Cisco StealthWatch

7.3.2 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

目次

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 Stealthwatch と 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

要件

Data Store がない Stealthwatch

- Stealthwatch v7.3.2 と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、『Stealthwatch Smart Software Licensing Guide 7.3』を参照してください。
- Cisco AnyConnect Secure Mobility Client v4.7 以降

Data Store がある Stealthwatch

- Stealthwatch v7.3.2 と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、『Stealthwatch Smart Software Licensing Guide 7.3』を参照してください。
- Cisco AnyConnect Secure Mobility Client v4.7 以降
- Stealthwatch レポートビルダー アプリ v1.4

Stealthwatch v7.3.2 での機能拡張

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 Stealthwatch 展開で Network Visibility Module（NVM）データを処理するようにフローコレクタが拡張されました。

この機能拡張により、エンドポイント コンセントレータは v7.3.2 ではサポートされません。

エンドポイントライセンスの機能

Data Store でサポートされるようになったエンドポイントライセンスは、以下を提供します。

- 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。

7.3.1 から 7.3.2 へのアップグレード

既存の Stealthwatch を 7.3.1 から 7.3.2 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、NVM の展開を再設定する必要があります。

次の手順を使用して、エンドポイントコンセントレータを削除し、Flow Collector を設定してください。

1. [集中管理（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. [アプリマネージャ（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」セクションを使用して、NVM クライアントからフローコレクタへのフローを設定します。
3. 『Stealthwatch Update Guide (v7.2.1 and v7.3.x to v7.3.2)』を使用して、クラスタを v7.3.2 に更新します。
4. 「Flow Collector の設定」セクションを使用して、フローコレクタの詳細設定に 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、レポートビルダーアプリまたは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。

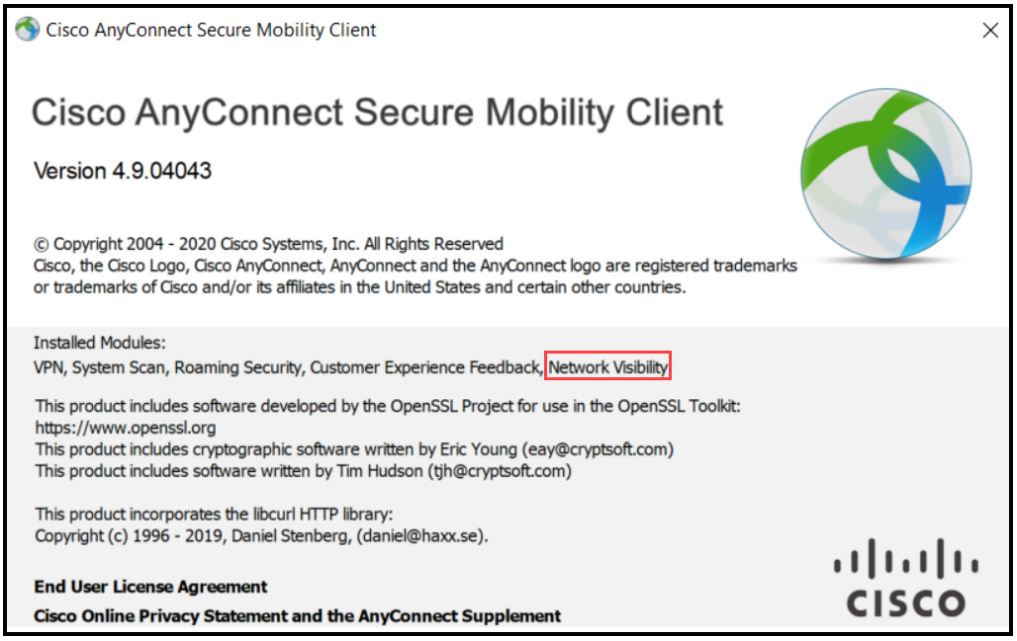
サポートが必要な場合は、Cisco Stealthwatch サポートに連絡してください。

