Configurar e solucionar problemas de SNMP em SWA

Contents

- Introdução
- Pré-requisitos
  - Requisitos
  - Componentes Utilizados
- Como funciona o SNMP
  - MIB
  - Interceptação SNMP
  - SNMPv3
- SNMP em SWA
  - Configurando oSNMPMonitor
  - Arquivos MIB SWA
  - INTERCEPTAÇÃO SNMP DE SWA
  - OIDs de monitoramento recomendados
- Solucionar problemas do SNMP
  - SNMPWALK
    - Instalar o SNMPWALK em sistemas operacionais Windows
    - Instale o SNMPWALK no kernel do Linux
    - Instalar o SNMPWALK no MacOS
  - SNMPTRAP
  - Logs SNMP em SWA
  - Problemas comuns com SNMP
    - Alguns OIDS falham (nenhum valor ou valor incorreto).

Introdução

Este documento descreve as etapas para solucionar problemas do SNMP (Simple Network Monitoring Protocol) no Secure Web Appliance (SWA).

Pré-requisitos

Requisitos

A Cisco recomenda o conhecimento destes tópicos:

- Acesso à interface de linha de comando (CLI)do SWA
- Acesso administrativo ao SWA.

- Conhecimento básico do SNMP.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Como funciona o SNMP

O SNMP é um protocolo de comunicação da camada de aplicação que permite aos dispositivos de rede trocar informações de gerenciamento entre esses sistemas e com outros dispositivos fora da rede.

Através do SNMP, os administradores de rede podem gerenciar o desempenho da rede, encontrar e resolver problemas de rede e planejar o crescimento da rede.

O SNMP torna o monitoramento de rede mais econômico e permite que sua rede seja mais confiável. (Para obter mais informações sobreSNMP, consulte RFCs 1065, 1066 e 1067.)

Uma rede gerenciada por SNMP consiste em um gerenciador, agentes e dispositivos gerenciados.

- O gerenciador fornece a interface entre o gerenciador de rede humana e o sistema de gerenciamento.
- O Agente fornece a interface entre o gerenciador e o dispositivo que está sendo gerenciado
- Os sistemas de gerenciamento executam a maioria dos processos de gerenciamento e fornecem a maior parte dos recursos de memória usados para o gerenciamento de rede.

Um agente reside em cada dispositivo gerenciado e converte dados de informações de gerenciamento local (como informações de desempenho ou informações de eventos e erros) capturados em armadilhas de software, em uma forma legível para o sistema de gerenciamento.

O agente SNMP captura dados da MIB (Management Information Base, base de informações de gerenciamento) (parâmetros de dispositivos e repositórios de dados de rede) ou de armadilhas de erro ou alteração.

MIB

A MIB é uma estrutura de dados que descreve elementos de rede SNMP como uma lista de objetos de dados. O gerenciador SNMP deve compilar o arquivo MIB para cada tipo de equipamento na rede para monitorar dispositivos SNMP.

O gerenciador e o agente usam uma MIB e um conjunto relativamente pequeno de comandos para trocar informações. A MIB é organizada em uma estrutura de árvore com variáveis

individuais sendo representadas como folhas nos ramos.

Uma tag numérica longa ou um identificador de objeto (OID) é usado para distinguir cada variável exclusivamente na MIB e em mensagens SNMP. A MIB associa cada OID a um rótulo legível e a vários outros parâmetros relacionados ao objeto.

A MIB serve então como um dicionário de dados ou livro de códigos que é usado para montar e interpretar mensagens SNMP.

Quando o gerenciador SNMP deseja saber o valor de um objeto, como o estado de um ponto de alarme, o nome do sistema ou o tempo de atividade do elemento, ele monta um pacote GET que inclui o OID para cada objeto de interesse.

O elemento recebe a solicitação e pesquisa cada OID em seu livro de códigos (MIB). Se o OID for encontrado (o objeto é gerenciado pelo elemento), um pacote de resposta será montado e enviado com o valor atual do objeto incluído.

Se o OID não for encontrado, uma resposta de erro especial será enviada, identificando o objeto não gerenciado

Interceptação SNMP

As armadilhas de SNMP permitem que um agente notifique a estação de gerenciamento sobre eventos significativos por meio de uma mensagem SNMP não solicitada.

O SNMPv1 e o SNMPv2c, junto com a MIB associada, incentivam a notificação direcionada por interceptação (trap-directed notification).

A ideia por trás da notificação direcionada por interceptação (trapping) é que se um gerenciador é responsável por um grande número de dispositivos, e cada dispositivo tem um grande número de objetos, é impraticável para o gerenciador pesquisar ou solicitar informações de cada objeto em cada dispositivo.

A solução é que cada agente no dispositivo gerenciado notifique o gerente sem solicitação. Ele faz isso enviando uma mensagem conhecida como Interceptação do evento.

Depois que o gerente recebe o evento, ele o exibe e pode optar por executar uma ação com base no evento. Por exemplo, o gerenciador pode pesquisar o agente diretamente ou pesquisar outros agentes de dispositivos associados para entender melhor o evento.

A notificação direcionada por interceptação (trapping) pode resultar em economias substanciais de recursos de rede e de agente, eliminando a necessidade de solicitações de SNMP frívolas. No entanto, não é possível eliminar totalmente as chamadas seletivas de SNMP.

