Cisco Secure Network Analytics

エンドポイントライセンスおよび NVM コンフィギュレーション ガイド 7.4.1

目次

はじめに **3**

概要 3

要件 3

7.3.0 または 7.3.1 から 7.4.1 へのアップグレード 3

エンドポイント コンセントレータの削除 3

レポートビルダー 4

エンドポイントライセンスの機能 4

設定 **5**

AnyConnect セキュア モビリティ クライアントでの NVM プロファイルの設定 5

Flow Collector の設定 7

初回セットアップの使用（Data Store のみ） 7

Flow Collector の詳細設定の使用 10

オフネットワーク キャッシュフローのFlow Collectorの設定（オプション） 12

検証 **13**

フロー検索 13

レポートビルダーを開く（Data Store のみ） 13

サポートへの問い合わせ **14**

はじめに

概要

このガイドを使用して、以下を実行できるように Cisco Secure Network Analytics（旧 Stealthwatch）と Cisco AnyConnect Secure Mobility Client Network Visibility Module（NVM）を設定できます。

- AnyConnect NVM フィールドの保存
- NVM フィールドの表示
- 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 を使用した Cisco Secure Network Analytics は UDP をサポートしていますが、DTLS はサポートしていません。

要件

- Cisco Secure Network Analytics エンドポイントライセンス を備えた Secure Network Analytics v7.4.x。エンドポイントライセンスの詳細については、スマート ソフトウェア ライセンシング ガイド 7.4 [英語] を参照してください。
- AnyConnect Secure Mobility Client v4.7 以降

7.3.0 または 7.3.1 から 7.4.1 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

> ℹ 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 を 7.3.0 または 7.3.1 から 7.4.1 にアップグレードする場合は、エンドポイント コンセントレータを削除して NVM の展開を再設定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. Central Management を開きます。
    b. [Appliance Manager] 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）] 列の ••• （[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）] を選択し、[はい（Yes）] をクリックします。
2. 「AnyConnect Secure Mobility Client での NVM プロファイルの設定」セクションの手順に従い、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 (v7.3.x to v7.4.1)』の手順に従い、クラスタを v7.4.1 に更新します。

4. 「Flow Collector の設定」セクションの手順に従い、Flow Collector の詳細設定に NVM 処理ポートを追加します。
5. 「検証」セクションの手順に従い、レポートビルダーかフロー検索を使用して NVM データ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、Cisco Stealthwatch サポートに連絡してください。

レポートビルダー

v7.4.x では、レポートビルダーを別のアプリケーションからコアの Secure Network Analytics に移動しました。以前のバージョンのアプリケーション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 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 アプリケーションはアンインストールしないでください。レポートビルダー をアンインストールすると、保存済みのレポートや一時ファイルを含めて、関連付けられているすべてのファイルが削除されます。

既存のアプリケーションをアンインストールする必要はありません。レポートビルダー をアンインストールすると、保存済みのレポートや一時ファイルを含めて、関連付けられているすべてのファイルが削除されます。レポートビルダー の既存のアプリは削除しないでください。

エンドポイントライセンスの機能

エンドポイントライセンス は Cisco Secure Network Analytics データストア に対してサポートされるようになり、以下の内容を提供します。

- 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

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）		バックアップファイル FC 4210 の数	バックアップファイル DS 6200 の数/保存期間 31 日
NetFlow	NVM		
300,000	150,000	1	3

