timeslice-join.md

1
2
3
4
5
6
7
8
9
10
11
12
13

14

15

16

17
18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

---

id: timeslice-join

title: Timeslice Join Results

sidebar_label: Timeslice Join Results

When you gather data using a [`join`](join.md) operator, you can slice data by time period using the [`timeslice`](timeslice.md) operator.

Syntax

The `timeslice` operator uses the metadata field `_messagetime` to organize the logs by slices. In your query, you need to specify the `timeslice` operator before the `join`, because the `_messagetime` field will no longer exist after the join is performed.

When you add the `timeslice` before the `join`, each of the tables created by the join will include a `_timeslice` field.

You can reference the table's `_timeslice` field to use in your group by operation. The name of the table is appended to the table's fields.

Example

For example, if your table is named *errors*, your field would be `errors__timeslice`. (Notice that the name contains two underscores.)

Here's an example query:

```sql

*

| timeslice 1h

| join

(parse "starting stream from * " AS streamId) AS table1,

(parse "starting search from parent stream * " AS streamId) AS table2

on table1.streamId = table2.streamId

| count table1_streamId, table1__timeslice

| formatDate(fromMillis(table1__timeslice ), "MM/dd/yyyy HH:mm:ss z") as timeslice

```