Day - 2

26 December 2024 14:35

① Basic Commands.
- eval - if-else
- Case
- Chart
- timechart
- Single Value Visualization.
- GeoMap
- Custom Visualization.
- Date&time function.
- Addcoltotal.
- Addtotals
- Sort

② Advance Commands:-
- Rex
- append | appendcols | appendpipe.
- join
- spath
- multikv
- mv
- makeresults
- eventstats
- streamstats

① Eval :- if else:- Initialize the Variable.

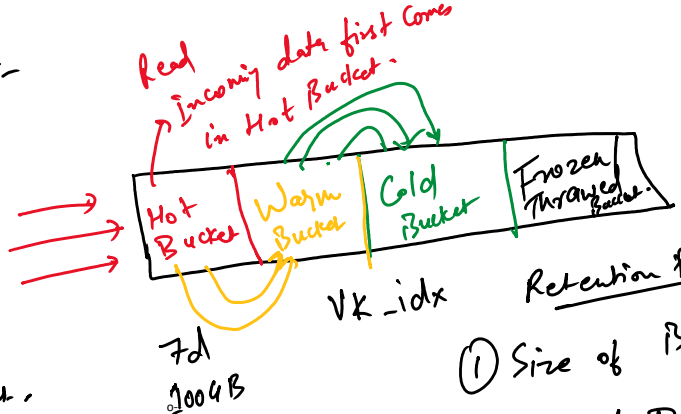
```
if(a>b)
  {
  Print a;
  }
else {
  Print b;
  }
```

```
if (Condition, True, False)

if (a>b; a; b)
```

Condition - True - False

Bucket Concept in splunk:-



① Hot Bucket
② Warm Bucket
③ Cold Bucket
④ Frozen & thrawed Bucket.

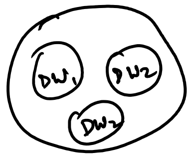
Retention Policy :-
① Size of Bucket
② Age of Data in the Bucket.

Data lake:- Any type of data - structured, Unstructured, Semistruct.

Structured - csv

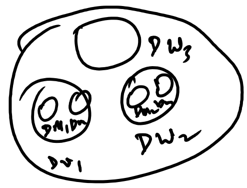
Unstructured - Video, pdf

Semistructured - json, xml



Datalake

Datawarehouse:- Similar data → structured & Semistructured.



Datalake

Datamart:- Subset of Data Warehouse.

Indexes.conf:-

1. homepath - Location.
2. coldpath - Location
3. thawedpath - Location
4. maxHotBucket
   ↓
   max. no. of Hot Bucket allowed.
5. maxWarmDBCount - max. no. of warm bucket to retain b/f roll, to cold.
6. maxTotalDataSize. - Total Size of Index
7. frozenTimeperoidInSecs ⟶ Retention of Index
8. maxDataSize → Size of Individual Bucket

Case statement:-

Case(Cond1, Value1, Cond2, Value2, Cond3, Value3, Cond4, Value4)

switch(0): —
switch(1): —
═
═
default: —

<field1> <field2>

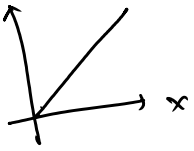
| | | count by severity

Chart:-

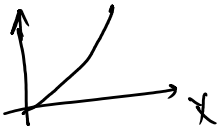
| chart count by severity

<field1> <field2>

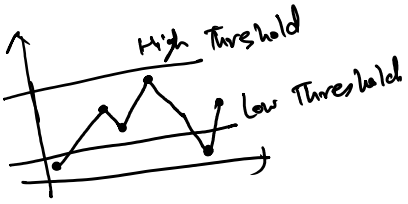
y-axis x-axis

Linear → 

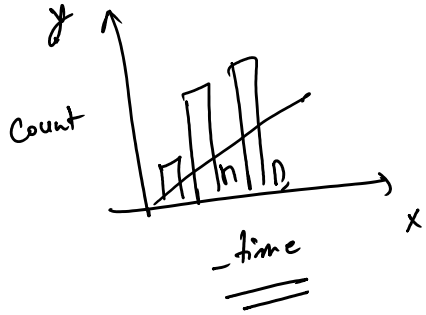
10, 20, 30, 40 - - -

Log → 

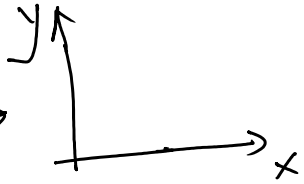
10, 100, 1000, 10000



Timechart:-



time_submitted
closed_date.



↓
external source.

Convert time field into epoc format.

Strptime

strptime(time_submitted, "____")

↳ Converted into epoc format.

09-09-09 09:09

VS → %.m-%d-%.y

EMEA → %.y-%.m-%.d

APAC → %.d-%.m-%.y

Single Value Visualization → | stats count

(timechart) Count.

Geostats Visualization → Latitude, Longitude.

| geostats latfield=VendorLatitude longfield=VendorLongitude count by Vendor

Install Custom Application →

1. Creater / owner of the App.
2. Compatability - Product, Version.

- Addcoltotal :- Addition Column wise

Addtotal :- Addition row wise.

Rex :- Regular exp. to extract the field from the raw event.