排除SNA上的SNMP輪詢和錯誤介面詳細資訊故障

目錄

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

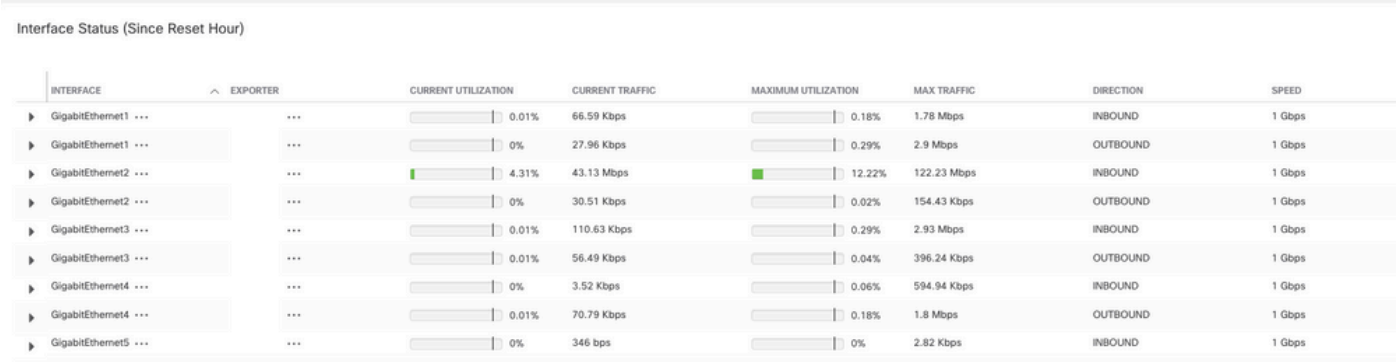
- 版本7.4.1或更高版本的SNA Manager
- 7.4.1版或更新版本中的SNA流量收集器
- SNMPwalk軟體
- Wireshark軟體

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

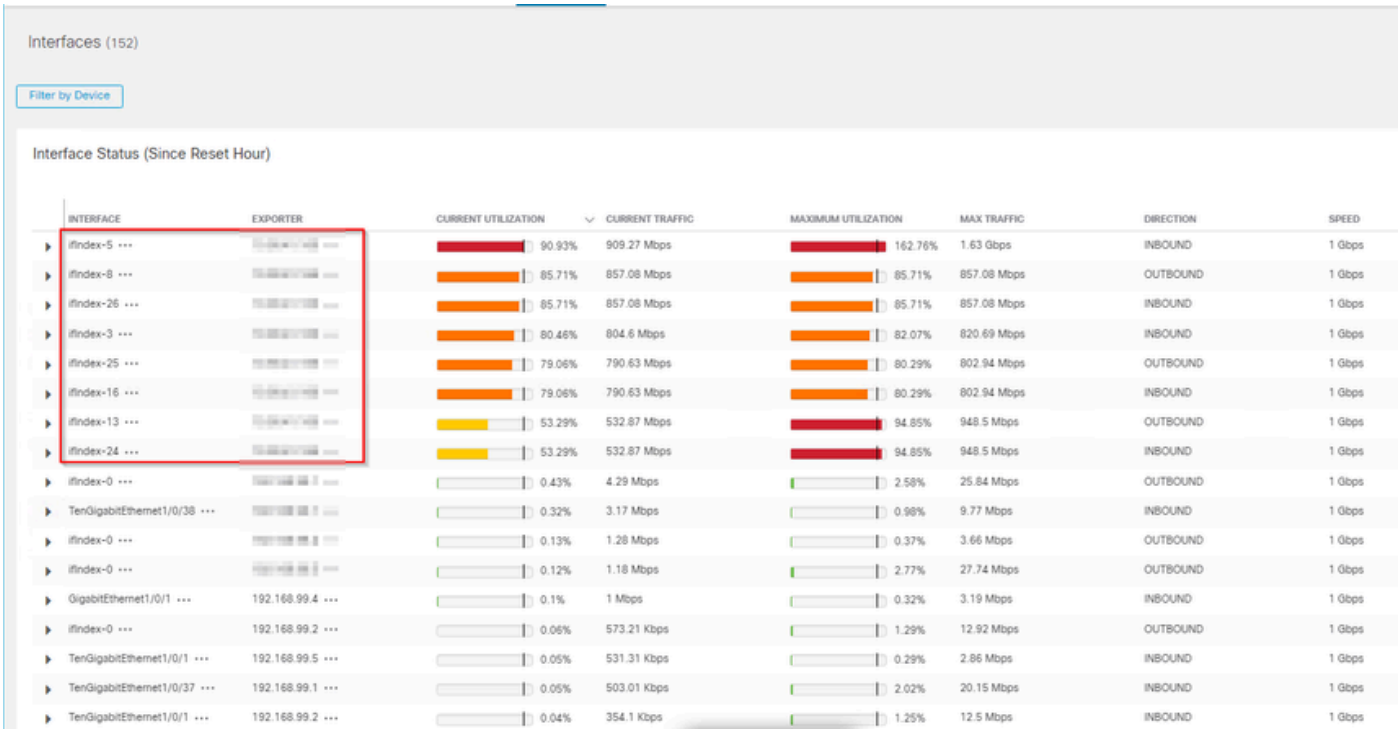
SNA具有提供全面的介面狀態報告的功能，以及顯示主動將NetFlow資料傳輸到流量收集器的匯出器的介面名稱的能力。 從Manager Web UI導航到Investigate -> Interfaces選單可檢視此介面詳細資訊。



