。

ルータ、スイッチ、または他の SNMP 対応デバイスを手動で調査するには、CA Application Delivery Analysis 管理者がネットワーク デバイスとしてそれを追加するようリクエストします。

データ センターを通じてのユーザからのデータ フローの分析

低品質のパフォーマンスに見舞われているユーザの診断に役立てるため、ユーザ デバイスからデータ センターまでのトレース ルート調査を開始し、問題領域を明らかにすることができます。

これを行う 1 つの方法として、ユーザ デバイスに移動して、そこからトレース ルートを開始します。管理コンソール を使用すると、CA Application Delivery Analysis にユーザ デバイスを追加してから、そのデバイスまでのトレース ルートを実行できます。

ユーザからデータ センターまでのデータ フロー レポートの生成

パフォーマンスが低品質のネットワーク上のユーザを探すには、［操作］ページを使用します。

1. ［操作］ページをクリックします。
2. ［表示項目］メニューの［ネットワーク］をクリックします。

   ［ネットワーク別のパフォーマンス］ページが表示されます。
3. ネットワーク名をクリックし、[エクスプローラ]をクリックします。

   ［メトリック詳細］ページが表示されます。
4. ［影響を受けたユーザ］タブをクリックします。

   ユーザ レポートが表示されます。
5. /24 または/32 のサブネット マスクを含む[IP アドレス/マスク]フィールドに注意します。
6. 管理コンソール の[管理環境]ページを使用して、対応するネットワーク デバイスを CA Application Delivery Analysis に追加します。
7. 管理コンソール の［インシデント］ページを使用して、トレース ルート調査を開始します。

影響を受けたデバイスの特定

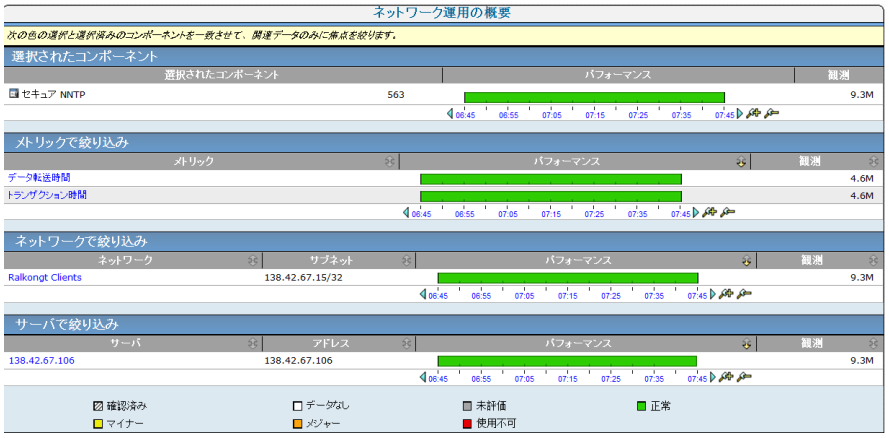
アプリケーションでパフォーマンスが低下すると、そのアプリケーションにアクセスするいくつかのネットワークに影響を与える可能性があります。

アプリケーション パフォーマンス

［操作］ページのアプリケーション別のパフォーマンス レポートに、管理コンソール に報告された、パフォーマンスが最低のアプリケーションが表示されます。 パフォーマンスの低下による影響を受けたすべてのネットワークを表示するには、リストの最上部のアプリケーション名をクリックします。

サーバとネットワークのグラフを下方まで参照しながら、その評価が［選択されたコンポーネント］ページの評価に一致するものを選択できます。たとえば、これがアプリケーション パフォーマンスの表示である場合は、次の手順に従います。

このパフォーマンス バーをクリックし、後続のページに［ネットワークで絞り込み］ページを表示します。



関与していたネットワークを簡単に参照できます。

［サーバ インシデント］からの影響を受けたネットワークの特定

サーバ インシデントが発生した場合は［インシデント］ページにその発生が表示されます。 そのインシデントが引き起こした影響を理解するため、以下を把握します。

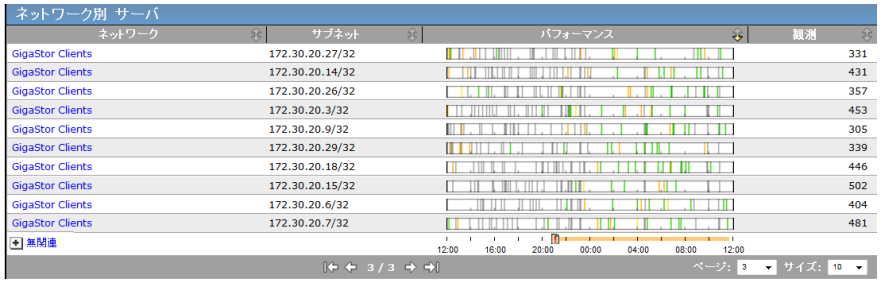
- どのようなネットワークおよびユーザ グループが影響を受けたか。
- 特定のどのユーザが影響を受けたか。
- インシデントが発生したときにシステムのユーザの数はどのように変化したか。
- 特定のサイトについては、どのユーザが影響を受けたか。

インシデントにより影響を受けたユーザおよびネットワークの特定

影響を受けたネットワークとユーザ グループを確認するには、以下の手順に従います。

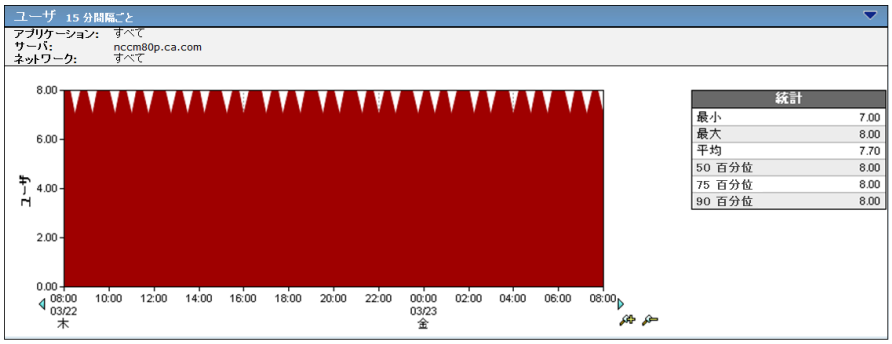
1. そのインシデントに関するより多くの詳細を表示するには、［サーバ インシデント］ページ上でインシデントのリンクをクリックします。

2. 影響を受けていないネットワークを確認するには、［無関連］リンクの横にあるプラス（+）アイコンをクリックします。



3. そのインシデントによる影響を受けた特定のユーザを把握するには、［エクスプローラ］をクリックします。
4. そのインシデントの発生時刻にアプリケーション/サーバにアクセスしていたすべてのユーザの IP アドレスおよびホスト名（使用可能な場合）のリストを表示するには、［影響を受けたユーザ］タブをクリックします。
5. そのインシデントが発生した時刻のユーザの総数と、その問題がどのように多数のユーザに影響を与えたかを確認するには、影響を受けたユーザ レポートを閉じて、［リンク：エンジニアリング］をクリックします。

   ［コンポーネント レポート］ページが表示されます。
6. ［表示項目］メニューの［QoS］をクリックします。
7. ［ユーザ］ビューまでスクロールし、ユーザ数の経時的な視覚的表現を確認します。



8. ［設定］をクリックし、ネットワークを選択して特定のネットワーク上のユーザを確認します。

ネットワークがアプリケーションの低品質なパフォーマンスの一因となっているかどうかの特定

次の手順に従ってください:

1. ［操作］ページをクリックします。
2. ［表示項目］メニューの［アプリケーション］をクリックします。

   アプリケーション別のパフォーマンス レポートが表示されます。
3. 低パフォーマンスを示しているアプリケーションをクリックします。このアプリケーション パフォーマンス プロファイルが次のページの［選択されたコンポーネント］セクションに表示されます。
4. ［設定］をクリックします。［設定］ページの［メトリック］から、［すべてのネットワーク メトリック］を選択します。
5. ページの下の［ネットワークで絞り込み］ビューで、アプリケーションが実行されているネットワークを表示します。これらのネットワークにアプリケーションと同様の低下プロファイルが示されている場合は、それらが一因となっています。ネットワークが正常なパフォーマンスを示しているにもかかわらず、アプリケーションが低速な場合、ネットワークは一因ではありませんでした。
6. あるいは、［操作］の［概要］ページにあるネットワーク別のパフォーマンス レポートで、最もパフォーマンスの低いネットワークを調べるという単純な方法もあります。これらの 1 つが対象のアプリケーションを実行している場合（ネットワークをクリックすると確認できます）は、［アプリケーションで絞り込み］リストの低品質のパフォーマンスの一因となっています。

アプリケーションのパフォーマンス低下をもたらすネットワーク コンポーネントの特定

以下の手順を実行します。

1. ［操作］ページをクリックします。
2. ［表示項目］メニューの［アプリケーション］をクリックします。

   アプリケーション別のパフォーマンス レポートが表示されます。
3. 低パフォーマンスを示しているアプリケーションをクリックします。このアプリケーション パフォーマンス プロファイルが次のページの［選択されたコンポーネント］セクションに表示されます。
4. ［設定］をクリックします。［設定］ページの［メトリック］から、［すべてのネットワーク メトリック］を選択します。
5. ページの下の［ネットワークで絞り込み］表示で、アプリケーションが実行されているネットワークを表示をします。これらのネットワークがアプリケーションと同様のプロファイル低下を示している場合、それらのネットワークも影響しています。アプリケーションが低速であっても、ネットワークが正常なパフォーマンスを示している場合、ネットワークは影響していません。
6. あるいは、［操作の概要］ページにあるネットワーク別のパフォーマンス レポートで、最もパフォーマンスの低いネットワークを調べるという簡単な方法もあります。これらの 1 つが問題のアプリケーションを実行している場合（ネットワークをクリックすると確認できます）、それが［アプリケーションで絞り込み］リストの低パフォーマンスに影響していることになります。

パフォーマンスの問題があるサーバの場所の特定

サーバ パフォーマンスの問題は、［操作］ページの［サーバ別のパフォーマンス］ビュー上ですぐに確認できます。 管理コンソール によるトラブルシューティングは、単一サーバの問題の原因を絞り込むのに役立ちます。以下を特定できます。

- ビューの時間軸における問題の最新性
- 色付きのセグメントの幅から問題の期間
- セグメントの色による問題の重大度
- 対応する［ネットワーク別のパフォーマンス］ビューで同様の低下プロファイルのネットワークがいくつ表示されるかによる問題の広がり方。

根本原因は調査から明らかになる場合があります。 管理コンソール は調査活動に集中し、根本原因を迅速に検索する他の専門ツールを使用できるようにます。

企業ネットワーク内にサーバの検出に役立てるには、Third Bank servers、South Building Server C など、デバイスを 管理コンソール 内で有意義な方法で命名することが最良の方法です。 Web サーバは同じように命名するなど、サーバ ファームのサーバには共通の識別子を含めることができます。

調査を使用する SNMP クエリ

このセクションでは、［インシデント］ページで SNMP パフォーマンス調査を使用する方法について説明します。

状況 1-- サーバ インシデント

サーバ インシデントは［概要］ページの［インシデント］ページで識別されます。

概要

インシデントが開いていた時間を確認することが重要です。 インシデントの継続時間が長いほど、ユーザはその問題による影響を大きく受けます。［インシデント］ページで、インシデントをクリックし、そのインシデントの詳細を表示します。 ［期間］フィールドのデータを確認します。

また、［重大度］フィールドを確認し、そのインシデントの最新のステータスを把握します。 ［メジャー］と評価されたインシデントは早急に調査します。そのインシデントが［クローズ］になっている場合、パフォーマンスの低下はすでに発生しておらず、長期間にわたって以前の正常なパフォーマンス レベルに達しています。

インシデント番号をクリックし、［詳細］ページを表示します。

インシデントの詳細

分析を行うため、まず、［メトリック］セクションの［サーバ］を確認し、インシデントを引き起こしたメトリックを特定します。［無応答］や［拒否されたセッション］などの［サーバ レスポンス時間］メトリックの低下を確認する場合、SNMP パフォーマンス クエリがきわめて役に立ちます。

［表示項目］のリストで、［調査］をクリックし、サーバまたはサーバ グループの関連 SNMP パフォーマンス調査を表示します。

このインシデントと関連付けられた調査が一覧表示されます。SNMP ポーリング調査タイプは、ホスト リソース MIB を使用して、SNMP パフォーマンス メトリックのサーバを照会します。［表示］ボタンをクリックして、SNMP ポーリング データを確認します。 SNMP ポーリング調査がリストにない場合は、以下の手順に従って開始します。

