管理者ガイド

CA Application Delivery Analysis Multi-Port Monitor

バージョン 10.1

ca technologies

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: Multi-Port Monitor の概要

CA Application Delivery Analysis Multi-Port Monitor は、監視対象のデータ センターからセッション レベル パケット データをキャプチャする強力なアプライアンスです。 このアプライアンスでは、CA Application Delivery Analysis および CA Application Performance Management（CA APM）でレポートするためのデータをキャプチャします。

- TCP パケット ヘッダのデータは、CA Application Delivery Analysis がエンド ツー エンド パフォーマンスを監視し、アプリケーション レスポンス時間を測定するのに役立ちます。
- 完全な HTTP パケットのデータは、CA APM がユーザ環境のトランザクションをマップしてエンド ユーザ エクスペリエンスを監視し、サービス レベル アグリーメントを測定するのに役立ちます。

大量のデータ センター トラフィックを複数のポートからパッシブに監視することによって、Multi-Port Monitor はエンド ツー エンド システム パフォーマンスの連続的記録を保持するのを支援します。

監視対象のミラー ポートを通過するすべてのトラフィックからのパケット ヘッダが記録され、Multi-Port Monitor に短時間格納されます。1 分間のレポート間隔のデータは数日間保持され、分析に使用されます。メトリックは、レポート用に CA Application Delivery Analysis に、または CA APM でのレポート用に CA Transaction Impact Manager （CA TIM）に転送されます。

Multi-Port Monitor 分析のグラフおよびテーブルは、ホストごとのアクティビティおよびパフォーマンス データを表示します。 分析は、セッション データ、ボリューム統計、およびレスポンス時間について複数のビューを提供します。 また、トラブルシューティング用のワークフロー、データをエクスポートするための複数のオプション、およびフィルタ オプションを提供して、IT スタッフの問題診断および対応をサポートします。

Multi-Port Monitor にはその機能を監視するための機能があります。

- 論理ポートごとのハードウェア ベース フィルタおよびパケット キャプチャ オプション。
- パフォーマンスを測定し、対象データのみをキャプチャするハードウェア フィルタ。
- 1 つの Web ページから管理される複数のデータ フィード。
- SNMP トラップによる、データ監視またはキャプチャに影響する可能性があるエラーに関する自動通知送信。

Multi-Port Monitor には以下のコンポーネントが含まれます。

アプライアンス

スイッチに出入りするトラフィックを監視するハードウェアおよびソフトウェア。 以下の機能を実行します。

- パケットをキャプチャし、ストレージに書き込む。
- トラフィック統計を収集し、パフォーマンス情報用のパケットを分析する。
- 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に関する統計データを高パフォーマンス データベースに格納する。
- レポートと分析のために CA TIM または CA Application Delivery Analysis に統計データを送信する。

Web インターフェース

ブラウザからアクセス可能な管理インターフェース。以下を実行できます。

- ドライブ、CPU、およびキャプチャ カードのステータスを含むアプライアンス統計を表示する。
- ポート定義、フィルタ オプション、安全なユーザ アカウントなどのシステム設定を構成する。
- キャプチャされたパケットに基づいており、フォーマットされたグラフまたはテーブルに表示されたパフォーマンス データを表示、フィルタ、およびソートする。
- ローカルに格納されたセッション レベル データを［分析］タブ上で確認する。

第 2 章: Web インターフェースにログインする方法

Multi-Port Monitor システムの健全性の監視など、管理タスクを実行するために Web インターフェースにログインします。

以下の手順に従います。

1. Web ブラウザで Web インターフェースにアクセスします。 ブラウザの［アドレス］フィールドに以下の構文を使用します。

   `http://<ホスト名または IP アドレス>/`

   Multi-Port Monitor の［ログイン］ページが開きます。

2. 割り当て済みのユーザ名およびパスワード（大文字と小文字を区別します）を使用してログインします。デフォルト値は以下のとおりです。

   - ユーザ名： admin
   - パスワード： admin

   Web インターフェースが開きます。

詳細情報

管理者アカウントのパスワードの変更 (P. 12)

第 3 章: 推奨構成

Multi-Port Monitor は、最小限の設定で実行されるように設計されています。ただし、管理者は、ハードウェアおよび Multi-Port Monitor ソフトウェアのインストール後、システムの整理、保護、カスタマイズを実行できます。

注: インストール タスクは「CA Application Delivery Analysis Multi-Port Monitor インストール ガイド」で説明されています。

このセクションには、以下のトピックが含まれています。

信頼済みのインターネット サイトの設定

Web インターフェースのパフォーマンスを改善するには、信頼済みのインターネット サイトのリストにアプライアンスのホスト名を追加します。Microsoft Internet Explorer には、信頼済みサイトへのナビゲーションを制限する高いセキュリティ設定が使用されています。

Internet Explorer で信頼済みサイトのリストにホスト名を追加するには、［ツール］-［インターネット オプション］-［セキュリティ］をクリックします。

管理者アカウントのパスワードの変更

Multi-Port Monitor には、出荷時に別の製品権限を提供する事前定義済みユーザ アカウントが設定されています。 デフォルトの管理者アカウントは、すべての設定オプションにアクセスできます。 以下のような状況ではこのアカウントのパスワードを変更します。

- Multi-Port Monitor は CA Application Delivery Analysis の監視デバイスになるようスケジュールされているが、CA Application Delivery Analysis がまだ展開されていない場合。

  注: CA Application Delivery Analysis が展開された後、Multi-Port Monitor は CA Application Delivery Analysis から、パスワードを含むすべてのユーザおよび役割情報を取得します。

- Multi-Port Monitor が CA APM 環境の CA TIM でのみ展開される場合。

以下の手順に従います。

1. Web インターフェースの［環境管理］-［Users］をクリックします。

   ［User Accounts］ページが表示されます。

2. admin アカウントの［Edit］リンクをクリックします。

   ［Edit User］ページが表示されます。

3. （*オプション*）［Description］フィールドのデフォルト テキストを編集してデフォルト パスワードが変更されたことを示します。この手順はオプションですが、ベスト プラクティスです。

4. ［Password］および［Confirm Password］フィールドで暗号化テキストを削除し、新しいパスワードを入力します。

5. ［Enabled］チェック ボックスをオンにします。この設定により、Web インターフェースにログインするアカウントを誤って無効にするのを妨げます。

6. ［Save］をクリックします。

   新しいパスワードが保存されます。

詳細情報:

ユーザと役割の概要 (P. 35)

ポートを介したパケット フローの確認

ハードウェアとソフトウェアのインストールが成功したことを判断するために、ポートを経由するパケット フローを確認します。

以下の手順に従います。

1. Web インターフェースの［システム ステータス］をクリックします。
2. ［キャプチャ カード物理ポート ステータス］セクションで以下の情報を確認してください。
   - アダプタ上で接続されているポート。
   - 各ポートを介して受信されるパケットの数。

   ポートがアクティブな場合、設定は成功です。

VLAN 識別子の確認

CA Application Delivery Analysis が論理ポート上のタグ付けされた VLAN トラフィックをドメインに割り当てる場合、論理ポートにミラーリングされたトラフィックが正しくタグ付けされていることを確認することをお勧めします。 以下について確認します。

- VLAN トラフィックが両方向にタグ付けされている。

  1 分間のメトリックを正しく計算するには、論理ポートで、サーバおよびクライアントの両方の間のタグ付けされた VLAN トラフィックを受信する必要があります。 ［分析］ページでは、1 方向にのみタグ付けされたセッションの 1 分間メトリックはレポートされません。

  1 方向のみに VLAN タグがある場合：

  - TCP 通信の場合、［受信側］または［送信側］のいずれかの方向の 1 パケットを除いて、セッションがメトリックなしでリスト表示されます。
  - ［分析］ページでは、トラフィックは 2 つの個別の 1 方向セッションとしてレポートされます。

- VLAN トラフィックは、1 つの VLAN 識別子でタグ付けされます。

  Multi-Port Monitor は、パケット ヘッダ内の最初の VLAN 識別子によって VLAN トラフィックを識別します。トラフィックが複数の VLAN 識別子でタグ付けされている場合、VLAN 識別子の順序が変わると、Multi-Port Monitor はトラフィックを正しく監視できません。

論理ポートの設定

Multi-Port Monitor アプライアンスには、ネットワーク内のスイッチからデータを受信する物理ポートが 2 つ、4 つ、または 8 つあります。 ミラーリングされたポートへ接続されると、物理ポートには Multi-Port Monitor アダプタ上のその ID 番号に相当する論理ポート定義が割り当てられます。

論理ポートに名前を関連付けると、TIM に対する CA Application Delivery Analysis 内での監視フィードの特定がより容易になります。 デフォルトの論理ポート定義は変更できます。

CA CEM TIM は VLAN ベースの監視フィードをサポートしません。TIM に対して論理ポート上で VLAN トラフィックをドメインに割り当てないでください。

論理ポート設定により、各ミラー セッションからキャプチャされ監視されるデータの量を制限することもできます。 ポート フィルタにより、監視されるネットワークまたはホストのセグメントおよびキャプチャ ファイルに含めるか除外するデータのタイプが決まります。

CA Transaction Impact Monitor （CA TIM）は、Multi-Port Monitor アプライアンスで複数の論理ポートが利用できる場合でも、1 つの論理ポートからのミラー ポートを監視します。 複数の物理ポートを 1 つの論理ポートにマップするには、WAN からの Web トラフィックを論理ポートにミラーリングします。 このトラフィックは CA TIM および CA CA Application Delivery Analysis のために処理されます。 ほかのポート ミラーリングのために、理想的にはサーバに最も近いアクセス層スイッチからのほかの論理ポートを使用します。TIM 以外の論理ポートは、CA Application Delivery Analysis のみのために処理されます。

次の手順に従ってください:

1. Web インターフェースの［環境管理］-［Logical Ports］をクリックします。 ［Logical Ports］ページが表示されます。
2. ［Name］フィールドにポートの新しい名前を入力します。 名前は、コア スイッチの名前または場所のように、監視するトラフィックのソースを識別するのに役立ちます。
3. ［Enabled］を選択して、監視用のポートを有効にします。

4. （*オプション*）［Save Packets To Disk］を選択して、アプライアンスのハード ディスク ドライブにキャプチャされたデータ パケットを保存します。

   注: このオプションが無効な場合、パケットは以下のような影響を受けます。

   - パケット キャプチャ ファイルは保存されません。
   - パケット キャプチャ ファイルは、CA Application Delivery Analysis から起動されるパケット キャプチャ調査に利用できません。
   - パケット キャプチャ ファイルは［PCAP へエクスポート］機能に利用できません。

5. ［TIM］を選択して、CA TIM ポートとして設定しているポートを識別します。 CA TIM が Multi-Port Monitor アプライアンスにインストールされているときに限り、このチェック ボックスを使用できます。また、TIM へのパケットを無効にするか有効にするためにこのオプションを使用できます。

   注: このオプションが無効な場合、パケットは以下のような影響を受けます。

   - パケットは TIM には送信されません。
   - TIM 用の論理ポート フィルタ設定が保持されます。

6. ［Filters］をクリックして、設定しているポートのハードウェア フィルタを有効にします。詳細については、「ハードウェア フィルタを使用したデータ管理 (P. 16)」を参照してください。

   CA TIM によって監視される Web トラフィックは、完全なパケットを含む必要があります。

7. 論理ポートへ物理ポートを割り当てる（マップする）チェック ボックスを選択します。利用可能なポートの数は、購入したキャプチャ カード構成によって異なります。 1 つの論理ポートへ 2 つ以上の物理ポートをマップできます。 この設定により、非対称のルーティングが設定されている環境でより正確に監視し、プライマリとフェールオーバの回路を監視できます。

   論理ポートの番号は、0 から始まります。キャプチャ層では、論理ポートに物理ポートをマップします。マッピング処理は、CA TIM に対して透過的に行われます。

8. ［Save］をクリックします。
9. 設定する各ポートに対して手順 2 ～ 8 を繰り返します。
10. ［Name］フィールド以外のパラメータを変更した場合は、nqcapd プロセスを再起動 (P. 58) します。
11. （*オプション*）［システム ステータス］ページで［キャプチャ カード論理ポート ステータス］テーブルを表示して、論理ポートのステータスを確認します。

詳細:

キャプチャ カード論理ポート ステータス (P. 49)
パケット スライスの概要 (P. 17)
正規表現構文 (P. 81)

ハードウェア フィルタを使用したデータ管理

ハードウェア フィルタを使用すると、スイッチから処理されるデータをさらに改善できるので、Multi-Port Monitor パフォーマンスを最適化できます。 例 :

- データ ボリュームがネットワーク上で重い場合、選択した論理ポート定義にフィルタリングまたはパケット スライスを適用できます。
- 特定の IP アドレスまたはサブネットを選択することにより、データのキャプチャを改善できます。

