

اهحال صإو SNMP عالطتسا إاطخأ فاشكتسا SNA سلع ةححصلا ريرغ ةهجال لاصافتو

تايوت حمل

[ةمدقملا](#)

[ةيساس الابلطت ملا](#)

[تابلطت ملا](#)

[ةمدختس ملا تانوك ملا](#)

[تانويوت ملا](#)

[ةيساس تامولعم](#)

[اهحال صإو عاطخأ ال فاشكتسا](#)

[ةححص ريرغ ةهجالو عامسا](#)

[نودوقف ملا نيردص ملا وأ تاهجالو](#)

[لاصتالا تالكشم](#)

[نيردص ملا صحف سلع \(SMC\) ريدم قردق ةحص نم ققحت ملا](#)

[نيردص ملا صإو ال IP ناو نع مادختسا اب SMC سلع ةمزح طاقت ملا عايشنا ب مق](#)

[SNMP قيقدت تادادعا ةحص نم ققحت ملا](#)

[رشابم لكشب اهحال صإو SNMP عارتقا عاطخأ فاشكتسا](#)

[رخأ زاغ نم SNMP عالطتسا راب تخا](#)

[ةلص تاذا تامولعم](#)

ةمدقملا

اهحال صإو ةدوقف ملا ردص ملا ةهجالو تامولعم عاطخأ فاشكتسا ةيفيك دنتس ملا اذه حضوي
ةنم ال ةكبشلا تاليلحت يف

ةيساس الابلطت ملا

- عالطتسا (SNMP) لوكوتورب ةرادا ةكبش طيسب يساسا تنأ يقولتي نأ ي صوي Cisco ةفرعم
- ةنم ال ةكبشلا ليلحتل ةيساسا ةفرعم دوجوب Cisco ي صوت (SNA/StealthWatch)

تابلطت ملا

- ثدحا وأ 7.4.1 رادص ال يف SNA ريدم
- ثدحا وأ 7.4.1 رادص ال يف SNA قفدت عمم
- طشن لكشب SNA سلع NetFlow لسري ردص ملا

ةمدختس ملا تانوك ملا

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجالو نم دنتس ملا اذه يف ةدراولا تامولعملا عايشنا مت

تنانك اذى (يضا رتفا) حوسم نيوكتب دن تسملا اذى ف ةمدختس مل ازه جال ا عي مج تادب رما يال لمحتم ل ريثا تلل كمهف نم دكأتف ، ليغشتل دي قكتك ب ش

- شدا واً 7.4.1 رادصال ا ي ف SNA ري دم
- شدا واً 7.4.1 رادصال ا ي ف SNA قفدت عمجم
- جم انرب SNMPwalk
- كراش ري و تا ي جم رب

تان يوكتلا

- نيوكت نمضتي اذو . SNMP لوصوب حامسل ل نيردصم ل نيوكت ب جي : زاه جال نيوكت ف م كحتل مئ او قو ، SNMP عم تجم لسال س دادع ك لذ ي ف امب ، زاه ج ل ك لى ع SNMP تاداع ا هم ادختس ا متيس ي ذل ا SNMP رادصا دي دحتو ، (ACLs) لوصول ا نيكمت متي ، نيردصم ل ج جان ل نيوكتل دن ع : SNA لى ع SNMP عالطتس ا نيوكت اقبسم اهن ي عت مت تام ل عم مادختس اب SMC لى ع يضا رتفا ل ك شب SNMP عالطتس ا لسال س لثم ، نيردصم ل اب قلع تمل ا ةبولطم ل لى صافتل ا ريفوت ةياغل ل م هم ل نم ةي ل ل م مع نامضل ، (SNMP) طيس ب ل تاك ب ش ل ا ةراد ا لوكتورب صوصنو SNMP عم تجم لثم ا ل وحن ل ا لى ع عارتقال

