Risoluzione dei problemi di acquisizione della telemetria NetFlow/IPFIX in Secure Network Analytics

Sommario

Introduzione

Questo documento descrive come risolvere i problemi relativi all'acquisizione di telemetria Netflow in Secure Network Analytics (SNA).

Prerequisiti

- Conoscenza SNA Cisco
- Conoscenze NetFlow/IPFIX

Requisiti

- Secure Network Analytics versione 7.5.0 o successive
- Flow Collector in 7.5.0 o versioni successive
- Accesso CLI come sysadmin a Flow Collector
- Accesso all'interfaccia utente dell'amministratore come amministratore di Flow Collector

Guide alla configurazione

- Configurazione di NetFlow/IPFIX per l'acquisizione della telemetria su analisi di rete sicure

Componenti usati

- SNA Manager e Flow Collector su 7.5.0
- Software Wireshark

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.

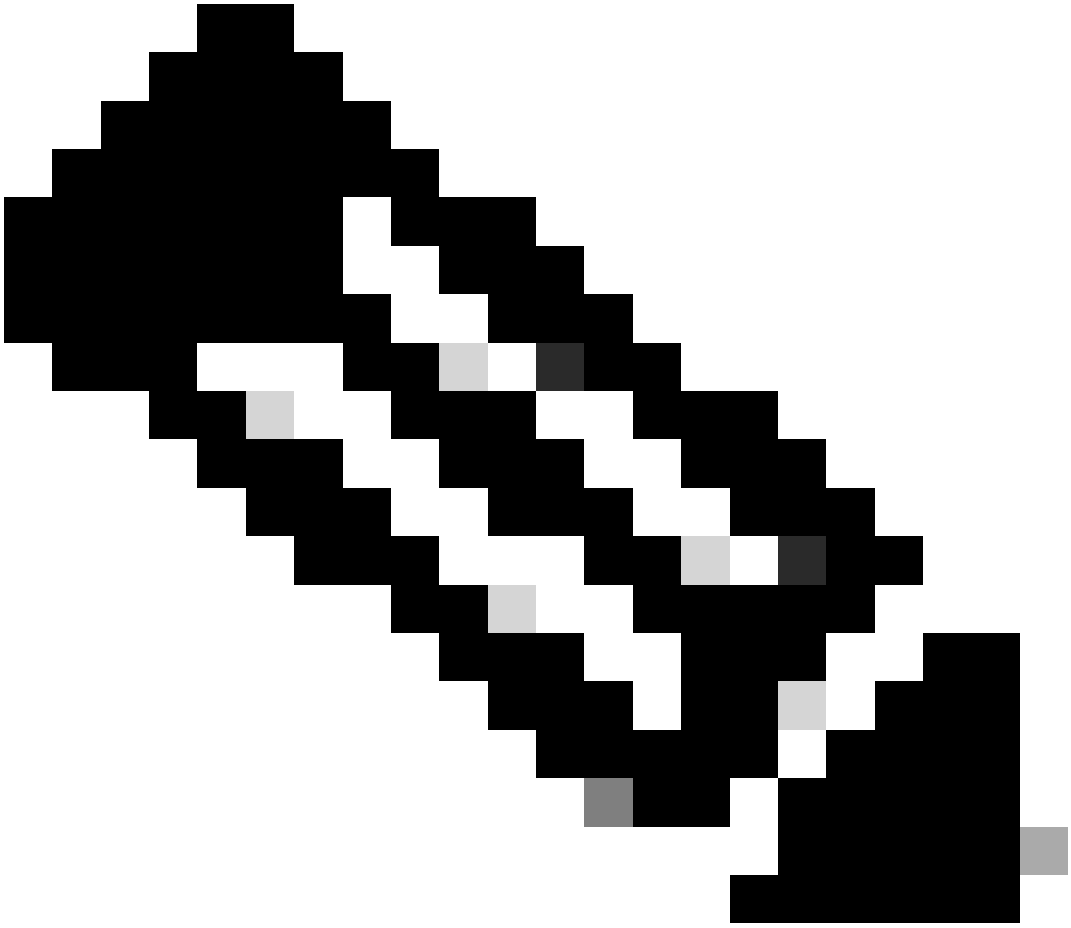
Premesse

Flow Collector è un'appliance SNA incaricata di raccogliere, elaborare e archiviare i flussi che vengono inviati a Secure Network Analytics. Per NetFlow versione 9 o IPFIX, è possibile includere diversi campi nel modello NetFlow/IPFIX per aggiungere ulteriori informazioni relative al traffico di rete. Tuttavia, sono disponibili 9 campi specifici che devono essere inclusi nel modello NetFlow/IPFIX affinché il Flow Collector possa elaborare tali flussi. Flow Collector non elabora i flussi in ingresso che includono un modello non valido, pertanto SNA non visualizza le informazioni sul flusso di tali esportatori sotto interfaccia utente Web o client desktop.

Campi obbligatori

I campi successivi devono essere inclusi nel modello NetFlow/IPFIX per il caricamento della telemetria. Verificare che questi 9 campi siano inclusi nel modello NetFlow/IPFIX per consentire a Secure Network Analytics di elaborare i flussi in ingresso.

