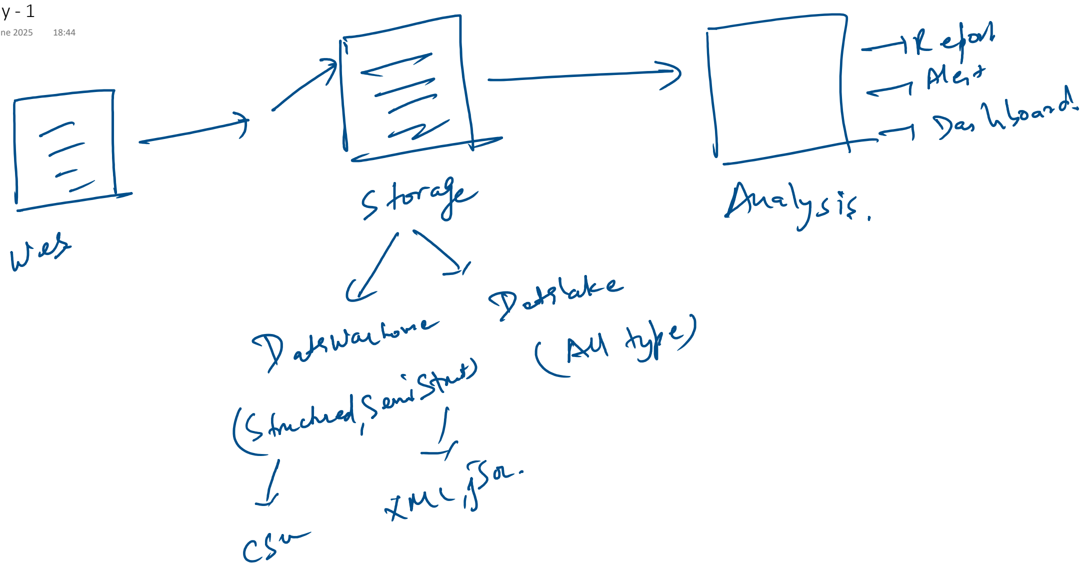
Day - 1

02 June 2025 18:44

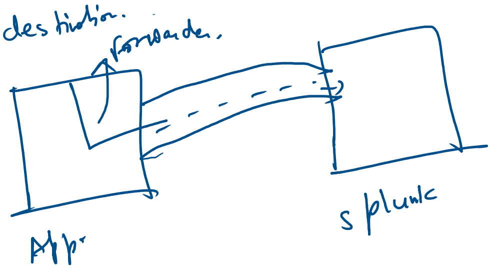


Component of splunk

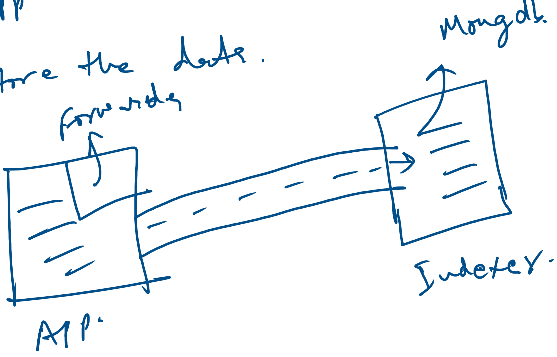
1. Forwarder
2. Indexer
3. Search head
4. License master
5. cluster master
6. Deployer
7. Deployment server

→ Management Server

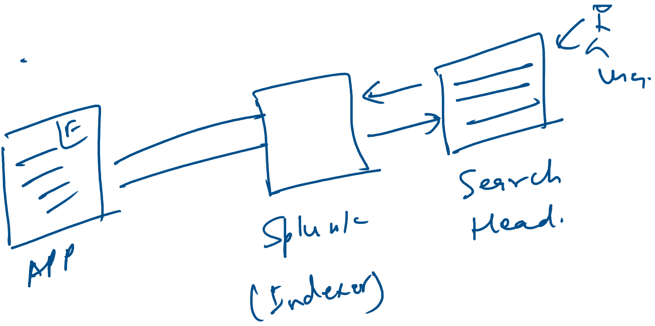
1. **Forwarder:-** Forward data from the source to the destination.



2. **Indexer:-** Store the data.



3. **Search Head:-** GUI.



