Fehlerbehebung bei Telemetrie-Installationsproblemen des AnyConnect Network Visibility Module in der sicheren Netzwerkanalyse

Inhalt

Einleitung Voraussetzungen Konfigurationsanleitungen Anforderungen Verwendete Komponenten **Fehlerbehebungsprozess SNA-Konfiguration** Lizenzierung überprüfen Überprüfen der NVM-Telemetrieingabe Überprüfen Sie, ob Flow Collector für die Überwachung von NVM-Telemetrie konfiguriert ist. Endgerätekonfiguration NVM-Profil überprüfen Überprüfen der TND-Einstellungen (Trusted Network Detection) **TND-Konfiguration in VPN-Profil TND-Konfiguration im NVM-Profil** Paketerfassung erfassen Verwandte Fehler Zugehörige Informationen

Einleitung

In diesem Dokument wird das Verfahren zur Fehlerbehebung bei NVM-Telemetriedaten (Network Visibility Module) in Secure Network Analytics (SNA) beschrieben.

Voraussetzungen

- Kenntnisse zu Cisco SNA
- Cisco AnyConnect

Konfigurationsanleitungen

- Konfigurationsleitfaden für Secure Network Analytics Endpoint License and Network Visibility <u>Module (NVM)</u>
- <u>Cisco AnyConnect Administrator Guide Network Visibility Module, Version 4.10</u>

Anforderungen

- SNA Manager und Flow Collector ab Version 7.3.2
- SNA Endpoint-Lizenz
- Cisco AnyConnect mit Network Visibility Module 4.3 oder höher

Verwendete Komponenten

- SNA Manager und Flow Collect Version 7.4.0 und Endpoint-Lizenz
- Cisco AnyConnect 4.10.03104 mit VPN und Network Visibility-Modul
- Virtuelles Windows 10-System
- Wireshark-Software

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Fehlerbehebungsprozess

SNA-Konfiguration

Lizenzierung überprüfen

Stellen Sie sicher, dass das virtuelle Smart Licensing-Konto, bei dem der SNA Manager registriert ist, über Endgerätelizenzen verfügt.

Überprüfen der NVM-Telemetrieingabe

So prüfen Sie, ob der SNA Flow Collector NVM-Telemetrie von den Endgeräten empfängt und einfügt:

1. Melden Sie sich über SSH oder die Konsole mit **Root-**Anmeldeinformationen beim Flow Collector an.

2. Führen Sie den Befehl grep 'NVM record this period:' /lancope/var/sw/today/logs/sw.log aus.

3. Überprüfen Sie anhand der zurückgegebenen Ausgabe, ob Flow Collector NVM-Datensätze einfügt und in die Datenbank einfügt.

ao-fc01-cds:~# grep 'NVM records this period:' /lancope/var/sw/today/logs/sw.log 04:00:01 I-pro-t: NVM records this period: received 0 at 0 rps, inserted 0 at 0 rps, discarded 0 04:05:00 I-pro-t: NVM records this period: received 0 at 0 rps, inserted 0 at 0 rps, discarded 0 04:10:00 I-pro-t: NVM records this period: received 0 at 0 rps, inserted 0 at 0 rps, discarded 0 04:15:00 I-pro-t: NVM records this period: received 0 at 0 rps, inserted 0 at 0 rps, discarded 0

Aus dieser Ausgabe scheint es, dass Flow Collector keinerlei NVM-Datensätze erhalten hat. Sie müssen jedoch bestätigen, ob es für die Überwachung der NVM-Telemetrie konfiguriert ist.

Überprüfen Sie, ob Flow Collector für die Überwachung von NVM-Telemetrie konfiguriert ist.

- 1. Melden Sie sich bei der Flow Collector Admin User Interface (UI) an.
- 2. Navigieren Sie zu **Support > Erweiterte Einstellungen**.
- 3. Stellen Sie sicher, dass die erforderlichen Attribute korrekt konfiguriert sind:

SNA Version 7.3.2 oder 7.4.0

• Suchen Sie das Attribut **nvm_netflow_port**, und überprüfen Sie den konfigurierten Wert. Dies muss mit dem Port übereinstimmen, der im AnyConnect NVM-Profil konfiguriert wurde.

cisco	Flow	FlowCollector for NetFlow VE		•
الل ا عر	Advanced Settings			
	nvm_netflow_port	2030		

Hinweis: Stellen Sie sicher, dass der konfigurierte Port ein nicht reservierter Port ist und nicht 2055, 514 oder 8514 ist. Wenn der konfigurierte Wert "0" lautet, ist die Funktion deaktiviert.

