Risoluzione dei problemi di polling SNMP e dettagli di interfaccia errati sulla SNA

Sommario

- Introduzione
- Prerequisiti
- Requisiti
- Componenti usati
- Configurazioni
- Premesse
- Risoluzione dei problemi
  - Nomi di interfaccia non corretti
  - Esportatori o interfacce mancanti
  - Problemi di connettività
    - Convalida la capacità del manager (SMC) di eseguire il polling degli esportatori
    - Generare un'acquisizione di pacchetti sull'SMC utilizzando l'indirizzo IP di un esportatore.
    - Convalida impostazioni di polling SNMP
    - Risoluzione dei problemi in tempo reale del polling SNMP
  - Test del polling SNMP da un altro dispositivo
- Informazioni correlate

Introduzione

Questo documento descrive come risolvere i problemi relativi alle informazioni mancanti sull'interfaccia dell'esportatore in Secure Network Analytics

Prerequisiti

- Cisco consiglia di avere una conoscenza base del polling SNMP (Simple Network Management Protocol).
- Cisco consiglia di possedere le conoscenze base di Secure Network Analytics (SNA/StealthWatch)

Requisiti

- SNA Manager versione 7.4.1 o successive
- SNA Flow Collector in versione 7.4.1 o successive
- Esportatore che invia attivamente NetFlow alla SNA

Componenti usati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi

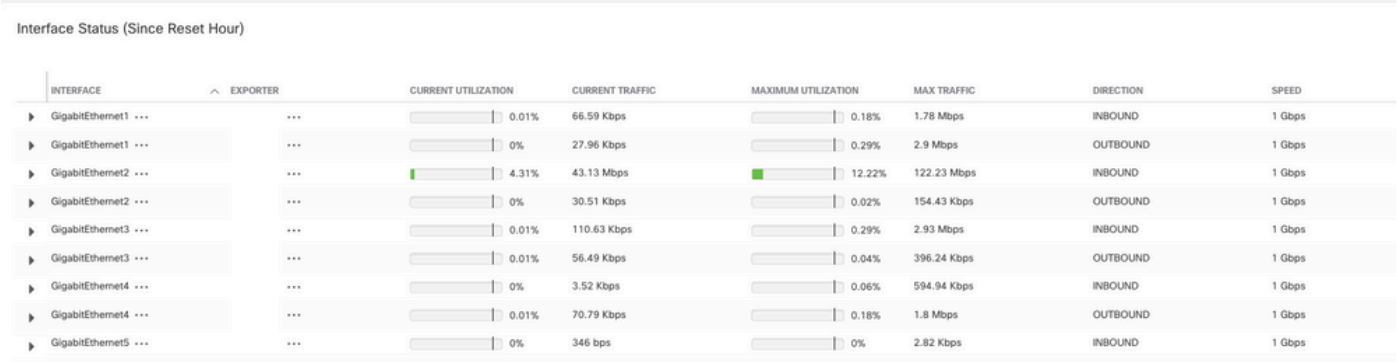
- SNA Manager versione 7.4.1 o successive
- SNA Flow Collector in versione 7.4.1 o successive
- software SNMPwalk
- Software Wireshark

Configurazioni

- Configurazione dispositivo: gli esportatori devono essere configurati per consentire l'accesso SNMP. Questo implica la configurazione delle impostazioni SNMP su ciascun dispositivo, inclusa la configurazione delle stringhe della community SNMP, degli elenchi di controllo di accesso (ACL) e la definizione della versione SNMP da utilizzare
- Configurazione del polling SNMP sulla SNA: dopo la corretta configurazione degli esportatori, il polling SNMP è abilitato per impostazione predefinita sull'SMC utilizzando parametri preimpostati. È fondamentale fornire i dettagli necessari relativi agli esportatori, come le stringhe della community SNMP e le versioni SNMP, per garantire il funzionamento ottimale del meccanismo di polling

Premesse

La SNA è in grado di fornire rapporti completi sullo stato dell'interfaccia e di visualizzare i nomi delle interfacce per gli esportatori che stanno trasmettendo attivamente i dati NetFlow a un Flow Collector. Per visualizzare i dettagli di questa interfaccia, accedere al menu Indaga -> Interfacce dall'interfaccia utente Web di Manager.


