レイヤ 3 のアウトオブバンドの NAC Profiler および NAC サーバ コレクタの設定ガイド

目次

概要

このドキュメントでは、レイヤ 3 のアウトオブバンドの導入で NAC Profiler および NAC Server Collector を実装する方法について説明します。 ハイ アベイラビリティ（HA）に NAC Server を配置すると、1 つの Collector のみアクティブになり、他はスタンバイになります。 HA を実装しない場合は、プロファイラに各コレクタを個別に追加し、両方の NAC サーバをコレクタとして実行することができます。 このガイドは、HA サーバ配置に関するものです。

前提条件

要件

このガイドの要件は、NAC マネージャ、NAC サーバ、NAC プロファイラ、およびネットワーク インフラストラクチャを、各製品のインストール ガイドや設定ガイドに従って設定済みであることです。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- NAC マネージャ
- NAC サーバ
- NAC プロファイラ
- 3750 ディストリビューション スイッチ
- 3750 リモート サイト アクセス スイッチ
- 2800 リモート サイト ルータ
- 3800 ディストリビューション ルータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

NAC Profiler の概要

Cisco NAC プロファイラを利用すれば、デバイス タイプにかかわらず、接続されたあらゆるネットワーク エンドポイントの機能を検出、検索、および特定できるので、ネットワーク管理者は、適切なネットワーク アクセスを確保し維持するために、スケールも複雑さもさまざまに異なる企業ネットワーク内に Network Admission Control（NAC; ネットワーク アドミッション コントロール）を効率的に展開し、管理することができます。 Cisco NAC プロファイラは、ネットワークに接続されたすべてのエンドポイントを発見、カタログ化、およびプロファイリングする、エージェントレス システムです。

NAC の概要

Cisco Network Admission Control（NAC）アプライアンス（別名 Cisco Clean Access）は、強力で使いやすい管理制御ソリューションであり、コンプライアンス適用ソリューションでもあります。 包括的なセキュリティ機能、インバンドまたはアウトオブバンドの配置オプション、ユーザ認証ツール、帯域およびトラフィックのフィルタリング制御機能を備えた Cisco NAC アプライアンスは、ネットワークを制御して保護するための完全なソリューションです。 Cisco NAC アプライアンスは、ネットワークの集中アクセス管理ポイントになるため、セキュリティ、アクセス、コンプライアンス ポリシーを一箇所で実装できます。ネットワークを通じて多くのデバイスにポリシーを伝播する必要はありません。

導入ガイドの概要

図 1 は、中央の HA NAC サーバがレイヤ 3 のアウトオブバンド デバイスに対する適用ポイントとして機能する、リモート サイトへのシンプルな導入例です。 NAC プロファイラおよび NAC マネージャは、同じ管理ネットワーク内に存在し、サーバおよびコレクタとの間で情報を送受信します。 また、データセンターまたはコア レイヤの SPAN を使用して、デバイスに関する必須の DHCP 情報を取得するスタンドアロンのコレクタも含まれています。 リモート エンドポイントは複数の方法で検出できます。このガイドは、導入環境に合わせてこれを行うのに役立ちます

。 必須のガイドではありませんが、コレクタ上の各モジュールの使用方法と、プロファイリングを自動で決定するためにプロファイラでエンドポイント データがどのように認識されるのかについて説明します。

NAC サーバ コレクタで使用する必須ツールとオプション ツールのリストを次に示します。

必須のコレクタ モジュール

NetTrap：このモジュールは、new-mac 通知やリンクアップ/リンクダウン通知としてスイッチから送信される SNMP トラップをリッスンします。 このモジュールは、新しい MAC アドレスのすべてを、プロファイリングのためにプロファイラに送信します。 この機能は、Cisco IOS® の SNMP-Server コンフィギュレーション コマンド ラインでスイッチごとに定義されます。

NetMap：このモジュールはコレクタ上に存在し、リモート ブランチ内のデバイスの SNMP ポーリングを一定間隔で実行します。 図 1 のダイアグラムでは、CAS1a のコレクタが、スイッチに対して読み取りアクセスを行い、特定の MIB 情報を対象にした SNMP ポーリングをリモート スイッチとルータに対して実行します。 このポーリングによって、MAC アドレスとポートの情報、インターフェイス、リンク ステータス、dot1x 情報、システム情報などを取得します。