ةيساس ا تامول عم

ضرع لى ع ةردق ل ا بناج ، ةه جاولا ةلا ح نع ةلماش ريراقت ريفوت لى ع ةردق ل اب SNA عت متي عمجم لى ل طشن ل ك شب NetFlow تان ا ي ب ل اسراب نومو قى نى ذل ا نيردصم ل ل ةه جاولا عامسا "تاه جاولا -> قى قحتل ا" ةمئاق لى ل ل قننل ا لال ح نم هذه ةه جاولا لى صافت ضرع نكمي . قفدت "ةرادال" بى و مدختسم ةه جاولا نم

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 |

اه جال صا و ا طاخ ا ل فاش كتسا

ةحى حص ريغ ةه جاولا عامسا

نيردصم ل ا ه جاولا عم قفاوتى ال ي ذل ا "ifindex-#" هؤاشن ا مت ي ذل ا ريرقتل ا ضرع ةلا ح ي ف . هسفن ردصم ل ا لى ع واً SMC لى ع ام ا SNMP عارتقا عم ةلمتحم نيوكت ةلكشم حرتقى هن ا ف ةراد ا لوكتورب عالطتس اب قلع تمل ا ةحضا و ةلكشم لى ع عوضال ا تطل س ، لاثم ل اذى ف نى عم ردصم ل (SNMP) طيس ب ل تاك ب ش ل ا

Interfaces (152)

Filter by Device

Interface Status (Since Reset Hour)

| INTERFACE | EXPORTER | CURRENT UTILIZATION | CURRENT TRAFFIC | MAXIMUM UTILIZATION | MAX TRAFFIC | DIRECTION | SPEED |
|--------------------------|--------------|---------------------|-----------------|---------------------|-------------|-----------|--------|
| ifindex-5 | | 90.93% | 909.27 Mbps | 162.76% | 1.63 Gbps | INBOUND | 1 Gbps |
| ifindex-8 | | 85.71% | 857.08 Mbps | 85.71% | 857.08 Mbps | OUTBOUND | 1 Gbps |
| ifindex-26 | | 85.71% | 857.08 Mbps | 85.71% | 857.08 Mbps | INBOUND | 1 Gbps |
| ifindex-3 | | 80.46% | 804.6 Mbps | 82.07% | 820.69 Mbps | INBOUND | 1 Gbps |
| ifindex-25 | | 79.06% | 790.63 Mbps | 80.29% | 802.94 Mbps | OUTBOUND | 1 Gbps |
| ifindex-16 | | 79.06% | 790.63 Mbps | 80.29% | 802.94 Mbps | INBOUND | 1 Gbps |
| ifindex-13 | | 53.29% | 532.87 Mbps | 94.85% | 948.5 Mbps | OUTBOUND | 1 Gbps |
| ifindex-24 | | 53.29% | 532.87 Mbps | 94.85% | 948.5 Mbps | INBOUND | 1 Gbps |
| ifindex-0 | | 0.43% | 4.29 Mbps | 2.58% | 25.84 Mbps | OUTBOUND | 1 Gbps |
| TenGigabitEthernet1/0/38 | | 0.32% | 3.17 Mbps | 0.98% | 9.77 Mbps | INBOUND | 1 Gbps |
| ifindex-0 | | 0.13% | 1.28 Mbps | 0.37% | 3.66 Mbps | OUTBOUND | 1 Gbps |
| ifindex-0 | | 0.12% | 1.18 Mbps | 2.77% | 27.74 Mbps | OUTBOUND | 1 Gbps |
| GigabitEthernet1/0/1 | 192.168.99.4 | 0.1% | 1 Mbps | 0.32% | 3.19 Mbps | INBOUND | 1 Gbps |
| ifindex-0 | 192.168.99.2 | 0.06% | 573.21 Kbps | 1.29% | 12.92 Mbps | OUTBOUND | 1 Gbps |
| TenGigabitEthernet1/0/1 | 192.168.99.5 | 0.05% | 531.31 Kbps | 0.29% | 2.86 Mbps | INBOUND | 1 Gbps |
| TenGigabitEthernet1/0/37 | 192.168.99.1 | 0.05% | 503.01 Kbps | 2.02% | 20.15 Mbps | INBOUND | 1 Gbps |
| TenGigabitEthernet1/0/1 | 192.168.99.2 | 0.04% | 354.1 Kbps | 1.25% | 12.5 Mbps | INBOUND | 1 Gbps |