Solicitações SNMP são necessárias para alterações de detecção e topologia. Além disso, um agente de dispositivo gerenciado não pode enviar uma armadilha, se o dispositivo tiver tido uma interrupção catastrófica.

As interceptações SNMPv1 são definidas no RFC 1157, com estes campos:

- Enterprise:identifica o tipo de objeto gerenciado que gera o trap.
- Endereço do agente: fornece o endereço do objeto gerenciado que gera o desvio.
- Tipo de interceptação genérica:Indica um dentre vários tipos de interceptação genérica.
- Código de armadilha específico:Indica um de vários códigos de armadilha específicos.
- Timestamp: Fornece a quantidade de tempo decorrido entre a última reinicialização da rede e a geração do trap.
- Vinculações de variáveis: o campo de dados da armadilha que contém PDU. Cada vinculação de variável associa uma determinada instância de objeto MIB ao seu valor atual.

SNMPv3

O SNMPv3 suporta o identificador "Engine ID" SNMP, identificando exclusivamente cada entidade SNMP. Podem ocorrer conflitos se duas entidades SNMP tiverem EngineIDs duplicados.

O EngineID é usado para gerar a chave para mensagens autenticadas. (Para obter mais informações sobre o SNMPv3, consulte RFCs 2571-2575.)

Muitos produtos SNMP permanecem basicamente os mesmos no SNMPv3, mas são aprimorados por estes novos recursos:

Security

- Autenticação
- Privacidade

Administração

- Autorização e controle de acesso
- Contextos lógicos
- Nomeação de entidades, identidades e informações
- Pessoas e políticas
- Nomes de usuário e gerenciamento de chaves
- Destinos de notificação e relações de proxy
- Configuração remota via operações SNMP

Os modelos de segurança SNMPv3 vêm principalmente de duas formas, como autenticação e criptografia.

A autenticação é usada para garantir que somente o destinatário pretendido leia interceptações. À medida que as mensagens são criadas, elas recebem uma chave especial baseada no EngineID da entidade. A chave é compartilhada com o destinatário desejado e usada para receber a mensagem.
Criptografia, privacidade criptografa o payload da mensagem SNMP para garantir que usuários não autorizados não possam lê-la. Qualquer interceptação preenchida com caracteres distorcidos

é ilegível. A privacidade é especialmente útil em aplicativos em que as mensagens SNMP devem ser roteadas pela Internet.
Há três níveis de segurança em um grupo SNMP:

noAuthnoPriv - Comunicação sem autenticação e privacidade.
authNoPriv - Comunicação com autenticação e sem privacidade. Os protocolos usados para autenticação são o algoritmo Message-Digest 5 (MD5) e o Algoritmo de Hash Seguro (SHA).
authPriv - Comunicação com autenticação e privacidade. Os protocolos usados para Autenticação são MD5 e SHA, e para Privacidade, podem ser usados os protocolos Padrão de Criptografia de Dados (DES - Data Encryption Standard) e Padrão de Criptografia Avançada (AES - Advanced Encryption Standard).

SNMP em SWA

O sistema operacional AsyncOS oferece suporte à monitoração de status do sistema via SNMP.

Observação:

- SNMPisofpor padrão.
- As operações SNMPSET (configuração) não estão implementadas.
- AsyncOS suporta SNMPv1, v2 e v3.
- A autenticação e a criptografia de mensagens são obrigatórias ao habilitar o SNMPv3. As senhas para autenticação e criptografia devem ser diferentes.
- O algoritmo de criptografia pode ser AES (recomendado) ou DES.
- O algoritmo de autenticação pode ser SHA-1 (recomendado) ou MD5.
- O comando nmpconfig "lembra" suas senhas na próxima vez que você executar o comando.
- Para versões do AsyncOS anteriores à 15.0, o nome de usuário SNMPv3 é: v3get.
- Para o AsyncOS versão 15.0 e posterior, o nome de usuário SNMPv3 padrão é: v3get. Como administrador, você pode optar por qualquer outro nome de usuário.
- Se você usar somenteSNMPv1 ouSNMPv2, deverá definir uma sequência de caracteres de comunidade. A sequência de caracteres de comunidade não assume o padrão public.
- ParaSNMPv1 eSNMPv2, você deve especificar uma rede da qual as solicitações SNMPGET são aceitas.
- Para usar interceptações, um gerenciador SNMP (não incluído no AsyncOS) deve estar em execução e seu endereço IP deve ser inserido como destino de interceptação. (Você pode usar um nome de host, mas se fizer isso, as interceptações só funcionarão se o DNS estiver funcionando.)

Configurando oSNMPMonitor

Para configurar o SNMPpara coletar informações de status do sistema para o equipamento, use o comando nmpconfig na CLI. Depois que você escolhe e configura valores para uma interface, o equipamento responde às solicitações SNMPv3 GET.

Ao usarSNMP, considere estes pontos:

- No SNMP versão 3, as solicitações devem incluir uma senha correspondente.
- Por padrão, as solicitações de versão 1 e 2 são rejeitadas.
- Se habilitadas, as solicitações de versão 1 e 2 devem ter uma sequência de comunidade correspondente.

```
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
```

Arquivos MIB SWA

Os arquivos MIB estão disponíveis no URL: https://www.cisco.com/c/en/us/support/security/web-security-appliance/series.html

Use a versão mais recente de cada arquivo MIB.