Interface Status (Since Reset Hour)

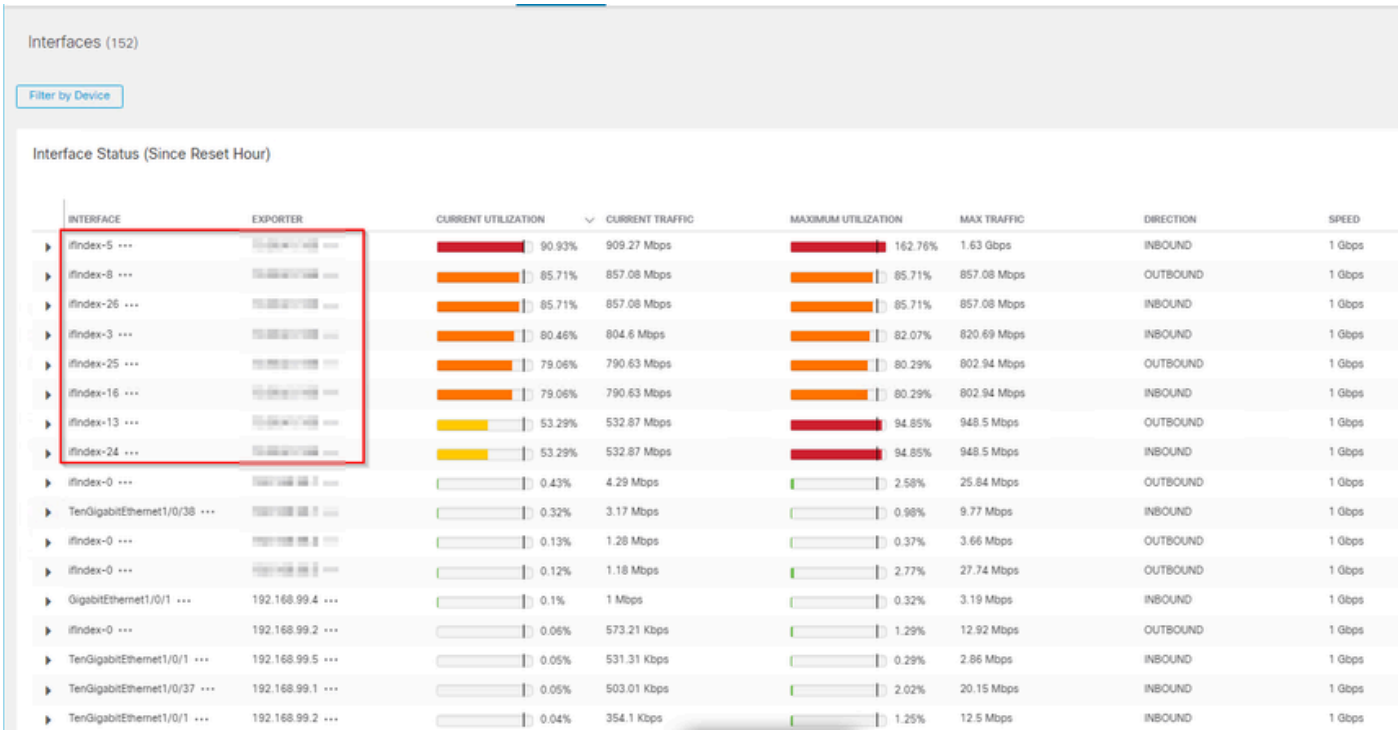
INTERFACE	EXPORTER	CURRENT UTILIZATION	CURRENT TRAFFIC	MAXIMUM UTILIZATION	MAX TRAFFIC	DIRECTION	SPEED
GigabitEthernet1		0.01%	66.59 Kbps	0.18%	1.78 Mbps	INBOUND	1 Gbps
GigabitEthernet1		0%	27.96 Kbps	0.29%	2.9 Mbps	OUTBOUND	1 Gbps
GigabitEthernet2		4.31%	43.13 Mbps	12.22%	122.23 Mbps	INBOUND	1 Gbps
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

Risoluzione dei problemi

Nomi di interfaccia non corretti

Nel caso in cui il report generato visualizzi un "ifindex-#" che non corrisponde alle interfacce di esportazione, viene suggerito un potenziale problema di configurazione con il polling SNMP sul SMC o sull'esportatore stesso. In questo esempio, ho evidenziato un problema apparente con il

polling SNMP di un dato esportatore.