نودوقفملا نيردصملا و اتاهجاولا

هجو ىلعو NetFlow تانايب عجالعم قاييس يف قرىبك ةيمهأ بلالقا نم ققحتلا لمحى لوقحلا عي مج ىلع يوتحي ردصملا نم هلابقتسا مت يذلا NetFlow بلالقا نأ نمضي، ديدحتلا يف لشفلا يدؤي. قفدتلا عمجم ةطساوب حجان لكشب عجالعمل او زيمرتلا كفل ةبولطملا يدؤي امم، ريفشتلا كف نم ةنرتقملا تاقفدتلا ةعمجم داعبتسا ىلإ حلاص بلالقا ةهجاوم اتاهجاولا ةمئاق نم اهبايغ ىلإ.

نم ققحتلا كىل عيجي، اتاهجاولا ةمئاق يف ةعقوتملا اتاهجاولا/ردصملا كيدل رهظي مل اذا ىلع ةمزح طاققتلا ءاشنإ نكمي، NetFlow بلالقا نم ققحتلل. دراولا netFlow تانايب dn بلالقا "x.x.x.x": ريفيغتب هنم NetFlow ىلع لصحن يذلا ردصملا نم IP دحوي، قفدتلا عمجم بناج

- رذجال دامتعا تانايب مادختساب مكحتلا ةدحو و SSH ربع قفدتلا عمجم ىلإ لوخدلا لجس
- ينعمل NetFlow ذفنم و IP ردصملا نم ةمزح طاققتلا ليفشتب مق

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

.pcap

- مدختسا، Wireshark قيبطت تيثبت عم لمع ةطحم ىلإ، زاهجال نم ةمزحلا طاققتلا خسنا (SCP و SFTP: لاثملا لىبس ىلع) ةلضفملا كتقيرط
- اهل سرى يتلا تانايبلاو بلالقا نم ققحتلا و Wireshark مادختساب ةمزحلا طاققتلا حتف قفدتلا عمجم ىلإ ردصملا

| Date | Source | Destination | Protocol | Length | Info | Dist Port |
|-----------------|------------|-------------|----------|--------|--|-----------|
| 19:35:07.222163 | 10.10.10.1 | 10.10.10.2 | CFLOW | 182 | total: 3 (v9) records Obs-Domain-ID= 257 [Data-Template:2856] [Option... | |
| 19:35:07.222299 | 10.10.10.1 | 10.10.10.2 | CFLOW | 1416 | total: 27 (v9) records Obs-Domain-ID= 257 [Data:2856] | |
| 19:35:07.222377 | 10.10.10.1 | 10.10.10.2 | CFLOW | 1416 | total: 27 (v9) records Obs-Domain-ID= 257 [Data:2856] | |
| 19:35:07.222385 | 10.10.10.1 | 10.10.10.2 | CFLOW | 1416 | total: 27 (v9) records Obs-Domain-ID= 257 [Data:2856] | |
| 19:35:07.222388 | 10.10.10.1 | 10.10.10.2 | CFLOW | 1416 | total: 27 (v9) records Obs-Domain-ID= 257 [Data:2856] | |
| 19:35:07.222462 | 10.10.10.1 | 10.10.10.2 | CFLOW | 1416 | total: 27 (v9) records Obs-Domain-ID= 257 [Data:2856] | |

```

Frame 1: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits)
Ethernet II, Src: Cisco_94:b4:fc (8c:60:4f:94:b4:fc), Dst: VMware_84:49:4f (00:50:56:84:49:4f)
Internet Protocol Version 4, Src: 10.10.10.1, Dst: 10.10.10.2
User Datagram Protocol, Src Port: 23384, Dst Port: 2055
Cisco NetFlow/IPFIX
  Version: 9
  Count: 3
  SysUptime: 6981.285000000 seconds
  Timestamp: Jul 20, 2021 15:23:50.000000000 Eastern Daylight Time
  FlowSequence: 226153525
  SourceId: 257
  FlowSet 1 [id=0] (Data Template): 2856
    FlowSet Id: Data Template (V9) (0)
    FlowSet Length: 68
      Template (Id = 2856, Count = 15)
        Template Id: 2856
        Field Count: 15
        Field (1/15): BYTES
        Field (2/15): PKTS
        Field (3/15): OUTPUT_SNMP
        Field (4/15): IP_DST_ADDR
        Field (5/15): SRC_VLAN
        Field (6/15): IP_TOS
        Field (7/15): IPv4 ID
        Field (8/15): FRAGMENT_OFFSET
        Field (9/15): IP_SRC_ADDR
        Field (10/15): L4_DST_PORT
        Field (11/15): L4_SRC_PORT
        Field (12/15): PROTOCOL
        Field (13/15): FIRST_SWITCHED
  
