設定ユーティリティ ユーザ ガイド

CA Application Delivery Analysis

10.1

ca technologies

CA Technologies 製品リファレンス

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

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

CA への連絡先

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

目次

第 1 章: 概要 7

設定ユーティリティを実行する場所 8
スイッチ ポート ミラーリング要件 9
パケット キャプチャ ファイル要件 10
設定ユーティリティの開始 11
ステータス情報 13

第 2 章: 対象トラフィックの検索 15

リストについて 16
　リストのリフレッシュ 17
　定義済みのエントリを非表示にする 18
　フィルタリング基準 20
アプリケーションのフィルタ 22
ネットワークのフィルタ 23
フィルタ サーバ 25
サーバの定義 27
ネットワークの定義 28

第 3 章: 設定の保持 31

第 4 章: トラブルシューティング 33

第 1 章: 概要

設定ユーティリティは、監視デバイスにミラーリングされる TCP セッションを特定します。通常、この情報はネットワーク全体を流れるトラフィックが明確でない場合に最も役に立ちます。 たとえば以下のカテゴリでトラフィックを検索します。

- サーバ サブネット
- サーバ VLAN
- クライアント ネットワーク

目的のトラフィックが見つかったら、サーバおよびネットワークの定義を CA ADA コンソールにエクスポートし、トラフィックの監視を開始します。設定ユーティリティは、ユーザ定義のアプリケーションを作成しません。

設定ユーティリティを実行する場所

CA ADA セットアップ プログラムは、設定ユーティリティ（ConfigurationUtility.exe）を <ADA_HOME>¥bin フォルダにインストールします。 トラフィックが監視される場所に応じて、設定ユーティリティを実行する場所が変わります。 以下の場所から監視する場合：

管理コンソール

設定ユーティリティは管理コンソール上で実行します。

Standard Monitor

設定ユーティリティは Standard Monitor 上で実行します。

Multi-Port Monitor

設定ユーティリティは管理コンソール上で実行します。

Multi-Port Monitor から設定ユーティリティに大量のトラフィックが送信される場合があります。 したがって、2 台のコンピュータをできるだけ近くに置いておく必要があります。

Cisco NAM

管理コンソール上の Cisco NAM からパケット キャプチャ ファイルを開きます。

GigaStor

管理コンソール上の GigaStor からパケット キャプチャ ファイルを開きます。

スイッチ ポート ミラーリング要件

サーバとクライアント間のアプリケーション ポート トラフィックを検出するには、設定ユーティリティが SYN-ACK パケットを観測できる必要があります。 クライアント リクエストを確認する SYN-ACK パケットは、TCP セッションのサーバ側から送信されます。 設定ユーティリティは、SYN-ACK パケットを観測して、そのアプリケーション、サーバおよびネットワーク リスト内の対応する TCP セッション データを表示する必要があります。

設定ユーティリティが、サーバ側のトラフィックのみを表示する場合（たとえば「サーバへのバイト数」ではなく「サーバからのバイト数」のみ）、ルーティングが非対称の可能性があります。 *非対称のルーティング*は、TCP セッションの一方向が、ミラーリングしているポートを流れていない場合に発生します。アプリケーションの TCP レスポンス時間を正しく監視するには、ポートを監視デバイスにミラーリングすることが必要な場合があります（たとえば TCP セッションのクライアント側を観測する冗長スイッチから）。

パケット キャプチャ ファイル要件

Cisco NAM または GigaStor 上でデータ収集を設定するには、設定ユーティリティの要件として、監視デバイス上で取得したパケット キャプチャ ファイルからネットワーク、サーバ、アプリケーションのデータをロードする必要があります。 パケット キャプチャ ファイルを使用する場合は、以下の点に注意してください。

- 設定ユーティリティでは、パケット キャプチャ ファイルが NA（DOS）形式である必要があります。 BNF 形式はサポートされていません。 キャプチャ ファイル形式を変換する任意のユーティリティを使用して、NA Sniffer （DOS）形式でファイルを保存します。
- CA ADA パケット ドライバとの競合を防ぐには、*WireShark* などのパケット キャプチャ ユーティリティを、CA ADA 管理コンソールまたは標準モニタにインストールしないでください。

