Configurazione e risoluzione dei problemi di SNMP in SWA

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi al protocollo SNMP (Simple Network Monitoring Protocol) in Secure Web Appliance (SWA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Access ToCommand Line Interface (CLI) di SWA
- Accesso amministrativo all'SWA.

- Conoscenze base di SNMP.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Funzionamento del protocollo SNMP

L'SNMP è un protocollo di comunicazione a livello di applicazione che consente ai dispositivi di rete di scambiare informazioni di gestione tra questi sistemi e con altri dispositivi esterni alla rete.

Tramite l'SNMP, gli amministratori di rete possono gestire le prestazioni, individuare e risolvere problemi e pianificare la crescita della rete.

L'SNMP rende il monitoraggio della rete più economico e consente di aumentare l'affidabilità della rete. Per ulteriori informazioni sul protocollo SNMP, vedere le RFC 1065, 1066 e 1067.

Una rete gestita da SNMP è composta da Manager, Agenti e Dispositivi gestiti.

- Il responsabile fornisce l'interfaccia tra il responsabile della rete umana e il sistema di gestione.
- L'agente fornisce l'interfaccia tra il manager e il dispositivo gestito
- I sistemi di gestione eseguono la maggior parte dei processi di gestione e forniscono la maggior parte delle risorse di memoria utilizzate per la gestione della rete.

Un agente risiede su ciascun dispositivo gestito e converte i dati delle informazioni di gestione locali (ad esempio informazioni sulle prestazioni o informazioni su eventi ed errori) rilevati in trap software in una forma leggibile per il sistema di gestione.

L'agente SNMP acquisisce i dati dal MIB (Management Information Base) (parametro del dispositivo e repository dei dati di rete) o da trap di errore o di modifica.

MIB

Il MIB, è una struttura di dati che descrive gli elementi di rete SNMP come un elenco di oggetti dati. Il manager SNMP deve compilare il file MIB per ogni tipo di apparecchiatura nella rete per monitorare i dispositivi SNMP.

Il manager e l'agente utilizzano un MIB e un set relativamente ridotto di comandi per lo scambio di informazioni. Il MIB è organizzato in una struttura ad albero con singole variabili rappresentate come foglie sui rami.

Per distinguere ogni variabile in modo univoco nel MIB e nei messaggi SNMP, viene utilizzato un

OID (Long Numic Tag) o un identificatore di oggetto (Object Identifier). Il MIB associa ogni OID a un'etichetta leggibile e a vari altri parametri correlati all'oggetto.

Il MIB viene quindi utilizzato come dizionario dati o codebook per assemblare e interpretare i messaggi SNMP.

Quando il manager SNMP desidera conoscere il valore di un oggetto, ad esempio lo stato di un punto di allarme, il nome del sistema o il tempo di attività dell'elemento, assembla un pacchetto GET che include l'OID per ciascun oggetto di interesse.

L'elemento riceve la richiesta e cerca ogni OID nella propria rubrica di codice (MIB). Se viene trovato l'OID (l'oggetto è gestito dall'elemento), viene assemblato un pacchetto di risposta che viene inviato con il valore corrente dell'oggetto incluso.

Se l'OID non viene trovato, viene inviata una risposta di errore speciale che identifica l'oggetto non gestito

Trap SNMP

Le trap SNMP consentono a un agente di notificare alla stazione di gestione eventi significativi tramite un messaggio SNMP non richiesto.

SNMPv1 e SNMPv2c, insieme al MIB associato, incoraggiano le notifiche trap-direct.

L'idea alla base della notifica trap-direct è che se un manager è responsabile di un numero elevato di dispositivi, e ogni dispositivo ha un numero elevato di oggetti, non è pratico per il manager raccogliere o richiedere informazioni da ogni oggetto su ogni dispositivo.

La soluzione è che ogni agente sul dispositivo gestito notifichi il manager senza richiesta. A tale scopo, invia un messaggio noto come Trap dell'evento.

Quando il manager riceve l'evento, lo visualizza e può scegliere di eseguire un'azione in base all'evento. Ad esempio, il manager può eseguire direttamente il polling dell'agente o di altri agenti di dispositivo associati per comprendere meglio l'evento.

La notifica Trap-Directed può comportare un notevole risparmio di risorse di rete e di agenti eliminando la necessità di richieste SNMP frivole. Tuttavia, non è possibile eliminare completamente i sondaggi SNMP.

Le richieste SNMP sono necessarie per l'individuazione e le modifiche alla topologia. Inoltre, un agente di dispositivo gestito non è in grado di inviare una trap se il dispositivo ha subito un'interruzione irreversibile.

I trap SNMPv1 sono definiti nella RFC 1157 con i seguenti campi:

- Enterprise:identifica il tipo di oggetto gestito che genera la trap.
- Indirizzo agente: fornisce l'indirizzo dell'oggetto gestito che genera la trap.
- Tipo di registrazione generica: indica uno dei diversi tipi di registrazione generica.

- Codice trap specifico: indica uno dei vari codici di trap specifici.
- Timestamp: fornisce l'intervallo di tempo trascorso tra l'ultima reinizializzazione della rete e la generazione della trap.
- Associazioni variabili: il campo dati della trap che contiene la PDU. Ogni associazione di variabile associa una particolare istanza dell'oggetto MIB al relativo valore corrente.

