

CA Application Delivery Analysis との統合

CA Application Delivery Analysis Multi-Port
Monitor

バージョン 10.1



このドキュメント（組み込みヘルプシステムおよび電子的に配布される資料を含む、以下「本ドキュメント」）は、お客様への情報提供のみを目的としたもので、日本CA株式会社（以下「CA」）により隨時、変更または撤回されることがあります。

CAの事前の書面による承諾を受ければ本ドキュメントの全部または一部を複写、譲渡、開示、変更、複本することはできません。本ドキュメントは、CAが知的財産権を有する機密情報です。ユーザは本ドキュメントを開示したり、

(i) 本ドキュメントが関係するCAソフトウェアの使用についてCAとユーザとの間で別途締結される契約または(ii) CAとユーザとの間で別途締結される機密保持契約により許可された目的以外に、本ドキュメントを使用することはできません。

上記にかかわらず、本ドキュメントで言及されているCAソフトウェア製品のライセンスを受けたユーザは、社内でユーザおよび従業員が使用する場合に限り、当該ソフトウェアに関連する本ドキュメントのコピーを妥当な部数だけ作成できます。ただしCAのすべての著作権表示およびその説明を当該複製に添付することを条件とします。

本ドキュメントを印刷するまたはコピーを作成する上記の権利は、当該ソフトウェアのライセンスが完全に有効となっている期間内に限定されます。いかなる理由であれ、上記のライセンスが終了した場合には、お客様は本ドキュメントの全部または一部と、それらを複製したコピーのすべてを破棄したことを、CAに文書で証明する責任を負います。

準拠法により認められる限り、CAは本ドキュメントを現状有姿のまま提供し、商品性、特定の使用目的に対する適合性、他者の権利に対して侵害のないことについて、黙示の保証も含めいかなる保証もしません。また、本ドキュメントの使用に起因して、逸失利益、投資損失、業務の中断、営業権の喪失、情報の喪失等、いかなる損害（直接損害か間接損害かを問いません）が発生しても、CAはお客様または第三者に対し責任を負いません。CAがかかる損害の発生の可能性について事前に明示に通告されていた場合も同様とします。

本ドキュメントで参照されているすべてのソフトウェア製品の使用には、該当するライセンス契約が適用され、当該ライセンス契約はこの通知の条件によっていかなる変更も行われません。

本ドキュメントの制作者はCAです。

「制限された権利」のもとでの提供：アメリカ合衆国政府が使用、複製、開示する場合は、FAR Sections 12.212、52.227-14 及び 52.227-19(c)(1)及び(2)、ならびに DFARS Section 252.227-7014(b)(3)または、これらの後継の条項に規定される該当する制限に従うものとします。

Copyright © 2014 CA. All rights reserved. 本書に記載された全ての製品名、サービス名、商号およびロゴは各社のそれぞれの商標またはサービスマークです。

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: CA Application Delivery Analysis のサポート	7
パケット キャプチャ調査	8
CA Application Delivery Analysis サポートのアーキテクチャ	10
CA Application Delivery Analysis Standard Monitor との比較	11
ネットワーク アドレス変換 (NAT)	13
CA Application Delivery Analysis データの概要	14
ポート要件	15
第 2 章: Multi-Port Monitor を監視デバイスとして設定	17
監視デバイスの追加	18
論理ポート ステータスの確認	21
TCP セッション情報の確認	22
第 3 章: 監視デバイスのインシデント	23
監視デバイス インシデントの有効化	24
非アクティブ監視デバイス インシデントへの応答	26
第 4 章: 特殊な初期化(.ini)ファイルのサポート	29
重複したパケットの解消	30
キープアライブ メッセージのフィルタ除外	32
第 5 章: WAN 最適化環境での監視	35
CA Application Delivery Analysis での Cisco WAAS のサポート	36
Multi-Port Monitor と WAN 最適化デバイスとの統合方法	37
CA Application Delivery Analysis 最適化レポート	37
WAN 最適化デバイスからのデータ共有	38

第 1 章: CA Application Delivery Analysis のサポート

Multi-Port Monitor アプライアンスでは、IPv4 ベースの TCP メトリックを集計し CA Application Delivery Analysis にエクスポートします。このアプライアンスは、複数の Standard Monitor よりも多くのデータを、より速く収集します。このアプライアンスは、柔軟性が高く、オーバーヘッドの少ない高ボリューム モニタリングを必要とする企業のための選択肢です。

IPv4 ベースのトラフィックの監視時、アプライアンスでは CA Application Delivery Analysis での拡張されたパケットキャプチャ調査をユーザが実行できるようパケットを保存します。Standard Monitor では、これらの調査により調査の開始後に送信されたパケットのみがキャプチャされます。対照的に、アプライアンスに格納されるキャプチャファイルでは、パフォーマンス問題のフォレンジック分析を実行できます。

Multi-Port Monitor および CA Application Delivery Analysis 管理コンソールで IPv4 ベースのトラフィックを監視する場合、下のようなタスクを実行できます。

- 複数の Single-Port Monitor と同等のネットワーク スループット レートを処理する。
- 1 分単位の精度でデータを表示し、複数のグラフ タイプから選択する。
- インシデントが発生した時点のパケットキャプチャ調査ファイルを生成し、そのファイルを 90 日間格納する。
- ネットワーク、サーバ、およびアプリケーションの迅速で正確な検出を実行する。
- 複数のスイッチで TCP セッションを追跡し、高レベル CA Application Delivery Analysis サマリ レポートから詳細なメトリックをドリルダウンする。
- 複数のフィルタおよび並べ替え機能を活用して、利用可能なデータを分析し、迅速に問題のあるホストを分離する。
- 頻繁に使用するフィルタおよびレポート オプションを組み合わせたトラブルシューティング ワーク フローである分析を作成し、保存する。

- パケットキャプチャファイルを PCAP 形式でエクスポートし、IT エンジニアリングスタッフに送信して詳細な分析を行う。
- 別のアグリゲータアプライアンスをインストールせずに、Cisco Wide-Area Application Services (WAAS) 環境を監視する。
- CA GigaStor が提供するパケット要約ファイルからレスポンス時間メトリックを計算する。

このセクションには、以下のトピックが含まれています。

[パケットキャプチャ調査 \(P. 8\)](#)

[CA Application Delivery Analysis サポートのアーキテクチャ \(P. 10\)](#)

