Probleemoplossing met AnyConnect Network Visibility and Module: Telemetrie in beveiligde netwerkanalyses

Inhoud

Inleiding Voorwaarden Configuratiehandleidingen Vereisten Gebruikte componenten Probleemoplossing **SNA-configuratie** Controleer de licenties Controleer de NVM-telemetrie-index Controleer of de Flow Collector is ingesteld om te luisteren naar NVM-telemetrie Endpoint configuratie **Controleer NVM-profiel** Controleer de TND-instellingen (Trusted Network Detection) **TND-configuratie in VPN-profiel TND-configuratie in NVM-profiel** Verzamelen van pakketvastlegging Verwante tekortkomingen Gerelateerde informatie

Inleiding

In dit document wordt de procedure beschreven om NVM-telemetrie (Network Visibility Module) te implementeren in Secure Network Analytics (SNA).

Voorwaarden

- Cisco SNA-kennis
- Cisco AnyConnect-kennis

Configuratiehandleidingen

- Configuratie-gids voor Secure Network Analytics Endpoint License and Network Visibility Module (NVM)
- Cisco AnyConnect Administrator Guide netwerkzichtbaarheidsmodule, release 4.10

Vereisten

- SNA Manager en Flow Collector in versie 7.3.2 of nieuwer
- Licentie voor SNA Endpoint
- Cisco AnyConnect met netwerkzichtbaarheidsmodule 4.3 of nieuwer

Gebruikte componenten

- SNA Manager en Flow Collector, versie 7.4.0 en Endpoint Licentie
- Cisco AnyConnect 4.10.3104 met VPN en netwerkzichtbaarheidsmodule
- Windows 10 virtuele machine
- Software voor draadloos shark

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Probleemoplossing

SNA-configuratie

Controleer de licenties

Zorg ervoor dat de Smart Licensing Virtual-account waarop SNA Manager is geregistreerd, de Endpoint Licenties heeft.

Controleer de NVM-telemetrie-index

Om te bevestigen of de SNA Flow Collector NVM-telemetrie van de eindpunten ontvangt en plaatst, gaat u als volgt te werk:

1. Meld u aan bij de Flow Collector via SSH of console met basisreferenties.

2. Start de grop 'NVM registreert deze periode:' /lancope/var/sw/today/logs/sw.log opdracht.

3. bevestig of de Flow Collector NVM records inneemt en deze in de database plaatst.

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

Uit deze output blijkt dat de Flow Collector helemaal geen NVM-bestanden heeft ontvangen, maar u moet wel bevestigen of het is ingesteld om te luisteren voor NVM-telemetrie.

Controleer of de Flow Collector is ingesteld om te luisteren naar NVM-telemetrie

1. Meld u aan bij de Flow Collector Admin User Interface (UI).

2. Navigeer naar Ondersteuning > Geavanceerde instellingen.

3. Zorg ervoor dat de vereiste eigenschappen correct zijn geconfigureerd:

SNA versie 7.3.2 of 7.4.0

• Pak de **nvm_netflow_port** eigenschap vast en controleer de geconfigureerde waarde. Dit moet overeenkomen met de poort die in het AnyConnect NVM-profiel is geconfigureerd.

cisco	1. D	FlowCollector for NetFlow VE	?	•
ال ة بر	Advanced Setting	S		
	nvm_netflow_port	2030		

Opmerking: Zorg ervoor dat de geconfigureerde poort een niet-gereserveerde poort is en niet 2055, 514 of 8514. Als de ingestelde waarde "0" is, wordt de optie uitgeschakeld.

N.B.: Als een veld niet wordt weergegeven, scrollen we naar de onderkant van de pagina. Klik op het veld **Nieuwe optie toevoegen**. Raadpleeg voor meer informatie over geavanceerde instellingen in de Flow Collector het online Help-onderwerp Geavanceerde instellingen.

SNA versie 7.4.1

=======================================	=======================================	
	=	

- Pak de **nvm_netflow_port** eigenschap vast en controleer de geconfigureerde waarde. Dit moet overeenkomen met de poort die in het AnyConnect NVM-profiel is geconfigureerd.
- Pak de eigenschap **Enable_nvm vast** en zorg ervoor dat de waarde is ingesteld op **1**, anders wordt de functie uitgeschakeld.



Advanced Settings		
Option Label	Option Value	Delete
enable_nvm	1	
nvm_netflow_port	2030	

Opmerking: Zorg ervoor dat de geconfigureerde poort een niet-gereserveerde poort is en niet 2055, 514 of 8514.

N.B.: Als een veld niet wordt weergegeven, scrollen we naar de onderkant van de pagina. Klik op het veld **Nieuwe optie toevoegen**. Raadpleeg voor meer informatie over geavanceerde instellingen in de Flow Collector het online Help-onderwerp Geavanceerde instellingen.

