Day - 3

24 January 2025 19:33

1. Splunk Dashboard
   1. classic Dashboard.
   2. Input filter.
   3. Addiy Panels.
   4. Drill down.
   5. optimization → Base search.
      → SavedSearch

2. Report

3. Alert

---

1. Splunk Dashboard:-

1. classic Dashboard
2. Studio Dashboard

1. classic Dashboard:-

Day One.

Feature loaded Dashboard.

1. XML
2. Drilldown
3. Visualization
4. Conditional set
5. Set & Unset token.

2. Studio Dashboard:-

Version 8.5.x

1. json
2. Drilldown
3. Visualization → Add background Image, Customize font, flowcharts, Background color.

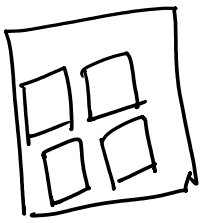
1. Visualization Driven Dashboard.

4. No Conditional Setting
5. [illegible] token Not used.

(1) Visual Dashboard.

(4) No Conditional Setting
(5) Set/unset token not used.

(1) classic Dashboard:- Collection of Panels & filters.



Collection of panels, filters → Style page → Dashboard

Application ← Collection of Dashboard, Alert, Report, Knowledge object.

Token:-

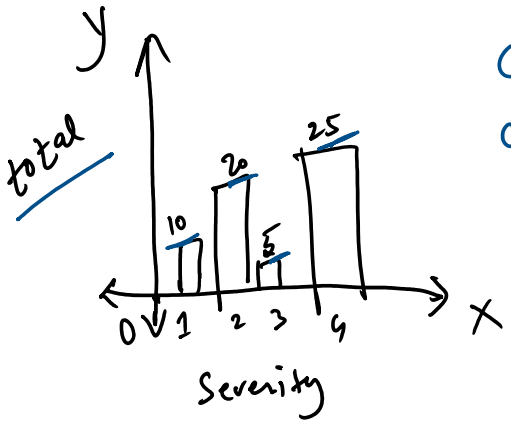
(1) Unique name throughout the Dashboard. → Define the token name.

(2) lower case, No space, No Digit → Recommend

Severity → 1, 2, 3, 4

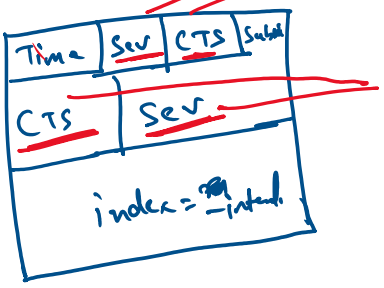
Single Dropdown → either All, 1, 2, 3, 4 (one value at a time)

Multiselect Dropdown → Combination of value (1,3) (1,3,4) (1,2,4) (1,4)



click.name = X-axis name = Severity
click.value = X-axis value = 1,2,3,4
click.name2 = y-axis name = total
click.value2 = y-axis value = 10,20,5,25

Vk-classic Dashboard.-



2 filters.

2-Panel

4 Times.

index=vk_idx

Source = Sample_tickets.csv.

To optimize it, we have to minimize the no. of time.

Listing the index.

Base Search

↓

ContinuousData

1. As Many Base Search as you want in one dashboard.
2. Base search name should be Unique.

SavedSearch :- Scheduled search.

Report <search id="_" ref="vk-report"> </search>

Report:- [Definition] → SPL, schedule, TimeRange.

[Action] → Email, Script, Lookup.


Action