在SWA中配置SNMP並對其進行故障排除

目錄

簡介

本文描述對安全Web裝置(SWA)中的簡單網路監控協定(SNMP)進行故障排除的步驟。

必要條件

需求

思科建議瞭解以下主題：

- 訪問SWA的命令列介面(CLI)。
- 對SWA的管理訪問。
- SNMP的基本知識。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

SNMP的運作方式

SNMP是一種應用層通訊協定，允許網路裝置在這些系統之間以及與網路外部的其他裝置交換管理資訊。

透過SNMP，網路管理員可以管理網路效能、查詢和解決網路問題，以及規劃網路成長。

SNMP使網路監控更具成本效益，並使您的網路更為可靠。 (有關SNMP的詳細資訊，請參閱RFC 1065、1066和1067。)

SNMP管理的網路由管理器、代理和受管裝置組成。

- 管理器提供以人為本的網路管理器和管理系統之間的介面。
- 代理提供管理器和受管裝置之間的介面
- 管理系統執行大部分的管理程式，並提供網路管理所需的大量記憶體資源。

每個受管裝置上都有一個代理，可將捕獲在軟體陷阱中的本地管理資訊資料（如效能資訊或事件和錯誤資訊）轉換為可讀的管理系統格式。

SNMP代理從管理資訊庫(MIB)（裝置引數和網路資料庫）或從錯誤或更改陷阱中捕獲資料。

MIB

MIB是一種資料結構，它將SNMP網路元素描述為資料對象的清單。SNMP管理器必須為網路中的每種裝置型別編譯MIB檔案以監控SNMP裝置。

管理器和代理使用MIB和相對較小的一組命令來交換資訊。MIB以樹形結構組織，各個變數以枝葉形式表示。

長數字標籤或對象識別符號(OID)用於在MIB和SNMP消息中唯一區分每個變數。MIB將每個OID與一個可讀標籤以及與對象相關的各種其它引數相關聯。

然後，MIB用作資料詞典或代碼簿，用於彙編和解釋SNMP消息。

當SNMP管理器想要瞭解對象的值（例如警報點的狀態、系統名稱或元素正常運行時間）時，它會組合一個包含每個感興趣對象的OID的GET資料包。

元素接收請求並在代碼簿(MIB)中查詢每個OID。如果找到OID（對象由元素管理），則組合響應資料包並傳送包含對象的當前值。

如果找不到OID，則會傳送特殊的錯誤回應，以辨識未管理的物件

SNMP陷阱

SNMP陷阱使代理能夠透過未經請求的SNMP消息通知管理站重大事件。

SNMPv1和SNMPv2c，以及相關的MIB，鼓勵陷阱定向通知。

陷阱定向通知背後的想法是，如果管理器負責大量的裝置，並且每個裝置都有大量對象，則管理器輪詢或請求每個裝置上每個對象的資訊是不切實際的。

解決方案是讓受管裝置上的每個代理通知管理器，而不進行請求。它透過傳送一個稱為「事件陷阱」的消息來完成此操作。

管理員收到事件後，會顯示該事件，並可選擇根據事件採取動作。例如，管理員可以直接輪詢代理，或者輪詢其他關聯的裝置代理，以便更好地瞭解事件。

陷阱定向通知可消除輕率的SNMP請求，從而顯著節省網路和代理資源。但是，不可能完全消除SNMP輪詢。

發現和拓撲更改需要SNMP請求。此外，如果裝置發生了災難性中斷，受管裝置代理也無法傳送陷阱。

RFC 1157中定義了SNMPv1陷阱，其欄位如下：

- 企業：辨識產生陷阱的受管理物件型別。
- 代理地址：提供生成陷阱的受管對象的地址。
- Generic trap type：表示這是若干種常規陷阱型別之一。
- Specific trap code：表示這是若干種特定陷阱代碼之一。
- Time stamp：提供從上次網路重新初始化到生成陷阱之間經過的時間。
- 變數繫結：陷阱中包含PDU的資料欄位。每個變數繫結將特定MIB對象例項與其當前值相關聯。

SNMPv3

SNMPv3支援SNMP「引擎ID」識別符號，可唯一標識每個SNMP實體。如果兩個SNMP實體具有重複的EngineID，則可能會發生衝突。

EngineID用於生成已驗證消息的金鑰。(有關SNMPv3的詳細資訊，請參閱RFC 2571-2575。)