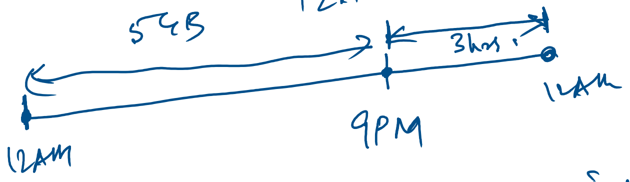
4 License master   Licensing

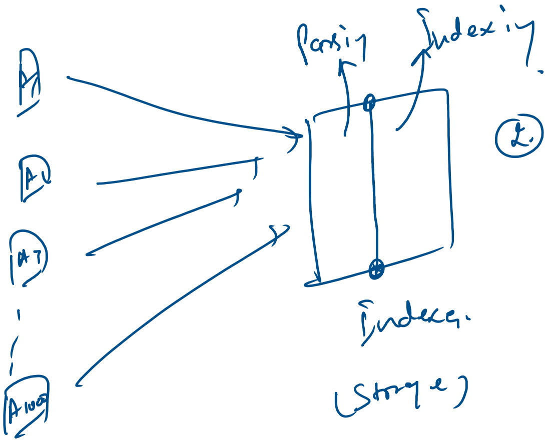
1. How much data you ingest on the daily basis?

5GB/day → 1 year → $$$

24hrs Cycle

12AM — 12AM



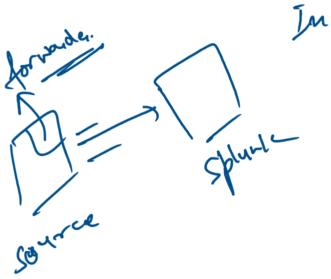


1. Data is stored ~~Segu~~ Secure.

2. Searching will be ~~display~~ disable.

I1	I2	I3	I4

Indexes

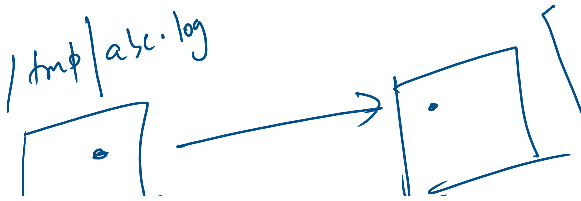


Index → Predefined Index → (_*) (internal dataset) (License not calculated)

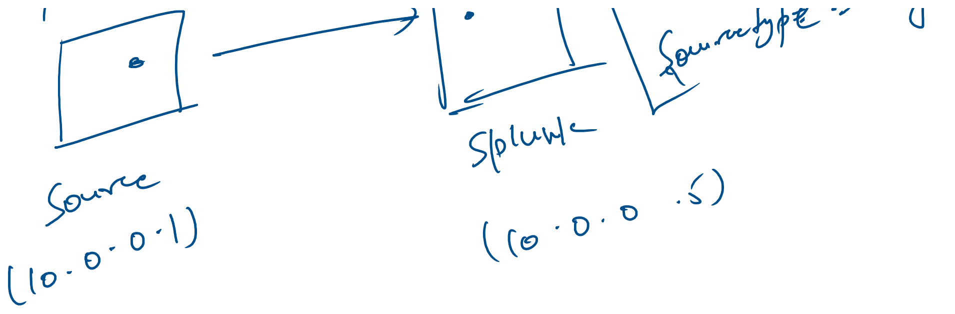
→ Default → "main"
↳ have the default data.

→ Custom Index
↓
vk_idx , Emp_list

License consumed,



host = 10.0.0.1
Source = /tmp/abc.log
Sourcetype = log (Datatype)