Há vários arquivos MIB:

- asyncoswebsecurityappliance-mib.txt é uma descrição compatível com SNMPv2 do Enterprise MIB paraSecure Web Appliances.
- ASYNCOS-MAIL-MIB.txt é uma descrição compatível com SNMPv2 da MIB empresarial para dispositivos de segurança de e-mail.
- IRONPORT-SMI.txt Este arquivo de "Estrutura de Informações de Gerenciamento" define a função do asyncoswebsecurityappliance-mib.

Esta versão implementa um subconjunto somente leitura de MIB-II conforme definido nas RFCs 1213 e 1907.

Seehttps://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118415-technote-wsa-00.htmlpara saber mais sobre o monitoramento de uso da CPU no dispositivo comSNMP.

INTERCEPTAÇÃO SNMP DE SWA

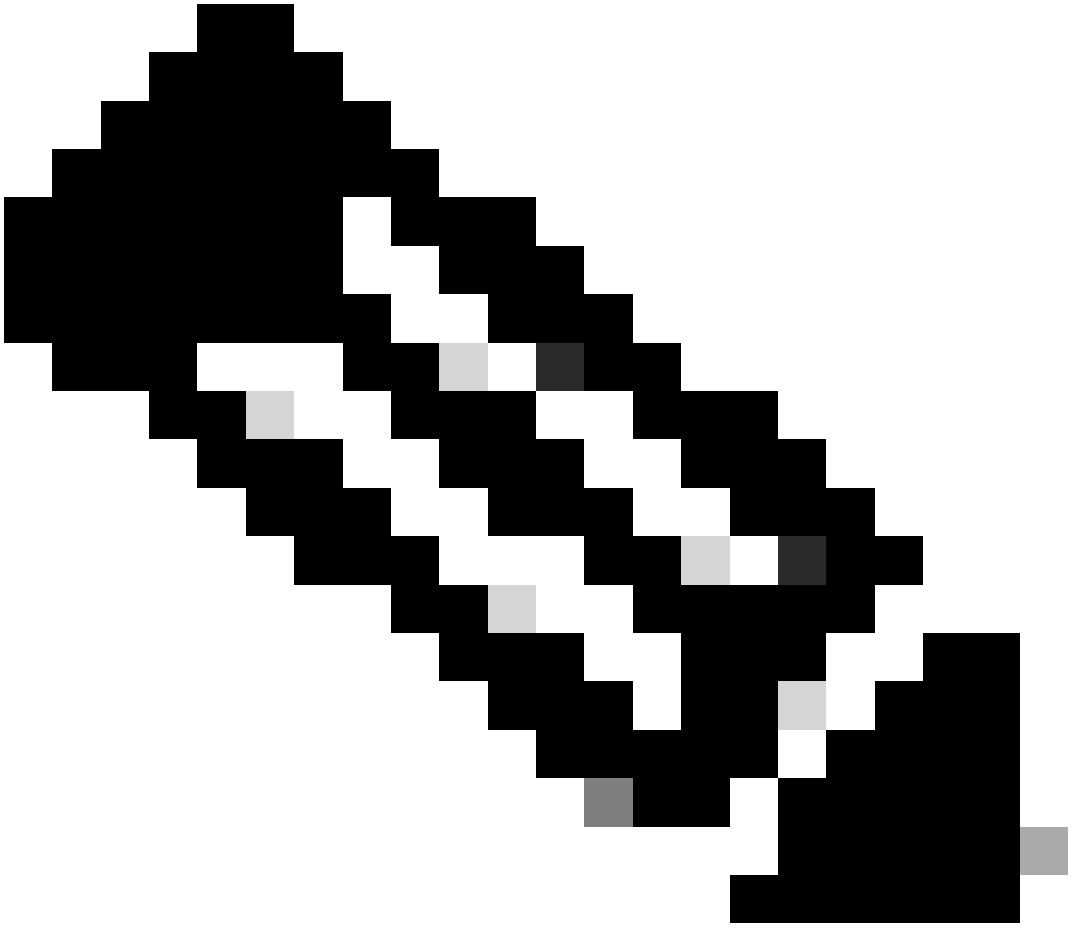
O SNMPfornece a capacidade de enviar interceptações, ou notificações, para aconselhar um aplicativo administrativo quando uma ou mais condições forem atendidas.

Traps são pacotes de rede que contêm dados relacionados a um componente do sistema que está enviando a interceptação.

As interceptações são geradas quando uma condição é atendida no agenteSNMP (nesse caso, o CiscoSecure Web Appliance).

Depois que a condição for atendida, o agente SNMP formará um pacote SNMP e o enviará ao host que executa o software do console de gerenciamento SNMP.

