



Cisco Secure Network Analytics

エンドポイントライセンスおよび NVM 設定ガイド 7.4.2



目次


はじめに	3
概要	3
要件	3
7.3.0 または 7.3.1 から 7.4.2 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と Data Store 機能	4
設定	5
AnyConnect での NVM プロファイルの設定	5
NVM トラフィックを取り込むための 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
レポートビルダーの開始 (Data Store のみ)	13
サポートへの問い合わせ	14
変更履歴	15

はじめに

概要

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

- 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


 NVM を使用した 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 付きの Secure Network Analytics v7.4.2。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 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 を 7.3.0 または 7.3.1 から 7.4.2 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. [アプライアンス 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)] をクリックし、[はい (Yes)] をクリックします。
2. 「[AnyConnect](#)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。

- 『[Secure Network Analytics Update Guide](#)』の手順に従い、クラスタを v7.4.2 に更新します。
- 「[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。
- 「[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、[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

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。


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 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
- 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)		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。

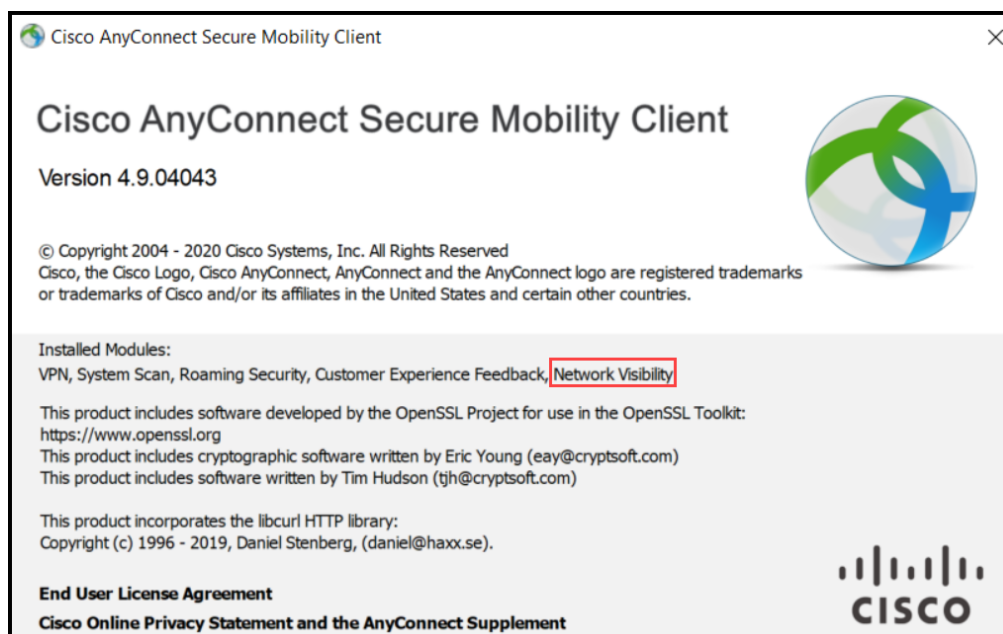
設定

AnyConnect 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。

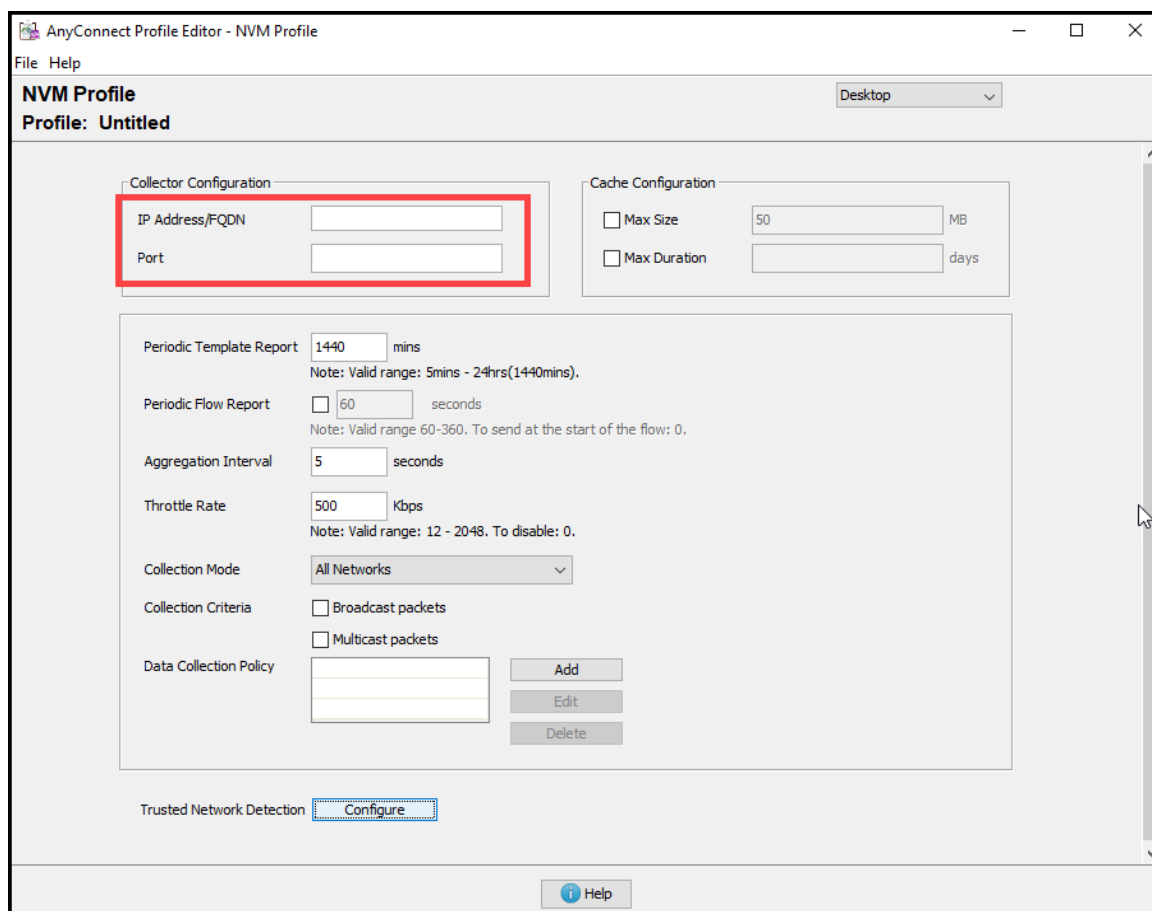


2. ネットワークの可視性モジュールのプロファイルエディタを開きます。
3. [コレクタの設定 (Collector Configuration)] セクションで、Flow Collectorの [IP アドレス (IP Address)] と [ポート (Port)] に入力します。



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。このポートは、『[Flow Collector](#) の設定」セクションで使用します。

