أستكشاف أخطاء NetFlow/IPFIX Telemetry وإصلاحها في تحليلات الشبكة الآمنة

المحتويات

المقدمة

المتطلبات الأساسية

المتطلبات

أدلة التكوين

المكونات المستخدمة

معلومات أساسية

القيود المعلومة

عملية أستكشاف الأخطاء وإصلاحها

التحقق من تطبيق Telemetry لتتبع NetFlow/IPFIX

التحقق من قالب NetFlow/IPFIX

التحقق من NetFlow/IPFIX Telemetry بعد إضافة الحقل (الحقول) المفقودة

التحقق من منفذ NetFlow/IPFIX Telemetry Est

التحقق من تمكين خيار NetFlow/IPFIX Telemetry NetFlow

معلومات ذات صلة

المقدمة

يوضح هذا المستند كيفية أستكشاف أخطاء NetFlow Telemetry وإصلاحها في تحليلات الشبكة الآمنة (SNA).

المتطلبات الأساسية

- معرفة Cisco SNA
- معرفة NetFlow/IPFIX

المتطلبات

- تحليلات الشبكة الآمنة في 7.5.0 أو أحدث
- مجمع التدفق في 7.5.0 أو أحدث
- CLI منفذ ك sysadmin إلى مجمع التدفق
- وصول Admin UI كمسؤول إلى مجمع التدفق

أدلة التكوين

- تكوين NetFlow/IPFIX ل Telemetry Est على تحليلات الشبكة الآمنة

المكونات المستخدمة

- مدير SNA مجمع التدفق على 7.5.0
- برنامج Wireshark

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

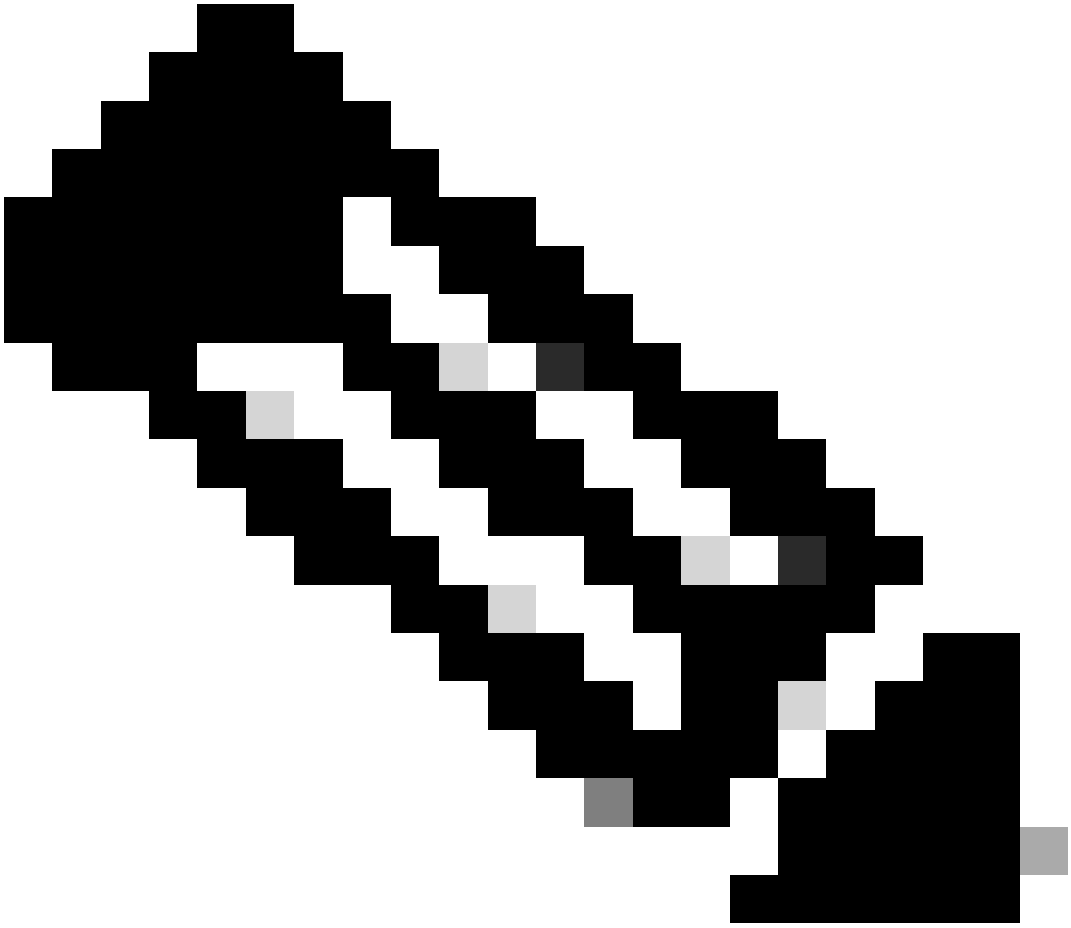
معلومات أساسية

مجمع التدفق هو جهاز SNA مسؤول عن تجميع تدفقات الشبكة ومعالجتها وتخزينها التي يتم إرسالها إلى تحليلات الشبكة الآمنة. بالنسبة للإصدار 9 من NetFlow أو IPFIX، يمكن تضمين عدة حقول على قالب NetFlow/IPFIX لإضافة مزيد من المعلومات المتعلقة بحركة مرور الشبكة، ومع ذلك، هناك 9 حقول محددة يجب تضمينها في قالب NetFlow/IPFIX لمجمع التدفق لمعالجة هذه التدفقات. الـ يقوم "مجمع التدفق" بمعالجة التدفقات الواردة التي تتضمن قالبا غير صالح، لذلك الـ يعرض SNA معلومات تدفق هؤلاء المصدرين ضمن واجهة مستخدم ويب أو عميل سطح المكتب.

