Configuración y solución de problemas de SNMP en SWA

Contenido

Introducción

En este documento se describen los pasos para solucionar problemas del protocolo simple de supervisión de red (SNMP) en el dispositivo web seguro (SWA).

Prerequisites

Requirements

Cisco recomienda conocer estos temas:

- Acceso a la interfaz de línea de comandos (CLI)de SWA
- Acceso administrativo al SWA.

- Conocimiento básico de SNMP.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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.

Cómo Funciona SNMP

SNMP es un protocolo de comunicación de capa de aplicación que permite a los dispositivos de red intercambiar información de administración entre estos sistemas y con otros dispositivos fuera de la red.

A través de SNMP, los administradores de red pueden administrar el rendimiento de la red, buscar y resolver problemas de red y planificar el crecimiento de la red.

SNMP hace que la supervisión de la red sea más rentable y permite que la red sea más fiable. (Para obtener más información sobre SNMP, consulte RFC 1065, 1066 y 1067.)

Una red gestionada por SNMP consta de un administrador, agentes y dispositivos gestionados.

- El administrador proporciona la interfaz entre el administrador de la red humana y el sistema de administración.
- El agente proporciona la interfaz entre el administrador y el dispositivo que se está gestionando
- Los sistemas de gestión ejecutan la mayoría de los procesos de gestión y proporcionan la mayor parte de los recursos de memoria utilizados para la gestión de la red.

Un agente reside en cada dispositivo gestionado y traduce los datos de información de gestión local (como la información de rendimiento o la información de eventos y errores) capturados en las capturas de software a un formato legible para el sistema de gestión.

El agente SNMP captura datos de la Base de información de administración (MIB) (parámetros de dispositivo y repositorios de datos de red) o de capturas de errores o cambios.

MIB

La MIB es una estructura de datos que describe los elementos de red SNMP como una lista de objetos de datos. El administrador SNMP debe compilar el archivo MIB para cada tipo de equipo en la red para monitorear los dispositivos SNMP.

El administrador y el agente utilizan una MIB y un conjunto relativamente pequeño de comandos para intercambiar información. La MIB está organizada en una estructura de árbol con variables

individuales representadas como hojas en las ramas.

Se utiliza una etiqueta numérica larga o un identificador de objeto (OID) para distinguir cada variable de manera única en la MIB y en los mensajes SNMP. La MIB asocia cada OID con una etiqueta legible y varios otros parámetros relacionados con el objeto.

La MIB entonces sirve como un diccionario de datos o libro de códigos que se utiliza para ensamblar e interpretar mensajes SNMP.

Cuando el administrador SNMP desea conocer el valor de un objeto, como el estado de un punto de alarma, el nombre del sistema o el tiempo de actividad del elemento, ensambla un paquete GET que incluye el OID para cada objeto de interés.

El elemento recibe la solicitud y busca cada OID en su libro de códigos (MIB). Si se encuentra el OID (el elemento administra el objeto), se ensambla un paquete de respuesta y se envía con el valor actual del objeto incluido.

Si no se encuentra el OID, se envía una respuesta de error especial que identifica el objeto no administrado

Trampa SNMP

Los mensajes de trampa SNMP habilitan un agente para notificar a la estación de administración de acerca de eventos significativos a través de un mensaje SNMP no solicitado.

SNMPv1 y SNMPv2c, junto con la MIB asociada, fomentan la notificación de trampa dirigida.

La idea detrás de la notificación de trampa dirigida es que si un administrador es responsable de un gran número de dispositivos, y cada dispositivo tiene un gran número de objetos, no es práctico que el administrador sondee o solicite información de cada objeto en cada dispositivo.

La solución consiste en que cada agente del dispositivo administrado notifique al administrador sin solicitarlo. Para ello, envía un mensaje denominado Trampa del evento.

Una vez que el administrador recibe el evento, lo muestra y puede decidir realizar una acción en función del evento. Por ejemplo, el administrador puede sondear al agente directamente o a otros agentes de dispositivos asociados para comprender mejor el evento.

La notificación dirigida a trampas puede resultar en un ahorro sustancial de recursos de red y agentes al eliminar la necesidad de solicitudes SNMP frívolas. Sin embargo, no es posible eliminar totalmente los sondeos SNMP.

Las solicitudes SNMP son necesarias para cambios de detección y de topología. Además, un agente de dispositivos gestionados no puede enviar una trampa si el dispositivo ha sufrido una interrupción catastrófica.

Las trampas SNMPv1 se definen en RFC 1157, con estos campos:

- Enterprise:Identifica el tipo de objeto gestionado que genera la captura.

- Dirección del agente: proporciona la dirección del objeto administrado que genera la captura.
- Tipo de trampa genérica:Indica uno de los diversos tipos de trampa genéricos.
- Código de trampa específico:indica uno de varios códigos de trampa específicos.
- Marca de tiempo: proporciona la cantidad de tiempo transcurrido entre la última reinicialización de la red y la generación de la trampa.
- Enlaces variables: campo de datos de la trampa que contiene PDU. Cada enlace de variable asocia una instancia de objeto MIB determinada con su valor actual.

SNMPv3

SNMPv3 admite el identificador "Engine ID" de SNMP, que identifica de forma única cada entidad SNMP. Los conflictos pueden ocurrir si dos entidades SNMP tienen EngineIDs duplicados.

EngineID se utiliza para generar la clave para los mensajes autenticados. (Para obtener más información sobre SNMPv3, consulte RFC 2571-2575.)

Muchos productos SNMP siguen siendo básicamente los mismos en SNMPv3, pero se mejoran con estas nuevas funciones:

Security

- Autenticación
- Privacidad

Administración

- Autorización y control de acceso
- Contextos lógicos
- Denominación de entidades, identidades e información
- Personas y políticas
- Nombres de usuario y gestión de claves
- Destinos de notificación y relaciones de proxy
- Configuración remota a través de operaciones SNMP

Los modelos de seguridad SNMPv3 se presentan principalmente de dos formas: autenticación y cifrado.

