

NetFlow/IPFIX Telemetry ءاطخأ فاشك تسأ ةنمآلا ةكبشلا تاليلحت يف اهالصل او

تايوتحمل

[ةمدقملا](#)

[ةيساسالاب لطلتلا](#)

[تاب لطلتلا](#)

[نيوكتلا ةلدأ](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[قبولطملا لوفحل](#)

[اهالصل او ءاطخألا فاشك تسأ ةيلمع](#)

[NetFlow/IPFIX عبتتل Telemetry قيبطت نم ققحتلا](#)

[NetFlow/IPFIX بلاق نم ققحتلا](#)

[ةدوقفملا \(لوفحل\) لقحلا ةفاضلا دعب NetFlow/IPFIX Telemetry نم ققحتلا](#)

[NetFlow/IPFIX Telemetry Est ذفنم نم ققحتلا](#)

[NetFlow/IPFIX Telemetry NetFlow راخ نيكم نم ققحتلا](#)

[ةلصل تاذا تامولعم](#)

ةمدقملا

تاليلحت يف اهالصل او NetFlow Telemetry ءاطخأ فاشك تسأ ةيفيك دنتسملا اذه حضوي (SNA) ةنمآلا ةكبشلا

ةيساسالاب لطلتلا

- Cisco SNA ةفرعم
- NetFlow/IPFIX ةفرعم

تاب لطلتلا

- شحأ وأ 7.5.0 يف ةنمآلا ةكبشلا تاليلحت
- شحأ وأ 7.5.0 يف قفدتلا عمجم
- قفدتلا عمجم ىلا sysadmin ك ذفنم CLI
- قفدتلا عمجم ىلا لوؤسمك Admin UI لوصو

نيوكتلا ةلدأ

- [ةنمآلا ةكبشلا تاليلحت ىلع NetFlow/IPFIX ل Telemetry Est نيوكت](#)

ةمدختسملا تانوكملا

- 7.5.0 ىلع قفدتال عمجم SNA ري دم
- Wireshark جم انرب

ةصاخ ةي لمعم ةئي ب ي ف ةدوجومال ةزهجال نم دنتسمال اذه ي ف ةدراول تامولعمل عاشنإ مت تناك اذا .(يضا رتفا) حوسمم نيوكتب دنتسمال اذه ي ف ةمدختسُمل ةزهجال عيمج تادب رما يأل لمحتمل ريثأتلل كمهف نم دكأتف ،ليغشتال دي قكتكبش

ةيساسأ تامولعم

يتال اهنيزخت واهتجالعمو ةكبشلل تاقفدت عيمجت نع لوؤسم SNA زاهج وه قفدتال عمجم نكمي ،IPFIX أو NetFlow نم 9 رادصلل ةبسنبلا ب .ةنمآلا ةكبشلل تاليلحت ىلإ اهلاسرا متي ةكرحب ةقلعتمل تامولعمل نم ديزم ةفاضل NetFlow/IPFIX بلال ىلع لوقح ةدع نيضت عمجل NetFlow/IPFIX بلال ي ف اهنيمضت بجي ةددحم لوقح 9 كانه ،كلذعمو ،ةكبشلل رورم يتال ةدراول تاقفدتال ةجالعمب "قفدتال عمجم" موقى ال .تاقفدتال هذه ةجالعمل قفدتال ةهجاو نمض ني ردصملا ءالؤه قفدت تامولعم SNA ضرعي ال كلذل ،حلص ريغ بلال نمضتت بتكمال حطس لي مع وأ بي و مدختسم

ةبولطمال لوقحال

نم دكأت .TeleEmetry قي بطتل NetFlow/IPFIX بلال ي ف ةيلاتل لوقحال نيضت بجي ةنمآلا ةكبشلل تاليلحت لجأ نم ،NetFlow/IPFIX بلال ي ف ةعستل لوقحال هذه نيضت ةدراول تاقفدتال ةجالعمل

- ردصم ال IP ناو نع
- IP ناو نع ةياغ
- ردصم ال ذفنم
- ءانيم ةياغ
- 3 ةقبطال لوكوتورب
- تيابل تادحو ددع
- مزحل ددع
- قفدتال ادب تقو
- قفدتال ءاهتنا تقو



نإف ،كلذ عمو ،NetFlow/IPFIX نيوكت يف لوقحل نم ديزملا نيضت نكمي :ةظحالم
Telemetry ل ةنمآلا ةكبشل تاليلحت تابلطتم نم ىندألا دحل يه ةقباسلا لوقحل
Ingest.