SNMPv3

SNMPv3 supporta l'identificatore "ID motore" SNMP, che identifica in modo univoco ogni entità SNMP. È possibile che si verifichino conflitti se due entità SNMP hanno EngineID duplicati.

Il EngineID viene utilizzato per generare la chiave per i messaggi autenticati. Per ulteriori informazioni su SNMPv3, vedere le RFC 2571-2575.

Molti prodotti SNMP rimangono fondamentalmente gli stessi in SNMPv3, ma sono potenziati da queste nuove funzioni:

Sicurezza

- Autenticazione
- Privacy

Amministrazione

- Autorizzazione e controllo degli accessi
- Contesti logici
- Denominazione di entità, identità e informazioni
- Persone e politiche
- Gestione dei nomi utente e delle chiavi
- Destinazioni di notifica e relazioni proxy
- Configurazione remota tramite operazioni SNMP

I modelli di sicurezza SNMPv3 si presentano principalmente in due forme: autenticazione e crittografia.

L'autenticazione viene utilizzata per garantire che solo il destinatario previsto legga le trap. Durante la creazione, ai messaggi viene assegnata una chiave speciale in base all'ID motore dell'entità. La chiave viene condivisa con il destinatario e utilizzata per ricevere il messaggio. Crittografia, privacy crittografa il payload del messaggio SNMP per garantire che utenti non autorizzati non possano leggerlo. Qualsiasi trap intercettata riempita di caratteri alterati è illeggibile. La privacy è particolarmente utile nelle applicazioni in cui i messaggi SNMP devono essere instradati su Internet.
In un gruppo SNMP sono disponibili tre livelli di protezione:

noAuthnoPriv - Comunicazione senza autenticazione e privacy.
authNoPriv - Comunicazione con autenticazione e senza privacy. I protocolli utilizzati per l'autenticazione sono MD5 (Message-Digest Algorithm 5) e SHA (Secure Hash Algorithm).

authPriv - Comunicazione con autenticazione e privacy. I protocolli utilizzati per l'autenticazione sono MD5 e SHA. Per la privacy, è possibile utilizzare i protocolli DES (Data Encryption Standard) e AES (Advanced Encryption Standard).

SNMP in SWA

Il sistema operativo AsyncOS supporta il monitoraggio dello stato del sistema tramite SNMP.

Nota:

- SNMPisoff per impostazione predefinita.
- Operazioni SNMPSET (configurazione) non implementate.
- AsyncOS supporta SNMPv1, v2 e v3.
- L'autenticazione e la crittografia dei messaggi sono obbligatorie quando si abilita SNMPv3. Le passphrase per l'autenticazione e la crittografia devono essere diverse.
- L'algoritmo di crittografia può essere AES (scelta consigliata) o DES.
- L'algoritmo di autenticazione può essere SHA-1 (scelta consigliata) o MD5.
- Il comando nmpconfig "ricorda" le passphrase alla successiva esecuzione del comando.
- Per le versioni AsyncOS precedenti alla 15.0, il nome utente di SNMPv3 è: v3get.
- Per AsyncOS versione 15.0 e successive, il nome utente predefinito di SNMPv3 è: v3get. Gli amministratori possono scegliere qualsiasi altro nome utente.
- Se si utilizza onlySNMPv1 o SNMPv2, è necessario impostare una stringa della community. La stringa della community non viene impostata su public per impostazione predefinita.
- Per SNMPv1 e SNMPv2, è necessario specificare una rete da cui vengono accettate le richieste SNMPGET.
- Per utilizzare i trap, è necessario che sia in esecuzione un SNMPmanager (non incluso in AsyncOS) e che il relativo indirizzo IP sia stato immesso come destinazione dei trap. È possibile utilizzare un nome host, ma in tal caso i trap funzionano solo se il DNS funziona.

Configurazione di SNMPonitor

Per configurare SNMP in modo da raccogliere le informazioni sullo stato del sistema per l'accessorio, usare il comando thesnmpconfig nella CLI. Dopo aver scelto e configurato i valori per un'interfaccia, l'accessorio risponde alle richieste GET di SNMPv3.

Quando si utilizza SNMP, tenere presenti i seguenti punti:

- Le richieste SNMP versione 3 devono includere una passphrase corrispondente.

- Per impostazione predefinita, le richieste versione 1 e versione 2 vengono rifiutate.
- Se abilitata, le richieste delle versioni 1 e 2 devono avere una stringa della community corrispondente.

```
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
```

File MIB SWA

I file MIB sono disponibili all'indirizzo URL: https://www.cisco.com/c/en/us/support/security/web-security-appliance/series.html

Utilizzare la versione più recente di ciascun file MIB.

Sono disponibili più file MIB:

- asyncoswebsecurityappliance-mib.txt è una descrizione compatibile con SNMPv2 del MIB Enterprise for Secure Web Appliance.
- ASYNCOS-MAIL-MIB.txt è una descrizione compatibile con SNMPv2 del MIB Enterprise per le appliance di sicurezza e-mail.
- IRONPORT-SMI.txt Questo file "Structure of Management Information" definisce il ruolo di asyncoswebsecurityappliance-mib.

Questa release implementa un sottoinsieme di sola lettura di MIB-II definito nelle RFC 1213 e 1907.

Seehttps://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118415-technote-wsa-00.html per ulteriori informazioni sul monitoraggio dell'utilizzo della CPU sull'accessorio con SNMP.

