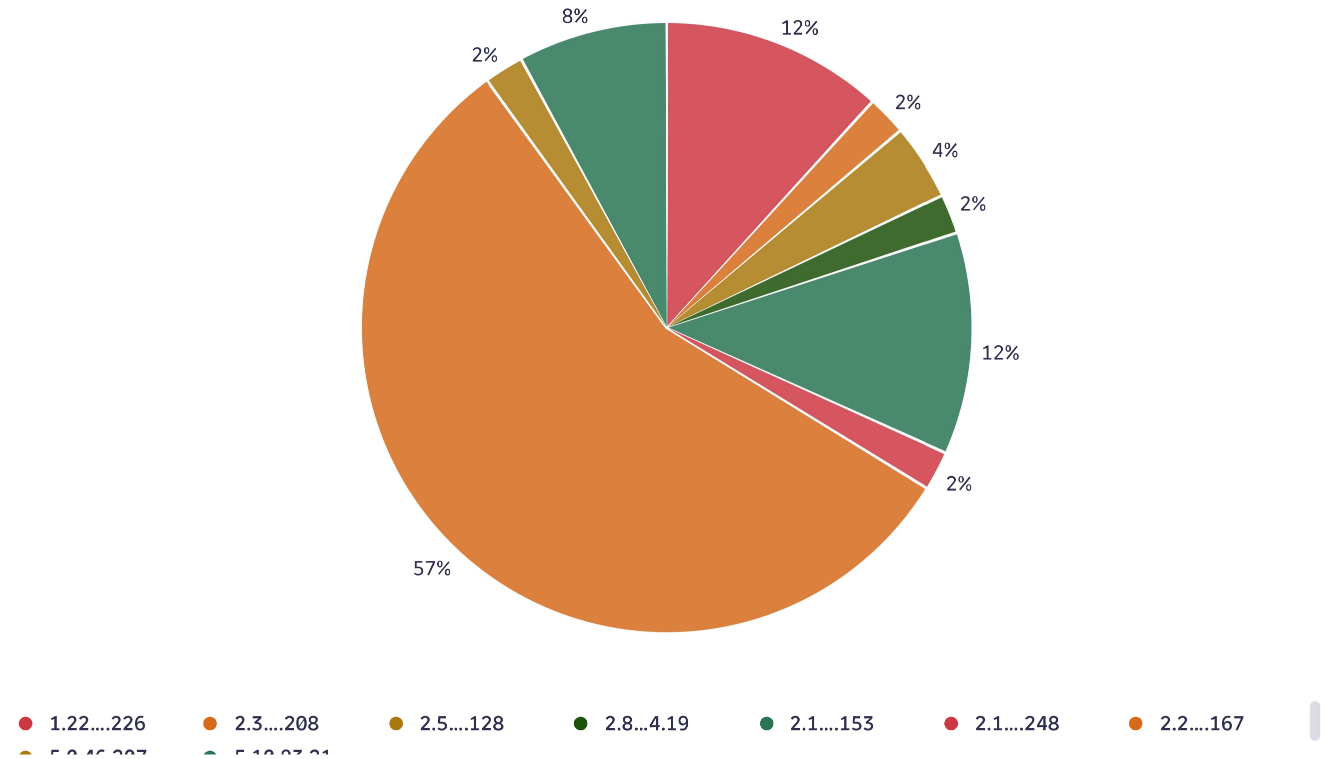
Apache Combined Logs

Apache logs

These logs are records maintained by the Apache HTTP Server to capture details about client requests, server activity, and errors. They are essential for monitoring performance, diagnosing issues, and enhancing security. The two most common types are access logs and error logs. Access logs record every incoming HTTP request, typically stored in `/var/log/apache2/access.log` on Debian/Ubuntu or `/var/log/httpd/access_log` on RHEL/CentOS systems. They often use the Common or Combined Log Format, which includes information such as the client IP address, user identity, timestamp, HTTP method, requested resource, protocol version, status code, and response size. The Combined Log Format also logs the referer and user-agent details. Error logs, found in /var/log/apache2/error.log or /var/log/httpd/error_log, store server-related error messages, warnings, and startup/shutdown events. Each entry usually contains the timestamp, module and severity level, process ID, client information, and a descriptive error message. Beyond these, Apache may also produce specialized logs such as mod_security audit logs, virtual host-specific logs, or custom logs