Network Visibility Module コレクタ リリース 5.1.1 インストールおよびコンフィギュレーション ガイド

改訂：2024 年 5 月 16 日,

Network Visibility Module コレクタの概要

このドキュメントでは、「Cisco Software Download」ページからダウンロードできる Network Visbility Module（NVM）コレクタをインストールおよび設定する方法を説明します。NVM のコンポーネント、セットアップ方法、インストールとコレクタのステータスの検証方法および基本的なトラブルシューティングの実行方法について説明します。詳細については、『Release Notes for Cisco Secure Client Network Visibility Module Collector』を参照してください。

Cisco Secure Client は、企業を保護するために複数のセキュリティサービスを提供する統合エージェントであり、エンタープライズ セキュリティのさまざまな側面に対応する追加モジュールもサポートします。この追加モジュールにより、ポスチャアセスメント、マルウェア保護、ローミングセキュリティなどのセキュリティ機能が有効になります。

Cisco Secure Client Network Visibility Module は、高価値なエンドポイントテレメトリの継続的なフィードを提供します。Network Visibility Module を使用して、組織はネットワーク上のエンドポイントとユーザーの動作を確認できます。ユーザー、アプリケーション、デバイス、場所、宛先など貴重なコンテキストとともに、オンプレミスとオフプレミス両方のエンドポイントからフローを収集します。このデータをキャッシュし、信頼できるネットワーク（オンプレミスまたは VPN 経由の企業ネットワーク）上にある Network Visibility Module コネクタに送信します。

Network Visibility Module コネクタは、Internet Protocol Flow Information Export（IPFIX） （4 ページ）のデータを受信し、必要に応じてフィルタ処理を実行して、syslog または Splunk にエクスポートするサーバーです。Network Visibility Module コレクタは、nvzFlow プロトコル仕様（https://developer.cisco.com/site/network-visibility-module/）に準拠する受信メッセージを処理します。コレクタは、スタンドアロンの Linux システムにインストールできます。

Network Visibility Module コネクタのコンポーネントと要件

次の項目に関する知識が推奨されます。

- Cisco Secure Client と Network Visibility Module
- Cisco Secure Client のライセンス
- Network Visibility Module コレクタのライセンス

NVM コレクタを別の Linux デバイスで実行する場合は、次の一般的な拡張性を使用して、デバイスあたり 35,000 ～ 40,000 エンドポイントで計画を立てる必要があります。

- CPU/メモリのサイジングを削減可能
- ロギングはコレクタと Linux に対してのみ行われるため、ディスクの入出力は適用不可
- OS およびコレクタコンポーネントを実行するための 50 GB のディスク容量

スタンドアロン Network Visibility Module コレクタのハードウェアサイジング

以下に、64 ビットの Linux で実行されるスタンドアロン Network Visibility Module コネクタインスタンスの推奨ハードウェア要件を示します。

（注） デフォルトでは、Network Visibility Module のマルチプロセスモードは有効になっています。

- 最大 1,000 のエンドポイント/サーバーインスタンス：
  - CPU コア：6 コア / 2.2 GHz（x86 64 ビット）
  - RAM サイズ：8 GB
  - 複合 IOPS：800 入出力処理/秒（IOPS）
  - ディスクサブシステム：任意（10k RPM 以上）
  - 総ディスク容量：50 GB
- 1,000 ～ 5,000 エンドポイント/サーバーインスタンス：
  - CPU コア：8 コア/2.4 GHz（x86 64 ビット）
  - RAM サイズ：16 GB
  - 複合 IOPS：1,000 入出力処理/秒（IOPS）
  - ディスクサブシステム：任意（10k RPM 以上）
  - 総ディスク容量：50 GB
- 7,500 ～ 10,000 エンドポイント/サーバーインスタンス：
  - CPU コア：12 コア/2.6 GHz（x86 64 ビット）
  - RAM サイズ：24 GB
  - 複合 IOPS：1,200 入出力処理/秒（IOPS）
  - ディスクサブシステム：任意（10k RPM 以上）
  - 総ディスク容量：50 GB

Internet Protocol Flow Information Export（IPFIX）

IPFIX は、アカウンティング、監査、セキュリティなどの多様な目的のために IP フロー情報をエクスポートする際の標準を定義する、IETF プロトコルです。IPFIX は Cisco NetFlow プロトコル v9 を基本にしています。ただし直接的な互換性はありません。Cisco vzFlow は、IPFIX プロトコルに基づくプロトコル仕様です。設計上、IPFIX は拡張可能なプロトコルで、情報を伝達する新しいパラメータを定義できます。Cisco nvzFlow プロトコルは、IPFIX 標準を拡張し、新しい情報要素と、Cisco Secure Client Network Visibility Module によって使用されるテレメトリの一部として伝達される IPFIX テンプレートの標準セットを定義します。

