



# DATADOG

## APM Monitoring

Datadog Partner 교육 (Day 2)  
2:00 PM에 시작합니다!

# Partner 교육 2 days 교육 일정

시간	Day1
14:00 ~ 14:50 (정영석 부장)	<b>Datadog Overview</b> <ul style="list-style-type: none"><li>- 기본 소개 및 전체 제품 구성 안내</li><li>- 계정 접속 및 ORG 구성/권한</li><li>- 기본 비용 체계</li><li>- Q&amp;A</li></ul> <b>Infrastructure monitoring</b> <ul style="list-style-type: none"><li>- 개요 및 설명</li></ul>
14:50 ~ 15:00	<b>Break</b>
15:00 ~ 15:50 (정영석 부장)	<b>Infrastructure monitoring</b> <ul style="list-style-type: none"><li>- 설치 및 구성 방법</li><li>- 최적화 사용 방안</li><li>- Q&amp;A</li></ul>
15:50 ~ 16:00	<b>Break</b>
16:00 ~ 17:00 (이성욱 부장)	<b>Log Management</b> <ul style="list-style-type: none"><li>- 설치 및 구성 방법</li><li>- 최적화 사용 방안</li><li>- Q&amp;A</li></ul>

시간	Day2
14:00 ~ 14:50 (이성욱 부장)	<b>Application Performance Monitoring (Back End)</b> <ul style="list-style-type: none"><li>- 개요 및 설명</li><li>- 설치 및 구성 방법</li><li>- 최적화 사용 방안</li><li>- Q&amp;A</li></ul>
14:50 ~ 15:00	<b>Break</b>
15:00 ~ 15:50 (정영석 부장)	<b>Real User Monitoring (Front End)</b> <ul style="list-style-type: none"><li>- 개요 및 설명</li><li>- 설치 및 구성 방법</li><li>- 최적화 사용 방안</li></ul>
15:50 ~ 16:00	<b>Break</b>
16:00 ~ 17:00	<b>2021년에 추가된 제품 및 기능 소개</b>

# #TOPIC (APM)

**1. Datadog APM Flow**

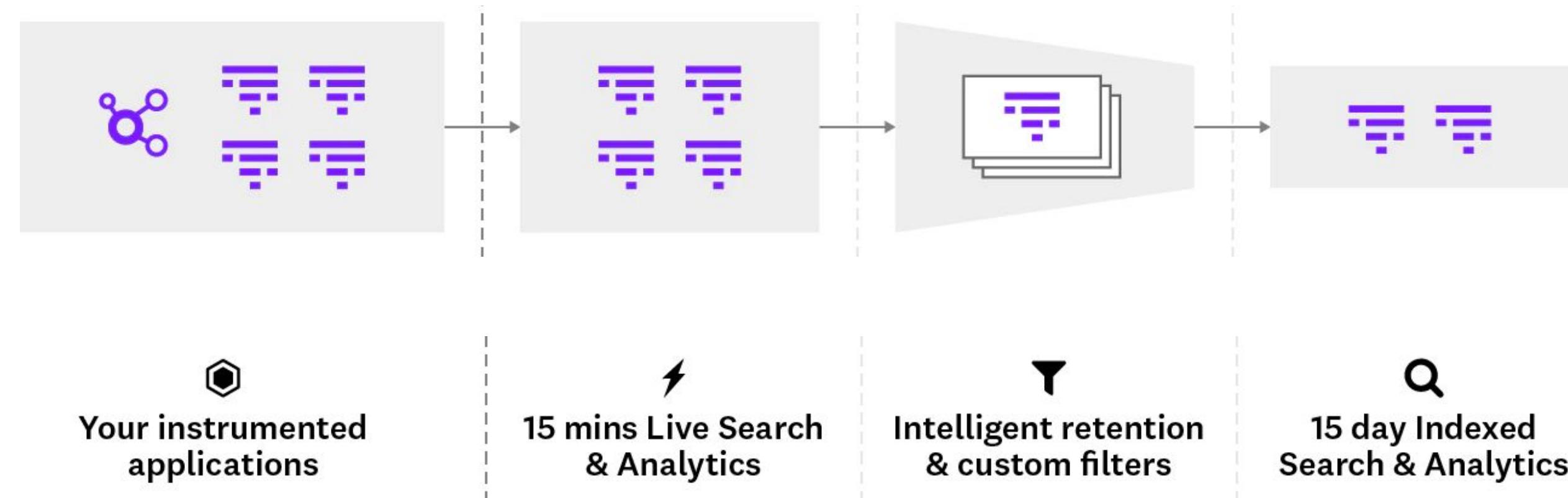
**2. APM Features**

**3. APM Optimization**

**4. Q&A**

# APM Flow

# #Datadog APM Flow



# APM Features

# #Sending Traces to Datadog

## 다양한 방법을 통한 Trace전송



## Things To Check

- 버전 및 호환성 체크
- Tag 및 Option 설정
- Sampling/Filter Traces

### Sample

```
export JAVA_OPTS="$JAVA_OPTS  
-javaagent:/app/datadog-trace/dd-java-latest.jar  
-Ddd.service.name=서비스명 -Ddd.env=환경  
-Ddd.version=버전 ...  
-Ddd.trace.header.tags=User-Agent:user-agent  
-Ddd.trace.db.client.split-by-instance=true  
-Ddd.http.server.tag.query-string=true ....
```

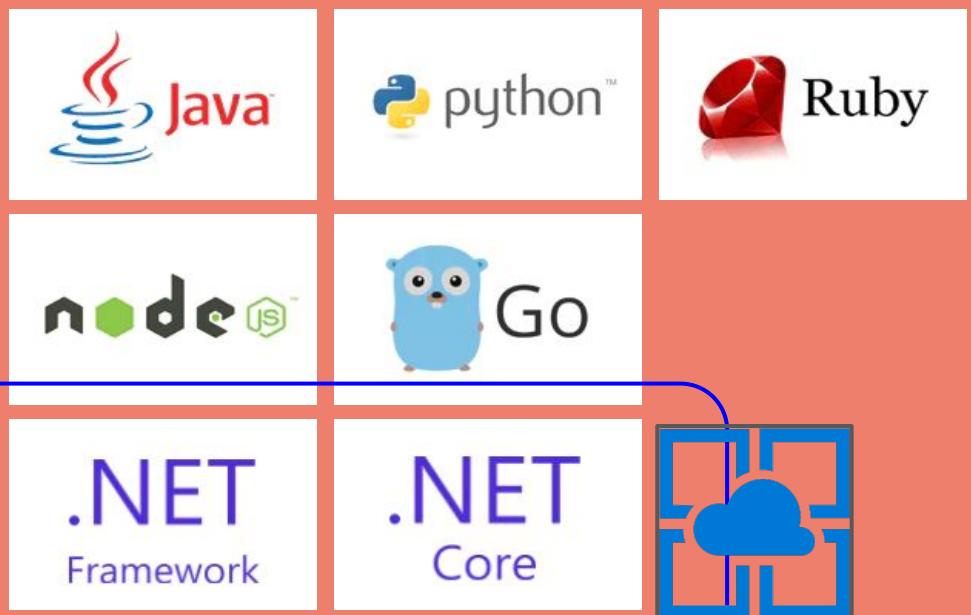
apm\_config :

```
ignore_resources: ["GET /healthcheck"]
```



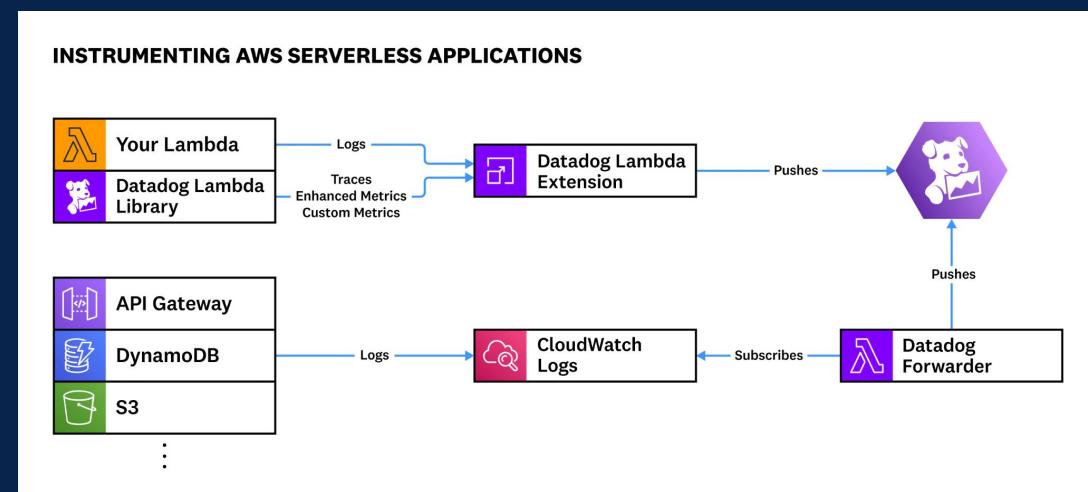
# #Sending Traces to Datadog

## Serverless



## Things To Check

- 버전 및 호환성 체크
- Extension 추가



# #Ingestion & Retention

## Ingestion

### - Ingestion Rate

Ex. DD\_TRACE\_SAMPLE\_RATE=1.0

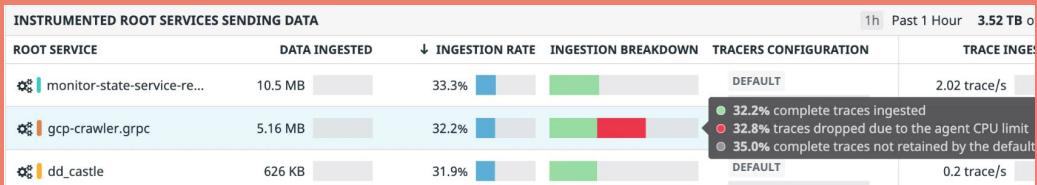
### - Ingestion Status

Green - Complete

Gray - Filtered

Orange - tracer rate limiter (100 traces per second)

Red - dropped agent CPU limit (max\_cpu\_percent)



## Retention

### - 필터 조건에 따라 15일간 저장

Add a Retention Filter

- Name the filter
- Set filters for the span to match
- Set span retention rate

38.1M Matching spans in the past 15 minutes

↓ DATE	SERVICE	RESOURCE	DURATION	HTTP METH...	STATUS COD
Aug 10 21:15:44.946	coffee-house	RecordOrder	40.43ms		200
Aug 10 21:15:44.923	ad-server	GET /find_ad/parameters.json	1994.14μs	GET	200
Aug 10 21:15:44.517	send-email-redis-queue	PUBLISH	955.59μs		
Aug 10 21:15:44.362	product-recommendation	GET /report	567.31ms	GET	200
Aug 10 21:15:44.347	web-store	ShoppingCartController#apply_-	649.66ms	POST	200
Aug 10 21:15:44.223	php.frontend.site	CoffeeHouse\Controllers\HomeC...	4.21s	GET	200
Aug 10 21:15:43.970	send-email-redis-queue	PUBLISH	775.78μs		
Aug 10 21:15:43.878	web-store	PUT 500	15.09s	PUT	500
Aug 10 21:15:43.683	web-store	ApplicationController#health	24.42ms	GET	200
Aug 10 21:15:43.599	shipping-queue-redis	BRPOP	1233.55ms		

Retain 100 % of matching indexed spans  
These spans will be stored for 15 days for search and analytics with the full trace flamegraph when available.

# #Additional Configuration

## 추가 설정

- Logs Injection - trace\_id and span\_id
- Unified Service Tagging - version, env, and service
- Collect runtime metrics



## Benefit

- APM/LOG 연계 분석
- 배포 전후 분석 및 환경별 분석
- Runtime Metric 비교 분석

```
<appender name="FILE" class="org.apache.log4j.FileAppender">
    <param name="File" value="logs/app.log"/>
    <param name="Append" value="true"/>

    <layout class="org.apache.log4j.PatternLayout">
        <param name="ConversionPattern" value="%d{yyyy-MM-dd HH:mm:ss} %-5p
Log4j
%c{1}:%L - %X{dd.trace_id} %X{dd.span_id} - %m%n"/>
    </layout>
</appender>
```

# #Common Inquiry

## FAQ

- Deployments 항목이 비활성화되어 있습니다
- 두개의 DB가 하나로 표시됩니다
- 특정 Request Header값을 추적하고 싶습니다
- /healthcheck 요청을 제외하고 싶어요
- 검색되지 않는 Trace가 있습니다
- Dashboard에서 View related traces 관련 요청을 볼수 없습니다



## Things To Check

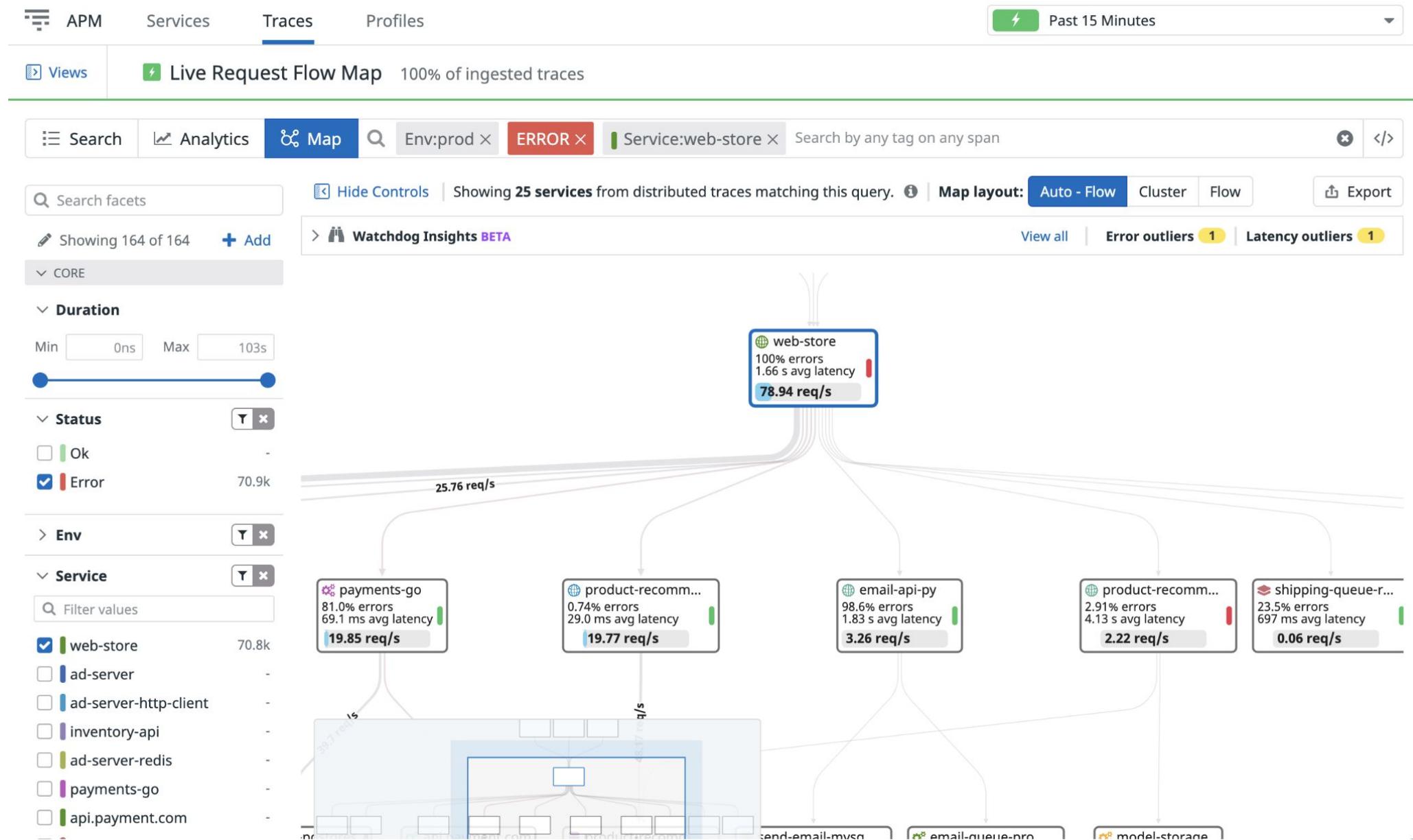
### Sample

```
export JAVA_OPTS="$JAVA_OPTS  
-javaagent:/app/datadog-trace/dd-java-latest.jar  
-Ddd.service.name=서비스명 -Ddd.env=환경  
-Ddd.version=버전 ...  
-Ddd.trace.header.tags=User-Agent:user-agent  
-Ddd.trace.db.client.split-by-instance=true  
-Ddd.http.server.tag.query-string=true ....
```

### apm\_config :

```
ignore_resources: ["GET /healthcheck"]
```

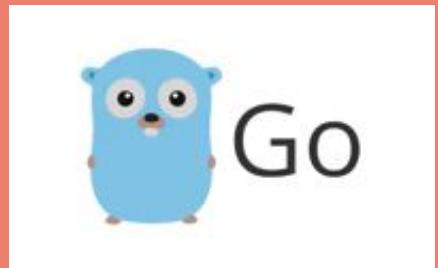
# #APM Features Demo



# Profiler & Database Monitoring

# #Profiler

지원 언어



Public Beta



Things To Check

- 지원 버전 Check

Ex.

