Day - 4

07 August 2025 08:05

Correlation & join Commands:-

1. append.
2. join.

1. append:- Combining a given list of record returned by sub queries.

Syn:- append executionBlock.

Q1 | append [Q2]

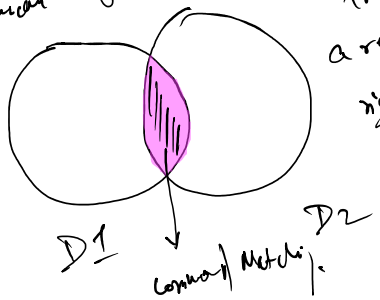
2. join:- merge two diff records of two tables & form a new table by matching record from each table.

1. Inner join - Default type of join.
2. left outer join
3. Outer join

Syn:- Q1 | join [Q2], on: {Unique-field}, kind: —

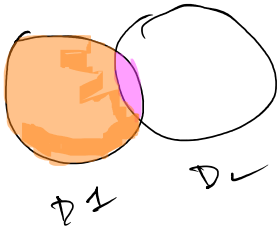
1. Inner join:- Default behaviour of the DQL join.

Produce the o/p record whenever a record in left (Q1), matches with right (Q2)



2. left outer:-

left side & only matching record from right side. If there no matching, it will only show left side record only



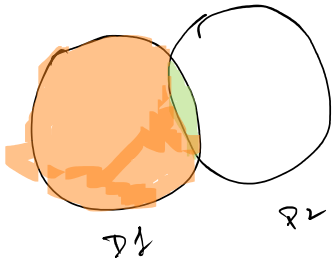
1. left 2. inner

2. Inner:-

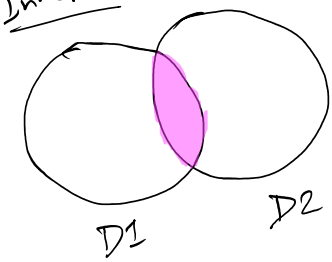
Splunk:-

1. left
2. inner

1. left



2. Inner



Syn:-

```
Q1 | join unique-key type="inner|left"
   [search Q2]
```

3. DQL → Outer joins → return matched & unmatched record from either or both side.

4. joinNested command:- one of the category of join command.

Adds matching result from the subquery as an array of nested records.

Syn:- Q1 | joinnested variable = [Q2], on:{key}

* Metrics Command:- timeseries command in DQL
  ↳ used in the starting of the query

Syn:- timeseries [column=] aggregation(metrickey[, filter,] [,rate:] [; interval] [, start:] [, sta

metrics key → key | series should be created for.

rollup → used for aggregation. can be min, max, sum, avg, total.

default → value.

rate → duration.

filter

default ' '
date → duration.
filter → additional filter.

Aggregation filter:-

1. sum.
2. avg.
3. min.
4. max.
5. count
6. percentile.
7. start
8. end

→ timestamp

* Structuring Commands:-

1. expand.
2. field flatten

1. expand:- An array into seperate record.

Syn:- expand. [alias=] expression [, limit]

→ restriction on the number of created record.

2. field flatten:- Extract/ flatten field from a nested record.

Syn:- field flatten expression [, prefix] [! field: {—}] [, depth]

field that you want to be flattened

Array functions

array
arrayAvg
arrayConcat
arrayDistinct
+

record → a = 1, 2, 3, 4

array

arrayCon
arrayDistinct
arrayFirst
arrayLast
arrayMax
arrayMin

Bitwise functions - Calculate bitwise and between two long expression.