SNMPによるCisco ESAの監視

はじめに

このドキュメントでは、SNMPを使用してCisco Secure Email Gateway(CEM)を監視する方法について説明します。MIB構造、OIDの使用、実用的なクエリーなどが含まれます。

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。

- SNMPプロトコルの基礎知識
- Cisco ESAアプライアンスへのアクセス
- Linuxコマンドラインに精通していること
- SNMPサービスが有効なCisco ESA
- SNMPクライアントがインストールされている（Net-SNMPツールなど）
- 使用可能でロードされているIronPort MIBファイル
- コミュニティストリングまたはSNMP v3クレデンシャル

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CiscoセキュアEメールゲートウェイ(ESA)
- Net-SNMPツールを使用するLinuxクライアント
- MIBファイル：IRONPORT-SMI.txt、ASYNCOS-MAIL-MIB.txt

SNMPの設定

ESAのSNMP設定は、CLIを介して行われます。 Cisco ESAでSNMPを有効にするには、CLIにアクセスしてsnmpconfigを実行します。

デフォルトの設定は次のとおりです。

- SNMPサービスの有効化
- 管理インターフェイスとポートの選択（通常は161）
- SNMPv3の有効化（デフォルトのセキュリティ：authPriv with SHA and AES）
- 認証とプライバシーのパスフレーズの設定
- SNMPv1/v2cを有効にし、コミュニティストリング（ironportなど）を指定する
- SNMP要求に対して許可されるIPv4ネットワークの定義
- SNMPトラップバージョンとトラップターゲットIPアドレスの設定
- システムの場所と連絡先情報の設定

SNMPを有効にすると、次のようなサマリが表示されます。

```
esa1.ironport.com> snmpconfig

Current SNMP settings:
Listening on interface "Management"



      port 161.
SNMP v3: Enabled. Security level: authPriv
Authentication Protocol: SHA
Encryption Protocol: AES
SNMP v1/v2: Enabled, accepting requests from subnet



      , .
SNMP v1/v2 Community String: ironport
Trap version: V3
Trap target:



Location: esxi data center
System Contact: ciscoros soc
```

SNMPを有効にして設定すると、アプライアンスは許可された送信元IPからのSNMPクエリを受け入れる準備が整います。

LinuxでのSNMPクライアントのセットアップとクエリ

この例では、Debianサーバを使用しました。インストール手順は、配布パッケージマネージャーによって異なる場合があります。

SNMPツールのインストール

```
sudo apt-get install snmp snmp-mibs-downloader
```

snmpwalkバイナリがインストールされていることを確認します。

```
diegoher@debian-server:/usr/share/snmp/mibs$ snmpwalk --version
NET-SNMP version: 5.9
```

MIBファイルのロード

IronPort MIBファイルを/usr/share/snmp/mibsフォルダに配置します。

```
root@debian-server:/usr/share/snmp/mibs# pwd
/usr/share/snmp/mibs
root@debian-server:/usr/share/snmp/mibs# ls
ASYNCOS-MAIL-MIB.txt  IRONPORT-SMI.txt        NET-SNMP-EXAMPLES-MIB.txt  NET-SNMP-PASS-MIB.txt  UCD-DEMO-MIB.txt    UCD-IPFWACC-MIB.txt
iana                  LM-SENSORS-MIB.txt      NET-SNMP-EXTEND-MIB.txt    NET-SNMP-TC.txt        UCD-DISKIO-MIB.txt  UCD-SNMP-MIB.txt
ietf                  NET-SNMP-AGENT-MIB.txt  NET-SNMP-MIB.txt           NET-SNMP-VACM-MIB.txt  UCD-DLMOD-MIB.txt
```

debianサーバのOID

注:MIBファイルは、このドキュメントの最後にあるSNMPの記事に記載されています。

OIDを使用したCPU使用率の監視

このコマンドは、現在のCPU使用率についてESAを照会します。OIDは、MIBで定義されているCPUメトリックを直接指します。出力には、INTEGER: 37などの値が表示され、デバイスのCPU使用率が37 %であることを示します。これにより、管理者はデバイスのパフォーマンスをリアルタイムで監視し、使用率が許容範囲を超えた場合に介入できます。

```
snmpwalk -v2c -c ironport

      .1.3.6.1.4.1.15497.1.1.1.2
```

SNMPコマンドでOIDを使用すると、特定のメトリックに直接アクセスできるため、効果的なモニタリングとトラブルシューティングが可能になります。

シンボリック名を有効にする

```
export MIBS=ALL
```

export MIBS=ALLを設定すると、SNMPツールは、長い数値のOIDの代わりに、MIBファイルで定義された人間が読める名前を使用できます。これにより、番号順序ではなくworkQueueMessagesのようなわかりやすい名前でオブジェクトを参照できるため、クエリの記述、理解、およびトラブルシューティングが容易になります。

SNMPクエリの実行

snmpwalkを使用して、主要なメトリックについてESAに照会します。 SNMPクエリを使用すると、Cisco ESAからリアルタイムステータスとパフォーマンスデータを取得できます。シンボリック名を使用すると、複雑な数値OIDを参照しなくても、キューのステータス、ライセンスの有効期限、ハードウェアの使用率などの特定のオブジェクトを簡単に監視できます。

ワークキューメッセージ

```
diegoher@debian-server:/usr/share/snmp/mibs$ snmpwalk -v2c -c ironport
      workQueueMessages
ASYNCOS-MAIL-MIB::workQueueMessages.0 = Gauge32: 0
```

