在SWA中配置SNMP并对其进行故障排除

目录

简介

本文档介绍对安全Web设备(SWA)中的简单网络监控协议(SNMP)进行故障排除的步骤。

先决条件

要求

建议掌握下列主题的相关知识：

- 访问SWA的命令行界面(CLI)。
- 对SWA的管理权限。
- SNMP基础知识。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

SNMP如何工作

SNMP是一种应用层通信协议，允许网络设备在这些系统之间以及与网络外部的其他设备交换管理信息。

通过SNMP，网络管理员可以管理网络性能，查找和解决网络问题，以及规划网络增长。

SNMP使网络监控更具成本效益，使您的网络更加可靠。 (有关SNMP的详细信息，请参阅RFC 1065、1066和1067。)

SNMP管理的网络包括管理器、代理和受管设备。

- Manager提供了以人为本的网络管理器和管理系统之间的接口。
- 代理提供管理器和受管设备之间的接口
- 管理系统执行大多数管理过程，并提供用于网络管理的大量内存资源。

位于每个受管设备上的代理将软件陷阱中捕获的本地管理信息数据（例如性能信息或事件和错误信息）转换为管理系统的可读形式。

SNMP代理从管理信息库(MIB)（设备参数和网络数据存储库）或错误或更改陷阱中捕获数据。

MIB

MIB是一种数据结构，它将SNMP网络元素描述为数据对象列表。SNMP管理器必须编译网络中每种设备类型的MIB文件，以监控SNMP设备。

管理器和代理使用MIB和相对较少的命令集交换信息。MIB以树形结构组织，各个变量在分支上表示为枝叶。

长数字标记或对象标识符(OID)用于区分MIB和SNMP消息中的唯一变量。MIB将每个OID与可读标签以及与对象相关的各种其他参数相关联。

然后，MIB用作数据字典或代码簿，用于汇编和解释SNMP消息。

当SNMP管理器希望了解对象的值（例如警报点的状态、系统名称或元素正常运行时间）时，它会组装一个GET数据包，其中包含每个相关对象的OID。

元素接收请求并在代码簿(MIB)中查找每个OID。如果找到OID（对象由元素管理），则会组合并发送包含对象的当前值的响应数据包。

如果未找到OID，则会发送特殊的错误响应来标识非托管对象

SNMP 陷阱

SNMP 陷阱支持代理以未经请求的 SNMP 消息的形式，向管理站发送关于重大事件的通知。

SNMPv1和SNMPv2c，以及相关的MIB，鼓励陷阱定向通知。

如果一个管理器要负责大量的设备，而每台设备都包含大量的对象，要让管理器向每台设备上的每个对象都进行轮询或请求数据是不切实际的。陷阱定向的通知这一想法由此产生。

其解决办法是让受管设备上的每个代理不经请求就向管理器发送通知。它通过发送称为“事件陷阱”的消息来完成此操作。

收到事件后，管理器会显示事件，并可以选择根据事件采取措施。例如，管理器可以直接轮询代理，也可以轮询其他关联的设备代理，以便更好地了解事件。

陷阱定向通知可消除对轻量SNMP请求的需要，从而显著节省网络和代理资源。但是，不可能完全消除SNMP轮询。

网络发现和拓扑更改必须使用 SNMP 请求。另外，如果设备遭遇灾难性断电，受管设备代理将不能发送陷阱。

RFC 1157 中对 SNMPv1 陷阱进行了定义，包括以下字段：

- 企业：标识生成陷阱的受管对象的类型。
- Agent address：提供生成陷阱的受管对象的地址。
- Generic trap type：表示这是若干种常规陷阱类型之一。
- Specific trap code：表示这是若干种特定陷阱类型之一。
- Time stamp：提供从上次网络重新初始化到生成陷阱之间经过的时间。
- Variable bindings：陷阱中包含PDU的数据字段。每个可变绑定都将一个特定 MIB 对象实例与其当前值相关联。

SNMPv3

SNMPv3支持SNMP“引擎ID”标识符，用于唯一标识每个SNMP实体。如果两个SNMP实体具有重复的EngineID，则可能发生冲突。

EngineID用于为经过身份验证的消息生成密钥。(有关SNMPv3的详细信息，请参阅RFC 2571-2575。)

