SWAでのSNMPの設定およびトラブルシューティング

内容

はじめに

このドキュメントでは、Secure Web Appliance(SWA)のSimple Network Monitoring Protocol(SNMP)をトラブルシューティングする手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- SWAのコマンドラインインターフェイス(CLI)へのアクセス
- SWAへの管理アクセス。

- SNMPに関する基礎知識

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

SNMPの仕組み

SNMPはアプリケーション層の通信プロトコルであり、ネットワークデバイスはこれらのシステム間で、およびネットワーク外の他のデバイスと管理情報を交換できます。

ネットワーク管理者は、SNMPを使用して、ネットワークのパフォーマンスを管理し、ネットワークの問題を検出して解決し、ネットワークの拡張を計画できます。

SNMPは、ネットワークモニタリングのコスト効果を高め、ネットワークの信頼性を高めます。(SNMPの詳細については、RFC 1065、1066、および1067を参照してください)。

SNMPによって管理されるネットワークは、マネージャ、エージェント、および管理対象デバイスで構成されます。

- マネージャは、ヒューマンネットワークマネージャと管理システム間のインターフェイスを提供します。
- エージェントは、マネージャと管理対象デバイス間のインターフェイスを提供します
- 管理システムは、管理プロセスのほとんどを実行し、ネットワーク管理に使用される大量のメモリリソースを提供します。

エージェントは、管理対象の各デバイスに常駐し、ソフトウェア· トラップで捕捉されたローカルの管理情報データ（パフォーマンス情報やイベントおよびエラー情報など）を、管理システムで読み取り可能な形式に変換します。

SNMPエージェントは、Management Information Base（MIB；管理情報ベース）（デバイスパラメータおよびネットワークデータリポジトリ）、またはエラーや変更のトラップからデータをキャプチャします。

MIB

MIBは、SNMPネットワーク要素をデータオブジェクトのリストとして記述するデータ構造です。SNMPマネージャは、ネットワーク内の機器タイプごとにMIBファイルをコンパイルして、SNMPデバイスを監視する必要があります。

マネージャとエージェントは、MIBと比較的小さなコマンドセットを使用して情報を交換します。MIBはツリー構造になっており、個々の変数はブランチのリーフとして表されます。

長い数字のタグまたはオブジェクト識別子(OID)は、MIBおよびSNMPメッセージ内の各変数を一意に区別するために使用されます。MIBは、各OIDを読み取り可能なラベルおよびオブジェクトに関連するその他のさまざまなパラメータに関連付けます。

MIBは、SNMPメッセージのアセンブルと解釈に使用されるデータディクショナリまたはコードブックとして機能します。

SNMPマネージャがオブジェクトの値（アラームポイントの状態、システム名、要素の稼働時間など）を知る必要がある場合、対象の各オブジェクトのOIDを含むGETパケットを作成します。

要素は要求を受信し、コードブック(MIB)内の各OIDを検索します。OIDが見つかった場合（オブジェクトは要素によって管理されます）、応答パケットが組み立てられ、オブジェクトの現在の値が含まれた状態で送信されます。

OIDが見つからない場合、管理されていないオブジェクトを識別する特別なエラー応答が送信されます

SNMP トラップ

SNMP トラップを使用すると、エージェントは非送信請求 SNMP メッセージを使用して管理ステーションに重要なイベントを通知できます。

SNMPv1とSNMPv2cは、関連するMIBとともに、トラップによる通知を推奨します。

トラップで指示される通知には、以下の狙いがあります。マネージャが多数のデバイスを管理する必要があり、各デバイスに多数のオブジェクトがある場合に、すべてのデバイスのすべてのオブジェクトに情報をポーリングまたは要求することは非現実的です。

ソリューションは、送信要求を行わずに、管理対象デバイス上のエージェントごとにマネージャに通知することです。これは、イベントのトラップと呼ばれるメッセージを送信することによって行われます。

イベントの受信後、マネージャはイベントを表示し、イベントに基づくアクションの実行を選択できます。たとえば、マネージャはエージェントを直接ポーリングしたり、他の関連するデバイスエージェントをポーリングしてイベントをより良く理解したりできます。

トラップによる通知を使用すると、不必要なSNMP要求が不要になり、ネットワークとエージェントのリソースを大幅に節約できます。ただし、SNMPポーリングを完全に排除することはできません。

SNMP 要求は、検出とトポロジ変更に必要です。また、管理対象デバイス エージェントは、デバイスに致命的な停止が生じた場合にはトラップを送信できません。

SNMPv1 トラップは RFC 1157 で定義されており、次のフィールドが有効です。

- Enterprise:トラップを生成する管理対象オブジェクトのタイプを識別します。
- Agent address：トラップを生成する管理対象オブジェクトのアドレスを示します。
- Generic trap type:標準トラップタイプの番号の1つを示します。

- Specific trap code:固有のトラップコードの番号の1つを示します。
- Time stamp:最後のネットワーク再初期化からトラップの生成までの経過時間を示します。
- Variable bindings:PDUを含むトラップのデータフィールド。個々の変数バインドでは、特定の MIB オブジェクト インスタンスとその現在の値が関連付けられます。