defined through configuration directives like CustomLog and ErrorLog. Administrators often use commands such as tail -f to monitor logs in real time, grep to search for specific errors, or awk to analyze request patterns by IP. Together, these logs form a vital part of web server management, enabling proactive issue detection and detailed forensic analysis.

```
fetch logs
| filter matchesValue(log.source, "apache.log")
| parse content, "IPADDR:clientip LD '[' HTTPDATE ']' LD 'HTTP/' LD SPACE INT:status L
| summarize numOf200Errors=countIf(status==200), numOf404Errors=countIf(status==404),
numOf301Errors=countIf(status==301), numOf206Errors=countIf(status==206), numOf403Erro
| limit 10
```

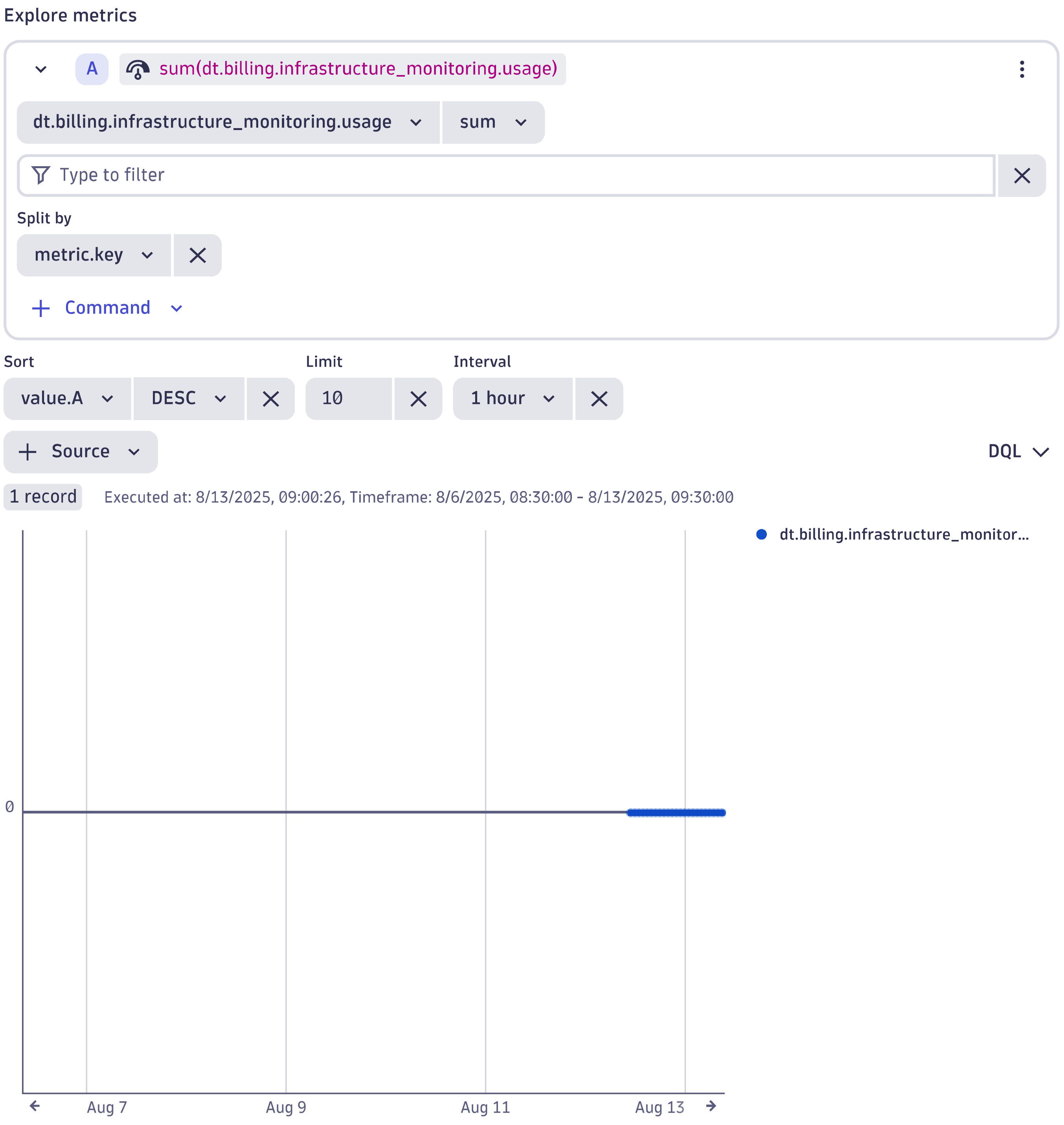
10 records ⓘ Executed at: 8/13/2025, 09:00:26, Timeframe: 8/6/2025, 09:00:25 - 8/13/2025, 09:00:25, Scanned bytes: 5 MB



```
fetch logs
| filter matchesValue(log.source, "apache.log")
| parse content, "IPADDR:clientip LD '[' HTTPDATE ']' LD 'HTTP/' LD SPACE INT:status S
| parse url, "LD SPACE LD:useragent"
| parse useragent, "DQS:useragent"
| summarize total_count=count(), by:{clientip,useragent}
| filterOut useragent=="-"
| sort - total_count
| filter isNotNull(useragent)
| limit 10
```

10 records Executed at: 8/13/2025, 09:00:26, Timeframe: 8/6/2025, 09:00:25 - 8/13/2025, 09:00:25, Scanned bytes: 5 MB

clientip	useragent	total_cou
46.105.14.53	UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/	3
130.237.218.86	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Ch...	2
66.249.73.135	Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Ge...	2
66.249.73.135	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	2
50.16.19.13	Tiny Tiny RSS/1.11 (http://tt-rss.org/)	1
68.180.224.225	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)	
75.97.9.59	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32....	
198.46.149.143	Tiny Tiny RSS/1.11 (http://tt-rss.org/)	
208.115.111.72	Mozilla/5.0 (compatible; Ezooms/1.0; help@moz.com)	
208.115.113.88	Mozilla/5.0 (compatible; Ezooms/1.0; help@moz.com)	



Explore metrics

A sum(dt.billing.infrastructure_monitoring.usage)

dt.billing.infrastructure_monitoring.usage | sum

Type to filter

Split by

metric.key

Sort: value.A DESC

Limit: 10

Interval: 1 hour

1 record

Executed at: 8/13/2025, 09:00:26, Timeframe: 8/6/2025, 08:30:00 - 8/13/2025, 09:30:00

Explore logs

log.source = sample_lookup.csv

log.source = sample_lookup.csv

Summarize

Count | All records

+ Command

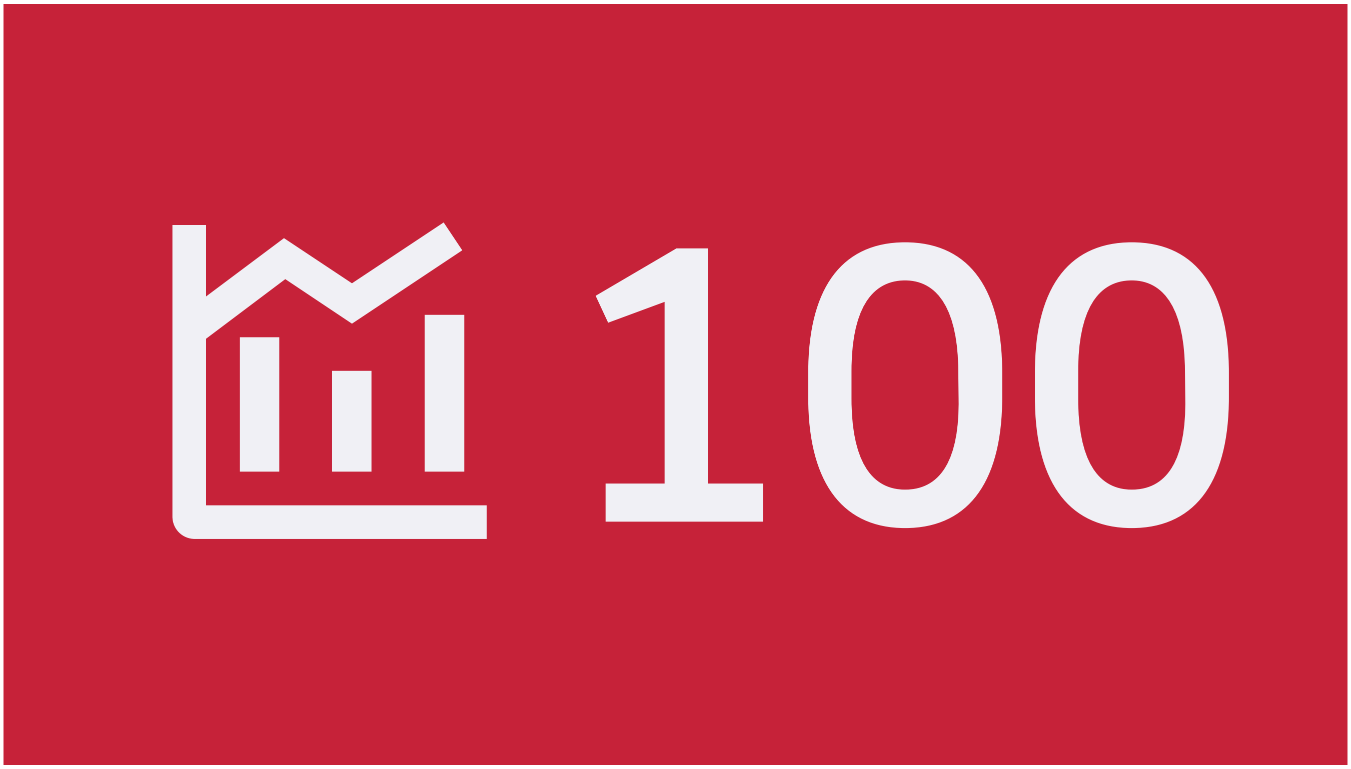
Limit

20

+ Sort

DQL

1 record ⚠ Executed at: 8/13/2025, 09:11:09, Timeframe: 8/6/2025, 09:11:08 - 8/13/2025, 09:11:08, Scanned bytes: 200 kB



Explore Events

host.name = ip-172-31-38-208.ec2.internal

host.name = ip-172-31-38-208.ec2.internal

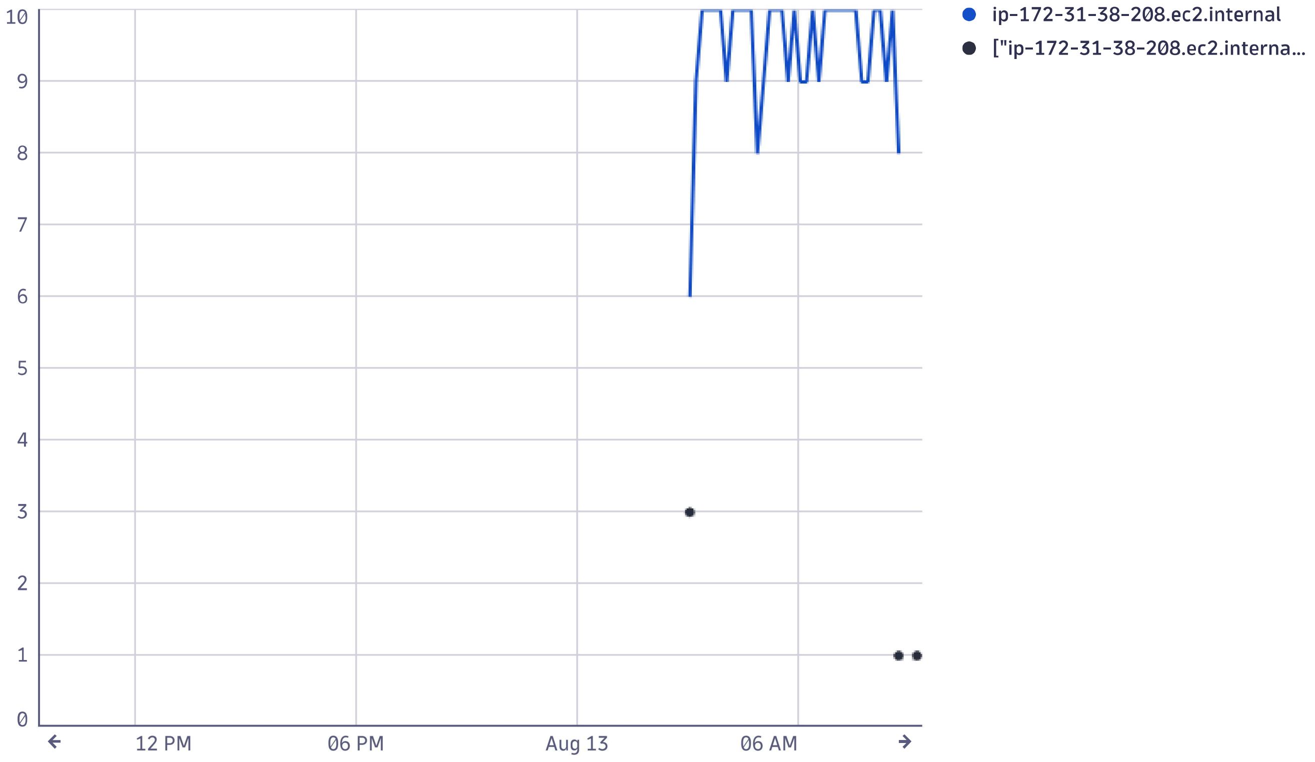
Convert to time series

Count | host.name

+ Command

+ Sort + Limit DQL

2 records Executed at: 8/13/2025, 09:22:01, Timeframe: 8/12/2025, 09:22:01 - 8/13/2025, 09:22:01, Scanned bytes: 471 kB