IPFIX フローテンプレートは、IPFIX 通信の開始時にコレクタに送信されます。これらのテンプレートは、コレクタが IPFIX データの意味を解明するために役立ちます。まれに、テンプレートが見つからないことがあります。この問題は、エンドポイントのパケットキャプチャの「No template found」メッセージ、またはコレクタログの「No templates for flowset」メッセージで示されます。この問題を解決するには、エンドポイントの 1 つを再起動します。

Network Visibility Module コレクタでエクスポートされるデータフィールド

Network Visibility Module コネクタは、エンドポイント、インターフェイス、およびフローの 3 種類のデータレコードをエクスポートします。各データレコードは、フィールドのキーと値のペアのセットです。以下の表に、フィールドキー、フィールド名、および指定のフィールドキーが存在するデータレコードのコンテキストを示します。

フィールドキー	フィールド名	フィールドコンテキスト	フィールドの説明
agv	Agent バージョン	endpoint	エージェント/クライアントのソフトウェアバージョン。通常は major_v.minor_v.build_no の形式（Cisco Secure Client Network Visibility Module 4.9 以降）。ネットワークフローが生成されるエンドポイントの物理デバイスにログインしているユーザー名（Authority\Principal 形式）ドメインユーザーは、デバイスにローカルでログインしているユーザーと同じ形式で表されます（MYDOMAIN\aduser または SOMEMACHINE\localuseracct など）。
aliul	追加のログインユーザーリスト	flow	（Windows のみ）nvzFlowLoggedInUser 以外のデバイスにログインしているユーザーのリスト（各ユーザーは SessionType:AccountType:Authority\Principal の形式で表される） 例：rdp:8001:ACME\JSmith console:0002:<machine>\Administrator （注） このフィールドは、非システムプロセスの場合は空です。

フィールドキー	フィールド名	フィールドコンテキスト	フィールドの説明
ampguid	AMP GUID	endpoint	Cisco Secure Endpoint（AMP）の一意のエンドポイントID
ctm	timestamp	エンドポイント、インターフェイス	エンドポイントデータまたはインターフェイスレコードの絶対タイムスタンプ（ミリ秒単位）
da	宛先IPv4アドレス	flow	フローがエンドポイントから生成された宛先の IPv4 アドレス。
da6	DestinationIPv6Address	flow	フローがエンドポイントから生成された宛先の IPv6 アドレス。
dh	FlowDestinationHostName	flow	ネットワークフローがエンドポイントに送信された宛先アドレスの宛先ドメイン。
DP	DestinationTransportPort	flow	フローがエンドポイントから生成された宛先ポート番号。
ds	FlowDNSSuffix	flow	エンドポイントでネットワークフローが生成されたときにユーザーが接続していたネットワークで設定された DNS サフィックス。
fd	フローの方向	flow	エンドポイントで観測されたフローの方向。定義される 2 つの値は 0（入力フロー）と 1（出力フロー）です。
fems	FlowEndMsec	flow	ネットワークフローがエンドポイントで完了したときのタイムスタンプ（ミリ秒単位）（Cisco Secure Client NVM 4.9 以降の場合）。
fes	EndSeconds	flow	ネットワークフローがエンドポイントで完了されたときのタイムスタンプ。
fsg	フローレポートステージ	flow	フローレコードのステージ。0：終了フローレコード、1：開始フローレコード、2：定期/中間フローレコード。
fsms	FlowStartMsec	flow	ネットワークフローがエンドポイントで開始されたときのタイムスタンプ（ミリ秒単位）（Cisco Secure Client NVM 4.9 以降の場合）。
fss	StartSeconds	flow	エンドポイントでネットワークフローが開始されたときのタイムスタンプ。
fv	FlowVersion	flow	クライアントから送信された Network Visibility Flow（nvzFlow）のバージョン。