اهحالصإو ءاطخألا فاشكتسا ةيلمع

NetFlow/IPFIX عبتتل Telemetry قيبطت نم ققحتلا

نم اهجرديو NetFlow/IPFIX عبتت تانايب لبقتسي SNA قفدت عمجم ناك اذا ام ديكأتل
نيردصل:

1. دامتعا تانايب مادختساب SNA قفدت عمجم قراد مدختسم ةهجاو ىل لوخدلا لفس
لؤؤسملا : <https://swa/login.html> <ناونع flow collector>
2. تافللمل حفصت > معدلا ىل حفصت ،ىرسىلا ةحولل ي ف
3. تالفسلا > مويلا > sw :ىلاتلا دلجملا ىل لقنتا
4. صوصن ررحم ىل عحتفاو يلفلملا زاهجلا ىل هليزنتل sw.log فلم قوف رقنا

قئاقءء سمء لك صءلمء اءء ءاشنء مءءو؁ لءسءلء فءسأء ف روءسءلء هءء نع ءءبء 5.

```
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
```



تانايب ةيافك مدع ببسب تاقفدتلا لهاجت مت هنأ إلى 8 رطسلا ريشي: ةظحالم
ةريخألا ةرتفلا في بلالقا

NetFlow/IPFIX بلالقا نم ققحتلا

NetFlow/IPFIX بلالقا في ةنمضمملا لوقحلا ديكأتلا

1. sysadmin دامتعا تانايب مادختساب SNA قفدت عمجمل رماوأل رطس ةهجاو إلى لوخدلا لجس.
2. ةمزحلا طاققتلا > مدقتم: إلى لقتنا، SystemConfig ةمئاق في
3. SNA: إلى تاقفدتلا رهظت اليتلا ردصملا تامولعم لخدأ.

Configure the packet capture below. Once initiated, the packet capture will stop at either the max duration or max packets, whichever comes first.

Interface:	eth0
Host IP Address (Optional):	
Port Filter (Optional):	
Duration (1 to 900 Seconds):	
Packets (1 to 100,000):	

<Start > <Cancel>

4. ةللمعمل لامتكا ىتح رظتنا.

5. SNA قفدت عمجم لوؤسم مدختسم ةهجاو ىلإ لوخدلا لىجستب مق ، فلمل لىزننل
ل: https://<flow_collector>swa/login.html ةاناي ب مادختساب

6. تافلمل حفصت > معدلا ىلإ لقتنا ، ىرسىل ةحولل ىلع.

7. tcpdump :ىلالت دلجملا ىلإ لقتنا

8. Wireshark: ىلع هحتفو ىلحملا كزاهج ىلإ هلىزننل ةمزل طاقنل فلم قوف رقنا:

Browse Files (/tcpdump)			
/tcpdump			
Parent Directory			
	Name	Size	Last Modified
	fc-cds.20240519185411.pcap	253.46k	May 19, 2024 6:59:12 PM UTC

9. هىف NetFlow/IPFIX بلاق مالتسا مت ىذل راطلإا ىلع فرعتل.

