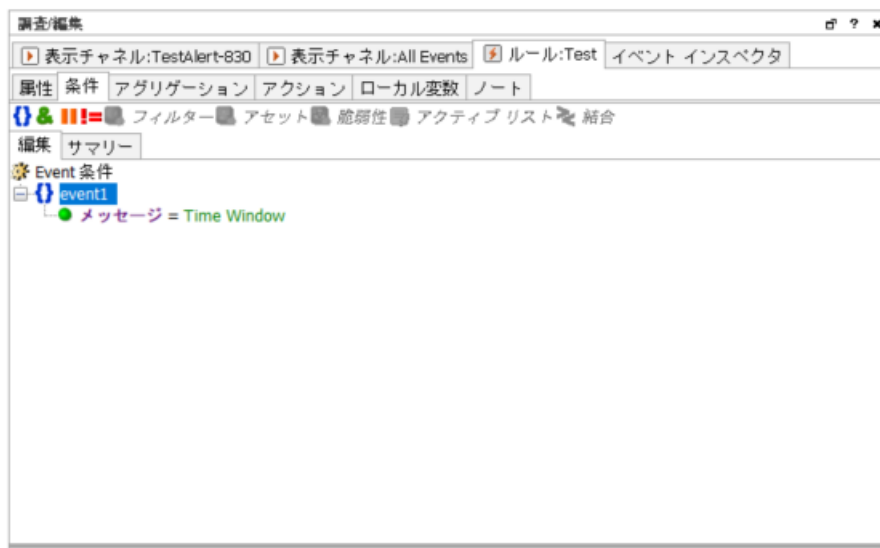


ルール アクション On Time Window Expiration (タイム ウィンドウの有効期限) の例

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

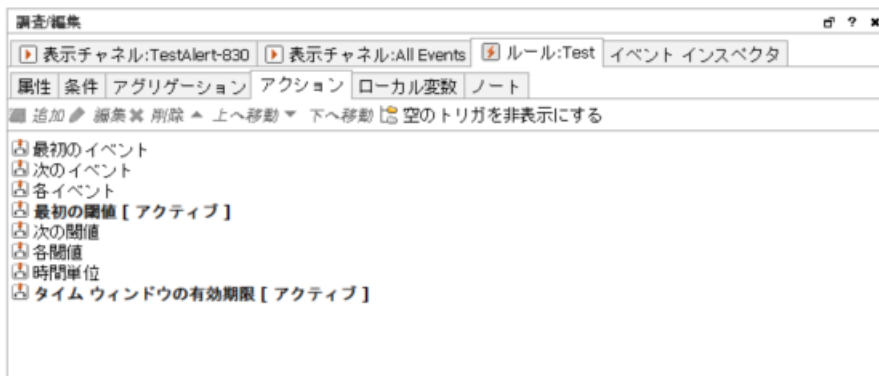
タイムフレーム2分、一致数5としています。

The screenshot shows the '調査/編集' (Search/Edit) window for an event aggregation rule. The window title is '調査/編集' and it has standard window controls. The main area is divided into several sections:

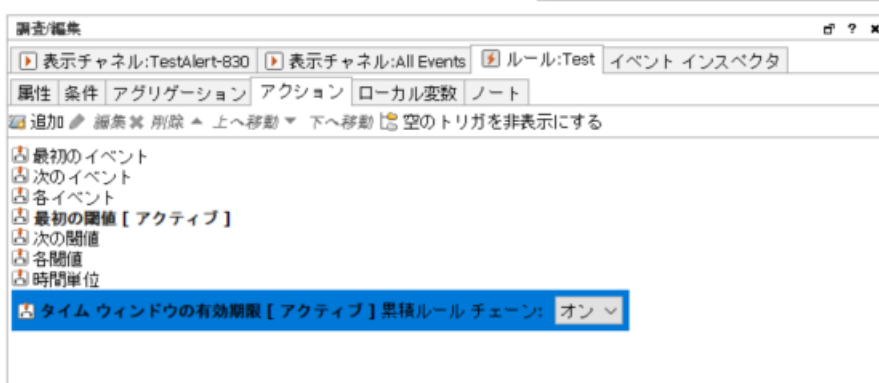
- Header:** Shows the current configuration: '表示チャンネル: TestAlert-830', '表示チャンネル: All Events', 'ルール: Test', and 'イベント インспекタ'.
- Navigation:** A tabbed interface with '属性' (Properties), '条件' (Conditions), 'アグリゲーション' (Aggregation), 'アクション' (Actions), 'ローカル変数' (Local Variables), and 'ノート' (Notes). The 'アグリゲーション' tab is active.
- Configuration Fields:**
 - '一致数: 5' (Consistency count: 5)
 - 'タイム フレーム: 2 分' (Time frame: 2 minutes)
 - '指定フィールドが異なるものをアグリゲート' (Aggregate items with different specified fields) - This is the selected aggregation mode.
- Aggregation List:** A list of aggregation rules. The first rule is selected and shows:
 - '指定フィールドが同一なものをアグリゲート' (Aggregate items with the same specified fields)
 - 'event1.メッセージ' (event1.message)
- Summary:** A section titled 'サマリー' (Summary) with the text: '2分の間で条件に5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。' (Aggregate when the condition matches 5 or more times within 2 minutes. Also, it depends on whether the event field (event1.message) is the same or not.)
- Buttons:** '追加...' (Add...) and '削除' (Delete) buttons are present next to each rule in the list.
- Footer:** A 'テスト' (Test) button with a green checkmark, and 'OK', 'キャンセル' (Cancel), '適用' (Apply), and 'ヘルプ' (Help) buttons.

