Day - 1

19 January 2026 09:37

Splunk:- Monitoring ① Dashboard → XML (classic) / JSON (Studio Dashboard)

② Alert

③ Report.

④ Predictive Analysis.

⑤ MLTK

Component of splunk:-

1. Forwarder.
2. Indexer.
3. Search Head.
4. License Master.

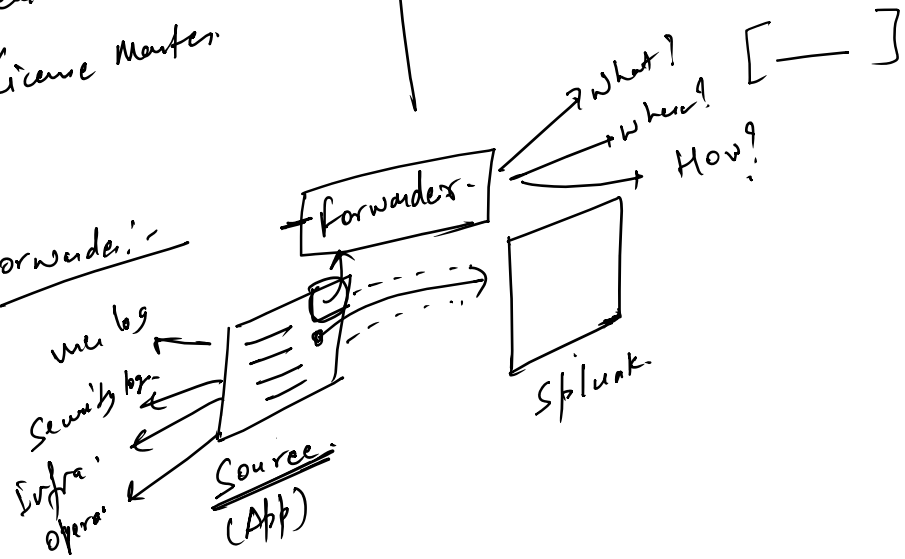
Managed Instance:-

① Deployment Server.

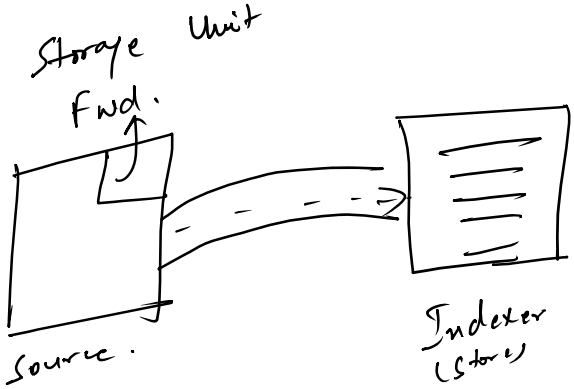
② Deployer.

