Los eventos de conexión parecen desaparecer de FireSIGHT Management Center

Contenido

Introducción

Este documento describe cómo determinar la causa raíz y solucionar el problema cuando los eventos de conexión desaparecen de FireSIGHT Management Center después de que el sistema se ejecute durante varios días. Esto puede ocurrir debido a los parámetros de configuración del centro de administración.

Prerequisites

Requirements

Cisco recomienda que conozca FireSIGHT Management Center.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software y hardware.

- Centro de administración de FireSIGHT
- Software versión 5.2 o 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). If your network is live, make sure that you understand the potential impact of any command.

Troubleshoot

Paso 1: Determinar el número de eventos almacenados

Para determinar el número de eventos de conexión que se almacenan en un FireSIGHT Management Center,

1. Elija **Analysis > Connections > Table View of Connection Events**.
2. Amplíe la ventana de tiempo a un amplio rango que abarque todos los eventos actuales, por ejemplo 12 meses.
3. Observe el número total de filas en la parte inferior de la página. Haga clic en la última página y observe la marca de tiempo del último evento de conexión disponible.

Esta información le da una idea de cuántos y durante cuánto tiempo puede conservar los eventos de conexión con su configuración actual.

Paso 2: Determinación de la opción de registro

Revise qué conexiones se registran y en qué parte del flujo se registran las conexiones. Debe registrar las conexiones de acuerdo con las necesidades de seguridad y cumplimiento de normativas de su organización. Si su objetivo es limitar el número de eventos que genera, active únicamente el registro de las reglas críticas para su análisis. Sin embargo, si desea tener una visión amplia del tráfico de red, puede habilitar el registro para reglas de control de acceso adicionales o para la acción predeterminada. Puede inhabilitar el registro de conexiones para el tráfico no esencial para ayudar a retener los eventos de conexión durante un período más largo de tiempo.

> **Sugerencia**: para optimizar el rendimiento, Cisco recomienda registrar el inicio o el final de la conexión, pero no ambos.

> **Nota**: Para una única conexión, el evento de fin de conexión contiene toda la información del evento de inicio de conexión, así como la información recopilada durante la sesión. Para las reglas Trust y Allow, se recomienda utilizar End-of-Connection (Fin de conexión).

Este gráfico explica las diferentes opciones de registro disponibles para cada acción de regla:

Acción de regla u Opción de registro	Registro al principio	Registro al final
Confianza Acción predeterminada: Trust	X	X
Permiso Acción predeterminada: intrusión	X	X
Acción predeterminada: detección Monitor		X (obligatorio)
Bloqueo Bloqueo con restablecimiento Acción predeterminada: Block	X	
Bloqueo interactivo Bloqueo interactivo con restablecimiento	X	X (Si se omite)

Paso 3: Ajustar el tamaño de la base de datos de conexión

Los eventos de conexión se recortan en función de la configuración Eventos de conexión máximos de la directiva del sistema. Para cambiar la configuración:

1. Elija **System > Local > System Policy**.
2. Haga clic en el icono del *lápiz* para editar la política aplicada actualmente.
3. Elija **Database > Connection Database > Maximum Connection Events**.
4. Cambie el valor de **Maximum Connection Events**.
5. Haga clic en **Save Policy and Exit** y, a continuación, en **Apply** policy to your appliances.

La cantidad máxima de eventos de conexión que se pueden almacenar depende del modelo de Management Center:

> **Nota**: el límite máximo de eventos se comparte entre los eventos de conexión y los eventos de inteligencia de seguridad; la suma de los máximos configurados para los dos eventos no puede superar el límite máximo de eventos.

Modelo de Management Center	Número máximo de eventos
FS750 y DC750	50 millones
FS1500 y DC1500	100 millones
FS2000	300 millones
FS3500 y DC3500	500 millones
FS4000	1000 millones
Dispositivo virtual	10 millones

> **Precaución**: un aumento en los límites de la base de datos puede tener un impacto negativo en el rendimiento del dispositivo. Para mejorar el rendimiento, debe adaptar los límites de eventos al número de eventos con los que trabaja habitualmente.

Para los widgets que muestran recuentos de eventos en un intervalo de tiempo, es posible que el número total de eventos no refleje el número de eventos para los que hay datos detallados disponibles en el visor de eventos. Esto ocurre porque el sistema a veces recorta detalles de eventos anteriores para administrar el uso del espacio en disco. Para minimizar la aparición del recorte de detalles de eventos, puede ajustar el registro de eventos para registrar sólo los eventos más importantes para su implementación.

Información Relacionada

- Configuración de Límites de Eventos de Base de Datos
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).