Hinweis: Wenn kein Feld angezeigt wird, blättern Sie zum Ende der Seite. Klicken Sie auf das Feld **Neue Option hinzufügen**. Weitere Informationen zu erweiterten Einstellungen auf Flow Collector finden Sie im Online-Hilfethema Erweiterte Einstellungen.

SNA Version 7.4.1

- Suchen Sie das Attribut **nvm_netflow_port**, und überprüfen Sie den konfigurierten Wert. Dies muss mit dem Port übereinstimmen, der im AnyConnect NVM-Profil konfiguriert wurde.
- Suchen Sie das **enable_nvm**-Attribut, und stellen Sie sicher, dass der Wert auf 1 festgelegt ist, andernfalls wird das Feature deaktiviert.

Ð	Flow	Collector	NetFlow \	/E
---	------	-----------	-----------	----

disco SECURE

Advanced Settings		
Option Label	Option Value	Delete
enable_nvm	1	
nvm_netflow_port	2030	

Hinweis: Stellen Sie sicher, dass der konfigurierte Port ein nicht reservierter Port ist und nicht 2055, 514 oder 8514 ist.

Hinweis: Wenn kein Feld angezeigt wird, blättern Sie zum Ende der Seite. Klicken Sie auf das Feld **Neue Option hinzufügen**. Weitere Informationen zu erweiterten Einstellungen auf Flow Collector finden Sie im Online-Hilfethema Erweiterte Einstellungen.

4. Nachdem die erweiterten Einstellungen für Flow Collector korrekt konfiguriert wurden, überprüfen Sie, ob die Telemetrie nun mit dem gleichen Verfahren wie im Abschnitt Verify NVM Telemetry Ingest (NVM-Telemetrieingaben verifizieren) integriert ist.

5. Wenn die Konfiguration des Endpunkts mit AnyConnect NVM und die Einstellungen für Flow Collector korrekt sind, muss die Datei **sw.log** Folgendes enthalten:

ao-fc01-cds:~# grep 'NVM records this period:' /lancope/var/sw/today/logs/sw.log 04:35:00 I-pro-t: NVM records this period: received 78 at 0 rps, inserted 78 at 0 rps, discarded 0 04:40:00 I-pro-t: NVM records this period: received 66 at 0 rps, inserted 66 at 0 rps, discarded 0 04:45:00 I-pro-t: NVM records this period: received 91 at 0 rps, inserted 91 at 0 rps, discarded 0 04:50:00 I-pro-t: NVM records this period: received 80 at 0 rps, inserted 80 at 0 rps, discarded 0

6. Wenn Flow Collector immer noch keine NVM-Datensätze erfasst, überprüfen Sie, ob der Collector die Pakete auf der Schnittstelle empfängt, und stellen Sie in jedem Fall sicher, dass die Konfiguration der Endpunkte korrekt ist.

Endgerätekonfiguration

Sie können AnyConnect NVM auf zwei Arten bereitstellen: a) wmit dem AnyConnect-Paket oder b) wmit dem eigenständigen NVM-Paket (nur auf AnyConnect-Desktop).

Die erforderliche Konfiguration ist für beide Bereitstellungen identisch. Der Unterschied liegt in der Konfiguration der Erkennung vertrauenswürdiger Netzwerke.

NVM-Profil überprüfen

Suchen Sie das vom Endpunkt verwendete NVM-Profil, und bestätigen Sie die **Collector-**Konfigurationseinstellungen.

Speicherort des NVM-Profils:

- Windows: %ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\NVM
- Mac: /opt/cisco/anyconnect/nvm

Anmerkung: Der Name des NVM-Profils muss **NVM_ServiceProfile** sein, da das Network Visibility Module keine Daten erfassen und senden kann.

I I I I I I I I I I I I I I I I I I I	Mary Mary				
File Prome 3	NOTE ALEM				
← → * ↑	Local Disk (C:) > Program	Nata > Cisco > Cisco A	AnyConnect Secure Mobili	ty Client → NVM	~ õ
	Name	^	Date modified	Type	Size
CANCE ACCESS	KConfig.dat		10/8/2021 11:52 PM	DAT File	1 KB
Desktop	* NVM		10/22/2021 4-58 PM	Data Base File	4 716 KB
Downloads	* NVM ServiceProfit	4	ALL DOLLARD	XML Document	1 KB
Documents	A D PersistedData dat	Open		DAT File	1 KB
Pictures	*	Edit		processing.	1 142
h Music		🥁 Edit with Notepad			
Durfle		년 Share			
Prome		Open with	>		
Videos		Cisco AMP For For	depints >		
 OneDrive 		Restore previous v	ersions		
This PC		Send to	>		

Der Inhalt des NVM-Profils hängt von Ihrer Konfiguration ab. Die für SNA relevanten Elemente des Profils sind jedoch fett markiert. Überprüfen Sie die Hinweise nach dem NVM-Profilbeispiel:

Anmerkung: Stellen Sie sicher, dass der konfigurierte Port ein nicht reservierter Port ist und nicht 2055, 514 oder 8514 ist. Der konfigurierte Port in diesem Profil muss mit dem auf dem FlowCollector konfigurierten Port identisch sein.