フィルタ オプションには、プロトコル、VLAN、サブネットまたは IP アドレス、およびポートごとの優先順位とパケットの包含または排除が含まれます。 パケット スライス機能では、ディスクに書き込まれるパケットの部分またはサイズを制限できます。

Multi-Port Monitor のフィルタおよびパケット スライス オプションは、論理ポート定義の一部としてポート単位で適用されます。 フィルタ優先度を設定して、フィルタが適用される順序を決めることができます。

ハードウェア フィルタは、キャプチャされたデータに適用できる分析フィルタとは異なります。

- ハードウェア フィルタは、データの*キャプチャ*に影響します。
- 分析フィルタは、データの*表示*に影響します。

パケットが有効なフィルタの条件に一致すると、トラフィックがキャプチャされます。 手順がオーバラップするフィルタは、優先順位の設定に従って順番に適用されます。 キャプチャ カードは、限られた数のハードウェア フィルタ リソースを提供します。 これらのフィルタを使用して、ミラーリングされたトラフィックの制限を調整します。

ヒント： キャプチャされたデータを改善するためにハードウェア フィルタを使用できます。ただし、正しく設定されたミラー ポート（キャプチャする前にデータをフィルタする）の代わりにハードウェア フィルタを使用しないでください。

詳細情報:

ポート ミラーリング (P. 76)
論理ポートの設定 (P. 14)

パケット スライスの概要

Multi-Port Monitor フィルタには、フレームがキャプチャされるとその一部を選択的に破棄できるパケット スライス オプションが含まれます。

パケット スライスは通常、データ量が多く、対象のデータがパケット ヘッダ内にある場合に実行します。 パケット ペイロードは、CA Application Delivery Analysis 監視に通常必要とされません。パケット スライスにより、Multi-Port Monitor ロードが軽減され、キャプチャ ファイルの保存に使用されるリソースが削減されます。

「すべてのトラフィック -- ヘッダのみ」フィルタは、すべてのタイプのパケットをキャプチャし、スライスして、ヘッダのみを保持することを指定します。 フィルタは、ヘッダからのフレームのサイズに 1 バイトのペイロードを加えてパケットをスライスします。 ユーザがフィルタを追加しないか、このフィルタを編集しない場合、パケット スライスは新しいインストール中のすべての新しい論理ポート定義に適用されます。 このフィルタは、CA Application Delivery Analysis で監視するために必要なデータをすべてキャプチャする間に Multi-Port Monitor パフォーマンスを最大化します。

Multi-Port Monitor アプライアンスにインストールされるネットワーク アダプタは、固定長切り捨ておよび動的なプロトコルごとの切り捨てを含む、パケットのスライス用のオプションを提供します。 キャプチャ カードは次の 2 つのタイプのスライスを実行します。

固定スライス

フレーム サイズは、バイトで設定できる最大指定長に切り捨てられます。

動的スライス

ヘッダが含められた後にフレーム サイズは最大長に切り捨てられます (たとえば、完全な TCP ヘッダと 8 バイトのペイロード) 。ペイロード データが破棄される場所を計算するとき、カードはカプセル化または TCP オプションを考慮します。

デフォルト ハードウェア フィルタの概要

ハードウェア フィルタでは、論理ポートによって監視されるプロトコル、サーバおよびポートを指定します。 キャプチャ カードでは、指定する優先度に基づいて複数のハードウェア フィルタを適用します。 より詳細な精度でキャプチャを行うために、特定の IP アドレスまたは TCP ポートをフィルタできます。

複数のハードウェア フィルタが論理ポートに対して作成された場合、それらは論理和（OR）として扱われます。 いずれかのハードウェア フィルタによって指定された条件に一致すると、トラフィックがキャプチャされます。 フィルタの優先度は、フィルタが適用される順序を示します。 したがって、フィルタ内にオーバラップする条件がある場合、優先度を使用してスライスなどの他のオプションを判断することができます。

使用可能なシステム リソースを最大化するために、必要なトラフィックをフィルタすることをお勧めします。 ハードウェア フィルタを作成するか、CA Multi-Port Monitor で提供されるハードウェア フィルタを使用します。

すべてのトラフィック -- ヘッダのみ

すべてのプロトコルのヘッダ情報と 1 ペイロード バイトをキャプチャします。このフィルタはデフォルトで有効です。このフィルタは以下で使用します。

- CA Multi-Port Monitor 非 TCP トラフィックのボリューム メトリックが含まれます。
- CA Application Delivery Analysis パケット キャプチャ調査にはヘッダのみが含まれます。

HTTP -- **完全なパケット**

ポート 80 およびポート 443 の完全なペイロードを持つ HTTP パケットをキャプチャします。このフィルタはデフォルトで無効になっています。 このフィルタは以下で使用します。

- CA TIM
- CA Application Delivery Analysis Web アプリケーションのパケット キャプチャ調査には完全なパケットが含まれます。

TCP -- **ヘッダのみ**

TCP プロトコルのヘッダ情報と 1 ペイロード バイトがキャプチャされ、その他のすべてのプロトコルのパケットは破棄されます。 このフィルタはデフォルトで無効になっています。 このフィルタは以下で使用します。

- CA Multi-Port Monitor 非 TCP トラフィックのボリューム メトリックは含まれません。
- CA Application Delivery Analysis パケット キャプチャ調査にはヘッダのみが含まれます。

ハードウェア フィルタの設定

事前定義済みフィルタおよびユーザ作成フィルタを作成、有効化、無効化、および変更できます。 たとえば、フィルタの設定を保持したまま一時的にフィルタを無効にする場合は、フィルタを無効にします。

ハードウェア フィルタを設定する場合、［IP アドレス］などの単一フィールドにリスト表示される条件は、論理和（OR）として扱われます。 たとえば、IP アドレスのリストを指定する場合、パケット ソースまたは宛先のアドレスがリスト内のいずれかの IP アドレスに一致すれば、パケットはフィルタに一致することになります。

複数のフィールドが使用される場合、各フィールドに対して条件は論理積（AND）として扱われます。 たとえば、IP アドレスのリストとポート番号の両方を指定した場合、ソースまたは宛先のアドレスがリスト内の IP アドレスに一致し、さらにソースまたは宛先のポート番号が指定したポート番号に一致したら、パケットはフィルタに一致することになります。

ハードウェア フィルタの詳細表示リンクをクリックすると、別のフィールドを組み合わせるときに使用されるロジックを参照できます。 構文は、ハードウェア フィルタを指定するために Napatech によって必要とされる構文に従います。 たとえば、mIPSrcAddr、mIPDestAddr、mTCPSrcPort、mTCPDestPort などのキーワードは、パケットのフィールドを示すマクロです。

より精巧なフィルタを作成するには、［Advanced Hardware Filter］ページを使用できます。

次の手順に従ってください:

1. Web インターフェースの［環境管理］-［Logical Ports］をクリックします。 ［Logical Ports］ページが表示されます。
2. フィルタする論理ポートの［Edit Filters］列の［Filters］リンクをクリックします。 ［Logical Ports: Hardware Filters］ページが表示されます。

3. *フィルタを作成するには、［New］をクリックします。*［Logical Ports: New Hardware Filter］ページが表示されます。

   a. 以下のフィールドに入力します。

   - **Filter Enabled**。フィルタを適用するには、このオプションを選択します。フィルタを渡すパケットは以下のオプションに基づいて分析されます。

     ADA にパケットを送信します。 フィルタされたパケットは、ネットワーク レベル メトリックに対して分析され、Multi-Port Monitor Web インターフェースの［分析］タブで表示され、コンソールの設定に基づいて Application Delivery Analysis コンソールに送信されます。このオプションは常に選択されておりオフにできません。

     TIM にパケットを送信します。 フィルタされたパケットは、Multi-Port Monitor の CA APM Transaction Impact Manager （TIM）によってアプリケーション レベル メトリックおよびイベントに対して分析されます。このオプションを表示するために TIM をインストールする必要があります。

     Filter Name。作成または編集中のフィルタの名前。フィルタ名は、フィルタが適用される論理ポートの［Hardware Filters］ページに表示されます。

   - **Filter Priority**。 優先度によって、フィルタ条件がオーバラップするときに優先されるフィルタが決まります。 2 つ以上のオーバラップしているフィルタの優先度が同じである場合、その優先順位は定義されていません。 値は 0（最高の優先度）から 62（最低の優先度）です。 デフォルトの優先度は 10 です。

     フィルタ優先度の設定はパケット スライスと共に使用できます。 たとえば、各 HTTP パケットのバイトをより多く保持するとします。スライシングを「TCP ヘッダ + 50 バイト」に設定し、優先度を 1 に設定して、TCP および ポート 80 のフィルタを指定します。 その後、スライシングを「TCP ヘッダ + 1 バイト」に設定し、優先度を 10 に設定して、TCP の別のフィルタを指定します。このシナリオで、他の TCP トラフィックより多い HTTP トラフィックのペイロード バイトが保持されます。

- **Packet Slicing Mode**。 各パケットの選択した部分のみをキャプチャするオプション。 ハードウェア フィルタを使用すると、TCP/IP 以外のプロトコルのパケットをキャプチャできます。ただし、Multi-Port Monitor は、TCP トラフィックのみのパフォーマンス メトリックを収集します。 ボリューム メトリックはすべてのトラフィック タイプに対して収集されます。

  Capture full packet： フィルタを通過する各パケットからすべての情報がキャプチャされます。

  Capture fixed size： すべてのパケットから一部のバイトがキャプチャされます。 ［Packet Slicing Size］フィールドで、キャプチャするバイトの数を入力します。

  Capture headers plus size： すべてのレイヤ 2、レイヤ 3、およびレイヤ 4 ヘッダに加えて、［Packet Slicing Size］フィールドの固定数のペイロード バイトがキャプチャされます。 レイヤ 2 ヘッダには Ether II、LLC、SNAP、Raw ヘッダ、および VLAN、ISL、MPLS タグが含まれます。 レイヤ 3 ヘッダには IPv4 （IPv4 オプションを含む）および IPX ヘッダが含まれます。 レイヤ 4 ヘッダには TCP、UDP、および ICMP ヘッダが含まれます。

- **Include only Protocols**。 キャプチャして処理するプロトコルを制限します。選択したプロトコルのみが監視対象に含まれます。チェック ボックスを選択しないと、すべてのプロトコルが含まれます。 Transport Control Protocol （TCP）は CA Application Delivery Analysis が監視する主なプロトコルです。 User Datagram Protocol （UDP）は、リアルタイムまたはストリーミング アプリケーションが送信するデータの転送に使用されます。 Internet Control Message Protocol （ICMP）は、サーバ間のエラー メッセージングおよび CA Application Delivery Analysis のトレースルート調査に使用されます。

- **VLAN**。 監視するか監視から除外する仮想ローカル エリア ネットワーク（VLAN）の識別子。 トラフィックが指定された論理ポートを通過する VLAN の識別子をリスト表示します。 複数の VLAN はカンマ（スペースなし）で区切ります。 ［Exclude］を選択して、リスト表示した VLAN からのトラフィックを破棄します。

- **Subnets**。監視するか監視から除外するサブネット。有効な IPv4 アドレスおよびサブネット マスクを指定します。 ［Exclude］を選択して、リスト表示したサブネットからのトラフィックを破棄します。

  IPv4 アドレスには x.x.x.x/*n* の形式を使用します。x.x.x.x はドット付き表記の IPv4 サブネット アドレスで、*n* はマスクに使用するビットの数です。

- **IP Addresses**。 監視または監視から除外する個別ホストの IPv4 アドレスまたはアドレスの範囲。複数のアドレスはカンマを使用し、スペースなしで区切ります。範囲は、ハイフンを使用し、スペースなしで区切ります。 リストしたアドレスからのトラフィックを破棄するには、［Exclude］を選択します。

  IPv4 アドレスにはドット付き表記を使用します。 たとえば、10.9.7.7、または 10.9.8.5-10.9.8.7 などです。

- **Ports**。 監視するか監視から除外する TCP ポートまたはポート範囲。 複数のポート番号はカンマ（スペースなし）で区切ります。 ポートの範囲には次の形式を使用します： 2483-2484。 ［Exclude］を選択して、リスト表示したポートからのトラフィックを破棄します。

b. （*オプション*）より正確なフィルタを作成するために正規表現を使用する (P. 25)には［Advanced］をクリックします。

c. ［保存］をクリックします。 新規フィルタが［Logical Ports: Edit Hardware Filter］ページに表示されます。

4. *フィルタを変更または有効にするには*、［Edit］をクリックします。 ［Logical Ports: Edit Hardware Filter］ページが表示されます。

   a. 手順 3a の説明に従ってフィールドに入力します。

   b. （*オプション*）［Show Details］をクリックして、正規表現として選択内容を表示します。

   c. ［保存］をクリックします。新規フィルタが［Logical Ports: Hardware Filters］ページに表示されます。

5. 変更を適用するために nqcapd プロセスを再起動 (P. 58)します。

正確なフィルタリングのための正規表現の使用

ハードウェア フィルタには、キャプチャされるか破棄されるデータを正確に制御する正規表現を含めることができます。 フィルタの作成時に正規表現を適用できます。

次の手順に従ってください:

1. ハードウェア フィルタを作成します。
2. ［Logical Ports: New Hardware Filter］ページの［Advanced］をクリックします。［Logical Ports: New Advanced Hardware Filter］ページが表示されます。
3. 以下のフィールドに入力します。
   - **Filter Enabled**。 名前が示された論理ポートにフィルタが適用されます。 選択すると、nqcapd プロセスの再起動後にフィルタが適用されます。
   - **Filter Name**。作成または編集中のフィルタの名前。フィルタ名は、フィルタが適用される論理ポートの ［Hardware Filters］ページに表示されます。
   - **Filter Priority**。 優先度によって、フィルタ条件がオーバラップするときに優先されるフィルタが決まります。 2 つ以上のオーバラップしているフィルタの優先度が同じである場合、その優先順位は定義されていません。 値は 0（最高の優先度）から 62（最低の優先度）です。 デフォルトの優先度は 10 です。

     フィルタ優先度の設定はパケット スライスと共に使用できます。 たとえば、各 HTTP パケットのバイトをより多く保持するとします。 スライシングを「TCP ヘッダ + 50 バイト」に設定し、優先度を 1 に設定して、TCP および ポート 80 のフィルタを指定します。その後、スライシングを「TCP ヘッダ + 1 バイト」に設定し、優先度を 10 に設定して、TCP の別のフィルタを指定します。 このシナリオで、他の TCP トラフィックより多い HTTP トラフィックのペイロード バイトが保持されます。

- **Packet Slicing Mode**。各パケットの選択した部分のみをキャプチャするオプション。 ハードウェア フィルタを使用すると、TCP/IP 以外のプロトコルのパケットをキャプチャできます。 ただし、Multi-Port Monitor は、TCP トラフィックのみのパフォーマンス メトリックを収集します。 ボリューム メトリックはすべてのトラフィック タイプに対して収集されます。
  - Capture full packet： フィルタを通過する各パケットからすべての情報がキャプチャされます。
  - Capture fixed size： すべてのパケットから一部のバイトがキャプチャされます。 ［Packet Slicing Size］フィールドで、キャプチャするバイトの数を入力します。
  - Capture headers plus size： すべてのレイヤ 2、レイヤ 3、およびレイヤ 4 ヘッダに加えて、［Packet Slicing Size］フィールドの固定数のペイロード バイトがキャプチャされます。 レイヤ 2 ヘッダには Ether II、LLC、SNAP、Raw ヘッダ、および VLAN、ISL、MPLS タグが含まれます。 レイヤ 3 ヘッダには IPv4 （IPv4 オプションを含む）および IPX ヘッダが含まれます。 レイヤ 4 ヘッダには TCP、UDP、および ICMP ヘッダが含まれます。

4. ［Field］リストおよび空白のフィールドで、式を構築します。 フィルタ構文に*一致する*パケットがすべてキャプチャされます。 ワイルドカードは使用できません。

   a. 最初のリストから、フィルタするパケット ヘッダからフィールドを選択します。 デフォルトでは、フィルタにはトラフィックが*含まれます*。 フィルタが適用される論理ポートでトラフィックからそのデータに相当するアイテムを選択します。 トラフィックを*除外する*フィルタを作成するには、除外するトラフィック *を除く*すべてのトラフィックを指定します。

      - **VLAN ID**： データを含める仮想 LAN （VLAN）の識別子。 VLAN ID をカンマ区切りリストで空のフィールドに指定します。たとえば、VLAN 165 および 140 からのトラフィックを含めるには、「165,140」と入力します。 この論理ポートにフィルタリングを追加しなかった場合、これらの VLAN ID のいずれか一方のパケットがキャプチャされます。「140-165」のように VLAN の範囲を指定することもできます。そのようなフィルタは包括的であり、最初と最後の値も含まれます。

- **カプセル化**： パケットに適用されるカプセル化。 キャプチャ ファイルから含めるカプセル化のタイプの値を指定します。有効な値は以下のとおりです。

  VLAN: フィルタ操作で VLAN ヘッダを持つすべてのパケットを含むカテゴリ。

  MPLS： マルチプロトコル ラベル スイッチング ネットワーク アーキテクチャ。MPLS は、サービス品質および TTL 情報など、パケット ルーティングを制御するラベルを含むヘッダを各パケットに添付します。

  ISL： 高性能リンク用の Cisco 独自の VLAN カプセル方式。

- **Layer 3 Protocol**： フィルタ操作に含めるレイヤ 3 プロトコル。このオプションを選択する場合は、1 つのプロトコル、またはプロトコルのカンマ区切りリストを指定します。有効な値は IP および IPv4 です。

- **レイヤ 4 プロトコル**: フィルタ操作に含めるレイヤ 4 プロトコル。 1 つのプロトコル、または複数プロトコルのカンマ区切りリストを指定します。 有効な値は TCP、UDP、および ICMP です。

- **IPv4 Source Subnet**、**IPv4 Destination Subnet**： フィルタ操作に含めるサブネットの IP アドレス。 ［IPv4 Source Subnet］または［IPv4 Destination Subnet］を選択するか、あるいは［AND］または［OR］ボタンをクリックして正規表現に両方を追加します。フィルタはパケット ヘッダの［ソース］または［宛先］フィールドに適用されます。 IP アドレス、およびサブネット マスクのビット数を指定します。 以下の構文を使用します： 123.45.67.0/24。

- **IPv4 ソース IP アドレス**、**IPv4 宛先 IP アドレス**： フィルタ操作に含めるホストの完全な IPv4 アドレス。 フィルタはパケット ヘッダの［ソース］または［宛先］フィールドに適用されます。 1 つの IPv4 アドレス、カンマ区切りリスト、または範囲を入力できます。 標準的な構文を使用します（123.45.67.89、123.45.67.8,123.45.67.15、123.45.67.8-123.45.67.15 など）。

- **TCP Source Port**、**TCP Destination Port**： フィルタ操作に含める単一のポート番号、ポート番号のカンマ区切りリスト、またはポート番号をハイフンで結んだ範囲。 フィルタはパケット ヘッダの［ソース ポート］または［宛先ポート］フィールドに適用されます。

b. 2 番目のリストから条件（等しい（==）または等しくない（!=））を選択します。

c. 空白のフィールドに、手順 a の選択内容に関連付けられている値を入力します。

d. （*オプション*）フィルタに条件を追加するには、ブール演算子ボタン（［AND］または［OR］）のいずれかをクリックし、手順 a ～ d を繰り返します。

フィルタの構文が［Conditions］フィールドに表示されます。

5. ［Save］をクリックします。フィルタが［Logical Ports: Hardware Filters］ページに表示されます。

6. フィルタを有効にした場合は、nqcapd プロセスを再起動 (P. 58)します。

グローバル環境設定の設定

以下のような設定など、データが自動的に収集、保存、転送される方法に影響するグローバル設定を設定できます。

- パケット キャプチャ ファイルを保持する時間数。
- 自動データベース メンテナンスの頻度。
- パケット デデュプリケーションを有効にするかどうか。

ほとんどの場合、デフォルト設定で問題ありません。 ただし、システムが最適に機能するように設定を変更できます。

次の手順に従ってください:

1. Web インターフェースの［環境管理］-［Application Settings］をクリックします。 ［Application Settings］ページが開きます。

2. 以下のフィールドに入力します。

   - **Perform automatic file maintenance every**。 自動ファイル メンテナンス操作の間隔（分）。必要な場合、最も古い未処理パケット キャプチャ ファイルがメンテナンス中に削除されます。 この設定は、キャプチャ ファイル削除の頻度を決定します。 デフォルトは 5 です。 この設定を変更する場合は、nqmaintd プロセスを再起動します。 未処理のパケットを削除するしきい値は、ファイル削除の頻度にも影響します。

- **When disk space usage is normal, keep raw packet capture files for**。未処理パケット キャプチャ ファイルが自動的に削除されるまで保存される時間。 これらのファイルは、通常の監視中に継続的に生成されます。デフォルトは 6 です。この設定を変更する場合は、nqmaintd プロセスを再起動します。
- **Automatically remove raw packet capture files older than one hour when disk utilization reaches**。 1 時間より古い未処理パケット キャプチャ ファイルが自動的にパージされるまで使用できるディスク容量の最大パーセンテージ。 自動ファイル メンテナンスの間隔も、ファイル削除の頻度に影響します。デフォルトは 80 パーセントです。 このしきい値はパケット キャプチャ調査ファイルに適用されません。 この設定を変更する場合は、nqmaintd プロセスを再起動します。
- **Keep Application Delivery Analysis packet capture investigation files for**。パケット キャプチャ調査ファイルが自動的に削除されるまで保存される日数。 これらのファイルは CA Application Delivery Analysis からのパケット キャプチャ調査リクエストに応じて生成されます。 パケット キャプチャ調査ファイルは、未処理キャプチャ ファイルとは別々に保存されます。 このしきい値は、未処理パケット キャプチャ ファイルには適用されません。デフォルトは 90 です。 この設定を変更する場合は、nqmaintd プロセスを再起動します。
- **Keep one-minute session metrics for。** キャプチャされたパケットから取得されたメトリック データが Multi-Port Monitor データベースで保持される日数。 デフォルトは 7 です。 内部最大しきい値がこのデータベースに適用されます。 データベース内の行数が 120 億行を超えると、選択した日数より少ない日数のデータが保持されます。 しきい値を超過すると、最も古いデータがまず破棄されます。
- **Perform packet deduplication**。 有効にすると、Multi-Port Monitor はミラーリングされたポートから受信できる重複したパケットを除外しようとします。 デフォルトでデデュプリケーションは有効です。 ［システム ステータス］ページでは、キャプチャ カードが破棄したパケットの数が追跡されます。この設定を変更する場合は、nqcapd プロセスを再起動します。

- **Encrypt raw packet capture files on disk**。 有効にすると、未処理パケット キャプチャ ファイルは Multi-Port Monitor ハード ディスクに暗号化された形式で保存されます。 デフォルトでは、これらのファイルには、キャプチャされたすべてのトラフィックのヘッダ情報のみが含まれます。 しかし、保持するパケットを増やすようにパケット スライス オプションを変更すると、ペイロード データを含めることができます。 パケット キャプチャ調査ファイル（単一のサーバからの情報を含むようにフィルタされる）は暗号化されません。 暗号化はプロセッサ負荷の高い処理です。 このオプションを有効にすると、監視デバイスがパケット キャプチャ ファイルを保存する機能が低下する場合があります。 Multi-Port Monitor を初めて起動するときに、暗号化用の一意のキーが作成されます。 キーはその後変更されません。 この設定を変更する場合は、nqcapd プロセスを再起動します。

3. ［Save］をクリックします。［Application Settings］ページが変更によって更新されます。
4. 必要に応じて、nqmaintd プロセスまたは nqcapd プロセスを再起動 (P. 58)します。

詳細情報:

パケット デデュプリケーション (P. 77)
キャプチャ カード物理ポート統計情報 (P. 50)
プロセスの停止または再起動 (P. 58)
パケット スライスの概要 (P. 17)
データベースからのデータのパージ (P. 62)

SNMP トラップの作成

SNMP アラート機能は、CA Application Delivery Analysis インシデント機能にエラー レポートのレイヤを追加します。 SNMP アラートを使用して、Multi-Port Monitor はいくつかの自己監視タスクを実行し、トラップ通知を送信して、パフォーマンスに影響を及ぼすことがある条件を警告します。

nqsnmptrap_[日付].log ファイルは、SNMP トラップのトリガになった条件を識別します。 詳細については、「システム ログの確認 (P. 58)」を参照してください。

エラー状態が検出されると、SNMP トラップがサードパーティ監視アプリケーションに自動的に送信されます。 SNMP トラップ設定を変更してトラップが送信される理由を変更できます。 トラップは管理情報ベース（MIB）で定義され、SNMP v2 通知として送信されます。

Multi-Port Monitor には、一意の OID が含まれる MIB ファイルがあります（CA-MULTI-PORT-MONITOR-MIB）。 Web インターフェースの［環境管理］-［SNMP Traps］を選択すると、MIB ファイルの内容を確認できます。