```

قيقدل مسالا فلتيخي نأ نكمي و،ةبولطملا 9 لوقحل مدختسي NetFlow بلاق نأ نم ققحت ردمملا عونب ةصاخلا قئاتولا ةعجارم نم دكأتف، ردمملا عونل اقفو هذه بلاقلا لوقحل هنيوكتب موقت يذلا ددحملا

- ردمملا IP ناونع
- IP ناونع ةياغ
- ردمملا ذفنم
- ءانيم ةياغ
- ةبارلا ةقبطلالوكوتورب
- تيابلل تادحو ددع
- مزحلا ددع
- قفدتلا ءدب تقو
- قفدتلا ءاهتنا تقو

ةفاضا اضايا ءاجرلا، ححص لكشب تاهجالا ضرعل

- ةهجالا جرخ
- ةهجالا لخد

عاداً ردصم ىطعم نم طبر طاقاتلا بلاق لاثم انه

- ةبولطملا NetFlow لوقح :عارمحلل مهسألل
- ةارضخلل مهسألل SNMP لوقح :

```
> User Datagram Protocol, Src Port: 51431, Dst Port: 2055
v Cisco NetFlow/IPFIX
  Version: 10
  Length: 120
  > Timestamp: Jun 20, 2023 00:24:38.000000000 CST
  FlowSequence: 41662155
  Observation Domain Id: 256
  v Set 1 [id=2] (Data Template): 260
    FlowSet Id: Data Template (V10 [IPFIX]) (2)
    FlowSet Length: 104
    v Template (Id = 260, Count = 24)
      Template Id: 260
      Field Count: 24
      > Field (1/24): IPv4 ID
      > Field (2/24): IP_SRC_ADDR ←
      > Field (3/24): IP_DST_ADDR ←
      > Field (4/24): IP_TOS
      > Field (5/24): IP_DSCP
      > Field (6/24): PROTOCOL ←
      > Field (7/24): IP TTL MINIMUM
      > Field (8/24): IP TTL MAXIMUM
      > Field (9/24): L4_SRC_PORT ←
      > Field (10/24): L4_DST_PORT ←
      > Field (11/24): TCP_FLAGS
      > Field (12/24): SRC_AS
      > Field (13/24): IP_SRC_PREFIX
      > Field (14/24): SRC_MASK
      > Field (15/24): INPUT_SNMP ←
      > Field (16/24): DST_AS
      > Field (17/24): IP_NEXT_HOP
      > Field (18/24): DST_MASK
      > Field (19/24): OUTPUT_SNMP ←
      > Field (20/24): DIRECTION
      > Field (21/24): BYTES ←
      > Field (22/24): PKTS ←
      > Field (23/24): FIRST_SWITCHED ←
      > Field (24/24): LAST_SWITCHED ←
```

