Dépannage des problèmes de base de télémétrie du module de visibilité réseau AnyConnect dans Secure Network Analytics

Contenu

Introduction Conditions préalables Guides de configuration **Conditions requises Components Used** Processus de dépannage **Configuration SNA** Vérifier la licence Vérifier l'entrée de télémétrie NVM Vérifier si le collecteur de flux est configuré pour écouter la télémétrie NVM Configuration des points de terminaison Vérifier le profil NVM Vérifier les paramètres TND (Trusted Network Detection) Configuration TND dans le profil VPN Configuration TND dans le profil NVM Collecter les captures de paquets Défauts associés Informations connexes

Introduction

Ce document décrit la procédure de dépannage des problèmes de télémétrie NVM (Network Visibility Module) dans Secure Network Analytics (SNA).

Conditions préalables

- Connaissances Cisco SNA
- Connaissances Cisco AnyConnect

Guides de configuration

- Guide de configuration des modules NVM (Secure Network Analytics Endpoint License) et NVM (Network Visibility Module)
- <u>Cisco AnyConnect Administrator Guide Network Visibility Module, version 4.10</u>

Conditions requises

- SNA Manager et Flow Collector dans la version 7.3.2 ou ultérieure
- Licence de terminaux SNA
- Cisco AnyConnect avec Network Visibility Module 4.3 ou ultérieur

Components Used

- SNA Manager et Flow Collector version 7.4.0 et licence de terminaux
- Cisco AnyConnect 4.10.03104 avec VPN et module de visibilité réseau
- Ordinateur virtuel Windows 10
- Logiciel Wireshark

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Processus de dépannage

Configuration SNA

Vérifier la licence

Assurez-vous que le compte virtuel Smart Licensing auquel le SNA Manager est enregistré dispose des licences de point de terminaison.

Vérifier l'entrée de télémétrie NVM

Pour vérifier si le collecteur de flux SNA reçoit et insère la télémétrie NVM des points d'extrémité, procédez comme suit :

1. Connectez-vous au collecteur de flux via SSH ou la console avec les informations d'identification **racine**.

2. Exécutez la commande grep 'NVM enregistre cette période : ' /lancope/var/sw/today/logs/sw.log.

3. À partir de la sortie renvoyée, vérifiez si le collecteur de flux ingère des enregistrements NVM et les insère dans la base de données.

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

Àpartir de cette sortie, il semble que le collecteur de flux n'a reçu aucun enregistrement NVM, mais vous devez confirmer s'il est configuré pour écouter la télémétrie NVM.

Vérifier si le collecteur de flux est configuré pour écouter la télémétrie NVM

1. Connectez-vous à l'interface utilisateur de Flow Collector Admin.

2. Accédez à Support > Advanced Settings.

3. Assurez-vous que les attributs requis sont configurés correctement :

SNA version 7.3.2 ou 7.4.0

• Recherchez l'attribut **nvm_netflow_port** et vérifiez la valeur configurée. Cela doit correspondre au port configuré dans le profil NVM AnyConnect.

cisco		FlowCollector for NetFlow VE	
# 2	Advanced Settings		
	nvm_netflow_port	2030	

Remarque : assurez-vous que le port configuré est un port non réservé et qu'il n'est pas 2055, 514 ou 8514. Si la valeur configurée est 0, la fonction est désactivée.

Remarque : si aucun champ n'est affiché, faites défiler la page jusqu'en bas. Cliquez sur le champ **Ajouter une nouvelle option**. Pour plus d'informations sur les paramètres avancés du collecteur de flux, reportez-vous à la rubrique d'aide en ligne Paramètres avancés.

SNA version 7.4.1

- Recherchez l'attribut **nvm_netflow_port** et vérifiez la valeur configurée. Cela doit correspondre au port configuré dans le profil NVM AnyConnect.
- Recherchez l'attribut **enable_nvm** et assurez-vous que la valeur est définie sur **1**, sinon la fonction est désactivée.



Advanced Settings					
Option Label	Option Value	Delete			
enable_nvm	1				
nvm_netflow_port	2030				

Remarque : assurez-vous que le port configuré est un port non réservé et qu'il n'est pas 2055, 514 ou 8514.

Remarque : si aucun champ n'est affiché, faites défiler la page jusqu'en bas. Cliquez sur le champ **Ajouter une nouvelle option**. Pour plus d'informations sur les paramètres avancés du collecteur de flux, reportez-vous à la rubrique d'aide en ligne Paramètres avancés.