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。



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。

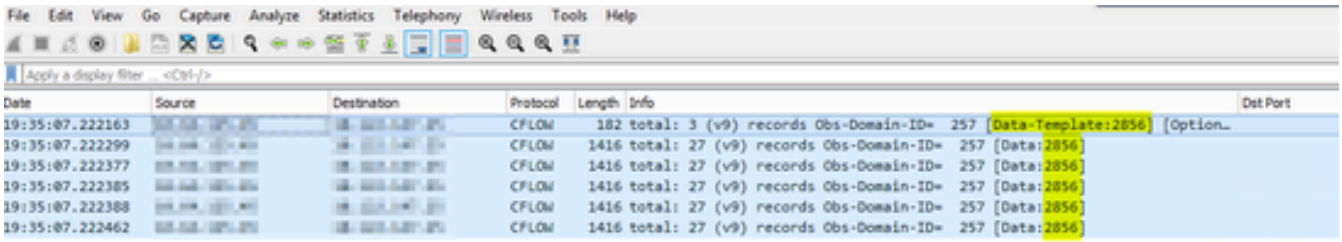
如果在介面清單中未看到預期的匯出器/介面，則應驗證傳入的netflow data dn模板。 為了驗證NetFlow模板，可以在流量收集器端建立資料包捕獲，通過更改「x.x.x.x」指定從匯出器獲取NetFlow的IP:

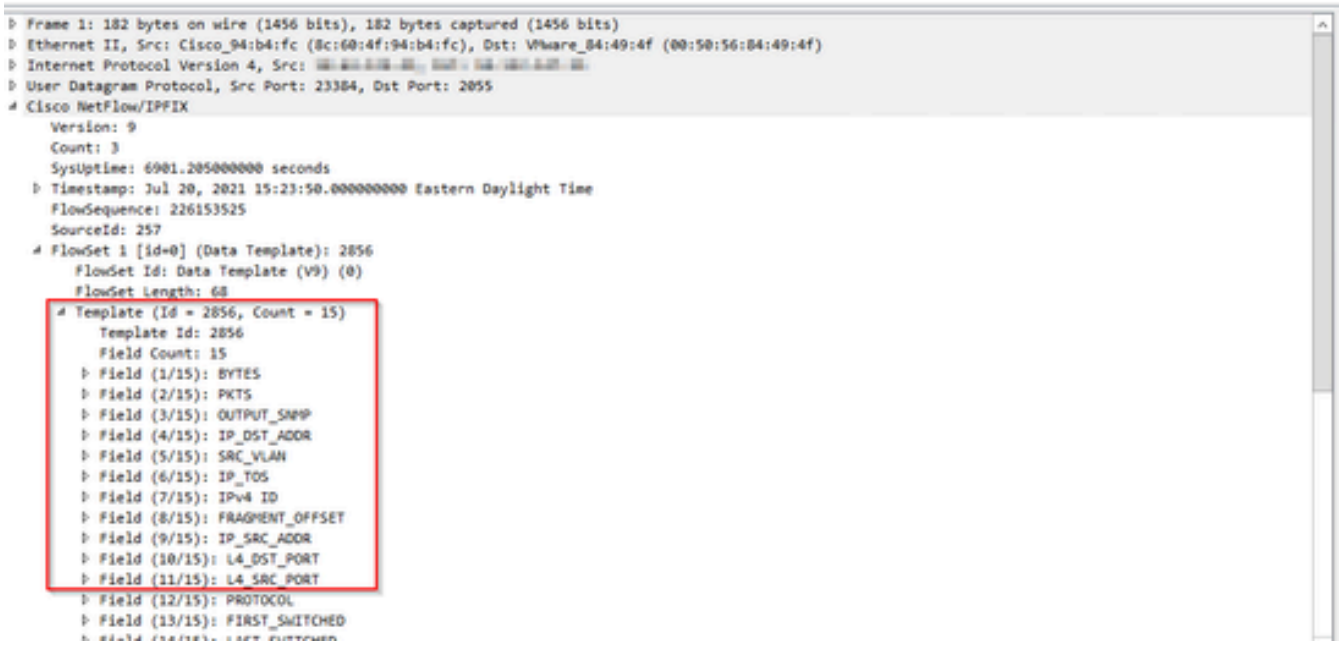
- 使用root憑據通過SSH或控制檯登入到流量收集器。
- 從有問題的匯出器IP和netflow埠運行資料包捕獲：

```
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





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：

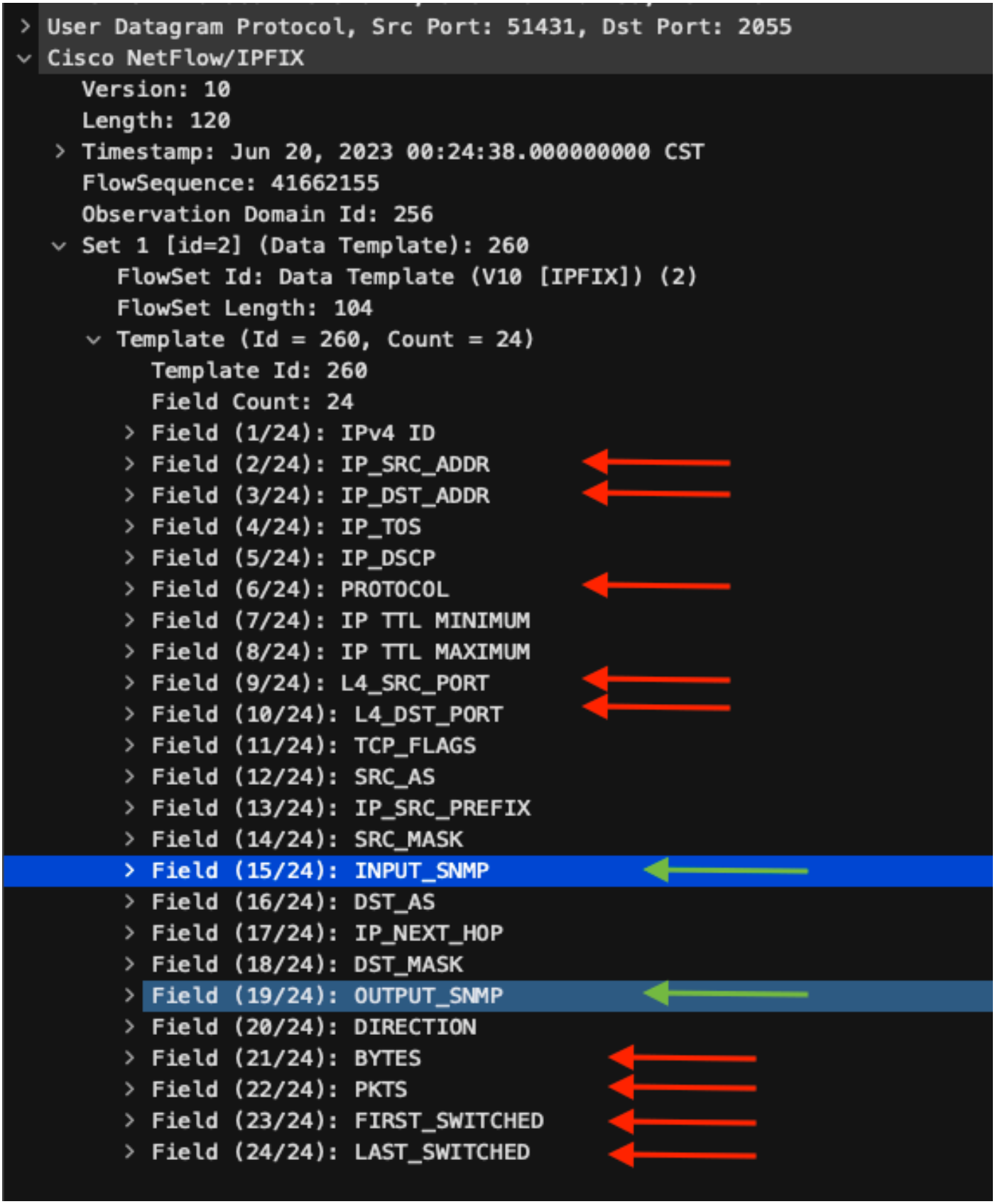
- 來源IP位址
- 目標IP地址
- 來源連線埠
- 目的地連線埠
- 第4層協定
- 位元組數
- 資料包計數
- 流開始時間
- 流結束時間

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



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
```