4. Controleer, zodra de geavanceerde instellingen op de Flow Collector correct zijn geconfigureerd, of de telemetrie nu wordt opgenomen, met dezelfde procedure als in het gedeelte **Controleer NVM Telemetry Ingest**.

5. Als de configuratie van het eindpunt met AnyConnect NVM en de instellingen op de Flow Collector juist zijn, moet het **sw.log**-bestand het volgende weergeven:

```
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. Als de Flow Collector nog steeds geen NVM-gegevens inneemt, controleert u of de verzamelaar de pakketten op de interface ontvangt en in ieder geval of de configuratie van de eindpunten juist is.

Endpoint configuratie

U kunt AnyConnect NVM op twee manieren implementeren: a) wmet het AnyConnect-pakket of b)Met het Standalone NVM-pakket (alleen op AnyConnect-desktop).

De gewenste configuratie is hetzelfde voor beide implementaties, het verschil is aanwezig in de configuratie van Trusted Network Detectie.

Controleer NVM-profiel

Zoek het NVM Profile dat door het eindpunt wordt gebruikt en bevestig de **Collector Configuration**instellingen.

NVM-profiel:

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

Opmerking: De naam van het NVM-profiel moet **NVM_ServiceProfile** zijn, anders worden er geen gegevens verzameld en verzonden door Network Visibility Module.



De inhoud van het NVM-profiel hangt af van uw configuratie, maar de elementen van het profiel die relevant zijn voor SNA worden vet weergegeven. Zorg ervoor dat de opmerkingen na het voorbeeld van het NVM-profiel worden bekeken:

Opmerking: Zorg ervoor dat de **geconfigureerde poort een niet-gereserveerde poort is en niet 2055, 514 of 8514**. De geconfigureerde poort in dit profiel moet dezelfde zijn als de poort die in de Flow Collector is ingesteld.

Opmerking: Zorg ervoor dat als het NVM Profile het Secure XML-element heeft, het op vals

is ingesteld, anders worden de stromen versleuteld met DTLS en kan de Flow Collector ze niet verwerken.

Controleer de TND-instellingen (Trusted Network Detection)

De Network Visibility Module stuurt alleen stroominformatie als deze op het vertrouwde netwerk is aanwezig. Standaard worden geen gegevens verzameld. Er worden alleen gegevens verzameld wanneer deze als zodanig in het profiel zijn geconfigureerd en de gegevens blijven verzameld worden wanneer het eindpunt is verbonden. Als de collectie op een onbetrouwbaar netwerk wordt gedaan, wordt het gecached en naar de verzamelaar gestuurd wanneer het eindpunt op een vertrouwd netwerk is. De Secure Network Analytics Flow Collector moet beschikken over een extra configuratie voor het verwerken van gecacheerde stromen (zie <u>het configureren van de Flow Collector voor</u> buiten <u>het netwerk gecompileerde stromen</u> voor de benodigde configuratie).

De vertrouwde netwerkstatus kan worden bepaald door de TND-functie van VPN (geconfigureerd in het VPN-profiel) of door de TND-configuratie in het NVM-profiel:

TND-configuratie in VPN-profiel

Opmerking: Dit is geen optie voor standalone NVM-implementaties.

1. Pak het VPN-profiel vast dat door het eindpunt wordt gebruikt en bevestig de geconfigureerde **automatische VPN-**beleidsinstellingen

VPN-profiellocatie:

. . .

- Windows: %Program Data%\Cisco AnyConnect Secure Mobility Client\Profile
- Mac: /opt/cisco/anyconnect/profile

In dit voorbeeld wordt het VPN-profiel ACSNAProfile genoemd.

📙 🕑 📙 🖬 Pro	ofile						
File Home	Share	View					
← → * ↑	« Pro	gramData > Cisco	> Cisco AnyConnect Sec	cure Mobility Client > Profile	e	~	õ
		Name	^	Date modified	Туре	Size	
Desktop		MgmtTun		10/8/2021 11:12 PM	File folder		
+ Downloads	*	AcSNAProfile	Open	P AM	XML Document XSD File		4 KB 96 KB
Documents			Edit		100110		
Fictures	\$		Edit with Notepad++				