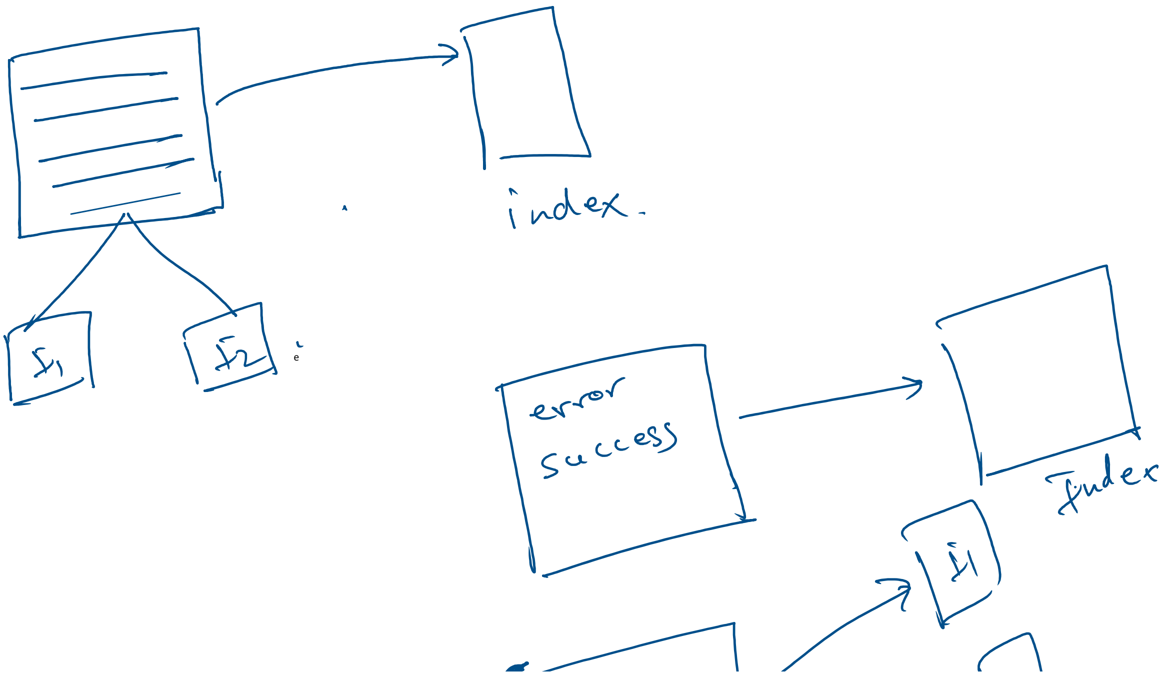
9AM - 9PM

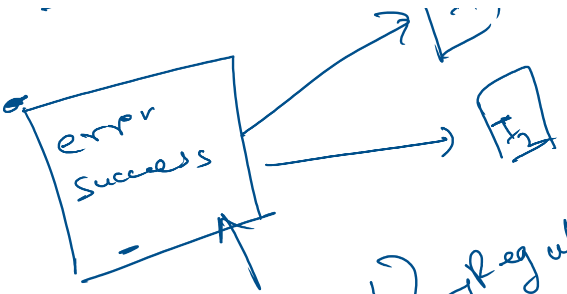
1. 2-3 PM

Mode → Smart Mode
→ Fast mode
→ Verbose Mode

Searching → Extract the fields + No. of events → Fast Mode → Smart Mode

Verbose mode - flexibility to navigate b/w Statistics & event tab.





Sourcetype/host/source ← {props.conf / transform.} → Regular expression

SPL :-

① Table.

② Rename

③ stats.

④ dedup

⑤ fillnull

⑥ sort

⑦ addcoltotal / addtotal.

⑧ Top / Rare.

1. Table:- Tabular output.

| table f1, f2, f3

f1	f2	f3

field Name → Case sensitive

field Value → Case insensitive.

(2.) **Rename:-** Rename the field.

|rename old-name AS New_name.

(3) **stats:-** Statistical data.

- → count → overall count of data.
- → Sum → |stats sum(numeric) as total.
- → Avg → |stats avg(numeric) as avg.
- → list → group the value.
  - → duplication.
- → Values →
  - → unique

(4.) **Top & Rare:-**

Top → Top 10 values.

|top sourcetype.

|top limit=3 sourcetype → top 3values.

Rare → Rarest 10 value
least

|rare sourcetype

|rare limit=3 sourcetype

|rare limit=0 sourcetype. → Unlimited.

(5) Sort → sorting . . → Ascending

(5) Sort → sorting

| Sort count → Ascending

↓ ↳ Default

+

| sort - count → Descending

(6) Eval → Evaluation purpose.

int a

var b

(1) Calculation.

(2) Case

(3) if-else

(1) Calculation:-

bytes → KB

(2) if-else:-

```
if( Condition)
    {
      Print(a);
    }

else { Print(b);
     }
```

→ if(a>b, a, b)

a>b ↓ Condition

True ↖ false

③ Case statement:-

Case (s1,"—", s2,"—", s3,"—", $\underbrace{1=1}_{1,}$,"—")

universal

⑦ Addcoltotal | Addtotal :-

Addcoltotal:- Column wise addition.

addtotal: Addition of Row wise.

Chart:-

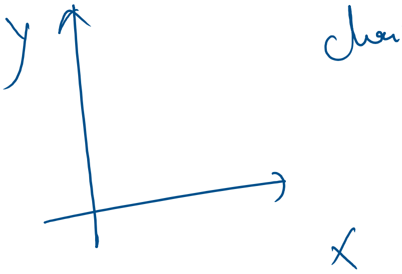
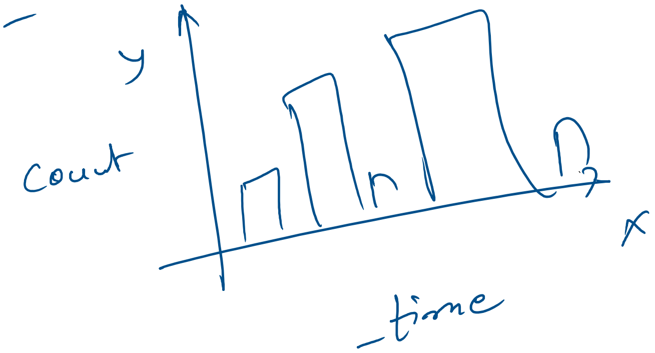


chart $\underbrace{\text{count}}_{Y}$ by $\underbrace{\text{severity}}_{X}$

Timechart:-



Single Value Visualization:-

visualize the single

Single V

Visualize the Single numeric Value