✎ صاخال ردمم لنيوكت بسح example رمأل ي ف جردم ل ذفنم ل فلتخي نأ نكمي :ةظالم 2055 وه يضارتفال ،كب

✎ نكمي ردمم للاقفو ،قئاقد 10 لى 5 نم ةمزحلال طاقتل لئغشت لى ع ظفاح :ةظالم زيمرت ك ف م تي تح بلالاقلا ك لذ طاقتل لى لجاتحتو ،ةقيقد N لك بلالاقلا لاسر لوطاً ةينمزةرتفل ةمزحلال طاقتل ررك ،بلالاقلا رهظي مل اذا ،ححص لكشب NetFlow

لاصتال تال كشم

نكمي هنا نم ققحت .نيردمم ل او SNA ةرادا زاهج نيب لاصتال دوجو نم دكأت :لاصتال نم ققحت مهب ةصاخال IP نيوانع قد قيرط نع Stealthwatch ةرادا مكحت ةدحو نم نيردمم لى لى لوصول اهلحو اهلصال واهئاطأ فاشكتسأ لكي لعف ،ةكبشلال لاصتال ي ف لكاشم ي اكانه تناك اذا ك لذ لاقفو .

نيردمم لاصح لى ع (SMC) ري دم ةردق ةحص نم ققحتل

- رذجل دامتعا تانايب مادختساب لوخدل لئجستو SSH ربع SNA ري دم ب لاصتال
- نم تالجلسال نع ثحباو /lancope/var/smc/log/smc-configuration.log فلم لئجحتب مق SourceSnmpSession: عونل

```
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
```

- هجاو ،ك لذ عمو .10.1.0.253 ردمم ل لاطأ نع فشكلا م تي مل ،اذه عارتقالا لاثم ي ف عارج نم ك لذ دعب نكمت هنكلو ،ةيادبل ي ف ةلهم لاطأ ةلاسر 10.1.0.254 ردمم ل ةي ناث 20 هتدم ريخأت دعب حاجنبا عارتقالا ةيلمع .

ردصم ب صاخال IP ناو نع مادختساب SMC لى ع ةمزحلال طاقتل لئغشتال عايشناب مق

- رذجل دامتعا تانايب مادختساب مكحتل ةدحو و SSH ربع ةرادال ةدقع لى لوخدل لئجس
- لئغشتال:

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

- لاثم ل لئبس لى ع) ةلضفم لك قيرط مادختساب زاهجال نم ةمزحلال طاقتل ري دصت SCP و SFTP
- ةحجانل ققحتل تالواح م ضرع ل Wireshark مادختساب ةمزحلال طاقتل لئغشتال
◦ نم مدقم بلط SMC:

```

17 2023-10-03 00:51:29.440263 116 SNMP getBulkRequest 1.3.6.1.2.1.2.2.1.2 1.3.6.1.2.1.2.2.1.3 1.3.6.1.2.1.2.2.1.5
> Frame 17: 116 bytes on wire (928 bits), 116 bytes captured (928 bits)
> Ethernet II, Src: [REDACTED] Dst: [REDACTED]
> Internet Protocol Version 4, Src: [REDACTED], Dst: [REDACTED]
> User Datagram Protocol, Src Port: 46876, Dst Port: 161
> Simple Network Management Protocol
  version: v2c (1)
  community: public
  > data: getBulkRequest (5)
    > getBulkRequest
      request-id: 1788921126
      non-repeaters: 0
      max-repetitions: 10
      variable-bindings: 3 items
        > 1.3.6.1.2.1.2.2.1.2: Value (Null)
          Object Name: 1.3.6.1.2.1.2.2.1.2 (iso.3.6.1.2.1.2.2.1.2)
          Value (Null)
        > 1.3.6.1.2.1.2.2.1.3: Value (Null)
          Object Name: 1.3.6.1.2.1.2.2.1.3 (iso.3.6.1.2.1.2.2.1.3)
          Value (Null)
        > 1.3.6.1.2.1.2.2.1.5: Value (Null)
          Object Name: 1.3.6.1.2.1.2.2.1.5 (iso.3.6.1.2.1.2.2.1.5)
          Value (Null)
  [Response In: 18]