SNMP パフォーマンス調査

以下の場合、手動で調査を開始すると役立つ場合があります。

- サーバ インシデントの SNMP ポーリングがない
- 調査の日付が古い（1 日以上前）
- 分析に追加サーバを含める必要がある

詳細:

SNMP 経由のパフォーマンス調査 (P. 80)

SNMP パフォーマンス データの分析

サーバの SNMP パフォーマンス レポートを表示した後、発生したサーバ インシデントのタイプに対応するトラブルシューティング セクションを見つけます。

サーバ レスポンス時間またはサーバ接続時間のインシデント分析

サーバ レスポンス時間またはサーバ接続時間のインシデントの場合、サーバはクライアントによるリクエストに対する応答が通常よりも遅くなります。

CPU

サーバの CPU 使用率を確認します。 70 ～ 100 パーセントに近く、高い場合は、CPU を消費しているプロセスを確認します。 CPU をすべて消費しているプロセスがある場合は、応答が遅くなります。 これは、同時ユーザが多すぎるか、プロセスによって大きな CPU 負荷がかかっていることが原因となっている場合があります。 CPU 使用率を低減するためにプロセスを再起動できます。 これにより、ユーザによって実行されたすべての作業が終了します。 プロセスが重大でない場合は、プロセスを停止します。 CPU 使用率が低い場合、CPU はこのインシデンの問題ではありません。

メモリ

サーバのメモリ使用率を確認します。70 パーセントを超える場合は、メモリを消費しているプロセスを確認します。 レスポンスの遅さは、同時ユーザが多すぎるか、プロセスでのメモリ漏洩によって引き起こされる場合があります。 メモリ使用率を低減するためにプロセスを再起動します。 プロセスが重大でない場合は、プロセスを停止します。 CPU とメモリの両方が低い場合、典型的なハードウェアの制約が問題ではありません。

インターフェース統計

メモリと CPU 使用率の両方がサーバに適切な場合は、NIC に問題が発生し、サーバ レスポンスを遅く見せている可能性があります。 インターフェース統計を確認します。 まず、すべてのインターフェースが正しく一覧表示され、接続されることを確認します。 NIC のインターフェース速度と IP アドレスの両方が正しく報告されていることを確認します。 二重化に不一致エラーがあると、データを送受信するインターフェースの機能が禁止されます。 二重化不一致エラー、ケーブルの問題、または CRC エラーは、NIC およびその接続の問題は［破棄］フィールドと［エラー］フィールドに表示されます。

ディスク容量

ドライブの容量を確認します。 データ用の容量が限定されていると、サーバは低速になります。 サーバーのディスク空き容量が不足した場合、データ処理能力が低下します。さらに検討すべき事項については、サーバにアクセスし、不正セグメントのフラグメント化や I/O エラーを確認する必要があります。 所定のドライブの空き容量が 10 ～ 15% 未満の場合は、大型の作業用データ セットを有するアプリケーションに関する問題である可能性があります。

サーバ拒否または無応答セッション インシデント分析

期限切れセッションと共に、無応答のセッションまたは拒否されたセッション（利用可能なスレッドのないサーバ）が検出された場合、リソースがアプリケーションによって解放されていないことを示します。

サーバ拒否または無応答セッション インシデントがある場合、サーバが新しいセッションのリクエストにタイムリーに応答していないことを示します。

トップ CPU プロセスまたはメモリ プロセス

CPU リソースを分析では、アプリケーションのホスティングを担当するプロセスが実行していることを確認します。たとえば、SQL Server のプロセス リストでは、sqlserver.exe が CPU またはメモリのプロセスに一覧表示されています。 そのプロセスが実行しており、CPU すべては消費していません。 CPU が 70 パーセントまたは 100 パーセントの近くと、高い場合は、CPU を消費しているプロセスを特定します。 このプロセスが重大でない場合は、プロセスを停止するか、再起動します。 プロセスがロックされているか、不良状態に陥っており、重大なアプリケーションの処理能力を不必要に奪っている場合があります。

メモリ使用率が 80 パーセントを超えている場合は、メモリを消費しているプロセスを特定します。 このプロセスが重大でない場合は、プロセスを停止するか、再起動します。 そのプロセスがロックされているか、不良状態に陥っており、重大なプロセスから重大なメモリ リソースを不必要に奪っている場合があります。 メモリを消費しているプロセスが重大な場合、プロセスの再起動によってそのメモリ キャッシュがクリアされ、正常に再起動できます。

ディスク容量

予期していたプロセスがリストにない場合は、ディスク空き容量の制限により障害が発生している可能性があります。 ドライブを確認し、アプリケーションを起動するために十分なディスク空き容量がサーバにあることを確認します。 次に、サーバにログインし、プロセスが実行されており、起動できるかどうかを確認します。 接続を復元するため、サービスまたはプロセスを再起動する必要がある場合があります。

インターフェース統計

プロセスが実行されており、正常に動作している場合は、NIC に問題が発生し、サーバが遅くなっている、または使用不可であるように見える可能性があります。インターフェース統計を確認します。すべてのインターフェースが正しく一覧表示され、接続されることを確認します。

SNMP データに問題がない場合は、以下を含めて、運用上の調査を開始できます。

- アクティブ セッション数、Time_Wait、およびサーバ上の他の TCP/IP パラメータを確認し、TCP ポート可用性を消耗していないことを確認します。
- サーバ接続時間を、リモート オフィスとサーバ間で実行されている他のアプリケーションと比較し、全体的に増加しているかどうかを確認します。

状況 2 -- ネットワーク インシデント

また、インフラストラクチャ内のルータおよびレイヤ 3 スイッチの SNMP 調査を開始することもできます。この状況については、TCP トレース ルート調査を使用して SNMP パフォーマンス調査を開始します。

［調査オプション］の下にある［トレース ルート］調査を設定する場合は、［SNMP 経由でのルータの調査］を［はい］に設定し、パスの各ルータにネットワーク デバイスを追加します。

詳細:

トレース ルート調査 (P. 85)

SNMP トレース ルート データの分析

複数のホップのあるルートがレポートに表示されます。 詳細に分析するには、大きな遅延のあるホップのパフォーマンス統計を選択します。 一番右側の列の［レポート］アイコンをクリックします。ルータの SNMP パフォーマンス レポートが新しいウィンドウで開きます。 ネットワーク インシデントについては、ネットワークの問題の根本原因を特定するためのチェックリストに従います。

1. デバイスの CPU およびメモリ使用率を確認します。メモリまたは CPU 使用率のいずれかが高い場合、ルータは大きな設定または過剰なパケット処理によって過負荷状態に陥っています。エラーのあるパケットで CPU がオーバーフローしたときにデバイス上でウィルスが発生したり、DDOS 攻撃があると、多くの場合は CPU 使用率が高くなる可能性があります。

   CPU またはメモリ使用率を引き下げ、正常なパフォーマンス レベルに戻すには、デバイスのタイプに応じたトラブルシューティング プロセスに従います。

2. すべてのインターフェースがすべて正し一覧表示され、ステータスが［稼働中］であることを確認します。 問題のインターフェースがセカンダリ インターフェースへフェールオーバーしている場合は、速度が同じであることを確認します。セカンダリ インターフェースが低速な場合、プライマリ インターフェースが正しく機能するようになるまで、ネットワーク遅延が増加する可能性があります。

3. インターフェースが破棄またはエラーを確認していないことを確認します。破棄またはエラー報告されている場合は、ルータにログインし、インターフェースのメディア タイプに関係する問題について、インターフェース接続をトラブルシュートします。 破棄エラーは、そのインターフェースと接続先のルータまたはデバイス間の接続に関する問題を示す傾向があります。

4. インターフェース使用率が容量を超えていないことを確認します。 インターフェース入口ビット/秒は回線定格未満である必要があります。回線使用率が問題である場合は、インターフェース上のトラフィック フローを調査し、突然の輻輳の原因を特定します。

5. デバイスが予想どおりに動作している場合は、同じワークフローの後、SNMP を経由して調査した残りのホップを確認し、ネットワーク インシデントによって影響を受けたエンド ユーザとサーバの間のネットワーク遅延の潜在的な問題を特定し、解決します。

パフォーマンスおよび可用性 OLA のトラッキング

運用レベル管理（OLM）は、統制された積極的な方法および手順で、ビジネス優先度に従い、納得のいくコストで、すべての IT ユーザに十分な操作レベルを提供することを保証するために使用します。 管理コンソール の運用レベル契約（OLA）レポートは、運用レベルが適合しているかどうかを明確にします。 OLA を設定する共通のパフォーマンス メトリックは以下のとおりです。

- データ センターのパフォーマンスを数値化するサーバ レスポンス時間
- ネットワーク インフラストラクチャのパフォーマンスを数値化するネットワーク ラウンドトリップ時間
- アプリケーションのエンドツーエンドのパフォーマンスをキャプチャするトランザクション時間

管理者は、「自分たちは目標を達成しているか」などの広範な問いに答えるために高レベルのサマリ レポートを必要としています。そのため、パフォーマンス エグゼクティブ OLA レポートは、各アプリケーションのそのような疑問に対する答えを素早く提供するバブルアップ レポートとなっています。 可用性エグゼクティブ OLA レポートは、アプリケーション可用性の目標に対する適合について、全体像を示します。 日単位および 1 時間ごとの詳細へは、これらのサマリ レポートをクリックすることによりアクセスできます。

理にかなった頻度で OLA レポートを生成します。

頻度	説明
日単位	きわめて詳細な短期間のトラブルシューティング。IT 部門中心の技術的な内容
週単位	異常または傾向の詳細情報が補完されたサマリ。IT 中心
月単位	事業単位と経営管理用のサマリで、通常、報告書として提示
四半期単位	コンプライアンスを含む包括的な運用レベルを数値化し、プランニング用の情報として使用

通常、OLA 違反は、以下の領域のいずれかで見られます。

- 時間（時刻や曜日など）
- ユーザ グループ（VPN ユーザ ネットワークなど）
- サーバ（たとえば、Web サーバ #2 および #5）

OLA レポートは、パフォーマンスの改善を目的とした活動を促進します。これらの領域に変更を加えると、OLA レポートの改善を見ることができます。

第 10 章: 分析

このセクションには、以下のトピックが含まれています。

影響度分析

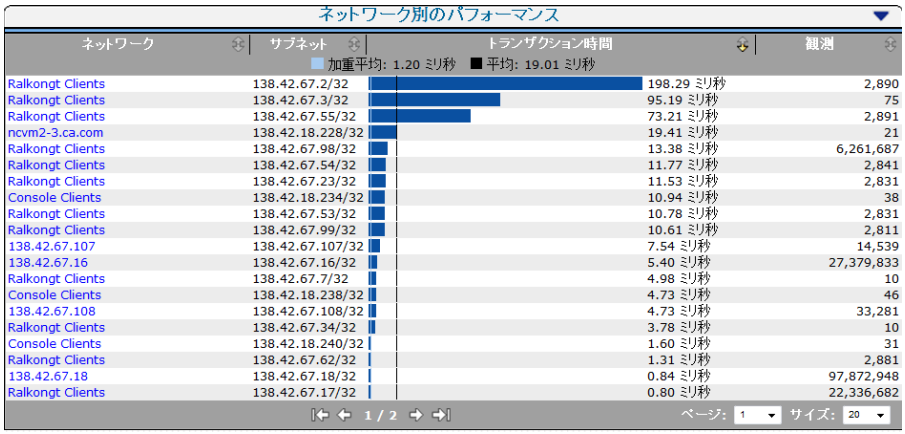
管理コンソール は、IT スタッフにインフラストラクチャ変更の影響を測定し検証する能力を提供します。分析テクニックの 2 つの例を以下に示します。

QoS ポリシー実装の検証

QoS ポリシーは、重大なアプリケーション トラフィックに優先順位を付けることにより、リモート ユーザのレスポンス時間を改善できます。 以下の例に、実際に行われた検証の方法を示します。 この例では、ポリシーは昨日の午後、昼食直後に実装されました。

