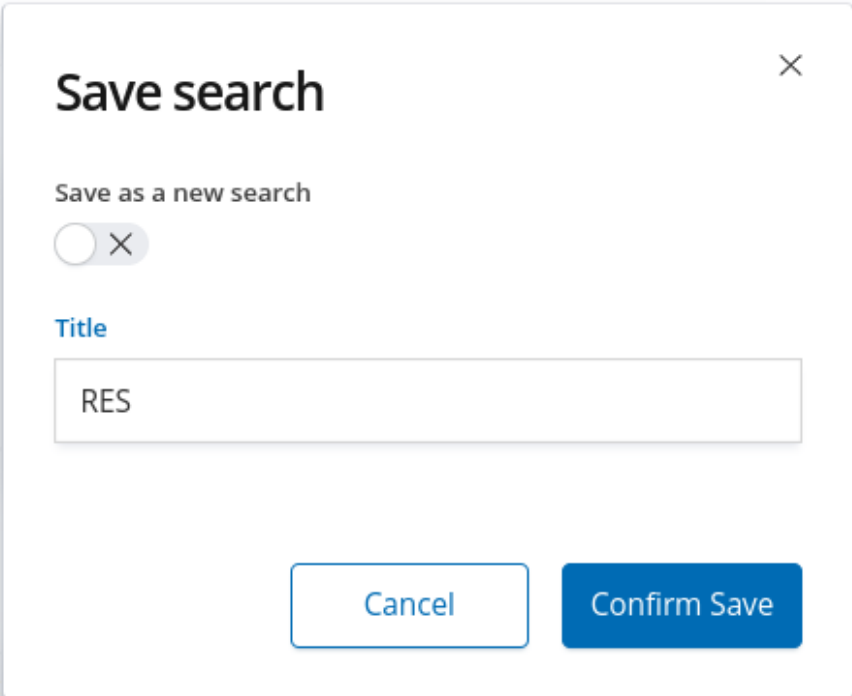


## 6.7.2

- сохранить поисковый запрос по индексу *test-\** за последние 12 часов, где выведены все поля, обработанные в Logstash