La autenticación se utiliza para garantizar que sólo el destinatario previsto lea las trampas. A medida que se crean los mensajes, se les da una clave especial basada en la entidad EngineID. La clave se comparte con el destinatario y se utiliza para recibir el mensaje.
Cifrado, la privacidad cifra la carga del mensaje SNMP para garantizar que los usuarios no autorizados no puedan leerlo. Cualquier trampa interceptada llena de caracteres incomprensibles y es ilegible. La privacidad es especialmente útil en aplicaciones en las que los mensajes SNMP deben enrutarse a través de Internet.

Hay tres niveles de seguridad en un grupo SNMP:

noAuthnoPriv - Comunicación sin autenticación y privacidad.
authNoPriv - Comunicación con autenticación y sin privacidad. Los protocolos utilizados para la autenticación son el algoritmo Message-Digest 5 (MD5) y el algoritmo hash seguro (SHA).
authPriv - Comunicación con autenticación y privacidad. Los protocolos utilizados para la autenticación son MD5 y SHA, y para la privacidad se pueden utilizar los protocolos Estándar de cifrado de datos (DES) y Estándar de cifrado avanzado (AES).

SNMP en SWA

El sistema operativo AsyncOS admite la supervisión del estado del sistema mediante SNMP.

Tenga en cuenta:

- SNMPisoff de forma predeterminada.
- Las operaciones SNMPSET (configuración) no están implementadas.
- AsyncOS admite SNMPv1, v2 y v3.
- La autenticación y el cifrado de mensajes son obligatorios al habilitar SNMPv3. Las frases de contraseña para la autenticación y el cifrado deben ser diferentes.
- El algoritmo de cifrado puede ser AES (recomendado) o DES.
- El algoritmo de autenticación puede ser SHA-1 (recomendado) o MD5.
- El comando nmpconfig "recuerda" las frases de contraseña la próxima vez que ejecute el comando.
- Para las versiones de AsyncOS anteriores a 15.0, el nombre de usuario de SNMPv3 es: v3get.
- Para AsyncOS versión 15.0 y posteriores, el nombre de usuario defaultSNMPv3 es: v3get. Como administrador, puede optar por cualquier otro nombre de usuario.
- Si utiliza solamente SNMPv1 o SNMPv2, debe establecer una cadena de comunidad. La cadena de comunidad no es pública de forma predeterminada.
- ParaSNMPv1 ySNMPv2, debe especificar una red desde la que se acepten solicitudes SNMPGET.
- Para utilizar las capturas, debe estar en ejecución un SNMPmanager (no incluido en AsyncOS) y su dirección IP debe introducirse como destino de la captura. (Puede utilizar un nombre de host, pero si lo hace, las trampas sólo funcionan si DNS funciona.)

Configuración de SNMPonitor

Para configurar SNMPpara recopilar información de estado del sistema para el dispositivo, utilice el comando snmpconfig en la CLI. Después de elegir y configurar los valores para una interfaz, el dispositivo responde a las solicitudes GET SNMPv3.

Al utilizar SNMP, tenga en cuenta estos puntos:

- En SNMP versión 3, las solicitudes deben incluir una frase de contraseña coincidente.
- De forma predeterminada, las solicitudes de las versiones 1 y 2 se rechazan.
- Si se habilita, las solicitudes de versión 1 y 2 deben tener una cadena de comunidad coincidente.

```
SWA_CLI> snmpconfig

Current SNMP settings:
SNMP Disabled.

Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]> SETUP

Do you want to enable SNMP? [Y]> Y

Please choose an IP interface for SNMP requests.
1. Management (10.48.48.184/24 on Management: wsa125to15-man.amojarra.calo)
2. P1 (192.168.13.184/24 on P1: wsa1255p1.amojarra.calo)
3. P2 (192.168.133.184/24 on P2: wsa1255p2.amojarra.calo)
[1]> 1

Which port shall the SNMP daemon listen on?
[161]> 161

Please select SNMPv3 authentication type:
1. MD5
2. SHA
[1]> 2

Please select SNMPv3 privacy protocol:
1. DES
2. AES
[1]> 2

Enter the SNMPv3 username or press return to leave it unchanged.
[w3get]> SNMPMUser

Enter the SNMPv3 authentication passphrase.
[]>
Please enter the SNMPv3 authentication passphrase again to confirm.
[]>

Enter the SNMPv3 privacy passphrase.
[]>
Please enter the SNMPv3 privacy passphrase again to confirm.
[]>
Service SNMP V1/V2c requests? [N]> N

Enter the Trap target as a host name, IP address or list of IP addresses
```

```
separated by commas (IP address preferred). Enter "None" to disable traps.
[10.48.48.192]>

Enter the Trap Community string.
[ironport]> swa_community

Enterprise Trap Status
1. CPUUtilizationExceeded       Enabled
2. FIPSModeDisableFailure       Enabled
3. FIPSModeEnableFailure        Enabled
4. FailoverHealthy              Enabled
5. FailoverUnhealthy            Enabled
6. connectivityFailure          Disabled
7. keyExpiration                Enabled
8. linkUpDown                   Enabled
9. memoryUtilizationExceeded    Enabled
10. updateFailure               Enabled
11. upstreamProxyFailure        Enabled
Do you want to change any of these settings? [N]> Y

Do you want to disable any of these traps? [Y]> N

Do you want to enable any of these traps? [Y]> Y

Enter number or numbers of traps to enable.  Separate multiple numbers with
commas.
[]> 6

Please enter the URL to check for connectivity failure, followed by the
checking interval in seconds, separated by a comma:
[http://downloads.ironport.com,5]>

Enterprise Trap Status
1. CPUUtilizationExceeded       Enabled
2. FIPSModeDisableFailure       Enabled
3. FIPSModeEnableFailure        Enabled
4. FailoverHealthy              Enabled
5. FailoverUnhealthy            Enabled
6. connectivityFailure          Enabled
7. keyExpiration                Enabled
8. linkUpDown                   Enabled
9. memoryUtilizationExceeded    Enabled
10. updateFailure               Enabled
11. upstreamProxyFailure        Enabled
Do you want to change any of these settings? [N]>

Enter the System Location string.
[location]>

Enter the System Contact string.
[snmp@localhost]>

Current SNMP settings:
Listening on interface "Management" 10.48.48.184/24 port 161.
SNMP v3: Enabled.
SNMP v3 UserName: SNMPMUser
SNMP v3 Authentication type: SHA
SNMP v3 Privacy protocol: AES
SNMP v1/v2: Disabled.
Trap target: 10.48.48.192
Location: location
System Contact: snmp@localhost
```

```
Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]>

SWA_CLI> commit
```

Archivos SWA MIB

Los archivos MIB están disponibles en la URL: https://www.cisco.com/c/en/us/support/security/web-security-appliance/series.html

Utilice la última versión de cada archivo MIB.