SNMPv3

SNMPv3は、各SNMPエンティティを一意に識別するSNMP「エンジンID」識別子をサポートします。2つのSNMPエンティティのEngineIDが重複していると、競合が発生する可能性があります。

EngineIDは、認証されたメッセージのキーを生成するために使用されます。(SNMPv3の詳細については、RFC 2571 ~ 2575を参照してください)。

多くのSNMP製品は、SNMPv3でも基本的には同じですが、次の新機能によって強化されています。

セキュリティ

- [Authentication]
- Privacy

管理

- 許可とアクセス制御
- 論理コンテキスト
- エンティティ、ID、および情報のネーミング
- 人とポリシー
- ユーザー名とキー管理
- 通知先とプロキシ関係
- SNMP操作によるリモート設定

SNMPv3セキュリティモデルには、主に認証と暗号化の2つの形式があります。

認証は、目的の受信者だけがトラップを読み取ることを保証するために使用されます。メッセージが作成されると、エンティティEngineIDに基づいて特別なキーが付与されます。このキーは目的の受信者と共有され、メッセージの受信に使用されます。
暗号化、プライバシー:SNMPメッセージのペイロードを暗号化して、不正なユーザが読み取ることができないようにします。傍受されたトラップの中に、不明瞭な文字が含まれていて、読み取ることができません。プライバシーは、SNMPメッセージをインターネット経由でルーティングする必要があるアプリケーションで特に役立ちます。
SNMPグループには、次の3つのセキュリティレベルがあります。

noAuthnoPriv：認証とプライバシーなしの通信。
authNoPriv：認証あり、プライバシーなしの通信。認証に使用されるプロトコルは、メッセージダイジェストアルゴリズム5(MD5)とセキュアハッシュアルゴリズム(SHA)です。
authPriv：認証とプライバシーを使用した通信。認証に使用されるプロトコルはMD5とSHAで、

プライバシーにはData Encryption Standard（DES；データ暗号規格）とAdvanced Encryption Standard（AES；高度暗号化規格）のプロトコルを使用できます。

SWAでのSNMP

AsyncOSオペレーティングシステムでは、viaSNMPによるシステムステータスの監視がサポートされています。

注：

- SNMPisoffbyデフォルト。
- SNMPSETの動作（設定）は実装されていません。
- AsyncOSはSNMPv1、v2、およびv3をサポートします。
- SNMPv3を有効にする場合、メッセージの認証と暗号化は必須です。認証と暗号化のパスフレーズは異なっている必要があります。
- 暗号化アルゴリズムには、AES（推奨）またはDESを使用できます。
- 認証アルゴリズムには、SHA-1（推奨）またはMD5を使用できます。
- nmpconfigコマンドは、次にコマンドを実行するときにパスフレーズを「記憶」します。
- 15.0より前のAsyncOSリリースでは、SNMPv3ユーザ名はv3getです。
- AsyncOSリリース15.0以降の場合、defaultSNMPv3ユーザ名はv3getです。管理者は、他のユーザ名を選択できます。
- onlySNMPv1 またはSNMPv2を使用する場合は、コミュニティストリングを設定する必要があります。コミュニティストリングのデフォルトはpublicではありません。
- SNMPv1およびSNMPv2では、SNMPGET要求を受け入れるネットワークを指定する必要があります。
- トラップを使用するには、SNMPmanager（AsyncOSには含まれない）が実行されていて、トラップターゲットとしてIPアドレスが入力されている必要があります。（ホスト名を使用できますが、使用した場合、トラップはDNSが機能している場合にのみ機能します）。

SNMPMonitorの設定

アプライアンスのシステムステータス情報を収集するようにSNMPを設定するには、CLIでthesnmpconfigコマンドを使用します。インターフェイスの値を選択して設定すると、アプライアンスはSNMPv3 GET要求に応答します。

