

graylog

SearchViewsStreamsAlertsDashboardsSourcesSystem1

0 in0 out?

Search in all messages

message: flask-logs

Update every 5 seconds

Saved searches

Search result

Found 21,455 messages in 4 ms, searched in 1 index.

Results retrieved at 2020-02-18 13:32:52.

Add count to dashboard

Save search criteriaMore actions

FieldsDecorators

DefaultAllNoneFilter fields

api_datetime

api_event_status

api_execution_time

api_request_name

List fields of current page or all fields.

Highlight results

Histogram

Add to dashboard

Year, Quarter, Month, Week, Day, Hour, Minute

1.5K

1K

500

Thu 13

Fri 14

Sat 15

Sun 16

Feb 17

Tue 18

Messages

Previous12345678910Next

Timestamp

source

2020-02-18 10:21:03.000

api

api flask-logs

INFO:root: Tempo de execucao - 0.00734

2020-02-18 10:21:03.000

api

api flask-logs

INFO:root:2020-02-18 13:20:54.465643 - Inicio da Requisicao get_data_order_by_lang

Um filtro simples no Graylog, buscando mensagens com a palavra flask-logs, padrão no log que foi desenvolvido

graylog

Search

Views ▾

Streams

Alerts

Dashboards

Sources

System ▾

1

0 in
0 out

?

Search result

Found **21,455 messages** in 2 ms, searched in [1 index](#).
Results retrieved at 2020-02-18 13:32:52.

Add count to dashboard ▾

Save search criteria

More actions ▾

Fields

Decorators

Default

All

None

Filter fields

▶ ☐ api_datetime

▶ ☐ api_event_status

▶ ☐ api_execution_time

▶ ☐ api_request_name

▼ ☐ api_severity

Generate chart

Quick values

Statistics

List fields of **current page** or **all fields**.

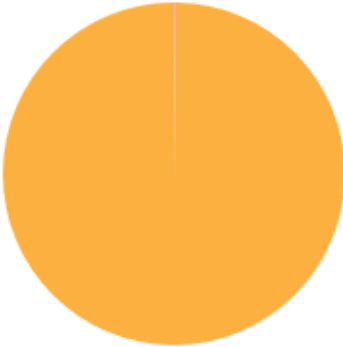
☒ Highlight results

Quick Values for *api_severity*

Add to dashboard ▾

Customize ▾

✕




Found 9,980 messages with field *api_severity*, and 11,475 messages without field *api_severity*.

Value	%	Count
Top 5 values		
INFO	99.88%	9,968
ERROR	0.12%	12

Histogram

Add to dashboard ▾

Year, Quarter, Month, Week, Day, Hour, Minute



O filtro de mensagens aqui foi criado através de um extrator do Graylog (expressão regular), trazendo somente a severidade do log.

graylog

SearchViewsStreamsAlertsDashboardsSourcesSystem1

0 in0 out?

Search in the last 1 day

Not updating

Saved searches

message: flask-logs

Search result

Found 71,065 messages in 39 ms, searched in 1 index.
Results retrieved at 2020-02-19 11:29:14.

Add count to dashboard

Save search criteria

More actions

FieldsDecorators

DefaultAllNoneFilter fields

api_datetime

api_event_status

api_request_name

api_severity

Generate chart

Quick values

Statistics

List fields of current page or all fields.

Highlight results

Quick Values for api_severity

Add to dashboard

Customize

Found 71,065 messages with field api_severity.

Value	%	Count
Top 5 values		
INFO	99.59%	70,773
ERROR	0.41%	292

Histogram

Year, Quarter, Month, Week, Day, Hour, Minute

40K

Add to dashboard

Aqui temos o mesmo filtro de severidade, com mais ocorrências de erro no Log.

graylog

Search

Views ▾

Streams

Alerts

Dashboards

Sources

System ▾

1

0 in
0 out

?

Search result

Found 1 messages in 1 ms, searched in 1 index.
Results retrieved at 2020-02-18 13:47:01.

Add count to dashboard ▾

Save search criteria

More actions ▾

Fields

Decorators

Default

All

None

Filter fields

▸ ☐ api_execution_time

▾ ☐ api_severity

Generate chart

Quick values

Statistics

World Map

▸ ☐ facility

▸ ☐ gl2_message_id

▾ ☐ .