```
/*
* This function will run in the DYNATRACE JavaScript runtime.
* For information visit https://dt-url.net/functions-help
*/
export default async function () {
  return "Hello, world!";
}
```

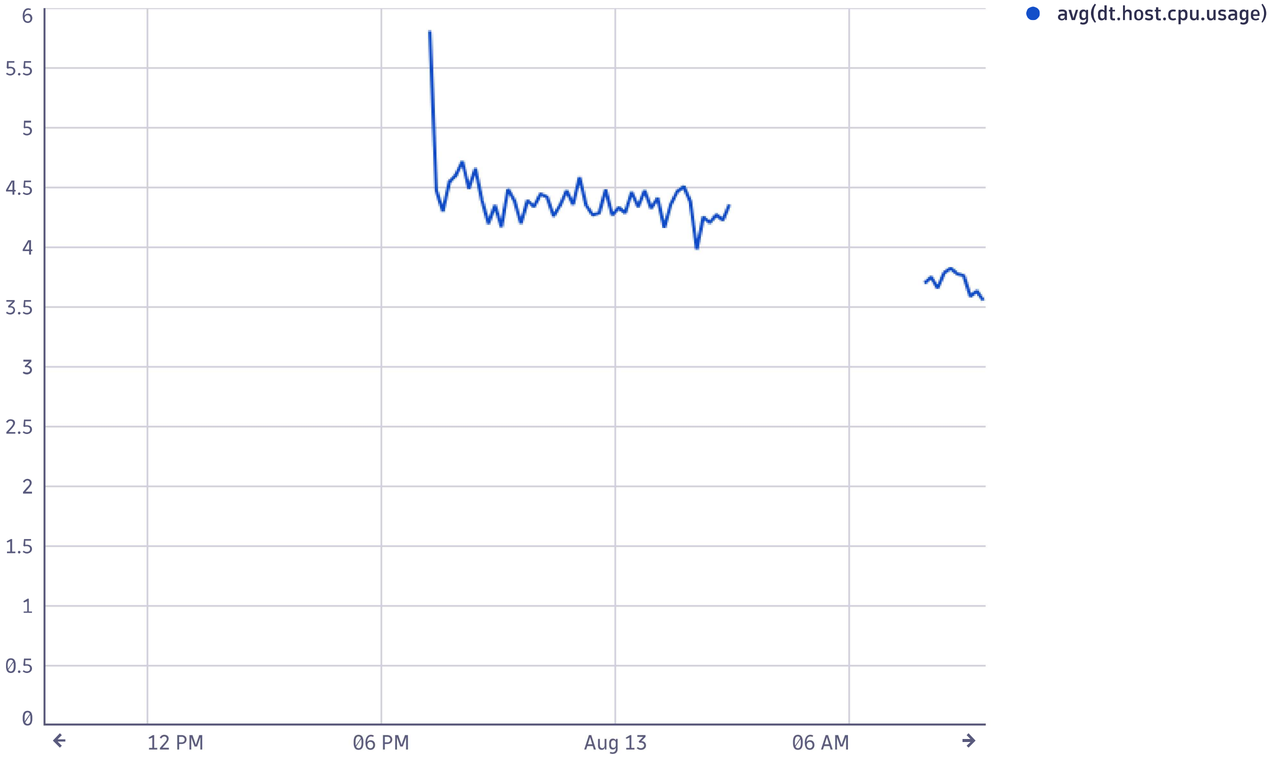
1 record Executed at: 8/13/2025, 09:26:48

