Secure Network AnalyticsでのNetFlow/IPFIXテレメトリインジェストのトラブルシューティング

内容

[はじめに](#)

[前提条件](#)

- [要件](#)
- [設定ガイド](#)
- [使用するコンポーネント](#)

[背景説明](#)

- [必須フィールド](#)

[トラブルシューティングプロセス](#)

- [NetFlow/IPFIXテレメトリ取り込みの確認](#)
- [NetFlow/IPFIXテンプレートの確認](#)
- [欠落しているフィールドを追加した後のNetFlow/IPFIXテレメトリインジェストの確認](#)
- [NetFlow/IPFIXテレメトリ取り込みポートの確認](#)
- [NetFlow/IPFIX Telemetry Ingest NetFlowオプションが有効になっていることを確認します。](#)

[関連情報](#)

はじめに

このドキュメントでは、Secure Network Analytics(SNA)のNetflowテレメトリインジェストをトラブルシューティングする方法について説明します。

前提条件

- Cisco SNAの知識
- NetFlow/IPFIXの知識

要件

- 7.5.0以降のSecure Network Analytics
- 7.5.0以降のフローコレクタ
- Flow CollectorへのsysadminとしてのCLIアクセス
- Flow Collectorへの管理者としての管理UIアクセス

設定ガイド

- Secure Network AnalyticsでのテレメトリインジェストのためのNetFlow/IPFIXの設定

使用するコンポーネント

- 7.5.0上のSNAマネージャおよびフローコレクタ
- Wiresharkソフトウェア

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

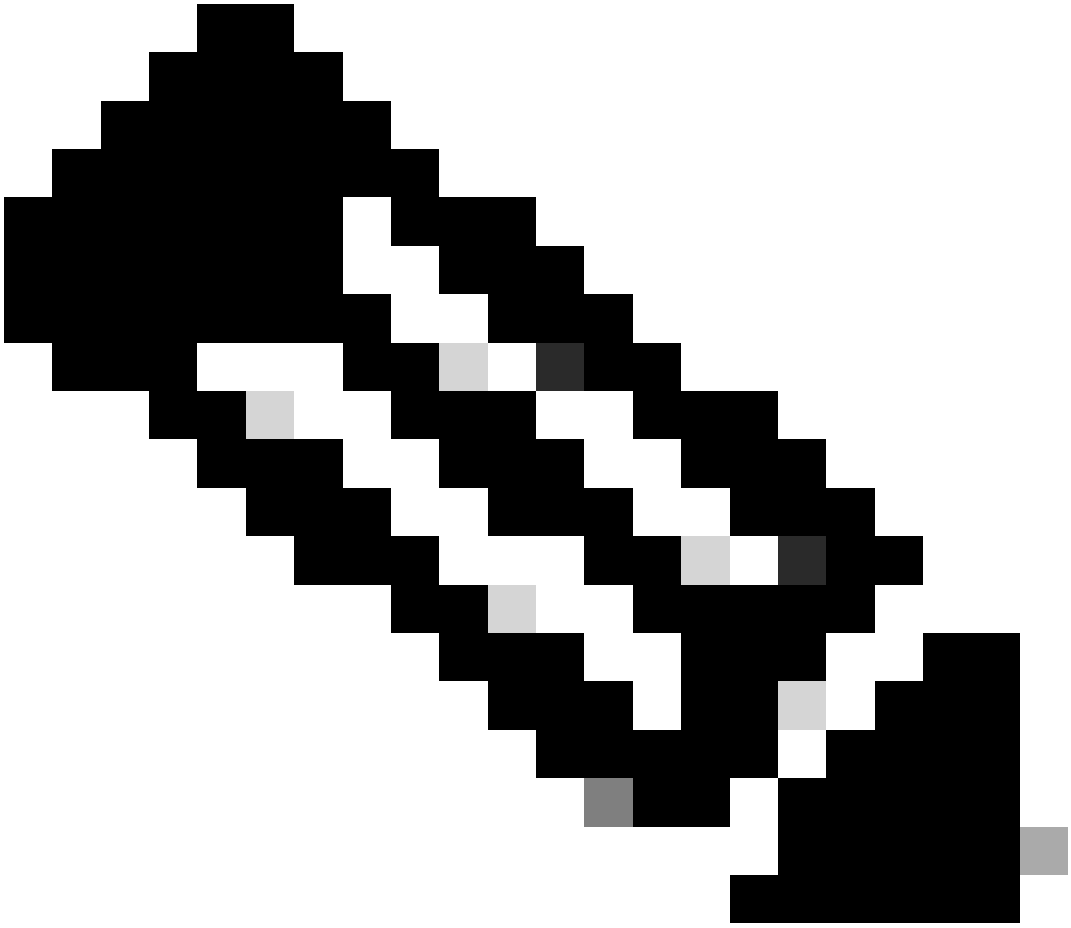
背景説明

Flow Collectorは、Secure Network Analyticsに送信されるフローの収集、処理、保存を担当するSNAアプライアンスです。NetFlowバージョン9またはIPFIXの場合、NetFlow/IPFIXテンプレートに複数のフィールドを含めてネットワークトラフィックに関する情報をさらに追加できますが、Flow Collectorがこれらのフローを処理するためには、9つの特定のフィールドをNetFlow/IPFIXテンプレートに含める必要があります。フローコレクタは、無効なテンプレートを含む着信フローを処理しません。そのため、SNAは、これらのエクスポータのフロー情報をWeb UIまたはデスクトップクライアントの下に表示しません。