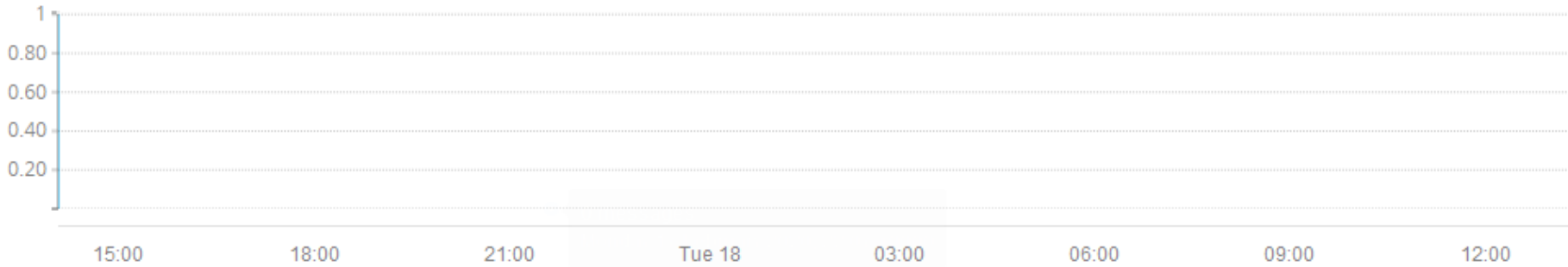
List fields of [current page](#) or [all fields](#).

☒ Highlight results

Histogram

Add to dashboard ▾

Year, Quarter, Month, Week, Day, Hour, Minute



Messages

Previous

1

Next

Timestamp ⓘ

source

2020-02-17 14:34:23.000

api

api flask-logs ERROR:root:2020-02-17 17:34:18.358704 ERROR T1 - Unread result found

Previous

1

Next

Aqui as mensagens de erro foram filtradas através do filtro de mensagens do Graylog, procurando por flask-logs e ERROR.

graylog

Search

Views ▾

Streams

Alerts

Dashboards

Sources

System ▾

1

0 in
0 out

?

Search result

Found **1,934 messages** in 6 ms, searched in **1 index**.
Results retrieved at 2020-02-18 18:04:08.

Add count to dashboard ▾

Save search criteria

More actions ▾

Fields

Decorators

Default

All

None

Filter fields

▶

☐

api_datetime

▶

☐

api_event_status

▶

☐

api_execution_time

▶

☒

api_request_name

▶

☐

api_severity

▶

☐

facility

▶

☐

gl2_message_id

▶

☐

level

▶

☐

List fields of **current page** or **all fields**.

☒ Highlight results

Quick Values for *api_request_name*

Add to dashboard ▾

Customize ▾

✕

Found 1,446 messages with field *api_request_name*, and 489 messages without field *api_request_name*.

Value	%	Count
Top 5 values		
<div></div> get_data_order_by_lang	28.42%	411
<div></div> get_data_order_by_followers	23.86%	345
<div></div> get_data_order_by_country	23.86%	345
<div></div> get_data_order_by_time	23.86%	345

Histogram

Add to dashboard ▾

🕒 Year, Quarter, Month, Week, Day, Hour, Minute

O filtro de mensagens aqui foi criado através de um extrator do Graylog (expressão regular), trazendo as APIs executadas por tipo.

graylog

SearchViewsStreamsAlertsDashboardsSourcesSystem1

0 in0 out?

Search in all messages

▶

Not updating

Saved searches

gl2_source_input:5e4442522ab79c001234f804 flask

Search result

Found 1,934 messages in 6 ms, searched in 1 index. Results retrieved at 2020-02-18 18:04:08.

Add count to dashboard

Save search criteria

More actions

FieldsDecorators

DefaultAllNoneFilter fields

▶

api_datetime

▼

api_event_status

Generate chart

Quick values

Statistics

List fields of current page or all fields.


☑

Highlight results

Quick Values for api_event_status

Add to dashboard

Customize



Found 1,472 messages with field api_event_status, and 1,479 messages without field api_event_status.

Value	%	Count
Top 5 values		
Inicio da Requisicao	50.00%	736
Fim da Requisicao	50.00%	736

Histogram

Add to dashboard

Outro exemplo de filtro usando expressão regular, buscando por chamadas de Inicio e Fim da Requisição.

graylog

SearchViewsStreamsAlertsDashboardsSourcesSystem1

0 in0 out

?

Search in all messages

gl2_source_input:5e4442522ab79c001234f804 flask

Search result

Found 1,934 messages in 6 ms, searched in 1 index. Results retrieved at 2020-02-18 18:04:08.

