Day - 2

05 August 2025 08:05

1. chart vs timechart. →

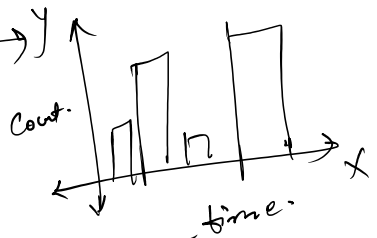


chart f1 by f2

↓ ↓

y x

span = interval ↳ interval

↓ ↓

Splunk. DSL

DSL → Dynatrace Query language

Pipe operator → chaining command.

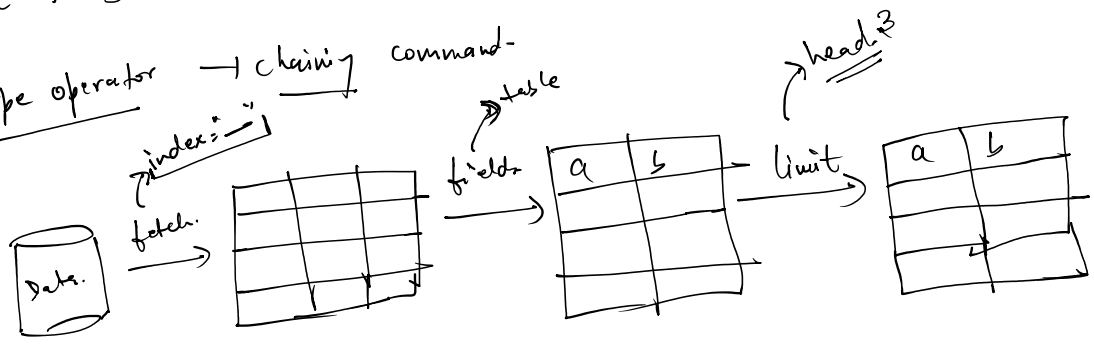


table or collection of table contains data

load data:-

fetch logs.

fetch → Defines which data to load from DT.

Search f_N = "_____" → splunk

filter log.source = = "linux.bg" → DSL

DSL operators:-

+ → Sum

− → min.

* → ×

/

%

= → =

== → equal

!= → Does not equal.

AND, OR → Same in splunk & DSL

1<2 XOR 1>2 → true if one operand

/
%
<
<=
>
>=

OR
XOR → Not supported DQL

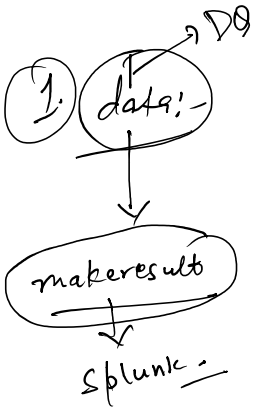
1<2 XOR 1>2
exclusive or true if one operand is true.

DQL commands →

- Aggregation Command → fieldsummary, summarize
- Correlation & join Command → append, join
- Data Source Command → data, describe, fetch, load.
- Extraction Command → parse → DPL, matchpattern
  - rex
- Filter & Search Command → dedup, filter, fieldformat, search
- Metrics Command → timeseries
- Ordering Command → limit, sort
- Selection & modification Commands → fields, fieldsAdd, fieldsRemove, fieldsRename.
- Structuring Command → expand, fieldsflatten.
- Smartscape command
  - Smartscape Node, Smartscape Edges, traverse → Apps → Node Connection Smartscape

DQL

data during Query runtime.



Generate the sample data during Query runtime.

Syn:- data [records] [, json : json_string]

record expression.

string

(2.) describe:- It will help to define the format of the field | dataset.

(3.) fetch :- load the data from the specific data object.

Syn:- DOL

fetch dataobject [, from] [, to] [, samplingRatio] [, time frame]

SPL ← index= main source = 'linux.log'

Sampling :- Set of the sample data out of overall data.

1/ <Sample ratio>

DOL ← fetch logs | ——— , samplingratio : 100

SPL → index= ——— , earliest= -1 latest= ———

|sample rate = 0-1

Only 2 option ← [<Sampleratio> ——— </Sampleratio>

manually drop down.

must have the same value for a given

Summarize:- Group the records that have the same value for a given field & aggregate them

Syn:- Summarize [field=] aggregation, ---[, by: [field=]---]

↓
Stats.

| stats count

| summarize count()

SPL ← [sum — | stats sum(f1) as — by —
avg — | stats avg(f1) as f2

DSL → | summarize sum(f1), avg(f1) —

Stats

① Aggregated Results

② event are removed. only aggregates remain.

③ events | group

eventstats

① Aggregated value to original event.

② Preserve original event.

③ event | group

Streamstats

① aggregated value per event (cumulative)

② Preserve original event.