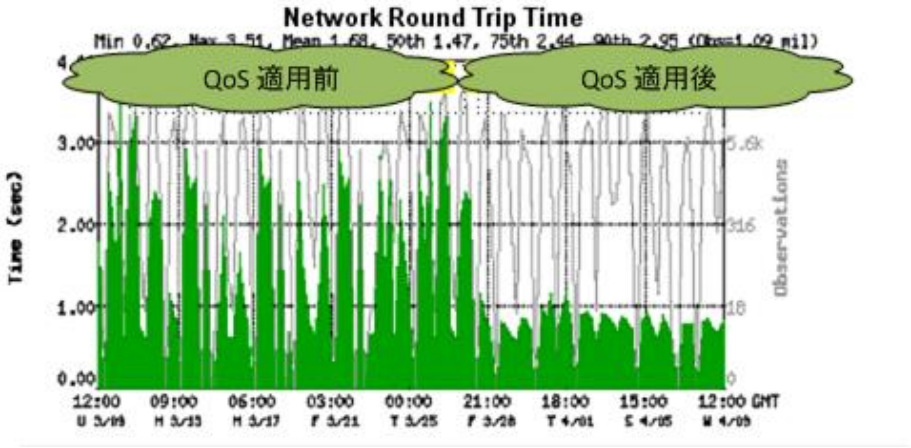
1. ［エンジニアリング］ページをクリックします。
2. ［表示項目］メニューの［パフォーマンス］、［ネットワーク］をクリックします。
3. ［設定］をクリックし、以下を選択します。
   - タイムフレーム： 過去 24 時間
   - メトリック： ネットワーク ラウンドトリップ時間
   - アプリケーション、サーバおよびネットワーク： 選択なし
4. ［OK］をクリックします。

以下のレポートが表示されます。



日単位のネットワーク ラウンドトリップ時間のこのビューには、遅延が最も高かったネットワークが表示されます。56 K および VPN 接続は通常、最も遅いレスポンスを示します。

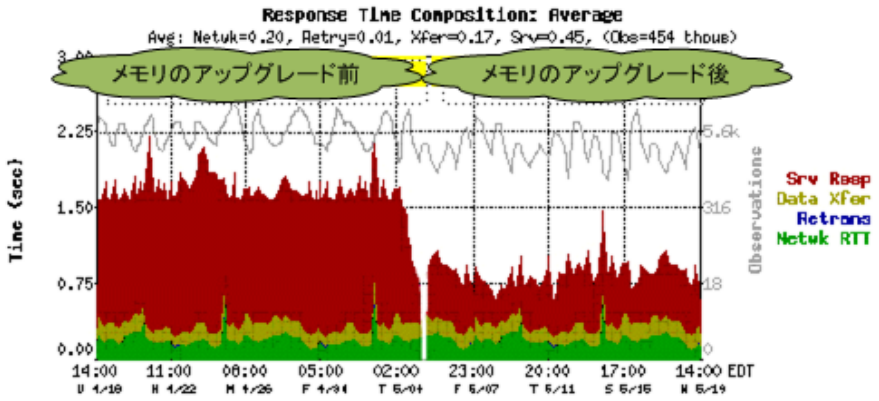
QoS ポリシーは、ピッツバーグ（PA リンク）で実装されました。 QoS ポリシー変更の影響は［ネットワーク ラウンドトリップ時間］ビューに示されています。



QoS ポリシー適用前の時間とは対照的に、ポリシー実装後の時間は速くなっています。

サーバ メモリのアップグレードの検証

多層アプリケーションからの低速レスポンス時間によって、アップグレードが必要なエレメントはどれかに混乱を生じさせる可能性があります。過負荷のバック エンド データベース サーバやアプリケーション サーバのメモリ不足が原因として考えられます。 管理コンソール を使用して効果的なソリューションを特定します。 以下の例では、合計レスポンス時間についてのアプリケーション サーバ メモリのアップグレードの結果を検討します。



サーバ レスポンス時間

サーバ レスポンス時間（SRT）は、サーバがクライアント リクエスト パケットを受け取った瞬間から、最初のレスポンス パケットをネットワークに置いた瞬間までに経過した、サーバの「待ち時間」です。 SRT は以下による影響を受けます。

- CPU 処理能力、使用可能なメモリ、ディスク I/O および NIC I/O などのサーバ ハードウェア
- クエリおよびインデックスの最適化やアプリケーション アルゴリズムなどのアプリケーション動作
- プロセスのハングおよび誤動作
- アプリケーションに必要な使用率または処理能力

通常、サーバ ハードウェアが高速であるほどアプリケーションの書き込みがスムーズに行われ、サーバ使用率が低くなり、SRT が低くなります。 SRT 値はサーバ プラットフォームおよびアプリケーションによって異なります。

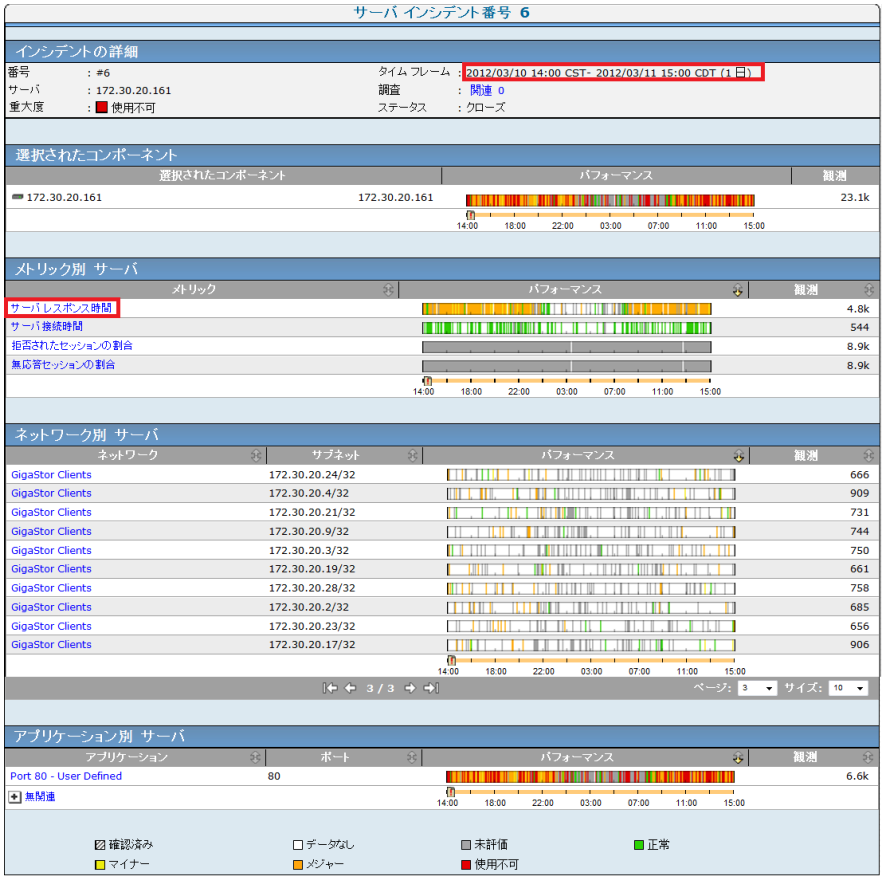
［サーバ レスポンス時間］値の一般的な評価を以下の表に示します。 特に注記のない限り、アプリケーションは単一層です。

アプリケーション	最高	良好	不良
Citrix	50 ミリ秒	75 ミリ秒	200 ミリ秒
Citrix（2 層）	90 ミリ秒	125 ミリ秒	200 ミリ秒
CRM （2 層）	70 ミリ秒	90 ミリ秒	200 ミリ秒
HTTP （Java、2 層）	120 ミリ秒	150 ミリ秒	250 ミリ秒
HTTP （Java なし）	75 ミリ秒	90 ミリ秒	200 ミリ秒
Lotus Notes	50 ミリ秒	75 ミリ秒	200 ミリ秒
MS Exchange	50 ミリ秒	75 ミリ秒	200 ミリ秒
MS SQL	60 ミリ秒	90 ミリ秒	150 ミリ秒
MS ターミナル サービス	50 ミリ秒	75 ミリ秒	200 ミリ秒
MS ターミナル サービス（2 層）	90 ミリ秒	125 ミリ秒	200 ミリ秒
Oracle	50 ミリ秒	75 ミリ秒	200 ミリ秒

アプリケーション	最高	良好	不良
その他	75 ミリ秒	90 ミリ秒	200 ミリ秒
その他（2 層）	90 ミリ秒	120 ミリ秒	200 ミリ秒

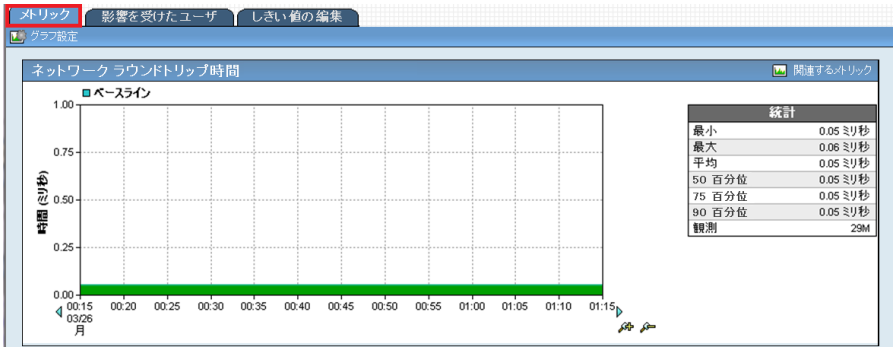
サーバ レスポンス時間を時間をかけて観察すると長期的な問題を特定できます。 表面化していないイベントが、詳しい分析の機会を示唆する場合があります。 ［インシデント］ページで以下のサーバ インシデントを検討します。

インシデントのリンクをクリックし、しきい値を超えてインシデントを起動させたメトリックの詳細を表示します。



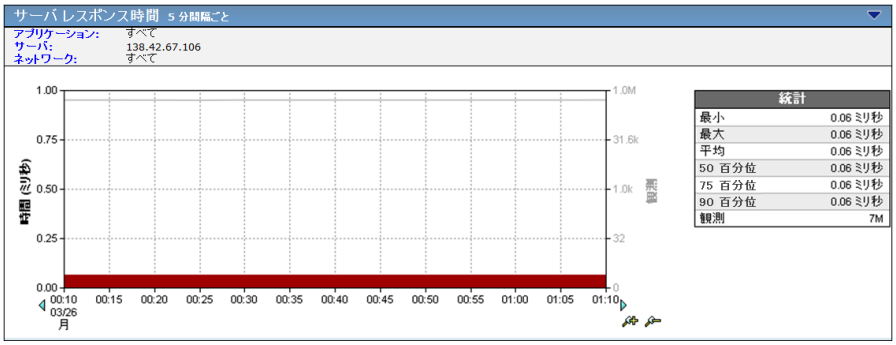
インシデントが起動していた 5 分間は簡単に確認できます。原因となったメトリックは［サーバ レスポンス時間］でした。

ヘッダの［エクスプローラ］をクリックし、次の詳細表示を確認します。この表示に示されたタイム フレームは、前のページのものと同じです。このサーバおよびメトリックの長期的な表示で何らかのパターンがあるかどうかを確認できます。 長期的な表示は［エンジニアリング］ページで利用できます。 このウィンドウを開いたままにして参照することができます。



以下の表示を表示するには、ヘッダの［エンジニアリング］リンクをクリックします。 この表示は同じタイム フレームであるため、［インシデント］ページの表示と同じように見えます。

タイム フレームを長期に変更するには、ページ最上部の［設定］をクリックします。



また、［エンジニアリング］ページの任意のレポート ページからは、このインシデントに関連する他のメトリックも調査できます。 ［拒否されたセッション］などメトリックが高い場合は、サーバが稼働中でも、過度にビジーであり、リクエストに応答できないことを示しています。

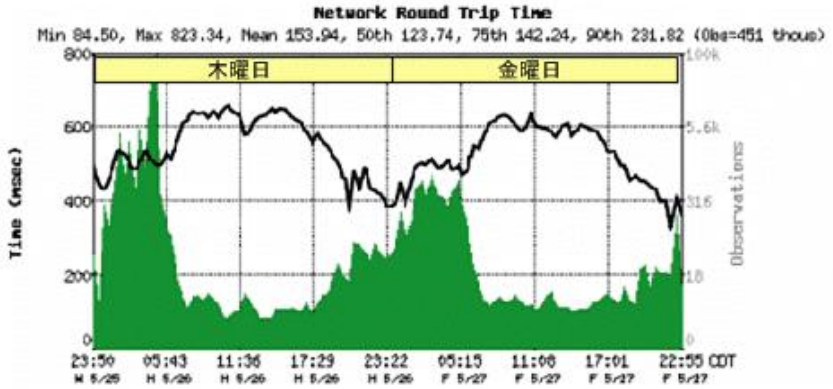
アプリケーションのパフォーマンスとボリューム トレンド

［パフォーマンス］ビューには、観測数と共にメトリック測定が表示されます。［レスポンス時間］ビューでは、左側に直線的な時間スケールを、右側の y 軸には対数の観測数スケールが使用されています。観測数の増減が若干であっても、対数スケール上では顕著になります。

