イベント アクション オーバーライドのトラブルシューティング

このドキュメントでは、Cisco Intrusion Prevention System（IPS）のイベント アクション オーバーライドによる潜在的な問題について説明し、インストールのチューニングおよびトラブルシューティングに推奨される方法を説明します。

> **注:** イベント アクション オーバーライドは、リスク レーティングに基づいてシグニチャに対して実行されるグローバル アクションです。 グローバル コンフィギュレーションと同様に、設定を変更したり追加したりするときには、十分な注意が必要です。

イベント アクション オーバーライドの問題

説明

イベント アクション オーバーライドは、シグニチャ イベントが指定のリスク レーティング範囲内にあるときに、アクションを追加します。 イベント アクション オーバーライドは慎重に使用してください。 頻繁にトリガーされるイベント（特に、IP ロギング アクションなどの高コストのアクション）のリスク レーティング範囲を広げてオーバーライドを作成すると、問題が発生する可能性があります。

影響

イベント ストアへ過度の書き込みを行うと、一般的に、CPU 使用率が高くなり、コマンドライン インターフェイス（CLI）や Cisco IPS Device Manager（IDM）など管理アクセス ツールに対しセンサーが反応しなくなります。

IP ロギング アクションとファイル記述子

ファイル記述子は、ファイルに対するハンドルを取得するためにプログラムで使用されるデータ構造です。 既知の記述子は、標準入力の場合は 0、標準出力の場合は 1、標準エラーの場合は 2 です。 ファイル記述子は、プロセスが新しいファイルまたはソケットを開くときに作成されます。

log-attacker-packets、log-pair-packets、または log-victim-packets などの IP ロギング アクションのイベント アクション オーバーライドを作成すると、ファイル記述子のプールが枯渇する可能性があります。 センサーの全体的なパフォーマンスが低下するおそれがあり、センサーが正しく動作しない場合があります。

SNMP トラップ アクションとイベント アクションのオーバーライド

1 つのアクション request-snmp-trap しか含まれていないシグニチャは、イベント ストアに書き込まれるアラート イベントも生成します。 そのため、Simple Network Management Protocol（SNMP）トラップ アクションを過度に実行した場合も、アラート アクションを過度に生成した場合と同じ問題が引き起こされる可能性があります。

Normalizer エンジン シグニチャのアクション

イベント ストアから Normalizer シグニチャへの書き込みを引き起こすアクション（製品アラート、request-snmp-trap、log-actions など）は追加しないでください。 これは、1200 ~ 1330 の範囲のシグニチャ ID すべてに適用されます。

簡単なトラブルシューティングのシナリオ以外には、Normalizer エンジンのシグニチャに対してイベント アクション オーバーライドを使用しないでください。 これは特に、次のシナリオで問題となる可能性があります。

- 高度に断片化された IP シナリオ（範囲 1200 のシグニチャによる）
- 顕著に順序が乱れている（ooo）TCP シナリオ（範囲 1300 のシグニチャ）

たとえば、すべての ooo TCP パケットについてイベント ストアへの書き込みを引き起こすイベント アクション オーバーライドの場合は、リソースと使用率の問題が発生する可能性があります。

リスク レーティング 0 ~ 100 のイベント アクションのオーバーライド

一般的に、リスク レーティングが 0 ~ 100 のイベント アクション オーバーライドの使用は回避してください。レーティングが低いと、特定の状況でセンサーにリスクが生じるおそれがあります。

メタ コンポーネント シグニチャは多くの場合、安全で一般的と思われるトラフィック タイプで起動されます。 メタ シグニチャは、親メタ シグニチャがアラートを起動する前にトリガーする 1 つ以上のメタ コンポーネント シグニチャの組み合わせを検索します。 メタ コンポーネント シグニチャには、デフォルトでは、アクションが関連付けられません。 これらは共通トラフィックに一致する場合が多いため、これは意図的なものです。 メタ コンポーネント シグニチャのデフォルトのベース リスク レーティングは 15 です。 イベント アクション オーバーライドでこれらのシグネチャの一致のキャプチャを除外するために、イベント アクション オーバーライドを作成するときには、25 を下回るリスク レーティングを使用しないことをお勧めします。 つまり、リスク レーティングは 25 ~ 100 未満であってはなりません。

IPS 使用率の検証

コマンド

> **注:** このセクションで使用されるコマンドの詳細については、コマンド検索ツール（登録ユーザ専用）を使用してください。

インスペクションの負荷率を取得するために、CLI で **show statistics virtual-sensor** コマンドを入力してください。

```
sensor# show statistics virtual-sensor | inc Load
Processing Load Percentage = 100
```
IPS バージョン 7.0(8)E4 および 7.1(6)E4 で、**show inspection-load** コマンドが追加されました。

```
sensor#  show inspection-load history
sensor 10:17:57 UTC Mon Apr 05 2013
```
このコマンドの出力例を次に示します。

負荷率が非常に高い（90% 以上）場合は、イベント アクション オーバーライドによってイベントが過度にトリガーされていることを示します。 この可能性を確認するには、ログを参照してください。

ログ

過剰なイベント アクション オーバーライドは主に、この例の main.log ファイルで確認できるように、イベント ストアのラッピングが頻繁に行われていることから分かります。

```
sensor#  show inspection-load history
sensor 10:17:57 UTC Mon Apr 05 2013
```
一般的に、イベント ストアのラッピングが 1 時間当たり 2 回以上行われる場合は、問題が発生している可能性があります。 一部のシナリオでは、ラッピングが 1 分以内に何度も実行される場合があります。 プラットフォームの全体的なパフォーマンス能力など、多数の変数を考慮する必要があります。

トラブルシューティング

どのタイプのイベント、トラフィック、またはアクションがイベント アクション オーバーライドの問題を引き起こしているかを判別してください。 それは製品アラートでしょうか、IP ロギングでしょうか、Normalizer シグニチャでしょうか、あるいはメタ コンポーネント シグニチャですか。

- 「chatty」シグニチャの場合は、シグニチャがイベントの誤検出を招いていることを突き止めたら、イベント アクション フィルタ（EAF）を記述してください。
- IP ロギングの場合は、EAF を回避するか、リスクを完全に理解したうえで EAF を慎重に使用してください。
- Normalizer シグニチャおよびメタ コンポーネント シグニチャの場合は、一時的なトラブルシューティングのシナリオ以外では、アラート アクションはありません。

関連情報

- イベント アクション オーバーライドの設定
- IPS 設定ガイド
- テクニカルサポートとドキュメント - Cisco Systems