SNMPを使用する場合は、次の点を考慮してください。

- SNMPバージョン3では、要求に一致するパスフレーズを含める必要があります。

- デフォルトでは、バージョン1と2の要求は拒否されます。
- 有効にした場合、バージョン1および2の要求には一致するコミュニティストリングが必要です。

```
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ファイル

MIBファイルは、https://www.cisco.com/c/en/us/support/security/web-security-appliance/series.htmlから入手できます。

各MIBファイルの最新バージョンを使用します。

複数のMIBファイルがあります。

- asyncoswebsecurityappliance-mib.txtは、Enterprise MIB forSecure Web AppliancesのSNMPv2互換の説明です。
- ASYNCOS-MAIL-MIB.txtは、Eメールセキュリティアプライアンス用のエンタープライズMIBに関するSNMPv2互換の説明です。
- IRONPORT-SMI.txt：この「管理情報の構造」ファイルでは、asyncoswebsecurityappliance-mibの役割を定義します。

このリリースでは、RFC 1213および1907で定義されているMIB-IIの読み取り専用サブセットが実装されています。

Seehttps://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118415-technote-wsa-00.htmlsnmpを使用したアプライアンスでのCPU使用率のモニタリングの詳細については、こちらを参照してください。

SWA SNMPトラップ

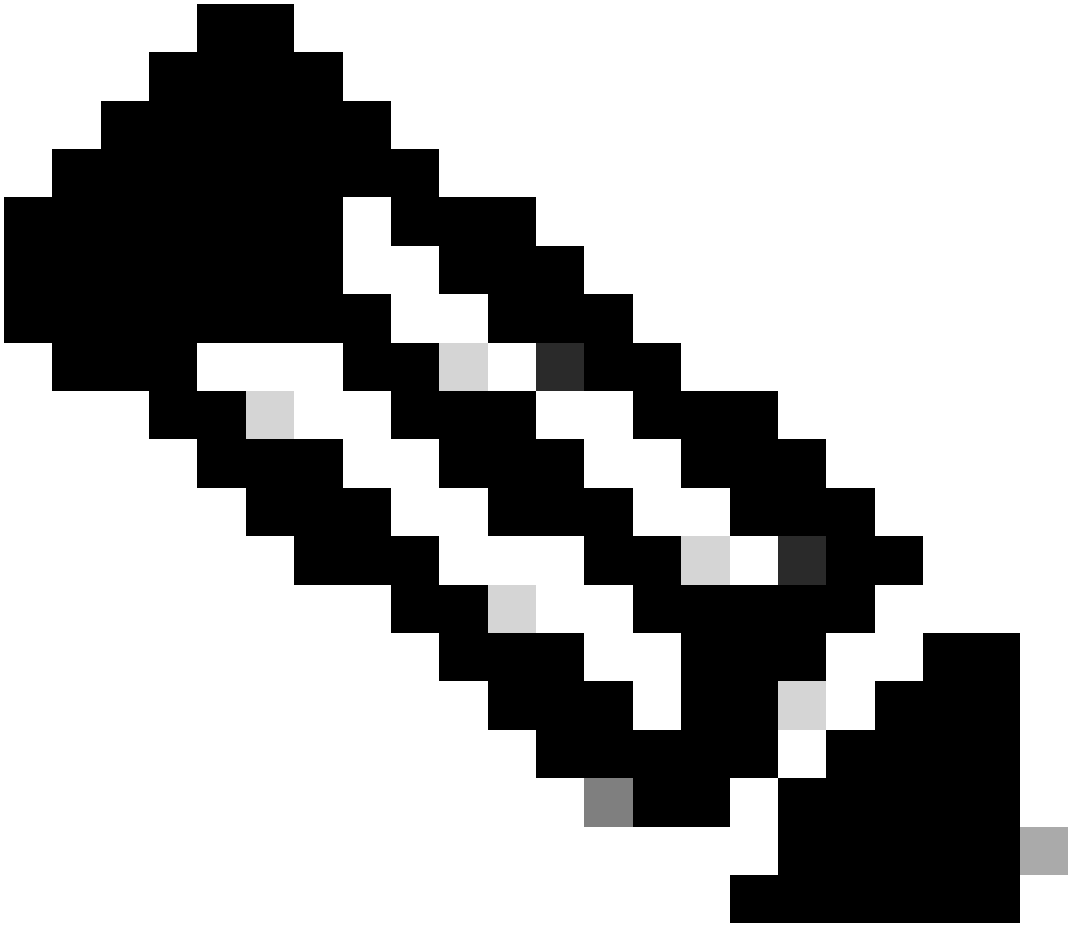
SNMPは、1つ以上の条件が満たされた場合に管理アプリケーションに通知するために、トラップまたは通知を送信する機能を提供します。

トラップは、トラップを送信するシステムのコンポーネントに関連するデータを含むネットワークパケットです。

トラップは、SNMPagent(この場合はCiscoSecure Web Appliance)で条件が満たされると生成されます。