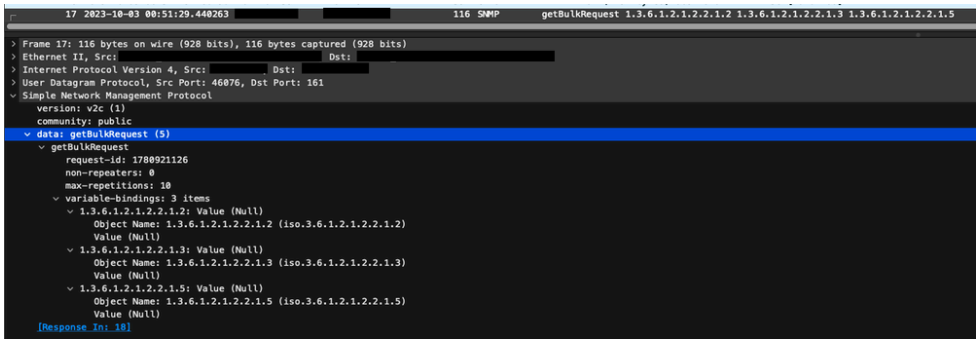
- 在此輪詢示例中，沒有檢測到匯出器10.1.0.253的錯誤。但是，匯出器10.1.0.254最初遇到超時錯誤消息，但隨後在延遲20秒後成功執行輪詢操作。

使用匯出器的IP地址在SMC上生成資料包捕獲。

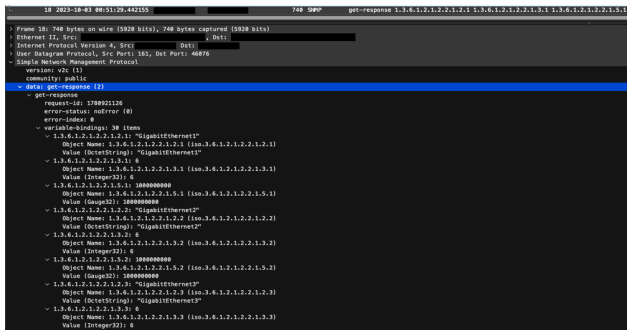
- 使用root憑據通過SSH或控制檯登入到Manager節點
- 運行：

```
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
  - 來自SMC的請求：



- 來自匯出器的SNMP響應（帶介面資訊）：



驗證SNMP輪詢設定

確保輪詢間隔合適，並且所需的度量包含在SNMP查詢中

- 在Web UI上，導航至：Configure -> Exporters -> Exporter SNMP Profiles:
- 驗證選擇的SNMP埠（通常為UDP埠161）和正確的SNMP查詢方法是否正確，這些埠必須與

  匯出器（ifxTable列、CatOS MIB、PanOS MIB）相匹配

註：如果您有10 Gbps介面，我們建議您為SNMP查詢方法選擇ifxTable columns選項。

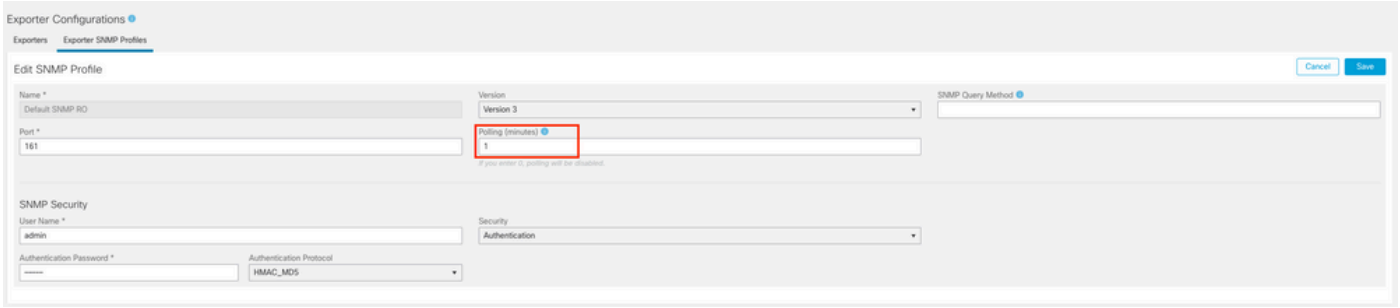
注意：為了獲得最佳的系統效能，請將SNMP輪詢設定為12小時的時間間隔。更頻繁的輪詢不會使您的利用率指標更具最新性，而且可能會導致您的系統運行速度變慢。

- 驗證SNA和匯出器上配置的SNMP版本是否相容。SNA支援SNMPv1、SNMPv2c和SNMPv3。檢查匯出器是否配置為使用SNA中配置的SNMP版本。
  - 如果使用SNMPv3，請驗證SNMP配置是否正確（使用者名稱、身份驗證密碼、身份驗證協定、隱私密碼、隱私協定）

SNMP輪詢即時故障排除

在Web UI上，導航至Configure -> Exporters -> Exporter SNMP Profiles

- 臨時將Polling(minutes)設定為1(minute)。



- 使用root憑據通過SSH或控制檯登入SMC。
- 導航到此資料夾：

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

- 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）。