الحقول المطلوبة

يجب تضمين الحقول التالية في قالب NetFlow/IPFIX لتطبيق TeleEmetry. تأكد من تضمين هذه الحقول التسعة في قالب NetFlow/IPFIX، من أجل تحليلات الشبكة الآمنة لمعالجة التدفقات الواردة.

- عنوان IP المصدر
- غاية عنوان IP
- منفذ المصدر
- غاية ميناء
- بروتوكول الطبقة 3
- عدد وحدات البايت
- عدد الحزم
- وقت بدء التدفق
- وقت انتهاء التدفق



> ملاحظة: يمكن تضمين المزيد من الحقول في تكوين NetFlow/IPFIX، ومع ذلك، فإن الحقول السابقة هي الحد الأدنى من متطلبات تحليلات الشبكة الآمنة ل Telemetry Ingest.

عملية أستكشاف الأخطاء وإصلاحها

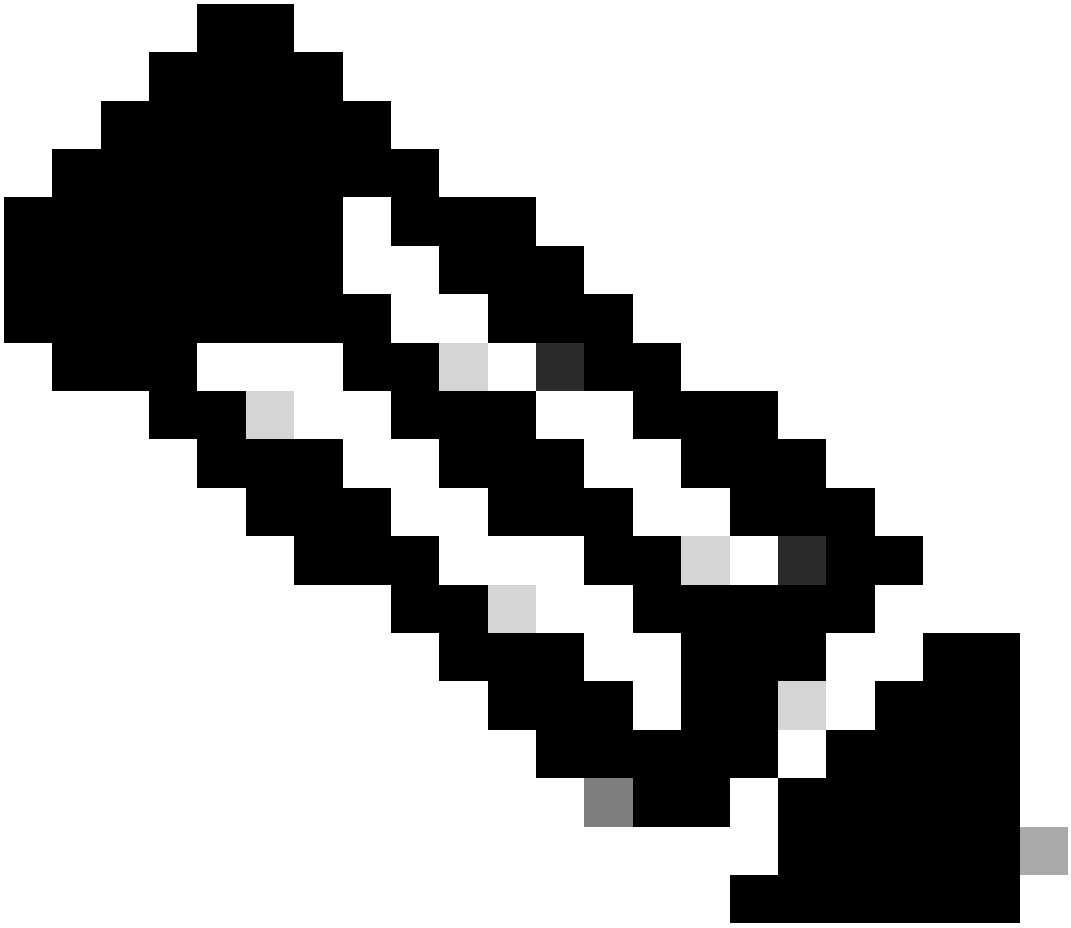
التحقق من تطبيق Telemetry لتتبع NetFlow/IPFIX

لتأكيد ما إذا كان مجمع تدفق SNA يستقبل بيانات تتبع NetFlow/IPFIX ويدرجها من المصدرين:

1. سجل الدخول إلى واجهة مستخدم إدارة مجمع تدفق SNA باستخدام بيانات اعتماد المسؤول: https://<flow collector عنوان>/swa/login.html
2. في اللوحة اليسرى، تصفح إلى الدعم > تصفح الملفات
3. انتقل إلى المجلد التالي: sw > اليوم > السجلات
4. انقر فوق ملف sw.log لتنزيله إلى الجهاز المحلي وافتحه على محرر نصوص.

