Gli eventi di connessione sembrano scomparire dal centro di gestione FireSIGHT

Sommario

Introduzione

Questo documento descrive come determinare la causa principale e risolvere il problema quando gli eventi di connessione scompaiono dal centro di gestione FireSIGHT dopo che il sistema è in esecuzione per diversi giorni. Ciò può verificarsi a causa delle impostazioni di configurazione del centro di gestione.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di FireSIGHT Management Center.

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni hardware e software:

- Centro di gestione FireSIGHT
- Software versione 5.2 o 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.

Risoluzione dei problemi

Passaggio 1: Determinare il numero di eventi memorizzati

Per determinare il numero di eventi di connessione memorizzati in un centro di gestione FireSIGHT,

a. Scegliere Analisi **>** Connessioni **>** Visualizzazione tabella degli eventi di connessione.
b. Espandere la Finestra temporale in un ampio intervallo che includa tutti gli eventi correnti, ad esempio 12 mesi.
c. Annotare il numero totale di righe nella parte inferiore della pagina. Fare clic sull'ultima pagina e annotare l'indicatore orario dell'ultimo evento di connessione disponibile.

Queste informazioni forniscono un'idea di quanti e per quanto tempo è possibile mantenere gli eventi di connessione con la configurazione corrente.

Passaggio 2: Determinare l'opzione di registrazione

Verificare quali connessioni vengono registrate e la posizione nel flusso in cui vengono registrate le connessioni. È consigliabile registrare le connessioni in base alle esigenze di sicurezza e conformità dell'organizzazione. Se si desidera limitare il numero di eventi generati, abilitare la registrazione solo per le regole critiche per l'analisi. Tuttavia, se si desidera una visualizzazione completa del traffico di rete, è possibile abilitare la registrazione per ulteriori regole di controllo di accesso o per l'azione predefinita. È possibile disattivare la registrazione delle connessioni per il traffico non essenziale in modo da conservare gli eventi di connessione per un periodo di tempo più lungo.

Suggerimento: per ottimizzare le prestazioni, Cisco consiglia di registrare l'inizio o la fine della connessione, ma non entrambi.

Nota: per una singola connessione, l'evento di fine connessione contiene tutte le informazioni dell'evento di inizio connessione, nonché le informazioni raccolte nel corso della sessione. Per le regole Trust e Allow, è consigliabile utilizzare End-of-Connection.

In questo grafico vengono illustrate le diverse opzioni di registrazione disponibili per ciascuna azione regola:

Azione regola o opzione di registrazione	Registra all'inizio	Registra alla fine
Trust (Considera attendibile) Azione predefinita: Trust	X	X
Allow (Autorizza) Azione predefinita: Intrusione	X	X

Azione predefinita: Individuazione		
Monitor (Monitora)		X (Obbligatorio)
Block (Blocca)		
Block with reset (Blocca con reset)	X	
Azione predefinita: Blocca		
Interactive Block (Blocco interattivo)	X	X (se ignorato)
Interactive Block with reset (Blocco interattivo e reset)		
Security Intelligence	X	

Passaggio 3: Regolare le dimensioni del database delle connessioni

Gli eventi di connessione vengono eliminati a seconda dell'impostazione Numero massimo di eventi di connessione nel criterio di sistema. Per modificare l'impostazione:

a. Scegliete Sistema > Locale > Criteri di sistema.
b. Per modificare il criterio applicato, fare clic sull'icona a forma di matita.
c. Scegliere Database > Database connessioni > Numero massimo di eventi di connessione.
d. Modificare il valore per Numero massimo di eventi di connessione.
e. Fare clic su Salva criterio ed esci, quindi su Applica il criterio agli accessori.

La quantità massima di eventi di connessione che è possibile archiviare dipende dal modello di Centro gestione:

Nota: il limite massimo di eventi è condiviso tra gli eventi di connessione e gli eventi di Security Intelligence. La somma dei valori massimi configurati per i due eventi non può superare il limite massimo di eventi.

Modello di Management Center	Numero massimo di eventi
FS750, DC750	50 milioni
FS1500, DC1500	100 milioni
FS2000	300 milioni
FS3500, DC3500	500 milioni
FS4000	1 miliardo
Appliance virtuale	10 milioni

Attenzione: un aumento dei limiti del database può avere un impatto negativo sulle prestazioni del dispositivo. Per migliorare le prestazioni, è necessario personalizzare i limiti degli eventi in base al numero di eventi con cui si lavora regolarmente.

Per i widget che visualizzano il conteggio degli eventi in un intervallo di tempo, il numero totale di eventi potrebbe non riflettere il numero di eventi per i quali sono disponibili dati dettagliati nel visualizzatore eventi. Ciò si verifica perché talvolta il sistema elimina i dettagli degli eventi meno recenti per gestire l'utilizzo dello spazio su disco. Per ridurre al minimo l'occorrenza dell'eliminazione dei dettagli degli eventi, è possibile ottimizzare la registrazione degli eventi in modo da registrare solo gli eventi più importanti per la distribuzione.

Informazioni correlate

- Configurazione dei limiti degli eventi del database
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).