Hay varios archivos MIB:

- asyncoswebsecurityappliance-mib.txt es una descripción compatible con SNMPv2 de Enterprise MIB forSecure Web Appliances.
- ASYNCOS-MAIL-MIB.txt es una descripción compatible con SNMPv2 de Enterprise MIB para dispositivos Email Security.
- IRONPORT-SMI.txt Este archivo de "Estructura de la información de administración" define la función del asyncoswebsecurityappliance-mib.

Esta versión implementa un subconjunto de solo lectura de MIB-II como se define en los RFC 1213 y 1907.

Seehttps://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118415-technote-wsa-00.htmlpara obtener más información sobre la supervisión del uso de la CPU en el dispositivo con SNMP.

TRAMPA SNMP SWA

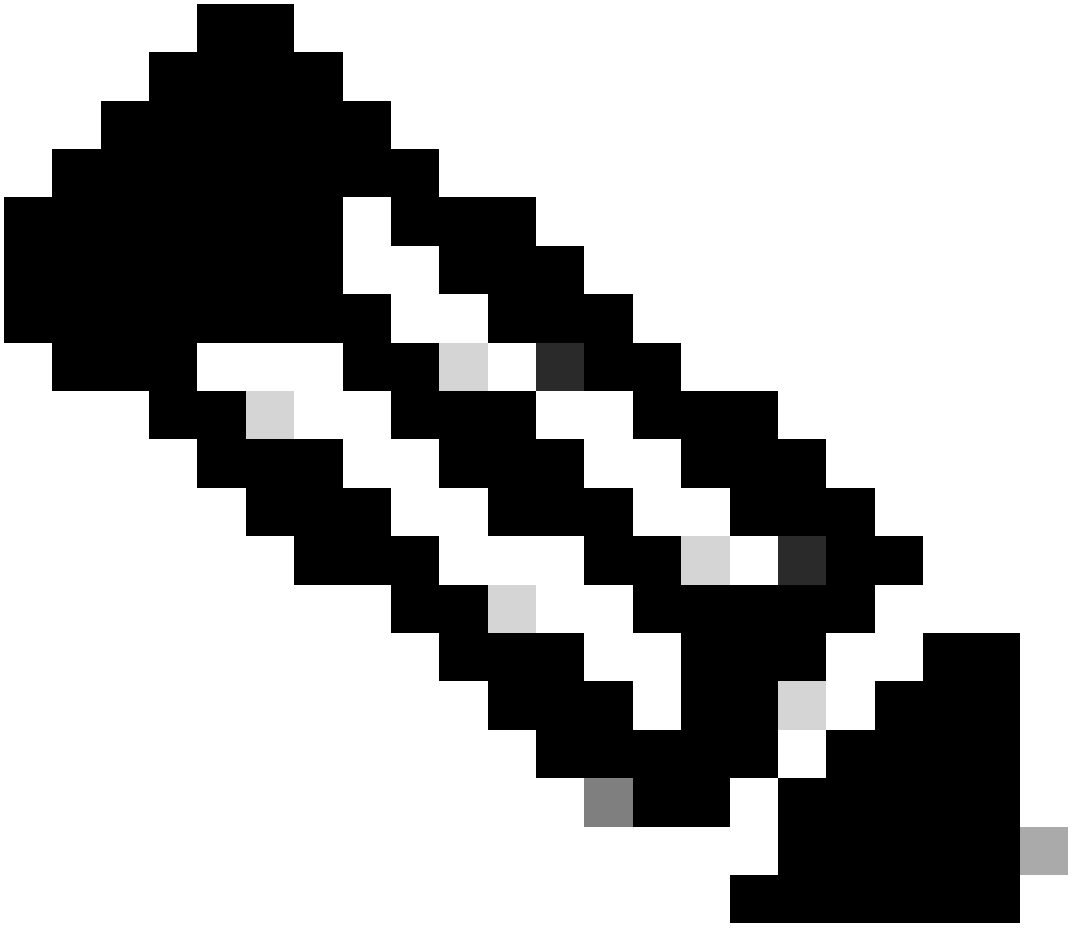
SNMP proporciona la capacidad de enviar trampas, o notificaciones, para avisar a una aplicación de administración cuando se han cumplido una o más condiciones.

Las trampas son paquetes de red que contienen datos relacionados con un componente del sistema que envía la trampa.

Las trampas se generan cuando se cumple una condición en elAgenteSNMP (en este caso, el CiscoSecure Web Appliance).

Una vez cumplida la condición, el SNMPagent forma unSNMPpacket y lo envía al host que ejecuta el software de la consola de administración SNMP.