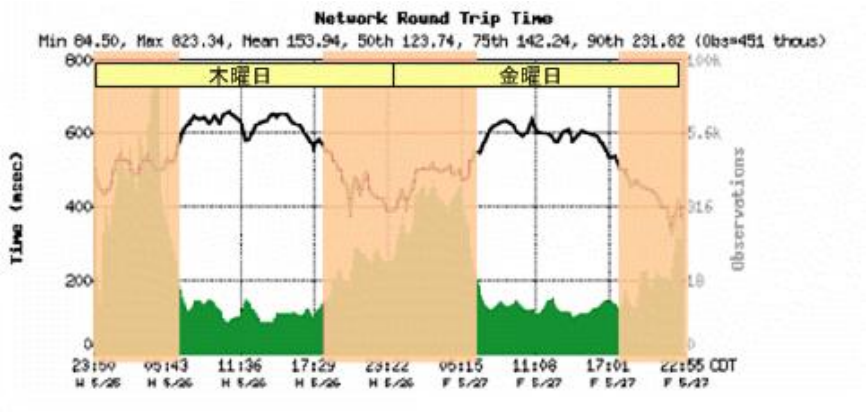
ユーザが体験したパフォーマンスは、このセクションのパフォーマンスの表示で見られるように、ネットワーク ラウンドトリップ時間（NRTT）とボリュームが一緒に変動するというものでした。 メトリックにおけるトレンドを確認するには、表示の期間を変更します。このセクションでは、パフォーマンス メトリックとボリューム トレンドの分析について説明します。

短期表示におけるトレンド

以下のパフォーマンス 表示では、営業日中の操作から同様のパターンを確認できます。

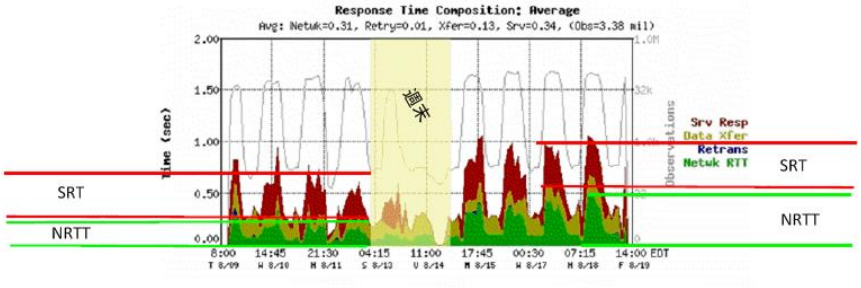


以下に示すように、観測数の高さは、ピーク時間の NRTT の低さと一致します。



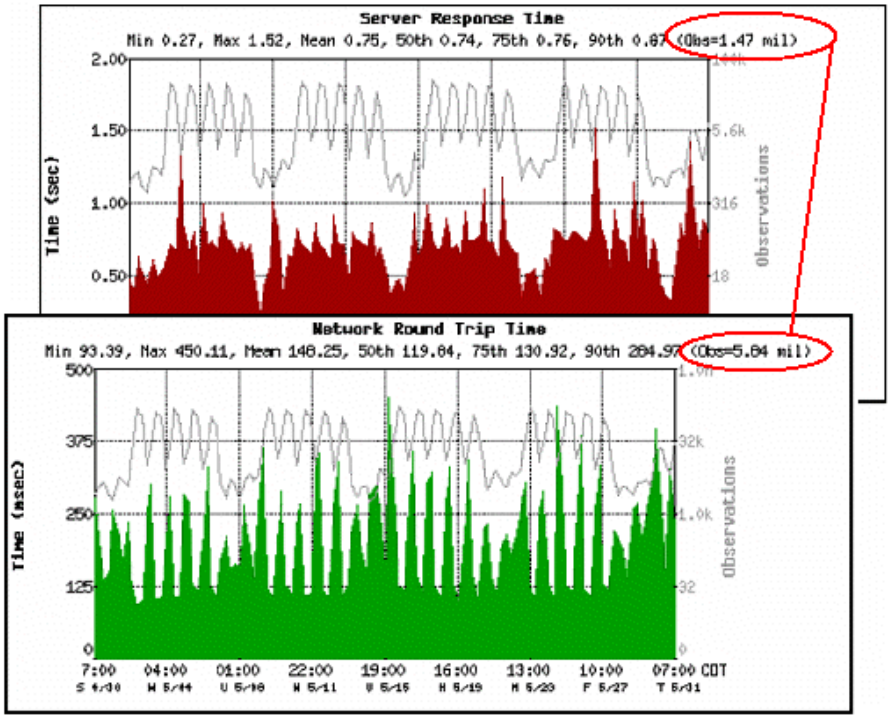
営業時間外では、逆のパターンが発生しています。 つまり、海外のユーザが夜間にアプリケーションにアクセスし、それらの回線に高い遅延 WAN アクセスが発生しています。 時刻および曜日について計算した基準値には、これらの正常なパターンが反映されています。

また、以降の 10 日間の表示では週単位のパターンを確認できます。 ボリュームが高いと、使用率がピーク時に NRTT および SRT が長くなります。 NRTT（緑）コンポーネントは第 1 週よりも第 2 週のほうが大きく、SRT コンポーネントは一定のままです。 このアプリケーションの観測数もこの期間中はきわめて一貫したパターンを示しています。第 2 週のレスポンス時間の増加は、ネットワーク変更または他のアプリケーションの使用方法の変化のためと考えられます。

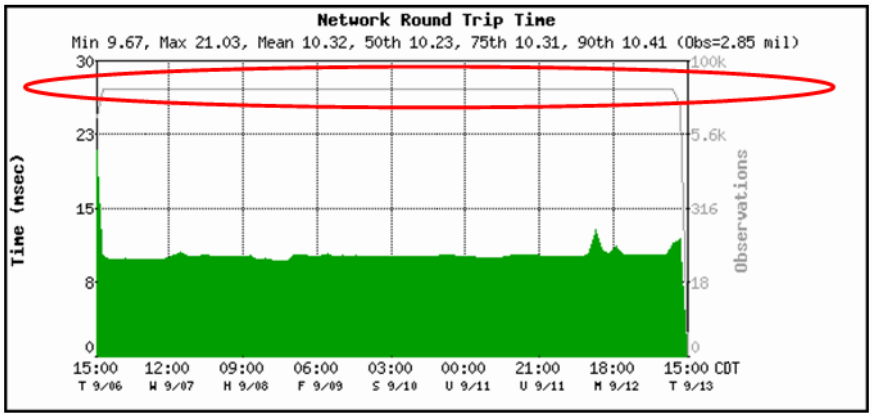


月単位のパターンを見ると、キャパシティ計画に影響を及ぼす可能性があるトレンドを確認できます。 以下の例では、NRTT 観測数と SRT 観測数がほぼ 4:1 の比率であることを確認できます。

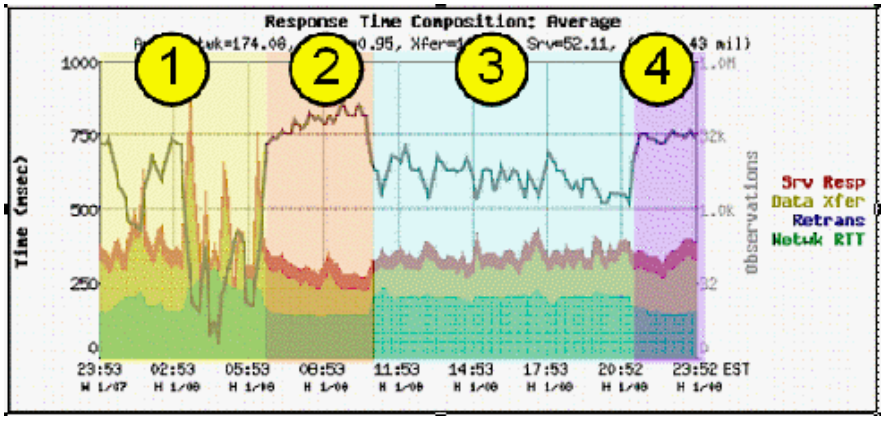
このアプリケーションでは、TCP トランザクションあたりの平均がほぼ 4 往復になります。 多くのターンを使用するように設計されているアプリケーションは、ターンが少ないアプリケーションよりも、ネットワークの低下による影響を受けやすい場合があります。



パフォーマンス表示上で変化がほとんどない観測数は、バッチ プロセスまたはアクティブなエージェントを示唆します。



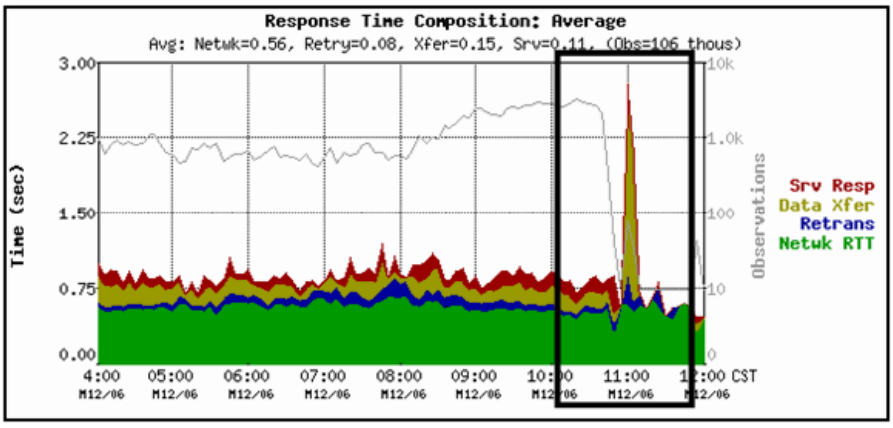
以下の表示に、輸送会社の荷物のトラッキング アプリケーションの日単位のパターンを示します。



パターンは日単位のワーク フローに応じて発生します。

1. 深夜から早朝にかけて、バッチ ウィンドウ オフライン処理およびバックアップが発生します。
2. 午前中にトラックに荷物を積み込む間、荷物がスキャンされます。 これによって、パターンのこの部分で高い観測数が生み出されます。
3. 配送業務は変化するため、安定したシステム レスポンスを示しています
4. 最後のセクションはトラックからの荷卸し作業を反映しています。

以下の表示はアプリケーション障害の例です。 観測数が著しく低下しています。



使用不可ステータス: 可用性メトリックおよびインシデントの分析

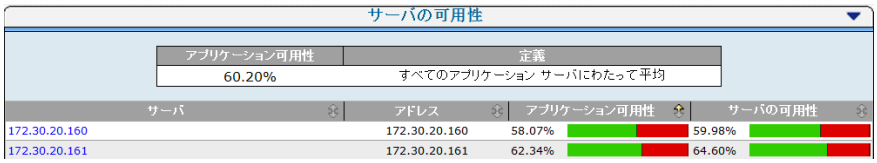
ユーザが可用性モニタリングを有効にした場合、管理コンソール はアプリケーションとサーバの両方の可用性を監視します。 サービスに割り込みがあった場合、そのどちらか一方が原因である可能性があります。 このセクションでは、そのデータを調査する方法について説明します。

1. ［エンジニアリング］ページをクリックします。
2. ［表示項目］メニューの［可用性］をクリックします。

   アプリケーション可用性レポートが表示されます。

3. アプリケーションをクリックして、アプリケーションをホストするサーバを確認します。

   ［サーバの可用性］レポートが表示されます。



4. ［アプリケーション可用性］列のパフォーマンス バーをクリックして、［可用性時系列］レポートを表示します。

   注: アプリケーションが 100% 使用可能（緑）であるとき、［サーバの可用性］ビューで、一部のサーバが 100% 使用可能として表示されない場合があります。 アプリケーションが使用可能であるためには、ファームのすべてのサーバが使用可能である必要はありません。 CA Application Delivery Analysis 管理者は、アプリケーション サーバが使用可能と見なされるために必要な、ファーム内で使用できるサーバ数を指定します。