1.3 アクション

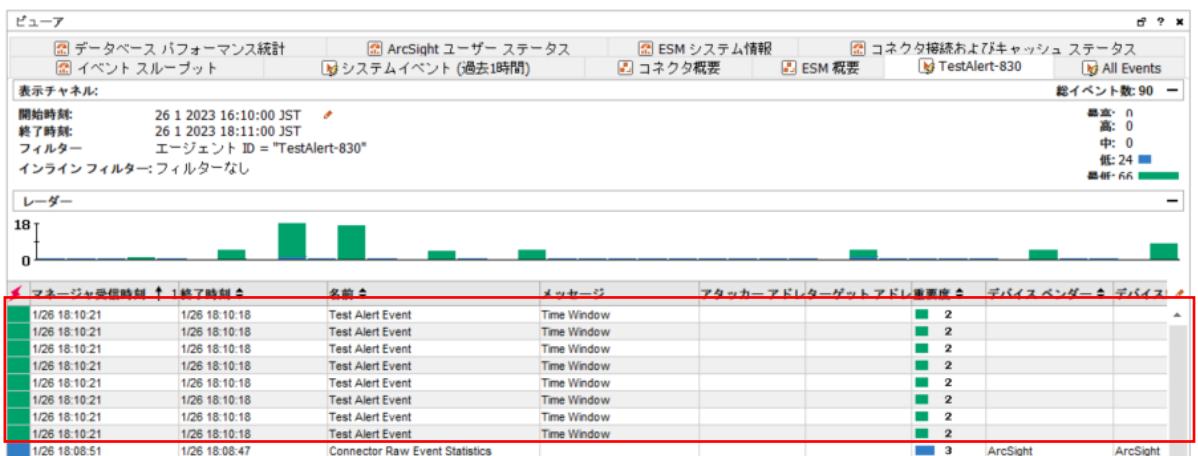
「最初の閾値」と「タイム ウィンドウの有効期限」をアクティブとしています。



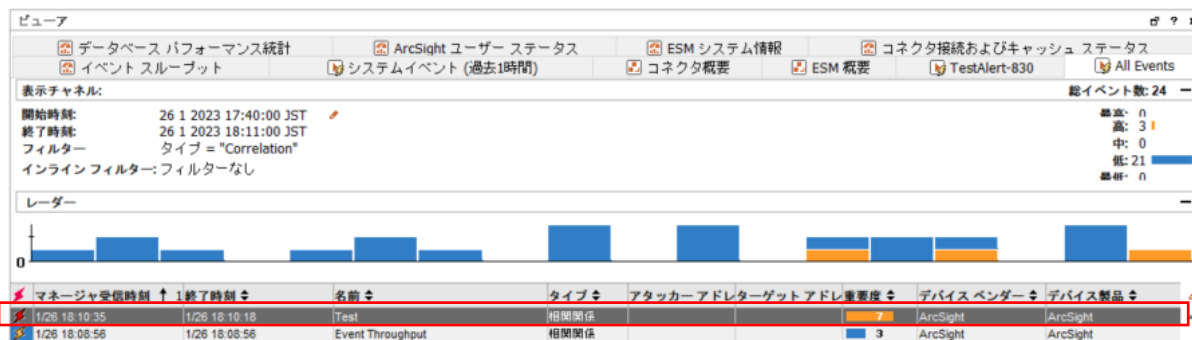
2. 累積ルールチェーンがオンの場合



2.1 ルールの条件にマッチする8つのイベントを送付した場合



2.2次の関連イベント（2分間で5つのイベント）が作成されます。こちらは「最初の閾値」アクションで作成された関連イベントです。

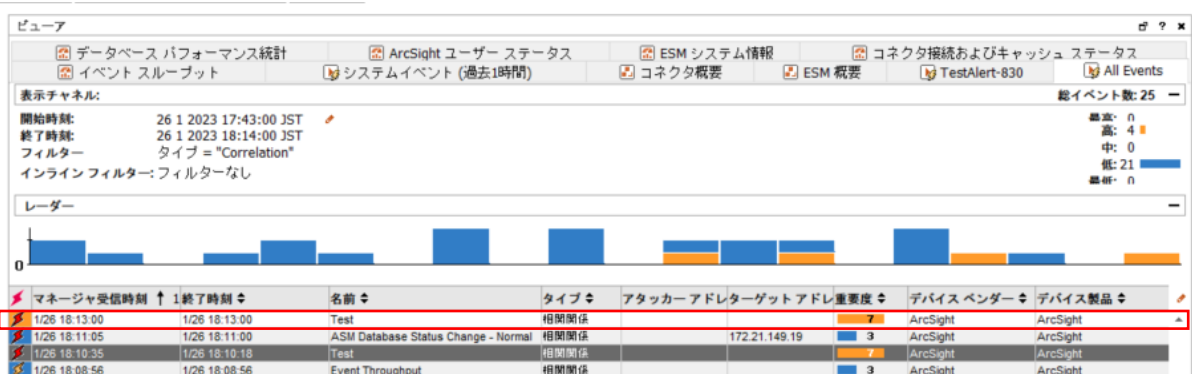


このイベントを右クリックし「イベント詳細表示」を選択すると次の様に表示されます。

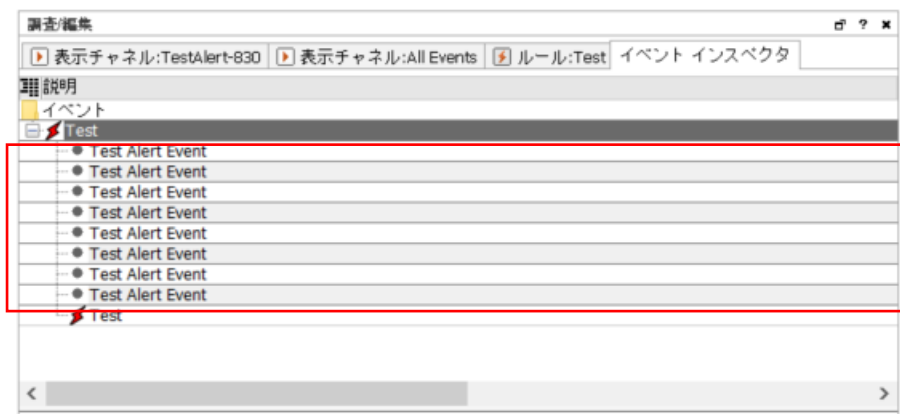


こちらはイベントのトリガとなった5つのベースイベントになります。

