

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.

Interfaces (152)

Filter by Device

Interface Status (Since Reset Hour)

INTERFACE	EXPORTER	CURRENT UTILIZATION	CURRENT TRAFFIC	MAXIMUM UTILIZATION	MAX TRAFFIC	DIRECTION	SPEED
ifindex-5	90.93%	909.27 Mbps	162.76%	1.63 Gbps	INBOUND	1 Gbps
ifindex-8	85.71%	857.08 Mbps	85.71%	857.08 Mbps	OUTBOUND	1 Gbps
ifindex-26	85.71%	857.08 Mbps	85.71%	857.08 Mbps	INBOUND	1 Gbps
ifindex-3	80.46%	804.6 Mbps	82.07%	820.69 Mbps	INBOUND	1 Gbps
ifindex-25	79.06%	790.63 Mbps	80.29%	802.94 Mbps	OUTBOUND	1 Gbps
ifindex-16	79.06%	790.63 Mbps	80.29%	802.94 Mbps	INBOUND	1 Gbps
ifindex-13	53.29%	532.87 Mbps	94.85%	948.5 Mbps	OUTBOUND	1 Gbps
ifindex-24	53.29%	532.87 Mbps	94.85%	948.5 Mbps	INBOUND	1 Gbps
ifindex-0	4.43%	4.29 Mbps	2.58%	25.84 Mbps	OUTBOUND	1 Gbps
TenGigabitEthernet1/0/38	0.32%	3.17 Mbps	0.98%	9.77 Mbps	INBOUND	1 Gbps
ifindex-0	0.13%	1.28 Mbps	0.37%	3.66 Mbps	OUTBOUND	1 Gbps
ifindex-0	0.12%	1.18 Mbps	2.77%	27.74 Mbps	OUTBOUND	1 Gbps
GigabitEthernet1/0/1 ...	192.168.99.4 ...	0.1%	1 Mbps	0.32%	3.19 Mbps	INBOUND	1 Gbps
ifindex-0 ...	192.168.99.2 ...	0.06%	573.21 Kbps	1.29%	12.92 Mbps	OUTBOUND	1 Gbps
TenGigabitEthernet1/0/1 ...	192.168.99.5 ...	0.05%	531.31 Kbps	0.29%	2.86 Mbps	INBOUND	1 Gbps
TenGigabitEthernet1/0/37 ...	192.168.99.1 ...	0.05%	503.01 Kbps	2.02%	20.15 Mbps	INBOUND	1 Gbps
TenGigabitEthernet1/0/1 ...	192.168.99.2 ...	0.04%	354.1 Kbps	1.25%	12.5 Mbps	INBOUND	1 Gbps

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/
```

.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

Date	Source	Destination	Protocol	Length	Info	Dest Port
19:35:07.222163	10.10.10.10	10.10.10.10	CFLOW	1416	total: 3 (v9) records Obs-Domain-ID= 257 [Data:2856]	
19:35:07.222299	10.10.10.10	10.10.10.10	CFLOW	1416	total: 27 (v9) records Obs-Domain-ID= 257 [Data:2856]	
19:35:07.222377	10.10.10.10	10.10.10.10	CFLOW	1416	total: 27 (v9) records Obs-Domain-ID= 257 [Data:2856]	
19:35:07.222385	10.10.10.10	10.10.10.10	CFLOW	1416	total: 27 (v9) records Obs-Domain-ID= 257 [Data:2856]	
19:35:07.222388	10.10.10.10	10.10.10.10	CFLOW	1416	total: 27 (v9) records Obs-Domain-ID= 257 [Data:2856]	
19:35:07.222462	10.10.10.10	10.10.10.10	CFLOW	1416	total: 27 (v9) records Obs-Domain-ID= 257 [Data:2856]	

