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

Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Convenciones](#)
[Métodos de monitor los eventos IPS](#)
[Información Relacionada](#)

Introducción

Este documento proporciona los diversos métodos para monitorear los eventos IPS.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

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

Métodos de monitor los eventos IPS

Actualmente, hay cuatro opciones para monitorear los sensores:

1. El administrador IPS expreso (IME) es disponible desde descarga del software en el cisco.com. Esta aplicación puede inscribir con seguridad al sensor IPS con SDEE y extraer los eventos/los registros que se han generado como resultado de cualesquiera problemas o firma que hayan encendido debido a una coincidencia.Llaman el administrador de dispositivo IPS (IDM) cuando usted accede el sensor directamente con el HTTPS.Vea el almacén del evento directamente en el sensor con las herramientas de la supervisión IDM o del monitoreo de evento IME. El IDM e IME son soluciones inválidas si usted necesita salvar el largo plazo de los eventos pues el almacén del evento local del sensor es un buffer circular del 30 MB y comienza al overwite sí mismo que el límite del 30 MB se alcanza una vez. Este límite es no configurable.
2. Utilice un dispositivo CS-MARS para tirar y correlacionar rutinario de los eventos del sensor. El CS-MARS utiliza el protocolo SDEE para establecer una conexión segura al sensor para extraer los eventos y extrae los nuevos eventos cada pocos segundos.Entre en contacto su equipo de cuenta/reseller/SE para más información si usted está interesado en la versión parcial de programa-ing el dispositivo CS-MARS.Para los dispositivos 5.x y 6.x del IPS de Cisco, MARTE tira de los registros con SDEE sobre el SSL. Por lo tanto, MARTE debe tener acceso HTTPS al sensor. Para preparar el sensor, usted debe permitir el tráfico HTTPS de la estación de administración IDM/IME, y se aseegura que la dirección IP de MARTE esté definida como 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. Monitoree los eventos con el IEV. El IDS Event Viewer es una aplicación de la Java basada que le permite para ver y para manejar las alarmas para hasta cinco sensores. Con el usted puede conectarse del IDS Event Viewer a y las alarmas de la visión en el tiempo real o en los archivos del registro importados. Usted puede configurar los filtros y las opiniones para ayudarle a manejar las alarmas. Usted puede también importar y exportar los datos de evento para el análisis adicional. Como MARTE, el IEV establece una conexión segura al sensor y extrae los eventos cada pocos segundos. El IEV salva estos eventos en una base de datos en el servidor en el cual el IEV está instalado. El DB se incluye con el IEV y está instalado junto con la aplicación. Tecleo IEV para descargar.**Nota:** La documentación para el IEV se encuentra a través del menú de ayuda después de que usted lo instale. El readme contiene la información de la instalación.
4. Configure las firmas en su sensor para tener una acción del petición-SNMP-**desvío** y para configurar el sensor para enviar los desvíos a un servidor SNMP. Usted puede entonces utilizar este servidor para retransmitir los mensajes como Syslog a otra máquina.El SNMP es un Application Layer Protocol que facilita el intercambio de la información para administración entre los dispositivos de red. El SNMP permite a los administradores de la red para manejar el rendimiento de la red, hallazgo y para solucionar los problemas de red, y el plan para el crecimiento de la red.El SNMP es una petición simple/Response Protocol. El sistema de administración de red publica una petición, y los dispositivos administrados vuelven las respuestas. Este comportamiento se implementa con el uso de una de cuatro operaciones de protocolo:ConsigaGetNextSetTrampaUsted puede configurar el sensor para monitorear por el SNMP. El SNMP define a un modo estándar para que las estaciones de administración de red monitoreen la salud y el estatus de muchos tipos de dispositivos, que

incluye el Switches, el Routers, y los sensores.

Información Relacionada

- Sensores Cisco IPS de la serie 4200
- Cisco Intrusion Prevention System
- Field Notice de seguridad del producto (CiscoSecure Intrusion Detection incluyendo)
- Soporte Técnico y Documentación - Cisco Systems