Cisco Secure Network Analytics

v7.4.2 エンドポイントライセンスおよび NVM 設定ガイド

目次

はじめに

概要

このガイドを使用して、Cisco Secure Network Analytics（旧称 Stealthwatch）Cisco AnyConnect Secure Mobility Client Network Visibility Module（NVM）を設定して以下を有効にします。

- NVM フィールドの保存と表示
- NVM フローからの既存のポリシー違反ルールのトリガー
- NVM トラフィックに基づく NetFlow 検出
- エンドポイント接続に基づくカスタム セキュリティ イベントの作成

> ⚠ Secure Network Analytics と NVM は UDP をサポートしますが、DTLS はサポートしません。

要件

- Secure Network Analytics v7.4.2 および Cisco Secure Network Analytics エンドポイントライセンス エンドポイントライセンス の詳細については、『Smart Software Licensing Guide 7.4』を参照してください。
- AnyConnect v4.7 以降

7.3.0 または 7.3.1 から 7.4.2 へのアップグレード

エンドポイント コンセントレータ の削除

> ⓘ v7.3.2 以降、エンドポイント コンセントレータはエンドポイントライセンスの展開に不要となり、Data Store を含むすべての Secure Network Analytics 展開で Network Visibility Module（NVM）のデータを処理するように Flow Collector が拡張されました。

既存の Secure Network Analytics 顧客が 7.3.0 または 7.3.1 から 7.4.2 にアップグレードしている場合は、エンドポイント コンセントレータ を削除し、NVM 展開を再構成する必要があります。

次の手順に従って、エンドポイント コンセントレータ を削除し、Flow Collector を設定します。

1. Central Management を使用して、クラスタから エンドポイント コンセントレータ を削除します。
   a. [集中管理（Central Management）] を開きます。
   b. [アプライアンスマネージャ（Appliance Manager ）] のページで、エンドポイント コンセントレータ の [アクション（Actions）] 列にある ••• （[省略記号（Ellipsis）]）アイコンをクリックします。
   c. [このアプライアンスを削除（Remove This Appliance）] をクリックし、[はい（Yes）] をクリックします。
2. 「AnyConnect の NVM プロファイルの設定」セクションを使用して、NVM クライアントから Flow Collector へのフローを設定します。
3. 『Secure Network Analytics Update Guide』を使用してクラスタを v7.4.2 に更新します。

4. Flow Collector の構成セクションを使用して NVM 処理ポートを Flow Collector 詳細設定に追加します。
5. レポートビルダー を使用するか、[検証（Verification）] セクションを使用してフロー検索を使用して、NVMno data が処理されていることを確認します。

> サポートが必要な場合は、シスコサポートまでお問い合わせください。

レポートビルダー

レポートビルダー を別のアプリから v7.4 のコア Secure Network Analytics に移動しました。以前のバージョンのアプリがインストールされている場合、アプリケーションは Secure Network Analytics v7.4.x への更新の一環として自動的に削除されます。更新ガイドの手順に従ってください。

> 既存の レポートビルダー アプリをアンインストールしてください。レポートビルダー をアンインストールする場合、保存されたレポートおよび一時的なファイルなどの関連している全てのファイルは削除されます。

エンドポイントライセンスと Data Store 機能

エンドポイントライセンス が Cisco Secure Network Analytics データストア でサポートされるようになり、以下が提供されます。

- オンネットワークとオフネットワークのデータを含む、エンドポイントに対する完全な可視性
- レポートビルダーアプリのエンドポイントトラフィック（NVM）レポートの NVM フィールドに対する可視性
- NVM データの 30 日間以上の保存
- 処理とクエリのパフォーマンス向上
- NVM トラフィックに基づく NetFlow 検出
- エンドポイント接続に基づくカスタム セキュリティ イベントの作成

次の表に、標準的な企業（大部分のお客様）のトラフィックプロファイルに関する推定パフォーマンスを示します。

1 秒あたりのフロー数（FPS）		FC 4210 の数	DS 6200 の数/保存期間 360 日
NetFlow	NVM		
300,000	150,000	1	3

