IPS 5.x e versioni successive: Vari metodi di monitoraggio degli eventi

Sommario

Introduzione

In questo documento vengono illustrati vari metodi per monitorare gli eventi IPS.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano su IPS 5.x e versioni successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Metodi di monitoraggio degli eventi IPS

Attualmente, sono disponibili quattro opzioni per il monitoraggio dei sensori:

1. IPS Manager Express (IME) è disponibile per il download del software all'indirizzo Cisco.com. Questa applicazione è in grado di effettuare una sottoscrizione sicura al sensore IPS con SDEE e recuperare gli eventi/registri generati in seguito a problemi o firme generati a causa di una corrispondenza.IPS Device Manager (IDM) viene chiamato quando si accede al sensore direttamente tramite HTTPS.Visualizzare l'archivio eventi direttamente sul sensore con gli strumenti Monitoraggio IDM o Monitoraggio eventi IME. IDM e IME non sono soluzioni valide se è necessario memorizzare gli eventi a lungo termine in quanto l'archivio eventi locale del sensore è un buffer circolare da 30 MB e inizia a sovrascriversi una volta raggiunto il limite di 30 MB. Questo limite non è configurabile.
2. Usare un dispositivo CS-MARS per estrarre e correlare regolarmente gli eventi dal sensore. Il CS-MARS utilizza il protocollo SDEE per stabilire una connessione sicura al sensore per recuperare gli eventi e recuperare i nuovi eventi ogni pochi secondi.Per ulteriori informazioni, contattate il vostro account team/rivenditore/SE e siete interessati alla dimostrazione del dispositivo CS-MARS.Per i dispositivi Cisco IPS 5.x e 6.x, MARS estrae i log con SDE su SSL. Pertanto, MARS deve avere accesso HTTPS al sensore. Per preparare il sensore, è necessario consentire il traffico HTTPS dalla stazione di gestione IDM/IME e assicurarsi che l'indirizzo IP di MARS sia definito come host consentito sul sensore.

```
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. Monitorare gli eventi con l'IEV. IDS Event Viewer è un'applicazione basata su Java che consente di visualizzare e gestire gli allarmi per un massimo di cinque sensori. Con il Visualizzatore eventi IDS è possibile connettersi e visualizzare gli allarmi in tempo reale o nei file di registro importati. È possibile configurare filtri e visualizzazioni per semplificare la gestione degli allarmi. È inoltre possibile importare ed esportare i dati degli eventi per ulteriori analisi. Analogamente a MARS, IEV stabilisce una connessione sicura al sensore e recupera gli eventi ogni pochi secondi. IEV memorizza questi eventi in un database sul server in cui è installato IEV. Il database è incluso con IEV e installato insieme all'applicazione. Fare clic su IEV per eseguire il download.**Nota:** la documentazione relativa a IEV è disponibile tramite il menu della Guida dopo l'installazione. Il file Leggimi contiene informazioni sull'installazione.
4. Configurare le firme sul sensore in modo che esegua un'azione di **request-snmp-trap** e configurare il sensore in modo che invii le trap a un server SNMP. È quindi possibile utilizzare questo server per inoltrare i messaggi come syslog a un altro computer.L'SNMP è un protocollo a livello di applicazione che semplifica lo scambio di informazioni di gestione tra i dispositivi di rete. L'SNMP consente agli amministratori di gestire le prestazioni, individuare e risolvere problemi e pianificare la crescita della rete.L'SNMP è un protocollo di richiesta/risposta semplice. Il sistema di gestione della rete invia una richiesta e i dispositivi gestiti restituiscono risposte. Questo comportamento viene implementato tramite una delle quattro operazioni di protocollo seguenti:ScaricaOttieniSuccessivoImpostaTrapÈpossibile configurare il sensore per il monitoraggio tramite SNMP. L'SNMP definisce un modo standard per le stazioni di gestione della rete di monitorare lo stato e lo stato di molti tipi di dispositivi, tra cui switch, router e sensori.

Informazioni correlate

- Cisco IPS serie 4200 Sensori
- Cisco Intrusion Prevention System
- Avvisi sui prodotti per la sicurezza (incluso Cisco Secure Intrusion Detection)
- Documentazione e supporto tecnico – Cisco Systems