Anmerkung: Stellen Sie sicher, dass das NVM-Profil das **Secure** XML-Element aufweist, es auf **false** festgelegt ist, andernfalls werden die Datenflüsse mit DTLS verschlüsselt gesendet, und der Flow Collector kann sie nicht verarbeiten.

Überprüfen der TND-Einstellungen (Trusted Network Detection)

Das Network Visibility-Modul sendet Flow-Informationen nur im vertrauenswürdigen Netzwerk. Standardmäßig werden keine Daten gesammelt. Daten werden nur erfasst, wenn sie als solche im Profil konfiguriert sind, und die Daten werden weiter erfasst, wenn der Endpunkt verbunden ist. Wenn die Erfassung in einem nicht vertrauenswürdigen Netzwerk erfolgt, wird sie zwischengespeichert und an den Collector gesendet, wenn sich der Endpunkt in einem vertrauenswürdigen Netzwerk befindet. Der Secure Network Analytics Flow Collector benötigt eine zusätzliche Konfiguration für die Verarbeitung zwischengespeicherter Datenflüsse (siehe Konfigurieren des Flow Collectors für außerhalb des Netzwerks gespeicherte Datenflüsse für die erforderliche Konfiguration).

Der Status eines vertrauenswürdigen Netzwerks kann durch die TND-Funktion des VPN (konfiguriert im VPN-Profil) oder durch die TND-Konfiguration im NVM-Profil bestimmt werden:

TND-Konfiguration in VPN-Profil

Anmerkung: Dies ist keine Option für eigenständige NVM-Bereitstellungen.

1. Suchen Sie das vom Endpunkt verwendete VPN-Profil, und bestätigen Sie die konfigurierten Einstellungen für **automatische VPN-Richtlinien.**

Standort des VPN-Profils:

. . .

- Windows: %ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
- Mac: /opt/cisco/anyconnect/profile
 In diesem Beispiel trägt das VPN-Profil den Namen ACSNAProfile.



2. Bearbeiten Sie das Profil mit einem Text-Editor, und suchen Sie das **AutomaticVPNPolicy**-Element. Stellen Sie sicher, dass die konfigurierte Richtlinie korrekt ist, um das vertrauenswürdige Netzwerk erfolgreich erkennen zu können. In diesem Fall: **Anmerkung:** Für NVM-Relevanz: Wenn sowohl die Trusted Network Policy als auch die UnTrusted Network Policy (Vertrauenswürdige Netzwerkrichtlinie) auf Do Nothing (Nichts tun) festgelegt sind, wird die Erkennung vertrauenswürdiger Netzwerke aus dem VPN-Profil deaktiviert.

TND-Konfiguration im NVM-Profil

Suchen Sie das vom Endpunkt verwendete NVM-Profil, und überprüfen Sie, ob die konfigurierten Einstellungen für die Liste vertrauenswürdiger Server korrekt sind.

Speicherort des NVM-Profils:

- Windows: %ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\NVM
- Mac: /opt/cisco/anyconnect/nvm

</NVMProfile>

Anmerkung: Eine SSL-Anfrage wird an das konfigurierte vertrauenswürdige Headend gesendet, das mit einem Zertifikat antwortet, wenn es erreichbar ist. Der Daumenabdruck (SHA-256-Hash) wird extrahiert und dem Hashsatz im Profil-Editor zugeordnet. Eine erfolgreiche Übereinstimmung bedeutet, dass sich der Endpunkt in einem vertrauenswürdigen Netzwerk befindet. Wenn das Headend jedoch nicht erreichbar ist oder der Zertifikats-Hash nicht übereinstimmt, gilt der Endpunkt als in einem nicht vertrauenswürdigen Netzwerk.

Anmerkung: Vertrauenswürdige Server hinter Proxys werden nicht unterstützt.

Paketerfassung erfassen

Sie können eine Paketerfassung auf dem Endpunkt-Netzwerkadapter sammeln, um zu überprüfen, ob Datenflüsse an Flow Collector gesendet werden.

antwort: Wenn sich der Endpunkt in einem vertrauenswürdigen Netzwerk befindet, aber NICHT mit dem VPN verbunden ist, muss die Erfassung auf dem physischen Netzwerkadapter aktiviert sein.