必須フィールド

次のフィールドは、テレメトリ取り込み用のNetFlow/IPFIXテンプレートに含める必要があります。Secure Network Analyticsが着信フローを処理するために、これら9つのフィールドがNetFlow/IPFIXテンプレートに含まれていることを確認します。

- 送信元 IP アドレス
- 宛先 IP アドレス
- 送信元ポート
- 宛先ポート
- レイヤ3プロトコル
- バイト数
- パケット数
- フロー開始時間
- フロー終了時間



注:NetFlow/IPFIXの設定ではさらに多くのフィールドを含めることができますが、前述のフィールドはSecure Network Analytics for Telemetry Ingestの最小要件です。

トラブルシューティングプロセス

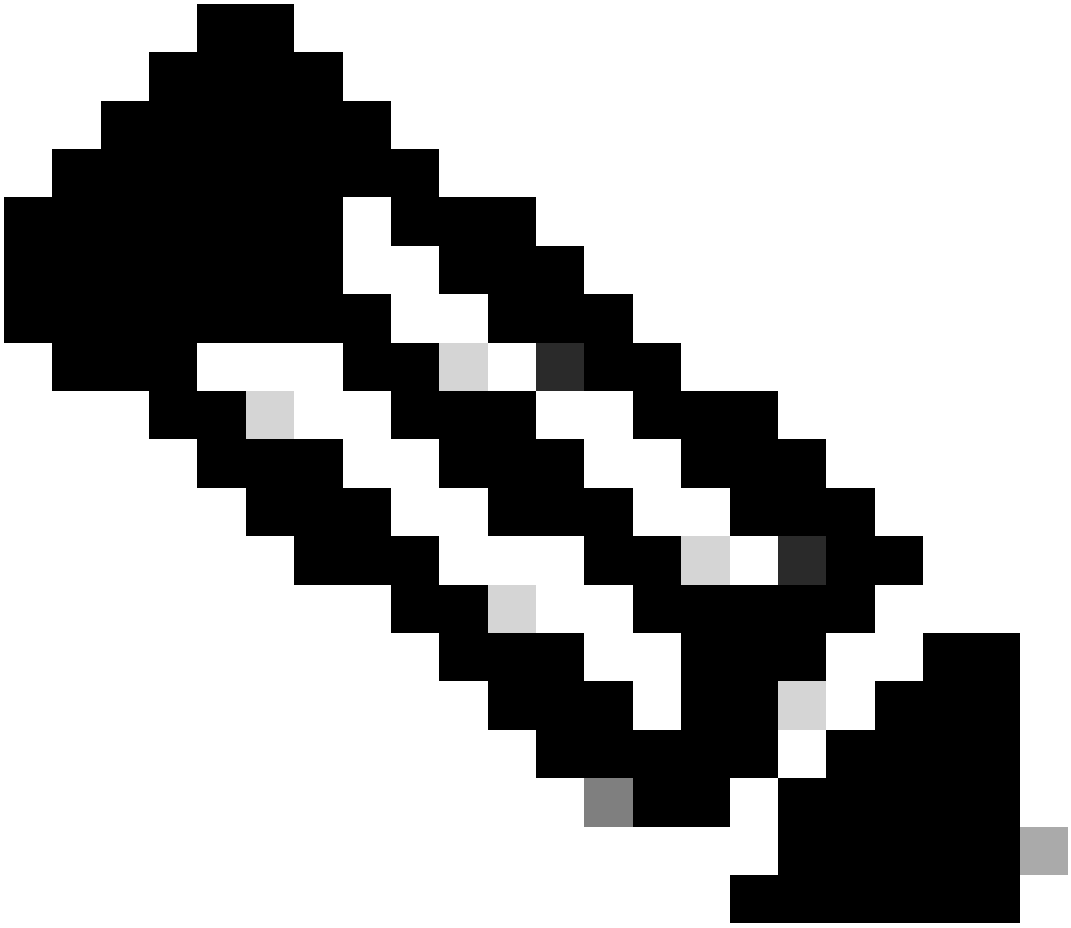
NetFlow/IPFIXテレメトリ取り込みの確認

SNAフローコレクタがエクスポータからNetFlow/IPFIXテレメトリを受信して挿入するかどうかを確認するには、次のコマンドを実行します。

1. 管理者クレデンシャル(https://<Flow Collector IP Address>/swa/login.html)を使用してSNA Flow Collector Admin UIにログインします。
2. 左側のパネルで、Support > Browse Filesの順に移動します。
3. 次のフォルダに移動します。sw > today > logs
4. sw.logファイルをクリックしてローカルマシンにダウンロードし、テキストエディタで開きます。

