Day - 4

13 August 2024 23:17

1. Event Breaking.

~~2~~ Timestamp

2 Index

4 Search Command - join, Append, Transaction, field, sort

5 Lookup & Field extraction.

1. Event Breaking:-

1 I can onboard:-

- 1 Size of data. — App Owner
- 2 Type of data.
- 3 Sample logs.-
- 4 PII Data.
- 5 Outcome from Data. Min 48 hrs.
- 6 How much data! why!!

1. New Index need to create

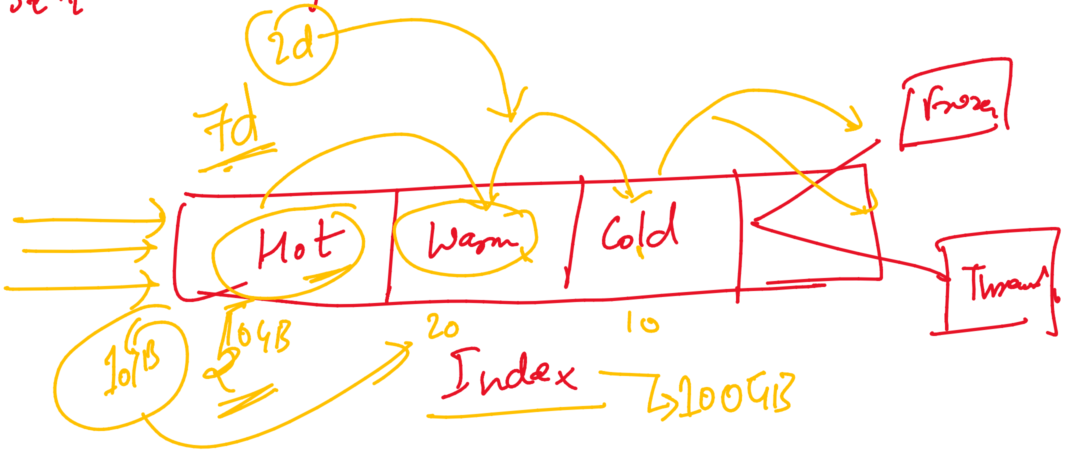
2. Structure of data. ← Field extraction / Timestamp formatting. / Event Breaking / line Breaking.

3 Sample data.

- 4 CAB → Change Advisory Board - All party Approve.

- 5 Start the change

Index:-



Hot
Warm
Cold
Thrawed frozen.

1 Size of Bucket

2 Age of Data in the Bucket.
→ 7d

Any of the condi Match

Data will move from one bucket to Another Bucket.

Why!!

Increment Search Speed.

Data Retention:- How much older Data you want to retain!!
→ 30d

Search Query:-

Table → Tabular output | table field1, field2, field3 | rename

Rename → Renaming of the field → Search Time field1 as abc
field3 as xyz

Stats →

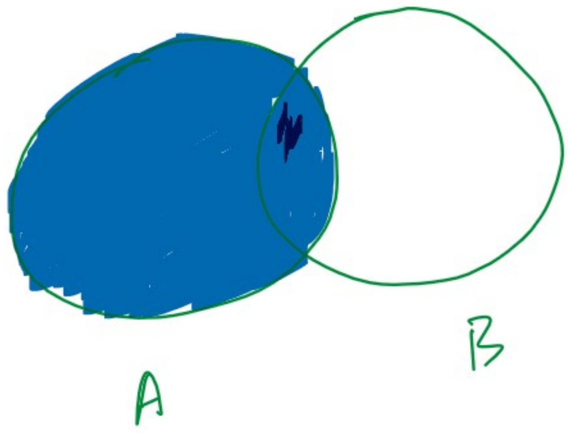
- Count → Count the events
- avg → Avg. value
- sum → Addition of value.
- list → Category & finding the list the values
- values →

old name ← field3 as xyz → New Name.

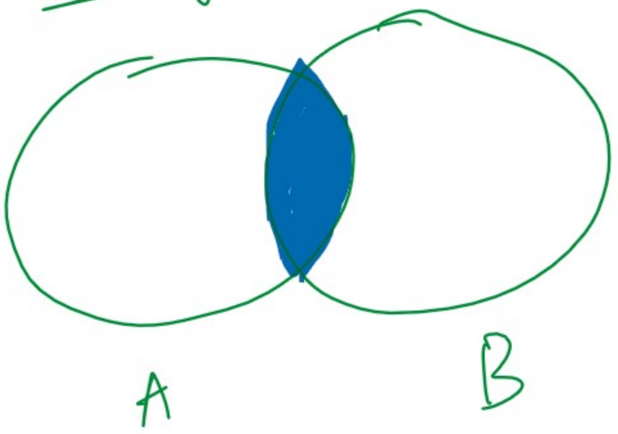
Join:-

- left join.
- Inner join

Left join:-



Inner join

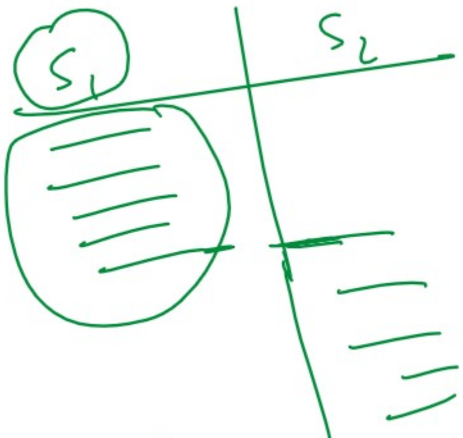


A·

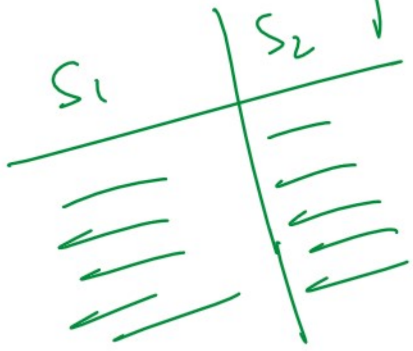
Append :-

append
append col
append pipe.
} →

Append →



Appendcol →



Append pipe:-

O/P S1 → input S2 → output S2