In diesem Fall gibt der AnyConnect-Client an, dass sich der Endpunkt in einem vertrauenswürdigen Netzwerk befindet. Dies bedeutet, dass die Datenflüsse über den konfigurierten Port über den physischen Netzwerkadapter des Endpunkts an den konfigurierten Flow Collector gesendet werden, wie im AnyConnect-Fenster und im nächsten Fenster von

Wireshark zu sehen ist.

€ *Ethernet0			- 🗆 ×			
File Edit View Go Capture Analyze Statistics	Telephony Wireless Tools Help					
▲ ■ ⊿ ⑧ 📄 🗟 🕅 🔍 🖨 🔍 ⇔ 🕾 🛐	👲 📃 🗏 Q Q 🖉					
p.addr == 10.64.0.32			×→ •			
No. Time Source	Destination Protocol	Length Info				
L 131 18:29:15.945621 10.64.0.100	10.64.0.32 UDP	1035 25001 → 2030 Len=993				
2802 18:29:45.628219 10.64.0.100	10.64.0.32 UDP	338 25001 → 2030 Len=296				
3793 18:30:00.242189 10.64.0.100	10.64.0.32 UDP	326 25001 → 2030 Len=284				
3953 18:30:06.013520 10.64.0.100	10.64.0.32 UDP	1035 25001 → 2030 Len=993				
4036 18:30:11.007494 10.64.0.100	10.64.0.32 UDP	1035 25001 → 2030 Len=993				
4183 18:30:19.168065 10.64.0.100	10.64.0.32 UDP	1035 25001 → 2030 Len=993				
4303 18:30:24.163226 10.64.0.100	10.64.0.32 UDP	1028 25001 → 2030 Len=986				
4802 18:30:54.601573 10.64.0.100	10.64.0.32 UDP	667 25001 → 2030 Len=625				
└── 4895 18:30:59.803915 10.64.0.100	10.64.0.32 🕥 Cisco /	AnyConnect Secure Mobility Client	– 🗆 X			
> Frame 131: 1035 bytes on wire (8280 bits), 1035 bytes captured > Ethernet II, Src: VMware_b3:39:57 (00:50:56:b3:39:57), Dst: VM > Internet Protocol Version 4, Src: 10.64.0.100, Dst: 10.64.0.32 > User Datagram Protocol, Src Port: 25001, Dst Port: 2030 > Data (993 bytes)						
0000 00 50 56 b3 da d0 00 50 56 b3 39 57 08 00 45 00 ·PV····P V·9W··E·						
Wireshark_Ethernet0YPO381.pcapng		Packets: 5217 · Displayed: 9 (0.2%)	Profile: Default			

b. Wenn der Endpunkt mit AnyConnect VPN verbunden ist, wird er automatisch als im vertrauenswürdigen Netzwerk registriert. Daher muss die Erfassung auf dem virtuellen Netzwerkadapter aktiviert werden.

Anmerkung: Wenn das VPN-Modul installiert ist und TND im Netzwerktransparenzmodul-Profil konfiguriert ist, führt das Network Visibility Module die Erkennung vertrauenswürdiger Netzwerke auch innerhalb des VPN-Netzwerks durch.

Der AnyConnect-Client gibt an, dass der Endpunkt mit dem VPN verbunden ist. Dies bedeutet, dass die Datenflüsse über den konfigurierten Port über den virtuellen Netzwerkadapter des Endpunkts (VPN-Tunnel) an den konfigurierten Flow Collector gesendet werden, wie im AnyConnect-Fenster und im anschließend angezeigten Wireshark-Fenster zu sehen ist.

Anmerkung: Die Split-Tunnel-Konfiguration des VPN-Profils, mit dem der Endpunkt verbunden ist, muss die IP-Adresse des FlowCollectors enthalten. Andernfalls werden die Datenflüsse nicht über den VPN-Tunnel gesendet.