この条件が満たされると、SNMPagentはSNMPパケットを形成し、SNMPmanagementコンソールソフトウェアを実行しているホストに送信します。

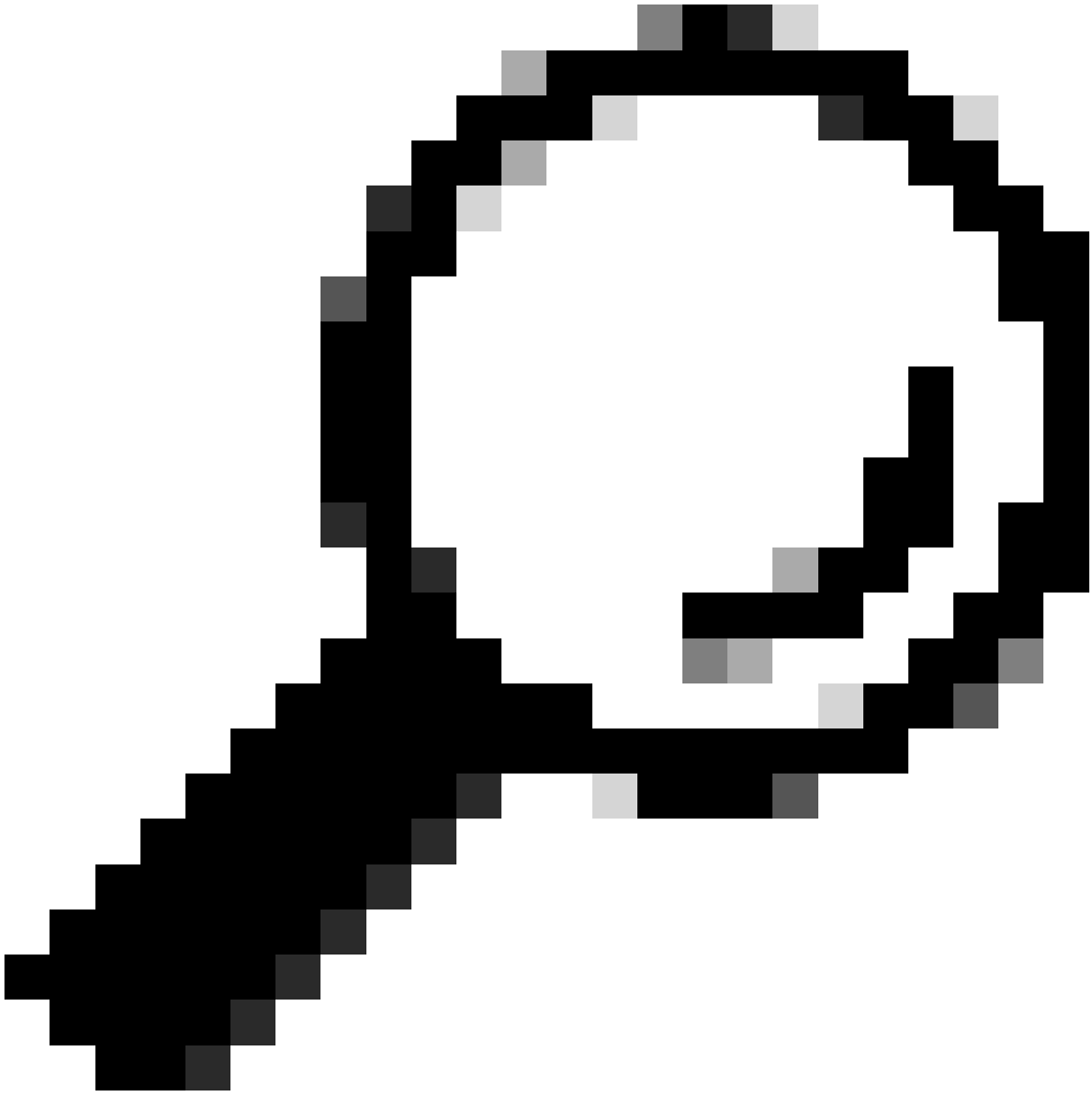
インターフェイスに対してSNMPをイネーブルにすると、SNMPtrapsを設定（特定のトラップをイネーブルまたはディセーブル）できます。



注：複数のトラップターゲットを指定するには：トラップターゲットの入力を求められたときに、最大10個のIPアドレスをカンマで区切って入力します。

connectivityFailure トラップは、インターネットへのアプライアンスの接続を監視することを目的としています。これは、5 ~ 7秒ごとに1つの外部サーバに接続してHTTP GET要求を送信することで行われます。デフォルトでは、モニタされるURLはポート80のdownloads.ironport.comです。

監視対象のURLまたはポートを変更するには、snmpconfigコマンドを実行し、connectivityFailureトラップがすでに有効になっている場合でも有効にします。URLを変更するプロンプトが表示されます。



ヒント:connectivityFailureトラップをシミュレートするには、CLIコマンドdnsconfigを使用して、機能していないDNSサーバに入ります。downloads.ironport.comのルックアップが失敗し、トラップが5 ~ 7秒ごとに送信されます。テストが終了したら、必ずDNSサーバを稼働中のサーバに戻してください。

推奨されるモニタリングOID

次に示すのは、監視が推奨されるMIBのリストであり、完全なリストではありません。

ハードウェアOID	[名前(Name)]
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	raidステータス

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	ファンテーブル
1.3.6.1.4.1.15497.1.1.1.9.1.2	摂氏

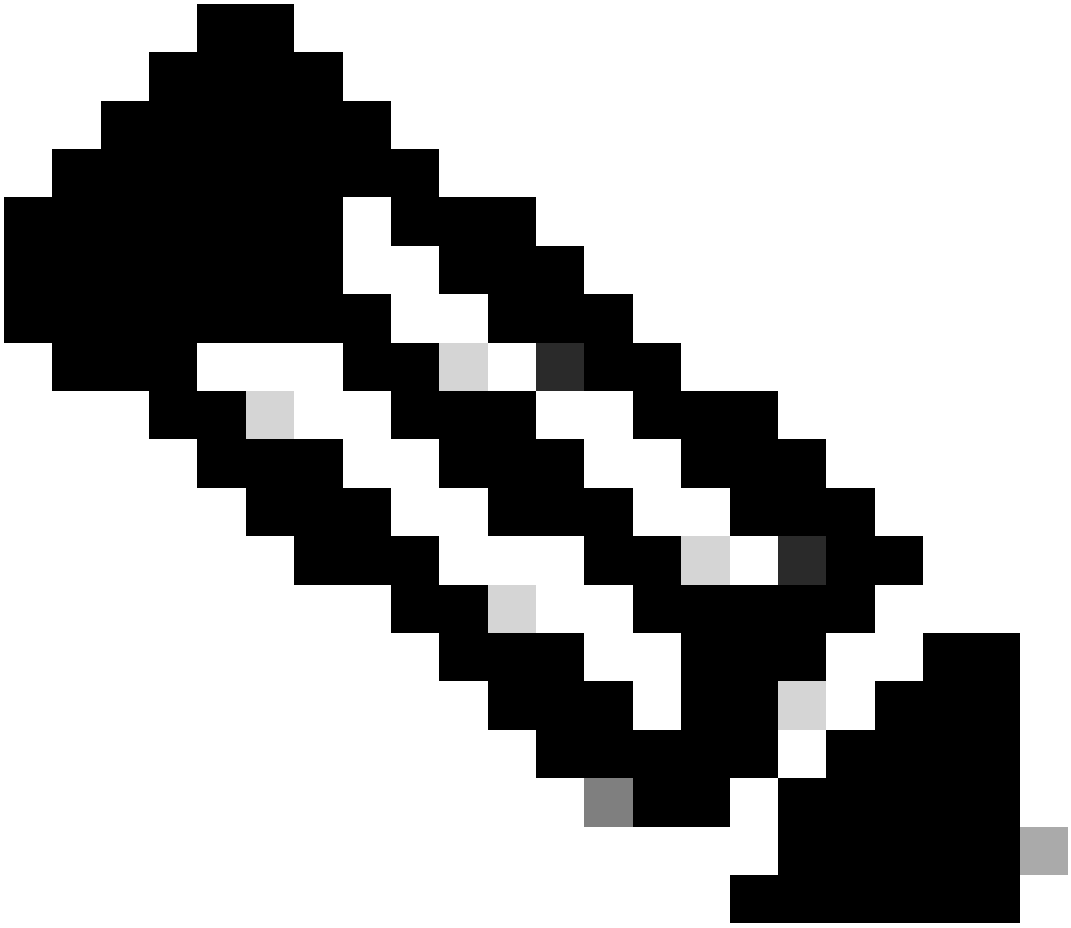
次に、status detailCLIコマンドの出力に直接OIDをマッピングした例を示します。