- Source IP Address
- Indirizzo IP di destinazione
- Porta di origine
- Porta di destinazione
- Protocollo di livello 3
- Conteggio byte
- Conteggio pacchetti
- Ora inizio flusso
- Ora fine flusso



Nota: È possibile includere più campi nella configurazione NetFlow/IPFIX, tuttavia i campi precedenti rappresentano i requisiti minimi di Secure Network Analytics per il caricamento della telemetria.

Risoluzione dei problemi del processo

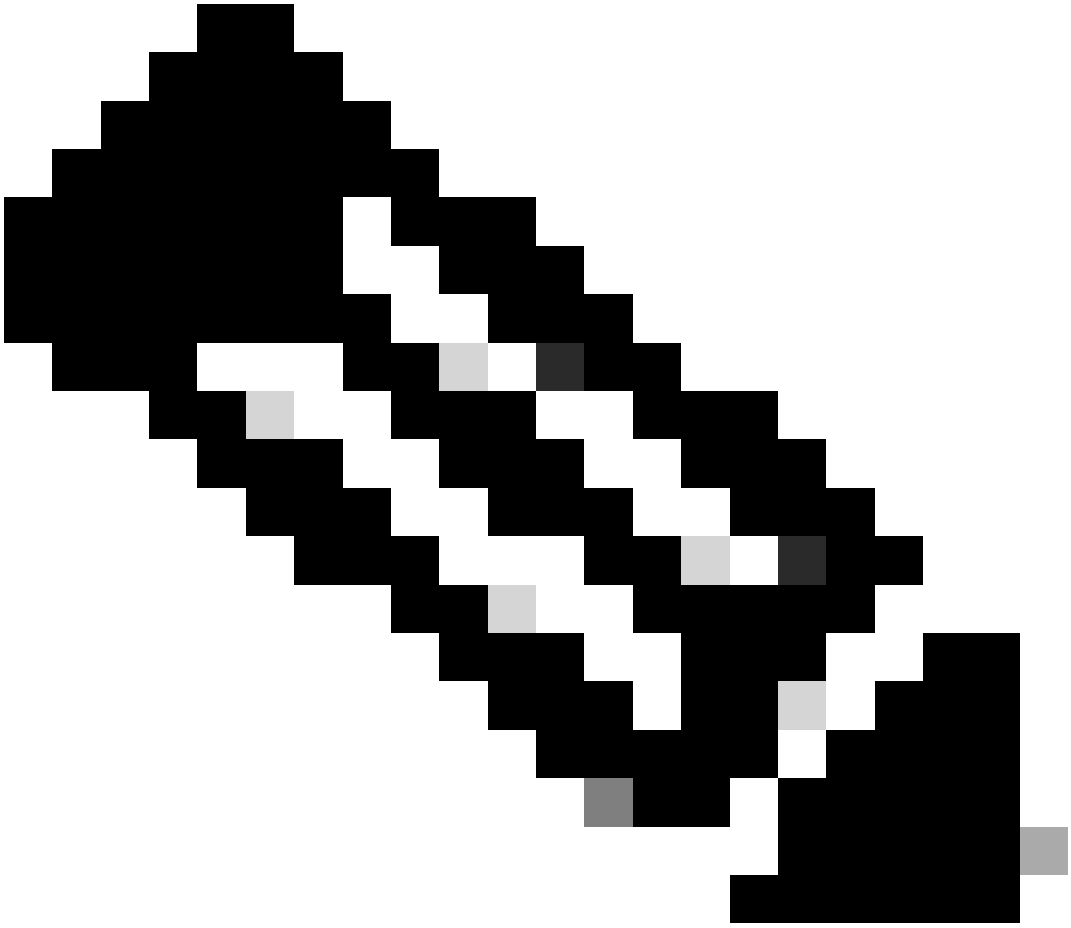
Verifica dell'inserimento della telemetria NetFlow/IPFIX

Per verificare se SNA Flow Collector riceve e inserisce la telemetria NetFlow/IPFIX dagli esportatori:

1. Accedere all'interfaccia utente Admin di SNA Flow Collector con le credenziali admin: https://<Flow Collector IP Address>/swa/login.html
2. Nel pannello sinistro, selezionare Supporto > Sfoglia file
3. Passare alla cartella successiva: sw > oggi > registri
4. Fare clic sul file sw.log per scaricarlo sul computer locale e aprirlo in un editor di testo.

5. Cercare queste righe nella parte inferiore del registro. Il riepilogo viene creato ogni cinque minuti:

```
18:45:00 I-sch-t: process_5_min_period: begin
18:45:00 I-sch-t: process_5_min_period: periods(177)
18:45:00 S-per-t: Performance Period 177
18:45:00 S-per-t:     Engine status Status normal
18:45:00 S-per-t:     Processed 6948 flows at 24 fps this period
18:45:00 S-per-t:     Processed 4226 biflows at 15 fps this period
18:45:00 S-per-t:     Dropped 0 flows this period
18:45:00 S-per-t:     Discarded 4358 flows this period due to insufficient template data
18:45:00 S-per-t:     Processed 1838743 flows at 35 fps today
18:45:00 S-per-t:     Dropped 0 flows today
18:45:00 S-per-t:     Discarded 11069 flows today due to insufficient template data
18:45:00 S-per-t:     Process instance 0 processed 3372 flows at 12 fps this period
18:45:00 S-per-t:     Process instance 0 processed 2066 biflows at 7 fps this period
18:45:00 S-per-t:     Process instance 1 processed 3576 flows at 12 fps this period
18:45:00 S-per-t:     Process instance 1 processed 2160 biflows at 8 fps this period
18:45:00 S-per-t:     Inserted 2048 flow stats at 7 fps this period
18:45:00 S-per-t:     Inserted 2013 interface stats at 7 fps this period
18:45:00 S-per-t:     Inserted 470932 flow stats at 9 fps today
18:45:00 S-per-t:     Inserted 678994 interface stats at 13 fps today
```