NetWatch（SPAN）：NetWatch モジュールは、スイッチの SPAN ポートでリッスンし、取り込んだトラフィック情報をプロファイラに送信することができます。 NAC サーバでは、データを収集するために NAC SERVER ごとに追加のインターフェイスが必要になります。 プロファイラは、デバイスから渡される DHCP 情報などのアプリケーション トラフィック マッチングを主に使用するため、これは不可欠です。

オプションのコレクタ モジュール

SPAN または Netflow を使用できます。 導入要件と顧客要件にもよりますが、コレクタ モジュールに送信されるトラフィック量、および NAC サーバで実行する必要のある他の機能を考慮すると、NAC サーバ上にどちらか 1 つのみを使用することを推奨します。 また、NetFlow を使用すると、ベンダー情報、URL 接続先、Web クライアント情報、Web サーバ情報などの、デバイスに関する重要な情報も失われます。

NetRelay：（Netflow）は、各ルータ上にインターフェイス単位で設定され、接続先は NAC SERVER の管理 IP アドレスになります。 NetFlow エージェントは NAC サーバ上に存在し、プロファイラで設定されたトラフィック ルールとネットワークに基づいて NetFlow 情報を分析します。

NetInquiry：これは、開いている TCP ポートなどに基づいて、パッシブまたはアクティブに機能します。 たとえば、NAC SERVER は、開かれている TCP ポートがないか特定のサブネット範囲をポーリングするために、SYN/ACK を実行してから接続をドロップします。 応答があった場合、ポーリングした IP アドレスと TCP ポートについての情報をプロファイラに送信します。

注: NetInquiry では、NetFlow や NetWatch では到達/表示できない特定のサブネットまたはホストのみを追加してください。 NetInquiry が正しく設定されていない場合、余分な処理、メモリや CPU の使用率などのハードウェア リソースの余分な消費が原因で、NAC サーバが過負荷状態になる恐れがあります。 この機能は最後の手段として使用してください。

注: スタンドアロンのコレクタを使用する場合は、同一デバイス上で Netflow と SPAN の両方を有効にできますが、コレクタをオーバーサブスクライブしないように注意してください。

図 1

設定

レイヤ 3 OOB トポロジでの NAC プロファイラの設定

- NAC Server は標準の NAC HA セットアップを通して設定する必要があります。
- NAC コレクタは、プロファイラとの通信に NAC サーバの仮想 IP アドレスを使用します。
- NAC コレクタの HA ペアは、単一項目としてプロファイラに追加され、CAS の仮想 IP アドレスと通信します。

図 2

設定

次の手順を実行します。

1. プロファイラには、新しい NAC コレクタに対する *クライアント接続*が必要です。
2. プロファイラには、スタンドアロン デバイスに対する *サーバ接続*が必要です。このスタンドアロン デバイスは、ネットワーク図の中のディストリビューション|データセンター|サービス レイヤの近くに置かれています。
3. [Configuration] > [NAC Profiler Modules – List NAC Profiler Modules] の順に選択して、[Server] タブをクリックします。ページの一番下までスクロールし、[Add Connection] をクリックします。**図3**
4. HA コレクタのサービス IP アドレスと秘密キー情報を入力し、[Add Connection] をクリックします。**図 4**
5. [Add Connection] をもう一度クリックします。**図 5 図 6**
6. スタンドアロン コレクタが接続するサーバ接続を設定するために、IP アドレスを入力します。
7. 完了したら、[Server configuration] ページに戻るために、[Connection] を選択します。
8. [Server configuration] ページで **[Update Server]** をクリックします。**図 7**

プロファイラに新しいコレクタを 2 つ追加します。 次の手順を実行します。

1. [Configuration] > [NAC Profiler Modules] > [Add Collector] の順に選択します。**図 8**
2. NAC Server HA ペアの新しい Collector 名を追加します。 任意の名前を入力できますが、コレクタの設定と一致する必要があります。コレクタ名：CAS-OOB-Pair1IP アドレス：192.168.97.10（NAC サーバの仮想アドレス）Connection：ここでは [None] のままにしておきます。 リッスン モードのサーバ接続に後から変更できます。
3. [Add Collector] ボタンをクリックします。**図 9**
4. Collector サービス モジュールを設定します。 NetMap および NetTrap はそのままにします。**図 10**
5. ディストリビューション スイッチの SPAN ポートに接続された NetWatch インターフェイス（eth3）を追加します。**図 11**
6. アクセス ネットワークから送信される対象トラフィックをリッスンするために、NetInquiry モジュールのサブネット ブロックを追加します。 NAC サーバに不要な負荷をかけないように、ネットワークを細かく指定してください。 このラボ設定では、192.168.0.0 のプライベート空間全体を指定しています。**図 12 注:** ping スイープと DNS コレクションは無効のままにします。 これは最後の手段として使用してください。 ping スイープと DNS コレクションは、[Network Blocks] セクションに入力した IP サブネットの範囲に対して ping と nslookup をトリガーします。 これは推奨されておらず、ほとんど使用されません。