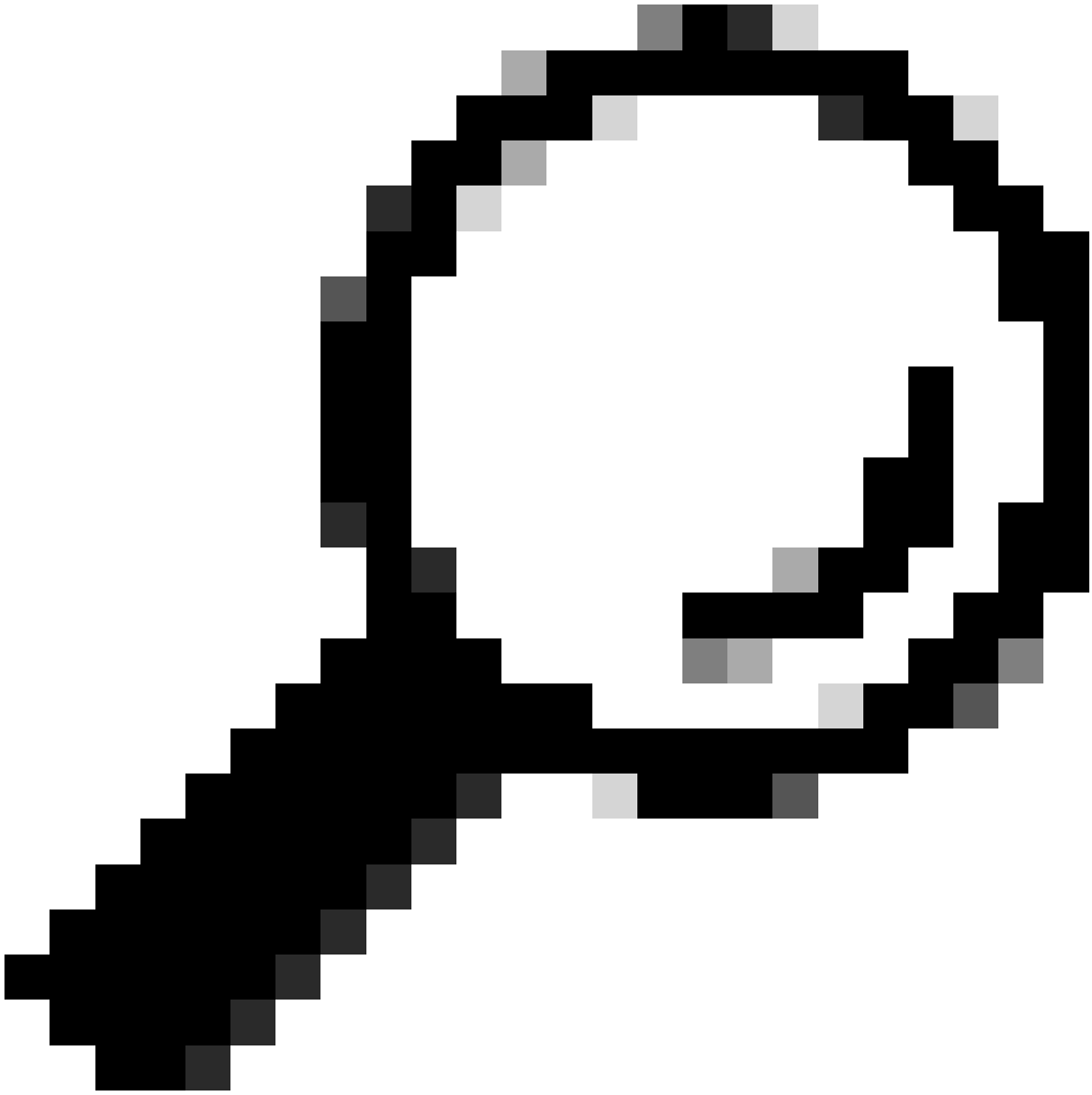
Puede configurarSNMPtraps (activar o desactivar capturas específicas) cuando habilitaSNMPpara una interfaz.



Nota: Para especificar varios destinos de captura: cuando se le solicite el destino de captura, puede introducir hasta 10 direcciones IP separadas por comas.

La trampa connectivityFailure tiene por objeto supervisar la conexión de su dispositivo a Internet. Para ello, intenta conectar y enviar una solicitud GET HTTP a un único servidor externo cada 5 o 7 segundos. De forma predeterminada, la URL supervisada es downloads.ironport.com en el puerto 80.

Para cambiar la URL o el puerto monitoreado, ejecute el comando snmpconfig y habilite la trampa connectityFailure, incluso si ya está habilitada. Puede ver un mensaje para cambiar la dirección URL.



Sugerencia: para simular trampas de falla de conectividad, puede utilizar el comando dnsconfig de la CLI para ingresar un servidor DNS que no funciona. Las búsquedas de downloads.ironport.com fallan y las trampas se envían cada 5-7 segundos. Asegúrese de volver a cambiar el servidor DNS a un servidor que funcione después de que finalice la prueba.

OID de supervisión recomendados

Esta es una lista de las MIB recomendadas para monitorear y no una lista exhaustiva:

OID de hardware	Nombre
1.3.6.1.4.1.15497.1.1.1.18.1.3	raidID
1.3.6.1.4.1.15497.1.1.1.18.1.2	raidStatus

1.3.6.1.4.1.15497.1.1.1.18.1.4	raidLastError
1.3.6.1.4.1.15497.1.1.1.10	fanTable
1.3.6.1.4.1.15497.1.1.1.9.1.2	gradosCelsius