OID	[名前(Name)]	Status Detailフィールド
System Resources		
1.3.6.1.4.1.15497.1.1.1.2.0	perCentCPUtilization	CPU
1.3.6.1.4.1.15497.1.1.1.1.0	メモリ使用率	RAM
1秒あたりのトランザクション		
1.3.6.1.4.1.15497.1.2.3.7.1.1.0	cacheThruputNow	最後の1分間の1秒あたりの平均トランザクション数。
1.3.6.1.4.1.15497.1.2.3.7.1.2.0	cacheThruput1hrPeak	過去1時間の1秒あたりの最大トランザクション数。
1.3.6.1.4.1.15497.1.2.3.7.1.3.0	cacheThruput1hrMean（平均）	過去1時間の1秒あたりの平均トランザクション数。
1.3.6.1.4.1.15497.1.2.3.7.1.8.0	cacheThruputLifePeak	プロキシ再起動以降の1秒あたりの最大トランザクション数。
1.3.6.1.4.1.15497.1.2.3.7.1.9.0	cacheThruPutLifeMean	プロキシ再起動以降の1秒あたりの平均トランザクション数。
帯域幅		
1.3.6.1.4.1.15497.1.2.3.7.4.1.0	cacheBwidthTotalNow	過去1分間の平均帯域幅。
1.3.6.1.4.1.15497.1.2.3.7.4.2.0	cacheBwidthTotal1hrPeak	過去1時間の最大帯域幅。
1.3.6.1.4.1.15497.1.2.3.7.4.3.0	cacheBwidthTotal1hrMean	過去1時間の平均帯域幅。
1.3.6.1.4.1.15497.1.2.3.7.4.8.0	cacheBwidthTotalLifePeak	プロキシ再起動後の最大帯域幅。
1.3.6.1.4.1.15497.1.2.3.7.4.9.0	cacheBwidthTotalLifeMean	プロキシ再起動以降の平均帯域幅。
応答所要時間		
1.3.6.1.4.1.15497.1.2.3.7.9.1.0	cacheHitsNow	過去1分間の平均キャッシュヒット率。
1.3.6.1.4.1.15497.1.2.3.7.9.2.0	キャッシュヒット1時間ピーク	過去1時間の最大キャッシュヒット率。