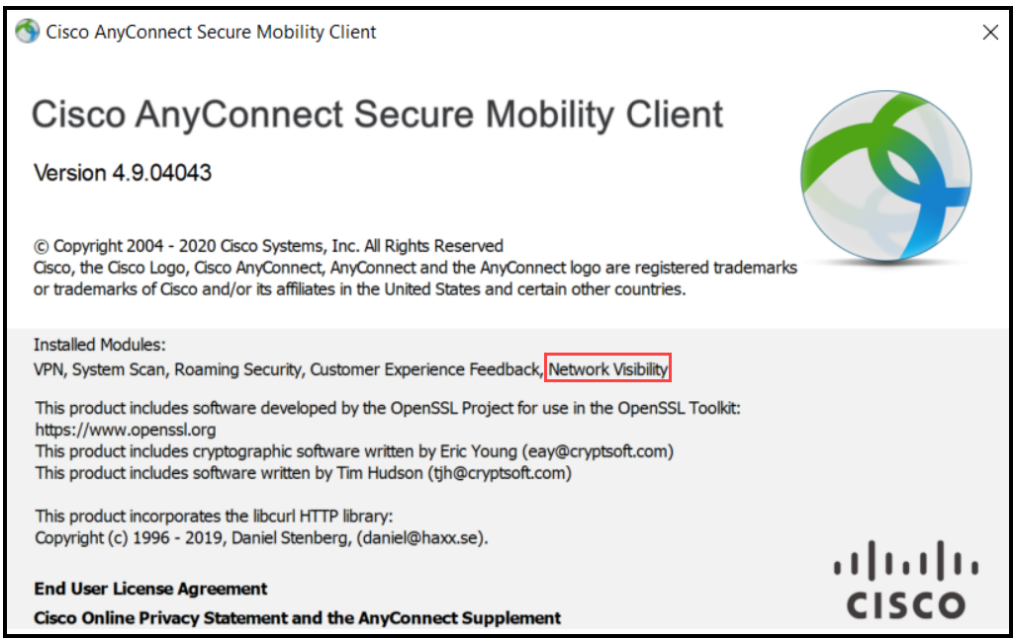
それぞれ環境でのパフォーマンスは、ホスト数やフローの平均サイズなど、いくつかの要因によって影響を受ける可能性があります。可能な限り公平かつ正確にデータを示すために最善を尽くしていますが、環境によって限界が異なる場合があります。

設定

AnyConnect セキュア モビリティ クライアントでの NVM プロファイルの設定

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、Cisco AnyConnect 管理者ガイド［英語］を参照してください。

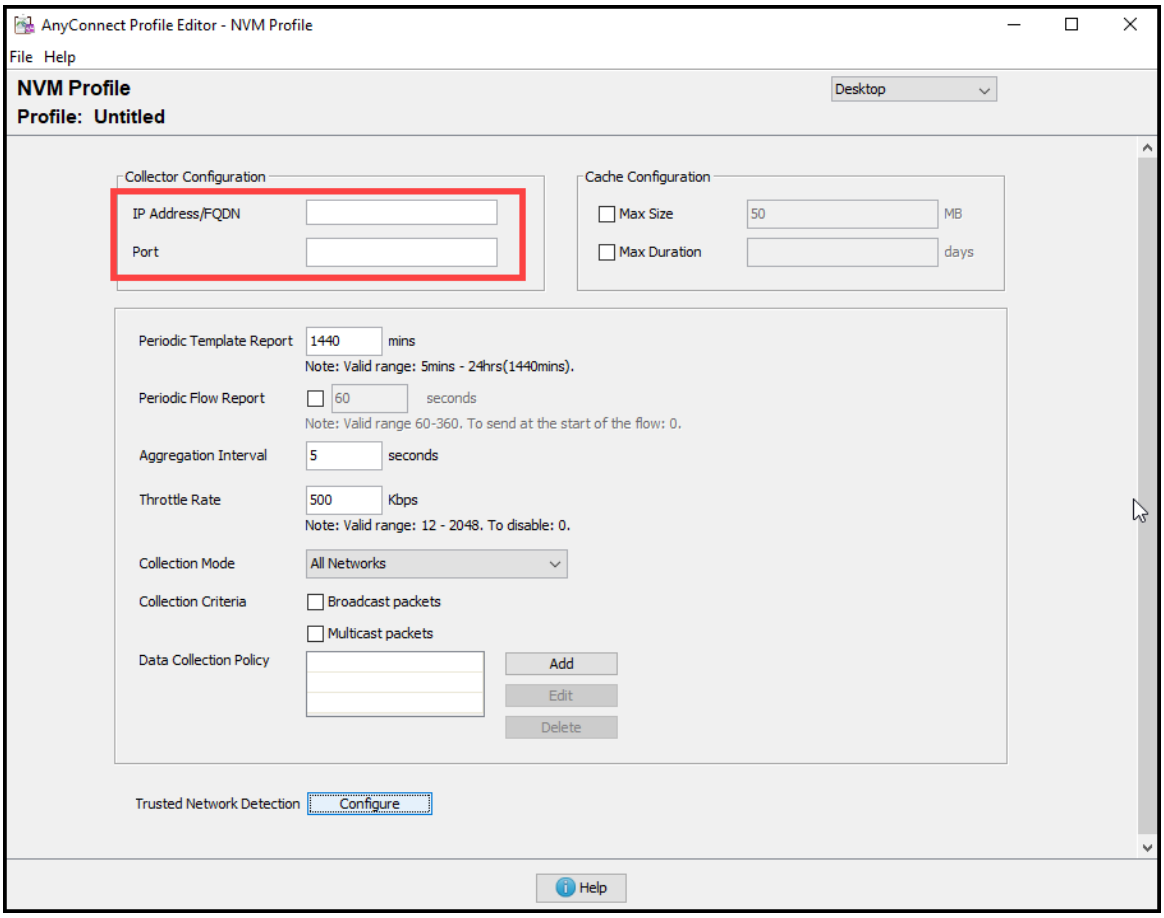
1. Network Visibility Module がインストールされていることを確認します。