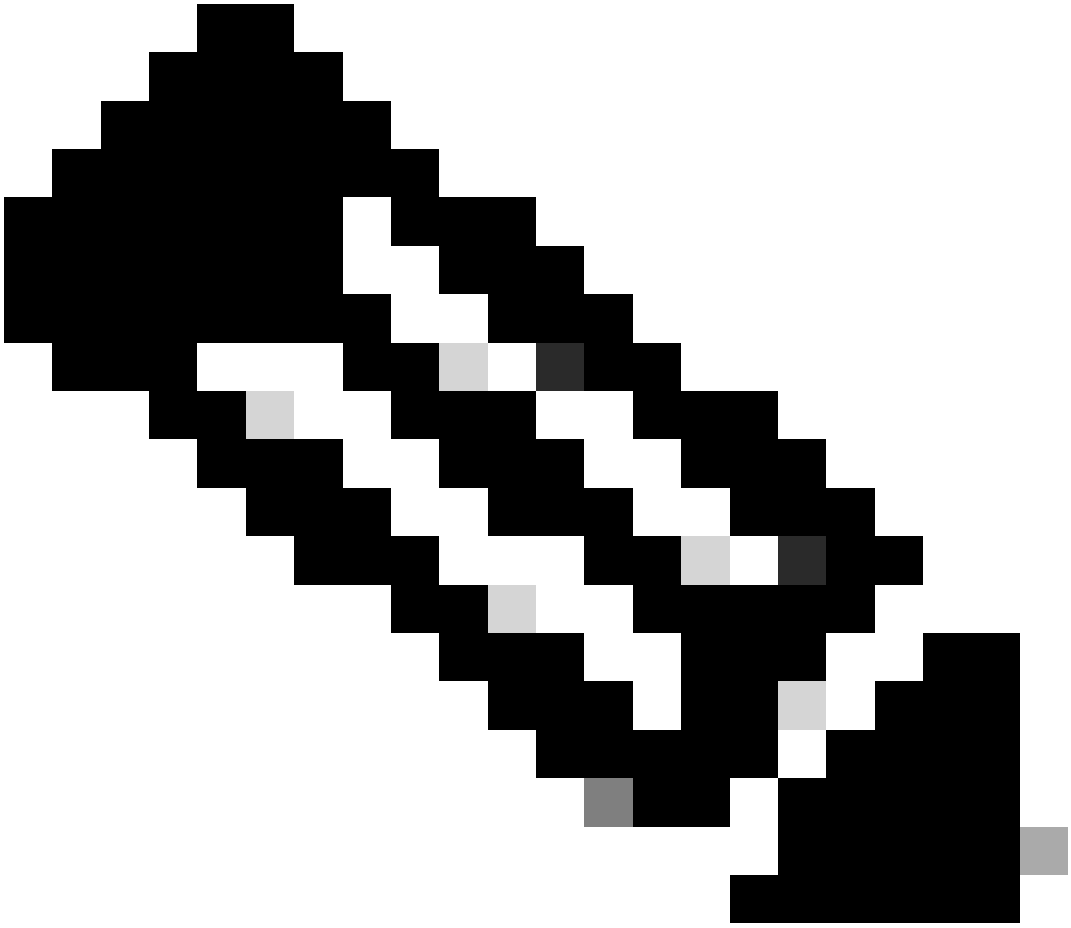
Este es un mapa de OID directamente a la salida del comando status detailCLI:

OID (ID del objeto)	Nombre	Campo de detalle de estado
Recursos del sistema		
1.3.6.1.4.1.15497.1.1.1.2.0	perCentCPUtilization	CPU
1.3.6.1.4.1.15497.1.1.1.1.0	porCientoUtilizaciónMemoria	RAM
Transacciones por segundo		
1.3.6.1.4.1.15497.1.2.3.7.1.1.0	cacheThruputNow	Transacciones promedio por segundo en el último minuto.
1.3.6.1.4.1.15497.1.2.3.7.1.2.0	cacheThruput1hrPeak	Número máximo de transacciones por segundo en la última hora.
1.3.6.1.4.1.15497.1.2.3.7.1.3.0	cacheThruput1hrMean	Transacciones promedio por segundo en la última hora.
1.3.6.1.4.1.15497.1.2.3.7.1.8.0	cacheThruputLifePeak	Número máximo de transacciones por segundo desde el reinicio del proxy.
1.3.6.1.4.1.15497.1.2.3.7.1.9.0	cacheThruputLifeMean	Transacciones medias por segundo desde el reinicio del proxy.
Ancho de banda		
1.3.6.1.4.1.15497.1.2.3.7.4.1.0	cacheBwidthTotalNow	Ancho de banda medio en el último minuto.
1.3.6.1.4.1.15497.1.2.3.7.4.2.0	cacheBwidthTotal1hrPeak	Ancho de banda máximo en la última hora.
1.3.6.1.4.1.15497.1.2.3.7.4.3.0	cacheBwidthTotal1hrMean	Ancho de banda medio en la última hora.
1.3.6.1.4.1.15497.1.2.3.7.4.8.0	cacheBwidthTotalLifePeak	Ancho de banda máximo desde el reinicio del proxy.
1.3.6.1.4.1.15497.1.2.3.7.4.9.0	cacheBwidthTotalLifeMean	Ancho de banda medio desde reinicio del proxy.
Tiempo de respuesta		

1.3.6.1.4.1.15497.1.2.3.7.9.1.0	cacheHitsNow	Tasa promedio de aciertos de caché en el último minuto.
1.3.6.1.4.1.15497.1.2.3.7.9.2.0	cacheHits1hrPeak	Tasa máxima de aciertos de caché en la última hora.
1.3.6.1.4.1.15497.1.2.3.7.9.3.0	cacheHits1hrMean	Tasa promedio de aciertos de caché en la última hora.
1.3.6.1.4.1.15497.1.2.3.7.9.8.0	cacheHitsLifePeak	Tasa de aciertos de caché máxima desde el reinicio del proxy.
1.3.6.1.4.1.15497.1.2.3.7.9.9.0	cacheHitsLifeMean	Tasa media de aciertos de caché desde el reinicio del proxy.
Tasa de aciertos de caché		
1.3.6.1.4.1.15497.1.2.3.7.5.1.0	cacheHitsNow	Tasa promedio de aciertos de caché en el último minuto.
1.3.6.1.4.1.15497.1.2.3.7.5.2.0	cacheHits1hrPeak	Tasa máxima de aciertos de caché en la última hora.
1.3.6.1.4.1.15497.1.2.3.7.5.3.0	cacheHits1hrMean	Tasa promedio de aciertos de caché en la última hora.
1.3.6.1.4.1.15497.1.2.3.7.5.8.0	cacheHitsLifePeak	Tasa de aciertos de caché máxima desde el reinicio del proxy.
1.3.6.1.4.1.15497.1.2.3.7.5.9.0	cacheHitsLifeMean	Tasa media de aciertos de caché desde el reinicio del proxy.
Conexiones		
1.3.6.1.4.1.15497.1.2.3.2.7.0	cacheClientIdleConns	Conexiones de cliente inactivas.
1.3.6.1.4.1.15497.1.2.3.3.7.0	cacheServerIdleConns	Conexiones de servidor inactivas.
1.3.6.1.4.1.15497.1.2.3.2.8.0	cacheClientTotalConns	Conexiones de cliente totales.
1.3.6.1.4.1.15497.1.2.3.3.8.0	cacheServerTotalConns	Conexiones de servidor totales.

