IPS 5.x和以后：监控事件的多种方法

目录

简介

本文提供多种方法监控IPS事件。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息根据IPS 5.x和以后。

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

箴言报方法IPS事件

目前，有监控的传感器四个选项：

1. IPS管理器Express (IME)从软件下载是可得到在Cisco.com。此应用程序能安全地订阅到IPS有SDEE的传感器和检索生成由于所有问题或签名射击了由于匹配的事件/日志。IPS设备管理器(IDM)呼叫，当您直接地通过HTTPS时访问传感器。查看事件存储直接地传感器的用IDM监控或IME事件监控工具。IDM和IME是无效解决方案，如果需要存储事件长期，因为传感器的本地事件存储是30 MB圆的缓冲区并且开始对overwite 30 MB限制一次被到达。此限制是不可配

置的。

2. 请使用一个CS-MARS设备为了定期地请求和关联从传感器的事件。CS-MARS使用SDEE协议为了建立对传感器的一个安全连接获取事件并且每隔几秒钟获取新的事件。如果是对演示ing感兴趣CS-MARS设备，请与您的客户团队/reseller/SE联系欲知更多信息。对于思科IPS 5.x和6.x设备，毁损下拉式与SDEE的日志在SSL。所以，火星必须得以进入对传感器的HTTPS。为了准备传感器，您必须允许从IDM/IME管理站的HTTPS流量，并且确保，火星的IP地址定义作为在传感器的一台允许主机。

```
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. 监控与IEV的事件。IDS Event Viewer是使您查看和管理五个传感器的报警的一基于Java的应用程序。使用IDS Event Viewer您能连接对和查看报警在实时或在已导入日志文件。您能配置过滤器和视图帮助您管理报警。您能也导入和导出进一步分析的事件数据。类似火星， IEV建立对传感器的一个安全连接并且每隔几秒钟获取事件。IEV存储在一个数据库的这些事件在IEV安装的服务器。DB包括与IEV并且与应用程序一起安装。点击IEV为了下载。**注意：** 在您安装它后， IEV的文档通过Help菜单被找到。README包含安装信息。
4. 配置在您的传感器的签名有请求SNMP**陷阱的**操作和配置传感器发送陷阱到SNMP服务器。您能然后使用此服务器中继消息作为Syslog到另一计算机。SNMP是实现管理信息交换在网络设备之间的应用层协议。SNMP使网络管理员管理网络性能，查找和解决网络问题和规划网络增长的。SNMP是一份简单请求/响应协议。网络管理系统问题请求和受管理设备返回答复。此行为实现与使用四协议的运行之一：获得GetNext集陷阱您能由SNMP配置监控的传感器。SNMP定义了网络管理站的一个标准的方式能监控设备的许多类型健康和状况，包括交换机、路由器和传感器。

相关信息

- Cisco IPS 4200 系列传感器
- Cisco Intrusion Prevention System
- 安全产品的问题信息通告（Field Notice）(包括CiscoSecure Intrusion Detection)
- 技术支持和文档 - Cisco Systems