③ cluster Master

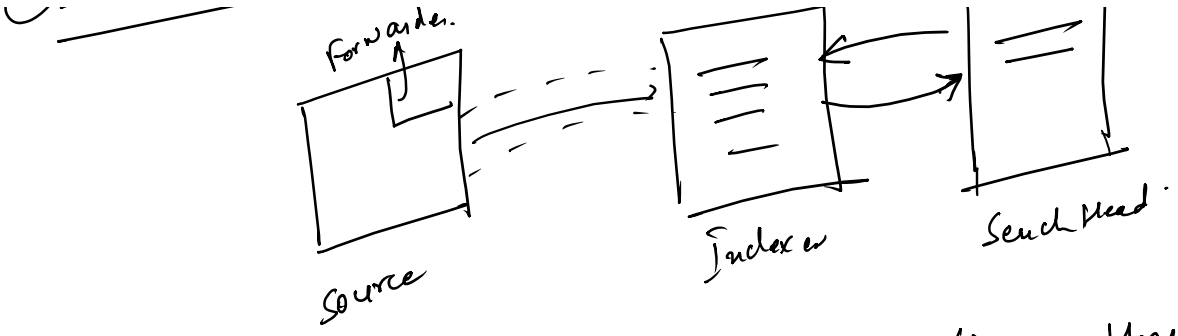
① Forwarder:-



② Indexer:-



③ Search Head:- GUI



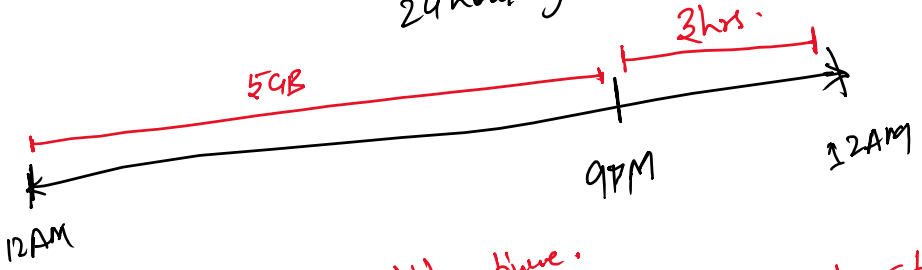
④ License Master:- Agent that Monitoring License Usage.

① How much data you are ingesting on the daily Basis

5 GB | day ↔ 1 year.

↓

24 hour cycle.

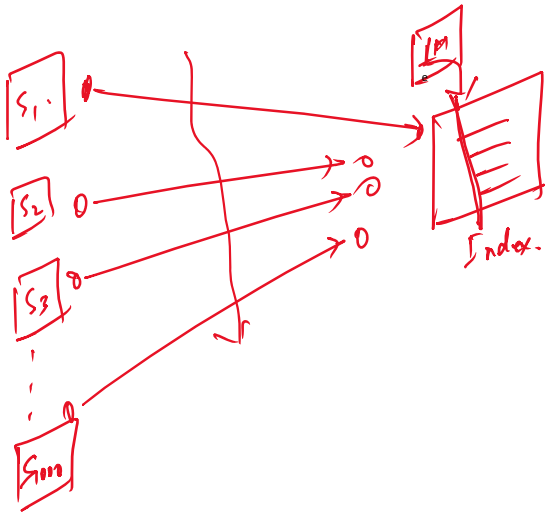


① Indexing will continue.

② Searching will be stopped.

↓

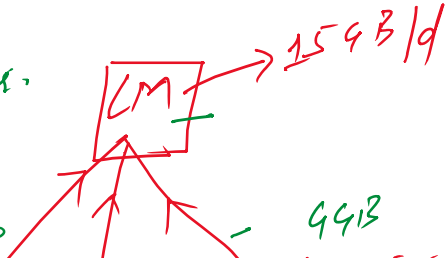
① Dashboard.
② Report.
③ Alert.