SWA SNMP TRAP

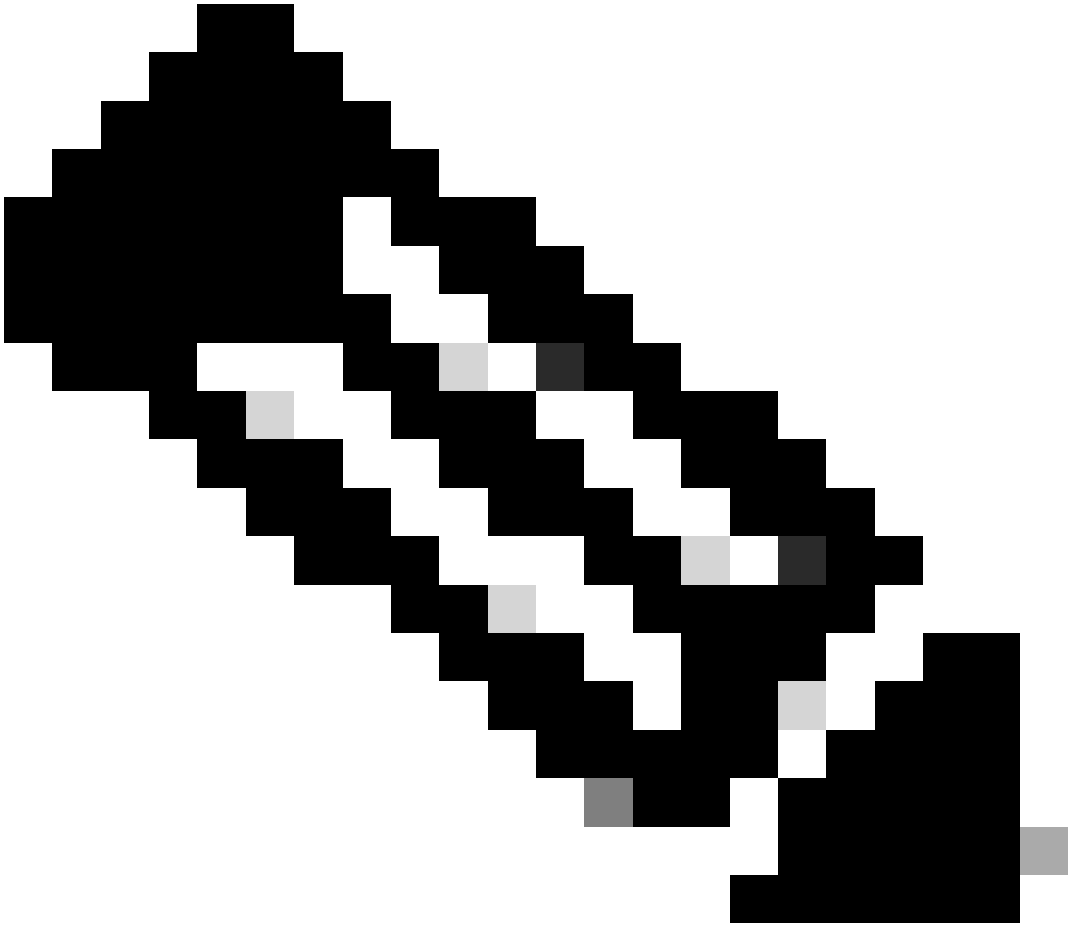
L'SNMP consente di inviare trap, o notifiche, per avvisare un'applicazione di amministrazione quando una o più condizioni sono state soddisfatte.

I trap sono pacchetti di rete contenenti dati relativi a un componente del sistema che invia la trap.

I trap vengono generati quando viene soddisfatta una condizione sull'agente SNMP (in questo caso, CiscoSecure Web Appliance).

Una volta soddisfatta la condizione, l'agente SNMP forma un pacchetto SNMP e lo invia all'host su cui è in esecuzione il software della console di gestione SNMP.