Apply a display filter ... <=>

No.	Time	Source	Destination	Protocol	Info
5	2024-05-19 12:54:16.246292	10.1.0.253	10.1.3.111	CFLOW	IPFIX flow (680 bytes) Obs-Domain-ID= 256 [Data:263]
6	2024-05-19 12:54:17.113063	10.1.0.253	10.1.3.111	CFLOW	IPFIX flow (1396 bytes) Obs-Domain-ID= 256 [Data:263]
7	2024-05-19 12:54:17.113228	10.1.0.253	10.1.3.111	CFLOW	IPFIX flow (1396 bytes) Obs-Domain-ID= 256 [Data:263]
8	2024-05-19 12:54:17.113985	10.1.0.253	10.1.3.111	CFLOW	IPFIX flow (1396 bytes) Obs-Domain-ID= 256 [Data:263]
9	2024-05-19 12:54:17.114085	10.1.0.253	10.1.3.111	CFLOW	IPFIX flow (76 bytes) Obs-Domain-ID= 256 [Data:263]
10	2024-05-19 12:54:18.113145	10.1.0.253	10.1.3.111	CFLOW	IPFIX flow (1396 bytes) Obs-Domain-ID= 256 [Data:263]
11	2024-05-19 12:54:18.114129	10.1.0.253	10.1.3.111	CFLOW	IPFIX flow (1396 bytes) Obs-Domain-ID= 256 [Data:263]
12	2024-05-19 12:54:18.114236	10.1.0.253	10.1.3.111	CFLOW	IPFIX flow (352 bytes) Obs-Domain-ID= 256 [Data:263]
13	2024-05-19 12:54:19.114473	10.1.0.253	10.1.3.111	CFLOW	IPFIX flow (1396 bytes) Obs-Domain-ID= 256 [Data:263]
14	2024-05-19 12:54:19.114534	10.1.0.253	10.1.3.111	CFLOW	IPFIX flow (408 bytes) Obs-Domain-ID= 256 [Data:263]
15	2024-05-19 12:54:20.132290	10.1.0.253	10.1.3.111	CFLOW	IPFIX flow (736 bytes) Obs-Domain-ID= 256 [Data:263]
16	2024-05-19 12:54:21.268759	10.1.0.253	10.1.3.111	CFLOW	IPFIX flow (572 bytes) Obs-Domain-ID= 256 [Data:263]
17	2024-05-19 12:54:21.807050	10.1.0.253	10.1.3.111	CFLOW	IPFIX flow (116 bytes) Obs-Domain-ID= 256 [Data-Template:263]
18	2024-05-19 12:54:22.303336	10.1.0.253	10.1.3.111	CFLOW	IPFIX flow (848 bytes) Obs-Domain-ID= 256 [Data:263]
19	2024-05-19 12:54:23.341554	10.1.0.253	10.1.3.111	CFLOW	IPFIX flow (408 bytes) Obs-Domain-ID= 256 [Data:263]
20	2024-05-19 12:54:24.396046	10.1.0.253	10.1.3.111	CFLOW	IPFIX flow (1176 bytes) Obs-Domain-ID= 256 [Data:263]

> Frame 17: 158 bytes on wire (1264 bits), 158 bytes captured (1264 bits)

> Ethernet II, Src: VMware_b3:4c:8e (00:50:56:b3:4c:8e), Dst: VMware_b3:4c:31 (00:50:56:b3:4c:31)

> Internet Protocol Version 4, Src: 10.1.0.253, Dst: 10.1.3.111

> User Datagram Protocol, Src Port: 53163, Dst Port: 2055

> Cisco NetFlow/IPFIX

Version: 10

Length: 116

> Timestamp: May 19, 2024 12:54:21.000000000 CST

FlowSequence: 19371

Observation Domain Id: 256

> Set 1 [id=2] (Data Template): 263

بالاقول الى رهظت ةبولطم ال ةستال لوقحل ال نا نم ققحت 10.

> Set 1 [id=2] (Data Template): 263

FlowSet Id: Data Template (V10 [IPFIX]) (2)

FlowSet Length: 100

> Template (Id = 263, Count = 23)

