

排除SNA上的SNMP輪詢和錯誤介面詳細資訊故障

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[組態](#)

[背景資訊](#)

[疑難排解](#)

[介面名稱不正確](#)

[缺少匯出器或介面](#)

[連線問題](#)

[驗證管理員\(SMC\)輪詢匯出器的能力](#)

[使用匯出器的IP地址在SMC上生成資料包捕獲。](#)

[驗證SNMP輪詢設定](#)

[SNMP輪詢即時故障排除](#)

[從其他裝置測試SNMP輪詢](#)

[相關資訊](#)

簡介

本文描述如何對Secure Network Analytics中缺少匯出器介面資訊進行故障排除

必要條件

- 思科建議您瞭解基本簡易網路管理通訊協定(SNMP)輪詢知識
- 思科建議您瞭解基本的安全網路分析(SNA/StealthWatch)知識

需求

- 版本7.4.1或更高版本的SNA Manager
- 7.4.1版或更新版本中的SNA流量收集器
- 匯出器主動將NetFlow傳送到SNA

採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響

- 版本7.4.1或更高版本的SNA Manager
- 7.4.1版或更新版本中的SNA流量收集器
- SNMPwalk軟體
- Wireshark軟體

組態

- 裝置配置：需要配置匯出器以允許SNMP訪問。這涉及在每個裝置上配置SNMP設定，包括設定SNMP社群字串、訪問控制清單(ACL)和定義要使用的SNMP版本
- SNA上的SNMP輪詢配置：成功配置匯出器後，將使用預設定引數在SMC上預設啟用SNMP輪詢。必須提供與匯出器相關的必要細節（例如SNMP社群字串和SNMP版本），才能確保輪詢機制以最佳方式運行

背景資訊

SNA具有提供全面的介面狀態報告的功能，以及顯示主動將NetFlow資料傳輸到流量收集器的匯出器的介面名稱的能力。從Manager Web UI導航到Investigate -> Interfaces選單可檢視此介面詳細資訊。

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

疑難排解

介面名稱不正確

如果生成的報告顯示的「ifindex-#」與匯出器介面不對應，則表明在SMC或匯出器自身上進行SNMP輪詢存在潛在的配置問題。在本例中，我突出顯示了給定匯出器的SNMP輪詢的一個明顯問題。

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

缺少匯出器或介面

在NetFlow資料處理中，模板驗證非常重要。具體來說，它確保從匯出器接收的NetFlow模板包含成功解碼和流量收集器處理所需的所有欄位。如果未能遇到有效模板，將導致相關流集無法進行解碼，從而導致它們不在介面清單中。

如果在介面清單中未看到預期的匯出器/介面，則應驗證傳入的netflow data dn模板。為了驗證NetFlow模板，可以在流量收集器端建立資料包捕獲，通過更改「x.x.x.x」指定從匯出器獲取NetFlow的IP：

- 使用root憑據通過SSH或控制檯登入到流量收集器。
- 從有問題的匯出器IP和netflow埠運行資料包捕獲：

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

.pcap

- 使用您首選的方法（例如：SCP、SFTP），將資料包捕獲從裝置複製到安裝了Wireshark應用程式的工作站。
- 使用Wireshark開啟資料包捕獲，驗證匯出器正在傳送到流量收集器的模板和資料

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: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
      Field (14/15): LAST_SWITCHED
  
```

驗證NetFlow模板是否使用9個必填欄位，這些模板欄位的確切名稱可能會因匯出器型別而異，因此請務必查閱您正在配置的特定匯出器型別的文檔：

- 來源IP位址
- 目標IP地址
- 來源連線埠
- 目的地連線埠
- 第4層協定
- 位元組數
- 資料包計數
- 流開始時間
- 流結束時間

要正確顯示介面，請同時新增：

- 介面輸出
- 介面輸入

以下是來自給定匯出器裝置的模板資料包捕獲示例

- 紅色箭頭：所需的NetFlow欄位
- 綠色箭頭：SNMP欄位