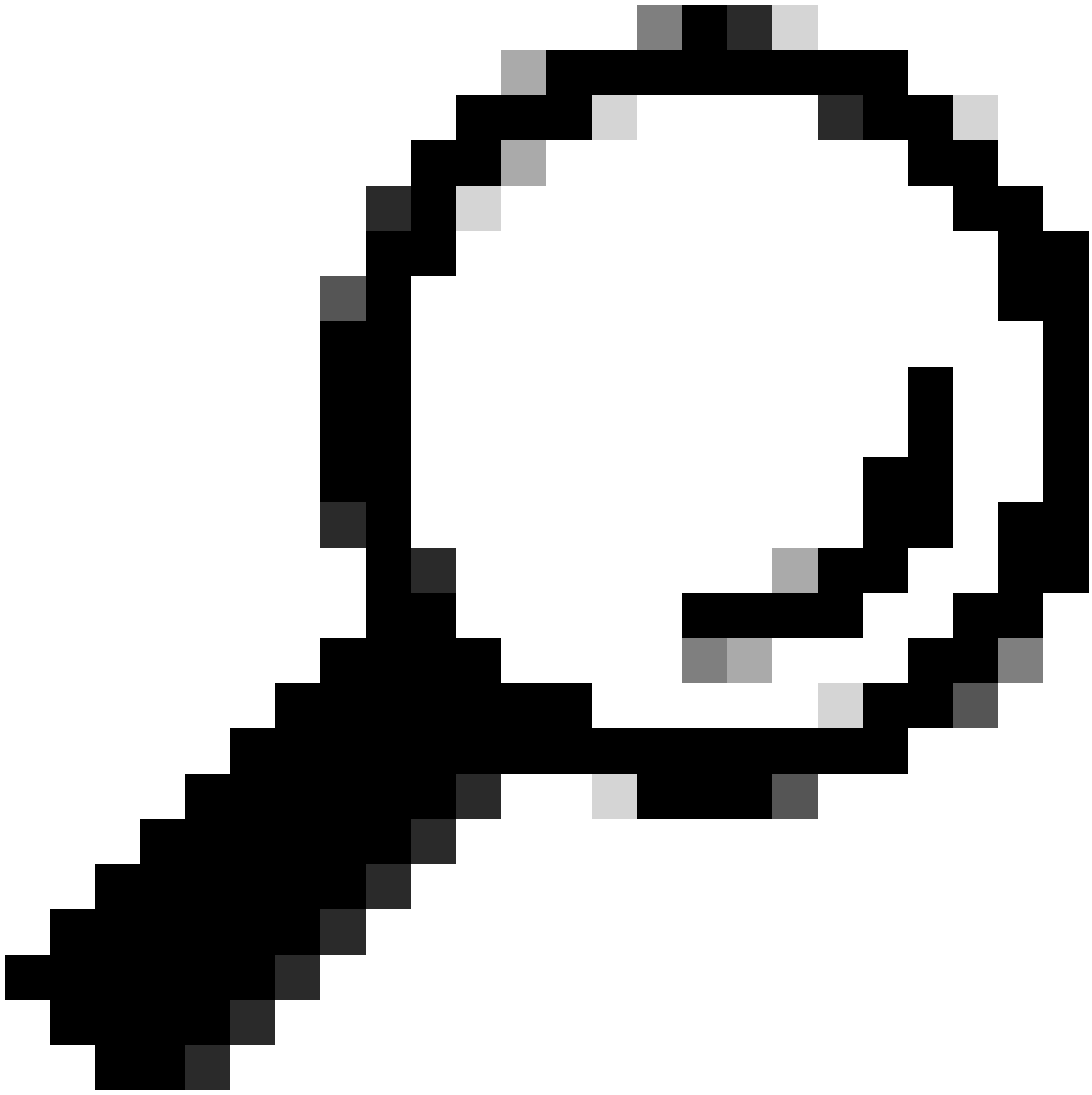
È possibile configurare SNMPtraps (abilitare o disabilitare trap specifiche) quando si abilita SNMPper un'interfaccia.



Nota: per specificare più destinazioni trap, quando viene richiesto di specificare la destinazione trap, è possibile immettere fino a 10 indirizzi IP separati da virgole.

La trap ConnectivityFailure consente di monitorare la connessione dell'accessorio a Internet. A tale scopo, tenta di connettersi e inviare una richiesta HTTP GET a un singolo server esterno ogni 5-7 secondi. Per impostazione predefinita, l'URL monitorato è downloads.ironport.com sulla porta 80.

Per modificare l'URL o la porta monitorata, eseguire il comando snmpconfig e abilitare la trap connecivityFailure, anche se è già abilitata. Viene visualizzata una richiesta di modifica dell'URL.



Suggerimento: per simulare i trap di errore di connettività, è possibile utilizzare il comando dnsconfig CLI per immettere un server DNS non funzionante. Le ricerche di downloads.ironport.com hanno esito negativo e i trap vengono inviati ogni 5-7 secondi. Accertarsi di ripristinare il server DNS funzionante al termine del test.

OID di monitoraggio consigliati

Questo è un elenco dei MIB consigliati da monitorare e non un elenco esaustivo:

OID hardware	Nome
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	statoRAID

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	TabellaVentagli
1.3.6.1.4.1.15497.1.1.1.9.1.2	gradi Celsius