👌 Music			E Share				
Postila			Open with	2			

2. Bewerk het profiel met een teksteditor en plaats het beleidselement **Automatisch** uitvoeren. Zorg ervoor dat het geconfigureerde beleid correct is voor het met succes detecteren van het Trusted Network. In dat geval: **Opmerking:** Voor NVM-relevantie: Als zowel het Trusted Network Policy als het Onvertrouwde netwerkbeleid zijn ingesteld op Niets doen, wordt de vertrouwde netwerkdetectie van het VPN-profiel uitgeschakeld.

TND-configuratie in NVM-profiel

Zoek het NVM profiel dat door het eindpunt wordt gebruikt en bevestig dat de geconfigureerde **Trusted Server List** instellingen correct zijn.

NVM-profiel:

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

</NVMProfile>

...

Opmerking: Een SSL sonde wordt naar het gevormde vertrouwde head-end verzonden, dat met een certificaat reageert indien bereikbaar. De thumbprint (SHA-256 shash) wordt dan geëxtraheerd en afgesloten tegen de hash die in de profieleditor is ingesteld. Een succesvolle match betekent dat het eindpunt in een betrouwbaar netwerk ligt. als het head-end echter onbereikbaar is of als de certificaathash niet overeenkomt, wordt het eindpunt geacht in een onbetrouwbaar netwerk te liggen.

Opmerking: Trusted servers achter proxy's worden niet ondersteund.

Verzamelen van pakketvastlegging

U kunt een pakketvastlegging op de netwerkadapter van Endpoint verzamelen om te controleren

of de stromen naar de Flow Collector worden verzonden.

a. Als het Endpoint op een Trusted Network is aangesloten maar NIET op VPN is aangesloten, moet de opname op de fysieke netwerkadapter zijn ingeschakeld.

In dit geval geeft de AnyConnect-client aan dat het eindpunt op een betrouwbaar netwerk is gelegen, wat betekent dat de stromen naar de geconfigureerde Flow Collector via de geconfigureerde poort worden verzonden door de Physical Network Adapter van het eindpunt, zoals we in het AnyConnect-venster en het venster Wireshark hierna kunnen zien.

	*Ethern	et0												_		\times
File	Edit	View Go	Capt	ure Ar	nalyze	Statistics	Telephony	Wireless	Tools Hel	р						
		O	\mathbf{X}	۹ (۵	1	& ⊒ ≡	⊕, ⊝, €	. 🏨							
i,	addr =	= 10.64.0.32													× →	• +
No.		Time		Source			Destination		Protocol	Length	Info					
Г	131	18:29:15.94	5621	10.64.	0.100		10.64.0.3	2	UDP	1035	5 25001 →	2030	Len=993			
	2802	18:29:45.62	8219	10.64.	0.100		10.64.0.3	2	UDP	338	3 25001 →	2030	Len=296			
	3793	18:30:00.24	2189	10.64.	0.100		10.64.0.3	2	UDP	320	5 25001 →	2030	Len=284			
	3953	18:30:06.01	3520	10.64.	0.100		10.64.0.3	2	UDP	1035	5 25001 →	2030	Len=993			
	4036	18:30:11.00	7494	10.64.	0.100		10.64.0.3	2	UDP	1039	5 25001 →	2030	Len=993			
	4183	18:30:19.16	8065	10.64.	0.100		10.64.0.3	2	UDP	1035	5 25001 →	2030	Len=993			
	4303	18:30:24.16	3226	10.64.	0.100		10.64.0.3	2	UDP	1028	3 25001 →	2030	Len=986			
	4802	18:30:54.60	1573	10.64.	0.100		10.64.0.3	2	UDP	667	7 25001 →	2030	Len=625			
	4895	18:30:59.80	3915	10.64.	0.100		10.64.0.3	2	🔄 🕥 Cisco	AnyCor	nnect Secur	e Mobili	ty Client	-		×
> F > E > J > U > T	> 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															
<	0 00	50 56 b3 da	a d0	00 50	56 b3	39 57 0	8 00 45 00	· PV · · ·	P. V. 9W - F							>
	V V V V V V V V V V V V V V V V V V V															
0	2 w	ireshark_Ethern	et0YP0	D3B1.pca	png				-	P	ackets: 5217	' Display	ed: 9 (0.2%	6)	Profile: D	efault

b. Als het Endpoint is verbonden met AnyConnect VPN wordt het automatisch geacht op het Trusted Network te zijn geïnstalleerd en moet de opname daarom op de Virtual Network Adapter zijn ingeschakeld.

Opmerking: Als de VPN-module is geïnstalleerd en TND is geconfigureerd in het profiel van Netwerkzichtbaarheidsmodule, dan voert de netwerkzichtbaarheidsmodule een betrouwbare netwerkdetectie uit, zelfs in het VPN-netwerk.

