CA Transaction Impact Monitor との統合

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: CA TIM のサポート

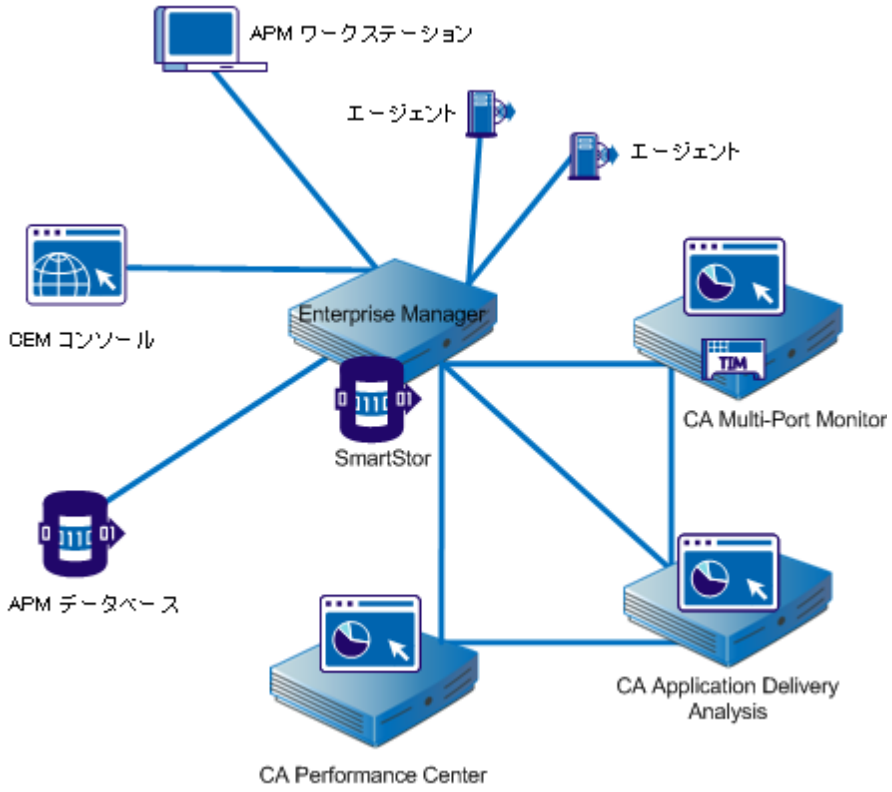
Multi-Port Monitor は CA Transaction Impact Manager （TIM）の HTTP パケットをキャプチャします。

- CA TIM は、ミラーリングされたポートからのトラフィックをパッシブに監視します。
- CA TIM では、以下の製品のユーザ ログインおよび関連するトランザクションを識別するための HTTP および HTTPS パケットを記録します。
  - CA Customer Experience Manager （CA CEM）
  - CA Application Performance Management (CA APM)
- CA TIM では SSL （Secure Sockets Layer）デコードを実行します。

CA TIM が Multi-Port Monitor アプライアンスにインストールされると、その結果*統合されたアプライアンス*では、ユーザごとのアプリケーション使用状況のアプリケーションおよびネットワーク レベル データを可視化できるようになります。スタンドアロンのアプライアンスとして、CA TIM は、リアルタイムで HTTP トランザクションを監視し、異常を検出すると障害を生成します。 Multi-Port Monitor は 1 分間隔でセッション レベル データを提供します。 統合アプライアンスでは、このより詳細なデータ精度を使用して CA TIM が検出する障害を調査できます。CA APM コンソールを使用し、障害から Multi-Port Monitor Web インターフェース内の関連するデータにドリルダウンします。

Web インターフェースでは、CA TIM の管理およびメンテナンス タスクを実行できます。

以下の図は、Multi-Port Monitor、CA APM、および CA Application Delivery Analysis がインストールされているネットワーク内のコンポーネントを示します。



図に示されているように、Multi-Port Monitor は CA TIM および CA Application Delivery Analysis を同時にサポートできます。このシナリオでは、CA TIM および CA Application Delivery Analysis のパケットは並行して処理されます。 個別の RAM ディスクでは、両方のアプリケーションのパケットをバッファできます。

