IPS 5.x 以降： モニタリング イベントのさまざまな方式

目次

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[表記法](#)
[IPS イベントのモニタ方法](#)
[関連情報](#)

概要

このドキュメントでは、IPS イベントをモニタするための各種方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、IPS 5.x 以降に基づくものです。

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たものです。 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。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

IPS イベントのモニタ方法

センサーをモニタするためのオプションは、現在次の 4 つがあります。

1. IPS Manager Express（IME）は、Cisco.com のソフトウェアのダウンロードから入手でき

ます。 このアプリケーションでは、SDEE を使用して IPS センサーを安全にサブスクライブしたり、一致のために生じた問題やシグニチャの結果として生成されたイベントまたはログを取得したりできます。HTTPS によってセンサーに直接アクセスすると、IPS Device Manager（IDM）が呼び出されます。IDM Monitoring ツールまたは IME Event Monitoring ツールを使用してセンサー上のイベント ストアを直接表示します。 イベントを長期間にわたって保存する必要がある場合、センサーのローカル イベント ストアが 30 MB の循環バッファで、30 MB の制限に達するとそのイベント ストア自体を上書きし始めるため、IDM および IME は有効なソリューションではありません。 この制限は設定できません。

2. センサーからイベントを定期的にプルして関連付けるには、CS-MARS デバイスを使用します。 CS-MARS では、イベントを取得するために SDEE プロトコルを使用してセンサーへのセキュアな接続を確立してから、新しいイベントを数秒ごとに取得します。CS-MARS デバイスのデモをご覧になりたい場合は、詳細についてアカウント（顧客）チーム、再販業者、または SE にお問い合わせください。Cisco IPS 5.x デバイスおよび 6.x デバイスの場合、MARS では SDEE over SSL を使用してログをプルします。 そのため、MARS からセンサーに対して HTTPS アクセスできる必要があります。 センサーを準備するために、IDM または IME の管理ステーションで HTTPS トラフィックを許可し、MARS の IP アドレスがセンサー上で許可されたホストとして定義されていることを確認する必要があります。

```
sensor#conf t
 sensor(config)#service host
 sensor(config-hos)#network-settings
 sensor(config-hos-net)#access-list x.x.x.x/subnet_mask
 sensor(config-hos-net)#exit
 sensor(config-hos)#exit
 Apply Changes?[yes]:
 sensor(config)#
```

3. IEV を使用してイベントをモニタします。 IDS Event Viewer は、最大 5 個のセンサーのアラームを表示および管理できる Java ベースのアプリケーションです。 IDS Event Viewer を使用すると、アラームをリアル タイムで、またはインポートされたログ ファイルとして接続および表示できます。 アラームの管理に役立てるためにフィルタおよびビューを設定できます。 イベント データをインポートおよびエクスポートして、さらに詳しく分析することもできます。 MARS 同様、IEV はセンサーへのセキュアな接続を確立してイベントを数秒ごとに取得します。 IEV では、IEV がインストールされているサーバ上のデータベースに、これらのイベントを保存します。 この DB は IEV に組み込まれており、アプリケーションとともにインストールされます。 [IEV] をクリックしてダウンロードします。**注:** IEV のドキュメントは、インストール後に [Help] メニューで見つかります。 readme には、インストールに関する情報が記載されています。
4. **request-snmp-trap** のアクションを含めるようにセンサーでシグニチャを設定し、トラップを SNMP サーバに送信するようにセンサーを設定します。 これにより、このサーバを使用してメッセージを別のマシンに syslog としてリレーできます。SNMP は、ネットワーク デバイス間での管理情報の交換を容易にするアプリケーション層プロトコルです。 SNMP により、ネットワーク管理者は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発見/解決でき、ネットワークの拡張を計画することができます。SNMP は単純な要求/応答プロトコルです。 ネットワーク管理システムが要求を発行し、管理対象デバイスが応答を返します。 この動作は、次の 4 つのプロトコル操作のいずれかを使用して実行されます。結果GetNextSetTrapSNMP によるモニタリングのためにセンサーを設定することができます。 SNMP では、ネットワーク管理ステーションがスイッチ、ルータ、センサーなどの多くのタイプのデバイスのヘルスとステータスをモニタするための標準的な方法を定義しています。

関連情報

- Cisco IPS 4200 シリーズ センサー
- Cisco Intrusion Prevention System
- セキュリティ製品に関する Field Notice (CiscoSecure Intrusion Detection を含む)
- テクニカルサポートとドキュメント - Cisco Systems