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［IP アドレス（IP Address）］と［ポート（Port）］に入力します。

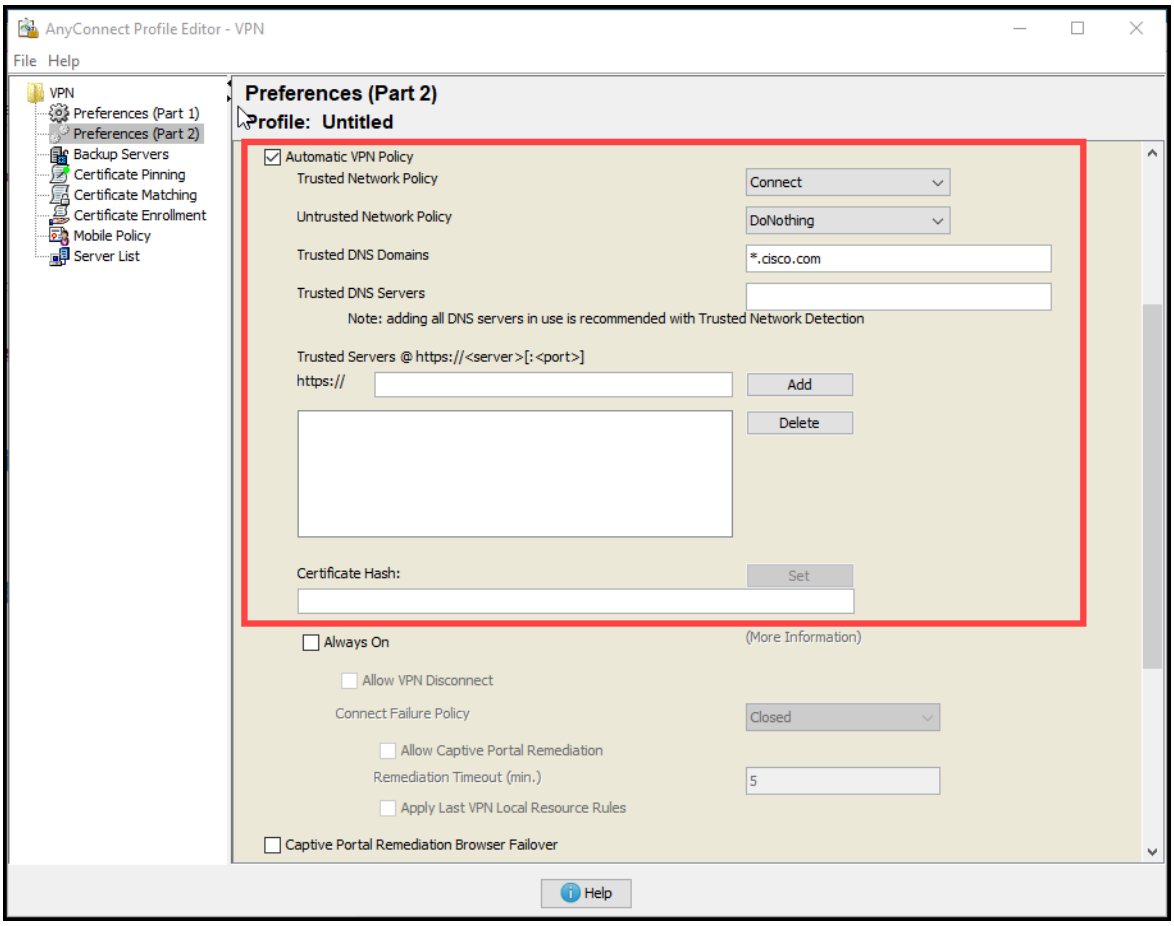
デフォルトポートの 2055 ではなく、ポート 2030 を使用することをお勧めします。ポート 2030 がすでに使用されている場合は、予約済みでない任意のポートを使用できます。このポートは、「Flow Collector の設定」セクションで使用します。

