Anscheinend verschwinden Verbindungsereignisse aus dem FireSIGHT Management Center

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die Ursache ermitteln und das Problem beheben, wenn Verbindungsereignisse im FireSIGHT Management Center nach mehrtägiger Ausführung des Systems nicht mehr auftreten. Dies kann durch die Konfigurationseinstellungen des Management Centers verursacht werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse des FireSIGHT Management Center verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Hardware- und Software-Versionen:

- FireSIGHT Management Center
- Softwareversion 5.2 oder höher

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer

gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Fehlerbehebung

Schritt 1: Bestimmen der Anzahl gespeicherter Ereignisse

Um die Anzahl der Verbindungsereignisse zu bestimmen, die in einem FireSIGHT Management Center gespeichert werden,

1. Wählen Sie **Analyse > Verbindungen > Tabellenansicht der Verbindungsereignisse**.
2. Erweitern Sie das Zeitfenster auf einen weiten Bereich, der alle aktuellen Ereignisse umfasst, z. B. 12 Monate.
3. Beachten Sie die Gesamtzahl der Zeilen am unteren Seitenrand. Klicken Sie auf die letzte Seite, und notieren Sie sich den Zeitstempel des letzten verfügbaren Verbindungsereignisses.

Anhand dieser Informationen können Sie ermitteln, wie viele und wie lange Sie Verbindungsereignisse mit Ihrer aktuellen Konfiguration beibehalten können.

Schritt 2: Bestimmen der Protokollierungsoption

Überprüfen Sie, welche Verbindungen protokolliert werden und wo im Datenfluss diese Verbindungen protokolliert werden. Sie sollten Verbindungen entsprechend den Sicherheits- und Compliance-Anforderungen Ihres Unternehmens protokollieren. Wenn Sie die Anzahl der von Ihnen generierten Ereignisse begrenzen möchten, aktivieren Sie die Protokollierung nur für die Regeln, die für Ihre Analyse wichtig sind. Wenn Sie jedoch eine umfassende Ansicht des Netzwerkverkehrs benötigen, können Sie die Protokollierung für zusätzliche Zugriffskontrollregeln oder für die Standardaktion aktivieren. Sie können die Verbindungsprotokollierung für nicht wichtigen Datenverkehr deaktivieren, um Verbindungsereignisse für einen längeren Zeitraum zu speichern.

> **Tipp:** Zur Leistungsoptimierung empfiehlt Cisco, entweder den Beginn oder das Ende der Verbindung zu protokollieren, jedoch nicht beides.

> **Hinweis**: Bei einer einzelnen Verbindung enthält das End-of-Connection-Ereignis alle Informationen des Beginns der Verbindung sowie Informationen, die während der Sitzung gesammelt wurden. Für Trust and Allow-Regeln wird empfohlen, End-of-Connection zu verwenden.

In diesem Diagramm werden die verschiedenen Protokollierungsoptionen erläutert, die für jede Regelaktion verfügbar sind:

Regelaktion oder Protokolloption	Zu Beginn protokollieren	Am Ende protokollieren
Vertrauen Standardaktion: Vertrauen	X	X
Zulassen	X	X

Standardaktion: Eindringen		
Standardaktion: Erkennung		
Überwachen		X (erforderlich)
Blockieren		
Blockieren mit Zurücksetzen	X	
Standardaktion: Sperren		
Interaktiver Block	X	X (bei Umgehung)
Interaktiver Block mit Zurücksetzen		
Sicherheitsinformationen	X	

Schritt 3: Anpassen der Größe der Verbindungsdatenbank

Verbindungsereignisse werden in Abhängigkeit von der Einstellung Maximale Verbindungsereignisse in der Systemrichtlinie bereinigt. So ändern Sie die Einstellung:

1. Wählen Sie **System > Local > System Policy**.
2. Klicken Sie auf das *Bleistiftsymbol*, um die aktuell angewendete Richtlinie zu bearbeiten.
3. Wählen Sie **Datenbank > Verbindungsdatenbank > Maximale Verbindungsereignisse aus**.
4. Ändern Sie den Wert für **Maximum Connection Events (Maximale Verbindungsereignisse)**.
5. Klicken Sie auf **Richtlinie speichern und beenden**, und **wenden Sie** dann die Richtlinie auf Ihre Appliances an.

Die maximale Anzahl von Verbindungsereignissen, die gespeichert werden können, hängt vom Management Center-Modell ab:

> **Hinweis**: Der maximale Ereignisgrenzwert wird auf Verbindungsereignisse und Sicherheitsinformationsereignisse aufgeteilt. Die Summe der konfigurierten Höchstwerte für die beiden Ereignisse darf den maximalen Ereignisgrenzwert nicht überschreiten.

Management Center-Modell	Maximale Anzahl Ereignisse
FS750, DC750	50 Mio.
FS 1500, DC 1500	100 Mio.
FS2000	300 Mio.
FS 3500, DC 3500	500 Mio.
FS4000	1 Milliarde
Virtuelle Appliance	10 Mio.

> **Vorsicht**: Eine Erhöhung der Datenbankgrenzwerte kann sich negativ auf die Leistung des Geräts auswirken. Um die Leistung zu verbessern, sollten Sie die Ereignislimits an die Anzahl der Ereignisse anpassen, mit denen Sie regelmäßig zusammenarbeiten.

Bei Widgets, die Ereigniszählungen über einen Zeitraum anzeigen, spiegelt die Gesamtzahl der Ereignisse möglicherweise nicht die Anzahl der Ereignisse wider, für die in der Ereignisanzeige detaillierte Daten verfügbar sind. Dies liegt daran, dass das System manchmal ältere Ereignisdetails bereinigt, um die Nutzung des Festplattenspeichers zu verwalten. Um das Auftreten von Ereignisdetailbereinigungen zu minimieren, können Sie die Ereignisprotokollierung so optimieren, dass nur die Ereignisse protokolliert werden, die für Ihre Bereitstellung am wichtigsten sind.

Zugehörige Informationen

- Grenzwerte für Datenbankereignisse konfigurieren
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.