- CA Application Delivery Analysis に対して、Multi-Port Monitor はヘッダのみのすべてのパケットを提供します。
- CA TIM に対して、Multi-Port Monitor は完全なペイロードを持つ、フィルタされた HTTP パケットを提供します。

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	■ 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
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。

第 2 章: Multi-Port Monitor アプライアンスへの CA TIM のインストール

Multi-Port Monitor アプライアンスには、CA Transaction Impact Manager（CA TIM）ソフトウェアの CD が含まれます。 または、CA テクニカル サポートから CA TIM ソフトウェアをダウンロードできます。

注: Multi-Port Monitor を CA Application Delivery Analysis でのみ使用する場合、CA TIM ソフトウェアをインストールする必要はありません。

Multi-Port Monitor Web インターフェースを使用して以下のファイルをインストールします。

- サードパーティ イメージ： third-party-update-xxxxxxxxxx.image
- TIM イメージ： tim-complete-xxxxxxxxxxxxx.image

次の手順に従ってください:

1. Multi-Port Monitor アプライアンスに Web ブラウザでアクセスできるワークステーションにセットアップ ファイルをダウンロードします。
2. 管理者権限を持つユーザとして Multi-Port Monitor Web インターフェースにログインします。

   Web インターフェースが開きます。
3. Web インターフェースの［システム セットアップ］-［Install Software］をクリックします。

   ［Install Software］ページが表示されます。
4. ［Browse］をクリックし、セットアップ ファイルをダウンロードした場所へ移動します。
5. third-party-update-xxxxxxxxxx.image ファイルを選択します。
6. ［Open］をクリックします。

   ファイルの名前が［Install Software］ページに表示されます。
7. ［Upload and Install］をクリックします。

8. ライセンス使用条件の内容を確認してから同意します。

   ソフトウェア インストール ログが表示されます。 ログに赤字で表示されているエラーが含まれる場合は、CA テクニカル サポートにお問い合わせください。

9. ［Install Software］ページ上で［Browse］をクリックし、セットアップ ファイルをダウンロードした場所へ移動します。

10. tim-complete-xxxxxxxxxxxx.image ファイルを選択し、次に、手順 6 ～ 8 を繰り返します。

11. Web インターフェースの［システム セットアップ］をクリックします。

    インストールが成功すると、インストールしたファイルの名前が［システム セットアップ］ページに表示されます。

12. CA TIM による監視で使用する論理ポートを識別します。詳細については、「論理ポートの設定 (P. 13)」を参照してください。

13. 完全なパケットをキャプチャする［HTTP - full packets］ハードウェア フィルタを有効にします。

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

    b. CA TIM 監視と関連付けられている論理ポートの［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。

    c. ［HTTP - full packets］フィルタの［Edit］リンクをクリックします。

       ［Logical Ports: Edit Hardware Filter］ページが表示されます。

    d. ［Filter Enabled］チェック ボックスを選択します。

    e. nqcapd プロセスを再起動します。

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。

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」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. 12)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。

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。

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**。名前が指定されている論理ポートにフィルタを適用します。選択した場合、nqcapd プロセスを再起動した後、フィルタが適用されます。
   - **Filter Name**。作成または編集するフィルタの名前。フィルタ名は、それが適用される論理ポート用の［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数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、および［Packet Slicing Size］フィールドのペイロード バイトの固定数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）、IPv6、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 traceroute 調査に使用されます。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。

- **VLAN**。 監視するまたは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 の識別子をリストします。 複数の VLAN はカンマを使用し、スペースなしで区切ります。 リストした VLAN からのトラフィックを破棄するには、［Exclude］を選択します。

- **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、または有効な IPv6 アドレスおよびプレフィックス ビットを指定します。 リストで IPv4 と IPv6 のアドレスを組み合わせないでください。 ［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。

  IPv6 アドレスには x:x:x:x:x/*n* の形式を使用します。x:x:x:x:x はコロン区切りの IPv6 サブネット アドレスで、*n* はプレフィックス ビットの数です。 標準の IPv6 アドレスの短縮形を使用できます。 たとえば、2001:ba0:1a0::/48 などです。