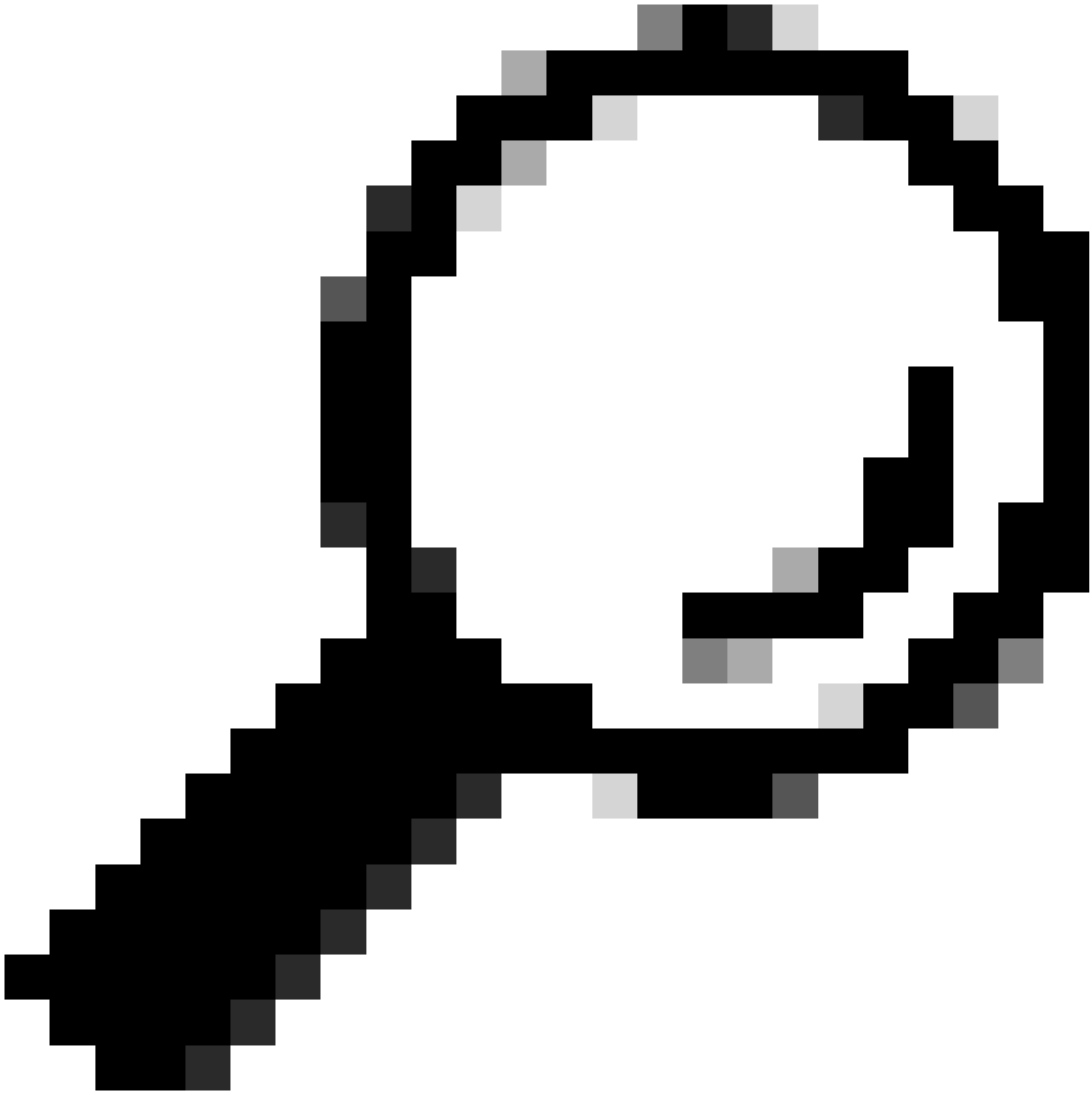
Você pode configurarSNMPtraps (habilitar ou desabilitar interceptações específicas) ao habilitarSNMPpara uma interface.



Observação: Para especificar vários destinos de interceptação: quando solicitado, você pode inserir até 10 endereços IP separados por vírgula.

A armadilha connectivityFailure tem como objetivo monitorar a conexão do seu dispositivo com a Internet. Ele faz isso tentando se conectar e enviar uma solicitação HTTP GET a um único servidor externo a cada 5 a 7 segundos. Por padrão, o URL monitorado é downloads.ironport.com na porta 80.

Para alterar a URL ou porta monitorada, execute o comando snmpconfig e habilite a interceptação connectionFailure, mesmo que ela já esteja habilitada. Você pode ver um prompt para alterar o URL.



Dica: para simular armadilhas connectivityFailure, você pode usar o comando CLI dnsconfig para inserir um servidor DNS inoperante. As pesquisas por downloads.ironport.com falham e as interceptações são enviadas a cada 5-7 segundos. Certifique-se de alterar o servidor DNS de volta para um servidor em funcionamento após o término do teste.

OIDs de monitoramento recomendados

Esta é uma lista das MIBs recomendadas para monitorar e não uma lista exaustiva:

OID de Hardware	Nome
1.3.6.1.4.1.15497.1.1.1.18.1.3	ID de raid
1.3.6.1.4.1.15497.1.1.1.18.1.2	status de raid