パケット キャプチャ ファイルを準備するには、**次の手順に従ってください：**：

1. Cisco NAM または CA GigaStor で、パケット キャプチャを取得し、結果をファイルに保存して、ローカル コンピュータにファイルをダウンロードします。

   CA GigaStor 上でパケット キャプチャを取得している場合、CA Observer Expert のみを使用して、サーバ ベースの通信をキャプチャするために SYN および SYN-ACK パケット用のフィルタ ルールを作成できます。CA Observer Expert を使用する詳細については、CA Observer Expert のヘルプを参照してください。

2. キャプチャ ファイル形式を変換する任意のユーティリティを使用して、パケット キャプチャ ファイルを開いた後、NA Sniffer （DOS）形式でファイルを保存します。

3. キャプチャ ファイルが NA Sniffer（DOS）形式であることを確認するには、ファイルの最初の行が TRSNIFF データから始まることを確認します。 コマンド プロンプトから以下のコマンドを入力し、Enter キーを押します。
   ```
   type <file name>.cap | more
   ```

4. 設定ユーティリティを実行する予定のコンピュータに、NA Sniffer （DOS）形式でパケット キャプチャ ファイルをコピーします。

設定ユーティリティの開始

設定ユーティリティを開始する前に、以下の点に留意してください。

- 設定ユーティリティを開始する場合、データ収集は監視デバイス上で一時的に停止します。 たとえば、Standard Monitor 上で設定ユーティリティを 1 時間実行する場合、監視デバイスによって収集されたデータには 1 時間のギャップがあります。
- パケット キャプチャ ファイルをロードするには、設定ユーティリティで、パケット キャプチャ ファイルが NA （DOS）形式である必要があります。
- リソースの消費を削減するため、設定ユーティリティを使用していない場合は閉じてください。

次の手順に従ってください:

1. 管理コンソール または CA Standard Monitor コンピュータで、<ADA_HOME>¥bin フォルダを参照し、ConfigurationUtility.exe をダブルクリックします。

   設定ユーティリティのログイン画面で 管理コンソール の IP アドレスが自動検出されます。

2. CA Standard Monitor 上でのデータ収集を設定する場合：

   a. 管理コンソール および CA Standard Monitor の IP アドレスが自動入力されます。

   b. たとえば、非対称のトラフィックを監視するために 監視 が複数の NIC で設定される場合は、すべての NIC 上のトラフィックを観測するために［All Adapters］チェック ボックスをオンにします。 このオプションは CA Multi-Port Monitor には適用されません。

   c. ［Start Detection］をクリックします。

3. CA Multi-Port Monitor でのデータ収集を設定している場合：

   a. ［Console］フィールドで、管理コンソール の IP アドレスを検証します。

   b. ［Collector IP］フィールドで、CA Multi-Port Monitor の IP アドレスを指定します。

   c. ［Start Detection］をクリックします。

   d. 設定する論理ポートを選択し、［OK］をクリックします。

4. Cisco NAM または CA GigaStor 用のデータ収集を設定している場合、管理コンソール の IP アドレスを検証し、デバイスから取得したパケット キャプチャ ファイルをロードします。
   a. ［Load Capture File］をクリックします。
   b. ［Browse］ダイアログ ボックスで、パケット キャプチャ ファイルの場所を NA Sniffer （DOS）形式で指定し、［OK］をクリックします。
   c. 設定ユーティリティのログイン画面で、［Process File］をクリックします。
5. 監視デバイス上でデータ収集を一時的に無効にする前に、設定ユーティリティはユーザに警告します。
6. ［OK］をクリックします。
7. 設定ユーティリティで［Refresh］メニューをクリックして、検出されたネットワーク、サーバおよびアプリケーションを表示します。 設定ユーティリティは、自動的にリストをリフレッシュしません。
8. 目的のトラフィックを見つけることが可能になりました。

ステータス情報

設定ユーティリティ下部のステータス バーは有用な情報を提供します。ステータスは以下のとおりです。

接続済み

ユーティリティが接続されているかどうか、またどの 管理コンソールと接続されているかを示します。

リスニング

監視対象ローカル アダプタの IP を示します。

検出された組み合わせ/パケット

（SPAN データのみ）観測されたクライアント/サーバ/ポートの組み合わせの最新数を示します。 この情報は、監視 が SPAN データを観測しているかどうかを判断する場合に役に立ちます。パケット キャプチャ ファイルを読み取るとき、組み合わせ数は変わりません。