Add count to dashboard

Save search criteria

More actions

FieldsDecorators

DefaultAllNoneFilter fields

Generate chart

Quick values

Statistics

World Map

☐ api_request_name

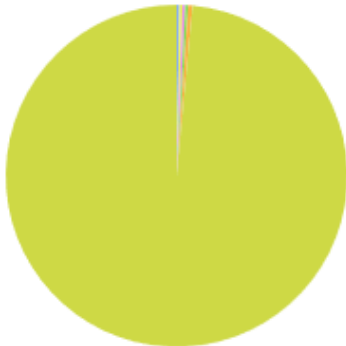
List fields of current page or all fields.

☒ Highlight results

Quick Values for api_execution_time

Add to dashboard

Customize



Found 736 messages with field api_execution_time, 2,215 messages without field api_execution_time, and 658 other values.

Value	%	Count
Top 5 values		
0.003667999990284443	0.41%	3
0.0030819999519735575	0.27%	2
0.003148999996483326	0.27%	2
0.0032210000790655613	0.27%	2
0.0031349998898804188	0.27%	2
Others		
0.007952000014483929	0.27%	2
0.008975000120699406	0.27%	2
0.010507999919354916	0.27%	2
0.0032289999071508646	0.27%	2

Este filtro de mensagens aqui foi criado no Graylog (expressão regular), trazendo somente o tempo de resposta da API.

graylog

SearchViewsStreamsAlertsDashboardsSourcesSystem1

0 in0 out

?

Search in all messages

▶

Not updating

Saved searches

gl2_source_input:5e4442522ab79c001234f804 flask

Search result

Found 1,934 messages in 6 ms, searched in 1 index. Results retrieved at 2020-02-18 18:04:08.

Add count to dashboard

Save search criteria

More actions

FieldsDecorators

DefaultAllNoneFilter fields

api_datetime

Generate chart

Quick values

Statistics

World Map

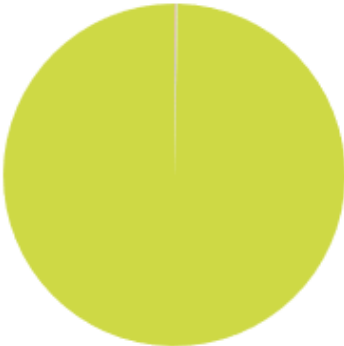
List fields of current page or all fields.

☒ Highlight results

Quick Values for api_datetime

Add to dashboard

Customize



Found 1,472 messages with field api_datetime, 1,479 messages without field api_datetime, and 1,422 other values.

Value	%	Count
Top 5 values		
2020-02-18 18:06:43.564501	0.07%	1
2020-02-18 18:06:43.574572	0.07%	1
2020-02-18 18:04:29.341796	0.07%	1
2020-02-18 18:07:17.962254	0.07%	1
2020-02-18 18:04:29.329845	0.07%	1
Others		
2020-02-18 18:08:34.552599	0.07%	1
2020-02-18 18:08:34.153805	0.07%	1
2020-02-18 18:07:17.966370	0.07%	1
2020-02-18 18:08:34.162965	0.07%	1

Outro exemplo trazendo o tempo de resposta.

Add extractor

Start by loading a message to have an example to work on. You can decide whether to load a recent message received by this input, or manually select a message giving its ID.

[Get started](#)

Configured extractors

[Sort extractors](#)

api_execution_time Regular expression

Trying to extract data from *message* into *api_execution_time*, leaving the original intact.

[Details](#)[Edit](#)[Delete](#)

api_request_name Regular expression

Trying to extract data from *message* into *api_request_name*, leaving the original intact.

[Details](#)[Edit](#)[Delete](#)

api_datetime Regular expression

Trying to extract data from *message* into *api_datetime*, leaving the original intact.

[Details](#)[Edit](#)[Delete](#)

api_event_status Regular expression

Trying to extract data from *message* into *api_event_status*, leaving the original intact.

[Details](#)[Edit](#)[Delete](#)

api_severity Regular expression

Trying to extract data from *message* into *api_severity*, leaving the original intact.

[Details](#)[Edit](#)[Delete](#)

Os extratores criados no Graylog.