Template Id: 263

Field Count: 23

> Field (1/23): IPv4 ID

> Field (2/23): IP_SRC_ADDR

> Field (3/23): IP_DST_ADDR

> Field (4/23): IP_TOS

> Field (5/23): IP_DSCP

> Field (6/23): PROTOCOL

> Field (7/23): IP TTL MINIMUM

> Field (8/23): IP TTL MAXIMUM

> Field (9/23): L4_SRC_PORT

> Field (10/23): L4_DST_PORT

> Field (11/23): TCP_FLAGS

> Field (12/23): SRC_AS

> Field (13/23): IP_SRC_PREFIX

> Field (14/23): SRC_MASK

> Field (15/23): INPUT_SNMP

> Field (16/23): DST_AS

> Field (17/23): IP_NEXT_HOP

> Field (18/23): DST_MASK

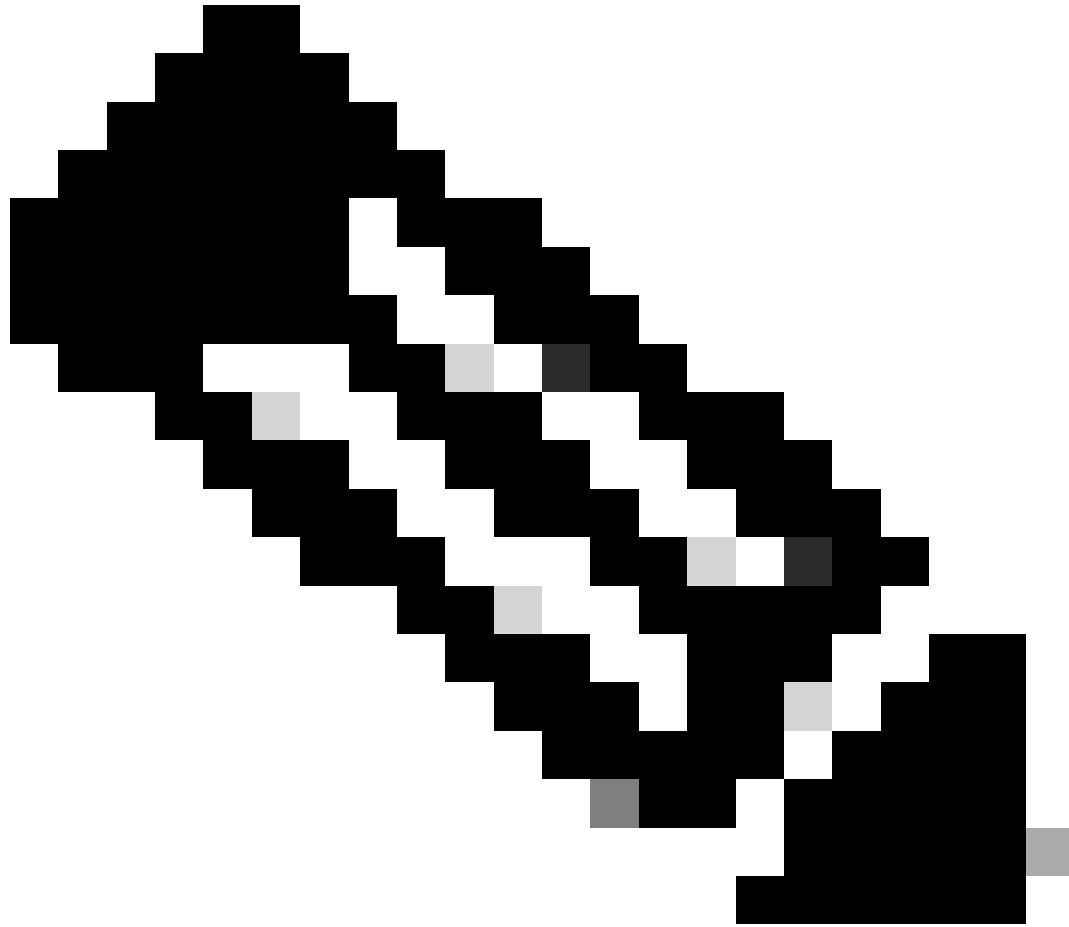
> Field (19/23): OUTPUT_SNMP

> Field (20/23): DIRECTION

> Field (21/23): PKTS

> Field (22/23): FIRST_SWITCHED

> Field (23/23): LAST_SWITCHED



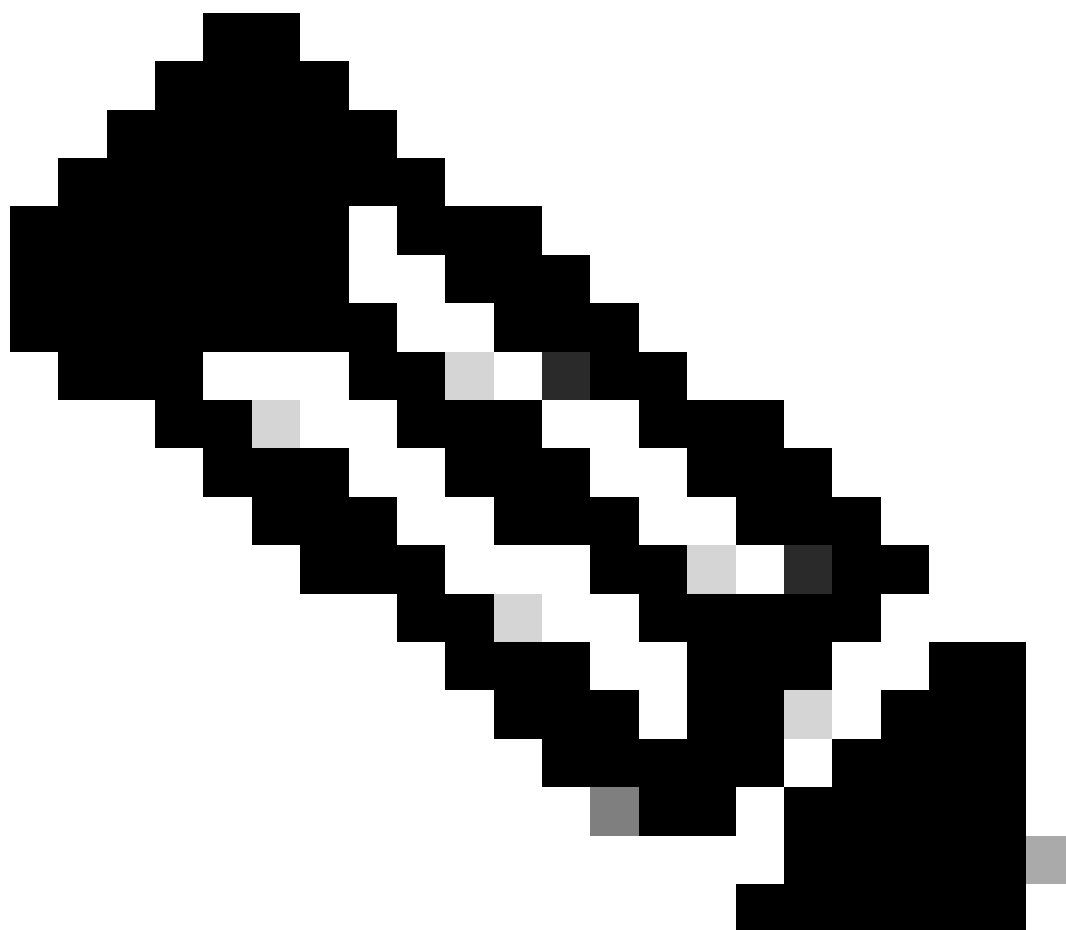
اهبلطتي يتي ال 9 ل اةيمازلإل لوقح ال نم طقف 8 بلالقل ىلع دجوي هنا طحال :ةطحال م
دوقفم تيابل تادحو ل قح ،ويرانيسل اذهل ،SNA ل TeleEmetry

ةدوقفم ال (لوقح ال) ل قح ال ةفاضل دعب NetFlow/IPFIX Telemetry نم ققحت ال

