



ネットワーク可視性モジュール

- [ネットワーク可視性モジュールについて, 1 ページ](#)
- [NVM プロファイルエディタ, 2 ページ](#)
- [NVM のコレクションパラメータ, 3 ページ](#)
- [データプライバシー, 4 ページ](#)
- [カスタマーフィードバックモジュールによる NVM ステータスの提供, 4 ページ](#)

ネットワーク可視性モジュールについて

ユーザが管理対象外デバイスを使用する状況が増加しているため、企業内管理者はネットワーク内外の状況を把握しにくくなっています。ネットワーク可視性モジュール (NVM) により、企業内管理者がキャパシティとサービスの計画、監査、コンプライアンス、およびセキュリティ分析を実行する能力が強化されます。NVM は次のサービスを提供します。

- ネットワーク設計を情報に基づいてより適切に改善する (VzFlow プロトコル仕様の IPFIX コレクタ要素の拡張) ために、アプリケーションの使用状況をモニタする
- アプリケーション、ユーザ、またはエンドポイントを論理グループに分類する
- 企業の資産を追跡し、移行アクティビティを計画するため、潜在的な異常を洗い出す

この機能により、インフラストラクチャ導入環境全体ではなく、テレメトリを対象とするかどうかを選択できます。NVM は、次の情報に対するより正確な可視性を得るため、エンドポイントテレメトリを収集します。

- デバイス：エンドポイント (場所に関係なく)
- ユーザ：エンドポイントにログインしているユーザ
- アプリケーション：トラフィックを生成するアプリケーション
- 場所：トラフィックが生成されるネットワークの場所
- 宛先：このトラフィックの宛先の実際の FQDN

信頼ネットワークでは、AnyConnect NVM はフローレコードをコレクタ（Landcope や LiveAction などのサードパーティベンダー）にエクスポートし、このコレクタがファイル分析を実行し、UI インターフェイスを提供します。Splunk などのサードパーティベンダーも、レポートを表示するための UI インターフェイスを提供します。ほとんどの企業内 IT 管理者は、データを使用して独自の可視化テンプレートを作成することを望みますが、シスコは Splunk アプリケーションプラグインを介していくつかのサンプルベーステンプレートを提供しています。

従来、シスコの NetFlow コレクタには IP ネットワークトラフィックがインターフェイスに入る時点またはインターフェイスから出る時点でこのトラフィックを収集できる機能がありました。これにより、ネットワークでの輻輳の原因を判別できる可能性がありました。NVM でエクスポートされるデータは、現在の Cisco NetFlow コレクタとは互換性がありません。これは、現在の Cisco NetFlow コレクタは IPFIX プロトコルを使用しているためです。

NVM の AnyConnect プロファイルは、ISE または ASA ヘッドエンドからプッシュされます（この機能が有効な場合）。ISE ヘッドエンドでは、スタンドアロンプロファイルエディタを使用し、NVM サービスプロファイル XML を生成して ISE にアップロードし、新しい NVM モジュールに対してマップできます。これは、Web セキュリティ、ネットワークアクセスマネージャなどでの操作と同様です。ASA ヘッドエンドでは、スタンドアロンプロファイルエディタまたは ASDM プロファイルエディタのいずれかを使用できます。

ネットワーク可視性モジュールのインストールを選択すると、AnyConnect Secure Mobility Client UI の [バージョン情報 (About)] 画面に、このモジュールがインストール済みとしてリストされます。NVM の実行中、AnyConnect UI に他の表示はありません。

VPN の状態が接続済みに変更した時点と、エンドポイントが信頼ネットワーク内にある場合に、NVM に通知が送信されます。

NVM プロファイルエディタ

このプロファイルエディタでは、コレクタサーバの IP/FQDN を設定し、データが匿名化されるかどうかを決定します。

IPv4 と IPv6 の両方をエンドポイントで有効にする場合は、コレクタの IPv4 IP アドレスを使用します。エンドポイントとコレクタ間の IPv6 通信はサポートされていません。