Nota: La riga 8 indica che sono presenti flussi scartati a causa di dati del modello insufficienti nell'ultimo periodo.

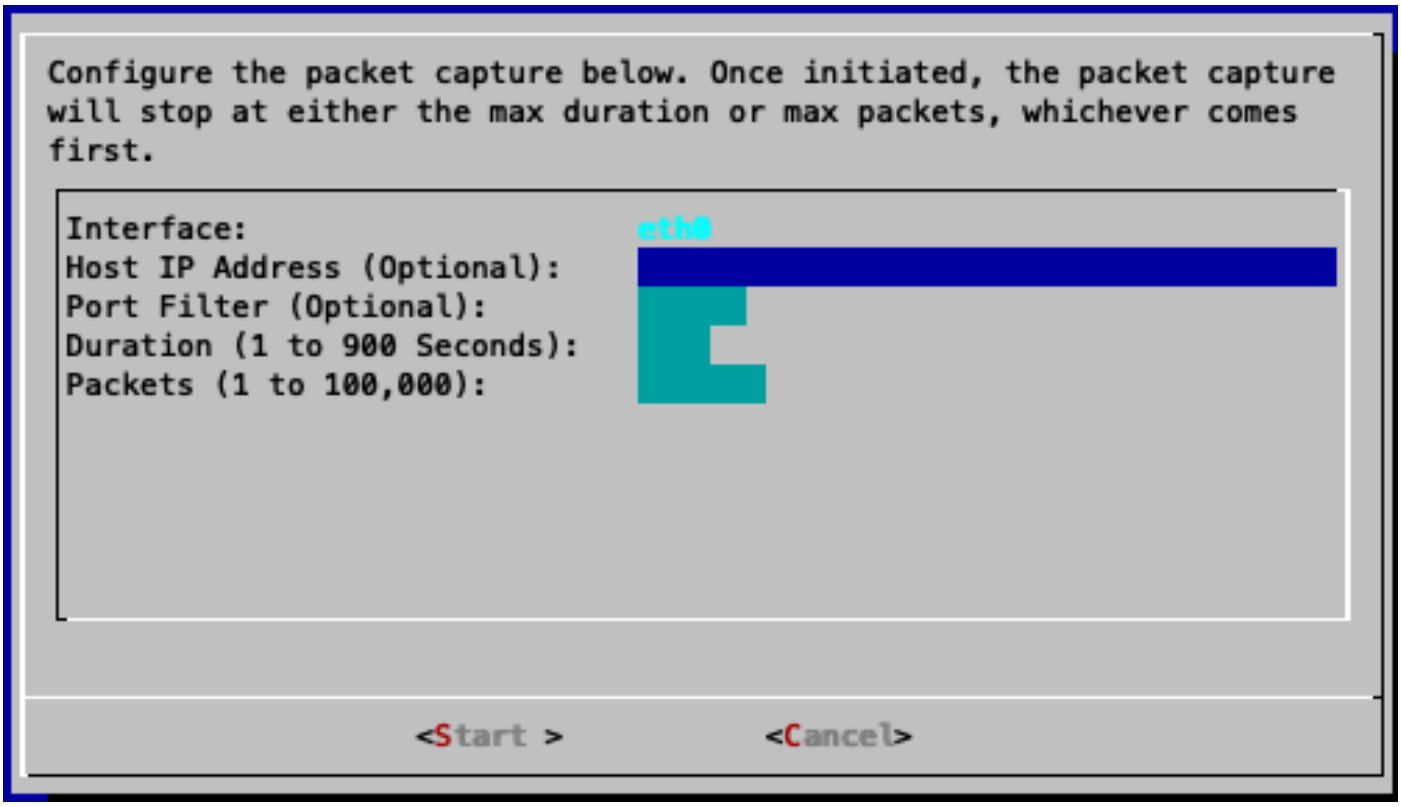
Verifica modello NetFlow/IPFIX

Per confermare i campi inclusi nel modello NetFlow/IPFIX:

1. Accedere alla CLI di SNA Flow Collector con le credenziali sysadmin.

2. Nel menu SystemConfig, passare a: Avanzate > Acquisizione pacchetti

3. Inserire le informazioni dell'esportatore che non mostra i flussi sulla SNA:



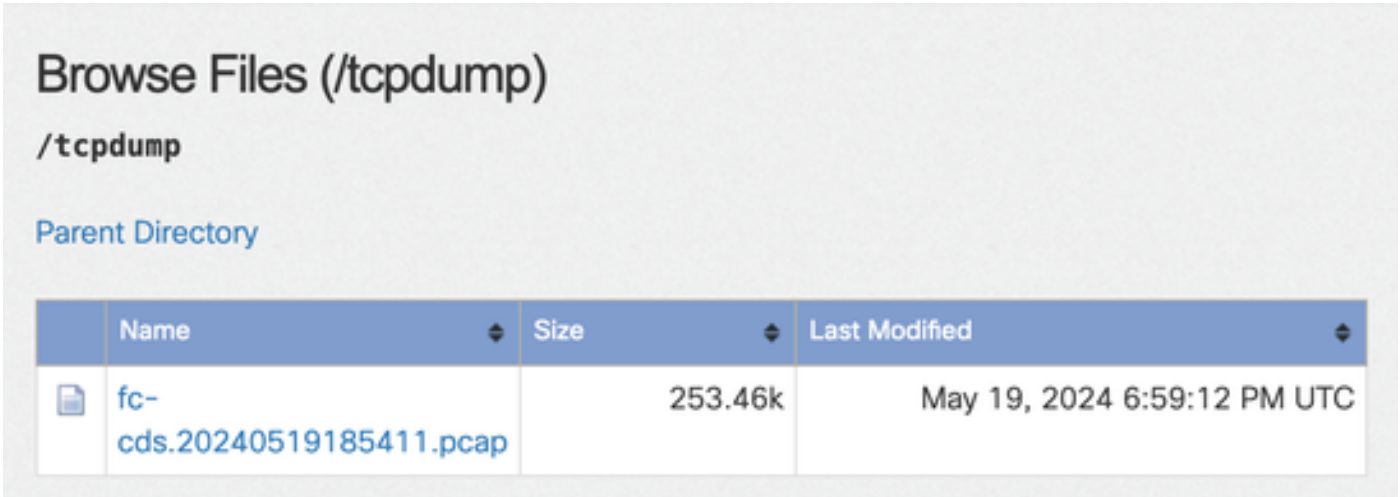
4. Attendere il completamento del processo.

5. Per scaricare il file, accedere all'interfaccia utente Admin di SNA Flow Collector con le credenziali admin: https://<Flow Collector IP Address>/swa/login.html

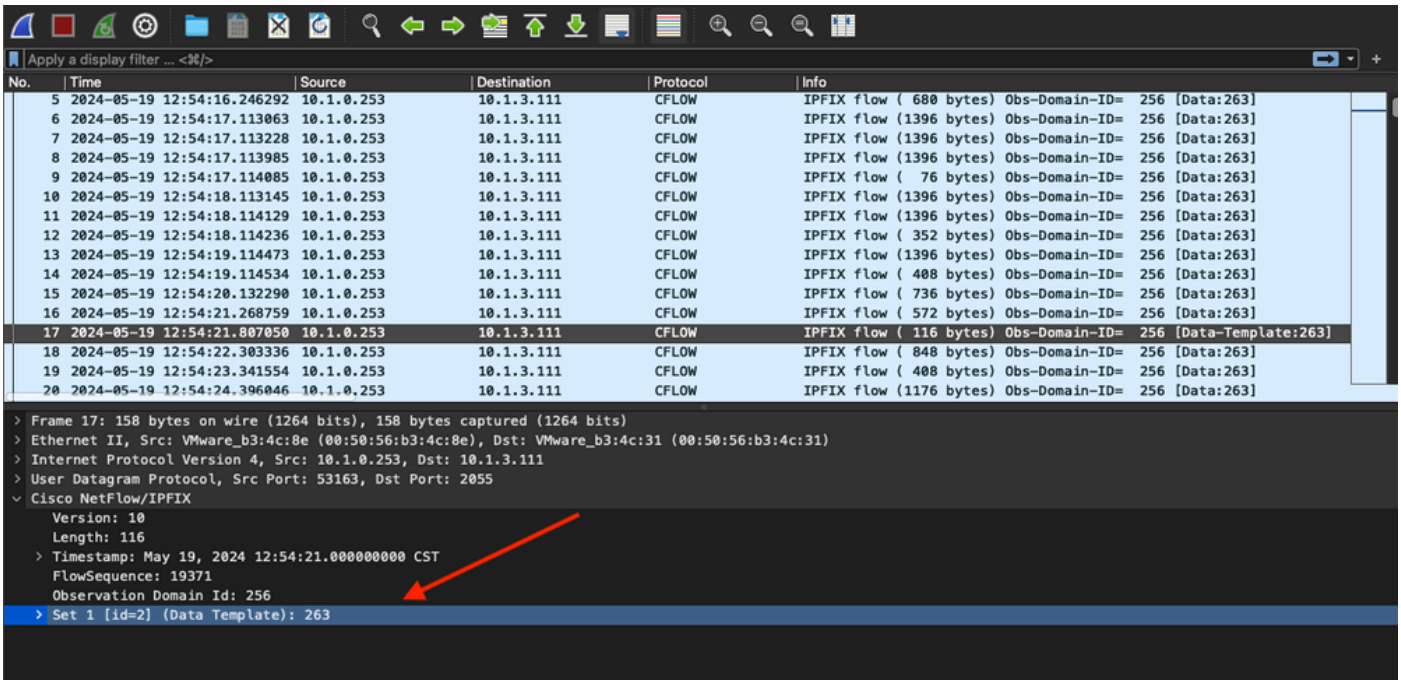
6. Nel pannello sinistro, selezionare Support > Browse Files