5. ابحث عن هذه السطور في أسفل السجل، ويتم إنشاء هذا الملخص كل خمس دقائق:

```
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
```



ملاحظة: يشير السطر 8 إلى أنه تم تجاهل التدفقات بسبب عدم كفاية بيانات القالب في الفترة الأخيرة.

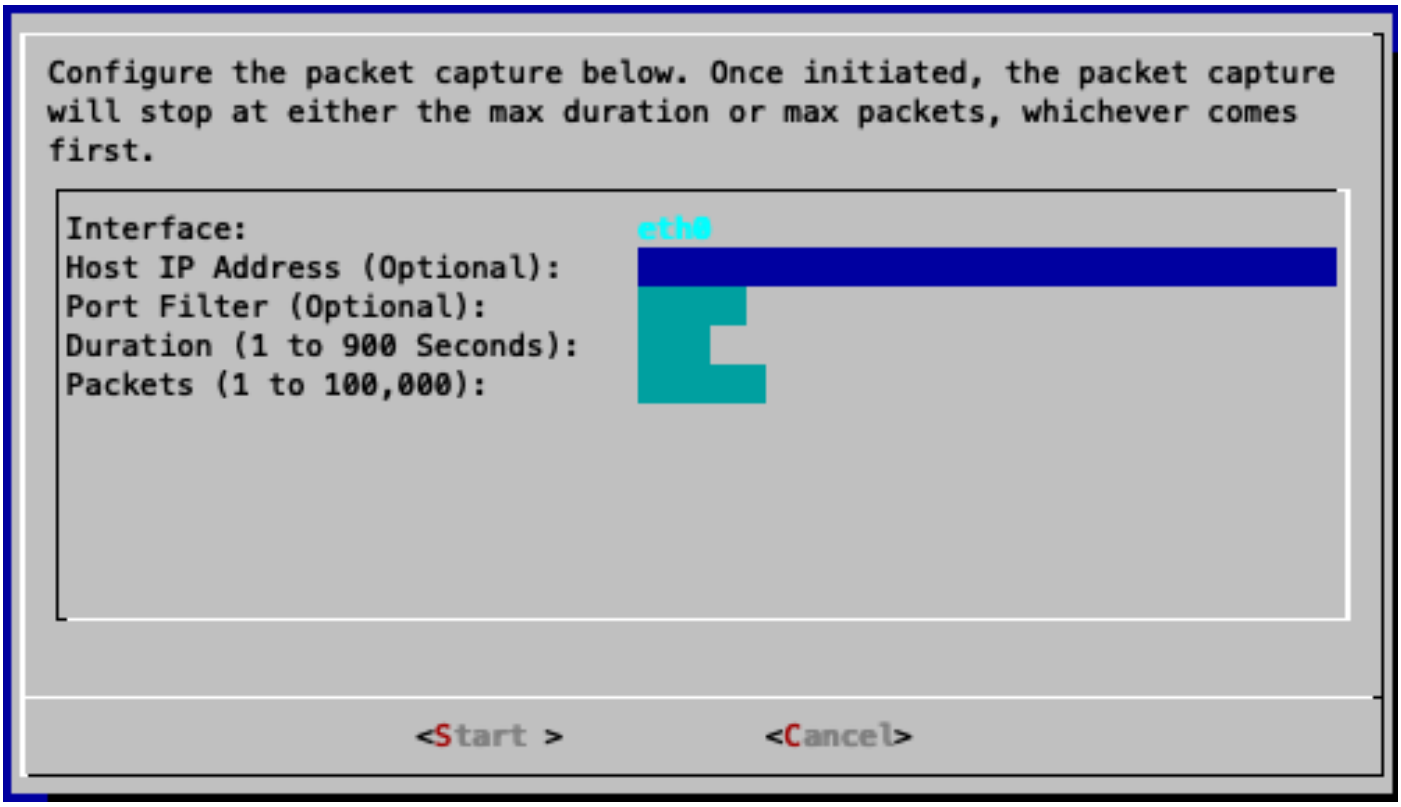
التحقق من قالب NetFlow/IPFIX

لتأكيد الحقول المضمنة في قالب NetFlow/IPFIX:

1. سجل الدخول إلى واجهة سطر الأوامر لمجمع تدفق SNA باستخدام بيانات اعتماد sysadmin.