フィールドキー	フィールド名	フィールドコンテキスト	フィールドの説明
hh	HTTP ホスト	flow	HTTP/1.1 トラフィックの HTTP ホストヘッダーの内容
ibc	InBytesCount	flow	レイヤ4のエンドポイントでの特定のフロー中にダウンロードされた合計バイト数（L4 ヘッダーを除く）。
ii	InterfaceIndex	interface	オペレーティングシステムによって報告されたネットワーク インターフェイスのインデックス。
iid	[InterfaceInfoUID]	flow interface	インターフェイスメタデータの一意の ID。InterfaceInfo レコードからインターフェイスメタデータを検索するために使用します。
im	InterfaceMacAddress	interface	インターフェイスの MAC アドレス。
in	InterfaceName	interface	オペレーティングシステムによって報告されたネットワーク インターフェイス/アダプタの名前。
ist	TrustState	interface	InterfaceDetailsList から解析されます。これは STATE 部分です（例: STATE=Trusted）。Cisco Secure Client VPN がアクティブであるか、TND に基づいてデバイスが信頼できるネットワーク上にあると判断しています。
it	InterfaceType	interface	インターフェイスのタイプ（有線、ワイヤレス、セルラー、VPN、トンネル化、Bluetooth など）。ネットワークタイプの列挙。
liuid	LoggedInUser	flow	このフィールドが空の場合、デバイスにログインしているユーザーがいないか、ユーザーが RDP、SSH などを介してリモートでデバイスにログインしていることを示します。その結果、liuida フィールドと liuidp フィールドも空になります。ユーザー情報は引き続きプロセスアカウント情報から取得できます。
liuida	LoggedInUserAuthority	flow	ネットワークフローが生成される物理デバイスにログインしているユーザー名の権限部分。
liuidp	LoggedInUserPrincipal	flow	ネットワークフローが生成される物理デバイスにログインしているユーザー名のプリンシパル部分。
luat	LoggedInUserAccountType	flow	AccountType の列挙に示される、ログインユーザーのアカウントタイプ。
mhl	ModuleHashList	flow	nvzFlowModuleNameList に関連付けられているモジュールの 0 個以上の SHA256 ハッシュのリスト。

フィールドキー	フィールド名	フィールドコンテキスト	フィールドの説明
mnl	ModuleNameList	flow	フローを生成したプロセスによってホストされているモジュールの 0 個以上の名前のリスト。この名前には、dllhost、svchost、rundll32 などの共通コンテナのメインの DLL を含めることができます。また、JVM の jar ファイルの名前など、ホストされている他のコンポーネントを含めることもできます。
obc	OutBytesCount	flow	レイヤ 4 のエンドポイントでの特定のフロー中にアップロードされた合計バイト数（L4 ヘッダーを除く）。
osn	[OS 名（OS Name）]	endpoint	エンドポイントのオペレーティングシステムの名前（WinNTなど）。この名前は、AnyConnect VPN から ASA に送信される値と一致します。
osv	[OS のバージョン（OS Version）]	endpoint	エンドポイントのオペレーティングシステムのバージョン（6.1.7601 など）このバージョンは、AnyConnect VPN から ASA に送信される値と一致します。
pa	ProcessAccount	flow	エンドポイントでネットワークフローを生成するアプリケーションが実行されたコンテキストでの Authority\Principal 形式の完全修飾アカウント。
paa	ProcessAccountAuthority	flow	エンドポイントでネットワークフローを生成するアプリケーションが実行されたコンテキストでの完全修飾アカウントの権限部分。
pap	ProcessAccountPrincipal	flow	エンドポイントでネットワークフローを生成するアプリケーションが実行されたコンテキストでの完全修飾アカウントのプリンシパル部分。
parg	ProcessArgs	flow	ネットワークフローを開始したプロセスのコマンドライン引数（Cisco Secure Client NVM 4.9 以降の場合）。
ph	ProcessHash	flow	エンドポイントでネットワークフローを生成する実行可能ファイルの一意の SHA256 ハッシュ。
pid	ProcessId	flow	ネットワークフローを開始したプロセスのプロセス ID（Cisco Secure Client NVM 4.9 以降の場合）。
pil	プロセス完全性レベル	flow	完全性レベルは、プロセスと別のオブジェクト（ファイル、プロセス、またはスレッド）間の信頼を定義します。