  ヒント： IPv4 *および*IPv6 のサブネットをフィルタするには、IPv4 サブネット用にハードウェア フィルタを 1 つ作成し、IPv6 サブネット用に別のハードウェア フィルタを作成します。

- **IP Addresses**。 監視するまたは監視から除外する個別のホストの IPv4 または IPv6 のアドレス、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。 リストで単一のアドレスと範囲を組み合わせないでください。アドレスの同じリストまたは範囲で IPv4 と IPv6 のアドレスを組み合わせないでください。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。

  コロン区切りの IPv6 アドレスを使用します。 標準の IPv6 アドレスの短縮形を使用できます。 たとえば、2001:f0d0:1002:51::4 などです。

  ヒント： IPv4 *および*IPv6 のアドレスをフィルタするには、IPv4 アドレス用にハードウェア フィルタを 1 つ作成し、IPv6 アドレス用に別のハードウェア フィルタを作成します。

Ports。 監視するまたは監視から除外する TCP ポートまたはポート範囲。 複数のポート番号はカンマを使用し、スペースなしで区切ります。 ポートの範囲については、2483-2484 のような形式を使用します。 リストしたポートからのトラフィックを破棄するには、［Exclude］を選択します。

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には［Advanced］をクリックします。

c. ［Save］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。

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. ［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。

5. フィルタを有効にした場合は、nqcapd プロセスを再起動 (P. 12)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 (P. 15)。
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. 12)します。

第 3 章: Multi-Port Monitor アプライアンス上の CA TIM のアップグレード

新しいリリースが使用可能である場合、管理者は 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 Web インターフェースを使用して以下のファイルをインストールします。

- サードパーティ イメージ： third-party-update-xxxxxxxxxx.image
- TIM イメージ： tim-complete-xxxxxxxxxxxxx.image

次の手順に従ってください:

1. セットアップ ファイルを、Multi-Port Monitor アプライアンスに Web ブラウザでアクセスできるワークステーションにダウンロードします。
2. 管理者権限を持つユーザとして、Multi-Port Monitor Web インターフェースにログインします。

   Web インターフェースが開きます。
3. Web インターフェースの［環境管理］-［Upgrade］をクリックします。

   ［Upgrade Software］ページが表示されます。
4. ［Browse］をクリックし、セットアップ ファイルをダウンロードした場所へ移動します。
5. third-party-update-xxxxxxxxxx.image ファイルを選択します。
6. ［Open］をクリックします。

   ファイルの名前が［Upgrade Software］ページに表示されます。
7. ［Upload and Install］をクリックします。
8. ライセンス使用条件の内容を確認してから同意します。

   ソフトウェア インストール ログが表示されます。 ログに赤字で表示されているエラーが含まれる場合は、CA テクニカル サポートにお問い合わせください。

9. ［Upgrade Software］ページ上で［Browse］をクリックし、セットアップ ファイルをダウンロードした場所へ移動します。
10. tim-complete-xxxxxxxxxxxxx.image ファイルを選択し、手順 6 ～ 8 を繰り返します。
11. Web インターフェースの［システム セットアップ］をクリックします。

    アップグレードが成功すると、インストールしたファイルの名前が［システム セットアップ］ページに表示されます。

第 4 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。

CA TIM が Napatech を使用するように設定されていない

問題の状況:

CA TIM のエラー ログに、以下のメッセージが表示されます。

```
Napatech software is installed but TIM is not configured to use Napatech.
```

解決方法:

このメッセージは、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場合に表示されます。 Multi-Port Monitor は Napatech カードを管理するように設定されているため、このメッセージは無視してもかまいません。

CA TIM の動作停止

症状:

Multi-Port Monitor にインストールされた TIM が正しく機能しなくなりました。 たとえば、統計の記録および生成が停止します。 また、TIM ログに「skip old packets」というメッセージが表示されます。

解決方法:

Multi-Port Monitor に TIM をインストールすると、Multi-Port Monitor 上の Napatech カードは、そのカードの時間を使用してパケットの到着時間をマークします。 Multi-Port Monitor 上のシステム時間と Napatech カードの時間が異なる場合、TIM が正常に動作しなくなることがあります。