Troubleshooting de SNMP

Para ver la conectividad entre SWA y su administrador SNMP, lo mejor es capturar paquetes, puede colocar el filtro de captura de paquetes en: (puerto 161 o puerto 162)



Nota: Este filtro se debe a los puertos SNMP predeterminados. Si ha cambiado los puertos, introduzca los números de puerto configurados en el filtro de captura de paquetes.

Pasos para capturar paquetes de SWA:

Paso 1. inicie sesión en la GUI

Paso 2. En la parte superior derecha, seleccione Soporte y Ayuda

Paso 3. seleccione Captura de paquetes

Paso 4. seleccione Editar configuración

Paso 5. Asegúrese de que se ha seleccionado la interfaz correcta

Paso 6. Introduzca las condiciones de filtrado.

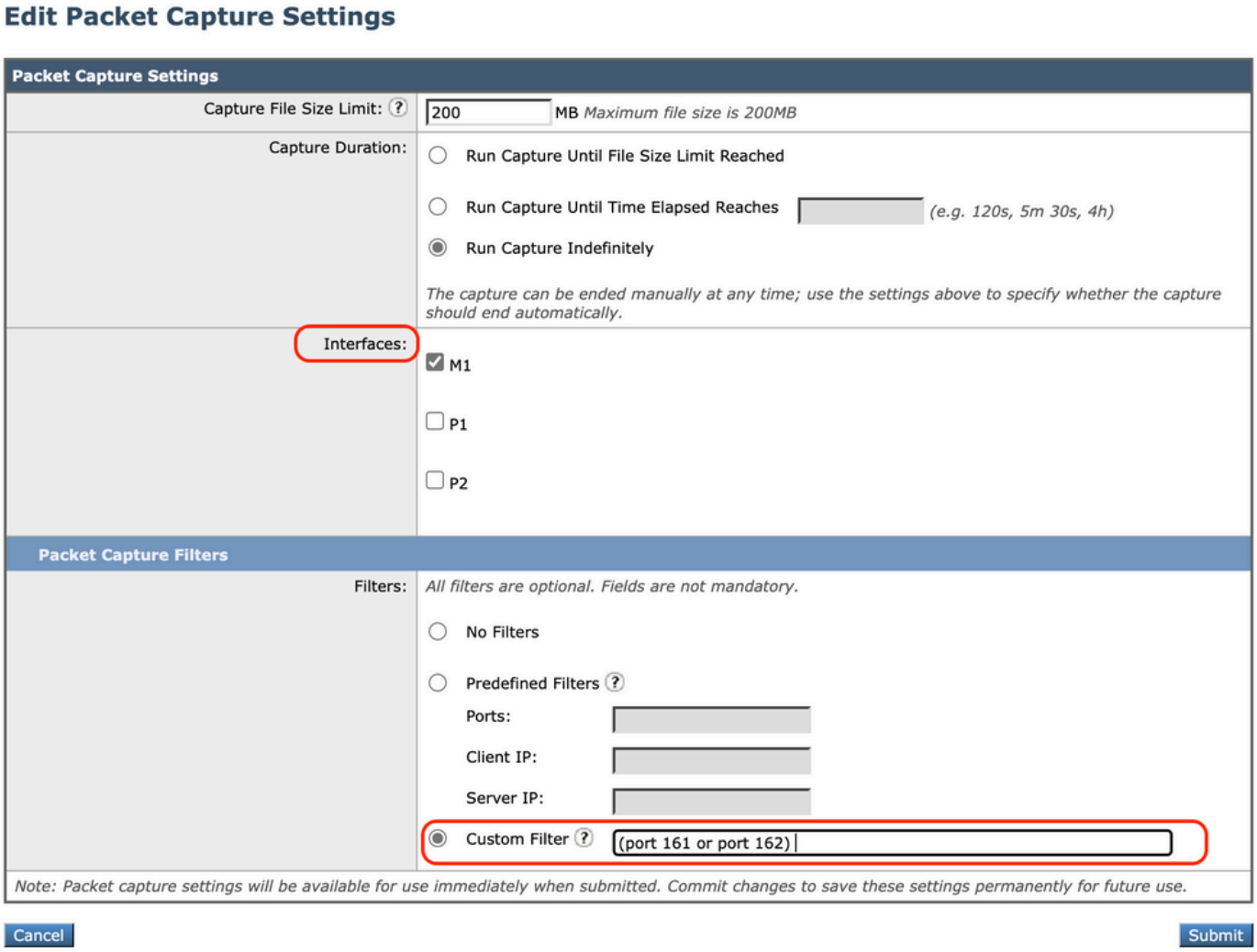
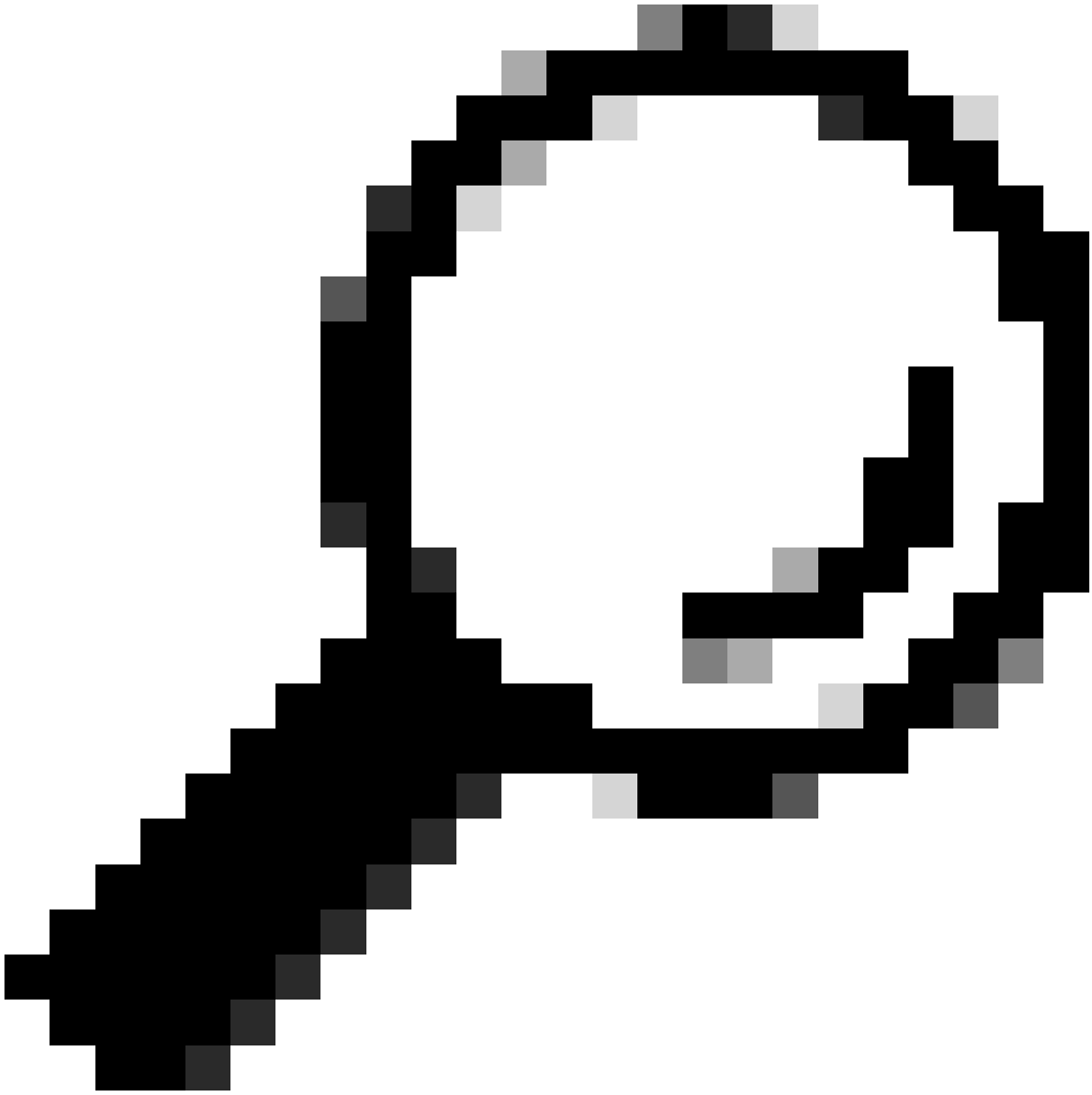