2. في قائمة SystemConfig، انتقل إلى: متقدم > التقاط الحزمة

3. أدخل معلومات المصدر التي تظهر التدفقات على SNA:



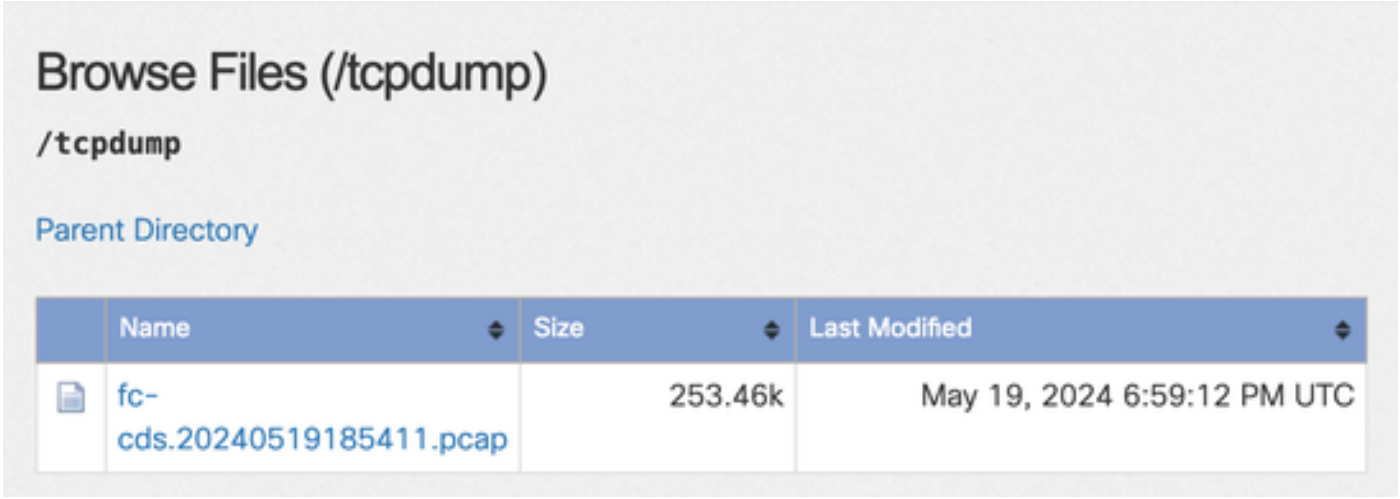
4. انتظر حتى اكتمال العملية.

5. لتنزيل الملف، قم بتسجيل الدخول إلى واجهة مستخدم مسؤول مجمع تدفق SNA باستخدام بيانات اعتماد المسؤول: https://<flow collector عنوان>/swa/login.html

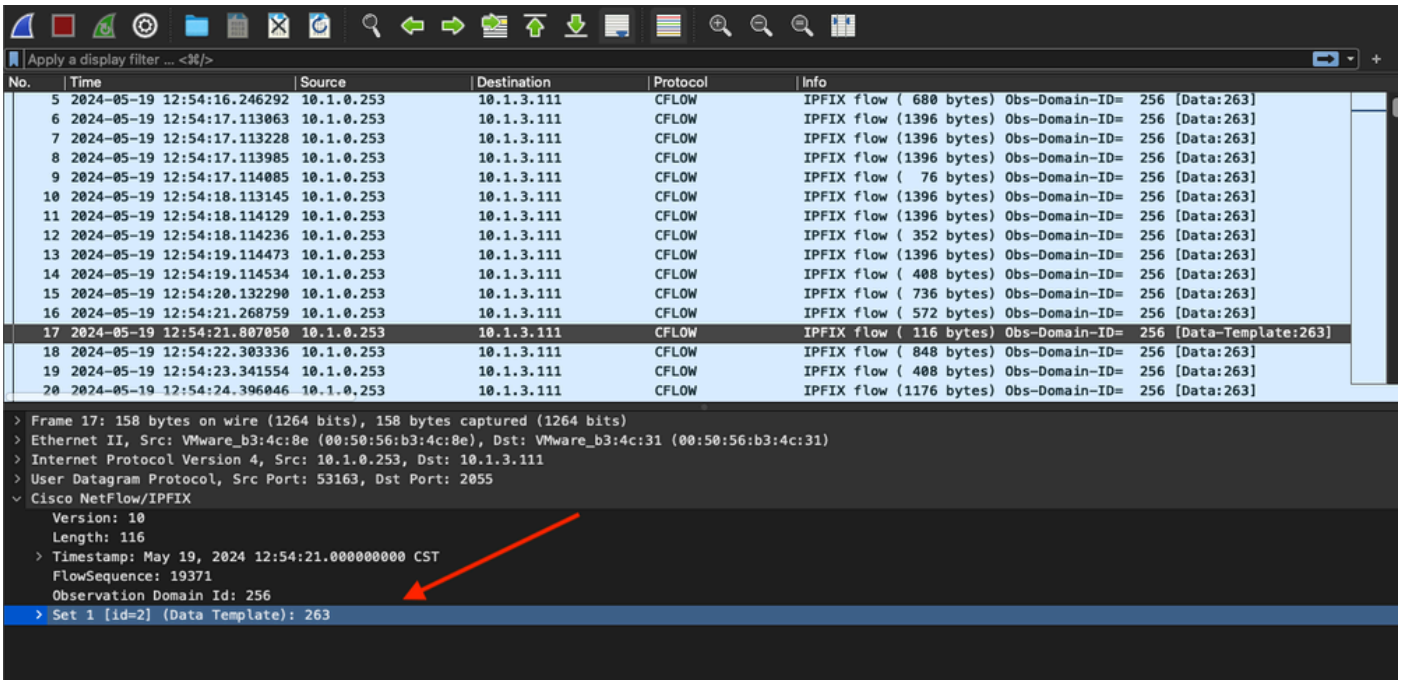
6.على اللوحة اليسرى، انتقل إلى الدعم > تصفح الملفات