5. ［関連するインシデント］リンクをクリックし、この表示の関連するインシデントを確認します。

パフォーマンス スコアカードの使用

［管理］ページで、［パフォーマンス スコアカード］をクリックします。結果の［アプリケーション リスト］ページには、アプリケーションが毎月、企業内でどのように実行しているかが表示されます［アプリケーション リスト］ページでは、以下のカラー コードを使用してパフォーマンスを評価します。

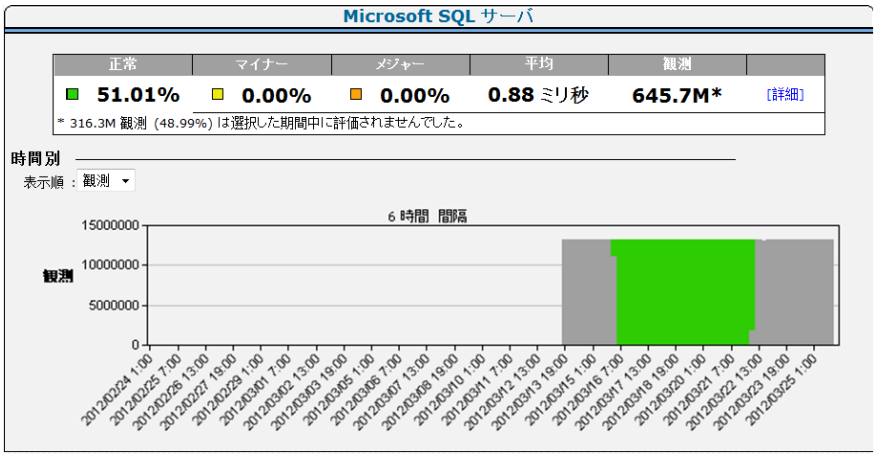
- 未評価（グレー）
- 正常（緑）
- マイナー（黄色）
- メジャー（オレンジ）

［アプリケーション リスト］は、観測数によって各アプリケーションのパフォーマンス評価を並べ替えます。

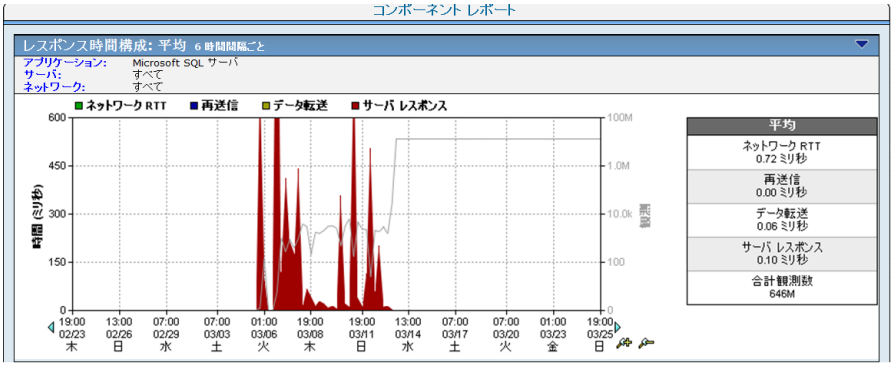
次の手順に従ってください：

1. ［管理］ページをクリックします。
2. ［表示項目］メニューの［パフォーマンス スコアカード］をクリックします。
3. ［アプリケーション リスト］までスクロールし、アプリケーションをクリックします。
4. ［設定］をクリックし、レポート設定を変更します。
5. 色分けされたパフォーマンス バーをクリックするか、アプリケーション名をクリックして、ピアと同じように実行していないサーバおよびネットワークについての詳細情報を表示します。

   アプリケーションの詳細表示には、時間間隔別にデータが表示されます。 データを観測数で表示するか、割合で表示するかを選択します。
6. ネットワーク別にアプリケーションの詳細情報を表示するには、［表示項目］メニューの［パフォーマンス スコアカード］および［ネットワーク］をクリックします。
7. サーバ別にアプリケーションの詳細情報を表示するには、［表示項目］メニューの［パフォーマンス スコアカード］および［サーバ］をクリックします。
8. ［詳細］をクリックして、アプリケーションの［コンポーネント レポート］を表示します。



［コンポーネント レポート］ページが表示されます。



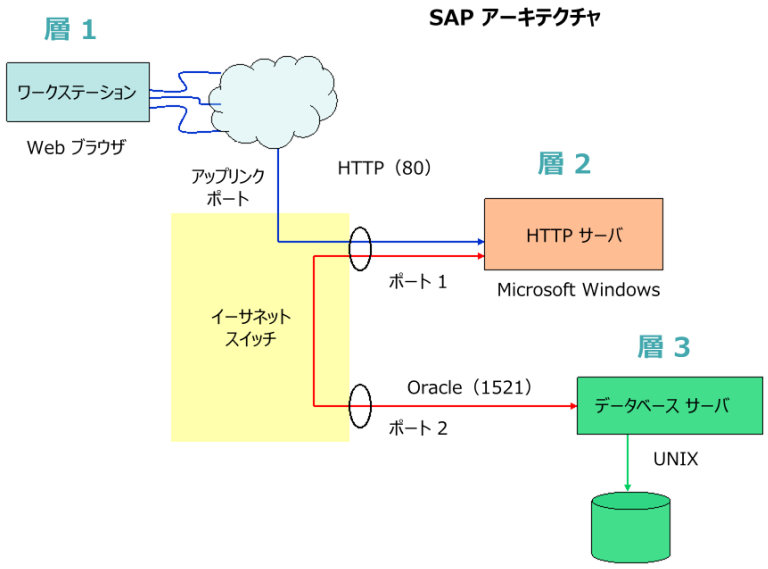
多層アプリケーションのパフォーマンス

管理コンソールを使用して、多層アプリケーションの各層のネットワーク、サーバおよびアプリケーションのパフォーマンスを視覚的に確認できるようにします。N 層アプリケーションを監視し、必要なデータを取得して、アプリケーション パフォーマンスの問題を特定の層、および各層内のサーバ、ネットワークまたはアプリケーションの特定の問題の発生源に分離します。

多層アプリケーション操作の理解

以下の層から構成される N 層 SAP アーキテクチャを考えます。

- 層 1 -- Internet Explorer がユーザ ワークステーション上で実行されています。
- 層 2 -- HTTP ベースのアプリケーションが Windows Server 2003 上で実行されています。
- 層 3 -- データベース サーバが UNIX 上で Oracle を実行しています。



以下のプロセスを図に示します。

1. Internet Explorer を使用して、ユーザは、青色の線で示されるように、層 2 HTTP サーバへの接続を開始します。
2. 接続が確立された後、ユーザはアプリケーション データをリクエストします。
3. HTTP サーバは、赤い線で示されるように、層 3 Oracle データベース サーバへこのリクエストを転送します。
4. Oracle サーバはユーザ クエリを実行し、層 2 HTTP サーバに結果を返します。
5. HTTP サーバは層 1 クライアントにデータを返信します。

アプリケーション層にわたる複数のハンドオフにより、パフォーマンスの問題が N 層アプリケーションで発生した場合にソースの識別が困難になる場合があります。操作上、層 2 が層 3 のレスポンスを待つとき、そのパフォーマンスは層 3 のパフォーマンスによって決まります。

多層アプリケーションのパフォーマンスの分析

管理コンソールを使用して、以下の 2 つの例外を除き、単一層アプリケーションの分析と同じ方法で複数層アプリケーションを分析します。

- 下位層のアプリケーションのパフォーマンスは、多くの場合、上位層のアプリケーションのパフォーマンスに依存します。
- 各層で報告を行う場合、ネットワークを設定するときに上位層を設定し、サーバとアプリケーションを設定するときに下位層を設定します。

前のセクションの例では、層 2 の HTTP Web アプリケーションのパフォーマンスが層 3 の Oracle データベース サーバのパフォーマンスの関数になります。層 N の HTTP Web サーバがレポート内にクライアントとして表示され、層 N+1 のホストがサーバ/アプリケーションとして表示されます。

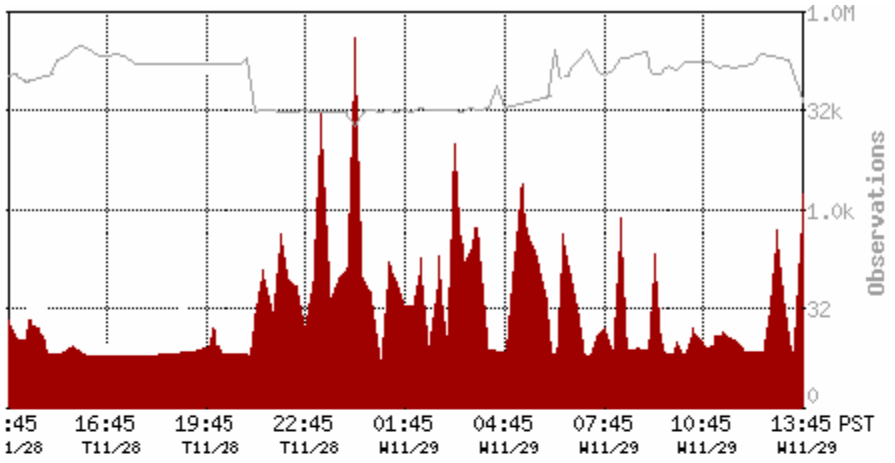
N 層のアプリケーションを分析する場合、最も高い位置の層（エンド ユーザから最も遠い位置の層）から開始し、ユーザ側へと向かいます。 従属層の従属パフォーマンス ポイントの影響に注意してください。 層間で共通の従属パフォーマンス ポイントはオカレンスの可能性が高い順に従います。

1. 層 N+1 のサーバ レスポンス時間（SRT）は層 N の SRT に影響を与えます。
   - SRT はサーバ リソース使用率の関数となります。値が高い場合は、所定の負荷のアプリケーションにサービスを提供するためのメモリ、CPU、またはディスク I/O リソースが十分にない可能性があることを示します。
   - セッションまたは QoS 表示を確認し、SRT が低速インスタンスにある間に、どのセッション、またはどのユーザが過度の負荷をサーバにかけているかを特定します。
2. 層 N と 層 N+1 間のネットワーク ラウンドトリップ時間（NRTT）が高く、データ スループットに影響します。
   - LAN 環境内の NRTT は、スイッチ間の共有アップリンク上の帯域幅に対するスイッチ バックプレーン速度と接続の関数となります。N 層のアプリケーションのプライマリ NIC を常に同じスイッチ上、および同じ VLAN 内に配置してアップリンク帯域幅の競合をなくし、サーバ間の 2 つの余分なスイッチ ホップを排除するのが最良の方法です。 これにより、N 層のアプリケーションのパフォーマンスを飛躍的に増加させることができます。

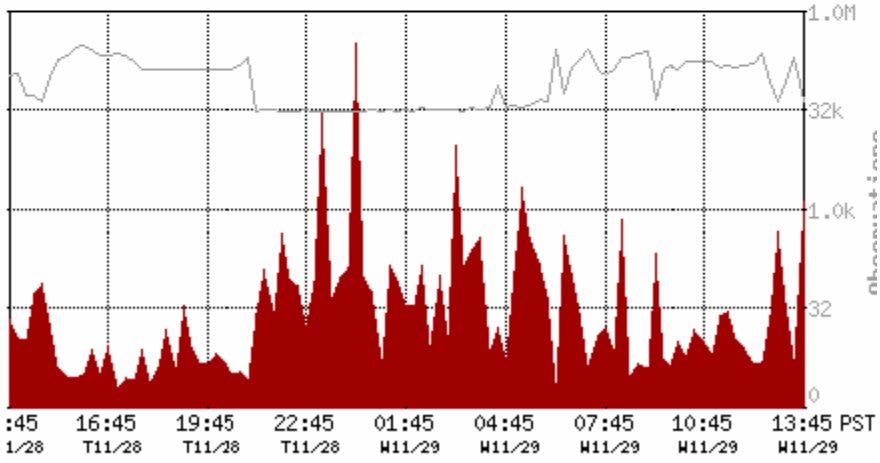
- ［トラフィック］および［データ ボリューム］ビューを確認し、NRTT がボリュームの増加につれて増加するかどうかを特定します。増加する場合は、アプリケーションの 2 つのサーバ間に十分な帯域幅がない場合があります。