```
Frame 1: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits) on interface 0
Ethernet II, Src: Cisco_94:b4:fc (8c:60:4f:94:b4:fc), Dst: VMware_84:49:4f (00:50:56:84:49:4f)
Internet Protocol Version 4, Src: 10.10.10.10, Dst: 10.10.10.10
User Datagram Protocol, Src Port: 23384, Dst Port: 2055
Cisco NetFlow/IPFIX
  Version: 9
  Count: 3
  SysUptime: 6981.285000000 seconds
  Timestamp: Jul 20, 2021 15:23:50.000000000 Eastern Daylight Time
  FlowSequence: 226153525
  SourceId: 257
  FlowSet 1 [id=0] (Data Template): 2856
    FlowSet Id: Data Template (V9) (0)
    FlowSet Length: 68
    Template (Id = 2856, Count = 15)
      Template Id: 2856
      Field Count: 15
      Field (1/15): BYTES
      Field (2/15): PKTS
      Field (3/15): OUTPUT_SNMP
      Field (4/15): IP_DST_ADDR
      Field (5/15): SRC_VLAN
      Field (6/15): IP_TOS
      Field (7/15): IPv4 ID
      Field (8/15): FRAGMENT_OFFSET
      Field (9/15): IP_SRC_ADDR
      Field (10/15): L4_DST_PORT
      Field (11/15): L4_SRC_PORT
      Field (12/15): PROTOCOL
      Field (13/15): FIRST_SWITCHED
      Field (14/15): LAST_SWITCHED
```

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

```
> User Datagram Protocol, Src Port: 51431, Dst Port: 2055
v Cisco NetFlow/IPFIX
  Version: 10
  Length: 120
  > Timestamp: Jun 20, 2023 00:24:38.000000000 CST
  FlowSequence: 41662155
  Observation Domain Id: 256
  v Set 1 [id=2] (Data Template): 260
    FlowSet Id: Data Template (V10 [IPFIX]) (2)
    FlowSet Length: 104
    v Template (Id = 260, Count = 24)
      Template Id: 260
      Field Count: 24
      > Field (1/24): IPv4 ID
      > Field (2/24): IP_SRC_ADDR ←
      > Field (3/24): IP_DST_ADDR ←
      > Field (4/24): IP_TOS
      > Field (5/24): IP_DSCP
      > Field (6/24): PROTOCOL ←
      > Field (7/24): IP TTL MINIMUM
      > Field (8/24): IP TTL MAXIMUM
      > Field (9/24): L4_SRC_PORT ←
      > Field (10/24): L4_DST_PORT ←
      > Field (11/24): TCP_FLAGS
      > Field (12/24): SRC_AS
      > Field (13/24): IP_SRC_PREFIX
      > Field (14/24): SRC_MASK
      > Field (15/24): INPUT_SNMP ←
      > Field (16/24): DST_AS
      > Field (17/24): IP_NEXT_HOP
      > Field (18/24): DST_MASK
      > Field (19/24): OUTPUT_SNMP ←
      > Field (20/24): DIRECTION
      > Field (21/24): BYTES ←
      > Field (22/24): PKTS ←
      > Field (23/24): FIRST_SWITCHED ←
      > Field (24/24): LAST_SWITCHED ←
```

 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 initialement rencontré un message d'erreur de délai d'attente, mais a réussi à effectuer l'opération d'interrogation après un délai de 20 secondes.

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]
```

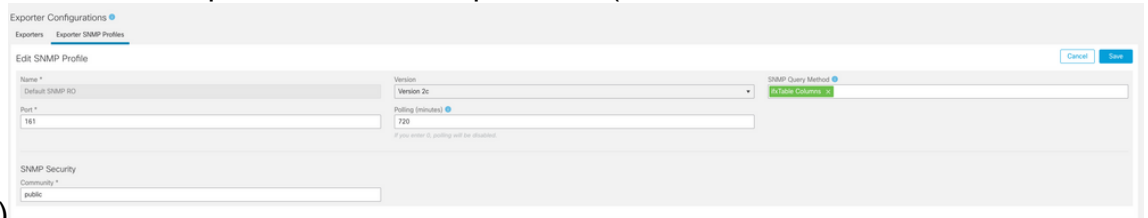
- Exportez la capture de paquets à partir de l'appliance avec la méthode de votre choix (exemple : SCP, SFTP)
- Ouvrez la capture de paquets avec Wireshark pour afficher les tentatives d'interrogation réussies
 - Demande faite auprès du SMC :

- 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 : Configurer -> Exporter -> 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.

