SNMP in SWA configureren en problemen oplossen

Inhoud

Inleiding

Dit document beschrijft de stappen voor het oplossen van problemen met Simple Network Monitoring Protocol (SNMP) in Secure Web Applicatie (SWA).

Voorwaarden

Vereisten

Cisco raadt kennis van deze onderwerpen aan:

- Access ToCommand Line Interface (CLI) van SWA
- Administratieve toegang tot de SWA.

- Basiskennis van SNMP.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Hoe SNMP werkt

SNMP is een communicatieprotocol op de toepassingslaag waarmee netwerkapparaten beheerinformatie kunnen uitwisselen tussen deze systemen en met andere apparaten buiten het netwerk.

Via SNMP kunnen netwerkbeheerders netwerkprestaties beheren, netwerkproblemen opsporen en oplossen en de groei van het netwerk plannen.

SNMP maakt netwerkbewaking rendabeler en maakt dat uw netwerk betrouwbaarder is. (Voor meer informatie over SNMP, zie RFC's 1065, 1066 en 1067.)

Een SNMP-beheerd netwerk bestaat uit een Manager, agents en beheerde apparaten.

- De beheerder zorgt voor de interface tussen de menselijke netwerkbeheerder en het beheersysteem.
- De Agent regelt de interface tussen de beheerder en het apparaat dat wordt beheerd
- Beheersystemen voeren de meeste beheerprocessen uit en bieden het grootste deel van de geheugenbronnen die voor netwerkbeheer worden gebruikt.

Op elk beheerd apparaat zit een agent die lokale managementinformatie (zoals prestatie-informatie of gebeurtenis- en foutinformatie) die gevangen is in softwarevallen, vertaalt naar een leesbare vorm voor het beheersysteem.

De SNMP-agent neemt gegevens op uit de Management Information Base (MIB) (apparaatparameter en netwerkgegevensopslagplaatsen) of uit fouten- of wijzigingsvallen.

MIB

MIB, is een gegevensstructuur die SNMP-netwerkelementen beschrijft als een lijst van gegevensobjecten. De SNMP-beheerder moet het MIB-bestand compileren voor elk type apparatuur in het netwerk om SNMP-apparaten te bewaken.

De manager en de agent gebruiken een MIB en een relatief kleine set opdrachten om informatie uit te wisselen. De MIB is georganiseerd in een boomstructuur met individuele variabelen die worden weergegeven als bladeren op de takken.

Een lange numerieke tag of object identifier (OID) wordt gebruikt om elke variabele in de MIB- en SNMP-berichten uniek te onderscheiden. De MIB associeert elke OID met een leesbaar label en diverse andere parameters die betrekking hebben op het object.

MIB dient dan als een gegevenswoordenboek of codebook dat wordt gebruikt om SNMP-berichten te assembleren en te interpreteren.

Wanneer de SNMP-beheerder de waarde van een object wil weten, zoals de status van een alarmpunt, de systeemnaam of het element uptime, wordt er een GET-pakket samengesteld dat de OID voor elk interessant object bevat.

Het element ontvangt het verzoek en kijkt omhoog elk OID in zijn coderekening (MIB). Als de OID wordt gevonden (het object wordt beheerd door het element), wordt een reactiepakket geassembleerd en verzonden met de huidige waarde van het object inbegrepen.

Als de OID niet wordt gevonden, wordt er een speciale fout-respons verzonden die het niet-beheerde object identificeert

SNMP-trap

Via SNMP-traps kan een agent het beheerstation op de hoogte te stellen van belangrijke gebeurtenissen door middel van een ongevraagd SNMP-bericht.

SNMPv1 en SNMPv2c moedigen, samen met de bijbehorende MIB, op val gerichte meldingen aan.

Het idee achter op traps gebaseerde meldingen is dat als een manager verantwoordelijk is voor een groot aantal apparaten, en elk apparaat een groot aantal objecten heeft, het voor de manager onpraktisch is om informatie van elk object op elk apparaat op te vragen.

De oplossing is dat elke agent op het beheerde apparaat de manager ongevraagd op de hoogte stelt. Het doet dit door een bericht te sturen dat bekendstaat als een Trap van de gebeurtenis.

Na het bericht ontvangen is, kan de manager dit inzien en op basis van de gebeurtenis gericht actie nemen. Bijvoorbeeld, kan de manager de agent direct opvragen, of andere geassocieerde apparatenagenten opvragen om de gebeurtenis beter te begrijpen.

Een melding via de trap kan aanzienlijke besparingen van netwerk- en agentresources opleveren doordat de noodzaak van ondoordachte SNMP-verzoeken wordt voorkomen. Het is echter niet mogelijk om SNMP-polls volledig te elimineren.

SNMP-verzoeken blijven noodzakelijk voor detectie en topologiewijzigingen. Bovendien kan de agent van een beheerd apparaat geen trap verzenden als het apparaat geheel is uitgevallen.

SNMPv1-traps worden gedefinieerd in RFC 1157, met volgende velden:

- Enterprise:Identificeert het type beheerd object dat de val genereert.
- Agent-adres: Hier vindt u het adres van het beheerde object dat de val genereert.

- Generic Trap Type:Geeft een aantal generieke overvultypen aan.
- Specifieke vangstcode:Geeft een van de specifieke vangstcodes aan.
- Tijdstempel: Geeft de tijd aan die is verstreken tussen de laatste netwerkherinitialisatie en de generatie van de val.
- Variabele bindingen: Het gegevensveld van de val die PDU bevat. Elke variable binding associeert een bepaalde MIB-objectinstantie met zijn huidige waarde.