Save search

Save as a new search

☐ X

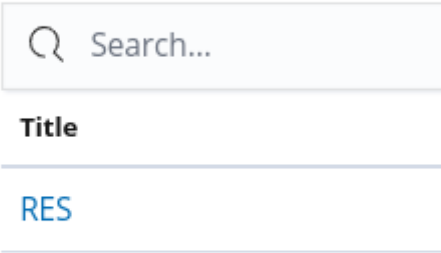
Title

RES

Cancel Confirm Save

---

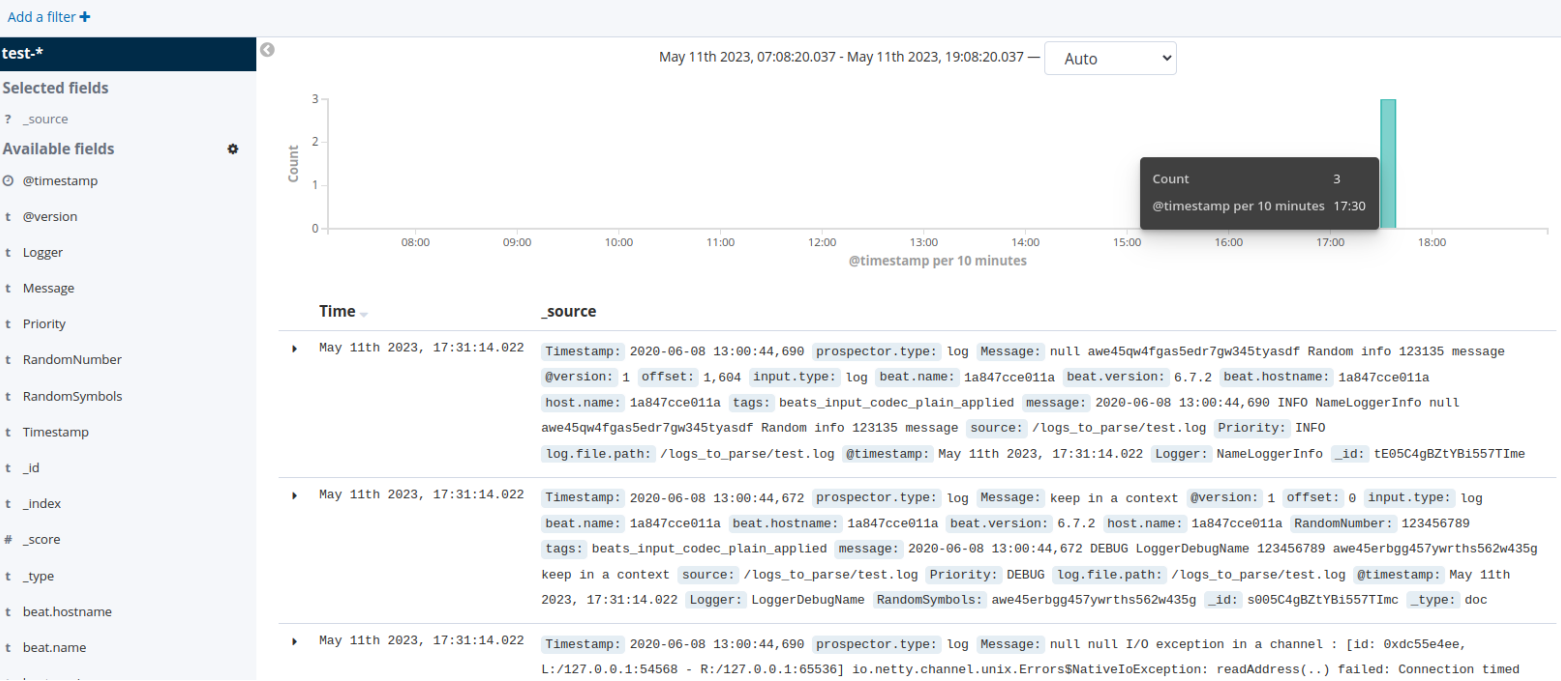
### Open Search



Search...

Title
RES

Rows per page: 10 ▾



Table

JSON

View surrounding documents

View sin

@timestamp	May 11th 2023, 17:31:14.022
@version	1
Logger	LoggerDebugName
Message	keep in a context
Priority	DEBUG
RandomNumber	123456789
RandomSymbols	awe45erbgg457ywrths562w435g
Timestamp	2020-06-08 13:00:44,672
_id	s005C4gBZtYBi557TImc
_index	test-2023.05.11
#_score	-
_type	doc
beat.hostname	1a847cce011a
beat.name	1a847cce011a
beat.version	6.7.2
host.name	1a847cce011a
input.type	log
log.file.path	/logs_to_parse/test.log
message	2020-06-08 13:00:44,672 DEBUG LoggerDebugName 123456789 awe45erbgg457ywrths562w435g keep in a context

- создать визуализацию, в которой указывается кол-во документов для каждого значения поля *Priority*

test-\*

Data

Metrics & Axes

Panel Settings

Metrics

Y-Axis Count

Add metrics

Buckets

X-Axis

Aggregation

Terms help

Terms

Field

Priority.keyword

Order By

metric: Count

Order

Descend

Size

5

☐

Group other values in separate bucket ?