現在

現在の時刻を示します。

最終リフレッシュ

リフレッシュが発生し、累積データによって表示が更新された最後の時刻を示します。

開始

ユーティリティが開始されたか再起動された最後の時刻を示します。

第 2 章: 対象トラフィックの検索

アプリケーション、サーバ、およびネットワークのリストをフィルタして関連エントリを見つけ、興味のあるトラフィックを検索します。 たとえば、以下によってフィルタします :

アプリケーション

関連するサーバおよびネットワークを表示します。

サーバ

関連するアプリケーションおよびクライアント ネットワークを表示します。

ネットワーク

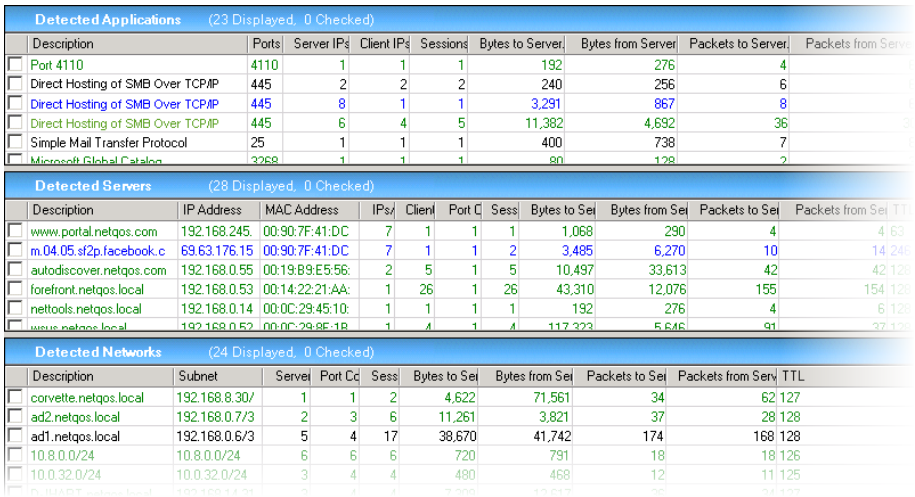
関連するサーバおよびアプリケーションを表示します。

リストについて

［リフレッシュ］をクリックし、現在検出されているネットワーク、サーバ、およびアプリケーションを表示します。 設定ユーティリティは、自動的にリストをリフレッシュしません。

色分けされたエントリ リストは、アプリケーション、サーバ、およびネットワーク エントリのステータスを示します。 以下の例では、トラフィックは CA ADA によって監視されていません。

重要: ［Bytes From］または［Bytes To］列が 0 のときは、TCP パケットがスイッチ ポートからミラーリングされる方法に問題があることを示している可能性があります。



ステータスは以下のとおりです。

未設定（黒）

設定ユーティリティが 監視デバイス またはパケット キャプチャ ファイル上でエントリを検出しましたが、設定ユーティリティまたは 管理コンソール 内にそのエントリ用の定義がないことを示しています。設定ユーティリティを使用して、エントリの定義を設定します。

管理コンソールで設定済み（緑）

エントリの定義が CA ADA に存在することを示します。 サーバまたはネットワークの定義を編集するには、CA ADA 管理コンソールを使用します。

設定ユーティリティで設定済み（青）

エントリの定義が管理コンソールではなく 設定ユーティリティ内に存在することを示します。 設定ユーティリティを使用して、エントリの定義を編集します。

未設定のサーバが設定済み（緑）のアプリケーションと同じポート上で通信する場合、アプリケーション ポートは、設定済み（緑）および未設定（黒）の両方のエントリとして 2 回表示されますので注意してください。 ［Detected Applications］のリストを［Port］によってソートし、重複したポート エントリを特定します。

リストのリフレッシュ

設定ユーティリティ レポートは、スイッチ ポートからミラーリングされるトラフィックをレポートしますが、最新のステータスを表示するにはリストを手動でリフレッシュする必要があります。