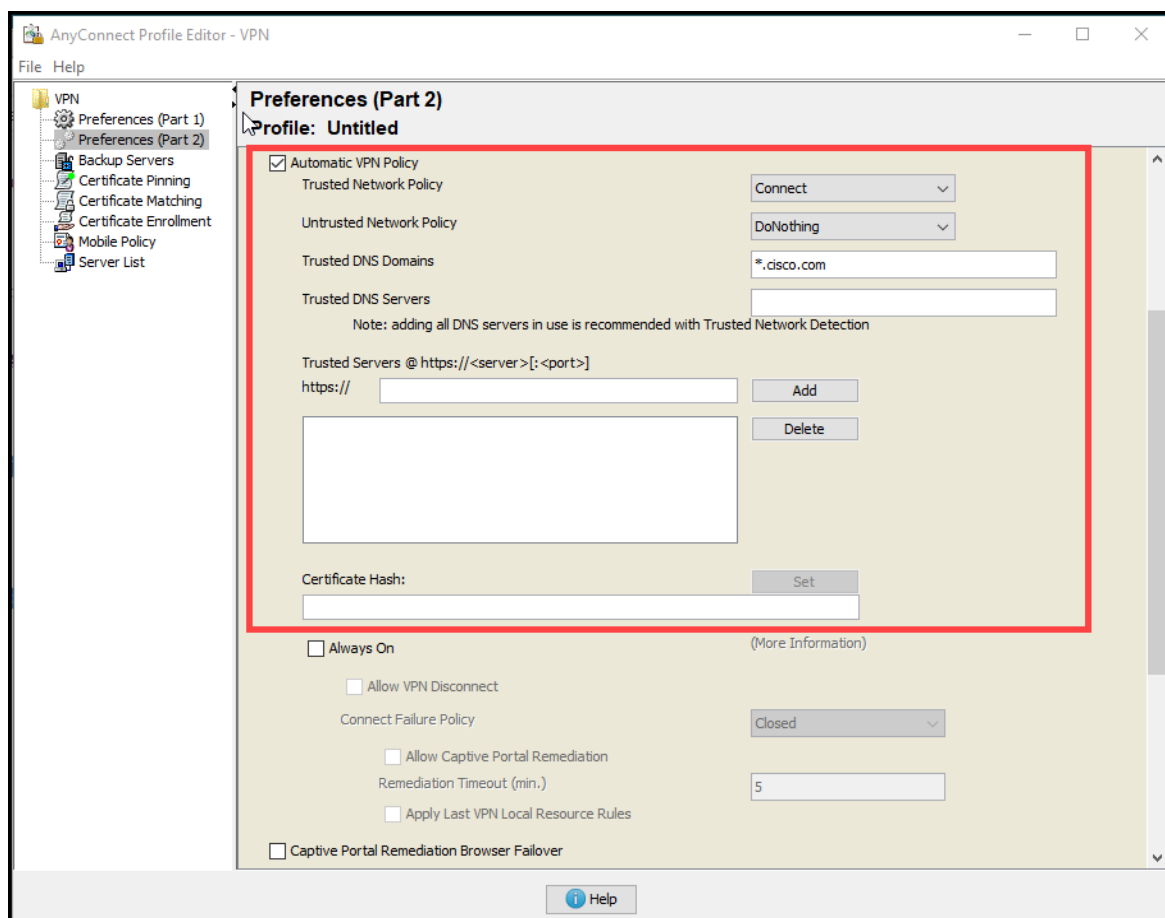
ポート 2055、514、8514 は使用しないでください。



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。

NVMトラフィックを取り込むための Flow Collector の設定

初回セットアップの使用 (Data Store のみ)

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。

```
Login information:
The user root has no failed login attempts.
Last login information:
root pts/0 10.0.7.10 Wed Nov 24 16:43 still logged in
root pts/0 10.0.7.10 Wed Nov 24 16:08 - 16:10 (00:02)
```

