Dépannage de l'interrogation SNMP et des détails d'interface incorrects sur SNA

Table des matières

- Introduction
- Conditions préalables
- Exigences
- Composants utilisés
- Configurations
- Informations générales
- Dépannage
  - Noms d'interface incorrects
  - Exportateurs ou interfaces manquants
  - Problèmes de connectivité
    - Valider la capacité du gestionnaire (SMC) à interroger les exportateurs
    - Générez une capture de paquets sur le SMC à l'aide de l'adresse IP d'un exportateur.
    - Valider les paramètres d'interrogation SNMP
    - Dépannage en direct de l'interrogation SNMP
  - Test de l'interrogation SNMP depuis un autre périphérique
- Informations connexes

Introduction

Ce document décrit comment dépanner les informations d'interface d'exportateur manquantes dans Secure Network Analytics

Conditions préalables

- Cisco vous recommande d'avoir des connaissances de base en matière d'interrogation SNMP (Simple Network Management Protocol).
- Cisco vous recommande d'avoir des connaissances de base en analyse de réseau sécurisé (SNA/StealthWatch)

Exigences

- SNA Manager version 7.4.1 ou ultérieure
- Collecteur de flux SNA version 7.4.1 ou ultérieure
- Exportateur envoyant activement NetFlow à SNA

Composants utilisés

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

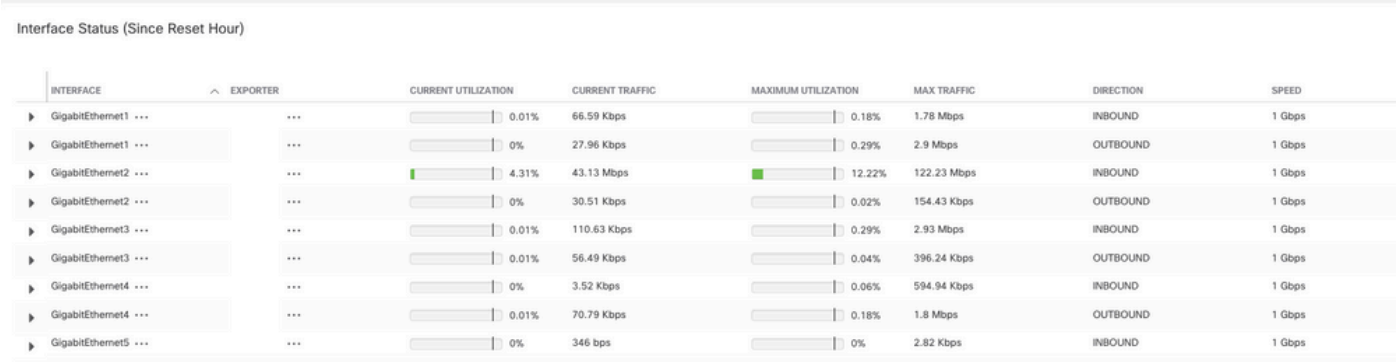
- SNA Manager version 7.4.1 ou ultérieure
- Collecteur de flux SNA version 7.4.1 ou ultérieure
- Logiciel SNMPwalk
- logiciel Wireshark

Configurations

- Device Configuration : les exportateurs doivent être configurés pour autoriser l'accès SNMP. Cela implique la configuration des paramètres SNMP sur chaque périphérique, y compris la configuration des chaînes de communauté SNMP, des listes de contrôle d'accès (ACL) et la définition de la version SNMP à utiliser
- Configuration de l'interrogation SNMP sur SNA : une fois les exportateurs correctement configurés, l'interrogation SNMP est activée par défaut sur le SMC à l'aide de paramètres prédéfinis. Il est essentiel de fournir les détails requis relatifs aux exportateurs, tels que les chaînes de communauté SNMP et les versions SNMP, pour garantir le fonctionnement optimal du mécanisme d'interrogation

Informations générales

SNA permet de fournir des rapports d'état complets sur les interfaces, ainsi que d'afficher les noms des interfaces pour les exportateurs qui transmettent activement des données NetFlow à un collecteur de flux. Vous pouvez afficher les détails de cette interface en accédant au menu Rechercher -> Interfaces à partir de l'interface utilisateur Web du gestionnaire.

