

ルール アクション On Time Unit (時間単位) の例

2023 年 3 月 16 日 ArcSight Support

1. ルールの設定

1.1 条件



1.2 アグリゲーション

タイムフレーム1分、一致数2としています。

The screenshot shows the '調査/編集' (Survey/Edit) dialog box for a rule named 'ルール:Test'. The 'アグリゲーション' (Aggregation) tab is selected. The configuration is as follows:

- 一致数: 2
- タイムフレーム: 1 分
- 指定フィールドが異なるものをアグリゲート (No fields specified)
- 指定フィールドが同一なものをアグリゲート (event1.メッセージ)

The summary section states: '1分間で条件に2回以上マッチングした場合にアグリゲートします。また、イベントフィールド(event1.メッセージが同じ場合かどうか)によります。'

Buttons at the bottom include: テスト (checked), OK, キャンセル, 適用, ヘルプ.

1.3 アクション

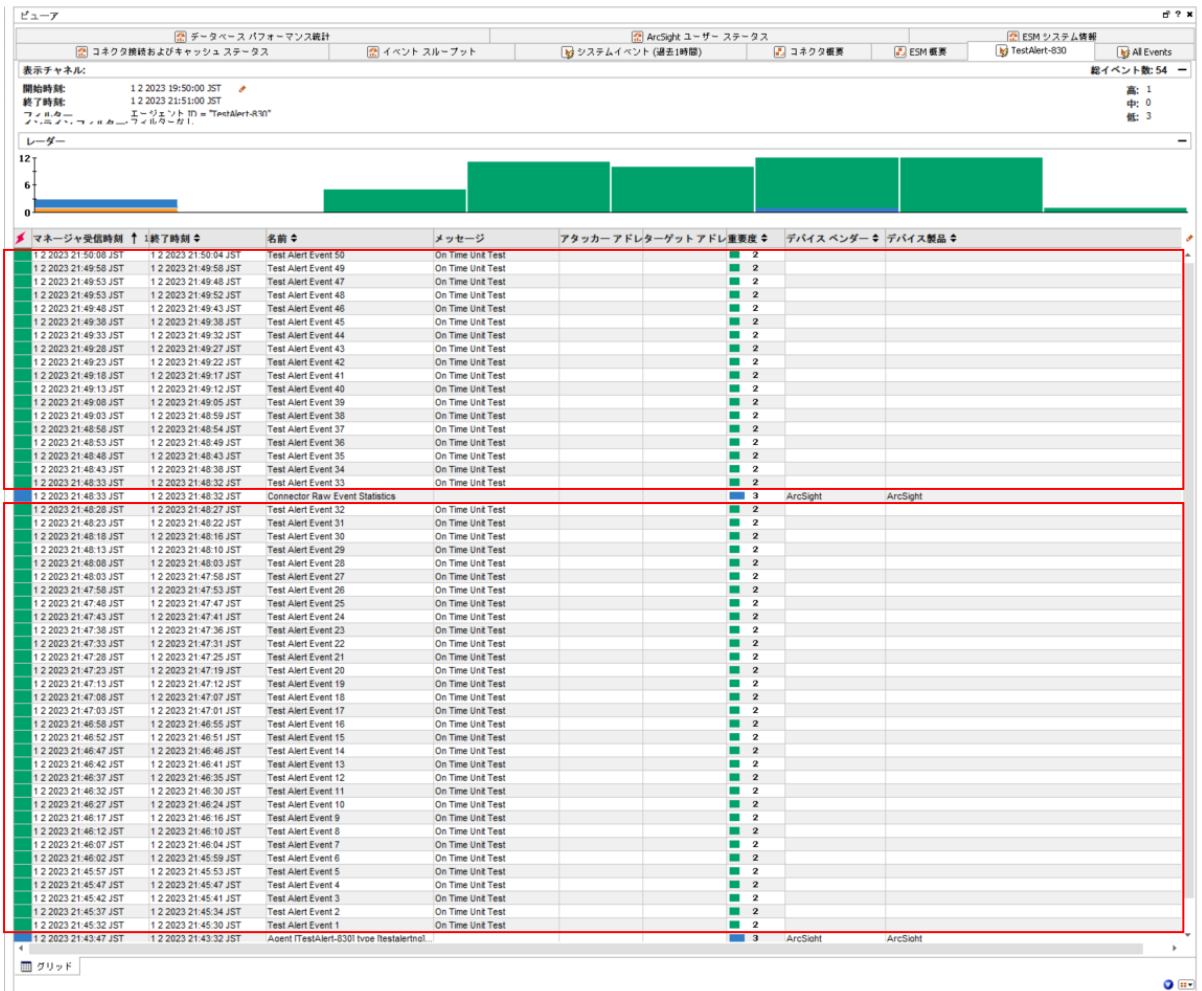
「最初の閾値」と「時間単位」をアクティブとしています。

なお、時間単位のトリガを有効とするために、イベントフィールドアクションの設定が必要になります。

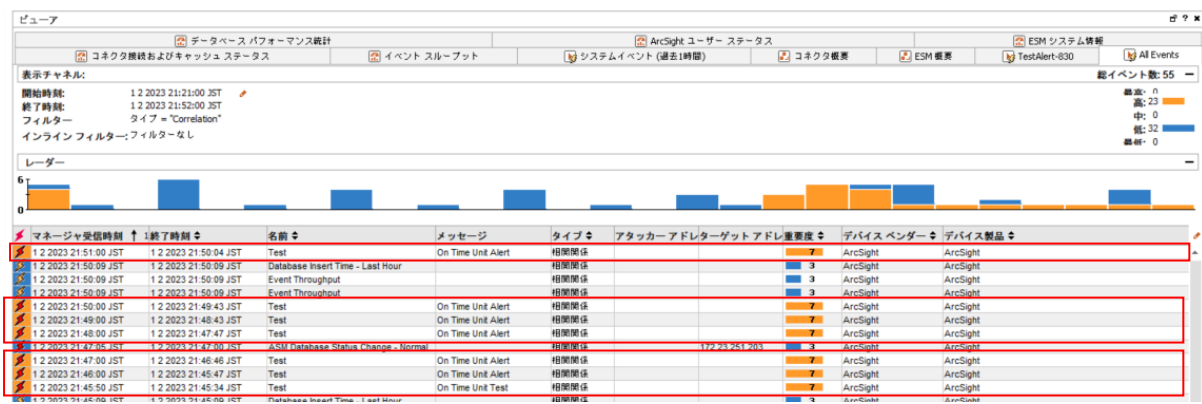
(まず、「時間単位」を右クリックし、「追加」で「イベントフィールドの設定」選択しています。また、トリガ条件：時間単位の発生閾値を1分としています。その後、このアクションのトリガを有効化します。)



2. ルールの条件に合う次の 50 件のイベントを送付

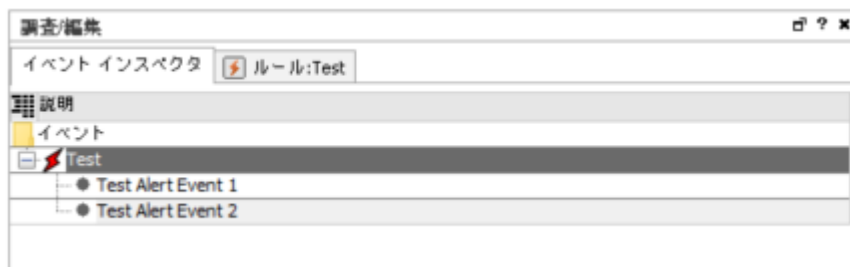


3. 次の 7 つの関連イベントが作成されます。



4.それぞれの相関イベントを右クリックし「イベントの詳細表示」を選択すると次のようになります。

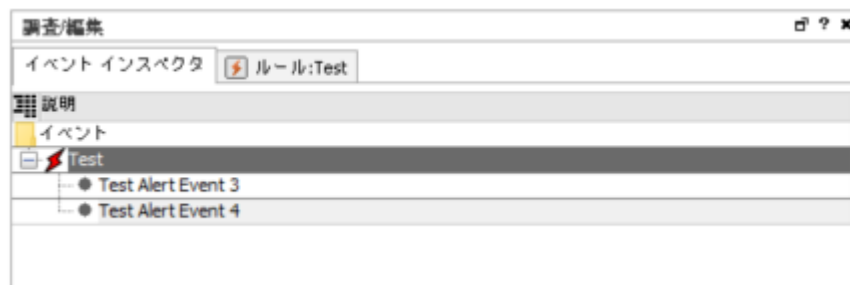
4.1次は、マネージャ受信時刻が 21時45分50秒のもので、「最初の閾値」アクションの相関イベントになります。（アグリゲーションの一致数を2としているので、2つのベースイベントになります。）