許多SNMP產品在SNMPv3下基本保持不變，但因以下新功能而得到增強：

安全性

- 驗證
- 隱私權

管理

- 授權與存取控制

- 邏輯前後關聯
- 實體、辨識及資訊的命名
- 人員和策略
- 使用者名稱和金鑰管理
- 通知目標和代理關係
- 透過SNMP操作進行遠端配置

SNMPv3安全模型主要有兩種形式，即身份驗證和加密。

身份驗證用於確保僅預期收件人讀取陷阱。建立消息時，會根據實體EngineID為其指定一個特殊金鑰。金鑰與預定收件人共用，用於接收郵件。
加密、隱私對SNMP消息的負載進行加密，以確保未經授權的使用者無法讀取該消息。任何被截獲的陷阱中填充有亂碼，並且無法讀取。在必須透過Internet路由SNMP消息的應用中，隱私尤其有用。
SNMP組中有三個安全級別：

noAuthnoPriv -無身份驗證和隱私的通訊。
authNoPriv -使用身份驗證且無隱私權的通訊。用於身份驗證的協定有消息摘要演算法5 (MD5)和安全雜湊演算法(SHA)。
authPriv -使用身份驗證和隱私進行通訊。用於身份驗證的協定是MD5和SHA，對於隱私，可以使用資料加密標準(DES)和高級加密標準(AES)協定。

SWA中的SNMP

AsyncOS作業系統透過SNMP支援系統狀態監控。

請注意：

- SNMPisoffdefault。
- 未實現SNMPSET操作（配置）。
- AsyncOS 支援SNMPv1、v2和v3。
- 啟用SNMPv3時，必須執行消息驗證和加密。驗證和加密的密碼必須不同。
- 加密演算法可以是AES（推薦）或DES。
- 驗證演演算法可以是SHA-1 （建議）或MD5。
- Thesnmpconfig命令會在您下次運行該命令時「記住」您的密碼。
- 對於15.0之前的AsyncOS版本，SNMPv3使用者名稱是：v3get。
- 對於AsyncOS版本15.0及更高版本，defaultSNMPv3使用者名稱是：v3get。作為管理員，您可以選擇任何其他使用者名稱。
- 如果使用onlySNMPv1或SNMPv2，則必須設定社群字串。社群字串未預設為public。

- 對於SNMPv1和SNMPv2，您必須指定可接受SNMPGET請求的網路。
- 要使用陷阱，必須運行SNMPmanager（未包含在AsyncOS中），並且必須輸入其IP地址作為陷阱目標。（可以使用主機名，但如果使用，則陷阱僅在DNS正常運行時有效。）