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	graus Celsius

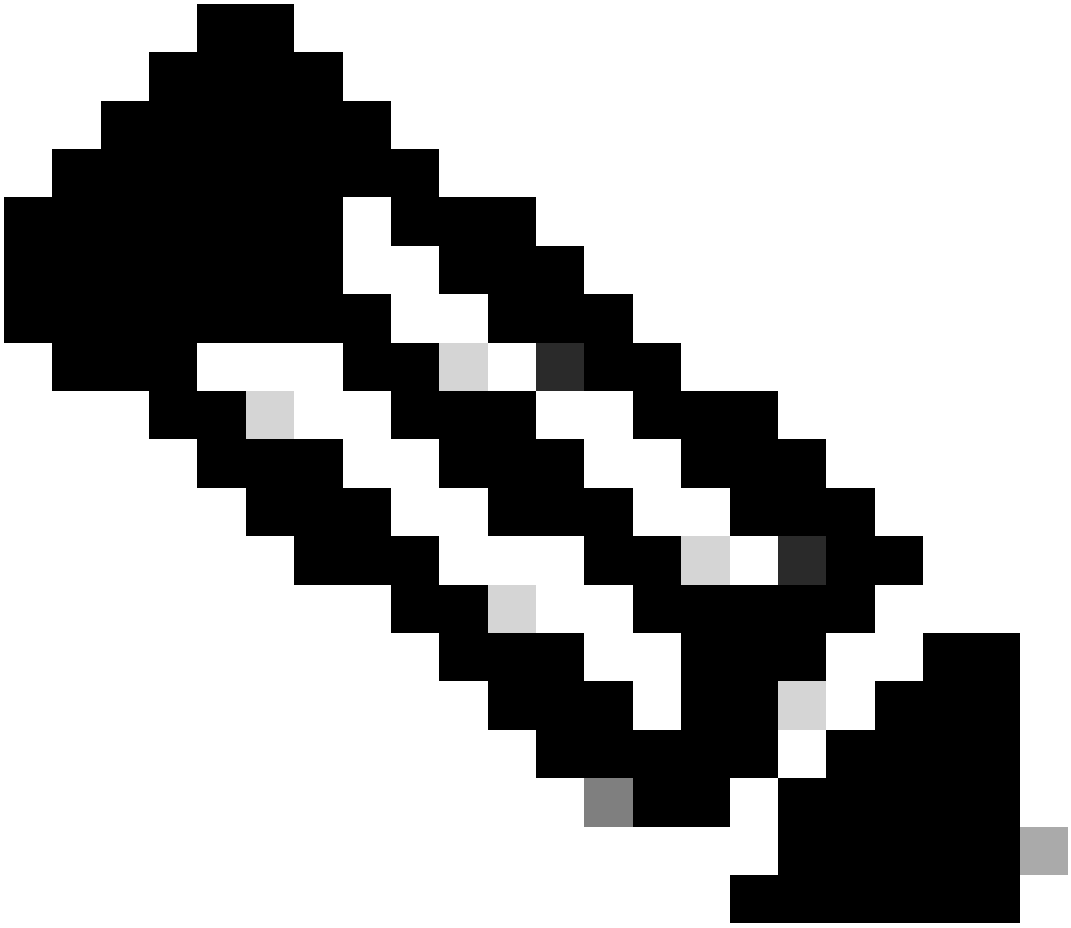
Os OIDs são mapeados diretamente para a saída do comando status detailCLI:

OID	Nome	Campo de detalhe de status
Recursos do sistema		
1.3.6.1.4.1.15497.1.1.1.2.0	perCentCPUtilização	CPU
1.3.6.1.4.1.15497.1.1.1.1.0	utilização de memória perCent	RAM
Transações por segundo		
1.3.6.1.4.1.15497.1.2.3.7.1.1.0	cacheThruputNow	Média de transações por segundo no último minuto.
1.3.6.1.4.1.15497.1.2.3.7.1.2.0	cacheThruput1hrPeak	Máximo de transações por segundo na última hora.
1.3.6.1.4.1.15497.1.2.3.7.1.3.0	cacheThruput1hrMédia	Média de transações por segundo na última hora.
1.3.6.1.4.1.15497.1.2.3.7.1.8.0	cacheThruputLifePeak	Máximo de transações por segundo desde a reinicialização do proxy.
1.3.6.1.4.1.15497.1.2.3.7.1.9.0	cacheThruputLifeMean	Média de transações por segundo desde a reinicialização do proxy.
Largura de banda		
1.3.6.1.4.1.15497.1.2.3.7.4.1.0	larguraLarguraCacheTotalAgora	Largura de banda média no último minuto.
1.3.6.1.4.1.15497.1.2.3.7.4.2.0	cacheBwidthTotal1hrPeak	Largura de banda máxima na última hora.
1.3.6.1.4.1.15497.1.2.3.7.4.3.0	cacheBwidthTotal1hrMédia	Largura de banda média na última hora.
1.3.6.1.4.1.15497.1.2.3.7.4.8.0	cacheBwidthTotalLifePeak	Largura de banda máxima desde a reinicialização do proxy.
1.3.6.1.4.1.15497.1.2.3.7.4.9.0	cacheBwidthTotalLifeMean	Largura de banda média desde a reinicialização do proxy.
Tempo de resposta		

