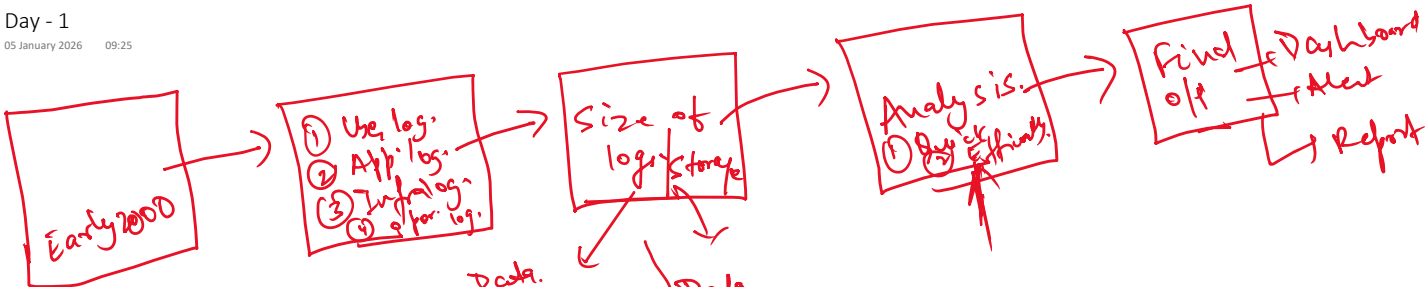
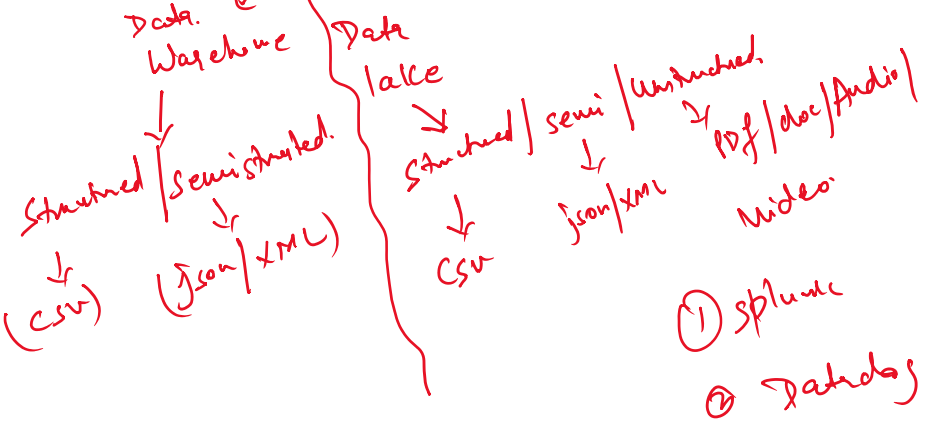
Day - 1

05 January 2026 09:25





① Splunk
② Datadog
③ ELK

1. Splunk:-

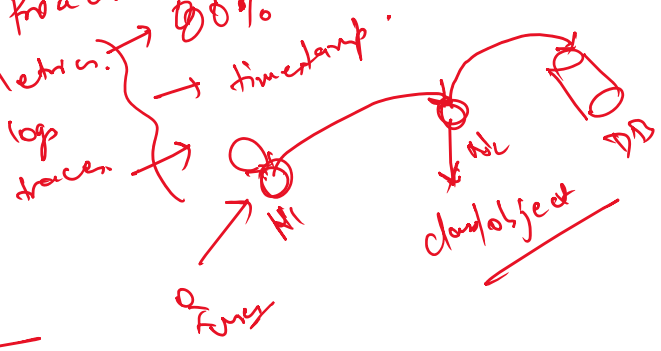
Monitor the log from diff. source / diff. logs.

① Dashboard
② Alert
③ Report
④ Predictive Analysis.

⑤ Machine learning (MLTK)

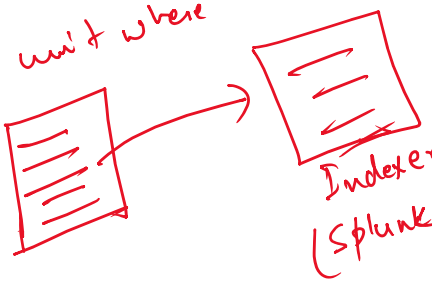
① Monitoring → Reactive.