構成

AnyConnect Secure Mobility Client での NVM プロファイルの設定

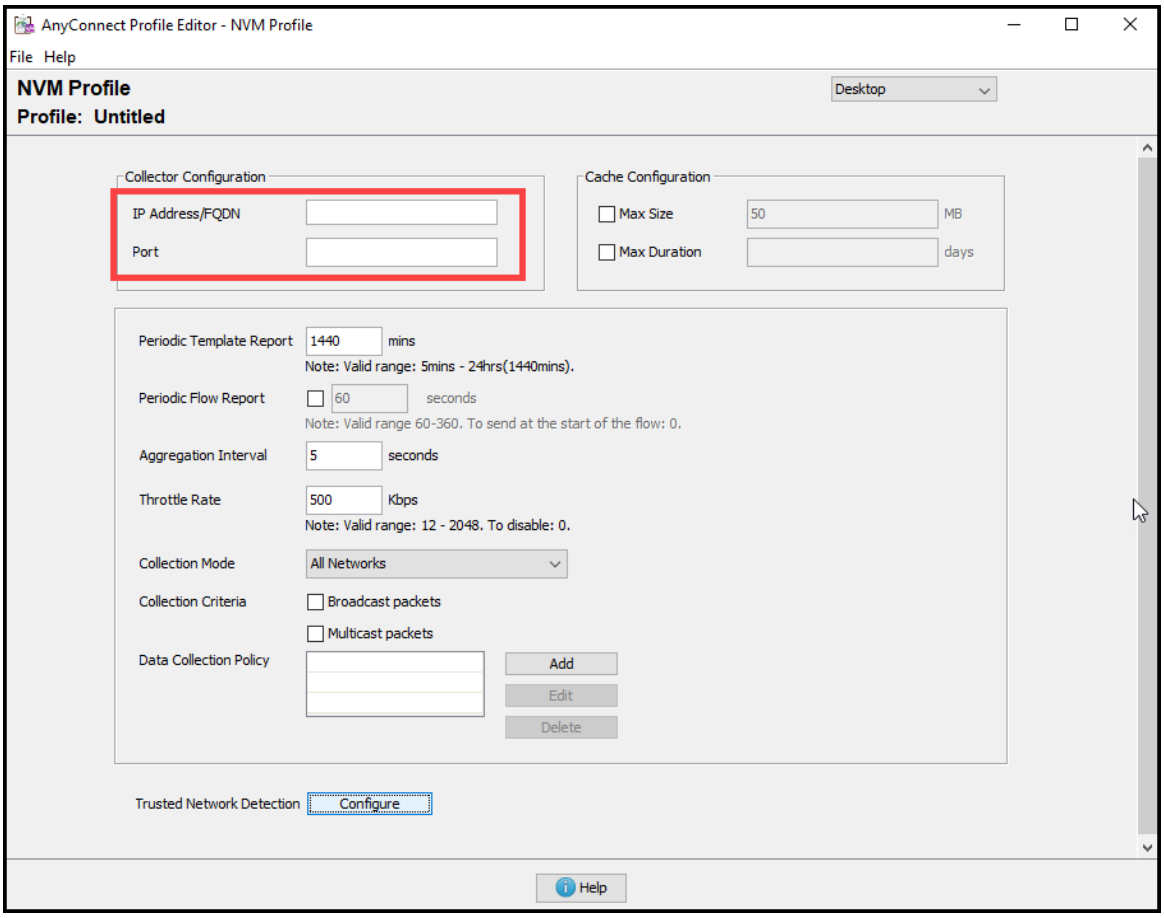
AnyConnect プロファイルエディタは、Cisco Adaptive Security Device Manager（ASDM）を介して、またはスタンドアロンとして提供されます。AnyConnect プロファイルエディタの使用方法の詳細については、『AnyConnect Administrator Guide』を参照してください。

