ルール アクション On Time Unit（時間単位）の例

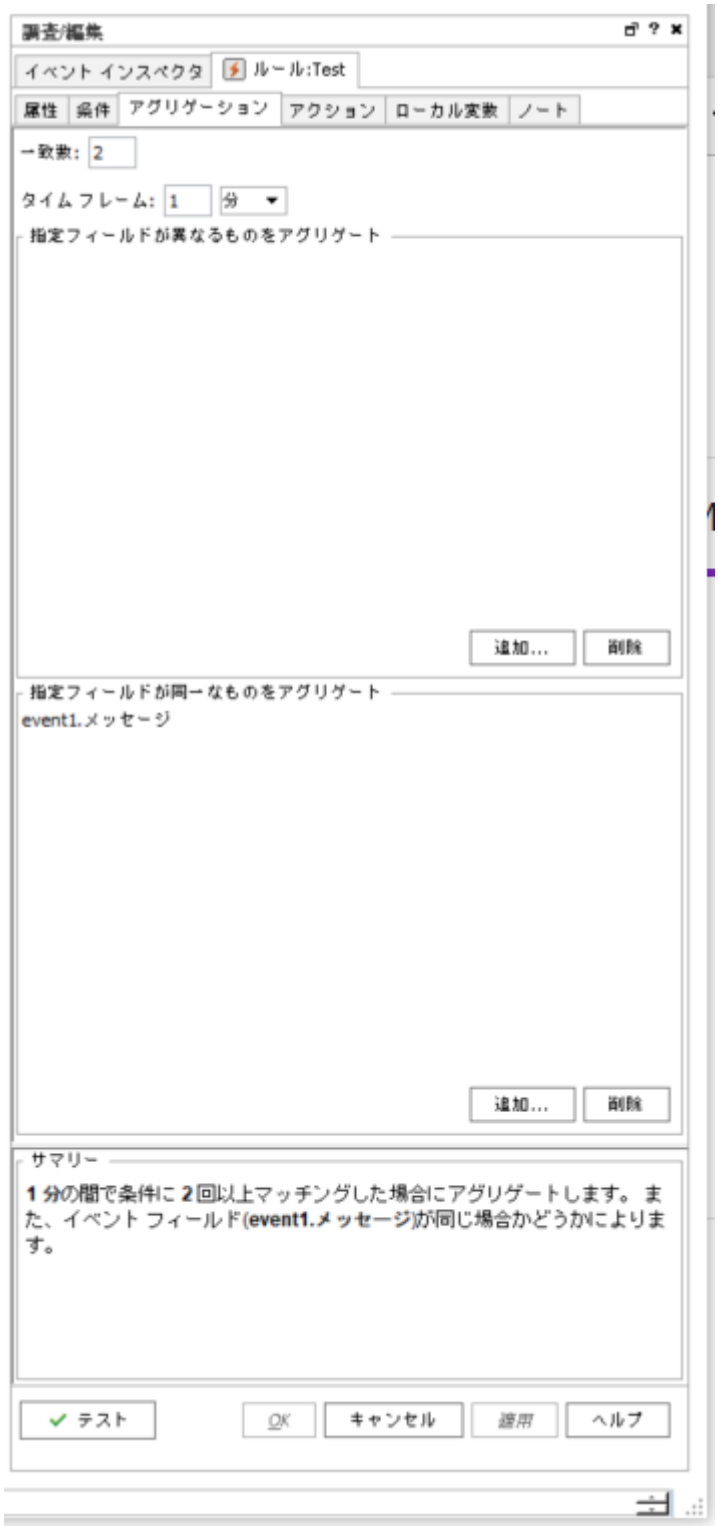
2023 年 3 月 16 日　ArcSight Support

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。



