### alert

Creates a Sonar event using the input record.

#### Syntax

alert

#### Description

This command is available only on the control node and can only be used by the cluster administrator. Basically, you can use it by setting up the alert command in a stream query that receives the event to be transmitted to the control node after real-time rule detection from each data node.

If a duplicate event is received, it may be removed due to the event deduplication setting of the real-time scenario. In addition, a ticket may be created or merged into an existing ticket depending on the real-time scenario settings. You can retrieve the created event in the event menu.

The input record must meet the following specifications:

|  |  |  |  |
| --- | --- | --- | --- |
| Field | Required | Type | Description |
| \_logger | Yes | 32-bit integer | Logger ID identifier |
| \_rule | Yes | 32-bit integer | Real-time scenario ID identifier |
| \_time | No | Date/Time | Time at which the original event occurred. If there is no value or the type does not match, it is treated as the time at which the input is made. |
| emp\_key | No | String | Employee number |
| emp\_name | No | String | Employee name |
| host\_ip | No | IP Address | Host IP address |
| src\_ip | No | IP Address | Source IP address |
| src\_country | No | String | Source ISO country code |
| src\_port | No | 32-bit integer | Source port number |
| dst\_ip | No | IP Address | Destination IP address |
| dst\_country | No | String | Destination ISO country code |
| dst\_port | No | 32-bit integer | Destination port number |
| protocol | No | String | Protocol |
| action | No | String | Response method |