Os eventos de conexão parecem desaparecer do FireSIGHT Management Center

Contents

Introduction

Este documento descreve como determinar a causa raiz e solucionar o problema quando os eventos de conexão desaparecem do FireSIGHT Management Center após a execução do sistema por vários dias. Isso pode acontecer devido às definições de configuração do centro de gerenciamento.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento do FireSIGHT Management Center.

Componentes Utilizados

As informações neste documento são baseadas nas seguintes versões de hardware e software:

- FireSIGHT Management Center
- Versão do software 5.2 ou posterior

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Troubleshoot

Passo 1: Determine o número de eventos armazenados

Para determinar o número de eventos do Connection armazenados em um FireSIGHT Management Center,

1. Escolha **Analysis > Connections > Table View of Connection Events**.
2. Expanda a Janela de Tempo para uma ampla faixa que inclua todos os eventos atuais, por exemplo, 12 meses.
3. Observe o número total de linhas na parte inferior da página. Clique na última página e anote o carimbo de data/hora do último Evento de Conexão disponível.

Essas informações dão uma ideia de quantos e por quanto tempo você pode reter Eventos do Connection com sua configuração atual.

Passo 2: Determine a opção de registro

Revise quais conexões estão sendo registradas e onde no fluxo essas conexões estão registradas. Você deve registrar conexões de acordo com as necessidades de segurança e conformidade da sua organização. Se o objetivo for limitar o número de eventos gerados, ative o registro somente para as regras críticas para a análise. No entanto, se desejar uma visão ampla do tráfego de rede, você poderá ativar o registro para regras de controle de acesso adicionais ou para a ação padrão. Você pode desabilitar o Registro de Conexão para tráfego não essencial para ajudar a reter Eventos de Conexão por um período de tempo maior.

> **Tip**: Para otimizar o desempenho, a Cisco recomenda que você registre o início ou o fim da conexão, mas não ambos.

> **Note**: Para uma única conexão, o evento de fim da conexão contém todas as informações do evento de início da conexão, bem como informações que foram coletadas durante a sessão. Para regras de Confiança e Permissão, é recomendável usar End-of-Connection.

Este gráfico explica as diferentes opções de log disponíveis para cada Ação de Regra:

Ação de regra ou opção de registro	Registrar no início	Registrar no fim
Confiança Ação padrão: Confiança	X	X
Permissão Ação padrão: Intrusão	X	X
Ação padrão: Descoberta Monitor		X (Obrigatório)
Bloqueio Bloqueio com reinicialização	X	
Ação padrão: Bloqueio Bloqueio interativo Bloqueio interativo com reinicialização	X	X (Se Ignorado)
Inteligência de segurança	X	

Passo 3: Ajustar o Tamanho do Banco de Dados do Connection

Os eventos de conexão são removidos dependendo da configuração de Máximo de Eventos de Conexão na política do sistema. Para alterar a configuração:

1. Escolha **System > Local > System** Policy.
2. Clique no ícone do *lápis* para editar a política aplicada atualmente.
3. Escolha **Banco de Dados > Banco de Dados de Conexão > Máximo de Eventos de Conexão**.
4. Altere o valor de **Máximo de Eventos de Conexão**.
5. Clique em **Save Policy and Exit** (Salvar política e sair) e em **Apply** (**Aplicar** a política aos seus aplicativos).

A quantidade máxima de Eventos de Conexão que pode ser armazenada depende do modelo do Centro de Gerenciamento:

> **Note**: O limite máximo de eventos é compartilhado entre eventos de conexão e eventos de inteligência de segurança; a soma dos máximos configurados para os dois eventos não pode exceder o limite máximo de eventos.

Modelo do Management Center	Número máximo de eventos
FS750, DC750	50 milhões
FS1500, DC1500	100 milhões
FS2000	300 milhões
FS3500, DC3500	500 milhões
FS4000	1 bilhão
Dispositivo virtual	10 milhões

> **Caution**: Um aumento nos limites do banco de dados pode ter um impacto negativo no desempenho do dispositivo. Para melhorar o desempenho, você deve ajustar os limites de eventos ao número de eventos com os quais trabalha regularmente.

Para widgets que exibem contagens de eventos ao longo de um intervalo de tempo, o número total de eventos pode não refletir o número de eventos para os quais dados detalhados estão disponíveis no visualizador de eventos. Isso ocorre porque o sistema às vezes remove detalhes de eventos mais antigos para gerenciar o uso do espaço em disco. Para minimizar a ocorrência de remoção de detalhes de eventos, você pode ajustar o registro de eventos para registrar somente os eventos mais importantes para sua implantação.

Informações Relacionadas

- Configurando Limites de Eventos de Banco de Dados
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.