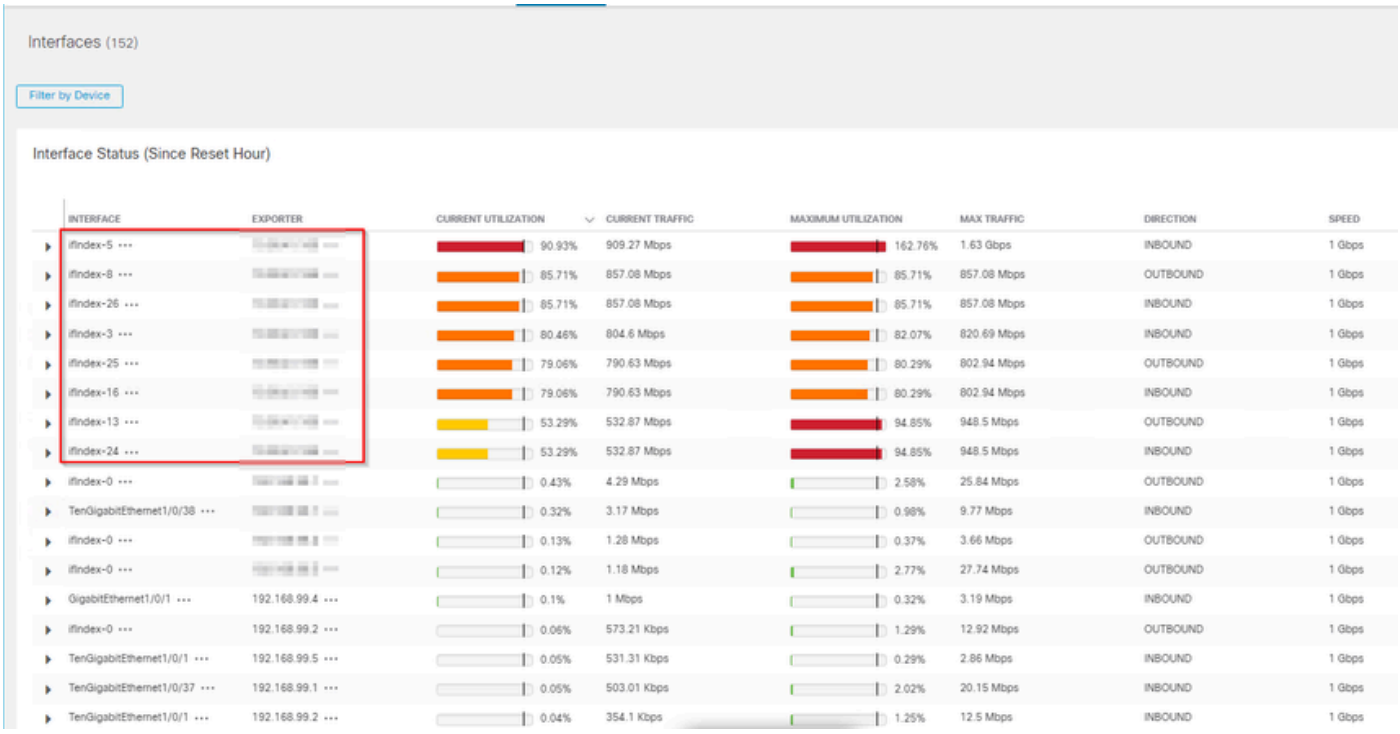

Interface Status (Since Reset Hour)