配置SNMPMonitor

要配置SNMP以收集裝置的系統狀態資訊，請在CLI中使用thesnmpconfig命令。選擇並配置介面值後，裝置將響應SNMPv3 GET請求。

使用SNMP時，請注意以下幾點：

- 在SNMP版本3中，請求必須包含匹配的密碼。
- 預設情況下，第1版和第2版請求被拒絕。
- 如果啟用，版本1和版本2請求必須具有匹配的社群字串。

```
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檔案

MIB檔案位於URL：https://www.cisco.com/c/en/us/support/security/web-security-appliance/series.html

使用每個MIB檔案的最新版本。

有多個MIB檔案：

- asyncoswebsecurityappliance-mib.txt是用於Secure Web裝置的企業MIB的SNMPv2相容描述。
- ASYNCOS-MAIL-MIB.txt是郵件安全裝置的企業MIB的SNMPv2相容說明。
- IRONPORT-SMI.txt此「管理資訊結構」檔案定義asyncoswebsecurityappliance-mib的角色。

此版本實現了MIB-II的只讀子集，如RFC 1213和1907中所定義。

Seehttps://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118415-technote-wsa-00.htmlto瞭解更多有關使用SNMP監視裝置上的CPU使用情況的信息。

SWA SNMP陷阱

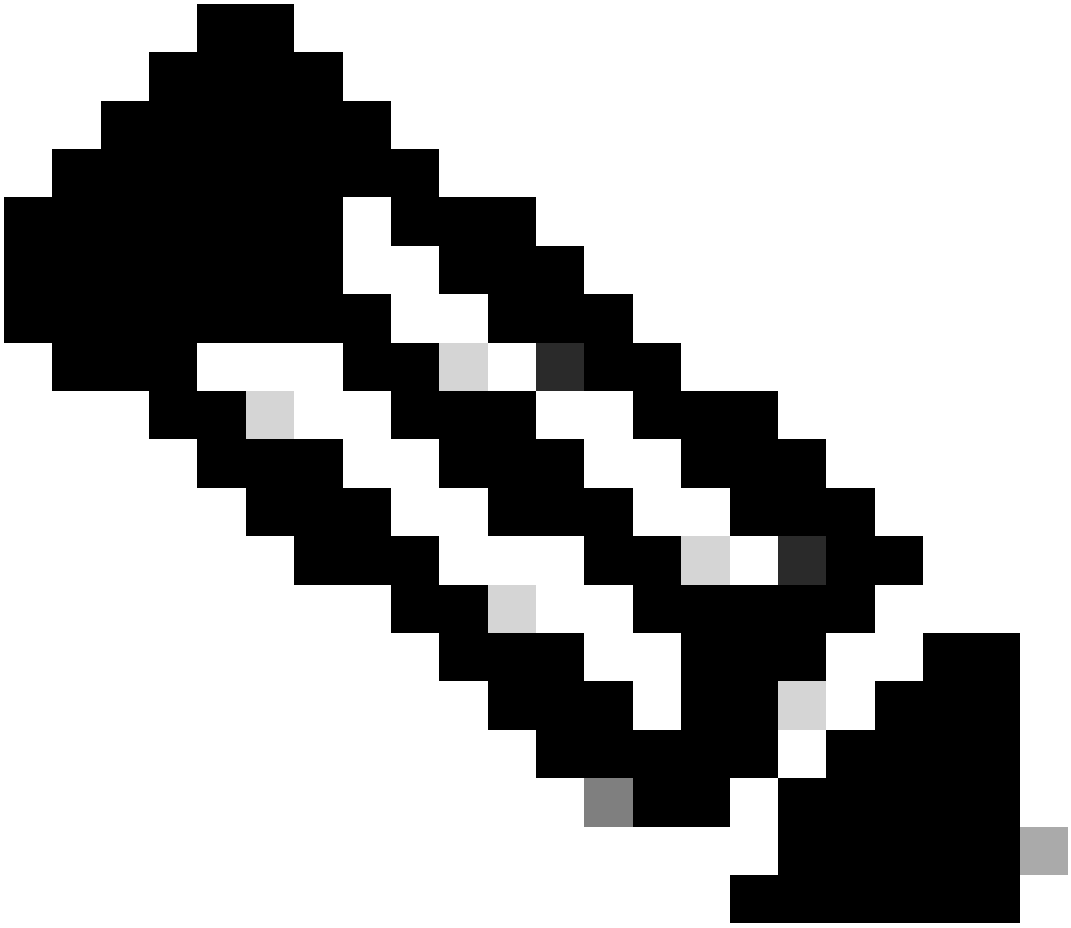
SNMP提供傳送設陷或通知的功能，可在符合一或多個條件時，通知管理應用程式。

陷阱是包含與傳送陷阱的系統元件相關的資料的網路資料包。

當滿足SNMPagent上的條件(在本例中為CiscoSecure Web裝置)時，生成陷阱。