4. Une fois que les paramètres avancés du collecteur de flux ont été configurés correctement, vérifiez si la télémétrie est maintenant ingérée, avec la même procédure que celle décrite dans la section Vérifier la télémétrie NVM.

5. Si la configuration du point de terminaison avec AnyConnect NVM et les paramètres du collecteur de flux sont corrects, le fichier **sw.log** doit le refléter :

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. Si le collecteur de flux n'ingère toujours pas d'enregistrements NVM, vérifiez si le collecteur reçoit les paquets sur l'interface et, dans tous les cas, assurez-vous que la configuration des points de terminaison est correcte.

Configuration des points de terminaison

Vous pouvez déployer AnyConnect NVM de deux manières : a) wavec le package AnyConnect ou b) wavec le package NVM autonome (sur le bureau AnyConnect uniquement).

La configuration requise est la même pour les deux déploiements, la différence réside dans la configuration de Trusted Network Detection.

Vérifier le profil NVM

Recherchez le profil NVM utilisé par le point de terminaison et confirmez les paramètres **de configuration du collecteur**.

Emplacement du profil NVM :

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

Note: Le nom du profil NVM doit être **NVM_ServiceProfile**, sinon le module de visibilité réseau ne collecte pas et n'envoie pas de données.



Le contenu du profil NVM dépend de votre configuration, mais les éléments du profil qui sont pertinents pour SNA sont indiqués en gras. Vérifiez les notes après l'exemple de profil NVM :

Note: Assurez-vous que le port configuré est un port non réservé et qu'il n'est pas 2055, 514 ou 8514. Le port configuré dans ce profil doit être identique à celui configuré sur le collecteur de flux.

Note: Assurez-vous que si le profil NVM possède l'élément **Secure** XML, il est défini sur **false**, sinon les flux sont envoyés chiffrés avec DTLS et le collecteur de flux ne peut pas les

traiter.

Vérifier les paramètres TND (Trusted Network Detection)

Le module de visibilité réseau envoie des informations de flux uniquement lorsqu'il se trouve sur le réseau approuvé. Par défaut, aucune donnée n'est collectée. Les données sont collectées uniquement lorsqu'elles sont configurées en tant que telles dans le profil, et les données continuent d'être collectées lorsque le point de terminaison est connecté. Si la collecte est effectuée sur un réseau non approuvé, elle est mise en cache et envoyée au collecteur lorsque le point d'extrémité est sur un réseau approuvé. Le collecteur de flux Secure Network Analytics doit disposer d'une configuration supplémentaire pour traiter les flux mis en cache (voir <u>Configurer le collecteur de flux pour les flux mis en cache hors réseau</u> pour la configuration requise).

L'état du réseau approuvé peut être déterminé par la fonction TND du VPN (configuré dans le profil VPN) ou par la configuration TND du profil NVM :

Configuration TND dans le profil VPN

Note: Il ne s'agit pas d'une option pour les déploiements autonomes NVM.

1. Localisez le profil VPN utilisé par le point de terminaison et confirmez les paramètres **de stratégie VPN automatique** configurés

Emplacement du profil VPN :

. . .

- Fenêtres: %ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
- Mac : /opt/cisco/anyconnect/profile

Dans cet exemple, le profil VPN est nommé ACSNAProfile.



2. Modifiez le profil à l'aide d'un éditeur de texte et localisez l'élément **AutomaticVPNPolicy**. Assurez-vous que la stratégie configurée est correcte pour une détection réussie du réseau de confiance. Dans ce cas : **Note**: Pour la pertinence NVM : si la stratégie de réseau approuvé et la stratégie de réseau non approuvé sont toutes deux définies sur Do Nothing, la détection de réseau approuvé du profil VPN est désactivée.

Configuration TND dans le profil NVM

Recherchez le profil NVM utilisé par le point de terminaison et vérifiez que les paramètres configurés de la **liste de serveurs approuvés** sont corrects.

Emplacement du profil NVM :

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

</NVMProfile>

...

Note: Une sonde SSL est envoyée à la tête de réseau de confiance configurée, qui répond avec un certificat, si accessible. L'empreinte numérique (hachage SHA-256) est ensuite extraite et mise en correspondance avec le jeu de hachages dans l'éditeur de profils. Une correspondance réussie signifie que le point de terminaison se trouve dans un réseau de confiance ; toutefois, si la tête de réseau est inaccessible ou si le hachage de certificat ne correspond pas, le point de terminaison est considéré comme se trouvant dans un réseau non fiable.

