ID do Documento: 118012

Atualizado em: maio 20, 2015

Contribuído por Nazmul Rajib, engenheiro de TAC da Cisco.

Transferência PDF
Imprimir
[+] Feedback

Produtos Relacionados

- Centro de gerenciamento 750 de Cisco FireSIGHT
- Centro de gerenciamento 3500 de Cisco FireSIGHT
- Centro de gerenciamento 1500 de Cisco FireSIGHT
- Centro de gerenciamento de Cisco FireSIGHT
- Dispositivo virtual do centro de gerenciamento de Cisco FireSIGHT

Índice

Introdução

Este documento descreve como determinar a causa de raiz e pesquisar defeitos a edição quando os eventos de conexão desaparecem do centro de gerenciamento de FireSIGHT depois que o sistema é executado por vários dias. Pôde acontecer devido aos ajustes de configuração do centro de gerenciamento.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento do centro de gerenciamento de FireSIGHT.

Componentes Utilizados

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

- Centro de gerenciamento de FireSIGHT
- Versão de software 5.2 ou mais atrasado

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Troubleshooting

Passo 1: Determine o número de eventos armazenados

A fim determinar o número de eventos de conexão que são armazenados em um centro de gerenciamento de FireSIGHT,

1. Escolha a **análise > as conexões > a ideia da tabela dos eventos de conexão**.
2. Expanda a janela de horário a um amplo intervalo que abranja todos os eventos atual, por exemplo 12 meses.
3. Note o número total de fileiras na parte inferior da página. Clique a última página e note o selo de tempo do último evento de conexão disponível.

Esta informação dá-lhe uma ideia de quanto e de quanto tempo você pode reter eventos de conexão com sua configuração atual.

Passo 2: Determine a opção de registro

Reveja que conexões estão sendo registradas, e onde no fluxo que as conexões estão registradas. Você deve registrar conexões de acordo com as necessidades da Segurança e da conformidade de sua organização. Se seu objetivo é limitar o número de eventos que você gera, simplesmente permita o registo para as regras críticas a sua análise. Contudo, se você quer uma ideia larga de seu tráfego de rede, você pode permitir o registo para regras adicionais do controle de acesso ou para a ação padrão. Você pode desabilitar a conexão que registra para o tráfego NON-essencial a fim ajudar a reter eventos de conexão por um período de tempo mais longo.

> Dica: A fim aperfeiçoar o desempenho, Cisco recomenda que você registra o começo ou a extremidade da conexão, mas não ambos.

> Nota: Para uma conexão única, o evento da fim--conexão contém toda a informação no

evento da começo--conexão assim como informação que foi recolhida sobre a duração da sessão. Para a confiança e permita regras, ele é recomendado que a Fim--conexão está usada.

Esta carta explica as opções de registro diferentes disponíveis para cada ação da regra:

Ação ou opção de registro da regra	Log no começo	Log na extremidade
Confiança Ação padrão: Confiança	X	X
Reserve Ação padrão: Intrusão	X	X
Ação padrão: Descoberta Monitor		X (exigido)
Bloco Bloco com restauração	X	
Ação de Defaut: Bloco Bloco interativo Bloco interativo com restauração	X	X (se contorneado)
Inteligência de Segurança	X	

Passo 3: Ajuste o tamanho da base de dados de conexão

Os eventos de conexão são dependente podado em cima dos eventos da conexão máxima que ajustam-se na política de sistema. A fim mudar o ajuste:

1. Escolha o **sistema > o Local > a política de sistema**.
2. Clique o ícone do *lápis* a fim editar a política atualmente aplicada.
3. Escolha **eventos do banco de dados > da base de dados de conexão > da conexão máxima**.
4. Mude o valor para **eventos da conexão máxima**.
5. Clique a **política e a saída da salvaguarda**, e **aplique** então a política a seus dispositivos.

A quantidade máxima de eventos de conexão que podem ser armazenados depende do modelo do centro de gerenciamento:

Nota: O limite máximo do evento é compartilhado entre eventos de conexão e eventos da inteligência de Segurança; a soma das máximas configuradas para os dois eventos não pode exceder o limite máximo do evento.

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

Cuidado: Um aumento nos limites do banco de dados pode ter um impacto no desempenho adverso no dispositivo. A fim melhorar o desempenho, você deve costurar limites do evento ao número de eventos que você trabalha regularmente com.

Para os widgets que indicam contagens de evento sobre um intervalo de tempo, o número total de eventos não pôde refletir o número de eventos para que os dados detalhados estão disponíveis no visualizador de eventos. Isto ocorre porque o sistema poda às vezes uns detalhes mais velhos do evento para controlar o uso do espaço de disco. A fim minimizar a ocorrência do detalhe do evento que poda, você pode ajustar o logging de evento para registrar somente aqueles eventos os mais importantes para seu desenvolvimento.

Informações Relacionadas

- Configurando limites do evento do banco de dados
- Suporte Técnico e Documentação - Cisco Systems

Cisco relacionado apoia discussões da comunidade

Cisco apoia a comunidade é um fórum para que você faça e responda a perguntas, sugestões da parte, e colabora com seus pares.

Refira convenções dos dicas técnicas da Cisco para obter informações sobre das convenções usadas neste documento.

Atualizado em: maio 20, 2015
ID do Documento: 118012