Esportatori o interfacce mancanti

La verifica dei modelli riveste una notevole importanza nel contesto dell'elaborazione dei dati NetFlow. In particolare, garantisce che il modello NetFlow ricevuto dall'esportatore contenga tutti i campi necessari per la corretta decodifica e elaborazione da parte del Flow Collector. Il mancato rilevamento di un modello valido comporta l'esclusione dalla decodifica del set di flussi associato, determinando quindi la loro assenza dall'elenco delle interfacce.

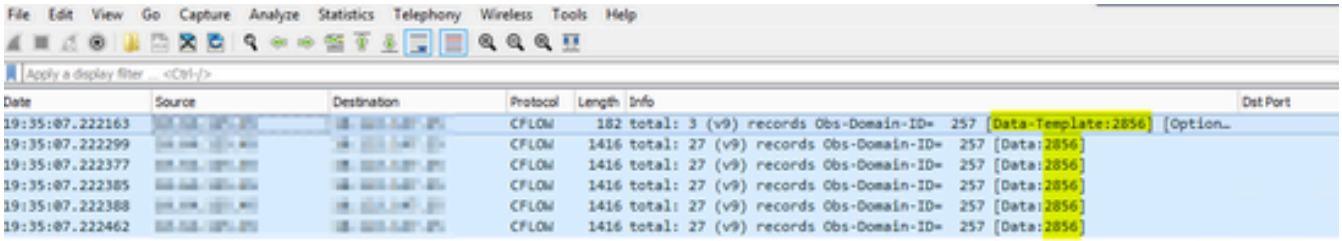
Se l'elenco delle interfacce non contiene l'indirizzo di esportazione/interfaccia previsto, è necessario verificare il modello dn dei dati netflow in arrivo. Per verificare il modello NetFlow, è possibile creare un pacchetto di acquisizione sul lato Flow Collector, specificando l'indirizzo IP dell'esportatore da cui otteniamo NetFlow cambiando "x.x.x.x":

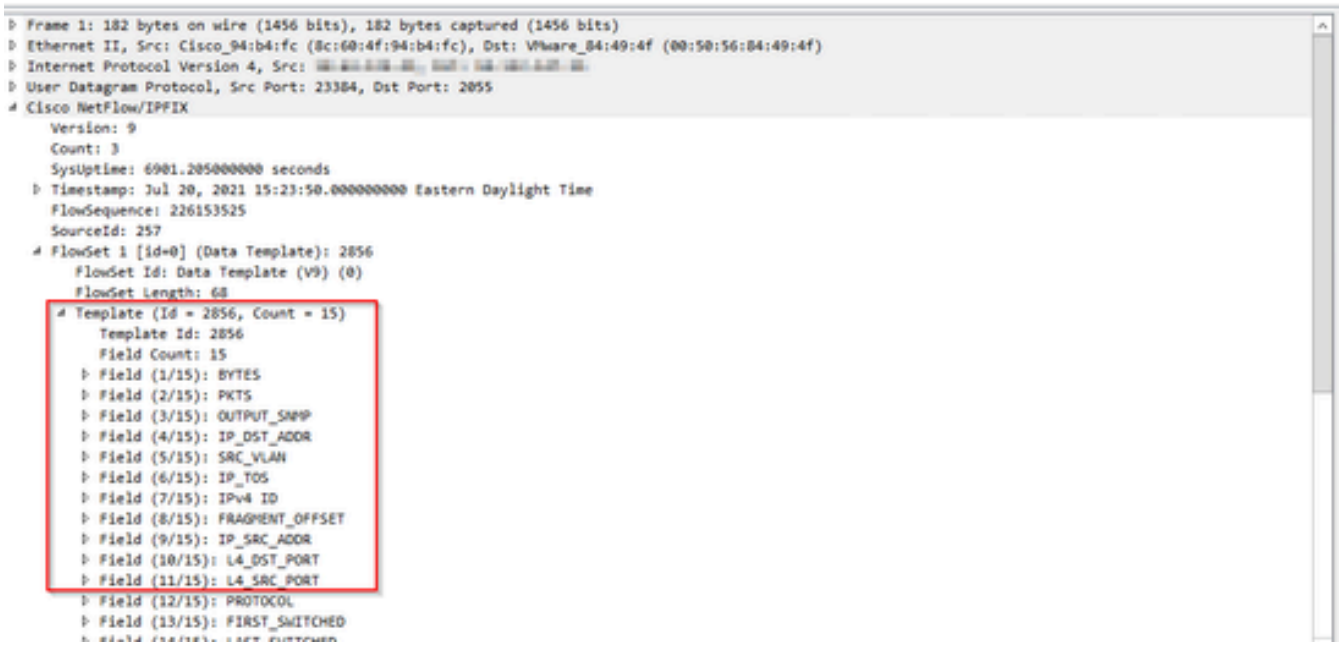
- Accedere a Flow Collector tramite SSH o la console con le credenziali radice.
- Eseguire un'acquisizione di pacchetto dall'indirizzo IP dell'esportatore e dalla porta netflow in questione:

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

```
.pcap
```

- Copiare l'acquisizione del pacchetto dall'accessorio a una workstation in cui è installata l'applicazione Wireshark, utilizzando il metodo preferito (ad esempio, SCP, SFTP).
- Aprire l'acquisizione del pacchetto con Wireshark e verificare il modello e i dati che l'esportatore sta inviando all'agente di raccolta del flusso





Verificare che il modello NetFlow utilizzi i 9 campi obbligatori, il nome esatto di questi campi del modello può variare a seconda del tipo di esportatore, quindi consultare la documentazione relativa al tipo di esportatore che si sta configurando:

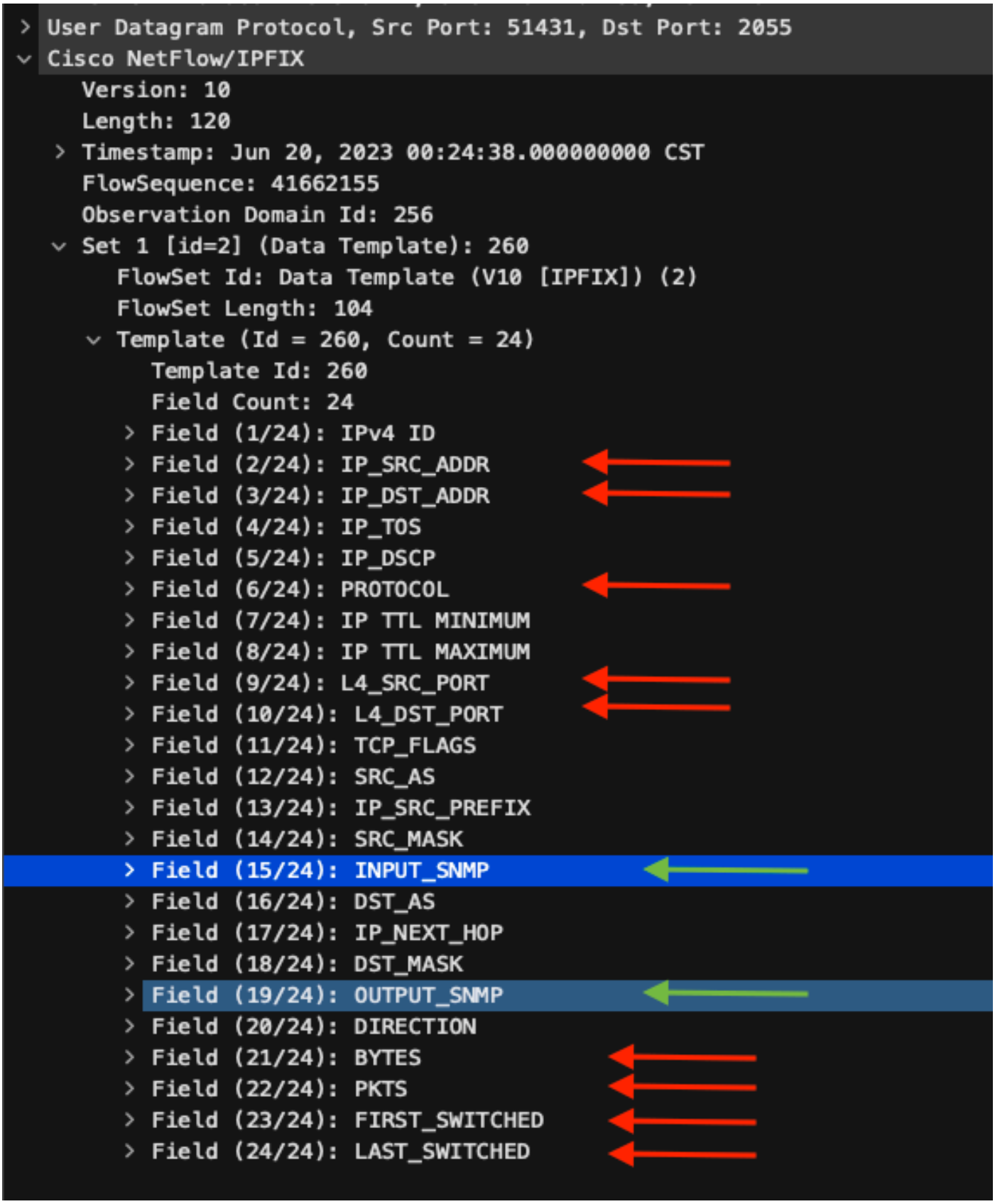
- Source IP Address
- Indirizzo IP di destinazione
- Porta di origine
- Porta di destinazione
- Protocollo di livello 4
- Conteggio byte
- Conteggio pacchetti
- Ora inizio flusso
- Ora fine flusso