フィールドキー	フィールド名	フィールドコンテキスト	フィールドの説明
-PN	ProcessName	flow	エンドポイントでネットワークフローを生成する実行可能ファイルの名前。
ppa	ParentProcessAccount	flow	エンドポイントでネットワークフローを生成するアプリケーションの親プロセスが実行されたコンテキストでの Authority\Principal 形式の完全修飾アカウント。
ppaa	ParentProcessAccountAuthority	flow	エンドポイントでネットワークフローを生成するアプリケーションの親プロセスが実行されたコンテキストでの完全修飾アカウントの権限部分。
ppap	ParentProcessAccountPrincipal	flow	エンドポイントでネットワークフローを生成するアプリケーションの親プロセスが実行されたコンテキストでの完全修飾アカウントのプリンシパル部分。
pparg	ParentProcessArgs	flow	ネットワークフローを開始したプロセスの親のコマンドライン引数（Cisco Secure Client NVM 4.9 以降の場合）。
ppath	ProcessPath	flow	ネットワークフローを開始したプロセスのファイルシステムパス（Cisco Secure Client NVM 4.9 以降の場合）。
pph	ParentProcessHash	flow	エンドポイントでネットワークフローを生成するアプリケーションの親プロセスの実行可能ファイルの一意の SHA256 ハッシュ。
ppid	ParentProcessId	flow	ネットワークフローを開始したプロセスの親のプロセス ID（Cisco Secure Client NVM 4.9 以降の場合）。
ppil	親プロセスの完全性レベル	flow	完全性レベルは、親プロセスと別のオブジェクト（ファイル、プロセス、またはスレッド）間の信頼を定義します。
ppn	ParentProcessName	flow	エンドポイントでネットワークフローを生成するアプリケーションの親プロセスの名前。
pppath	ParentProcessPath	flow	ネットワークフローを開始したプロセスの親のファイルシステムパス。
ppuat	ParentProcessAccountType	flow	AccountType の列挙に示される、親プロセスアカウントのアカウントタイプ。
pr	ProtocolIdentifier	flow	各フローに関連付けられたネットワークプロトコル番号。現在、TCP（6）と UDP（17）のみをサポートしています。

フィールドキー	フィールド名	フィールドコンテキスト	フィールドの説明
puat	ProcessAccountType	flow	AccountType の列挙に示される、プロセスアカウントのアカウントタイプ。
sa	SourceIPv4Address	flow	フローがエンドポイントで生成されたインターフェイスの IPv4 アドレス。
sa6	SourceIPv6Address	flow	フローがエンドポイントで生成されたインターフェイスの IPv6 アドレス。
sm	[SystemManufacturer]	endpoint	エンドポイントの製造元（Lenovo、Apple など）。
sp	sourceTransportPort	flow	フローがエンドポイントで生成された送信元ポート番号。
SSID	SSID	interface	InterfaceDetailsList から解析されます。これは SSID 部分です（例：SSID=internet）。
st	System Type	endpoint	
udid	UDID	flow endpoint interface	ネットワーク内の各エンドポイントの一意の識別子。ハードウェア属性から取得および再作成され、レコードを単一のソースに関連付けるために使用されます。これは、AnyConnect VPN から ASA に送信される同じ値と一致します。
vsn	VirtualStationName	endpoint	エンドポイントで設定されたデバイス名（Boris-Macbook など）。ドメイン参加マシンの形式は [machinename].[domainname].[com]（CESA-WIN10-1mydomain.com など）になります。

NVM コネクタのホスト型ファイアウォールの推奨事項

Network Visibility Module コネクタノードで推奨されるホスト型ファイアウォール設定は次のとおりです。

- インバウンド：acnvm.conf ファイルで構成された *netflow_collector_port* ですべての Network Visibility Module ホストの UDP トラフィックを許可します。
- アウトバウンド：acnvm.conf ファイルで設定された（*syslog_flowdata_server_port*、*syslog_sysdata_server_port*、および *syslog_intdata_server_port* の）設定済み *syslog_server_ip*ポートへの UDP トラフィックのみを許可します。

コレクタからの他のすべての着信および発信トラフィックは、コレクタノードの他のソフトウェアに必要ない限り、ブロックされます。

Network Visibility Module コレクタのセットアップ

Network Visibility Module コレクタをセットアップするには、次の手順に従います。

1. Linux での Network Visibility Module コレクタのインストールまたはアップグレード （10 ページ）。

   または

   Docker イメージのビルド （10 ページ）。

2. 複数コアを持つホストのサーバープロセスの調整 （10 ページ）。

3. Network Visibility Module コネクタフローのフィルタ処理 （11 ページ）。

その後、以下のコレクタのエクスポートのオプション （12 ページ）に進みます。

Linux での Network Visibility Module コレクタのインストールまたはアップグレード

手順

ステップ 1 *Cisco* ソフトウェア ダウンロード サイトから acnvmcollector-version.zip をダウンロードします。

ステップ 2 .zip ファイルを任意の一時ディレクトリに解凍します。

ステップ 3 新規インストールの場合は、コレクタのエクスポートのオプション （12 ページ）、コレクタ DTLS の設定 （13 ページ）、またはNetwork Visibility Module コネクタフローのフィルタ処理 （11 ページ）に従って構成設定を変更します。アップグレードの場合、既存の設定は保持されます。