② observability → Proactive Approach.



Component of splunk:-

① Indexer:- Storage unit where the log will be saved:-

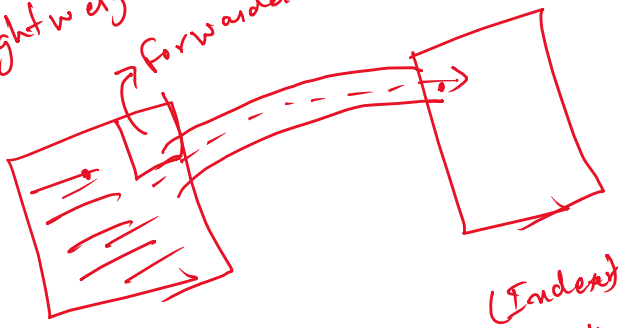


the log will saved.

Source. (App)

(Splunk)

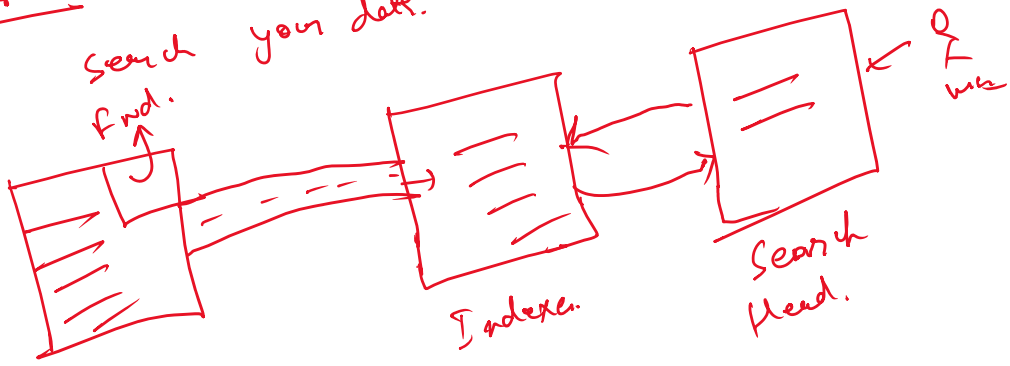
② Forwarder:- → lightweight package that will forward the log from source to the splunk side.



Source (App)

(Indexer) Splunk.

③ Search Head:- → GUI where the user will go & search your data.



Source

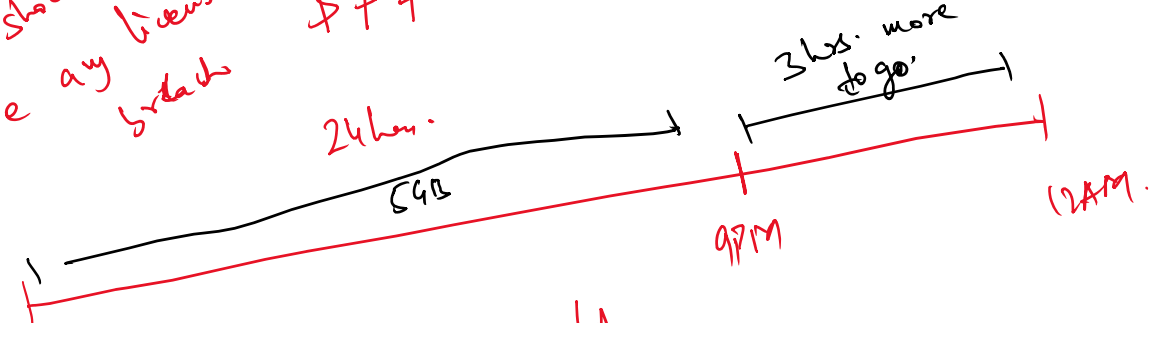
Indexer.

④ License Master:- → How much data you ingest on the daily basis.

Policy Agent that will make sure that their should be any license breaks

5GB/day → 1 year.

$ $ $



① Payment letter for extra data.
② Secondary storage & once you pay, you can use it.
③ License Quota from next day.