INTERFACE	EXPORTER	CURRENT UTILIZATION	CURRENT TRAFFIC	MAXIMUM UTILIZATION	MAX TRAFFIC	DIRECTION	SPEED
GigabitEthernet1		0.01%	66.59 Kbps	0.18%	1.78 Mbps	INBOUND	1 Gbps
GigabitEthernet1		0%	27.96 Kbps	0.29%	2.9 Mbps	OUTBOUND	1 Gbps
GigabitEthernet2		4.31%	43.13 Mbps	12.22%	122.23 Mbps	INBOUND	1 Gbps
GigabitEthernet2		0%	30.51 Kbps	0.02%	154.43 Kbps	OUTBOUND	1 Gbps
GigabitEthernet3		0.01%	110.63 Kbps	0.29%	2.93 Mbps	INBOUND	1 Gbps
GigabitEthernet3		0.01%	56.49 Kbps	0.04%	396.24 Kbps	OUTBOUND	1 Gbps
GigabitEthernet4		0%	3.52 Kbps	0.06%	594.94 Kbps	INBOUND	1 Gbps
GigabitEthernet4		0.01%	70.79 Kbps	0.18%	1.8 Mbps	OUTBOUND	1 Gbps
GigabitEthernet5		0%	346 bps	0%	2.82 Kbps	INBOUND	1 Gbps

Dépannage

Noms d'interface incorrects

Si le rapport généré affiche un « ifindex-# » qui ne correspond pas à vos interfaces d'exportateur, il suggère un problème de configuration potentiel avec l'interrogation SNMP sur le SMC ou sur l'exportateur lui-même. Dans cet exemple, j'ai mis en évidence un problème apparent avec l'interrogation SNMP d'un exportateur donné.



Exportateurs ou interfaces manquants

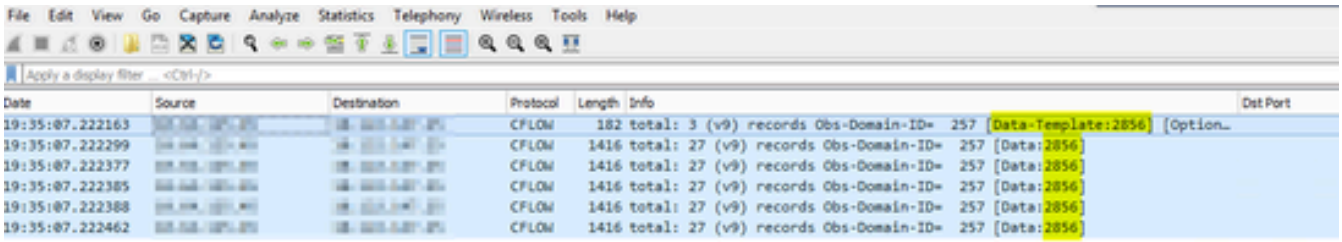
La vérification des modèles revêt une importance significative dans le contexte du traitement des données NetFlow. Plus précisément, il garantit que le modèle NetFlow reçu de l'exportateur contient tous les champs requis pour un décodage et un traitement réussis par le collecteur de flux. L'absence d'un modèle valide conduit à l'exclusion du décodage de l'ensemble de flux associé, d'où leur absence de la liste des interfaces.