Note: Les serveurs approuvés derrière les serveurs proxy ne sont pas pris en charge.

Collecter les captures de paquets

Vous pouvez collecter une capture de paquets sur la carte réseau du point de terminaison pour vérifier que les flux sont envoyés au collecteur de flux.

a. Si le point de terminaison se trouve sur un réseau de confiance mais NON connecté au VPN, la capture doit être activée sur la carte réseau physique.

Dans ce cas, le client Anyconnect indique que le point de terminaison se trouve sur un réseau de confiance, ce qui signifie que les flux sont envoyés au collecteur de flux configuré sur le port configuré via l'adaptateur réseau physique du point de terminaison, comme nous pouvons le voir dans la fenêtre AnyConnect et la fenêtre Wireshark affichée ensuite.



b. Si le point de terminaison est connecté à AnyConnect VPN, il est automatiquement considéré comme étant sur le réseau approuvé, par conséquent la capture doit être activée sur l'adaptateur réseau virtuel.

Note: Si le module VPN est installé et que TND est configuré dans le profil du module de visibilité réseau, le module de visibilité réseau effectue une détection de réseau fiable même à l'intérieur du réseau VPN.

Le client AnyConnect indique que le point de terminaison est connecté au VPN, ce qui signifie que les flux sont envoyés au collecteur de flux configuré sur le port configuré via l'adaptateur réseau virtuel du point de terminaison (tunnel VPN), comme nous pouvons le voir dans la fenêtre AnyConnect et la fenêtre Wireshark affichée suivante.