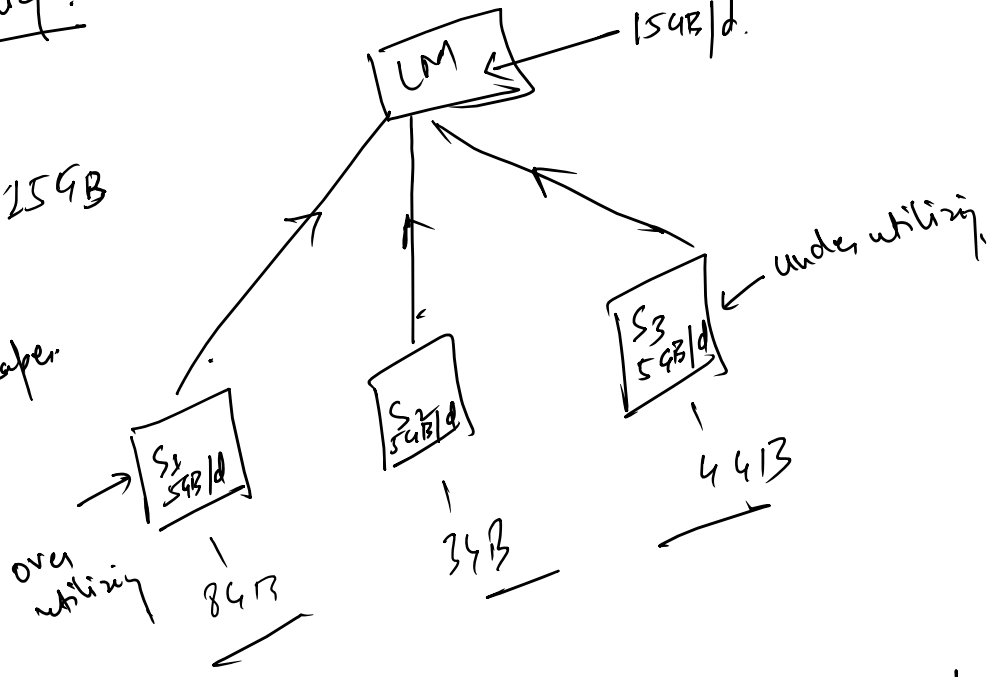
① Data will continue to index
No searching at all.
↓
Dashboard, Alert & Report.
↓
System will come to stable mode.
↓
Flag state.