7. Passare alla cartella successiva: tcpdump

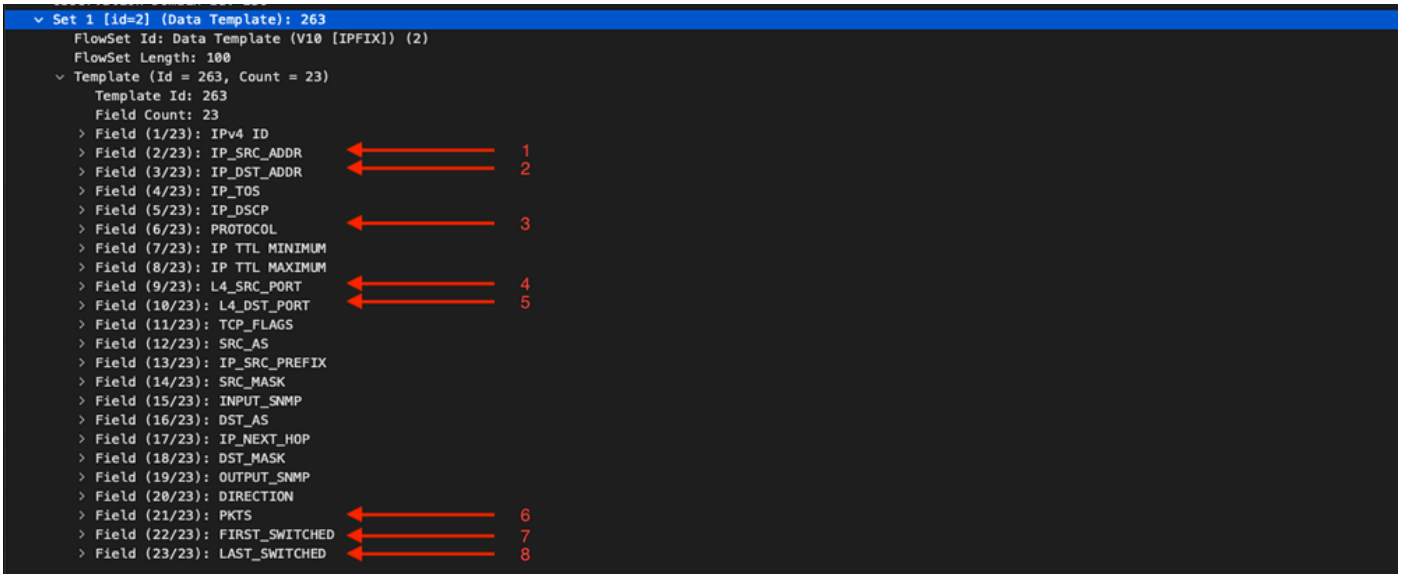
8. Fare clic sul file di acquisizione dei pacchetti per scaricarlo sul computer locale e aprirlo su Wireshark:

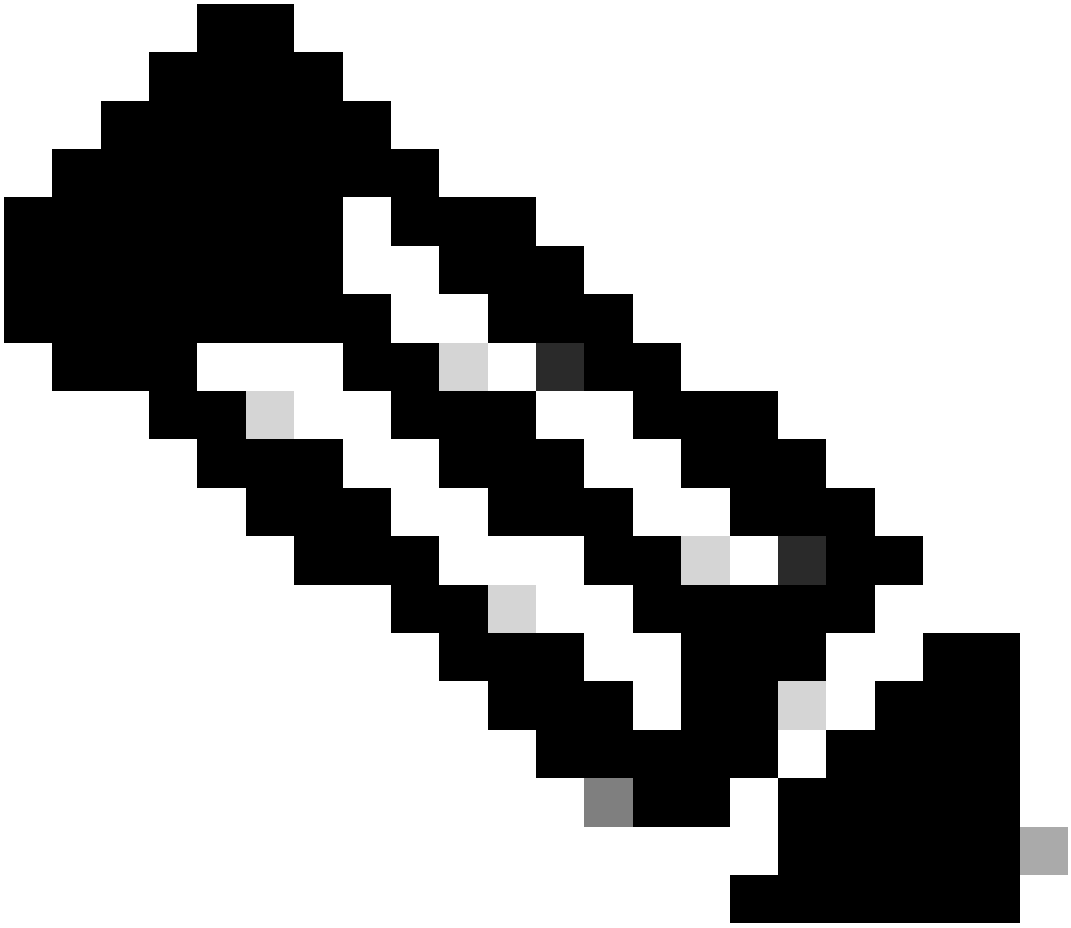


9. Identificare il frame in cui è stato ricevuto il modello NetFlow/IPFIX.



10. Verificare che i 9 campi obbligatori siano presenti nel modello





Nota: Notare che sul modello ci sono solo 8 dei 9 campi obbligatori che SNA richiede per il caricamento della telemetria; per questo scenario, manca il campo BYTE.

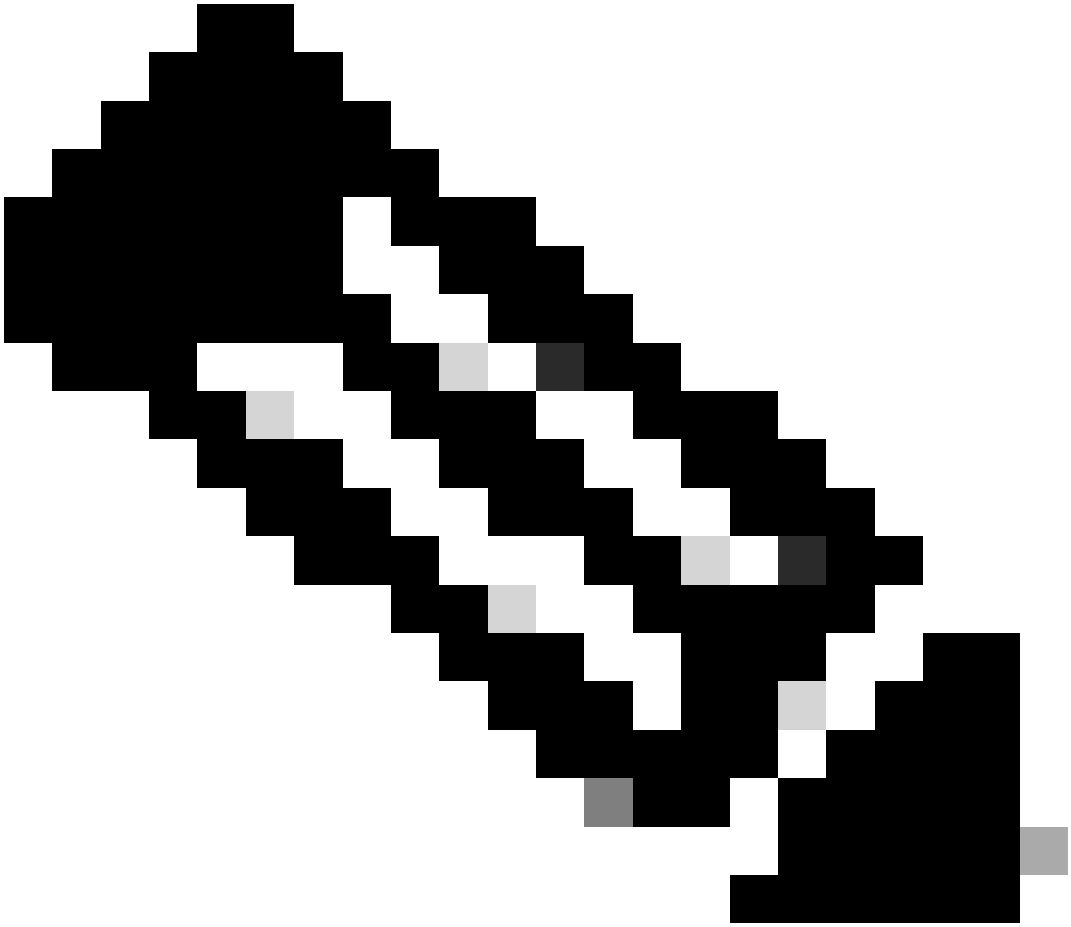
Verificare l'inserimento della telemetria NetFlow/IPFIX dopo aver aggiunto i campi mancanti

Per confermare se SNA Flow Collector riceve e inserisce la telemetria NetFlow/IPFIX dall'esportatore dopo la modifica:

1. Accedere all'interfaccia utente Admin di SNA Flow Collector con le credenziali admin: https://<Flow Collector IP Address>/swa/login.html
2. Nel pannello sinistro, selezionare Supporto > Sfoglia file
3. Passare alla cartella successiva: sw > oggi > registri
4. Fare clic sul file sw.log per scaricarlo sul computer locale e aprirlo in un editor di testo.
5. Cerca queste righe nella parte inferiore del registro

```
19:20:00 I-sch-t: process_5_min_period: begin
```

```
19:20:00 I-sch-t: process_5_min_period: periods(184)
19:20:00 S-per-t: Performance Period 184
19:20:00 S-per-t:     Engine status Status normal
19:20:00 S-per-t:     Processed 10992 flows at 37 fps this period
19:20:00 S-per-t:     Processed 4176 biflows at 14 fps this period
19:20:00 S-per-t:     Dropped 0 flows this period
19:20:00 S-per-t:     Discarded 0 flows this period due to insufficient template data
19:20:00 S-per-t:     Processed 1896017 flows at 35 fps today
19:20:00 S-per-t:     Dropped 0 flows today
19:20:00 S-per-t:     Discarded 36041 flows today due to insufficient template data
19:20:00 S-per-t:     Process instance 0 processed 5575 flows at 19 fps this period
19:20:00 S-per-t:     Process instance 0 processed 2195 biflows at 8 fps this period
19:20:00 S-per-t:     Process instance 1 processed 5417 flows at 19 fps this period
19:20:00 S-per-t:     Process instance 1 processed 1981 biflows at 7 fps this period
19:20:00 S-per-t:     Inserted 2878 flow stats at 10 fps this period
19:20:00 S-per-t:     Inserted 4510 interface stats at 16 fps this period
19:20:00 S-per-t:     Inserted 486734 flow stats at 9 fps today
19:20:00 S-per-t:     Inserted 696260 interface stats at 13 fps today
```



Nota: La riga 8 indica che non vi sono flussi scartati nell'ultimo periodo.

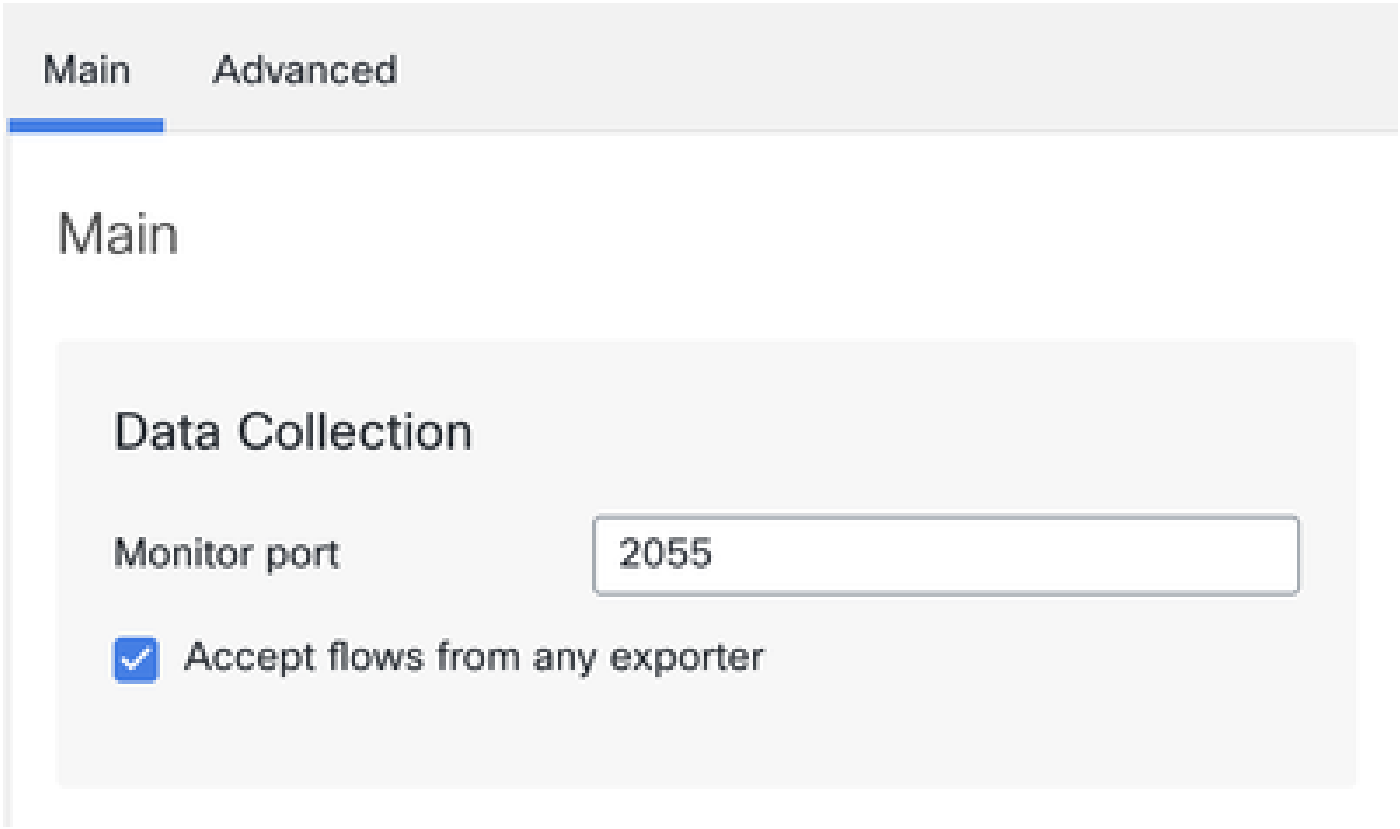
Verifica della porta di acquisizione della telemetria NetFlow/IPFIX