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。

- 信頼できるDNSドメインは、Flow Collectorが実行されているドメインと同じ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。

Flow Collector の設定

初回セットアップの使用(Data Store のみ)

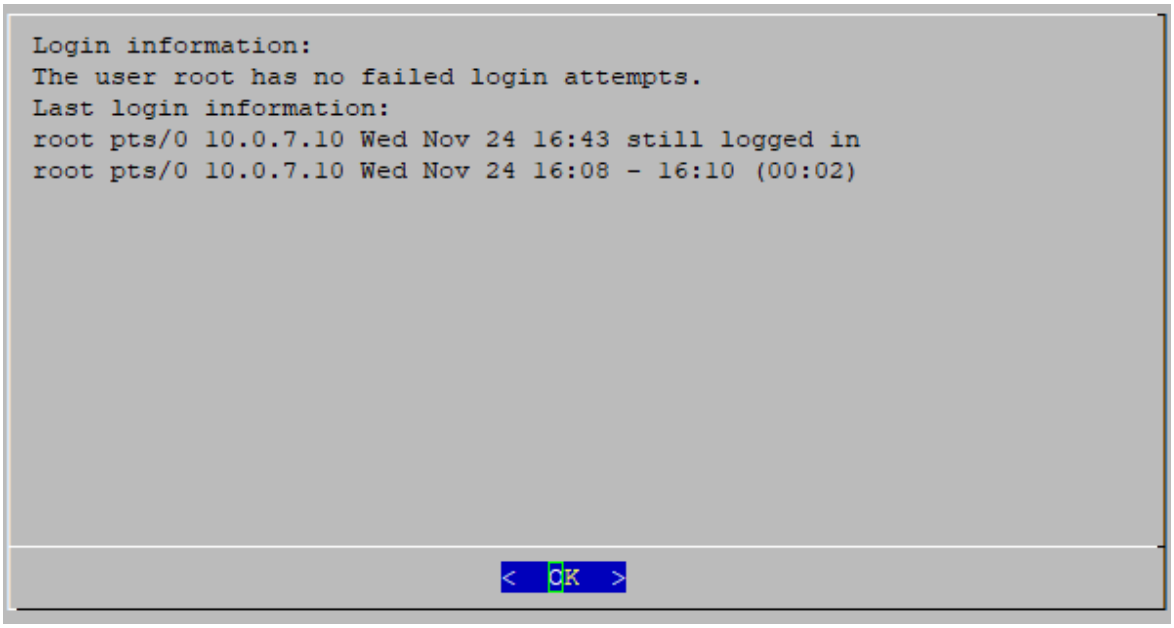
新しい Flow Collector で NVM フローの取り込みを有効にするには、次の手順を実行します。