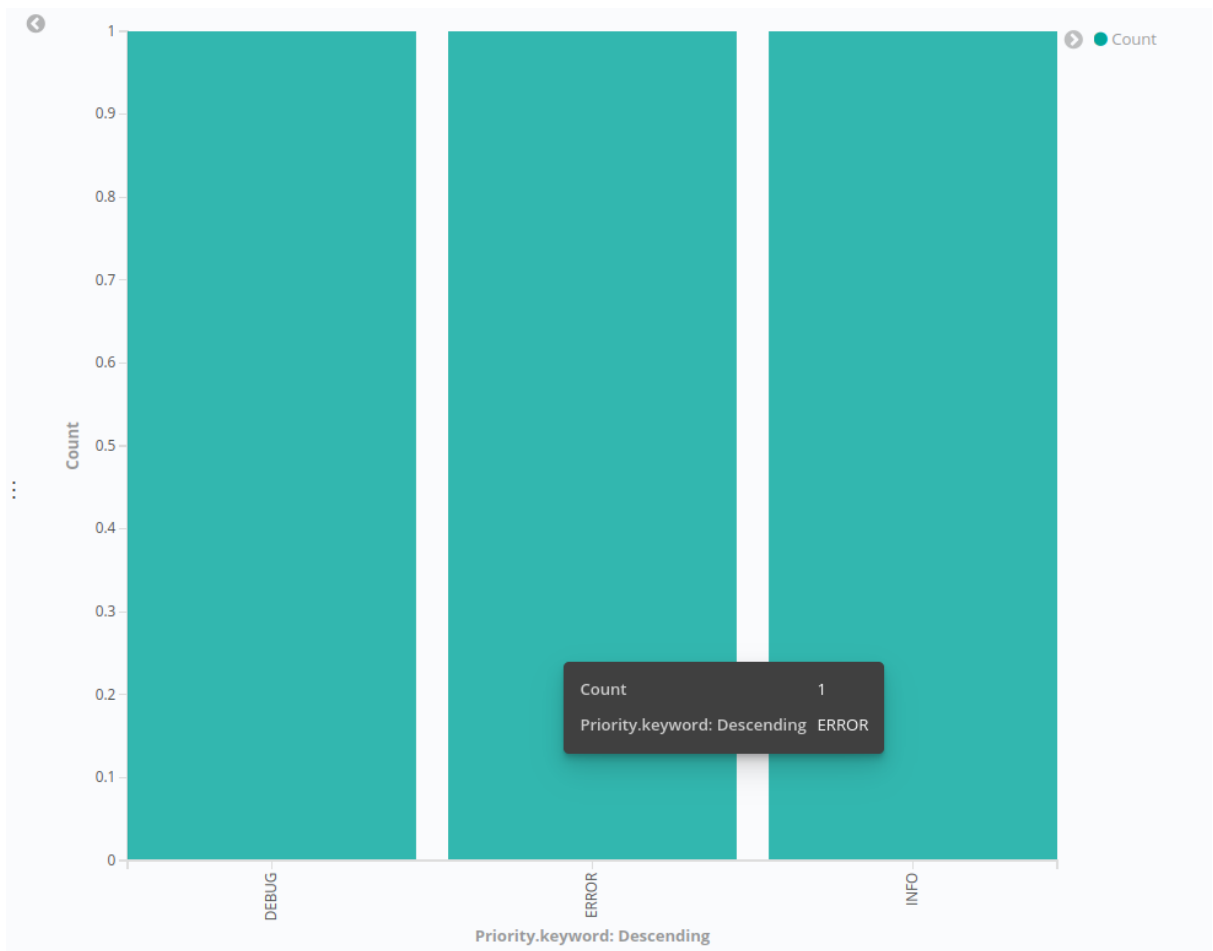
☐

Show missing values ?

Custom Label

Advanced



Add sub-buckets




- такую же визуализацию, но уже для поля *Logger*

**test-\***

[Data](#) [Metrics & Axes](#) [Panel Settings](#)




 

### Metrics

 **Y-Axis** Count

Add metrics

### Buckets

 **X-Axis**  

Aggregation [Terms help](#)