前提条件

- Multi-Port Monitor と通信するトラップ受信者を設定します。
- トラップ受信者に CA-MULTI-PORT-MONITOR-MIB をインポートします。 MIB ファイルをインポートするプロセスはトラップ受信者に固有です。

次の手順に従ってください:

1. Web インターフェースの［環境管理］-［SNMP Traps］をクリックします。

   ［SNMP Traps］ページが表示されます。

2. SNMP トラップ受信者がインストールされているコンピュータの IP アドレスまたはホスト名を入力します。
3. ［Save］をクリックします。

   デフォルトでは、テーブルで表示されるトラップはすべて有効で、警告の重大度レベルが表示されます。 この設定は、デフォルトでは情報トラップが送信されないことを示します。 ただし、トラップは、警告条件またはエラー条件のいずれかを満たす条件に応じて送信されます。

詳細情報:

システム ログの確認 (P. 58)

SNMP トラップの重大度レベル

Multi-Port Monitor の SNMP トラップは、パフォーマンスに影響するエラー状態を検出する主要プロセスと関連付けられます。 以下の重大度に相当するエラー状態が各トラップのトリガになります。

- 情報（重大度が最も低い状態）
- 警告（重大度が中程度の状態）
- エラー（重大度が最も高い状態）

Multi-Port Monitor が送信するトラップの最小限の重大度を選択できます。トラップは、最小限の重大度の条件を満たすか超えるあらゆる状態に対して送信されます。 デフォルトでは、すべてのトラップは、情報の重大度ではなく、警告またはエラーの重大度に有効です。

以下の SNMP トラップが使用可能です。

mtpProcessTrap

Multi-Port Monitor プロセスが失敗するか再起動されると、このトラップが送信されます。トラップ テキストには再起動されたプロセスの名前が示されます。 トラップはデフォルトで以下の状態に対して送信されます。

- 監視プロセスが別のプロセスを再起動すると、警告が送信されます。
- 監視プロセスが同じプロセスを最大回数再起動すると、エラーが送信されます。

mtpCaptureTrap

このトラップは、ネットワーク アダプタ（キャプチャ カード）からのエラーまたは警告メッセージに応じて送信されます。 該当する場合、トラップ テキストに影響を受けたアダプタを識別するための情報が示されます。

- 物理ポートが接続されなくなると、警告が送信されます。
- nqcapd プロセスでパケットをキャプチャする間に問題が発生すると、エラーが送信されます。

mtpDiskUsageTrap

ファイル システムのディスク使用率のしきい値を超えると、このトラップが送信されます。

- ディスク使用率が 80% に到達すると、警告が送信されます。
- ディスク使用率が 95% に到達すると、エラーが送信されます。

ヒント：

- mtpDiskUsageTrap は、/nqtmp/headers ファイル システム（RAM ディスク ファイル システム）を監視します。 nqmetricd プロセスが十分にヘッダ ファイルを処理していないと、/nqtmp/headers ファイル システムはしきい値を超えます。 以下のような理由が考えられます。
  - nqmetricd プロセスが CA Application Delivery Analysis 管理コンソールに設定情報を照会できません。SQL エラーの兆候がないか nqMetricReader.log ファイルを確認します。
  - Multi-Port Monitor アプライアンスに、nqmetricd プロセスに影響するリソース問題が発生している可能性があります。アプライアンスを再起動します。問題が解決しない場合または再度発生する場合は、CA テクニカル サポートにお問い合わせください。
- mtpDiskUsageTrap は、/nqtmp/tim ファイル システム（RAM ディスク ファイル システム）も監視します。 TIM プロセスが十分にパケット ファイルを処理していないと、/nqtmp/tim ファイル システムはしきい値を超えます。

mtpRAIDTrap

このトラップは、RAID アレイまたはディスク ドライブの障害に応じて送信されます。

- 再構築していた RAID アレイが最適な状態に戻ると、情報が送信されます。
- ディスク ドライブが再構築しているのでディスクの RAID アレイが劣化すると、警告が送信されます。
- ディスク ドライブの障害によってディスクの RAID アレイに障害または劣化が検出されると、エラーが送信されます。

注: Adaptec Storage Manager（arcconf）ユーティリティがインストールされている場合にのみ、このトラップは利用可能です。 詳細については、「CA ADA Multi-Port Monitor インストール ガイド」を参照してください。

詳細情報:

プロセス情報 (P. 46)
アプライアンスへのログイン (P. 64)
システム ログの確認 (P. 58)

トラップ動作の変更

トラップの各タイプの重大度を変更できます。mtpDiskUsageTrap については、使用率のしきい値を変更することもできます。 トラップの各タイプにはいくつかの重大度パラメータが含まれます。 トラップ通知のトリガになる最小限の重大度レベルを選択できます。 重大度レベルは、重大度が最も低い情報から、重大度が最も高いエラーまであります。

次の手順に従ってください:

1. Web インターフェースの［環境管理］-［SNMP Traps］をクリックします。

   ［SNMP Traps］ページには、設定されたトラップ受信者の IP アドレスまたはホスト名および SNMP トラップを説明するテーブルが表示されます。

2. 無効化または変更するトラップの［Edit］をクリックします。

   ［Edit SNMP Trap Settings］ページが表示されます。

3. ［Setting］フィールドでトラップの重大度レベルを選択します。

4. ［Send Warning trap when disk utilization reaches］フィールドの値を変更します。 デフォルトは 80 です。

   注: このフィールドは mtpDiskUsageTrap に適用されます。

5. ［Send Error trap when disk utilization reaches］フィールドの値を変更します。 デフォルトは 95 です。

   注: このフィールドは mtpDiskUsageTrap に適用されます。

6. ［保存］をクリックします。

   ［SNMP Traps］ページが表示されます。 トラップ設定の変更内容がテーブルに表示されます。

ユーザと役割の概要

Multi-Port Monitor を CA Application Delivery Analysis の監視デバイスとして設定する前は、admin と user という 2 つのデフォルト ユーザ アカウントを使用できます。

Multi-Port Monitor を監視デバイスとして設定した後は、Multi-Port Monitor は CA Application Delivery Analysis からユーザおよび役割に関する情報を取得します。 CA Application Delivery Analysis 管理者は、CA Application Delivery Analysis および Multi-Port Monitor に対して有効な安全なユーザ アカウントを作成し、管理します。 これらのアカウントにより、オペレータは［システム ステータス］ページ、［分析］ページ、［システム セットアップ］ページ、［環境管理］ページにアクセスできます。 また、これらのアカウントは同期され、Web インターフェースの［User Accounts］ページに表示されます。

重要: Multi-Port Monitor は、CA TIM または CA APM からユーザおよび役割に関する情報を取得しません。 CA TIM がアプライアンスにインストールされ、かつアプライアンスが CA Application Delivery Analysis の監視デバイスでない場合は、適用できるのはデフォルト ユーザ アカウントのみです。

Multi-Port Monitor セキュリティは、CA Application Delivery Analysis と完全に互換性があり、ログイン アクセス権限に基づいています。

- ユーザの権限、および少なくとも 1 つの役割権限を持つユーザは、［システム ステータス］タブでそのデータを表示できます。ユーザ製品権限を持ち、役割権限を持たないユーザは［システム ステータス］ページへのアクセスが拒否されます。
- CA Application Delivery Analysis 管理者権限を持つユーザは、Multi-Port Monitor の［環境管理］タブにアクセスできます。

ユーザ アカウント役割に関連付けられた権限によってさらにアクセスが決定されます。

- CA Application Delivery Analysis エンジニアリング役割を持つユーザは、［分析］ページを表示できます。
- CA Application Delivery Analysis 調査役割を持つユーザは、［分析］ページを表示でき、［PCAP へエクスポート］機能を使用できます。

CA Application Delivery Analysis 管理者は、Multi-Port Monitor ステータスを追跡してデータ監視を設定するために追加のユーザ アカウントを作成できます。 セキュリティを強化するために、管理者とユーザ アカウントのデフォルト パスワードを変更します。

詳細情報:

管理者アカウントのパスワードの変更 (P. 12)

ユーザ アカウント情報

Multi-Port Monitor は別の製品権限および別の役割をデフォルト ユーザ アカウントに提供します。 デフォルト アカウントの製品権限では、Web インターフェースへの異なる 2 つのレベルのアクセス権が許可されます。

ユーザ権限レベル

［システム ステータス］および［分析］ページへの表示のみのアクセス権。

管理者権限レベル

すべての製品機能へのアクセス権。

各ユーザ アカウントに割り当てられる役割により、ユーザがアクセスできる Web ページおよび製品機能が決定されます。

Multi-Port Monitor が CA Application Delivery Analysis の監視デバイスである場合、管理者は管理コンソールまたは CA Performance Center でアカウントを作成および変更できます。 これらのアカウントは同期され、Multi-Port Monitor Web インターフェース上に表示されます。 ［環境管理］-［Users］を選択すると、ユーザ アカウントに関する詳細を表示できます。

Name

このアカウントのユーザ名およびログイン ID。ユーザ アカウントを識別します。 デフォルト アカウントの製品権限レベルを識別します。

Role

ユーザの製品機能へのアクセスのレベルを決定します。

Privilege

製品設定へのアクセスのレベル (管理者またはユーザのいずれか)。管理者権限を持つユーザのみが、キャプチャ フィルタの設定、データベース保存設定の変更など、製品設定を変更できます。

Status

ユーザ アカウントのステータス（有効または無効のいずれか）。

Time Zone

ユーザ アカウントを最もよく使用しているオペレータのローカル タイム ゾーン。

ユーザ アカウントのプロパティの変更

ユーザ アカウントにより、Multi-Port Monitor を操作し、特定のタスクを実行する権限があるユーザの認証情報が設定されます。 デフォルト ユーザ アカウント（admin と user）に関する情報は、Web インターフェースの［User Accounts］ページで表示できます。

ただし、Multi-Port Monitor を CA Application Delivery Analysis 用の監視デバイスとして追加するまでは、Web インターフェースを使用してデフォルト ユーザ アカウントを変更できます。 たとえば、アカウント パスワードの変更、関連するタイム ゾーンの更新、別の役割の割り当てを実行できます。

注: Multi-Port Monitor を監視デバイスとして追加して同期すると、これらのアカウント設定は CA Application Delivery Analysis の設定で更新されます。監視デバイスとして Multi-Port Monitor を追加した後、CA Application Delivery Analysis 管理コンソールまたは CA Performance Center を使用してユーザ アカウントを作成および変更します。

次の手順に従ってください:

1. Web インターフェースの［環境管理］-［Users］をクリックします。

   ［User Accounts］ページには、事前定義済みユーザ アカウントおよび作成したカスタム アカウントが表示されます。

2. 編集するアカウントの［Edit］リンクをクリックします。

   ［Edit User］ページが表示されます。

3. 以下のフィールドに入力します。

   - **Description**。アカウントまたは最近の変更について説明します。たとえば、パスワードが変更されたことを示すことができます。 このオプションの手順がベスト プラクティスです。
   - **Password**、**Confirm Password**。 各フィールドの暗号文を削除し、各フィールドに新しいパスワードを入力します。
   - **Product Privilege**。 ユーザが管理タスクを実行できるかどうかを決定する権限レベルを選択します。
   - **Role**。 レポート データを表示し、製品機能にアクセスする必要がある権限を決定する役割を選択します。
   - **Time Zone**。このユーザ アカウントを最もよく使用するオペレータのローカル タイム ゾーンを選択します。
   - **Enabled**。Web インターフェースにログインするアカウントを誤って無効にするのを防ぐには、このチェック ボックスを選択します。admin アカウントを無効にするには、管理者の製品権限を持つ別のユーザを作成し、そのユーザでログインします。その後、admin アカウントを無効にできます。

4. ［Save］をクリックします。

役割情報

役割は、製品メニューおよびデータ ソースへのアクセスを制御します。製品機能へのユーザ アクセスを制限するために役割を割り当てます。 たとえば、Multi-Port Monitor の［システム ステータス］ページへのユーザ アクセスを制限します。 役割がユーザのアクセスを制限する場合、ユーザは製品の制限された部分を表示できません。

ユーザ アカウントと関連付けられる役割によって以下の制限が決定されます。

- ユーザがアクセスできるメニューおよびレポート ページ。
- ユーザがデータをカスタマイズし、詳細情報を得るためにドリル ダウンできるかどうか。

CA Application Delivery Analysis では、各役割には CA Application Delivery Analysis レポートおよびオンデマンド調査などのその他の機能へのページ レベル アクセスを決定する［領域アクセス］パラメータがあります。 CA Application Delivery Analysis データ ソースが登録された後、同じ役割が CA Performance Center 内でも動作します。

役割が制御する権限は環境管理には拡張されません。 ユーザ アカウントが作成される場合、管理者権限はユーザに割り当てられます。

Multi-Port Monitor の［Roles］ページは、事前定義済み役割名および説明の読み取り専用リストです。

IT マネージャ

Multi-Port Monitor および CA Application Delivery Analysis のこの管理者役割は、以下の CA Application Delivery Analysis レポートにアクセスできます。