7. フォワーダを IP アドレス 192.168.97.10（VIP）および TCP ポート 31416 をリッスンするように設定します。 これにより、コレクタはサーバのように機能して、プロファイルから特定の TCP ポートへの接続をリッスンできます。 これはサーバの構成の最初のいくつかの手順に反映されます。
8. コレクタ ペアの NetFlow を有効にします。（オプション）リモート コレクタがないため、リモート ルータから Netflow が渡されるので、ここでこの手順を実行できます。
9. 図で示すように、リモート サイトの IP アドレス ブロックを入力します。 この例では、192.168.0.0 のプライベート空間全体を使用します。**図 13**
10. 設定を保存するために、[Save Collector] をクリックします。

プロファイラへのスタンドアロン コレクタの追加

次の手順を実行します。

1. [Add Collector] をクリックします。**図 14**
2. コレクタは任意の名前にすることができます。 この例では CAS2 です。
3. フォワーダの IP アドレスは自身のアドレスです。 eth0 の IP アドレスは管理用です。この例では 192.168.97.12 です。[Connection] には、Profiler の IP アドレスを指定する必要があります。 この例では 192.168.96.21 です。
4. [Add Collector] をクリックします。**図 15**
5. この後、コレクタの設定ページに移動します。 前の項の手順 5 ~ 9 を実行します。 これにより、スタンドアロン コレクタの一意の IP アドレスおよび構成設定を変更および追加できます。
6. スタンドアロン コレクタに特異的な設定の 1 つとして、NetWatch 設定に複数のインターフェイスを追加できます。 ここで複数のインターフェイスを追加すると、リモート エンドポイントからの DHCP、DNS、および IP テレフォニーのトラフィックを調べることができます。
7. このセットアップ用の NetWatch インターフェイスを設定します。 この例では、スタンドアロンのコレクタの SPAN トラフィックに、3 つのインターフェイスが追加されています。**図 16**
8. **注:** 設定を保存するために、[Configuration] > [Apply Changes] > [Update Modules] を選択します。

NAC サーバでの NAC コレクタ モジュールの設定

注: この設定はすべてのコレクタで実行する必要があります。

この設定により、プロファイラとコレクタが通信を行い、デバイスに関する情報の送信を開始するために必要なセキュアな接続を確立することができます。 次の手順を実行します。

1. SSH またはコンソールを使用してコレクタに接続し、コンソールから **root** としてログインするか、SSH セッションから**ビーコン**を実行します。
2. **service collector config** コマンドを入力します。
3. NAC のコレクタ部分を設定するために、設定スクリプトを通じて実行します。**HA コレクタの例**コレクタは、*サーバ接続*タイプとして設定されます。`[root@cas1 ~]#service collector config Enable the NAC Collector (y/n) [y]: Configure NAC Collector (y/n) [y]: Enter the name for this remote collector. Please note that if this collector exists on a HA pair that this name must match its pair's name for proper operation. (24 char max) [cas1]: CAS-OOB-Pair1 Network configuration to connect to a NAC Profiler Server Connection type`

(server/client) [server]: Listen on IP [192.168.97.10]: NPS の IP アドレスを入力するように求められます。 これは、このコレクタで使用するアクセス コントロール リストを設定するために必要です。 NPS が HA ペアの一部である場合は、フェールオーバー時に正常に接続できるように、各 NPS の実際の IP アドレスと仮想 IP を含める必要があります。 NAC プロファイラの IP アドレスを入力します。(Finish by typing 'done') [127.0.0.1]:
192.168.96.20 (Real IP address of NAC Server1)
Enter the IP address(es) of the NAC Profiler.
(Finish by typing 'done') [192.168.96.20]: 192.168.96.21 (Virtual IP of NAC Server)
Enter the IP address(es) of the NAC Profiler.
(Finish by typing 'done') [done]: 192.168.96.22 (Real IP of NAC Server2)
Enter the IP address(es) of the NAC Profiler.
(Finish by typing 'done') [done]: done
Port number [31416]:
Encryption type (AES, blowfish, none) [none]: AES
Shared secret []: cisco123
•Configured CAS-OOB-Pair1-fw
•Configured CAS-OOB-Pair1-nm
•Configured CAS-OOB-Pair1-nt
•Configured CAS-OOB-Pair1-nw
•Configured CAS-OOB-Pair1-ni
•Configured CAS-OOB-Pair1-nr

NAC Collector has been configured.

