排除SNMP轮询和SNA上不正确的接口详细信息故障

目录

简介

先决条件

要求

使用的组件

配置

背景信息

故障排除

- 接口名称不正确
- 缺少导出器或接口
- 连通性问题
  - 验证管理器(SMC)轮询导出器的能力
  - 使用导出器的IP地址在SMC上生成数据包捕获。
  - 验证SNMP轮询设置
  - SNMP轮询实时故障排除
- 测试来自其他设备的SNMP轮询

相关信息

简介

本文档介绍如何对Secure Network Analytics中缺少的导出器接口信息进行故障排除

先决条件

- Cisco建议您掌握基本的简单网络管理协议(SNMP)轮询知识
- 思科建议您掌握基本的安全网络分析(SNA/StealthWatch)知识

要求

- 7.4.1或更高版本的SNA Manager
- 7.4.1或更高版本的SNA流量收集器
- 导出器主动将NetFlow发送到SNA

使用的组件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响

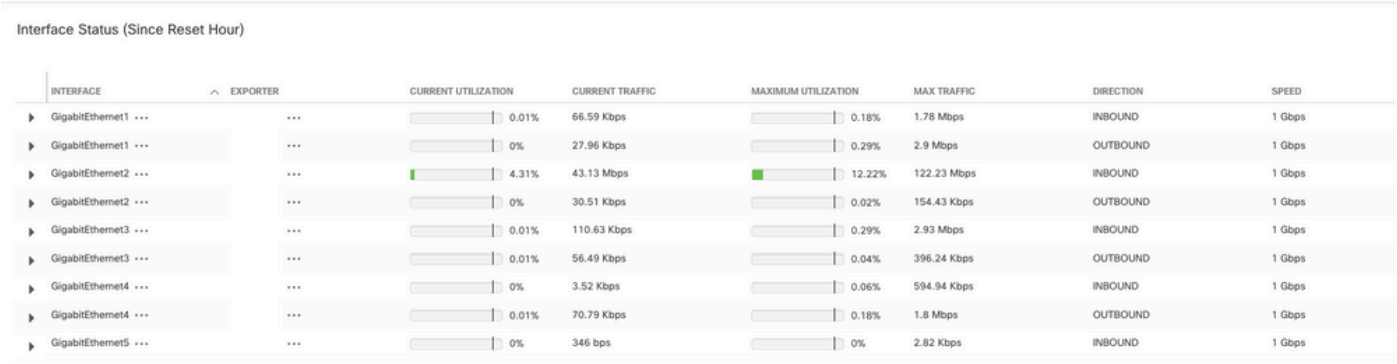
- 7.4.1或更高版本的SNA Manager
- 7.4.1或更高版本的SNA流量收集器
- SNMPwalk软件
- Wireshark软件

配置

- 设备配置：需要配置导出器以允许SNMP访问。这涉及到在每台设备上配置SNMP设置，包括设置SNMP社区字符串、访问控制列表(ACL)和定义要使用的SNMP版本
- SNA上的SNMP轮询配置：成功配置导出器后，SMC上将使用预设参数默认启用SNMP轮询。必须提供与导出器相关的必要详细信息，例如SNMP社区字符串和SNMP版本，以确保轮询机制以最佳状态运行

背景信息

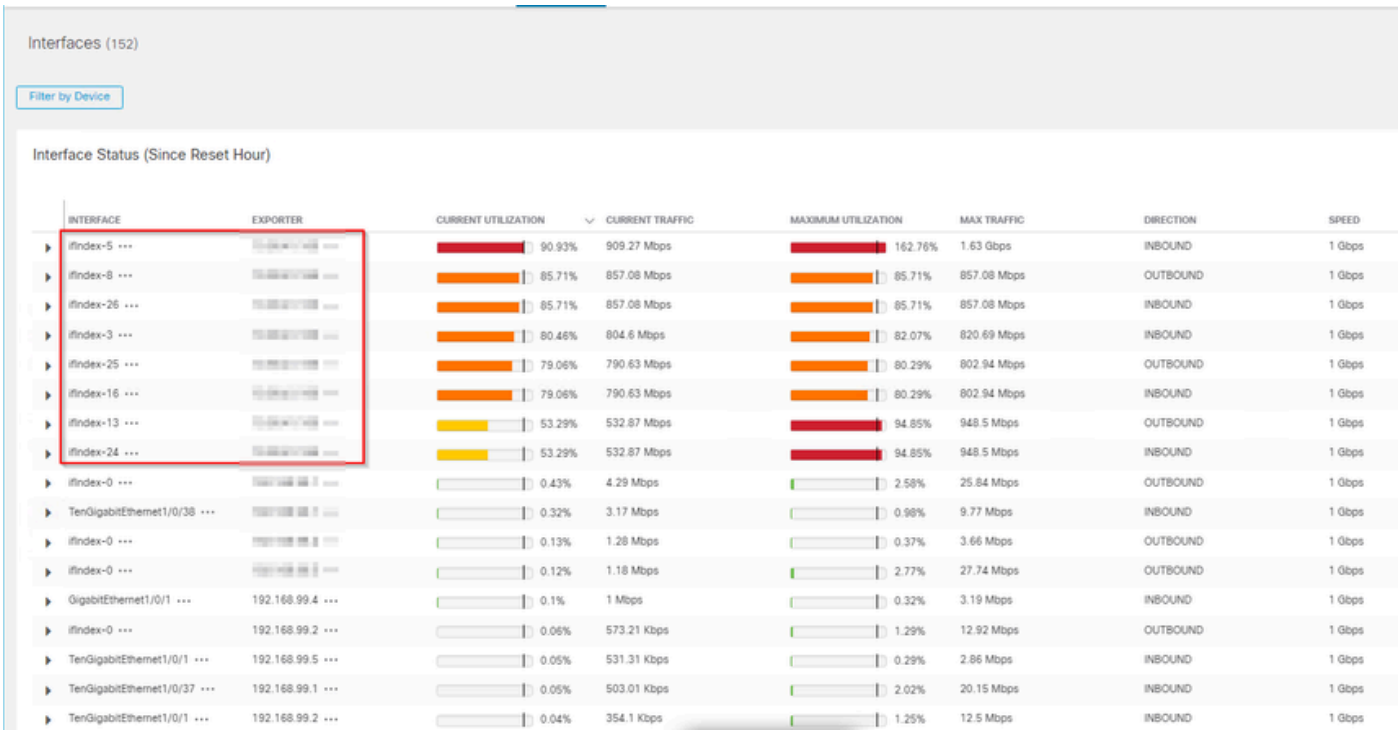
SNA能够提供全面的接口状态报告，同时还能够显示主动向流量收集器传输NetFlow数据的导出器的接口名称。 从Manager Web UI导航至Investigate -> Interfaces菜单可查看此界面详细信息。



故障排除

接口名称不正确

如果生成的报告显示的“ifindex-#”与导出器接口不对应，则表明在SMC或导出器自身上进行SNMP轮询存在潜在的配置问题。 在本例中，我突出显示了一个特定导出器的SNMP轮询明显问题。



缺少导出器或接口

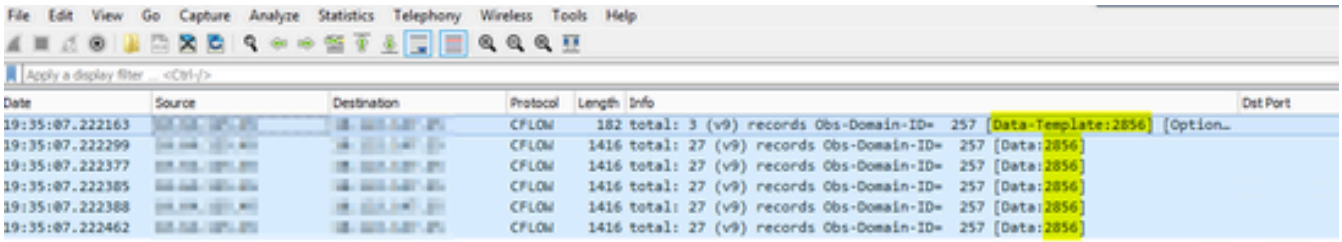
在NetFlow数据处理中，模板验证非常重要。具体而言，它确保从导出器接收的NetFlow模板包含流量收集器成功解码和处理所需的所有必要字段。如果未能遇到有效模板，则会导致相关流集被排除在解码范围之外，从而导致它们从接口列表中消失。

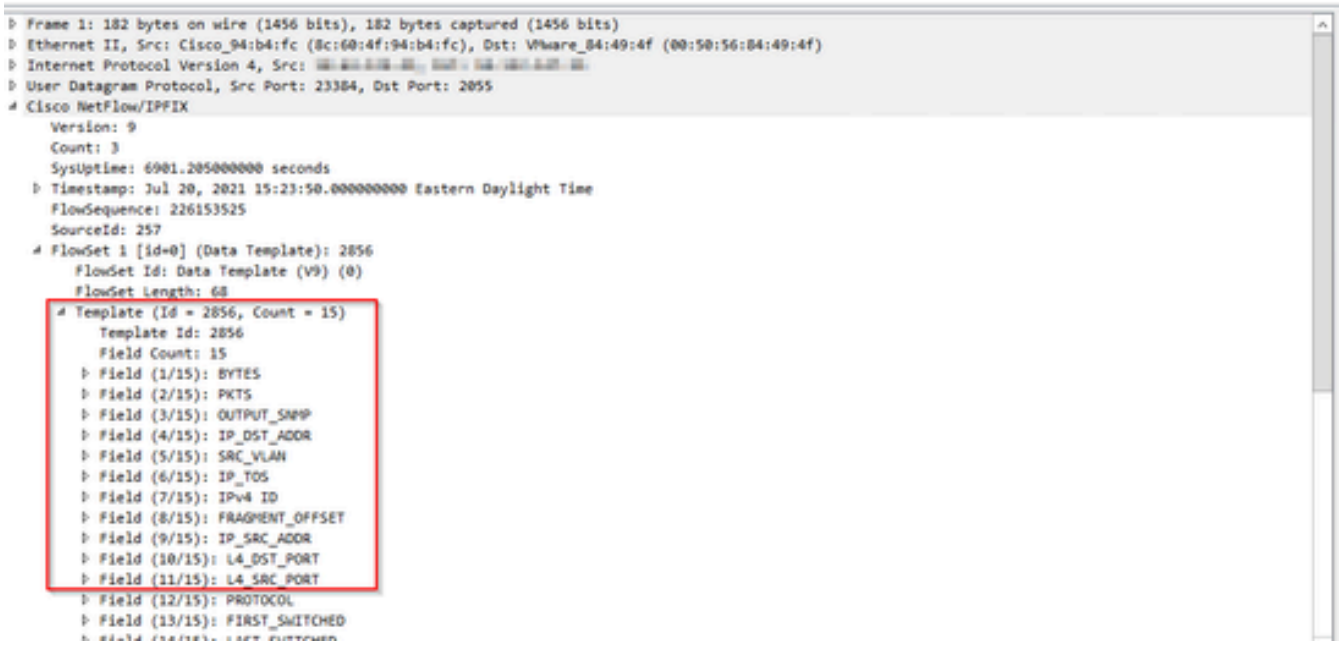
如果在接口列表中未看到预期的导出器/接口，则应验证传入的netflow data dn模板。 为了验证NetFlow模板，可以在流量收集器端创建数据包捕获，通过更改“x.x.x.x”指定从导出器获取NetFlow的IP：

- 使用根凭证通过SSH或控制台登录流量收集器。
- 从相关导出器IP和NetFlow端口运行数据包捕获：

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

- 使用首选方法（例如：SCP、SFTP）将数据包捕获从设备复制到安装了Wireshark应用的工作站。
- 使用Wireshark打开数据包捕获，验证导出器正在发送到流量收集器的模板和数据





验证NetFlow模板是否使用9个必填字段，这些模板字段的确切名称可能因导出器类型而异，因此，请确保参阅正在配置的特定导出器类型的文档：

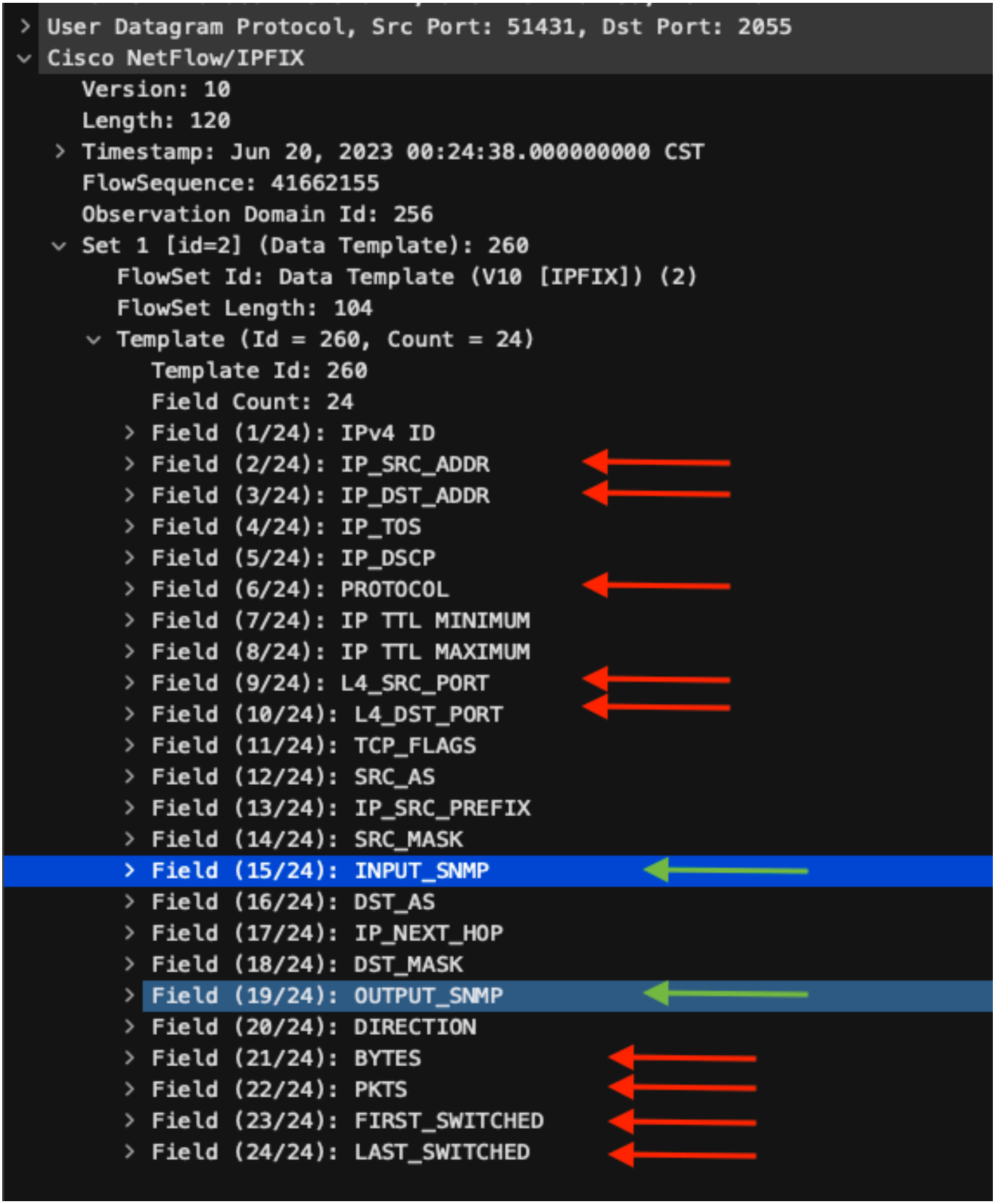
- 源 IP 地址
- 目的 IP 地址
- 源端口
- 目标端口
- 第4层协议
- 字节计数
- 数据包计数
- 流开始时间
- 流结束时间

要正确显示接口，请同时添加：

  - 接口输出
  - 接口输入

以下是来自给定导出器设备的模板数据包捕获示例

- 红色箭头：必需的NetFlow字段
- 绿色箭头：SNMP字段



注意：示例命令中列出的端口可能因导出器配置而异，默认值为2055

注意：保持数据包捕获在5-10分钟内运行，具体取决于导出器，模板可以每N分钟发送一次，并且您需要捕获该模板以使NetFlow正确解码。如果模板未显示，请重复数据包捕获较长时间

连通性问题

检查连接：确保SNA Manager设备和导出器之间存在连接。通过ping导出器的IP地址，验证是否可以从Stealthwatch管理控制台访问它们。如果存在任何网络连接问题，请进行相应的故障排除并解决。

验证管理器(SMC)轮询导出器的能力

- 通过SSH连接到SNA管理器并使用根凭证登录
- 分析/lancope/var/smc/log/smc-configuration.log文件并搜索ExporterSnmpSession：

```
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
```

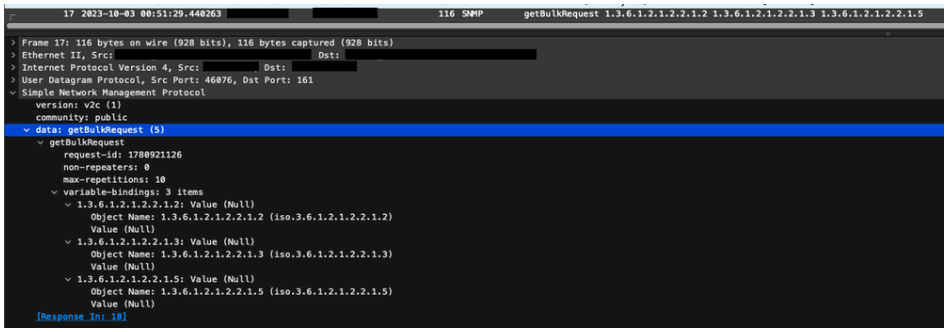
- 在此轮询示例中，未检测到导出器10.1.0.253的错误。但是，导出器10.1.0.254遇到超时。 默认超时间隔为5000毫秒，重试计数为3。因此，从轮询导出器到它超时的时间应该是20秒，而您尚未更改设置。

使用导出器的IP地址在SMC上生成数据包捕获。

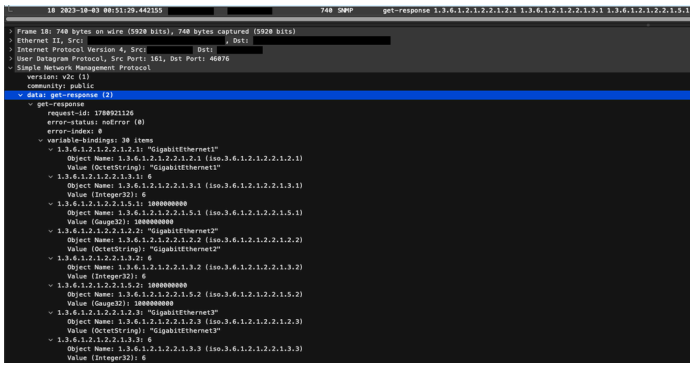
- 使用根凭证通过SSH或控制台登录到Manager节点
- 运行：

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

- 使用首选方法从设备导出数据包捕获（示例：SCP、SFTP）
- 使用Wireshark打开数据包捕获，查看成功的轮询尝试
  - 从SMC发出的请求：



- 来自导出器的SNMP响应及接口信息：



验证SNMP轮询设置

确保轮询间隔合适，并且所需的度量包含在SNMP查询中

- 在Web UI上，导航至：配置->导出器->导出器SNMP配置文件：
- 验证是否选择了正确的SNMP端口（通常为UDP端口161）和正确的SNMP查询方法，这些必须与导出器（ifxTable列、CatOS MIB、PanOS MIB）相匹配



注意：如果您有10 Gbps接口，我们建议您为SNMP查询方法选择ifxTable columns选项。

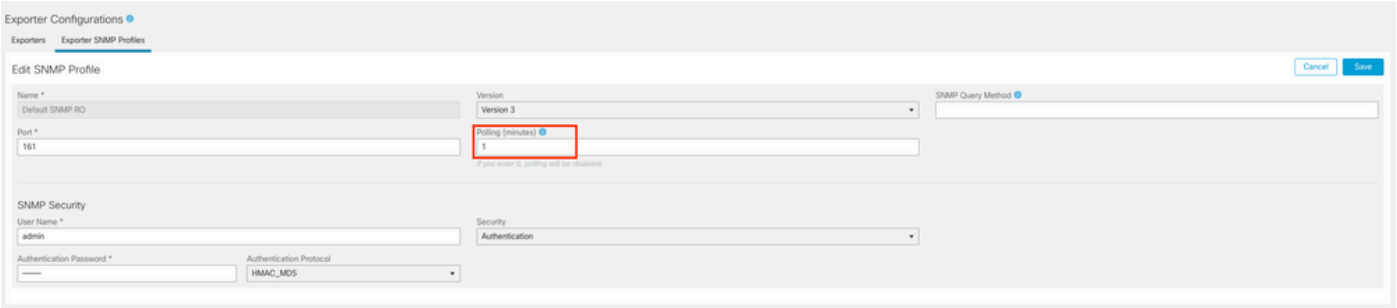
注意：为了获得最佳系统性能，请将SNMP轮询设置为12小时间隔。更频繁的轮询不会使利用率指标更具最新性，而且可能会导致系统运行速度变慢。

- 验证SNA和导出器上配置的SNMP版本是否兼容。SNA支持SNMPv1、SNMPv2c和SNMPv3。检查导出器是否配置为使用SNA中配置的SNMP版本。
  - 如果使用SNMPv3，请验证SNMP配置是否正确（用户名、身份验证密码、身份验证协议、隐私密码、隐私协议）

SNMP轮询实时故障排除

在Web UI上，导航到配置->导出器->导出器SNMP配置文件

- 将Polling (minutes)临时设置为1 (minute)。



- 使用根凭证通过SSH或控制台登录到SMC。
- 导航到此文件夹：

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

- 运行：

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

- 对于SNMPv3，常见的错误消息是：

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

- 验证SNMP配置文件中的身份验证密码是否设置为8个字符或以上。
- 完成实时故障排除后，请将导出器或其配置模板的轮询（分钟）配置返回至其以前的值。

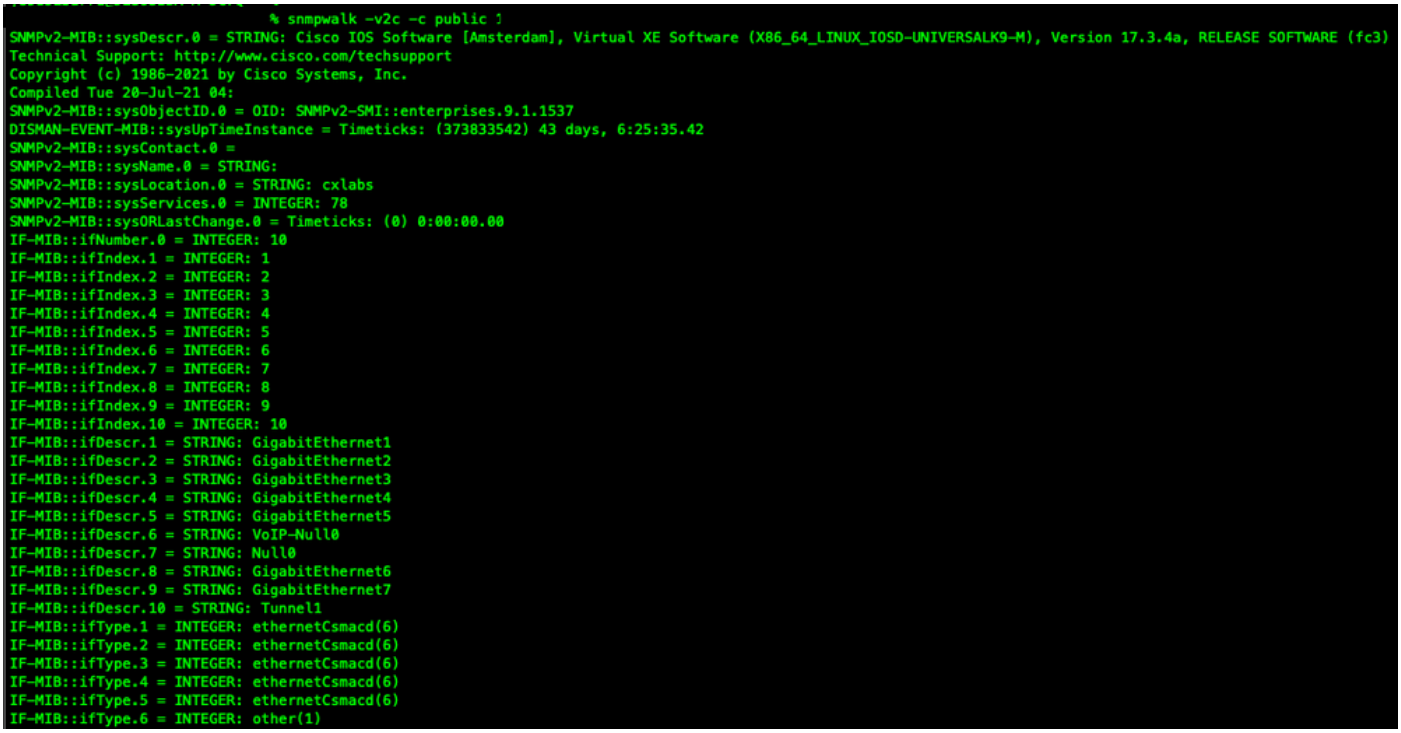
测试来自其他设备的SNMP轮询

测试SNMP轮询：手动从本地计算机向特定网络设备发起SNMP轮询，并检查其是否收到响应。这可以通过使用SNMP轮询工具或实用程序（如SNMPwalk）来完成。检验网络设备是否使用请求的SNMP数据做出响应。如果没有响应，则表示SNMP配置或连接存在问题。

- 在使用SNMPwalk软件的本地计算机上，为导出器IP替换“x.x.x.x”，并在CLI上运行：

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

  - -v2c：指定要使用的SNMP版本
  - -c：设置社区字符串



- 验证导出器是否使用SNMP数据做出响应

相关信息

- 如需其他帮助，请联系技术支持中心(TAC)。需要有效的支持合同：思科全球支持联系人。
- 您还可以访问思科安全分析社区。
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。