SNMP in SWA konfigurieren und Fehlerbehebung dafür durchführen

Inhalt

Einleitung

In diesem Dokument werden die Schritte zur Fehlerbehebung für das Simple Network Monitoring Protocol (SNMP) in Secure Web Appliance (SWA) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Zugriff auf die Befehlszeilenschnittstelle (CLI) von SWA
- Administratorzugriff auf die SWA.

- Grundkenntnisse von SNMP.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Funktionsweise von SNMP

SNMP ist ein Kommunikationsprotokoll auf Anwendungsebene, das Netzwerkgeräten den Austausch von Verwaltungsinformationen zwischen diesen Systemen und mit anderen Geräten außerhalb des Netzwerks ermöglicht.

Über SNMP können Netzwerkadministratoren die Netzwerkleistung verwalten, nach Netzwerkproblemen suchen und diese beheben und das Netzwerkwachstum planen.

SNMP macht die Netzwerküberwachung kosteneffizienter und erhöht die Zuverlässigkeit Ihres Netzwerks. (Weitere Informationen zu SNMP finden Sie unter RFCs 1065, 1066 und 1067.)

Ein von SNMP verwaltetes Netzwerk besteht aus einem Manager, Agenten und verwalteten Geräten.

- Der Manager stellt die Schnittstelle zwischen dem Human Network Manager und dem Managementsystem zur Verfügung.
- Der Agent stellt die Schnittstelle zwischen dem Manager und dem verwalteten Gerät bereit.
- Managementsysteme führen die meisten Managementprozesse aus und stellen den Großteil der für das Netzwerkmanagement verwendeten Speicherressourcen bereit.

Ein Agent, der sich auf jedem verwalteten Gerät befindet, übersetzt lokale Verwaltungsinformationsdaten (wie Leistungsinformationen oder Ereignis- und Fehlerinformationen), die in Software-Traps erfasst werden, in eine lesbare Form für das Verwaltungssystem.

Der SNMP-Agent erfasst Daten aus der Management Information Base (MIB) (Geräteparameter und Netzwerk-Daten-Repositorys) oder aus Fehler- oder Change-Traps.

MIB

MIB ist eine Datenstruktur, die SNMP-Netzwerkelemente als Liste von Datenobjekten beschreibt. Der SNMP-Manager muss die MIB-Datei für jeden Gerätetyp im Netzwerk kompilieren, um SNMP-Geräte zu überwachen.

Der Manager und der Agent tauschen Informationen mithilfe einer MIB und einer relativ kleinen Gruppe von Befehlen aus. Die MIB ist in einer Baumstruktur organisiert, wobei einzelne Variablen

als Blätter auf den Verzweigungen dargestellt werden.

Ein langes numerisches Tag oder eine lange Objektkennung (OID) wird verwendet, um jede Variable eindeutig in der MIB und in SNMP-Meldungen zu unterscheiden. Die MIB ordnet jeder OID ein lesbares Label und verschiedene andere, mit dem Objekt verknüpfte Parameter zu.

Die MIB dient dann als Datenwörterbuch oder Codebuch, das zum Zusammenstellen und Interpretieren von SNMP-Meldungen verwendet wird.

Wenn der SNMP-Manager den Wert eines Objekts ermitteln möchte, z. B. den Status eines Alarmpunkts, den Systemnamen oder die Betriebszeit des Elements, stellt er ein GET-Paket zusammen, das die OID für jedes gewünschte Objekt enthält.

Das Element empfängt die Anforderung und sucht jede OID in seinem Codebuch (MIB). Wenn die OID gefunden wird (das Objekt wird vom Element verwaltet), wird ein Antwortpaket zusammengestellt und mit dem aktuellen Wert des enthaltenen Objekts gesendet.

Wenn die OID nicht gefunden wird, wird eine spezielle Fehlerantwort gesendet, die das nicht verwaltete Objekt identifiziert

SNMP-Trap

SNMP-Traps ermöglichen es einem Agenten, die Managementstation über wichtige Ereignisse mittels einer nicht angeforderten SNMP-Nachricht zu benachrichtigen.

SNMPv1 und SNMPv2c regen zusammen mit der zugehörigen MIB die Trap-gerichtete Benachrichtigung an.

Die Idee hinter der Trap-gesteuerten Benachrichtigung ist, dass, wenn ein Manager für eine große Anzahl von Geräten verantwortlich ist und jedes Gerät eine große Anzahl von Objekten hat, es für den Manager unpraktisch ist, Informationen von jedem Objekt auf jedem Gerät abzufragen oder anzufordern.

Die Lösung besteht darin, dass jeder Agent auf dem verwalteten Gerät den Manager ohne Aufforderung benachrichtigt. Dazu sendet er eine Nachricht, die als Trap des Ereignisses bezeichnet wird.

Nachdem der Manager die Veranstaltung erhalten hat, zeigt er sie an und kann je nach Veranstaltung eine Aktion auswählen. So kann der Manager beispielsweise den Agenten direkt abfragen oder andere zugehörige Geräte-Agenten abfragen, um ein besseres Verständnis des Ereignisses zu erhalten.

Trap-gesteuerte Benachrichtigungen können zu erheblichen Einsparungen bei Netzwerk- und Agenten-Ressourcen führen, da keine unhandlichen SNMP-Anfragen mehr erforderlich sind. SNMP-Abfragen können jedoch nicht vollständig eliminiert werden.

SNMP-Anforderungen sind für die Erkennung und für Topologieänderungen erforderlich. Darüber hinaus kann ein Agent eines verwalteten Geräts kein Trap senden, wenn ein schwerwiegender Geräteausfall aufgetreten ist.

SNMPv1-Traps werden in RFC 1157 definiert und verfügen über die folgenden Felder:

- Enterprise:Identifiziert den Typ des verwalteten Objekts, das das Trap generiert.
- Agent address (Agentadresse): Gibt die Adresse des verwalteten Objekts an, das das Trap generiert.
- Generischer Trap-Typ: Gibt einen generischen Trap-Typ an.
- Spezifischer Trap-Code: Gibt einen von mehreren spezifischen Trap-Codes an.
- Zeitstempel: Gibt die Zeit an, die zwischen der letzten Netzwerkneuinitialisierung und der Generierung des Traps vergangen ist.
- Variable Bindings: Das Datenfeld des Traps, das PDU enthält. Jede Variablenbindung ordnet eine bestimmte MIB-Objektinstanz ihrem aktuellen Wert zu.

SNMPv3

SNMPv3 unterstützt den SNMP "Engine ID" Identifier, der jede SNMP-Einheit eindeutig identifiziert. Konflikte können auftreten, wenn zwei SNMP-Entitäten über doppelte Engine-IDs verfügen.

Die EngineID wird zum Generieren des Schlüssels für authentifizierte Nachrichten verwendet. (Weitere Informationen zu SNMPv3 finden Sie unter RFCs 2571-2575.)

Viele SNMP-Produkte bleiben unter SNMPv3 im Wesentlichen gleich, werden jedoch durch folgende neue Funktionen erweitert:

Sicherheit

- Authentifizierung
- Datenschutz

Verwaltung

- Autorisierung und Zugriffskontrolle
- Logische Kontexte
- Benennung von Einheiten, Identitäten und Informationen
- Personen und Richtlinien
- Benutzernamen und Schlüsselverwaltung
- Benachrichtigungsziele und Proxy-Beziehungen
- Remote-Konfiguration über SNMP-Betrieb

Die SNMPv3-Sicherheitsmodelle werden hauptsächlich in zwei Formen bereitgestellt: Authentifizierung und Verschlüsselung.

Die Authentifizierung wird verwendet, um sicherzustellen, dass nur der beabsichtigte Empfänger Traps liest. Beim Erstellen von Nachrichten wird ihnen ein spezieller Schlüssel basierend auf der EngineID der Entität zugewiesen. Der Schlüssel wird für den beabsichtigten Empfänger

freigegeben und zum Empfang der Nachricht verwendet.
Verschlüsselung: Der Datenschutz verschlüsselt die Nutzlast der SNMP-Nachricht, um sicherzustellen, dass nicht autorisierte Benutzer sie nicht lesen können. Alle abgefangenen Fallen gefüllt mit verstümmelten Zeichen und ist unlesbar. Datenschutz ist besonders bei Anwendungen nützlich, bei denen SNMP-Nachrichten über das Internet geroutet werden müssen.
Eine SNMP-Gruppe weist drei Sicherheitsstufen auf:

noAuthnoPriv - Kommunikation ohne Authentifizierung und Datenschutz.
authNoPriv - Kommunikation mit Authentifizierung und ohne Privatsphäre. Die für die Authentifizierung verwendeten Protokolle sind Message-Digest Algorithm 5 (MD5) und Secure Hash Algorithm (SHA).
authPriv - Kommunikation mit Authentifizierung und Datenschutz. Die für die Authentifizierung verwendeten Protokolle sind MD5 und SHA, und für die Protokolle Privacy, Data Encryption Standard (DES) und Advanced Encryption Standard (AES) können sie verwendet werden.

SNMP in SWA

Das Betriebssystem AsyncOS unterstützt die Systemstatusüberwachung über SNMP.

Bitte beachten:

- SNMPisoff ist standardmäßig aktiviert.
- SNMPSET-Vorgänge (Konfiguration) sind nicht implementiert.
- AsyncOS unterstützt SNMPv1, v2 und v3.
- Nachrichtenauthentifizierung und -verschlüsselung sind erforderlich, wenn SNMPv3 aktiviert wird. Die Passphrasen für die Authentifizierung und Verschlüsselung müssen unterschiedlich sein.
- Der Verschlüsselungsalgorithmus kann AES (empfohlen) oder DES sein.
- Der Authentifizierungsalgorithmus kann SHA-1 (empfohlen) oder MD5 sein.
- Der Befehl snmpconfig "merkt sich" Ihre Passphrase beim nächsten Ausführen des Befehls.
- Bei AsyncOS-Versionen vor 15.0 lautet der SNMPv3-Benutzername: v3get.
- Für AsyncOS Version 15.0 und höher lautet der Standard-SNMPv3-Benutzername: v3get. Als Administrator können Sie sich für jeden anderen Benutzernamen entscheiden.
- Wenn Sie nur SNMPv1 oder SNMPv2 verwenden, müssen Sie einen Community String festlegen. Der Community-String ist nicht standardmäßig öffentlich.
- Für SNMPv1 und SNMPv2 müssen Sie ein Netzwerk angeben, von dem SNMPGET-Anforderungen akzeptiert werden.
- Zur Verwendung von Traps muss ein SNMPmanager (der nicht in AsyncOS enthalten ist)

ausgeführt werden, und seine IP-Adresse muss als Trap-Ziel eingegeben werden. (Sie können einen Hostnamen verwenden, Traps funktionieren in diesem Fall jedoch nur, wenn DNS funktioniert.)

Konfigurieren vonSNMPMonitor

Um SNMP so zu konfigurieren, dass Systemstatusinformationen für die Appliance gesammelt werden, verwenden Sie den Befehl nmpconfig in der CLI. Nachdem Sie Werte für eine Schnittstelle ausgewählt und konfiguriert haben, antwortet die Appliance auf SNMPv3 GET-Anforderungen.

Wenn Sie SNMP verwenden, berücksichtigen Sie folgende Punkte:

- In der SNMP-Version 3 müssen Anforderungen eine passende Passphrase enthalten.
- Standardmäßig werden Anforderungen der Versionen 1 und 2 abgelehnt.
- Wenn diese Funktion aktiviert ist, müssen Anforderungen der Versionen 1 und 2 über einen übereinstimmenden Community String verfügen.

```
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-Dateien

MIB-Dateien stehen unter folgender URL zur Verfügung: https://www.cisco.com/c/en/us/support/security/web-security-appliance/series.html

Verwenden Sie die neueste Version jeder MIB-Datei.

Es gibt mehrere MIB-Dateien:

- asyncoswebsecurityappliance-mib.txt ist eine mit SNMPv2 kompatible Beschreibung der Enterprise-MIB für sichere Web-Appliances.
- ASYNCOS-MAIL-MIB.txt ist eine SNMPv2-kompatible Beschreibung der Enterprise MIB für Email Security-Appliances.
- IRONPORT-SMI.txt Diese Datei "Structure of Management Information" definiert die Rolle der asyncoswebsecurityappliance-mib.

Diese Version implementiert eine schreibgeschützte Teilmenge von MIB-II, wie in RFCs 1213 und 1907 definiert.

Seehttps://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118415-technote-wsa-00.htmlweitere Informationen zur Überwachung der CPU-Auslastung auf der Appliance mit SNMP.

SWA SNMP-TRAP

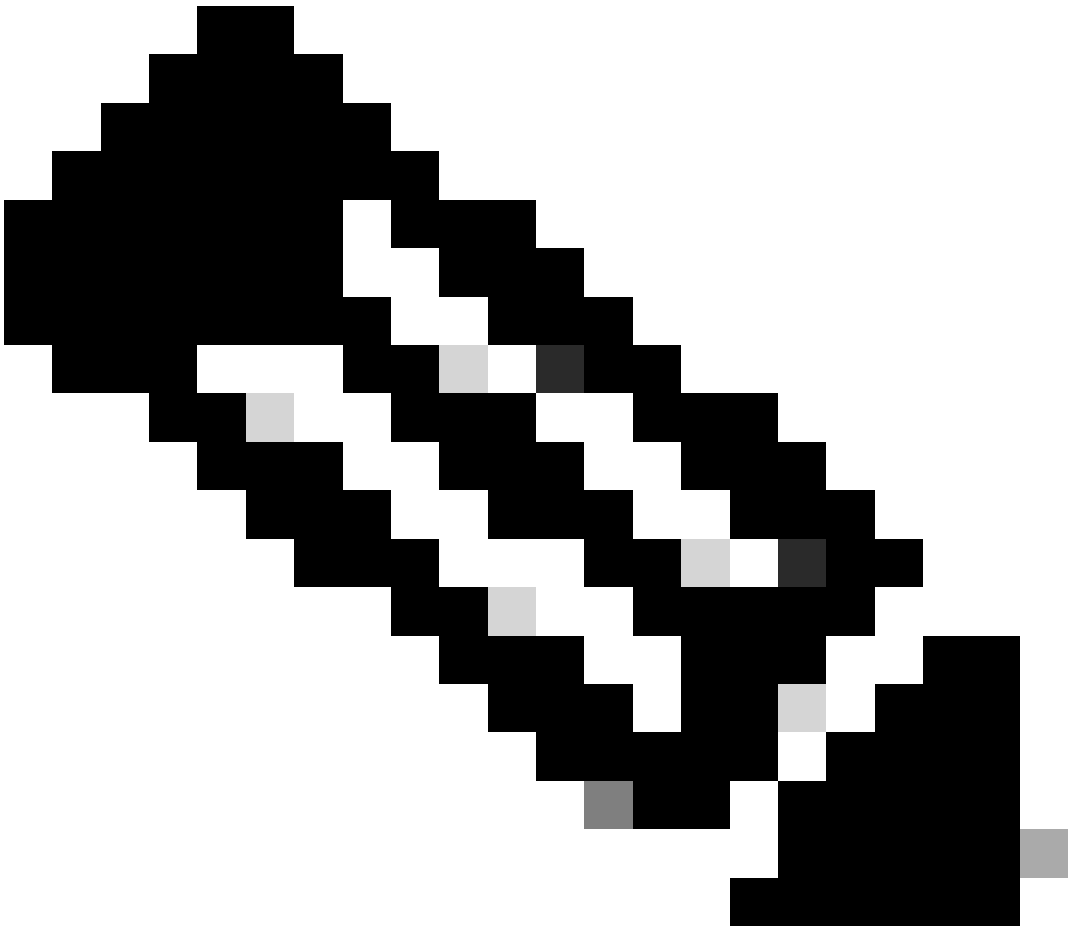
SNMP bietet die Möglichkeit, Traps oder Benachrichtigungen zu senden, um eine Verwaltungsanwendung zu benachrichtigen, wenn eine oder mehrere Bedingungen erfüllt wurden.

Traps sind Netzwerkpakete, die Daten enthalten, die sich auf eine Komponente des Systems beziehen, die das Trap sendet.

Traps werden generiert, wenn eine Bedingung auf dem SNMP-Agenten (in diesem Fall der CiscoSecure Web Appliance) erfüllt wurde.

Wenn die Bedingung erfüllt ist, erstellt der SNMPagent dann ein SNMP-Paket und sendet es an den Host, auf dem die SNMP-Verwaltungskonsolensoftware ausgeführt wird.

Sie können SNMPtraps konfigurieren (bestimmte Traps aktivieren oder deaktivieren), wenn Sie SNMP für eine Schnittstelle aktivieren.

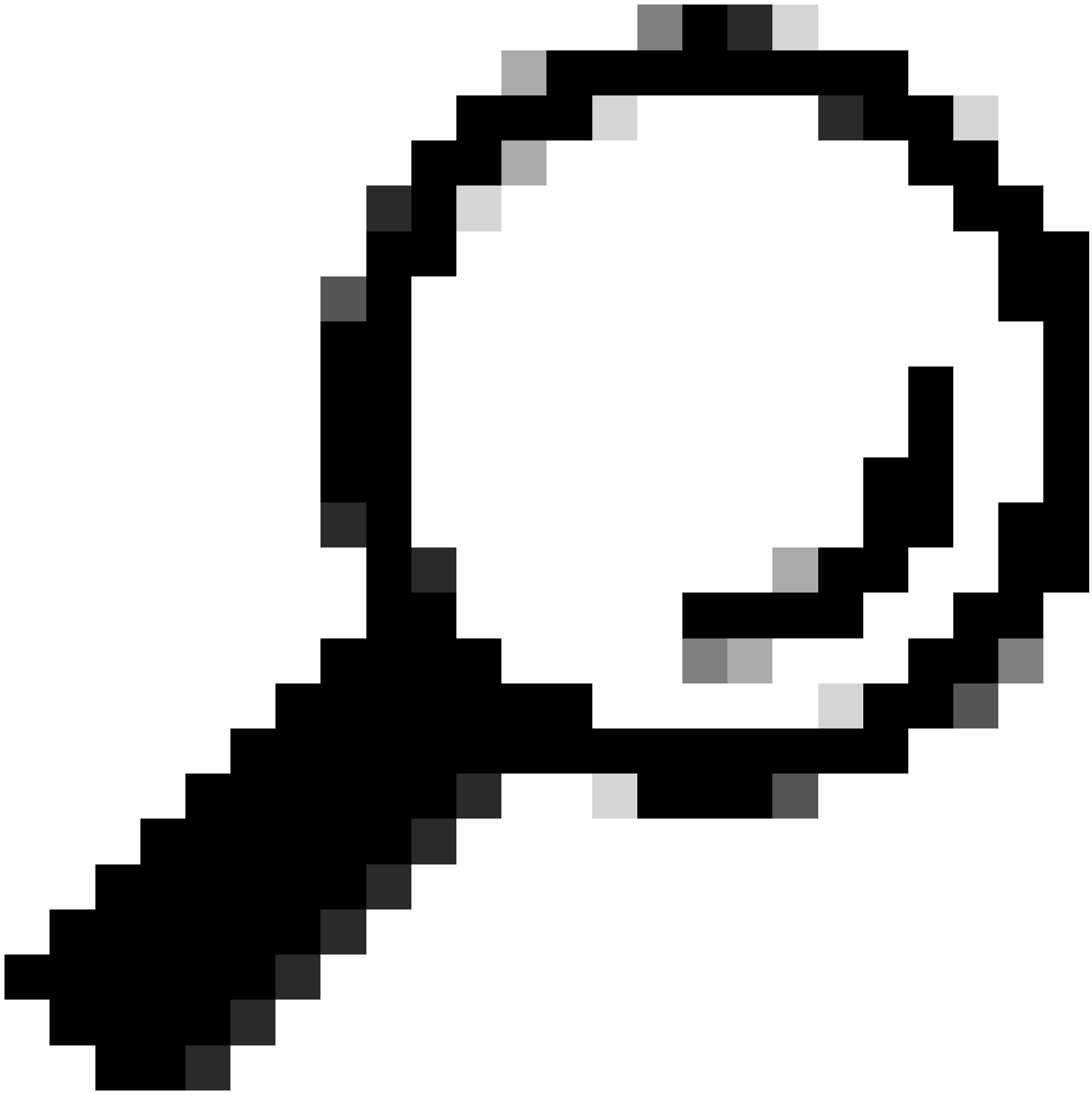


> Hinweis: So geben Sie mehrere Trap-Ziele an: Wenn Sie zur Eingabe des Trap-Ziels aufgefordert werden, können Sie bis zu 10 durch Komma getrennte IP-Adressen eingeben.

Der ConnectivityFailure-Trap dient dazu, die Appliance-Verbindung mit dem Internet zu überwachen. Zu diesem Zweck versucht er, eine Verbindung herzustellen und alle 5 bis 7 Sekunden eine HTTP GET-Anforderung an einen einzelnen externen Server zu senden. Standardmäßig lautet die überwachte URL downloads.ironport.com auf Port 80.

Um die überwachte URL oder den überwachten Port zu ändern, führen Sie den Befehl snmpconfig aus, und aktivieren Sie das ConnectivityFailure-Trap, selbst wenn es bereits aktiviert ist. Sie

werden aufgefordert, die URL zu ändern.



Tipp: Um connectivityFailure-Traps zu simulieren, können Sie den CLI-Befehl dnsconfig verwenden, um einen nicht funktionierenden DNS-Server einzugeben. Die Suche nach downloads.ironport.com schlägt fehl, und Traps werden alle 5-7 Sekunden gesendet. Stellen Sie sicher, dass Sie den DNS-Server nach Abschluss des Tests wieder in einen funktionierenden Server zurücksetzen.

Empfohlene OIDs für die Überwachung

Es handelt sich hierbei um eine Liste der zu überwachenden empfohlenen MIBs, nicht jedoch um eine vollständige Liste:

Hardware-OID	Name

1.3.6.1.4.1.15497.1.1.1.18.1.3	RAID-ID
1.3.6.1.4.1.15497.1.1.1.18.1.2	RAID-Status
1.3.6.1.4.1.15497.1.1.1.18.1.4	raidLetzterFehler
1.3.6.1.4.1.15497.1.1.1.10	Lüftertabelle
1.3.6.1.4.1.15497.1.1.1.9.1.2	Grad Celsius

Dies sind OIDs, die direkt der Ausgabe des Befehls status detailCLI zugeordnet werden:

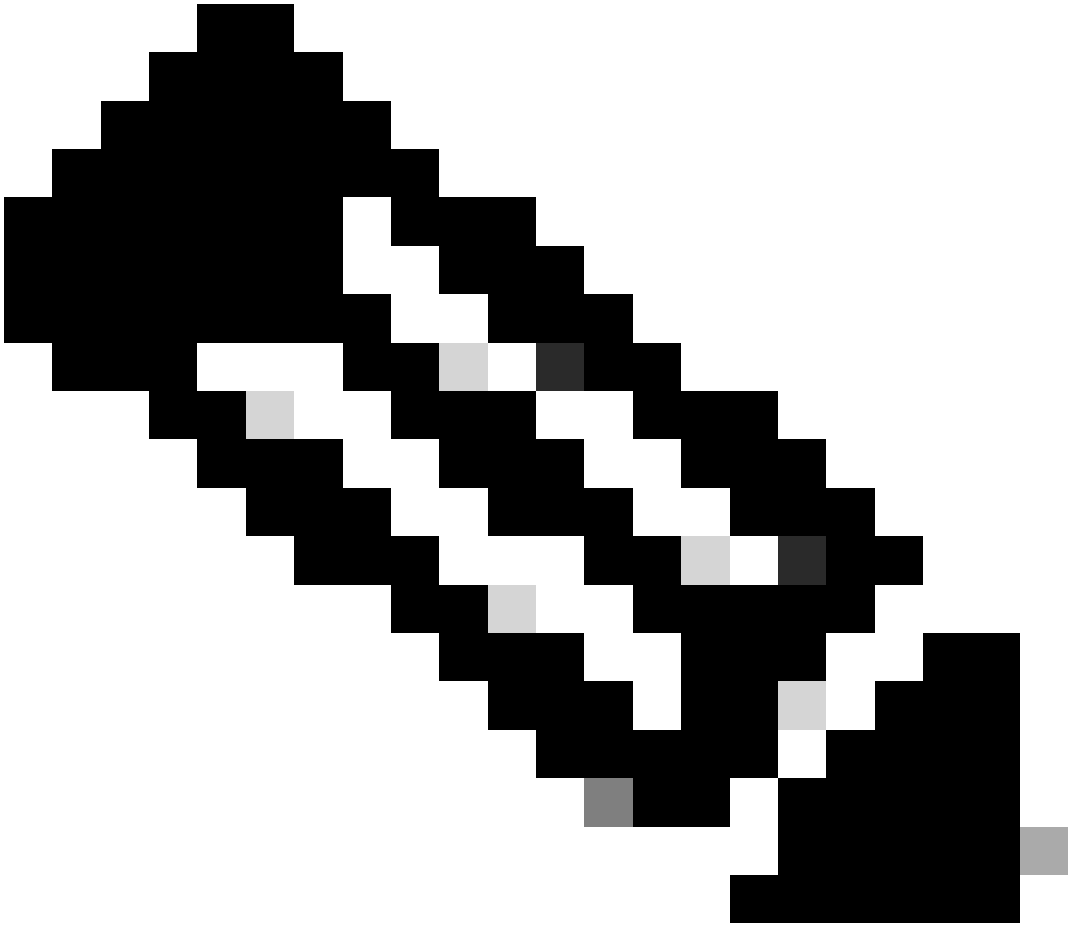
OID	Name	Statusdetailfeld
Systemressourcen		
1.3.6.1.4.1.15497.1.1.1.2.0	proCentCPU-Auslastung	CPU
1.3.6.1.4.1.15497.1.1.1.1.0	perCentSpeicherauslastung	RAM
Transaktionen pro Sekunde		
1.3.6.1.4.1.15497.1.2.3.7.1.1.0	CacheDurchsatzJetzt	Durchschnittliche Transaktionen pro Sekunde in letzter Minute.
1.3.6.1.4.1.15497.1.2.3.7.1.2.0	CacheDurchsatz1StdPeak	Maximale Anzahl von Transaktionen pro Sekunde in der letzten Stunde.
1.3.6.1.4.1.15497.1.2.3.7.1.3.0	CacheDurchsatz1StdMittel	Durchschnittliche Transaktionen pro Sekunde in der letzten Stunde.
1.3.6.1.4.1.15497.1.2.3.7.1.8.0	CacheDurchsatzLifePeak	Maximale Anzahl von Transaktionen pro Sekunde seit dem Neustart des Proxys.
1.3.6.1.4.1.15497.1.2.3.7.1.9.0	CacheDurchsatzLebensmittel	Durchschnittliche Transaktionen pro Sekunde seit dem Neustart des Proxys.
Bandbreite		
1.3.6.1.4.1.15497.1.2.3.7.4.1.0	cacheBreiteGesamtJetzt	Durchschnittliche

		Bandbreite in letzter Minute.
1.3.6.1.4.1.15497.1.2.3.7.4.2.0	CacheBwidthTotal1StdPeak	Maximale Bandbreite in der letzten Stunde.
1.3.6.1.4.1.15497.1.2.3.7.4.3.0	CacheBreiteInsgesamt1StdMittel	Durchschnittliche Bandbreite in der letzten Stunde.
1.3.6.1.4.1.15497.1.2.3.7.4.8.0	CacheBwidthTotalLifePeak	Maximale Bandbreite seit dem Neustart des Proxys.
1.3.6.1.4.1.15497.1.2.3.7.4.9.0	ZwischenspeicherGesamtlebensdauerMittel	Durchschnittliche Bandbreite seit dem Neustart des Proxys.
Reaktionszeit		
1.3.6.1.4.1.15497.1.2.3.7.9.1.0	cacheTrefferJetzt	Durchschnittliche Cache-Trefferrate in letzter Minute.
1.3.6.1.4.1.15497.1.2.3.7.9.2.0	CacheTreffer1StdPeak	Maximale Cache-Trefferrate in der letzten Stunde.
1.3.6.1.4.1.15497.1.2.3.7.9.3.0	CacheHits1StdMean	Durchschnittliche Cache-Trefferrate in der letzten Stunde.
1.3.6.1.4.1.15497.1.2.3.7.9.8.0	ZwischenspeicherTrefferLebensspitze	Die maximale Cache-Trefferrate seit dem Neustart des Proxys.
1.3.6.1.4.1.15497.1.2.3.7.9.9.0	ZwischenspeicherTrefferLebensmittel	Durchschnittliche Cache-Trefferrate seit Proxy-Neustart.
Cache-Trefferrate		
1.3.6.1.4.1.15497.1.2.3.7.5.1.0	cacheTrefferJetzt	Durchschnittliche Cache-Trefferrate in letzter Minute.
1.3.6.1.4.1.15497.1.2.3.7.5.2.0	CacheTreffer1StdPeak	Maximale Cache-Trefferrate in der letzten Stunde.
1.3.6.1.4.1.15497.1.2.3.7.5.3.0	CacheHits1StdMean	Durchschnittliche Cache-Trefferrate in

		der letzten Stunde.
1.3.6.1.4.1.15497.1.2.3.7.5.8.0	ZwischenspeicherTrefferLebensspitze	Die maximale Cache-Trefferrate seit dem Neustart des Proxys.
1.3.6.1.4.1.15497.1.2.3.7.5.9.0	ZwischenspeicherTrefferLebensmittel	Durchschnittliche Cache-Trefferrate seit Proxy-Neustart.
Verbindungen		
1.3.6.1.4.1.15497.1.2.3.2.7.0	cacheClientIdleConns	Inaktive Clientverbindungen.
1.3.6.1.4.1.15497.1.2.3.3.7.0	cacheServerIdleVerbindungen	Inaktive Serververbindungen
1.3.6.1.4.1.15497.1.2.3.2.8.0	CacheClientGesamtVerbindungen	Clientverbindungen gesamt
1.3.6.1.4.1.15497.1.2.3.3.8.0	CacheServerInsgesamtVerbindungen	Serververbindungen gesamt

Fehlerbehebung bei SNMP

Um die Verbindung zwischen SWA und Ihrem SNMP-Manager anzuzeigen, ist es am besten, Pakete zu erfassen. Sie können den Paketerfassungsfilter wie folgt einstellen: (Port 161 oder Port 162)



Hinweis: Dieser Filter beruht auf SNMP-Standardports. Wenn Sie die Ports geändert haben, fügen Sie die konfigurierten Portnummern in den Paketerfassungsfilter ein.

Schritte zur Paketerfassung von SWA:

Schritt 1: Anmeldung an der GUI

Schritt 2. Wählen Sie oben rechts Support und Hilfe aus.

Schritt 3: Wählen Sie Packet Capture aus

Schritt 4. Wählen Sie Einstellungen bearbeiten.

Schritt 5: Stellen Sie sicher, dass die richtige Schnittstelle ausgewählt wurde.

Schritt 6: Geben Sie die Filterbedingungen ein.

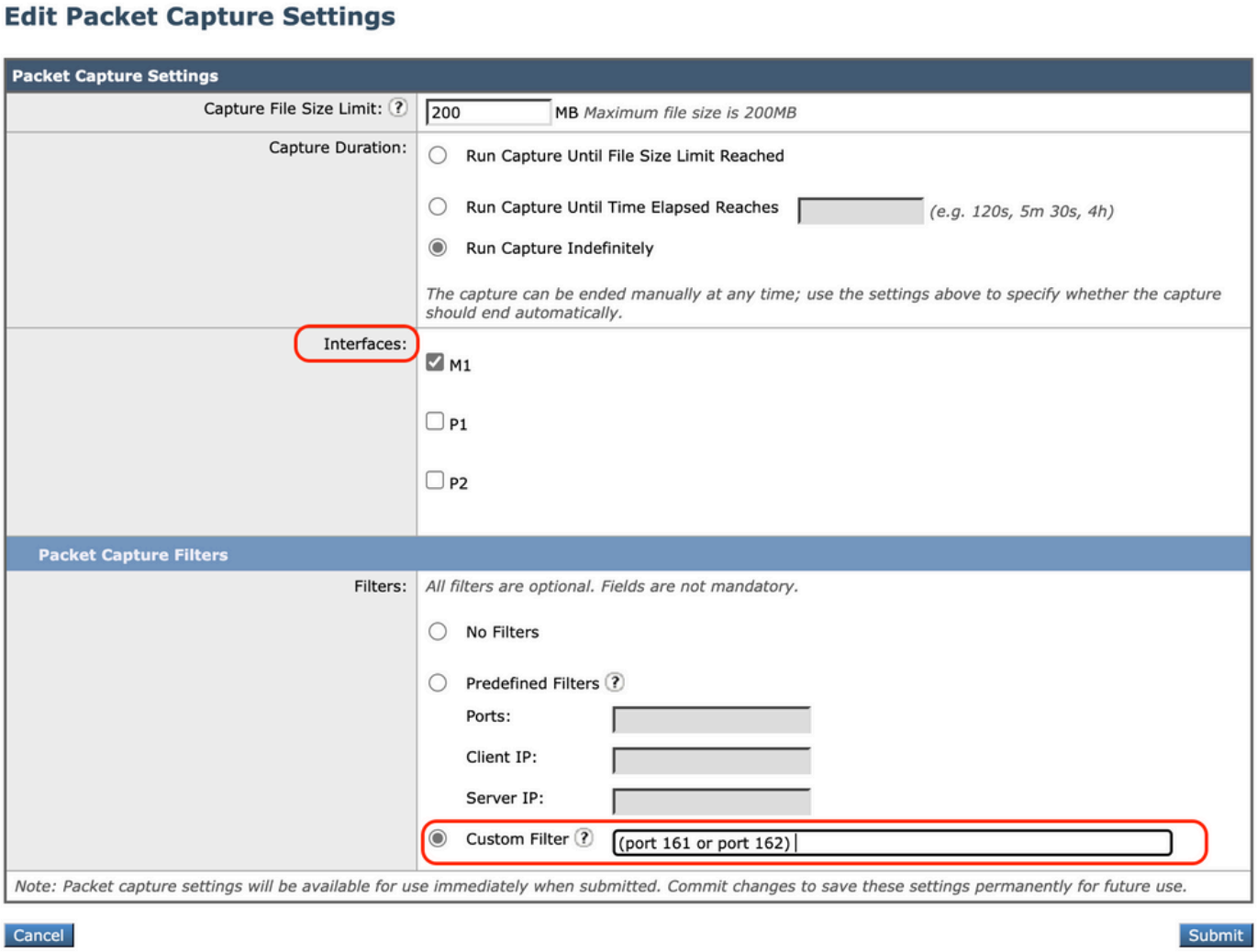
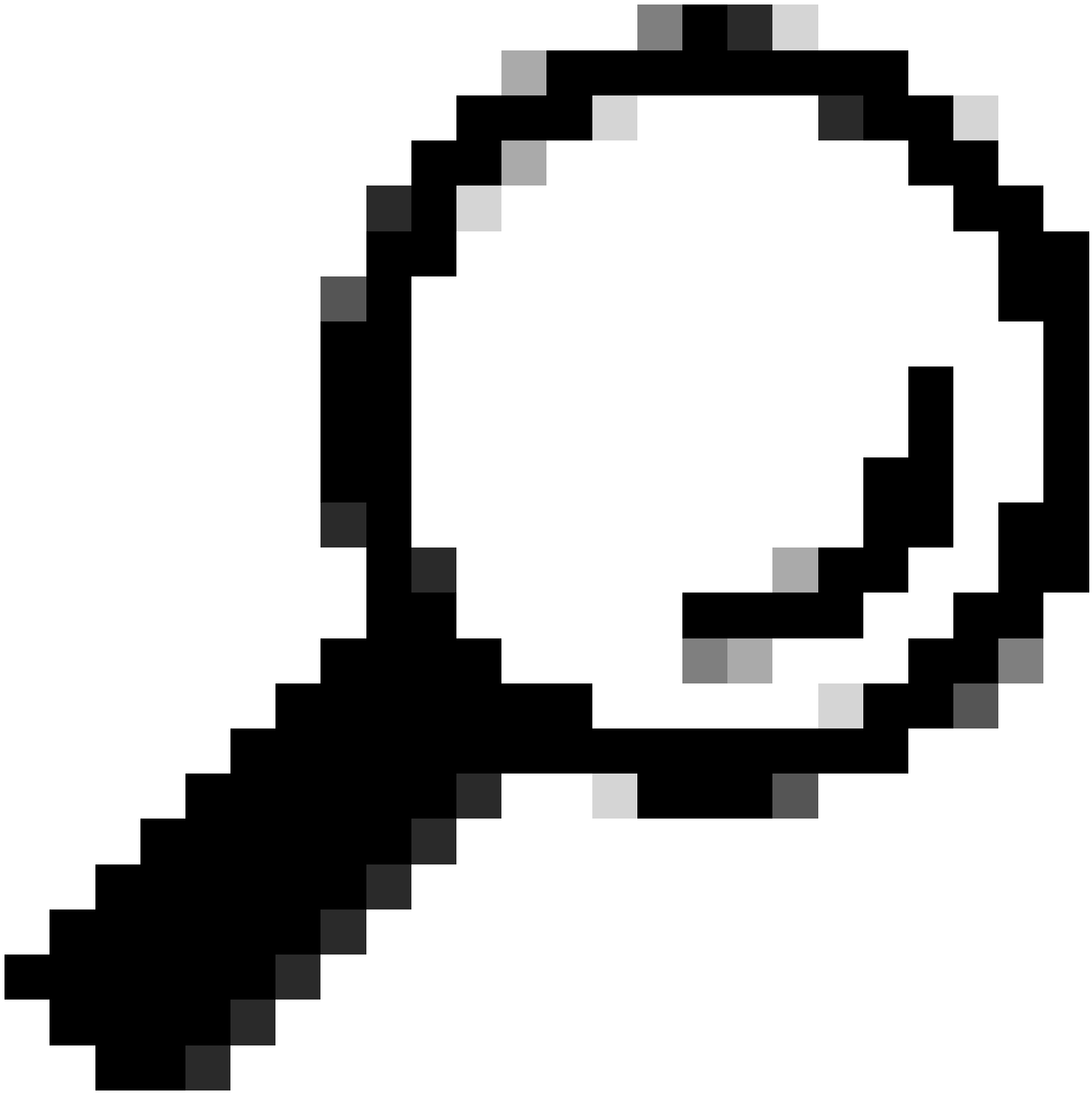


Image: Konfiguration der Paketerfassungsfilter

Schritt 7. Senden auswählen

Schritt 8: Wählen Sie Erfassung starten aus.



Tipp: Sie können SNMPv3-Paketerfassungen mit Wireshark entschlüsseln. Weitere Informationen finden Sie unter diesem Link: How-to-decrypt-snmpv3-packages-using-wireshark

SNMPWALK

snmpwalk ist der Name einer SNMP-Anwendung, die mehrere GET-NEXT-Anforderungen automatisch ausführt. Die SNMP GET-NEXT-Anforderung wird verwendet, um ein aktiviertes Gerät abzufragen und SNMP-Daten von einem Gerät zu empfangen. Der Befehl snmpwalk wird verwendet, da er dem Benutzer ermöglicht, GET-NEXT-Anforderungen zusammenzufassen, ohne für jede OID oder jeden Knoten in einem Unterbaum eindeutige Befehle eingeben zu müssen.

Installieren von SNMPWALK unter Windows-Betriebssystemen

Für Microsoft Windows-Benutzer müssen Sie das Tool zunächst herunterladen.

Installation von SNMPWALK auf Linux-Kernel

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

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

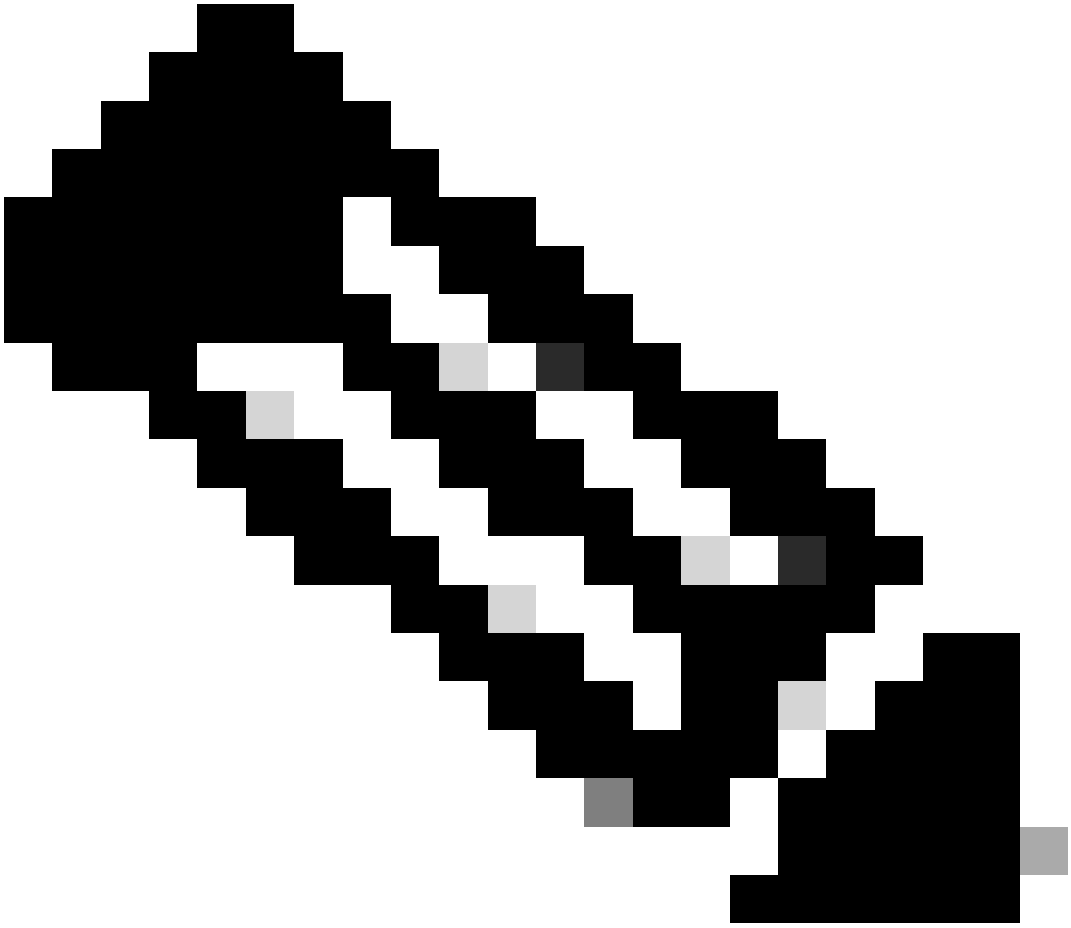
Installation von SNMPWALK unter MacOS

Standardmäßig ist snmpwalk unter MacOS installiert

Um eine SNMP GET-Anforderung zu generieren, können Sie den snmpwalk-Befehl von einem anderen Computer in Ihrem Netzwerk aus verwenden, der über eine Verbindung mit SWA verfügt. Hier einige Beispiele für den snmpwalk-Befehl:

```
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>
```



Hinweis: Sie können die Sicherheitsstufe auf noAuthNoPriv oder authNoPriv festlegen. Dies hängt von Ihrer SWA-Konfiguration ab.

SNMPTRAP

snmptrap ist ein versteckter CLI-Befehl, der SNMP auf dem SWA aktiviert haben muss. Sie können SNMP-Traps generieren, indem Sie das Objekt auswählen. Traps ist ein Beispiel:

```
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-Protokolle in SWA

SWA hat zwei Protokolle, die sich auf SNMP beziehen. Einige Protokolltypen, die sich auf die Webproxykomponente beziehen, sind nicht aktiviert. Sie können sie aktivieren unter:

- In GUI :Systemverwaltung > Protokoll-Subscriptions
- In CLI: logconfig > new

Protokolldateityp	Beschreibung	Unterstützt Syslog Push?	Standardmäßig aktiviert?
SNMP-Protokolle	Zeichnet Debug-Meldungen für das SNMP-Netzwerkmanagement-Modul auf.	Ja	Ja
SNMP-Modulprotokolle	Protokolliert Webproxy-Meldungen, die sich auf die Interaktion mit dem SNMP-	Nein	Nein

	Überwachungssystem beziehen.		

Häufige Probleme mit SNMP

Einige OIDS schlagen fehl (entweder kein Wert oder falscher Wert).

Dieses Problem hängt mit dem SNMP Pull zusammen. Es werden zwei Beispiele für die erwartete Ausgabe und Ausgabe mit einem Fehler angezeigt:

```
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
```

Sie können in snmp_logs nach "Application Faults" suchen

Sie können snmp_logs über die CLI überprüfen > grep > die Nummer auswählen, die snmp_logs zugeordnet ist:

```
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]>
```

Referenz

Benutzerhandbuch für AsyncOS 15.0 für Cisco Secure Web Appliance - LD (begrenzte Bereitstellung) - Fehlerbehebung [Cisco Secure Web Appliance] - Cisco

Berechnung der Proxy-CPU-Auslastung auf der WSA mit SNMP - Cisco

snmpcmd(1) (freebsd)

snmptrap (freebsd)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.