滿足條件後，SNMPagent會形成一個SNMPpacket並將其傳送到運行SNMPmanagement console軟體的主機。

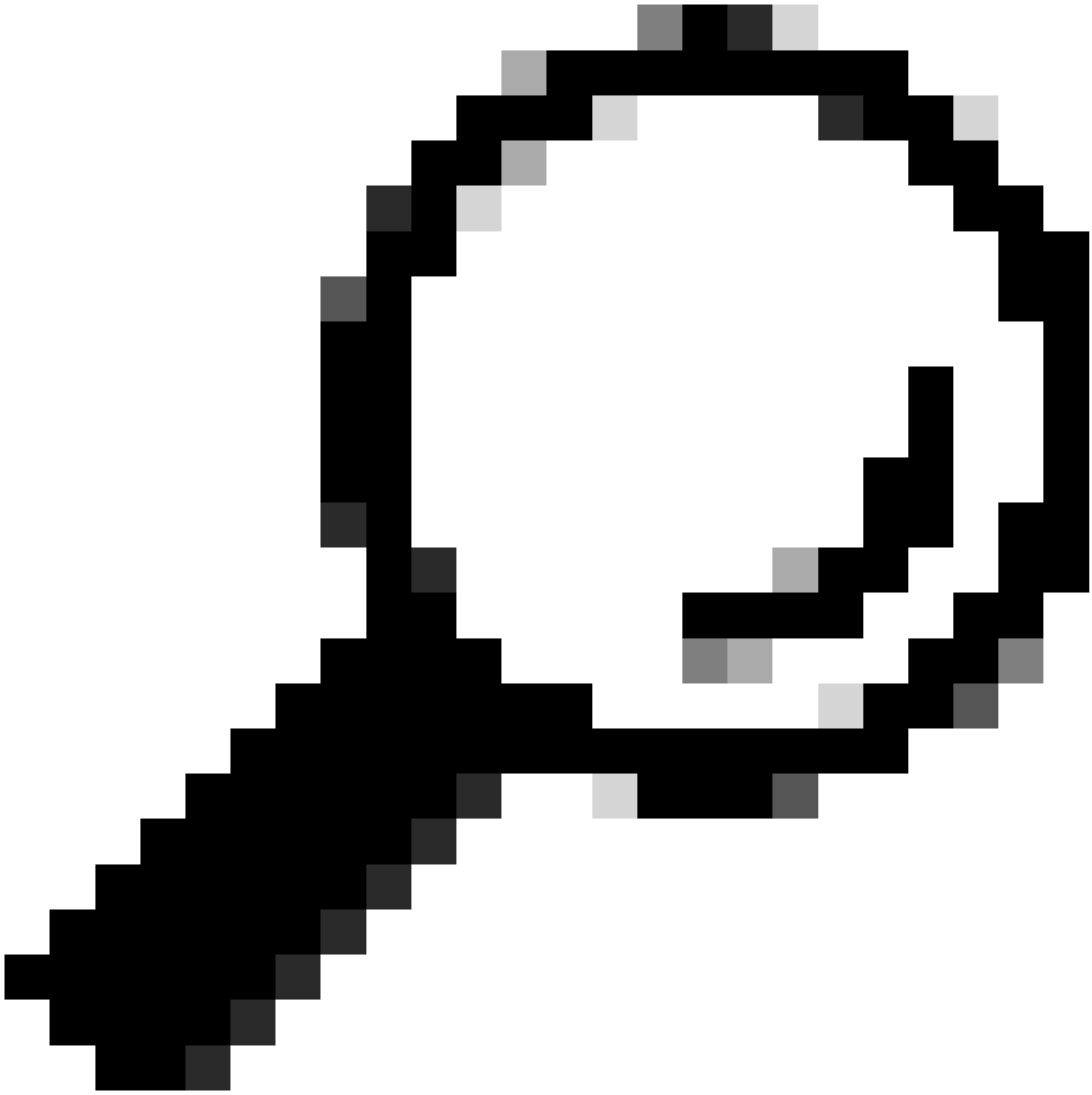
為介面啟用SNMP時，可以配置SNMPtraps(啟用或停用特定陷阱)。



注意：要指定多個陷阱目標：提示輸入陷阱目標時，最多可輸入10個逗號分隔的IP地址。

connectivityFailure 陷阱可用於監控裝置與Internet的連線。它透過嘗試連線並每5到7秒向單個外部伺服器傳送HTTP GET請求來完成此操作。預設情況下，埠80上的受監控URL是downloads.ironport.com。

要更改監控的URL或埠，請運行snmpconfig命令並啟用connectivityFailure陷阱（即使已啟用）。您會看到變更URL的提示。



提示：要模擬connectivityFailure 陷阱，可以使用dnsconfig CLI命令輸入不工作的DNS伺服器。對downloads.ironport.com的查詢失敗，並且每5-7秒傳送一次陷阱。請確保在測試結束後將DNS伺服器更改回工作伺服器。

建議的監視OID

這是建議監控的MIB清單，而不是詳盡的清單：

硬體OID	名稱
1.3.6.1.4.1.15497.1.1.1.18.1.3	raidID
1.3.6.1.4.1.15497.1.1.1.18.1.2	raidStatus
1.3.6.1.4.1.15497.1.1.1.18.1.4	raidLastError

1.3.6.1.4.1.15497.1.1.1.10	fanTable
1.3.6.1.4.1.15497.1.1.1.9.1.2	攝氏度

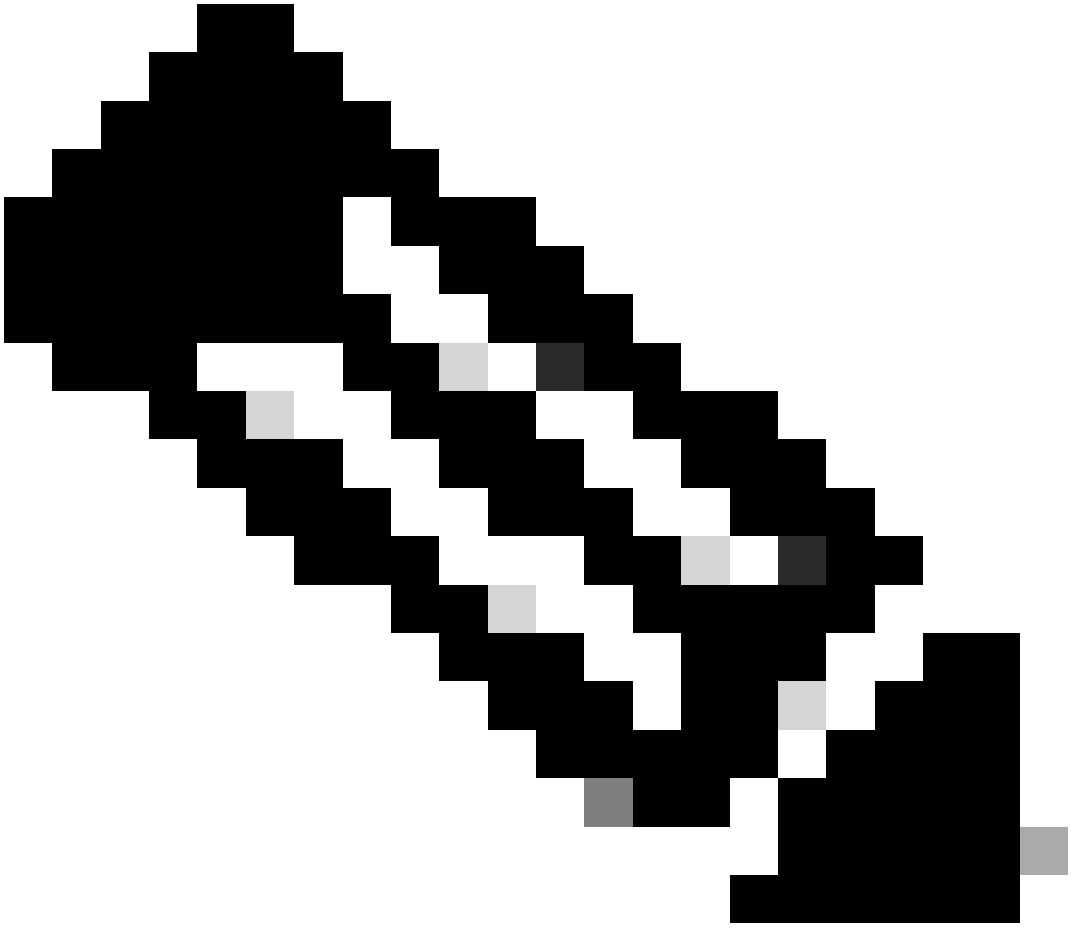
下面是OID直接對映到status detailCLI命令的輸出：

OID	名稱	狀態詳細資訊欄位