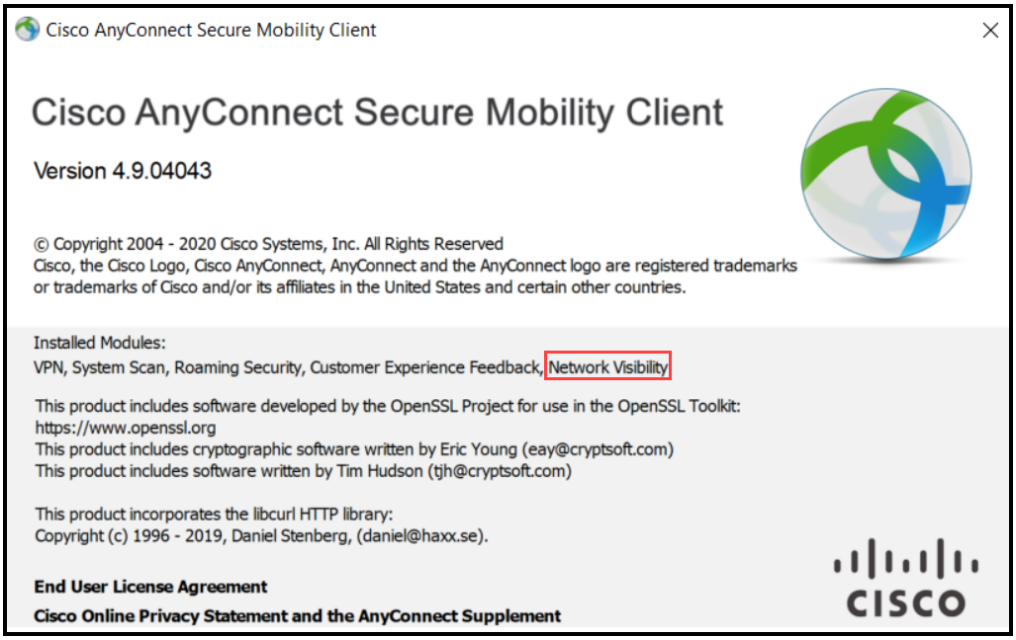
> それぞれ環境でのパフォーマンスは、ホスト数やフローの平均サイズなど、いくつかの要因によって影響を受ける可能性があります。可能な限り公平かつ正確にデータを示すために最善を尽くしていますが、環境によって限界が異なる場合があります。

構成

NVM プロファイルを AnyConnect に構成する

AnyConnect プロファイルエディタは、Cisco Adaptive Security Device Manager（ASDM）を介して、またはスタンドアロンとして提供されます。AnyConnect プロファイル エディタの使用方法の詳細については、『AnyConnect Administrator Guide』を参照してください。

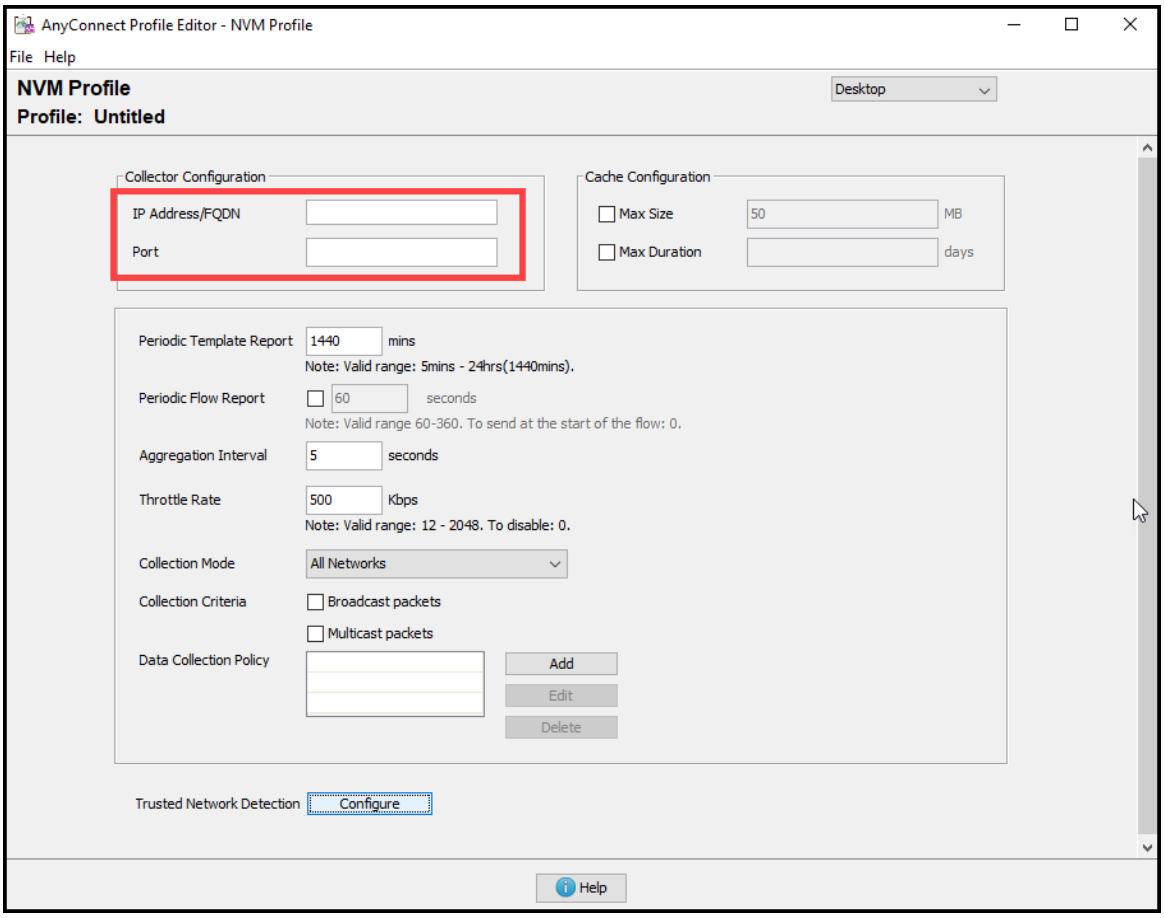
1. Network Visibility Module がインストールされていることを確認します。