5. ログの下部で次の行を検索します。この要約は5分ごとに作成されます。

```
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
```



注：行8は、最終期間のテンプレートデータが不十分だったために廃棄されたフローがあることを示しています。

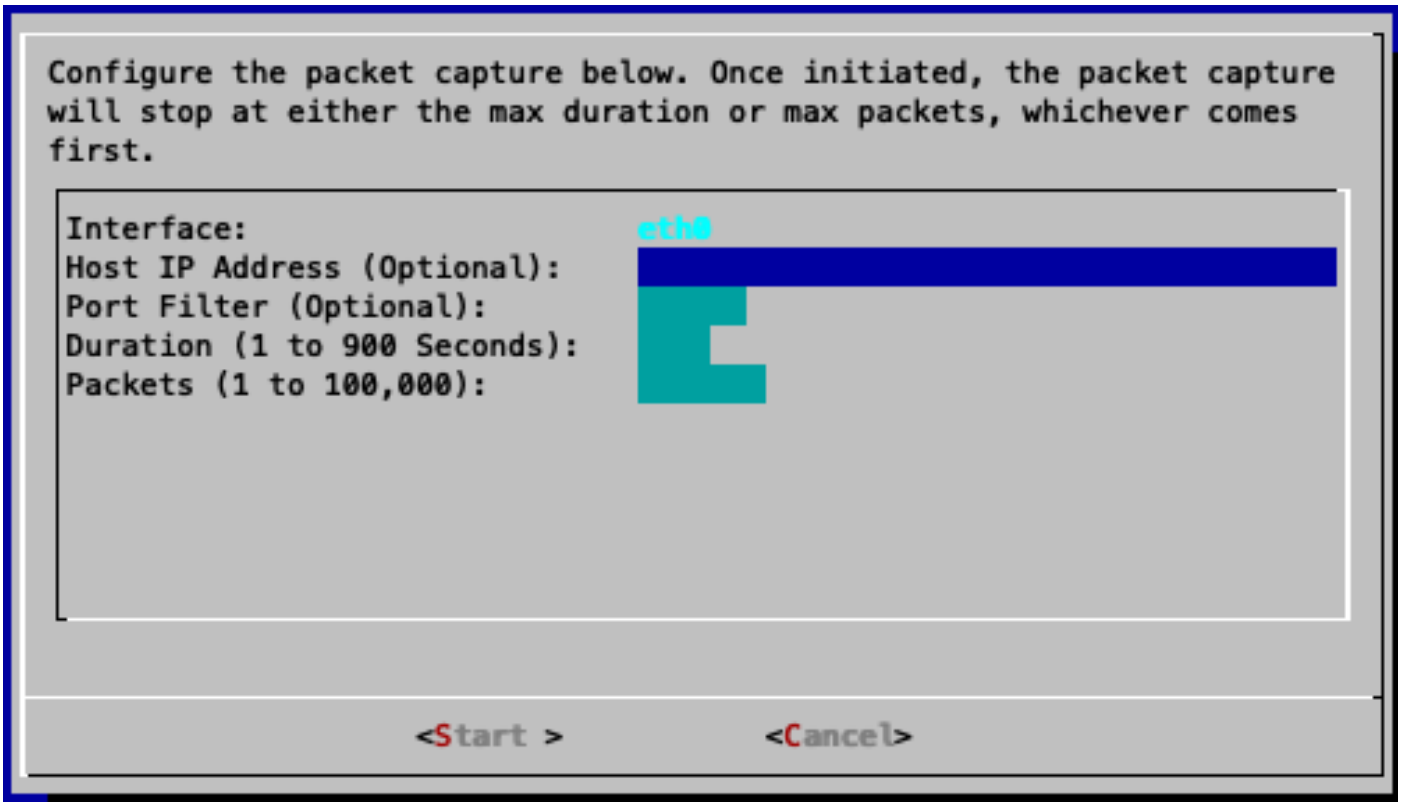
NetFlow/IPFIXテンプレートの確認

NetfFlow/IPFIXテンプレートに含まれるフィールドを確認するには、次の手順を実行します。

1. sysadminクレデンシャルを使用してSNAフローコレクタCLIにログインします。