[CA Application Delivery Analysis Standard Monitor との比較 \(P. 11\)](#)

[ネットワークアドレス変換 \(NAT\) \(P. 13\)](#)

[CA Application Delivery Analysis データの概要 \(P. 14\)](#)

[ポート要件 \(P. 15\)](#)

パケットキャプチャ調査

CA Application Delivery Analysis は、ネットワークまたはサーバのパフォーマンスインシデントに応じて自動的にパケットキャプチャ調査を実行します。これらの調査は、さらに分析可能なパケットレベルデータを自動的に記録することにより、パフォーマンスマトリック分析の精度を向上させます。

パケットキャプチャ調査が CA Application Delivery Analysis Standard Monitor で実行される場合、キャプチャされたデータには必ずしも必要なトラフィックが含まれるとは限りません。Multi-Port Monitor が実行するパケットキャプチャ調査ははるかに包括的です。アプライアンスの短期パケットストレージ機能では、パケットキャプチャ調査によりインシデント発生時のトラフィックの詳細が提供されます。

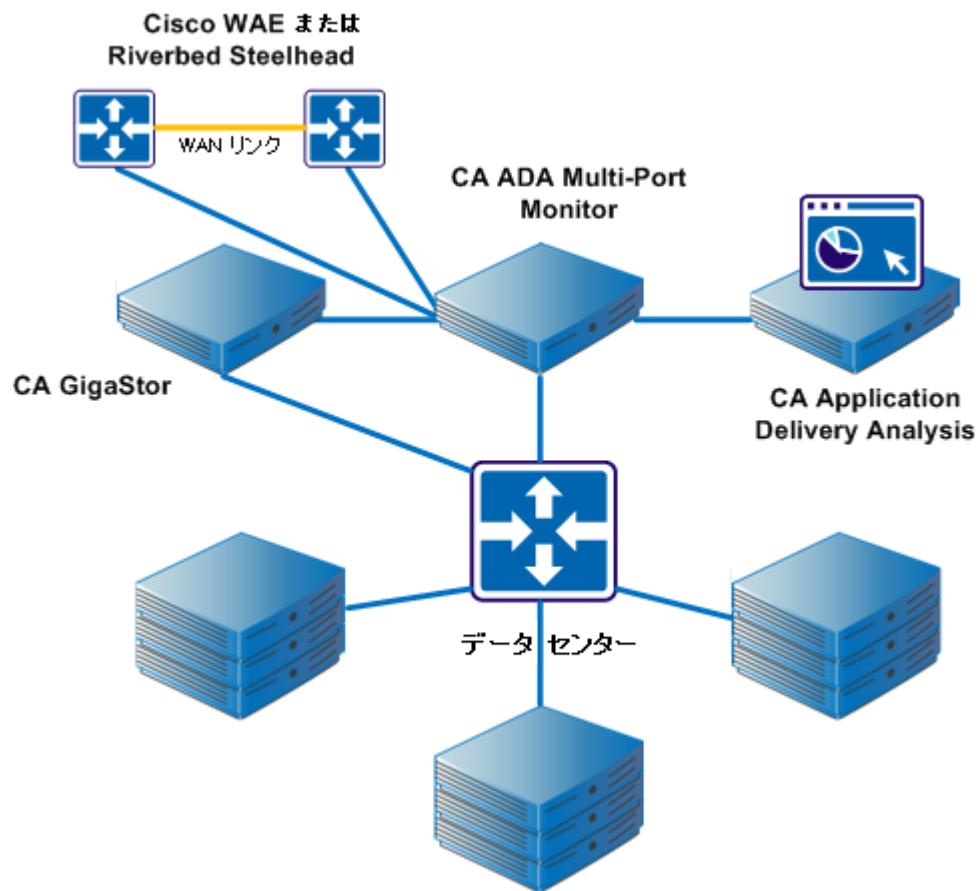
キャプチャおよび監視用のオプションでは、パケットヘッダまたはパケット全体を検査できます。デフォルトでは、アプライアンスはパケットキャプチャ調査ファイルを 90 日間保存します。それらにアクセスするには、CA Application Delivery Analysis 管理コンソールにログインしてパケットキャプチャ調査のレポートに移動します。[インシデント] タブをクリックして [調査レポート] ページへのリンクを確認します。

CA GigaStor が監視デバイスとして CA Application Delivery Analysis に割り当てられると、集計用に CA Application Delivery Analysis にパケット要約を送信します。CA Application Delivery Analysis パケットキャプチャ調査は、CA GigaStor に格納されるパケットにのみ基づきます。

CA Application Delivery Analysis サポートのアーキテクチャ

以下の図は、CA Application Delivery Analysis をサポートするための Multi-Port Monitor アーキテクチャおよび設定を示します。Multi-Port Monitor は標準的な CA Application Delivery Analysis 分散設定で動作し、CA Application Delivery Analysis 管理コンソールにネットワーク接続します。

購入した設定に応じて、1つのアプライアンスを最大 8 つの個別のスイッチ上のミラー ポートに接続できます。アプライアンスは監視対象のスイッチから管理コンソールへデータを送信します。そこでデータがすべての CA Application Delivery Analysis レポートに含まれます。



CA Application Delivery Analysis Standard Monitor との比較

Multi-Port Monitor アプライアンスおよび CA Standard Monitor はともに IPv4 ベースの TCP メトリックを集計し、CA Application Delivery Analysis にエクスポートします。以下の表では、IPv4 ベースの TCP トラフィック監視時の CA Application Delivery Analysis Single-Port Monitor と Multi-Port Monitor の最も顕著な相違点の概要について説明します。

機能	Standard Monitor	Multi-Port Monitor
複数のミラーリングされたスイッチ ポートの監視	はい	はい
サーバ、アプリケーションおよびネットワークの可用性の監視	はい	はい
自己監視およびアラート	はい	はい。 CA Application Delivery Analysis 非アクティブ監視デバイス インシデントがサポートされています。 SNMP トラブルは追加のアラートを提供します。
URL の監視	はい	いいえ
CA Application Delivery Analysis 管理コンソールからの調査のサポート	はい	はい。拡張されたパケットキャプチャ調査がサポートされています。
すべての CA Application Delivery Analysis メトリックの収集	はい	はい
サーバ、アプリケーション、およびネットワークの自動設定のサポート	はい	はい
(たとえばミラーリングされた VLAN からの) 重複パケットの無視	はい (追加設定後)	はい (自動)
1 分単位の精度でパフォーマンス データの提供	いいえ	はい