许多SNMP产品在SNMPv3下基本保持不变，但通过以下新功能得到增强：

安全

- 身份验证
- 隐私

管理

- 授权和访问控制
- 逻辑情景
- 实体、身份和信息的命名
- 人员和策略
- 用户名和密钥管理
- 通知目标和代理关系
- 通过SNMP操作进行远程配置

SNMPv3安全模型主要有两种形式：身份验证和加密。

身份验证用于确保仅预期收件人读取陷阱。创建消息时，会根据实体EngineID为其指定一个特殊密钥。密钥与预定收件人共享并用于接收邮件。
加密，隐私对SNMP消息的负载进行加密，以确保未经授权的用户无法读取该消息。任何被截获的、充满错误字符且无法读取的陷阱。在必须通过Internet路由SNMP消息的应用程序中，隐私尤其有用。
SNMP组中有三个安全级别：

noAuthnoPriv -无身份验证和隐私的通信。
authNoPriv -使用身份验证和隐私进行通信。用于身份验证的协议是消息摘要算法5 (MD5)和安全散列算法(SHA)。
authPriv -使用身份验证和隐私进行通信。用于身份验证的协议是MD5和SHA，对于隐私，可以使用数据加密标准(DES)和高级加密标准(AES)协议。

SWA中的SNMP

AsyncOS操作系统通过SNMP支持系统状态监控。

请注意：

- SNMPisoffdefault。
- 未实现SNMPSET操作（配置）。
- AsyncOS支持SNMPv1、v2和v3。
- 启用SNMPv3时，必须执行消息身份验证和加密。身份验证和加密的口令必须不同。
- 加密算法可以是AES（推荐）或DES。
- 身份验证算法可以是SHA-1（推荐）或MD5。
- Thesnmpconfig命令会在您下次运行该命令时“记住”您的密码。
- 对于15.0之前的AsyncOS版本，SNMPv3用户名是：v3get。
- 对于AsyncOS版本15.0及更高版本，默认SNMPv3用户名是：v3get。作为管理员，您可以选择任何其他用户名。
- 如果仅使用SNMPv1或SNMPv2，则必须设置社区字符串。社区字符串未默认为public。

- 对于SNMPv1和SNMPv2，必须指定从其接受SNMPGET请求的网络。
- 要使用陷阱，必须运行SNMPmanager（未包括在AsyncOS中），并且输入其IP地址作为陷阱目标。（您可以使用主机名，但如果这样做，陷阱仅在DNS正常运行时才有效。）