Note: La configuration du tunnel partagé du profil VPN auquel le point de terminaison est connecté doit inclure l'adresse IP du collecteur de flux, sinon les flux ne sont pas envoyés à travers le tunnel VPN.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Hep 	*Ethernet 3	- 🗆 ×						
Image: Source in the	File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help							
Image: Protocol Length Info Protocol Length Info 1 16:21:21.444614 192.168.100.4 4 18:21:22.12.12.12.12.12.12.12.12.12.12.12.12.1	◢ ■ ⊿ ⊙ □ ⊠ ⊠ □ ੧ ⇔ ⇔ ≌ ↑ ୬ 🔄 들 @ ٩ ٩ ٩ ₩							
No. Time Source Destination Protocol Length Info 1 18:21:21.444614 192.168.100.4 10.64.0.32 UDP 635 25001 + 2030 Len=613 4 18:21:26.25175 192.168.100.4 10.64.0.32 UDP 384 25901 + 2030 Len=613 5 18:21:26.372552 192.168.100.4 10.64.0.32 UDP 384 25901 + 2030 Len=993 6 18:21:26.3736.65243 192.168.100.4 10.64.0.32 UDP 1035 25901 + 2030 Len=993 8 18:22:22.975969 192.168.100.4 10.64.0.32 UDP 648 25001 + 2030 Len=606 11 18:23:08.0570612 192.168.100.4 10.64.0.32 UDP 433 25001 + 2030 Len=993 15 18:23:28.057062 192.168.100.4 10.64.0.32 UDP 438 25001 + 2030 Len=993 15 18:23:28.057307 192.168.100.4 10.64.0.32 UDP 638 25001 + 2030 Len=993 16 18:24:38.097307 192.168.100.4 10.64.0.32 UDP 638 25001 + 2030 Len=613 17 18:25:28.586362 192.168.100.4 10.64	p.addr == 10.64.0.32	× +						
1 18:21:21.444614 192.168.100.4 10.64.0.32 UDP 655 25001 + 2030 Lem=613 4 18:21:26.259175 192.168.100.4 10.64.0.32 UDP 1035 25001 + 2030 Lem=342 6 18:21:26.259175 192.168.100.4 10.64.0.32 UDP 1085 25001 + 2030 Lem=947 7 18:21:47.93468 192.168.100.4 10.64.0.32 UDP 648 25001 + 2030 Lem=947 7 18:21:47.93468 192.168.100.4 10.64.0.32 UDP 648 25001 + 2030 Lem=947 11 18:23:03.411742 192.168.100.4 10.64.0.32 UDP 648 25001 + 2030 Lem=993 15 18:23:23.539071 392.168.100.4 10.64.0.32 UDP 437 25001 + 2030 Lem=993 16 18:24:28.117600 192.168.100.4 10.64.0.32 UDP Gisco AnyConnect Secure Mobility Client — X 19 18:25:28.663613 192.168.100.4 10.64.0.32 UDP Ocioo:0: Connected to VPN headend for SNA. 20 18:25:28.653613 192.168.100.4 10.64.0.32 UDP Ocioo:0:0: IPv4 21 18:26:33.226458 19	No. Time Source Destination Protocol Length Info							
4 18:21:26.259175 192.168.100.4 10.64.0.32 UDP 384 25801 + 2030 Lem=942 5 18:21:26.32252 192.168.100.4 10.64.0.32 UDP 999 25001 + 2030 Lem=947 7 18:21:47.934603 192.168.100.4 10.64.0.32 UDP 1035 25001 + 2030 Lem=947 1 18:23:03.411742 192.168.100.4 10.64.0.32 UDP 437 25001 + 2030 Lem=966 1 1 18:23:03.597612 192.168.100.4 10.64.0.32 UDP 437 25001 + 2030 Lem=993 1 6 18:24:28.117600 192.168.100.4 10.64.0.32 UDP 1035 25001 + 2030 Lem=993 1 6 18:24:28.117600 192.168.100.4 10.64.0.32 UDP 1035 25001 + 2030 Lem=993 1 1 8:23:03.59073 192.168.100.4 10.64.0.32 UDP 1035 25001 + 2030 Lem=993 1 1 8:24:38.007397 192.168.100.4 10.64.0.32 UDP 1035 25001 + 2030 Lem=903 2 1 8:25:28.663613 192.168.100.4 10.64.0.32 UDP Connected to VPN headend for SNA, Lem=903 2 1 8:26:33.226458 192.168.100.4 10.64.0.32 UDP VPN: Connected to VPN headend for SNA, 2 1 18:26:33.226458 192.168.100.4,	□ 1 18:21:21.444614 192.168.100.4 10.64.0.32 UDP 655 25001 → 2030 Len=613							
5 18:21:26.312552 192.168.100.4 10.64.0.32 UDP 1035 25001 + 2030 Len=993 6 18:21:36.652493 192.168.100.4 10.64.0.32 UDP 989 25001 + 2030 Len=993 8 18:22:22.975969 192.168.100.4 10.64.0.32 UDP 648 25001 + 2030 Len=993 11 18:23:03.411742 192.168.100.4 10.64.0.32 UDP 648 25001 + 2030 Len=993 14 18:23:08.570612 192.168.100.4 10.64.0.32 UDP 648 25001 + 2030 Len=993 15 18:23:23.539073 192.168.100.4 10.64.0.32 UDP 1035 25001 + 2030 Len=993 16 18:24:28.07037 192.168.100.4 10.64.0.32 UDP 1035 25001 + 2030 Len=993 19 18:24:38.07307 192.168.100.4 10.64.0.32 UDP IDP 1035 Len=993 23 18:25:38.695000 192.168.100.4 10.64.0.32 UDP IDP IDE IDE IDE 24 18:26:03.586302 192.168.100.4 10.64.0.32 UDP <td>4 18:21:26.259175 192.168.100.4 10.64.0.32 UDP 384 25001 → 2030 Len=342</td> <td></td>	4 18:21:26.259175 192.168.100.4 10.64.0.32 UDP 384 25001 → 2030 Len=342							