CA Application Delivery Analysis Standard Monitor との比較

機能	Standard Monitor	Multi-Port Monitor
指定されたホスト、サーバ、またはアプリケーション用のキャプチャされたデータのフィルタおよび表示	いいえ	はい
Cisco WAE デバイスからのパケット要約データの受信	はい	はい
CA GigaStor からのパケット要約データの受信	はい	はい
64 ビット オペレーティングシステムでの CA Application Delivery Analysis のサポート	はい	はい。 Multi-Port Monitor との互換性を確保するために、CA Application Delivery Analysis は 64 ビット オペレーティングシステム上で実行されている必要があります。

ネットワークアドレス変換(NAT)

Multi-Port Monitor では、Multi-Port Monitor および ADA マネージャの間でネットワークアドレス変換 (NAT) が有効な環境で正しく動作するためにはいくつかの追加設定が必要となります。以下を実行してください。

1. `setNatInfo` コマンドラインユーティリティを使用して、変換された IP アドレスで Multi-Port Monitor を更新します。
2. 監視デバイスを CA Application Delivery Analysis に追加する際に Multi-Port Monitor の変換済み IP アドレスを指定します。

デフォルトでは、Multi-Port Monitor および ADA マネージャは、互いと通信するために自身の管理 IP アドレスを使用します。

Multi-Port Monitor と ADA マネージャが互いに通信するために現在使用している IP アドレスを参照するには、[システムステータス] ページをクリックします。[システム情報] セクションには、管理 IP アドレスが表示され、指定されている場合は変換済み IP アドレスが表示されます。

コマンドラインユーティリティ `/opt/NetQoS/scripts/setNATInfo.php` を使用して、変換済み IP アドレスを指定します。使用方法は以下のとおりです。

```
/opt/NetQoS/scripts/setNATInfo.php [--console d.d.d.d] [--probe d.d.d.d]
```

各項目の説明 :

`--console`

ADA マネージャの変換済み IP アドレスです。Multi-Port Monitor は、このアドレスを介して ADA マネージャにアクセスします。

`--probe`

Multi-Port Monitor の変換済み IP アドレスです。ADA マネージャは、このアドレスを介して Multi-Port Monitor にアクセスします。

コマンドラインユーティリティを使用して以下のタスクを実行します。

使用方法を表示

パラメータなしで次のユーティリティを実行します :

```
/opt/NetQoS/scripts/setNATInfo.php
```

ADA マネージャの変換済み IP アドレスを指定

以下のパラメータでユーティリティを実行します：
`/opt/NetQoS/scripts/setNATInfo.php --console d.d.d.d`

Multi-Port Monitor の変換済み IP アドレスを指定

以下のパラメータでユーティリティを実行します：
`/opt/NetQoS/scripts/setNATInfo.php --probe d.d.d.d`

ADA マネージャおよび Multi-Port Monitor の変換済み IP アドレスを指定

以下のパラメータでユーティリティを実行します：
`/opt/NetQoS/scripts/setNATInfo.php --console d.d.d.d --probe d.d.d.d`

データベース内の NAT 情報をリセット(クリア)

NULL キーワードでユーティリティを実行します：
`/opt/NetQoS/scripts/setNATInfo.php --console NULL --probe NULL`

CA Application Delivery Analysis データの概要

CA Application Delivery Analysis 製品ドキュメントは、レポートデータを解釈し、監視対象のネットワーク、サーバ、またはアプリケーションから生じる問題を診断するための情報を提供します。

トラブルシューティングアクティビティの出発点として役立つメトリックは、トランザクション時間（レスポンス時間を表す別の用語）です。トランザクションは、以下のコンポーネントで構成されています。

- 1つのリクエストおよび1つのサーバ レスポンス
- 1つの期間のデータ転送
- 1つ以上の応答確認
- 再送信されたパケットからの監視された遅延

CA Application Delivery Analysis データではネットワークの観点からパフォーマンスが識別されます。分析における対応するデータでは、TCP セッション、ボリューム統計、およびレスポンス時間の複数のビューでアクティビティとパフォーマンスのデータが強調表示されます。パフォーマンス問題を調査する場合、スループットなど、トランザクション時間および関連するメトリックを考慮します。

注: セッションレベルパフォーマンスデータは、Multi-Port Monitor の論理ポートで受信される IPv4 ベースのポート ミラー データでのみ利用可能です。セッションレベルデータは、CA GigaStor または WAE デバイスからのパケット要約データでは利用できません。

処理は、以下のとおりです。

- CA Application Delivery Analysis レポートの [セッション分析] をクリックします。
- CA Application Delivery Analysis から Multi-Port Monitor へ情報が送信され、選択されたネットワーク、サーバ、またはアプリケーションのデータのコンテキストおよびタイムフレームを識別します。
- 個別のブラウザ ウィンドウで、Multi-Port Monitor Web インターフェースにより [分析] ページが開きます。データは選択されたコンテキスト用の関連するパフォーマンスデータを表示するためにフィルタされます。Multi-Port Monitor データは 1 分単位で利用可能なので、分析のグラフは CA Application Delivery Analysis に表示されたグラフとは異なります。最も小さな CA Application Delivery Analysis レポート間隔は 5 分です。

また、異なるレポート間隔によりメトリックの平均も異なります。設定により、分析で表示されたデータが管理コンソール内に表示されるかどうかが決まります。たとえば、CA Application Delivery Analysis で定義されていないネットワークからのデータは分析内にのみ利用可能です。

- 追加フィルタの適用、別のグラフ形式の選択、タイムフレームの変更、カスタム分析の保存が可能です。

ポート要件

Multi-Port Monitor アプライアンスでは、以下の通信パスをサポートするために複数のポートを開く必要があります。

- CA Application Delivery Analysis とアプライアンスの間。
- Enterprise Manager とアプライアンスの間 (CA TIM がインストールされている場合)。
- Multi-Port Monitor 管理用 Web インターフェースへのアクセス。

ポート	方向	説明
80	CA Application Delivery Analysis および Enterprise Manager からの受信	<ul style="list-style-type: none"> ■ Web インターフェース アクセスのための HTTP ■ Enterprise Manager の CA TIM との通信