2. ネットワークの可視性モジュールのプロファイルエディタを開きます。
3. [コレクタの設定（Collector Configuration）] セクションで、Flow Collector の自分の **IP アドレスとポート**を入力します。

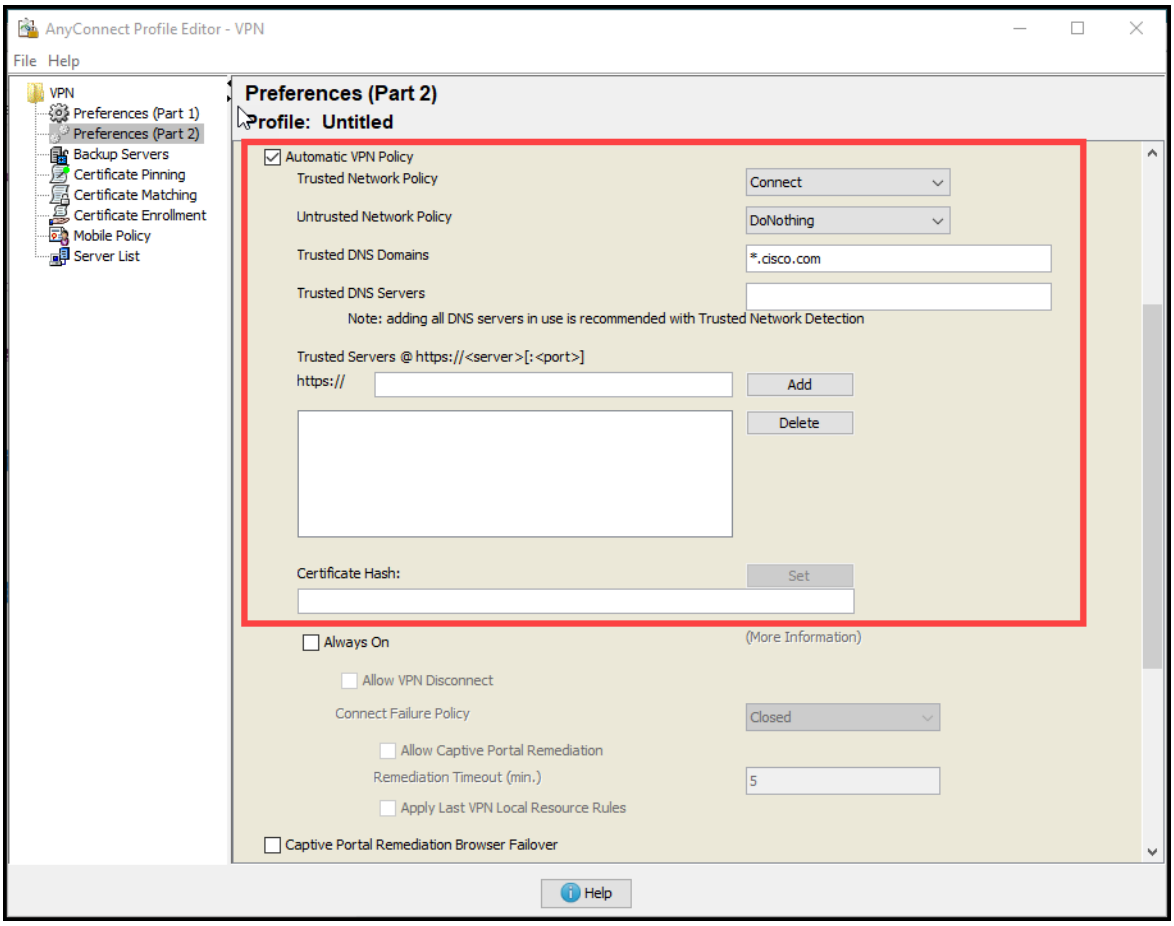
デフォルトポートの 2055 ではなく、ポート 2030 を使用することをお勧めします。ポート 2030 がすでに使用されている場合は、予約済みでない任意のポートを使用できます。このポートは、「Flow Collector を構成する」セクションでこのポートを使用します。

ポート 2055、514、8514 は使用しないでください。



4. **[ファイル(File)]>[保存(Save)]**をクリックして NVM プロファイルを保存します。
5. NVM プロファイルエディタを閉じます。
6. VPN プロファイルエディタを開きます。
7. [設定(パート2)(Preferences (Part 2))]をクリックします。
8. [自動VPNポリシー(Automatic VPN Policy)]チェックボックスをオンにします。
9. [信頼できるネットワークポリシー(Trusted Network Policy)]で、ドロップダウンから[接続(Connect)]を選択します。
10. [信頼できないネットワークポリシー(Untrusted Network Policy)]で、ドロップダウンから[何もしない(DoNothing)]を選択します。
11. [信頼できるDNSドメイン(Trusted DNS Domains)]、[信頼できるサーバ(Trusted Servers)]、および[証明書ハッシュ(Certificate Hash)]に入力します。

