Day - 2

23 January 2025 19:37

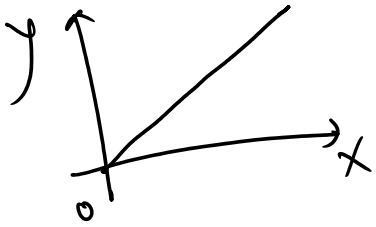
1. Visualization
   1. chart
   2. Timechart
   3. Single Value Visualization.
   4. Geo Map.
   5. Custom Visualization.
2. Date & Time function:-
3. Knowledge object – Field extraction. Tags & Event type | Alert Report

---

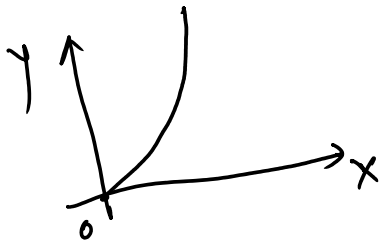
1. Visualization –

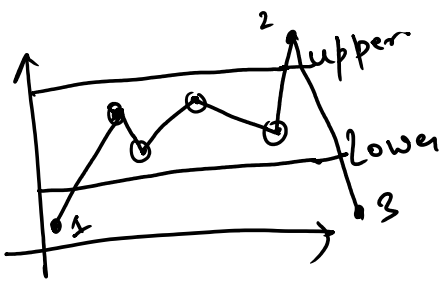
Chart:- |chart count by current_ticket_state
count → y-axis
current_ticket_state → x-axis

Linear:- 10, 20, 30, 40



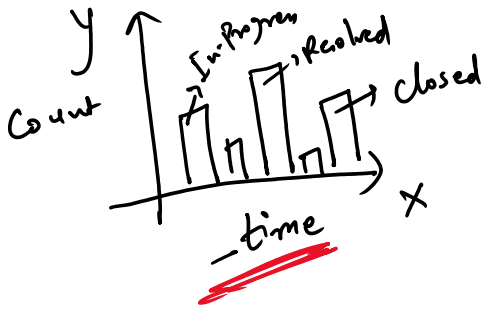
Log:- 10, 100, 1000, 10000, ---





Timechart:-

|timechart count by asset_id.



day = d
month = mon
year = y

week = w
Minute = m
second = s
hour = H

09-09-09 → Application.

%d %m %y
%m %d %y
%y %m %d

↳ Epoc format (System Readable format)

↓

operation (Diff. b/w Two fields)

Single Value Visualization:-

Single Numeric Value as a visualization.

Count

40

Count

10 → Displayed
20
30
40

1. Single Value
2. Radial Gauge
3. Filler gauge
4. Marker gauge

All 4 works for → Single Value Visualization.

GeoMap:- on the Geographical Map.

Coordinates → Latitude & Longitude Values.

Custom Visualization:- Install the Visualization App. availble in the appstore.

Prerequisite

① Support Type → splunk | 3rd Party Organization / Independent Developer.
- splunk → splunk LLC → Author.

② Product Compability → splunk Cloud / splunk Enterprise.

③ Version Compability → Which Version of App support which Version of splunk Product.

App | Addon → .tar.gz format.

Head:- Head command is going to pick the value from the top list.

Tail:- Pick the record/event from the bottom of the list.

Rex:- fields are not extracted in splunk.

Regular expression -

e.mail, phone, text.

Regular expression:
email, phone, text.

Knowledge object:-

① Field Extraction:-

Consistent data.

Data is unconsistent / Mixed format. It will not do any extraction.

- ① Regular expression
- ② Delimiter Type.

① **Regular exp:-** Select the value what you want to capture. Splunk is going to write the expression using ML.

② **Delimiter type:-** extract the field using the splitting of the event with the help of symbol like space, ",", tab, pipe.

② **Alert:-** Notify the User, after a certain condition is triggered.

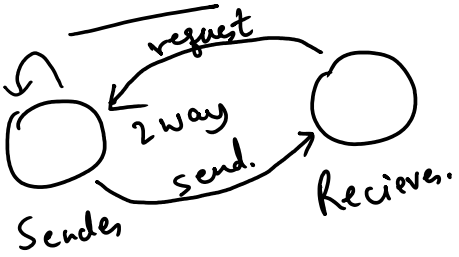
① [ ] → Definition (SPL, Schedule, Timeperiod)

② [Trigger Condition] → When ? → No. of result = 0

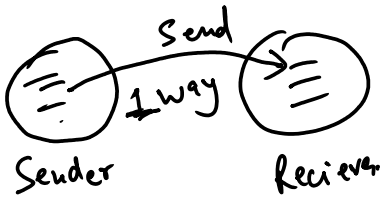
③ [Trigger Action] → Email, SMS, Triggered Alert, script etc.

③ [Trigger Action] → Email, Alert, script etc.

API



Webhook



- Notification