7. انتقل إلى المجلد التالي: tcpdump

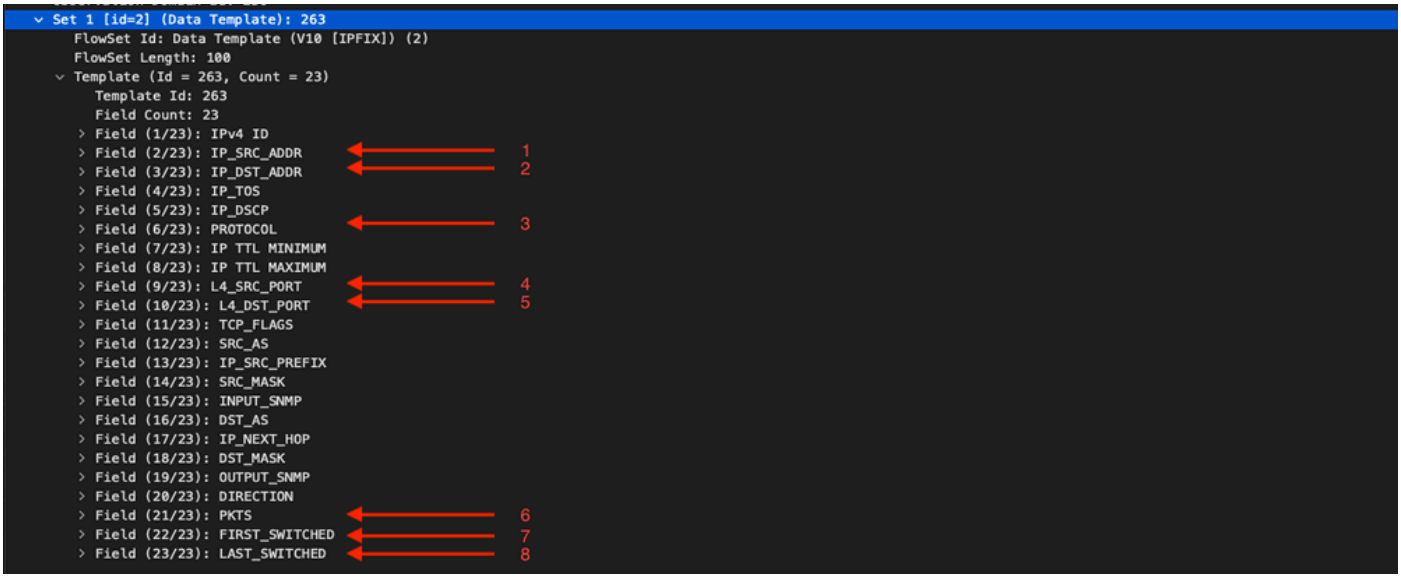
8. انقر فوق ملف التقاط الحزمة لتنزيله إلى جهازك المحلي وفتحه على Wireshark:

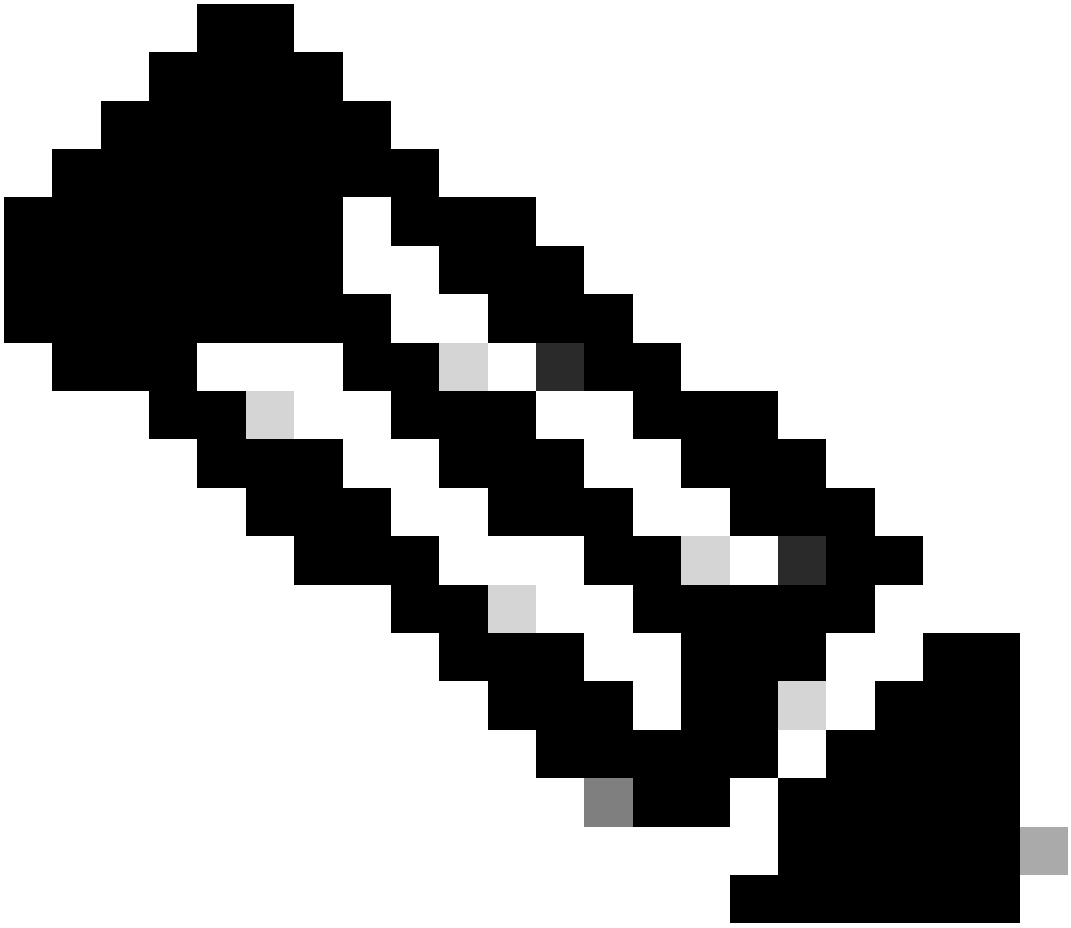


9. التعرف على الإطار الذي تم إستلام قالب NetFlow/IPFIX فيه.



10. تحقق من أن الحقول التسعة المطلوبة تظهر على القالب





ملاحظة: لاحظ أنه يوجد على القالب 8 فقط من الحقول الإلزامية ال 9 التي يتطلبها SNA ل TeleEmetry، لهذا السيناريو، حقل وحدات البايت مفقود.

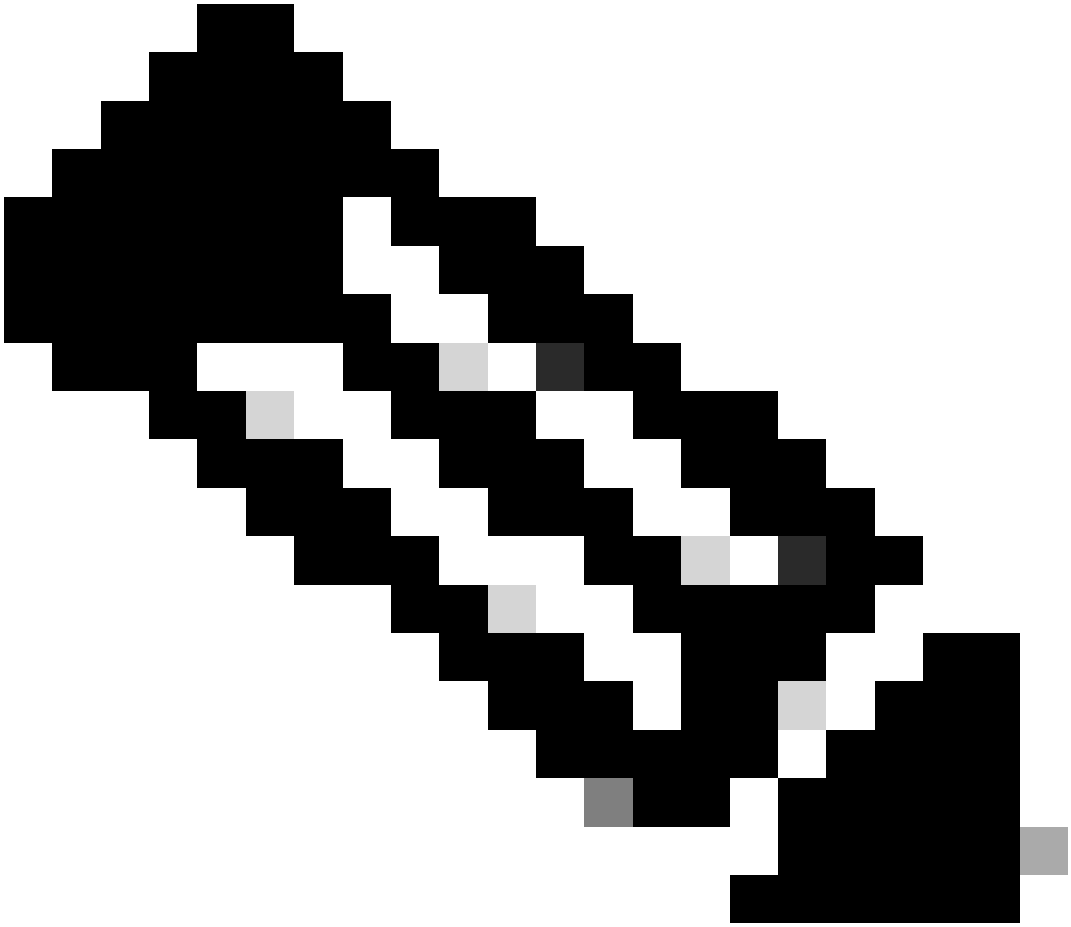
التحقق من NetFlow/IPFIX Telemetry بعد إضافة الحقل (الحقول) المفقودة