2. SystemConfigメニューから、Advanced > Packet Captureに移動します。

3. SNA上のフローを表示していないエクスポータの情報を入力します。



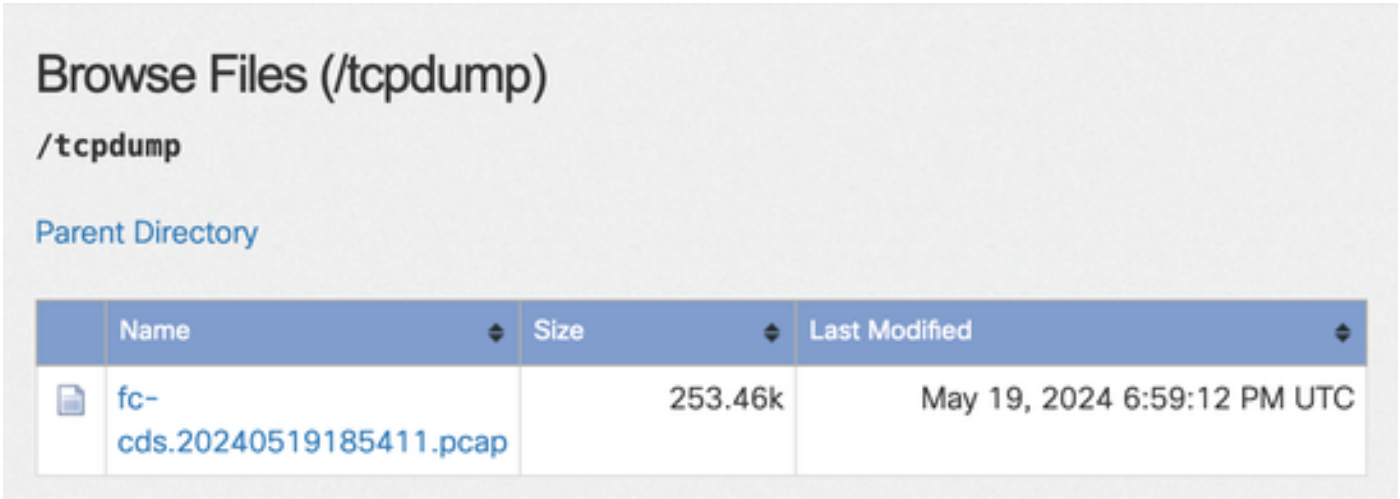
4. 処理が完了するまで待ちます。

5. ファイルをダウンロードするには、次の管理者クレデンシャルを使用してSNAフローコレクタ管理UIにログインします：https://<フローコレクタIPアドレス>/swa/login.html

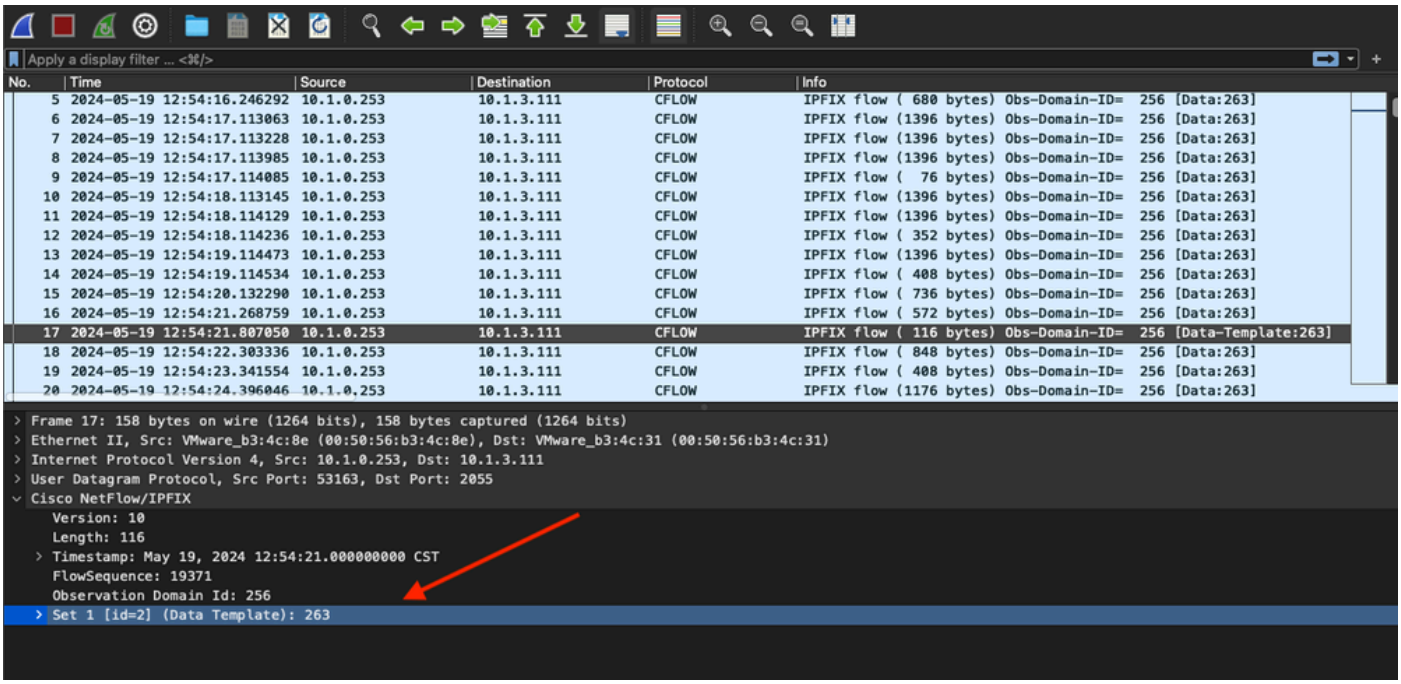
6. 左側のパネルで、Support > Browse Filesの順に移動します。