ردصم ال نم اهجرديو NetFlow/IPFIX عبتت تانايب ملتسي SNA قفدت عمجم ناك اذا ام ديكأتل
رييغت ال دعب :

1. دامتعا تانايب مادختساب SNA قفدت عمجم ةراد مدختسم ةهجاو ىل لوخدل ل جس
ل وؤسم ال : <https://swa/login.html> <ناونع flow collector>
2. تافل ملل حفصت > معدل ىل حفصت ، ىرسل ال ةحولل ي ف
3. تال جسل > مويل > sw : لال ال دلجمل ال ىل ل قتنا
4. ىصن ررحم ي ف حت فاو يل حمل ال زاهج ال ىل هل يزنتل sw.log فلم قوف رقنا
5. ل جسل لفسأ ي ف روطسل ال هذ نع ثحبا

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



ةريخألا ةرتفلا يف ةلمهم تاقفدت دوجو مدع ىلإ 8 رطسلا ريشي :ةطحالم

NetFlow/IPFIX Telemetry Est ذفنم نم ققحتلا

ىلع نيردصملا نم NetFlow/IPFIX عبتت لبقتسي SNA قفدت عمجم ناك اذا ام ديكأتل
حيحصلا ذفنملا:

1. لوؤسملا تانوذا هيدل مدختسم مادختساب SNA بيو مدختسم هجاو ىلا لوخدلا لجس.
2. تاودالا هذه رتخاو قفدتلا عيمجت تاودا نيوكت ىلا لقتنا ،ايلا عمئاقلا يف.
3. هنيوكتب نوردصملا ماق يذلا ذفنملا سفن مدختسي SNA قفدت عمجم نا نم دكأت
NetFlow/IPFIX لاسرلا

