AnyConnect 4.2.x および Splunk 経由の Cisco Network Visibility Module のインストールと設定

目次

はじめに 前提条件 要件 <u>使用するコンポーネント</u> 背景説明 Cisco AnyConnect セキュア モビリティ クライアント Internet Protocol Flow Information Export (IPFIX) IPFIX コレクタ Splunk トポロジ 設定 AnyConnect NVM クライアント プロファイル ASDM を介した NVM クライアント プロファイルの設定 AnyConnect プロファイル エディタでの NVM クライアント プロファイルの設定 Cisco ASA 上での Web 展開の設定 Cisco ISE 上での Web 展開の設定 信頼ネットワーク検出 展開 手順1: Cisco ASA/ISE 上での AnyConnect NVM の設定 <u>手順2:IPFIX コレクタ コンポーネントの設定</u> 手順3: Cisco NVM アプリケーションでの Splunk のセットアップ 確認 AnyConnect NVM インストールの検証 コレクタの実行中ステータスの確認 Splunk の検証 トラブルシューティング パケット フロー 基本的なトラブルシューティング ステップ 信頼ネットワーク検出(TND) フロー テンプレート 推奨リリース 関連する障害 関連リンク

概要

このドキュメントでは、Cisco AnyConnect Network Visibility Module (NVM)を、エンドユーザ システム上で AnyConnect 4.2.x 以降を使用してインストールおよび設定する方法を説明します。 Cisco AnyConnect NVM は、セキュリティ分析を展開するための手段として使用されます。 NVM により組織は、そのネットワーク上にあるエンドポイントやユーザの行動を表示し、オンプレミ スとオフプレミスの両方にあるエンドポイントからのフローを、ユーザ、アプリケーション、デ バイス、ロケーション、および接続先などの追加のコンテキストとともに収集できるようになり ます。

この TechNote で取り上げているのは、Splunk を使用した AnyConnect NVM の設定例です。

前提条件

要件

次の項目に関する知識が推奨されます。

- NVM を備えた AnyConnect 4.2.01022 以降
- AnyConnect APEX ライセンス
- ASDM 7.5.1 以降

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco AnyConnect Security Mobility Client 4.2 以降
- Cisco AnyConnect Profile Editor
- Cisco 適応型セキュリティ アプライアンス(ASA) バージョン 9.5.2
- Cisco Adaptive Security Device Manager (ASDM) バージョン 7.5.1
- Splunk Enterprise 6.3
- コレクタのデバイスとしての Ubuntu 14.04.3 LTS

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメン トで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています。 稼働中 のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してくだ さい。

背景説明

Cisco AnyConnect セキュア モビリティ クライアント

Cisco AnyConnect は、企業を保護する各種のセキュリティ サービスを提供する統合エージェン トです。 AnyConnect は、最も一般的には企業 VPN クライアントとして使用されていますが、 企業セキュリティのさまざまな面に対応する追加モジュールもサポートしています。 この追加モ ジュールにより、ポスチャ アセスメント、Web セキュリティ、マルウェア保護、ネットワーク 可視性などのセキュリティ機能が有効になります。

この TechNote は、Network Visibility Module(NVM)に関するものです。この機能は Cisco AnyConnect と統合されており、管理者はこれを使用してエンドポイント アプリケーションの使

用状況をモニタできます。

Cisco AnyConnect の詳細については、次を参照してください。

Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.3

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 プロトコルに基づいて拡張されたプロトコル仕様です。 IPFIX には、AC NVM の一部として収集できるすべてのパラメータをサポートする、十分な標準情報要素はありま せん。 Cisco vzFlow プロトコルは IPFIX 標準を拡張し、新しい情報要素を定義します。さらに、 IPFIX データのエクスポートのために AC NVM により使用される標準セットの IPFIX テンプレー トを定義します。

IPFIX の詳細については、<u>rfc5101</u>、<u>rfc7011</u>、<u>rfc7012</u>、<u>rfc7013</u>、<u>rfc7014</u>、<u>rfc7015</u> を参照してく ださい。

IPFIX コレクタ

コレクタは、IPFIX データを受信して保存するサーバです。 これはそのデータを Splunk にフィ ードします。 たとえば、Lancope

シスコは、自社製の IPFIX コレクタも提供しています。

Splunk

Splunk は、診断データを収集して分析し、IT インフラストラクチャに関する意味深い情報を提供 する強力なツールです。 これは管理者がネットワークのヘルスを把握するために重要なデータを 収集する、ワンストップのロケーションです。