ポート要件

ポート	方向	説明
80	CA Application Delivery Analysis への送信	Multi-Port Monitor Web サービスによる設定データの要求
161	インバウンド	SNMP MIB クエリ
162	アウトバウンド	SNMP トрап
7878	インバウンド	WAE デバイスからのパケット要約を含む TCP フロー 注: WAE デバイスが監視フィードである場合にのみ必要です。
8080	CA Application Delivery Analysis および Enterprise Manager からの受信	<ul style="list-style-type: none">CA Application Delivery Analysis Web サービスによるデータの要求Enterprise Manager によるネットワーク ヘルス データの要求。CA APM コンソールの [障害詳細] ページに表示されます。
9995	インバウンド	CA GigaStor コネクタからのパケット要約を含む UDP フロー 注: CA GigaStor が監視フィードである場合にのみ必要です。

第 2 章: Multi-Port Monitor を監視デバイスとして設定

Multi-Port Monitor アプライアンスは CA Application Delivery Analysis 用の監視デバイスです。

Multi-Port Monitor と ADA マネージャの間でネットワーク アドレス変換 (NAT) が有効な環境で、以下を実行してください。

1. `setNatInfo` コマンド ライン ユーティリティを使用して、変換された IP アドレスで Multi-Port Monitor を更新します。
2. 監視デバイスを CA Application Delivery Analysis に追加する際に Multi-Port Monitor の変換済み IP アドレスを指定します。

ヒント : アプライアンスを監視デバイスとして設定する前に、任意で以下の手順を実行します。

- CA Application Delivery Analysis に送信されるデータを制御するために ハードウェア フィルタを設定します。
- 各データ ソースを識別しやすくするために、各論理ポートに意味のあるラベルを割り当てます。

このセクションには、以下のトピックが含まれています。

[監視デバイスの追加 \(P. 18\)](#)

[論理ポート ステータスの確認 \(P. 21\)](#)

[TCP セッション情報の確認 \(P. 22\)](#) 詳細 :

[ネットワーク アドレス変換 \(NAT\) \(P. 13\)](#)

監視デバイスの追加

CA Application Delivery Analysis 用の監視デバイスとして Multi-Port Monitor を追加します。

Multi-Port Monitor と ADA マネージャの間でネットワークアドレス変換 (NAT) が有効な環境で、以下を実行してください。

1. `setNatInfo` コマンドラインユーティリティを使用して、変換された IP アドレスで Multi-Port Monitor を更新します。
2. 監視デバイスを CA Application Delivery Analysis に追加する際に Multi-Port Monitor の変換済み IP アドレスを指定します。

デフォルトでは、Multi-Port Monitor および ADA マネージャは、互いと通信するために自身の管理 IP アドレスを使用します。

以下の手順に従います。

1. Web ブラウザのポップアップブロック機能を無効にします。 CA Application Delivery Analysis では監視デバイスを追加するときにポップアップを使用します。
2. 管理者権限を持つユーザとして CA Application Delivery Analysis 管理コンソールにログインします。
3. [環境管理] - [データ監視] - [監視デバイス] をクリックします。 [ADA 監視デバイス リスト] が表示されます。
4. [ADA 監視の追加] をクリックします。 [Standard Monitor のプロパティ] ページが表示されます。
5. 以下のフィールドに入力します。
 - **サーバ名** アプライアンス用のサーバ名を入力します。サーバ名が不明な場合は、[管理アドレス] フィールドに IP アドレスを入力し、[DNS] をクリックします。CA Application Delivery Analysis は、IP アドレス解決を試行します。
 - **管理アドレス** Multi-Port Monitor 管理 NIC の IP アドレスを入力します。IP アドレスが不明な場合は、[サーバ名] フィールドに DNS 名を入力し、[IP] をクリックします。CA Application Delivery Analysis は、DNS 名解決を試行します。
 - **インシデント レスポンス** 監視デバイスインシデントのレスポンスを選択します。

- **可用性監視**（オプション） [有効] を選択すると、CA Application Delivery Analysis は 5 分ごとにアプライアンスの可用性を監視します。
- **Multi-Port Monitor** CA Multi-Port Monitor を追加するには、このオプションを選択します。このオプションは、管理コンソールがホスト名または IP アドレスにより監視デバイスに接続できない場合に表示されます。

注: 以下のフィールドは Multi-Port Monitor に適用されません。

- 複数の監視 NIC の有効化
- 監視アドレス
- パケット監視の無効化

6. [OK] をクリックします。

[ADA 監視デバイスリスト] が更新され、アプライアンスが利用可能であることを示します。

7. (オプション) ドメインが CA Performance Center で実装される場合は、各監視フィードに正しいドメインを割り当てます。デフォルトでは、すべての監視フィードはデフォルト ドメインに割り当てられます。
 - a. CA Multi-Port Monitor 監視デバイスをクリックして編集します。
 - b. Multi-Port Monitor プロパティで、監視フィードのリストは CA Multi-Port Monitor 上の論理ポートに対応します。以下のものを含む各監視フィードを管理します。
 - レポートするドメイン：
 - VLAN にタグ付けされたトラフィック [VLAN の割り当て] をクリックして特定の VLAN トラフィックをドメインに割り当て、未割り当ての VLAN トラフィックのドメインを指定します。
 - タグ付けのないトラフィック。編集アイコン (✎) をクリックして、監視フィード上のタグ付けのないトラフィックに対してドメインを指定します。
 - 重複する IP トラフィックを分けるためにドメインを使用していない場合には、適用されません。
 - たとえば、同じトラフィックが別のネットワークにフェールオーバする場合の冗長データ監視のための監視フィード。

セカンダリ監視フィードをペアにするには、編集アイコン (✎) をクリックし、次に、セカンダリフィード列をクリックします。監視フィードと同じトラフィックを参照するセカンダリ監視フィードのみを割り当てることにより、データ重複を回避します。
 - アクティブ セッション情報。

アクティブ セッション情報を表示するには、[アクティブ セッション] をクリックします。アクティブ セッション情報は、監視フィードがアクティブな TCP セッションを監視しているかどうかを確認するために役立ちます。
8. 青い歯車メニュー (⚙) をクリックし、[監視デバイスを同期] をクリックします。

CA Application Delivery Analysis はアプライアンスに監視手順を送信します。
9. 監視するネットワーク、サーバ、およびアプリケーションを設定します。「CA Application Delivery Analysis 管理者ガイド」に詳しい手順が記載されています。

10. [ADA 監視デバイスリスト] に移動して、同期を再実行します。
11. [ADA 監視デバイスリスト] を参照して、アプライアンスが CA Application Delivery Analysis にデータを送信していることを確認します。

