Day - 2

04 January 2025 15:38

1. Basic SPL Commands.

(a) table → tabular output. Syntax:- |table field1, field2, field3

(b) Rename → change the name at search level. Syntax:- |rename oldfield as newfield

(c) dedup → remove the duplicate values. Syntax:- |dedup field.

(d) stats → statistical output.

(a) Count → total count. Syntax:- |stats count by source.

(b) Avg → Avg. value. Syntax:- |stats avg(—) by —

(c) Sum. → Sum value. Syntax:- |stats sum(—) by —

(d) list → grouping of the field, duplicate |stats list(source) by sourcetype

(e) Values → " " " , unique. |stats values(source) by sourcetype.

(e) eval → evaluation Activity.

(a) Calculation → [bytes → Kb] | eval kb = round(bytes/1024,3)." KB"

(b) if-else → if (a>b, a, b) → True, → False. | eval state = if(bytes>475380, "High", "Low")

(c) case → 3, conditional. | eval state = case(bytes>0 OR bytes<100000, "Low", bytes>100000 OR bytes<500000, "Medium", bytes>=500000 OR bytes<=800000, "High", 1=1, "Normal")

(f) Addcoltotal →

(g) Addtotal →

(h) chart → | chart count by sourcetype → y-axis. → x-axis.

(i) timechart → | timechart count by source

(j) Single value Visualization → Recomm. → Single numeric Value.

(k) Appende →

(l) Appendcol →

(m) Appendpipe →

(n) join →

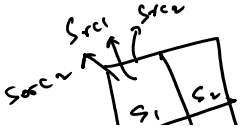
(o) multikv →

(p) rex →

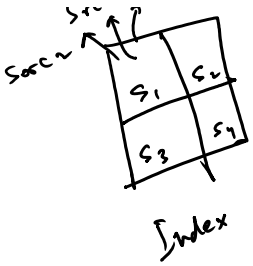
(q) tstats →

(r) spath →

(s) fillnull → Handle the blank spaces. | fillnull value="NULL" bytes

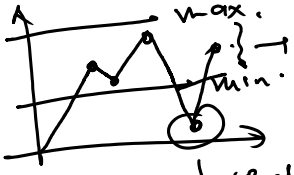


| stats list(source) by sourcetype



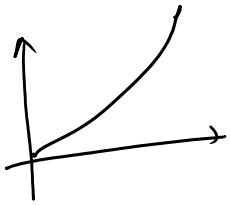
Stats list(source)

result → index, source, sou...



↳ Below the threshold value.

10^x → 10, 100, 1000, 10000



10, 20, 30, 40, 50 . - - -