系統資源		
1.3.6.1.4.1.15497.1.1.1.2.0	百分比	CPU
1.3.6.1.4.1.15497.1.1.1.1.0	百分比記憶體利用率	RAM
每秒交易數		
1.3.6.1.4.1.15497.1.2.3.7.1.1.0	cacheThruNow	最後一分鐘內的平均每秒交易數。
1.3.6.1.4.1.15497.1.2.3.7.1.2.0	cacheThru1hrPeak	過去一小時內每秒交易數目上限。
1.3.6.1.4.1.15497.1.2.3.7.1.3.0	cacheThru1hrMean	過去一小時內每秒的平均作業事件。
1.3.6.1.4.1.15497.1.2.3.7.1.8.0	cacheThruLifePeak	代理重新啟動後每秒的最大事務數。
1.3.6.1.4.1.15497.1.2.3.7.1.9.0	cacheThruLifeMean	代理重新啟動後每秒的平均事務數。
頻寬		
1.3.6.1.4.1.15497.1.2.3.7.4.1.0	cacheBwidthTotalnow	過去一分鐘內的平均頻寬。
1.3.6.1.4.1.15497.1.2.3.7.4.2.0	cacheBwidthTotal1hrPeak	過去一小時內的最大頻寬。
1.3.6.1.4.1.15497.1.2.3.7.4.3.0	cacheBwidthTotal1hrMean	過去一小時的平均頻寬。
1.3.6.1.4.1.15497.1.2.3.7.4.8.0	cacheBwidthTotalLifePeak	代理重新啟動後的最大頻寬。
1.3.6.1.4.1.15497.1.2.3.7.4.9.0	cacheBwidthTotalLifeMean	代理重新啟動後的平均頻寬。
回應時間		
1.3.6.1.4.1.15497.1.2.3.7.9.1.0	快取命中	過去一分鐘內的平均快取命中率。
1.3.6.1.4.1.15497.1.2.3.7.9.2.0	cacheHits1hrPeak	過去一小時內快取命中率上限。
