接続イベントが FireSIGHT Management Center から消えたように見える

内容

概要

このドキュメントでは、システムを数日間実行すると、接続イベントが FireSight Management Center から消える問題の根本原因を判別してトラブルシュートする方法について説明します。これは、Management Center の設定が原因で発生する可能性があります。

前提条件

要件

FireSIGHT Management Centerに関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、次のハードウェアとソフトウェアのバージョンに基づいています。

- FireSIGHT 管理センター
- ソフトウェア バージョン 5.2 以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

トラブルシュート

ステップ 1：保存されたイベントの数の決定

FireSIGHT Management Centerに保存されている接続イベントの数を確認するには、

1. [Analysis] > [Connections] > [Table View of Connection Events] を選択します。
2. タイムウィンドウを拡張して、現在のすべてのイベント（12ヵ月など）を含む広い範囲を表示します。
3. ページの下部にある行の総数を確認します。最後のページをクリックし、使用可能な最後の接続イベントのタイムスタンプをメモします。

この情報から、現在の設定で接続イベントを保持できる数と時間がわかります。

ステップ 2：ロギングオプションの決定

記録されている接続と、接続が記録されているフロー内の場所を確認します。接続は、組織のセキュリティとコンプライアンスのニーズに従ってログに記録する必要があります。生成するイベントの数を制限する場合は、分析に重要なルールのロギングのみを有効にします。ただし、ネットワークトラフィックを幅広く表示する必要がある場合は、追加のアクセスコントロールルールまたはデフォルトアクションに対してロギングを有効にできます。接続イベントをより長い期間にわたって保持するために、不要なトラフィックの接続ロギングを無効にすることができます。

> **ヒント**：パフォーマンスを最適化するために、接続の開始または終了のいずれかをログに記録し、両方はログに記録しないことを推奨します。

> **注**：単一の接続の場合、接続の終了イベントには、接続の開始イベントのすべての情報と、セッションの間に収集された情報が含まれます。TrustルールとAllowルールでは、End-of-Connectionを使用することを推奨します。

次の表に、各ルールアクションで使用できるさまざまなログオプションを示します。

ルールアクションまたはロギングオプション	開始時にログ	終了時にログ
信頼性 デフォルトのアクション：信頼性	X	X
プライベート ネットワーク間で デフォルトのアクション：侵入	X	X
デフォルトのアクション：ディスカバリ モニタ		X（必須）
Block		
Block with reset	X	
既定のアクション：Block		
インタラクティブブロック リセット付きインタラクティブ ブロック	X	X（バイパスされた場合）
セキュリティインテリジェンス	X	

ステップ 3：接続データベースのサイズの調整

接続イベントは、システムポリシーの[Maximum Connection Events]設定に応じてプルーニングされます。設定を変更するには、次の手順を実行します。

1. **System > Local > System Policy**の順に選択します。
2. 現在適用されているポリシーを編集するには、*鉛筆*アイコンをクリックします。
3. [Database] > [Connection Database] > [Maximum Connection Events] を選択します。
4. [Maximum Connection Events] の値を変更します。
5. **Save Policy and Exit**をクリックし、次に**Apply**をアプライアンスに適用します。

保存できる接続イベントの最大量は、Management Centerモデルによって異なります。

> **注**：イベントの最大数は、接続イベントとセキュリティインテリジェンスイベントで共有されます。2つのイベントに設定されている最大値の合計は、イベントの最大値の制限を超えることはできません。

Management Centerモデル	イベントの最大数
FS750、DC750	5,000万
FS1500、DC1500	1億
FS2000	3億
FS3500、DC3500	5億
FS4000	10億
仮想アプライアンス	1,000万

> **注意**：データベースの制限が増加すると、デバイスのパフォーマンスに悪影響が及ぶ可能性があります。パフォーマンスを向上させるには、定期的に作業するイベント数に合わせてイベント制限を調整する必要があります。

時間範囲のイベント数を表示するウィジェットの場合、イベントの合計数は、イベントビューアで詳細データを利用できるイベントの数を反映していない可能性があります。これは、ディスク領域の使用状況を管理するために、システムが古いイベントの詳細をプルーニングする場合があるためです。イベント詳細プルーニングの発生を最小限に抑えるために、イベントログを微調整して、展開にとって最も重要なイベントのみをログに記録することができます。

関連情報

- データベース・イベント制限の構成
- テクニカル サポートとドキュメント – Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。