ステップ 4 スーパーユーザー権限で install.sh スクリプトを実行します。

Docker イメージのビルド

Docker コンテナで Network Visibility Module コレクタを実行できます。acnvmcollector ファイルには、Dockerfile イメージが含まれています。Docker イメージをビルドするためのパラメータは acnvm.conf ファイルに依存するため、Docker イメージをビルドする前に（必要に応じて）acnvm.conf ファイルの設定を調整する必要があります。Docker ファイルを含むディレクトリで、イメージをビルドします。

```
docker build -t nvmcollector
```

コレクタがポート 2055 でリッスンし、syslog サーバーが同じホスト上にあるデフォルト設定では、次のように入力します。

```
docker run -t -p 2055:2055/udp --net="host" nvmcollector
```

複数コアを持つホストのサーバープロセスの調整

Network Visibility Module コネクタのマルチコア動作を調整したり、フィルタリング機能を包含または除外できます。この調整は、主にLinuxのインストールを実行した場合に使用されます。デフォルトでは、複数のコアを持つホストで実行する場合、コレクタはコアごとに個別のサーバープロセスを作成します。プロセスを調整して、1つのサーバープ

ロセスのみ実行するか、2つのサーバープロセスを実行できます。マルチコアプロセスを無効にするオプションもあります。

マルチプロセッシングを無効にして単一プロセスを実行するには、次のようにします。

```
{
            "multiprocess":
                {"enabled": false}
}
```

2 つのサーバープロセスを実行するには次のようにします。

```
{
    "multiprocess":
        {
            "enabled": true,
            "numProcesses": 2
        }
}
```

Network Visibility Module コネクタフローのフィルタ処理

コネクタは、別の JSON ポリシーファイルで定義されているオプションの 3 つのフローフィルタリングモード（包含、除外、ハイブリッド）をサポートします。コネクタの起動時にポリシーファイルのパスを指定する必要があります。コネクタはデフォルトでは /opt/acnvm/conf/acnvmfilters.conf ファイルに保存されているポリシーを検索します。

ポリシーが存在しない場合、フィルタリングは無効になり、すべてのフローが処理されてエクスポートされます。3つのフィルタリングモードは次のように動作します。

- [包含のみ（Include Only）]：デフォルトでは、包含ルールに一致しない限りフローはドロップされます。
- [除外のみ（Exclude Only）]：デフォルトでは、除外ルールに一致しない限りフローが収集されます。
- [包含＋除外（ハイブリッド）（Include + Exclude (hybrid)）]：デフォルトでは、フローが包含ルールかつ除外ルールに一致した場合を除き、フローはドロップされます。

各ルールはJSONディクショナリとして指定され、各キーと値の各ペアでフローフィールド（名前がキーと一致する）の一致基準を指定します。文字列フィールドタイプではサフィックスワイルドカードがサポートされ、アスタリスクで示されます。

すべての DNS フローを除外する例

```
{
    "rules":
        {
            "exclude":
            [
                {"dp": 53, "pr": 17}
            ]
        }
}
```

特定の DNS サーバーへのフローを除外する例

```
{
     "rules":
        {
            "exclude":
            [
                {"dp": 53, "pr": 17, "da": "1.2.*"}
```

```
                {"dp": 53, "pr": 17, "da": "8.8.8.8"}
            ]
        }
}
```

Angry Birds（Android アプリ）からのみフローを収集し、DNS フローを無視する例

```
{
    "rules":
        {
            "include":
            [
                {"pname": "com.rovio.angrybirds")
            ],
            "exclude":
            [
                {"dp": 53, "pr": 17, "da": "1.2.*"},
                {"dp": 53, "PRP: 17, "da": "8.8.8.8"}
            ]
        }
}
```