	*Ethernet 3						_		\times
File	e Edit View Go Capt	ture Analyze Stati	stics Telephony	Wireless To	ols Help				
	📕 🙋 💿 📄 🗟 📕	ि ९ ७ 🗢 😫	〒 🕹 📃 🔳	⊕ ⊖ ⊜					
	ip.addr == 10.64.0.32							$\times \rightarrow$	- +
No.	Time	Source	Destination	Protoco	l Length Info	o			
Г	1 18:21:21.444614	192.168.100.4	10.64.0.32	UDP	655 256	001 → 2030 Len=613			
	4 18:21:26.259175	192.168.100.4	10.64.0.32	UDP	384 250	001 → <mark>2030</mark> Len=342			
	5 18:21:26.312552	192.168.100.4	10.64.0.32	UDP	1035 250	001 → <mark>2030</mark> Len=993			
	6 18:21:36.652493	192.168.100.4	10.64.0.32	UDP	989 250	001 → 2030 Len=947			
	7 18:21:47.934603	192.168.100.4	10.64.0.32	UDP	1035 250	001 → 2030 Len=993			
	8 18:22:22.975969	192.168.100.4	10.64.0.32	UDP	648 250	001 → 2030 Len=606			
	11 18:23:03.411742	192.168.100.4	10.64.0.32	UDP	437 256	$301 \rightarrow 2030 \text{ Len} = 395$			
	14 18:23:08.50/612	192.168.100.4	10.64.0.32		1035 256	001 → 2030 Len=993			
	16 18.24.28 117600	192.168.100.4	10.64.0.32		resco Any Cisco Any	Connect Secure Mobility Client	-		×
	19 18:24:38.007397	192.168.100.4	10.64.0.32	UDP					
	20 18:25:28.663613	192.168.100.4	10.64.0.32	UDP		VPN:			
	23 18:25:38.695000	192.168.100.4	10.64.0.32	UDP		Connected to VPN headend for SNA.			
	24 18:26:03.586302	192.168.100.4	10.64.0.32	UDP					
L	27 18:26:33.226458	192.168.100.4	10.64.0.32	UDP	_	VPN headend for SNA		Disconnect	
					00:07:05			I	Pv4
					Ö				վախ
	Enome 1, SEE bytes on	wine (E240 bits)	655 hutos es	ntuned (E246	hits) on	intenface \Device\NDE (2000		E40 4710	
5	Fthernet II. Spc: Cise	0 3c · 7a · 00 (00 · 0	5.9a.3c.7a.00)	Dst. CTMSV	S 33.44.55	(00.11.22.33.44.55)	1250-0		-0090-
5	Internet Protocol Vers	sion 4. Src: 192.	168.100.4. Dst	: 10.64.0.32	5_55.44.55	(00.11.22.33.44.33)			
> User Datagram Protocol, Src Port: 25001, Dst Port: 2030									
>	Data (613 bytes)								
L									
									>
000	00 00 11 22 33 44 55	00 05 9a 3c 7a	00 08 00 45 00	· · "3DU · ·	· <z··e·< td=""><td></td><td></td><td></td><td>^</td></z··e·<>				^
00.	00 00 TC DG 16 20	00 11 /C 00 C0	ao o4 04 0a 40		Ia(a)	Dedictor 27 - Disclounds 15 (55 cm)	11	Des flas De	IL
	 wireshark_Ethernet 382 	2JUB 1.pcapng				Packets: 27 • Displayed: 15 (55.6%)		Profile: De	rault

c. Wenn sich der Endpunkt nicht in einem vertrauenswürdigen Netzwerk befindet, werden die Datenflüsse nicht an den Flow Collector gesendet.

	*Ethernet0				- 🗆 ×
File	Edit View Go	Capture Analyz	e Statistics Telephony Wirel	ess Tools Help	
	i 🧕 🙆 📕	X C 9 🗢	🗢 🕾 🗿 🛓 📃 🔍 (e, e, II	
ir	.addr == 10.64.0.32				+ 💌 🔁
No.	Time	Source	Destination	Protocol Length Info	
				Sy Cisco AnyConnect Secure Mobility Clie	nt – 🗆 X
				Ready to connect.	
				VPN headend for SNA	✓ Connect
				A 0	alulu
				* •	CISCO
<					>

Verwandte Fehler

Derzeit gibt es zwei bekannte Fehler, die sich auf den NVM-Telemetrie-Aufnahmeprozess für sichere Netzwerkanalysen auswirken können:

- FC Engine kann NVM-Telemetrie nicht auf eth1 empfangen. Siehe Cisco Bug-ID <u>CSCwb84013</u>
- Flow Collector fügt keine NVM-Datensätze von AnyConnect Version 4.10.04071 oder höher ein. Siehe Cisco Bug-ID <u>CSCwb91824</u>

Zugehörige Informationen

- Weitere Unterstützung erhalten Sie vom Technical Assistance Center (TAC). Ein gültiger Support-Vertrag ist erforderlich: <u>Weltweiter Kontakt zum Cisco Support.</u>
- Sie können auch die Cisco Security Analytics Community hier besuchen.
- <u>Technischer Support und Dokumentation für Cisco Systeme</u>