- 信頼された DNS ドメインは、Flow Collector を実行しているドメインと同じドメインである必要があります。DNS サフィックスでは、ワイルドカード(*)がサポートされます。
- 信頼できるサーバは、ネットワーク上の DNS サーバの IP アドレスである必要があります。



12. **[ファイル(File)]** > **[保存(Save)]** をクリックして設定を保存します。
13. AnyConnect プロファイルエディタを閉じます。

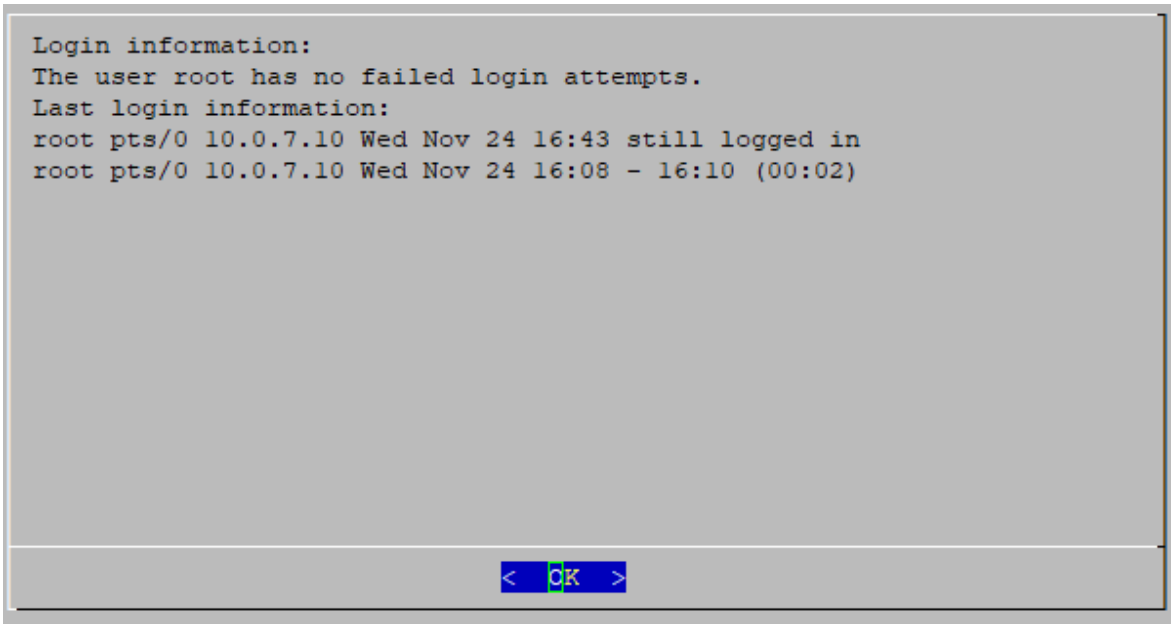
初回セットアップ(Data Store のみ)を使用して

Flow Collector を構成し、NVM トラフィックを取り込む

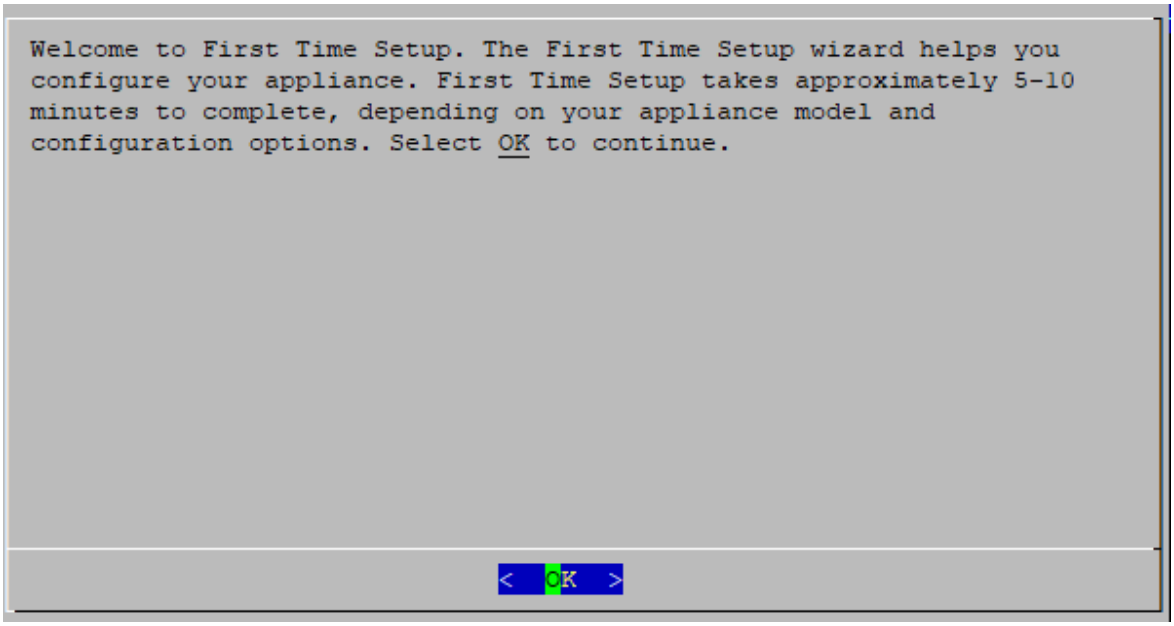
Data Store を使用して新しい Flow Collector で NVM トラフィックの取り込みを有効にするには、次の手順を実行します。