コレクタのエクスポートのオプション

現在、コレクタエクスポータは、syslog、Kafka、またはユーザー独自のエクスポータ（カスタムプラグインを使用）をサポートしています。

Syslog エクスポートの設定例

```
{
    "exporter": {
        "type": "syslog",
        "syslog_server": "localhost",
        "flow_port": 20519,
        "endpoint_port": 20520,
        "interface_port": 20521
    }
}
```

Kafka エクスポートの設定例

```
{
    "exporter": {
        "type": "kafka",
        "bootstrap_server": "localhost:9092",
        "flow_port": "flow",
        "endpoint_port": "endpoint",
        "interface_port": "interface"
    }
}
```

カスタムプラグインの例

プラグイン API に対して共有ライブラリを構築することで、ネイティブ C++ コードを使用してコレクタのエクスポート機能を拡張できます。カスタムプラグインを使用するには、メインコレクタの設定に特別な設定が必要です。

```
{
    "exporter": {
        "type": "plugin"
    }
}
```

コレクタ DTLS の設定

データが DTLS 経由でコレクタに安全に送信されるように Network Visibility Module（NVM）を設定できます。Network Visibility Module プロファイルエディタで、[セキュア（Secure）] チェックボックスがオンになっている場合、Network Visibility Module はトランスポートとして DTLS を使用します。DTLS 接続を機能させるためには、DTLS サーバー（コレクタ）証明書がエンドポイントによって信頼されている必要があります。信頼できない証明書はサイレントに拒否されます。サポートされる最小バージョンは DTLS 1.2 です。コレクタは、セキュアまたは非セキュアのいずれかのモードでのみ機能します。

次の証明書要件も満たされている必要があります。

- コレクタ証明書/証明書チェーンがクライアントによって信頼されている必要があります（Cisco Secure Client には設定は存在しません）。
- 証明書は PEM 形式である必要があります。
- 証明書キーのパスワードはサポートされていません（Cisco Identity Services Engine（ISE）およびその内部認証局に必要）。
- Cisco Secure Client で信頼されている証明書であればコネクタではどの証明書でも使用できます（たとえば、内部 Public Key Infrastructure（PKI）やその他のよく知られている証明書は信頼されます）。
- Cisco Secure Client NVM プロファイルコレクタの設定は、証明書の共通名（CN）が使用するものに基づいて、IP または FQDN に設定する必要があります。IP アドレスが変更された場合は、常に FQDN が優先されます。IP アドレスを使用する場合、コレクタ証明書の CN またはサブジェクト代替名（SAN）にその IP が必要です。証明書に CN として FQDN が含まれる場合、Network Visibility Module プロファイルにコレクタと同じ FQDN が必要があります。

構成ファイルが更新されたら、Cisco Secure Client Network Visibility Module サービスを再起動します。ISE または ASA からプッシュされたプロファイルはすべて、ネットワークから切断して再接続する必要があります。

DTLS 用のコレクタの設定

コレクタをホストするデバイスで次の手順を実行します。

始める前に

コレクタ DTLS の設定 （13 ページ）セクション参照してください。

手順

ステップ 1 **/opt/acnvm/certs** ディレクトリを作成します。

ステップ 2 証明書をコレクタに適用できるように、証明書とキーを /opt/acnvm/certs ディレクトリに保存します。証明書と秘密キーファイルが PEM 形式であることを確認します。

ステップ 3 コマンド **sudo chown -R acnvm:acnvm certs/:** を使用して、フォルダの所有者とグループを **acnvm:acnvm** に変更します。

ステップ 4 コマンド **sudo chmod 400 *** で、/opt/acnvm/certs にある証明書と秘密キーファイルのアクセス許可を 400 に設定します。

ステップ 5 証明書とキーを使用して acnvm.conf セクションを設定します。

ステップ 6 設定と証明書の準備ができたら、**sudo systemctl restart acnvm.service** でコレクタを再起動します。

ステップ 7 **sudo systemctl status acnvm.service** コマンドを使用して、コレクタのステータスを確認します。

```
{
    "security": {
        "dtls_enabled": true,
         "server_certificate":"opt/acnvm/certs/public.pem",
         "server_pkey":"/opt/acnvm/certs/private.pem",
    }
```

他の設定は次のようになります。

```
"syslog_server_ip" : "192.0.2.113",
        "syslog_flowdata_server_port" : 20519,
        "syslog_sysdata_server_port" : 20520,
        "syslog_intdata_server_port" : 20521,
        "netflow_collector_port" : 2055
},
```