```

```

18 2023-10-03 00:51:29.442116 140 SNMP get-response 1.3.6.1.2.1.2.2.1.3 1.3.6.1.2.1.2.2.1.3 1.3.6.1.2.1.2.2.1.5
> Frame 18: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits)
> Ethernet II, Src: [REDACTED] Dst: [REDACTED]
> Internet Protocol Version 4, Src: [REDACTED], Dst: [REDACTED]
> User Datagram Protocol, Src Port: 161, Dst Port: 46876
> Simple Network Management Protocol
  version: v2c (1)
  community: public
  > data: get-response (11)
    > get-response
      request-id: 1788921126
      error-status: noError (0)
      error-index: 0
      variable-bindings: 30 items
        > 1.3.6.1.2.1.2.2.1.3: "getBulkRequest"
          Object Name: 1.3.6.1.2.1.2.2.1.3 (iso.3.6.1.2.1.2.2.1.3)
          Value (Integer32): 9
        > 1.3.6.1.2.1.2.2.1.5: 9
          Object Name: 1.3.6.1.2.1.2.2.1.5 (iso.3.6.1.2.1.2.2.1.5)
          Value (Integer32): 9
        > 1.3.6.1.2.1.2.2.1.3: 98888888
          Object Name: 1.3.6.1.2.1.2.2.1.3 (iso.3.6.1.2.1.2.2.1.3)
          Value (Integer32): 98888888
        > 1.3.6.1.2.1.2.2.1.2: "getBulkRequest"
          Object Name: 1.3.6.1.2.1.2.2.1.2 (iso.3.6.1.2.1.2.2.1.2)
          Value (Integer32): 98888888
        > 1.3.6.1.2.1.2.2.1.5: 9
          Object Name: 1.3.6.1.2.1.2.2.1.5 (iso.3.6.1.2.1.2.2.1.5)
          Value (Integer32): 9
        > 1.3.6.1.2.1.2.2.1.3: 98888888
          Object Name: 1.3.6.1.2.1.2.2.1.3 (iso.3.6.1.2.1.2.2.1.3)
          Value (Integer32): 98888888
        > 1.3.6.1.2.1.2.2.1.2: "getBulkRequest"
          Object Name: 1.3.6.1.2.1.2.2.1.2 (iso.3.6.1.2.1.2.2.1.2)
          Value (Integer32): 98888888
        > 1.3.6.1.2.1.2.2.1.5: 9
          Object Name: 1.3.6.1.2.1.2.2.1.5 (iso.3.6.1.2.1.2.2.1.5)
          Value (Integer32): 9

```

◦ أهجاولا تامول عم رخصم ال نم SNMP عباقت سا

SNMP قيقدت اتاداع عحص نم ققحت ال

يف اهنيمضت متي ةبولطم ال سيسي اقم ال نأ ةبس انم عارت قالا تارتف نأ نم دكت اتم ال عت سا

- SNMP فيرعت تافل م -> نيرخصم ال -> نيوكت: يل لقت نا بيولا مدخت سم ةهجاو يل ع نيرخصم لل
- مالعت سا ةقيرطو (UDP 161 ذفنم صاخ لك شب) حيحص ال SNMP ذفنم نأ نم ققحت (ةدمعأ) كي دل رخصم ال عم كلذل اقفو هذه قباطت نأ بجيو، ةددحم ال حيحص ال SNMP



ifxTable، و CatOS MIB، و PanOS MIB)

رايتخاب ي صون ان نإف، ةيناث ال يف تباچي ج 10 ةعربب تاهجاو كي دل تناك اذا: ةظالم ال SNMP مالعت سا ةقيرط ال ifxTable ةدمعأ رايج