OpenJDK 11+, Oracle JDK 11+,  
OpenJDK 8 (version 8u262+)



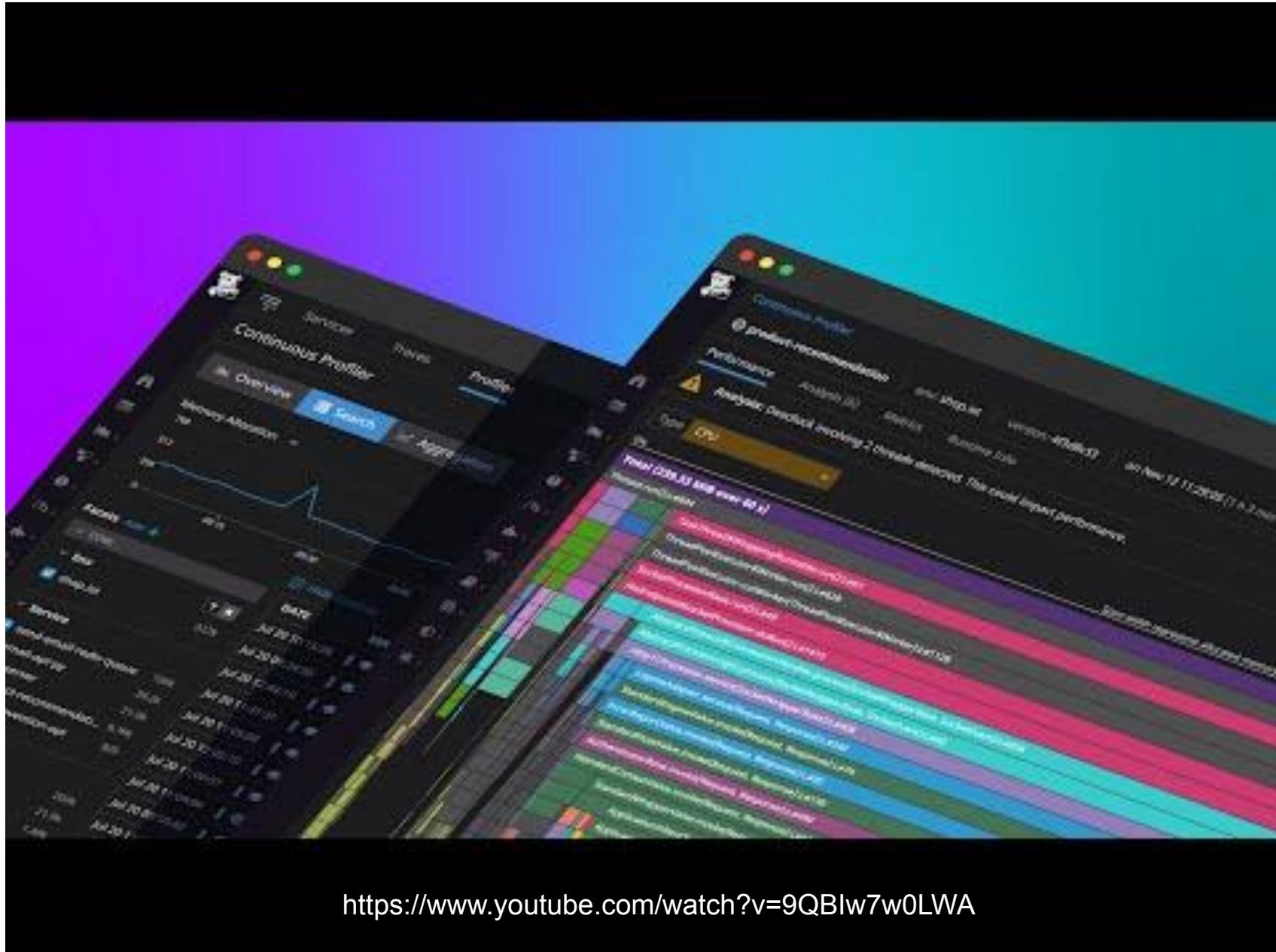
# #Profiler

## APM & Profiler 비교

	APM & Distributed Tracing	Profiling
Visibility level	Services & 3rd party libraries	100% of the code (methods, classes, threads)
Measurement	Requests, Errors, Duration (latency)	Resource consumption (cpu, memory & time)
Flame graph	Execution path of a request across multiple services, including duration and errors	Aggregated 1-min view of resource consumption per method, per application process

Traces tell you **WHICH** requests were slow at the **service** level  
Profiles tell you **WHY** they were slow at the **line of code** level

# #Profiler



# #Database

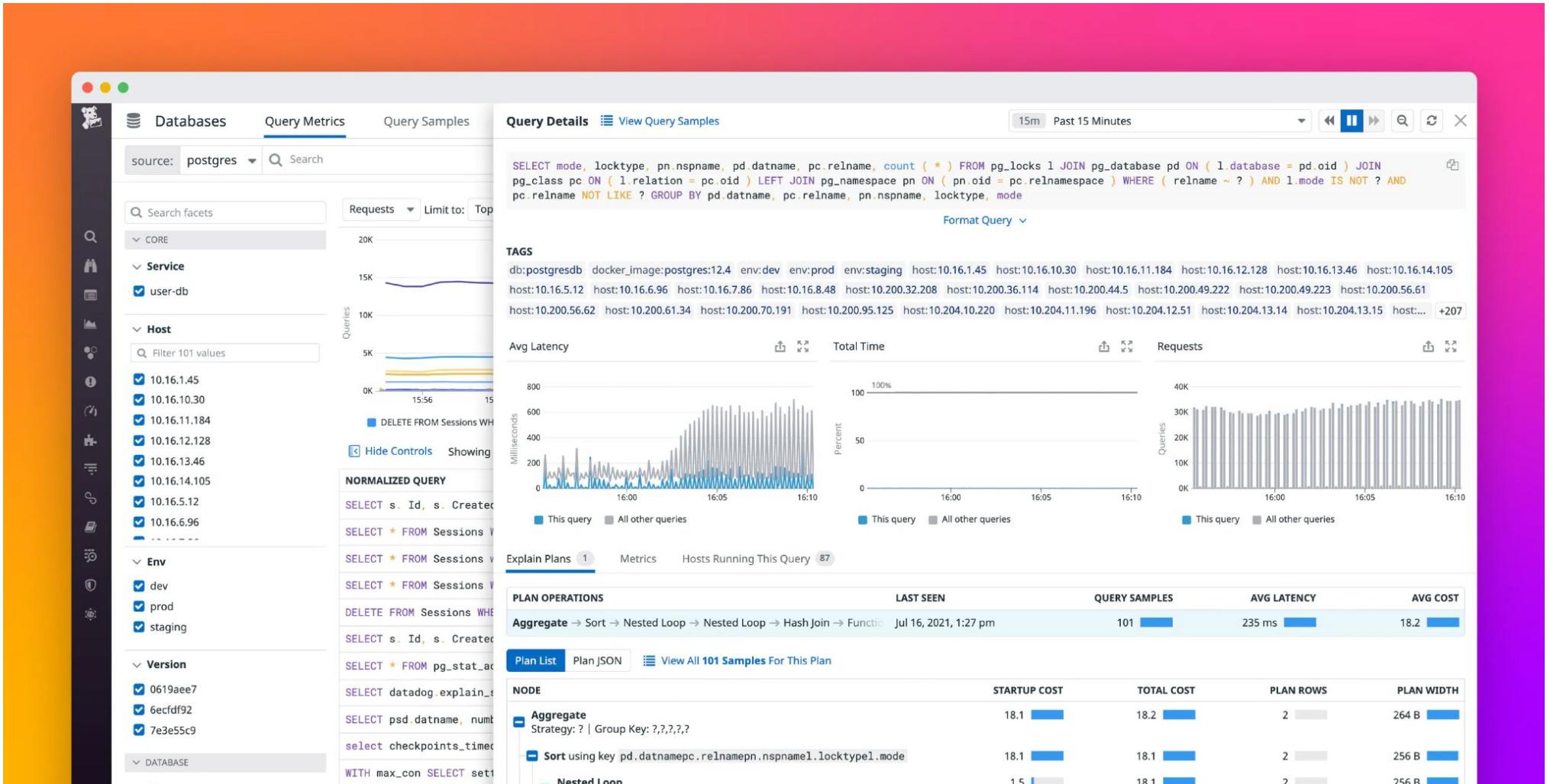
## Database Monitoring

	APM & Distributed Tracing	Database
Visibility level	Services & 3rd party libraries Including Database Query Call	performance of normalized queries historical trends in query performance
Measurement	Requests, Errors, Duration (latency)	slow queries with detailed explain plans & costs
Flame graph (Details Provided)	Execution path of a request across multiple services, including duration and errors	Sampled queries with trend / query plans and costs

Traces tell you **WHICH** requests(query) were slow at the **service(resource)** level  
Database tell you **WHY** they were slow based on **Trends, Plans & Costs** details

# #Database

## Database Monitoring



# APM Optimization

# #APM Optimization

## Trace Without Limits™

- INGEST
  - Filter Logs
  - Generate Metrics
- INDEX
  - Trace 중요도별 저장 유무 조정
  - 사용량에 따른 알람 생성

## After

- INGEST
  - Ingest 비용 절감
  - Trace 저장 없이 특정 패턴 발생시 알람
- INDEX
  - Error 혹은 @duration: >1s Trace 저장
  - Dashboard 및 알람으로 특이사항 감지



# #APM Optimization

## Metric을 활용한 사용량 모니터링



# #Quick Review

**Q1. Code level 분석시 적합한 Datadog Solution은**

1. APM
2. Continuous Profiler
3. Database Monitoring

**Continuous Profiler**

**Q2. 배포 이후 전후 특이사항 분석을 위해 필요한 Tag는**

1. DD\_ENV
2. DD\_SERVICE
3. DD\_VERSION

**DD\_VERSION Tag**



# Real User Monitoring

3시 5분에 이어서 진행 예정입니다.

# 오늘 살펴볼 내용..

## ❑ RUM 사용 USE Case

- a. RUM을 이용한 사용자 성능 분석
- b. 프론트 코드 에러 트래킹
- c. RUM Analytics를 이용한 사용자 통계 분석한 사용자 성능 분석

## ❑ RUM 연동 방법

## ❑ RUM Best Practice

# Event!

## Quiz



[Day 1]

정상기 님 - 3매  
한유종 님 - 3매  
유도영 님 - 2매  
김민영 님 - 2매  
김영환 님  
송정규 님  
송현준 님  
신민수 님  
이정훈 님  
임명진 님  
장유창 님  
정창덕 님  
최성일 님

## Great Questions



3만원권

[Day 1]

김용철 님

# RUM은 언제 사용하면 되나요?

## 1. 우리 서비스 사용자의 체감 성능 모니터링이 필요할 때

- a. 브라질 사용자가 정말로 페이지 로딩을 잘하고 있나?
- b. 페이지 로딩 시 어디 구간에 병목이 있나?

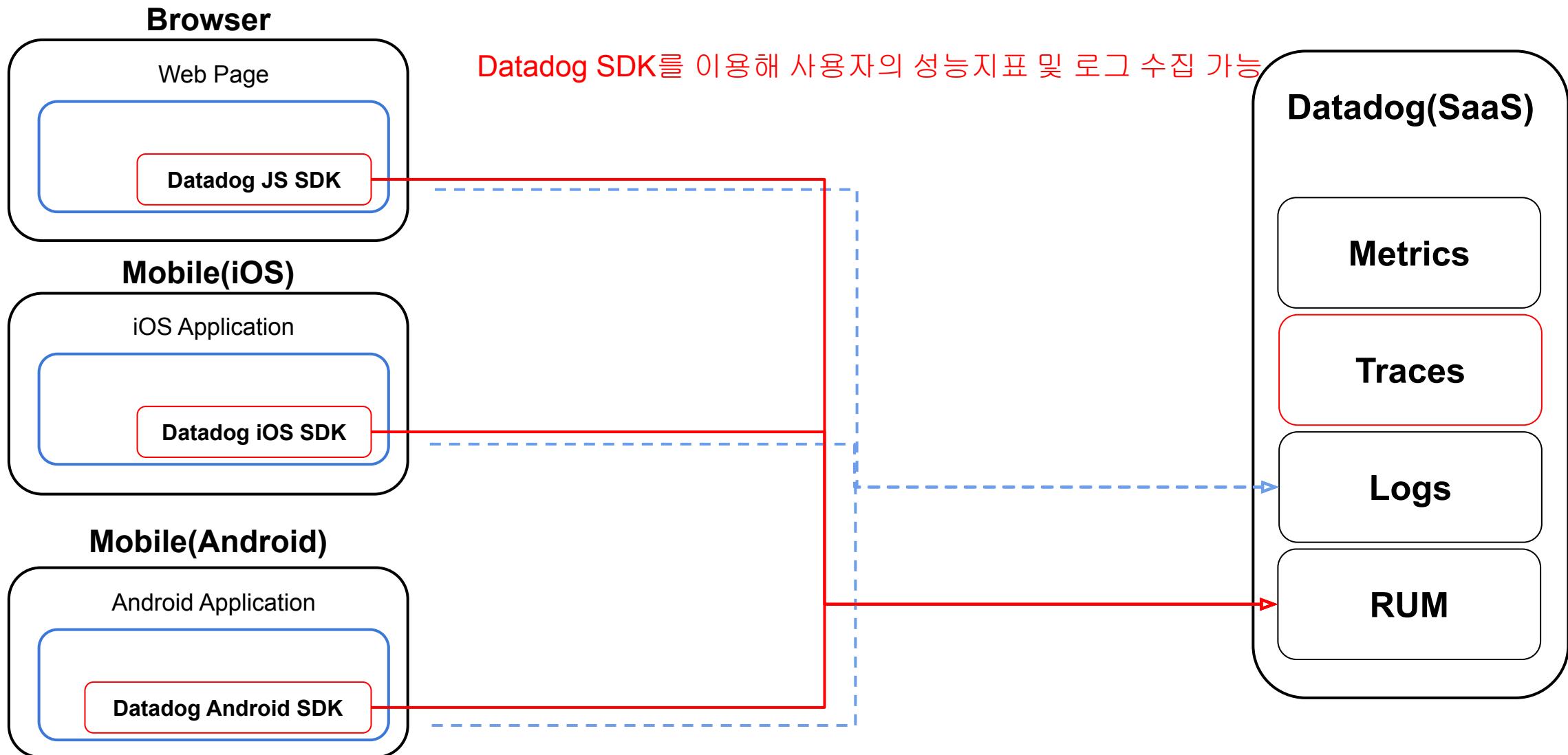
## 2. 프론트 코드에서 발생하는 에러를 수집하고자 할 때

- a. 테스트되지 않은 Device에서 어떤 에러들이 발생하는지 확인

## 3. 서비스 사용자 관점의 통계 분석이 필요할 때

- a. Daily active user가 어떻게 되나요?
- b. 서비스 유입 경로에 대한 통계
- c. 페이지별 상주시간

# RUM 연동 아키텍쳐

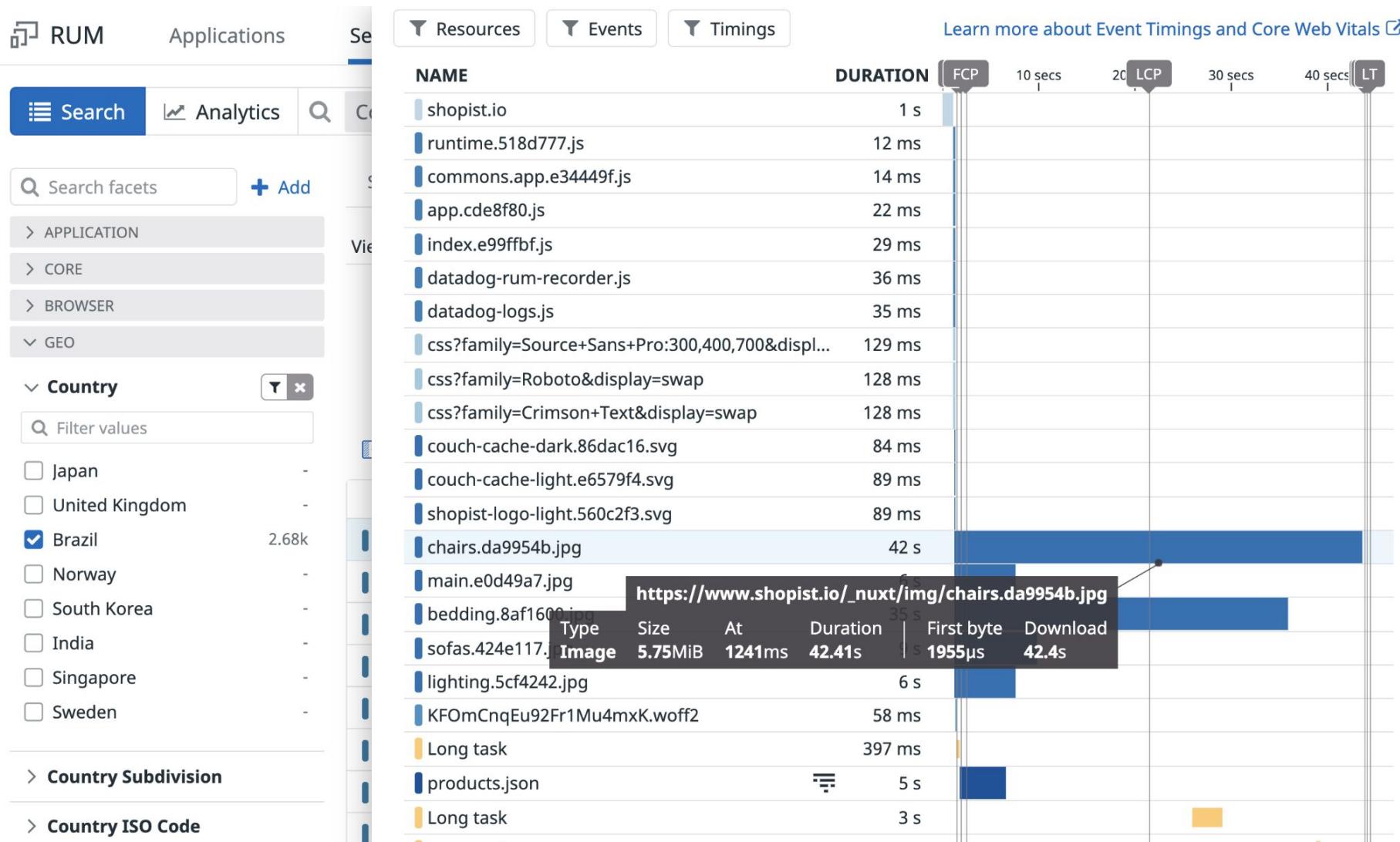


# RUM 연동 예

Browser	Android
<pre>import { datadogRum } from '@datadog/browser-rum' datadogRum.init({   applicationId: '&lt;DATADOG_APPLICATION_ID&gt;',   clientToken: '&lt;DATADOG_CLIENT_TOKEN&gt;',   site: '&lt;DATADOG_SITE&gt;',   service: 'my-web-application',   env: 'production',   version: '1.0.0',   sampleRate: 100,   trackInteractions: true, })</pre>	<pre>class SampleApplication : Application() {   override fun onCreate() {     super.onCreate()      val configuration = Configuration.Builder(       rumEnabled = true,       crashReportsEnabled = true     )       .trackInteractions()       .trackLongTasks(durationThreshold)       .useViewTrackingStrategy(strategy)       .build()      val credentials =       Credentials(&lt;TOKEN&gt;,&lt;ENV_NAME&gt;,&lt;APP_NAME&gt;,&lt;APPLICATION_ID&gt;)     Datadog.initialize(this, credentials, configuration, trackingConsent)   } }</pre>
iOS	<pre>Datadog.initialize(   applicationContext: .init(),   trackingConsent: trackingConsent,   configuration: Datadog.Configuration     .builderUsing(       rumApplicationID:       "&lt;rum_application_id&gt;",       clientToken: "&lt;client_token&gt;",       environment: "&lt;environment_name&gt;"     )     .set(serviceName: "app-name")     .trackUIKitRUMViews()     .trackUIKitActions()     .trackURLSession()     .build() )</pre>

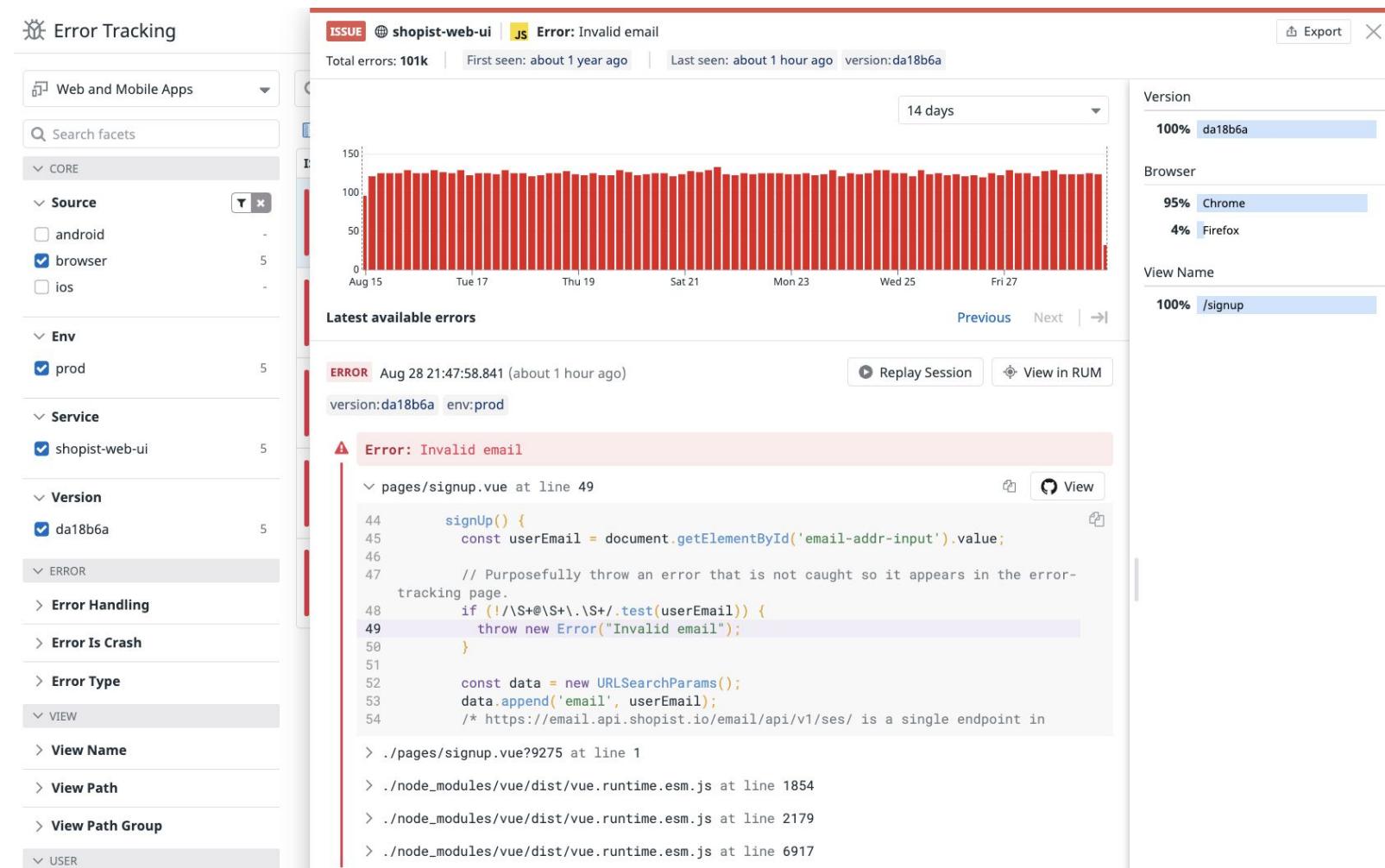
# RUM을 이용한 사용자 성능 분석

- End User 관점의 성능 트래킹
- Backend API와 연계하여 분석
- End User 이벤트 트래킹



# 프론트 에러 트래킹

- 프론트 코드 레벨에서 발생한 에러 수집
- 에러의 타임 라인 및 코드 추적



# RUM Analytics를 이용한 사용자 통계 분석

사용자로 부터 수집되는 Raw Data 샘플

- 사용자 Device/IP 정보
- 페이지별 로딩 시간/에러
- 수집희망하는 custom attribute(ex: 사용자 식별 정보)

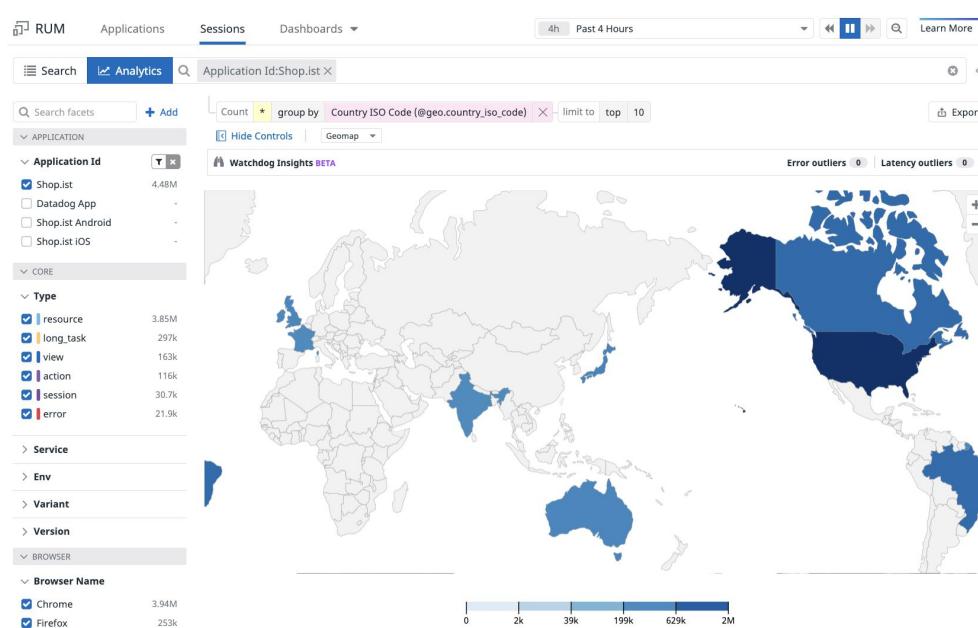
```
JSON
{
  "application": {
    "id": "75d50c62-8b66-403c-a453-aaa1c44d64bd"
  },
  "browser": {
    "name": "Chrome",
    "version": "91.0.4472.77",
    "version_major": 91
  },
  "context": {
    "browser_test": true,
    "user": {
      "email": "melissa@doe.com",
      "id": "8ff199cab6",
      "name": "Melissa Doe",
      "team": "product"
    }
  },
  "device": {
    "name": "Other",
    "type": "Desktop"
  },
  "geo": {
    "as": {
      "domain": "amazon.com",
      "name": "Amazon.com, Inc.",
      "type": "business"
    },
    "city": "Montréal",
    "continent": "North America",
    "continent_code": "NA",
    "country": "Canada",
    "country_iso_code": "CA",
    "country_subdivision": "Quebec"
  },
  "location": [
    -73.58781,
    45.50884
  ],
  "os": {
    "name": "Linux"
  },
  "service": "shopist-web-ui"
}

session: {
  "action": {
    "count": 6
  },
  "crash": {
    "count": 0
  },
  "error": {
    "count": 2
  },
  "has_replay": true,
  "id": "6984fa4c-6020-48ba-916a-98f151c35532",
  "initial_view": {
    "id": "b1f1e05e-9419-42aa-9ef5-3d8ad4e20b73",
    "name": "/",
    "url_host": "www.shopist.io",
    "url_path": "/",
    "url_path_group": "/",
    "url_scheme": "https"
  },
  "ip": "99.79.87.237",
  "is_active": false,
  "last_view": {
    "id": "ed3a2266-aee3-4150-afde-ae325c40bb33",
    "name": "/checkout",
    "url_host": "www.shopist.io",
    "url_path": "/checkout",
    "url_path_group": "/checkout",
    "url_scheme": "https"
  },
  "long_task": {
    "count": 13
  },
  "resource": {
    "count": 215
  },
  "time_spent": 5012000000,
  "type": "synthetics",
  "view": {
    "count": 9
  }
},
  "type": "session"
}
```

# RUM Analytics를 이용한 사용자 통계 분석 예

## 수집된 정보를 이용한 통계 정보 추출 예

- Daily active user가 어떻게 되나요?
- 서비스 유입 경로에 대한 통계
- 페이지별 상주시간
- Client 버전 별 특이사항 분석
- 국가별 접속자 현황



Analytics view for Application Id:Shop.list showing initial and last view paths.

INITIAL VIEW PATH	LAST VIEW PATH	COUNT
/	/checkout	30.74k
/	/	27.46k
	/cart	11.42k
	/department/sofas	5.274
	/profile-edit	4.594
	/department/chairs/product/1/index.html	1,941
	/department/lighting	495
	/department/chairs/product/8	336
		222
		182

Analytics view for Application Id:Shop.list showing average resource duration by browser and version.

BROWSER NAME	BROWSER VERSION	AVG:RESOURCE DURATION
Edge	91.0.831.1	465 ms
Edge Mobile	91.0.831.1	530 ms
Chrome	91.0.4472.77	487 ms
	92.0.4515.159	481 ms
Firefox Mobile	89.0	224 ms
		370 ms

# Recommendations

## 1. Datadog RUM 과정 구조와 세션 개념에 대해 이해 필요

- Session은 사용자 별로 생성됩니다. (접속자 많을 수록 비용이 올라가는 구조)
- Session은 End User가 아무런 동작이 없으면 15분 후 소멸
- Session은 End User가 지속적으로 요청을 만들 경우 최대 4시간까지 유효

## 2. Datadog의 권장 Tag를 활용하세요

- service, env, version tag 기준으로 분석 데이터를 뽑는 경우가 많습니다
- 개별 사용자를 구분할 수 정보를 추가하면 좀 더 정확한 비지니스 인사이트 확보가 가능합니다([참고](#))

## 3. RUM event를 선별적으로 수집할 수 있도록 RUM 초기화 블록에 조건문을 추가

- 특정 등급의 End User일 경우만 수집되도록 조건문으로 추가하여 선별적 수집
- sampleRate도 동적으로 제어할 수 있도록 구현하시면 예산에 맞춰 RUM을 사용하시는데 도움이 됩니다.

## 4. RUM event와 Backend 요청을 연결하여 볼 수 있도록 옵션 설정

- allowedTracingOrigin 옵션에 연결하고자 하는 도메인을 넣으면 APM Trace와 연계하여 분석이 가능합니다.

# RUM 삽입 코드 샘플

```
import { datadogRum } from '@datadog/browser-rum';
```

```
datadogRum.init({
```

```
    applicationId: '<DATADOG_APPLICATION_ID>',  
    clientToken: '<DATADOG_CLIENT_TOKEN>',  
    site: '<DATADOG_SITE>',  
    service: 'my-web-application',  
    env: 'production',  
    version: '1.0.0',  
    sampleRate: 100,  
    replaySampleRate: 100,  
    trackInteractions: true  
    allowedTracingOrigins: ["https://api.example.com",  
        "https://V.*\my-api-domain\com/"]
```

```
});
```

```
datadogRum.startSessionReplayRecording();
```

# 그 외의 Recommendation

## # minify된 javascript의 경우 Source map을 등록하면 Error 발생 코드까지 확인이 가능합니다

Sourcemap 적용 전  
가능합니다

ERROR Sep 14 17:09:57.411 (39 minutes ago)

 View in RUM

 Error: Actions must be plain objects. Use custom middleware for async actions.

https://static.datadoghq.com/static/v/35.3030471/js/spa.min.js at line 1

https://static.datadoghq.com/static/v/35.3030471/js/spa.min.js at line 1

https://static.datadoghq.com/static/v/35.3030471/js/spa.min.js at line 1

https://static.datadoghq.com/static/v/35.3030471/js/spa.min.js at line 1

https://static.datadoghq.com/static/c/profiling-ExplorerPage.3d48d8c7b950e5de8042.min.js at line 1

Sourcemap 적용 후

ERROR Sep 14 17:45:33.762 (4 minutes ago)

 View in RUM

 TypeError: Cannot read property 'addUserAction' of undefined

▼ pages/department/\_dept/product/\_product.vue at line 42

```
37     const sessionID = window.localStorage.getItem("session_id");
38
39     // Attempt to register a user action for a specific product id. The DD_RUM property is
40     // intentionally misspelled to trigger a source code error (to be displayed in error-tracking).
41     if (this.product.id == "31") {
42         window.DD_RUMM.addUserAction("add_product", { productId });
43     }
```

참고링크

# #Quick Review

**Q1. RUM은 어떤 경우에 사용하면 좋을까요? USE Case 2개만 알려주세요**

**Q2. Browser RUM event와 APM의 Trace를 연결하는데 사용되는 옵션은??**

1. allowedTracingOrigins
2. trackInteractions
3. sampleRate
4. service

```
import { datadogRum } from '@datadog/browser-rum'

datadogRum.init({
  applicationId: '<DATADOG_APPLICATION_ID>',
  clientToken: '<DATADOG_CLIENT_TOKEN>',
  ...otherConfig,
  allowedTracingOrigins: ["https://api.example.com", /https:\/\/.*\my-
api-domain\.com/]
})
```

**Q3. RUM 세션은 사용자 이벤트가 없을 경우 15분 후 Expire가 됩니다. 지속적으로 이벤트가 있을 경우 최대 몇 시간 유지가 가능한가요?**



# DATADOG

## Synthetic Monitoring

# Synthetic 주요 기능

## New API Test



### Monitor uptime and availability

Test your websites and APIs from several locations around the world to assess availability and uptime.

## New Multistep API Test

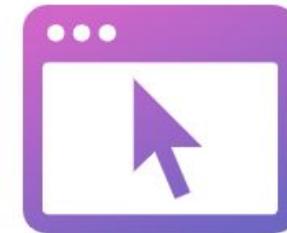


NEW

### Monitor uptime and availability by linking multiple requests

Create a test by using the response data from a series of linked HTTP tests.

## New Browser Test



### Monitor key business flows

Create step by step recordings of your key business flows to make sure they are meeting your performance goals from multiple locations around the world.

다수의 테스팅 노드로 부터 API 엔트포인트에 대한 성능 테스트

Multistep API Test가 필요할 경우 사용  
예) 로그인 토큰 획득 ⇒ 로그인 테스트

레코딩 기반으로 UX 테스트 시나리오 작성하여 다수의 테스팅 노드로부터 테스트시 사용

# Synthetic Browser 테스트 생성 가이드

UX Monitoring ⇒ New Test ⇒ New Browser Test 선택

Create a new synthetic test



New API Test



**Monitor uptime and availability**

Test your websites and APIs from several locations around the world to assess availability and uptime.

New Multistep API Test

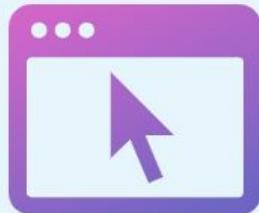


NEW

**Monitor uptime and availability by linking multiple requests**

Create a test by using the response data from a series of linked HTTP tests.

New Browser Test



**Monitor key business flows**

Create step by step recordings of your key business flows to make sure they are meeting your performance goals from multiple locations around the world.

# Synthetic Browser 테스트 생성 가이드 (테스트 URL 및 Device 선택)

Synthetics > New Browser Test

## 1 Set your test details

Starting URL

`https://www.datadoghq.com/`



- ❖ 테스트 희망 도메인 입력
- ❖ 필요시 Advanced Options를 이용하여 Header 설정

> Advanced Options

Name

www.datadoghq.com 페이지 렌더링 테스트

Environment (env)

env:prod X

- ❖ 테스트에 대한 tag를 적절하게 추가하여 알람 및 대시보드 구성에 활용합니다

Additional Tags

url:www.datadoghq.com X site:datadog\_home X team:front X



Browsers & Devices

Chrome

Firefox

Edge NEW

Laptop Large



Tablet



Mobile Small



# Synthetic Browser 테스트 생성 가이드 (테스팅 노드 및 주기 설정)

2

## Select locations

### All Locations (2)

### Managed Locations (2)

### Americas (1)

- Canada Central (AWS)
- N. California (AWS)
- Ohio (AWS)
- Oregon (AWS)
- São Paulo (AWS)
- Virginia (Azure) NEW

### Asia Pacific (1)

- Mumbai (AWS)
- Seoul (AWS)
- Singapore (AWS)
- Sydney (AWS)
- Tokyo (AWS)

### Europe (0)

- Frankfurt (AWS)
- Ireland (AWS)
- London (AWS)
- Paris (AWS)
- Stockholm (AWS)

- ❖ 희망하는 테스팅 노드 위치 및 테스트 주기 선택
- ❖ 필요시 다음의 링크를 참고하여 테스트 노드 추가가 가능
  - [Private location 참고](#)

3

## Specify test frequency

Run your test every

5

minutes



# Synthetic Browser 테스트 생성 가이드 (알람 설정)

## 4 Define alert conditions

Retry test  times after  ms in case of failure

An alert is triggered if your test fails for  minutes from any  of 2 locations

In case of failure, retry test 2 times, with 2000 ms of wait between retries.

The test is in failure and a notification is sent if during the last 2 minutes, at least one location was in failure.

알람 조건 설정

- ❖ 몇 분간 지속적으로 실패시 알람을 수신할 지 정의

## 5 Notify your team

Monitor Name ?

Home 페이지 렌더링 이슈

@ {{}}

알람 수신자 지정

- ❖ @을 이용하여 email 혹은 slack 등으로 알람 전송 가능

Edit Preview Markdown Help Use Message Template Variables

홈페이지 렌더링에 이슈가 있습니다.

다음의 링크를 참고하여 확인 바랍니다.

[link text](https://p.datadoghq.com/sb/rkIUVX-5444ed3c96132c9e32ff0bd758ef43e5)

@front-team@synthetics.com

Notify your service and your team members

[Never] ▼ renotify if the monitor has not been resolved

Monitor Priority

P2 (High) ▼

Priority 지정

- ❖ 테스트 실패의 영향도를 고려하여 Priority 지정

Cancel

Save & Exit

Save & Edit Recording →

Save & Edit Recording을 클릭하여 테스트 시나리오

레코드

# Synthetic Browser 테스트 생성 가이드(시나리오 생성)

Synthetics > Test details > Edit Browser Test > Edit Recording

www.datadoghq.com 페이지 렌더링 테스트

Run from 2 locations and 2 devices

https://www.datadoghq.com/

Go →

Select device ▾

Open in Popup ↗



Start Recording

클릭 후 오른쪽에 보이는 화면에서 웹페이지를 브라우징 하면 자동으로 Recording 이 됩니다. (Chrome에서만 가능)

Add New:

✓ Assertion

Navigation

+ Special Actions

+ Variables

Subtest

HTTP Request

시나리오에 Scroll, Wait 등의 Action을 추가하기 위한 기능

페이지 Refresh나 다른 URL로 이동하고자 할때 사용

HTTP Endpoint 테스트 스텝을 추가하기 위한 기능

다른 Synthetics 테스트를 추가하기 위한 기능

페이지 컨텐츠에 대한 점검을 위한 조건 설정위한 기능

Datadog Database Monitoring is now available



ABOUT BLOG LOGIN

FREE TRIAL

## Modern monitoring & security

See inside any stack, any app, at any scale, anywhere.

FREE TRIAL

SEE THE PLATFORM



# Synthetic Browser 테스트 주요 USE Case

## 1. UX 시나리오에 대한 자동화 테스트 진행

### a. 주요 테스트 조건

- i. Element에 특정 text가 보이는지 점검
- ii. URL에 예상되는 string이 잘 포함되어 있는지 점검
- iii. Email에 원하는 텍스트가 포함되어 전송되었는지 확인
- iv. 파일이 잘 다운로드되었는지 확인

## 2. CI 솔루션과 연계 하여 새로 commit한 코드에서 문제 확인시 CI pipeline 를 백 및 알람 전송

## 3. 테스트 수행시간을 트래킹 하여 페이지 로드 성능이 느려진 시점에 대한 분석 진행

## 4. APM과 연계하여 API단 문제 발생시 Front ↔ Backend를 연계하여 분석

# 1. UX 시나리오에 대한 자동화 테스트 진행

## 1. 클릭 기반으로 테스트 시나리오를 Recording하여 테스트 케이스 작성

Synthetics > Test details > Edit Browser Test > Edit Recording  
www.datadoghq.com 페이지 렌더링 테스트  
Run from 2 locations and 2 devices

**Stop Recording**

Add New:  
✓ Assertion    Navigation    + Special Actions  
+ Variables    Subtest    HTTP Request

> 2 variables available

4 steps recorded    Clear All Steps

- 1 Free Trial 텍스트가 정상적으로 보이는지 확인  
Should contain "FREE TRIAL"
- 2 Test active page URL's content  
Should contain "datadoghq"
- 3 Test text is present on the active page monitoring
- 4 Test the active page does not contain text forbidden

https://www.datadoghq.com/ Go Select device Open in Popup DATADOG Modern monitoring & security See inside any stack, any app, at any scale, anywhere. FREE TRIAL SEE THE PLATFORM

## 2. 컨텐츠에 특정 text가 잘 보이는지

확인  
Synthetics > Test details > Edit Browser Test > Edit Recording  
www.datadoghq.com 페이지 렌더링 테스트  
Run from 2 locations and 2 devices

Test active page URL's content  
Should contain "datadoghq"

Step position: 2  
Step Name: Test active page URL's content  
Value: Content should contain given value: datadoghq

Advanced Options    Cancel    Apply

https://www.datadoghq.com/ Go Select device Open in Popup DATADOG Modern monitoring & security See inside any stack, any app, at any scale, anywhere. FREE TRIAL SEE THE PLATFORM

## 3. URL에 특정 text가 보이는지 점검

Synthetics > Test details > Edit Browser Test > Edit Recording  
www.datadoghq.com 페이지 렌더링 테스트  
Run from 2 locations and 2 devices

Test active page URL's content  
Should contain "datadoghq"

Step position: 2  
Step Name: Test active page URL's content  
Value: Content should contain given value: datadoghq

Advanced Options    Cancel    Apply

https://www.datadoghq.com/ Go Select device Open in Popup DATADOG Modern monitoring & security See inside any stack, any app, at any scale, anywhere. FREE TRIAL SEE THE PLATFORM

## 4. Email이 정상적으로 전달되었는지

테스트 Browser Test > Edit Recording  
Sig. up suggests you're a developer  
Run from 1 location and 1 device

Test that an email was received

Subject: should equal given value: Welcome to Shopist!  
> Use Variable

Body: should match regex given value: Your verification code is \d{1,6}  
> Use Variable

Wait for 0 s before declaring this step as failed

Cancel    Apply

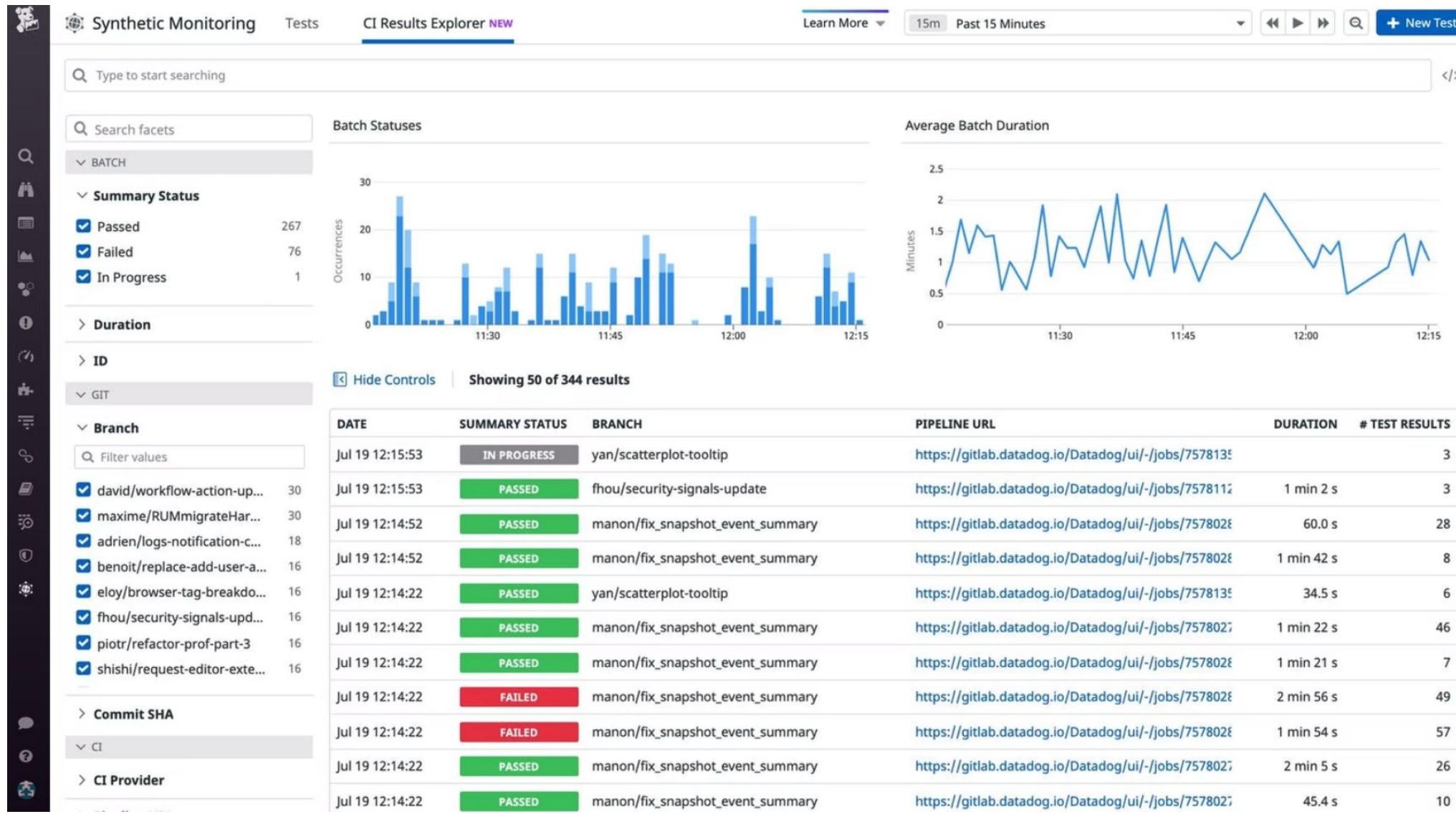
https://shopist.io/signup-verify?email=d7z-re-aqr9.2757529511%40synthetics.dtdg.co Go Select Open in Popup COUCH CACHE CHAIRS SOFAS BEDDING LIGHTING MY PROFILE CART (0)

You've got Email! Verification required  
You must first verify your email address d7z-re-aqr9.2757529511@synthetics.dtdg.co.  
We've sent you an email with a verification link, please check your inbox for further instructions.

CONTINUE SHOPPING

## 2. CI 솔루션과 연계하여 특이사항 탐지 시 CI Pipeline

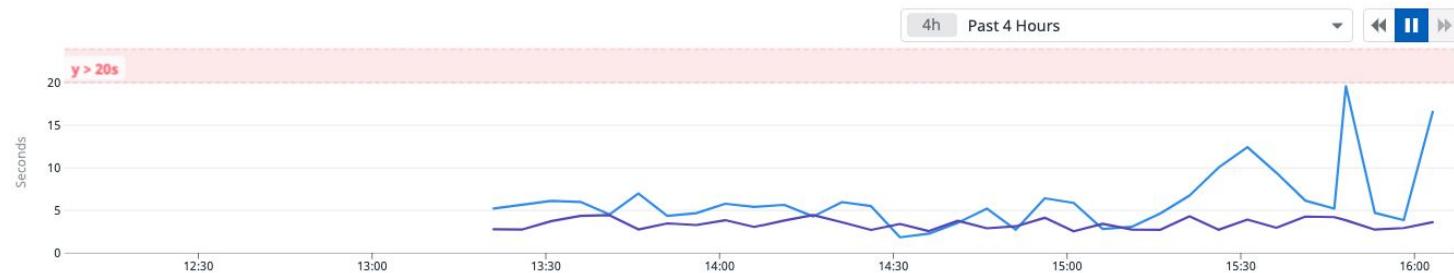
USE Case: 서비스 동작에 영향을 주는 코드 반영 시 CI Pipeline에서 롤백하거나 특이사항을 담당자에게 알람 전송



### 3. 테스트 수행시간을 트래킹 하여 특이사항 발생시 알람

USE Case: 서비스 동작에 영향을 주는 코드 반영시 CI Pipeline에서 롤백하거나 특이사항을 담당자에게 알람 전송

New Monitor > Metric Monitor



- 테스트 수행결과는 `synthetics.browser.*` 메트릭으로 기록됨
- 메트릭을 이용하여 다양한 형태의 Dashboard 구성 가능
- 메트릭을 이용하여 담당자에게 이메일/Slack 등으로 전송

#### 1 Choose the detection method

Threshold Alert Change Alert Anomaly Detection Outliers Alert Forecast Alert

An alert is triggered whenever a metric crosses a threshold. [?](#)

#### 2 Define the metric

Source Edit

a `synthetics.browser.test_duration` from `url:www.datadoghq.com` avg by `location`

Multi Alert [Trigger a separate alert for each](#) `location` reporting your metric [?](#)

#### 3 Set alert conditions

Trigger when the metric is `above` the threshold `on average` during the last `5 minutes` for any `location`

Alert threshold: >  (20000ms)

# 4. APM 과의 연계 분석

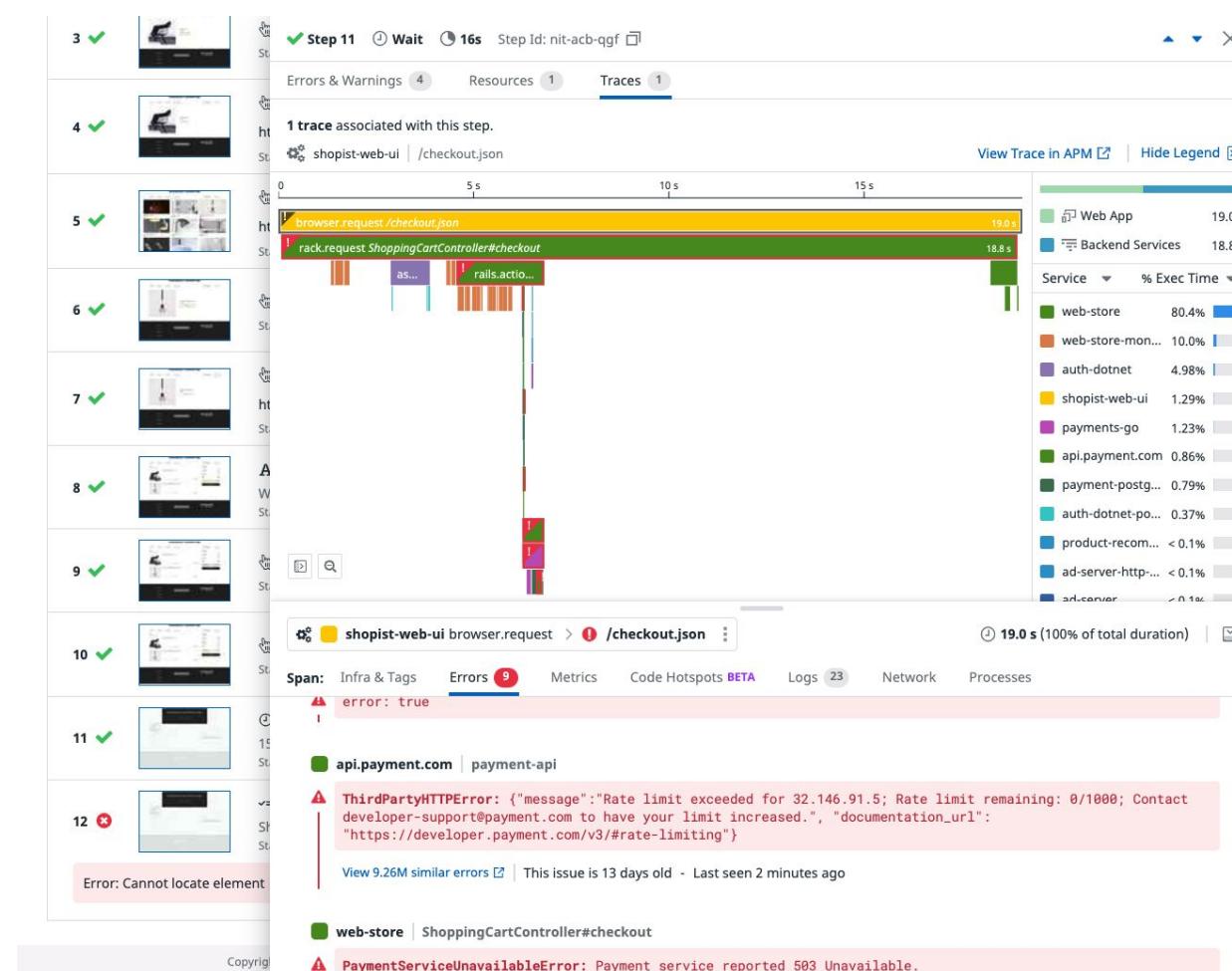
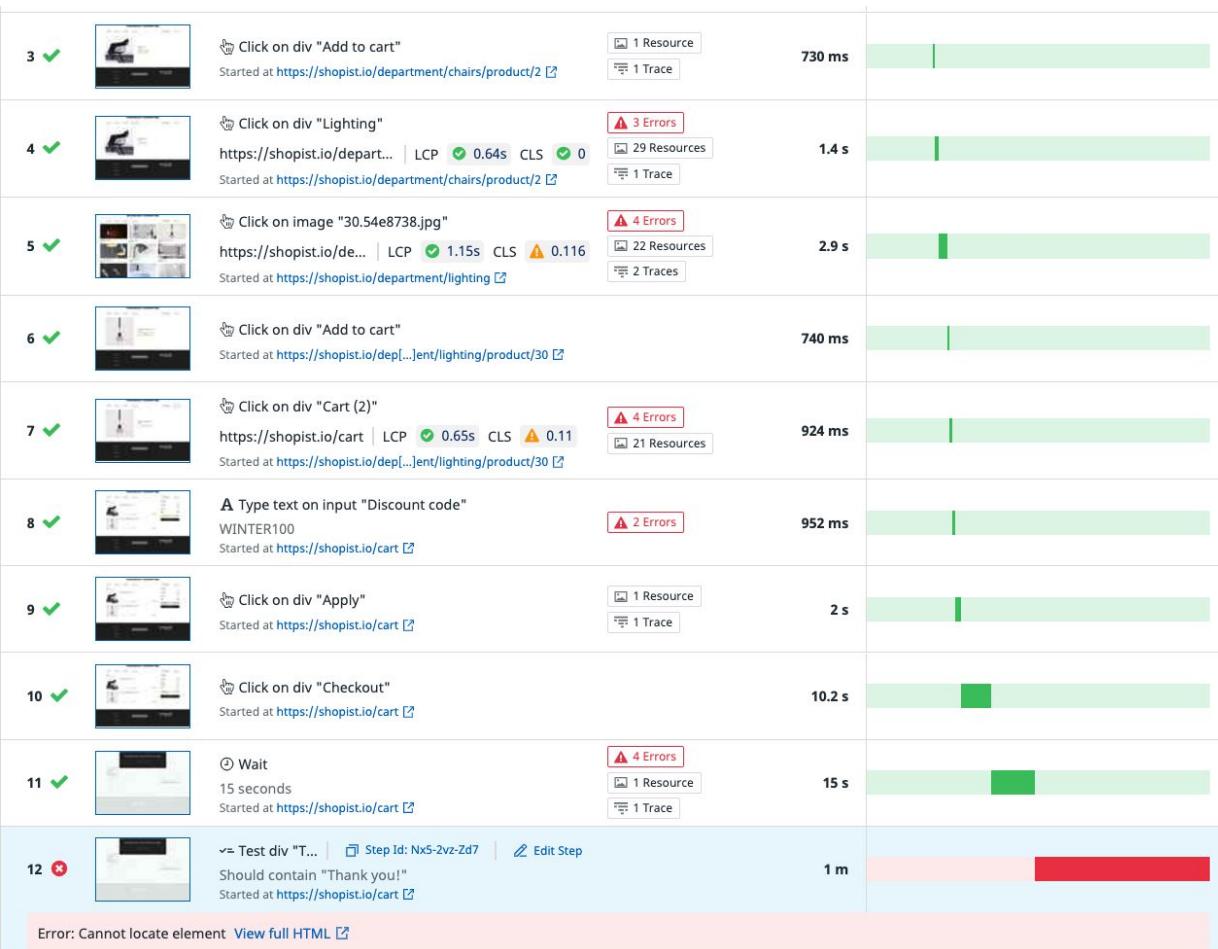
USE Case: Synthetics 테스트를 통해 문제 확인 후 문제가 발생한 구간이 프론트 이슈인지 백엔드 이슈인지

연계하여 분석

Synthetics 테스트 결과를 통해 문제가 되는 구간 확인 후 클릭



문제가된 구간의 API 응답 결과 및 백엔드 상태 확인을 통해 이슈 확인



# Synthetic 주요 메트릭 정보

`synthetics.browser.time_to_interactive`

- 페이지가 interactive 하는데까지 걸린 시간

## Step Results

STATUS	STARTING URL	STEPS	DURATION
OK	<a href="https://www.datadoghq.com/">https://www.datadoghq.com/</a>	5 / 5	4s

LOCATION Ohio (AWS) DEVICE Laptop Large BROWSER firefox 92.0.1 TIME RAN 2 mins ago (Nov 21, 2021, 4:23 pm) RUN TYPE Scheduled

### SCREENSHOT ACTION

0 ✓		☑ Navigate to start URL <a href="https://www.datadoghq.com/">https://www.datadoghq.com/</a> Started at <a href="#">about:blank</a>
1 ✓		✗= Free Trial 텍스트가 정상적으로 보이는지 확인 Should contain "FREE TRIAL" Started at <a href="https://www.datadoghq.com/">https://www.datadoghq.com/</a>
2 ✓		URL Test active page URL's content Should contain "datadoghq" Started at <a href="https://www.datadoghq.com/">https://www.datadoghq.com/</a>
3 ✓		ABC Test text is present on the active page Found "monitoring" on the page Started at <a href="https://www.datadoghq.com/">https://www.datadoghq.com/</a>
4 ✗		✗ Test the active page does not contain text Could not find "forbidden" in the element Started at <a href="https://www.datadoghq.com/">https://www.datadoghq.com/</a>



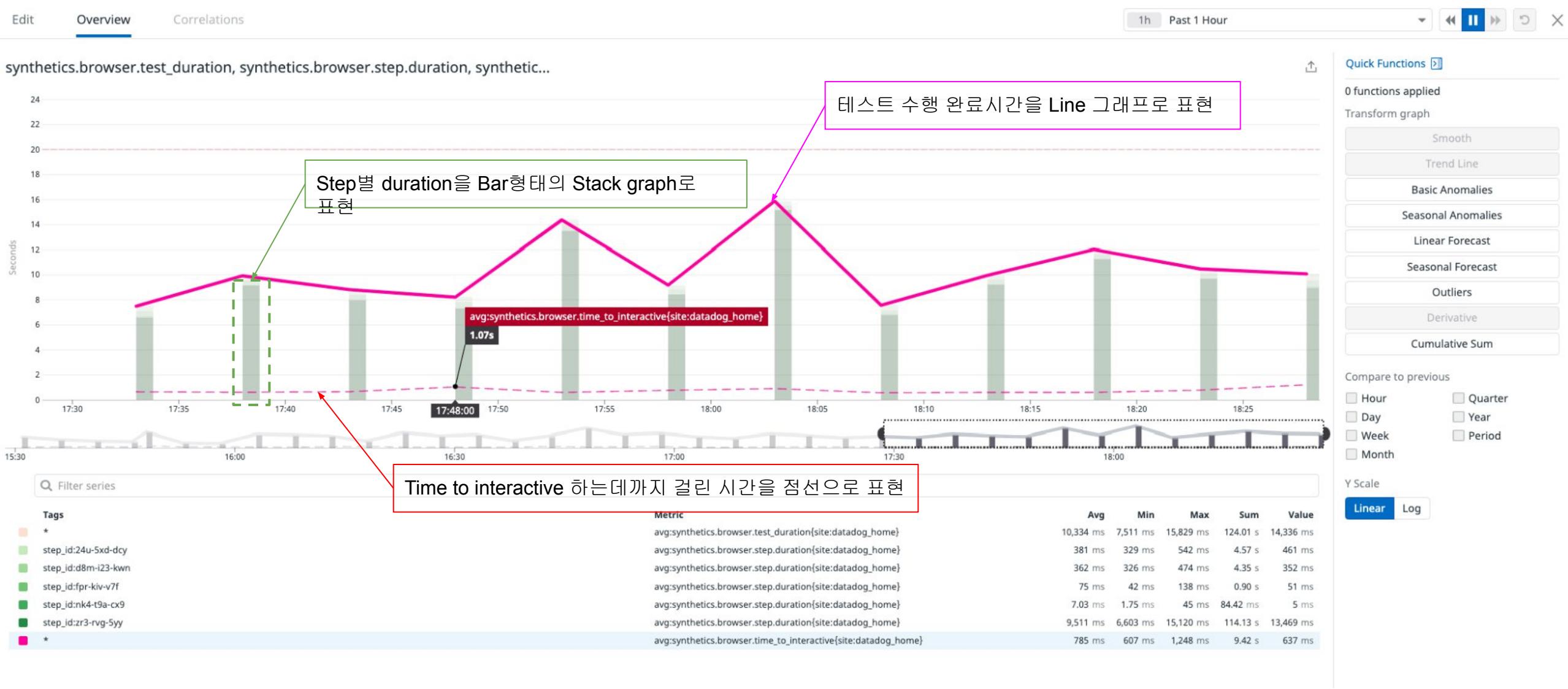
`synthetics.browser.step.duration`

- 개별 Step이 완료되는데 시간을 트래킹 (step\_id tag로 구분)

`synthetics.browser.test_duration`

- 5개의 step을 다 마치는데 까지 걸린 소요 시간

# Synthetic 메트릭을 활용한 Dashboard 위젯



# Synthetic Pricing

## API Tests

STARTING AT

\$ **5**

Per ten thousand test runs, per month\*

API 테스트 및 MultiStep API에서 실행 테스트 수로 과금

Proactively monitor site availability

- Monitor uptime SLAs and SLOs
- Globally managed locations
- Sophisticated alerting capabilities

\*Billed annually or \$7.20 on-demand

## Browser Tests

STARTING AT

\$ **12**

Per thousand test runs, per month\*

Easily monitor critical user journeys

- Record tests without code
- Intelligent, self-maintaining tests
- View screenshots and front-end errors for every step

\*Billed annually or \$18 on-demand

테스트 결과에 대한 스크린샷  
보관

# #Quick Review

**Q1. Synthetic은 Agent를 설치해야만 사용이 가능한가요?**

**Q2. Synthetic Use case 2개만 알려주세요**

**Q3. 외부에서 접근 불가능한 엔드포인트 (private VPC)에 Synthetic 테스트가 가능한가요? 가능하다면 어떻게 하나요?**

# RUM & Synthetic 세션 정리

## ❖ Datadog RUM

- 사용자 관점의 성능 지표를 상세 분석
- APM 연동하여 백엔드 지표와 함께 연계된 분석
- 수집된 사용자 데이터를 통해 비지니스 인사이트 분석

## ❖ Datadog Synthetic

- 글로벌 테스팅 노드를 활용하여 우리 서비스의 지역별 성능 파악
- 문제 탐지시 백엔드와 연계되어 신속하게 분석할 수 있도록 지원



# DATADOG

## New Features

Datadog Partner 교육 (Day 2)  
4:21 PM에 시작합니다!

# 2021년에 추가된 제품 및 기능 소개(50min)

## APM

- Request Flow Map
- Error Tracking
- Database Monitoring

## RUM

- RUM Funnel
- Session Replay

## Incident Management

## CI Visibility

4시 20분에 이어서 진행하겠습니다.