< OK >

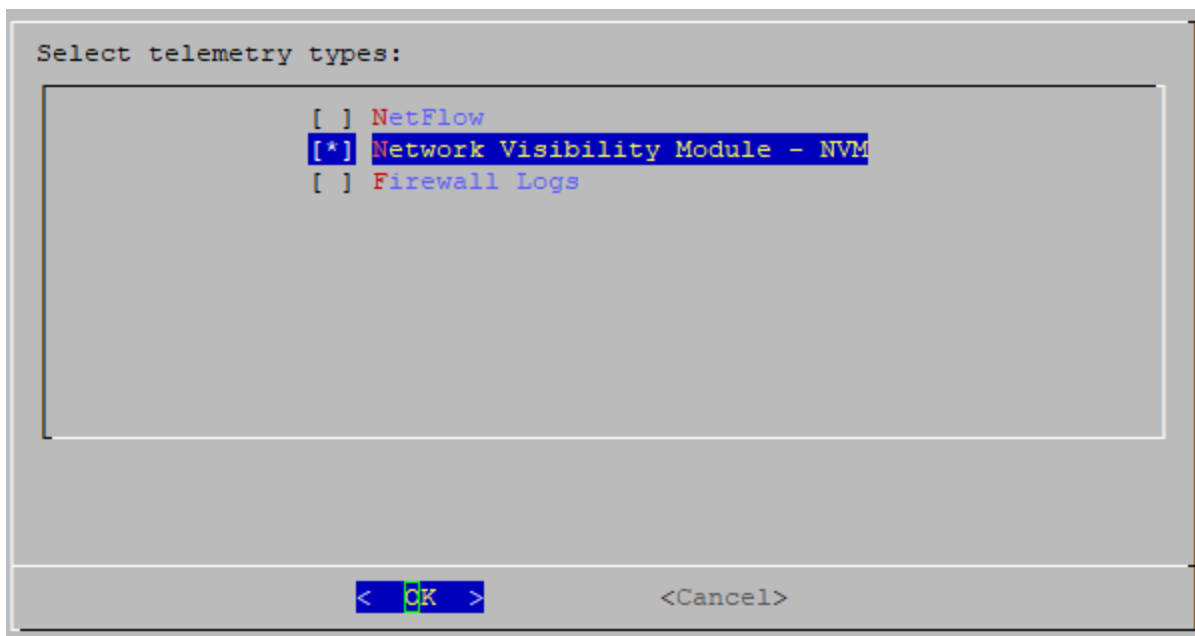
6. 初回セットアップの概要を確認します。[OK]を選択して続行します。

```
Welcome to First Time Setup. The First Time Setup wizard helps you
configure your appliance. First Time Setup takes approximately 5-10
minutes to complete, depending on your appliance model and
configuration options. Select OK to continue.
```

< OK >

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。

i 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。



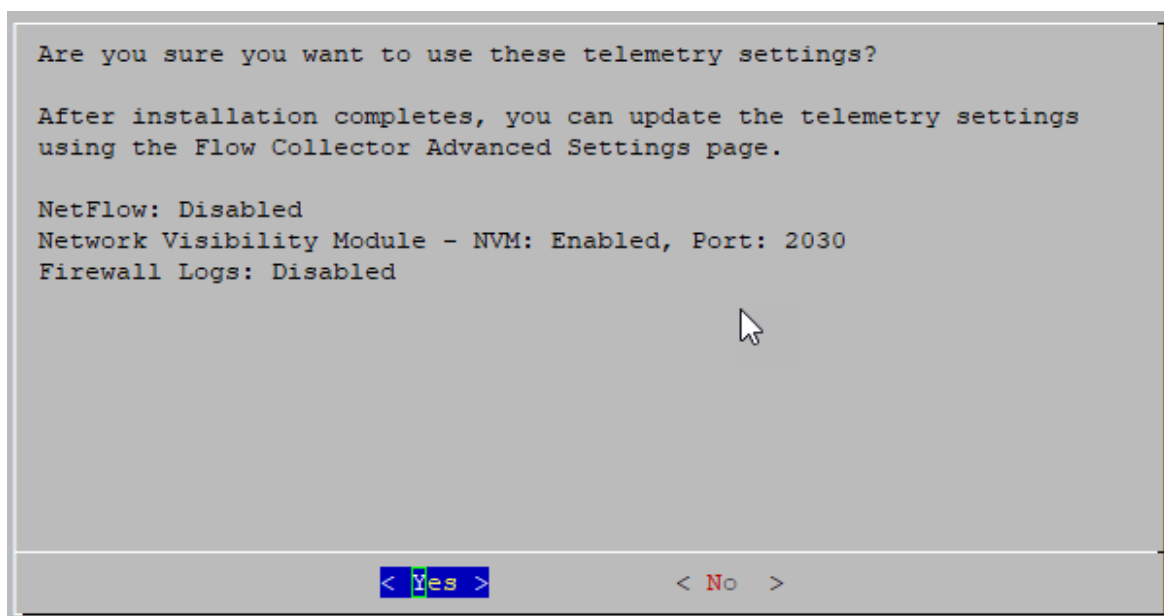
8. [Network Visibility Module - NVM] の UDP ポートを入力します。[OK] を選択します。