Per visualizzare correttamente le interfacce, aggiungere anche:

    - uscita interface
    - input interfaccia

Di seguito è riportato un esempio di acquisizione pacchetto modello da un determinato dispositivo di esportazione

- Frecce rosse: campi NetFlow obbligatori
- Frecce verdi: campi SNMP



Nota: le porte elencate nel comando di esempio possono variare a seconda della configurazione di esportazione in uso. Il valore predefinito è 2055

Nota: mantenere l'acquisizione del pacchetto in esecuzione da 5 a 10 minuti, a seconda

dell'esportatore il modello può essere inviato ogni N minuti ed è necessario acquisire il modello in modo che NetFlow venga decodificato correttamente. Se il modello non viene visualizzato, ripetere l'acquisizione del pacchetto per un periodo di tempo più lungo

Problemi di connettività

Controllare la connettività: verificare che esista una connettività tra l'accessorio SNA Manager e gli esportatori. Verificare che gli esportatori siano raggiungibili dalla console di gestione Stealthwatch eseguendo il ping dei loro indirizzi IP. In caso di problemi di connettività di rete, risolverli e risolvere i problemi di conseguenza.

Convalida la capacità del manager (SMC) di eseguire il polling degli esportatori

- Connettersi a SNA manager tramite SSH e accedere con le credenziali root
- Analizzare il file /lancope/var/smc/log/smc-configuration.log e cercare i log di tipo ExporterSnmpSession:

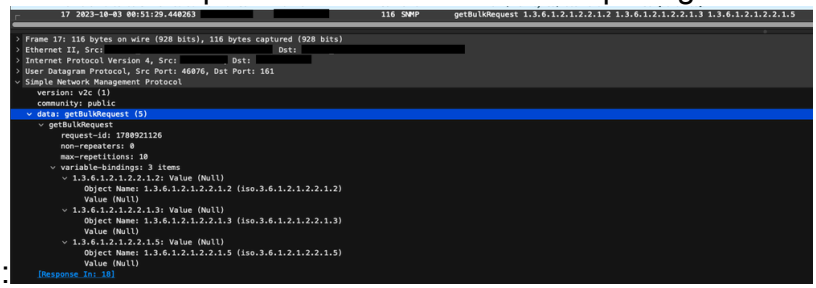
```
INFO [ExporterSnmpSession] SNMP polling for 10.1.0.253 took 0s
INFO [ExporterSnmpSession] SNMP polling for 10.1.0.253 took 0s
WARN [ExporterSnmpSession] SNMP polling for 10.10.0.254 failed: java.lang.Exception: timeout
INFO [ExporterSnmpSession] SNMP polling for 10.10.0.254 took 20s
WARN [ExporterSnmpSession]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

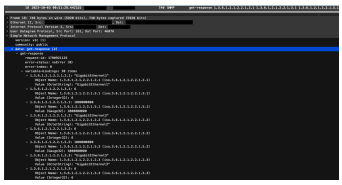
- In questo esempio di sondaggio non sono stati rilevati errori per l'esportatore 10.1.0.253. Tuttavia, l'esportatore 10.1.0.254 ha inizialmente riscontrato un messaggio di errore di timeout, ma in seguito è riuscito a eseguire correttamente l'operazione di polling dopo un ritardo di 20 secondi.

Generare un'acquisizione di pacchetti sull'SMC utilizzando l'indirizzo IP di un esportatore.

- Accedere al nodo Manager tramite SSH o la console con le credenziali radice
- Lanciare:

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

- Esportare l'acquisizione del pacchetto dall'accessorio con il metodo preferito (ad esempio, SCP, SFTP)
- Aprire l'acquisizione del pacchetto con Wireshark per visualizzare i tentativi di polling riusciti
  - Richiesta presentata dal CSM: 

- Risposta SNMP dell'esportatore con informazioni di interfaccia: 

Convalida impostazioni di polling SNMP

Verificare che gli intervalli di polling siano appropriati e che le metriche desiderate siano incluse nelle query SNMP

- Nell'interfaccia utente del Web passare a: Configure -> Exporters -> Exporter SNMP Profiles:
- Verificare che la porta SNMP corretta (in genere la porta UDP 161) e il metodo di query SNMP corretto selezionati corrispondano all'utilità di esportazione (ifxTable Columns, CatOS MIB, PanOS MIB) 

Nota: se si dispone di interfacce a 10 Gbps, si consiglia di scegliere l'opzione FixTable columns per il metodo di query SNMP.

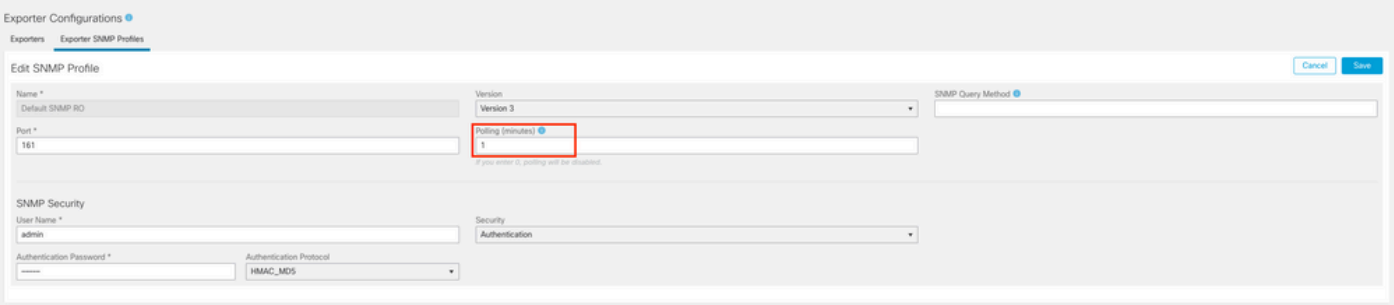
Nota: per prestazioni ottimali del sistema, impostare il polling SNMP su un intervallo di 12 ore. Il polling più frequente non rende le metriche di utilizzo più aggiornate e può rallentare l'esecuzione del sistema.

- Verificare che le versioni SNMP configurate sia su SNA che sugli esportatori siano compatibili. La SNA supporta SNMPv1, SNMPv2c e SNMPv3. Verificare che gli esportatori siano configurati per utilizzare la stessa versione SNMP configurata nella SNA.