6 18:21:36.652493 192.168.100.4 7 18:21:47.934663 192.168.100.4 8 18:22:22.957969 192.168.100.4 10.64.0.32 11 18:23:03.411742 192.168.100.4 10.64.0.32 11 18:23:03.9773 192.168.100.4 10.64.0.32 10 P 648 25001 + 2030 Len=903 11 18:23:03.9773 192.168.100.4 10.64.0.32 10 P 648 25001 + 2030 Len=903 12 168:23:23.539073 192.168.100.4 10.64.0.32 10 P 437 25001 + 2030 Len=993 15 18:23:23.539073 192.168.100.4 10.64.0.32 10 P 437 25001 + 2030 Len=993 15 18:25:28.663613 192.168.100.4 10.64.0.32 10 P 437 25001 + 2030 Len=993 10 18:25:38.907397 192.168.100.4 10.64.0.32 10 P 437 25001 + 2030 Len=993 10 18:25:38.90900 192.168.100.4 10.64.0.32 10 P 437 25001 + 2030 Len=993 10 18:4:38.007397 192.168.100.4 10.64.0.32 10 P 437 25001 + 2030 Len=993 10 18:25:38.90900 192.168.100.4 10.64.0.32 10 P 437 25001 + 2030 Len=993 10 18:25:38.9000 192.168.100.4 10 0:07:05 IP 4 27 18:26:33.226458 192.168.100.4 10.64.0.32 10 18:4000 00:05:9a:3c:7a:00 (00:05:9a:3c:7a:00), Dst: CIMSYS_33:44:55 (00:11:22:33:44:55) 1 Internet Protocol Version 4, Src: 192.168.100.4, Dst: 10.64.0.32 10 User Datagram Protocol, Src Port: 25001, Dst Port: 2030 2 Data (613 bytes) 2 Mode 00 11 22 33 44 55 00 05 9a 3c 7a 00 08 00 45 00 ····3DU···<2···E· 0000 00 11 22 33 44 55 00 05 9a 3c 7a 00 08 00 45 00 ····3DU··<2···E· 0000 00 11 22 33 44 55 00 05 9a 3c 7a 00 08 00 45 00 ····3DU··<2···E· 0000 00 21 122 33 44 55 00 05 9a 3c 7a 00	5 18:21:26.312552 192.168.100.4 10.64.0.32 UDP 1035 25001 → 2030 Len=993							
7 18:221:47.934603 192.168.100.4 10.64.0.32 UDP 1035 25001 + 2030 Len=993 11 18:22:22.975969 192.168.100.4 10.64.0.32 UDP 648 25001 + 2030 Len=395 14 18:23:08.507612 192.168.100.4 10.64.0.32 UDP 1035 25001 + 2030 Len=395 15 18:23:23.539073 192.168.100.4 10.64.0.32 UDP 1035 25001 + 2030 Len=395 16 18:24:28.117600 192.168.100.4 10.64.0.32 UDP 1035 25001 + 2030 Len=395 19 18:24:38.007397 192.168.100.4 10.64.0.32 UDP 1035 25001 + 2030 Len=393 20 18:25:28.663613 192.168.100.4 10.64.0.32 UDP IDP IDP ID35 25001 + 2030 Len=395 24 18:26:33.226458 192.168.100.4 10.64.0.32 UDP IDP IDP IDS Connect 4 to VPN headend for SNA. 27 18:26:33.226458 192.168.100.4 10.64.0.32 UDP IDP IDS 2001 + 2030 Len=395 10 10.64.0.32 UDP IDP IDS 2001 + 2030 Len=395 IDE IDE 27 18:26:33.226458 192.168.100.4 10.64.0	6 18:21:36.652493 192.168.100.4 10.64.0.32 UDP 989 25001 → 2030 Len=947							
8 18:22:22.27.975969 192.168.100.4 10.64.0.32 UDP 648 25901 + 2030 Len=696 11 18:23:03.411742 192.168.100.4 10.64.0.32 UDP 437 25901 + 2030 Len=993 14 18:23:03.557612 192.168.100.4 10.64.0.32 UDP 1035 25901 + 2030 Len=993 15 18:23:23.539073 192.168.100.4 10.64.0.32 UDP 1035 25901 + 2030 Len=993 19 18:24:28.067397 192.168.100.4 10.64.0.32 UDP 105 Cisco AnyConnect Secure Mobility Client — X 19 18:25:28.663613 192.168.100.4 10.64.0.32 UDP 10.64.0.32 UDP 20 18:25:28.69300 192.168.100.4 10.64.0.32 UDP 10.64.0.32 UDP 27 18:26:33.226458 192.168.100.4 10.64.0.32 UDP 10.64.0.32 UDP 10.64.0.32 UDP 10.64.0.32 UDP 10.64.0.32 UDP 27 18:26:33.226458 192.168.100.4 10.64.0.32 UDP 10.64.0.32 UDP 10.64.0.32 2 Frame 1: 655 bytes on wire (5240 bits), 655 bytes captured (5240 bits) on interface \Device\NPF_{3A925E5D-6F49-4710-8B90- Ethernet II, Src: Cisco_3c:7a:00 (00:05:9a:3c:7a:00), Dst: CIMSYS_33:44:55 (00:11:22:33:44:55) Internet Protocol Version 4, Src: 192.168.100.4, Dst: 10.64.0.32 2 User Datagram Protocol, Src Port: 25001, Dst Port: 2030 <td< td=""><td>7 18:21:47.934603 192.168.100.4 10.64.0.32 UDP 1035 25001 → 2030 Len=993</td><td></td></td<>	7 18:21:47.934603 192.168.100.4 10.64.0.32 UDP 1035 25001 → 2030 Len=993							