7. 次のフォルダに移動します：tcpdump

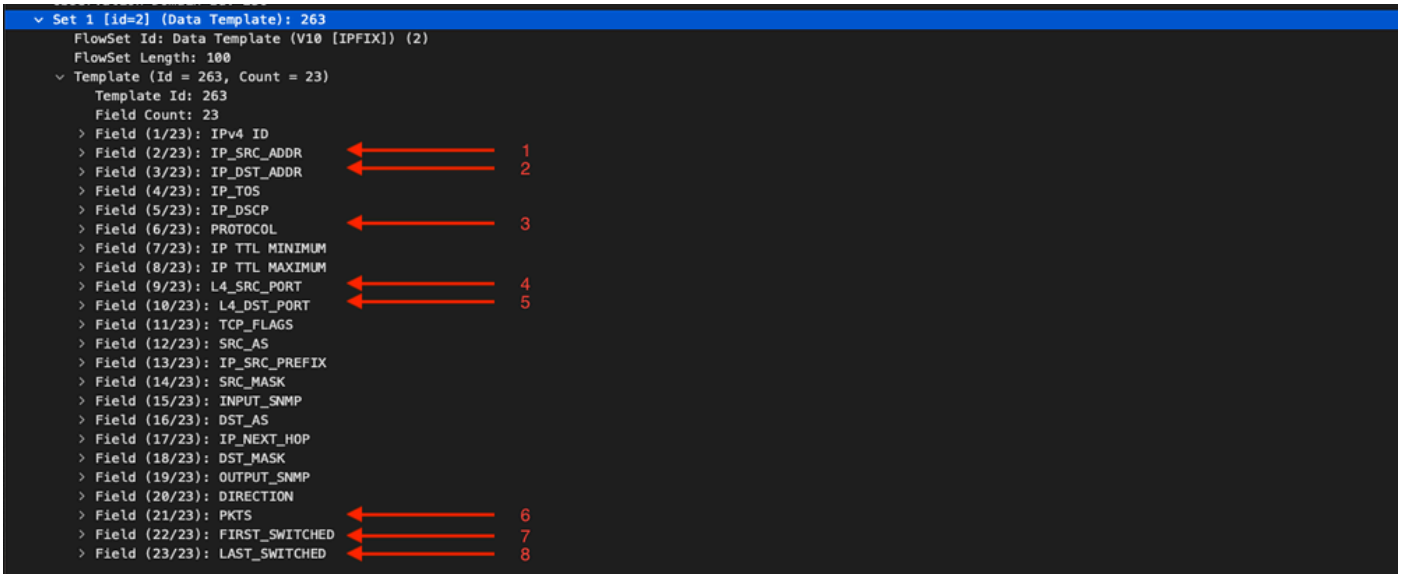
8. パケットキャプチャファイルをクリックしてローカルマシンにダウンロードし、Wiresharkで開きます。