SNMPv3

SNMPv3 ondersteunt de SNMP "Engine ID"-identificatiecode, die elke SNMP-entiteit op unieke wijze identificeert. Er kunnen conflicten optreden als twee SNMP-entiteiten dubbele EngineID's hebben.

EngineID wordt gebruikt om de sleutel voor geverifieerde berichten te genereren. (Zie RFC's 2571-2575 voor meer informatie over SNMPv3.)

Veel SNMP-producten blijven fundamenteel hetzelfde onder SNMPv3, maar worden verbeterd door deze nieuwe functies:

Beveiliging

- Verificatie
- Privacy

Beheer

- Vergunning en toegangscontrole
- Logische context
- Benoeming van entiteiten, identiteiten en informatie
- Mensen en beleid
- Gebruikersnamen en sleutelbeheer
- Meldingsbestemmingen en proxy-relaties
- Configuratie op afstand via SNMP-bewerkingen

SNMPv3-beveiligingsmodellen worden voornamelijk in twee vormen geleverd als verificatie en encryptie.

Verificatie wordt gebruikt om ervoor te zorgen dat alleen de beoogde ontvanger vallen leest. Aangezien berichten worden gemaakt, krijgen ze een speciale sleutel op basis van de entiteit EngineID. De sleutel wordt gedeeld met de beoogde ontvanger en gebruikt om het bericht te ontvangen.
Encryptie, privacy versleutelt de payload van het SNMP-bericht om ervoor te zorgen dat niet-geautoriseerde gebruikers het niet kunnen lezen. Eventuele onderschepte vallen gevuld met vervormde tekens en zijn onleesbaar. Privacy is met name nuttig in toepassingen waarin SNMP-berichten via het internet moeten worden gerouteerd.
Een SNMP-groep heeft drie beveiligingsniveaus:

noAuthnoPriv - Communicatie zonder authenticatie en privacy.
authNoPriv - Communicatie met authenticatie en zonder privacy. De protocollen die voor de verificatie worden gebruikt, zijn Message-Digest-algoritme 5 (MD5) en Secure Hash Algorithm (SHA).
authPriv - Communicatie met authenticatie en privacy. De protocollen die voor de verificatie worden gebruikt, zijn MD5 en SHA, en voor de protocollen Privacy, Data Encryption Standard (DES) en Advanced Encryption Standard (AES) kunnen worden gebruikt.

SNMP in SWA

Het AsyncOS-besturingssysteem ondersteunt bewaking van de systeemstatus via SNMP.

Let op:

- SNMP is standaard uitgeschakeld.
- SNMP-SET-bewerkingen (configuratie) zijn niet geïmplementeerd.
- AsyncOS ondersteunt SNMPv1, v2 en v3.
- Berichtverificatie en -codering zijn verplicht bij het inschakelen van SNMPv3. De wachtwoorden voor verificatie en codering moeten verschillen.
- Het encryptie-algoritme kan AES (aanbevolen) of DES zijn.
- Het verificatiealgoritme kan SHA-1 (aanbevolen) of MD5 zijn.
- De opdracht mmpconfig "herinnert" uw wachtwoorden de volgende keer dat u de opdracht uitvoert.
- Voor versies van AsyncOS voorafgaand aan 15.0 is de SNMPv3-gebruikersnaam: v3get.
- Voor AsyncOS release 15.0 en hoger is de standaardSNMPv3 gebruikersnaam: v3get. Als beheerder kunt u kiezen voor een andere gebruikersnaam.
- Als u alleen SNMPv1 of SNMPv2 gebruikt, moet u een community-string instellen. De community string is niet standaard op public.
- Voor SNMPv1 en SNMPv2 moet u een netwerk opgeven waarvan SNMP-verzoeken worden geaccepteerd.
- Om traps te kunnen gebruiken, moet een SNMP-beheerder (niet opgenomen in AsyncOS) actief zijn en moet zijn IP-adres worden ingevoerd als het doel van de trap. (U kunt een hostnaam gebruiken, maar als u dat doet, werken traps alleen als DNS werkt.)

SNMP-monitor configureren

Als u SNMP wilt configureren om systeemstatusinformatie voor het apparaat te verzamelen, gebruikt u de opdracht mpconfig in de CLI. Nadat u waarden voor een interface hebt gekozen en

geconfigureerd, reageert het apparaat op SNMPv3 GET-verzoeken.

Wanneer u SNMP gebruikt, dient u rekening te houden met deze punten:

- In SNMP versie 3 moeten verzoeken een bijpassend wachtwoord bevatten.
- Standaard worden versie 1- en versie 2-verzoeken afgewezen.
- Indien ingeschakeld, moeten de verzoeken van versie 1 en 2 een overeenkomende community string hebben.

```
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
```

SWA MIB-bestanden

MIB-bestanden zijn beschikbaar via URL: https://www.cisco.com/c/en/us/support/security/web-security-appliance/series.html

Gebruik de nieuwste versie van elk MIB-bestand.

Er zijn meerdere MIB-bestanden:

- asyncoswebsecurity applicatie-mib.txt is een SNMPv2 compatibele beschrijving van de Enterprise MIB voor Secure Web applicaties.
- ASYNCOS-MAIL-MIB.txt is een SNMPv2 compatibele beschrijving van de Enterprise MIB voor e-mail security applicaties.
- IRONPORT-SMI.txt Dit bestand "Structure of Management Information" definieert de rol van het asyncoswebsecurity apparaat-mib.