```
> 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 ←
```

 注意：示例命令中列出的埠可能因匯出器配置而異，預設值為2055

 註：保持資料包捕獲在5到10分鐘內運行，具體取決於匯出器，模板可以每N分鐘傳送一次，並且您需要捕獲該模板，以便正確解碼NetFlow，如果模板未顯示，請更長時間重複資料包捕獲

連線問題

檢查連線：確保SNA Manager裝置和匯出器之間存在連線。通過ping匯出器的IP地址，驗證是否可以從Stealthwatch管理控制檯訪問匯出器。如果存在任何網路連線問題，請相應地排除故障並解決這些問題。

驗證管理員(SMC)輪詢匯出器的能力

- 通過SSH連線到SNA管理器並使用根憑證登錄
- 分析/lancope/var/smc/log/smc-configuration.log檔案並搜尋ExporterSnmpSession型別的日誌：

```
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
```

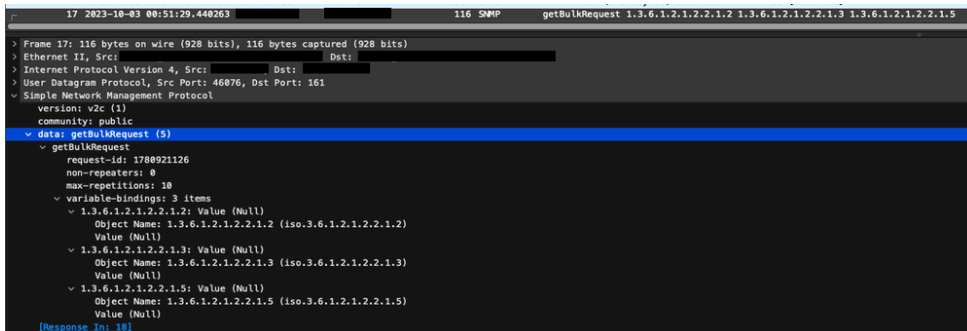
- 在此輪詢示例中，沒有檢測到匯出器10.1.0.253的錯誤。但是，匯出器10.1.0.254最初遇到超時錯誤消息，但隨後在延遲20秒後成功執行輪詢操作。

使用匯出器的IP地址在SMC上生成資料包捕獲。

- 使用root憑據通過SSH或控制檯登入到Manager節點
- 運行：

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

- 使用您的首選方法從裝置匯出資料包捕獲 (示例：SCP、SFTP)
- 使用Wireshark開啟資料包捕獲以檢視成功的輪詢嘗試



```
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:
> Internet Protocol Version 4, Src: , Dst:
> User Datagram Protocol, Src Port: 46076, Dst Port: 161
> Simple Network Management Protocol
  version: v2c (1)
  community: public
  data: getBulkRequest (5)
    getBulkRequest
      request-id: 1780921126
      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: 16]
```

- 來自SMC的請求：

- 運行：

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

- 對於SNMPv3，常見的錯誤消息為：

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

- 驗證SNMP配置檔案中的身份驗證密碼是否設定為8個字元或更多。
- 完成即時故障排除後，將匯出器或其配置模板的輪詢（分鐘）配置返回為其以前的值。

從其他裝置測試SNMP輪詢

測試SNMP輪詢：手動啟動從本地電腦到特定網路裝置的SNMP輪詢，並檢查它是否收到響應。這可以通過使用SNMP輪詢工具或SNMPwalk之類的實用程式來完成。驗證網路裝置是否使用請求的SNMP資料做出響應。如果沒有回應，就表示SNMP設定或連線發生問題。

- 在使用SNMPwalk軟體的本地電腦上，為匯出器IP替換「x.x.x.x」，並在CLI上運行：

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

- -v2c：指定要使用的SNMP版本
- -c：設定社群字串

```
% snmpwalk -v2c -c public :
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)
```

- 驗證匯出器是否使用SNMP資料做出響應

相關資訊

- 如需其他協助，請聯系技術協助中心(TAC)。需要有效的支援合約：[思科全球支援聯絡人](#)。
- 您還可以在此處訪問思科安全分析社群。
- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。