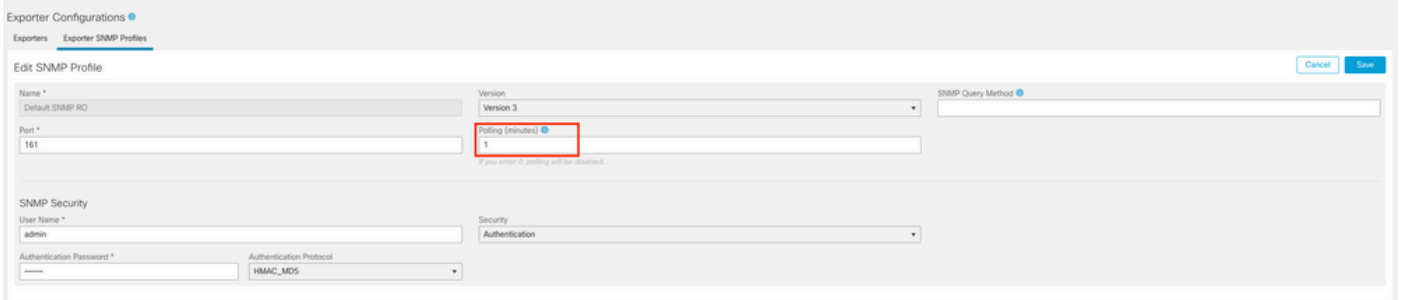
12 ةرتف يل ع SNMP صحف نيبيعتب مق، ماظن لل لثم أ ال اءال يل ع لوصحلل: ةظالم ال لك شب مادخت سا ال سيسي اقم شي دحت يل ركتم لك شب عاصقت سا ال يدوي ال. ةعاس ماظن ال ليغشت عاطب ال يدوي نأ نكمي امك، ربك أ

- عم دي. نيرخصم ال و SNA نم لك يل ع اهنيمضت متي ال SNMP تارادصا قفاوت نم ققحت نيرخصم ال نيوكت مت اذا امم ققحت. SNMPv3 و SNMPv2c و SNMPv1 لو كوتورب SNA يف هنيوكت مت امك SNMP رادصا سفن مادخت سا ال. ةم لك، مدخت سم ال مسا) SNMP نيوكت عحص نم ققحت، SNMPv3 مادخت سا علاح يف لو كوتورب، ةيصوصخ ال رورم ةم لك، ةقداصم ال لو كوتورب، ةيصوصخ ال (ةيصوصخ ال)

رشابم لكشب اهحالص او SNMP عارتقا اءاطخأ فاشكسأ

SNMP فيرعت تافلـم -> نيردصملا -> نيوكت يلى لقتنا ، بيولا مدختم ةهجاو يلى
نيردصم لل

- تقؤم لكشب (ةقيقد) 1 يلى (قئاقدلأب) عارتقالا طبض .



- رذجال دامتعا تانايب مادختساب مكحتلا ةدحو وأ SSH ربع SMC يلى لوخدلا لچس .
- دلجملا اذه يلى لقتنا :

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

- ليغشتلا :

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

- ةعئاشلا اءطخالا ةلاسر نوكتس ، SNMPv3 ل ةبسنلاب :

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

- رثكأ وأ فرحأ 8 يلى SNMP فيرعت فلم يف ةقداصملا رورم ةملك نييعت نم ققحت .
- ةيلىم مع نيوكت ةءاعإب مق ، ةرشابملا اهحالص او اءاطخأ فاشكسأ ةيلىم مع ءاهتنا درجمب .
ةقباسلا هتميق يلى هب صاخلا نيوكتلا بلاق وأ ردصم لل (قئاقدلأب) ققحتلا .

رخآ زاھج نم SNMP عالطتسا رابتخا

ددحم ةكبش زاھج يلى يلجم زاھج نم ايودي SNMP عاصقتسا ءدبب مق : SNMP عارتقا رابتخا
ةءعاسم تاودأ وأ تاودأ مادختساب كلذب مايقلا نكمي . ةباجتسا ملتسي ناك اذا ام صحفو
ةبولطملا SNMP تانايب عم ةكبشلا زاھج ةباجتسا نم ققحت . SNMPwalk لثم SNMP عارتقا
للاصتالا وأ SNMP نيوكت يف ةلكشم يلى ريشته انإف ، ةباجتسا كانه نكت مل اذا .