4. Collector サービスを起動します。[root@cas1 ~]#**service collector start** **スタンドアロン コレクタの例**[root@cas2 ~]#**service collector config** Enable the NAC Collector (y/n) [y]: Configure NAC Collector (y/n) [y]: Enter the name for this remote collector. Please note that if this collector exists on a HA pair that this name must match its pair's name for proper operation. (24 char max) [cas2]: Network configuration to connect to a NAC Profiler Server Connection type (server/client) [client]: Connect to IP [192.168.96.21]: Port number [31416]: Encryption type (AES, blowfish, none) [none]: Shared secret []: -- Configured cas2-fw -- Configured cas2-nm -- Configured cas2-nt -- Configured cas2-nw -- Configured cas2-ni -- Configured cas2-nr NAC Collector has been configured. [root@cas2 ~]#**service collector start**

NAC コレクタに SNMP トラップを送信するためのリモート アクセス スイッチの設定

この設定により、プロファイラは、MAC 通知トラップを通じて、スイッチポートに接続されたすべての新しいデバイスを動的に受信することができます。 このトポロジでは IP Phone と PC が同じポートに接続されているため、これが特に重要になります。

スイッチ (nac-3750-access#) に対して、コンソールまたは Telenet で接続します。

```
snmp-server community cleanaccess RW snmp-server community profiler RO snmp-server enable traps mac-notification snmp-server host 192.168.96.10 version 2c cleanaccess snmp-server host 192.168.97.10 version 1 profiler
```

SNMP 情報の収集に必要なプロファイラのリモート アクセス スイッチの設定

次の手順を実行します。

1. [Profiler GUI] > [Configuration] > [Network devices] > [Add Device] の順に選択します。**図 18**
2. スイッチのホスト名と管理 IP アドレスを追加します。
3. また、スイッチで設定されている読み取り専用の SNMP ストリングを入力します。 NAC コレクタのマッピング モジュールを選択してください。これにより、アクセス スイッチに対

して 1 時間おきに SNMP ポーリングを実行し、プロファイラに情報を送信するコレクタが選択されます。
4. GUI の左側のペインから、[Add Device] および [Apply Changes] をクリックし、モジュールを更新します。**図 19**

SNMP 情報の収集に必要なプロファイラのリモート アクセス ルータの設定

これにより、プロファイラ データベースでレイヤ 3 の IP アドレスと MAC のバインディングが可能になります。

1. [Profiler GUI] > [Configuration] > [Network devices] > [Add Device] の順に選択します。**図 20** 図 21 を参照してください。
2. ルータのホスト名と管理 IP アドレスを追加します。
3. また、ルータで設定されている読み取り専用の SNMP ストリングを入力します。 NAC コレクタのマッピング モジュールを選択してください。これにより、アクセス スイッチに対して 1 時間おきに SNMP ポーリングを実行し、プロファイラに情報を送信するコレクタが選択されます。
4. GUI の左側のペインから、[Add Device] および [Apply Changes] をクリックし、モジュールを更新します。**図 21**

ローカル スイッチで SPAN トラフィックを受信するための NAC コレクタの設定

注: これにより、NetWatch モジュールがネットワーク上のトラフィックをリッスンし、プロファイラに情報を転送し始めることができます。 NAC Collector のインターフェイスをオーバーサブスクライブしないようにします。 1 GB/sec の制限があります。 スイッチのインターフェイスまたは VLAN をソースにすることができます。これは、コードのスイッチ モデルおよびバージョンによって異なります。

注: アクセス スイッチでエンドポイントからの DHCP の要求およびオファーを最小限に調査する必要があります。 これが不可能な場合は、ネットワークの DHCP サーバの上または近くに、NAC コレクタを追加してみてください。 この構成ガイドではこの例を説明します。