Main

Advanced

Main

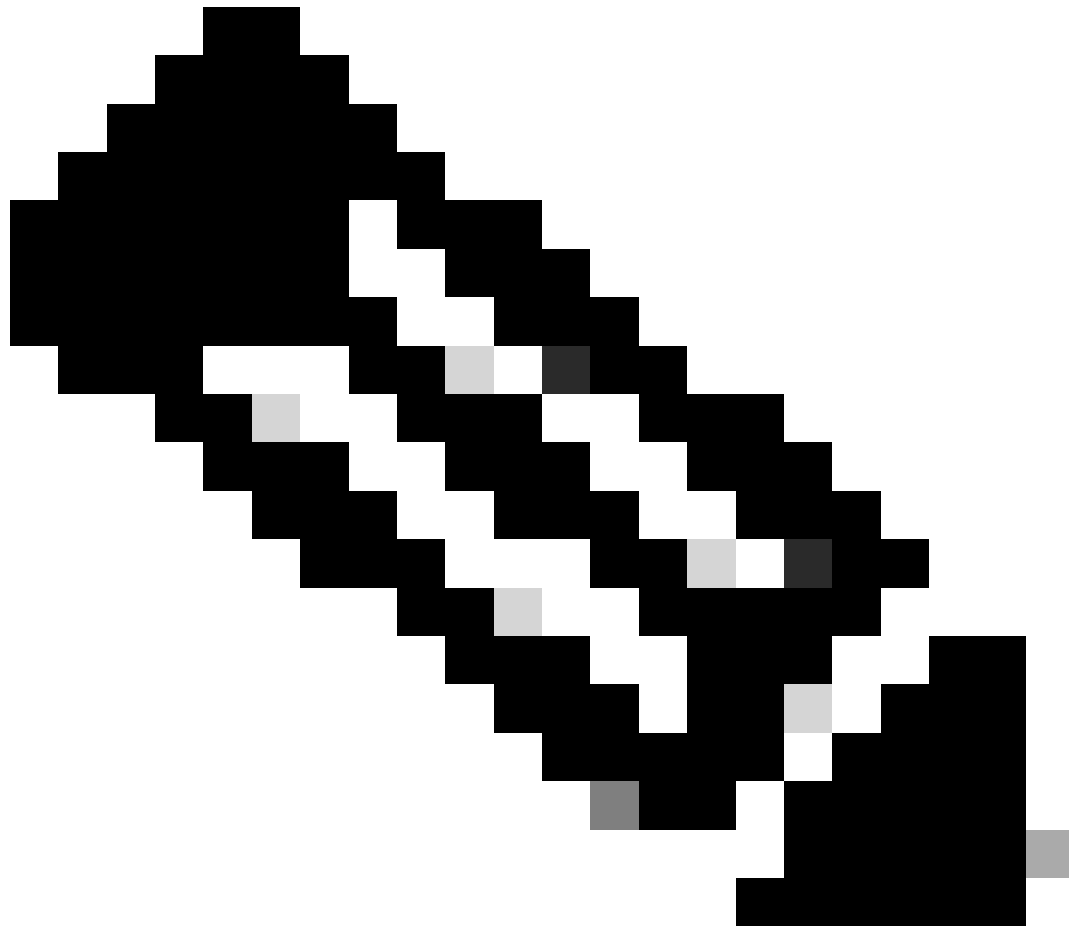
Data Collection

Monitor port

2055



Accept flows from any exporter



رځ، آ ذفنم ديدحت كننكمي كلذ عمو، 2055 وه NetFlow ل يضارت فالال ذفنم ال: ةطحال م
عمجم يلعل لوالال ةرمل دادعلا ةيلمع ءانثا ذفنم ال سفن مادختسا نم دكأتلا ىجري
قفدتلا (تاعجم).

NetFlow/IPFIX Telemetry NetFlow راځ ني كمت نم ققحتلا

انكمم NetFlow/IPFIX في دعب نع سايق لل SNA قفدت عمجم راځ ناك اذا ام ديكأتلا

1. دامتعا تانايب مادختساب SNA قفدت عمجم ةرادا مدختسم ةهجاو ىلا لوخدلا لچس
ل: <https://swa/login.html> [ناونع](https://flow_collector) flow_collector
2. ةمدقتملا تادادعلا > معدلا ىلا لقتنا، ىرسىلا ةحوللا في
3. 1: ىلعل هنييغت مت enable_netflow راځلا نا نم دكأت.

enable_netflow

1



ةلص تاذا تامولعم

- مزلي (TAC) ةينقتلا ةدعاسملا زكرمب لاصتالايچري، ةيفاضا ةدعاسم ىلع لوصحلل
- [Cisco](#) نم ةيملاعلا معدلا لاصتا تاهج: حلاص معد دقع
- [Cisco](#) ينه نامألا تاليلحت عم تجم ةرايز اضيأ كنكمي
- [Cisco Systems](#) - تادنتسم لاوي نقتلا معدلا

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا