Resolución de Problemas de Sondeo SNMP y Detalles de Interfaz Incorrectos en SNA

Contenido

Introducción

Este documento describe cómo resolver problemas de información de interfaz de exportador faltante en Secure Network Analytics

Prerequisites

- Cisco recomienda que cuente con conocimientos básicos de sondeo del Protocolo simple de administración de red (SNMP)
- Cisco recomienda contar con conocimientos básicos de Secure Network Analytics (SNA/StealthWatch)

Requirements

- SNA Manager en la versión 7.4.1 o posterior
- SNA Flow Collector en la versión 7.4.1 o posterior
- Exportador enviando activamente NetFlow a SNA

Componentes Utilizados

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando

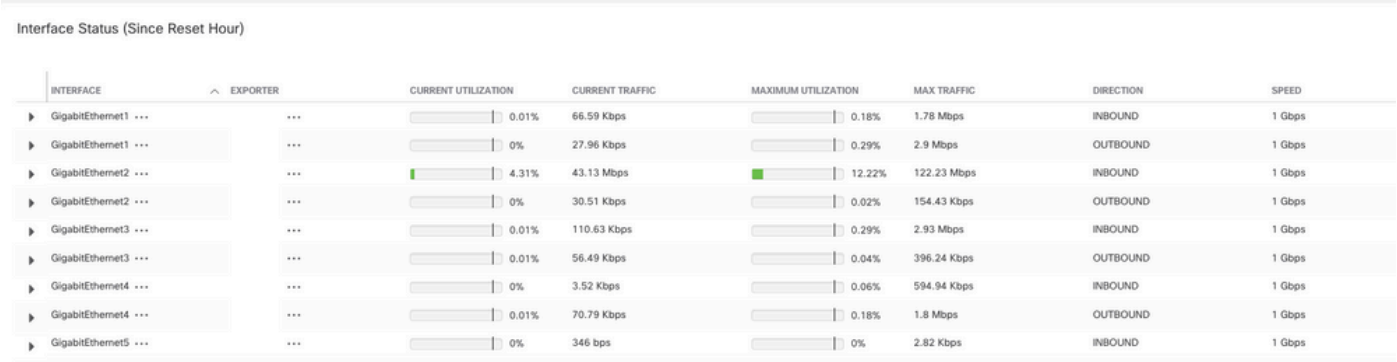
- SNA Manager en la versión 7.4.1 o posterior
- SNA Flow Collector en la versión 7.4.1 o posterior
- software SNMPwalk
- software Wireshark

Configuraciones

- Configuración del dispositivo: los exportadores deben configurarse para permitir el acceso SNMP. Esto implica la configuración de los parámetros SNMP en cada dispositivo, incluida la configuración de cadenas de comunidad SNMP, listas de control de acceso (ACL) y la definición de la versión de SNMP que se utilizará
- Configuración de sondeo SNMP en SNA: Una vez que los exportadores se configuran correctamente, el sondeo SNMP se habilita de forma predeterminada en el SMC mediante parámetros predefinidos. Es fundamental proporcionar los detalles necesarios relativos a los exportadores, como las cadenas de comunidad SNMP y las versiones de SNMP, para garantizar que el mecanismo de sondeo funcione de forma óptima

Antecedentes

SNA posee la capacidad de proporcionar informes completos de estado de interfaz, junto con la capacidad de mostrar nombres de interfaz para los exportadores que están transmitiendo activamente datos de NetFlow a un Flow Collector. Para ver estos detalles de la interfaz, acceda al menú Investigar -> Interfaces desde la interfaz de usuario web del jefe.

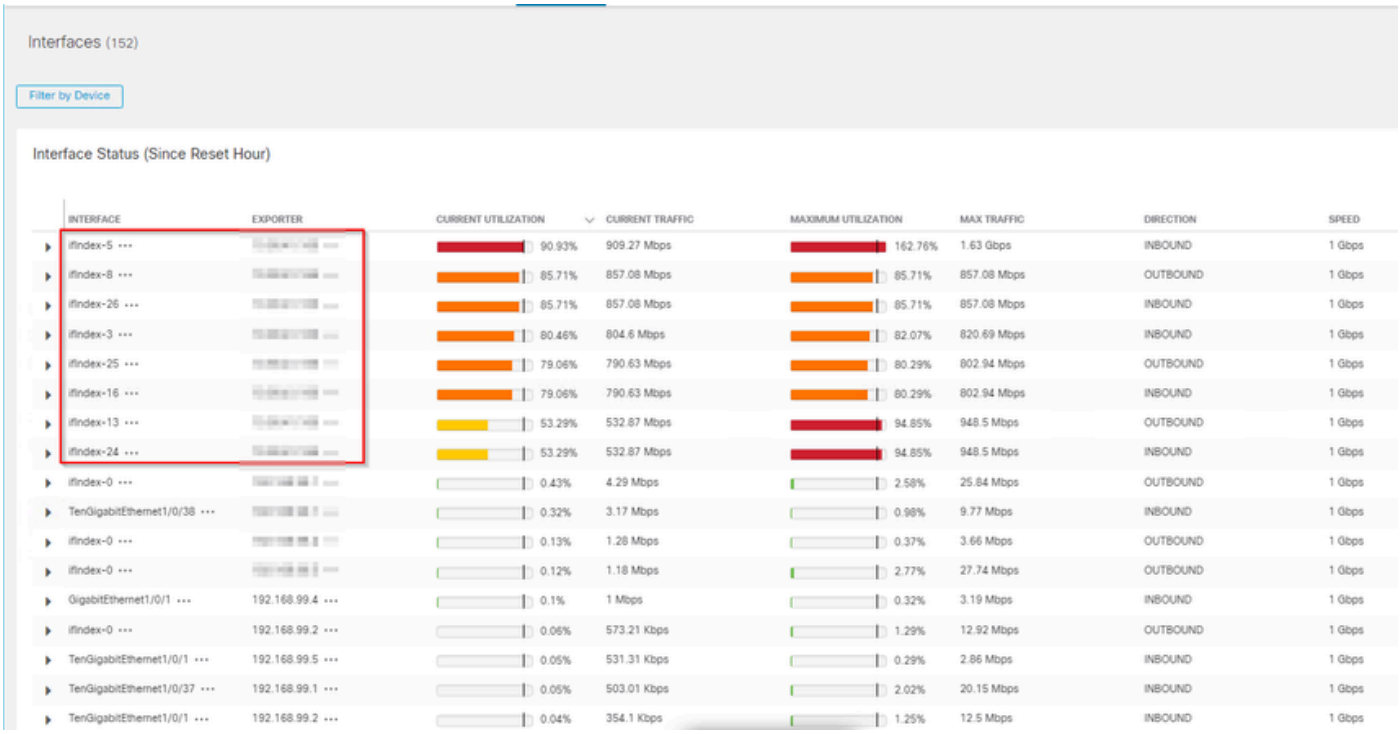


Resolución de problemas

Nombres de interfaz incorrectos

En el caso de que el informe generado muestre un "ifindex-#" que no corresponde a sus interfaces de exportador, sugiere un problema de configuración potencial con el sondeo SNMP en el SMC o en el exportador en sí. En este ejemplo, he destacado un problema aparente con el

sondeo SNMP de un exportador determinado.



Faltan exportadores o interfaces

La verificación de plantillas tiene una importancia significativa en el contexto del procesamiento de datos de NetFlow. En concreto, garantiza que la plantilla de NetFlow recibida del exportador contiene todos los campos necesarios para que el Flow Collector pueda descodificar y procesar correctamente. Si no se encuentra una plantilla válida, se excluye el conjunto de flujos asociado de la descodificación, lo que provoca su ausencia de la lista de interfaces.

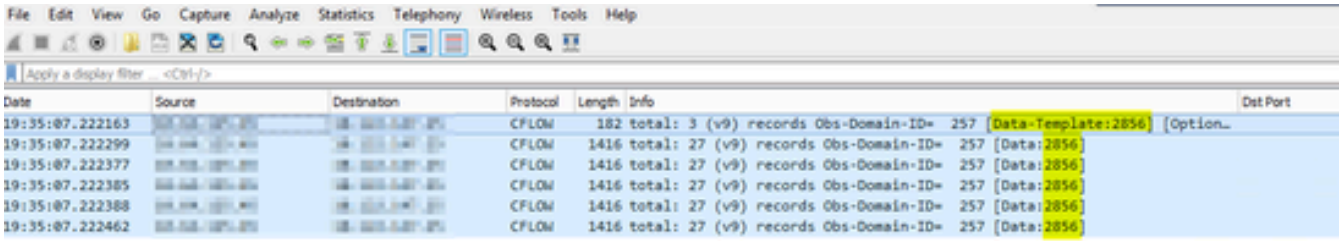
Si no ve el exportador o las interfaces esperadas en la lista de interfaces, debe verificar la plantilla de dn de datos de NetFlow entrante. Para verificar la plantilla de NetFlow, se puede crear una captura de paquetes en el lado del Flow Collector, especificando la IP del exportador del que estamos obteniendo NetFlow cambiando "x.x.x.x":

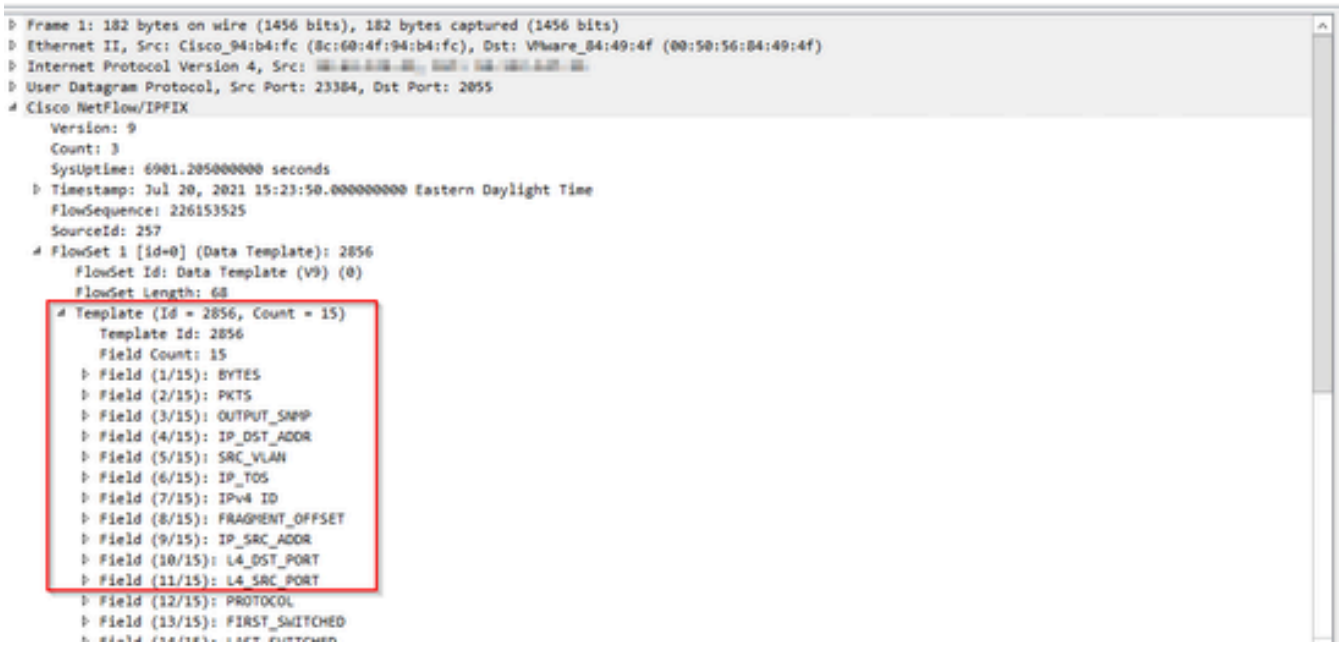
- Inicie sesión en el Flow Collector a través de SSH o de la consola con credenciales raíz.
- Ejecute una captura de paquetes desde la IP del exportador y el puerto de NetFlow en cuestión:

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

```
.pcap
```

- Copie la captura de paquetes desde el dispositivo a una estación de trabajo con la aplicación Wireshark instalada y utilice el método que prefiera (por ejemplo, SCP o SFTP).
- Abra la captura de paquetes con Wireshark y verifique la plantilla y los datos que el exportador envía al recolector de flujo





Verifique que la plantilla de NetFlow esté utilizando los 9 campos obligatorios; el nombre exacto de estos campos de plantilla puede variar en función del tipo de exportador, por lo que debe consultar la documentación del tipo de exportador específico que está configurando:

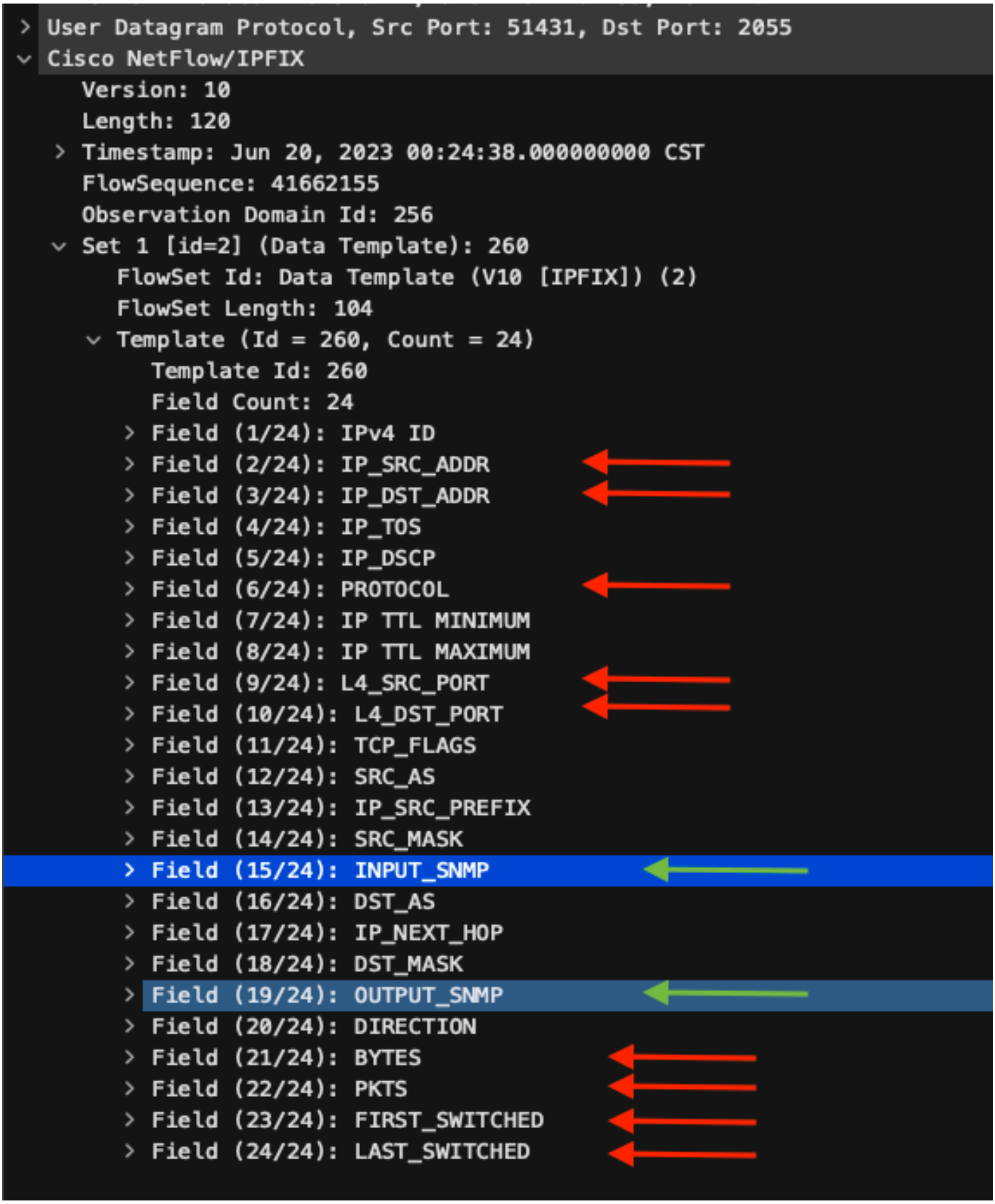
- Dirección IP de origen
- Dirección IP de destino
- Puerto de Origen
- Puerto de destino
- Protocolo de capa 4
- Número de bytes
- Recuento de paquetes
- Tiempo de inicio de flujo
- Tiempo de finalización de flujo

Para mostrar las interfaces correctamente, agregue también:

    - salida de la interfaz
    - entrada de la interfaz

Este es un ejemplo de captura de paquetes de plantilla de un dispositivo exportador dado

- Flechas rojas: campos obligatorios de NetFlow
- Flechas verdes: campos SNMP



Nota: El puerto enumerado en el comando de ejemplo puede variar según la configuración del exportador, el valor predeterminado es 2055

Nota: Mantenga la captura de paquetes en ejecución de 5 a 10 minutos, dependiendo del

exportador al que se pueda enviar la plantilla cada N minutos y necesite capturar esa plantilla para que NetFlow se descodifique correctamente; si la plantilla no se muestra, repita la captura de paquetes durante un período más largo

Problemas de conectividad

Comprobar conectividad: asegúrese de que hay conectividad entre el dispositivo SNA Manager y los exportadores. Verifique que los exportadores estén localizables desde la consola de administración de StealthWatch haciendo ping a sus direcciones IP. Si hay algún problema de conectividad de red, soluciónelo y soluciónelo en consecuencia.

Capacidad del administrador de validación (SMC) para sondear exportadores

- Conectar con el administrador SNA a través de SSH e iniciar sesión con credenciales raíz
- Analice el archivo /lancope/var/smc/log/smc-configuration.log y busque los registros del tipo ExporterSnmpSession:

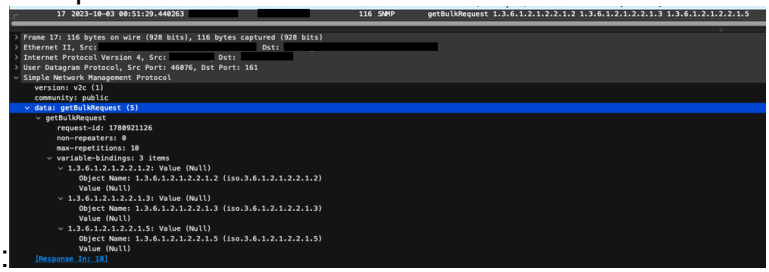
```
INFO [ExporterSnmpSession] SNMP polling for 10.1.0.253 took 0s
INFO [ExporterSnmpSession] SNMP polling for 10.1.0.253 took 0s
WARN [ExporterSnmpSession] SNMP polling for 10.10.0.254 failed: java.lang.Exception: timeout
INFO [ExporterSnmpSession] SNMP polling for 10.10.0.254 took 20s
WARN [ExporterSnmpSession] SNMP polling for 10.10.0.254 failed: java.lang.Exception: timeout
INFO [ExporterSnmpSession] SNMP polling for 10.10.0.254 took 20s
```

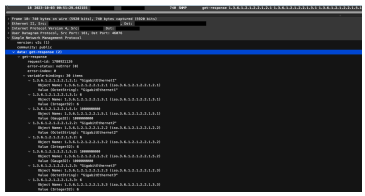
- En este ejemplo de sondeo, no se detectaron errores para el exportador 10.1.0.253. Sin embargo, el exportador 10.1.0.254 experimentó un mensaje de error de tiempo de espera inicialmente, pero posteriormente logró realizar con éxito la operación de sondeo después de un retraso de 20 segundos.

Genere una captura de paquetes en el SMC usando la dirección IP de un exportador.

- Inicie sesión en el nodo Manager a través de SSH o de la consola con credenciales raíz
- Ejecute:

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

- Exporte la captura de paquetes desde el dispositivo con el método que prefiera (por ejemplo, SCP o SFTP).
- Abra la captura de paquetes con Wireshark para ver los intentos de sondeo correctos
  - Solicitud realizada desde el SMC: 

- Respuesta SNMP del exportador con información de interfaz: 

Validar configuración de sondeo SNMP

Asegúrese de que los intervalos de sondeo sean apropiados y de que las métricas deseadas estén incluidas en las consultas SNMP

- En la interfaz de usuario web, vaya a: Configure -> Exporters -> Exporter SNMP Profiles:
- Valide que el puerto SNMP correcto (por lo general, el puerto UDP 161) y el método de consulta SNMP correcto seleccionados coincidan con su exportador (ifxTable Columns, CatOS MIB, PanOS MIB) 

Nota: Si tiene interfaces de 10 Gbps, se recomienda que elija la opción ifxTable columns para el método de consulta SNMP.

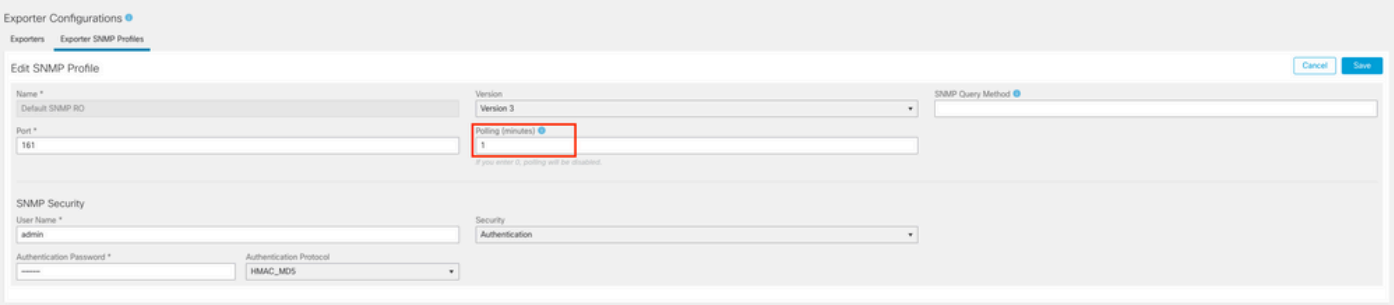
Nota: Para un rendimiento óptimo del sistema, establezca el sondeo SNMP en un intervalo de 12 horas. El sondeo con mayor frecuencia no actualiza las métricas de utilización y puede hacer que el sistema se ejecute más lentamente.

- Valide que las versiones de SNMP configuradas en SNA y en los exportadores sean compatibles. SNA admite SNMPv1, SNMPv2c y SNMPv3. Compruebe si los exportadores están configurados para utilizar la misma versión de SNMP configurada en SNA.
  - En caso de utilizar SNMPv3, verifique que la configuración de SNMP sea correcta (Nombre de usuario, Contraseña de autenticación, Protocolo de autenticación, Contraseña de privacidad, Protocolo de privacidad)

Resolución de problemas en directo de sondeo SNMP

En la interfaz de usuario web, vaya a Configurar -> Exportadores -> Perfiles SNMP de exportador

- Establecer sondeo (minutos) en 1 (minutos) temporalmente.



- Inicie sesión en el SMC a través de SSH o la consola con credenciales raíz.
- Vaya a esta carpeta:

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

- Ejecute:

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

- Para SNMPv3, un mensaje de error común sería:

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

- Verifique que la contraseña de autenticación en el perfil SNMP esté configurada en 8 caracteres o más.
- Una vez finalizada la resolución de problemas en directo, devuelva la configuración de sondeo (en minutos) del exportador o su plantilla de configuración a su valor anterior.

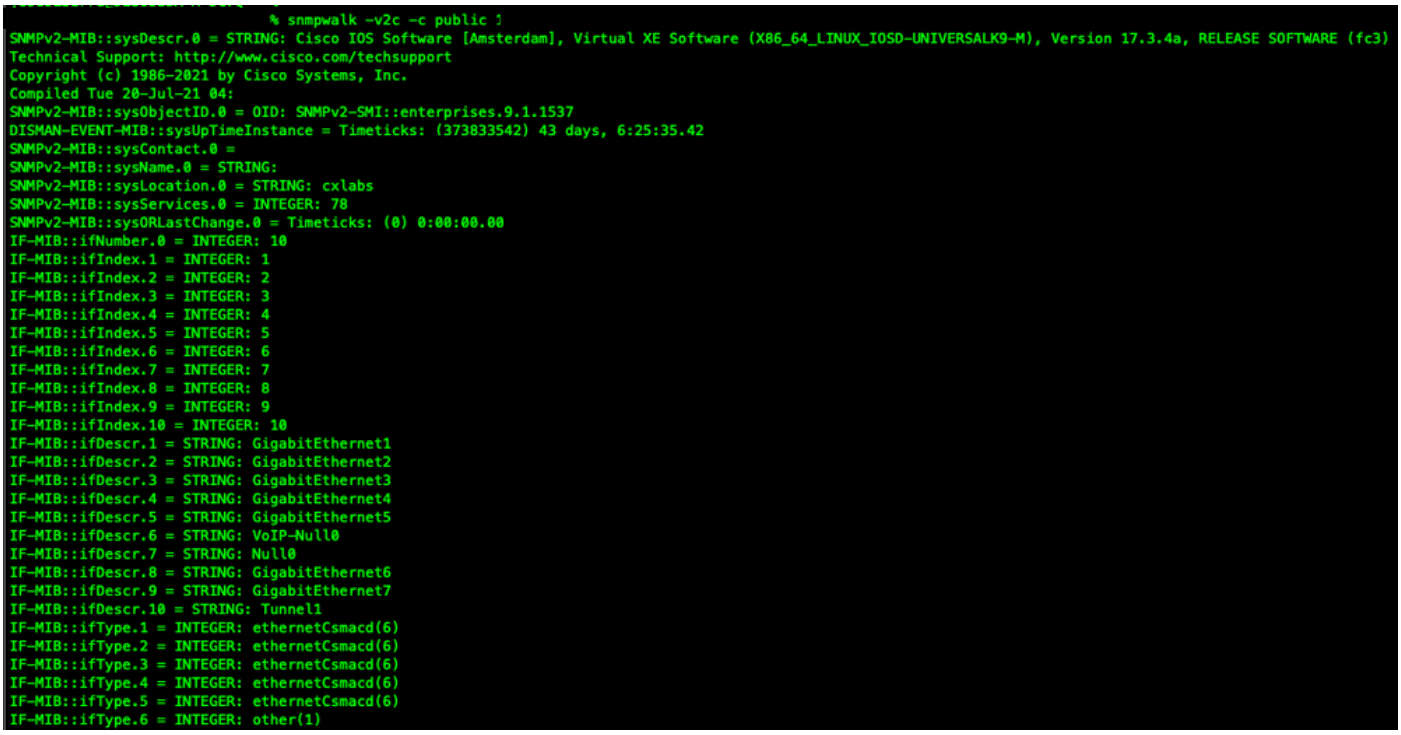
Prueba de sondeo SNMP desde otro dispositivo

Probar sondeo SNMP: inicie manualmente un sondeo SNMP desde una máquina local a un dispositivo de red específico y verifique si recibe una respuesta. Esto se puede hacer mediante herramientas de sondeo SNMP o utilidades como SNMPwalk. Verifique que el dispositivo de red responda con los datos SNMP solicitados. Si no hay respuesta, indica un problema con la configuración o conectividad SNMP.

- En su equipo local con el software SNMPwalk, reemplace "x.x.x.x" por la IP del exportador y ejecute en CLI:

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

    - -v2c: especifica la versión de SNMP que se va a utilizar
    - -c: establece la cadena de comunidad



- Verifique que el exportador responda con datos SNMP

Información Relacionada

- Para obtener asistencia adicional, póngase en contacto con el Technical Assistance Center (TAC). Se necesita un contrato de soporte válido: Contactos de soporte a nivel mundial de Cisco.
- También puede visitar la Comunidad de análisis de seguridad de Cisco aquí.
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).