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



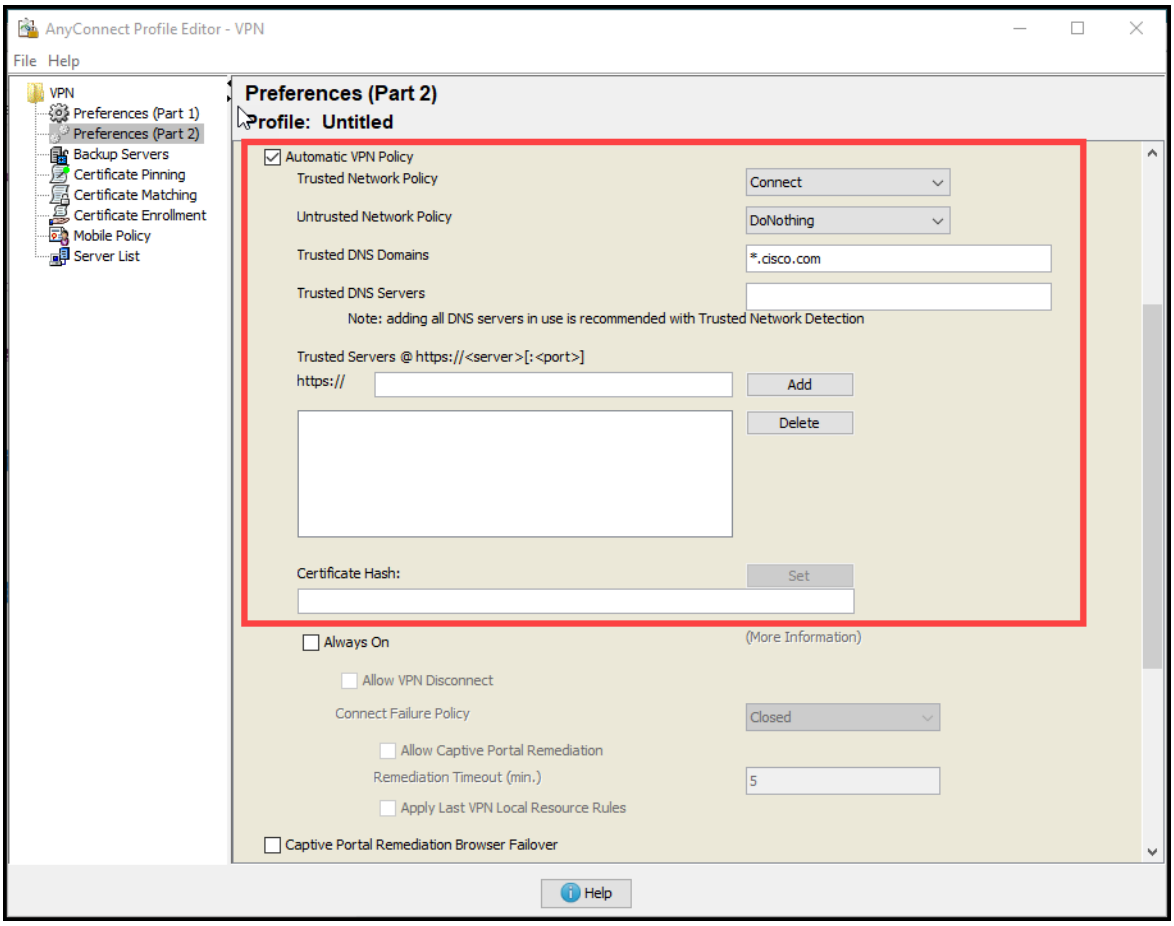
2. ネットワークの可視性モジュールのプロファイルエディタを開きます。
3. [コレクタの設定（Collector Configuration）] セクションで、Flow Collector の [IPアドレス（IP Address）] と [ポート（Port）] に入力します。

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。ポート 2055、514、8514 は使用しないでください。このポートは、「フローコレクタの設定」セクションのステップ 5 で使用します。