1.3.6.1.4.1.15497.1.2.3.7.9.3.0	cacheHits1hrMean	過去1時間の平均キャッシュヒ

		ット率。
1.3.6.1.4.1.15497.1.2.3.7.9.8.0	cacheHitsLifePeak	プロキシ再起動後の最大キャッシュヒット率。
1.3.6.1.4.1.15497.1.2.3.7.9.9.0	cacheHitsLifeMean	プロキシ再起動後の平均キャッシュヒット率。
キャッシュヒット率		
1.3.6.1.4.1.15497.1.2.3.7.5.1.0	cacheHitsNow	過去1分間の平均キャッシュヒット率。
1.3.6.1.4.1.15497.1.2.3.7.5.2.0	キャッシュヒット1時間ピーク	過去1時間の最大キャッシュヒット率。
1.3.6.1.4.1.15497.1.2.3.7.5.3.0	cacheHits1hrMean	過去1時間の平均キャッシュヒット率。
1.3.6.1.4.1.15497.1.2.3.7.5.8.0	cacheHitsLifePeak	プロキシ再起動後の最大キャッシュヒット率。
1.3.6.1.4.1.15497.1.2.3.7.5.9.0	cacheHitsLifeMean	プロキシ再起動後の平均キャッシュヒット率。
接続		
1.3.6.1.4.1.15497.1.2.3.2.7.0	cacheClientIdleConns	アイドル状態のクライアント接続。
1.3.6.1.4.1.15497.1.2.3.3.7.0	cacheServerIdleConns	アイドル状態のサーバ接続
1.3.6.1.4.1.15497.1.2.3.2.8.0	cacheClientTotal接続	クライアント接続の合計。
1.3.6.1.4.1.15497.1.2.3.3.8.0	cacheServerTotalConns	サーバー接続の合計。

SNMPのトラブルシューティング

SWAとSNMPマネージャ間の接続を表示するには、パケットをキャプチャするのが最適です。パケットキャプチャフィルタを次のように設定します(ポート161またはポート162)。



注：このフィルタはデフォルトのSNMPポートが原因です。ポートを変更した場合は、設定したポート番号をパケットキャプチャフィルタに含めてください。