1.3.6.1.4.1.15497.1.2.3.7.9.3.0	cacheHits1hrMean	過去一小時的平均快取命中率。
1.3.6.1.4.1.15497.1.2.3.7.9.8.0	cacheHitsLifePeak	代理重新啟動後的最大快取命中率。

1.3.6.1.4.1.15497.1.2.3.7.9.9.0	cacheHitsLifeMean	代理重新啟動後的平均快取記憶體命中率。
快取命中率		
1.3.6.1.4.1.15497.1.2.3.7.5.1.0	快取命中	過去一分鐘內的平均快取命中率。
1.3.6.1.4.1.15497.1.2.3.7.5.2.0	cacheHits1hrPeak	過去一小時內快取命中率上限。
1.3.6.1.4.1.15497.1.2.3.7.5.3.0	cacheHits1hrMean	過去一小時的平均快取命中率。
1.3.6.1.4.1.15497.1.2.3.7.5.8.0	cacheHitsLifePeak	代理重新啟動後的最大快取命中率。
1.3.6.1.4.1.15497.1.2.3.7.5.9.0	cacheHitsLifeMean	代理重新啟動後的平均快取記憶體命中率。
連線		
1.3.6.1.4.1.15497.1.2.3.2.7.0	cacheClientIdleConns	空閒客戶端連線。
1.3.6.1.4.1.15497.1.2.3.3.7.0	cacheServerIdleConns	空閒伺服器連線。
1.3.6.1.4.1.15497.1.2.3.2.8.0	cacheClientTotalConns	使用者端連線總數。
1.3.6.1.4.1.15497.1.2.3.3.8.0	cacheServerTotalConns	伺服器連線總數。

排除SNMP故障

要檢視SWA與SNMP管理器之間的連線，最好捕獲資料包，您可以將資料包捕獲過濾器放置在（埠161或埠162）