De AnyConnect-client geeft aan dat het eindpunt met VPN is verbonden, wat betekent dat de stromen naar de geconfigureerde Flow Collector via de geconfigureerde poort worden verzonden door de Virtual Network Adapter of the Endpoint (VPN-tunnelheid), zoals we in het AnyConnect-venster en het Wireshark-venster hieronder kunnen zien.

Opmerking: De configuratie van de Split-tunnelconfiguratie van het VPN-profiel dat het Endpoint is verbonden met inbegrip van het IP-adres van de Flow Collector, anders worden de stromen niet over de VPN-tunnel verzonden.

	*Ethernet 3						_		\times
File	Edit View Go Capt	ure Analyze Stati	stics Telephony	Wireless Tools	Help				
	d 🛛 🗋 🕅	G 9 0 0 2	₮ 🕹 📃 🔳	⊕, ⊖, ⊜, ∰					
I III	p.addr == 10.64.0.32							$\times \rightarrow$	• +
No.	Time	Source	Destination	Protocol L	ength Info				
Г	1 18:21:21.444614	192.168.100.4	10.64.0.32	UDP	655 2500	01 → 2030 Len=613			
	4 18:21:26.259175	192.168.100.4	10.64.0.32	UDP	384 2500	01 → 2030 Len=342			
	5 18:21:26.312552	192.168.100.4	10.64.0.32	UDP	1035 2500	01 → 2030 Len=993			
	6 18:21:36.652493	192.168.100.4	10.64.0.32	UDP	989 2500	01 → 2030 Len=947			
	7 18:21:47.934603	192.168.100.4	10.64.0.32	UDP	1035 2500	01 → 2030 Len=993			
	8 18:22:22.975969	192.168.100.4	10.64.0.32	UDP	648 2500	01 → 2030 Len=606			
	11 18:25:05.411/42	192.168.100.4	10.64.0.32	UDP	437 2508	$21 \rightarrow 2030 \text{ Len}=395$			
	14 10:25:00.50/012	192.100.100.4	10.04.0.32		1055 2500	2050 Len=995			
	16 18:24:28.117600	192.168.100.4	10.64.0.32	UDP	Cisco AnyO	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	
					0.07.05				2.4
					0:07:05			1	7V4
					ن \$				iliilii cisco
>	Frame 1: 655 bytes on	wire (5240 bits)	, 655 bytes cap	tured (5240 b	its) on i	nterface \Device\NPF_{3A925	E5D-6	F49-4710	-8890-
> 1	Ethernet II, Src: Cisc	:o_3c:7a:00 (00:0	5:9a:3c:7a:00),	Dst: CIMSYS_	33:44:55	(00:11:22:33:44:55)			
> :	Internet Protocol Vers	sion 4, Src: 192.	168.100.4, Dst:	10.64.0.32					
> (User Datagram Protocol	l, Src Port: 2500	01, Dst Port: 20	30					
>	Data (613 bytes)								
<									>
000	0 00 11 22 33 44 55	00 05 9a 3c 7a	00 08 00 45 00	···"3DU···· <z< td=""><td>2···Ε·</td><td></td><td></td><td></td><td>^</td></z<>	2···Ε·				^
001	0 02 81 8d 5f 00 00	80 11 7c 00 c0	a8 64 04 0a 40		··d··@				~
\bigcirc	Wireshark_Ethernet 3B2	JUB1.pcapng				Packets: 27 · Displayed: 15 (55.6%)		Profile: De	fault

c. Als het Endpoint niet op een betrouwbaar netwerk is, worden er geen stromen naar de Flow Collector verzonden.

	*Ethernet0				– 🗆 X
File	Edit View Go	Capture Analy	ze Statistics Telephony Wirele	ess Tools Help	
	i 🧕 🙆 🖪	X 🖸 🍳 🤄	• 🗢 🕾 👔 🛓 📃 🔍 🤤		
🔳 ip	.addr == 10.64.0.32				+
No.	Time	Source	Destination	Protocol Length Info	
				Circo Any Connect Secure Mahility Clier	
				Gisco Anyconnect secure mobility citer	
				VPN-	
				Ready to connect.	
				VPN headend for SNA	Connect
				VPN headend for SiNA	Connect
				Ö (i)	alaala
					CISCO
<					>

Verwante tekortkomingen

Er zijn momenteel twee bekende defecten die van invloed kunnen zijn op het ingeslikte NVMtelemetrie-proces bij Secure Network Analytics:

- FC Engine kan NVM-telemetrie niet op eth1 innemen. Zie Cisco bug-id CSCwb84013
- Flow Collector voegt geen NVM records in vanaf AnyConnect versie 4.10.04071 of hoger. Zie Cisco bug-id <u>CSCwb91824</u>

Gerelateerde informatie

- Voor extra hulp kunt u contact opnemen met het Technical Assistance Center (TAC). Een geldig ondersteuningscontract is vereist: <u>Cisco's wereldwijde contactgegevens voor ondersteuning.</u>
- U kunt hier ook de Cisco Security Analytics-community bezoeken.
- <u>Technische ondersteuning en documentatie Cisco Systems</u>