1. Flow Collector の該当するアプライアンス インストール ガイド の手順に従ってください。次に、システム コンフィギュレーション ガイドを使用して、複数のテレメトリタイプのアプライアンス構成に関する詳細な手順を確認します。
2. 仮想マシン コンソールにアクセスします。仮想アプライアンスの起動が完了します。
3. コンソールでログインします。
   - **ログイン**:root
   - **デフォルト パスワード**:lan1cope
   - システムを設定するときに、デフォルトのパスワードを変更します。
4. コマンドプロンプトで、`SystemConfig` と入力します。Enter キーを押します。

5. 失敗したログイン試行の情報を確認します。[OK] を選択して続行します。

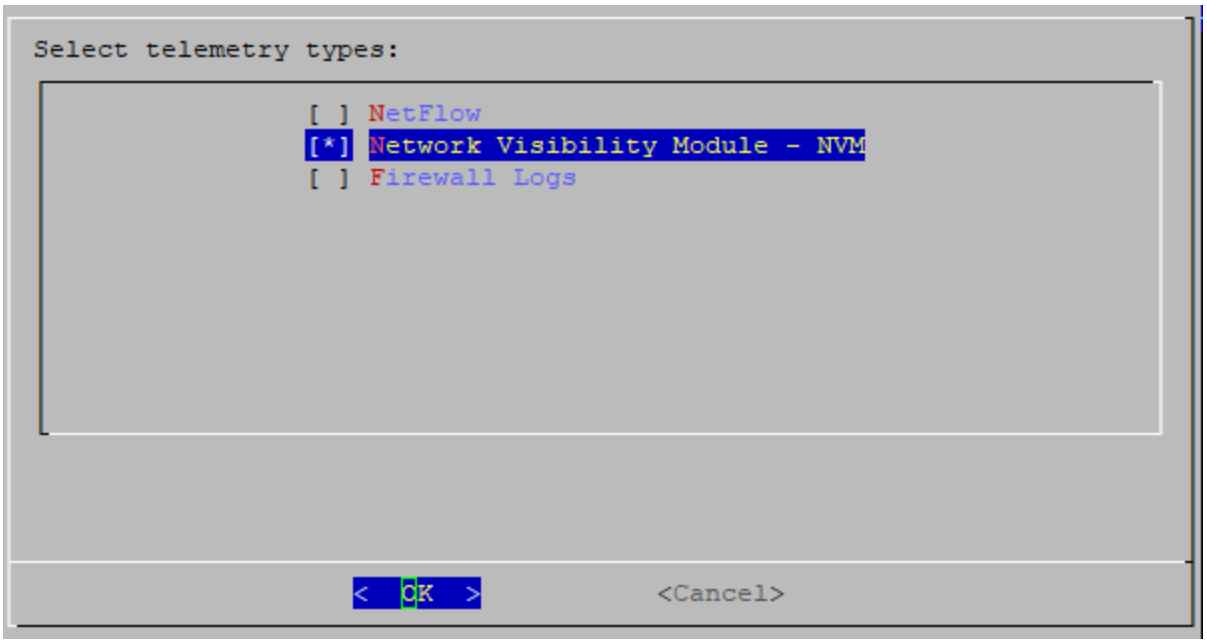


6. 初回セットアップの概要を確認します。[OK] を選択して続行します。



7. テレメトリタイプリストから [Network Visibility Module – NVM] を選択します。[Yes] を選択して続行します。

> デフォルトでは、すべてのテレメトリタイプが選択されています。