- 調査
- エンジニアリング
- 操作
- インシデント
- 管理

IT エンジニア

この役割：

- レポートされた問題のトラブルシューティングを行うためのユーザ権限で構成され、以下の CA Application Delivery Analysis レポートへのアクセスが提供されます。
  - 調査
  - エンジニアリング
  - 操作
  - インシデント
  - 管理
- ［データ ソースへのドリル イン］役割権限を付与します。 この役割権限を使用して、ユーザは Performance Center から CA Application Delivery Analysis 管理コンソールなどのデータ ソース、および CA Application Delivery Analysis 管理コンソールから Multi-Port Monitor にドリル インできます。

  重要: Multi-Port Monitor では CA Performance Center からの権限セットは適用されません。 たとえば、特定のサーバ グループがユーザに割り当てられる場合、Multi-Port Monitor ではそのドメインのすべてのサーバのパフォーマンス データが表示されます。

IT オペレータ

この役割：

- レポートされた問題のトラブルシューティングを行うためのユーザ権限で構成され、以下の CA Application Delivery Analysis レポートへのアクセスが提供されます。
  - エンジニアリング
  - 操作
  - インシデント
  - 管理
- ［データ ソースへのドリル イン］役割権限は付与されませんが、この役割は CA Application Delivery Analysis 管理コンソールへのユーザのログイン、管理コンソールから Multi-Port Monitor へのドリル インは妨げません。

  重要: Multi-Port Monitor では CA Performance Center からの権限セットは適用されません。 たとえば、特定のサーバ グループがユーザに割り当てられる場合、Multi-Port Monitor ではそのドメインのすべてのサーバのパフォーマンス データが表示されます。

製品権限

*製品権限*は、管理機能へのアクセスを付与するか制限するユーザ アカウントの一部です。

製品権限の各レベルは事前定義済み役割に相当します。 CA Application Delivery Analysis 管理者は、ユーザ アカウントに異なる役割および権限を割り当てることができ、役割をカスタマイズして異なる製品領域へのアクセスを付与できます。

パワー ユーザ権限は Multi-Port Monitor には存在しません。 ただし、CA Application Delivery Analysis エンジニアリング製品領域へのアクセス権を持つパワー ユーザは、［環境管理］ページの機能以外のすべての Multi-Port Monitor 機能にアクセスできます。

CA Performance Center は CA Application Delivery Analysis および Multi-Port Monitor で使用される製品権限をサポートしていますが、その製品権限は異なるレベルで動作します。製品権限を使用すると、1 つのユーザ アカウントで、別の CA データ ソース製品への異なるレベルのアクセスが可能になります。たとえば、CA Performance Center 内の選択されたアイテムを表示できる CA Application Delivery Analysis のユーザにすることができます。CA Performance Center ビューからナビゲートすると、この同じユーザを CA Application Delivery Analysis の特定のインスタンスの管理者にすることもできます。

すべての Multi-Port Monitor オペレータには、［システム ステータス］ページへのアクセス権があります。 ただし、ユーザ権限では、［システム ステータス］ページにアクセスするために少なくとも 1 つの役割権限が付与されることが必要です。

管理者の製品権限は、オペレータが［環境管理］ページにアクセスするのに必要です。 ただし、ユーザ アカウントの役割によって分析領域へのアクセスが決定されます。 また、PCAP 形式に分析をエクスポートする機能は、2 つ目の［領域アクセス］パラメータにさらに制限されます。

Multi-Port Monitor の［分析］ページへのアクセス権は CA Application Delivery Analysis［エンジニアリング］タブへのアクセス権と関連付けられています。ユーザ アカウントの役割の［領域アクセス］パラメータによって、このアクセス権が決定されます。 しかし、このアクセス権でも、調査領域へのアクセスを必要とする PCAP ファイルのエクスポートをユーザに許可するのには十分ではありません。

CA Performance Center では、製品権限設定がデータ ソース レベルでの役割設定とオーバーラップします。 以下のタスクを実行するには、ユーザはデータ ソースのアクセス権限および少なくともユーザの製品権限が必要です。

- レポートの表示。
- ビューのドリル イン。
- CA Performance Center からそのデータ ソースへの移動。

CA Performance Center で適用される権限および役割によって決定されるアクセス権は、Multi-Port Monitor Web インターフェースに保存されます。

以下のリストでは、CA Application Delivery Analysis および Multi-Port Monitor で利用可能な製品権限のタイプの概要を示し、デフォルトのアクセス領域について説明します。

管理者レベル

このレベルは、通常 IT マネージャ役割と関連付けられ、以下の機能にアクセスできます。

- ［分析］ページ
- ［システム ステータス］ページ
- ［環境管理］ページ
- PCAP への分析のエクスポート機能

パワー ユーザまたは調査者レベル

Multi-Port Monitor では、事前定義済みパワー ユーザ アカウントは利用できません。このレベルは、ネットワーク エンジニア役割のデフォルト値で、以下の機能にアクセスできます。

- ［分析］ページ
- ［システム ステータス］ページ
- PCAP への分析のエクスポート機能

ユーザ レベル

このレベルは、IT オペレータ役割のデフォルト値で、以下の機能にアクセスできます。

- ［分析］ページ
- ［システム ステータス］ページ

デフォルトの IT オペレータ役割では、関連付けられたユーザは機密データが含まれる可能性のあるデータを PCAP 形式にエクスポートできません。この役割を持つユーザに必要な領域へのアクセスを付与するために、CA Application Delivery Analysis 管理者は IT オペレータ役割に調査領域を追加できます。

第 4 章: システム ヘルスおよびメンテナンス

Multi-Port Monitor は、システムをピーク レベルで実行し続けるためにそれ自体を監視します。 さらに、管理者は以下のタスクを実行できます。

- システム ステータスの表示
- システム メンテナンス オプションのカスタマイズ
- プロセスの停止または再起動
- ソフトウェアのアップグレードのアプライアンスへの適用
- トラブルシューティング目的でのシステム ログの表示

このセクションには、以下のトピックが含まれています。

システム ステータス (P. 45)
メンテナンス タスク (P. 56)
システム セットアップ (P. 65)
マシン設定 (P. 66)

システム ステータス

［システム ステータス］ページには、以下のメトリックを含むすべてのアクティブな Multi-Port Monitor プロセスのステータスが表示されます。

- キャプチャ カードおよびディスクのパフォーマンス
- ファイル システム ステータス
- メモリおよび CPU 使用率

［システム ステータス］ページには、ユーザと管理者の両方がアクセスできます。

システム情報

［システム情報］セクションでは、Multi-Port Monitor アプライアンスに関する詳細情報が提供されます。

ホスト名 (IP アドレス)

アプライアンスの DNS ホスト名および IPv4 アドレス。

CA Application Delivery Analysis マネージャ

CA Application Delivery Analysis 管理コンソールの IPv4 アドレスと、CA Application Delivery Analysis ログイン ページへのリンク。

この情報は、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使用できます。

Multi-Port Monitor バージョン

ソフトウェアのバージョンおよびビルド番号。

プロセス情報

Multi-Port Monitor は、パケットのキャプチャ、メトリックの計算、パケットの検査、自動システム メンテナンスを実行する複数のプロセスまたはデーモンで構成されています。 ［プロセス情報］セクションでは、以下のプロセスの頻繁に更新されるステータス情報が提供されます。

nqcapd

パケット キャプチャ デーモン。 そのログ ファイル名は nqnapacapd.log です。

ヒント： ポート統計情報をリセットするには、nqcapd プロセスを再起動します。

nqmetricd

メトリック計算エンジンは、CA Application Delivery Analysis Single-Port Monitor 上の Metric Compute Module とほぼ同等です。そのログ ファイル名は nqMetricReader.log です。

nqinspectoragentd

インスペクタ デーモンは、Single-Port Monitor 上の SA Monitor サービスとほぼ同等です。 そのログ ファイル名は nqInspectorAgentd.log です。

nqwatchdog

監視プロセスは、他のプロセスのステータスを監視し、必要に応じてそれらのプロセスを再起動します。 そのログ ファイル名は nqwatchdog.log です。

nqmaintd

システム メンテナンス デーモン。そのログ ファイル名は nqmaintd.log です。

sadatatransfermanager

Data Transfer Manager プロセスは、Cisco Wide-Area Application Services 展開からデータを受信および転送します。 Multi-Port Monitor が CA Application Delivery Analysis 監視デバイスとして設定されていない場合、このプロセスのステータスは［停止］になります。 監視デバイスを設定すると、このプロセスは使用されていない場合でも常に実行中になります。 そのログ ファイル名は saDataTransferManager.log です。

ヒント： これらのプロセスのステータスは、［環境管理］-［Processes］にある［Process Status］ページでも表示できます。

詳細情報:

プロセスの停止または再起動 (P. 58)

データベース ステータス

［データベース ステータス］セクションでは、Multi-Port Monitor アプライアンス上の高パフォーマンス データベースのステータスを示します。このセクションでは、ローカル データベースの名前および以下のいずれかのステータス レベルが示されます。

- 稼働中
- ダウン
- シャットダウン中
- 初期化中

タイム スタンプは、ステータスの更新された時間を示します。

詳細:

データベース ステータスおよび使用状況 (P. 60)

キャプチャ カード物理ポート ステータス

［キャプチャ カード物理ポート ステータス］セクションでは、各ポートを通して流れるトラフィックに関する情報が提供されると共に、各リンクの説明が表示されます。ほとんどの値は動的に更新され、ブラウザは 5 秒ごとに更新されます。

物理ポート

Multi-Port Monitor アプライアンス上の物理ポート。

タイプ

接続に使用されているケーブルのタイプ。

リンク状態

このポートへのリンクが接続されるかどうか。

リンク品質

ネットワーク アダプタからの情報に基づいた、この接続の品質。リンクがダウンしているかどうかを示します。

リンク速度

このリンクの通常の速度。

詳細情報:

キャプチャ カードのクロックがシステム クロックと異なる (P. 72)

キャプチャ カード論理ポート ステータス

［キャプチャ カード論理ポート ステータス］セクションでは、各論理ポートのステータスと、処理されたパケット数およびドロップされたパケット数が提供されます。以下のような理由で、1 つの論理ポート定義に複数の物理ポート（またはデータ フィード）を割り当てることができます。

- プライマリ回線およびフェールオーバ回線に関するレポートを構成するため。
- 非対称のルーティング環境でより正確な監視を行うため。

論理ポート

［論理ポート］ページで定義された論理ポート。キャプチャ カード上の各物理ポートは、論理ポート定義に関連付けられます。この関連付けは、データ フィードの識別に役立つだけでなく、データの各ソースを集約してまとめて監視できるようになります。論理ポート定義には、ポート番号、名前、およびキャプチャされるトラフィックを決定するために使用できるハードウェア フィルタ設定が含まれます。

論理名

論理ポート名。ポートに名前を割り当てない場合は、ポート 0、ポート 1 などのデフォルト値が使用されます。

状態

このポートへのリンクのステータス（［有効］または［無効］）。

ステータス

現在のポート ステータス（［実行中］、［停止］、または［エラー］）。ステータスが［エラー］である場合は、マウス ポインタをエラー アイコンの上に置くとエラーの原因が表示されます。

処理されたパケット

ハードウェア フィルタが適用された後、キャプチャ カードで配信されるパケットの総数を示します。nqcapd プロセスが起動または再起動されると、この統計はリセットされます。

ドロップ数

キャプチャ カードがドロップし、処理しなかった、この論理ポートから受信したパケットの数。ドロップの数は、キャプチャ カードの負荷を示します。正常なパフォーマンス条件では、ドロップの数はゼロになります。

詳細:

論理ポートの設定 (P. 14)

キャプチャ カード物理ポート統計情報

［キャプチャ カード物理ポート統計情報］セクションでは、Multi-Port Monitor アプライアンス上の各物理ポートを通して流れるデータ量に関する情報が提供されます。 統計はハードウェア フィルタが適用される前に計算されます。そのため、この統計はスイッチから受信される実際の回線速度を示します。

このセクションではまた、現在のエラーの数も識別されます。 これらの情報を使用すると、ミラー ポートの設定を検証して、ミラーリングされたセッションが過負荷になっていないことを確認できます。

nqcapd プロセスが起動または再起動されると、これらの統計はゼロにリセットされます。

物理ポート

データが Multi-Port Monitor に流れるときの物理ポート。［すべて］（すべてのチャネルの合計）か、または物理ポートの識別子のどちらかです。物理ポートの数は、使用されているキャプチャ カードのタイプによって異なります。