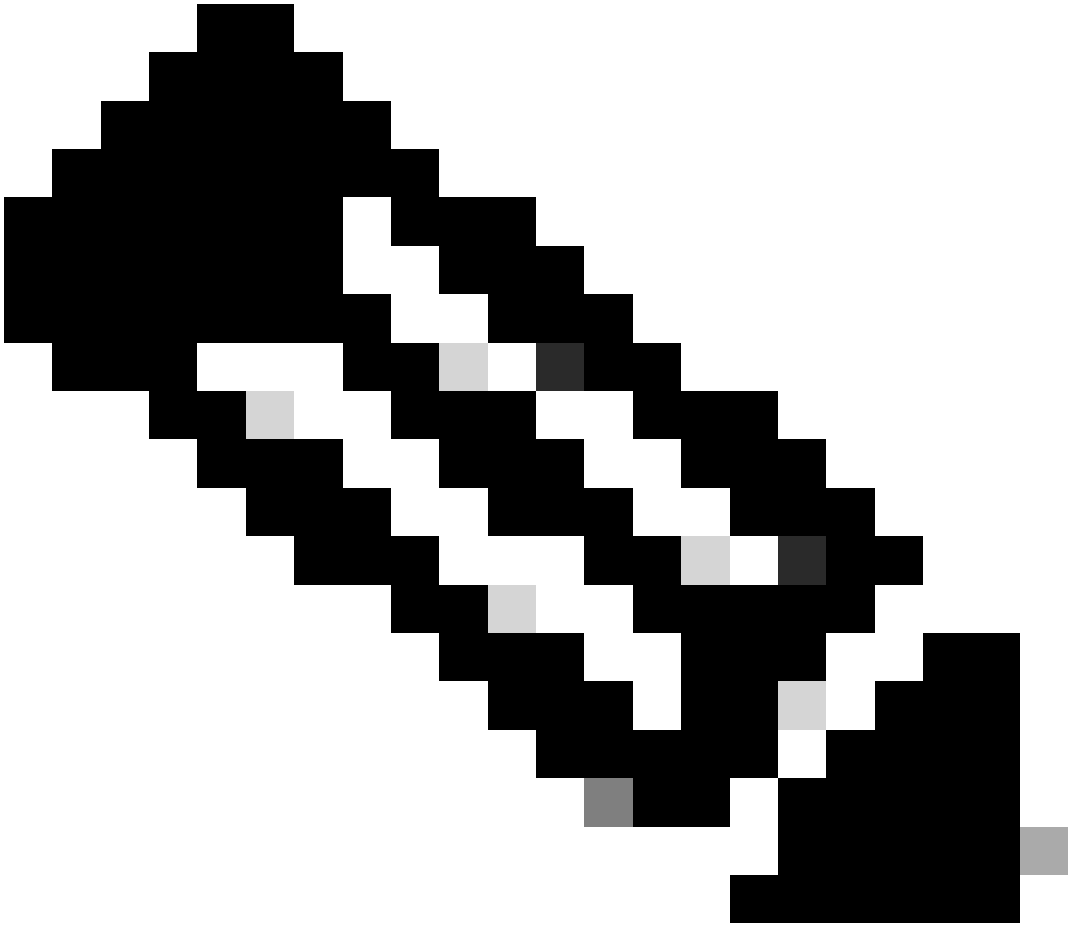
Gli OID vengono mappati direttamente all'output del comando status detailCLI:

OID	Nome	Campo Dettaglio stato
Risorse di sistema		
1.3.6.1.4.1.15497.1.1.1.2.0	PercentualeCPUtilizzazione	CPU
1.3.6.1.4.1.15497.1.1.1.1.0	PercentualeUtilizzoMemoria	RAM
Transazioni al secondo		
1.3.6.1.4.1.15497.1.2.3.7.1.1.0	cacheThroughputOra	Media transazioni al secondo nell'ultimo minuto.
1.3.6.1.4.1.15497.1.2.3.7.1.2.0	CacheThruput1hrPeak	Numero massimo di transazioni al secondo nell'ultima ora.
1.3.6.1.4.1.15497.1.2.3.7.1.3.0	cacheThruput1hrMean	Media transazioni al secondo nell'ultima ora.
1.3.6.1.4.1.15497.1.2.3.7.1.8.0	cacheThruputLifePeak	Numero massimo di transazioni al secondo dal riavvio del proxy.
1.3.6.1.4.1.15497.1.2.3.7.1.9.0	DurataThroughputCacheMedia	Numero medio di transazioni al secondo dal riavvio del proxy.
Larghezza di banda		
1.3.6.1.4.1.15497.1.2.3.7.4.1.0	cacheLarghezzaBandaTotaleOra	Larghezza di banda media nell'ultimo minuto.
1.3.6.1.4.1.15497.1.2.3.7.4.2.0	cacheBwidthTotal1hrPeak	Larghezza di banda massima nell'ultima ora.
1.3.6.1.4.1.15497.1.2.3.7.4.3.0	cacheBwidthTotal1hrMean	Larghezza di banda media nell'ultima ora.
1.3.6.1.4.1.15497.1.2.3.7.4.8.0	cacheBwidthTotalLifePeak	Larghezza di banda massima dal riavvio del proxy.
1.3.6.1.4.1.15497.1.2.3.7.4.9.0	cacheBwidthTotalLifeMean	Larghezza di banda media dal riavvio del proxy.
Tempo di risposta		
1.3.6.1.4.1.15497.1.2.3.7.9.1.0	cacheAccessiOra	Frequenza media riscontri

		cache nell'ultimo minuto.
1.3.6.1.4.1.15497.1.2.3.7.9.2.0	cacheHits1hrPeak	Frequenza massima di accesso alla cache nell'ultima ora.
1.3.6.1.4.1.15497.1.2.3.7.9.3.0	cacheHits1hrMean	Frequenza media di riscontri nella cache nell'ultima ora.
1.3.6.1.4.1.15497.1.2.3.7.9.8.0	cacheHitsLifePeak	Frequenza massima di accesso alla cache dal riavvio del proxy.
1.3.6.1.4.1.15497.1.2.3.7.9.9.0	cacheHitsLifeMean	Frequenza media di riscontri nella cache dal riavvio del proxy.
Frequenza riscontri cache		
1.3.6.1.4.1.15497.1.2.3.7.5.1.0	cacheAccessiOra	Frequenza media riscontri cache nell'ultimo minuto.
1.3.6.1.4.1.15497.1.2.3.7.5.2.0	cacheHits1hrPeak	Frequenza massima di accesso alla cache nell'ultima ora.
1.3.6.1.4.1.15497.1.2.3.7.5.3.0	cacheHits1hrMean	Frequenza media di riscontri nella cache nell'ultima ora.
1.3.6.1.4.1.15497.1.2.3.7.5.8.0	cacheHitsLifePeak	Frequenza massima di accesso alla cache dal riavvio del proxy.
1.3.6.1.4.1.15497.1.2.3.7.5.9.0	cacheHitsLifeMean	Frequenza media di riscontri nella cache dal riavvio del proxy.
Connessioni		
1.3.6.1.4.1.15497.1.2.3.2.7.0	.CacheClientIdleConns	Connessioni client inattive.
1.3.6.1.4.1.15497.1.2.3.3.7.0	cacheServerInattivitàConn	Connessioni server inattive.
1.3.6.1.4.1.15497.1.2.3.2.8.0	cacheClientTotaleConn	Totale connessioni client.
1.3.6.1.4.1.15497.1.2.3.3.8.0	cacheServerTotaleConn	Totale connessioni server.