「[AnyConnect](#)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。



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 にエクスポートを作成し、Flow Collector エンジンのエクスポート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

- i** この手順を開始する前に、必ず [最新の Flow Collector NetFlow ロールアップパッチ](#) をインストールしてください。

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. Manager 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. インベントリページで 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情報の表示 (View Appliance Statistics)] を選択します。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)] を選択します。

- i** 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。

5. [enable_nvm] フィールドで、値を 1 に設定します。このフィールドのデフォルトは 0 です。
6. [nvm_netflow_port] フィールドで、「[AnyConnect](#) 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。

- !** 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にエクスポートを作成し、Flow Collectorエンジンのエクスポート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. NVM 取り込みフローのネットワークベースの検出をキャプチャするには、[nvm_to_flow_cache] フィールドの値を 1 に設定します。このフィールドのデフォルトは 0 です。
8. [nvm_filter_untrusted_flows] フィールドで、値を 1 に設定します。このフィールドを有効にすると、ネットワークベースの検出から信頼できないトラフィックが除外され、IP アドレスの競合などの問題が回避されます。このフィールドのデフォルトは 0 です。

Flow Collector NetFlow VE

Home	max_periods_with_drops	4	<input type="checkbox"/>
Configuration	max_valid_ping_len	90	<input type="checkbox"/>
Manage Users	min_asymmetric_flows	50	<input type="checkbox"/>
Support	min_emails_per_period	30	<input type="checkbox"/>
Audit Log	min_threat_confidence_level	10	<input type="checkbox"/>
Operations	nat_fw_subnet_len	24	<input type="checkbox"/>
Logout	nvm_age_limit_days	0	<input type="checkbox"/>
Help	nvm_endpoint_retention_minutes	1440	<input type="checkbox"/>
	nvm_filter_untrusted_flows	1	<input type="checkbox"/>
	nvm_interface_retention_minutes	1440	<input type="checkbox"/>
	nvm_netflow_port	2030	<input type="checkbox"/>
	nvm_to_flow_cache	1	<input type="checkbox"/>

i Data Store があり、[nvm_filter_untrusted_flows] フィールドの値を 1 に設定すると、信頼できないトラフィックは除外されますが、エンドポイントトラフィック(NVM)レポートの作成に使用される NVM テーブルに保存されたままになります。Data Store がない場合、信頼できないトラフィックは保持されません。

9. [適用 (Apply)] をクリックします。
10. 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 の設定 (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。

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 Administrator 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 の詳細設定 (Flow Collector Advanced Settings)] ページで、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。

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. インベントリページで 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情報の表示 (View Appliance Statistics)] を選択します。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)] 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 に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持続期間 (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


i 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. Manager 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。

レポートビルダーの開始 (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。

i 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. Manager 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 <i>Flow Collector</i> (オプション) セクションを更新しました。
2_0	2023年5月26日	<code>nvm_to_flow_cache</code> および <code>nvm_filter_untrusted_flows</code> フィールドに関連する情報を含めるために、「 <i>Flow Collector</i> の詳細設定の使用」セクションを更新しました。

著作権情報

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、URL: <https://www.cisco.com/go/trademarks> をご覧ください。記載されている第三者機関の商標は、それぞれの所有者に帰属します。「パートナー」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。(1721R)