ステップ 8 スーパーユーザー権限 **sudo./install.sh** で **install.sh** スクリプトを実行します 。
このアカウントには、install.sh スクリプトを実行するための sudo 権限または root と、acnvm サービス アカウントの権限が必要です。

Network Visibility Module のインストールの検証

インストールが成功したら、Network Visibility Module が、 Cisco Secure Client の [情報（Information）] セクション内にある [インストール済みモジュール（Installed Modules）] にリストされます。Network Visibility Module サービスがエンドポイントで実行されているかどうか、およびプロファイルが必要なディレクトリにあるかどうかを確認します。

コレクタのステータスの確認

コレクタが常にエンドポイントから IPFIX/cflow を受信していることを確認して、コレクタが実行されていることを確認します。コネクタが実行されていない場合は、ファイルの acnvm アカウント権限で /opt/acnvm/bin/acnvmcollector の実行が許可されているか確認します。

コレクタ診断ツール

コレクタ診断ツールは、Network Visibility Module コレクタのインストールおよび接続の問題をトラブルシューティングするためのデータを収集するためのコマンドラインツールです。このツールによってログ、ステータス、診断情報が収集され、それを Cisco Technical Assistance Center（TAC）での分析に使用できます。NVM コレクタが実行されているデバイスで acnvmcolldiag ツールを実行し、スーパーユーザーとしてコマンドラインから起動して、診断情報を収集します。

コレクタ診断ツールの実行

以下のコマンドによって実行されるタスクは、/opt/acnvm/conf/acnvmcolldiagconf.json ファイルにある構成ファイルによって異なります。

手順

ステップ 1 /opt/acnvm/bin/acnvmcolldiag - p **<診断結果を保存するディレクトリパス>**と入力してコレクタ診断ツールを起動します。

ステップ 2 acnvmcolldiag というプレフィックスが付いた zip ファイルが作成され、指定されたパスに保存されていることを確認します。

基本的なトラブルシューティング

結果が予想どおりでない場合は、次の点を確認してください。

- クライアントのエンドポイントとコレクタ間のネットワーク接続。
- クライアントエンドポイントへの Network Visibility Module のインストール。
- エンドポイントのキャプチャに IPFIX トラフィックが生成されていることが示されているかどうか。
- コレクタのキャプチャに IPFIX トラフィックが受信および転送されていることが示されているかどうか。
- サードパーティコレクタのキャプチャにトラフィックを受信したことが示されているかどうか。
- DTLS の場合、Cisco Secure Client クライアントはコレクタ証明書を信頼し、Network Visibility Module プロファイルをセキュアとして有効化している必要があります。また、コレクタが証明書用に設定されている必要があります。クライアントとコレクタの間で DTLS を実行している場合は、Wireshark 内の DTLS トラフィックをフィルタ処理する必要があります。

Network Visibility Module データベースのサイズが拡大している

C:/%ProgramData%\Cisco\Cisco Secure Client で Network Visibility Module データベースのサイズが拡大していることに気づいた場合、ログはクライアントから送信されていません。Network Visibility Module フォルダと SQL データベースはサイズの拡大を示し、さらにデータがコレクタに送信されていないことを示しています。Network Visibility Module でのキャッシュ方法、およびキャッシュに関する制御については、『Cisco Secure Client Administrator Guide』の「Network Visibility Module」の章で説明されています。

信頼できるネットワークの設定要件

Cisco Secure Client Network Visibility Module 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。Cisco Secure Client の信頼ネットワーク検出（TND）機能を使用して、エンドポイントが信頼できるネットワーク上にあるかどうかを学習します。ネットワークの状態は、いつ Network Visibility Module データをエクスポートし、いつ適切なデータ収集ポリシーに適用するかを決定するために Network Visibility Module によって使用されます。Network

Visibility Module には独自の TND 設定があります。この設定では、SSL プローブが設定済みの信頼できるヘッドエンドに送信され、応答に証明書が必要になります（到達可能な場合）。Network Visibility Module の TND は NVM プロファイルエディタで設定されます。Network Visibility Module の TND が設定されていない場合は、VPN モジュールの TND 設定に依存します。

（注） 内部ネットワーク外から操作している場合、TND は DNS 要求を行い、設定されたサーバへの SSL 接続を確立しようとします。シスコでは、内部ネットワーク外のデバイスでこのような要求によって組織内の名前や内部構造が明らかになることを防ぐために、エイリアスの使用をお勧めします。