次の手順を実行します。

1. リモート サイトの入出力トラフィックを監視するために、ディストリビューション スイッチ #1 にモニタ セッションを設定します。`monitor session 1 source interface F0/0`
`monitor session 1 destination interface Gi1/0/44`
2. リモート サイトの入出力トラフィックを監視するために、ディストリビューション スイッチ #2 に複製モニタ セッションを設定します。`monitor session 1 source interface F0/0`
`monitor session 1 destination interface Gi1/0/44`
3. スタンドアロンのコレクタに対して別のモニタ セッションを設定します。 この例では、コア スイッチに接続された重要な複数のインターフェイスを監視します。 監視対象は、このラボのセットアップの DHCP、DNS、CallManager サーバです。`monitor session 1 source interface G1/0/7-9`
`monitor session 1 destination interface G1/0/48`

メイン サイトのコレクタに NetFlow データを送信するためのリモート アクセス ルータの設定

次の手順を実行します。

1. リモート ルータに Telnet で接続します。
2. Netflow をグローバルにイネーブルにします。`ip flow-export version 5`
   `ip flow-export destination 192.168.97.12 2055`**注:** コレクタは、UDP ポート 2055 で NetFlow をリッスンします。 Netflow を送信する IP アドレスは、常にコレクタの管理 IP アドレスです。
3. インターフェイスで NetFlow をイネーブルにします。`interface FastEthernet0/1`
   `ip address 192.168.121.1 255.255.255.0`
   `ip flow ingress`
   `ip route-cache flow`

確認

設定が正常に機能していることを確認するには、「トラブルシューティング手順 」の項を参照してください。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

注: debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

トラブルシューティング手順

次の手順に従って、設定のトラブルシューティングを行います。

1. プロファイラとコレクタが通信して、機能していることを確認します。 機能していない場合、ネットワークのデバイスに関する情報は表示されません。 問題がある場合は、コレクタ モジュールとサーバがすべて機能するようになるまで先に進まないでください。プロファイラで、[Configuration] > [NAC Profiler Modules] > [List NAC Profiler Modules] の順に選択します。
2. アクセス スイッチがコレクタに対して new-mac 通知トラップを送信していることを確認します。 デバッグを有効にする場合は慎重に行ってください。そのリスクを理解していることが必要です。`nac-3750-access#`**`debug snmp packet`** `nac-3750-access#`**`debug snmp header`**
3. コレクタがスイッチに対して SNMP ポーリングを実行したことを確認します。[Last Scan] 列を確認します。
4. スイッチでもう一度 SNMP をデバッグします。
5. プロファイラから、[Configuration] > [Network Devices] の順に選択します。 [Network Devices] の一覧表示を選択し、[Device] を選択します。
6. [Query] を選択します。
7. スイッチのデバッグ出力を参照して、コレクタがスイッチに対して SNMP ポーリングを実行したことを確認します。`*Mar 30 23:09:24: SNMP: Packet` **`received via UDP from 192.168.97.11`** `on Vlan100 *Mar 30 23:09:24: SNMP: Get-next request, reqid 1347517983, errstat 0, erridx 0 ifType = NULL TYPE/VALUE *Mar 30 23:09:24: SNMP: Response, reqid 1347517983, errstat 0, erridx 0 ifType.1 = 53 *Mar 30 23:09:24: SNMP: Packet` **`sent via UDP to 192.168.97.11`**
8. スイッチに IP Phone を差し込むか、インターフェイスで **shut then no shut** コマンドを実行

します。15w4d: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/4, changed state to down
15w4d: %ILPOWER-5-POWER_GRANTED: Interface Gi1/0/4: Power granted
15w4d: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/4, changed state to up
15w4d: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/4, changed state to up
15w4d: SNMP: Queuing packet to 192.168.97.12
15w4d: Outgoing SNMP packet
15w4d: v2c packet
15w4d: community string: profiler
15w4d: SNMP: V2 Trap, reqid 14430, errstat 0, erridx 0
 sysUpTime.0 = 949829672
 snmpTrapOID.0 = cmnMacChangedNotification
 cmnHistMacChangedMsg.0 =
01 00 79 00 07 50 C6 82 27 00 04 00