1. Flow Collector の該当する『Data Store アプライアンス設置ガイド』を参照します。指示に従って、「初回セットアップを使用した環境の設定」セクションに進みます。

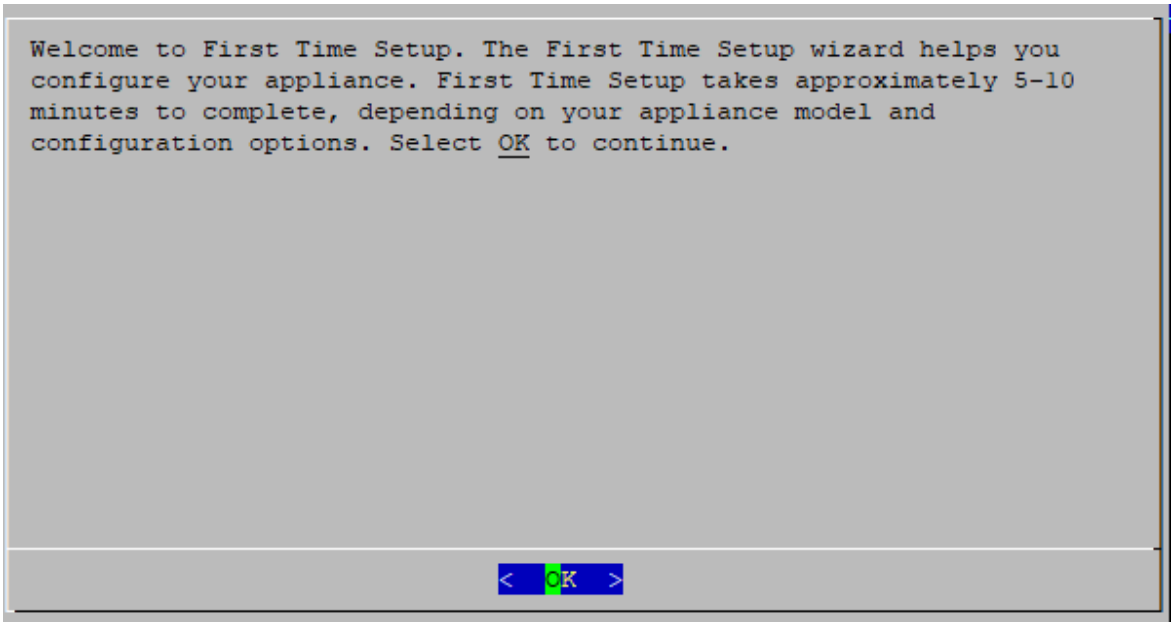
   アプライアンスの設置と複数のテレメトリタイプの設定に関する詳細な手順については、『Data Store アプライアンス設置ガイド』を参照してください。