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。

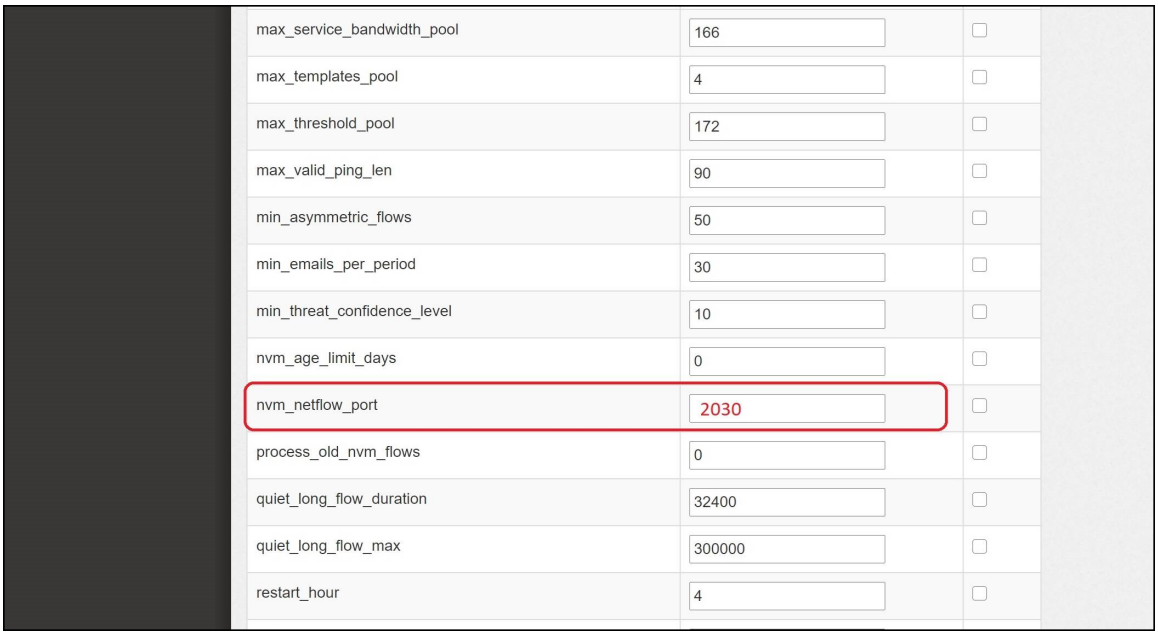


12. [ファイル(File)]>[保存(Save)]をクリックして設定を保存します。
13. AnyConnect プロファイルエディタを閉じます。

Configure the Flow Collector

1. SMC 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. [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、「Advanced Settings」オンライン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。
8. オフラインデータ収集用にフローコレクタを設定するには、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、この構成を有効にしないでください。

構成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。フローコレクタエンジンの [サポート（Support）] > [詳細設定（Advanced Settings）] で、この構成を続行します。フローコレクタ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。

- SMC 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、「Advanced Settings」オンライン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。

レポートビルダーアプリのインストール（Data Store のみ）

レポートビルダーのダウンロード

Stealthwatch アプリケーションをダウンロードするには、https://software.cisco.com で Cisco スマートアカウントにログインするか、管理者にお問い合わせください。

設置 レポートビルダー

Central Management のアプリケーションマネージャを使用してレポートビルダーをインストールします。ブラウザは Chrome または Firefox を使用することをお勧めします。アプリのインストールの詳細については、『Report Builder Release Notes』を参照してください。

> ⚠ レポートビルダーの以前のバージョンがインストールされている場合は、既存のバージョン上に新しいバージョンをインストールしてください。レポートビルダーアプリは削除しないでください。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。

1. プライマリ Stealthwatch 管理コンソールにログインします。
2. ⚙（[グローバル設定（Global Settings）]）アイコンをクリックします。
3. [集中管理（Central Management）]を選択します。
4. [アプリケーションマネージャ（App Manager）]タブをクリックします。
5. [参照（Browse）]をクリックします。
6. 画面に表示される指示に従って、アプリケーションファイルをアップロードします。

> ⓘ **必要な空きディスク領域**：/lancope/var に 600 MB。詳細については、『Report Builder Release Notes』を参照してください。

検証

フロー検索

1. Stealthwatch Management Console 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。

レポートビルダーの開始（Data Store のみ）

1. Stealthwatch 管理コンソールにログインします。
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。

> レポートビルダーのオンラインヘルプにアクセスするには、([ヘルプ（Help）]) アイコンをクリックします。ヘルプには、エンドポイントトラフィック（NVM）レポートの説明と詳細が含まれています。

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。
- Cisco Stealthwatch サポートのお問い合わせ先：
- 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

著作権情報

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワークトポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際の IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。