この出力は、現在、ESA作業キューにメッセージが存在しないことを示しています。この値は、処理待ちの電子メールのリアルタイム数を表します。

CPU Utilization

```
diegoher@debian-server:/usr/share/snmp/mibs$ snmpwalk -v2c -c ironport
```

これは、ESAのCPUの使用率が現在37 %であることを示しています。この値は、クエリが実行された時点でのアプライアンスの処理負荷に関する情報を提供します。

ライセンスキーの有効期限テーブル

```
diegoher@debian-server:/usr/share/snmp/mibs$ snmpwalk -v2c -c ironport


       keyExpirationTable
ASYNCOS-MAIL-MIB::keyExpirationIndex.1 = INTEGER: 1
ASYNCOS-MAIL-MIB::keyExpirationIndex.2 = INTEGER: 2
ASYNCOS-MAIL-MIB::keyExpirationIndex.3 = INTEGER: 3
ASYNCOS-MAIL-MIB::keyExpirationIndex.4 = INTEGER: 4
ASYNCOS-MAIL-MIB::keyExpirationIndex.5 = INTEGER: 5
ASYNCOS-MAIL-MIB::keyExpirationIndex.6 = INTEGER: 6
ASYNCOS-MAIL-MIB::keyExpirationIndex.7 = INTEGER: 7
ASYNCOS-MAIL-MIB::keyExpirationIndex.8 = INTEGER: 8
ASYNCOS-MAIL-MIB::keyDescription.1 = STRING: Bounce Verification
ASYNCOS-MAIL-MIB::keyDescription.2 = STRING: Data Loss Prevention
ASYNCOS-MAIL-MIB::keyDescription.3 = STRING: External Threat Feeds
ASYNCOS-MAIL-MIB::keyDescription.4 = STRING: Incoming Mail Handling
ASYNCOS-MAIL-MIB::keyDescription.5 = STRING: IronPort Anti-Spam
ASYNCOS-MAIL-MIB::keyDescription.6 = STRING: IronPort Email Encryption
ASYNCOS-MAIL-MIB::keyDescription.7 = STRING: Outbreak Filters
ASYNCOS-MAIL-MIB::keyDescription.8 = STRING: Sophos Anti-Virus
ASYNCOS-MAIL-MIB::keyIsPerpetual.1 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keyIsPerpetual.2 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keyIsPerpetual.3 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keyIsPerpetual.4 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keyIsPerpetual.5 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keyIsPerpetual.6 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keyIsPerpetual.7 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keyIsPerpetual.8 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.1 = Gauge32: 0
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.2 = Gauge32: 0
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.3 = Gauge32: 0
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.4 = Gauge32: 0
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.5 = Gauge32: 0
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.6 = Gauge32: 0
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.7 = Gauge32: 0
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.8 = Gauge32: 0
```

- keyExpirationIndex.X：各インデックスは、Cisco ESAにインストールされている固有の機能キーを表します。
- keyDescription.X: 「バウンス検証」、「データ損失防止」、「IronPortアンチスパム」、「Sophosアンチウイルス」など、各機能キーの名前または説明を提供します。
- keyIsPerpetual.X：各機能のライセンスが無期限かどうかを示します。値true (1)は、ライセンスの有効期限がないことを意味します。
- keySecondsUntilExpire.X：ライセンスの有効期限が切れるまでの残り秒数を示します。値0は、ライセンスが無期限

であるか、すでに期限切れであることを示します。

```
[]> summary

Feature Name                                                    License Authorization Status
-----------------------------------------------------------------------------------------------
Email Security Appliance Anti-Spam License                      In Compliance
Email Security Appliance Outbreak Filters                       In Compliance
Email Security Appliance Graymail Safe-unsubscribe              Not requested
Email Security Appliance External Threat Feeds                  In Compliance
Email Security Appliance Advanced Malware Protection Reputation Not requested
Mail Handling                                                   In Compliance
Email Security Appliance Sophos Anti-Malware                    In Compliance
Email Security Appliance PXE Encryption                         In Compliance
Email Security Appliance Advanced Malware Protection            Not requested
Email Security Appliance McAfee Anti-Malware                    Not requested
Email Security Appliance Intelligent Multi-Scan                 Not requested
Email Security Appliance Image Analyzer                         Not requested
Email Security Appliance Bounce Verification                    In Compliance
Email Security Appliance Data Loss Prevention                   In Compliance
```

ライセンスの例

この出力では、アプライアンスの現在の機能キー、その説明、およびライセンスステータスを確認できます。記載されているすべてのライセンスは、keyIsPerpetualおよびkeySecondsUntilExpireで示されるように、永続的です。この情報は、重要なセキュリティ機能がCisco ESAでアクティブかつ有効であることを確認するのに役立ちます。

数値OIDと記号名の違い

数値OID:

- これらは普遍的で、MIBファイルがシステムにロードされていない場合でも常に動作します。
- 例： .1.3.6.1.4.1.15497.1.1.2
- 読みにくく、覚えづらいことがあります。

シンボル名：

- これらは、perCentCPUUtilizationなど、MIBファイルで定義されているユーザにとってわかりやすい名前です。
- コマンドの記述と理解が容易になります。
- MIBファイルを正しくロードし、MIBS環境変数を設定する必要があります。
- 例：snmpwalk -v2c -c ironport 10.31.124.165 perCentCPUUtilization

同じですか？

どちらの方法でも同じメトリックを照会して同じ結果が得られますが、シンボリック名の方が実用的で人間が読める形式に近く、数値OIDの方がMIBファイルが存在しない、またはロードできない環境で信頼性が高くなります。

関連情報

- SNMPを使用したシステムの健全性とステータスのモニタリング
- シスコのテクニカルサポートとダウンロード

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。