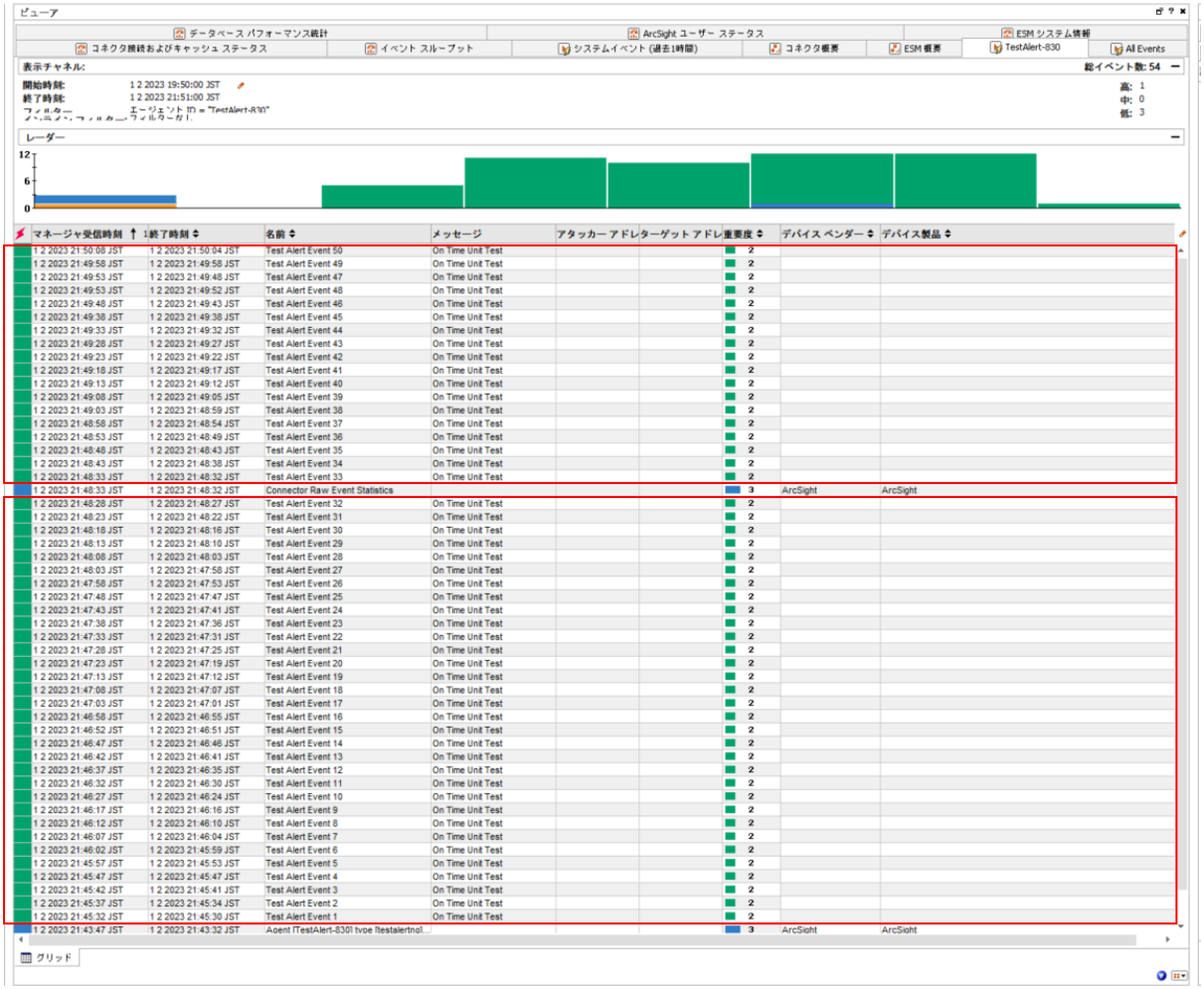
1.3 アクション

「最初の閾値」と「時間単位」をアクティブとしています。

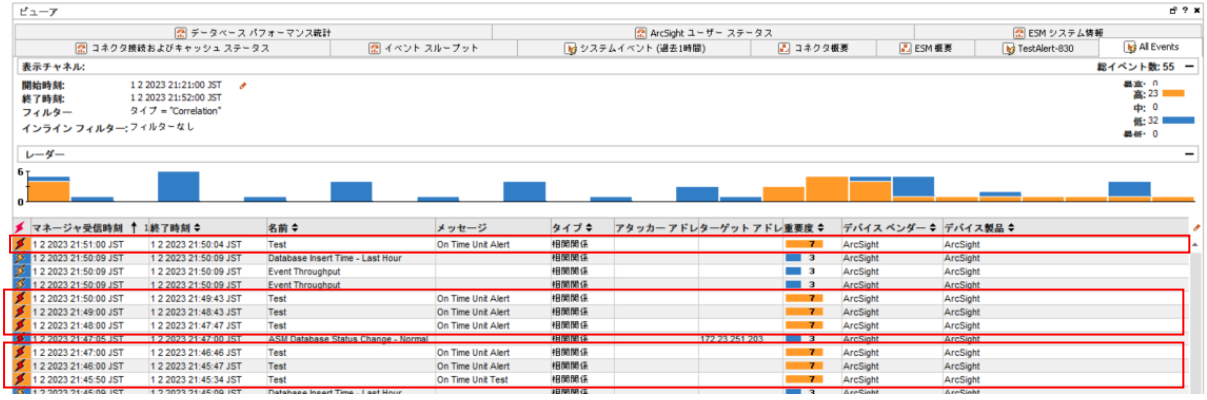
なお、時間単位のトリガを有効とするために、イベントフィールドアクションの設定などが必要になります。