3. 層 N と層 N+1 間の［データ転送時間］（DTT）は、ちょうど 0 になるか、ゼロに収束します。［レスポンス サイズ］および［レスポンス サイズ別データ転送時間］ビューを確認し、1 つのパケット内に収容するデータ量である 1.45 KB を超えるさまざまなレスポンス サイズをアプリケーションが使用しているかどうかを確認します。ゼロまたは約 0 の DTT は、通常、各ユーザ リクエストのバック オフィス サーバによって単一のパケットが送信されることを示します。 データベース サーバの場合は、これは、通常、単一のクエリ内ですべての行を要求する代わりに、データの 1 つの行を何回もリクエストするクエリの形式となっています。 最適なパフォーマンスのクエリを再度作成します。
4. 層 N と層 N+1 間の再送信時間が大幅なパケット ロスを示しています。
   - ［トラフィック］および［データ ボリューム］ビューを確認し、再送信時間が高い間に大量のデータが転送されているかどうかを特定します。
   - ［セッション数］および［ネットワーク接続時間］を確認し、TCP セッション スタートアップについての遅延を特定します。 値が高い場合は、2 つの層間の輻輳を示しています。

以下のグラフは、アプリケーション アーキテクチャの層 2 と層 3 間の［サーバ レスポンス時間］の依存性を示しています。層 2 のサーバの SRT は、レスポンス時間が高い間は層 3 のサーバの SRT に従います。



Server Response Time - Tier 2



Server Response Time - Tier 3

2 つの層間の後続のデータ ポイントは、層 3 のサーバ パフォーマンスが層 2 のサーバ パフォーマンスに影響することを示します。 層 3 のサーバがこのアプリケーション アーキテクチャのボトルネックです。

層 N のアプリケーション遅延が、ピーク遅延スパイク時の層 N+1 のアプリケーション遅延と同じ一般曲線を持つ場合、層 N のアプリケーションは層 N+1 のアプリケーションによって悪影響を受けている可能性があります。

層 N+1 アプリケーションのパフォーマンス ボトルネック（SRT が高い場合はサーバの問題を示し、NRTT および再転送時間が高い場合はネットワークの問題を示し、SRT および NRTT が低いときにデータ転送時間がゼロまたは高い場合は一般的にアプリケーションの問題を示す）を特定した後、そのボトルネックを修正し、分析プロセスを繰り返して第 2 のボトルネックを特定します。

用語集

3 方向ハンドシェーク

TCP プロトコルにおける *3 方向ハンドシェーク*は、クライアントとサーバの間で接続を確立するために使用されます。 SYN パケット (P. 238)がクライアントからサーバに送信され、接続準備が開始されます。 すると、SYN-ACK パケット (P. 238)がサーバからクライアントに送信され、クライアントからの SYN の受信の確認応答が行われます。最後に、ACK パケット (P. 234)がクライアントからサーバに送信され、サーバからの SYN-ACK の受信の確認応答が行われた後、TCP 接続が確立されます。監視デバイスは、ネットワーク上で監視されている接続の時間調整および分析で 3 方向ハンドシェイクを使用します。

5 分サマリ ファイル

*5 分サマリ ファイル*は、CA Application Delivery Analysis Standard Monitor、Multi-Port Monitor、Virtual Systems Monitor、CA GigaStor、または Cisco NAM によって作成されます。各パフォーマンス メトリック/アプリケーション/サーバ/ネットワークの組み合わせ (P. 243)に対する 5 分間の平均から構成されます。

ACK パケット

TCP 接続の設定中、サーバからの SYN-ACK パケット (P. 238)の受信を確認するために、*ACK パケット*がクライアントによってサーバに送信されます。

CA ADA Availability Poller サービス

CA ADA Availability Poller サービスは、アプリケーションの可用性をチェックします。 アプリケーションをホストするサーバが CA Standard Monitor によって監視されている場合、このチェックは監視デバイスによって実行されます。 それ以外の場合は、CA ADA マネージャ上の CA ADA Availability Poller サービスがアプリケーションの可用性をチェックします。

CA ADA Batch サービス

*CA ADA Batch サービス*は、CA ADA マネージャ上で CA ADA Master Batch サービスによって処理される .dat データ ファイルをステージングします。このサービスは CA Standard Monitor 上で実行されます。

CA ADA Data Pump サービス

*CA ADA Data Pump サービス*は、CA ADA マネージャ上でデータベース メンテナンスを毎週実行します。

CA ADA Data Transfer Manager サービス

*CA ADA Data Transfer Manager サービス*は、CA ADA マネージャ上で定義されたアプリケーション、サーバ、クライアント ネットワークに基づいて、Cisco WAE デバイス監視を同期します。 このサービスは CA ADA マネージャ上で実行されます。

CA ADA Inspector Agent サービス

CA ADA Inspector Agent サービスは、アプリケーション、サーバ、および関連するネットワーク上で調査を起動します。 アプリケーションをホストするサーバが CA Standard Monitor によって監視されている場合、調査は監視デバイスから起動されます。 そうでない場合、CA ADA マネージャ上の CA ADA Inspector Agent サービスが調査を起動します。

CA ADA Inspector サービス

*CA ADA Inspector サービス*は、CA ADA Master Batch サービスによって処理される 5 分間の .dat ファイルを CA ADA マネージャ データベースにロードし、CA ADA Inspector Agent サービスと通信して調査を起動します。 このサービスは CA ADA マネージャ上で実行されます。

CA ADA Master Batch サービス

*CA ADA Batch サービス*は、管理コンソール 上で実行され、CA Standard Monitor で CA ADA Batch サービスから受信したデータ ファイルを 5 分の .dat ファイルに格納します。 このサービスは CA ADA マネージャ上で実行されます。

CA ADA Messenger サービス

*CA ADA Messenger サービス*は、CA ADA マネージャ上に定義されたアプリケーション、サーバ、クライアント ネットワークに基づいて、割り当てられた CA Standard Monitor、CA Multi-Port Monitor、CA GigaStor 監視デバイス 上で監視を同期します。このサービスは CA ADA マネージャ上で実行されます。

CA ADA Monitor Management サービス

*CA ADA Monitor Management サービス*は、CA ADA マネージャからの要求に応答し、.dat ファイルを転送します。 このサービスは CA Standard Monitor 上で実行されます。

CA ADA Monitor サービス

*CA ADA Monitor サービス*は、ミラーリングされた TCP パケットおよびパケット要約ファイルを CA ADA 監視デバイスから受信します。 このサービスは、CA Standard Monitor および CA ADA マネージャ上で実行されます。

CA ADA Reader サービス

*CA ADA Reader サービス*は、CA GigaStor 上で実行され、TCP ヘッダから構成されるパケット要約ファイルを、割り当てられた CA ADA Standard Monitor または Multi-Port Monitor にメトリック計算のために送信します。

CA Application Delivery Analysis マネージャ（CA ADA マネージャ）

*CA Application Delivery Analysis マネージャ（CA ADA マネージャ）*は、CA ADA アーキテクチャのコンポーネントで、複数の監視デバイスに対して中央での設定、分析、管理、およびレポーティング機能を提供します。 CA ADA マネージャは、割り当てられた監視デバイスからレスポンス時間メトリックを受信します。これには、CA ADA Standard Monitor、Multi-Port Monitor、Virtual Systems Monitor、CA GigaStor、または Cisco NAM が含まれます。

CA Observer Expert

CA Observer Expert は CA GigaStor にバンドルされています。これは、CA ADA からのアプリケーション レスポンス時間の監視を、根本原因解析のためにパケット レベル データへのドリル イン機能と組み合わせます。

FIN パケット

TCP プロトコルでは、サーバへの TCP 接続を確立するときは、SYN パケットがクライアントによって使用されます。 同様に、FIN パケットは TCP 接続の切断または終了を開始するために使用されます。監視デバイスは、FIN パケットまたは RST パケットを受信したときに、TCP 通信が終了されていると判断します。

NetQoS MySql51 サービス

CA ADA マネージャ データベースをホストする MySql サーバを開始および停止します。

OLA

パフォーマンス OLA（運用レベル契約） (P. 251)および可用性 OLA（運用レベル契約） *(P. 241)を参照*。

ping レスポンス時間調査

ping レスポンス時間調査は、ping 要求を送信してから ping 応答を受信するまでにかかる時間を測定するサーバ インシデント レスポンス (P. 245)であり、パケットのラウンドトリップ時間についてレポートします。 CA Application Delivery Analysis 管理者は、この調査を開始またはスケジュールすることもできます。

ping レスポンス時間とパケット サイズの比較調査

*ping レスポンス時間とパケット サイズの比較調査*は、さまざまなサイズの ping 要求（データ パケット）に対する ping 応答を受信するのにかかる時間を測定します。 この調査は、さまざまなパケット サイズでの過度の遅延や接続不良状態を追跡するのに役立ちます。 CA ADA 管理者はこの調査を起動またはスケジュールすることもできます。

RST パケット

RST パケットは、TCP セッションを正常に終了するための方法です。 Web ブラウザは通常 FIN ではなく RST でセッションを終了します。 管理コンソールは、接続ハンドシェークの間、RST パケットのみを「未対応のセッション リクエスト」としてカウントします。 監視デバイスが、TCP 3 方向ハンドシェークが完了する前に RST を検出した場合、管理コンソールはセッションが拒否されたものと認識します。

severity

重大度は、特定の期間にわたるパフォーマンス データを指定したしきい値によって分類（［なし］、［未評価］、［マイナー］、［メジャー］、および［使用不可］）します。

SNMP 経由のパフォーマンス調査

*SNMP 経由のパフォーマンス調査*は、SNMP が CPU 使用率およびメモリ使用率などのパフォーマンス情報をサーバに対してポーリングするサーバ インシデント レスポンス (P. 245)です。CA ADA 管理者はこの調査を起動またはスケジュールすることもできます。

SNMP トラップ通知

SNMP トラップ通知は、影響を受けたアプリケーション、サーバ、ネットワークの［オープン］または［クローズ］のインシデント ステータスについて SNMP マネージャに通知するアプリケーション インシデント レスポンス (P. 240)、ネットワーク インシデント レスポンス (P. 249)、またはサーバ インシデント レスポンス (P. 245)です。

SNMP プロファイル

SNMP プロファイルは、SNMPv3 ユーザ認証情報および SNMPv1 コミュニティ名と SNMPv2 コミュニティ名を管理するために管理コンソールによって使用されます。 SNMP プロファイルには、サーバまたはネットワーク デバイス上の SNMP エージェントにクエリしたり、SNMP トラップ メッセージを送信するために管理コンソールが必要とする SNMP ユーザ認証情報があります。

SPAN

SPAN（*Switched Port Analyzer*）は、ポート ミラーリングとしても知られており、1 つのスイッチ ポート上で確認されたすべてのネットワーク パケットのコピーを、別のスイッチ ポート上のネットワーク監視接続に送信するために、Cisco ネットワーク スイッチ上で使用されます。これは、通常、ネットワーク トラフィックを監視するためにネットワーク アプライアンスによって使用されます。 SPAN により、監視デバイス が、もう 1 つのスイッチ ポート上の複数のブロードキャスト ドメイン上で発生するトラフィックを確認できるようになります。 SPAN の機能はシャーシによって異なります。

SYN-ACK パケット

TCP 接続セットアップ中、クライアントからの SYN パケットの受信を確認するために、SYN-ACK パケット (P. 238)がサーバによってクライアントに送信されます。 監視デバイスは、ネットワーク上で監視されている接続の時間調整および分析で SYN-ACK パケットを使用します。

SYN パケット

TCP プロトコルでは、クライアントとサーバの間の通信（接続）は 3 方向ハンドシェークによって確立されます。SYN パケットがクライアントからサーバに送信され、接続準備が開始されます。 監視デバイスは、ネットワーク上で監視されている接続の時間調整および分析で SYN パケットを使用します。

Traceroute

Traceroute は、インシデント分析で使用される 2 種類の診断ツール（ICMP または TCP）のいずれかを指します。

WAN

WAN（広域ネットワーク）は、通常複数の LAN（ローカル エリア ネットワーク）で構成される広いさまざまな地域をカバーするネットワークです。WAN は、1 つの企業の複数のオフィスで私的に使用されることも、インターネットなどで公的に使用されることもあります。

WAN 最適化デバイス

WAN 最適化デバイスは、圧縮または他のアルゴリズムによってデータ センターとリモート オフィスの間で転送されるトラフィック ボリュームを削減します。 WAN 最適化デバイスの例は、Cisco WAE デバイスや Riverbed Steelhead アプライアンスなどです。

アクション

応答アクション *(P. 241)を参照*。

アクセス層

標準的な 3 層（アクセス、ディストリビューション、コア）LAN ネットワークでは、*アクセス層*はサーバに最も近い層で、サーバをネットワークに接続します。 スイッチとハブは、通常アクセス層に分類されます。 通常、すべてのサーバ トラフィックはこの層で発生しますが、これには最多の監視ポイントが必要になります。