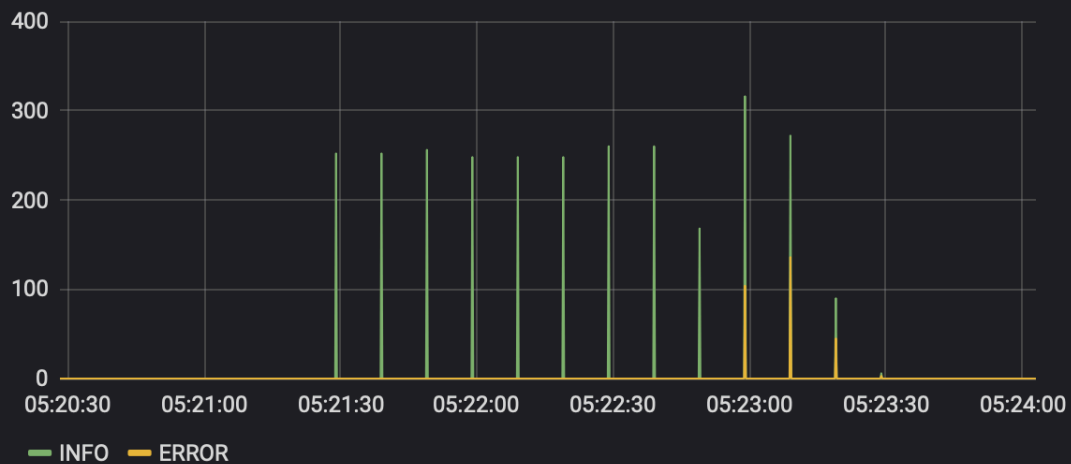
Execution Time ▾



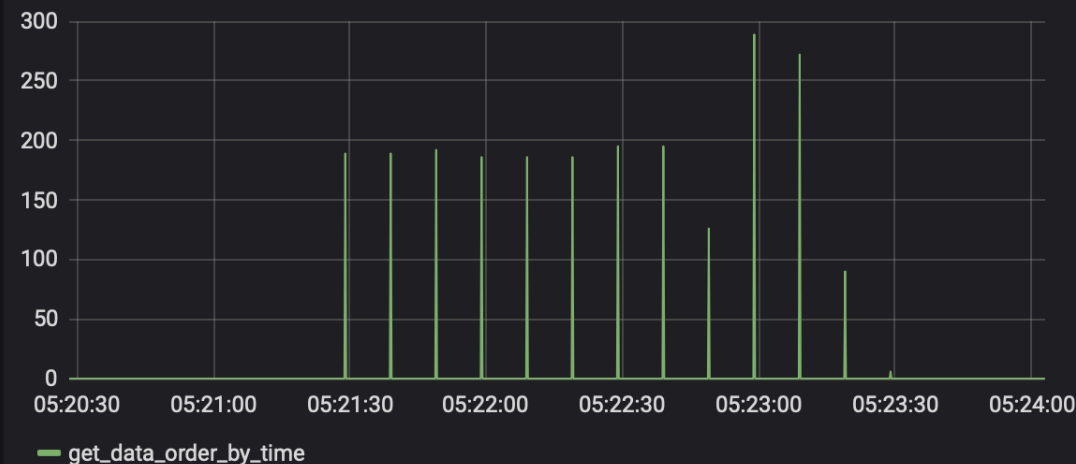
🕒 2020-02-19 05:20:28 to 2020-02-19 05:24:03 ▾