Risoluzione dei problemi di SNMP

Per visualizzare la connettività tra SWA e il programma di gestione SNMP, è consigliabile acquisire i pacchetti. È possibile impostare il filtro di acquisizione su: (porta 161 o porta 162)



Nota: questo filtro è dovuto alle porte SNMP predefinite. Se le porte sono state modificate, inserire i numeri di porta configurati nel filtro di acquisizione pacchetti.

Passaggi per acquisire i pacchetti da SWA:

Passaggio 1. accedere alla GUI

Passaggio 2. in alto a destra scegliere Supporto e Guida

Passaggio 3. selezionare Packet Capture

Passaggio 4. scegliere Modifica impostazioni

Passaggio 5. Assicurarsi che sia stata selezionata l'interfaccia corretta

Passaggio 6. Immettere le condizioni del filtro.

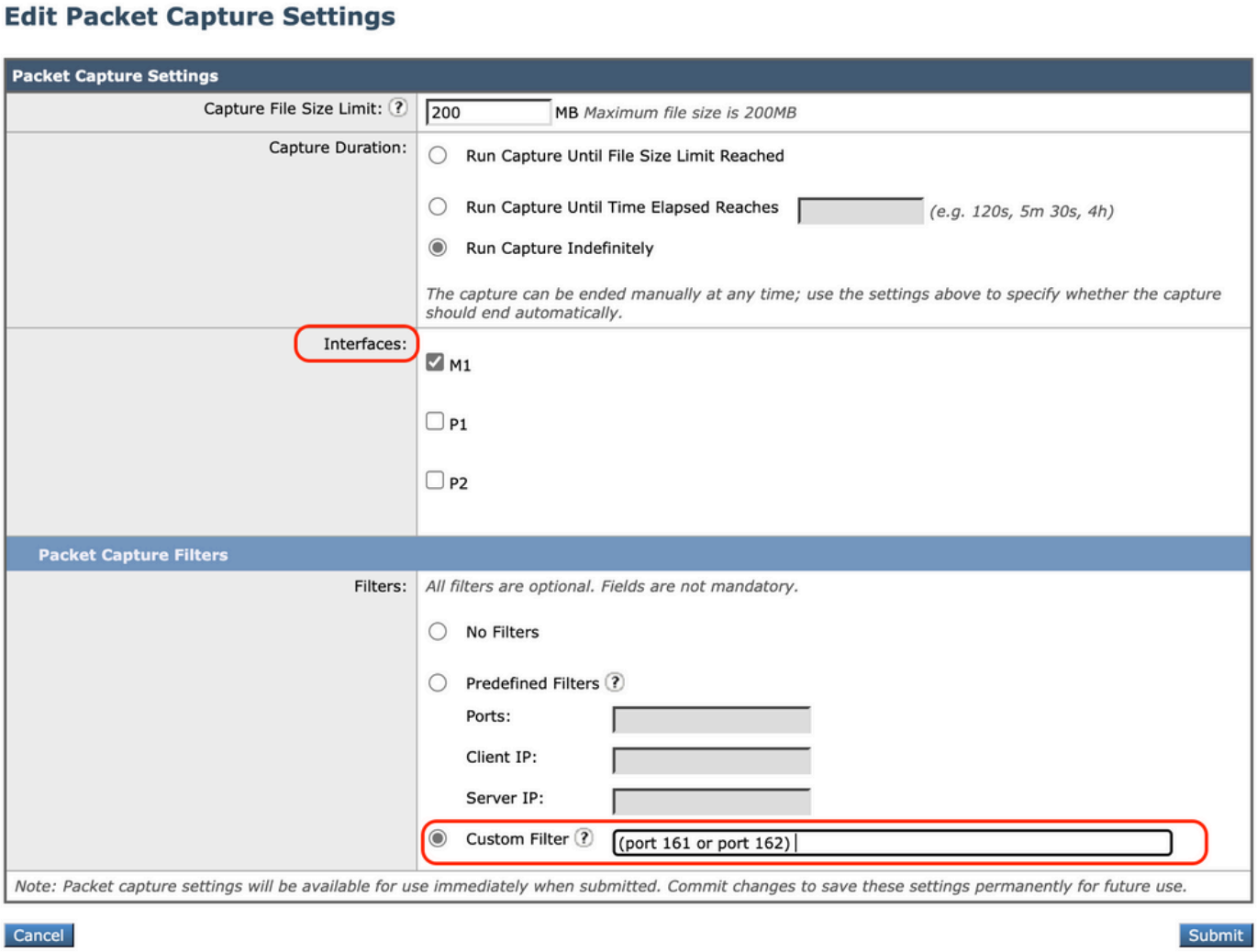
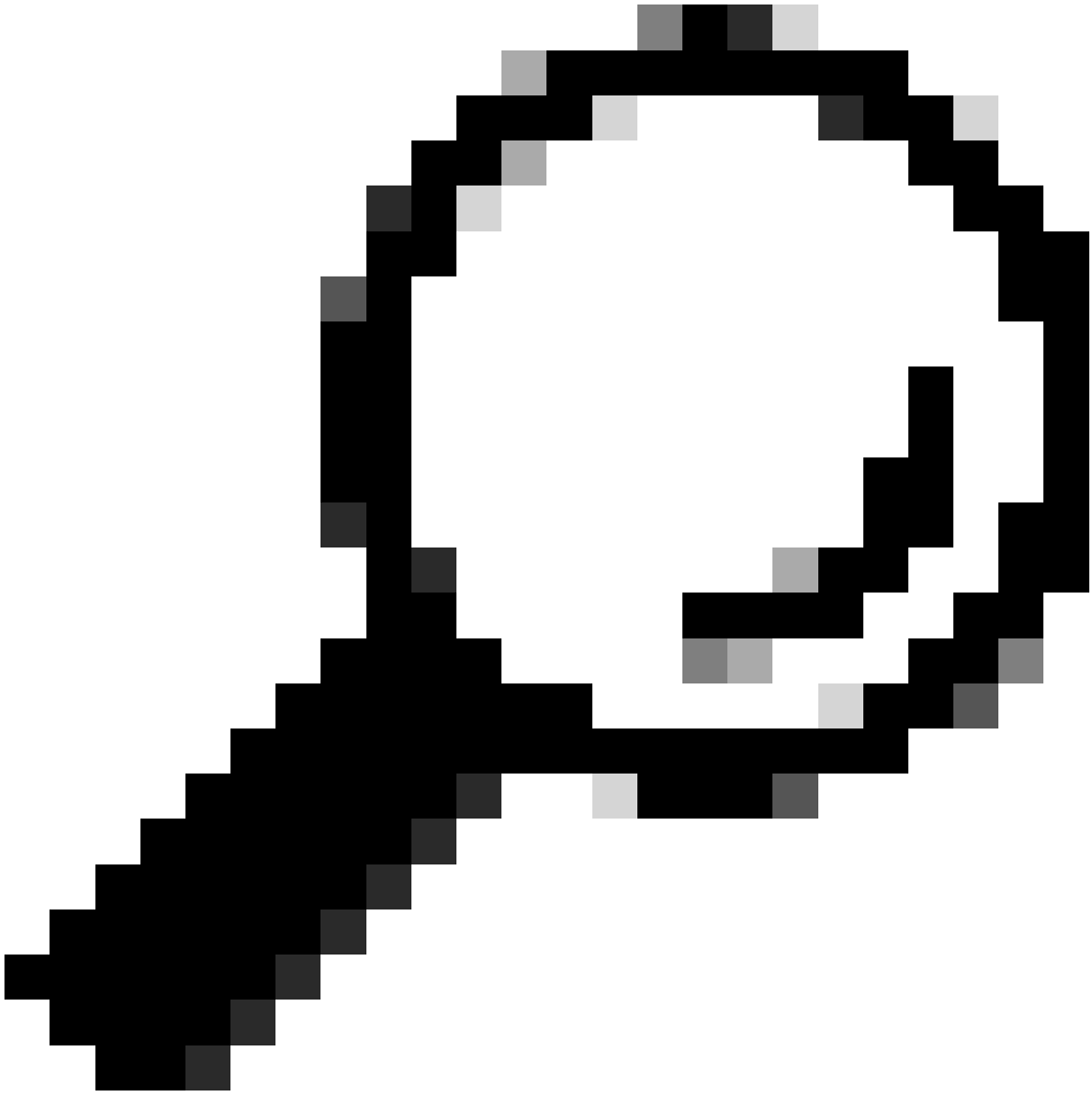


Immagine - Configurazione dei filtri di acquisizione dei pacchetti

Passaggio 7. Scegliere Invia

Passaggio 8. Scegliere Avvia acquisizione.



Suggerimento: con Wireshark è possibile decrittografare le acquisizioni di pacchetti SNMPv3. per ulteriori informazioni, visitare questo collegamento: procedura per decrittografare pacchetti SNMPv3 utilizzando wireshark

SNMPWALK

snmpwalk è il nome assegnato a un'applicazione SNMP che esegue automaticamente più richieste GET-NEXT. La richiesta SNMP GET-NEXT viene utilizzata per eseguire query su un dispositivo abilitato e prelevare dati SNMP da un dispositivo. Il comando snmpwalk viene utilizzato perché consente all'utente di concatenare le richieste GET-NEXT senza dover immettere comandi univoci per ogni OID o nodo all'interno di una sottostruttura

Installazione di SNMPWALK nei sistemi operativi Windows

Per gli utenti di Microsoft Windows, è innanzitutto necessario scaricare lo strumento.