5 License Breach
↓
30 days window.

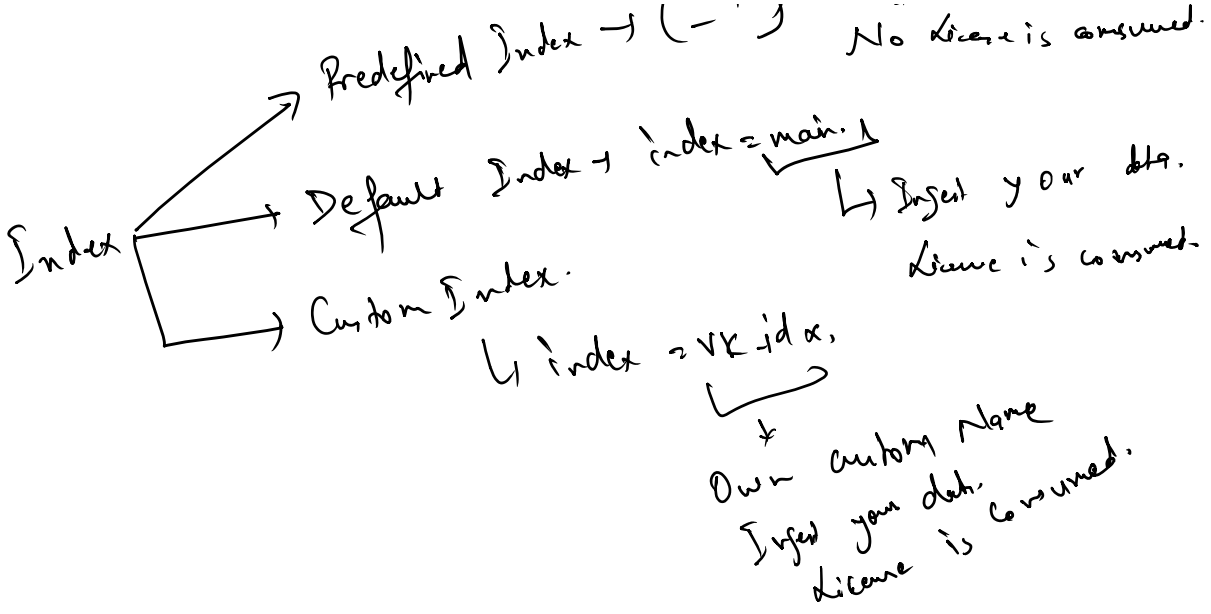
License Policy :-

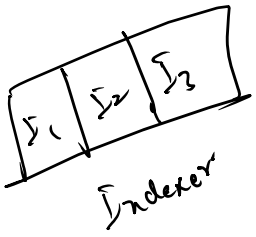
$S_1 + S_2 + S_3 \not> 15GB$

Bulk cost is cheaper.

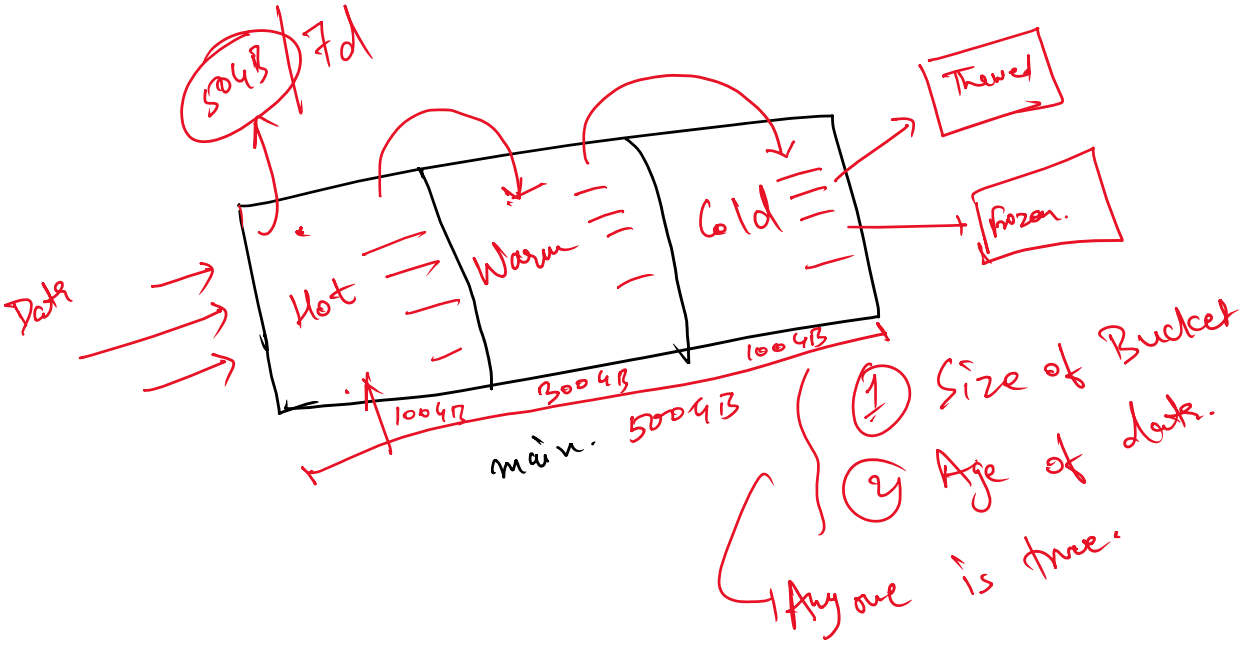


- Predefined Index → (_ *) → Only reserved for internal data.
No License is consumed.





① pulling of your event.
② field extraction. → not happening in fast mode.



SPL:-

1. Table.
2. Rename.
3. Dedup
4. Sort.

1. Table → Tabular output.

Syn:- |table f1, f2, f3 - - -

2. Rename → rename field

Usecase level.

Syn:- |rename ON AS NN

3. Dedup → Remove duplicate values.

Syn:- |dedup f1

4. Sort → Sorting purpose.

|sort f1 → Ascending Order.

|sort - f1 → Descending order.