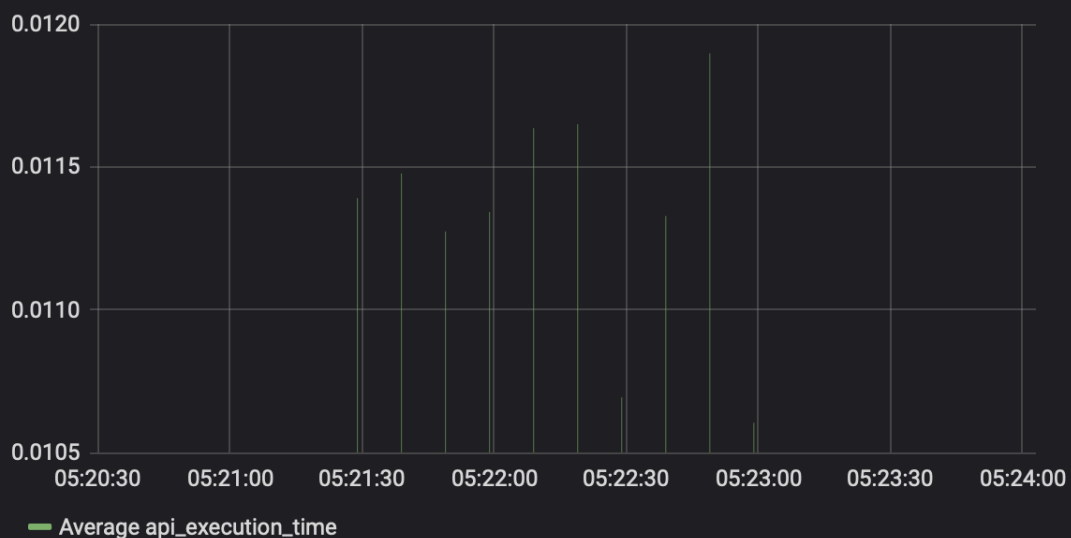
API Severity



Requests Type



Execution Time



Dashboard do Grafana com os gráficos gerados.



Execution Time ▾



🕒 2020-02-19 05:20:28 to 2020-02-19 05:24:03 ▾



API Severity ▾



Gráfico com total de execuções da API, com sucesso e erro, que usa o extrator do Graylog como base da busca.