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。

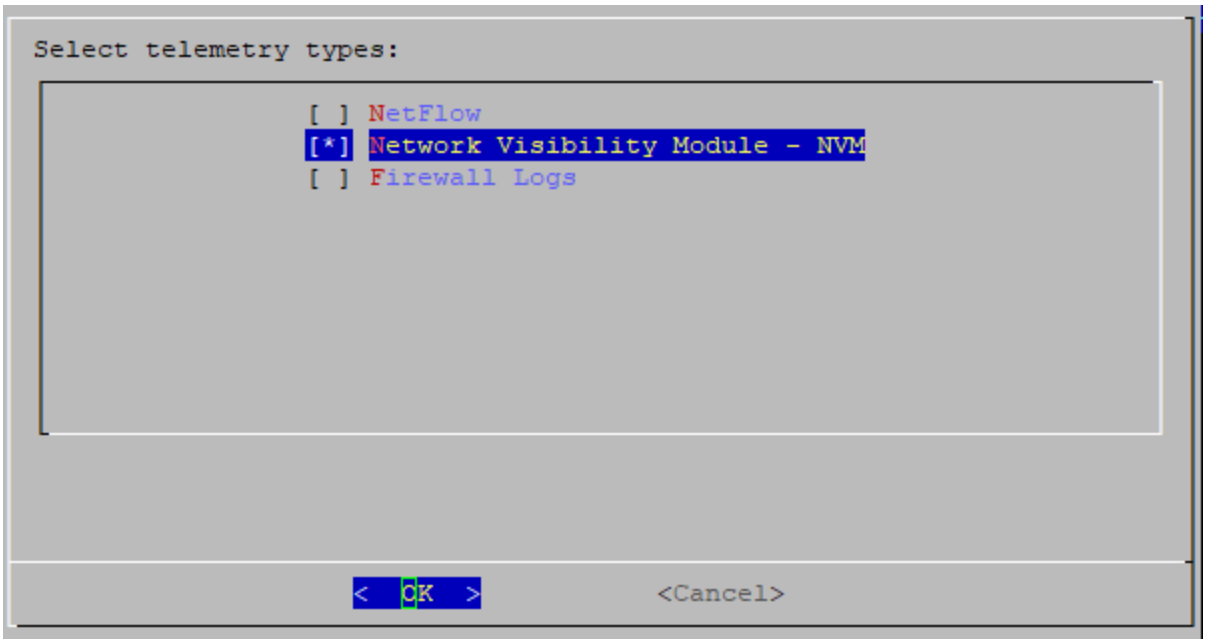


6. 初回セットアップの概要を確認します。[OK] を選択して続行します。



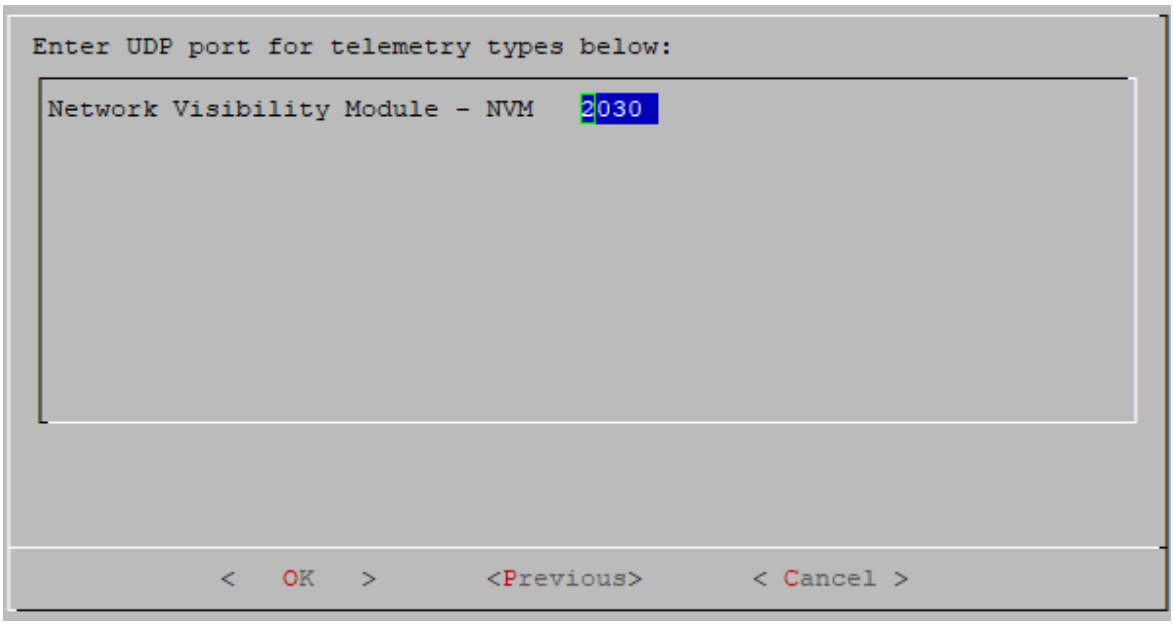
7. テレメトリタイプリストから [Network Visibility Module – NVM] を選択します。[Yes] を選択して続行します。