Deze release implementeert een alleen-lezen subset van MIB-II zoals gedefinieerd in RFC's 1213 en 1907.

Seehttps://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118415-technote-wsa-00.htmlom meer te weten te komen over de controle van het CPU-gebruik op het apparaat met SNMP.

SWA SNMP-TRAP

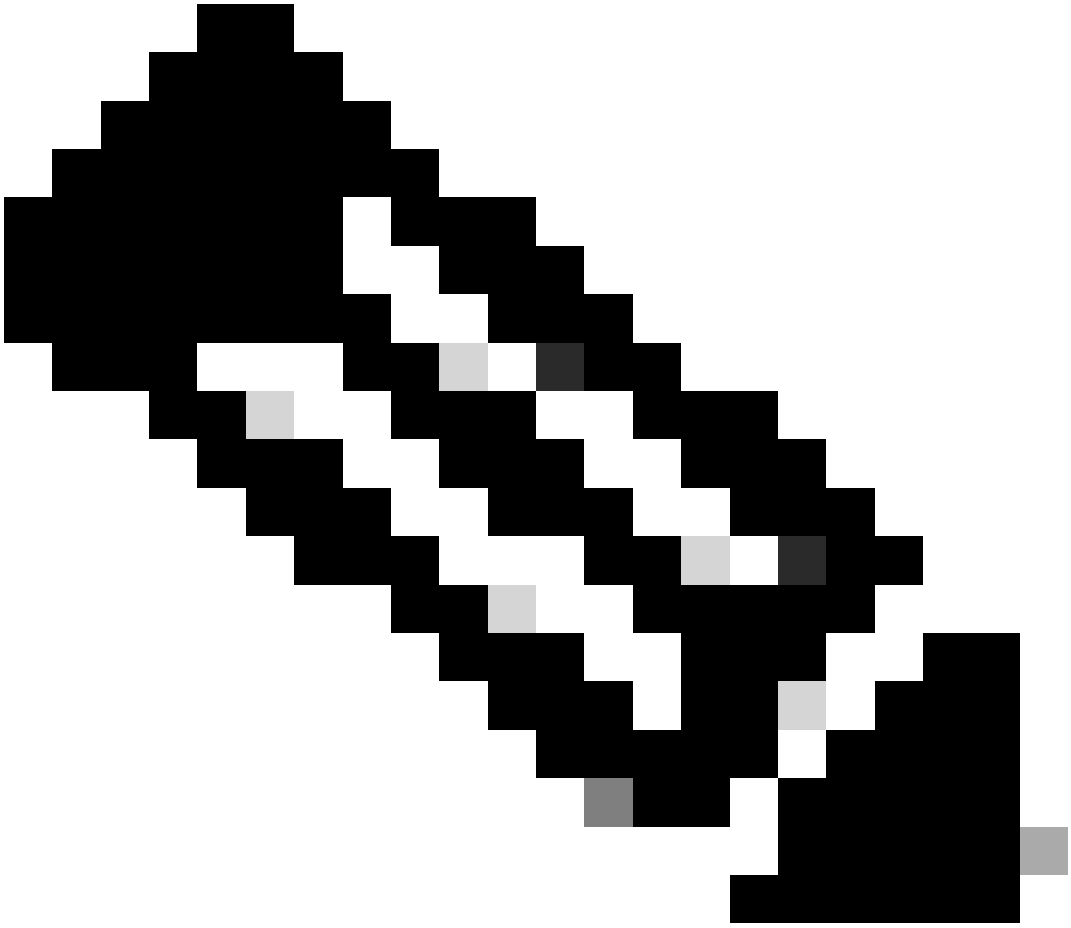
SNMP biedt de mogelijkheid om vallen of meldingen te verzenden om een beheerapplicatie te adviseren wanneer aan een of meer voorwaarden is voldaan.

Traps zijn netwerkpakketten die gegevens bevatten met betrekking tot een component van het systeem dat de val verzendt.

Er worden traps gegenereerd wanneer aan een voorwaarde is voldaan op de SNMP-agent (in dit geval de Cisco Secure Web Applicatie).

Nadat aan de voorwaarde is voldaan, vormt de SNMP-agent vervolgens een SNMP-pakket en stuurt het naar de host waarop de SNMP-beheerconsolesoftware wordt uitgevoerd.