配置SNMPMonitor

要配置SNMP以收集设备的系统状态信息，请在CLI中使用thesnmpconfig命令。在选择并配置接口的值后，设备将对SNMPv3 GET请求做出响应。

使用SNMP时，请考虑以下几点：

- 在SNMP第3版中，请求必须包含匹配的密码。
- 默认情况下，会拒绝第1版和第2版请求。
- 如果启用，版本1和2请求必须具有匹配的社区字符串。

```
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文件

MIB文件可从以下URL获得：https://www.cisco.com/c/en/us/support/security/web-security-appliance/series.html

使用每个MIB文件的最新版本。

有多个MIB文件：

- asyncoswebsecurityappliance-mib.txt是用于安全Web设备的企业MIB的SNMPv2兼容说明。
- ASYNCOS-MAIL-MIB.txt是邮件安全设备的企业MIB的SNMPv2兼容说明。
- IRONPORT-SMI.txt此“管理信息结构”文件定义了asyncoswebsecurityappliance-mib的角色。

此版本实施了RFC 1213和1907中定义的MIB-II只读子集。

Seehttps://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118415-technote-wsa-00.htmlto了解有关使用SNMP监控设备上的CPU使用情况的更多信息。

SWA SNMP陷阱

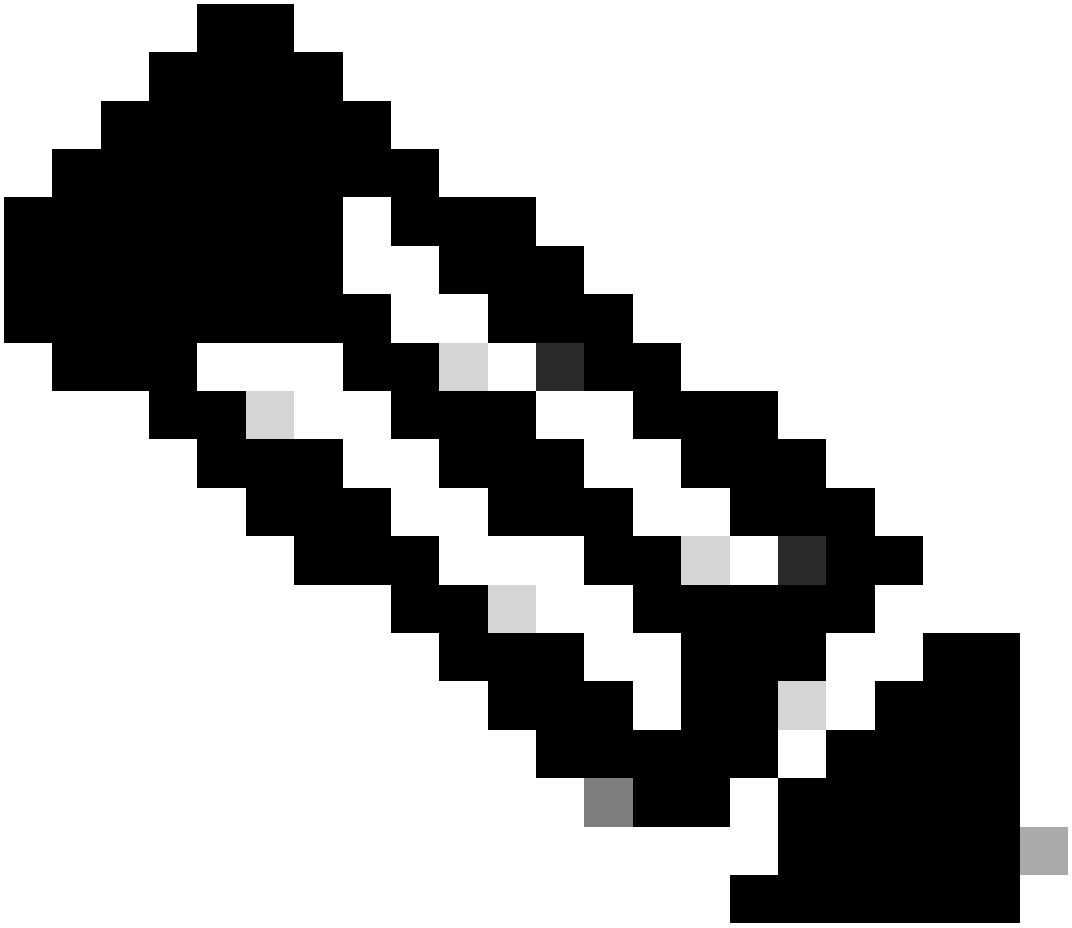
SNMP能够在满足一个或多个条件时发送陷阱或通知，以通知管理应用。

陷阱是包含与发送陷阱的系统组件相关的数据的网络数据包。

在SNMPagent上满足条件时(在本例中为CiscoSecure Web设备)生成陷阱。