（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

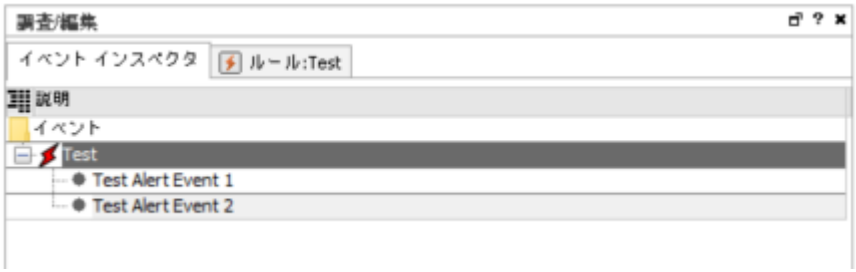


3. 次の 7 つの相関イベントが作成されます。



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。

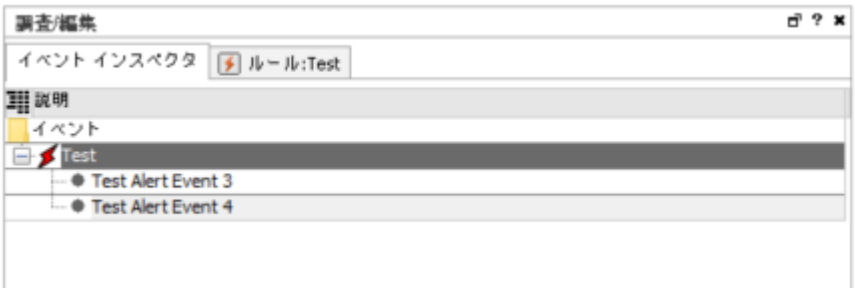
4.1 次は、マネージャ受信時刻が　21 時 45 分 50 秒のもので、「最初の閾値」アクションの相関イベントになります。（アグリゲーションの一致数を 2 としているので、2 つのベースイベントになります。）