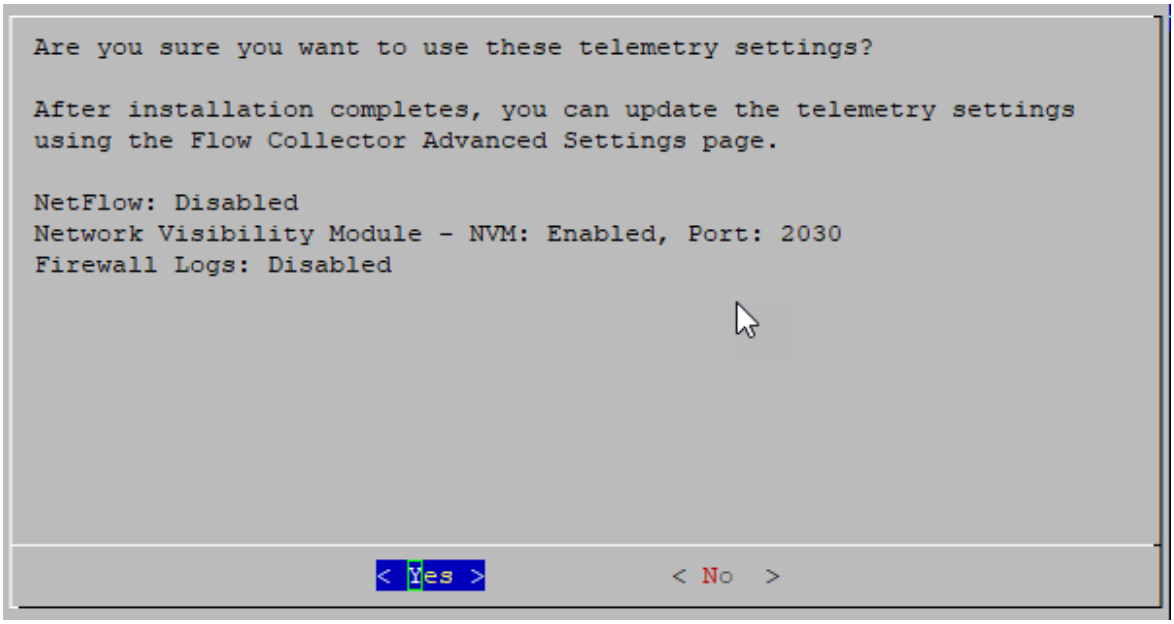


8. [Network Visibility Module – NVM] の UDP ポートを入力します。[OK] を選択します。

「AnyConnect の NVM プロファイルの構成」セクションのステップ 2 で指定されたポートに値を設定します。ポート 2030 がデフォルト ポートです。ポート 2055、514、8514 は使用しないでください。

⚠ テレメトリポートが一意であることを確認します。テレメトリポートを重複して設定すると、フローデータの消失を回避するためにポートが内部のデフォルト値にリセットされます。たとえば、NetFlow と NVM が同じテレメトリポートにエクスポートされると、NVM データをエクスポートする各デバイスが Flow Collector にエクスポータを作成し、Flow Collector エンジンのエクスポータリソースを使い切ってしまうため、フローデータが消失します。

9. 設定を確認します。[Yes] を選択して続行します。



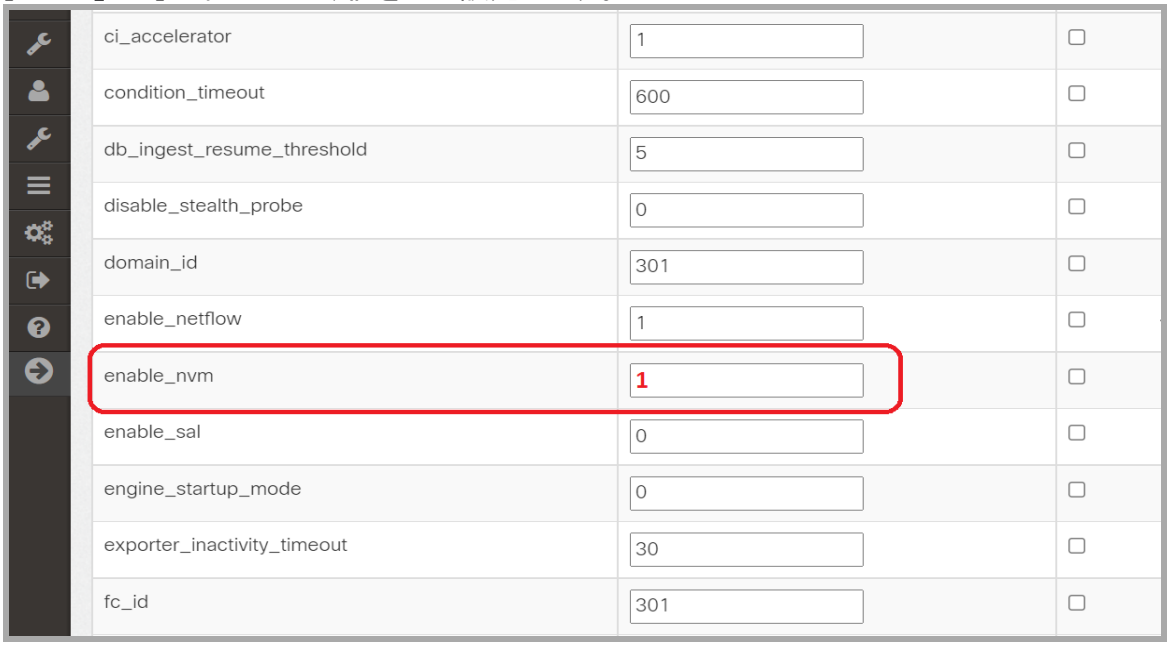
10. 画面に表示される指示に従って仮想環境を終了し、アプライアンスを再起動します。