element
Hello, world!

Chart average CPU across all hosts

```
timeseries avg(dt.host.cpu.usage)
```

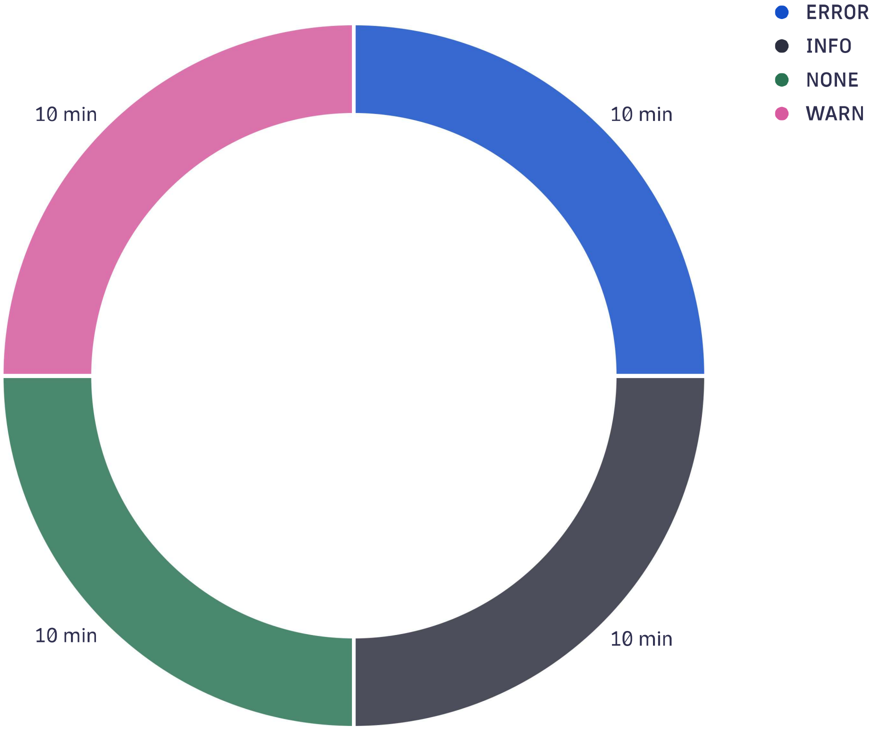
1 record Executed at: 8/13/2025, 09:27:09, Timeframe: 8/12/2025, 09:20:00 - 8/13/2025, 09:30:00



Area chart (Logs by status)

```
fetch logs
| makeTimeseries count(), by:{status}
```