Terms

Field

Logger.keyword

Order By

metric: Count

Order

Descending

Size

5

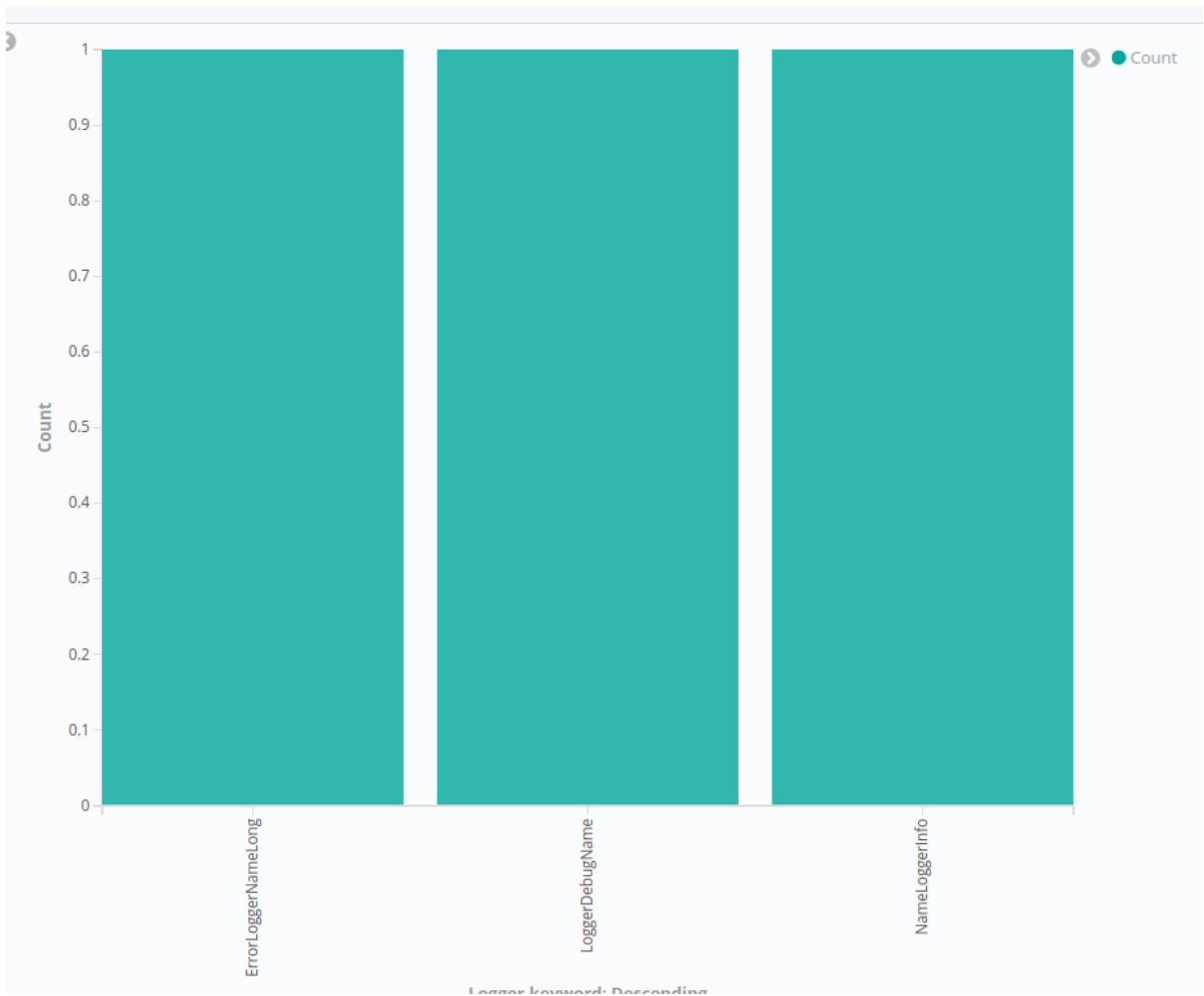
☐ Group other values in separate bucket ?

☐ Show missing values ?

