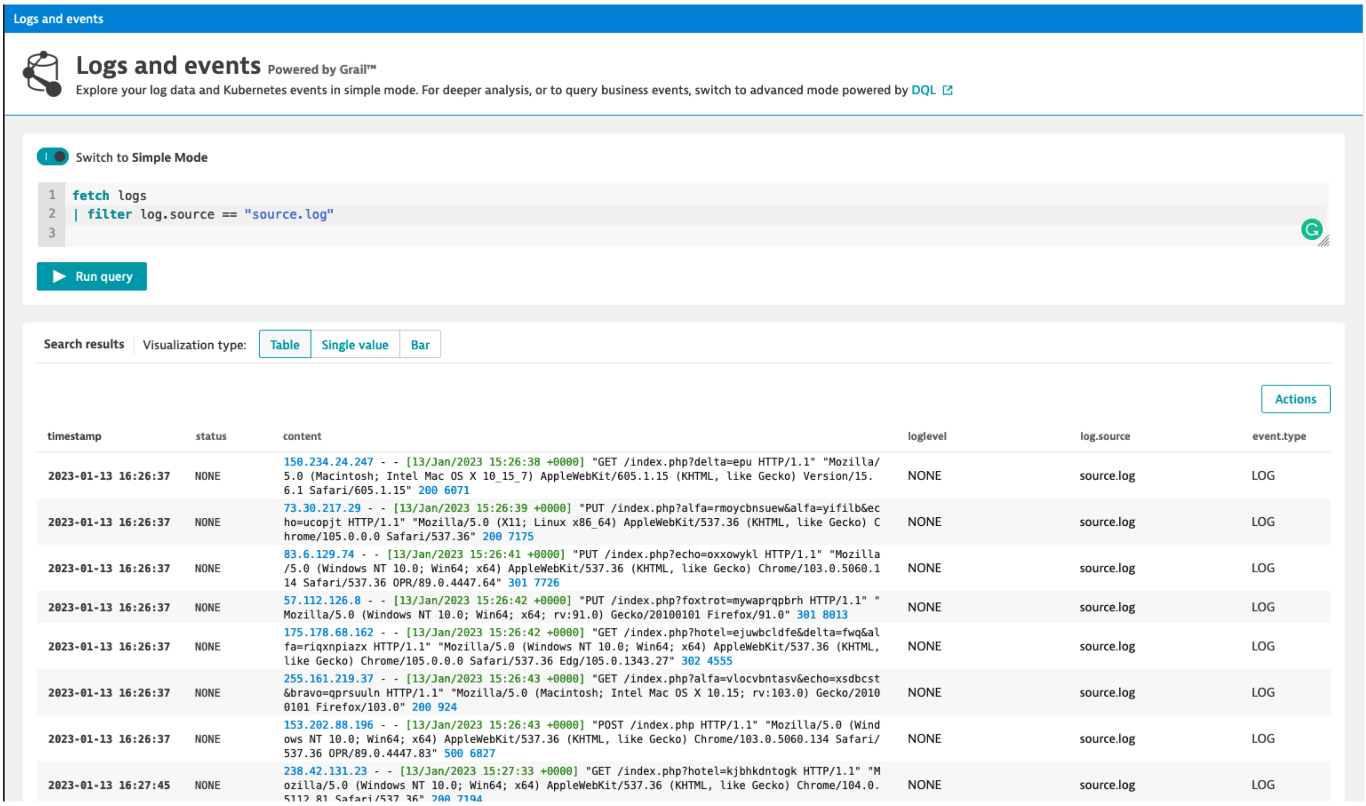
# Hello DQL

## Your first query

Open the Dynatrace instance and go to *Observe and explore* > *Logs*, make sure that you are in the advanced mode (toggle at the top) and execute the following query:

```
fetch logs
|  filter log.source == "source.log"
```


Logs and events
Logs and events Powered by Grail™
Explore your log data and Kubernetes events in simple mode. For deeper analysis, or to query business events, switch to advanced mode powered by DQL
Switch to Simple Mode
Run query
Search results
Visualization type:
Table
Single value
Bar
Actions

```
fetch logs
| filter log.source == "source.log"
```

