IPS 5.x e mais tarde: Vários métodos de eventos da monitoração

Índice

Introdução

Este documento fornece vários métodos para monitorar os eventos IPS.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada em IPS 5.x e mais tarde.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Métodos do monitor os eventos IPS

Atualmente, há quatro opções para monitorar os sensores:

1. O gerente IPS expresso (IME) está disponível do download do software no cisco.com. Este aplicativo pode subscrever firmemente ao sensor IPS com SDEE e recuperar os eventos/logs que foram gerados em consequência de todas as edições ou assinaturas que atearem fogo a devido a um fósforo.O gerenciador de dispositivo IPS (IDM) é chamado quando você alcança o sensor diretamente com o HTTPS.Veja a loja do evento diretamente no sensor com as ferramentas da monitoração IDM ou do monitoramento de evento IME. O IDM e IME são soluções inválidas se você precisa de armazenar o prazo dos eventos porque a loja do evento local do sensor é um buffer circular do 30 MB e começa ao overwite próprio o limite do 30 MB é alcançado uma vez que. Este limite é não-configurável.
2. Use um dispositivo CS-MARS a fim puxar e correlacionar rotineiramente os eventos do sensor. O CS-MARS usa o protocolo SDEE a fim estabelecer uma conexão segura ao sensor para recuperar os eventos e recupera eventos novos cada poucos segundos.Contacte seu equipe de conta/reseller/SE para mais informação se você está interessado no programa demonstrativo-ing o dispositivo CS-MARS.Para os dispositivos 5.x e 6.x do ips Cisco, MARTE puxa os logs com o SDEE sobre o SSL. Consequentemente, MARTE deve ter o acesso HTTPS ao sensor. A fim preparar o sensor, você deve permitir o tráfego HTTPS da estação de gerenciamento IDM/IME, e certifica-se de que o endereço IP de Um ou Mais Servidores Cisco ICM NT de MARTE está definido como um host permitido no 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. Monitore os eventos com o IEV. O IDS Event Viewer é um aplicativo com base em Java que o permita de ver e controlar alarmes para até cinco sensores. Com IDS Event Viewer você pode conectar a e alarmes da vista no tempo real ou em arquivos de registro importados. Você pode configurar filtros e vistas para ajudá-lo a controlar os alarmes. Você pode igualmente importar e exportar dados de evento para a análise mais aprofundada. Como MARTE, o IEV estabelece uma conexão segura ao sensor e recupera eventos cada poucos segundos. O IEV armazena estes eventos em um base de dados no server em que o IEV é instalado. O DB é incluído com IEV e instalado junto com o aplicativo. Clique IEV a fim transferir.**Nota:** A documentação para o IEV está encontrada através do menu de ajuda depois que você o instala. O README contém a informação de instalação.
4. Configurar as assinaturas em seu sensor para ter uma ação da pedido-SNMP-**armadilha** e para configurar o sensor para enviar as armadilhas a um servidor SNMP. Você pode então usar este server para retransmitir as mensagens como Syslog a uma outra máquina.O SNMP é um protocolo de camada do aplicativo que facilite a troca de informação de gerenciamento entre dispositivos de rede. O SNMP permite administradores de rede de controlar o desempenho da rede, achado e de resolver problemas de rede, e plano para o crescimento de rede.O SNMP é um pedido/protocolo de resposta simples. O sistema de gerenciamento de rede emite um pedido, e os dispositivos gerenciado retornam respostas. Este comportamento é executado com o uso de uma de quatro operações do protocolo:ObtenhaGetNextConfiguradoArmadilhaVocê pode configurar o sensor para monitorar pelo SNMP. O SNMP define uma maneira padrão para que as estações de gerenciamento de rede monitorem a saúde e o estado de muitos tipos de dispositivos, que inclui o Switches, o Roteadores, e os sensores.

Informações Relacionadas

- Cisco IPS 4200 Series Sensors
- Cisco Intrusion Prevention System
- Field Notice de produto de segurança (que incluem a intrusion detection do CiscoSecure)
- Suporte Técnico e Documentação - Cisco Systems