لتأكيد ما إذا كان مجمع تدفق SNA يستلم بيانات تتبع NetFlow/IPFIX ويدرجها من المصدر بعد التغيير:

1. سجل الدخول إلى واجهة مستخدم إدارة مجمع تدفق SNA باستخدام بيانات اعتماد المسؤول: https://<flow collector عنوان>/swa/login.html
2. في اللوحة اليسرى، تصفح إلى الدعم > تصفح الملفات
3. انتقل إلى المجلد التالي: sw > اليوم > السجلات
4. انقر فوق ملف sw.log لتنزيله إلى الجهاز المحلي وافتح في محرر نصي.
5. ابحث عن هذه السطور في أسفل السجل

```
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
```



ملاحظة: يشير السطر 8 إلى عدم وجود تدفقات مهملة في الفترة الأخيرة.

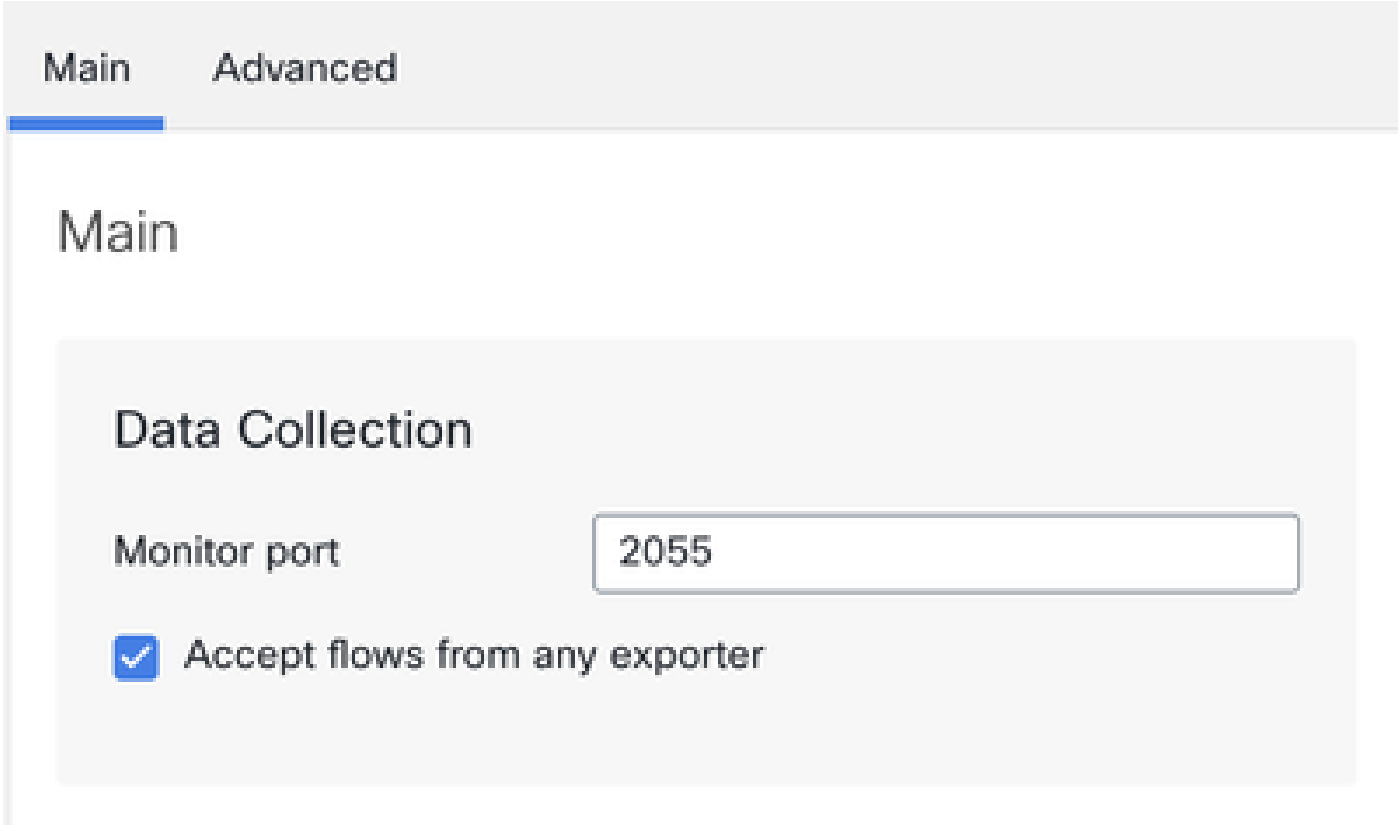
التحقق من منفذ NetFlow/IPFIX Telemetry Est