アプリケーション、サーバ、またはネットワークが非表示になったり、ボリュームが小さくなった場合は、1 つ以上のサーバが［Maximum IPs/MAC］しきい値を超えたことが原因と思われます。 それらのサーバからの統計は、関連付けられたアプリケーションおよびネットワークの方にはカウントされません。もしカウントした場合、合計が減少したり、ゼロに減った時に完全に表示されなくなることがあります。［Maximum IPs/MAC］フィルタを増やしたり、［All］にするとこれらのエントリが再度表示されます。

パケット キャプチャ ファイルをロードし、ビューをリフレッシュした後、設定ユーティリティはパケット キャプチャ ファイルの内容を表示します。再度ビューをリフレッシュする必要はありません。

次の手順に従ってください:

- ［Refresh］メニューをクリックします。

詳細:

ステータス情報 (P. 13)

定義済みのエントリを非表示にする

すでに定義されているエントリを非表示にすることにより、アプリケーション、サーバ、およびネットワークのリストをより簡単に参照できるようにします。

重要: エントリを非表示にしている場合、サーバまたはネットワーク定義を作成することはできません。 非表示にした場合は、すべてのエントリが表示されていることを確認します。

フィルタ方法

すべてのアプリケーション、サーバ、およびネットワーク エントリ

- ［View］-［All］-［Display All］をクリックして、フィルタを削除してエントリをすべて表示します。 定義を作成するには、すべてのアプリケーション、サーバ、およびネットワーク エントリが表示されるようにビューを設定する必要があります。
- ［View］-［All］-［Ignore Configured］をクリックして、未設定（黒）エントリをすべて表示します。設定ユーティリティで設定されている（青）か、管理コンソール で設定されている（緑）エントリは表示されません。
- ［View］-［All］-［Configured Only］をクリックして、設定ユーティリティで設定されている（青）または 管理コンソール で設定されている（緑）すべてのエントリを表示します。 未設定のエントリ（黒）は表示されません。

アプリケーション、サーバ、またはネットワークのエントリ別

- ［View］-［Applications|Servers|Networks］-［Display All］をクリックして、アプリケーション、サーバ、またはネットワーク エントリをすべて表示します。
- ［View］-［Applications|Servers|Networks］-［Ignore Configured］をクリックして、未設定（黒）のアプリケーション、サーバ、またはネットワークのエントリをすべて表示します。設定ユーティリティで設定されている（青）か、管理コンソール で設定されている（緑）エントリは表示されません。
- ［View］-［Applications|Servers|Networks］-［Configured Only］をクリックして、設定ユーティリティで設定されている（青）、または 管理コンソール で設定されている (緑) すべてのアプリケーション、サーバ、またはネットワーク エントリを表示します。 未設定のエントリ（黒）は表示されません。

フィルタリング基準

検出条件グループは、現在のビューに適用されるフィルタ条件を表示します。

アプリケーション フィルタ

フィルタ条件：

- 単一ポート（80）。 特定のアプリケーション ポートをフィルタするには、［Detected Applications］のリストで右クリックし、［Apply description (port) as Application Filter］をクリックする方法もあります。
- ポートの範囲（1024-2000）。

サーバ フィルタ

フィルタ条件：

- 単一 IP アドレス（192.168.0.10）。 特定のサーバをフィルタするには、［Detected Servers］または［Detected Networks］のリストで右クリックし、［Apply description (IP) as Server Filter］をクリックする方法もあります。
- IP アドレスの範囲（192.168.0.0-192.168.0.255）。
- サブネット（192.168.0.0/24）。

  タグ付けされた VLAN トラフィックをフィルタする場合、［Server Filter］の［Group By Mask］を特定の VLAN に対応するサーバ サブネットに設定します。 または、［Group By Mask］をサーバ（/32）に設定すると、タグ付けされた VLAN トラフィックがすべて表示されます。

［Maximum IPs/MAC］は、同じ MAC アドレスを共有するサーバからのデータをフィルタアウトします。 比率が高ければ、サーバがルータの反対側に、CA ADA の監視対象ではないことを示している可能性があります。 この比率は、［Detected Servers］パネルの［IP/MAC］列に表示されます。 このフィルタをオフにする［All］という値が、このリストの最上部にあります。

以前は表示されていた検出済みアプリケーション、サーバ、またはネットワークがその後のリフレッシュで非表示になった場合、データに関連付けられたサーバが［Maximum IPs/MAC］フィルタを超えている可能性があります。