  - In caso di utilizzo di SNMPv3, verificare che la configurazione SNMP sia corretta (Nome utente, Password di autenticazione, Protocollo di autenticazione, Password privacy, Protocollo privacy)

Risoluzione dei problemi in tempo reale del polling SNMP

Nell'interfaccia utente del Web, selezionare Configure -> Exporters -> Exporter SNMP Profiles

- Impostare temporaneamente Polling (minuti) su 1 (minuti).



- Accedere all'SMC tramite SSH o la console con le credenziali root.
- Passa alla cartella:

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

- Lanciare:

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

- Per SNMPv3, un messaggio di errore comune sarebbe:

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

- Verificare che la password di autenticazione nel profilo SNMP sia impostata su almeno 8 caratteri.
- Al termine della risoluzione dei problemi in tempo reale, ripristinare il valore precedente della configurazione di Polling (minuti) per l'utilità di esportazione o il relativo modello di configurazione.

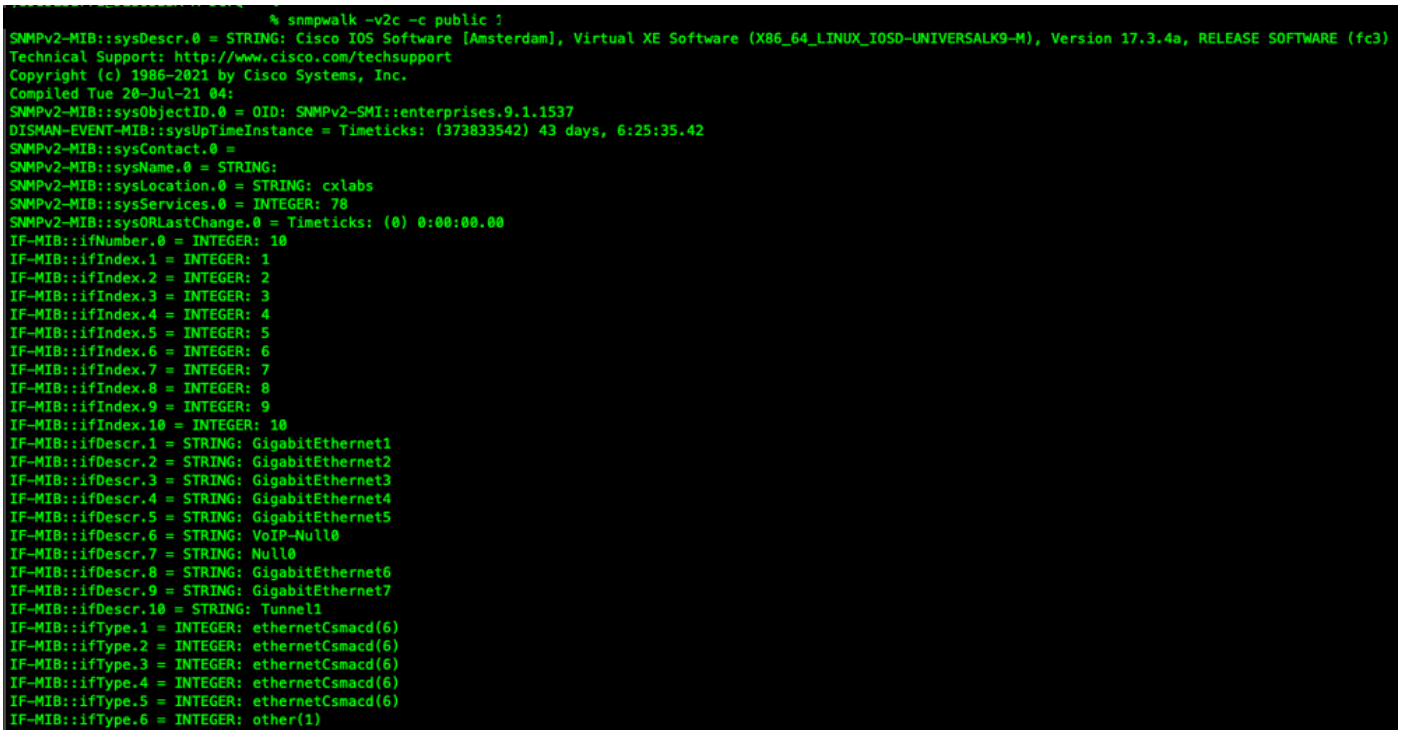
Test del polling SNMP da un altro dispositivo

Test del polling SNMP: avviare manualmente un polling SNMP da un computer locale a un dispositivo di rete specifico e verificare se riceve una risposta. A tale scopo, è possibile utilizzare strumenti di polling SNMP o utilità quali SNMPwalk. Verificare che il dispositivo di rete risponda con i dati SNMP richiesti. In assenza di risposta, viene indicato un problema di configurazione o connettività SNMP.

- Sul computer locale con software SNMPwalk, sostituire "x.x.x.x" per l'indirizzo IP dell'utilità di esportazione ed eseguire il comando sulla CLI:

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

    - -v2c: specifica la versione SNMP da utilizzare
    - -c: imposta la stringa della community



- Verificare che l'esportatore risponda con i dati SNMP

Informazioni correlate

- Per ulteriore assistenza, contattare il Technical Assistance Center (TAC). È necessario un contratto di supporto valido: Contatti del supporto Cisco internazionali.
- In questa sezione è possibile anche visitare la Cisco Security Analytics Community.
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).