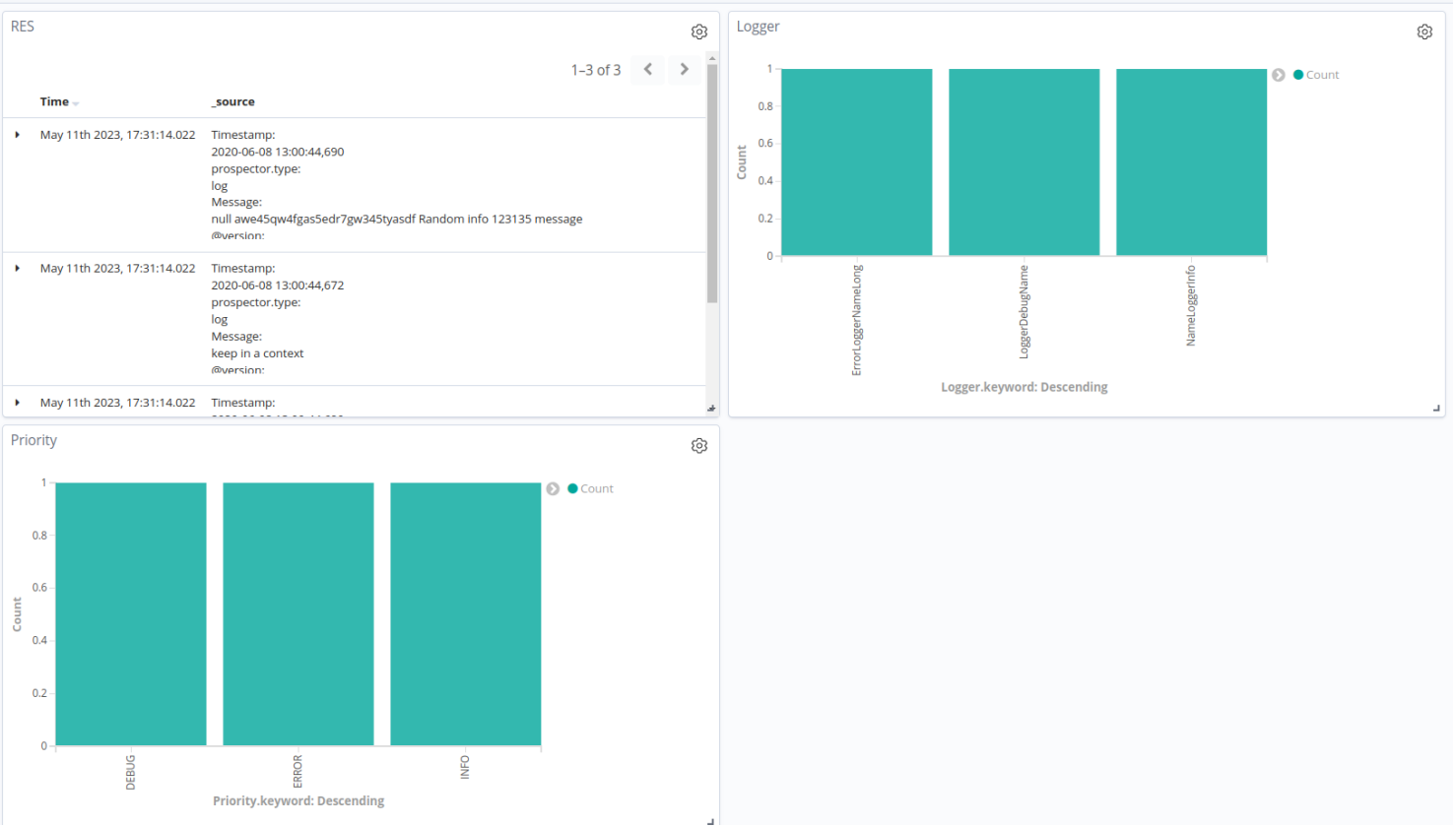
Custom Label

[Advanced](#)

Add sub-buckets



- создать *dashboard*, в котором будут содержаться все выше перечисленные запросы и визуализации



### 7.7.0

*- сохранить поисковый запрос по индексу test-\* за последние 12 часов, где выведены все поля, обработанные в Logstash*