Flow Collector の詳細設定の使用

設定済みの Flow Collector で NVM トラフィックの取り込みを有効にするには、次の手順を実行します。

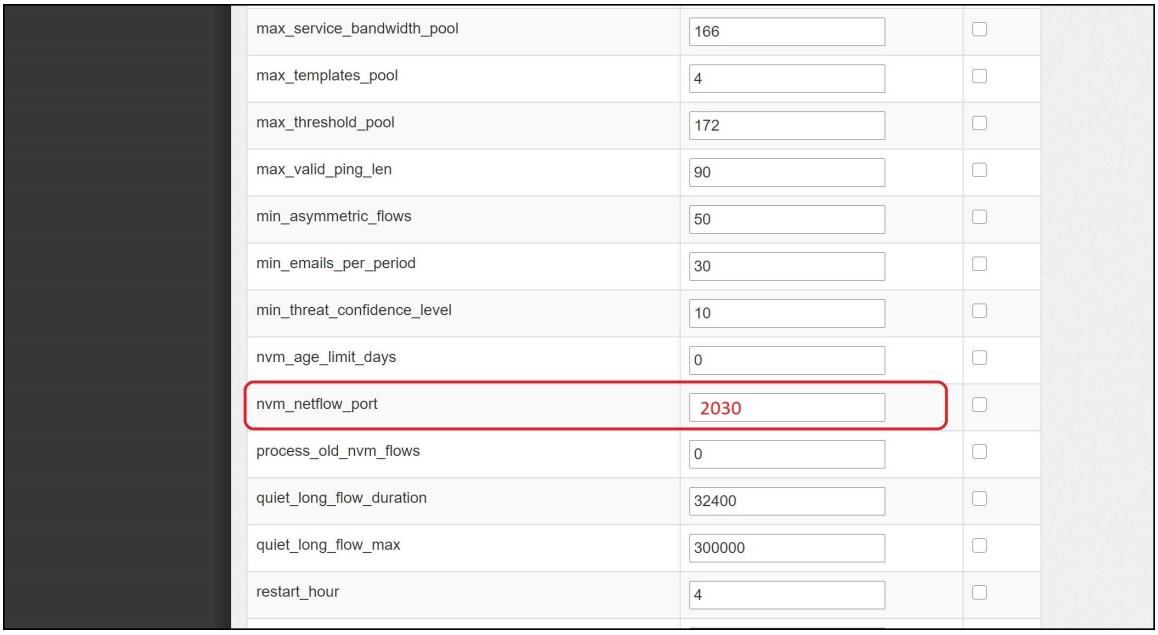
1. マネージャにログインします。
2. メインメニューから [構成(Configure)] > [グローバル集中管理(GLOBAL Central Management)] を選択します。
3. [在庫(Inventory)] ページで、Flow Collector の ••• ([省略記号(Ellipsis)]) アイコンをクリックし、[アプライアンス統計の表示(View Appliance Statistics)] を選択します。Flow Collector 管理インターフェイスが開きます。
4. [サポート(Support)] > [詳細設定(Advanced Settings)] を選択します。

5. [enable_nvm] フィールドで、値を 1 に設定します。



6. [nvm_netflow_port] フィールドで、「AnyConnect の NVM プロファイルの構成」セクションのステップ 2 で指定されたポートに値を設定します。たとえば、ポート 2030 に設定します。

> フィールドが表示されていない場合は、ページの下部までスクロールしてください。[新しいオプションの追加（Add New Option）] フィールドをクリックしてください。Flow Collector での詳細設定の編集の詳細については、[詳細設定（Advanced Settings）] のヘルプトピックを参照してください。



「AnyConnect の NVM プロファイルの構成」セクションのステップ 2 で指定されたポートに値を設定します。ポート 2030 がデフォルト ポートです。ポート 2055、514、8514 は使用しないでください。

⚠ テレメトリポートが一意であることを確認します。テレメトリポートを重複して設定すると、フローデータの消失を回避するためにポートが内部のデフォルト値にリセットされます。たとえば、NetFlow と NVM が同じテレメトリポートにエクスポートされると、NVM データをエクスポートする各デバイスが Flow Collector にエクスポータを作成し、Flow Collector エンジンのエクスポータリソースを使い切ってしまうため、フローデータが消失します。

7. [適用(Apply)] をクリックします。
8. 確認メッセージが表示されたら [OK] をクリックします。

NVM トラフィックの検出の構成(オプション – Data Store のみ)

Data Store 展開で NVM トラフィックに基づく NetFlow 検出を有効にするには、Flow Collector 詳細設定ページでこの構成を続行します。Flow Collector が閉じている場合は、直接ログインするか、または:

ℹ 非 Data Store 展開では、この設定を構成する必要はなく、NVM トラフィックに基づいた NetFlow 検出が自動的に含まれます。

1. マネージャ にログインします。
2. メインメニューから [構成(Configure)] > [グローバル集中管理(GLOBAL Central Management)] を選択します。
3. [在庫(Inventory)] ページで、Flow Collector の ••• ([省略記号(Ellipsis)]) アイコンをクリックし、[アプライアンス統計の表示(View Appliance Statistics)] を選択します。Flow Collector 管理インターフェイスが開きます。
4. [サポート(Support)] > [詳細設定(Advanced Settings)] を選択します。
5. [nvm_to_flow_cache] フィールドで、値を 1 に設定します。
6. [適用(Apply)] をクリックします。
7. 確認メッセージが表示されたら [OK] をクリックします。