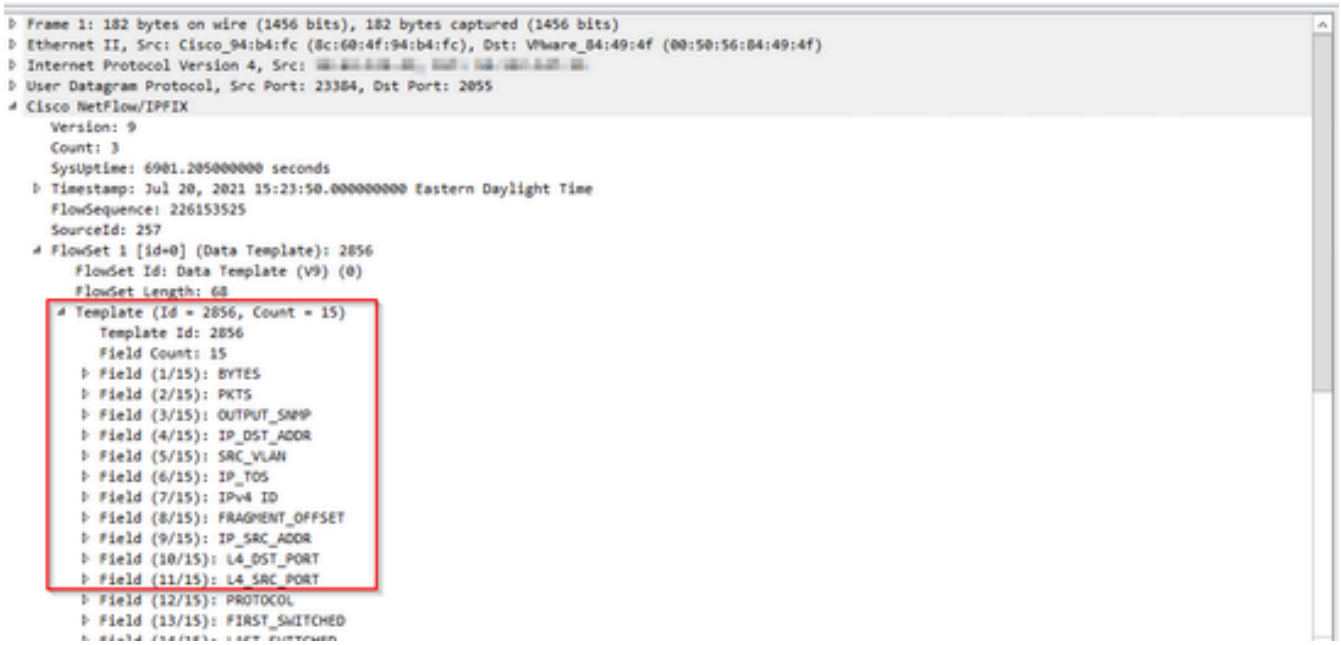
Si vous ne voyez pas l'exportateur/les interfaces attendu(e)s dans la liste des interfaces, vous devez vérifier le modèle dn de données netflow entrant. Afin de vérifier le modèle NetFlow, une capture de paquets peut être créée du côté du collecteur de flux, spécifiant l'IP de l'exportateur dont nous obtenons NetFlow en changeant "x.x.x.x" :

- Connectez-vous au collecteur de flux via SSH ou la console avec les informations d'identification racine.
- Exécutez une capture de paquets à partir de l'adresse IP de l'exportateur et du port netflow en question :

```
tcpdump -s0 -v -nnn -i eth0 host x.x.x.x and port 2055 -w /lancope/var/admin/tmp/<name>.pcap
```

- Copiez la capture de paquets de l'appliance vers une station de travail où l'application Wireshark est installée. Utilisez la méthode de votre choix (par exemple : SCP, SFTP).
- Ouvrez la capture de paquets avec Wireshark et vérifiez le modèle et les données que l'exportateur envoie au collecteur de flux





Vérifiez que le modèle NetFlow utilise les 9 champs obligatoires. Le nom exact de ces champs de modèle peut varier selon le type d'exportateur. Veillez donc à consulter la documentation du type d'exportateur que vous configurez :