满足条件后，SNMPagent会形成一个SNMPpacket并将其发送到运行SNMP管理控制台软件的主机。

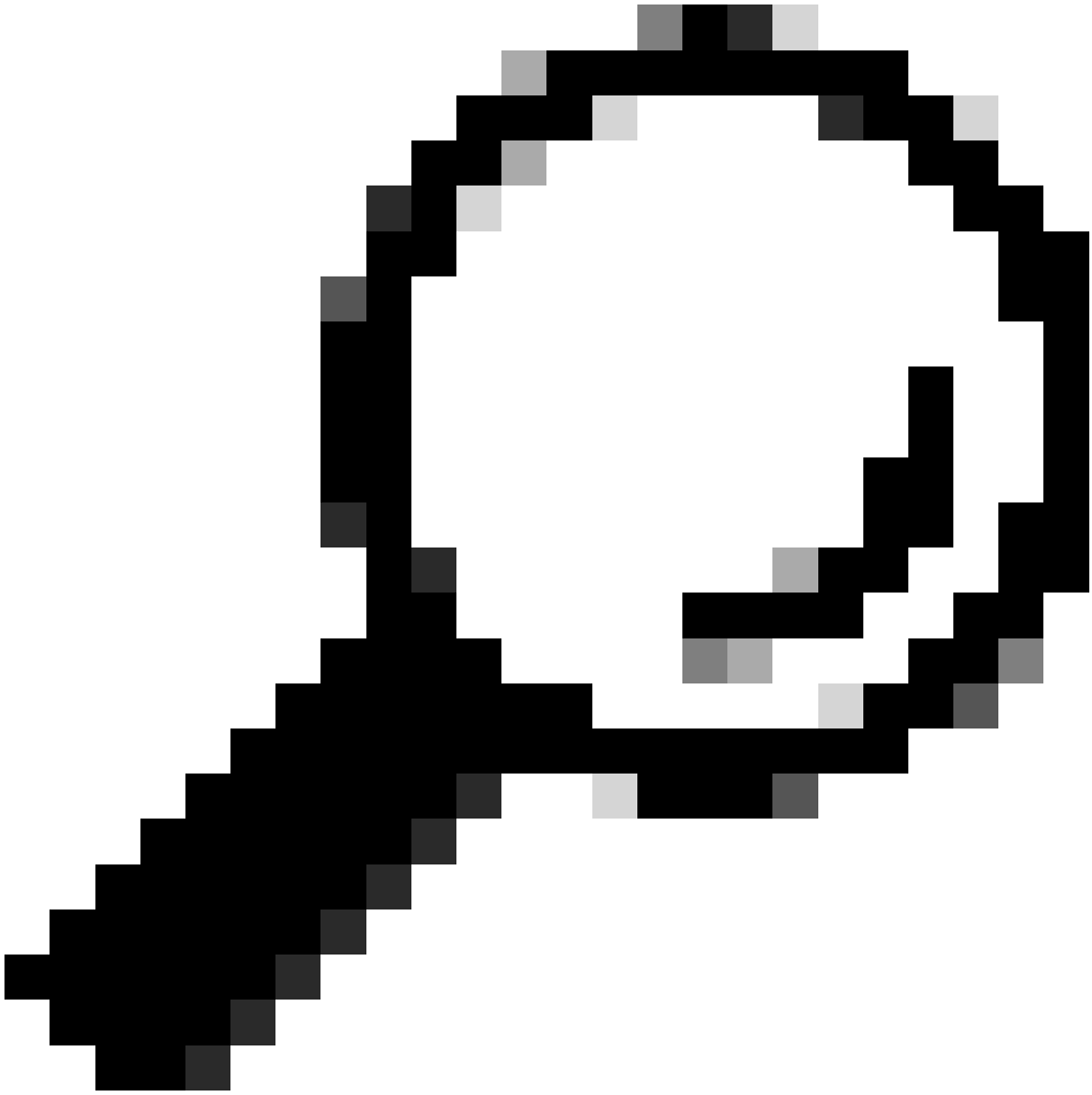
为接口启用SNMP时，可以配置SNMPtraps(启用或禁用特定陷阱)。



注意：要指定多个陷阱目标：当系统提示输入陷阱目标时，最多可以输入10个逗号分隔的IP地址。

connectivityFailure陷阱旨在监控设备与Internet的连接。它通过每5到7秒尝试连接并向单个外部服务器发送HTTP GET请求来完成此操作。默认情况下，受监控的URL为端口80上的downloads.ironport.com。

要更改受监控的URL或端口，请运行snmpconfig命令并启用connectivityFailure陷阱（即使陷阱已启用）。您可以看到更改URL的提示。



提示：要模拟connectivityFailure 陷阱，可以使用dnsconfig CLI命令输入无法正常运行的DNS服务器。查找downloads.ironport.com失败，并且每5-7秒发送一次陷阱。测试结束后，请务必将DNS服务器改回工作服务器。

推荐的监控OID

这是推荐监控的MIB的列表，而不是详尽的列表：

硬件OID	名称
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	摄氏度

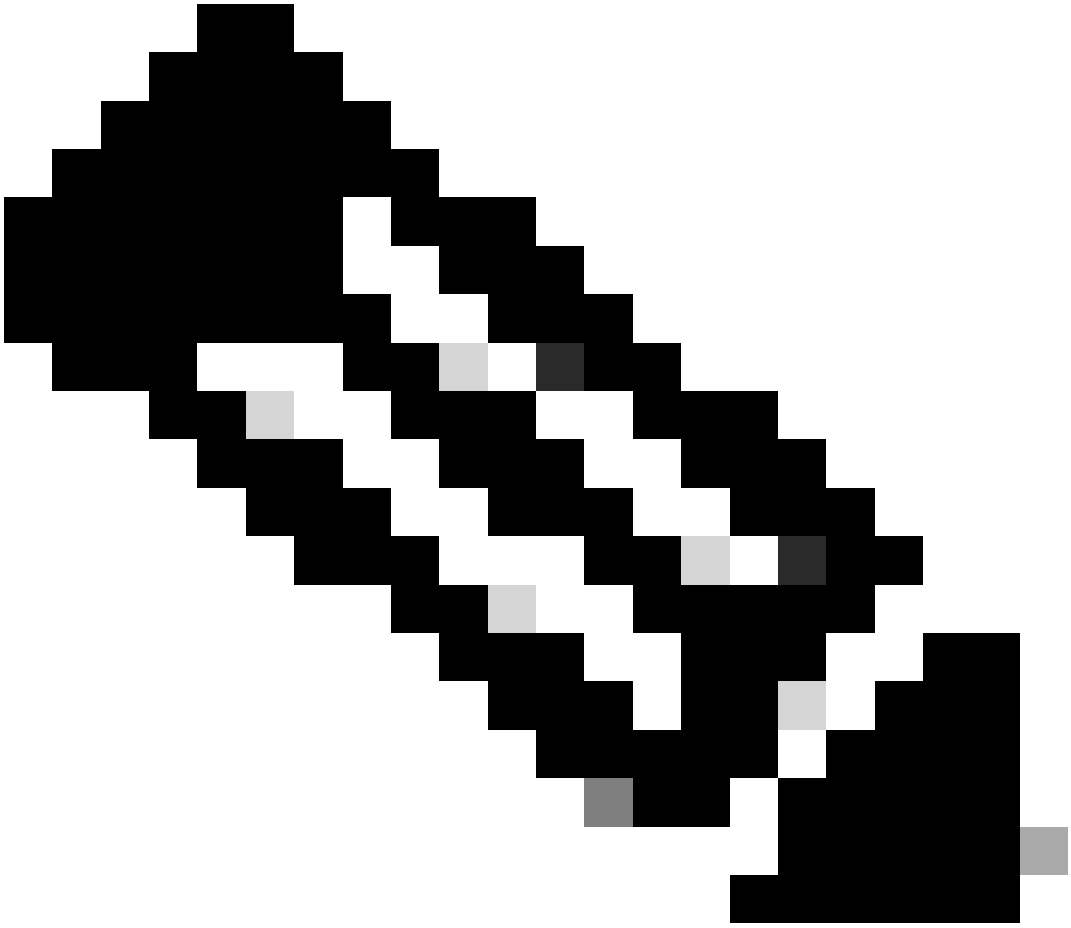
这是OID直接映射到status detailCLI命令的输出：

OID	名称	状态详细信息字段
系统资源		
1.3.6.1.4.1.15497.1.1.1.2.0	百分比CPUutilization	CPU
1.3.6.1.4.1.15497.1.1.1.1.0	percentMemoryUtilization	RAM
每秒事务数		
