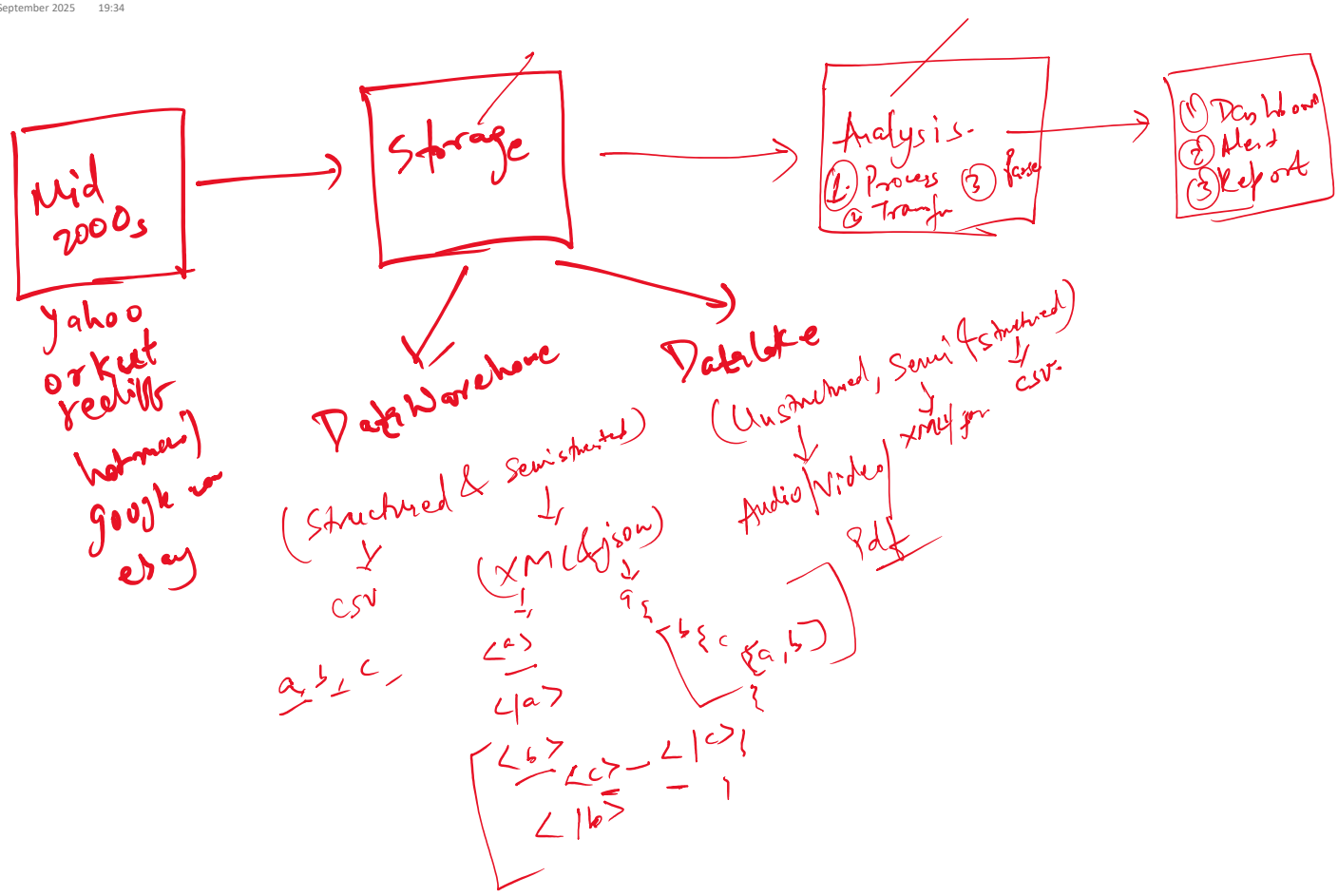
Day - 1

03 September 2025 19:34



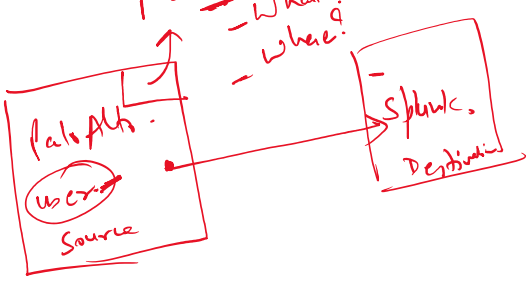

1. License Cost
2. Customer Availability
3. Processing of the data
4. Integration

1. **Splunk:-** 1. log monitoring
2. Dashboard, Alert, Report, knowledge object & prediction Analysis.