## Datadog Portal

- Event Analytics
- Audio Log

## Infrastructure

- Network Device Monitoring
- Serverless 업데이트
- Azure Auto muting

## Log

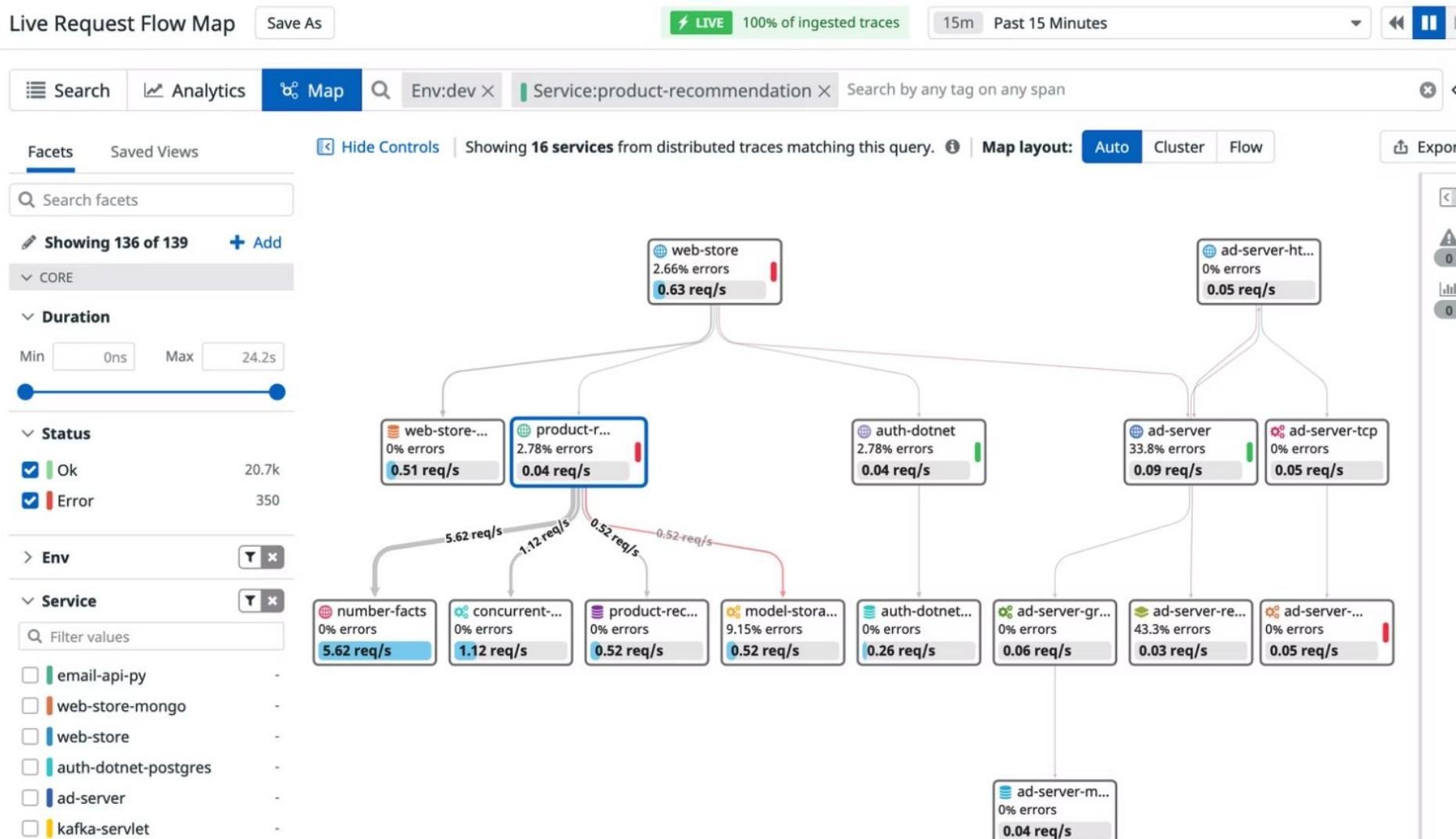
- Log 복합 쿼리

## Security

- CSPM
- Workload Security

# #APM - Request Flow Map

マイクロ 서비스 아키텍쳐에 대한 가시성 확보 및 어떤 구간에 이슈가 있는지 시각적으로 확인하여 분석



[https://docs.datadoghq.com/tracing/trace\\_search\\_and\\_analytics/request\\_flow\\_map/](https://docs.datadoghq.com/tracing/trace_search_and_analytics/request_flow_map/)

# #Database Monitoring

Database 쿼리별 성능 정보에 대한 가시성을 제공하여 쿼리 호출 비용(Row Scan)이 큰 쿼리에 대해 쉽게 찾을 수 있도록 분석 데이터 제공

The screenshot shows the Datadog Database Monitoring interface for a PostgreSQL source. The left sidebar contains navigation links for Databases, Query Metrics (selected), Query Samples, and a search bar. Under 'CORE' facets, 'user-db' is selected. The main area displays a query details card with a complex SQL query and its execution plan. Below this are three time-series charts: 'Avg Latency' (milliseconds vs. time), 'Total Time' (percentile vs. time), and 'Requests' (queries vs. time). The bottom section shows the 'Explain Plans' tab with a table of operations like 'Aggregate', 'Sort', and 'Nested Loop' along with their metrics.

source: postgres ▾ Search

Search facets Requests Limit to: Top 20K

**TAGS**

db:postgresdb docker\_image:postgres:12.4 env:dev env:prod env:staging host:10.16.1.45 host:10.16.10.30 host:10.16.11.184 host:10.16.12.128 host:10.16.13.46 host:10.16.14.105 host:10.16.5.12 host:10.16.6.96 host:10.16.7.86 host:10.16.8.48 host:10.200.32.208 host:10.200.36.114 host:10.200.44.5 host:10.200.49.222 host:10.200.49.223 host:10.200.56.61 host:10.200.56.62 host:10.200.61.34 host:10.200.70.191 host:10.200.95.125 host:10.204.10.220 host:10.204.11.196 host:10.204.12.51 host:10.204.13.14 host:10.204.13.15 host:... +207

**Avg Latency**

Milliseconds

0 200 400 600 800

15:56 15:57 15:58 15:59 15:60 15:56 15:57 15:58 15:59 15:60

This query All other queries

**Total Time**

Percent

0 50 100

16:00 16:05 16:10

This query All other queries

**Requests**

Queries

0K 10K 20K 30K 40K

16:00 16:05 16:10

This query All other queries

**NORMALIZED QUERY**

SELECT s.Id, s.Created

SELECT \* FROM Sessions V

SELECT \* FROM Sessions V

DELETE FROM Sessions WHE

EXPLAIN PLANS 1 Metrics Hosts Running This Query 87

**PLAN OPERATIONS**

LAST SEEN

Aggregate → Sort → Nested Loop → Nested Loop → Hash Join → Function Jul 16, 2021, 1:27 pm

QUERY SAMPLES

AVG LATENCY

AVG COST

101 235 ms 18.2

**NODE**

Aggregate Strategy: ? | Group Key: ?,?,?,? STARTUP COST 18.1

Sort using key pd.datnamepc.relnamelpn.nspnamel.locktypel.mode TOTAL COST 18.2

Nested Loop PLAN ROWS 2

PLAN WIDTH 264 B

WITH max\_con SELECT set

# #RUM - Session Replay

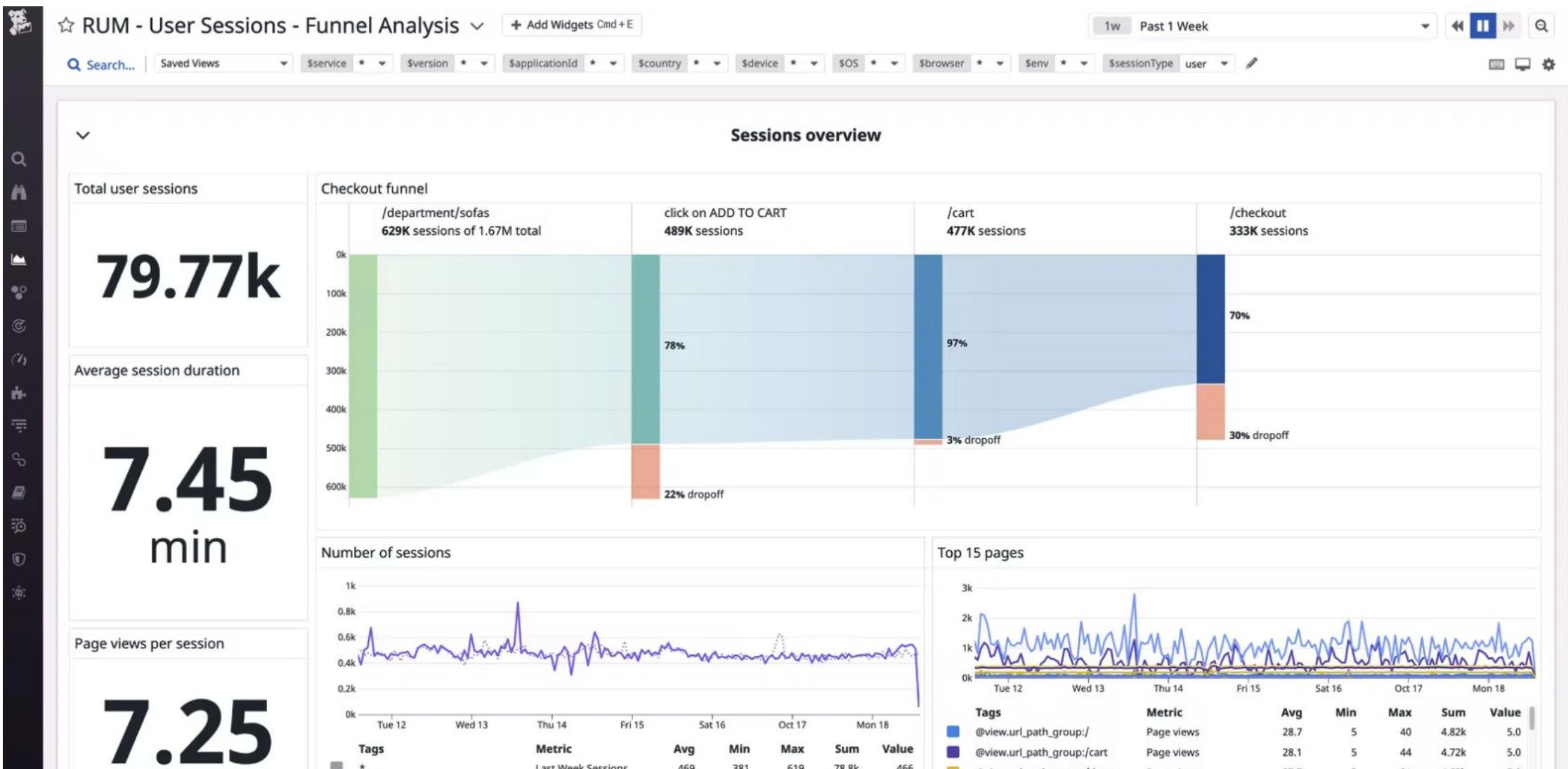
사용자의 UX 여정을 Video 재생하듯이 Play하여 UX 여정 중 문제가 되는 구간을 빠르게 찾을 수 있도록 기능지원

The screenshot displays a browser session replay interface. On the left, a sidebar contains various monitoring icons. The main area shows a grid of nine lighting products from a store. Each product has an image, name, and price. A play button at the bottom indicates the session is paused at 00:20 / 00:38, with a URL of /department/lighting. To the right, a timeline titled "IN PROGRESS" shows the sequence of events from July 27, 9:38 am, including page loads and user interactions. A legend at the top of the timeline indicates "View", "Action", and "Error". The timeline lists several errors related to "TypeError" and "ReferenceError" occurring during profile edits.

Event Time	Action	Details
0 s	Load Page	/
19.6 s	Load Page	/department/lighting
20.6 s	Load Page	/department/lighting/product/?
22.6 s	Click on ADD TO CART	on page /department/lighting/product/?
22.6 s	source error	TypeError: Cannot read property 'addUserAction' ...
22.6 s	console error	console error: TypeError: Cannot read property '...'
30.7 s	Load Page	/profile
34.9 s	SPA Route Change	/profile-edit
36.6 s	Click on SAVE PROFILE	on page /profile-edit
36.6 s	source error	TypeError: Converting circular structure to JSON --...
36.6 s	source error	TypeError: Converting circular structure to JSON --...
36.6 s	console error	console error: TypeError: Converting circular str...
37.5 s	source error	ReferenceError: profile is not defined
37.5 s	source error	ReferenceError: profile is not defined
37.5 s	console error	console error: ReferenceError: profile is not defined
37.5 s	SPA Route Change	/profile

# #RUM - FUNNEL (엔드유저에 대한 이탈률 분석)

RUM 세션 데이터 기반으로 UX 구간 이동중 이탈률이 어느정도 되는지 인사이트 제공



# #Incident Management

장애 발생시 분석 및 조치에 대한 타임라인 기록 및 Task를 관리 할 수 있도록 기능제공 (Datadog에 저장된 메트릭 그래프를 이용해 효과적인 보고서 작성 가능)