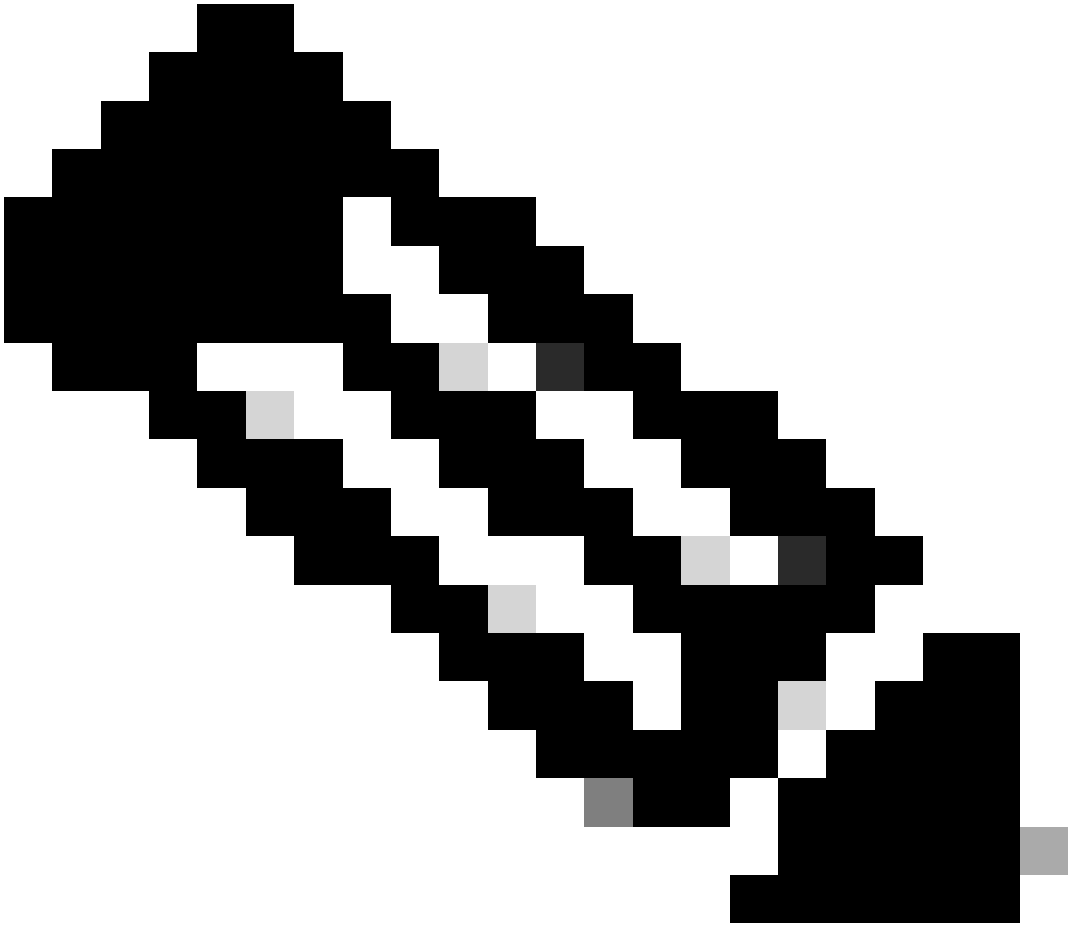
لتأكيد ما إذا كان مجمع تدفق SNA يستقبل تتبع NetFlow/IPFIX من المصدرين على المنفذ الصحيح:

1. سجل الدخول إلى واجهة مستخدم ويب SNA باستخدام مستخدم لديه أذونات المسؤول.

2. في القائمة العليا، انتقل إلى تكوين أدوات تجميع التدفق واختر هذه الأدوات

3. تأكد من أن مجمع تدفق SNA يستخدم نفس المنفذ الذي قام المصدرون بتكوينه لإرسال NetFlow/IPFIX





ملاحظة: المنفذ الافتراضي ل NetFlow هو 2055، ومع ذلك يمكنك تحديد منفذ آخر، يرجى التأكد من إستخدام نفس المنفذ أثناء عملية إعداد المرة الأولى على مجمع (مجمعات) التدفق.

التحقق من تمكين خيار NetFlow/IPFIX Telemetry NetFlow

لتأكيد ما إذا كان خيار مجمع تدفق SNA للقياس عن بعد في NetFlow/IPFIX ممكنا:

1. سجل الدخول إلى واجهة مستخدم إدارة مجمع تدفق SNA باستخدام بيانات اعتماد المسؤول: https://<flow collector عنوان>/swa/login.html
2. في اللوحة اليسرى، انتقل إلى الدعم > الإعدادات المتقدمة
3. تأكد من أن الخيار enable_netflow تم تعيينه على 1:

enable_netflow	1 ←	☐

معلومات ذات صلة

- للحصول على مساعدة إضافية، يرجى الاتصال بمركز المساعدة التقنية (TAC). يلزم عقد دعم صالح: جهات اتصال الدعم العالمية من Cisco.
- يمكنك أيضا زيارة مجتمع تحليلات الأمان من Cisco هنا.
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).