×

## Save search

Save your Discover search so you can use it in visualizations and dashboards

Title

RES

Cancel

Save

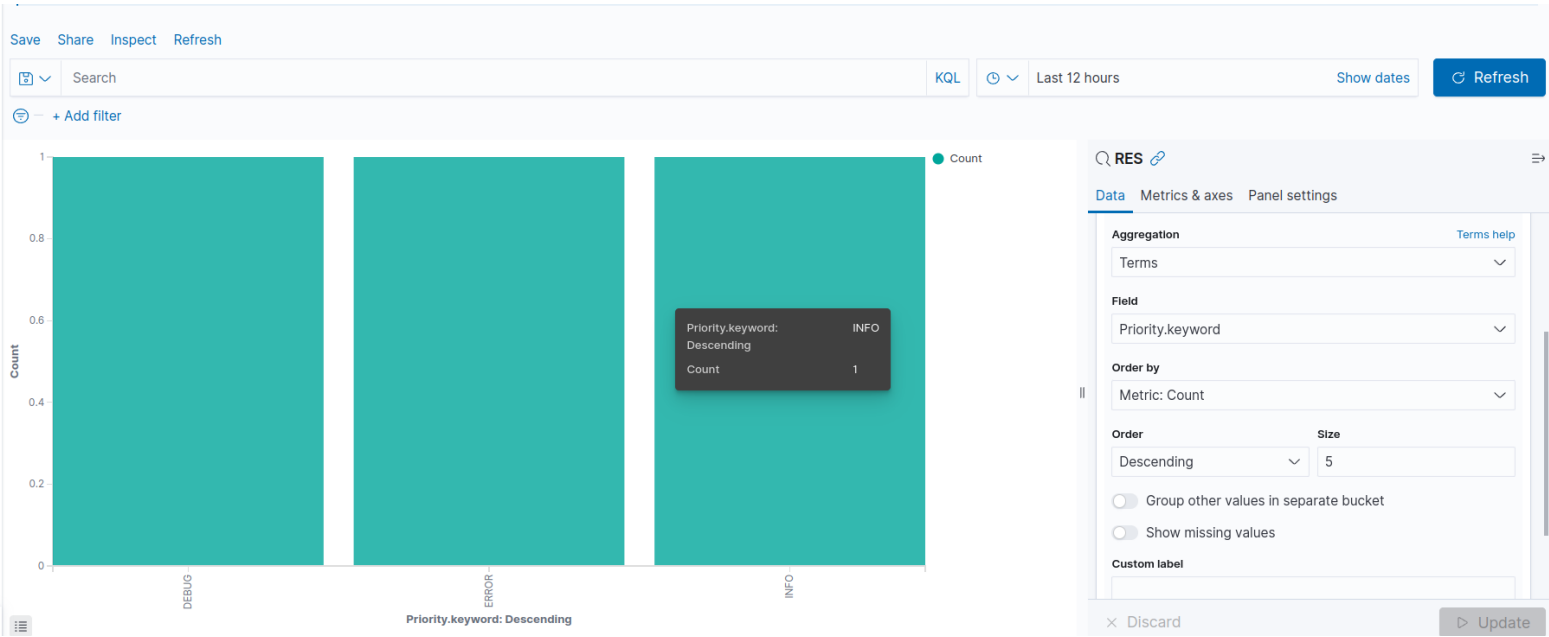
## Open search

🔍 Search...

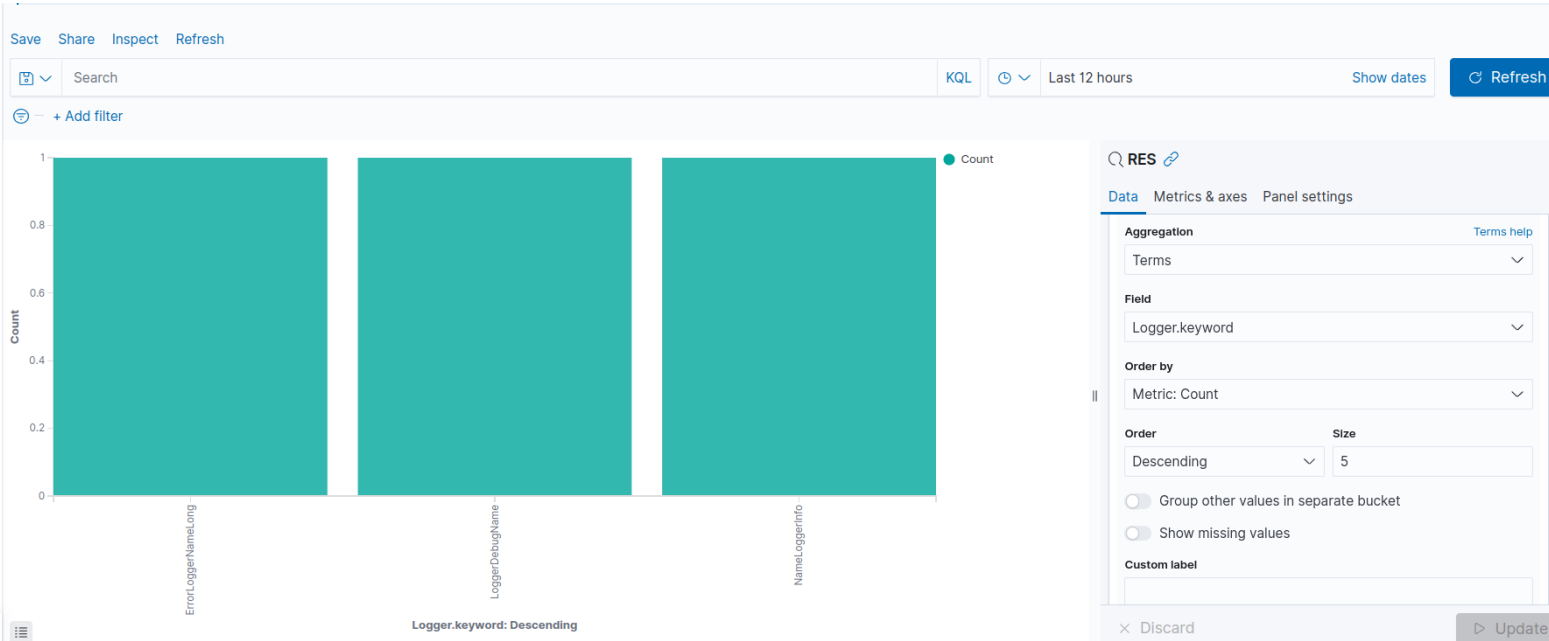
🔍 RES



**- создать визуализацию, в которой указывается кол-во документов для каждого значения поля *Priority***



**- такую же визуализацию, но уже для поля *Logger***



- создать *dashboard*, в котором будут содержаться все выше перечисленные запросы и визуализации