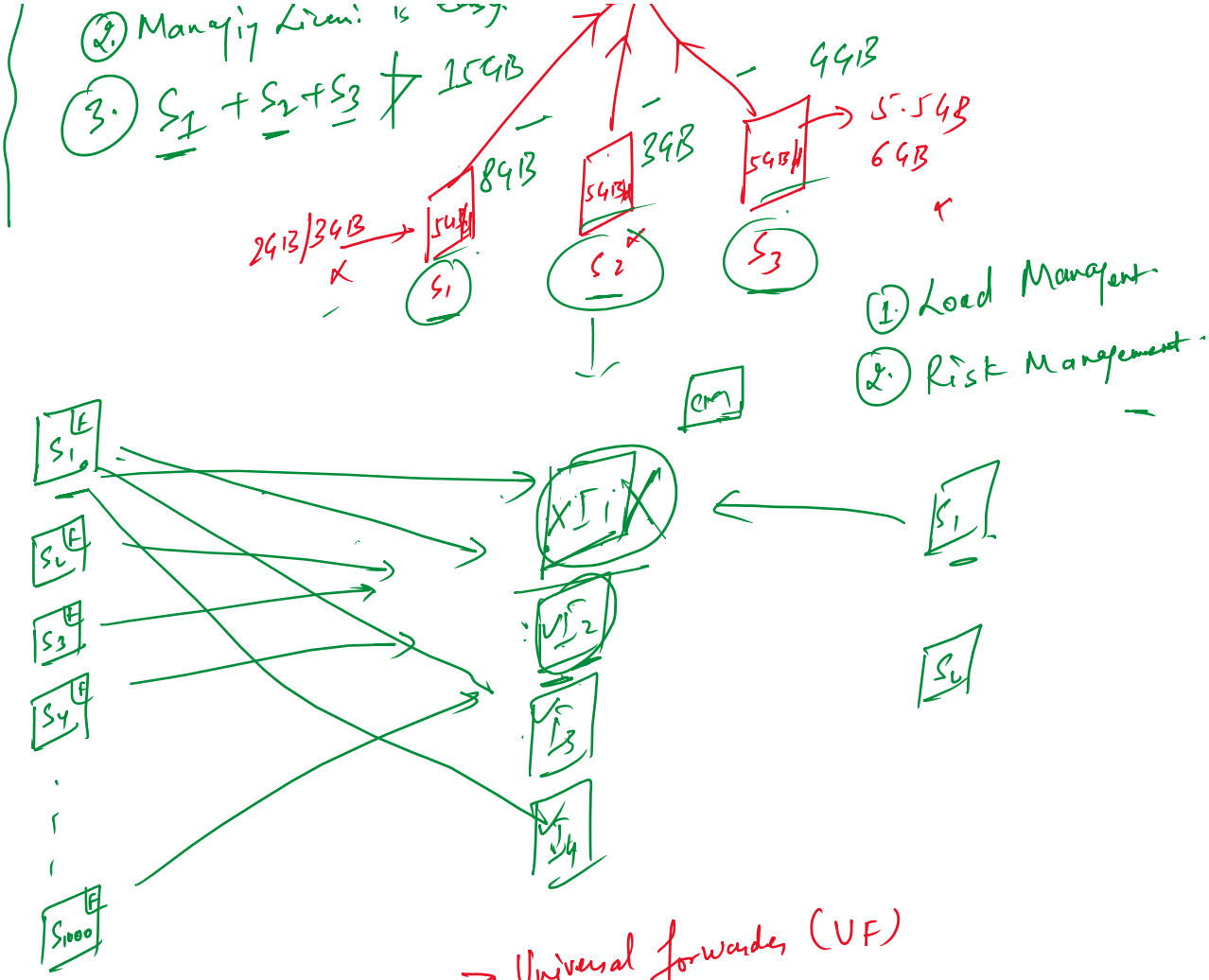


30 days → 5 times

License Pooling:-

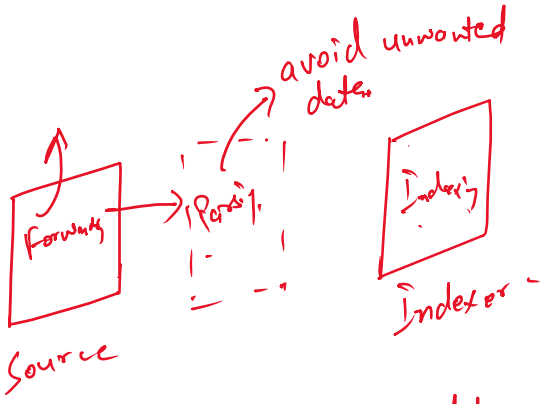
① License Cost is cheaper.
② Managing License is easy.





Forwarders:

- Universal forwarder (UF)
- Heavy forwarder (HF)



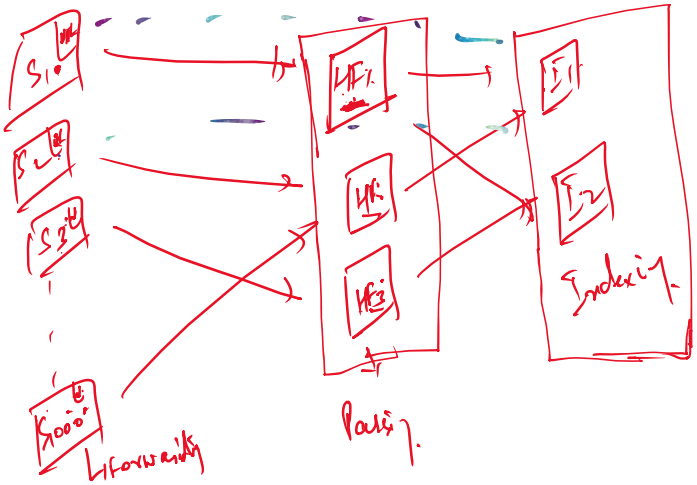
No GUI ← UF → Forward the data, same as it is.
Indexer will do the Parsing activity

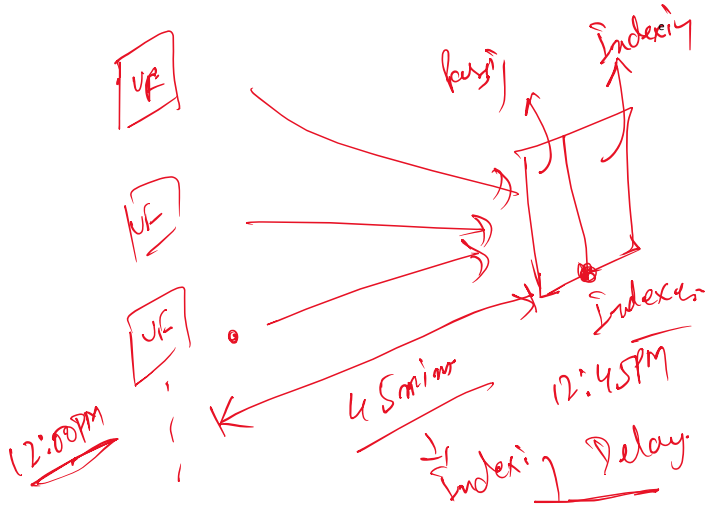
GUI ← HF → Parsing is happening at forwarder side.
Indexer will only do the indexing.

← Including HF, IDX, SH, DS, CM, Deployer, LM — 4.5GB

① Splunk Enterprise - HF, IDX, SH, DS, CM, Deployer, LM - 4.5GB

② splunk UF - Standlone package. - 150MB





Index

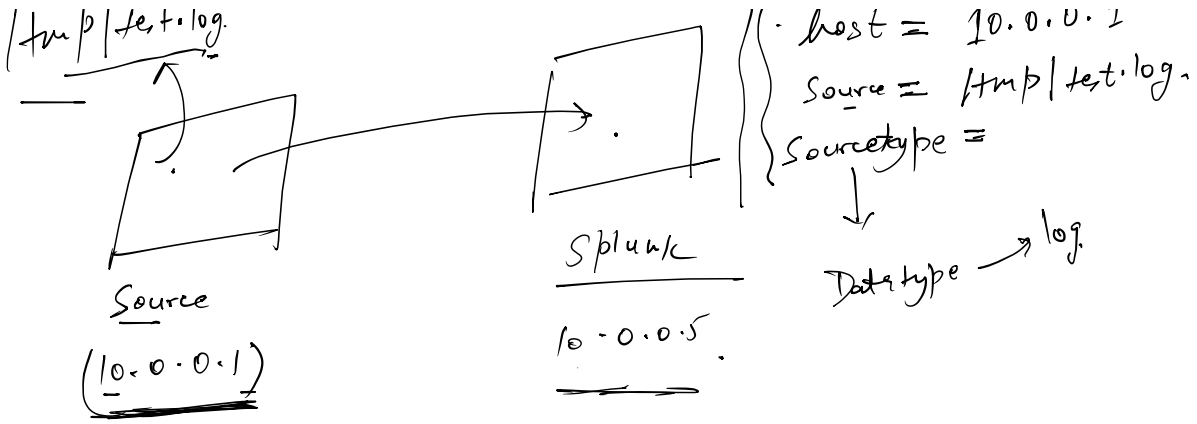
Predefined Index → (_*) → _internal, _audit, _introspection
Reserved for splunk logs.
No License is Consumed.

Default Index → (main) → Index your own data.
License will be consumed.

Custom Index → (VK-main, Sample_idx)
Index name you can customize & Create.
License will be Consumed.

/tmp/test.log

host = 10.0.0.1
source = /tmp/test.log.