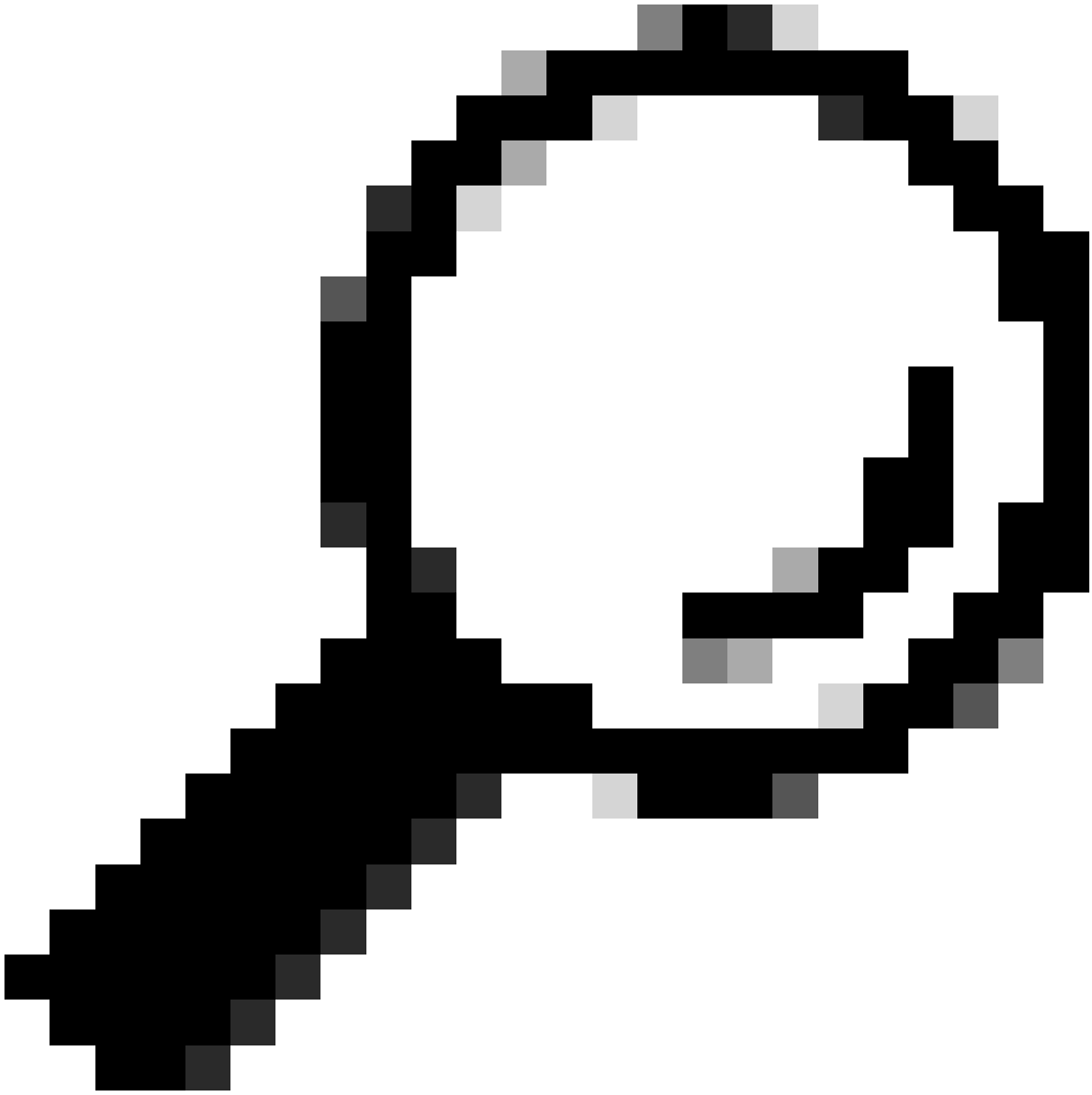
U kunt SNMP-traps configureren (specifieke traps in- of uitschakelen) wanneer u SNMP inschakelt voor een interface.



Opmerking: om meerdere overvuldoelen te specificeren: wanneer u om het overvuldoel wordt gevraagd, kunt u maximaal 10 komma-gescheiden IP-adressen invoeren.

De connectiviteitsFailure val is bedoeld om de internetverbinding van uw apparaat te bewaken. Het doet dit door te proberen om verbinding te maken en een HTTP GET aanvraag te verzenden naar een enkele externe server elke 5 tot 7 seconden. Standaard is de bewaakte URL downloads.ironport.com op poort 80.

Als u de bewaakte URL of poort wilt wijzigen, voert u de opdracht snmConfig uit en schakelt u de val ConnectivityFailure in, zelfs als deze al is ingeschakeld. U kunt een melding zien om de URL te wijzigen.



Tip: om connectiviteitFailure traps te simuleren, kunt u de dnsconfig CLI-opdracht gebruiken om een niet-werkende DNS-server in te voeren. Zoekopdrachten naar downloads.ironport.com mislukken, en traps worden elke 5-7 seconden verzonden. Verzeker u ervan dat u de DNS-server terugzet naar een werkende server nadat uw test is afgelopen.

Aanbevolen OID's voor bewaking

Dit is een lijst van te controleren aanbevolen MIB's en geen uitputtende lijst:

Hardware-OID	Naam
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	ventilatoreenheid
1.3.6.1.4.1.15497.1.1.1.9.1.2	graden Celsius

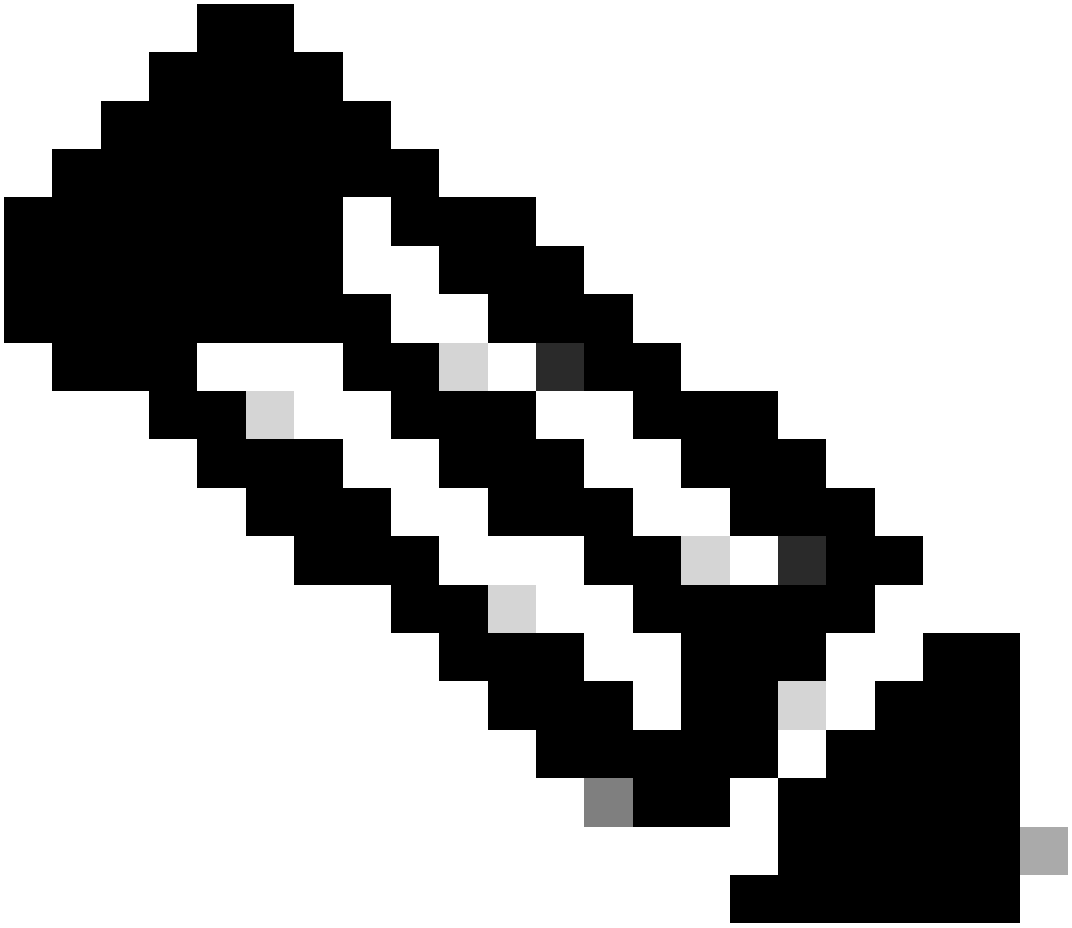
Dit is OIDs-kaart rechtstreeks naar de uitvoer van de status detailCLI-opdracht:

OID	Naam	Het veld Statusdetails
Systeembronnen		
1.3.6.1.4.1.15497.1.1.1.2.0	benutting per centimeter	CPU
1.3.6.1.4.1.15497.1.1.1.1.0	PerCentMemory-gebruik	RAM
Transacties per seconde		
1.3.6.1.4.1.15497.1.2.3.7.1.1.0	cacheThruputNow	Gemiddelde transacties per seconde in last minute.
1.3.6.1.4.1.15497.1.2.3.7.1.2.0	cachegeheugenDoorvoersnelheid1 uurPiek	Maximum aantal transacties per seconde in afgelopen uur.
1.3.6.1.4.1.15497.1.2.3.7.1.3.0	cacheDoorvoersnelheid1 uurGemiddeld	Gemiddelde transacties per seconde in afgelopen uur.
1.3.6.1.4.1.15497.1.2.3.7.1.8.0	cacheThruputLifePeak	Maximum aantal transacties per seconde sinds het opnieuw opstarten van proxy.
1.3.6.1.4.1.15497.1.2.3.7.1.9.0	cacheDoorvoersnelheidGemiddeld	Gemiddelde transacties per seconde sinds proxy opnieuw opstarten.
Bandbreedte		
1.3.6.1.4.1.15497.1.2.3.7.4.1.0	cacheBreedteTotalNow	Gemiddelde bandbreedte in de laatste minuut.
1.3.6.1.4.1.15497.1.2.3.7.4.2.0	cacheBreedteTotaal1 uurPiek	Maximale bandbreedte in afgelopen uur.
1.3.6.1.4.1.15497.1.2.3.7.4.3.0	cacheBreedteTotaal1kGemiddeld	Gemiddelde bandbreedte in afgelopen uur.
1.3.6.1.4.1.15497.1.2.3.7.4.8.0	cacheBreedteTotalLifePeak	Maximale bandbreedte sinds opnieuw opstarten van proxy.
1.3.6.1.4.1.15497.1.2.3.7.4.9.0	cacheBreedteTotaleLifeGemiddeld	Gemiddelde bandbreedte sinds proxy opnieuw opstarten.
Responstijd		

1.3.6.1.4.1.15497.1.2.3.7.9.1.0	cacheHitsNow	Gemiddelde cachesnelheid in last minute.
1.3.6.1.4.1.15497.1.2.3.7.9.2.0	cachegeheugenHits1hrPeak	Maximale cachesnelheid in afgelopen uur.
1.3.6.1.4.1.15497.1.2.3.7.9.3.0	cacheHits1hrGemiddeld	Gemiddelde cachesnelheid in afgelopen uur.
1.3.6.1.4.1.15497.1.2.3.7.9.8.0	cacheHitsLifePeak	Maximale cachesnelheid sinds opnieuw starten van proxy.
1.3.6.1.4.1.15497.1.2.3.7.9.9.0	cacheHitsLifeMean	Gemiddelde cache hit rate sinds proxy opnieuw opstarten.
Cache hit rate		
1.3.6.1.4.1.15497.1.2.3.7.5.1.0	cacheHitsNow	Gemiddelde cachesnelheid in last minute.
1.3.6.1.4.1.15497.1.2.3.7.5.2.0	cachegeheugenHits1hrPeak	Maximale cachesnelheid in afgelopen uur.
1.3.6.1.4.1.15497.1.2.3.7.5.3.0	cacheHits1hrGemiddeld	Gemiddelde cachesnelheid in afgelopen uur.
1.3.6.1.4.1.15497.1.2.3.7.5.8.0	cacheHitsLifePeak	Maximale cachesnelheid sinds opnieuw starten van proxy.
1.3.6.1.4.1.15497.1.2.3.7.5.9.0	cacheHitsLifeMean	Gemiddelde cache hit rate sinds proxy opnieuw opstarten.
Aansluitingen		
1.3.6.1.4.1.15497.1.2.3.2.7.0	cacheClientIdleConns	Inactiviteitsclient verbindingen.
1.3.6.1.4.1.15497.1.2.3.3.7.0	cacheServerIdleConns	Inactiviteitsserververbindingen.
1.3.6.1.4.1.15497.1.2.3.2.8.0	cacheClienttotaalConns	Totale aantal clientverbindingen.
1.3.6.1.4.1.15497.1.2.3.3.8.0	cacheServerTotalConns	Totale aantal serververbindingen.

Probleemoplossing voor SNMP

Om de connectiviteit tussen SWA en uw SNMP-beheerder te bekijken, is het het beste om pakketten op te nemen, kunt u het pakketopnamefilter plaatsen naar: (poort 161 of poort 162)



Opmerking: dit filter komt door de standaard SNMP-poorten. Als u de poorten hebt gewijzigd, zet u de ingestelde poortnummers in het pakketopnamefilter.

Stappen om pakketten van SWA op te nemen:

Stap 1. Meld u aan bij GUI

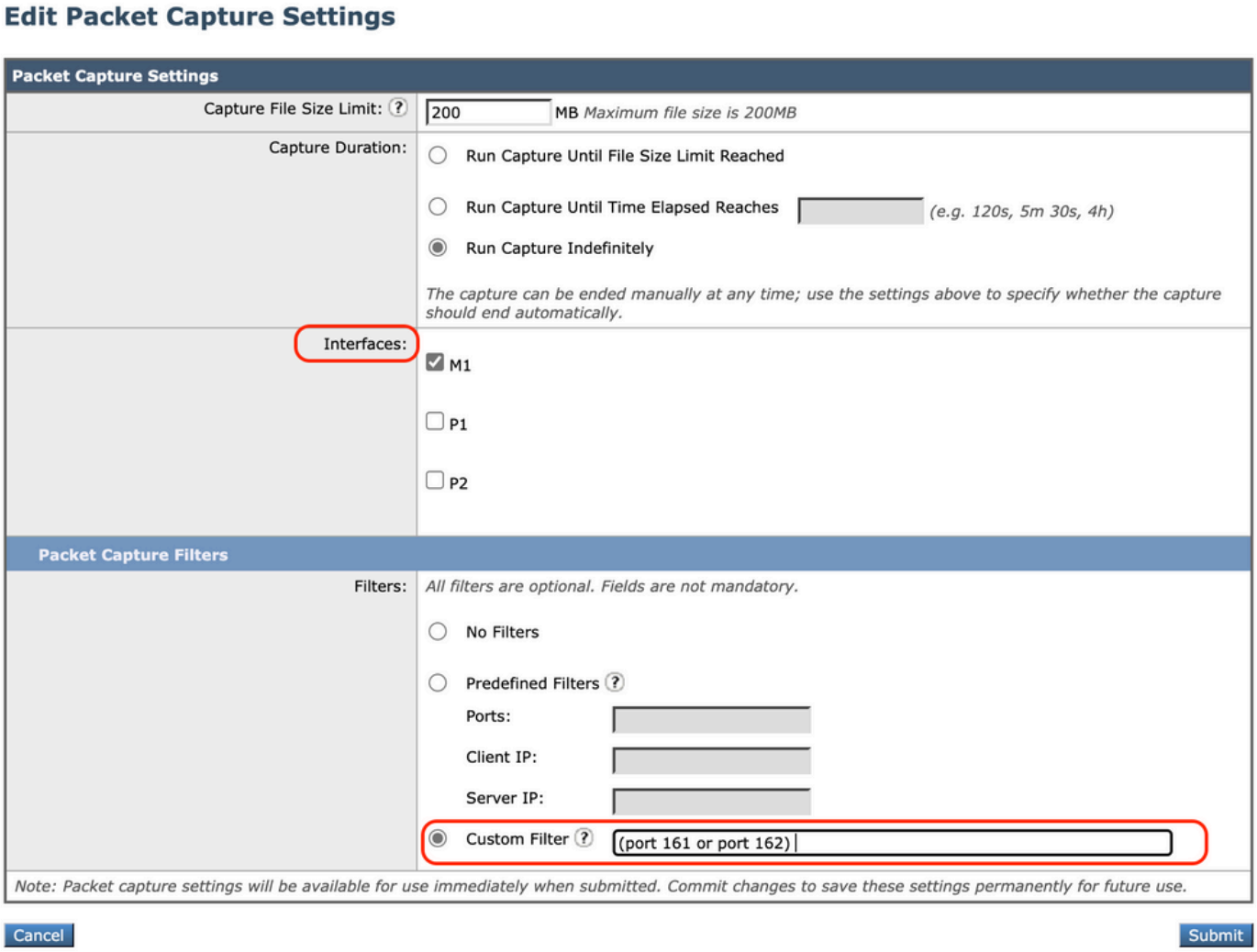
Stap 2. kies rechtsboven Ondersteuning en Help

Stap 3. selecteer Packet Capture

Stap 4. kies Instellingen bewerken

Stap 5. Zorg ervoor dat de juiste interface is geselecteerd

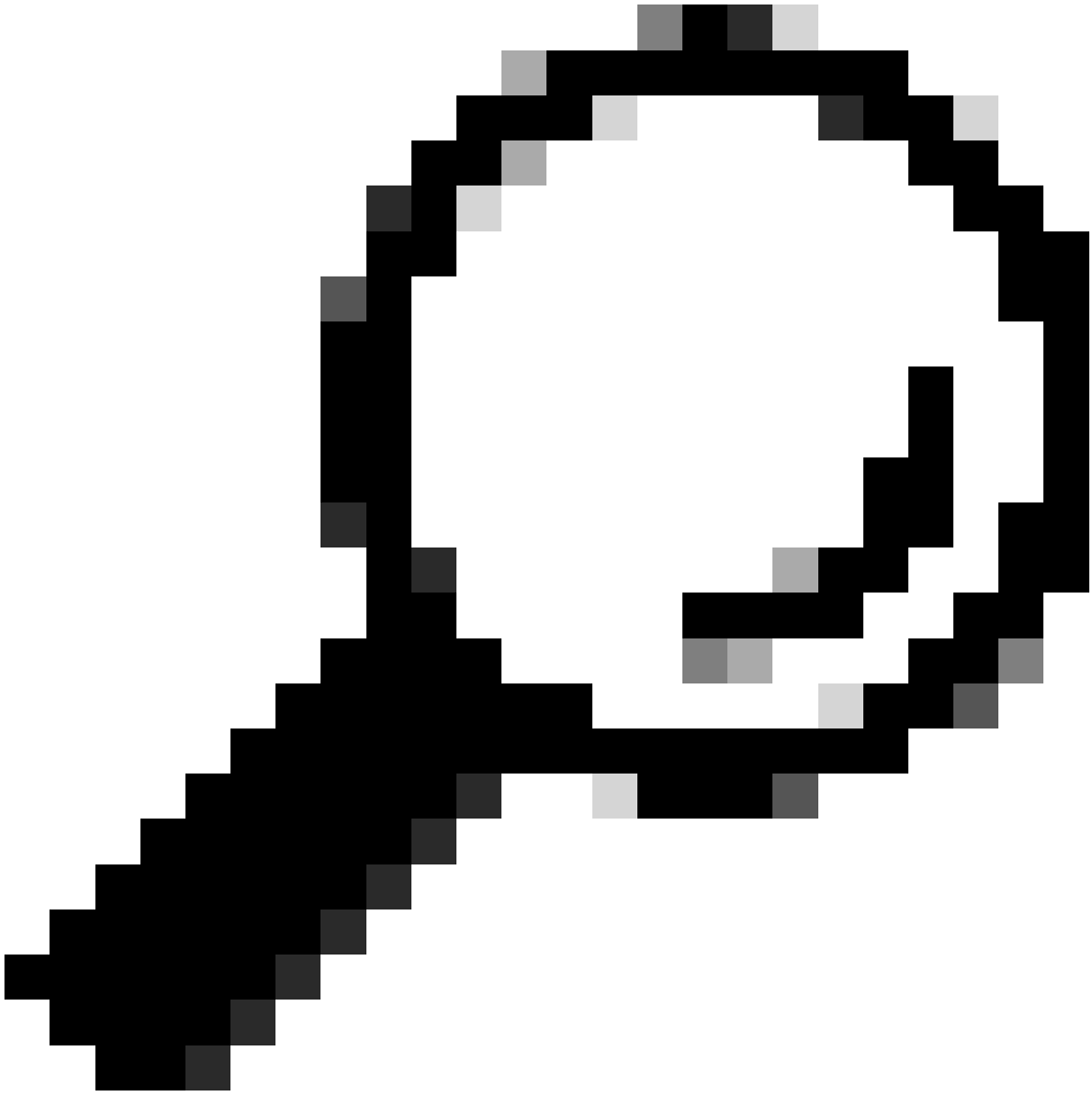
Stap 6. Voer de filteromstandigheden in.



Afbeelding - Packet Capture Filters configureren

Stap 7. Kies Verzenden

Stap 8. Kies Start Capture.



Tip: u kunt SNMPv3-pakketopnamen decrypteren met Wireshark. Ga voor meer informatie naar deze link: [How-to-decrypt-snmpv3-packets-using-wireshark]

SNMP

snmpwalk is de naam gegeven aan een SNMP applicatie die meerdere GET-NEXT aanvragen automatisch uitvoert. Het SNMP GET-NEXT-verzoek wordt gebruikt om een ingeschakeld apparaat te bevragen en SNMP-gegevens van een apparaat te nemen. De snmpwalk commando wordt gebruikt omdat het de gebruiker in staat stelt om GET-NEXT verzoeken samen te ketenen zonder unieke commando's in te voeren voor elke OID of node binnen een substructuur

SNMPwalk op Windows-besturingssystemen installeren

Voor Microsoft Windows-gebruikers moet u eerst de tool downloaden.

Installeer SNMPwalk op Linux kernel

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

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

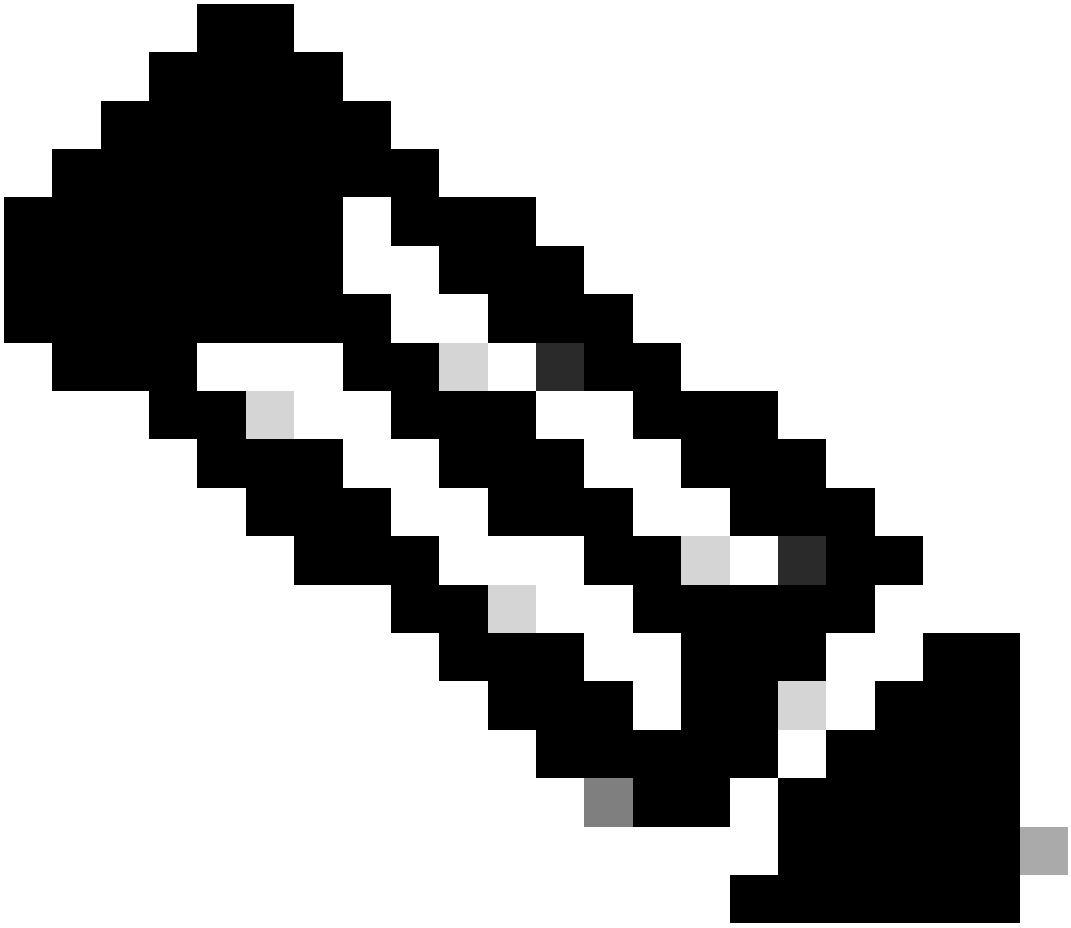
Installeer SNMPwalk op MacOS

Standaard is snmpwalk op MacOS geïnstalleerd

Om SNMP GET verzoek te genereren, kunt u snmpwalk opdracht gebruiken van een andere computer in uw netwerk die verbinding met SWA heeft, hier zijn een paar voorbeelden van snmpwalk opdracht:

```
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>
```



Opmerking: u kunt het beveiligingsniveau instellen op noAuthNoPriv of authNoPriv of authPriv afhankelijk van uw SWA configuraties.

SNMP

snmptrap is verborgen CLI-opdracht waarvoor SNMP op de SWA ingeschakeld moest worden. U kunt SNMP-trap genereren door het object te selecteren, en hier is een voorbeeld:

```
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
```

SNMP-logbestanden in SWA

SWA heeft twee logboeken met betrekking tot SNMP, Sommige logtypen met betrekking tot de webproxycomponent zijn niet ingeschakeld. U kunt ze inschakelen:

- In GUI: systeembeheer > abonnementen op logs
- In CLI: logfig > nieuw

Type logbestand	Beschrijving	Ondersteunt Syslog Push?	Standaard ingeschakeld?
SNMP-logbestanden	Records debuggen berichten met betrekking tot de SNMP-netwerkbeheerengine.	Ja	Ja
Logboeken voor	Registreert webproxyberichten met	Nee	Nee

SNMP-module	betrekking tot interactie met het SNMP-bewakingssysteem.		

Veelvoorkomende problemen met SNMP

Sommige OIDS mislukken (geen of verkeerde waarde).

Dit probleem is gerelateerd aan SNMP pull. Hier zijn twee voorbeelden van verwachte uitvoer en uitvoer met fout:

```
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
```

U kunt controleren op "Toepassingsfouten" in snmp_logs

U kunt de snmp_logs controleren via CLI > grep > het nummer kiezen dat gekoppeld is aan 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]>
```

Referentie

Gebruikershandleiding voor AsyncOS 15.0 voor Cisco Secure Web Applicatie - LD (Beperkte implementatie) - Problemen oplossen [Cisco Secure Web Applicatie] - Cisco

Het berekenen van het gebruik van proxy-CPU's op het WAN met SNMP - Cisco

snmpcmd(1) (vrij)

snampval (freebsd)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.