1.3.6.1.4.1.15497.1.2.3.7.9.1.0	acertos de cacheAgora	Taxa média de acertos do cache no último minuto.
1.3.6.1.4.1.15497.1.2.3.7.9.2.0	cacheHits1hrPeak	Taxa máxima de acertos do cache na última hora.
1.3.6.1.4.1.15497.1.2.3.7.9.3.0	cacheHits1hrMédia	Taxa média de acertos do cache na última hora.
1.3.6.1.4.1.15497.1.2.3.7.9.8.0	cacheHitsLifePeak	Taxa máxima de acertos no cache desde a reinicialização do proxy.
1.3.6.1.4.1.15497.1.2.3.7.9.9.0	CacheHitsLifeMean	Taxa média de acertos no cache desde a reinicialização do proxy.
Taxa de acertos do cache		
1.3.6.1.4.1.15497.1.2.3.7.5.1.0	acertos de cacheAgora	Taxa média de acertos do cache no último minuto.
1.3.6.1.4.1.15497.1.2.3.7.5.2.0	cacheHits1hrPeak	Taxa máxima de acertos do cache na última hora.
1.3.6.1.4.1.15497.1.2.3.7.5.3.0	cacheHits1hrMédia	Taxa média de acertos do cache na última hora.
1.3.6.1.4.1.15497.1.2.3.7.5.8.0	cacheHitsLifePeak	Taxa máxima de acertos no cache desde a reinicialização do proxy.
1.3.6.1.4.1.15497.1.2.3.7.5.9.0	CacheHitsLifeMean	Taxa média de acertos no cache desde a reinicialização do proxy.
Conexões		
1.3.6.1.4.1.15497.1.2.3.2.7.0	cacheClientIdleConns	Conexões de cliente ociosas.
1.3.6.1.4.1.15497.1.2.3.3.7.0	cacheServidorIdleConns	Conexões de servidor ociosas.
1.3.6.1.4.1.15497.1.2.3.2.8.0	TotalConnsClienteCache	Total de conexões de cliente.
1.3.6.1.4.1.15497.1.2.3.3.8.0	TotalConnsServidorCache	Total de conexões do servidor.

Solucionar problemas do SNMP

Para visualizar a conectividade entre o SWA e o gerenciador SNMP, é melhor capturar os pacotes. Você pode colocar o filtro de captura de pacotes em: (porta 161 ou porta 162)



Observação: esse filtro é devido às portas SNMP padrão. Se você tiver alterado as portas, coloque os números de porta configurados no filtro de captura de pacotes.

Etapas para capturar pacotes de SWA:

Etapa 1. iniciar sessão na GUI

Etapa 2. na parte superior direita, escolha Suporte e Ajuda

Etapa 3. selecione Captura de pacotes

Etapa 4. escolha Editar configurações

Etapa 5. Verifique se a interface correta foi selecionada

Etapa 6. Insira as condições do filtro.