11 18:23:08.411/42 192.168.100.4 10.64.0.32 14 18:23:08.507612 192.168.100.4 10.64.0.32 15 18:23:23.539073 192.168.100.4 10.64.0.32 19 18:24:28.117600 192.168.100.4 10.64.0.32 19 18:24:38.007397 192.168.100.4 10.64.0.32 20 18:25:38.695000 192.168.100.4 10.64.0.32 21 18:25:38.695000 192.168.100.4 10.64.0.32 22 18:25:38.695000 192.168.100.4 10.64.0.32 24 18:26:33.226458 192.168.100.4 10.64.0.32 UDP UDP UDP UDP VPN: Connected to VPN headend for SNA. 27 18:26:33.226458 192.168.100.4 10.64.0.32 VDP UDP UDP VPN: 0:07:05 IPv4 Itheres IPv4 Ithes Ithes Ithes Ithes Ithes Ithes Ithes Ithes Ithes Ithes Ithes Ithes Ithes Ithes Ithes	8 18:22:22.975969 192.168.100.4 10.64.0.32 UDP 648 25001 → 2030 Len=606							
14 18:123:130:0.90*012 192.166.100.4 100.64.0.32 15 18:224:28.117600 192.168.100.4 100.64.0.32 19 18:24:28.117600 192.168.100.4 100.64.0.32 19 18:24:28.117600 192.168.100.4 100.64.0.32 19 18:25:28.665613 192.168.100.4 100.64.0.32 10 10.64.0.32 100.64.0.32 UDP 18:25:28.665613 192.168.100.4 100.64.0.32 UDP 18:26:33.226458 192.168.100.4 100.64.0.32 UDP 18:26:33.226458 192.168.100.4 100.64.0.32 UDP 10:64.0.32 UDP UDP VPN: Connected to VPN headend for SNA, 27 18:26:33.226458 192.168.100.4 100.64.0.32 UDP UDP VPN headend for SNA Disconnect 0:0:07:05 IPv4 Internet II, Src: Cisco_3c:7a:00 (00:05:9a:3c:7a:00), Dst: CIMSYS_33:44:55 (00:11:22:33:44:55) Internet Protocol Version 4, Src: 192.168.100.4, Dst: 10.64.0.32 Visor Datagram Protocol, Src Port: 25001, Dst Port: 2030 Data (613 bytes) St 00:01:22:33:44:55) St 00:01:22:33:44:55) Internet Protocol Version 4, S	11 18:23:03.411/42 192.168.100.4 10.64.0.32 UDP 437 25001 \rightarrow 2030 Len=395							
13 16:32:42:317600 192.168:100.4 10:64.0.32 UDP Cisco AnyConnect Secure Mobility Client — — X 19 18:24:28.117600 192.168.100.4 10:64.0.32 UDP UDP UDP UDP UDP Cisco AnyConnect Secure Mobility Client — X 20 18:25:28.663613 192.168.100.4 10:64.0.32 UDP UDP UDP Connected to VPN headend for SNA. 24 18:26:33.226458 192.168.100.4 10:64.0.32 UDP UDP UDP Connected to VPN headend for SNA. Disconnect 27 18:26:33.226458 192.168.100.4 10:64.0.32 UDP UDP UDP VPN headend for SNA Disconnect 00:07:05 IPv4 10:64.0.32 UDP UDP VPN headend for SNA Disconnect > Frame 1: 655 bytes on wire (5240 bits), 655 bytes captured (5240 bits) on interface \Device\NPF_{3A925E5D-6F49-4710-8B90- Ethernet II, Src: Cisco_3c:7a:00 (00:05:9a:3c:7a:00), Dst: CIMSYS_33:44:55 (00:11:22:33:44:55) Internet Protocol Version 4, Src: 192.168.100.4, Dst: 10:64.0.32 VER VER VER VER 0000 00 11 22 33 44 55 00 05 9a 3c 7a 00 08 00 45 00 ························	14 16:25:06.50/612 192.106.100.4 10.64.0.52 UDP 1055 25001 + 2050 Left=995							
10 10 12 13 12 16 10 10 64.0.32 UDP 10 13 12 16 10 64.0.32 UDP UDP </td <td>16 18:24:28,117600 192,168,100.4 10.64,0.32 UDP Cisco AnyConnect Secure Mobility Client</td> <td>- 🗆 X</td>	16 18:24:28,117600 192,168,100.4 10.64,0.32 UDP Cisco AnyConnect Secure Mobility Client	- 🗆 X						
20 18:25:28.663613 192.168.100.4 23 18:25:38.695000 192.168.100.4 24 18:26:03.586302 192.168.100.4 192.168.100.4 192.168.100.4 27 18:26:33.226458 192.168.100.4 192.168.100.4 192.168.100.4 192.168.100.4 192.168.100.4 192.168.100.4 192.168.100.4 192.168.100.4 192.168.100.4 192.168.100.4 192.168.100.4 192.168.100.4 192.168.100.4 192.168.100.4 192.168.100.4 192.168.100.4 192.168.100.4 192.168.100.4 192.168.100.4 192.168.100.4 192.168.100.4 18.655 bytes captured (5240 bits) on interface \Device\NPF_{3A925E5D-6F49-4710-8B90- 2 Ethernet II, Src: Cisco_3c:7a:00 (00:05:9a:3c:7a:00), Dst: CIMSYS_33:44:55 (00:11:22:33:44:55) 2 Internet Protocol Version 4, Src: 192.168.100.4, Dst: 10.64.0.32 2 User Datagram Protocol, Src Port: 25001, Dst Port: 2030 2 Data (613 bytes) 4 0000 00 11 22 33 44 55 00 05 9a 3c 7a 00 08 00 45 00 ···* 3DU··· <z···e·< td=""> 0010 02 81 8d 5f 00 00 80 11 7c 00 c0 a8 64 04 0a 40 ···* 3D</z···e·<>	19 18:24:38.007397 192.168.100.4 10.64.0.32 UDP							