次に、ルールタイムフレーム（今回は2分）経過すると次の追加の関連イベントが作成されます。こちらが「タイムウィンドウの有効期限」アクションで作成された関連イベントになります。



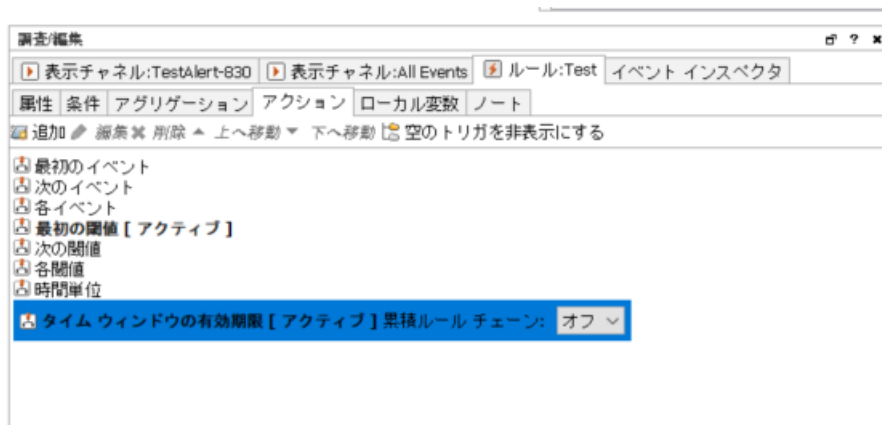
このイベントを右クリックし「イベント詳細表示」を選択すると次の様に表示されます。



本来であれば後半の3つのベースイベントはトリガの要件を満たしていませんが、**On Time Window Expiration**（タイム ウィンドウの有効期限）をアクティブにしているためこの関連イベントが作成されます。

3. 累積ルールチェーンがオフの場合

なお、次の様に累積ルールチェーンがオフの場合には、



「タイムウィンドウの有効期限」アクションで作成された関連イベントは、次の様にトリガの要件を満たしていない後半の3つのベースイベントとなります。



以上