> 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。

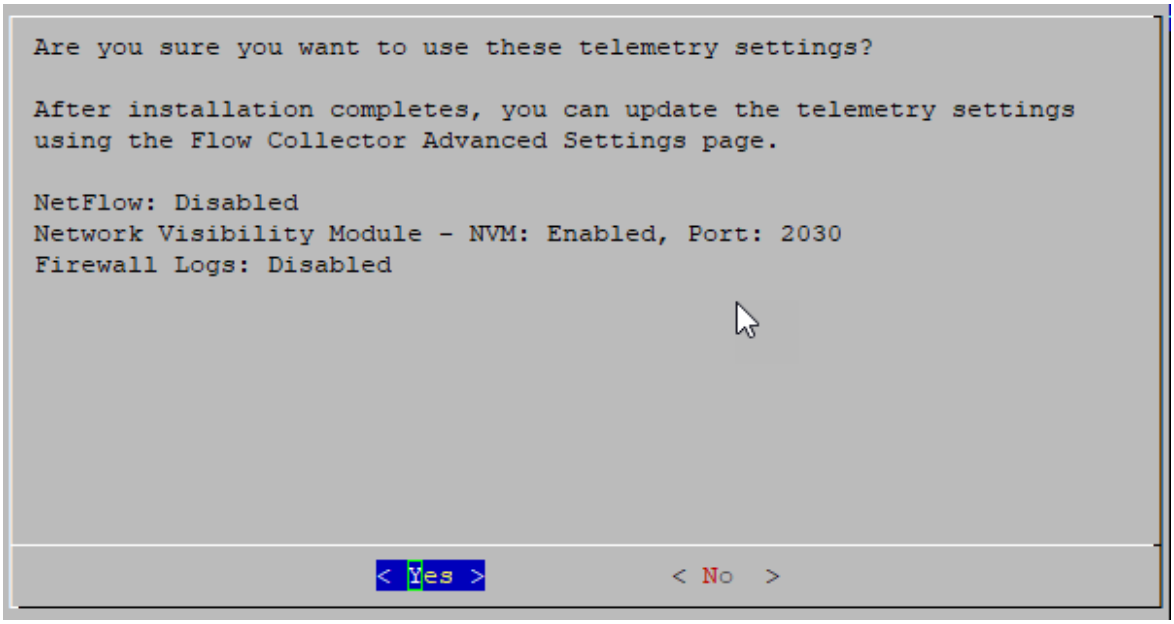


8. [Network Visibility Module – NVM] の UDP ポートを入力します。[OK] を選択します。

> 「AnyConnect Secure Mobility Client での NVM プロファイルの設定」セクションの手順 2 で指定し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。