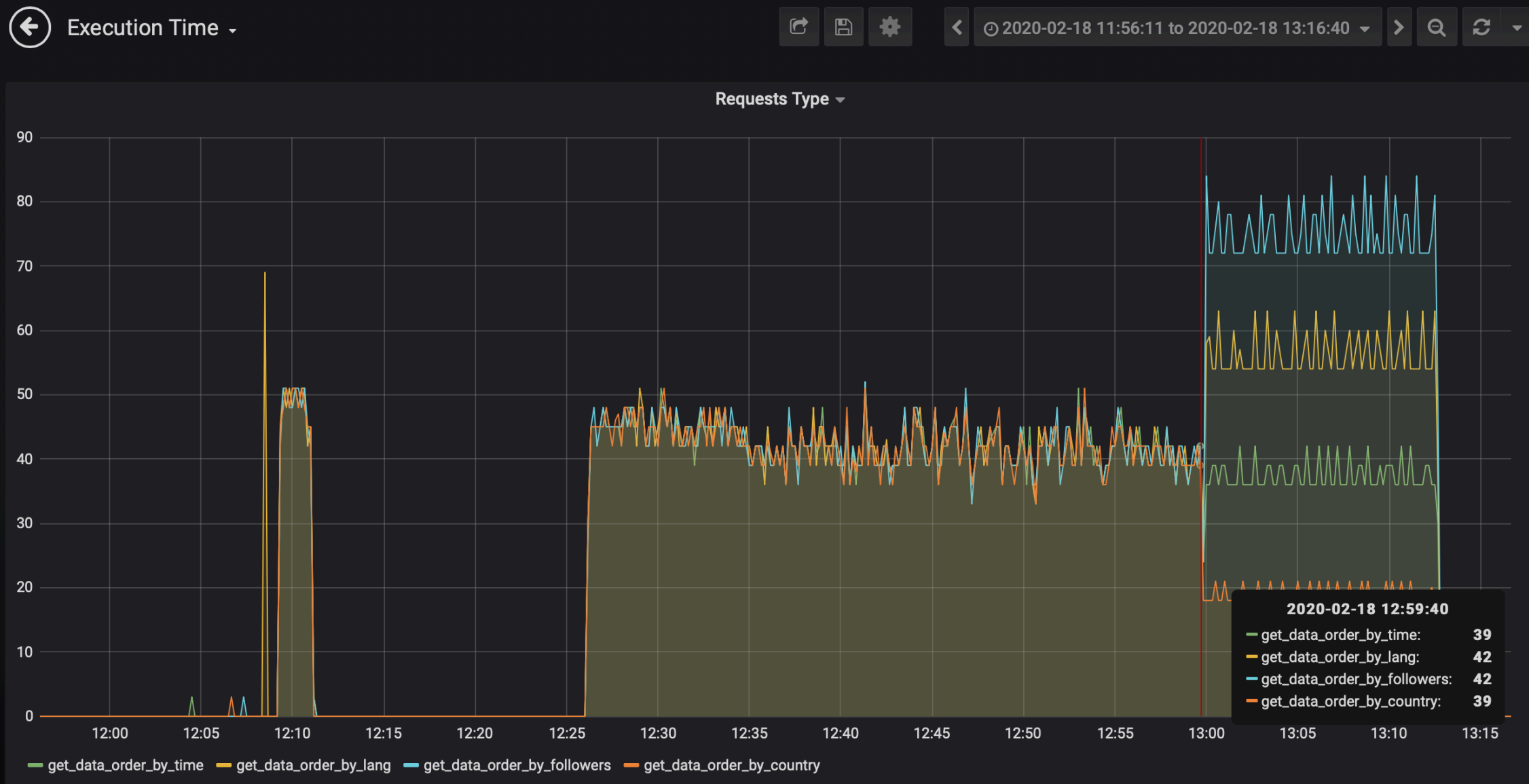


Gráfico mostrando as execuções das diversas chamadas, também usando o extrator do graylog como base da busca.



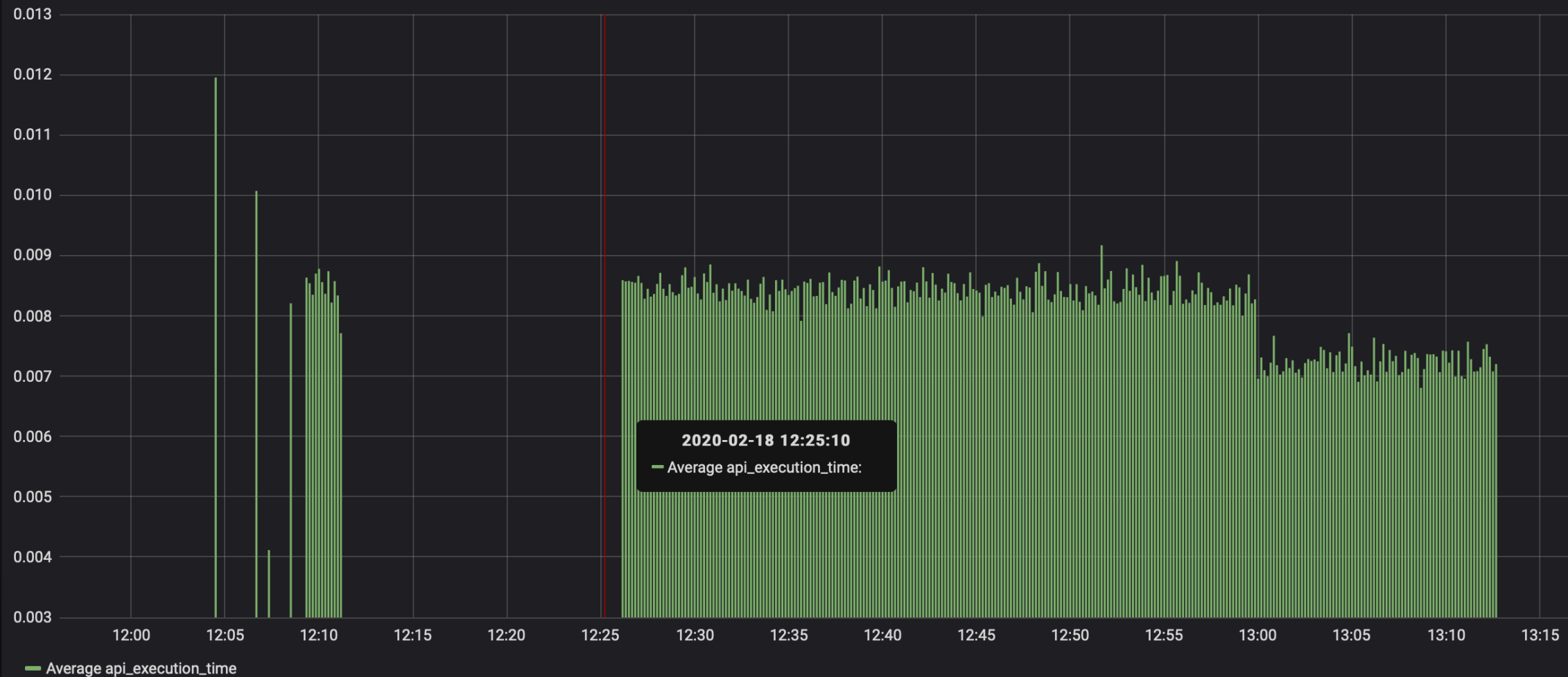
Execution Time ▾



🕒 2020-02-18 11:56:11 to 2020-02-18 13:16:40 ▾



Execution Time ▾



Por fim o gráfico de tempo de resposta, que usa o extrator do Graylog como base da busca.