注意：此過濾器是由預設SNMP埠導致的，如果您已更改埠，請將配置的埠號放入資料包捕獲過濾器中。

從SWA捕獲資料包的步驟：

步驟1.登入GUI

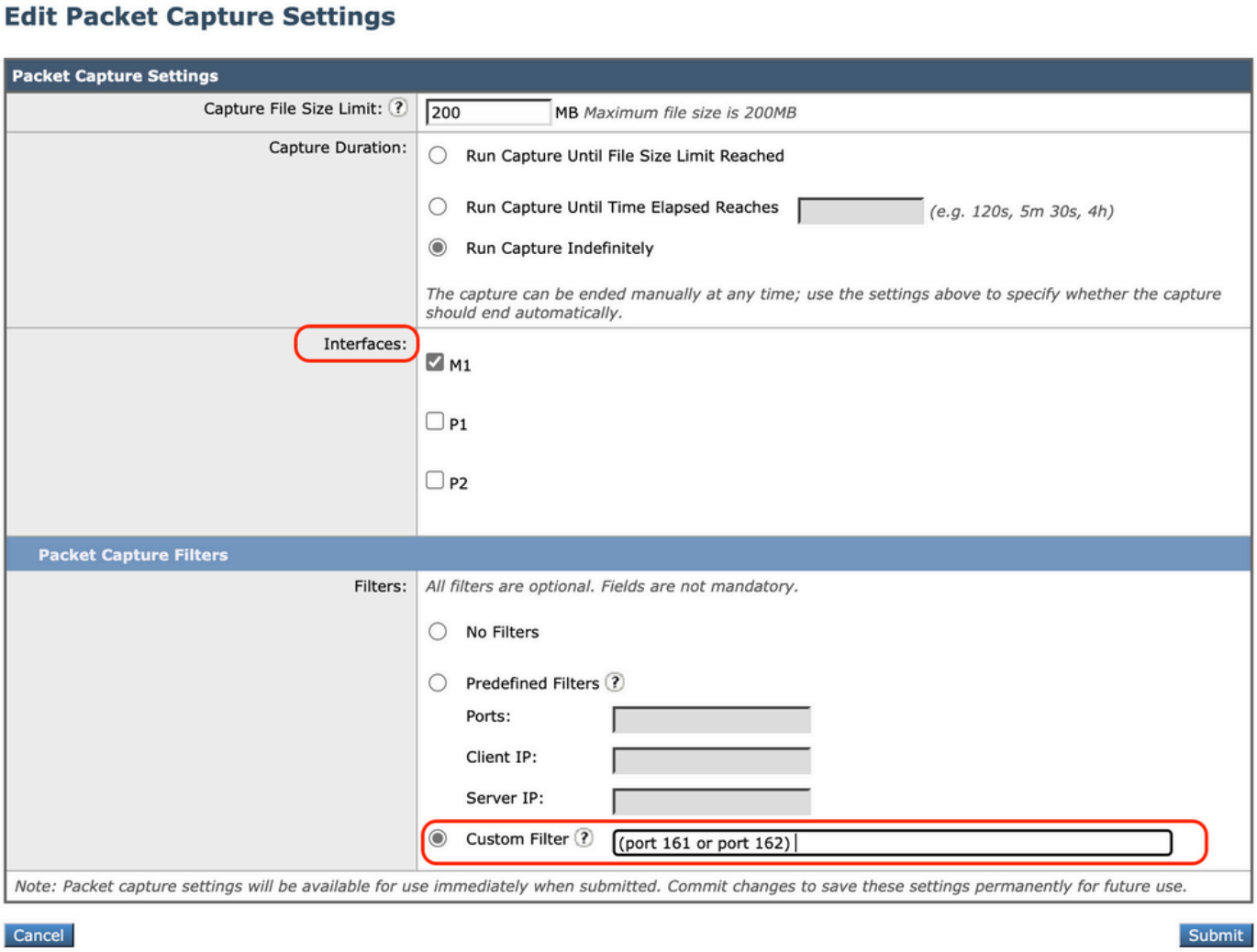
步驟2.在右上角選擇「Support and Help（支援和幫助）」

步驟3.選擇資料包捕獲

步驟4.選擇編輯設定

步驟 5.確保選擇了正確的介面

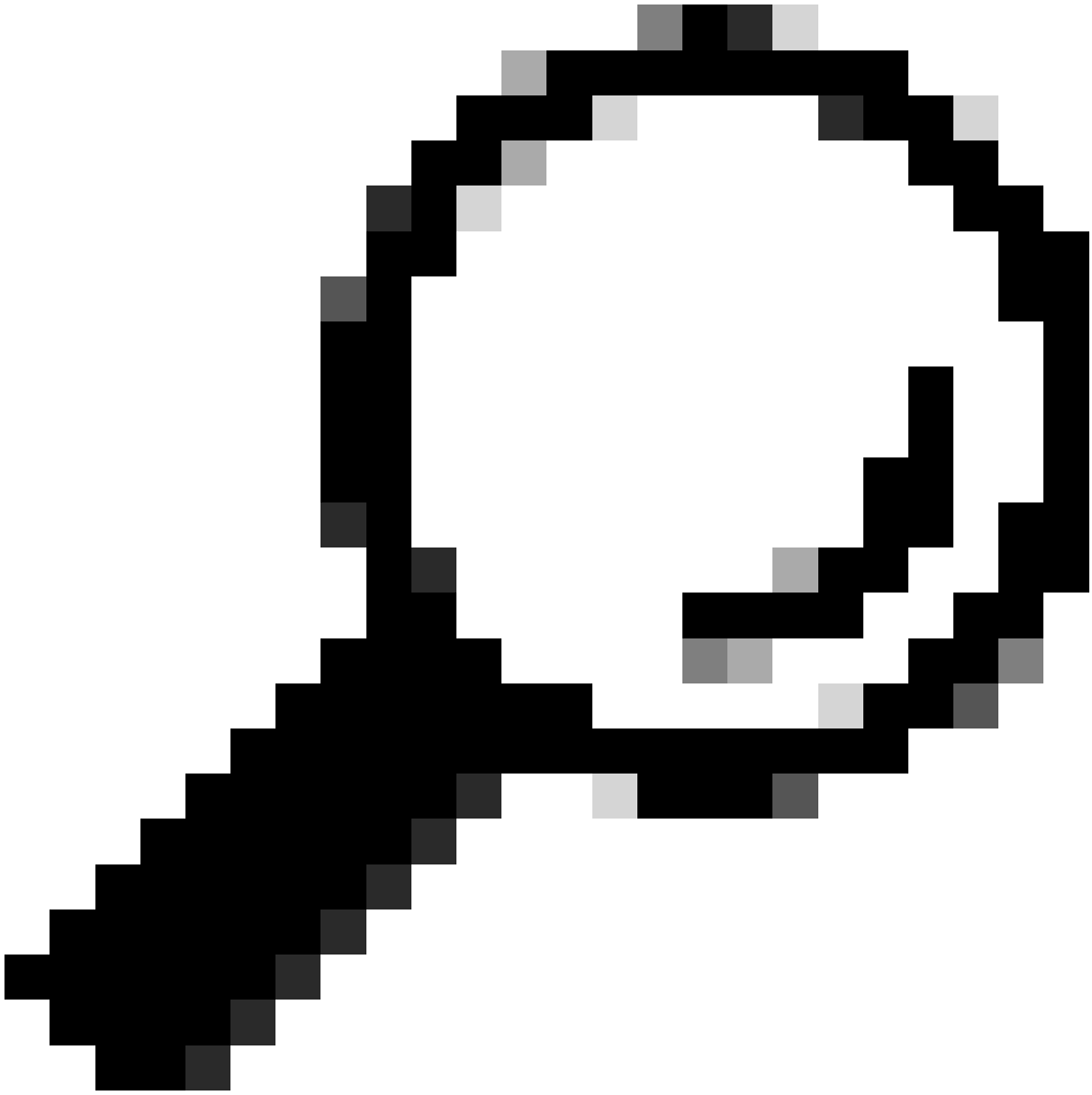
步驟 6.輸入篩選條件。



映像-配置資料包捕獲過濾器

步驟 7.選擇提交

步驟 8. 選擇開始捕獲。



提示：您可以使用Wireshark解密SNMPv3資料包捕獲。有關詳細資訊，請訪問此連結：How-to-decrypt-snmpv3-packets-using-wireshark

SNMPWALK

snmpwalk是自動運行多個GET-NEXT請求的SNMP應用程式的名稱。SNMP GET-NEXT請求用於查詢已啟用的裝置並從裝置獲取SNMP資料。之所以使用snmpwalk命令，是因為它允許使用者將GET-NEXT請求連結在一起，而無需為子樹中的每個OID或節點輸入唯一的命令

在Windows作業系統上安裝SNMPWALK

對於Microsoft Windows使用者，您首先需要下載該工具。

在Linux核心上安裝SNMPWALK

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

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

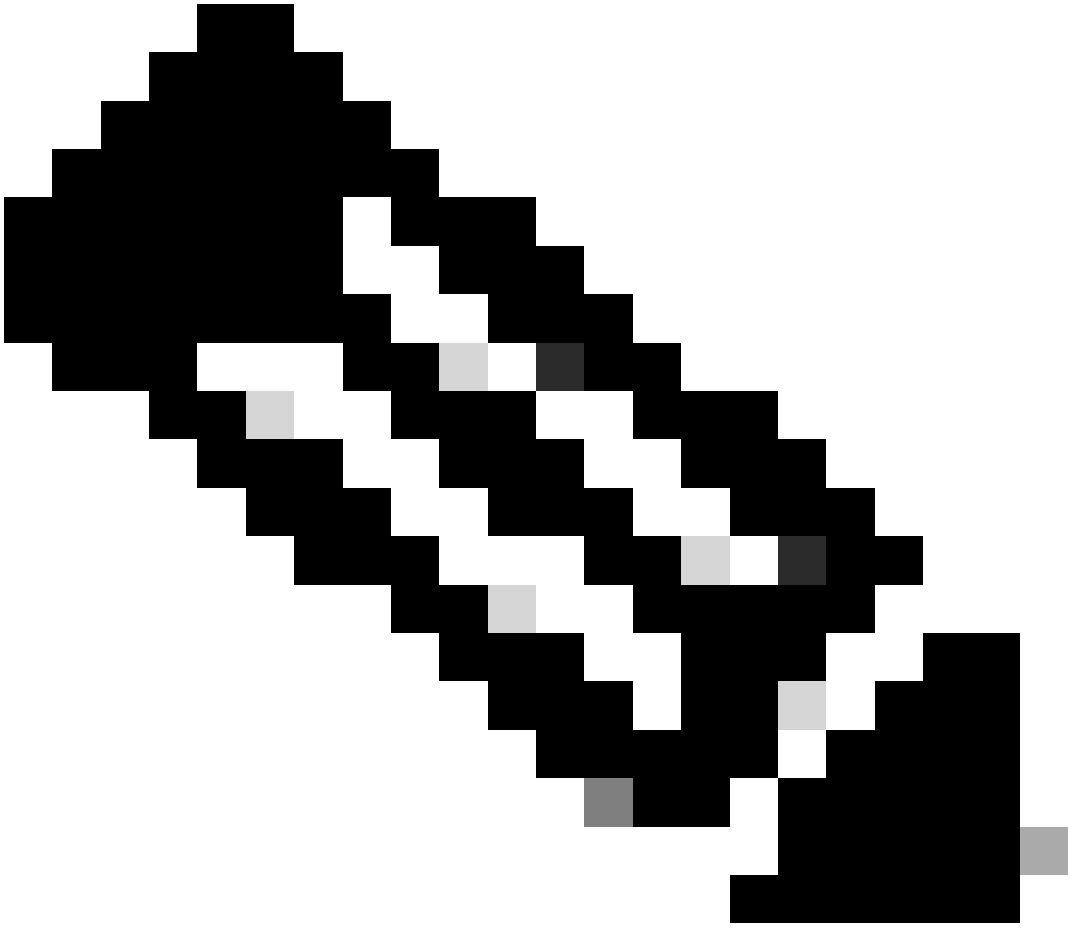
在MacOS上安裝SNMPWALK

預設情況下，snmpwalk安裝在MacOS上

要生成SNMP GET請求，您可以從網路中連線到SWA的另一台電腦使用snmpwalk命令，以下是snmpwalk命令的一些示例：