9. 設定を確認します。[Yes] を選択して続行します。

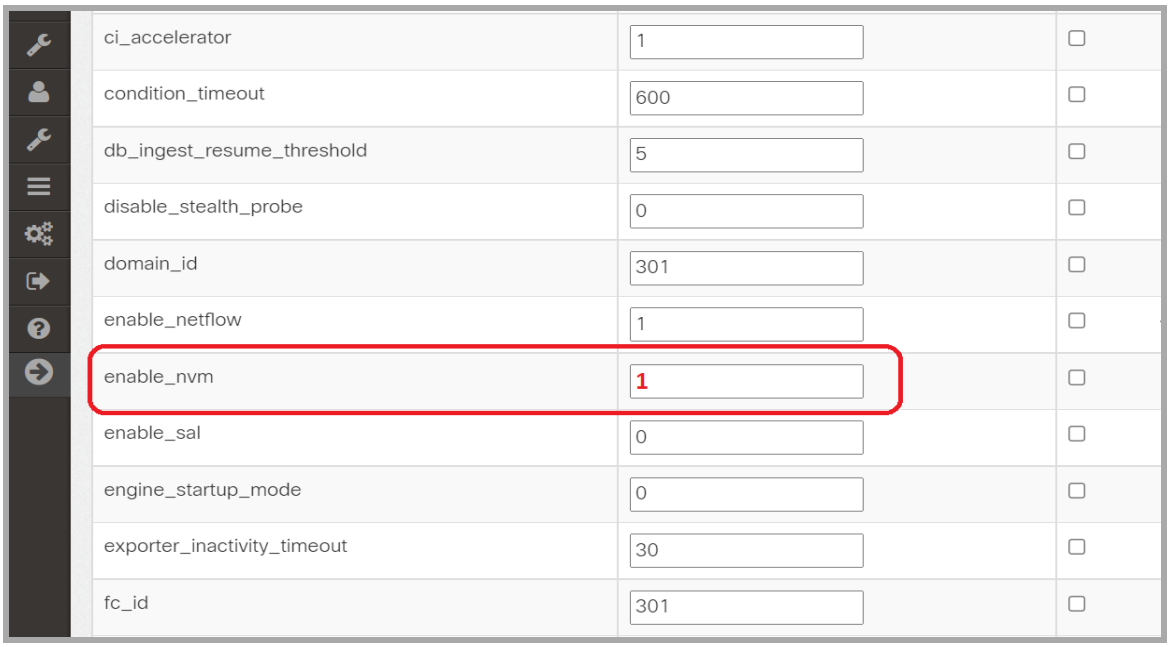


10. 画面に表示される指示に従って仮想環境を終了し、アプライアンスを再起動します。

Flow Collector の詳細設定の使用

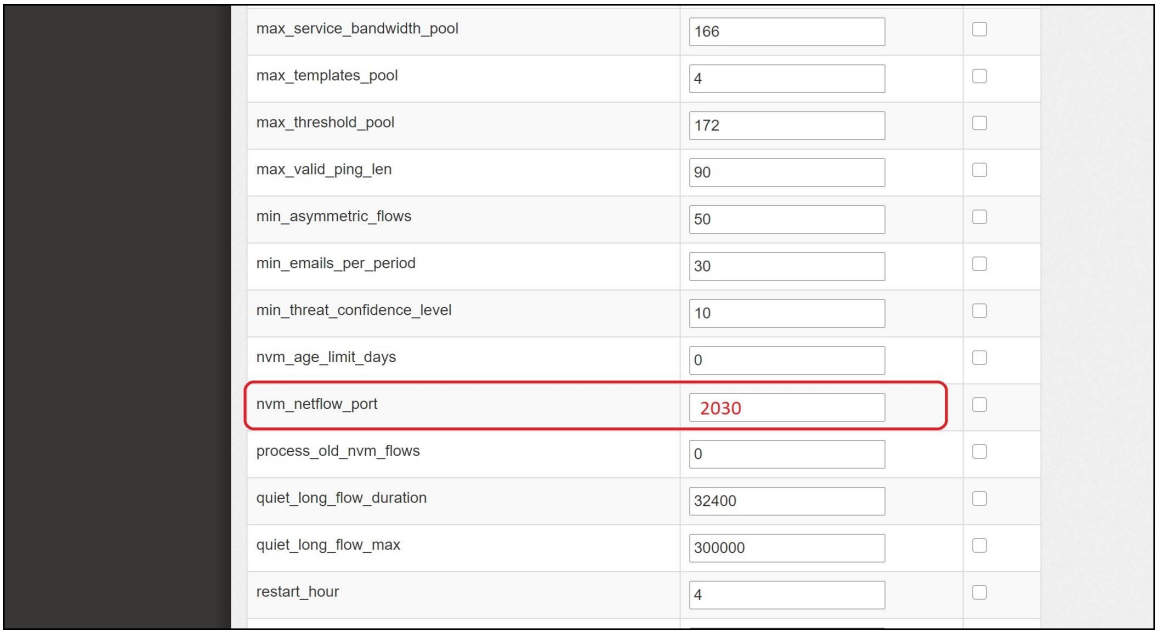
設定済みの Flow Collector で NVM フローの取り込みを有効にするには、次の手順を実行します。

1. マネージャにログインします。
2. ナビゲーションメニューで、⚙ ([グローバル設定(Global Settings)]) アイコン をクリックし、[集中管理(Central Management)] を選択します。
3. 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情報の表示(View Appliance Statistics)] をクリックします。Flow Collector の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)] の順にクリックします。
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 Secure Mobility Client での NVM プロファイルの設定」セクションのステップ 2 で指定し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、詳細設定のヘルプトピックを参照してください。



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。
9. オフラインデータ収集用にFlow Collectorを設定するには、次のセクションに進みます。Flow Collectorを閉じないでください。

オフネットワーク キャッシュフローのFlow Collectorの設定(オプション)

オフネットワーク NVM データ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。

> オフネットワーク NVM データの収集は、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)。

1. 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エンジンの[サポート(Support)]>[詳細設定(Advanced Settings)]で、この設定を続行します。Flow Collectorが開いていない場合は、直接ログインするか、次の手順を実行します。
   - マネージャにログインします。
   - ナビゲーションメニューで、⚙([グローバル設定(Global Settings)])アイコン をクリックし、[集中管理(Central Management)]を選択します。
   - 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情報の表示(View Appliance Statistics)]をクリックします。Flow Collector の管理インターフェイスが開きます。
   - [サポート(Support)]>[詳細設定(Advanced Settings)]の順にクリックします。
2. 次のフィールドを更新します。
   - [process_old_nvm_flows]:キャッシュフローを有効にするには、1 を入力します。
   - [nvm_age_limit_days]:キャッシュフローを収集する最大日数を入力します。たとえば、7 と入力すると、過去 7 日間のデータが収集されます。0(ゼロ)を入力した場合、制限なしになります。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、詳細設定のヘルプトピックを参照してください。

3. [適用(Apply)]をクリックします。
4. 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

フロー検索

1. マネージャにログインします。
2. [分析（Analyze）] > [フロー検索（Flow Search）] をクリックします。
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 で 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. [ダッシュボード（Dashboards）] メニューを選択します。
3. [レポートビルダー（Report Builder）] を選択します。
4. [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。
5. [実行（Run）] をクリックします。
6. レポートに NVM フィールド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。
- シスコサポートにご連絡ください。
- 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

著作権情報