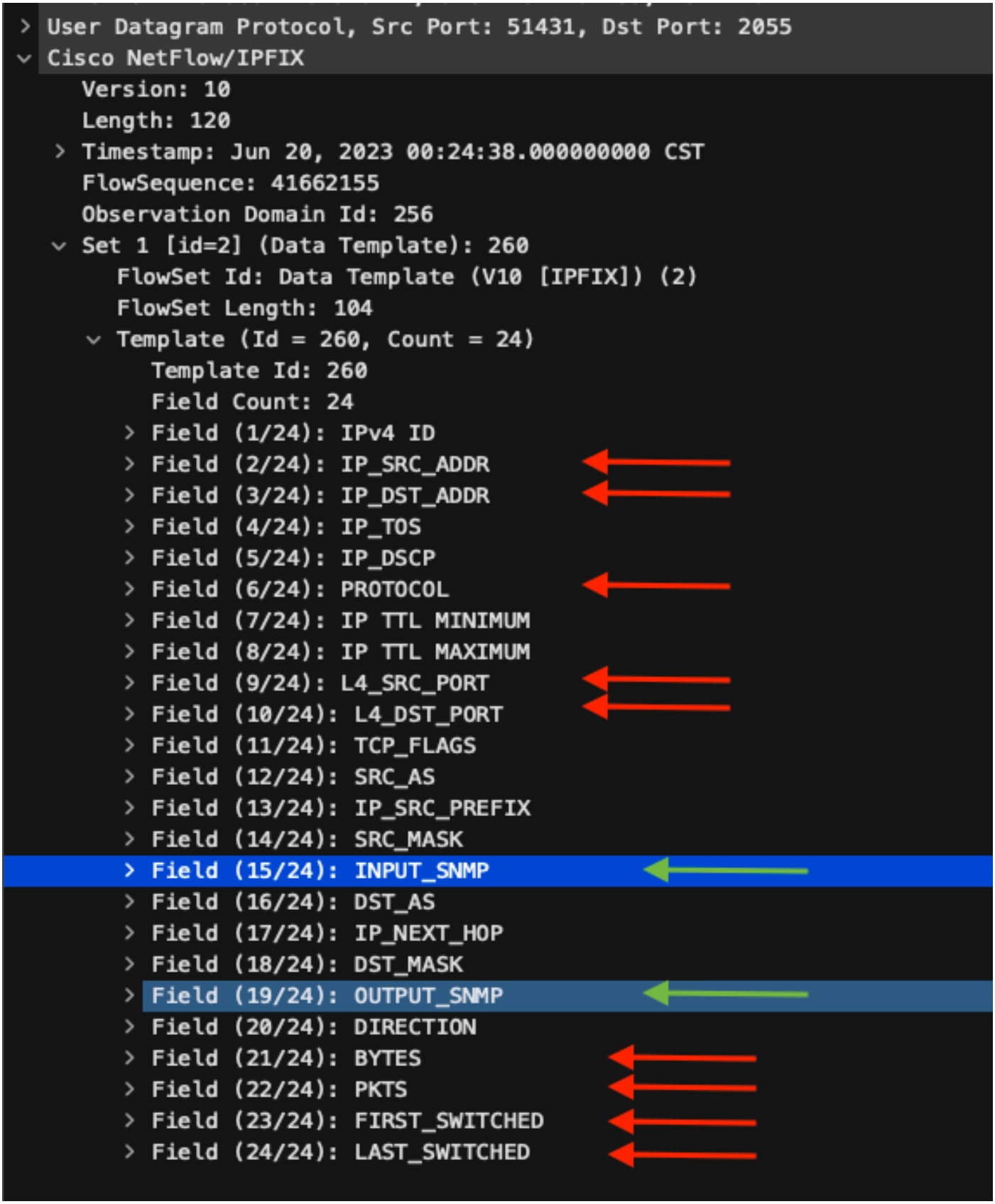
- adresse IP source
- adresse IP de destination
- Port source
- Port de destination
- Protocole de couche 4
- Nombre d'octets
- Nombre de paquets
- Heure de début du flux
- Heure de fin du flux

Pour afficher correctement les interfaces, veuillez également ajouter :

  - sortie d'interface
  - entrée d'interface

Voici un exemple de modèle de capture de paquets à partir d'un périphérique exportateur donné

- Flèches rouges : champs NetFlow obligatoires
- Flèches vertes : champs SNMP



Remarque : le port répertorié dans l'exemple de commande peut varier selon la configuration de votre exportateur. La valeur par défaut est 2055

Remarque : gardez la capture de paquets en cours d'exécution de 5-10 minutes, selon l'exportateur le modèle peut être envoyé toutes les N minutes et vous devez attraper ce modèle afin que le NetFlow soit décodé correctement, si le modèle ne s'affiche pas, répétez la capture de paquets pendant une période plus longue

Problèmes de connectivité

Check Connectivity : vérifiez la connectivité entre l'appliance SNA Manager et les exportateurs. Vérifiez que les exportateurs sont accessibles depuis la console de gestion StealthWatch en envoyant une requête ping à leurs adresses IP. Si vous rencontrez des problèmes de connectivité réseau, résolvez-les en conséquence.