- ردصملا IP ل "x.x.x.x" ل دبتسا ، SNMPwalk جم انرب مادختساب كيدل يلجملا زاھجلا يلى
ع لى ليغشتلاب مقو CLI :

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

- -v2c: همادختسالا SNMP رادصا ديءحت
- -c: عمءجملا ةلسلس نييعت


```

% snmpwalk -v2c -c public 1
SNMPv2-MIB::sysDescr.0 = STRING: Cisco IOS Software [Amsterdam], Virtual XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 17.3.4a, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2021 by Cisco Systems, Inc.
Compiled Tue 20-Jul-21 04:
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.1537
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (373833542) 43 days, 6:25:35.42
SNMPv2-MIB::sysContact.0 =
SNMPv2-MIB::sysName.0 = STRING:
SNMPv2-MIB::sysLocation.0 = STRING: cxlabs
SNMPv2-MIB::sysServices.0 = INTEGER: 78
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00
IF-MIB::ifNumber.0 = INTEGER: 10
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.2 = INTEGER: 2
IF-MIB::ifIndex.3 = INTEGER: 3
IF-MIB::ifIndex.4 = INTEGER: 4
IF-MIB::ifIndex.5 = INTEGER: 5
IF-MIB::ifIndex.6 = INTEGER: 6
IF-MIB::ifIndex.7 = INTEGER: 7
IF-MIB::ifIndex.8 = INTEGER: 8
IF-MIB::ifIndex.9 = INTEGER: 9
IF-MIB::ifIndex.10 = INTEGER: 10
IF-MIB::ifDescr.1 = STRING: GigabitEthernet1
IF-MIB::ifDescr.2 = STRING: GigabitEthernet2
IF-MIB::ifDescr.3 = STRING: GigabitEthernet3
IF-MIB::ifDescr.4 = STRING: GigabitEthernet4
IF-MIB::ifDescr.5 = STRING: GigabitEthernet5
IF-MIB::ifDescr.6 = STRING: VoIP-Null0
IF-MIB::ifDescr.7 = STRING: Null0
IF-MIB::ifDescr.8 = STRING: GigabitEthernet6
IF-MIB::ifDescr.9 = STRING: GigabitEthernet7
IF-MIB::ifDescr.10 = STRING: Tunnel1
IF-MIB::ifType.1 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.2 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.3 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.4 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.5 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.6 = INTEGER: other(1)

```

- SNMP تانايې مادختساب ردصملا ةباجتسا نم ققحتلا

ةلص تاذا تامولعم

- مزلي (TAC) ةينقتلا ةدعاسملا زكرمب لاصتالا ىجرى، ةيفاضا ةدعاسم ىلع لوصحلل
- [ملاعلا عاجنا عيمج في Cisco معد لاصتا تاهج](#): جلاص معد دقع
- [انه Cisco نم](#) نامألا تاليلحت عم تجم ةرايز اضيا كنكمي
- [Cisco Systems - تادنتسملا وينقتلا معدلا](#)

ةمچرتل هذه ل و ح

ةيلأل تاي نقتل ن مة و مچم مادختساب دن تسمل اذ ه Cisco ت مچرت
ملاعلاء نأ عي مچي ف ني مدختسمل معد ي و تحم مي دقتل قيرشبل او
امك قيق دنوكت نل قيل أة مچرت ل ضفأ نأ ظحال م يچري . صاخل م ه تلغ بل
Cisco ي لخت . فرتحم مچرت م امدقي ي تل ا قيفار ت حال اة مچرتل عم ل حال او ه
ي لأمئاد وچرلاب ي صؤت و تامچرتل هذه ققد ن ع اهتيل وئس م Cisco
Systems (رفو تم طبارل) ي لصلأل يزي لچن إل دن تسمل ا