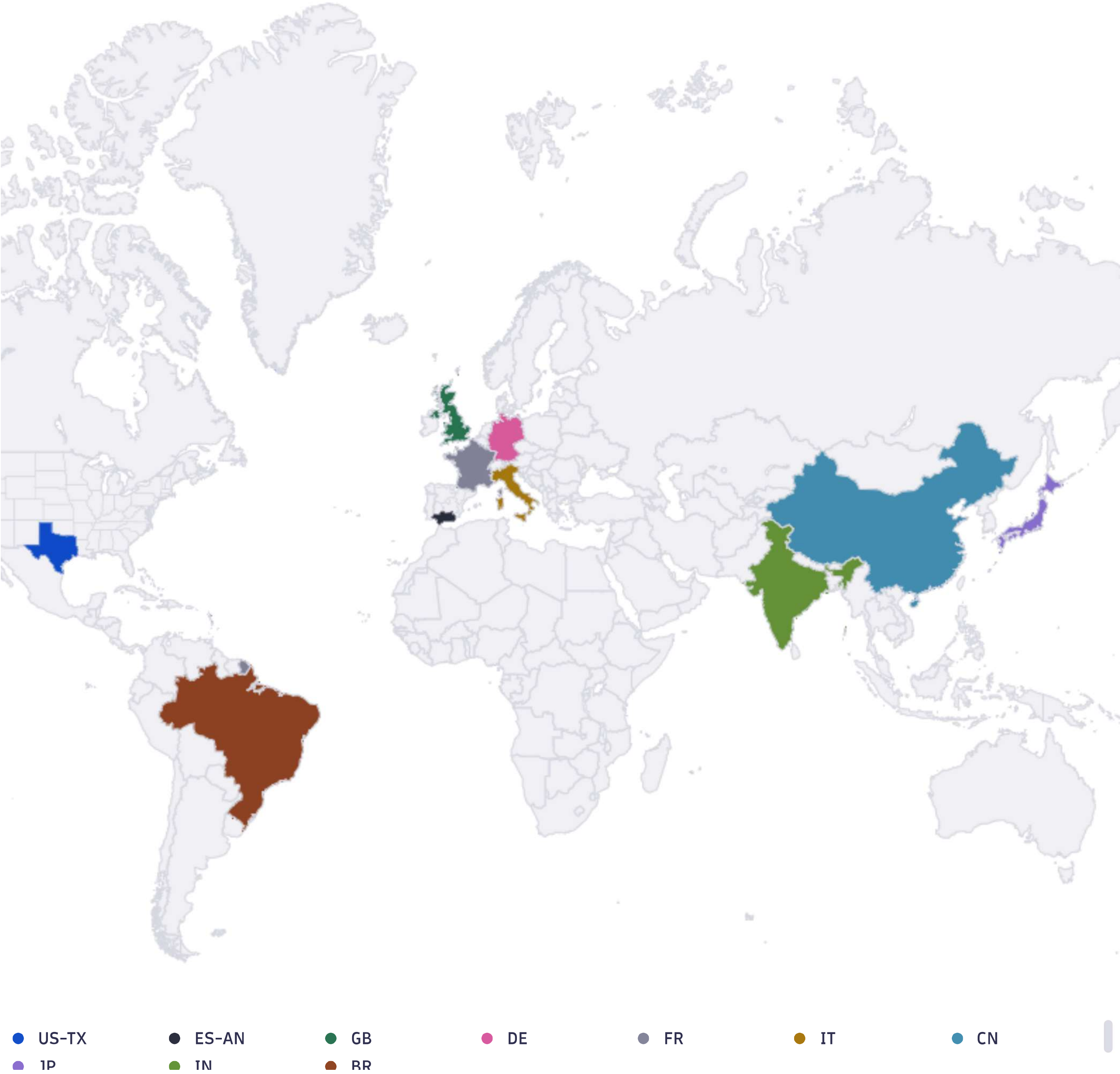
4 records Executed at: 8/13/2025, 09:27:42, Timeframe: 8/12/2025, 09:27:41 - 8/13/2025, 09:27:41, Scanned bytes: 9 MB



Choropleth (Apdex representation by country)

```
data
    record(country_code = "US-TX", apdex = "Unacceptable"),
    record(country_code = "ES-AN", apdex = "Unacceptable"),
    record(country_code = "GB", apdex = "Excellent"),
    record(country_code = "DE", apdex = "Poor"),
    record(country_code = "FR", apdex = "Fair"),
    record(country_code = "IT", apdex = "Fair"),
    record(country_code = "CN", apdex = "Unacceptable"),
    record(country_code = "JP", apdex = "Excellent"),
    record(country_code = "IN", apdex = "Good"),
    record(country_code = "BR", apdex = "Fair")
```

10 records Executed at: 8/13/2025, 09:28:24


● US-TX
● ES-AN
● GB
● DE
● FR
● IT
● CN
● JP
● IN
● BR