注: 少なくとも 1 つの有効なサーバ サブネットおよび 1 つのネットワークを設定すると、[最終監視] および [ステータス] フィールドが更新されます。アプライアンスが CA Application Delivery Analysis にデータを送信する前に、10 分以内の時間がかかることがあります。

論理ポートステータスの確認

CA Application Delivery Analysis からの Multi-Port Monitor 用の論理ポートステータスを確認します。論理ポートは TCP レスポンス時間データのソースです。CA Application Delivery Analysis 管理コンソール内の監視フィードとして識別される論理ポートのステータスを表示できます。

この手順は、アプライアンスが CA Application Delivery Analysis の監視デバイスとして設定されている場合にのみ有効です。

次の手順に従ってください:

1. CA Application Delivery Analysis 管理コンソールの [環境管理] - [データ監視] - [監視デバイス] をクリックします。
アプライアンスのデバイス名が [ADA 監視デバイスリスト] に表示されます。
2. [オプション] 列の [編集] アイコンをクリックします ()。
[Multi-Port Monitor のプロパティ] ページが表示されます。 [監視フィード] テーブルには、各論理ポートのステータス情報が表示されます。
3. テーブル内の情報の説明を参照するには [ヘルプ] をクリックします。

TCP セッション情報の確認

CA Application Delivery Analysis 内の Multi-Port Monitor 用 TCP セッション情報を確認します。Multi-Port Monitor 上の各論理ポートについては、CA Application Delivery Analysis は、トラフィックを識別するために、アクティブな IPv4 ベースの TCP セッションの番号、サーバ名、アドレス、VLAN 識別子、およびポート番号をレポートします。論理ポートは CA Application Delivery Analysis 管理コンソール内の監視フィードとして識別されます。監視フィードが、ドメインへのタグ付けされた VLAN トラフィックを区別する場合、CA Application Delivery Analysis は監視フィード内のセッションをすべてレポートします。

次の手順に従ってください:

1. CA Application Delivery Analysis 管理コンソールの [環境管理] - [データ監視] - [監視デバイス] をクリックします。
アプライアンスのデバイス名が [ADA 監視デバイスリスト] に表示されます。
2. [オプション] 列の [編集] アイコンをクリックします ()。
[Multi-Port Monitor のプロパティ] ページが表示されます。
3. 3 番目の [表示項目] リスト内の [アクティブセッション数] をクリックします。
[アクティブセッション数] ページが表示されます。
4. セッション情報を表示するための監視フィードを選択します。
[アクティブセッション数] ページには、監視対象のサーバおよびそれらの対応するフィードについての情報が表示されます。 [アクティブセッション数] データは、アプライアンスとミラー ポートのセットアップの確認、およびネットワークまたはサーバの問題のトラブルシューティングに役立ちます。
5. [アクティブセッション数] ページのフィールドの詳細については、[ヘルプ] をクリックしてください。

第3章: 監視デバイスのインシデント

CA Application Delivery Analysis 管理コンソールでは、管理者は、Multi-Port Monitor または監視フィードが非アクティブになったときに監視デバイスインシデントを作成するかどうかを指定できます。

非アクティブ監視インシデントは、CA Application Delivery Analysis が Single-Port Monitor、Multi-Port Monitor、または監視フィードからのデータ受信を停止したときに発生します。すべての監視デバイスインシデントは重大度が [超過] になります。CA Application Delivery Analysis では、[低下] の監視デバイスインシデントは作成されません。

また、Multi-Port Monitor は以下のイベントと関連付けられた問題に応答して SNMP トランプを送信します。

- 重大なプロセスステータス
- パケットキャプチャ機能
- ディスク使用量レベル
- RAID アレイおよびディスクドライブの障害

CA Application Delivery Analysis が監視デバイスからのパフォーマンスデータの受信を停止すると、そのデバイスは非アクティブであるとみなされます。例 :

- ネットワークがダウンしている。データは生成されません。
- 監視デバイスがダウンしている。データはミラーポート上に存在しますが、監視デバイスがアクティブではありません。

- 監視デバイスに割り当てられているフィードが非アクティブです。たとえば、WAN 最適化デバイスが使用できません。
- ミラー ポートの接続が失われている。データは生成されますが、ポートがアクティブではありません。

インシデントは、一部の論理ポートが引き続き CA Application Delivery Analysis にデータを送信している場合でも作成されることがあります。たとえば、Multi-Port Monitor に割り当てられた監視フィードがパケット要約の送信を停止したが、他のポートはアクティブなままの場合です。そのため、インシデントは必ずしも Multi-Port Monitor の完全な非アクティブ状態を示すわけではありません。

このセクションには、以下のトピックが含まれています。

[監視デバイス インシデントの有効化 \(P. 24\)](#)

[非アクティブ監視デバイス インシデントへの応答 \(P. 26\)](#)

監視デバイス インシデントの有効化

各監視デバイスには、デフォルトの監視デバイス インシデント レスポンスが割り当てられています。デフォルトのレスポンスはアクションと関連付けられていません。CA Application Delivery Analysis の [Multi-Port Monitor プロパティ] ページで、インシデント レスポンスをアクションに関連付けます。CA Application Delivery Analysis の標準的なワーク フローは以下のとおりです。

- 監視デバイス インシデント レスポンスを作成する
- 電子メール通知などのアクションをレスポンスに追加する
- デバイス プロパティ内で新しいインシデント レスポンスを選択する。

[Multi-Port Monitor プロパティ] ページにある [可用性監視] の設定により、CA Application Delivery Analysis が Multi-Port Monitor の非アクティブ監視デバイス インシデントを生成するかどうかが決定されます。この設定は、すべての新しい監視デバイス上でデフォルトで有効になっています。CA Application Delivery Analysis で非アクティブ監視デバイス インシデントが作成されないようにするには、そのデバイス上で可用性監視を無効にします。

CA Application Delivery Analysis のオンラインヘルプには、インシデントレスポンスを作成するためのガイダンスが含まれています。ただし、以下に示す手順の概要もその方法の理解に役立ちます。

次の手順に従ってください:

1. CA Application Delivery Analysis 管理コンソールの [環境管理] - [ポリシー] - [インシデント レスポンス] をクリックします。
2. [監視デバイス レスponsの追加] をクリックします。
[監視デバイス インシデント レスponsのプロパティ] ページが表示されます。
3. 新しいインシデント レスponsの名前を入力し、[OK] をクリックします。
新しいインシデント レスponsが、[監視デバイス インシデント レスpons] リストに表示されます。
4. 新しいレスponsの [編集] アイコンをクリックします。
[監視デバイス インシデント レスpons アクション] ページが表示されます。
5. [アクションの追加] をクリックします。
[監視デバイス アクションタイプ] ページが表示されます。
6. [電子メールの送信] または [SNMP トランプの送信] を選択し、[次へ] をクリックします。
7. 必須フィールドに入力します。これらの必須フィールドは、選択したアクションによって異なります。
8. [OK] をクリックします。
アクションの説明が [監視デバイス インシデント レスpons アクション] ページに表示されます。

9. インシデント レスポンスを有効にします。
 - a. 管理コンソールの [環境管理] - [データ監視] - [監視デバイス] をクリックします。
[ADA 監視デバイス リスト] が表示されます。
 - b. Multi-Port Monitor の [編集] アイコンをクリックします。
[Multi-Port Monitor のプロパティ] ページが表示されます。
 - c. [インシデント レスポンス] フィールドから、新しいインシデント レスポンスを選択します。
 - d. [OK] をクリックします。

非アクティブ監視デバイス インシデントが作成されると、選択したアクションが実行されます。

非アクティブ監視デバイス インシデントへの応答

非アクティブ監視デバイス インシデントを受信した場合は、以下の 1 つ以上のタスクを実行します。

- [CA Application Delivery Analysis インシデント] ページにある日付のリンクをクリックして詳細情報を表示します。
- アラートのトラップ受信者を確認します。 Multi-Port Monitor は、データ監視やキャプチャに影響を与える可能性のある問題の SNMP トラップを送信します。
- Multi-Port Monitor の Web インターフェースで、[システムステータス] ページを確認します。 このページで、インシデントが以下のどの原因で発生しているかを評価できます。
 - ハードウェアまたはソフトウェアの問題。 [プロセス情報] テーブルを確認して、停止されたプロセスを探します。
 - ネットワークの問題。 [キャプチャカード物理ポートステータス] テーブルを確認して、接続されていないリンクまたはダウンしたリンクを探します。
 - 監視フィードの問題。 [キャプチャカード論理ポートステータス] テーブルを確認して、非アクティブなフィードを探します。 ここでは、非アクティブな WAN 最適化デバイスや CA GigaStor は報告されません。

- 設定の問題。[キャプチャ カード論理ポート ステータス] テーブルを確認して、状態が [無効] になっている論理ポートを探します。これらのポートの [処理されたパケット数] 列にパケット数が表示されているかどうかを確認します。
- パケット キャプチャの問題。[キャプチャ カード物理ポート 統計情報] テーブルを確認して、異常なエラー数や、[パケット数] または [受信バイト数] 列の「0」の値を探します。
- RAID ドライブの問題。RAID テーブルを確認して、RAID ステータスや障害が発生したドライブを探します。

第4章: 特殊な初期化(.ini)ファイルのサポート

Multi-Port Monitor では、追加のパラメータを指定して、無関係なデータを無視するよう監視デバイスに指示することができます。これらのパラメータは、サポートされる以下の初期化 (.ini) ファイルによって監視デバイスに配布されます。

DataTransferManager.ini

sadatransfermanager プロセスがクライアント接続を待機する TCP ポート番号を設定します。このポート番号を変更しないでください。

DTMDistributedConsoles.ini.sav

共有されたパケット要約データをどの IP アドレスで受信するかを制御します。 詳細については、Multi-Port Monitor アプライアンス上の /opt/NetQoS/bin ディレクトリにある DTMDistributedConsoles.ini.readme ファイルを参照してください。

LimitDTTParams.ini.sav

データ転送時間のしきい値を制御します。

LimitServerResponseParams.ini.sav

サーバレスポンス時間のしきい値を制御します。

RetransPacketDefs.ini.sav

ソフトウェアデデュプリケーションを制御します。

saCollectorOptions.ini

nqmetricd サービスで使用されるデフォルトのデバッグトレースログ フラグが含まれています。より多くのログが必要な場合、[CA テクニカルサポート](#) の技術者からどのフラグを有効にするかを指示されることがあります。

saLinuxCollectorDirectives.ini

ログファイルの命名形式や、ローカル MySQL データベースにアクセスするためのパラメータを定義します。これらの情報を変更しないでください。

saMetricEngine.ini.sav

[アクティブセッション数] レポートのサイズを制御します。 詳細については、Multi-Port Monitor アプライアンス上の /opt/NetQoS/bin ディレクトリにある saMetricEngine.ini.readme ファイルを参照してください。

その他の初期化ファイルは、「CA Application Delivery Analysis 管理者ガイド」に記載されています。

このセクションには、以下のトピックが含まれています。

[重複したパケットの解消 \(P. 30\)](#)

[キープアライブメッセージのフィルタ除外 \(P. 32\)](#)

重複したパケットの解消

複数のミラー ポート設定のために、Multi-Port Monitor フィード上でパケットの重複が発生する場合があります。このセクションでは、標準的なハードウェア フィルタ オプションでは不十分な環境で Multi-Port Monitor への TCP トラフィックをミラーリングするためのベスト プラクティスについて説明します。

SuperAgentErrors.log ファイル内の破棄されたパケットは、この場合の要因ではありません。 CA Application Delivery Analysis Single-Port Monitor は、CA Application Delivery Analysis の設定に一致しないパケットを破棄します。これに対して、ドロップされたパケットの場合は、CA Application Delivery Analysis によって分析されないため問題が発生する可能性があります。

複数の VLAN を CA Application Delivery Analysis 監視デバイスにミラーリングすると、CA Application Delivery Analysis は、各 VLAN パケットの 2 つのコピーを受信します。この重複パケットの状態を修正するために、Multi-Port Monitor に追加の設定パラメータを渡すことができます。このディレクトリ内のファイルを変更するにはスーパーユーザ権限が必要なため、「sudo」コマンドプレフィックスを使用します。

次の手順に従ってください:

1. Multi-Port Monitor アプライアンス上の `/opt/NetQoS/bin/` ディレクトリに移動します。

```
cd /opt/NetQoS/bin
```

2. `RetransPacketDefs.ini.sav` ファイルをコピーして拡張子を削除します。

```
sudo cp RetransPacketDefs.ini.sav RetransPacketDefs.ini
```

