TAC

ID del Documento: 118012

Actualizado: Mayo 20, 2015

Contribuido por Nazmul Rajib, ingeniero de Cisco TAC.

Descarga PDF
Imprimir
[+] Feedback

Productos Relacionados

- Centro de administración 750 de Cisco FireSIGHT
- Centro de administración 3500 de Cisco FireSIGHT
- Centro de administración 1500 de Cisco FireSIGHT
- Centro de administración de Cisco FireSIGHT
- Dispositivo virtual del centro de administración de Cisco FireSIGHT

Contenido

Introducción

Este documento describe cómo determinar la causa raíz y resolver problemas el problema cuando los eventos de conexión desaparecen del centro de administración de FireSIGHT después de que el sistema se ejecute por varios días. Puede ser que suceda debido a los ajustes de la configuración del centro de administración.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento del centro de administración de FireSIGHT.

Componentes Utilizados

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

- Centro de administración de FireSIGHT
- Versión de software 5.2 o más adelante

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.

Troubleshooting

Paso 1: Determine el número de eventos salvados

Para determinar el número de eventos de conexión que se salvan en un centro de administración de FireSIGHT,

1. Elija el **análisis > las conexiones > la opinión de la tabla de los eventos de conexión**.
2. Amplíe la ventana de fecha y hora a una amplia gama 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 la página más reciente y observe el sello de fecha/hora del evento de conexión disponible más reciente.

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

Paso 2: Determine la opción de registro

Revise se están registrando qué conexiones, y donde en el flujo que las conexiones están registradas. Usted debe registrar las conexiones de acuerdo con las necesidades de la Seguridad y de la conformidad de su organización. Si su meta es limitar el número de eventos que usted genera, sólo registro del permiso para las reglas críticas a su análisis. Sin embargo, si usted quiere una visión de conjunto de su tráfico de la red, usted puede habilitar el registro para las reglas adicionales del control de acceso o para la acción predeterminada. Usted puede inhabilitar el registro de la conexión para el tráfico no esencial para ayudar a conservar los eventos de conexión por un período de tiempo más largo.

> Consejo: Para optimizar el funcionamiento, Cisco recomienda que usted registra el principio o el extremo de la conexión, pero no ambos.

Nota: Para una sola conexión, el evento de la fin-de-conexión contiene toda la información en el evento de la principio-de-conexión así como la información que fue recopilada sobre la duración de la sesión. Para la confianza y permita las reglas, él se recomienda que la Fin-de-conexión está utilizada.

Esta carta explica las diversas opciones de registro disponibles para cada acción de la regla:

Acción o opción de registro de la regla	Registro al principio	Registro en el extremo
Confianza Acción predeterminada: Confianza	X	X
Permita Acción predeterminada: Intrusión	X	X
Acción predeterminada: Detección Monitor		X (requerido)
Bloque Bloque con la restauración	X	
Acción de Defaut: Bloque Bloque interactivo Bloque interactivo con la restauración	X	X (si está desviado)
Inteligencia de Seguridad	X	

Paso 3: Ajuste el tamaño de la base de datos de conexiones

Los eventos de conexión son dependiente podado sobre los eventos de la cantidad máxima de conexiones que fijan en la política del sistema. Para cambiar la configuración:

1. Elija el **sistema > el Local > la política del sistema**.
2. Haga clic el icono del *lápiz* para editar la directiva actualmente aplicada.
3. Elija los **eventos de la base de datos > de la base de datos de conexiones > de la cantidad máxima de conexiones**.
4. Cambie el valor para los **eventos de la cantidad máxima de conexiones**.
5. Haga clic la **directiva y la salida de la salvaguardia**, y después **aplique la** directiva a sus dispositivos.

La cantidad máxima de eventos de conexión que puedan ser salvados depende del modelo del centro de administración:

Nota: El límite del evento máximo se comparte entre los eventos de conexión y los eventos de la inteligencia de Seguridad; la suma de Máximos configurados para los dos eventos no puede exceder el límite del evento máximo.

Modelo del centro de administración	Número máximo de eventos
FS750, DC750	50 millones
FS1500, DC1500	100 millones
FS2000	300 millones
FS3500, DC3500	500 millones
FS4000	1 mil millones
Dispositivo virtual	10 millones

Precaución: Un aumento en los límites de la base de datos puede tener un impacto del

rendimiento adverso en el dispositivo. Para mejorar el funcionamiento, usted debe adaptar los límites del evento al número de eventos que usted trabaja regularmente con.

Para los aparatos que visualizan las cuentas de evento sobre un rango de tiempo, el número total de eventos no pudo reflejar el número de eventos para los cuales los datos detallados están disponibles en el visor de eventos. Esto ocurre porque el sistema poda a veces más viejos detalles del evento para manejar el uso del espacio en disco. Para minimizar el acontecimiento de la poda del detalle del evento, usted puede ajustar el registro de evento para registrar solamente esos eventos más importantes para su despliegue.

Información Relacionada

- Configurar los límites del evento de la base de datos
- Soporte Técnico y Documentación - Cisco Systems

Discusiones relacionadas de la comunidad del soporte de Cisco

La comunidad del soporte de Cisco es un foro para que usted haga y conteste a las preguntas, las sugerencias de la parte, y colabora con sus pares.

Refiera a los convenios de los consejos técnicos de Cisco para la información sobre los convenios usados en este documento.

Actualizado: Mayo 20, 2015
ID del Documento: 118012