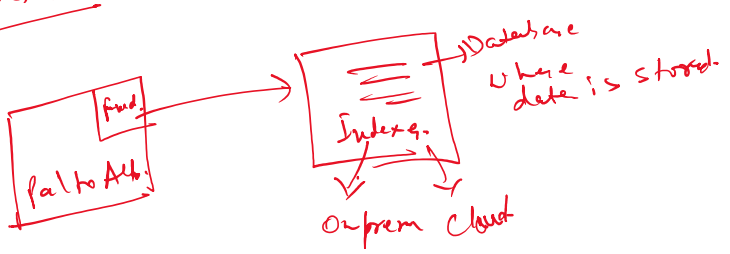
1. Splunk Enterprise
2. Splunk Universal forwarder

Component of Splunk:-

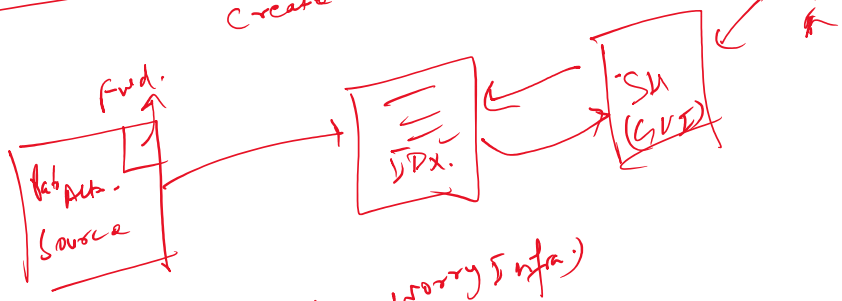
1. **Forwarder:-**



(2.) Indexer :- Store the data.



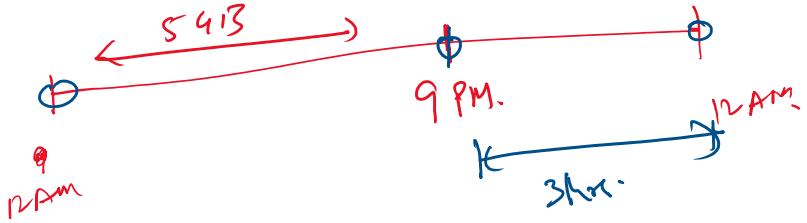

(3) Search Head :- GUI where the end user will create DB, Reports or Alert.




Splunk → SAAS (No worry Infra.)
→ managed. → (Infra.)

(4.) License Master :-

(1) How much data you will be ingesting in 24hrs window. 5 GB | day.




5 times-3 day Windows.

(1) Index ; will continue.

(2) Search ; will be disabled.

Fwd data - full the event + extract the field

Search data = full the event + extract the field

Fast mode = Full the event.

Smart = Full the event + Extract the field.

## SPL (Search Processing Language)

1. Table
2. Rename.
3. dedup.
4. stats.
5. eval.
6. addcoltotal.
7. addtotal
8. sort
9. chart
10. timechart.

1. Table:- Create the tabular output.

Syn:- |table f1, f2, f3

fieldname is case sensitive

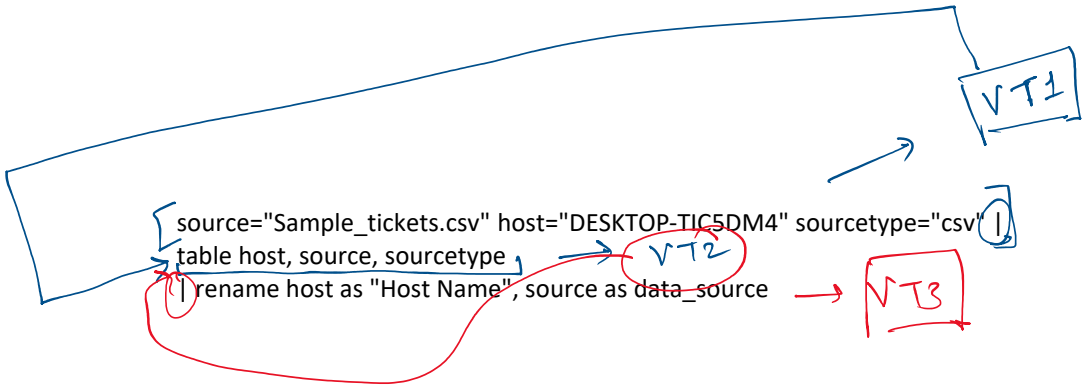
fieldvalue is case insensitive.