(注) ネットワーク可視性モジュールがフロー情報を送信するのは、信頼できるネットワーク上に限られます。デフォルトで、エンドポイントが非信頼ネットワークに接続されている場合は引き続きデータが収集され、エンドポイントが信頼ネットワーク上に存在する場合はデータが送信用にキャッシュされます。NVM は、VPN の TND 機能を使用してエンドポイントが信頼ネットワーク上にあるかどうかを確認します。また、VPN 接続状態にある場合、エンドポイントは信頼ネットワークにあると見なされ、フロー情報が送信されます。TND パラメータの設定については、[AnyConnect プロファイルエディタ](#)、[プリファレンス \(Part 2\)](#) を参照してください。

手順

- ステップ 1 コレクタとして使用される IPv4 IP アドレス/FQDN を入力します。
- ステップ 2 コレクタがリスニングするポート番号を入力します。
- ステップ 3 [ユーザ匿名化 (User Anonymization)] ドロップダウンメニューで、ユーザ情報がデータ内で匿名化される (True) かまたは匿名化されない (False) かを決定します。
- ステップ 4 エンドポイントのデータを収集する時点を指定するには、[収集モードがオフ (collection mode is off)]、[信頼ネットワークのみ (trusted network only)]、[信頼できないネットワークのみ (untrusted network only)]、または [すべてのネットワーク (all networks)] を選択します。
- ステップ 5 プロファイルを NVM_ServiceProfile.xml として保存します。
この名前でプロファイルを保存する必要があります。そうしないと、NVM はデータの収集と送信に失敗します。

NVM のコレクションパラメータ

エンドポイントで収集され、コレクタにエクスポートされるパラメータを次に示します。

フローの詳細

- [送信元 IP (Source IP)] : エンドポイントの IP アドレス。
- [送信元ポート (Source Port)] : 接続元エンドポイントのポート。
- [宛先 IP (Destination IP)] : ホストの IP アドレス。
- [宛先ポート (Destination Port)] : ホストエンドポイントが接続しようとしているポート。

[UIDID] : 固有識別子。各フローに対応するエンドポイントを一意に識別します。

[OS名 (OS Name)]

[OS のバージョン (OS Version)]

[システム製造元 (System Manufacturer)]

[システムタイプ (System Type)] : x86 または x64

[プロセスアカウント (Process Account)] : フローに関連付けられているプロセスの権限/ユーザ名

[親プロセスアカウント (Parent Process Account)] : フローに関連付けられているプロセスの親の権限/ユーザ名

[プロセス名 (Process Name)] : フローに関連付けられているプロセスの名前

[プロセスハッシュ (Process Hash)] : フローに関連付けられているプロセス イメージの SHA256 ハッシュ

[親プロセス名 (Parent Process Name)] : フローに関連付けられているプロセスの親の名前

[親プロセスハッシュ (Parent Process Hash)]: フローに関連付けられている親プロセスのプロセスイメージの SHA256 ハッシュ

[DNSサフィックス (DNS suffix)]: エンドポイントでフローに関連付けられているインターフェイスで設定されている DNS サフィックス

[宛先ホスト名 (Destination hostname)]: エンドポイントの宛先 IP に解決される実際の FQDN/ホスト名

[L4ByteCountIn]: レイヤ 4 でのそのフローの入力バイト合計数 (ペイロードのみ、L4 ヘッダーは含まない)

[L4ByteCountOut]: レイヤ 4 でのそのフローの出力バイト合計数 (ペイロードのみ、L4 ヘッダーは含まない)



(注) また NVM は、エンドポイントのアイデンティティに関する情報を定期的に送信します。

データ プライバシー

ディスクに保存される NVM データはすべて難読化されます。デバイスを再起動すると、データが失われます。

カスタマーフィードバックモジュールによるNVMステータスの提供

カスタマーフィードバックモジュールコレクションの一部は、NVM がインストールされているかどうかを示すデータを提供します。