Incidents > IR-1193: [Jacky] 사용자 접속 불가능

Notify



ACTIVE SEV-2 (High) Slack Channel Video Call Jira Issue Postmortem

Declared 25 days ago 17 minutes of customer impact

Overview Timeline Remediation Responders BETA Notifications



Write a note, link or code block. Press Shift + Return to submit

Add Note

Hide Controls

12 entries

Oldest First ↓

FILTERS

Content Type

- Incident Update 4
- Integration Update 3
- Responder Note 4
- Graph 2
- Task 2

Important

- Yes 3
- No 9

Responder

- Jacky Jung 12

Oct 29, 2021  
3:06 pm GMT+9

Incident declared ACTIVE by Jacky Jung

IR-1193: [Jacky] 사용자 접속 불가능

Severity SEV-2

Slack #incident-1193

Incident Commander Jacky Jung

Notified slack-jacky-demo

3:06 pm  
 Jacky Jung  
DB 장애 발생

3:08 pm  
 Customer impact updated by Jacky Jung

Scope 웹 접속 불가

Started at 10/29/2021 3:06 pm

3:10 pm  
 Jira Issue created by Jacky Jung

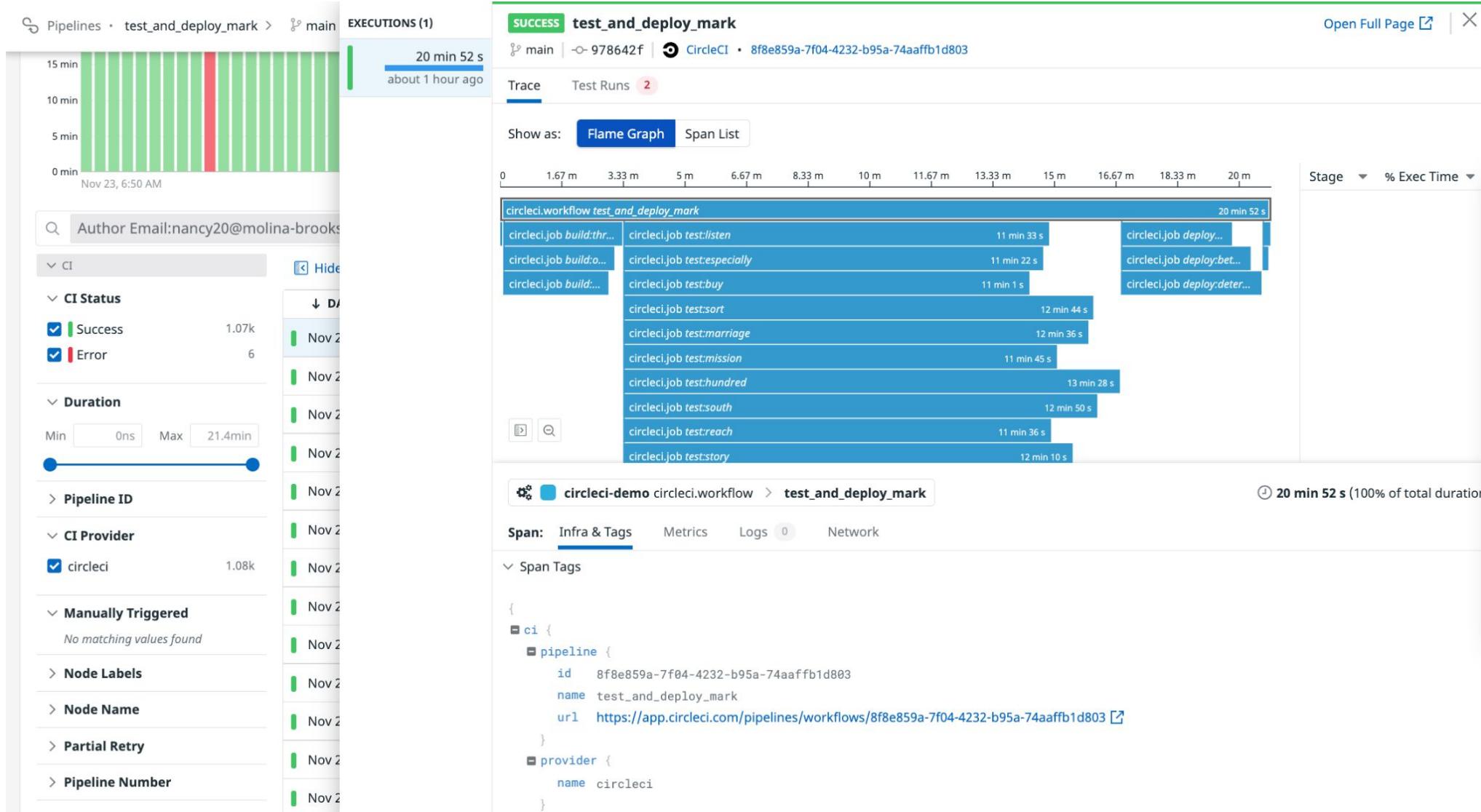
SHOP-57

3:10 pm  
 Jacky Jung  
DB Slow 쿼리 확인



# #CI Visibility

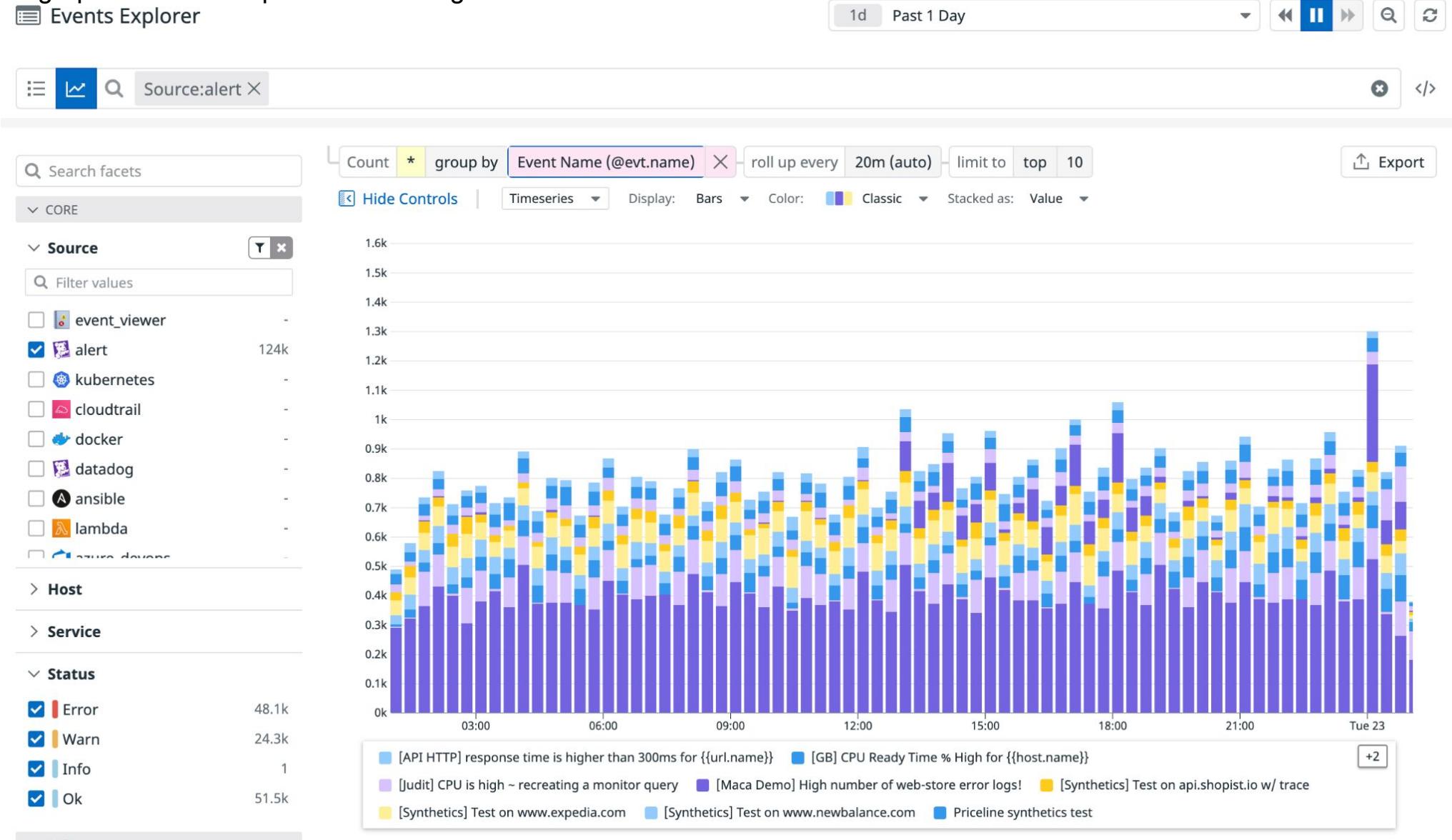
CI Pipeline에 대해 가시성을 확보하여 문제가되는 job이나 Test 등을 분석할 수 있도록 기능 제공



# #Event Analytic

참조 문서:

<https://docs.datadoghq.com/events/explorer/#time-range>



# #Audit Log

참조 문서: [https://docs.datadoghq.com/account\\_management/audit\\_logs/](https://docs.datadoghq.com/account_management/audit_logs/)

ACCOUNTS

Users

Service Accounts

GROUPS

Roles

SAML Group Mappings

ACCESS

API Keys

Application Keys

Client Tokens

Events API Emails

SECURITY

Public Sharing

Login Methods

Audit Logs **BETA**

Audit Log Settings **BETA**

OAuth Apps

COMPLIANCE

Sensitive Data Scanner

GENERAL

Rename Organization

## Audit Log Settings BETA

Audit Logs enabled

[Disable](#)

## Event Types

**Access Management**

Managing access, such as roles and users

**Authentication**

Successful and failed login events

**Dashboard**

Additions, deletions, and changes to dashboard resources

**Log Management**

Additions, deletions, and changes to log management

**Monitor**

Additions, deletions, and changes to monitor resources

**Notebook**

Additions, deletions, and changes to notebook resources

**OAuth**

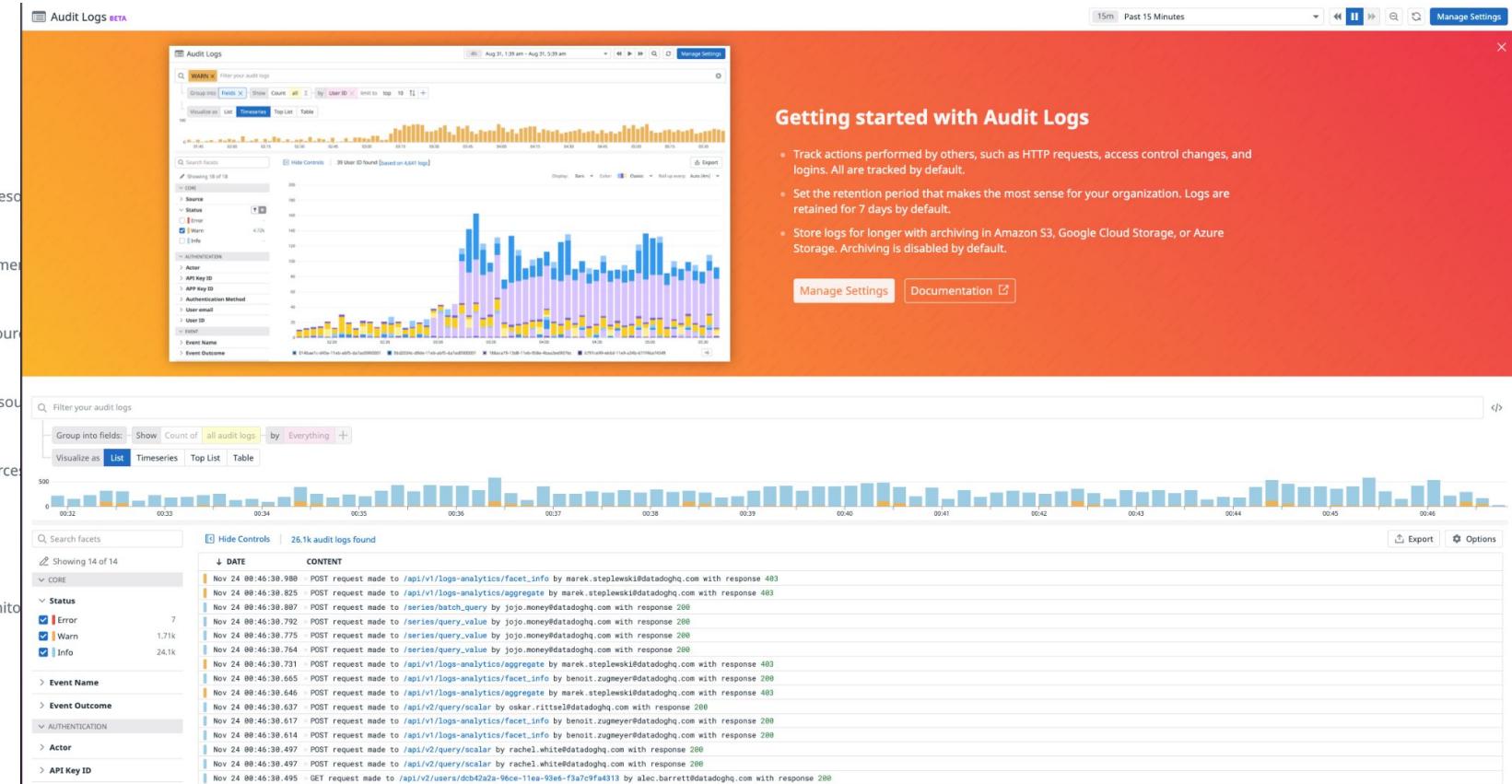
Additions, deletions, and changes to oauth resources

**Request**

All web requests

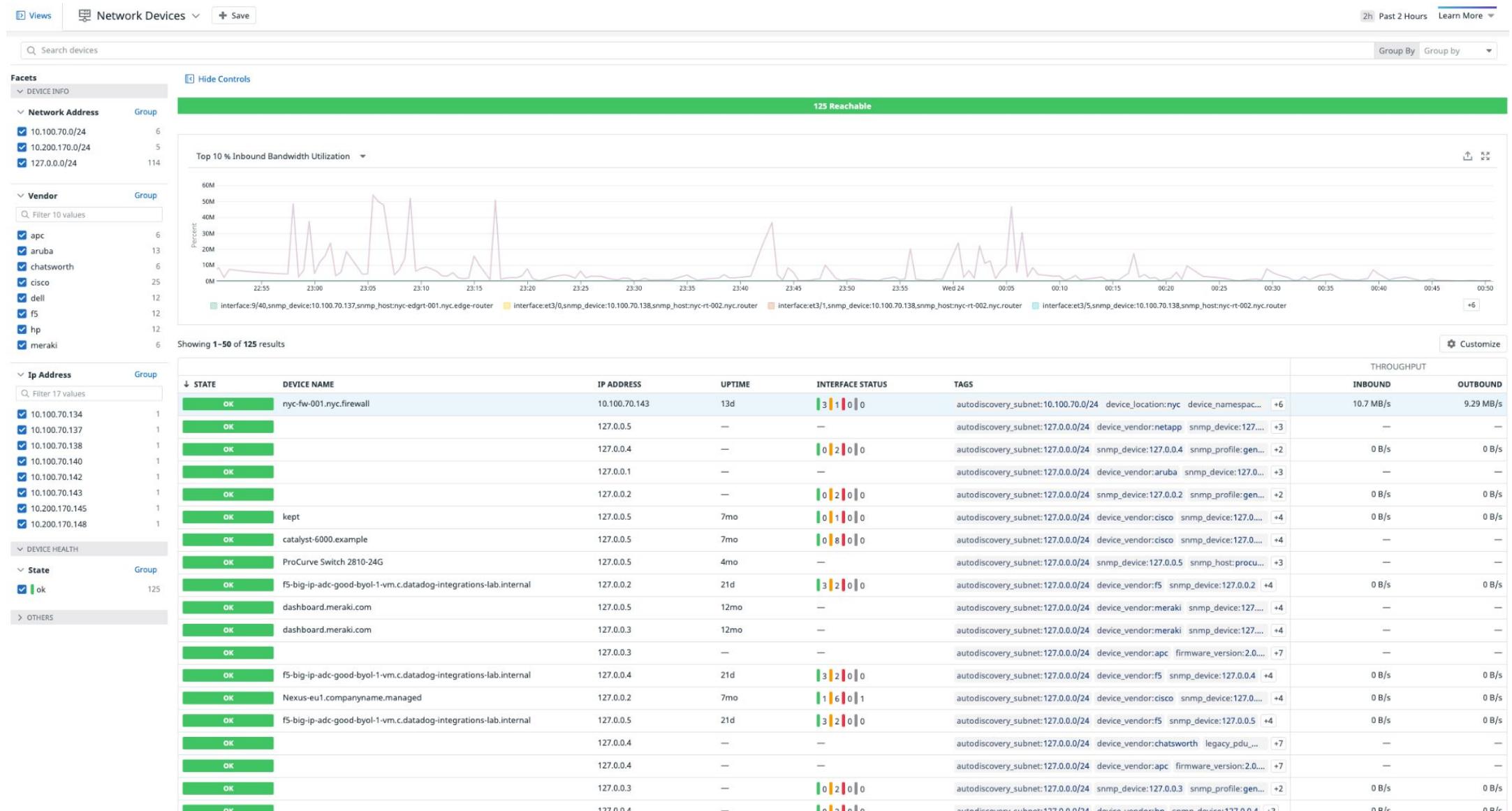
**Security Monitoring**

Additions, deletions, and changes to security monitoring



# #Network Device Monitoring

참조 문서: [https://docs.datadoghq.com/network\\_monitoring/devices/#overview](https://docs.datadoghq.com/network_monitoring/devices/#overview)



# #Serverless Update Part-1

참조 문서: [https://docs.datadoghq.com/network\\_monitoring/devices/#overview](https://docs.datadoghq.com/network_monitoring/devices/#overview)

The screenshot shows the Datadog Serverless dashboard with the following details:

**APP SERVICE PLAN: aas-demo-orchard-plan**

- PLAN TIER:** premiumv2
- REGION:** eastus2
- INSTANCE COUNT (AVG):** 1

**DATA INTEGRATION:** APM Tracing Detected

**ALL TAGS:** autodeploy:false, client\_id:f1504495-28da-4e99-85f6-a5e37a23c863, demo:true, extension:true, kind:app, operating\_system:windows, per\_site\_scaling:false, plan\_size:p1v2, plan\_tier:premiumv2, region:eastus2, resource\_group:azure-app-service-demo, resource\_id:/subscr...

**Apps Metrics**

APP	↓ APP REQUESTS	ERRORS	RESPONSE TIME (AVG)	CPU TIME (AVG)	DATA
aas-demo-orchard-netcore31	266	0	24.8 ms	116 ms	10.0 GB

**Showing 1-2 of 2 Functions**

FUNCTION	FUNCTION EXECUTIONS	FUNCTION BYTES SENT	HTTP 5XX	FUNCTION MEMORY WORKING SET	DATA
aas-demo-self-requesting	1.29k	356 KB	0	10.0 GB	2.29 GB
orchardcore-load	3.23k	359 KB	0	10.0 GB	2.29 GB

**Left sidebar (Views):**

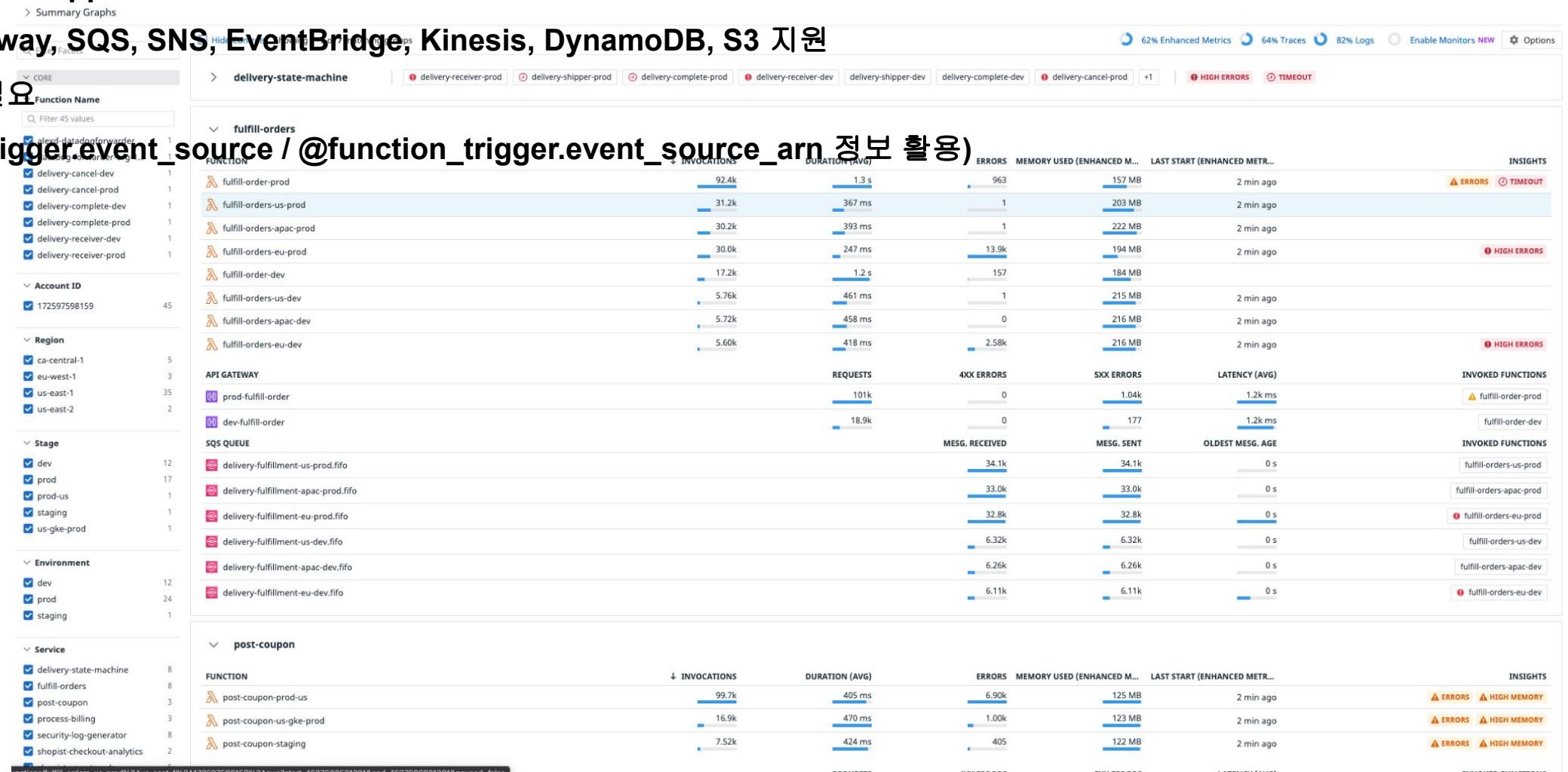
- All Resources (selected)
- App Service Plans
- Web Apps
- Azure Functions
- Filter facets
- CORE
  - App Service Plans
  - Web Apps
  - Functions
- Subscription Name
  - datadog-agent-build... (369)
  - datadog-agent-build... (369)
- Subscription ID
  - 8c56d827-5f07-45ce-8f... (369)
  - langerappserviceplan
- Tenant Name
  - 4d3bac44-0230-4732-9... (369)
  - claudia-test
  - apm-azure-app-services-plan
- Region
  - centralus (106)
  - eastus2 (106)
  - eastus (78)
  - westus2 (22)
  - francecentral (14)
  - southcentralus (10)
  - japaneast (6)
  - koreacentral (6)
- Resource Group
  - eclairstandarddbgroup (29)
  - apm-azure-app-services (26)
  - apm-dotnet (22)
  - helene-tuto (12)
  - apm-aas-junkyard (10)
  - apm-functions-testing (10)
  - apm-support-demo (8)
  - maxim-azure-demo (7)
- Environment
  - fact (6)