ネットワーク フィルタ

フィルタ条件：

- 単一 IP アドレス（192.168.0.10）。特定のネットワークをフィルタするには、ネットワークまたはサーバのリストで右クリックし、［Apply description (IP) as Network Filter］をクリックする方法もあります。
- IP アドレスの範囲（192.168.0.0-192.168.0.255）。
- サブネット（192.168.0.0/24）。

［Group By Mask］は、検出された（ただし未設定の）クライアント IP をサブネットに編成する方法を定義します。 たとえば、3 つのクライアント IP（192.168.0.2、192.168.1.3、192.168.1.23）が検出され、［Group By Mask］設定が 24 であると仮定します。これらの IP は、192.168.0.0/24（192.168.0.2）および 192.168.1.0/24（192.168.1.3 および 192.168.1.23）の 2 つのネットワークに編成されます。

アプリケーションのフィルタ

アプリケーションとは、TCP ポートまたはポートの範囲に関する 1 セットのリクエストとレスポンスです。設定ユーティリティは、サーバ上のポート トラフィックを自動検出し、［Detected Applications］ペイン内のアプリケーション ポートを表示します。

アプリケーション ポートにアプリケーション フィルタを適用して、これらのポートにアクセスするネットワークを持つサーバを特定します。 たとえば、ポートをフィルタすると、関連付けられたサーバおよびネットワークのリストが表示されます。

このリストを並べ替えるには、列見出しをクリックします。

説明

アプリケーション ポートの名前を表示します。 設定済みアプリケーション（緑）と未設定アプリケーション（黒）の両方で同じアプリケーション名がリスト表示されている場合、アプリケーション ポート上にトラフィックがあっても CA ADA によって監視されないサーバがあります。

バイト数（受信側）、バイト数（送信側）、パケット数（受信側）、パケット数（送信側）

トラフィックが最も多いアプリケーションを表示します。ベストプラクティスとして、最もビジーなアプリケーションを監視することをお勧めします。

次の手順に従ってください:

1. ［Detected Applications］ペインで、ポートを右クリックし、［Apply description (port) as Application Filter］をクリックします。

   ポート範囲によってアプリケーションをフィルタする場合は、アプリケーション フィルタ検出条件フィールドで、ポート範囲（たとえば 60-80）を入力し、Enter キーを押します。

2. （オプション）ネットワークまたはサーバの定義を CA ADA に追加します。

詳細:

サーバの定義 (P. 27)
ネットワークの定義 (P. 28)

ネットワークのフィルタ

ネットワークとは、特定の場所またはユーザの論理グループを表す、IP アドレス範囲または 1 つの IP アドレスです。 設定ユーティリティはクライアント IP を自動検出し、現在の［Group By Mask］設定に従って［Detected Networks］ペインにそれらを表示します。 たとえば、［Group By Mask］が 24 に設定されている場合、設定ユーティリティは未設定のクライアント IP を /24 ネットワークにグループ化します。

ネットワークをフィルタする場合、/24 ネットワークのフィルタリングをお勧めします。 /24 クライアント ネットワーク（1 つの領域）を定義すると、ユーザに対する QoS レポートで、ネットワーク上の実際のクライアント IP を一覧できます。 特定の /24 ネットワーク用の検出済みクライアント IP を表示するには、希望の /24 ネットワークにネットワーク フィルタを配置した後、［Group By Mask］を 32 に設定します。

ネットワーク リストを並べ替えるには、列見出しをクリックします。

バイト数（受信側）、バイト数（送信側）、パケット数（受信側）、パケット数（送信側）

トラフィックが最も多いネットワークを表示します。 ベストプラクティスとして、最もビジーなネットワークを監視することをお勧めします。

TTL

ネットワーク内のすべてのクライアントからすべての表示されたサーバへの生存時間（TTL）値を表示します。 サーバの TTL 値と異なり、監視対象ネットワークはデフォルト以外のさまざまな値を持つことがあり、またそれが普通です。

対象のネットワークを見つけるにはフィルタリングを使用します。

ネットワーク フィルタ

クライアント ネットワークがアクセスするサーバおよびポートをリスト表示します。たとえば、クライアント ネットワークにネットワーク フィルタを適用すると、ネットワーク フィルタ条件にネットワークが追加され、関連付けられたサーバおよびアプリケーション ポートのリストが表示されます。

