IPS 5.x及更高版本：監視事件的各種方法

目錄

簡介

本文提供監控IPS事件的各種方法。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據IPS 5.x及更新版本。

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

監視IPS事件的方法

目前，有四個選項可用於監控感測器：

1. IPS Manager Express(IME)可從Cisco.com中的軟體下載獲得。此應用程式能夠使用SDEE安全地訂閱IPS感測器，並檢索由於匹配而引發的任何問題或特徵碼所生成的事件/日誌。直接通過HTTPS訪問感測器時，將呼叫IPS裝置管理器(IDM)。使用IDM Monitoring或IME Event Monitoring工具直接在感測器上檢視事件儲存。如果您需要長期儲存事件，則IDM和IME不是有效的解決方案，因為感測器的本地事件儲存是30 MB循環緩衝區，一旦達到30 MB的限制

，就會開始自行覆蓋。此限制不可配置。

2. 使用CS-MARS裝置定期從感測器提取事件並關聯事件。CS-MARS使用SDEE協定來建立與感測器的安全連線，以便檢索事件並每隔幾秒鐘檢索一次新事件。如果您有興趣演示CS-MARS裝置，請聯絡您的客戶團隊/經銷商/SE瞭解更多資訊。對於Cisco IPS 5.x和6.x裝置,MARS通過SSL提取SDEE日誌。因此，MARS必須能夠通過HTTPS訪問感測器。為了準備感測器，必須允許來自IDM/IME管理站的HTTPS通訊量，並確保MARS的IP地址被定義為感測器上允許的主機。

```
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. 使用IEV監視事件。IDS事件檢視器是一個基於Java的應用程式，可用於檢視和管理最多五個感測器的警報。通過IDS事件檢視器，您可以即時連線並檢視警報，也可以在匯入的日誌檔案中檢視警報。您可以配置過濾器和檢視以幫助管理警報。還可以匯入和匯出事件資料以進行進一步分析。與MARS一樣，IEV建立與感測器的安全連線，並每隔幾秒鐘檢索一次事件。IEV將這些事件儲存在安裝IEV的伺服器上的資料庫中。DB隨IEV一起提供，並隨應用程式一起安裝。按一下IEV以下載。**注意：**安裝IEV後，可通過幫助選單找到其文檔。自述包含安裝資訊。
4. 將感測器上的特徵碼配置為**request-snmp-trap**操作，並將感測器配置為將陷阱傳送到SNMP服務器。然後，您可以使用此伺服器將消息作為系統日誌中繼到另一台電腦。SNMP是一種應用層協定，可促進網路裝置之間的管理資訊交換。SNMP 使網路系統管理員得以管理網路效能、尋找和解決網路問題，以及規劃網路擴充事宜。SNMP是一種簡單的請求/響應協定。網路管理系統發出請求，受管裝置返迴響應。此行為通過使用以下四種協定操作之一來實施：獲取GetNext設定陷阱您可以配置感測器以通過SNMP進行監控。SNMP為網路管理站定義了一種標準方法，可監控多種型別的裝置（包括交換器、路由器和感應器）的健康狀態和狀態。

相關資訊

- Cisco IPS 4200系列感應器
- 思科入侵防禦系統
- 安全產品現場通知（包括CiscoSecure Intrusion Detection）
- 技術支援與文件 - Cisco Systems