23 18:25:38.695000 192.168.100.4 10.64.0.32 UDP Connected to VPN headend for SNA. 24 18:26:33.226458 192.168.100.4 10.64.0.32 UDP UDP VPN headend for SNA. Disconnect 27 18:26:33.226458 192.168.100.4 10.64.0.32 UDP UDP VPN headend for SNA. Disconnect > 64.0.32 10.64.0.32 UDP VDP VPN headend for SNA. Disconnect > 0:07:05 IPv4 IPv4 IPv4 IPv4 IPv4 IPv4 > Image: State of the st	20 18:25:28.663613 192.168.100.4 10.64.0.32 UDP							
24 18:26:03.586302 192.168.100.4 10.64.0.32 UDP UDP UDP UDP UDP UDP 0:07:05 IPv4 > Frame 1: 655 bytes on wire (5240 bits), 655 bytes captured (5240 bits) on interface \Device\NPF_{3A925E5D-6F49-4710-8B90- 2 10.64.0.32 0:07:05 IPv4 > Image: Click on the second of t	23 18:25:38.695000 192.168.100.4 10.64.0.32 UDP Connected to VPN headend for S	NA.						
27 18:26:33.226458 192.168.100.4 10.64.0.32 UDP VPN headend for SNA ✓ Disconnect 00:07:05 IPv4 ◇ i	24 18:26:03.586302 192.168.100.4 10.64.0.32 UDP							
00:07:05 IPv4 ▷ ○ ○ > Frame 1: 655 bytes on wire (5240 bits), 655 bytes captured (5240 bits) on interface \Device\NPF_{3A925E5D-6F49-4710-8B90- > Ethernet II, Src: Cisco_3c:7a:00 (00:05:9a:3c:7a:00), Dst: CIMSYS_33:44:55 (00:11:22:33:44:55) > Internet Protocol Version 4, Src: 192.168.100.4, Dst: 10.64.0.32 > User Datagram Protocol, Src Port: 25001, Dst Port: 2030 > Data (613 bytes) 0000 00 11 22 33 44 55 00 05 9a 3c 7a 00 08 00 45 00 ···*3DU···<	27 18:26:33.226458 192.168.100.4 10.64.0.32 UDP VPN headend for SNA	 Disconnect 						
00:07:05 IPV4 ▷ :: :: ▷ :: :: ▷ :: :: ▷ :: :: ○ :: :: :: :: :: :: :: :: :: :: :: :: :: :: :: ::		TD (
↓ (i)	00:07:05	IPv4						
<pre></pre>	ひ	alah						
<pre>> Hrame 1: 055 bytes on where (5240 bits), 055 bytes captared (5240 bits) on interface (bevice (wr(5852550-0145-4710-0550- > Ethernet II, Src: Cisco_3c:7a:00 (00:05:9a:3c:7a:00), Dst: CIMSYS_33:44:55 (00:11:22:33:44:55) > Internet Protocol Version 4, Src: 192.168.100.4, Dst: 10.64.0.32 > User Datagram Protocol, Src Port: 25001, Dst Port: 2030 > Data (613 bytes)</pre>	Ename 1: 655 bytes on wire (5240 bits) 655 bytes cantured (5240 bits) on interface \Device\NPE /34	CISCO						
<pre>> Internet Protocol Version 4, Src: 192.168.100.4, Dst: 10.64.0.32 > User Datagram Protocol, Src Port: 25001, Dst Port: 2030 > Data (613 bytes) </pre>	Ethernet II. Src: (isco 3c:7a:00 (00:05:9a:3c:7a:00), Dst: (INSYS 33:44:55 (00:11:22:33:44:55))	22220-0149-4/10-0090-						
> User Datagram Protocol, Src Port: 25001, Dst Port: 2030 > Data (613 bytes) <	Thernet Protocol Version 4. Src: 192 168 100 4. Dst: 10 64 0 32							
<pre>> Data (613 bytes) </pre>	> User Datagram Protocol, Src Port: 25001, Dst Port: 2030							
> 0000 00 11 22 33 44 55 00 05 9a 3c 7a 00 08 00 45 00 ···"3DU·· · <z··e·< td=""> ∧ 0010 02 81 8d 5f 00 00 80 11 7c 00 c0 a8 64 04 0a 40 ···· ··· ··· ··· ··· ···· ···</z··e·<>	> Data (613 bytes)							
> 0000 00 11 22 33 44 55 00 05 9a 3c 7a 00 08 00 45 00 ···"3DU·· · <z···e·< td=""> 0010 02 81 8d 5f 00 00 80 11 7c 00 c0 a8 64 04 0a 40 ···· ··· ··· ···· ···· ····· ······ ····</z···e·<>								
0000 00 11 22 33 44 55 00 05 9a 3c 7a 00 08 00 45 00 ···"3DU··· <z··e·< td=""> ^ 0010 02 81 8d 5f 00 00 80 11 7c 00 c0 a8 64 04 0a 40 ···· ····d··@ V</z··e·<>								
0000 00 11 22 33 44 55 00 05 9a 3c 7a 00 08 00 45 00 ···"3DU··· <z···e·< td=""> 0010 02 81 8d 5f 00 00 80 11 7c 00 c0 a8 64 04 0a 40 ····· ····d··@</z···e·<>		>						
	0000 00 11 22 33 44 55 00 05 9a 3c 7a 00 08 00 45 00 ····3DU··· <z···e·< td=""></z···e·<>							
wireshark Ethernet 3821/JB1 propp	2 01 00 01 00 00 00 11 /C 00 C0 d0 04 04 04 40 ····· 0··0·0 Darkate: 27 · Dieplayad: 15/55 6	%) Profile: Default						