サーバ フィルタ

サーバ サブネット上のすべてのアプリケーションをリスト表示します。たとえば、サーバ フィルタ 192.168.0.0/16 を適用すると、そのサーバ サブネット上のサーバとアプリケーションが表示されます。

次の手順に従ってください:

1. ［Detected Networks］ペインで、ネットワークを右クリックし、［Apply *network (network) as* Network Filter］または［Apply *network (network) as* Server Filter］をクリックします。

   IP 範囲またはサブネットによってサーバをフィルタする場合は、ネットワーク フィルタ検出条件フィールドに IP 範囲またはサブネットを入力し、Enter キーを押します。

2. （オプション）ネットワークまたはサーバの定義を CA ADA に追加します。

フィルタ サーバ

サーバは、クライアント TCP リクエストに応答するネットワーク上のコンピュータです。設定ユーティリティは SYN-ACK パケットを検出し、対応するサーバを［Detected Servers］ペインに自動的に表示します。

サーバ トラフィックを監視するためにサーバ サブネットを定義することをお勧めします。

このリストを並べ替えるには、列見出しをクリックします。

バイト数（受信側）、バイト数（送信側）、パケット数（受信側）、パケット数（送信側）

トラフィックが最も多いサーバを特定します。ベストプラクティスとして、最もビジーなサーバ上のアプリケーションを監視することをお勧めします。［Bytes From］または［Bytes To］列が 0 のときは、TCP パケットが監視デバイスにミラーリングされる方法に問題があることを示している可能性があります。

VLAN

タグ付けされたサーバ VLAN トラフィックを特定します。

タグ付けされた VLAN トラフィックをフィルタする場合、［Server Filter］の［Group By Mask］を特定の VLAN に対応するサーバ サブネットに設定します。 または、［Group By Mask］をサーバ（/32）に設定すると、タグ付けされた VLAN トラフィックがすべて表示されます。

TTL

サーバからクライアントへの生存時間（TTL）の観測値を示します。理想的な設定では、監視対象サーバは 監視 によって直接測られ、しかもこの値がデフォルトの減分しない TTL 値である必要があります。 128 と 64 は、それぞれ Windows と UNIX サーバに対する共通の TTL 値です。

TTL がデフォルト値でない場合、デフォルトと値の間の差は、サーバと測定対象スイッチの間のネットワーク ホップ数です。ベストプラクティスとして、測定対象スイッチに最も近いサーバを監視することをお勧めします。 生存時間（TTL）列を使用して、監視対象の候補を見つけます。

Maximum IPs/Mac および Group By Mask

フィルタ結果を調整します。 SPAN 内のサーバをすべて参照する場合は［All］に設定し、MAC アドレス 1 つあたりの IP アドレスの比率が低いサーバを探します。

対象のサーバを見つけるにはフィルタリングを使用します。

サーバ フィルタ

サーバにアクセスするクライアント ネットワーク、およびアクセスされるアプリケーション ポートをリスト表示します。 たとえば、サーバにサーバ フィルタを適用すると、サーバ フィルタ条件にサーバが追加され、関連付けられたアプリケーション ポートおよびクライアント ネットワークのリストが表示されます。

VLAN ベースの SPAN （VSPAN）で、VLAN 列を使用して SPAN 内のサーバを検索するか、または対象のサーバ トラフィックを持つ VLAN に対応するサーバ サブネット マスクでフィルタします。 たとえば、サーバ フィルタ 192.168.0.0/16 を追加すると、そのサブネット上のサーバとアプリケーションがすべて表示されます。

ネットワーク フィルタ

サーバが別のサーバに対するクライアントとして機能しているかどうか、および使用されているポートを示します。 多層アプリケーションを監視する場合は、CA ADA が各サーバ定義の /32 ネットワークを自動作成することに留意してください。 たとえば、サーバにネットワーク フィルタを適用すると、ネットワーク フィルタ条件にサーバが追加され、関連付けられたサーバおよびアプリケーション ポートのリストが表示されます。 このフィルタは多層アプリケーションを検出するのに役立ちます。

［Group By Mask］リストから希望のマスクを選択することにより、一致するネットワークをグループ化します。

次の手順に従ってください:

1. ［Detected Servers］ペインで、サーバを右クリックし、［Apply description (port) as Server Filter］または［Apply description (port) as Network Filter］をクリックします。