この `.ini` ファイルは、次の監視同期中または `nqmetricd` プロセスが再起動したときにアクティブ化されます。

3. `RetransPacketDefs.ini` ファイルに以下のコード行を追加します。

```
<nologging>  
50 1000  
10 20 30 40 50 60
```

先頭の行は、CA Application Delivery Analysis に、重複したパケットに関する情報をログ記録しないよう指示します。Single-Port Monitor は、このタイプのログ記録をサポートしています。Multi-Port Monitor ではサポートされていません。

2行目は、再送されたデータのフィルタリングの適用方法を示します。数字 50 と 1000 は、CA Application Delivery Analysis に、重複を探すための 50 パケットのバッファを保持するよう指示します。このパラメータを減らすと、重複を探すときに Multi-Port Monitor によって消費される CPU サイクルが減少します。その結果、Multi-Port Monitor のパフォーマンスは向上しますが、見つかる重複は少なくなります。これらのデフォルト値を推奨します。

3行目は、重複のヒストグラムの bin を示します。Single-Port Monitor は、ログ記録オプションの一部としてヒストグラムをサポートしています。Multi-Port Monitor ではサポートされていません。

4. Multi-Port Monitor の Web インターフェースから `nqmetricd` プロセスを再起動します。

キープアライブ メッセージのフィルタ除外

アプリケーションのキープアライブ メッセージがレポート内の統計の監視に与える影響を制限できます。サーバレスポンス時間 (SRT) またはデータ転送時間 (DTT) を最大値に制限すれば、不要な SRT または DTT の観測は無視されます。この値を、キープアライブの頻度を下回る数秒に設定できます。

アプリケーションがキープアライブ メッセージを送信していると考えられる場合、観測数と SRT の間で逆比例の関係を探します。また、ミリ秒あたりではなく秒あたりの SRT 平均を探します。アプリケーションがキープアライブ メッセージを送信していることが確認できたら、SRT にしきい値を適用します。

アプリケーションが、DTT の増加につながるキープアライブ メッセージを使用している場合は、DTT をフィルタするため同様の制限を適用できます。

選択されたアプリケーションのキープアライブの頻度に自信がない場合は、開始点として 10 秒を使用してください。一般に、サーバがユーザ要求に応答し始めるのにかかる時間が 10 秒を超えることはめったにありません。ほとんどの場合、キープアライブの頻度は 10 秒を超えます。

注: CA Application Delivery Analysis Single-Port Monitor で SRT および DTT フィルタを適用することもできます。詳細については、「CA Application Delivery Analysis 管理者ガイド」を参照してください。

次の手順に従ってください:

1. Multi-Port Monitor アプライアンス上の /opt/NetQoS/bin ディレクトリに移動します。

```
cd /opt/NetQoS/bin
```

注: /opt/NetQoS/bin ディレクトリ内のファイルを変更するには、root 権限が必要です。そのため、この手順で説明されているすべてのコマンドで「sudo」プレフィックスを使用します。

2. SRT のしきい値を指定します。

a. `LimitServerResponseParams.ini.sav` ファイルをコピーして拡張子を削除します。

```
sudo cp LimitServerResponseParams.ini.sav LimitServerResponseParams.ini
```

この `.ini` ファイルは、次の同期中または `nqmetricd` プロセスが再起動されるときにアクティブ化されます。

b. 新しいファイルが書き込み可能であることを確認します。

```
sudo chmod u+w LimitServerResponseParams.ini
```

c. `.ini` ファイルを編集して、フィルタするポートごとに SRT のしきい値を変更します。

各アプリケーションについて、ポート番号と、許容可能な SRT の最大量を入力します。最大の SRT を、キープアライブの頻度よりわずかに小さい値に設定します。たとえば、60 秒の頻度で発生する Citrix のキープアライブメッセージを無視するには、以下の値を入力します。

```
-port=1494 -max seconds=59
```

注: この例では、`max seconds` が、スペースを含む 1 つのパラメータ名です。

d. ファイルを保存します。

3. フィルタするポートごとに DTT のしきい値を指定します。

a. `LimitDTTParams.ini.sav` ファイルをコピーして拡張子を削除します。

```
sudo cp LimitSDTTParams.ini.sav LimitDTTParams.ini
```

b. この新規ファイルを書き込み可能に設定します。

```
sudo chmod u+w LimitDTTParams.ini
```

c. `.ini` ファイルを編集し、手順 2 の説明に従って DTT のしきい値を変更します。

d. ファイルを保存します。

4. Multi-Port Monitor の Web インターフェースで、`nqmetricd` プロセスを再起動します。

第5章: WAN 最適化環境での監視

CA Application Delivery Analysis は、Cisco Wide Area Application Services (WAAS) などの WAN 最適化ソリューションと統合され、アプリケーションのパフォーマンスを監視します。WAN 最適化環境では、アプリケーションデータは監視システムから見えません。データは、実際のホストからではなく、WAAS デバイスから来たように見えます。WAN 最適化デバイスと統合された CA Application Delivery Analysis は、WAN 最適化が個々のアプリケーションのレスポンス時間に与えている影響を把握することができます。

Cisco WAAS では、データセンターや支店などのネットワーク内の主要な地点に複数の Cisco Wide Area Application Engine (WAE) デバイスが必要です。Cisco WAE デバイスと WAN 最適化デバイスは、CA Application Delivery Analysis 監視デバイスにパフォーマンスデータを送信します。このデータによって、WAN 最適化がネットワークの各セグメントでのアプリケーションのレスポンス時間にどのような影響を与えているかを把握できるようになります。

WAN 最適化デバイスが監視対象ミラー ポート経由でパフォーマンスデータを送信すると、Multi-Port Monitor はそれらのデバイスからデータを受信します。WAN 最適化のサポートは、Multi-Port Monitor の設定中に手動でアクティブ化します。このプロセスは、「CA Application Delivery Analysis 管理者ガイド」に記載されています。

このセクションには、以下のトピックが含まれています。

[CA Application Delivery Analysis での Cisco WAAS のサポート \(P. 36\)](#)

[Multi-Port Monitor と WAN 最適化デバイスとの統合方法 \(P. 37\)](#)

[CA Application Delivery Analysis 最適化レポート \(P. 37\)](#)

[WAN 最適化デバイスからのデータ共有 \(P. 38\)](#)