論理名

この物理ポートに関連付けられた論理ポートの名前。

受信パケット数

統計がリセットされた後に受信された個別パケットの総数。

Bytes Received

統計がリセットされた後に受信されたバイト数。

CRC/アライメント エラー数

巡回冗長検査（CRC）エラーまたはアライメント エラーを含むフレーム数。

破棄された複製

すでに受信されたパケットの重複であったために、キャプチャ カードが、そのデデュプリケーション ロジックに従って破棄したパケットの数。 自動デデュプリケーションは、［Application Settings］ページで有効または無効にすることができます。

この値はミラー ポートが適切に設定されているかどうかを示します。キャプチャされたトラフィックの大きな割合が重複したパケットで構成されている場合は、ポート ミラーリングの設定を確認してください。

受信レート

このチャネルを通して 1 秒あたりに受信されたパケットの数。

詳細:

グローバル環境設定の設定 (P. 28)
プロセスの停止または再起動 (P. 58)

RAID ステータス情報

［RAID］セクションでは、Multi-Port Monitor アプライアンス上の RAID アレイからのディスク パフォーマンスに関する情報が提供されます。

注: RAID 情報は、Adaptec Storage Manager（arcconf）ユーティリティがインストールされている場合にのみ使用できます。 詳細については、「CADA Multi-Port Monitor インストール ガイド」を参照してください。

アレイ

RAID アレイの識別子。 この情報がシステム アレイまたはデータ アレイに適用されるかどうかを示します。

ステータス

アレイのステータス

- 最適： 最も高いレベルで実行中
- 低下： 最も高いレベルでは実行されていない

- 失敗： 実行されていない。エラー状態を示します。 影響を受けるドライブのエラー タイプと ID およびシリアル番号が示されます。
- 再構築中： オンラインに戻しています。 再構築中のドライブを RAID コントローラが検出すると、このステータスは［最適］に変更されます。 その間、アレイは引き続き［低下］状態で実行されます。 メトリックはすべて、引き続き収集されます。

注: データ アレイがドライブの［失敗］ステータスを示す場合でもメトリック処理は中断されませんが、パケット キャプチャ調査は実行できません。 メトリック処理を中断することなく、障害が発生したドライブを変更できます。

タイプ

RAID アレイのタイプ。

- CA6000 Multi-Port Monitor RAID アレイは、RAID 5 として設定されます。
- CA6300 RAID アレイ：
  - システム アレイ： RAID 1
  - データ アレイ： RAID 6

ドライブ数

アレイが制御するディスク ドライブの数。

失敗ドライブ

障害が発生したドライブ、エラーを示すドライブ、または再構築中のドライブの表示。 ドライブ番号、ID 番号、およびシリアル番号が含まれます。 システム アレイ ドライブの ID 番号は 1 ～ 4 です。 データ アレイ ドライブの ID 番号は 5 ～ 16 です。

ファイル システム

［ファイル システム］セクションでは、Multi-Port Monitor アプライアンス上のファイル システムの使用統計が提供されます。

ファイル システム

統計が表示されているファイル システムの名前。

サイズ

このファイル システムの総容量（バイト数）。

使用済み

このファイル システム内の使用中のバイト数。

使用可

このファイル システム内の空いていて使用できるバイト数。

使用 %

使用中のファイル システム容量のパーセンテージ。

マウント

オペレーティング システム ディレクトリ内のファイル システムのマウント ポイント。

メモリ

［メモリ］セクションでは、メモリ サイズ、使用中のバイト数と空きバイト数、およびバッファ処理の統計に関する情報が提供されます。

Linux では、プロセスで使用可能な十分なメモリが引き続き存在する場合でも高いメモリ使用率が表示される場合があります。 その理由は、オペレーティング システムが使用可能なメモリをディスク キャッシングに使用しますが（キャッシュ済み）、必要な場合にプロセスにこのメモリを譲るためです。 これは Linux オペレーティング システムの標準の動作であり、パフォーマンスの改善のために実行されます。

メモリ情報を解釈時には、以下の点を考慮します。

- ［メモリ空き］列が小さい場合でも、［キャッシュ済み］数が大きく、［使用済みスワップ］が小さいかゼロの場合、Multi-Port Monitor は正常に動作しています。
- ［メモリ空き］列が小さく、［キャッシュ済み］が小さく、［使用済みスワップ］が大きい場合（この状態は Multi-Port Monitor でスワップが発生していることを示しています）、一部のプロセスでかなりの量のメモリを使用しており、パフォーマンスに影響を及ぼしている可能性があることを示しています。

Multi-Port Monitor アプライアンスは、 64 ビットの CentOS Linux で実行されます。 メモリ情報は、Linux の「free –o」コマンドを使用して取得されます。 以下の列が表示されます。

合計

物理メモリまたはスワップ領域のバイトの総数を示します。

使用済み

使用中の物理メモリまたはスワップ領域のバイトの数を示します。 物理メモリに関しては、この数字にはキャッシュ済みのバイト数が含まれることに注意してください。

空き

物理メモリまたはスワップ領域の空き領域のバイトの数を示します。

バッファ

カーネル バッファによって使用される物理メモリのバイトの数を示します。

キャッシュ済み

カーネルによってディスク キャッシングに使用される物理メモリのバイトの数を示します。

Linux メモリ管理の詳細については、以下の記事を参照してください。

- http://www.linuxhowtos.org/System/Linux%20Memory%20Management.htm
- http://www.itworld.com/it-managementstrategy/280695/making-sense-memory-usage-linux
- http://www.linuxintheshell.org/2012/06/05/episode-008-free-understanding-linux-memory-usage/

CPU

CPU セクションでは、CPU 使用率およびパフォーマンス統計についての情報が提供されます。これは Multi-Port Monitor パフォーマンスおよび負荷を示します。

CPU

統計が対応するアプライアンス上の CPU を識別します。以下の値のいずれかを示します。

- すべて： すべてのプロセッサに対して平均された統計。
- 0 ～ 15： 0 ～ 15 の CPU 識別子。 Multi-Port Monitor プラットフォームは、16 CPU として見えるハイパースレッディング機能を備えたデュアル クワッドコア CPU を搭載しています。

User

ユーザ レベルで実行されているプロセスの CPU 時間の割合。

ナイス

ユーザ レベルで実行されているナイス優先度を持つプロセスの CPU 時間の割合。 優先度はカーネルによって決定されます。

システム

カーネル自体に起因する CPU 使用率のパーセンテージ。

IO 待機

CPU はアイドル状態にあったが、システムに未処理のディスク I/O 要求が存在した時間のパーセンテージ。

IRQ

割り込み要求の処理に費やされた CPU 時間のパーセンテージ。

ソフト

ソフト割り込み状態で費やされた CPU 時間のパーセンテージ。

スチール

ハイパーバイザが別の仮想プロセッサにサービスを提供しているときに仮想 CPU が実 CPU を待機している CPU 時間のパーセンテージ。

アイドル

CPU がアイドル状態にあり、システムに未処理のディスク I/O 要求が存在しなかった時間のパーセンテージ。

割り込み数/秒

CPU が 1 秒あたりに受信した割り込みの総数。

メンテナンス タスク

一部のシステム メンテナンスは自動的に実行されます。 デーモンやプロセスの再起動などの、その他のタスクは手動で実行されます。

データベース保守の場合でも、Multi-Port Monitor アプライアンスにログインする必要性は最小限で済みます。 Web インターフェースを使用して、以下のタスクを実行できます。

- ソフトウェアをアップグレードする。
- プロセスを停止および起動する。
- システム ログを開いてファイルに保存する。
- サポート ファイルを生成する。
- データベースからデータをパージする。

ソフトウェアのアップグレード

新しいリリースまたはパッチが使用可能になると、管理者は Multi-Port Monitor ソフトウェア、オペレーティング システム、および CA TIM ソフトウェアをアップグレードできます。 製品のアップグレード ファイルは、CA テクニカル サポートから提供されます。

Multi-Port Monitor ソフトウェア（前提条件ファイル、Multi-Port Monitor ソフトウェア、オペレーティング システムを含む）のアップグレードは、Web インターフェースの［環境管理］-［Upgrade］ページで行います。 CA TIM ソフトウェアをアップグレードする場合は［System Setup］-［Install Software］ページを使用します。

Multi-Port Monitor ソフトウェアとオペレーティング システムのアップグレード

「CA ADA Multi-Port Monitor アップグレード ガイド」には、Multi-Port Monitor と CentOS オペレーティング システム（該当する場合）をアップグレードする手順がすべて記載されています。

CA TIM ソフトウェアのアップグレード

CA TIM のアップグレード手順は、CA TIM のインストール手順と同じです。 詳細については、「TIM ソフトウェアのインストール」を参照してください。

一般に、アップグレード プロセスは以下のとおりです。

1. アップグレード ファイルを保存した場所を参照します。
2. それを選択し、［Open］をクリックします。
3. ［Upgrade］をクリックしてプロセスを起動します。

   パッチまたはアップグレードの進行状況がメッセージで示されます。 完了を示すメッセージが表示されるまで、このページから離れないでください。

プロセスの停止または再起動

特定のエラー状態が発生するか、またはシステム全体にわたる設定を変更した場合は、Multi-Port Monitor プロセスを停止または再起動します。

注: Web インターフェースによって nqmaintd プロセスを再起動できます。ただし、Web インターフェースによってプロセスを停止または起動することはできません。 nqmaintd プロセスが停止されている場合は、直接アプライアンスにログインして起動します。

次の手順に従ってください:

1. Web インターフェースで、［環境管理］-［Processes］をクリックします。

   ［Process Status］ページが開きます。 ［Process］列には、プロセスの名前が一覧表示されます。

2. ［Start/Stop］列でリンクをクリックして、プロセスを起動、停止、または再起動します。

ヒント： ポート統計情報をリセットするには、nqcapd プロセスを再起動します。

詳細情報:

プロセス情報 (P. 46)

システム ログの確認

Multi-Port Monitor プロセスのログ ファイルに記録されたアクティビティのうち最新の 200 行を表示できます。Multi-Port Monitor プロセスのログに加えて、以下のログ内の最新のエントリを表示できます。

SAService.log

CA Application Delivery Analysis から Multi-Port Monitor への通信（ハートビートやフィード ステータス更新を含む）のエントリが含まれています。

また、APM コンソールの［障害詳細］ページに表示されるネットワーク ヘルス情報に対する要求も含まれています。

SAInvestigations.log

CA Application Delivery Analysis からのパケット キャプチャ調査要求を記録するエントリが含まれています。

nqsnmptrap.log

SNMP トラップをトリガした条件ごとのエントリが含まれています。

次の手順に従ってください:

1. Web インターフェースで、［環境管理］-［System Logs］をクリックします。

   ［System Logs］ページが表示されます。

2. ［Log File］フィールドからログ ファイルを選択します。

   ［System Logs］ページが、選択したログのサイズを表示するように更新されます。 例：

   ```
   The file nqInspectorAgentd_20110228.log is 300160 bytes in size.
   ```

3. ［View］をクリックします。

   ［System Logs］ページが、選択したログの最後の 200 行を表示するように更新されます。

詳細情報:

プロセス情報 (P. 46)

サポート ファイルの生成

CA テクニカル サポートの担当者に必要なトラブルシューティング情報を含むサポート ファイルを生成できます。 サポート ファイルには、すべてのプロセスからの最新のすべてのログがまとめられ、圧縮された tar 形式（.tgz）でデータが保存されます。

次の手順に従ってください:

1. Web インターフェースで、［環境管理］-［System Logs］をクリックします。

   ［System Logs］ページが表示されます。

2. （*オプション*） Multi-Port Monitor メトリック データベース上の診断ユーティリティからの情報を含めるために［Include metrics database diagnostics］を選択します。

   注: このオプションを選択すると、サポート ファイルの生成に時間がかかる場合があります。 CA テクニカル サポートの担当者から指示された場合にのみ、このオプションを選択します。

3. ［Generate］をクリックします。

   ［System Logs］ページに、新しいサポート ログ ファイルの名前が表示されます。

4. ［Select the support file for download］フィールドからログ ファイルを選択します。

5. ［ダウンロード］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。

6. ［保存］をクリックし、ファイルを保存する場所に移動します。

データベース ステータスおよび使用状況

［データベース ステータス］ページ上の統計では、データベース ステータスおよび使用状況が示されます。［Application Settings］ページ上でパージ（ファイル保存期間）設定を選択する場合、この情報をガイドとして使用します。 ［Database Usage］セクションの情報は、1 分間隔のメトリックが含まれた古いデータベース エントリをいつパージするかを決定するために特に役立ちます。