SWAからパケットをキャプチャする手順：

ステップ1:GUIにログインします。

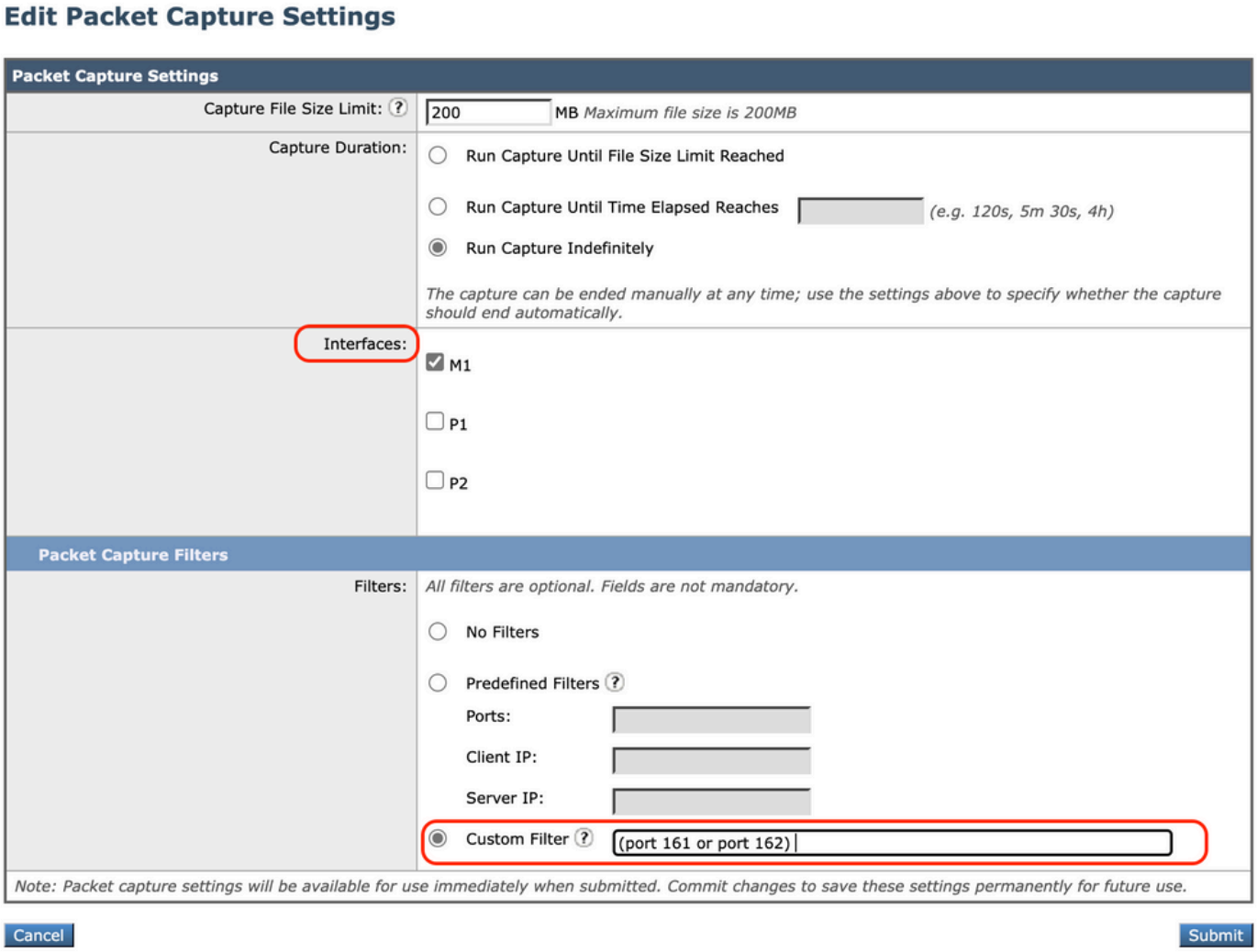
ステップ2:右上でSupport and Helpを選択します。

ステップ3:パケットキャプチャの選択

ステップ4:設定の編集を選択します

ステップ 5：正しいインターフェイスが選択されていることを確認します。

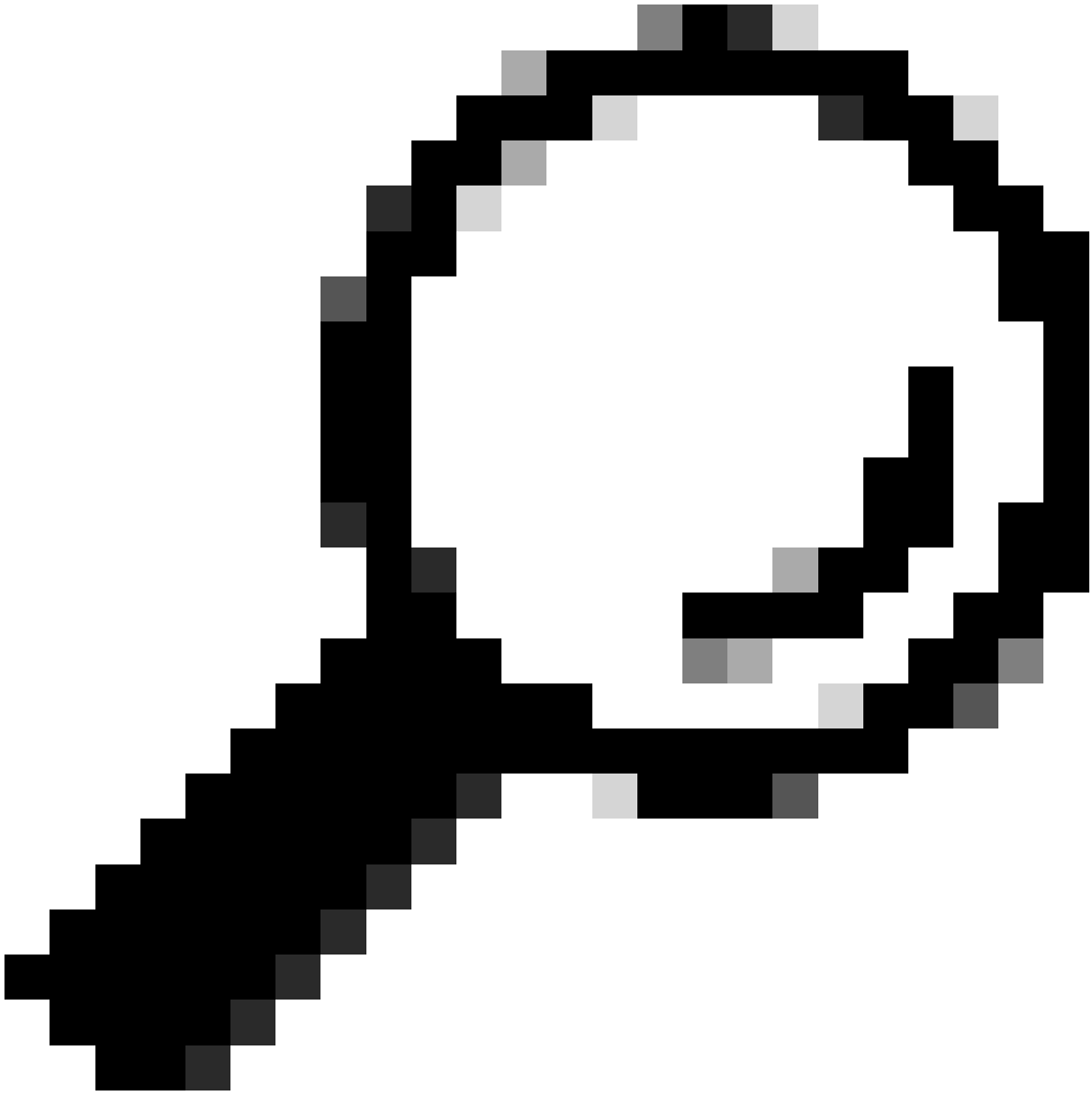
手順 6：フィルタ条件を入力します。



イメージ：パケットキャプチャフィルタの設定

手順 7：Submitを選択します。

ステップ 8： Start Captureを選択します。



ヒント:SNMPv3パケットキャプチャはWiresharkで復号できます。詳細については、How-to-decrypt-snmpv3-packets-using-wiresharkを参照してください。

SNMPWALK

snmpwalkは、複数のGET-NEXT要求を自動的に実行するSNMPアプリケーションに付けられた名前です。SNMP GET-NEXT要求は、有効なデバイスを照会し、デバイスからSNMPデータを取得するために使用されます。snmpwalkコマンドが使用される理由は、ユーザがサブツリー内の各OIDまたはノードに一意のコマンドを入力することなく、GET-NEXT要求を連結できるためです

WindowsオペレーティングシステムへのSNMPWALKのインストール

Microsoft Windowsユーザの場合、最初にツールをダウンロードする必要があります。

LinuxカーネルへのSNMPWALKのインストール

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

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

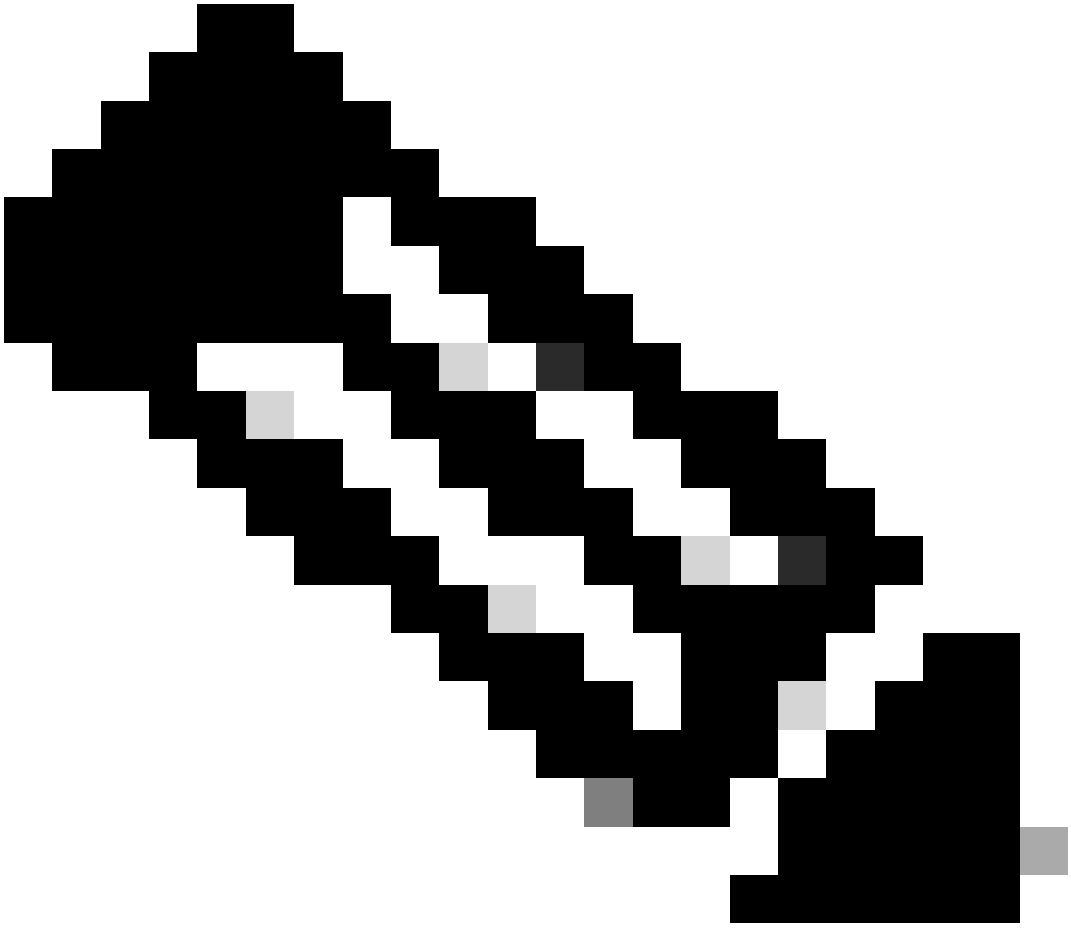
MacOSへのSNMPWALKのインストール

MacOSには、デフォルトでsnmpwalkがインストールされます

SNMP GET要求を生成するには、ネットワーク上にありSWAに接続できる別のコンピュータからsnmpwalkコマンドを使用します。次にsnmpwalkコマンドの例を示します。