CA Application Delivery Analysis での Cisco WAAS のサポート

CA Application Delivery Analysis が Cisco WAAS 環境を監視するように設定されると、WAE デバイスは FlowAgent データを CA データ ソースにエクスポートします。Cisco WAAS は、ネットワークのための 3 つの個別の TCP セグメントを効率的に作成します。各セグメントからトランザクションパフォーマンス データが収集され、相関されます。CA Application Delivery Analysis は、1 つの最適化されたアプリケーション サーバ ネットワークの組み合わせについて、複数の監視ポイントから監視します。そのため、CA Application Delivery Analysis は TCP セグメントごとに個別のメトリック 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。

Cisco WAAS の有効性を完全に把握できるように、CA Application Delivery Analysis は、セグメントごとのアプリケーションのパフォーマンスを以下のように報告します。

- [クライアント] セグメント： ブランチ ロケーション内のクライアントと、そのブランチ ロケーションの WAE デバイスの間のネットワーク セグメント
- [WAN] セグメント： ブランチ WAE デバイスと、データ センター内で実行されている WAE デバイスの間のネットワーク セグメント
- [サーバ] セグメント： WAE デバイスとデータ センター内のサーバの間のネットワーク セグメント

3 つのすべてのセグメント上のアプリケーションの動作は、3 層アプリケーションの動作に類似しています。ソースおよび宛先ポートとアドレスは、これらの層全体にわたって同じままです。新しい CA Application Delivery Analysis アプリケーション プロパティは WAN 最適化 アプリケーションを監視し、各セグメントを識別します。

CA Application Delivery Analysis レポートでは、アプリケーション名にセグメント識別子が追加されます。たとえば、HTTP アプリケーション ラフィックは、HTTP [クライアント]、HTTP [WAN]、HTTP [サーバ] の 3 つの個別の項目として識別できます。追加のレポートである CA Application Delivery Analysis の [最適化] ページには、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。デフォルト ビューである [最適化されたトランザクションのクライアント 環境] は、セグメント化されたデータを含むアプリケーションに対するクライアント セグメントのパフォーマンスマップを提供します。

Multi-Port Monitor と WAN 最適化デバイスとの統合方法

`sadatatransfermanager` プロセスは、WAN 最適化デバイスから受信した TCP ヘッダ上のデータを集計します。このプロセスは、データをアクティブに転送または集計していない場合でも常に動作しています。このプロセスを停止または再起動することができます。

WAN 最適化デバイスは、Multi-Port Monitor アプライアンスを 5 分ごとにポーリングして監視対象サーバのリストを作成します。このデバイスは、アプライアンスにパケット要約ファイルを送信します。これらのファイルには、WAN 最適化デバイス上のサーバリストに一致する最適化トラフィックからの TCP ヘッダが含まれています。このデバイスは、最適化されていないトラフィックの TCP ヘッダを送信しません。

アプライアンスは、WAN 最適化デバイスから受信したパケットヘッダに対して以下のタスクを実行します。

- クライアントおよび WAN セグメント上の最適化されたトラフィックのパフォーマンスマトリックを計算します。
- WAN 最適化デバイスから送信されたサーバセグメントのパフォーマンスデータを、ミラーリングされたポートから送信されたより正確なデータに置き換えます。
- ポートミラー内のアプリケーショントラフィックを自動的に検出し、更新されたサーバのリストを提供します。CA Application Delivery Analysis は、すべてのサーバが監視されていることを確認するために、このリストをすべての WAN 最適化デバイスに継承します。

`sadatatransfermanager` プロセスは、WAN 最適化デバイスからの受信パケットヘッダをポート 7878 上でリスンします。

CA Application Delivery Analysis 最適化レポート

Multi-Port Monitor はパケット要約の内容を処理し、CA Application Delivery Analysis にパフォーマンスマトリックを送信します。これらのメトリックは、管理コンソールの [最適化] ページに表示されます。

[最適化] ページのデフォルト ビューは、トランザクション時間と観測数のパフォーマンスマップである [最適化されたトランザクションのクライアント環境] です。トランザクション時間（レスポンス時間）が最長のアプリケーションが最初に表示されます。

[最適化] ページを使用して **Multi-Port Monitor** のセッション分析に移動することはできません。ただし、各アプリケーションの名前が、そのアプリケーションのコンポーネントレポートへのリンクになっています。このレポートでは、トランザクション時間を以下のコンポーネントに切り分けます。

- サーバレスポンス時間
- ネットワークラウンドトリップ時間
- 再送信遅延
- データ転送速度およびボリューム

[コンポーネントレポート] ページでは、関連するインシデントや可用性に関する情報へのリンクが提供されます。

WAN 最適化デバイスからのデータ共有

1 つの CA Application Delivery Analysis 管理コンソールは通常、環境内のすべての WAN 最適化デバイスをサポートできます。ただし、WAN 最適化の展開に管理コンソールでサポート可能な数以上の監視デバイスが必要な場合は、負荷を分散することができます。以下の手順では、複数の **Multi-Port Monitor** 間で [クライアント]、[WAN]、および [サーバ] セグメントのパフォーマンスデータを共有する方法を説明します。

次の手順に従ってください:

1. **DTMDistributedConsoles.ini** という名前の設定ファイルを作成します。
2. この .ini ファイルを開きます
3. **Multi-Port Monitor** に割り当てられた管理コンソールの IP アドレスを入力します。この管理コンソールは、共有データを受信する他の監視デバイスを見つける方法を **Multi-Port Monitor** に指示します。
注: サンプルファイルが提供されています。このサンプルには、正しいファイル形式を示すための無効な IP アドレスが含まれています。このサンプルは /opt/NetQoS/bin フォルダにあります。
4. 新しい行の各 IP アドレスをドット区切りの 10 進表記を使用して区切ります。
5. **DTMDistributedConsoles.ini** ファイルをすべての監視デバイスにコピーします。 **Multi-Port Monitor** の場合は、このファイルを /opt/NetQoS/bin フォルダにコピーします。

6. `sadatatransfermanager` プロセスを再起動します。

WAN 最適化クライアントセグメントのデータが監視デバイス間で共有されるまでに最大 25 分かかる可能性があります。

7. その他の監視デバイスでデータを共有するには、手順 2 ~ 5 を繰り返します。

注: WAN 最適化デバイスからのデータ共有に関する詳細な情報は、「CA Application Delivery Analysis 管理者ガイド」に記載されています。