アプリケーション

アプリケーションは、一連のサーバ IP アドレスにわたって監視すべき TCP ポートまたはポートの範囲を指定します（たとえば /29 サーバ サブネットにおける TCP-80 トラフィックなど）。

アプリケーション インシデント

ネットワーク インシデントまたはサーバ インシデントがアプリケーションのパフォーマンスに影響を与える場合、アプリケーション インシデントが発生します。

基盤のネットワーク インシデントまたはサーバ インシデントによって、アプリケーションの結合メトリックがパフォーマンスしきい値を超える場合、結合メトリックがしきい値を超過します。

結合メトリックがしきい値を超えると場合、管理コンソールはアプリケーションへのパフォーマンス影響度を「メジャー」（オレンジ）または「マイナー」（黄色）と評価しますが、アプリケーション インシデント レスポンスを作成しません。 基盤のネットワークまたはサーバのインシデントがアプリケーションに対して発生する場合に起動するアプリケーション インシデント レスポンスを定義する必要があります。

アプリケーション インシデント レスポンス

*アプリケーション インシデント レスポンス*は、ネットワーク インシデント (P. 249)またはサーバ インシデント (P. 245)に対するアプリケーション レスポンスです。 たとえば、Exchange アプリケーションに対してアプリケーション インシデント レスポンスを設定した場合、ネットワーク インシデントが Exchange アプリケーションにアクセスするクライアントによって作成されるか、またはサーバ インシデントがアプリケーションをホストするサーバによって作成されたら、管理コンソール がインシデント レスポンスを起動します。 データ転送時間などの結合メトリック (P. 243)のしきい値を超えた場合、管理コンソール はアプリケーション インシデント レスポンスを開始しません。 管理コンソール では、アプリケーションに次のレスポンスを割り当てることができます。電子メール通知 (P. 248)、SNMP トラップ通知 (P. 237)、およびアプリケーション接続時間調査 (P. 240)。

アプリケーション接続時間調査（用語）

アプリケーション接続時間調査は、IT 部門のスタッフが TCP/IP アプリケーション ポートへの接続にかかる時間を知ることができるアプリケーション インシデント レスポンス (P. 240)です。 これには、サーバが接続確認で応答する時間が含まれます。 CA ADA 管理者はこの調査を起動またはスケジュールすることもできます。

インシデント

インシデントは、アプリケーション、サーバ、またはクライアント ネットワーク上の異常な動作の期間に対する注意を喚起するために、管理コンソールによってオープンされます。 「応答アクション (P. 241)」を参照してください。

インシデント レスポンス

インシデント レスポンスを使用すると、問題が発生した時点でトラブルシューティングを行い、平均修復時間を短縮することができます。 インシデント レスポンスは、ビジネス クリティカルなアプリケーション、サーバおよびネットワークに割り当てます。 インシデント レスポンスは、パフォーマンス低下についてユーザのチームに通知すると共に、パフォーマンス低下の根本原因を識別する助けになる詳細を収集するため、精力的に問題を調査するものです。

応答アクション

応答アクションは、通知の送信や調査の開始など、パフォーマンスしきい値違反に対する応答です。

可用性 OLA（運用レベル契約）

可用性 OLA は、アプリケーションが使用可能である時間の割合をレポートします。たとえば、サーバ上のアプリケーションが 1 か月の期間の 99% の間使用可能である必要があります。

監視単位

監視単位は、監視デバイスの追加によって、CA ADA マネージャ上で作成される処理の負荷です。 たとえば、CA Standard Monitor は 1 つの監視単位を利用します。CA ADA マネージャは最大 15 までの監視単位をサポートします。

監視デバイス

監視デバイスは、TCP トランザクションを監視し、アプリケーション、サーバおよびネットワークのレスポンス時間メトリックを計算します。

監視デバイス インシデント

監視デバイス インシデントは、監視デバイスのパフォーマンスおよび可用性のしきい値に対する違反が発生した場合に管理コンソールによって作成されます。 たとえば、デバイスが到達不可になった場合、デバイスではデータが表示されないか、またはデバイスがパケットを破棄します。

監視デバイスの同期

管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義に基づいて TCP セッションを監視する場合に、監視デバイスを同期します。 同期中の監視への一時的な割り込み数を最小限にするには、監視デバイスを同期する前にすべての変更を完了します。

監視フィード

監視フィードは、CA Standard Monitor など、レスポンス時間情報のソースです。

観測数

観測数は、5 分間の監視の間に、監視デバイスが特定のアプリケーション/サーバ/ネットワークの組み合わせに対してパフォーマンス メトリックを計算した回数を測定します。 1 つの TCP トランザクション内でも、メトリックによって観測数が異なる場合があります。 たとえば、ネットワーク ラウンドトリップ時間の観測数の方が、サーバ レスポンス時間の観測数よりも多い場合が考えられます。 また、常に観測数が同じである、リンクなどのメトリックもあります。たとえば、各 TCP トランザクションに、それぞれ 1 つのサーバ レスポンス時間およびデータ転送時間の観測があります。 メトリックを正常、マイナー（黄色）またはメジャー（オレンジ）として評価するには、メトリックに最小観測数があることが必要です。

感度レベル

感度レベルは、0 から 200 の尺度で表される単位のない基準値です。これは、クライアント、サーバ、およびアプリケーションの各組み合わせに対して、その履歴データに基づいて新しいしきい値を計算するための固有の計算式に適用されます。 管理コンソールは、過去 30 日のパーセンタイル統計を使用して、毎晩 GMT の午前 0 時にメトリックの新しいしきい値を自動的に生成します。 管理コンソールは、各クライアント ネットワークからアプリケーションにアクセスするユーザのために、独立したしきい値のセットを自動的に生成します。

キープアライブ メッセージ

要求/レスポンスごとに新しい TCP 接続を確立するのではなく、TCP 接続を永続的に確立し、アクティブにしておくメソッドです。TCP *キープ アライブ メッセージ*は既知の形式に従うため、レスポンス時間メトリックが不正確になることはありません。 アプリケーションのキープ アライブは、シーケンス番号を 1 増やし、ペイロードを持っており、SRT（サーバ レスポンス時間）などいくつかのサーバ メトリックの測定値を不正確にする可能性があります。

拒否されたセッションの割合

*拒否されたセッションの割合*は、サーバがレポート間隔中に明示的に拒否した接続要求の割合を測定するサーバ メトリック (P. 245)です。 このメトリックは、CA ADA 管理コンソールの「未対応の TCP/IP セッション リクエスト」レポートに含まれます。

組み合わせ

*組み合わせ*は、CA ADA がレスポンス時間メトリックを計算したタイムフレーム、アプリケーション ポート、サーバ、ネットワーク、およびパフォーマンス メトリックを特定します。たとえば、管理コンソールは、過去 24 時間に Development クライアント ネットワークと通信したすべてのアプリケーションおよびサーバの平均ネットワーク接続時間をレポートすることができます。

結合メトリック

*結合メトリック*は、アプリケーションのパフォーマンス問題の原因が、アプリケーションをホストするサーバ、またはアプリケーションと通信しているネットワークのいずれか、または両方にあることを示します。CA ADA 管理コンソールでは、結合メトリックである［データ転送時間 (P. 247)］と［トランザクション時間 (P. 248)］のそれぞれに対して、パフォーマンスしきい値を設定できます。 管理コンソールはアプリケーション インシデントを作成しないことに注意してください。 ただし、結合メトリックには、ネットワークおよびサーバの両方のメトリックが含まれるので、管理コンソールはサーバやネットワークをマイナー（黄色）またはメジャー（オレンジ）と評価し、アプリケーションへの対応するパフォーマンス インパクトを評価できます。 たとえば、サーバ メトリックがマイナーと評価された場合は、管理コンソールでもアプリケーションの結合メトリックがマイナーと評価されます。

権限セット

ユーザが表示する権限を持つアプリケーション集約、サーバ集約、およびネットワーク集約の定義されたリスト。集約は 1 つ以上の権限セットのメンバになります。

コア層

標準的な 3 層（アクセス、ディストリビューション、コア）LAN ネットワークでは、*コア層*は、ディストリビューション層デバイスの高速相互接続を可能にします。 コア層には、通常、ネットワークで最も強力なルータとスイッチおよび最高速の相互接続があります。 通常、この層では、クライアントからサーバへのトランザクションのみが確認できます。

コントロール ポート アプリケーション

コントロール ポート アプリケーションは 2 つの TCP ポートを使用します。コントロール ポートはリクエスト情報を送受信します。また、データ ポートは実際のデータを送受信します。同じ監視デバイスは、トランザクション レスポンス時間を決定するためにコントロール ポートおよびデータ ポート トラフィックの両方を監視する必要があります。 どのタイプの監視デバイスも、コントロール ポート アプリケーションを監視できます。

サーバ インシデント

サーバ インシデントは、5 分間隔中に特定のアプリケーション、サーバ、ネットワークの組み合わせに対してサーバ レスポンス時間、サーバ接続時間、拒否されたセッションの割合、無応答セッションの割合など、サーバ メトリックのしきい値を超えた場合に、管理コンソールによって作成されます。

サーバ インシデント レスポンス

サーバ インシデント レスポンスは、サーバ インシデント (P. 245)に対する管理コンソールのレスポンスです。 管理コンソールでは、サーバ インシデントに次のレスポンスを割り当てることができます： 電子メール通知 (P. 248)、SNMP トラップ通知 (P. 237)、ping レスポンス時間調査 (P. 237)、SNMP 経由のパフォーマンス調査 (P. 237)、パケット キャプチャ調査 (P. 251)。

サーバ サブネット

サーバ サブネットは、各監視デバイスによって監視されるサーバ IP アドレスの連続した範囲を指定します。 アプリケーションを定義する際、アプリケーションに特定のサーバ サブネットを割り当てることで、サーバ IP アドレスの連続する範囲において管理コンソールがアプリケーションのパフォーマンスを自動的に監視できるようになります。

サーバ接続時間

SCT（サーバ接続時間）は、サーバがクライアントの SYN パケットに対して Syn-Ack を送信することで初期クライアント接続要求を確認するのにかかる時間の長さを測定するサーバ メトリック (P. 245)です。

サーバ メトリック

サーバ メトリックは、アプリケーションのパフォーマンス問題の原因が、アプリケーションをホストするサーバにあることを示します。 CA ADA 管理コンソールを使用して、次の各サーバ メトリックのパフォーマンスしきい値をカスタマイズできます： サーバ レスポンス時間 (P. 245)、サーバ接続時間 (P. 245)、拒否されたセッションの割合 (P. 243)、無応答セッションの割合 (P. 252)。

サーバ レスポンス時間

*サーバ レスポンス時間*は、サーバがクライアント要求に対して最初のレスポンスを送信するのにかかる時間または初期サーバ思考時間を測定する サーバ メトリック (P. 245)です。 サーバ レスポンス時間が増加した場合、通常は CPU、メモリ、ディスク /O などのサーバ リソースが不足しているか、アプリケーションの設計に問題があるか、または多層アプリケーション内にパフォーマンスの悪い層があることを示しています。

再送信遅延

再送信遅延は、元のパケット送信から最後の重複するパケット送信までに経過した時間を測定するネットワーク メトリック (P. 250)です。 管理コンソールは、再送信パケット数に対してだけではなく観測を通した平均としての再送信遅延をレポートします。 たとえば、10 個で 1 セットの 1 つのパケットが 300 ミリ秒の再送信時間を必要とする場合、再送信遅延は 30 ミリ秒（300 ミリ秒/10 パケット）としてレポートされます。

しきい値

「パフォーマンスしきい値 (P. 251)」を参照してください。

失効したセッション

失効したセッションは、CA ADA Monitor サービスが TCP セッションの終了（FIN または RST パケット）を検出しなかった TCP セッションの数を測定します。 一定期間非アクティブであるセッションは、メモリからクリアされ、「期限切れ」としてマークされます。 管理コンソールは、15 分間の間にパケットを観測しない場合、セッションを［期限切れ］として分類します。 オープンのままになっている期限切れセッション数が多すぎると、サーバが応答しなくなる可能性があります。

実効ネットワーク ラウンドトリップ時間

実効ネットワーク ラウンドトリップ時間は、再送信遅延 (P. 246)とネットワーク ラウンドトリップ時間 (P. 250)から構成されるネットワーク メトリック (P. 250)です。 再送信遅延は、再送信による遅延ではなく、1 ラウンドトリップあたりの再送信遅延の平均時間であることに注意してください。管理コンソールでは、2 つの平均が追加され、実際に 2 つのメトリックを組み合わせています。