Imagen: Configurar filtros de captura de paquetes

Paso 7. Elija Enviar

Paso 8. Seleccione Iniciar captura.



Sugerencia: puede descifrar capturas de paquetes SNMPv3 con Wireshark. Para obtener más información, visite este enlace: [How-to-decrypt-snmpv3-packets-using-wireshark]

SNMPWALK

snmpwalk es el nombre dado a una aplicación SNMP que ejecuta varias solicitudes GET-NEXT automáticamente. La solicitud SNMP GET-NEXT se utiliza para consultar un dispositivo habilitado y tomar datos SNMP de un dispositivo. El comando snmpwalk se utiliza porque permite al usuario encadenar solicitudes GET-NEXT sin tener que ingresar comandos únicos para cada OID o nodo dentro de un subárbol

Instalación de SNMPWALK en sistemas operativos Windows

Para los usuarios de Microsoft Windows, primero debe descargar la herramienta.

Instalar SNMPWALK en el kernel de Linux

```
#For Redhat, Fedora, CentOs:
yum install net-snmp-utils

#For Ubuntu:
apt-get install snmp
```

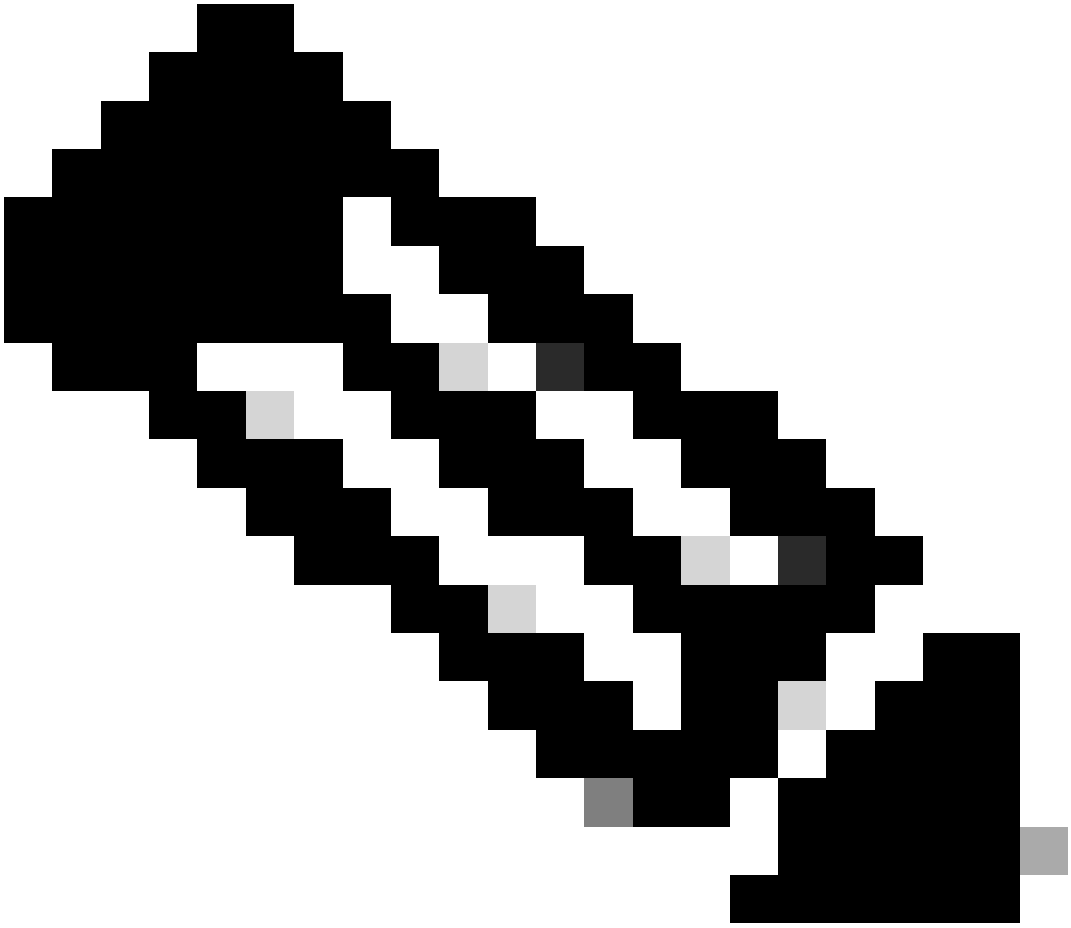
Instalar SNMPWALK en MacOS

De forma predeterminada, snmpwalk está instalado en MacOS

Para generar una solicitud GET de SNMP, puede utilizar el comando snmpwalk desde otro equipo de la red que tenga conectividad con SWA. A continuación se muestran algunos ejemplos del comando snmpwalk:

```
snmpwalk -v2c -c <Community Name>  <SWA IP Address>

snmpwalk -v3 -l authPriv  -u v3get  -a SHA -A <Password>  -x AES -X <Password>  <SWA IP Address>
```



Nota: Puede elegir establecer el nivel de seguridad en noAuthNoPriv o authNoPriv o authPriv depende de las configuraciones SWA.

SNMPTRAP

snmptrap es un comando CLI oculto que requiere que SNMP esté habilitado en el SWA. Puede generar capturas de SNMP seleccionando el objeto y las capturas. A continuación se incluye un ejemplo:

```
SWA_CLI>nmptrap

1. CPUUtilizationExceeded
2. FIPSModeDisableFailure
3. FIPSModeEnableFailure
4. FailoverHealthy
5. FailoverUnhealthy
6. connectivityFailure
7. keyExpiration
```

```
8. linkUpDown
9. memoryUtilizationExceeded
10. updateFailure
11. upstreamProxyFailure
Enter the number of the trap you would like to send.
[]> 8

1. CPUUtilization
2. FIPSApplicationName
3. FailoverApplicationName
4. RAIDEvents
5. RAIDID
6. connectionURL
7. ifIndex
8. ip
9. keyDescription
10. memoryUtilization
11. raidStatus
12. updateServiceName
Enter the number of the object you would like to send.
[]> 8

Enter the trap value.
[]> 10.20.3.15