［データベース ステータス］ページでは、以下の情報が提供されます。

データベース

Multi-Port Monitor アプライアンス上のローカル データベースの名前。

ステータス

データベースのステータス（［稼働中］、［ダウン］、［シャットダウン中］、または［初期化中］）。

Start/Stop

データベースを起動または停止するために使用できるリンク。アプライアンスをシャットダウンまたは再起動する場合は、先にデータベースを停止します。

Date of oldest data

データベース内に存在するデータの最も古いタイムスタンプ。

Date of newest data

データベース内に存在するデータの最新のタイムスタンプ。

Rows in database

データベース内の使用中の行の総数。 最大行数は 120 億です。 最大しきい値を超えると、夜間のメンテナンス ルーチンによって 120 億行未満に廃棄されます。

Rows for past day

過去 24 時間に使用されたデータベース行の数。

Rows for past 7 days

過去 1 週間に使用されたデータベース行の数。

ヒント：

- データベース使用率セクションでは、最も古いデータと最新のデータが挿入された時期を示す日付の範囲と、いくつかのデータベース行数が提供されます。 これらの情報は、データが蓄積されている速度を測定するのに役立ちます。 これらの情報に基づいて、情報がデータベース内に保持される日数を調整できます。
- データベースに追加される行数を削減するには、各論理ポートに適用されるフィルタを調整します。 たとえば、すべてのプロトコル トラフィックをキャプチャするデフォルトのフィルタを使用する代わりに、TCP パケットのみをキャプチャすることができます。
- データベースのステータスは、60 秒ごとに自動的に更新されます。 行数は、［データベース ステータス］ページに移動するか、またはブラウザを更新したときにのみ更新されます。
- 管理者製品権限を持っていないユーザは、［システム ステータス］ページでデータベース ステータスを確認できます。 Multi-Port Monitor ユーザはすべて、［システム ステータス］ページにアクセスできます。

詳細情報:

グローバル環境設定の設定 (P. 28)
コマンド ライン構文 (P. 79)
システム ステータス (P. 45)
ハードウェア フィルタを使用したデータ管理 (P. 16)

データベースからのデータのパージ

通常の動作中、Multi-Port Monitor はデータベースとファイル システムに対してルーチン メンテナンスを実行します。ルーチン メンテナンスには、さまざまなタイプのデータやファイルのパージが含まれます。 通常、未処理パケット キャプチャ ファイルは、パージされる前に 6 時間保持されます。 1 分の間隔からのパフォーマンス メトリックを含むファイルは、パージされる前に 1 週間保持されます。

以下のような複数の理由では、Multi-Port Monitor データベースを手動でパージできます。

- ［データベース ステータス］ページで問題が検出されている。
- ［システム ステータス］ページ上の統計で、ファイル システムがほぼいっぱいであることが示されている。
- ディスク使用量がしきい値を超えていることを示す mpcDiskUsage SNMP トラップを受信した。

重要: パージされたデータは、データベースから完全に削除されます。パージされたデータを回復することはできません。

次の手順に従ってください:

1. Web インターフェースで、［環境管理］-［Purge Data］をクリックします。

   ［Purge Data］ページが表示されます。

2. ［Purge all data and metric database tables］を選択して、すべてのデータおよびデータベース テーブルを削除します。

   このオプションにより、データを収集するプロセスが停止されます。このプロセスを再起動するまで、新しいデータは収集されません。

   このオプションを選択すると、このページ上のその他のオプションはすべて使用できなくなります。

3. 選択したデータのみを削除するには、以下のオプションのうちの少なくとも 1 つを選択します。 プロセスは実行を継続し、新しいデータが引き続き収集されます。

   - **Purge one-minute session metrics**： メトリック データベースから 1 分のセッション メトリックを削除します。
   - **Purge raw capture files**： パケット キャプチャ ファイルを削除します。 これらのファイルは通常の監視中も継続的に生成され、パフォーマンス統計を導き出すために使用されます。 デフォルトは 6 です。
   - **Purge packet capture investigations**： パケット キャプチャ調査のファイルを削除します。 調査ファイルは、未処理キャプチャ ファイルとは別に格納されます。 デフォルトは 90 です。
   - **Purge log files**： Multi-Port Monitor が作成するログ ファイルを削除します。

4. 手順 3 で選択したデータを削除する際のタイムフレームを選択します。

   - **Purge across all dates**： タイムフレームに関係なく、選択したタイプのデータを削除します。
   - **Purge prior to this date**： 指定した日付より前に収集されたデータを削除します。

     注: データは協定世界時（UTC）で格納されます。 このオプションにより、真夜中 UTC の前に収集されたデータが削除されます。ローカル時間を使用してデータを表示すると、以前の日の一部のデータが引き続き存在するように見える可能性があります。

5. ［OK］をクリックします。
6. 手順 2 の説明に従ってすべてのデータをパージした場合は、停止されたプロセスを再起動します。

詳細情報:

グローバル環境設定の設定 (P. 28)
データベース ステータス (P. 47)
システム ステータス (P. 45)
SNMP トラップの作成 (P. 30)

アプライアンスへのログイン

通常、ハードウェアとソフトウェアをインストールした後に Multi-Port Monitor アプライアンスにログインする必要はありません。 ほとんどの管理タスクは Web インターフェースから実行できます。 ただし、以下のタスクでは直接アプライアンスにアクセスします。

メンテナンス デーモン（nqmaintd）が停止されていた場合は起動する

このデーモンは、他のプロセスを起動または再起動するために必要です。 このデーモンを Web インターフェースから起動または停止することはできません。

アプライアンスをシャットダウンまたは再起動する

アップグレードの場合であっても、シャットダウンや再起動は必要ありません。 ただし、コンピュータをオフラインにするには、ログインの手順とコマンドを使用して正しくシャットダウンします。

ロードまたはマージの操作中にアプライアンスをシャットダウンすると、ローカル データベースが破損する場合があります。アプライアンスをシャットダウンする前に、データベースを停止します。

接続されたキーボードとモニタを使用して、アプライアンスに直接ログインします。 また、Microsoft Windows 上で実行される、PuTTY などのセキュア シェル（SSH）クライアントを使用してリモート システムからログインすることもできます。

次の手順に従ってください:

1. 初期画面で Alt+F2 キーを押します。

   Linux のログイン画面が開きます。

2. 以下の認証情報でログインします。

   - ユーザ名： netqos
   - パスワード： Multi-Port Monitor ソフトウェアのインストール時に作成したパスワード

   Linux のコマンド ライン インターフェースが開きます。

3. 必要なコマンドを実行します。

詳細情報:

データベース ステータス (P. 47)
コマンド ライン構文 (P. 79)

システム セットアップ

［システム セットアップ］ページは、Multi-Port Monitor アプライアンスにインストールされているコンポーネントが識別されます。 多くの場合、コンポーネントの名前は詳細情報へのハイパーリンクです。

Machine Settings

ビルド番号、および［Machine Settings］ページへのリンク。［Machine Settings］ページを使用して、ネットワーク設定を確認し、タイム ゾーンを設定し、アプライアンスをシャットダウンまたは再起動します。

Multi-Port Monitor

ビルド番号、および［環境管理］ページへのリンク。［環境管理］ページを使用して、データ監視、システム設定、および認証を設定し、メンテナンスを実行します。

Multi-Port Monitor Prerequisites

最後にダウンロードされた前提条件となるパッケージのビルド番号。

システム ヘルス

ビルド番号、および Customer Experience Manager（CEM）コンソール上の［Appliance Health］ページへのリンク。 ［Appliance Health］ページを使用して、ディスクとメモリの使用量、ログイン ユーザ、および実行中のプロセスに関する情報を確認します。 このアイテムは、アプライアンスに CA TIM がインストールされている場合にのみ使用できます。

Third-party

アプライアンスにインストールされている CA TIM サードパーティ アプリケーションのバージョンおよびビルド番号。 このアイテムは、アプライアンスに CA TIM がインストールされている場合にのみ使用できます。

TIM

ビルド番号、および CEM コンソール上の［TIM Setup］ページへのリンク。［TIM Setup］ページを使用して、CA TIM の停止と開始、ステータスと統計の表示、および Watchdog 設定を行います。このアイテムは、アプライアンスに CA TIM がインストールされている場合にのみ使用できます。

詳細情報:

マシン設定 (P. 66)

マシン設定

［Machine Settings］ページでは、以下のページへのリンクが提供されます。

- Network Setup（P. 66）
- Set Time Zone（P. 67）
- System Shutdown/Restart（P. 68）

ネットワーク設定

［Network Setup］ページでは、Multi-Port Monitor ソフトウェアをインストールし、ネットワーク アクセスを有効にしたときに作成されたネットワーク設定が識別されます。 詳細については、アプライアンスに付属の「CA ADA Multi-Port Monitor インストール ガイド」を参照してください。

このページ上のフィールドを使用して、ネットワーク設定を変更できます。

Select which interface to configure

このフィールドでの選択によって、このページ上の他のフィールドの内容が決定されます。 インターフェースを選択し、残りのフィールドの情報を変更する前に［設定］をクリックします。ページが更新され、インターフェースに IPv4 アドレスが存在するかどうかが示されます。

Automatically obtain IP address settings with DHCP

このオプションは、DHCP（Dynamic Host Configuration Protocol）を使用して管理 NIC の IP アドレスを取得する場合に選択します。 管理 NIC の DHCP ホスト名を指定できます。

Manual IP Address Settings

このオプションは、管理 NIC の IP アドレス、サブネット マスク、およびデフォルト ゲートウェイ アドレスを入力する場合に選択します。

注: 管理 NIC の IP アドレスは、CA Application Delivery Analysis 管理コンソールで Multi-Port Monitor に割り当てられた IP アドレスと一致している必要があります。

Manual DNS Settings

［DNS server 1］フィールドに、ローカル DNS サーバの IP アドレスを入力します。

（*オプション*）［DNS server 2］および［DNS server 3］フィールドに、セカンダリ DNS サーバの IP アドレスを入力します。

Submit

変更をネットワーク設定に保持する場合にクリックします。

タイム ゾーンの選択

Multi-Port Monitor アプライアンスのタイム ゾーンを変更できます。

次の手順に従ってください:

1. Web インターフェースで、［システム セットアップ］-［Machine Settings］をクリックします。

   ［Machine Settings］ページが開きます。

2. ［Set Time Zone］をクリックします。

   ［Set Time Zone］ページが開きます。

3. アプライアンスのタイム ゾーンを選択します。
4. 確認プロンプトで［Set Time Zone］をクリックします。

   確認メッセージが表示されます。

アプライアンスのシャットダウンまたは再起動

CA6000 および CA6300 のアプライアンスに該当

アプライアンスをシャットダウンまたは再起動する場合、常に Vertica メトリック データベースを先にシャットダウンします。 アプライアンスのシャットダウンまたは再起動を以下の場所から行う場合：

Multi-Port Monitor Web **インターフェース**

1. Vertica メトリック データベースをシャットダウンします。
   a. ［環境管理］をクリックして［環境管理］ページを開きます。
   b. ［Database Status］をクリックして［Database Status］ページを開きます。
   c. Metrics データベースを停止するために Stop をクリックします。
2. アプライアンスをシャットダウンまたは再起動します。
   a. ［System Setup］をクリックして［System Setup］ページを開きます。
   b. ［Machine Settings］をクリックして［Machine Settings］ページを開きます。
   c. ［System Shutdown/Restart］をクリックします。
   d. 次のオプションをクリックします。
      - **Shut down the computer** このオプションは、アプライアンスの電源を切る場合に選択します。 再び電源を入れるには、アプライアンスに物理的にアクセスできる必要があります。
      - **Restart the computer** このオプションは、アプライアンスの電源を切ってから再起動する場合に選択します。 Vertica メトリック データベースは、アプライアンスの再起動時に自動的に起動します。

コマンド ライン

以下のコマンドを実行します。

1. Vertica メトリック データベースを停止します。
   ```
   sudo /opt/NetQoS/scripts/doVerticaCmd.sh --shutdown
   ```
2. アプライアンスをシャットダウンまたは再起動します。

   アプライアンス をシャット ダウンするには、以下を実行します。
   ```
   sudo /sbin/shutdown -h now
   ```

アプライアンスを再起動するには、以下を実行します。

```
sudo /sbin/shutdown –r now
```

詳細:

アプライアンスへのログイン (P. 64)

第 5 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。

IPv6 トラフィックが正しくキャプチャされない

問題の状況:

IPv6 トラフィックをキャプチャしようとすると、以下のエラーが発生します。

- Traffic that is sliced to "Headers Only" includes the IPv6 header but no TCP header.
- Filters based on Layer 4 header information (such as TCP port number) do not capture IPv6 traffic.