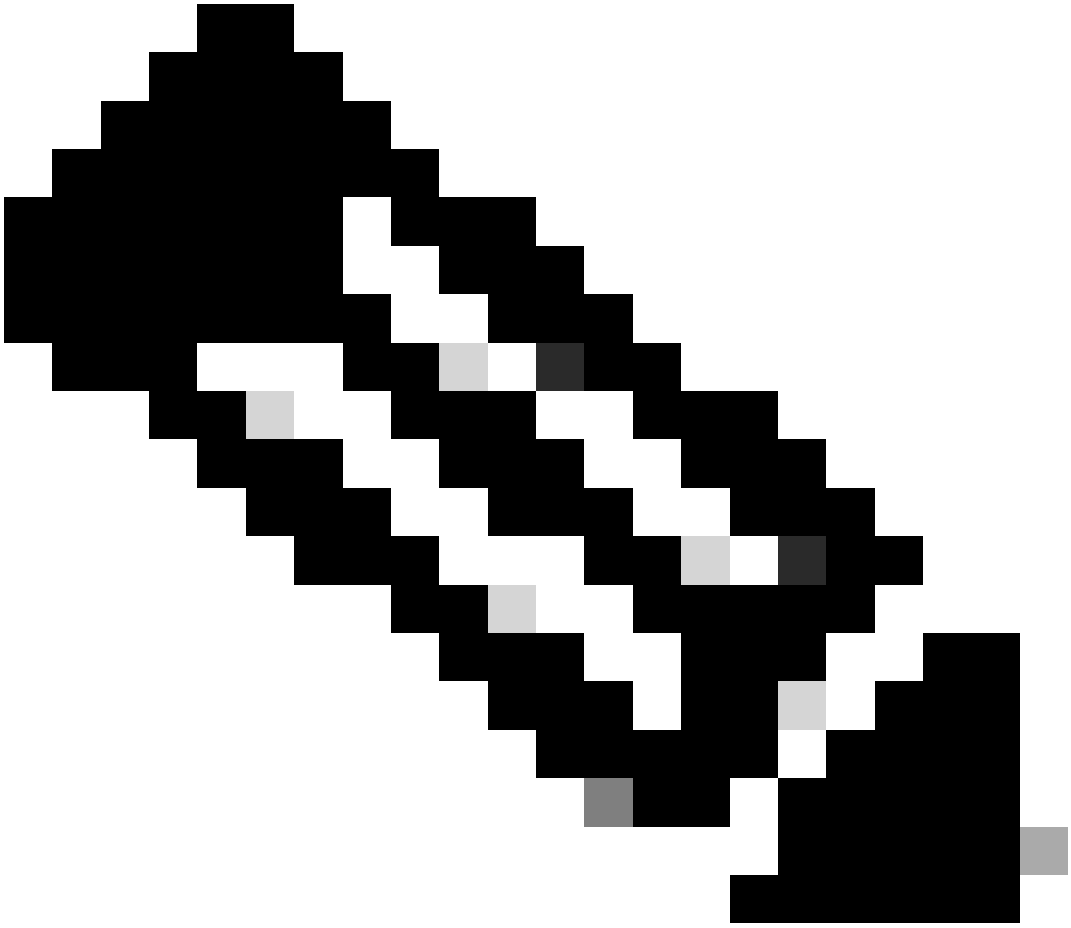
Per verificare se SNA Flow Collector riceve la telemetria NetFlow/IPFIX dagli esportatori sulla porta corretta:

1. Accedere all'interfaccia utente Web SNA con un utente con autorizzazioni di amministratore.

2. Nel menu superiore, passare a Configura e scegliere Raccoglitori flusso

3. Confermare che SNA Flow Collector utilizzi la stessa porta configurata dagli esportatori per inviare il comando NetFlow/IPFIX





Nota: La porta predefinita per NetFlow è 2055. Tuttavia, è possibile selezionare un'altra porta. Accertarsi di utilizzare la stessa porta durante il primo processo di configurazione sul Flow Collector(s).

Verificare che l'opzione NetFlow per l'inserimento della telemetria NetFlow sia abilitata

Per verificare se l'opzione SNA Flow Collector per la trasmissione telemetrica di NetFlow/IPFIX è abilitata:

1. Accedere all'interfaccia utente Admin di SNA Flow Collector con le credenziali di amministratore: https://<Flow Collector IP Address>/swa/login.html
2. Nel pannello sinistro, selezionare Supporto > Impostazioni avanzate
3. Confermare che l'opzione enable_netflow sia impostata su 1:

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).