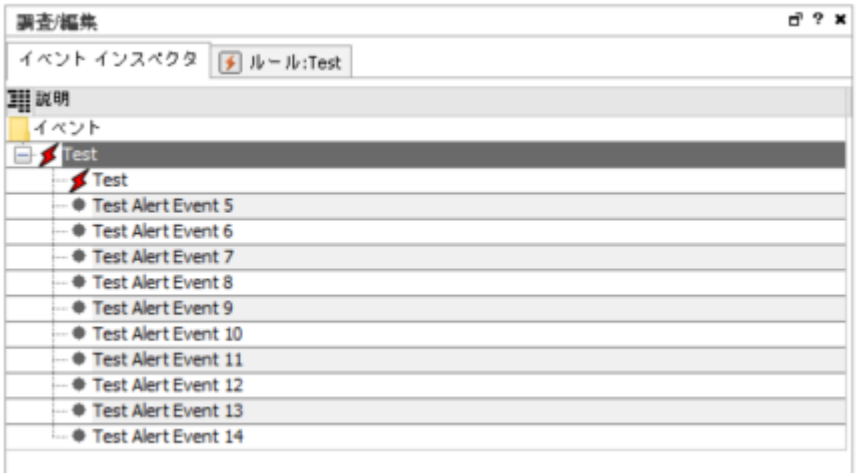
以降は「時間単位」アクションにより 1 分間隔での相関イベントになります。

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。

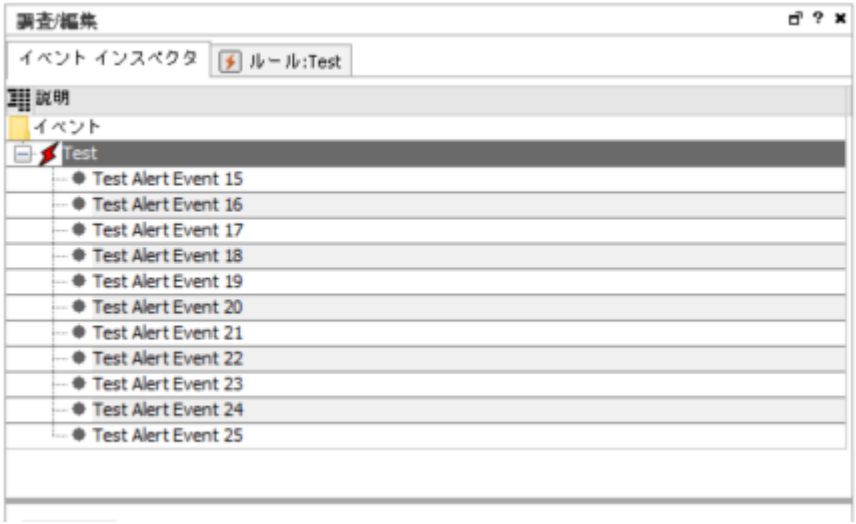
4.2 マネージャ受信時刻が　21 時 46 分 00 秒の相関イベント



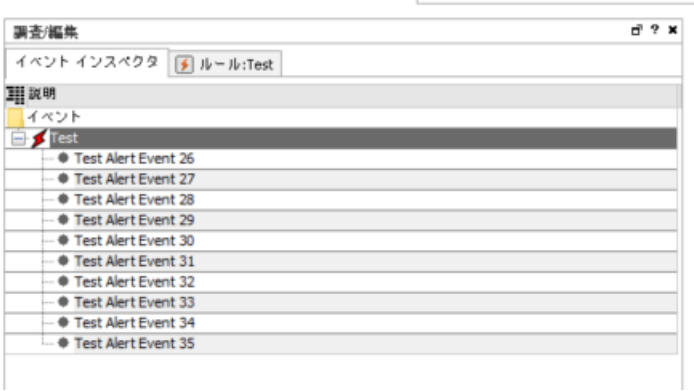
4.3 マネージャ受信時刻が　21 時 47 分 00 秒の相関イベント



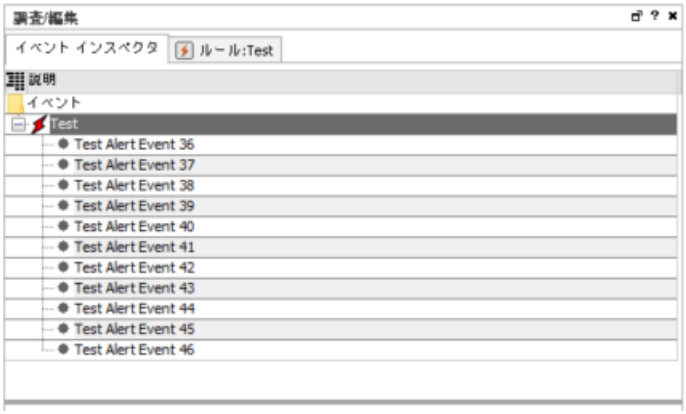
4.4 マネージャ受信時刻が　21 時 48 分 00 秒の相関イベント



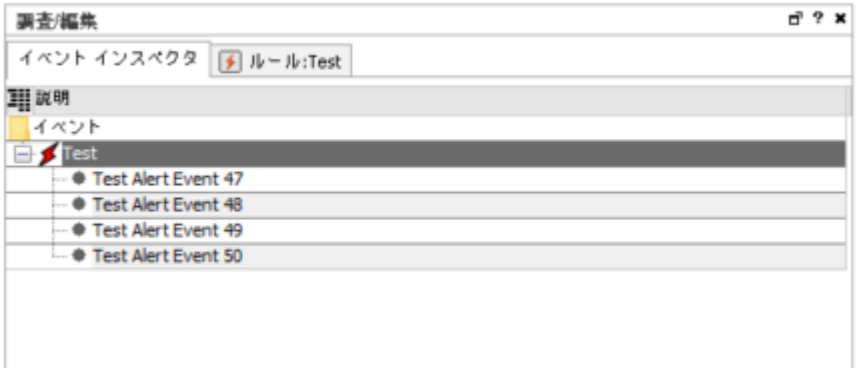
4.5 マネージャ受信時刻が　21 時 49 分 00 秒の相関イベント



4.6 マネージャ受信時刻が　21 時 50 分 00 秒の相関イベント



4.7 マネージャ受信時刻が　21 時 51 分 00 秒の相関イベント



以上