Day - 3

03 June 2025 09:39

1. Field Alias.
2. Calculated field.
3. Macros.
4. lookup (CSV)
5. Data Model & Pivot
6. Command – Append, Appendcols, date & time fun.
7. Multi value.
8. String, informational, statistical, Mathematical, Crypto fun.

---

1. Field Alias :– New name to the field.

Field Alias :– New Name

field

Severity → priority.

New Names

old Name

HR

e_id

employee_id

Sales

employee_id

Finance

emp_id.

employee_id

FA :– employee_id

* New field

old field. → New field.

Severity = Priority

2. Calculated field :–

eval. KB = bytes / 1024 → byte

variable

Multiple place ↓ use field "KB" multiple times.

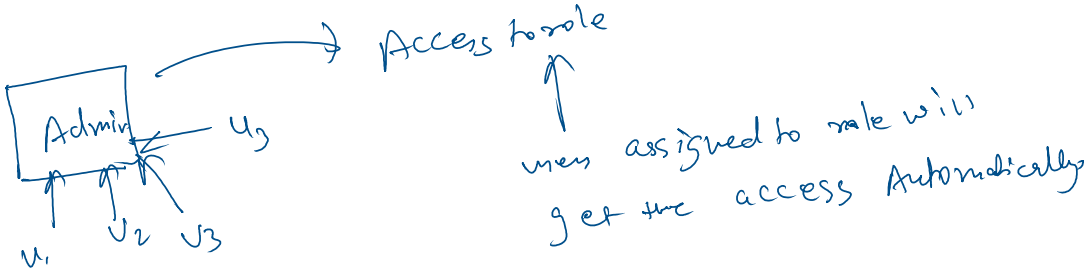
field generated as Normal field.

expression.

Multiply

Define the field "KB"

Calculated field. → template → expression.



(3) Macros :- Function

No Arg.
one Arg.
multi Arg.

function a(5, c)
{ d = b+c;
return d;
}

a(3, 4)
a(5, 6)

Search → filtering purpose
where

A	B
a	5
b	10
c	15
d	20

search B > 10

A	B
c	15
d	20

where: Compare two field.

A	B
5	5
10	28
25	45
30	

where A=B

A	B
5	5
10	

(4) lookup → CSV → As per syllabus.
→ geospatial

Kvstore

External

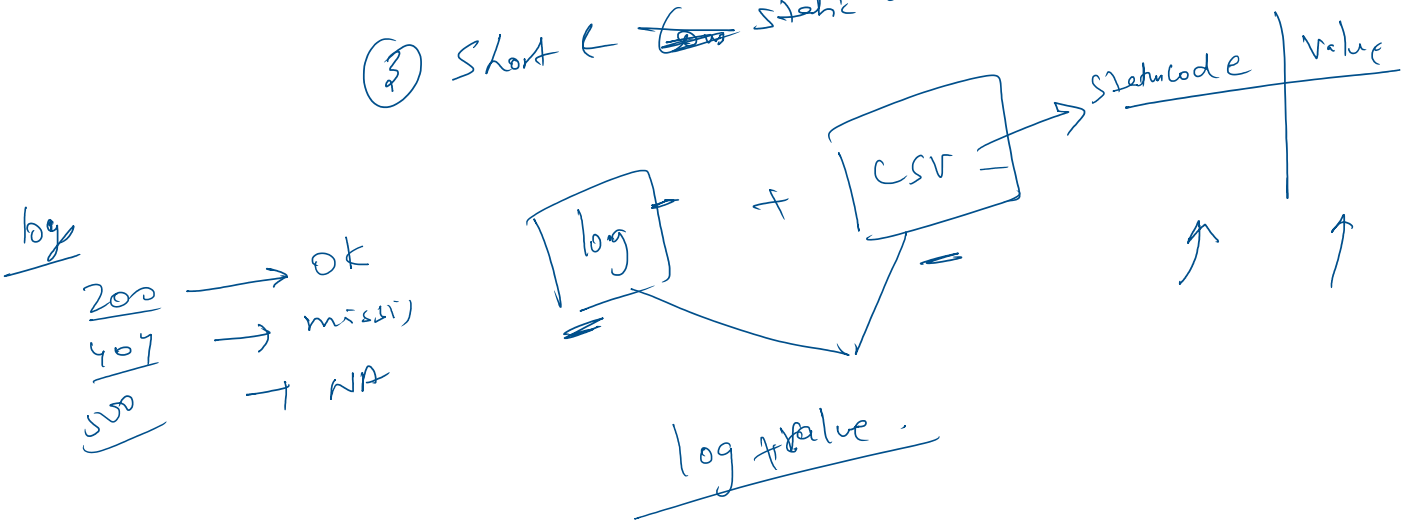
Database.

csv lookup:-

(1) csv format

(2) upload the file in splunk. No license calculated.

(3) Short ← ~~Long~~ static data with csvlookup



Index:-

TN, Sev, CTS

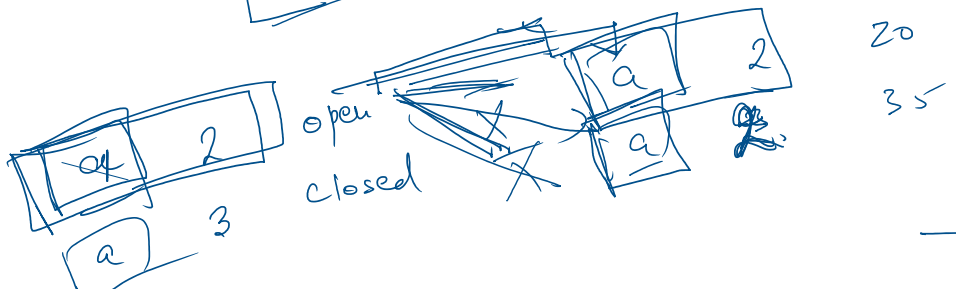
a 2

Lookup:-

TN, Sev, TimeConsumed.

a 3

TN, SN



@ 3

Sourcetype → csv
source → source:; Sample_tickets.csv
host → host:; localhost

Data Model & Pivot :-

execute → collect the event + field extraction

Data model - define the field in the advance only.

Hierachical Concept
↳ root
↳ child
↳ child 2

Pivot → DM

w/o DM → Pivot

chart, timechart

Append :-

I_1 , I_2

+

↓

final output

I_1 | I_2

No common joining

'it just combine & see o/p in single window.