1.3.6.1.4.1.15497.1.2.3.7.1.1.0	cacheThruNow	过去一分钟内每秒的平均事务数。
1.3.6.1.4.1.15497.1.2.3.7.1.2.0	cacheThruput1hrPeak	过去一小时内每秒的最大事务数。
1.3.6.1.4.1.15497.1.2.3.7.1.3.0	cacheThruput1hrMean	过去一小时内每秒的平均事务数。
1.3.6.1.4.1.15497.1.2.3.7.1.8.0	cacheThruputLifePeak	自代理重新启动以来每秒的最大事务数。
1.3.6.1.4.1.15497.1.2.3.7.1.9.0	cacheThruputLifeMean	自代理重新启动以来的平均每秒事务数。
带宽		
1.3.6.1.4.1.15497.1.2.3.7.4.1.0	cacheBwidthTotalNow	过去一分钟内的平均带宽。
1.3.6.1.4.1.15497.1.2.3.7.4.2.0	cacheBwidthTotal1hrPeak	过去一小时内的最大带宽。
1.3.6.1.4.1.15497.1.2.3.7.4.3.0	cacheBwidthTotal1hrMean	过去一小时内的平均带宽。
1.3.6.1.4.1.15497.1.2.3.7.4.8.0	cacheBwidthTotalLifePeak	自代理重新启动以来的最大带宽。
1.3.6.1.4.1.15497.1.2.3.7.4.9.0	cacheBwidthTotalLifeMean	自代理重新启动以来的平均带宽。
响应时间		
1.3.6.1.4.1.15497.1.2.3.7.9.1.0	cacheHitsNow	过去一分钟内的平均缓存命中率。
1.3.6.1.4.1.15497.1.2.3.7.9.2.0	cacheHits1hrPeak	过去一小时内的最大缓存命中率。