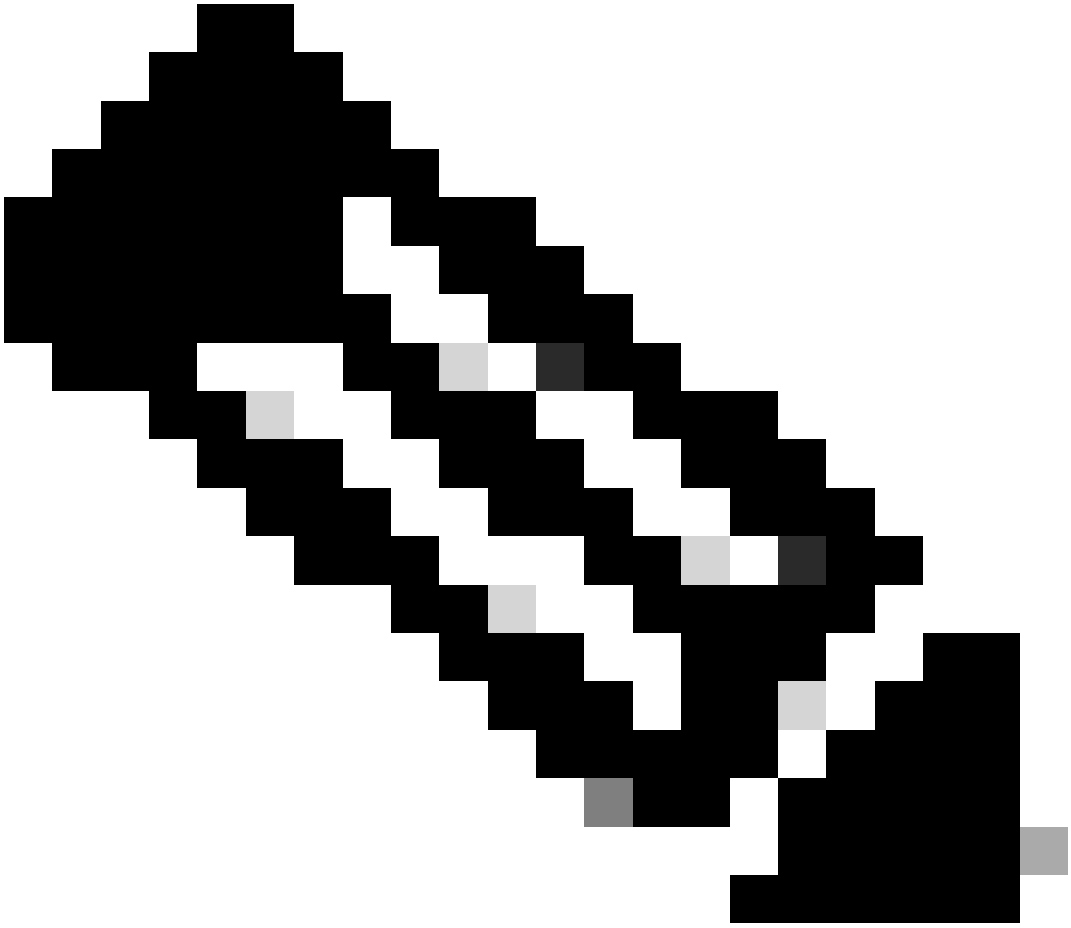


9. NetFlow/IPFIXテンプレートが受信されたフレームを識別します。



10. テンプレートに9つの必須フィールドが表示されていることを検証します





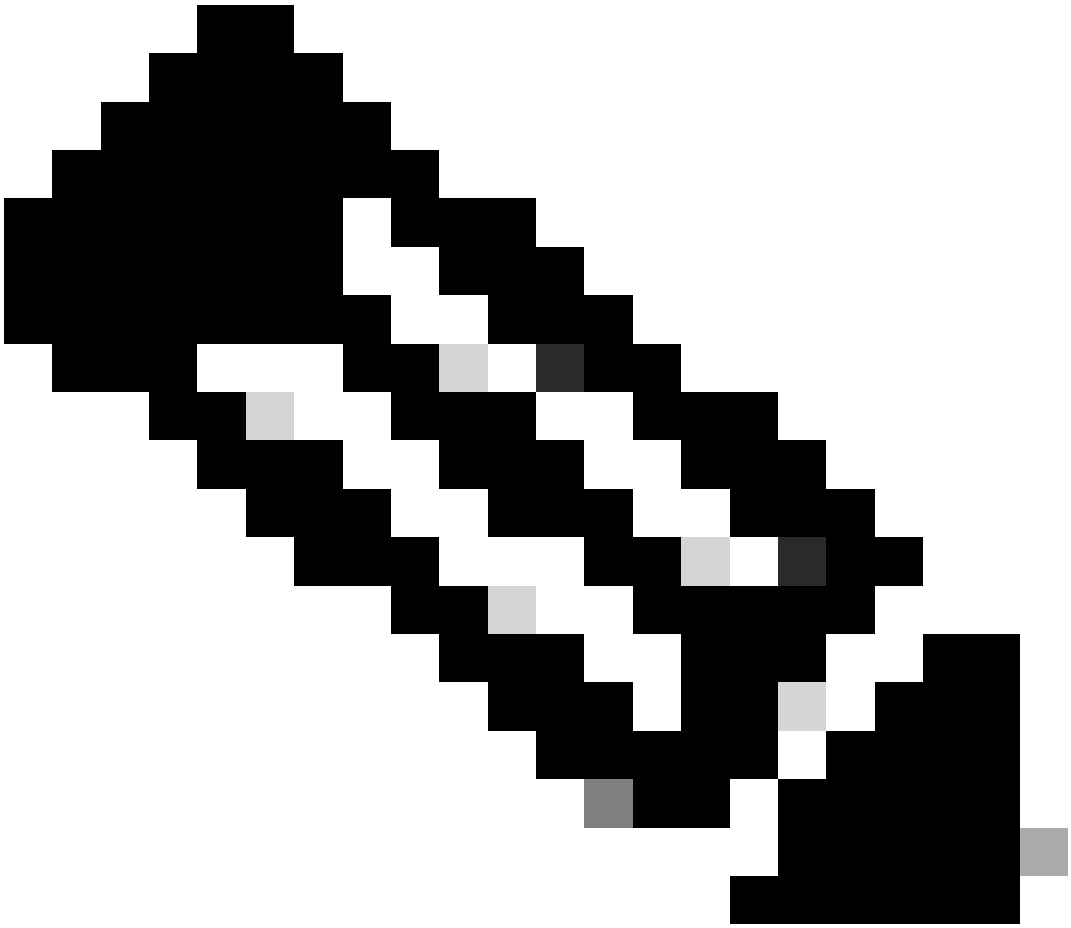
注：テンプレートには、テレメトリ取り込みに必要な9つの必須フィールドのうち8つしかありません。このシナリオでは、BYTESフィールドがありません。

