TAC

Document ID: 118012

Updated: 2015 年 5月 20 日

著者：Cisco TAC エンジニア、Nazmul Rajib

PDF のダウンロード
印刷
[+] フィードバック

関連製品

- Cisco FireSIGHT Management Center 750
- Cisco FireSIGHT Management Center 3500
- Cisco FireSIGHT Management Center 1500
- Cisco FireSIGHT Management Center
- Cisco FireSIGHT Management Center 仮想アプライアンス

目次

概要

システムが数日間稼動した後接続イベントが FireSIGHT Management Center から消えるときこの資料に根本的な原因を判別し問題を解決する方法を記述されています。 それは管理センターのコンフィギュレーションの設定が原因で起こるかもしれません。

前提条件

要件

Cisco は FireSIGHT Management Center のナレッジがあることを推奨します。

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くものです。

- 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たものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

トラブルシューティング

ステップ 1： 保存されたイベントの数を判別して下さい

FireSIGHT Management Center で保存される接続イベントの数を判別するため、

1. **分析 > 接続 > 接続イベントのテーブル ビュー**を選択して下さい。
2. すべての発生したイベントを取囲む広範囲に時間 の ウィンドウを、たとえば 12 か月拡張して下さい。
3. ページの一番下に行の総数に注意して下さい。 最後のページをクリックし、最後の利用可能 な 接続イベントのタイムスタンプに注意して下さい。

この情報は現在のコンフィギュレーションを用いる接続イベントを保てるどの位のか何、そしてか概念を提供します。

ステップ 2： ロギング オプションを判別して下さい

接続は記録 されることどの接続が記録 されて いる、そしてところでフローかで検討して下さい。 組織のセキュリティおよび準拠性必要に従って接続を記録 する必要があります。 目標が生成するイベントの数を制限することなら、分析に重要なルールのために記録 する イネーブル。 ただし、ネットワークトラフィックの広い見解がほしいと思えば、追加アクセスコントロール ルールまたはデフォルト アクションのための口ギングを有効に することができます。 より長いある一定の時間のための接続イベントを保つのを助けるために非本質的なトラフィックのための接続口ギングをディセーブル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、Cisco は接続の始まりか端を記録 する、両方ことを推奨しません。

> **注** 単一の接続に関しては、終りの接続イベントはセッションの期間にわたって収集された始まりの接続イベントで情報が、また情報すべてが含まれています。 信頼および割り当て

ルールに関しては、終りの接続が使用されることが推奨されます。

この図は各ルール処理のために利用可能 な異なる口ギング オプションを説明します:

ルール処理かロギング オプション	始まりのログ	端にログ
信頼 デフォルト アクション: 信頼	X	X
プライベート ネットワーク間で デフォルト アクション: 不正侵入	X	X
デフォルト アクション: ディスカバリ モニタ		X（必要とされる）
ブロック リセットのブロック	X	
Defaut 処理: ブロック 対話型ブロック リセットの対話型ブロック	X	（バイパスされた場合）X
安全保障局	X	

手順 3： 接続データベースのサイズを調整して下さい

接続イベントはシステム ポリシーで設定 する 最大接続 イベントにプルーニングされた依存です。 設定を変更するため:

1. **システム > ローカル > システム ポリシーを**選択して下さい。
2. 現在適用されたポリシーを編集するために*鉛筆*アイコンをクリックして下さい。
3. **> 接続データベース > 最大接続 イベント** 『Database』 を選択 して下さい。
4. **最大接続 イベント**の値を変更して下さい。
5. **ポリシーおよび終了を**『SAVE』 をクリック し、次にアプライアンスにポリシーを**適用して下さい**。

保存することができる接続イベントの最大量は管理センター モデルによって決まります:

注 最大イベント制限は接続イベントと安全保障局イベントの間で共有されます; 2 つのイベントのための設定最大値の合計は最大イベント制限を超過できません。

管理センター モデル	イベントの最大数
FS750、DC750	50，000,000
FS1500、DC1500	100，000,000
FS2000	300，000,000
FS3500、DC3500	500，000,000
FS4000	10億
仮想アプライアンス	10，000,000

注意： データベース制限の増加はデバイスの不利なパフォーマンス影響がある場合があります。 パフォーマンスを改善するために、規則的にとはたらかせるイベントの数へのイベント制限を合わせる必要があります。

時間 範囲上のイベント カウントを表示するウィジェットに関しては、イベントの総数は詳細なデータがイベント ビューアで利用できるイベントの数を反映しないかもしれません。 これはディスク領域の使用率を管理するためにシステムが時々より古いイベント詳細をプルーニングするので

発生します。 プルーニングするイベント詳細の発生回数を最小限に抑えるために配備にとって最も重要なそれらのイベントだけ記録 するためにイベント ロギングを最適化できます。

関連情報

- **データベース イベント制限の設定**
- **テクニカルサポートとドキュメント - Cisco Systems**

このドキュメントは有用でしたか。 はい いいえ

フィードバックいただき、ありがとうございました。

サポート ケースのオープン（シスコ サービス契約<ts generic='1' nval='P%1,2%%'が必要です）。

Cisco サポート コミュニティ - 特集対話

Cisco サポート コミュニティでは、フォーラムに参加して情報交換することができます。

このドキュメントで使用されている表記法の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

Updated: 2015 年 5月 20 日
Document ID: 118012