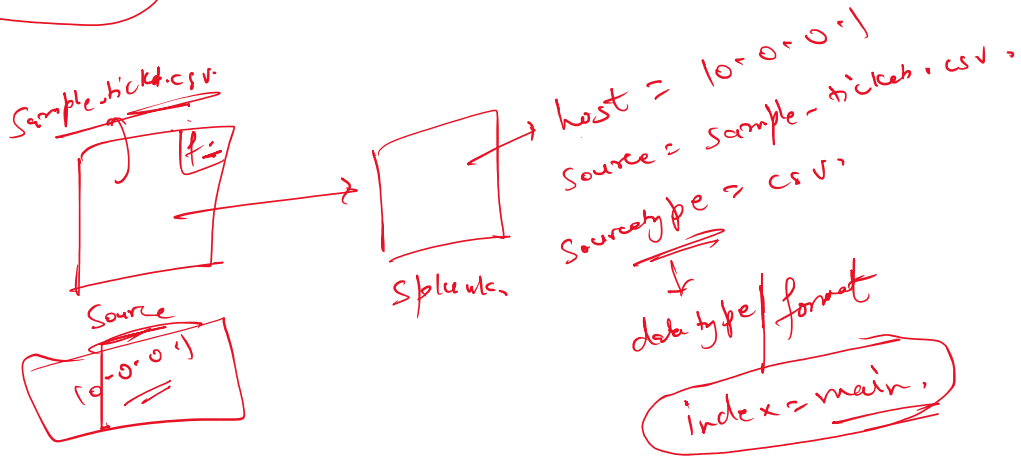
2. Rename- Rename the field name at the search level.

Syn:- rename oldname AS newname

3. dedup- exclude the duplicate value.

Syn:- |dedup f1




4. stats – statistical command.

a. count
b. sum
c. avg
d. dc
e. list
f. values

a) count :- Count the event.

b) sum | Avg :- summation | Avg. numeric value.

list – categorize the field on the basis of certain val.

values – " " " " " " " "

| stats list(source) by sourcetype

dc – distinct_count( ) → distinct value | count.
dc( )

5) Eval – Evaluation Activity. byte → KB

⑤ Eval - Evaluation Activity.

Eval
↳ initialize variable.

bytes → KB

- KB = (bytes | words)

int
var
str
→ define the variable.

if-else:-

```
if (a>b)
{
  print(a);
}
else { print(b);
}
```

→ SPL.

if (a>b, a, b)
↳ false.
↳ True

1, Condition.

Case statement:-

```
switch
  case(a) ——
  case(b) ——
  case(c) ——
  ——
  ——
  ——
  default ——
```

→ case (cond1, "——", cond2, "——",
1=1, "——")

Sort:-

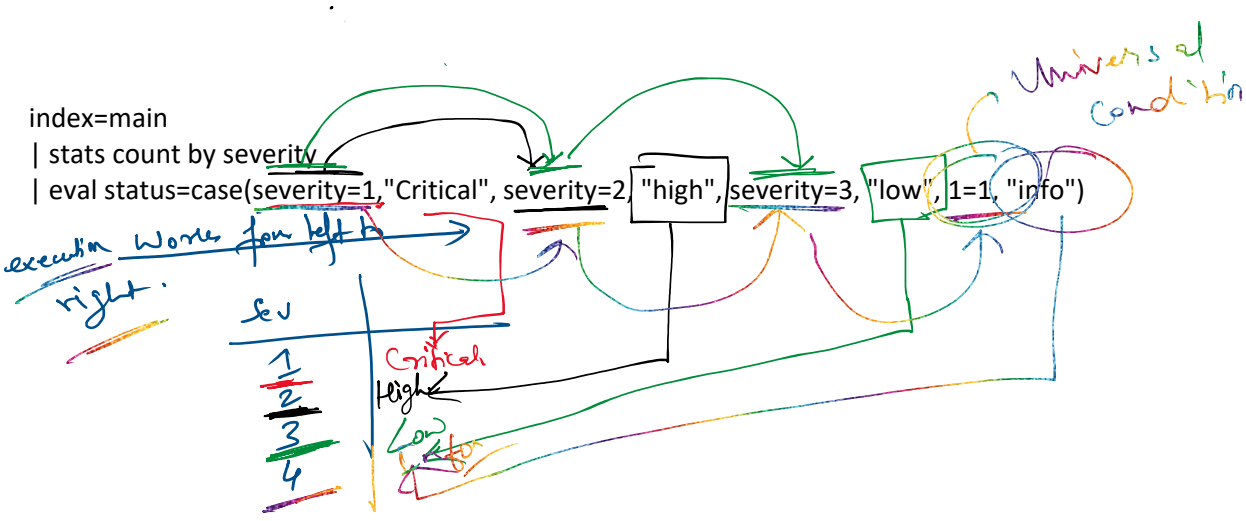
Ascend → sort + f2
sort f1

Descend → sort - f1.

Addition row wise

Addtotal - Addition row wise

Addcoltotal - Addition columnwise.




Tomorrow:-

1. Visualization
2. SPL
3. Field extraction
4. Macros
5. tags & eventtype