```
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>
```



註：您可以根據您的SWA配置，選擇將安全級別設定為noAuthNoPriv、authNoPriv或authPriv。

SNMPTRAP

snmptrap是隱藏的CLI命令，需要在SWA上啟用SNMP。您可以透過選擇對象和陷阱來生成SNMP陷阱，以下是一個示例：

```
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
```

SWA中的SNMP日誌

SWA有兩個與SNMP相關的日誌，某些與Web代理元件相關的日誌型別未啟用。您可以從以下位置啟用它們：

- 在GUI中：System Administration > Log subscriptions
- 在CLI中：logconfig > new

記錄檔型別	說明	是否支援Syslog推送？	預設情況下是否啟用？
SNMP日誌	記錄與SNMP網路管理引擎相關的調試消息。	是	是
SNMP模組日誌	記錄與SNMP監控系統互動相關的Web Proxy消息。	否	否

SNMP的常見問題

有些OID失敗（無值或值錯誤）。

此問題與SNMP提取有關。以下是預期輸出和錯誤輸出的兩個示例：

```
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
```

您可以在snmp_logs中檢查「應用程式故障」

您可以透過CLI > grep >選擇與snmp_logs關聯的數字，來檢查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]>
```

參考

[Cisco Secure Web Appliance的AsyncOS 15.0使用手冊- LD（有限部署）-故障排除[Cisco Secure Web Appliance] -思科]

[使用SNMP計算WSA上的代理CPU利用率- Cisco]

snmpcmd(1) (freebsd)

snmptrap (freebsd)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。