1.3.6.1.4.1.15497.1.2.3.7.9.3.0	cacheHits1hrMean	过去一小时内的平均高速缓存命中率。

1.3.6.1.4.1.15497.1.2.3.7.9.8.0	cacheHitsLifePeak	自代理重新启动以来的最大缓存命中率。
1.3.6.1.4.1.15497.1.2.3.7.9.9.0	cacheHitsLifeMean	自代理重新启动以来的平均缓存命中率。
缓存命中率		
1.3.6.1.4.1.15497.1.2.3.7.5.1.0	cacheHitsNow	过去一分钟内的平均缓存命中率。
1.3.6.1.4.1.15497.1.2.3.7.5.2.0	cacheHits1hrPeak	过去一小时内的最大缓存命中率。
1.3.6.1.4.1.15497.1.2.3.7.5.3.0	cacheHits1hrMean	过去一小时内的平均高速缓存命中率。
1.3.6.1.4.1.15497.1.2.3.7.5.8.0	cacheHitsLifePeak	自代理重新启动以来的最大缓存命中率。
1.3.6.1.4.1.15497.1.2.3.7.5.9.0	cacheHitsLifeMean	自代理重新启动以来的平均缓存命中率。
连接		
1.3.6.1.4.1.15497.1.2.3.2.7.0	cacheClientIdleConns	空闲客户端连接。
1.3.6.1.4.1.15497.1.2.3.3.7.0	cacheServerIdleConns	空闲服务器连接。
1.3.6.1.4.1.15497.1.2.3.2.8.0	cacheClientTotalConns	客户端连接总数。
1.3.6.1.4.1.15497.1.2.3.3.8.0	cacheServerTotalConns	服务器连接总数。

排除SNMP故障

要查看SWA与SNMP管理器之间的连接，最好捕获数据包，您可以将数据包捕获过滤器设置为：（端口161或端口162）



注意：此过滤器是由默认SNMP端口导致的，如果您更改了端口，请将配置的端口号放入数据包捕获过滤器中。