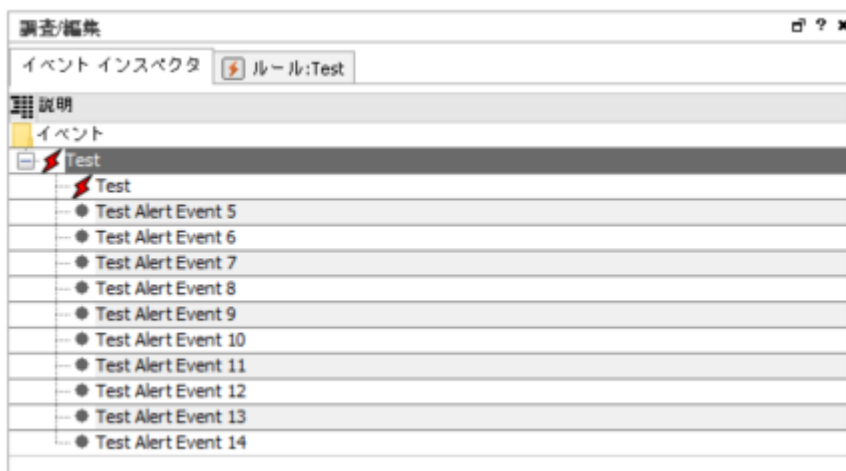
以降は「時間単位」アクションにより1分間隔での相関イベントになります。

なお、マネージャ受信時刻が00秒までの1分間毎にアラートが発生しています。

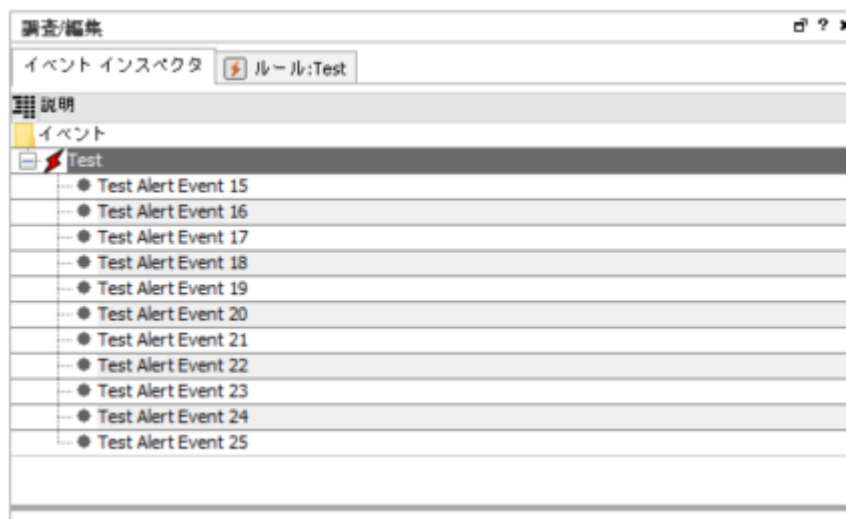
4.2 マネージャ受信時刻が 21時46分00秒の相関イベント



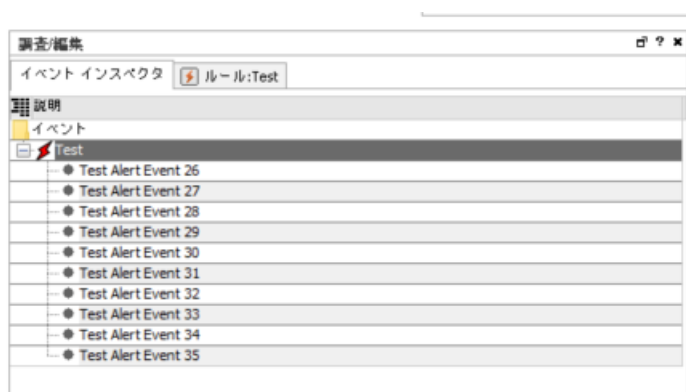
4.3 マネージャ受信時刻が 21時47分00秒の関連イベント



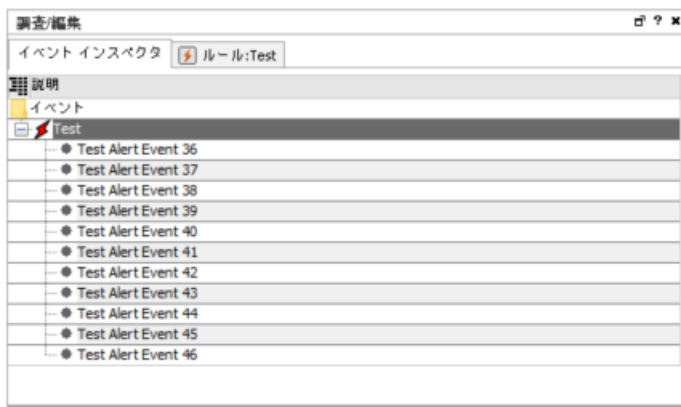
4.4 マネージャ受信時刻が 21時48分00秒の関連イベント



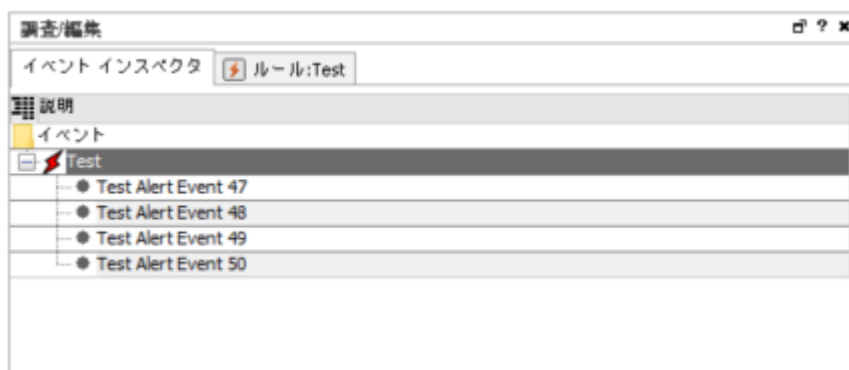
4.5 マネージャ受信時刻が 21時49分00秒の関連イベント



4.6 マネージャ受信時刻が 21時50分00秒の関連イベント



4.7 マネージャ受信時刻が 21時51分00秒の関連イベント



以上