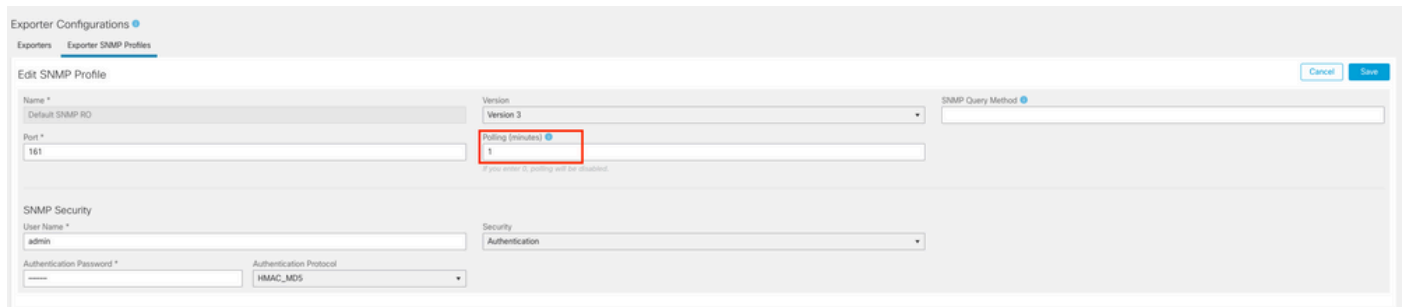
Remarque : pour optimiser les performances du système, définissez l'interrogation SNMP sur un intervalle de 12 heures. Une interrogation plus fréquente ne met pas à jour vos mesures d'utilisation et peut ralentir le fonctionnement de votre système.

- 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 Configurer -> Exporter -> Exporter SNMP Profiles

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



The screenshot shows the 'Export SNMP Profiles' configuration page. The 'Polling (minutes)' field is highlighted with a red box and contains the value '1'. Other fields include 'Name', 'Default SNMP ID', 'Port', 'SNMP Security', 'User Name', 'Authentication Password', and 'Authentication Protocol'.

- 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

```
% snmpwalk -v2c -c public 1
SNMPv2-MIB::sysDescr.0 = STRING: Cisco IOS Software [Amsterdam], Virtual XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 17.3.4a, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2021 by Cisco Systems, Inc.
Compiled Tue 20-Jul-21 04:
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.1537
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (373833542) 43 days, 6:25:35.42
SNMPv2-MIB::sysContact.0 =
SNMPv2-MIB::sysName.0 = STRING:
SNMPv2-MIB::sysLocation.0 = STRING: cxlabs
SNMPv2-MIB::sysServices.0 = INTEGER: 78
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00
IF-MIB::ifNumber.0 = INTEGER: 10
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.2 = INTEGER: 2
IF-MIB::ifIndex.3 = INTEGER: 3
IF-MIB::ifIndex.4 = INTEGER: 4
IF-MIB::ifIndex.5 = INTEGER: 5
IF-MIB::ifIndex.6 = INTEGER: 6
IF-MIB::ifIndex.7 = INTEGER: 7
IF-MIB::ifIndex.8 = INTEGER: 8
IF-MIB::ifIndex.9 = INTEGER: 9
IF-MIB::ifIndex.10 = INTEGER: 10
IF-MIB::ifDescr.1 = STRING: GigabitEthernet1
IF-MIB::ifDescr.2 = STRING: GigabitEthernet2
IF-MIB::ifDescr.3 = STRING: GigabitEthernet3
IF-MIB::ifDescr.4 = STRING: GigabitEthernet4
IF-MIB::ifDescr.5 = STRING: GigabitEthernet5
IF-MIB::ifDescr.6 = STRING: VoIP-Null0
IF-MIB::ifDescr.7 = STRING: Null0
IF-MIB::ifDescr.8 = STRING: GigabitEthernet6
IF-MIB::ifDescr.9 = STRING: GigabitEthernet7
IF-MIB::ifDescr.10 = STRING: Tunnel1
IF-MIB::ifType.1 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.2 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.3 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.4 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.5 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.6 = INTEGER: other(1)
```

- 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 : [Coordonnées du service d'assistance Cisco à l'échelle mondiale](#).
- 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.