IPS 5.x y posterior: Diversos métodos de supervisión de eventos

Contenido

Introducción

Este documento proporciona varios métodos para monitorear los eventos IPS.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en IPS 5.x y posteriores.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Métodos para supervisar los eventos IPS

Actualmente, hay cuatro opciones para monitorear los sensores:

1. IPS Manager Express (IME) está disponible en la descarga de software en Cisco.com. Esta

aplicación puede suscribirse de forma segura al sensor IPS con SDEE y recuperar los eventos/registros que se han generado como resultado de cualquier problema o firma que se haya disparado debido a una coincidencia.Se llama al administrador de dispositivos IPS (IDM) cuando se accede al sensor directamente a través de HTTPS.Vea el almacén de eventos directamente en el sensor con las herramientas IDM Monitoring o IME Event Monitoring. IDM y IME no son soluciones válidas si necesita almacenar los eventos a largo plazo, ya que el almacén de eventos local del sensor es un búfer circular de 30 MB y comienza a volverse a utilizar una vez que se alcanza el límite de 30 MB. Este límite no se puede configurar.

2. Utilice un dispositivo CS-MARS para extraer y correlacionar rutinariamente los eventos del sensor. CS-MARS utiliza el protocolo SDEE para establecer una conexión segura con el sensor para recuperar los eventos y recuperar nuevos eventos cada pocos segundos.Póngase en contacto con su equipo de cuentas/revendedor/SE para obtener más información si está interesado en la demostración del dispositivo CS-MARS.Para dispositivos Cisco IPS 5.x y 6.x, MARS extrae los registros con SDEE sobre SSL. Por lo tanto, MARS debe tener acceso HTTPS al sensor. Para preparar el sensor, debe permitir el tráfico HTTPS de la estación de administración IDM/IME y asegurarse de que la dirección IP de MARS se define como un host permitido en el sensor.

```
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. Supervise los eventos con IEV. IDS Event Viewer es una aplicación basada en Java que le permite ver y administrar alarmas para hasta cinco sensores. Con IDS Event Viewer puede conectarse y ver alarmas en tiempo real o en archivos de registro importados. Puede configurar filtros y vistas para ayudarle a gestionar las alarmas. También puede importar y exportar datos de eventos para realizar un análisis adicional. Al igual que MARS, IEV establece una conexión segura al sensor y recupera los eventos cada pocos segundos. El IEV almacena estos eventos en una base de datos del servidor en el que está instalado IEV. La base de datos se incluye con IEV y se instala junto con la aplicación. Haga clic en IEV para descargar.**Nota:** La documentación de IEV se encuentra a través del menú de ayuda después de instalarla. El readme contiene información de instalación.
4. Configure las firmas en su sensor para tener una acción de **request-snmp-trap** y configure el sensor para enviar las trampas a un servidor SNMP. A continuación, puede utilizar este servidor para retransmitir los mensajes como syslogs a otra máquina.SNMP es un protocolo de capa de aplicación que facilita el intercambio de información de administración entre los dispositivos de red. SNMP permite que los administradores de redes administren el rendimiento de la red, detecten y resuelvan problemas de red y planifiquen el crecimiento de la red.SNMP es un protocolo simple de solicitud/respuesta. El sistema de administración de redes emite una solicitud y los dispositivos administrados devuelven respuestas. Este comportamiento se implementa con el uso de una de cuatro operaciones de protocolo:GETGetNextSetTrampaPuede configurar el sensor para que sea monitoreado por SNMP. SNMP define una manera estándar para que las estaciones de administración de red monitoreen el estado y estado de muchos tipos de dispositivos, que incluye switches, routers y sensores.

Información Relacionada

- Sensores Cisco IPS de la serie 4200
- Cisco Intrusion Prevention System
- Avisos de campo de productos de seguridad (incluida CiscoSecure Intrusion Detection)
- Soporte Técnico y Documentación - Cisco Systems