シスコは Splunk を所有または保守しているわけではありませんが、シスコは Cisco AnyConnect NVM App for Splunk を提供しています。

Splunk の詳細については、その Web サイトを参照してください。

トポロジ



この TechNote の IP アドレスの表記法:

コレクタ IP アドレス: 192.0.2.123

Splunk IP アドレス: 192.0.2.113

設定

このセクションでは、Cisco NVM コンポーネントの設定について説明します。

AnyConnect NVM クライアント プロファイル

AnyConnect NVM 設定は、コレクタ IP アドレスやポート番号に関する情報を含む XML ファイル に、そのほかの情報とともに保存されます。 コレクタ IP アドレスとポート番号は、NVM クライ アント プロファイルで正しく設定される必要があります。 NVM モジュールを正しく操作するには、XML ファイルがこのディレクトリ内に置かれている必要があります。

- ・Windows 7 以降の場合: %%ALLUSERSPROFILE%\Cisco\Cisco AnyConnect Secure Mobility Client\NVM
- Mac OS X の場合: //opt/cisco/anyconnect/nvm

プロファイルが Cisco ASA または Identity Services Engine(ISE)に存在している場合、 AnyConnect NVM 展開とともに自動展開されます。

XML プロファイルの例:

<?xml version="1.0" encoding="UTF-8"?> -<NVMProfile xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="NVMProfile.xsd"> -<CollectorConfiguration> <CollectorIP>**192.0.2.123**</CollectorIP> <Port>**2055**</Port> </CollectorConfiguration> <Anonymize>**false**</Anonymize> <CollectionMode>**all**</CollectionMode> </NVMProfile> NVM プロファイルは、次の2つのツールを使用して作成できます。

- Cisco ASDM
- AnyConnect プロファイル エディタ

ASDM を介した NVM クライアント プロファイルの設定

この方式は、AnyConnect NVM が Cisco ASA を介して展開される場合に推奨されます。

1. [Configuration] > [Remove Access VPN] > [Network (Client) Access] > [AnyConnect Client Profile]の順に移動します。

2. [Add] をクリックします。

Remote Access VPN 🗗 म	Configuration > Remote Acce	ess VPN > Network (Client) Access > AnyConr	<u>iect Client Profile</u>		
Introduction Network (Client) Access AnyConnect Connection Profiles AnyConnect Customization/Localiza AnyConnect Client Profile AnyConnect Client Software Ornamic Access Policies Group Policies Group Policies Psec(IKEV1) Connection Profiles	This panel is used to manage A select the 'Add' button to add a The profile Usage field is introd	AnyConnect Client Profiles and perform group assign new profile. Pressing the Import or Export button i duced with the Secure Mobility Solution. This field or roup Policy 👔 Delete 🕑 Import 🚳 Export 🚳 Vali	iment for AnyConnect version 2.5 or later. You ca s for upload and download of client profiles betwontains different profile usage in AnyConnect ver untains different profile usage in AnyConnect ver	an select a profile to edit, change group or to delete. You can veen local machine and device. sion 3.0 and later.	
Besc(IKEv2) Connection Profiles Besc(IKEv2) Connection Advanced Advanced Advanced Description Advanced	Profile Name	Profile Usage	Group Policy	Profile Location	
<►					
A Device Setup					
🚺 Firewall					
Remote Access VPN					
Site-to-Site VPN					
Device Management		_			
» *			Apply Reset		

3. プロファイルの名前を入力します。 [Profile Usage]で、[Network Visibility Service Profile] を選 択します。

4. AnyConnect ユーザが使用するグループ ポリシーにこれを割り当てます。 [OK] をクリックします。

Remote Access VPN 🗗 🕂	Configuration > Remote Ac	cess VPN > Network (Client) Access > An	<u>yConnect Client Profile</u>			
Introduction Introduction Network (Client) Access MayConnect Connection Profiles MayConnect Customization/Localiza AnyConnect Client Profile MayConnect Client Software MayConnect Client Software Stroup Policies Group Policies For Policies	This panel is used to manage select the 'Add' button to add The profile Usage field is intr Add of Edit 🔀 Change	a AnyConnect Client Profiles and perform group d a new profile. Pressing the Import or Export b douced with the Secure Mobility Solution. This Group Policy 👔 Delete 🛃 Import 🖷 Export	assignment for AnyConnect version 2. utton is for upload and download of cli field contains different profile usage in D Validate	5 or later.You can select a pro ent profiles between local ma AnyConnect version 3.0 and l	ofile to edit, change group or to delete. You can chine and device. ater.	
IPsec(IKEv2) Connection Profiles Secure Mobility Solution	Profile Name	Profile Usage	Group Policy		Profile Location	
Advances Assignment Advanced Advanced AAv/Local Users AAv/Local Users Certificate Management Language Localization Longuage Localization DHCP Server DHCP Server Advanced	Add Any Profile N Profile U Enter a c created I Profile Lo Group Po		file. The file will be automatically	Browse Flash Upload		
Device Setup		ОК	Cancel Help			
🗊 Firewall					1	
Remote Access VPN						
Device Management			Apply Reset			

5. 新しいポリシーが作成されました。 [編集(Edit)]をクリックします。

Remote Access VPN 🗗 🖗	Configuration > Remote Acce	ss VPN > Network (Client) Access > AnyConnect C	lient Profile		
Introduction I	This panel is used to manage A select the 'Add' button to add a The profile Usage field is introc	AnyConnect Client Profiles and perform group assignment new profile. Pressing the Import or Export button is for u fuced with the Secure Mobility Solution. This field contains roup Policy 1 Delete B Import 5 Export 1 Deltate	for AnyConnect version 2.5 or later.You can pload and download of client profiles betwee different profile usage in AnyConnect versio	select a profile to edit, change group or to delete. You can n local machine and device. n 3.0 and later.	
Pisec(IKEV2) Connection Profiles	Profile Name	Profile Usage	Group Policy	Profile Location	
Address Assignment	NVM_policy	Network Visibility Service Profile	GroupPolicy_anyconnect	disk0:/nvm_policy.nvmsp	
Given Constraints SSL VPN Access Given Constraints SSL VPN Access AAA/Local Users AAA/Local Users Certificate Management Certificate Management Certificate Management Ded Balancing DHCP Server DNS DNS Advanced					
< III +					
A Device Setup					
Firewall					
Remote Access VPN					
Site-to-Site VPN					
🔣 Device <u>M</u> anagement					
»		Ap	Reset		

6. コレクタ IP アドレスとポート番号に関する情報を入力します。 [OK] をクリックします。

7. [Apply] をクリックします。

Remote Access VPN 🗗 🖗	AnyConnect Client Profile Editor - NVM policy	X	
Introduction Network (Client) Access AnyConnect Connection Profiles AnyConnect Customization/Localiza AnyConnect Client Profile	Profile: NVM_policy NVM Profile	About	or to delete. You can
AnyConnect Client Software ApyConnect Client Software ApyConnect Client Software Dynamic Access Policies Dynamic Access Policies Insec(IKEv1) Connection Profiles Secure Mobility Solution Socure Mobility Solution	Collector Configuration		
Advanced	IP Address/FQDN 192.0.2.123		
AAA/Local Users Secure Desktop Manager Certificate Management	Port 2055		
- 변경 Language Localization - 옷 Load Balancing 에 DHCP Server - 읎 DNS 관 행 Advanced	User Anonymization False		
	Collection Mode All Networks		
4 III •			
A Device Setup			
Firewall			
Remote Access VPN	OK Cancel Help		
)	
Bevice Management	Apply		
	лери Косс		

AnyConnect プロファイル エディタでの NVM クライアント プロファイルの設定

これは Cisco.com で使用できるスタンドアロン ツールです。 この方式は、AnyConnect NVM が Cisco ISE を介して展開される場合に推奨されます。 このツールを使用して作成された NVM プ ロファイルは、Cisco ISE にアップロードするか、またはエンドポイントに直接コピーできます

AnyConr	nect Profile Editor - NVM Pro	file	
File Help			
NVM Pr	ofile		
Brofile	Untitled		
Frome.	Unitied		
	Collector Configuration		
	IP Address/FQDN	192.0.2.123	
	Port	2055	
	User Anonymization	False	
	Collection Mode	All Networks	
		Help	

AnyConnect プロファイル エディタの詳細については、以下を参照してください。

AnyConnect プロファイル エディタ

0

Cisco ASA 上での Web 展開の設定

この TechNote は、AnyConnect が ASA 上にすでに設定済みであり、NVM モジュール設定のみ 追加が必要であると想定しています。 ASA AnyConnect の設定の詳細については、以下を参照し てください。

<u>ASDM ブック 3: Cisco ASA シリーズ VPN ASDM コンフィギュレーション ガイド 7.5</u>

Cisco ASA 上で AnyConnect NVM モジュールを有効にするには、次の手順を実行します。

1. [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies]を選択します。

2. 関連グループ ポリシーを選択し、[Edit]をクリックします。



- 3. グループ ポリシー ポップアップ内で、[Advanced] > [AnyConnect Client]を選択します。
- 4. [Optional Client Modules to Download]を展開し、[AnyConnect Network Visibility] を選択します
- 5. [OK]をクリックし、変更を適用します。

o

Edit Internal Group Policy: Gr	oupPolicy_anyconnect		X
General Keep	Installer on Client System:	Inherit 🔿 Yes 💿 No	
Advanced Datag	gram Transport Layer Security (DTLS):	Inherit 🔿 Enable 🔿 Disable	
Browser Proxy DTLS	Compression:	Inherit 🔿 Enable 🔿 Disable	
	Compression:	🗹 Inherit 🔿 Deflate 🔿 LZS 💿 Disable	
Ignor	e Don't Fragment(DF) Bit:	🗹 Inherit 🔘 Enable 🔘 Disable	
Client	t Bypass Protocol:	🗹 Inherit 🔘 Enable 🔘 Disable	
FQDN	of This Device:	V FQDN	
MTU:		Inherit 1000	
Кеера	alive Messages:	✓ Inherit Disable Interval: seconds	
Optio	nal Client Modules to Download:	Inherit dart,nvm	0
Alway	ys-On VPN:	Inherit AnyConnect DART	
Client	t Profiles to Download:	Inherit AnyConnect Network Visibility	
		Add Add Ayconnect Posture	
		Profile Nam AnyConnect Web Security	
		AnyConnect ISE Posture	
		OK Cancel	
Find:	🔘 Next 🌘	Previous	
		OK Cancel Help	

Cisco ISE 上での Web 展開の設定

• Cisco ISE を AnyConnect Web 展開用に設定するには、次の手順を実行します。

- Cisco ISE GUI で、[Policy] > [Policy Elements] > [Results]を選択します。
- [Client Provisioning]を展開して [Resources] を表示し、[Resources] を選択します。

AnyConnect イメージの追加

[Add] > [Agent Resources]を選択し、AnyConnect パッケージ ファイルをアップロードします。

cisco Identity Services Engine Home	Operations ▼Policy ► Guest Act	cess ► Administration ► Work Cente	rs	0 0	. 0	1	\$
Policy Sets Profiling Posture Client Provisioning	▼ Policy Elements						
Dictionaries Conditions Results							
Agent Resource	ces From Local Disk > Agent Resources Fro	om Local Disk					
Authentication Agent Res	sources From Local Disk						
➤ Authorization							
Profiling	Category Cisco Provided Pac	kages T					
▶ Posture	Browse anyo	connect-win-4 2 02075-k9 pkg					
✓ Client Provisioning	Blowse anyo	onnou-mn-4.2.02010-60.pkg					
Resources	▼ AnyConnect Up	loaded Resources					
	Name	▲ Туре	Version Description				
	AnyConnectDesktopV	Windows 4.2.207 AnyConnectDesktopWin	lows 4.2.2075.0 AnyConnect Secure	Mobility Clien			
Submit	Cancel						

ポップアップでパッケージのハッシュを確認します。

ファイルハッシュは、Cisco.com ダウンロード ページで照会するか、またはサードパーティ製ツ ールを使用して確認できます。

複数の AnyConnect イメージを追加するには、この手順を繰り返すことができます (Mac OSX および Linux OS の場合)。



AnyConnect NVM プロファイルの追加:

[Add] > [Agent Resources]を選択し、NVM クライアント プロファイルをアップロードします。

dentity Services Engine	Home > Operations - P	blicy Guest Access	Administration	► Work Centers	0	0	±	۵.
Policy Sets Profiling Posture C	ient Provisioning Policy Elemen	ts						
Dictionaries ► Conditions	S							
Authentication	Agent Resources From Local Disk >	Agent Resources From Local D	Disk					
Automotion	Agent Resources From Lo	cal Disk						
▶ Authorization								
▶ Profiling	Category	Customer Created Packages	Ţ	D				
▶ Posture	Туре	AnyConnect Profile	T					
- Client Provisioning	* Name	AnyConnect Network Visibilit	y .					
Resources	Description	Browse NVM_serviceP	rofile.xml					
	Submit Cancel							

AnyConnect 設定ファイルの追加:

[Add]> [AnyConnect Configuration] の順にクリックします。

前のステップでアップロードしたパッケージを選択します。

dentity Services Engine	Home ► Operations ▼Policy ► O	Suest Access Administration	on 🔹 🕨 Work Cer	iters			
Policy Sets Profiling Posture Clie	ent Provisioning - Policy Elements						
Dictionaries Conditions Results							
0							
	Resources						
Authentication							Selected 0 Total 56 Selected 0 Total 56
Authorization	/ Edit - Add - Chapter - Chapter				St		12
	Agent resources from Cisco site		Marrian	Last Hadata	Description		
▶ Profiling	Agent resources from local disk	Minord		2015/10/08 02:24:16	Description		
	Native Supplicant Profile	Rupplicent Brofile	Not Appliaghle	2015/10/08 02:24:16	Bro configured Native Supplicant		
▶ Posture	Cis AnyConnect Configuration	Drofile VSDWizord		2015/10/08 02:24:15	ISE 2.0 Supplicant Provisioning	_	
	AMP Enabler Profile	ent	4 9 0 28	2015/10/08 02:24:15	NAC WebAgent (ISE 1 1 3 release)		
✓ Client Provisioning	MacOsXSPWizard 1.0.0.30	MacOsXSPWizard	10030	2015/12/16 15:25:17	Supplicant Provisioning Wizard f	_	
Resources	WebAgent 4.9.0.24	WebAgent	4.9.0.24	2015/12/16 15:25:24	NAC WebAgent (ISE 1.1.1 or later)		
	MacOsXAgent 4.9.0.661	MacOsXAgent	4.9.0.661	2015/12/16 15:25:32	NAC Posture Agent for Mac OS	_	
	MACComplianceModule 3.6.10255.2	MACComplianceModule	3.6.10255.2	2015/12/16 15:25:37	MACAgent ComplianceModule v		
	MacOsXAgent 4.9.0.1006	MacOsXAgent	4.9.0.1006	2015/12/16 15:25:44	NAC Posture Agent for Mac OS	_	
	NACAgent 4.9.0.52	NACAgent	4.9.0.52	2015/12/16 15:25:52	NAC Windows Agent (ISE 1.1.3		
	NACAgent 4.9.0.1009	NACAgent	4.9.0.1009	2015/12/16 15:26:06	NAC Windows Agent (ISE 1.2 rel		
	NACAgent 4.9.4.3	NACAgent	4.9.4.3	2015/12/16 15:26:21	NAC Windows Agent - ISE 1.2 , I		
	AnyConnectComplianceModuleWind	AnyConnectComplianceMo	3.6.10255.2	2015/12/16 15:26:39	AnyConnect Windows Complian	_	
	NACAgent 4.9.5.4	NACAgent	4.9.5.4	2015/12/16 15:26:49	NAC Windows Agent - ISE 1.2 a		
	NACAgent 4.9.5.10	NACAgent	4.9.5.10	2015/12/16 15:27:05	NAC Windows Agent - ISE 1.2.1		
	NACAgent 4.9.0.42	NACAgent	4.9.0.42	2015/12/16 15:27:19	NAC Windows Agent (ISE 1.1.1		
	MacOsXSPWizard 1.0.0.21	MacOsXSPWizard	1.0.0.21	2015/12/16 15:27:29	Supplicant Provisioning Wizard f		
	WebAgent 4.9.0.1005	WebAgent	4.9.0.1005	2015/12/16 15:27:34	NAC WebAgent (ISE 1.2 release)		
	NACAgent 4.9.5.8	NACAgent	4.9.5.8	2015/12/16 15:27:43	NAC Windows Agent - ISE 1.2 a		
	NACAgent 4.9.5.7	NACAgent	4.9.5.7	2015/12/16 15:27:59	NAC Windows Agent - ISE 1.2 a		

[AnyConnect Module Selection]内の [NVM] を、必要なポリシーとともに有効にします。

dentity Services Engine	Home → Operations → Policy → Guest Access → Administration → Work Centers	0	O,	?	2	\$
Policy Sets Profiling Posture C	ient Provisioning Policy Elements					
Dictionaries + Conditions - Result	S					
0						
Authentication	AnyConnect Configuration > New AnyConnect Configuration					
Authorization	* Select AnyConnect Package: AnyConnectDesktopWindows 4.2.2075.0					
▶ Profiling	* Configuration Name: AnyConnect Configuration					
▶ Posture	Description:					
✓ Client Provisioning	DescriptionValue Notes Compliance Module					
Resources						
	AnyConnect Module Selection ISE Posture VPNV Network Access Manager Web Security AMP Enabler ASA Posture Network Visibility Start Before Logon Diagnostic and Reporting Tool					

上のセクションでは、AnyConnect Client モジュール、プロファイル、カスタマイズ/言語パッケ ージ、および Opswat パッケージを有効にしました。

Cisco ISE 上の Web 展開設定に関する詳細情報については、以下を参照してください。

<u>AnyConnect の Web 展開</u>

信頼ネットワーク検出

NVM は、信頼ネットワーク内にある場合にのみフロー情報を送信します。 これはエンドポイン トが信頼ネットワーク内にあるかどうかを調べるために、AnyConnect クライアントの TND 機能 を使用します。 TND は、エンドポイントが信頼ネットワーク内にあるかどうかを判断するため に、DNS/ドメイン情報を使用します。 VPN は、接続されると、信頼ネットワーク内にあると見 なされ、フロー情報はコレクタに送信されます。

TND は、NVM が正しく機能するために、正しく設定される必要があります。 TND 設定の詳細に ついては、次を参照してください。

信頼ネットワーク検出の設定

展開

AnyConnect NVM ソリューションの展開には、次の手順が関係しています。

1. Cisco ASA/ISE 上での AnyConnect NVM の設定

2. IPFIX コレクタ コンポーネントの設定

3. Cisco NVM アプリケーションでの Splunk のセットアップ

ステップ 1: Cisco ASA/ISE 上での AnyConnect NVM の設定

この手順は、「設定」のセクションで詳しく扱われています。

NVM を Cisco ISE/ASA 上で設定すると、クライアント エンドポイントに自動展開できます。

手順 2: IPFIX コレクタ コンポーネントの設定

コレクタ コンポーネントはエンドポイントからすべての IPFIX データを収集して変換し、それを Splunk アプリケーションに転送します。 さまざまなサードパーティのコレクタ ツールを利用で きますが、Cisco NVM は IPFIX を理解するすべてのコレクタと互換性があります。 この TechNote では、64 ビット Linux 上で稼働するシスコ製のコレクタ ツールを使用します。 CentOS および Ubuntu 設定スクリプトは、Splunk アプリケーションに含まれています。 CentOS のインストール スクリプトおよび設定ファイルは、Fedora や Redhat のディストリビュ ーションでも使用できます。 コレクタは、スタンドアロン 64 ビット Linux システム、または 64 ビット Linux 上で稼働する Splunk Forwarder のいずれかの上で実行する必要があります。

コレクタをインストールするには、\$APP_DIR\$/appserver/addon/ ディレクトリにある CiscoNVMCollector_TA.tar ファイル内のアプリケーションを、インストールを予定しているシス テムにコピーする必要があります。

この TechNote では、Splunk は E: ドライブの Windows ワークステーションにインストールされ ます。 ドライブにします。

CiscoNVMCollector_TA.tar ファイルは、以下のディレクトリ内にあります。

E:\Program Files\Splunk\etc\apps\CiscoNVM**appserver\addon**

コレクタのインストールを予定しているシステム上で tar ファイルを抽出し、スーパー ユーザ権 限で install.sh スクリプトを実行します。 install.sh スクリプトを実行する前に、.tar バンドル内 の \$PLATFORM\$_README ファイルを読むことをお勧めします。 \$PLATFORM\$_README フ ァイルには、install.sh スクリプトを実行する前に確認および(必要であれば)変更が求められる 、関連する構成設定についての情報が記載されています。

Ubuntu サーバ上のコレクタのディレクトリ:

root@ubuntu-splunkcollector:~/Downloads/CiscoNVMCollector_TA\$ ls							
acnvmcollector	CENTOS_README	libboost_log.so.1.57.0					
acnvmcollectord	install_centos.sh	libboost_system.so.1.57.0					
acnvm.conf	install.sh	libboost_thread.so.1.57.0					
acnvm.conf~	install_ubuntu.sh	UBUNTU_README					
acnvm.service	libboost_filesystem.so.1.57.0						
root@ubuntu-splunkcollector:~/Downloads/CiscoNVMCollector_TA\$							

情報は、構成ファイル(acnvm.conf)内で設定する必要があります。

1. Splunk インスタンスの IP アドレスとリスニング ポート。

2. コレクタ (着信 IPFIX データ)のリスニング ポート。

フローごとのデータ ポート、エンドポイント ID データ ポート、およびコレクタ ポートは、設定 ファイル内でデフォルト設定に事前設定されています。 デフォルト以外のポートを使用する場合 は、これらの値を必ず変更します。