オフネットワーク キャッシュ フローの Flow Collector を設定します(オプション)

オフネットワーク NVM トラフィックを収集するためにキャッシュフロー処理を設定するには、次の手順を使用します。

ℹ オフネットワーク NVM トラフィックの収集は、システムのパフォーマンスに影響します。このデータを収集または分析する必要がない場合は、この設定を有効にしないでください。

設定を有効にしてシステムのパフォーマンスが低下した場合は、スロットルレートを調整するか(『AnyConnect Administator Guide』を参照)、nvm_age_limit_days の値を小さくしてください(このセクションの手順を参照)。

この手順を開始する前に、前の手順を完了してください。Flow Collector 詳細設定ページでこの構成を続行します。Flow Collector が閉じている場合は、直接ログインするか、または：

1. マネージャ にログインします。
2. メインメニューから [構成（Configure）] > [グローバル集中管理（GLOBAL Central Management）] を選択します。
3. [在庫（Inventory）] ページで、Flow Collector の ••• （[省略記号（Ellipsis）]）アイコンをクリックし、[アプライアンス統計の表示（View Appliance Statistics）] を選択します。Flow Collector では管理インターフェイスが開きます。
4. [サポート（Support）] > [詳細設定（Advanced Settings）] を選択します。
5. 次のフィールドを更新します。

    - [process_old_nvm_flows]：キャッシュされたフローが Flow Collector よって処理されるようにするには、1 を入力します。
    - **nvm_age_limit_days**：Flow Collector によってキャッシュされたフローを収集するための最大存続期間（日数）を入力します。たとえば、7 を入力すると、最大 7 日前のキャッシュされたフローが処理されます。0（ゼロ）を入力すると、キャッシュされた**すべて**のフローが処理されます。最大限のパフォーマンスを得るには、制限のある日数を設定します。

> フィールドが表示されていない場合は、ページの下部までスクロールしてください。[新しいオプションの追加（Add New Option）] フィールドに情報を入力します。Flow Collector での詳細設定の編集の詳細については、[詳細設定（Advanced Settings）] のヘルプトピックを参照してください。

6. [適用（Apply）] をクリックします。
7. 確認メッセージが表示されたら [OK] をクリックします。

検証

Secure Network Analytics 展開に応じて、NVM データがフロー検索またはレポートビルダーに表示されます。

フロー検索

> Data Store を展開している場合、フロー検索で NVM データを表示するには、[NVM トラフィックの検出（Detections for NVM Traffic）] を有効にする必要があります。

1. マネージャにログインします。
2. メインメニューから [調査（Investigate）] > [フロー検索（Flow Search）] を選択します。
3. フロー検索を実行します。
4. [フロー検索結果（Flow Search Results）] で、[サブジェクトプロセス名（Subject Process Name）] を使用してテーブルをフィルタ処理し、NVM フローを取得していることを確認します。

レポートビルダー を開く（Data Store のみ）

レポートビルダー は、Data Store を使用した Secure Network Analytics の 3 つの NVM 関連レポートを提供します。

- **NVM データベース取り込みトレンド**には、データベースにデータが正常に取り込まれたときに通知が示されます。
- **NVM 収集トレンド**には、NVM から Flow Collector へのフローの到達率が示されます。
- **エンドポイントトラフィック（NVM）**には、終了時刻に基づいて最新の 300 レコードが表示されます。

> これらのレポートの詳細については、（[ヘルプ（Help）]）アイコンをクリックして レポートビルダー のヘルプにアクセスしてください。

たとえば、エンドポイントトラフィック（NVM）レポートを表示するには、次の手順を実行します。

1. マネージャにログインします。
2. メインメニューで、**[レポート（Reports）] > [レポートビルダー（Report Builder）]** を選択します。
3. [新規レポートの作成（Create New Report）] をクリックし、[エンドポイントトラフィック（NVM）（Endpoint Traffic（NVM））] を選択します。
4. [実行（Run）] をクリックします。
5. レポートに NVM トラフィックが表示されていることを確認します。

サポートへの問い合わせ

テクニカル サポートが必要な場合は、次のいずれかを実行してください。

- 最寄りのシスコ パートナーにご連絡ください。
- シスコサポートの連絡先
- Web でケースを開く場合：http://www.cisco.com/c/en/us/support/index.html
- 電子メールでケースを開く場合：tac@cisco.com
- 電話でサポートを受ける場合：800-553-2447（米国）
- ワールドワイド サポート番号：
  https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

変更履歴

マニュアルのバージョン	公開日	説明
1_0	2023 年 3 月 1 日	最初のバージョン。
1_1	2023 年 3 月 27 日	*オフネットワーク キャッシュ フローの Flow Collector（オプション）*セクションを更新しました。

著作権情報