c. Si le point de terminaison n'est pas sur un réseau de confiance, les flux ne sont pas envoyés au collecteur de flux.

	*Ethernet0				– 🗆 X			
File	Edit View Go	o Capture Analyze	e Statistics Telephony Wirele	ess Tools Help				
	d 💿 📘	- X G 9 🗢	🗢 🕾 🗿 🛓 📃 🔳 🔍 G					
📕 ip	ip.addr == 10.64.0.32							
No.	Time	Source	Destination	Protocol Length Info				
				S Cisco AnyConnect Secure Mobility Client	- L X			
				Ready to connect.				
				VPN headend for SNA	✓ Connect			
					abab			
				₩ ♥	cisco			
<					>			

Défauts associés

Il existe actuellement deux défauts connus qui peuvent affecter le processus d'entrée de données de télémétrie NVM sur Secure Network Analytics :

- Le moteur FC ne peut pas ingérer la télémétrie NVM sur eth1. Voir ID de bogue Cisco
 <u>CSCwb84013</u>
- Collecteur de flux n'insérant pas d'enregistrements NVM à partir de AnyConnect version 4.10.04071 ou ultérieure. Voir ID de bogue Cisco <u>CSCwb91824</u>

Informations connexes

- Pour obtenir de l'aide supplémentaire, veuillez contacter le Centre d'assistance technique (TAC). Un contrat d'assistance valide est requis : <u>Coordonnées du service d'assistance Cisco</u> <u>à l'échelle mondiale.</u>
- Vous pouvez également visiter la communauté Cisco Security Analytics ici.
- <u>Support et documentation techniques Cisco Systems</u>