| timestamp | status | content | loglevel | log.source | event.type |
|---|---|---|---|---|---|
| 2023-01-13 16:26:37 | NONE | 150.234.24.247 - - [13/Jan/2023 15:26:38 +0000] "GET /index.php?delta=epu HTTP/1.1" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.6.1 Safari/605.1.15" 200 6071 | NONE | source.log | LOG |
| 2023-01-13 16:26:37 | NONE | 73.30.217.29 - - [13/Jan/2023 15:26:39 +0000] "PUT /index.php?alfa=rmoycbnsuew&alfa=yifilb&echo=ucopjt HTTP/1.1" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36" 200 7175 | NONE | source.log | LOG |
| 2023-01-13 16:26:37 | NONE | 83.6.129.74 - - [13/Jan/2023 15:26:41 +0000] "PUT /index.php?echo=oxxowykl HTTP/1.1" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.114 Safari/537.36 OPR/89.0.4447.64" 301 7726 | NONE | source.log | LOG |
| 2023-01-13 16:26:37 | NONE | 57.112.126.8 - - [13/Jan/2023 15:26:42 +0000] "PUT /index.php?foxtrot=mywaprqpbrh HTTP/1.1" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0" 301 8013 | NONE | source.log | LOG |
| 2023-01-13 16:26:37 | NONE | 175.178.68.162 - - [13/Jan/2023 15:26:42 +0000] "GET /index.php?hotel=ejuwbcldfe&delta=fwq&alfa=riqxnpiazx HTTP/1.1" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36 Edg/105.0.1343.27" 302 4555 | NONE | source.log | LOG |
| 2023-01-13 16:26:37 | NONE | 255.161.219.37 - - [13/Jan/2023 15:26:43 +0000] "GET /index.php?alfa=vlocvbntasv&echo=xsdbcst&bravo=qprsuuln HTTP/1.1" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:103.0) Gecko/20100101 Firefox/103.0" 200 924 | NONE | source.log | LOG |
| 2023-01-13 16:26:37 | NONE | 153.202.88.196 - - [13/Jan/2023 15:26:43 +0000] "POST /index.php HTTP/1.1" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36 OPR/89.0.4447.83" 500 6827 | NONE | source.log | LOG |
| 2023-01-13 16:27:45 | NONE | 238.42.131.23 - - [13/Jan/2023 15:27:33 +0000] "GET /index.php?hotel=kjbhkdntogk HTTP/1.1" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.81 Safari/537.36" 200 7194 | NONE | source.log | LOG |

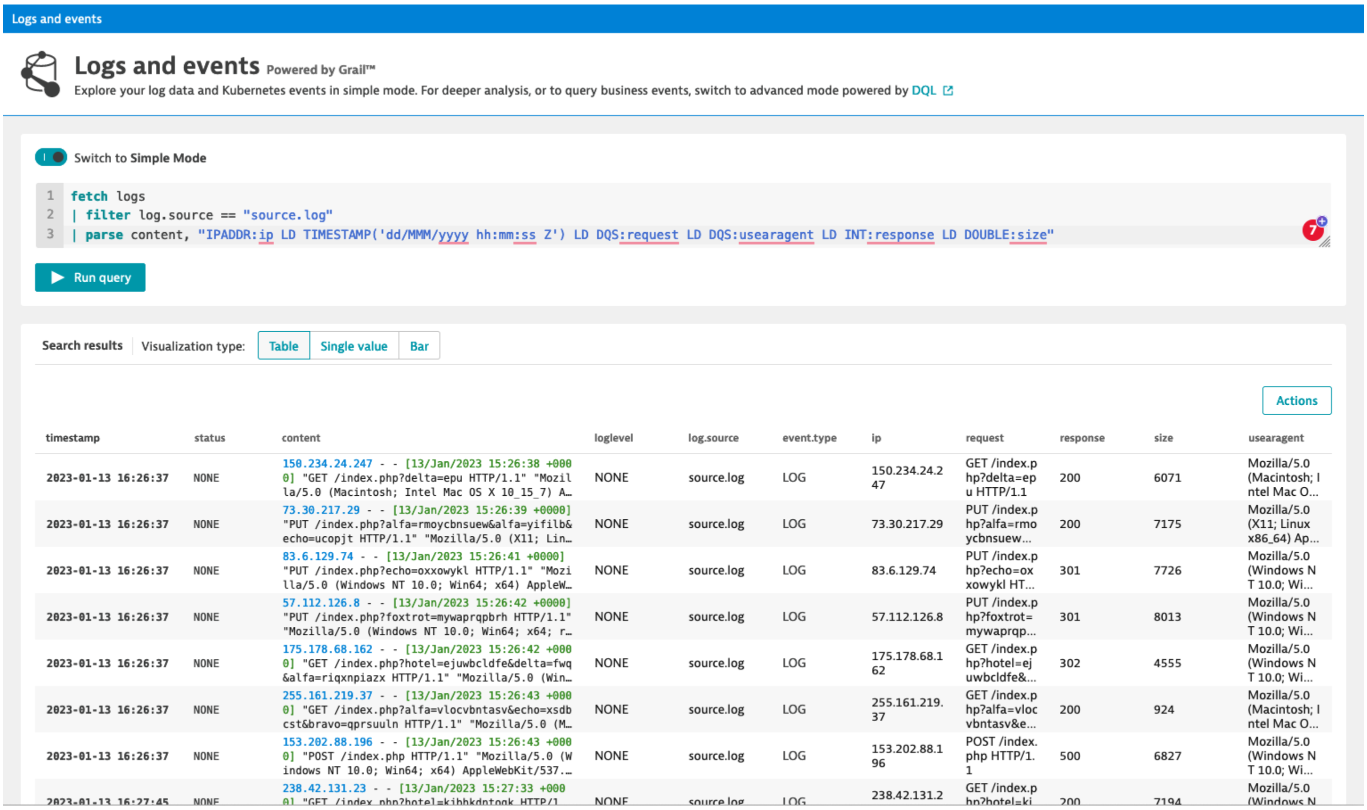
## Parse this

Break the content field into several, more useful fields, by adding the following command to your query:

```
| parse content, "IPADDR:ip LD TIMESTAMP('dd/MMM/yyyy hh:mm:ss Z') LD
DQS:request LD DQS:useragent LD INT:response LD DOUBLE:size"
```