③ Running aggregation (sequential)

CountDistinct Exact (expression) → DSL
dc (exp.) or Distinctcount(exp.) → SPL
→ correlate

CountIf → Count the no. of records that matches the specific condition.

countIf (condition) → DSL

countIf →

countIf(condition) → DQL

takefirst → Return the first value of a field for a list of a records.

takefirst(a) → DQL

head 1 → SPL

takelast :→ Return the last value of a field for a list of records.

takelast(a) → DQL

tail 1 → SPL

CollectArray :→ Collect the value provided field into an array.

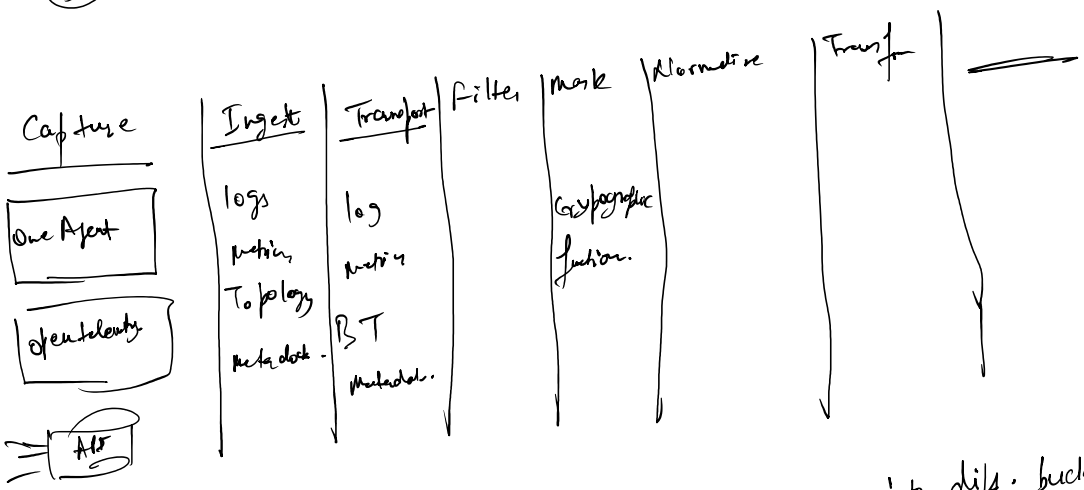
Syn:- collectArray(expression [, expand] [, max length])

* openpipeline in Dynatrace :→ (Dynatrace) → data lakehouse.

(1) Manage ingest of data in grail.

(2) optimize for streaming ingest at large scale.

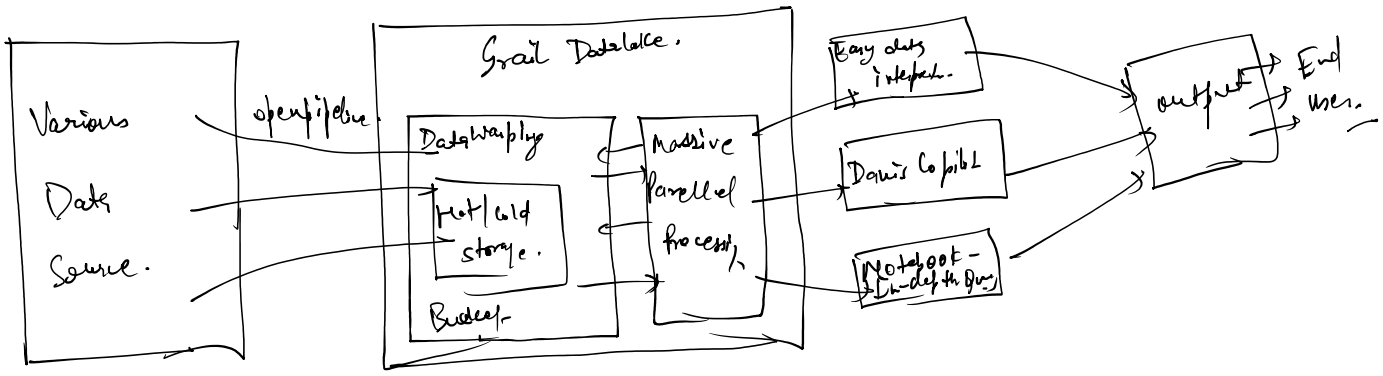
(3) Data processing in real time.



Bucket :→ (1) Split data of diff. type into diff. bucket

(2) Retention of data works on bucketwise.

Budget:- (1) Sp...
(2) Retention of data work...



Value additions-

1. Remove, filter, aggregate or drop data.
2. mask, or hash data.
3. Extract, transform data.
4. Structure & Normalize the data.
5. 1TB/day right now & 2TB+ Near future.