9. コレクタが、受信した MAC アドレスに対する新しいトラップ要求を送信したことを確認します。15w4d: SNMP: Packet received via UDP from 192.168.97.11 on Vlan120
15w4d: SNMP: Get request, reqid 1576567642, errstat 0, erridx 0
 system.1.0 = NULL TYPE/VALUE
 ifIndex.10104 = NULL TYPE/VALUE
 ifDescr.10104 = NULL TYPE/VALUE
 ifType.10104 = NULL TYPE/VALUE
 ifSpeed.10104 = NULL TYPE/VALUE
 ifPhysAddress.10104 = NULL TYPE/VALUE
 ifAdminStatus.10104 = NULL TYPE/VALUE
 ifOperStatus.10104 = NULL TYPE/VALUE
 ifName.10104 = NULL TYPE/VALUE
 dot1xAuthAuthControlledPortStatus.10104 = NULL TYPE/VALUE
 dot1xAuthAuthControlledPortControl.10104 = NULL TYPE/VALUE
paeMIBObjects.2.4.1.9.10104 = NULL TYPE/VALUE

-------snip ----------
ifIndex.10104 = 10104
 ifDescr.10104 = GigabitEthernet1/0/4
 ifType.10104 = 6
 ifSpeed.10104 = 100000000
 ifPhysAddress.10104 = 00 14 A8 2E A5 04
 ifAdminStatus.10104 = 1
 ifOperStatus.10104 = 1
 ifName.10104 = Gi1/0/4
 dot1xAuthAuthControlledPortStatus.10104 = 1
 dot1xAuthAuthControlledPortControl.10104 = 3
15w4d: SNMP: Packet sent via UDP to 192.168.97.11

10. プロファイラが、コレクタから IP Phone の新しい MAC アドレスを受信したことを確認します。[Endpoint Console] > [View/Manage Endpoints] > [Display Endpoints by device ports] > [ungrouped] > [Table of Devices] の順に選択し、スイッチを選択します。
11. スイッチで SPAN が動作していること、および Collector がトラフィックを受信していることを確認します。SSH to the NAC Profiler :
Type : tcpdump –i eth3

16:54:36.432218 IP cas2.nacelab2.cisco.com.9308 > elab2-dns-dhcp.nacelab2.cisco.com.domain: 48871+ PTR? 68.39.168.192.in-addr.arpa. (44) 画面の出力を確認します。 出力量が心配な場合、出力を NAC Collector のファイルに保存できます。この操作方法については、Linux の man ページを参照してください。
12. IP Phone のエンドポイントに関する DHCP トラフィックが SPAN ポートによって認識され、プロファイラに送信されたことを確認します。[Endpoint Console] > [View/Manage Endpoints] > [Display Endpoints by device ports] > [ungrouped] > [Table of Devices] の順に選択し、スイッチを選択します。次に、デバイスの **MAC アドレス**を選択します。[View Profile Data] をクリックします。コレクタの NetWatch/SPAN トラフィックからキャプチ

ャされた、デバイスの DHCP ベンダー クラス情報が表示されるはずです。 この情報は、ルーティングや環境によって、DHCP サーバからのものである場合と、クライアントに戻された SPAN ポートの DHCP オファーである場合があります。

13. NetFlow がリモート ルータからコレクタの管理インターフェイスに渡されていることを確認します。`NAC-2800-Remote#`**`show ip flow export`** `Flow export v5 is enabled for main cache Exporting flows to 192.168.97.12 (2055) Exporting using source IP address 10.0.0.2 Version 5 flow records 2602429 flows exported in 554968 udp datagrams 0 flows failed due to lack of export packet NAC-2800-Remote#`**`show ip flow top 10 aggregate source-address`** 上位 4 人の通話者を確認できます。
```
IPV4 SRC-ADDR         bytes        pkts       flows
===============  ==========  ==========  ==========
192.168.122.60           44           1           1
192.168.122.59           88           2           2
192.168.121.90          367           3           3
10.0.0.1              19320         322           1
```
14. プロファイラがコレクタから NetFlow を受信したことを確認します。 リモート MAC またはエンドポイント IP を選択し、プロファイルされたデータを確認します。[Endpoint Console] > [View/Manage Endpoints] > [Display Endpoints by device ports] > [ungrouped] > [Table of Devices] の順に選択し、スイッチを選択します。次に、デバイスの MAC アドレスを選択します。[View Profile Data] をクリックします。出力に、宛先 IP が 192.168.70.50 で宛先ポートが 2000 のトラフィックが表示されます。 これは Cisco CallManager の IP アドレスであり、宛先ポート 2000 は SCCP 制御トラフィック用に使用されます。

関連情報

- テクニカルサポートとドキュメント - Cisco Systems