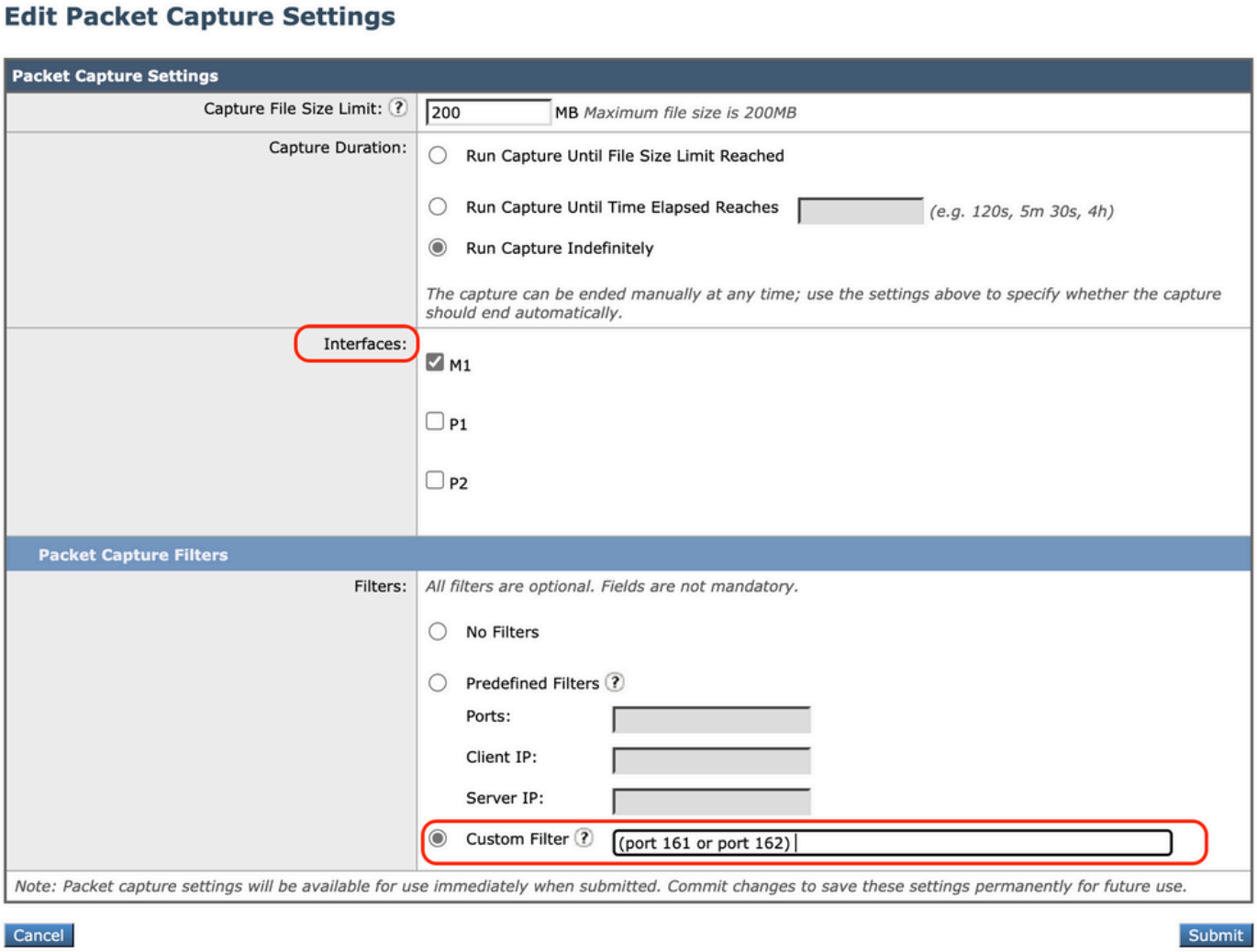
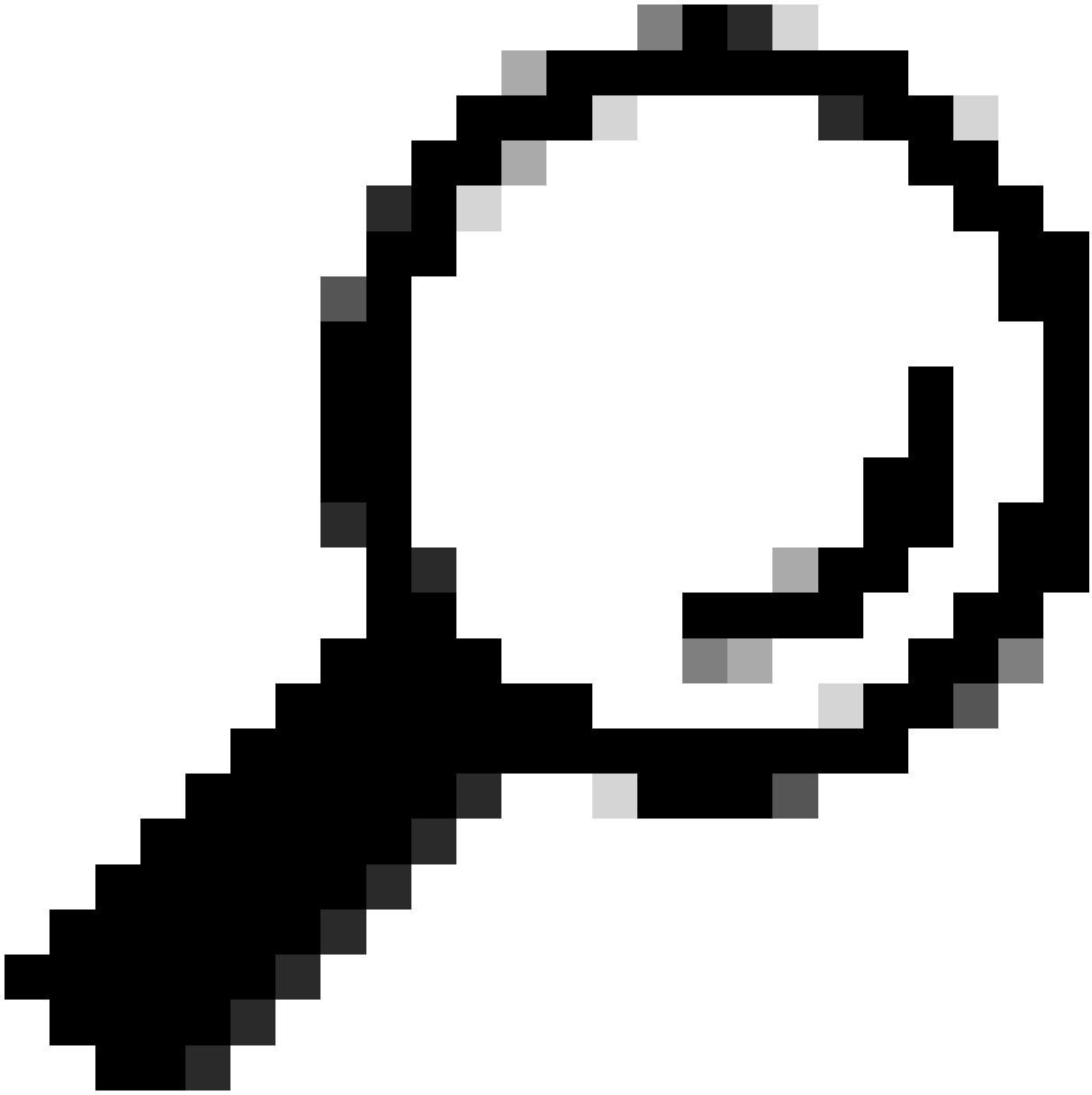


Imagem - Configurar filtros de captura de pacotes

Passo 7. Escolha Enviar

Etapa 8. Escolha Iniciar captura.



Dica: você pode descriptografar capturas de pacotes SNMPv3 com o Wireshark. para obter mais informações, visite este link: How-to-decrypt-snmpv3-packets-using-wireshark

SNMPWALK

snmpwalk é o nome dado a um aplicativo SNMP que executa várias solicitações GET-NEXT automaticamente. A solicitação SNMP GET-NEXT é usada para consultar um dispositivo habilitado e obter dados SNMP de um dispositivo. O comando snmpwalk é usado porque permite que o usuário encadeie solicitações GET-NEXT sem ter que inserir comandos exclusivos para cada OID ou nó em uma subárvore

Instalar o SNMPWALK em sistemas operacionais Windows

Para usuários do Microsoft Windows, primeiro é necessário fazer o download da ferramenta.