欠落しているフィールドを追加した後のNetFlow/IPFIXテレメトリインジェストの確認

SNA Flow Collectorが変更後にエクスポータからNetFlow/IPFIXテレメトリを受信して挿入するかどうかを確認するには、次の手順を実行します。

1. 管理者クレデンシャル(https://<Flow Collector IP Address>/swa/login.html)を使用してSNAフローコレクタ管理UIにログインします。
2. 左側のパネルで、Support > Browse Filesの順に移動します。
3. 次のフォルダに移動します。sw > today > logs
4. sw.logファイルをクリックしてローカルマシンにダウンロードし、テキストエディタで開きます。
5. ログの下部で次の行を検索します

```
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
```



注：行8は、最終期間に廃棄されたフローがないことを示しています。

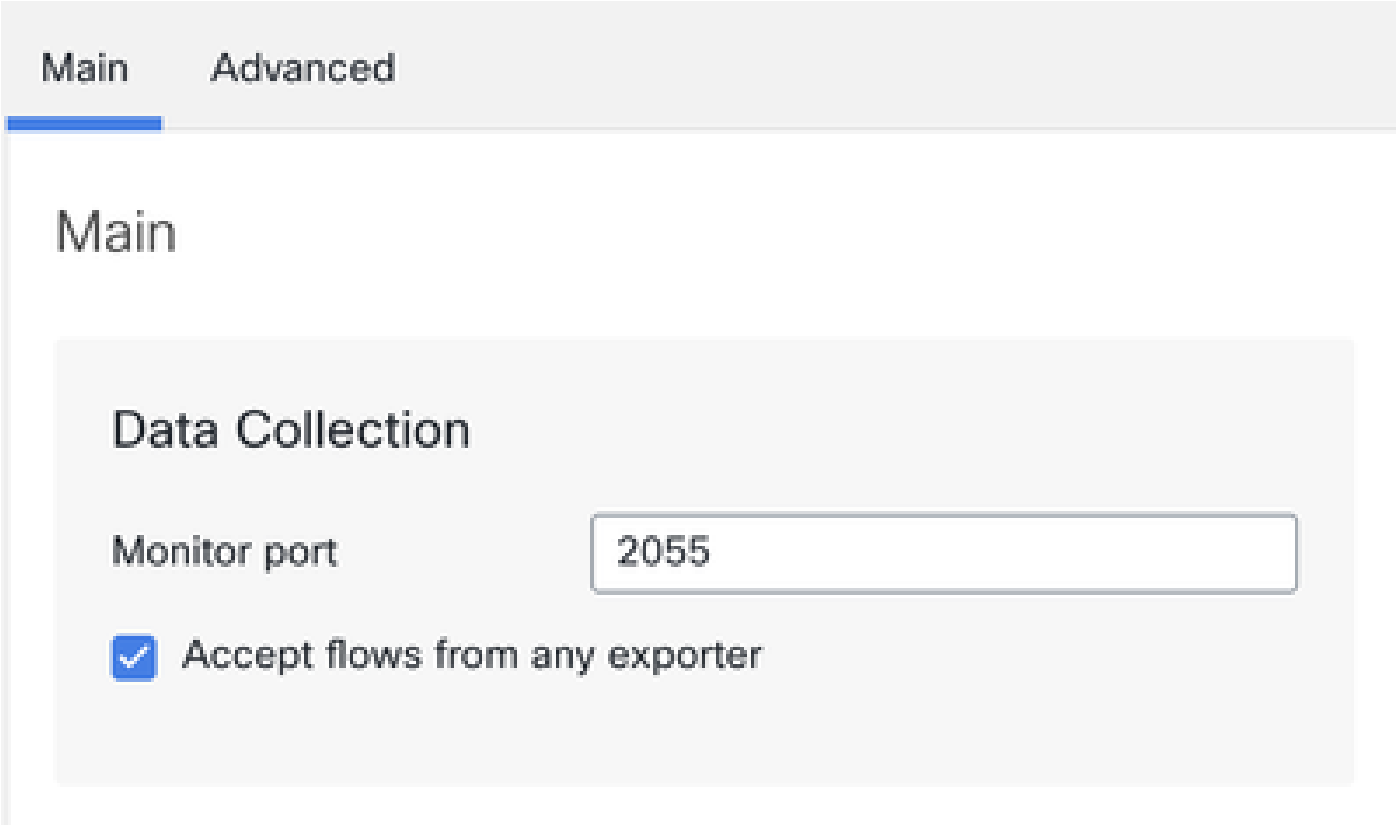
NetFlow/IPFIXテレメトリ取り込みポートの確認

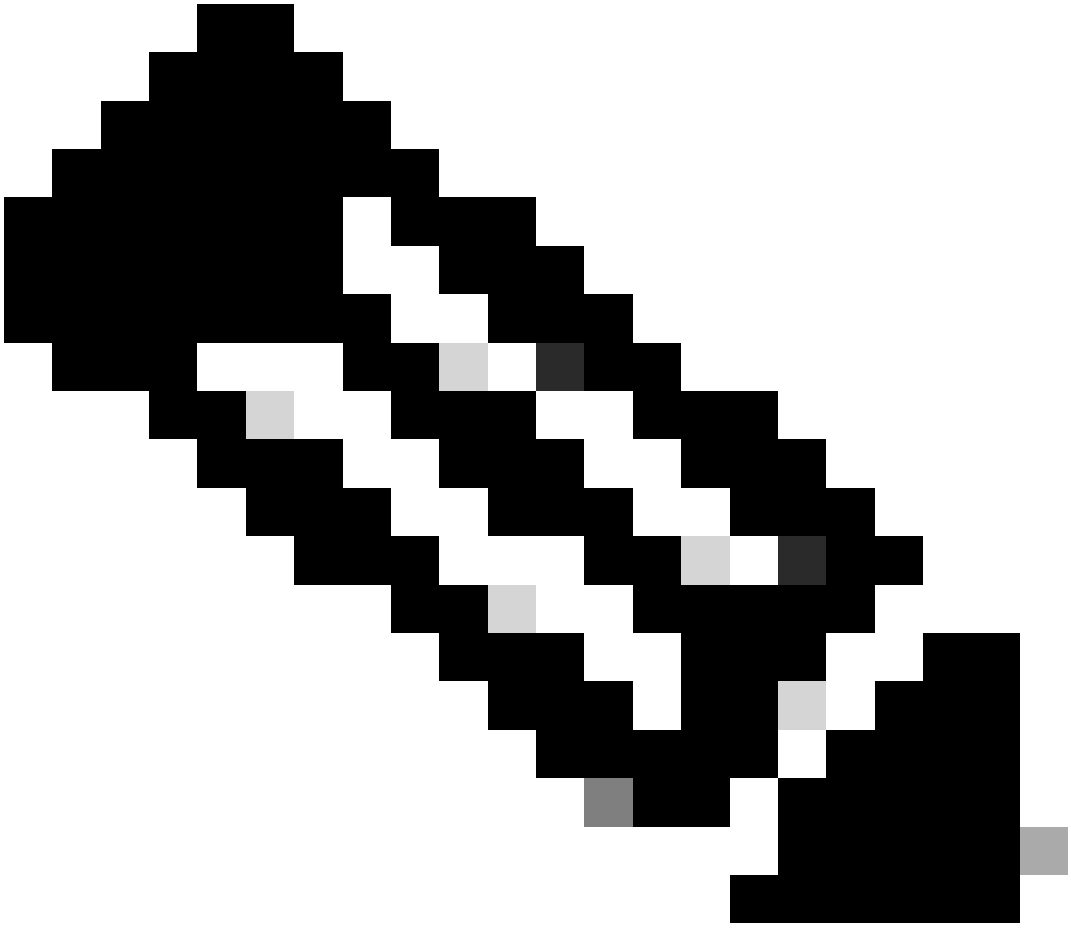
SNA Flow Collectorが正しいポートでエクスポータからNetFlow/IPFIXテレメトリを受信しているかどうかを確認するには、次の手順を実行します。

1. 管理者権限を持つユーザでSNA Web UIにログインします。

2. トップ・メニューで、「構成」にナビゲートし、「フロー・コレクタ」を選択します

3. SNAフローコレクタが、エクスポータがNetFlow/IPFIXを送信するように設定したポートと同じポートを使用していることを確認します。





注:NetFlowのデフォルトポートは2055ですが、別のポートを選択することもできます。Flow Collectorでの初回セットアッププロセスでは、必ず同じポートを使用してください。

NetFlow/IPFIX Telemetry Ingest NetFlowオプションが有効になっていることを確認します。

NetFlow/IPFIXのテレメトリ取り込みに対するSNAフローコレクタオプションが有効かどうかを確認するには、次のコマンドを実行します。

1. 管理者クレデンシャル(https://<Flow Collector IP Address>/swa/login.html)を使用してSNAフローコレクタ管理UIにログインします。
2. 左側のパネルで、Support > Advanced Settingsの順に移動します。
3. オプションenable_netflowが1に設定されていることを確認します。

関連情報

- 詳細については、Technical Assistance Center(TAC)にお問い合わせください。 有効なサポート契約が必要です。シスコワールドワイドサポートの連絡先です。
- また、Cisco Security Analyticsコミュニティもご覧ください。
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。