SPL Commands:-

1. Table.
2. Rename.
3. dedup
4. Stats.
5. eval.
6. Addtotal.
7. Addcoltotal.
8. Sort.
9. Spath.
10. Join
11. append.
12. Transaction.
13. chart.
14. Timechart.
15. Geomaps.
16. Sitzevalue

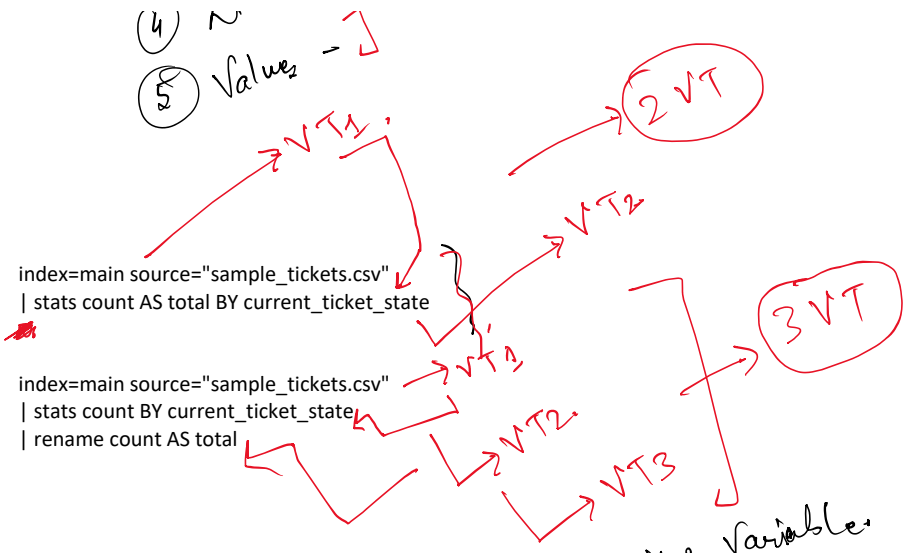
→ Visualization.

1. Table:- |table f1, f2, f3 - - -

2. Rename:- |rename count AS Total.
count → Original field Name.
AS → clause → New field Name.

3. Stats:- Statistical output.
1. Count -- Count of events. Ex:- |stats count BY severity.
2. Sum - } Summation
3. Avg. - } Average Value
4. List - } Grouping
5. Values - } Grouping

|stats sum(bytes) AS Bytes



(4) Eval → Evaluation Activity. → initialize the Variable.

way to initialize the Variable

int a
Str b
Var c

eval a = b+c

(3) Case.

1. Calculation
2. if-else

(1) Calculation:

bytes → Kb

eval (Kb) = (bytes / 1024)

(2) if-else:

```
if (a>b)
  {
  Print(a);
  }

else {
  Print(b);
  }
```

if (a > b, a, b)

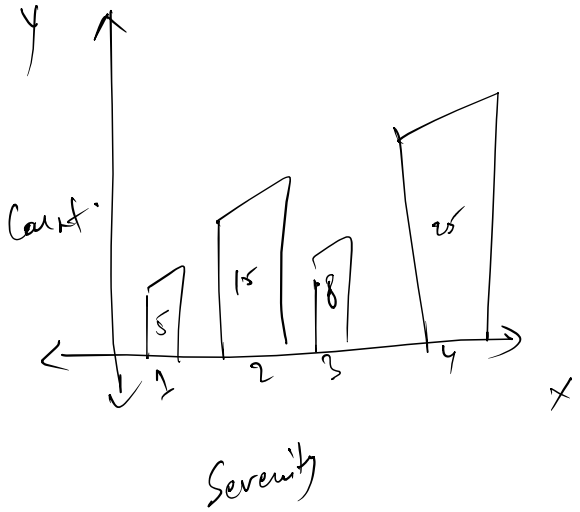
a → True.
b → false.

Conditional statement

3. Case:

```
Switch (a):
    (b):
    .
    .
    .
    default):
```

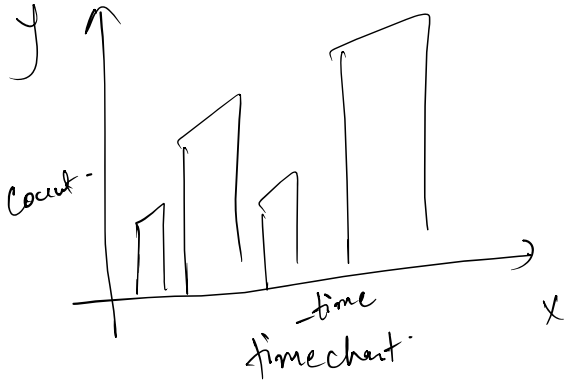
Case (cond1, op1, cond2, op2, ----, 1=1, op_F)



| chart count by severity

count → y-axis

severity → x-axis



| timechart count by current_ticket_state.