信頼ネットワーク検出は、VPN コンポーネントが環境で使用されているかどうかに関係なく、VPN に使用される Cisco Secure Client プロファイル（xml）で設定されます。TND は、Cisco Secure Clientプロファイルエディタの [設定（パート 2）（Preferences (Part 2)）] の [自動 VPN ポリシー（Automatic VPN Policy）] セクションを構成することで有効になります。VPN の TND は、DHCP 経由で受信した情報（ドメイン名と DNS サーバー）を使用します。DNS サーバーまたはドメイン名（あるいはその両方）が設定値と一致する場合、ネットワークは信頼できると見なされます。VPN は、TLS 証明書ベースの TND 検出もサポートします。クライアントが信頼できるネットワーク上にあるときに Cisco Secure Client で実行するアクションを決定します。たとえば、[信頼されたネットワークポリシー（Trusted Network Policy）] および [信頼されていないネットワークポリシー（Untrusted Network Policy）] を [何もしない（Do Nothing）] に設定できます。

TND の設定が正しくないと、Network Visibility Module で問題が発生します。信頼ネットワーク検出を予想どおりのパフォーマンスにするために、次のアクションを実行します。

- TND 設定が正しいことを確認します。Network Visibility Module では、信頼できるネットワーク上にある場合にのみエクスポートを行います。無効な TND 設定として、3 つの DNS サーバーがあっても、3 つが定義されていない場合などがあります。
- TND VPN 設定から信頼できるドメインを削除します。
- VPN のスプリット包含設定に常にコレクタの IP アドレスを含めます。コレクタの IP アドレスがスプリットトンネルに含まれておらず、信頼できない場合、データはパブリックインターフェイスに送信されます。
- CollectionMode が現在の（信頼または信頼されていない）ネットワークで収集するように設定されていることを確認します。
- VPN.xml および NVM_ServiceProfile.xml が正しいフォルダにあることを確認してから、再起動します。
- すべての Cisco Secure Client サービスを開始してから停止します。
- DNS サーバーに接続している内部に接続されているネットワークをバウンスします。
- プロキシの背後での TND 検出はサポートされていません。

クライアント/エンドポイント側でのログの収集

Cisco Secure Client の動作のトラブルシューティングを行うには、Network Visibility Module コンポーネントで Diagnostic and Reporting Tool（DART）を実行します。Network Visibility Module に必要なすべてのログは、DART によって処理されます。ログファイルや設定などを収集します。Windows ログはさまざまな場所にあります。Cisco Secure Client で Network Visibility Module のイベントビューアを調べます。macOS および Linux のログは、nvmagent のフィルタ処理で検出されます。

Network Visibility Module コレクタのインストールに失敗する

コレクタのインストール中またはインストールスクリプトの実行中に、システムログディレクトリに*Acnvm.conf error:line number 17: expected key string* メッセージが表示された場合は、不適切なカンマまたは余分なカンマがないか確認してください。

Network Visibility Module コレクタの起動に失敗する

acnvmcollector ファイル /opt/acnvm/bin/acnvmcollector でコードの実行に失敗した場合、ユーザーおよびグループに acnvmcollector の eXecute がない可能性があります。

ロギングレベルとコレクタのバージョン

コレクタのバージョンは、**/opt/acnvm/bin/acnvmcollector -v** コマンドで取得できます。

ロギングレベルをデバッグに設定するには、acnvmlog.conf ファイルで **log4cplus.rootLogger=DEBUG, STDOUT, NvmFileAppender** を使用します。デフォルトのレベルは *INFO* です。

DTLS の問題

DTLS が設定されていない：acnvm.conf.file にないことを示します。

サーバーキーが無効：パスワードキーの組み合わせがサポートされていないことを示します。

Network Visibility Module コレクタの関連ドキュメント

関連資料については、次のマニュアルを参照してください。

- 『Cisco Secure Client Administrator Guide, Release 5.x』の「Network Visibility Module」の章：Network Visibility Module とその関連のプロファイルエディタやコレクションパラメータの詳細な説明
- 「Cisco Network Visibility Solution」コミュニティページ：Cisco Endpoint Security Analytics（CESA）のユーザー向け Splunk ガイド
- 『CESA Built On Splunk Quickstart POV Kit and Deployment Guide』：Cisco Endpoint Security Analytics（CESA）ユーザーが価値の実証または実稼働の導入をセットアップする方法
- 『Cisco Endpoint Security Analytics (CESA) Dashboard Overview and FAQ』：CESA ユーザーがダッシュボードを理解するために必要な情報

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255（フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。