推定ホップ遅延

推定ホップ遅延は、2 つのノード間で発生した遅延時間の推定値です。 管理コンソール は、たとえばトレース ルート調査 (P. 248)中に採取したすべてのサンプルの平均を使用してこの推定値を決定します。

多層アプリケーション

多層アプリケーションは複数のサーバを使用するアプリケーションで、サーバ間の通信は、クライアントへのリクエストを処理するサーバとして機能すると同時に共に別のサーバのクライアントとしても機能するサーバによって実行されます。

タップ

「ネットワーク タップ (P. 250)」を参照してください。

調査

調査とは、アプリケーション、ネットワーク、およびサーバの特定のパフォーマンス データをアクティブに照会することです。 管理コンソール は、インシデントに対して調査を自動的に起動することができます。 CA ADA 管理者は、この調査を起動またはスケジュールすることもできます。

ディストリビューション層

標準的な 3 層 (アクセス、ディストリビューション、コア) LAN ネットワークでは、*ディストリビューション層*はルーティング、フィルタリング、およびポリシー管理が処理される場所です。 この層には、通常、ルータおよび第 3 層のスイッチが含まれます。 アクセス スイッチがディストリビューション層にデータを送信すると、データが収集されます。 サーバが別々のスイッチ上にある場合、一部のサーバからサーバへのトランザクションはこの層で発生する可能性があります。

データ転送時間

*データ転送時間*は、最初のレスポンス (サーバ レスポンス時間 (P. 245)の終了) からその要求で送信された最後のパケットに至るアプリケーション レスポンス全体を送信するのにかかる時間を測定する結合メトリック (P. 243)です。

TCP ウィンドウに収容しきれない大量のデータを送信する場合は、データ転送時間から初期サーバ レスポンス時間を除外し、ネットワーク ラウンドトリップ時間を含めます。 レスポンス時間は、アプリケーションの設計またはサーバやネットワークのパフォーマンスの影響を受ける場合があります。

管理コンソールは、データ転送時間のしきい値を超えた場合にインシデントをオープンしません。

デバイス

デバイスは、監視されているネットワークに接続された任意の TCP/IP システムです。

電子メール通知

電子メール通知は、アプリケーション インシデント レスポンス (P. 240)、サーバ インシデント レスポンス (P. 245)、またはネットワーク インシデント レスポンス (P. 249)であり、影響を受けたアプリケーション、サーバ、またはネットワークのしきい値違反について受信者に通知します。

ドメイン

*ドメイン*は、レポート目的のためクライアント IP トラフィックを分離し、サーバのホスト名を解決するために管理コンソールが使用する DNS サーバを特定します。

トランザクション

トランザクションは、TCP 要求および後続のすべてのレスポンスのことです。 Web ページのロードなどの単一のアプリケーション トランザクションが、複数の TCP トランザクションから構成されている場合があります。

トランザクション時間

トランザクション時間は、クライアントが要求を送信してからレスポンスの最後のパケットを受信するまでに経過した時間の長さを測定する結合メトリック (P. 243)です。 トランザクション時間は、サーバ レスポンス時間 (P. 245)、ネットワーク ラウンドトリップ時間 (P. 250)、再送信遅延 (P. 246)、データ転送時間 (P. 247)の合計です。 トランザクション時間のしきい値を超えた場合、管理コンソールはインシデントをオープンしません。

トレース ルート調査

トレース ルート調査はネットワーク インシデント レスポンス (P. 249)であり、遅延とルーティングの問題を監視するために、監視デバイスとエンド ポイントの間のパスとすべてのホップを記録します。必要な場合は、各ルータに対してパフォーマンス情報を SNMP ポーリングします。 CA ADA 管理者はこの調査を起動またはスケジュールすることもできます。

ドロップされたパケット

*ドロップされたパケット*は、CA Standard Monitor 上のパケット キャプチャ ドライバか、または CA GigaStor 上の GigaStor Connector によって分析されなかったパケットです。分析されなかった理由は、監視デバイスが極度のビジー状態のため、受信したパケットの一部を処理できなかったためです。監視デバイスによってドロップされるパケットの数が多すぎる場合は、管理コンソールがメジャーの監視デバイス インシデントを作成します。 管理コンソールは、監視デバイス上の監視 NIC またはサーバ スイッチ ポートにおけるパケットのロスを監視しません。

ネットワーク インシデント

特定のアプリケーション、サーバ、ネットワークの組み合わせについて、ネットワーク ラウンドトリップ時間、ネットワーク接続時間、実効ラウンドトリップ時間、再送信遅延などのネットワーク メトリックのしきい値を 5 分間超えた場合、管理コンソールはネットワーク インシデントを作成します。

ネットワーク インシデント レスポンス

*ネットワーク インシデント レスポンス*は、ネットワーク インシデント (P. 249)に対する CA ADA のレスポンスです。 CA ADA 管理者は、電子メール通知 (P. 248)、SNMP トラップ通知 (P. 237)、トレース ルート調査 (P. 248)をネットワーク インシデントに割り当てることができます。

ネットワーク接続時間

ネットワーク接続時間（*NCT*）は、サーバが Syn-Ack を送信してからクライアントが Ack を返送するまでの時間の長さを測定するネットワーク メトリック (P. 250)です。 ネットワークが混雑していない場合、それは距離およびシリアライゼーションによる最低限の遅延を表すネットワーク遅延を示し、現在のネットワーク アーキテクチャで可能な最良のラウンドトリップ時間を示します。 この値が突然上昇した場合は、一般に輻輳状態が原因と考えられますが、停滞している（上昇したままになる）場合は通常パス変更が原因です。

ネットワーク タイプ

アプリケーションへの同じ物理アクセスを共有するネットワークのグループ。 たとえば、リモートサイトでのサブネットはすべて、データ センターへの同じ WAN リンクを共有します。

ネットワーク タップ

ネットワーク タップは、コンピュータ ネットワークで転送されるデータにアクセスするためのハードウェア デバイスです。タップの設置後、タップに監視デバイスを接続できます。この場合、監視されているネットワークには影響を与えません。タップを使用する場合、表示できるトラフィックは、スイッチ ネットワークのただ 1 つのブロードキャスト ドメインにおいて両方向（アップストリームおよびダウンストリーム）で発生するトラフィックです。

ネットワーク メトリック

ネットワーク メトリックは、アプリケーションのパフォーマンス問題がアプリケーションと通信しているネットワークによって引き起こされていることを示します。 CA Application Delivery Analysis 管理コンソールを使用して、次の各ネットワーク メトリックのパフォーマンスしきい値をカスタマイズできます： ネットワーク ラウンドトリップ時間 (P. 250)、ネットワーク接続時間 (P. 249)、実効ネットワーク ラウンドトリップ時間 (P. 246)、および再送信遅延 (P. 246)。

ネットワーク ラウンドトリップ時間

*ネットワーク ラウンドトリップ時間*は、ロスしたパケットを除くパケットがネットワーク上のサーバとクライアントの間（双方向）を送信されるのにかかる時間を測定するネットワーク メトリック (P. 250)です。 アプリケーション、サーバおよびクライアント処理時間は除外されます。

ネットワーク領域

ネットワーク領域は、広範のサブネット定義をより狭いサブネットに自動的に展開するために使用される管理コンソール ツールです。 ネットワークは最大 256 の領域まで定義できます。たとえば 256 の /24 ネットワークを定義するために /16 ネットワークの 256 の領域を定義します。 ネットワーク領域を使用する場合、管理コンソールは広範のネットワーク定義ではなく狭い方のネットワーク領域サブネット定義をレポートします。

廃棄パケット

廃棄パケットは、パケットが管理コンソールで指定されたアプリケーション、サーバ、およびクライアント ネットワークのリストに一致しなかったために、監視デバイスによって意図的に破棄されたパケットのことです。

パケット キャプチャ調査

パケット キャプチャ調査は、問題が発生している特定のサーバ、アプリケーション ポート、およびネットワークをフィルタしてキャプチャするアプリケーション インシデント レスポンス (P. 240)またはサーバ インシデント レスポンス (P. 245)です。CA ADA 管理者はこの調査を起動またはスケジュールすることもできます。

パケット要約ファイル

パケット要約ファイルには、Cisco WAE デバイスまたは CA GigaStor Connector からの TCP ヘッダが含まれます。

パケット ロスの割合

*パケット ロスの割合*は、サーバの隣にある監視デバイスからのネットワーク内のデータ全体に対して再送信されたデータの比率を測定するネットワーク メトリック (P. 250)です。監視デバイスは、ネットワーク パスにおけるサーバからクライアントへの方向でのデータ ロスにより、サーバによって再送信されたパケットを確認できます。 データ ロスがクライアントからサーバへの方向でサーバに到達する前に発生した場合、監視デバイスはパケット ロスを観測できないため、そのロスは［パケット ロスの割合］には含まれません。 管理コンソールの［エンジニアリング］ページでは、パケット ロスの割合は QoS レポートに含まれます。

パフォーマンス運用レベル アグリーメント（パフォーマンス OLA）

パフォーマンス運用レベル アグリーメント（パフォーマンス OLA）は、リモートサイトのアプリケーション パフォーマンス目標の適合を評価することができます。 デフォルトでは、管理コンソールは、アプリケーション パフォーマンスの運用レベルを定義していません。

パフォーマンスしきい値

パフォーマンスしきい値は、許容可能なパフォーマンス挙動の境界値です。これは、すべてのアプリケーションに対してデフォルトで存在します。管理コンソールは、しきい値によってデータを評価できます。 インシデント作成、インシデント レスポンス、および調査に貢献します。

フラグメント化されたパケット

フラグメント化されたパケットとは、ネットワークをトラバースするときに複数のパケットに分割されたパケットです。

ベースライン

ベースラインは、ネットワークの過去の標準的なパフォーマンスを参照できるようにします。管理コンソールは、サーバ上のアプリケーション ポートとクライアント ネットワークの間の全 TCP セッションのベースラインを自動的にレポートします。 ベースラインは、アプリケーションの現在のパフォーマンスを過去のパフォーマンスの平均と比較するために使用します。 ベースラインを超えた場合でも、問題が発生しているとは限りません。 ベースラインは 1 時間ごとに計算され、時刻、曜日および日付が考慮されます。

ホップ

ホップとは、ネットワーク内の 2 つのゲートウェイの間の論理的なリンクです。 データ パケットがネットワークをトラバースする場合、通常 1 つ以上のルータまたはゲートウェイを通過します。論理上隣接している 2 つのゲートウェイ間のパスは、「ホップ」と考えられます。

マイナーのパフォーマンス評価

マイナーのパフォーマンス評価は、管理コンソールで使用される重大度の状態の 1 つ（黄色）で、メトリックの値がマイナーのしきい値を超えたことを示します。 管理コンソールでは、マイナーおよびメジャーの両方のパフォーマンス低下に対してしきい値を設定します。

未評価のパフォーマンス評価

未評価のパフォーマンス評価は、管理コンソール［操作］ページでグレーの重大度状態によって示され、しきい値を設定するには過去のデータが不十分である（正味 2 営業日分のデータが必要）ことを意味するか、または、観測数が少なかったために、設定された最小の観測しきい値を超える観測がなかったことを意味します。

無応答セッションの割合

*無応答セッションの割合*は、接続要求が送信されたがサーバが応答しなかったセッションの割合を測定するサーバ メトリック (P. 245)です。 このメトリックは、［未対応の TCP/IP セッション リクエスト］ビューに含まれています。

メジャーのパフォーマンス評価

メジャーのパフォーマンス評価は、管理コンソールで使用される重大度の状態の 1 つ（オレンジ）で、メトリックの値がメジャーのしきい値を超えたことを示します。 管理コンソールでは、マイナーおよびメジャーの両方のパフォーマンス低下に対してしきい値を設定します。

メトリック要約ファイル

メトリック要約ファイルには、事前に計算された Cisco NAM からのレスポンス時間メトリックが含まれます。CA ADA マネージャは、Cisco NAM からメトリック要約ファイルを受信します。

役割

*役割*は、CA ADA ユーザに表示される CA ADA 管理コンソールのページを指定します。

レポート ページ

管理コンソールは、標準 *レポート ページ*の下にレポート データを整理し、特定のタイプのユーザ（運用担当者、経営者、エンジニアなど）用にわかりやすく表示します。