# #Serverless Update Part-2

참조 문서: [https://docs.datadoghq.com/serverless/troubleshooting/connect\\_invoking\\_resources/](https://docs.datadoghq.com/serverless/troubleshooting/connect_invoking_resources/)

## Enhanced Serverless View

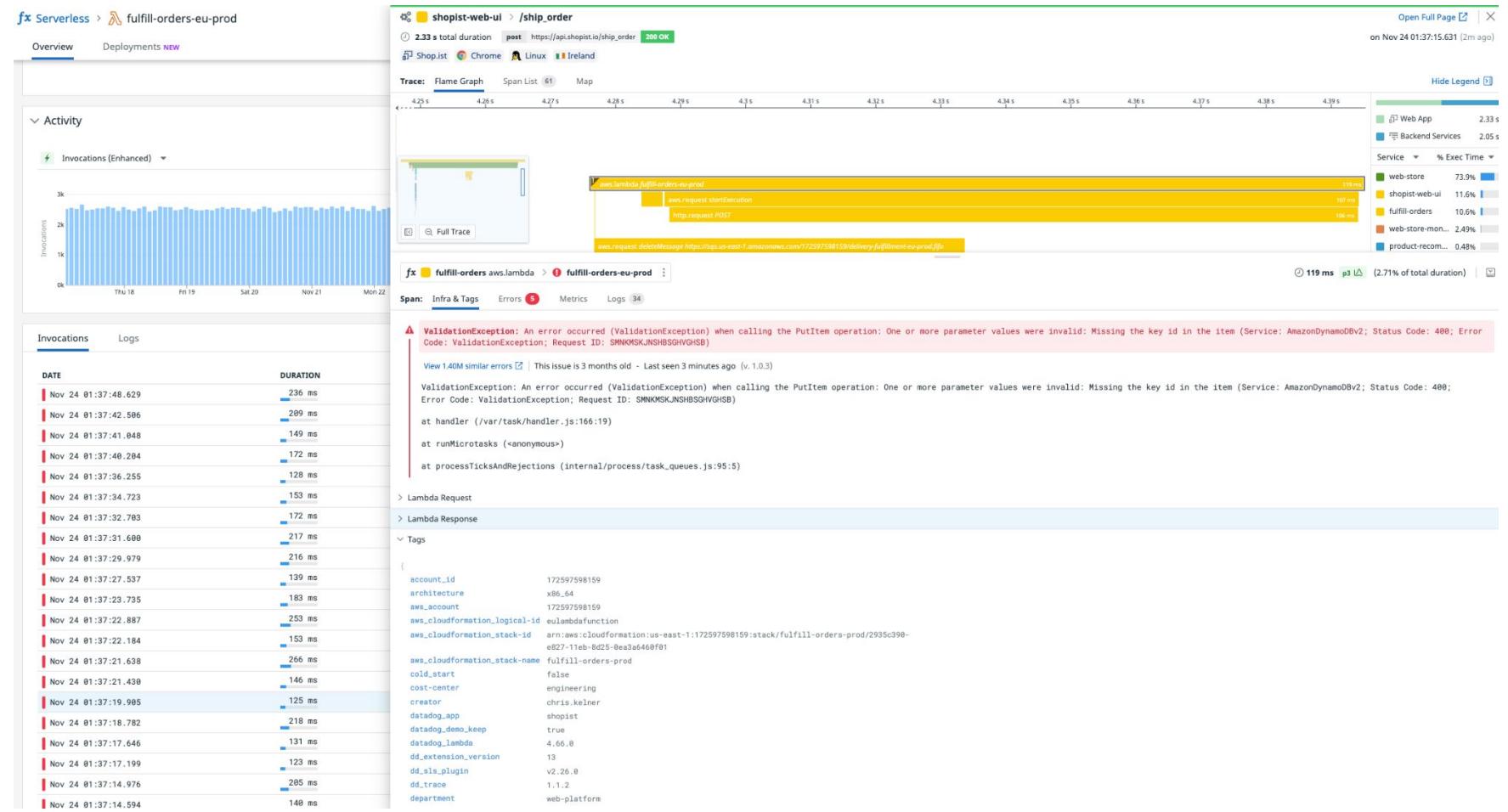
- Node.js/Python Supported
- 현재 API Gateway, SQS, SNS, EventBridge, Kinesis, DynamoDB, S3 지원
- APM 활성화 필요



# #Serverless Update Part-3

참조 문서: [https://docs.datadoghq.com/serverless/distributed\\_tracing/collect\\_lambda\\_payloads/](https://docs.datadoghq.com/serverless/distributed_tracing/collect_lambda_payloads/)

## Lambda payloads 데이터 수집 (Node.js/Python)



# #Azure Automutting



## Azure Integration

Microsoft Azure is an open and flexible cloud platform.

**✓ INSTALLED**

Overview Configuration Metrics

This integration is working properly.

Installing the Azure Integration could increase the number of billable servers that Datadog monitors. For more information on how this may affect your billing, visit the [Billing FAQ](#) page.

Create an App Registration for Datadog in your Azure Active Directory, grant it the "Monitoring Reader" role in the subscription(s) you want to monitor, and add the credentials here. (See [detailed instructions](#).)

### App Registrations

Client ID: **f1504495-28da-4e99-85f6-a5e37a23c863**

Client ID:

Tenant ID:

Client Secret:

Limit metrics collection to hosts with tag: [?](#) (Optional)

Limit metrics collection to App Service Plans with tag: [?](#) (Optional)

Silence monitors for expected Azure VM shutdowns

Azure Automutting [?](#)

Monitored Subscriptions

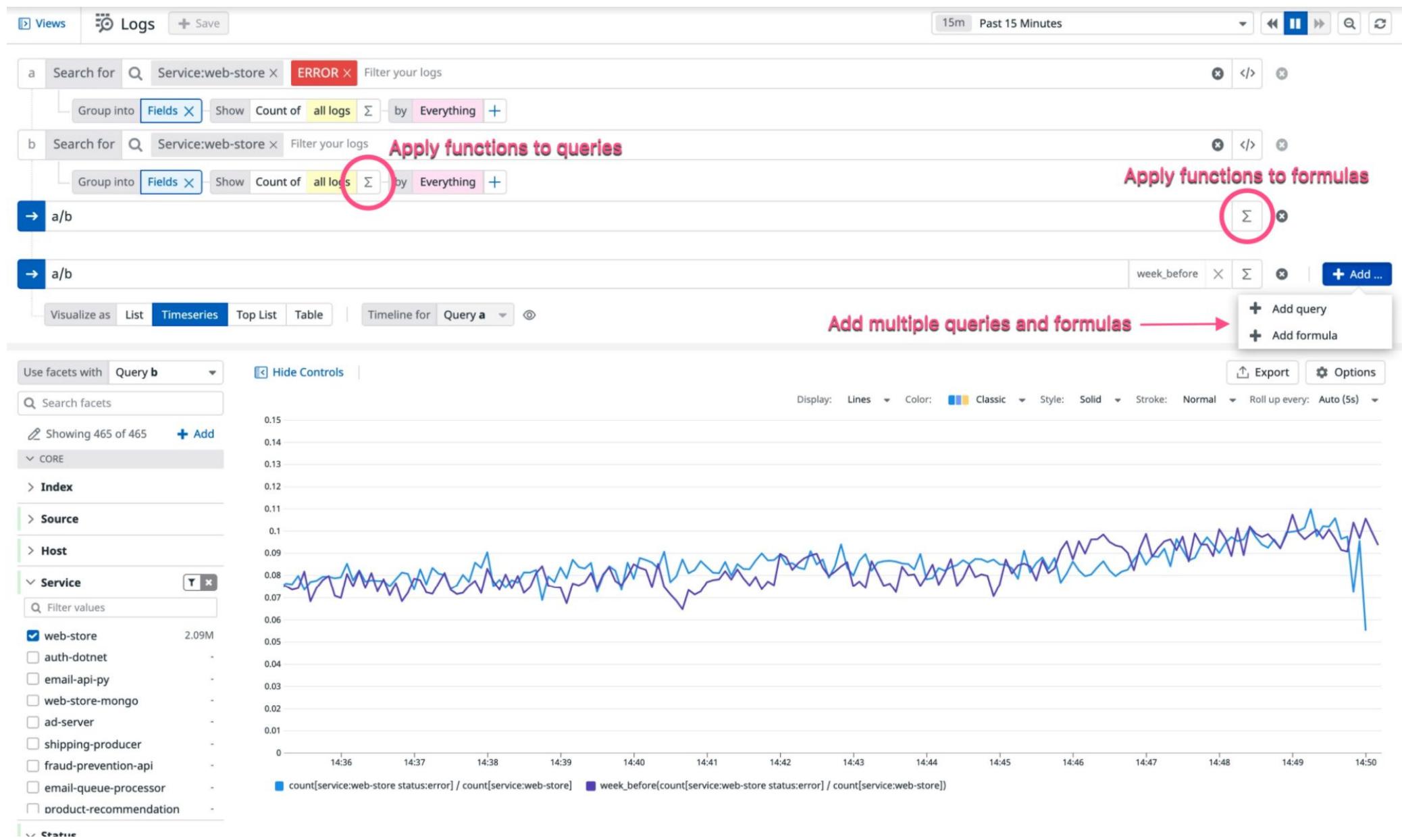
**datadog-agent-build**  
ID: 8c56d827-5f0

Datadog can proactively mute monitors related to the manual shutdown of Azure virtual machines, as well as instance termination triggered by Azure autoscaling, based on host statuses from the Azure Resource Health API. Automated Azure virtual machines are listed on the [Monitor Downtime](#) page.

If metrics collection is limited to hosts with tags, only virtual machines matching the tags are automatically muted.

[Remove](#)

# #Log Multiple Query and Formulas



# #Security



## Security Monitoring

Detect and investigate security threats in real time

STARTING AT  
\$ **0.20**

Per GB of analyzed logs, per month\*

## Cloud Workload Security

Real-time threat detection across hosts and containers

STARTING AT  
\$ **15**

Per host, per month\*

## Cloud Security Posture Management

Continuous configuration audits across cloud accounts, hosts, and containers

STARTING AT  
\$ **7.50**

Per host, per month\*

# Security Monitoring

## Security Monitoring

1w Past 1 Week

**15.8 TB**  
Logs Analyzed  
across 17 sources

**4.56K**  
Signals Generated  
triggered by 24 rules

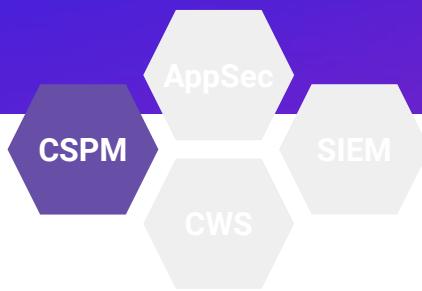
**600**  
Threats Detected  
across 1.61K entities

### Sources Analyzed ?

Name	Status	Logs Analyzed	Rules Triggered	Signals Generated
kubernetes	INSTALLED	4.6GB	0 / 11	No signals
cisco	INSTALLED	1.8GB	2 / 2	2K
gcp	INSTALLED	1.8GB	0 / 16	No signals
nginx	INSTALLED	1.1GB	0 / 1	No signals
cloudtrail	INSTALLED	322MB	11 / 24	679

# #Security

## CSPM



Posture Management    Home    Findings

### Average security posture score

**75%**

533 of 712 resources passed

[Explore all resources](#)

### Posture score per account

473437055159	(267 resources)
363525035937	(218 resources)
363525035921	(28 resources)

70%  
68%  
39%

[Manage accounts](#)

### Top high-severity issues

37.00	S3 bucket employs default encryption at-rest
30.00	CloudTrail multi-region is enabled
30.00	ELB listener is securely configured
30.00	Network ACLs do not allow ingress from 0.0.0.0/0 to rem...
29.00	S3 bucket is not publicly accessible to anonymous users

[Analyze issues](#)

CIS - AWS

### Rules evaluation



[Configure rules](#)

### Requirements with the most issues

Logging	3	1
Networking	0	1
Storage	1	1
IAM	1	0

[Analyze requirements](#)

### Resource types with the most failed resources

aws_s3_bucket	37	37
aws_network_acl	0	30
aws_vpc	29	5
aws_cloudtrail_trail	60	0
aws_ebs_volume	30	0

[Analyze resource types](#)

CIS - Kubernetes

### Rules evaluation



### Requirements with the most issues

API-Server	10	1
General-Policies	1	0
Worker-Node-Configuration-Files	2	0

### Resource types with the most failed resources

kubernetesNode	157	8
kubernetesCluster	25	0

# #Security



# Cloud Workload Security

The screenshot shows the Workload Security interface. At the top, there are tabs for Home, Signals, and Rules, with Home being the active tab. A search bar at the top right includes icons for back, forward, and search. Below the tabs, there are dropdown filters for Env, Cluster, Image, Host, and Service. The main dashboard displays three key metrics: 93 Hosts Monitored (with 684 containers), 11.23K Events Analyzed, and 14 Signals Generated. Below these metrics, under the heading 'Essential security signals', there are three sections: 'Latest Critical Signal' (Log data in /var/log/ was deleted, Attack > Defense Evasion > Indicator Removal on Host, 2 min ago), 'Most frequent issue' (Log data in /var/log/ was deleted, Attack > Defense Evasion > Indicator Removal on Host, 300 entities), and 'Fastest growing issue' (Log data in /var/log/ was deleted, Attack > Defense Evasion > Indicator Removal on Host, +33% growth).

Workload Security

Home Signals Rules

1h Past hour

Env \* Cluster \* Image \* Host \* Service \*

Current policy: 1.2 Download latest policy: 1.21

93 Hosts Monitored  
684 containers

11.23K Events Analyzed

14 Signals Generated

Essential security signals

Latest Critical Signal

**Log data in /var/log/ was deleted**  
Attack > Defense Evasion > Indicator Removal on Host

2 min ago

See all critical signals ↗

Most frequent issue

**Log data in /var/log/ was deleted**  
Attack > Defense Evasion > Indicator Removal on Host

300 entities

See all frequent issues ↗

Fastest growing issue

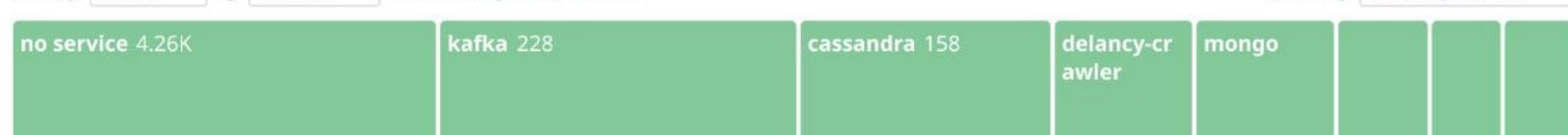
**Log data in /var/log/ was deleted**  
Attack > Defense Evasion > Indicator Removal on Host

+33%

See all growing issues ↗

## Cloud Workload Security Coverage

Group Hosts ▾ by Service ▾ and size by **host** count.



#### MITRE ATT&CK® coverage

TACTIC	MAPPED RULES	TRIGGERED RULES	SIGNALS GENERATED
Reconnaissance	3	2	10 
Resource development	0	0	0 

## Whats Next?

날짜: 2021년 12월 10일 금요일

시간: 오후 2시~오후 3시 45분(한국시간)

Universal Service Monitoring

RUM Impact Analysis

Online Archives

Log Pattern Anomalies

Observability Pipelines

And More!!!



등록 : <https://bit.ly/3CDMg4u>

# Q&A