この情報は、設定ファイル(acnvm.conf)に追加されます。

```
"syslog_server_ip" : "192.0.2.113",
"syslog_flowdata_server_port" : 20519,
"syslog_sysdata_server_port" : 20520,
"netflow_collector_port" : 2055,
"log_level" : 7
}
```

詳細については、次のサイトを参照してください。

https://splunkbase.splunk.com/app/2992/#/documentation

手順 3: Cisco NVM アプリケーションでの Splunk のセットアップ

Cisco AnyConnect NVM App for Splunk は、Splunkbase 上で使用できます。 このアプリケーションは、事前定義レポートやダッシュボードで、有用なレポートによるエンドポイントからの IPFIX (nvzFlow) データを使用するために役立ちます。また、ユーザとエンドポイントの動作を 相関させます。

Splunkbase 上での Cisco NVM アプリケーションのリンク:

https://splunkbase.splunk.com/app/2992/

インストール:

[Splunk] > [Apps]と選択し、Splunkbase からダウンロードしたかまたは [Apps] セクション内で検索した **tar.gz** ファイルをインストールします。



デフォルトでは、Splunk はフローごとのデータおよびエンドポイント ID データの 2 つのデータ 入力フィードを、UDP ポート 20519 および 20520 でそれぞれ受け取ります。 コレクタ コンポ ーネントは、デフォルトではこれらのポートでフィードを送信します。 Splunk ではデフォルト のポートは変更できます。しかし、コレクタ設定では同じポートを指定する必要があります(手 順 2 を参照)。

デフォルトのポートを変更するには、[Splunk] > [Settings] > [Data Input] > [UDP]を選択します。

splunk'> Apps ~			Administrator \sim	Messages 🗸	Settings \sim	Activity \sim Help \sim	Find
UDP Data inputs » UDP							
							٩
New							Results per page 25
UDP port \$	Source type ¢	Status ‡				Actions	
20519	syslog	Enabled Disable				Clone	
20520	syslog	Enabled Disable				Clone	
About Support File a Bug Documentation Privac	y Policy					© 2005-201	6 Splunk Inc. All rights reserved.

確認

AnyConnect NVM 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、AnyConnect Secure Mobility クライア ントの**情報セクション**内にある [Installed Modules] にリストされます。



また、nvm サービスがエンドポイント上で実行しており、プロファイルが要求されたディレクト リ内にあることを確認します。

コレクタの実行中ステータスの確認

コレクタのステータスが実行中であることを確認します。 これにより、コレクタがエンドポイン トから常時 IPFIX/cflow を受信していることを確認できます。

```
GNU nano 2.2.6
{
   "syslog_server_ip" : "192.0.2.113",
   "syslog_flowdata_server_port" : 20519,
   "syslog_sysdata_server_port" : 20520,
   "netflow_collector_port" : 2055,
   "log_level" : 7
}
```

Splunk の検証

Splunk と関連サービスが実行していることを確認します。 Splunk のトラブルシューティングに 関する資料については、Splunk の Web サイトを参照してください。

File: acnvm.conf

トラブルシューティング

パケット フロー

1. IPFIX パケットは、AnyConnect NVM モジュールによってクライアント エンドポイントで生成 されます。

2. クライアント エンドポイントは、IPFIX パケットをコレクタ IP アドレスに転送します。

3. コレクタは情報を収集して、Splunk に転送します。

4. コレクタは、トラフィックを Splunk に、次の 2 つの異なるストリームで送信します。 つまり 、フローごとのデータと、エンドポイント ID データです。

すべてのトラフィックは UDP ベースであり、トラフィックの確認はありません。

トラフィックのデフォルト ポート:

IPFIX データ 2055

フローごとのデータ 20519

フローごとのデータ 20520

NVM モジュールは IPFIX データをキャッシュに入れ、信頼ネットワーク内であればそれをコレク タに送信します。 これは、ラップトップが社内ネットワーク(on-prem)に接続されているか、 または VPN を介して接続されているかのいずれかの場合に実行されます。

基本的なトラブルシューティング ステップ

・クライアントエンドポイントとコレクタとの間のネットワーク接続を確認します。

- •コレクタと Splunk との間のネットワーク接続を確認します。
- NVM がクライアント エンドポイントに正しくインストールされていることを確認します。
- IPFIX トラフィックが生成されているかどうかを確認するには、エンドポイントにキャプチ