Valider la capacité du gestionnaire (SMC) à interroger les exportateurs

- Connectez-vous au gestionnaire SNA vis SSH et connectez-vous avec les informations d'identification racine
- Analysez le fichier /lancope/var/smc/log/smc-configuration.log et recherchez les journaux de type ExporterSnmpSession :

```
INFO [ExporterSnmpSession] SNMP polling for 10.1.0.253 took 0s
INFO [ExporterSnmpSession] SNMP polling for 10.1.0.253 took 0s
WARN [ExporterSnmpSession] SNMP polling for 10.10.0.254 failed: java.lang.Exception: timeout
INFO [ExporterSnmpSession] SNMP polling for 10.10.0.254 took 20s
WARN [ExporterSnmpSession] SNMP polling for 10.10.0.254 failed: java.lang.Exception: timeout
INFO [ExporterSnmpSession] SNMP polling for 10.10.0.254 took 20s
```

- Dans cet exemple de sondage, aucune erreur n'a été détectée pour l'exportateur 10.1.0.253. Cependant, l'exportateur 10.1.0.254 a connu un délai d'attente. Le délai d'attente par défaut est de 5 000 ms avec un nombre de tentatives égal à 3. Ainsi, du moment où un exportateur est interrogé au moment où il a dépassé le délai d'attente, il devrait y avoir 20 secondes dans un environnement où vous n'avez pas modifié les paramètres.

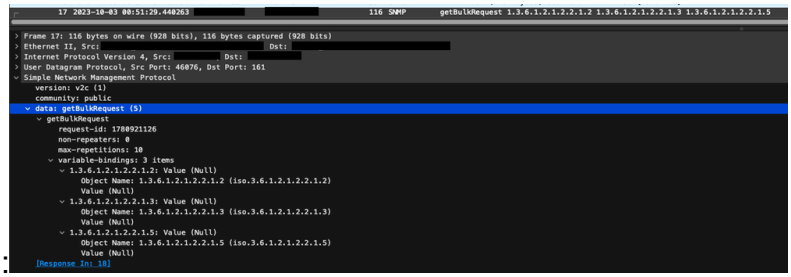
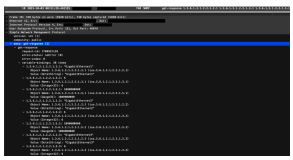
Générez une capture de paquets sur le SMC à l'aide de l'adresse IP d'un exportateur.

- Connectez-vous au noeud Manager via SSH ou la console avec les informations d'identification racine
- Exécutez la commande :

```
tcpdump -s0 -v -nnn -i [Interface] host [Exporter_IP_address] -w /lancope/var/admin/tmp/[file_name
```

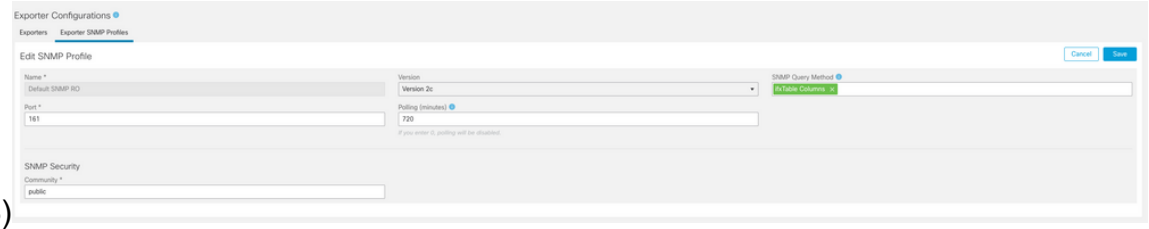
- Exportez la capture de paquets à partir de l'appliance avec la méthode de votre choix (exemple : SCP, SFTP)
- Ouvrez la capture de paquets avec Wireshark pour afficher les tentatives d'interrogation

réussies

- Demande faite auprès du SMC : 
- Réponse SNMP de l'exportateur avec les informations d'interface : 

Valider les paramètres d'interrogation SNMP

Assurez-vous que les intervalles d'interrogation sont appropriés et que les métriques souhaitées sont incluses dans les requêtes SNMP

- Sur l'interface utilisateur Web, accédez à : Configure -> Exporters -> Exporter SNMP Profiles:
- Vérifiez que le port SNMP correct (généralement le port UDP 161) et la méthode de requête SNMP sélectionnée correspondent à votre exportateur (ifxTable Columns, CatOS MIB, PanOS MIB) 

Remarque : si vous disposez d'interfaces 10 Gbit/s, nous vous recommandons de choisir l'option de colonnes ifxTable pour la méthode de requête SNMP.