从SWA捕获数据包的步骤：

步骤1.登录到GUI

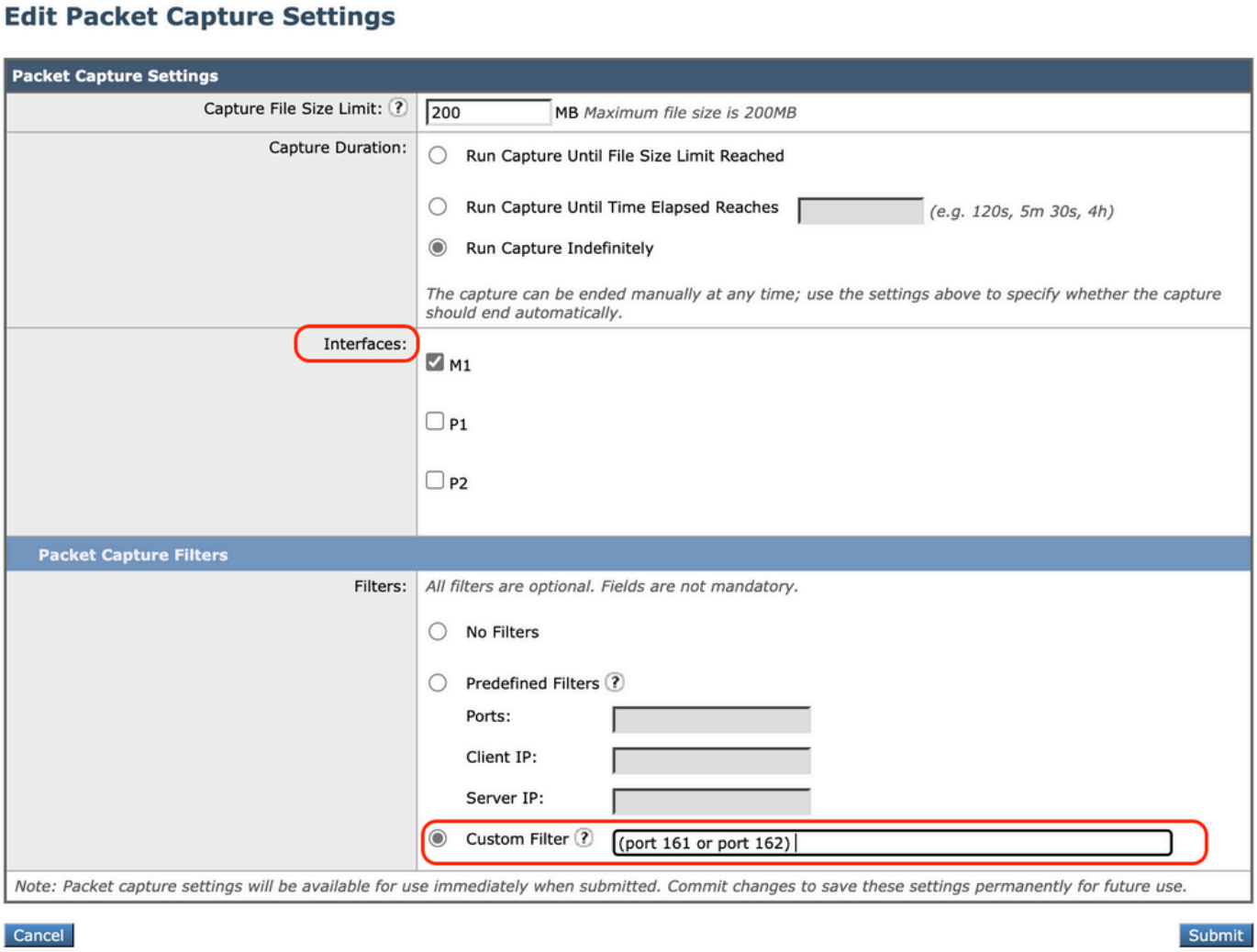
第2步：在右上方选择支持和帮助

第3步：选择数据包捕获

第4步：选择编辑设置

第五步：确保选择了正确的接口

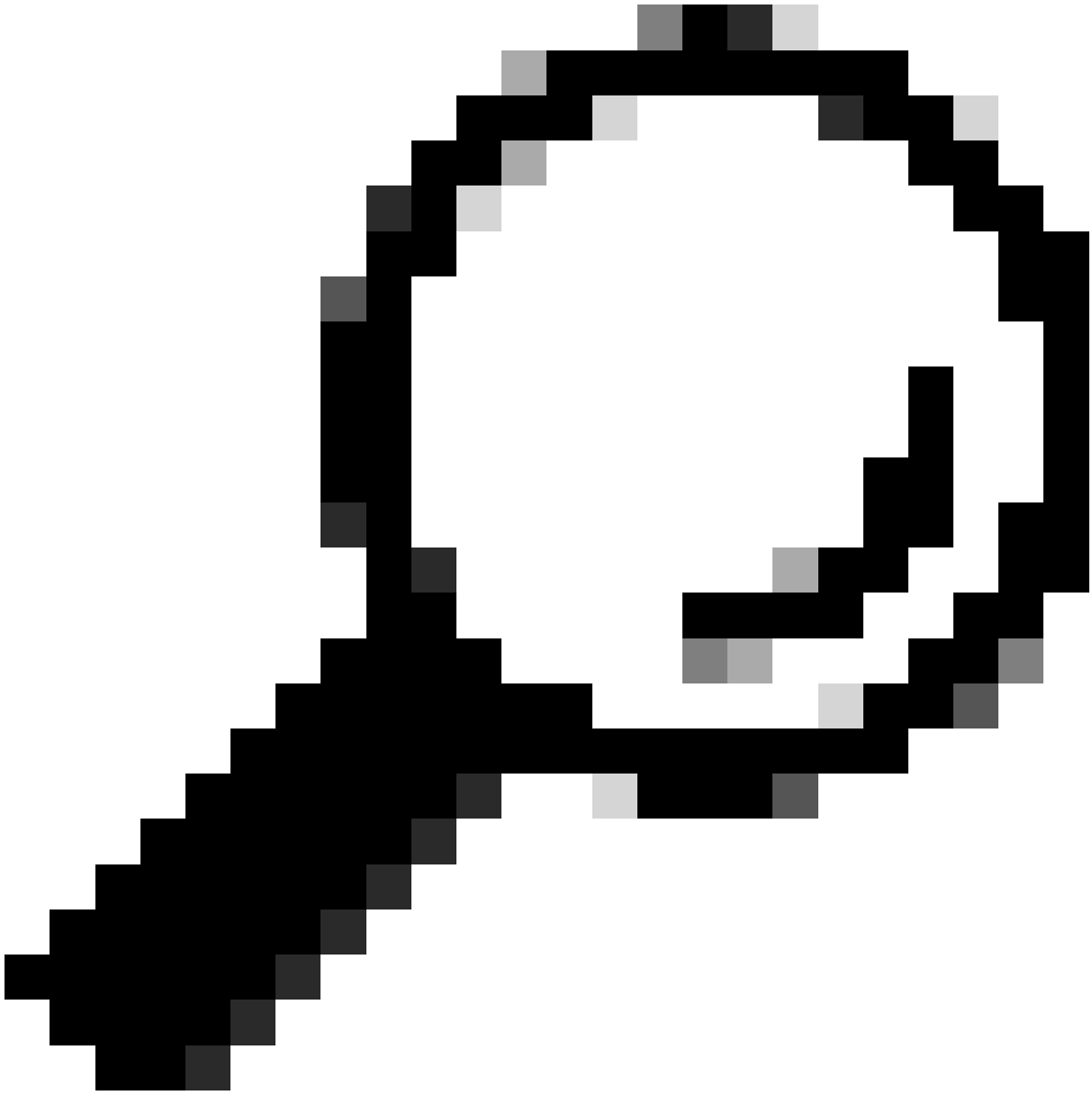
第六步：输入过滤条件。



映像-配置数据包捕获过滤器

步骤 7.选择提交

步骤 8 选择Start Capture。



提示：您可以使用Wireshark解密SNMPv3数据包捕获。有关详细信息，请访问此链接：How-to-decrypt-snmpv3-packets-using-wireshark

---

SNMPWALK

snmpwalk是自动运行多个GET-NEXT请求的SNMP应用程序的名称。SNMP GET-NEXT请求用于查询已启用的设备并从设备获取SNMP数据。之所以使用snmpwalk命令，是因为它允许用户将GET-NEXT请求链接在一起，而无需为子树中的每个OID或节点输入唯一的命令

在Windows操作系统上安装SNMPWALK

对于Microsoft Windows用户，您首先需要下载该工具。

在Linux内核上安装SNMPWALK

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

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

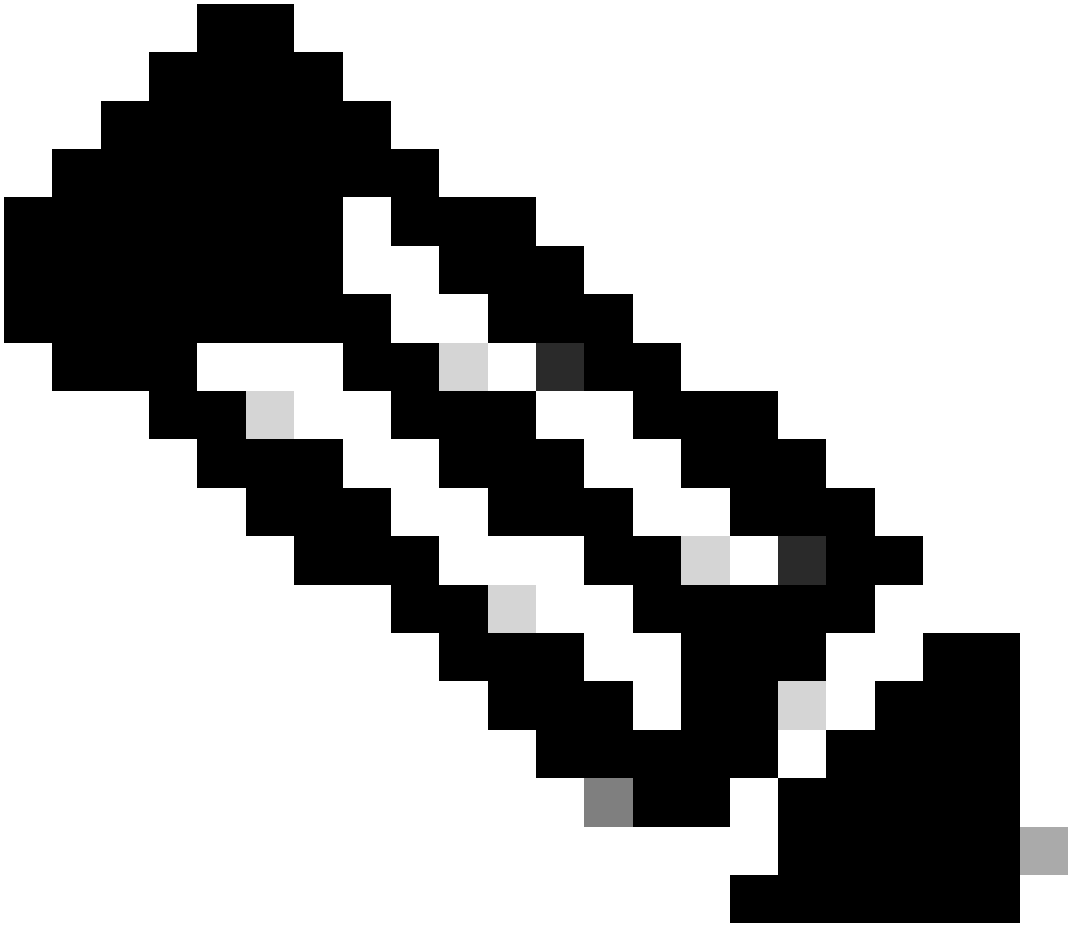
在MacOS上安装SNMPWALK

默认情况下，snmpwalk安装在MacOS上

要生成SNMP GET请求，您可以从网络中与SWA连接的另一台计算机使用snmpwalk命令，下面是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>
```



注：您可以根据您的SWA配置，选择将安全级别设置为noAuthNoPriv、authNoPriv或authPriv。

SNMPTRAP

snmptrap是隐藏的CLI命令，需要在SWA上启用SNMP。您可以通过选择对象和陷阱来生成SNMP陷阱，以下是一个示例：

```
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日志

SWA具有两个与SNMP相关的日志，某些与Web代理组件相关的日志类型未启用。您可以从以下位置启用它们：

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

日志文件类型	描述	是否支持系统日志推送？	默认情况下是否启用？
SNMP日志	记录与SNMP网络管理引擎相关的调试消息。	Yes	Yes
SNMP模块日志	记录与与SNMP监控系统交互相关的Web代理消息。	无	无

SNMP的常见问题

某些OID失败（无值或值错误）。

此问题与SNMP提取有关。以下是预期输出和错误输出的两个示例：

```
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中检查“应用故障”

您可以从CLI > grep >选择与snmp_logs相关的编号来检查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]>
```

参考

[思科安全网络设备AsyncOS 15.0用户指南- LD（有限部署）-故障排除[思科安全网络设备] -思科

[使用SNMP计算WSA上的代理CPU利用率- Cisco

snmpcmd(1) (freebsd)

snmptrap (freebsd)

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。