



# Datadog Korea User Group

## Datadog 한국 사용자 모임

Datadog과 함께 성장한 여정, 꿀팁과 노하우

인프랩

DevOps 정인호



# 안녕하세요, 정인호입니다.

정인호 (조슈아)

DevOps 엔지니어

인프랩



2019년 입사, 백엔드 + 인프라 업무 담당  
2021년 데브옵스



지난 3년 동안 경험한 Datadog의 좋았던  
점,  
그리고 조심해야하는 점을 이야기하고자  
합니다.



# 순서

- 인프런(Inflearn)과 랠릿(Rallit)
- Datadog 첫 시작
- 잘 사용하고 있는 Datadog 제품 활용 사례
- Datadog 자체를 잘 써보기
- 마무리



# 인프런 (Inflearn)과 랠릿 (Rallit)



# 인프런과 랠릿

인프런: 라이프타임 커리어 플랫폼

랠릿: IT 인재 채용 플랫폼

The screenshot shows the Inflearn homepage with various course categories and search filters. Courses are listed with their names, descriptions, and ratings.

- Course 1: 관계기능 엔지니어링 (2/20 (10.0%) 2일 전 학습)
- Course 2: 쉽게 설명하는 AWS 기초 강의 (0/180 (0.0%) 8일 전 학습)
- Course 3: 개념부터 철저한 gRPC! (with Python) (5/23 (21.7%) 17일 전 학습)
- Course 4: [마스터기본] 평론 인디자인 정복하기 (0/112 (0.0%) 19일 전 학습)

Below the courses, there are several course cards:

- Course 1: 마인과 풍물심 속 나의 이음으로 살아남기 (LIVE)
- Course 2: Excel Practice (Original)
- Course 3: React.js For FE Beginner
- Course 4: 25 Object-Oriented Design Patterns by Yalo (Global vet.)
- Course 5: 한반에 끝나는 직장인을 위한 스타트업 창업 키즈 (Yalo)
- Course 6: 알락한 코딩시전 (campilestudy)
- Course 7: 30% W28,300 (W18,200)
- Course 8: 문화하기 (New)

The screenshot shows the AWS Classroom interface for the "OSI 7 Layer Model (1) – Physical/Data Link" course. The video player shows the first 15 minutes of the lecture. A sidebar lists other modules of the course.

- OSI 7 Layer Model 1 -Physical/Data Link- (15분)
- OSI 7 Layer Model 2 -Network- (23분)
- OSI 7 Layer Model 3 -Transport- (25분)
- OSI 7 Layer Model 4 -Session/Presentation/Application- (15분)
- Domain Name Service (27분)
- 캐싱(Caching) (25분)
- 암호화 & SSL/TLS (15분)

The screenshot shows the Rallit homepage displaying job listings from different companies. The search bar and filter options are visible at the top.

- SK(주) C&C Enterprise IT서비스 영업 전문가 영입
- 코웨이(주) [코웨이] ERP[ERP] 경력직 채용
- 브레이브모바일 [송고] [송고] Growth Marketer
- 브레이브모바일 [송고] [송고] Sr. Front-end Engineer
- Braze | Amplitude | SQL | Slack | Notion
- TypeScript | React | Redux | Slack
- 경력무관 | 강남 | 시니어(9년 이상) | 강남

The screenshot shows a specific job listing for Inflearn. The listing details include the company name, position, requirements, and application information.

**교육 콘텐츠 영업 매니저**

경력: 경력무관  
최소 연령: 회사 내규에 따름  
마감일: 채용 시 마감  
사전 질문: 미리보기 >  
회사명: 인프런(인프린)

지원하기

**인프런(인프린), 어떤 곳인가요?**

우리는 때로 무언가를 배워야만 합니다.  
꿈을 이루기 위해서, 무엇을 배우고 더 나아가기 위해서는 그 분야에 대한 학습이 필요합니다. 그러나 모든 사람들에게 그 기회가 동등하게 주어지지 않습니다. 금전적인 부담, 지역적인 제한, 다양한 이유로 사람들은 학습에 어려움을 겪고 있습니다. 우리는 이런 현실을 돌파하려 합니다.

인프런은 2017년에 시작된 “인프런”을 통해 누구나 배우고 지식을 나눌 수 있는 환경을 만들었습니다. 2021년 한국판자비트너스, 미래에셋캐피탈, 벤처밸스, 알로이스벤처스로부터 시리즈 A 투자를 받으며, 단단한 팀워크와 협상을 통해 꾸준한 성장을 이어오고 있습니다. 인프런은 1140만 명의 유저, 6,000여개의 저작자, 3,000여개의 기관/



# 인프런과 랠릿

데브옵스 관점

## 인프런: 온라인 동영상 학습

### 플랫폼

- Node.js, Kotlin 기반
- API 호출 대량 발생
- 동영상 인코딩 및 암호화, 그리고 자막과 더빙을 위한 배치성 파이프라인 작업
- 동영상 탈취 시도 방지