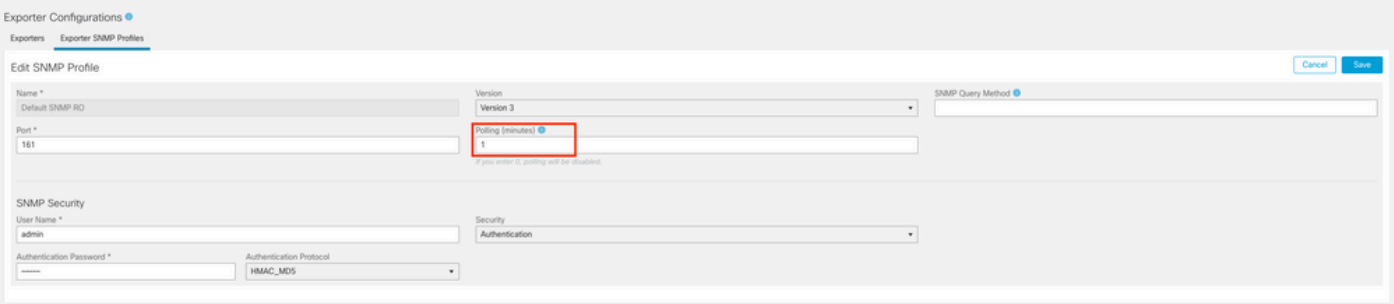
Remarque : pour optimiser les performances du système, définissez l'interrogation SNMP sur un intervalle de 12 heures. Une interrogation plus fréquente ne met pas à jour vos mesures d'utilisation et peut ralentir le fonctionnement de votre système.

- Vérifiez que les versions SNMP configurées sur SNA et sur les exportateurs sont compatibles. SNA prend en charge SNMPv1, SNMPv2c et SNMPv3. Vérifiez si les exportateurs sont configurés pour utiliser la même version SNMP que celle configurée dans SNA.
  - Si vous utilisez SNMPv3, vérifiez que la configuration SNMP est correcte (Nom d'utilisateur, Mot de passe d'authentification, Protocole d'authentification, Mot de passe de confidentialité, Protocole de confidentialité)

Dépannage en direct de l'interrogation SNMP

Sur l'interface utilisateur Web, naviguez jusqu'à Configure -> Exporters -> Exporter SNMP Profiles

- Définissez temporairement l'interrogation (minutes) sur 1 (minutes).



- Connectez-vous au SMC via SSH ou la console avec les informations d'identification racine.
- Accédez à ce dossier :

```
cd /lancope/var/smc/log
```

- Exécutez la commande :

```
tail -f smc-configuration.log
```

- Pour SNMPv3, un message d'erreur courant serait :

```
failed: java.lang.IllegalArgumentException: USM passphrases must be at least 8 bytes long (RFC3414
```

- Vérifiez que le mot de passe d'authentification dans le profil SNMP est défini sur 8 caractères ou plus.
- Une fois le dépannage en direct terminé, rétablissez la valeur précédente de la configuration d'interrogation (minutes) de l'exportateur ou de son modèle de configuration.