   IP 範囲またはサブネットによってサーバをフィルタする場合は、サーバ フィルタ検出条件フィールドに IP 範囲またはサブネットを入力し、Enter キーを押します。

2. （オプション）サーバまたはネットワークの定義を CA ADA に追加します。

サーバの定義

最もビジーな対象のサーバをまず定義することをお勧めします。 VLAN ベースの SPAN （VSPAN）で、VLAN 列を使用して SPAN 内のサーバを検索するか、または対象のサーバ トラフィックを持つ VLAN に対応するサーバ サブネット マスクでフィルタし、サーバのリストをソートして最もビジーなサーバを見つけます。 最もビジーなサーバを特定したら、サーバ フィルタを適用して、最もビジーなアプリケーションに対応するサーバ上のアプリケーション ポートを特定します。

サーバを定義する場合は、以下の命名規則を使用することをお勧めします。

サーバ タイプ	推奨命名規則	例
単一機能サーバ	*DNSName* CA ADA、CA PC および CA NPC 内の多くのレポート ビューが IP アドレスを追加することに注意してください。	Goliath-196.128.34.1
ファームに複数のサーバ、1 つのアプリケーション	*ApplicationName-DNSName* アプリケーション名を識別しやすくするには、サーバ フィルタを適用して、対応するアプリケーション ポートを検索します。	Citrix-Zeus Citrix-Athena Citrix-Mercury
1 つのアプリケーション、複数のサーバ、複数の場所	*ApplicationName-DNSName-Location* アプリケーション名を識別しやすくするには、サーバ フィルタを適用して、対応するアプリケーション ポートを検索します。	Citrix-Hamlet-NewYork Citrix-Romeo-Milan Citrix-Othello-London

次の手順に従ってください:

1. ［Detected Servers］ペインでサーバを右クリックし、［Define Server Subnet *description*］をクリックします。

   サーバのグループを定義するには、対象の各サーバのチェック ボックスをオンにした後、サーバを右クリックし、［Quick Define Checked Servers］をクリックします。

2. ［Export］-［To Management Console］をクリックし、CA ADA に変更を保存します。

   重要: 新しい定義の監視を開始するには、CA ADA 内の監視デバイスを同期します。

詳細:

フィルタ サーバ (P. 25)

ネットワークの定義

環境内の実際のクライアント サブネットワークに対応するクライアント ネットワークを定義します。 クライアント トラフィックをフィルタするために［Group By Mask］を設定します。

ネットワークを定義する場合は、以下の命名規則を使用することをお勧めします。

ネットワーク タイプ	推奨命名規則	例
ネットワーク	*Location-Description*	Singapore-backbone
サブネットワーク	*Location-Region-Bandwidth*	Austin-Subnet10-128k

次の手順に従ってください:

1. ［Detected Networks］ペインでネットワークを右クリックし、［Define Network *description*］をクリックします。

   ネットワークのグループを定義するには、対象の各ネットワークを選択した後、ネットワークを右クリックし、［Quick Define Checked Networks］をクリックします。

2. ［Export］-［To Management Console］をクリックし、CA ADA に変更を保存します。

   重要: 新しい定義の監視を開始するには、CA ADA 内の監視デバイスを同期します。

詳細:

ネットワークのフィルタ (P. 23)

第 3 章: 設定の保持

ネットワーク上のトラフィックを特定するために設定ユーティリティを定期的に使用することをお勧めします。

第 4 章: トラブルシューティング

このセクションでは、よく発生する質問について説明します。

- タグ付けされた VLAN トラフィックが見つかりません。 なぜですか。

  タグ付けされた VLAN トラフィックをフィルタする場合、［Server Filter］の［Group By Mask］を特定の VLAN に対応するサーバ サブネットに設定します。 または、［Group By Mask］をサーバ（/32）に設定すると、タグ付けされた VLAN トラフィックがすべて表示されます。

- 下部のインジケータは検出済みパケット数が多いことを示しています。しかし、設定ユーティリティはキャプチャしたデータを全く表示しません。 なぜですか。

  これは、1 つ以上のサーバが［Maximum IPs/MAC］しきい値を超えたことが原因と思われます。 それらのサーバからの統計は、関連付けられたアプリケーションおよびネットワークの方にはカウントされません。もしカウントした場合、合計が完全に表示されなくなることがあります。 ［Maximum IPs/MAC］フィルタを増やしたり、［All］にすると、これらのエントリが表示されます。