Enter the user name
[admin]> SNMPuser

Please select Trap Protocol version:
1. 2c
2. 3
[1]> 2
```

Registros SNMP en SWA

SWA tiene dos registros relacionados con SNMP. Algunos tipos de registro relacionados con el componente de proxy web no están activados. Puede activarlos desde:

- En la GUI:Administración del sistema > Suscripciones de registro
- En CLI: logconfig > new

Tipo de archivo de registro	Descripción	¿Admite Syslog Push?	¿Habilitado de forma predeterminada?
Registros SNMP	Registra los mensajes de depuración relacionados con el motor de administración de red SNMP.	Yes	Yes

Registros del módulo SNMP	Registra mensajes de proxy web relacionados con la interacción con el sistema de supervisión SNMP.	No	No

Problemas comunes con SNMP

Algunos OIDS fallan (sin valor o valor incorrecto).

Este problema está relacionado con la extracción de SNMP. Aquí hay dos ejemplos de salida esperada y salida con error:

```
Sample Output without Error:
$ snmpwalk -O a -v 3 -M "/var/lib/mibs/" -m "ALL" -l authPriv -a MD5 -x DES -u v3get -A xxx -X xxx proxy
iso.3.6.1.4.1.15497.1.1.1.9.1.1.1 = INTEGER: 1
iso.3.6.1.4.1.15497.1.1.1.9.1.2.1 = INTEGER: 22
iso.3.6.1.4.1.15497.1.1.1.9.1.3.1 = STRING: "Ambient"

Sample Output with Error:
$ snmpwalk -O a -v 3 -M "/var/lib/mibs/" -m "ALL" -l authPriv -a MD5 -x DES -u v3get -A xxx -X xxx proxy
iso.3.6.1.4.1.15497.1.1.1.9 = No Such Instance currently exists at this OID
```

Puede verificar si hay "fallas de la aplicación" en snmp_logs

Puede verificar snmp_logs desde CLI > grep > elija el número asociado con snmp_logs:

```
SWA_CLI> grep

Currently configured logs:
1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
2. "adc_logs" Type: "ADC Engine Logs" Retrieval: FTP Poll
...
37. "snmp_logs" Type: "SNMP Logs" Retrieval: FTP Poll
...
Enter the number of the log you wish to grep.
[]> 37

Enter the regular expression to grep.
[]>

Do you want this search to be case insensitive? [Y]>

Do you want to search for non-matching lines? [N]>

Do you want to tail the logs? [N]> y

Do you want to paginate the output? [N]>
```

Referencia

Guía del usuario de AsyncOS 15.0 para Cisco Secure Web Appliance - LD (implementación limitada) - Resolución de problemas [Cisco Secure Web Appliance] - Cisco

Cálculo del Uso de CPU Proxy en el WSA Usando SNMP - Cisco

snmpcmd(1) (freebsd)

snmptrap (freebsd)

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).