解決方法:

Napatech カードの FPGA （ファームウェア）の更新が必要な場合があります。 以下の表で、IPv6 トラフィックをキャプチャするために必要な FPGA バージョンを確認できます。

Napatech **カード モデル**	FPGA **バージョン**
NT4E （4x1Gb）	200-9015-**42**-08
NTPORT4 （4x1Gb 拡張カード）	200-9019-**42**-05
NT20E （2x10Gb）	200-9014-**42**-07

確認が必要な箇所は、FPGA バージョン番号の太字の部分です。 該当箇所に 42 未満の数字を含む FPGA は、IPv6 パケット ヘッダのデコードを完全にはサポートしません。

以下のいずれかの方法を使用して、FPGA のバージョンを確認します。

- Multi-Port Monitor Web インターフェースの［バージョン情報］をクリックします。［バージョン情報］ページで、アクティブな Napatech FPGA のバージョン番号を確認できます。
- Linux のコマンド ラインから以下のコマンドを実行します。
  ```
  sudo  /opt/napatech/bin/AdapterInfo
  ```
  コマンドの出力に、アクティブな FPGA イメージを示す行が含まれます。

Multi-Port Monitor ソフトウェアをアップグレードしても、Napatech FPGA は更新されません。 更新の手順および FPGA イメージの詳細については、CA テクニカル サポートまでお問い合わせください。

キャプチャ カードのクロックがシステム クロックと異なる

問題の状況:

［キャプチャ カード物理ポート ステータス］セクションの［システム ステータス］ページに以下のメッセージが表示されます。

```
"Capture card clock differs from system clock by N seconds."
```

解決方法:

キャプチャ カードは、受信パケットの時刻をスタンプするための独立したクロックを備えています。 通常の動作では、このクロックは Multi-Port Monitor のシステム クロックと同期されます。 このエラー メッセージは、Multi-Port Monitor のシステム クロックとキャプチャ カード上のクロックの間に不一致が存在する場合に表示されます。たとえば、システム クロックの時刻が手動で変更された場合に、この不一致が発生することがあります。

以下の方法を使用して、クロックを同期します。

- **直ちにクロックを同期する**。アプライアンス上の Linux コマンド ライン インターフェースから、以下のコマンドを実行します。このコマンドによって nqcapd プロセスと nqmetricd プロセスが停止され、それにより監視が中断されます。これらのプロセスは、クロックが同期された後に再起動されます。

  ```
  sudo /opt/NetQoS/scripts/syncNapatechClock --force
  ```

- **同期を維持する**。ネットワーク タイム プロトコル(NTP)を実行して、クロック間の同期を維持します。NTP は、アプライアンス上でネットワーク設定ユーティリティを使用して設定できます。このユーティリティを開くには、Linux コマンド ライン インターフェースから、以下のコマンドを実行します。

  ```
  sudo /opt/NetQoS/tui/tui-setup.php
  ```

  このユーティリティで、［NTP Server］フィールドに NTP サーバのホスト名または IP アドレスを入力します。デフォルトは pool.ntp.org です。

時間範囲が未処理パケットの保持期間を超えている

問題の状況:

データを PCAP 形式にエクスポートしようとすると、以下の警告メッセージが表示されます。

```
Time range exceeds raw packet capture retention time.
```

解決方法:

Web インターフェースの［Application Settings (P. 28)］ページには、［PCAP へエクスポート］機能に影響を与えるファイル保存期間設定が含まれています。このエラーは、エクスポートするデータのタイムフレームが「Keep raw packet capture files for」の設定より小さい場合に発生します。

［システム ステータス］ページを使用して、［ファイル システム］セクションでデータのディスク使用量を評価します。十分な空き領域がある場合は、「Keep raw packet capture files for」の設定の値を増やします。将来の PCAP エクスポートには、さらに前の過去からのデータが含まれる予定です。

付録 A: 展開のベスト プラクティス

このセクションには、以下のトピックが含まれています。

アプライアンスの配置

Multi-Port Monitor アプライアンスには、監視対象トラフィックを処理する各ネットワーク スイッチ上の SPAN またはミラー ポートへの接続が必要です。 接続は通常、アクセス層で実行されます。

アプライアンスは、関連するネットワーク トラフィックをできるだけ多く*認識*できる必要があります。 以下の事柄を検討します。

- どのアプリケーションを監視しますか。
- どのサーバがこれらのアプリケーションをホストしますか。
- これらのサーバはどのスイッチに接続されていますか。
- ユーザはどのサブネットから監視対象アプリケーションにアクセスしますか。

ネットワークまたはトラフィック量が並外れて大きい場合は、追加のアプライアンスを購入して処理負荷のバランスをとることができます。

ポート ミラーリング

ネットワーク スイッチでは、*ポート ミラーリング*機能により、ネットワーク パケットのコピーを分析のためにあるポートから別のスイッチまたはポートに送信します。 ポート ミラーリングは、トラフィックを CA Application Delivery Analysis 監視デバイスにミラーリングする安全で効果的な方法です。 一部のスイッチでは、多様な TCP パケット ミラーリング機能が提供されません。 トラフィックを最適にミラーリングできない場合は、ファイバ タップなどの代替手段を使用してください。

注: Cisco スイッチ上のポート ミラーリング機能は、Switched Port Analyzer（SPAN）と呼ばれます。

監視対象サーバとの間のトラフィックが通過するスイッチ ポートを、Multi-Port Monitor が接続されているポートにミラーリングします。 ミラー ポートが正しく設定されている場合、CA Application Delivery Analysis は、デスクトップまたはサーバ エージェントを使用することなくクライアントとサーバの間のアプリケーションのフローを監視します。

詳細については、「CA Best Practices for Data Acquisition Guide」を参照してください。

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	■ 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
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

ポート	方向	説明
161	インバウンド	SNMP MIB クエリ
162	アウトバウンド	SNMP トラップ
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	■ 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。

パケット デデュプリケーション

*パケット デデュプリケーション*という用語は、スイッチ上のインターフェースをパケットが通過するときに同一トラフィックが複数回、レポートされることを指します。 すべてのポートからのトラフィックが Multi-Port Monitor に転送されるため、いくつかのポート ミラーリング設定で重複が発生することがあります。

重複パケットが存在すると、収集されるメトリックが不正確になることがあります。 重複パケットは再送信として表示されるので、パケット ロス統計に影響を与えます。

ベストプラクティスは、重複パケットを最小限にするか除去するようにミラー ポートを設定することです。Multi-Port Monitor には、キャプチャ カードに適用されるパケット デデュプリケーション設定があり、デフォルトで有効になっています。 この設定により、処理済みパケットと重複しているように見えるパケットが破棄されます。

ポート ミラーリングの初期設定中は、一時的にパケット デデュプリケーションのグローバル設定を無効にできます。 この設定を無効にすると重複パケットを確認できるため、ミラーリング セッションから重複を除去するのに役立ちます。

デデュプリケーションのロジックは、指定した論理ポートで受信されたすべてのパケットに適用されます。 そのため、重複パケットが異なる論理ポートで受信されると、同一の VLAN からの重複パケットは破棄されません。 2 つの物理ポートを組み合わせて 1 つの論理ポート定義にする場合、以下の状況で重複が破棄されます。

- 元のパケットが 1 つ目の物理ポートに到着した直後に、重複パケットが別の物理ポートに到着する場合。
- 重複パケットが別のスイッチに到着する場合。

2 つの物理ポートを組み合わせて 1 つの論理ポートにしない場合は、両方のパケットが保持されます。

付録 B: コマンド ライン構文

Multi-Port Monitor アプライアンスのデフォルトのユーザ名とパスワードでは、スーパーユーザのアクセス権が提供されます。 スーパーユーザ コマンドを識別する「sudo」プレフィックスを使用して、Linux のコマンド ライン インターフェースで以下の操作を実行できます。

sudo /sbin/service nqmaintd status

メンテナンス デーモン（nqmaintd）のステータスを確認します。

sudo /sbin/service nqmaintd restart

メンテナンス デーモンを再起動します。 ステータス メッセージでプロセスが実行中であることが示されている場合にのみ使用してください。

sudo /sbin/service nqmaintd start

メンテナンス デーモンを起動します。 ステータス メッセージでプロセスが停止していることが示されている場合にのみ使用してください。

sudo /opt/NetQoS/scripts/stopprocs.sh

すべてのデーモン（プロセス）を停止します。

sudo /opt/NetQoS/scripts/startprocs.sh

すべてのデーモン（プロセス）を起動します。

sudo /sbin/shutdown -h now

アプライアンスを直ちに停止します。アプライアンスを停止する前に、Multi-Port Monitor データベースを停止してください。

sudo reboot

アプライアンスを直ちに停止して再起動します。アプライアンスを停止する前に、Multi-Port Monitor データベースを停止してください。

sudo /opt/NetQoS/scripts/doVerticaCmd.sh --shutdown

Vertica メトリック データベースを停止します。 また、Web インターフェースからデータベースを停止することもできます。

sudo /opt/NetQoS/scripts/doVerticaCmd.sh --start

Vertica メトリック データベースを開始します。

sudo /opt/NetQoS/scripts/doVerticaCmd.sh --status

Vertica メトリック データベースのステータスを確認します。 また、Web インターフェースからステータスを確認することもできます。

sudo /opt/NetQoS/tui/tui-setup.php

アプライアンス上でネットワーク設定ユーティリティを起動します。

sudo /opt/NetQoS/scripts/syncNapatechClock --force

Multi-Port Monitor キャプチャ カード上のクロックをシステム クロックと直ちに同期します。 このコマンドによって nqcapd プロセスと nqmetricd プロセスが一時的に停止され、それにより監視が中断されます。 クロックが同期された後、両方のプロセスが再起動されます。

詳細情報:

アプライアンスへのログイン (P. 64)
データベース ステータス (P. 47)
データベース ステータスおよび使用状況 (P. 60)
キャプチャ カードのクロックがシステム クロックと異なる (P. 72)

付録 C: 正規表現構文

高度なフィルタでは、［条件］フィールドに書き込まれた構文が、キャプチャ カードの互換性のためのベンダー仕様に自動的に従います。 生成された式（特に、式をグループ化するかっこの位置）を見直して、式が正しい順序で評価されることを確認してください。 たとえば、以下のグループ化

```
(A OR B) AND C
```

は、このグループ化とは異なる結果になります。

```
A OR (B AND C)
```

この構文は、［条件］フィールドで編集できます。

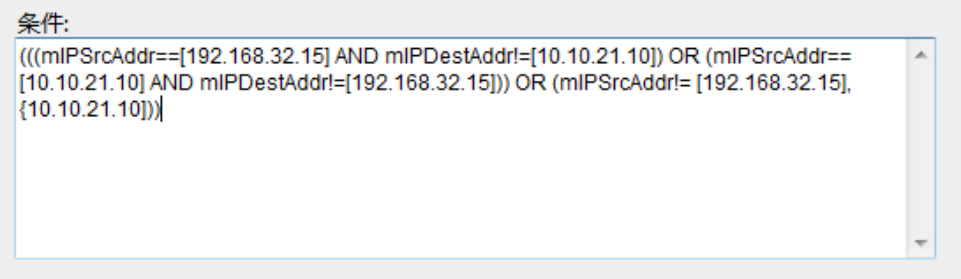
Multi-Port Monitor のフィルタでは、条件に一致するパケットが含まれます。特定のホストまたはサブネットからパケットを*除外する*フィルタを作成する場合は、特に注意してください。 式の構文について質問がある場合は、CA テクニカル サポートにお問い合わせください。

例

ホスト A（192.168.32.15）とホスト B（10.10.21.10）の間の通信を無視するとします。この通信は、週に 1 回実行され、そのたびにベースラインにひずみを生じさせる自動バックアップ プロセスを表します。 「その他のすべてのトラフィック」に関するレポートが必要です。また、除外されたペア以外のホストに転送されるトラフィックのすべてのパケットを保持することも必要です。 そのため、以下のパケットを保持するフィルタを作成します。

- ホスト A がソースであるが、宛先がホスト B に等しくないすべてのパケット、または
- ホスト B がソースであるが、宛先がホスト A に等しくないすべてのパケット、または
- ホスト A およびホスト B の IP アドレスに等しくないソース アドレスを含むすべてのパケット（その他のすべてのトラフィック）

［条件］フィールドでは、正しい構文は以下のようになります。



英語で記述した場合、作成する式は以下のようになります。

```
(IP Source Address EQUALS 192.168.32.15 AND IP Destination Address does NOT EQUAL
10.10.21.10) OR (IP Source Address EQUALS 10.10.21.10 AND IP Destination Address
does NOT EQUAL 192.168.32.15) OR (IP Source Address does NOT EQUAL 192.168.32.15,
10.10.21.10)
```

正規表現を使用して高度なフィルタを作成する場合、「==」を挿入するには［Equals］を選択します。「!=」を挿入するには［Not Equals］を選択します。

詳細情報:

正確なフィルタリングのための正規表現の使用 (P. 25)