- ［Refresh］をクリックすると、アプリケーション、サーバ、またはネットワークが表示されなくなったり、ボリュームが減少しました。 これはバグですか。

  これは、1 つ以上のサーバが［Maximum IPs/MAC］しきい値を超えたことが原因と思われます。 それらのサーバからの統計は、関連付けられたアプリケーションおよびネットワークの方にはカウントされません。もしカウントした場合、合計が減少したり、ゼロに減った時に完全に表示されなくなることがあります。 ［Maximum IPs/MAC］フィルタを増やしたり、［All］にするとこれらのエントリが再度表示されます。

- CA Multi-Port Monitor に接続すると例外が発生するのはなぜですか。

  設定ユーティリティを CA Multi-Port Monitor に接続しようとして以下のメッセージが表示された場合は、設定ユーティリティを終了し、監視デバイスを同期してから、設定ユーティリティを再接続してください。

  `System.Exception： There is already one SuperAgent Configuration Utility request in process.`

  この問題を回避するには、CA Multi-Port Monitor の論理ポート上でアプリケーション、サーバ、ネットワークの定義を完了したときに、別の論理ポートの設定を試行する前に、設定ユーティリティの接続を切断し、監視デバイス上の設定を同期します。

- 設定ユーティリティを開始すると例外が発生するのはなぜですか。

  コンピュータの、設定ユーティリティを実行する場所は 管理コンソール や CA Standard Monitor もホストする必要があります。そうしないと、次のメッセージが表示されます。

  `System.NullReferenceException`： オブジェクト参照がオブジェクトのインスタンスに設定されていません。

- 監視 に対し SPAN に問題があるかどうかは分かりますか。

  ［Bytes From］または［Bytes To］列が 0 のときは、TCP パケットが監視デバイスにミラーリングされる方法に問題があることを示している可能性があります。

- 検出済みネットワーク内でオーバラップするサブネットはどのように編成されますか。

  2 つのネットワーク定義がサブネット 192.168.0.0/16 と 192.168.10.0/24 で存在すると仮定します。 /24 は /16 の中に含まれていますが、データも /24、/16、または両方に格納されていますか。 CA ADA コンソールと設定ユーティリティの両方について回答は同じです。より詳細な（高い方の /x）ネットワーク定義がデータを取得します。

  前の例で、192.168.10.0/24 は範囲が 192.168.10.0 ～ 192.168.10.255 の IP からデータを取得します。一方、192.168.0.0/16 は範囲が 192.168.0.0 ～ 192.168.9.255 および 192.168.11.0 ～ 192.168.255.255 の IP からデータを取得します。

  より詳細なサブネット データ編成により、設定ユーティリティで推奨されるワークフローは、より綿密なサブネットを定義し、より広範囲（低い方の /x）なサブネットに解決することです。 0.0.0.0/0 など、広範囲なユーザ定義のサブネットを最初に作成してしまうと、すべてがその 1 つのエントリに集約され、より詳細なサブネットを作成することが難しくなります。

- 定義の追加や 管理コンソール へのエクスポートができないのはなぜですか。
  - 既存のコンソール設定エントリ（緑）は、ユーティリティでは変更できません。 これは、コンソールのユーザ インターフェースから実行する必要があります。
  - 検出されたが未設定のエントリ（黒）は追加できます。
  - ユーティリティ内に設定された（青）エントリのみは、編集および削除ができます。
  - ［All］以外のビュー メニューからのオプションが適用されると、定義の変更や 管理コンソール へのエクスポートが無効になります。 これは、設定ユーティリティと 管理コンソール の間の定義衝突を回避するために実行されます。

  一般に、クライアント ネットワークとサーバ サブネットのリストを更新し、監視するアプリケーション トラフィックを指定する必要があります。 CA ADA コンソールが期待するアプリケーション トラフィックを表示しない場合、設定ユーティリティを使用して、監視デバイスがアプリケーション トラフィックを観測しているかを確認します。

詳細:

スイッチ ポート ミラーリング要件 (P. 9)
設定ユーティリティを実行する場所 (P. 8)