Installazione di SNMPWALK sul kernel Linux

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

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

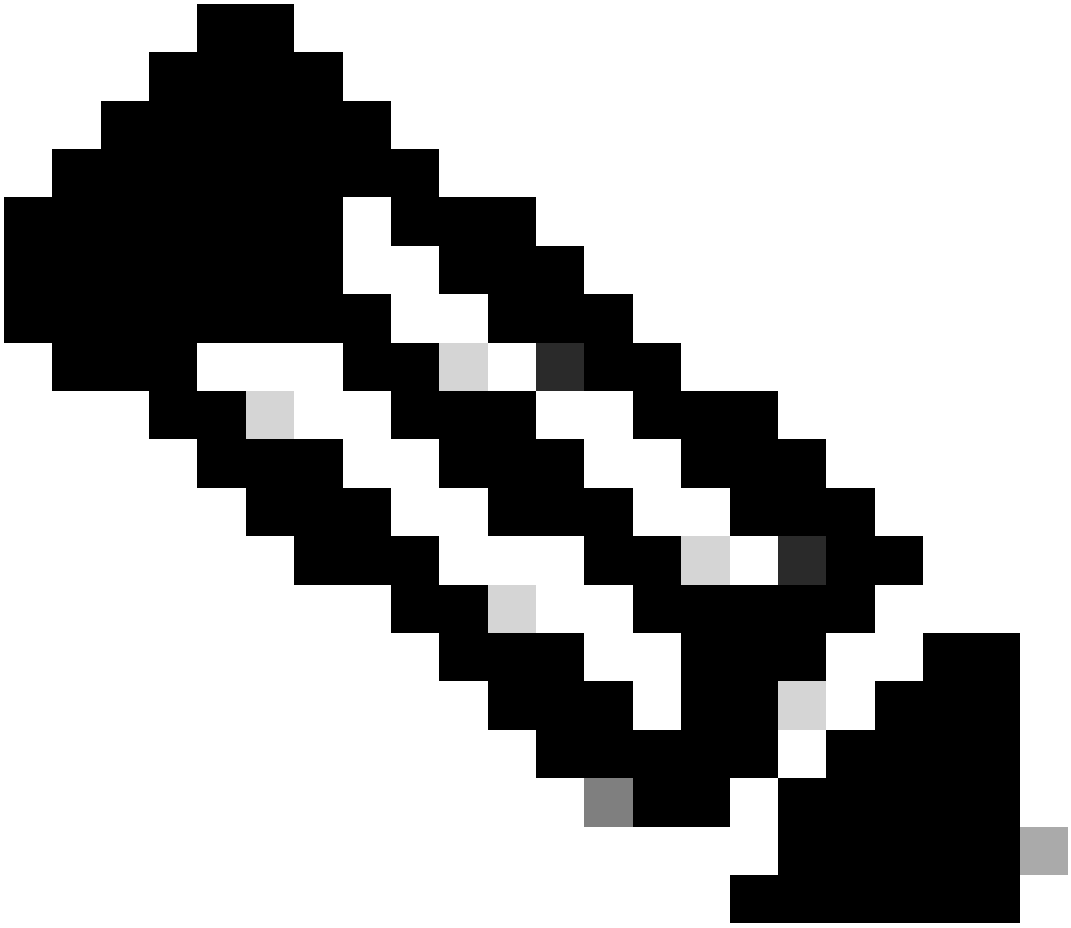
Installazione di SNMPWALK su MacOS

Per impostazione predefinita, snmpwalk è installato in MacOS

Per generare la richiesta SNMP GET, è possibile utilizzare il comando snmpwalk da un altro computer della rete connesso a SWA. Di seguito sono riportati alcuni esempi di 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: è possibile scegliere di impostare il livello di protezione su noAuthNoPriv o authNoPriv o authPriv a seconda delle configurazioni SWA.

SNMPTRAP

snmptrap è un comando CLI nascosto che richiede l'abilitazione del protocollo SNMP sull'interfaccia SWA. È possibile generare la trap SNMP selezionando l'oggetto e la trap, come illustrato nell'esempio seguente:

```
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
```

Log SNMP in SWA

SWA dispone di due log relativi a SNMP. Alcuni tipi di log relativi al componente proxy Web non sono abilitati. è possibile abilitarli da:

- In GUI: Amministrazione di sistema > Registra sottoscrizioni
- Nella CLI: logconfig > new

Tipo file registro	Descrizione	Supporta Syslog Push?	Attivato per impostazione predefinita?
Log SNMP	Registra i messaggi di debug correlati al motore di gestione della rete SNMP.	Sì	Sì
Registri del	Registra i messaggi proxy Web relativi	No	No

modulo SNMP	all'interazione con il sistema di monitoraggio SNMP.		

Problemi comuni di SNMP

Alcuni OIDS hanno esito negativo (nessun valore o valore errato).

Questo problema è correlato al pull SNMP. Di seguito sono riportati due esempi di output previsto e di output con errore:

```
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
```

È possibile verificare la presenza di "Errori applicazione" in snmp_logs

È possibile controllare snmp_logs da CLI > grep > scegliere il numero associato 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]>
```

Riferimento

Guida per l'utente di AsyncOS 15.0 per Cisco Secure Web Appliance - LD (installazione limitata) - Risoluzione dei problemi [Cisco Secure Web Appliance] - Cisco

Calcolo dell'utilizzo della CPU proxy sul server WSA tramite SNMP - Cisco

snmpcmd(1) (libere)

snmptrap (freebsd)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).