The full query should no be:

```
fetch logs
| filter log.source == "source.log"
| parse content, "IPADDR:ip LD TIMESTAMP('dd/MMM/yyyy hh:mm:ss Z') LD
DQS:request LD DQS:useragent LD INT:response LD DOUBLE:size"
```



## Logs and events Powered by Grail™

Explore your log data and Kubernetes events in simple mode. For deeper analysis, or to query business events, switch to advanced mode powered by DQL

```
fetch logs
| filter log.source == "source.log"
| parse content, "IPADDR:ip LD TIMESTAMP('dd/MMM/yyyy hh:mm:ss Z') LD DQS:request LD DQS:useragent LD INT:response LD DOUBLE:size"
```

| timestamp | status | content | loglevel | log.source | event.type | ip | request | response | size | usearagent |
|---|---|---|---|---|---|---|---|---|---|---|
| 2023-01-13 16:26:37 | NONE | 150.234.24.247 - - [13/Jan/2023 15:26:38 +0000] "GET /index.php?delta=epu HTTP/1.1" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) A… | NONE | source.log | LOG | 150.234.24.247 | GET /index.php?delta=epu HTTP/1.1 | 200 | 6071 | Mozilla/5.0 (Macintosh; Intel Mac O... |
| 2023-01-13 16:26:37 | NONE | 73.30.217.29 - - [13/Jan/2023 15:26:39 +0000] "PUT /index.php?alfa=rmoycbnsuew&alfa=yifilb&echo=ucopjt HTTP/1.1" "Mozilla/5.0 (X11; Lin… | NONE | source.log | LOG | 73.30.217.29 | PUT /index.php?alfa=rmoycbnsuew... | 200 | 7175 | Mozilla/5.0 (X11; Linux x86_64) Ap... |
| 2023-01-13 16:26:37 | NONE | 83.6.129.74 - - [13/Jan/2023 15:26:41 +0000] "PUT /index.php?echo=oxxowykl HTTP/1.1" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW… | NONE | source.log | LOG | 83.6.129.74 | PUT /index.php?echo=oxxowykl HT... | 301 | 7726 | Mozilla/5.0 (Windows NT 10.0; Wi... |
| 2023-01-13 16:26:37 | NONE | 57.112.126.8 - - [13/Jan/2023 15:26:42 +0000] "PUT /index.php?foxtrot=mywaprqpbrh HTTP/1.1" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; r… | NONE | source.log | LOG | 57.112.126.8 | PUT /index.php?foxtrot=mywaprqp... | 301 | 8013 | Mozilla/5.0 (Windows NT 10.0; Wi... |
| 2023-01-13 16:26:37 | NONE | 175.178.68.162 - - [13/Jan/2023 15:26:42 +0000] "GET /index.php?hotel=ejuwbcldfe&delta=fwq&alfa=riqxnpiazx HTTP/1.1" "Mozilla/5.0 (Win… | NONE | source.log | LOG | 175.178.68.162 | GET /index.php?hotel=ejuwbcldfe&... | 302 | 4555 | Mozilla/5.0 (Windows NT 10.0; Wi... |
| 2023-01-13 16:26:37 | NONE | 255.161.219.37 - - [13/Jan/2023 15:26:43 +0000] "GET /index.php?alfa=vlocvbntasv&echo=xsdbcst&bravo=qprsuuln HTTP/1.1" "Mozilla/5.0 (M… | NONE | source.log | LOG | 255.161.219.37 | GET /index.php?alfa=vlocvbntasv&e... | 200 | 924 | Mozilla/5.0 (Macintosh; Intel Mac O... |
| 2023-01-13 16:26:37 | NONE | 153.202.88.196 - - [13/Jan/2023 15:26:43 +0000] "POST /index.php HTTP/1.1" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.… | NONE | source.log | LOG | 153.202.88.196 | POST /index.php HTTP/1.1 | 500 | 6827 | Mozilla/5.0 (Windows NT 10.0; Wi... |
| 2023-01-13 16:27:45 | NONE | 238.42.131.23 - - [13/Jan/2023 15:27:33 +0000] "GET /index.php?hotel=kibhkdntoqk HTTP/1 | NONE | source.log | LOG | 238.42.131.2 | GET /index.php?hotel=ki | 200 | 7194 | Mozilla/5.0 (Windows N |