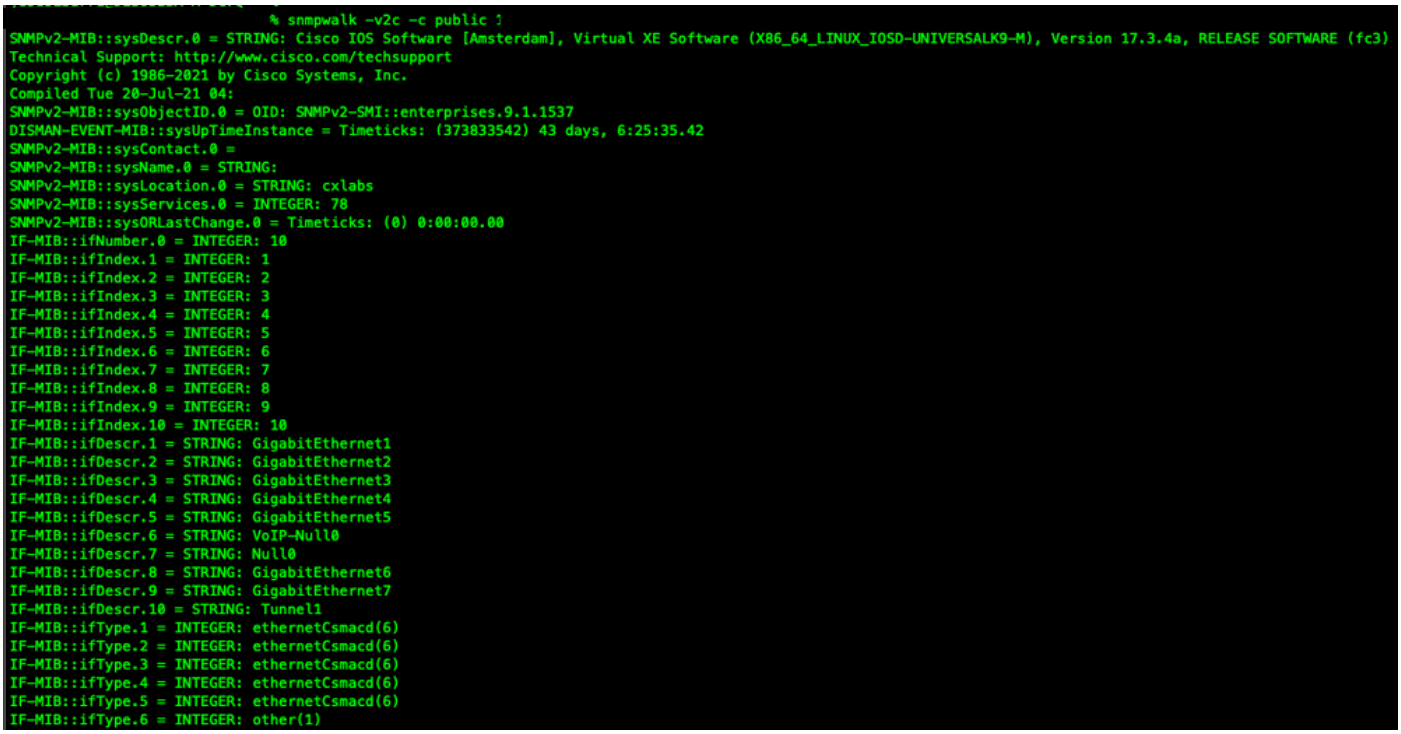
Test de l'interrogation SNMP depuis un autre périphérique

Test SNMP Polling : lancez manuellement une interrogation SNMP à partir d'une machine locale vers un périphérique réseau spécifique et vérifiez qu'il reçoit une réponse. Pour ce faire, vous pouvez utiliser des outils d'interrogation SNMP ou des utilitaires tels que SNMPwalk. Vérifiez que le périphérique réseau répond avec les données SNMP demandées. En l'absence de réponse, cela indique un problème de configuration ou de connectivité SNMP.

- Sur votre machine locale avec le logiciel SNMPwalk, remplacez « x.x.x.x » pour l'adresse IP de l'exportateur et exécutez sur l'interface de ligne de commande :

```
snmpwalk -v2c -c public x.x.x.x
```

  - -v2c : spécifie la version SNMP à utiliser
  - -c : définit la chaîne community



- Vérifiez que l'exportateur répond avec les données SNMP

Informations connexes

- Pour obtenir de l'aide supplémentaire, veuillez contacter le Centre d'assistance technique (TAC). Un contrat d'assistance valide est requis : Cisco Worldwide Support Contacts.
- Vous pouvez également visiter la communauté Cisco Security Analytics ici.
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.