ャを適用します。

 IPFIX トラフィックを受信しているかどうか、およびトラフィックを Splunk に転送している かどうかを確認するために、コレクタにキャプチャを適用します。

トラフィックを受信しているかどうかを確認するには、Splunk にキャプチャを適用します。
 Wireshark に表示される IPFIX トラフィック:

🖟 Apply a display filter < Ctri-/>						
No.	Tim Source	Destination	Protocol	Length Info		
Г	1 0 192.168.100.1	10.76.76.161	CFLOW	269 IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]		
	2 0 192.168.100.1	10.76.76.161	CFLOW	269 IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]		
	3 0 192.168.100.1	10.76.76.161	CFLOW	269 IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]		
	4 0 192.168.100.1	10.76.76.161	CFLOW	269 IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]		
	5 0 192.168.100.1	10.76.76.161	CFLOW	269 IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]		
	6 2 192.168.100.1	10.76.76.161	CFLOW	269 IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]		
	7 0 192.168.100.1	10.76.76.161	CFLOW	269 IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]		=
	8 1 192.168.100.1	10.76.76.161	CFLOW	269 IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]		-
	9 2 192.168.100.1	10.76.76.161	CFLOW	269 IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]		
	10 2 192.168.100.1	10.76.76.161	CFLOW	269 IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]		
	11 2 192.168.100.1	10.76.76.161	CFLOW	269 IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]		
	12 0 192.168.100.1	10.76.76.161	CFLOW	269 IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]		
	13 0 192.168.100.1	10.76.76.161	CFLOW	269 IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]		
	14 2 192.168.100.1	10.76.76.161	CFLOW	269 IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]		

信頼ネットワーク検出(TND)

NVM は、TND に依存して、エンドポイントが信頼ネットワーク内にあるときを検出します。 TND 設定が誤っている場合、NVM の問題が発生する原因になります。

TND は DHCP を介して受け取る情報に基づいて動作します。 ドメイン名および DNS サーバ。 DNS サーバまたはドメイン名(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。

NVM がトラフィックをコレクタに転送しない場合、TND に問題がある可能性があります。

フロー テンプレート

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。 この情報がコレクタに 送信されないと、コレクタは IPFIX データを収集できません。 これにより、データ コレクショ ンに関する問題が発生します。

このような問題は、コレクタが後から設定された場合や、IPFIX の最初の数パケットがネットワ ークでドロップする場合(VPN では一般的)に見られます。 これを軽減するには、次のイベン トの 1 つが必要です。

1. NVM クライアント プロファイルに変更がある。

2. ネットワーク変更イベントがある。

3. nvmagent サービスが再起動する。

4. エンドポイントがリブート/再起動する。

この問題は、エンドポイントをリブートするか、VPN を再接続することで回復できる可能性があ ります。

この問題は、エンドポイントのパケット キャプチャ内の no template found、またはコレクタ ロ グ内の no templates for flowset を確認することで特定できます。

パケット キャプチャ

コレクタ ログ:

```
GNU nano 2.2.6
{
  "syslog_server_ip" : "192.0.2.113",
  "syslog_flowdata_server_port" : 20519,
  "syslog_sysdata_server_port" : 20520,
  "netflow_collector_port" : 2055,
  "log_level" : 7
}
```

Recommended Release

シスコは常に、使用時または更新時に最新ソフトウェア バージョンの AnyConnect を選択するように推奨しています。 AnyConnect のバージョンを選択するときは、最新の 4.2.x または 4.3.x ク ライアントを使用してください。 これにより各 NVM に最新の拡張と不具合の修正が提供され、 最近の変更は Microsoft コード署名証明書の適用により緩和されます。 <u>詳細については、こちら</u> <u>をご覧ください。</u>

File: acnvm.conf

関連する不具合

1. <u>CSCva21660</u>: acnvmagent.exe*32 プロセスの AnyConnect NVM ハンドル/リーク

関連リンク

- 1. Cisco AnyConnect Network Visibility (NVM) App for Splunk : <u>https://splunkbase.splunk.com/app/2992/</u>
- 2. Splunk コレクタのセットアップおよびコレクタ スクリプトのインストールに関する Splunk の資料: <u>https://splunkbase.splunk.com/app/2992/#/documentation</u>
- 3. Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.3.
- 4. <u>AnyConnect 4.3 のリリース ノート</u>