```
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:SWAの設定に応じて、セキュリティレベルをnoAuthNoPriv、authNoPriv、またはauthPrivに設定できます。

SNMPTRAP

snmptrapはCLIの隠しコマンドであり、SWAでSNMPを有効にする必要があります。SNMPトラップは、オブジェクトとトラップを選択して生成できます。次に例を示します。

```
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のSNMPログ

SWAにはSNMPに関連する2つのログがあり、Webプロキシコンポーネントに関連する一部のログタイプは有効になっていません。これらは次の場所で有効にできます。

- GUIの場合：System Administration > Log subscriptions
- CLIの場合：logconfig > new

ログファイルの種類	説明	Syslogプッシュをサポートしていますか。	デフォルトで有効?
SNMPログ	SNMPネットワーク管理エンジンに関連するデバッグメッセージを記録します。	Yes	Yes
SNMPモジュールログ	SNMP監視システムとの対話に関連するWebプロキシメッセージを記録します。	いいえ	いいえ

SNMPに関する一般的な問題

一部のOIDが失敗します（値がないか、または間違った値です）。

この問題はSNMPプルに関連しています。予期される出力とエラーのある出力の2つのサンプルを次に示します：

```
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
```

snmp_logsで「Application Faults」をチェックできます

snmp_logsは、CLI > grepの順に選択して、snmp_logsに関連付けられている番号を確認できます。

```
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

AsyncOS 15.0 for Cisco Secure Web Applianceユーザガイド – LD（限定導入） – トラブルシューティング[Cisco Secure Web Appliance] – シスコ

SNMPを使用したWSAでのプロキシCPU使用率の計算：シスコ

snmpcmd(1) (freebsd)

snmptrap(freebsd)

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。