以下の 2 つのユースケースが考えられます。どちらのユースケースを適用できるかを判断してください。

1. TIM 処理は、Multi-Port Monitor からのパケット ファイルより遅れることがあります。 たとえば、TIM が停止して再起動された場合、または TIM が処理できるよりも速いタイミングで Multi-Port Monitor がパケット ファイルを生成している場合です。 以下のタスクを実行して、TIM の遅延時間を確認します。

   a. Napatech カードの時間が、Multi-Port Monitor 上のシステム時間と同期していることを確認します。

   b. Multi-Port Monitor のシステム ステータス ページを確認し、警告メッセージが表示されていないことを確認します。

   この 2 つのシナリオを確認済みの場合、TIM には問題はありません。TIM は、15 分（このデフォルト値は変更可能）を越える時間を経過したプロセス パケット ファイルを処理しません。 これらの古いパケット ファイルをスキップした後、TIM は通常の処理を再開します。 TIM には、Multi-Port Monitor の生成ファイルに追いつく時間が必要なだけです。

2. Napatech カードの時間を、Multi-Port Monitor 上のシステム時間と比較します。 Napatech カードの時間を参照するには、端末から以下のコマンドを使用します。

   ```
   /opt/napatech/bin/TimeConfig  -cmd time_get
   ```

   Multi-Port Monitor のシステム時間を確認するには、端末から以下のコマンドを使用します。

   ```
   date
   ```

   2 つの時間が異なっていて、Multi-Port Monitor のシステム ステータス ページに警告メッセージが表示されている場合は、Napatech カードと NTP （Network Time Protocol）サーバの時間を確認します。

   以下の Web サイトでタイム ゾーンを選択して、NTP 時間を取得します。

   ```
   http://www.time.gov/
   ```

   以下のシナリオを検討し、状況へ適用するものを決定します。

   シナリオ 1

   状態

   - Napatech カードの時間が、NTP 時間と**大幅**に異なります（15 分を超える差）。
   - Multi-Port Monitor 上のシステム時間が、NTP 時間とほとんど変わりません（5 秒未満の差）。

アクション

- 以下のコマンドを実行して、NapaTech の時間をシステム クロックと同期します。
  `/opt/NetQoS/scripts/syncNapatechClock`
- Napatech の時間と Multi-Port Monitor のシステム時間との差が 5 分**未満**の場合は、Napatech ドライバ OS の同期により、徐々に Napatech のクロックが調整されます。Napatech の時間と Multi-Port Monitor のシステム時間との差が 5 分を**超える**場合は、Napatech の時間は直ちに Multi-Port Monitor のシステム時間と同期されます。

シナリオ 2

状態

- Napatech カードの時間が、NTP 時間とほとんど変わりません。
- Multi-Port Monitor 上のシステム時間および CEM コンソール時間が、NTP 時間と大幅に異なります。

アクション

- CEM コンソール時間を NTP 時間と同期するように調節します。
- 待機して、Multi-Port Monitor 上のシステム時間が設定され、NTP 時間とも同期していることを確認します。
- Multi-Port Monitor 上の ntpd プロセスが実行されていることを確認します。 実行されていない場合は開始します。

  Multi-Port Monitor 上のシステム時間と NTP 時間との差が 1000 秒を越えているとき、ntpd プロセスは自動的に停止できます。

シナリオ 3

状態

- Napatech カードの時間が、NTP 時間と**大幅**に異なります。
- Multi-Port Monitor 上のシステム時間および CEM コンソール時間も、NTP 時間と**大幅**に異なります。

アクション

- CEM コンソール時間を NTP 時間と同期するように調節します。
- 待機して、Multi-Port Monitor 上のシステム時間が設定され、NTP 時間とも同期していることを確認します。
- Multi-Port Monitor 上の ntpd プロセスが実行されていることを確認します。 実行されていない場合は開始します。
- 以下のコマンドを実行して、Napatech の時間をシステム クロックと同期します。
  ```
  /opt/NetQoS/scripts/syncNapatechClock
  ```