### alert

入力レコードを利用してソナーイベントを生成します。

#### 構文

alert

#### 説明

alertはコントロールノードでのみ使用可能で、クラスター管理者のみが実行できます。通常、各データノードでストリームルール検出後、コントロールノードに送信されるイベントを受信するストリームクエリにalertコマンドを設定して使用します。

重複したイベントが受信された場合、ストリーム検出シナリオのイベント集約設定により除外されることがあります。また、ストリーム検出シナリオの設定に応じてチケットが生成されたり、既存のチケットに統合されたりする場合があります。生成されたイベントはイベントメニューから確認できます。

入力レコードは以下の仕様を満たす必要があります。

入力レコードは次のフィールドで構成されている必要があります：

|  |  |  |  |
| --- | --- | --- | --- |
| フィールド名 | 必須/任意 | 型 | 説明 |
| \_logger | 必須 | 32ビット整数 | ロガーID識別子 |
| \_rule | 必須 | 32ビット整数 | ストリーム検出シナリオID識別子 |
| \_time | 任意 | 日時 | 元イベント発生時刻。値がない場合や型が一致しない場合は、入力時点の時刻として処理されます。 |
| emp\_key | 任意 | 文字列 | 従業員番号 |
| emp\_name | 任意 | 文字列 | 従業員氏名 |
| host\_ip | 任意 | IPアドレス | 社内ホストIP |
| src\_ip | 任意 | IPアドレス | 送信元IP |
| src\_country | 任意 | 文字列 | 送信元ISO国コード |
| src\_port | 任意 | 32ビット整数 | 送信元ポート |
| dst\_ip | 任意 | IPアドレス | 宛先IP |
| dst\_country | 任意 | 文字列 | 宛先ISO国コード |
| dst\_port | 任意 | 32ビット整数 | 宛先ポート |
| protocol | 任意 | 文字列 | プロトコル |
| action | 任意 | 文字列 | 対応方式 |