Instale o SNMPWALK no kernel do Linux

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

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

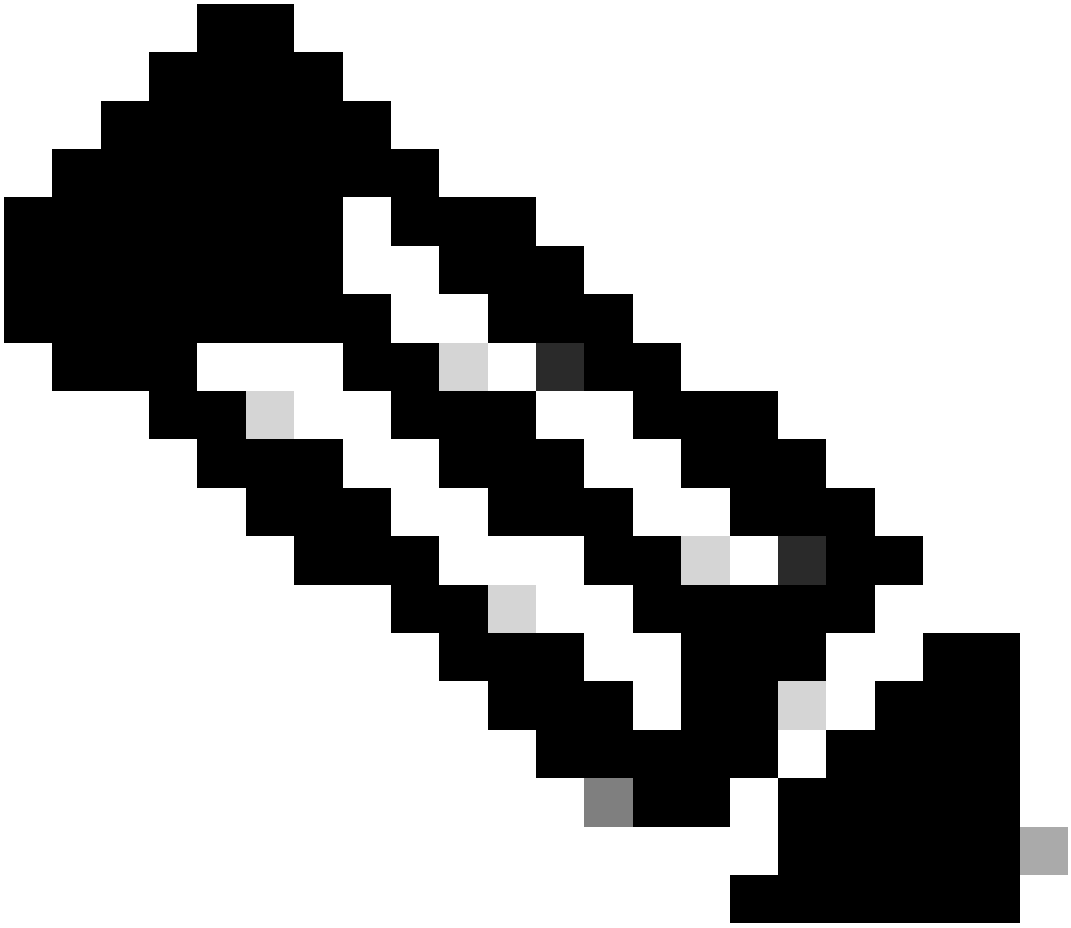
Instalar o SNMPWALK no MacOS

Por padrão, o snmpwalk é instalado no MacOS

Para gerar uma solicitação SNMP GET, você pode usar o comando snmpwalk de outro computador na rede que tenha conectividade com o SWA. Aqui estão alguns exemplos do 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>
```



Observação: você pode escolher definir o nível de segurança como noAuthNoPriv ou authNoPriv ou authPriv depende das configurações de SWA.

SNMPTRAP

snmptrap é um comando oculto da CLI que exigia que o SNMP fosse habilitado no SWA. Você pode gerar o trap SNMP selecionando o objeto, e o trap, aqui está um exemplo:

```
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
```

Logs SNMP em SWA

O SWA tem dois logs relacionados ao SNMP. Alguns tipos de log relacionados ao componente de proxy da Web não estão habilitados. Você pode habilitá-los em:

- Na GUI :Administração do sistema > Inscrições de log
- Na CLI : logconfig > new

Tipo de arquivo de log	Descrição	Suporta envio de syslog?	Ativado por padrão?
Logs SNMP	Registra mensagens de depuração relacionadas ao mecanismo de gerenciamento de rede SNMP.	Yes	Yes
Logs do	Registra mensagens do Web Proxy relacionadas à	No	No

módulo SNMP	interação com o sistema de monitoramento SNMP.		

Problemas comuns com SNMP

Alguns OIDS falham (nenhum valor ou valor incorreto).

Esse problema está relacionado ao pull do SNMP. Há dois exemplos de saída esperada e saída com erro:

```
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 prox
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 prox
iso.3.6.1.4.1.15497.1.1.1.9 = No Such Instance currently exists at this OID
```

Você pode verificar "Application Faults" em snmp_logs

Você pode verificar snmp_logs em CLI > grep > escolher o número associado a 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]>
```

Referência

Manual do usuário do AsyncOS 15.0 para Cisco Secure Web Appliance - LD (Implantação limitada) - Solução de problemas [Cisco Secure Web Appliance] - Cisco

Calculando a utilização da CPU do proxy no WSA usando SNMP - Cisco

snmpcmd(1) (freebsd)

snmptrap (freebsd)

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.