## 랠릿: 취업 채용 연결

### 플랫폼

- Node.js 기반
- 구직자 정보 암호화 및 접근제어 필수

• 봉사형 서비스 구조로 서비스간 호출  
반복



# 인프런과 랠릿

Datadog 관점

## 인프런: 온라인 동영상 학습

### 플랫폼

- Application Performance Monitoring (APM)
- Database Monitoring (DBM)
- Datastream Monitoring (DSM)
- CI Visibility
- Log
- ASM

## 랠릿: 취업 채용 연결

### 플랫폼

- APM
- Cloud SIEM

- 
- Service Catalog, Service Map
  - Monitoring



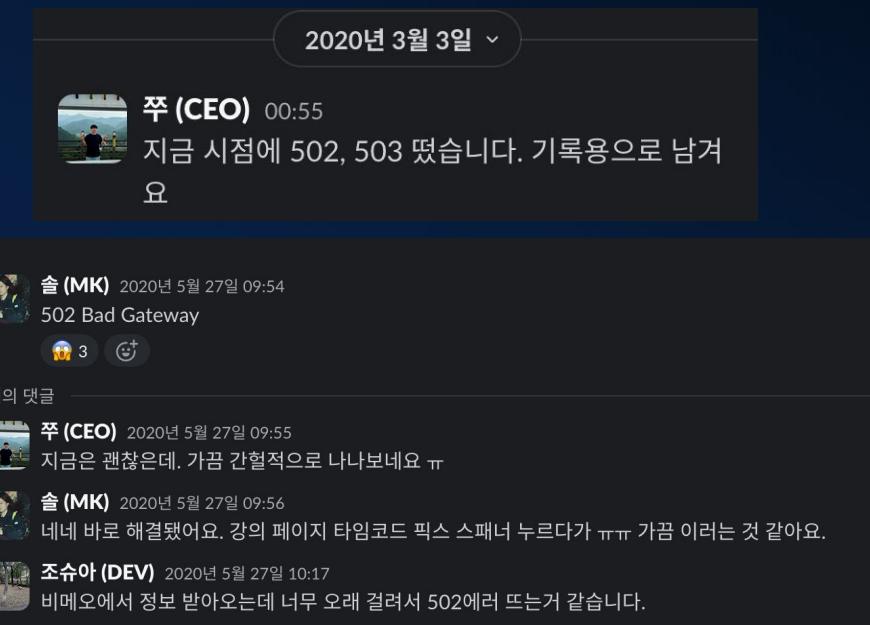
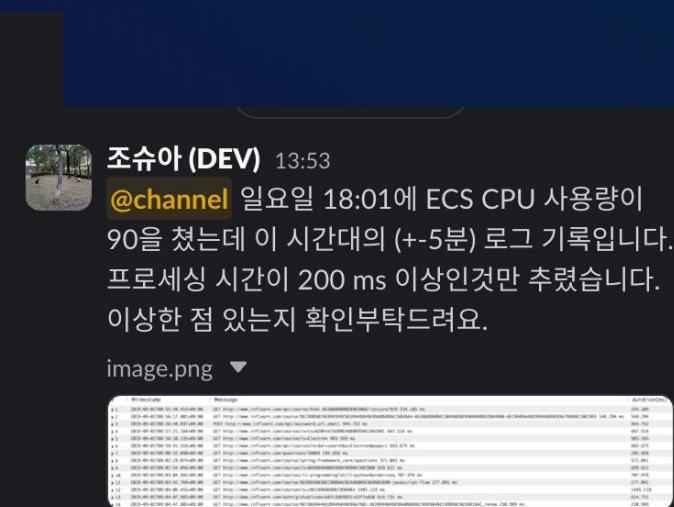
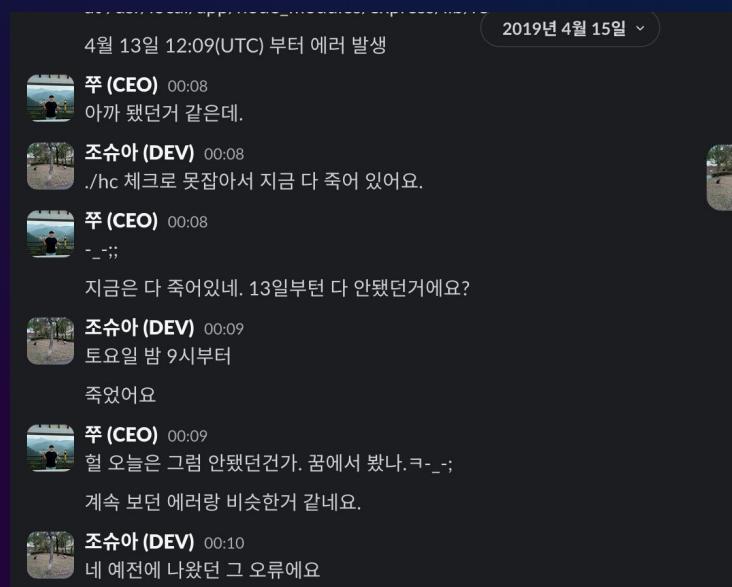
# Datadog 첫 시작



# APM 도입의 필요성

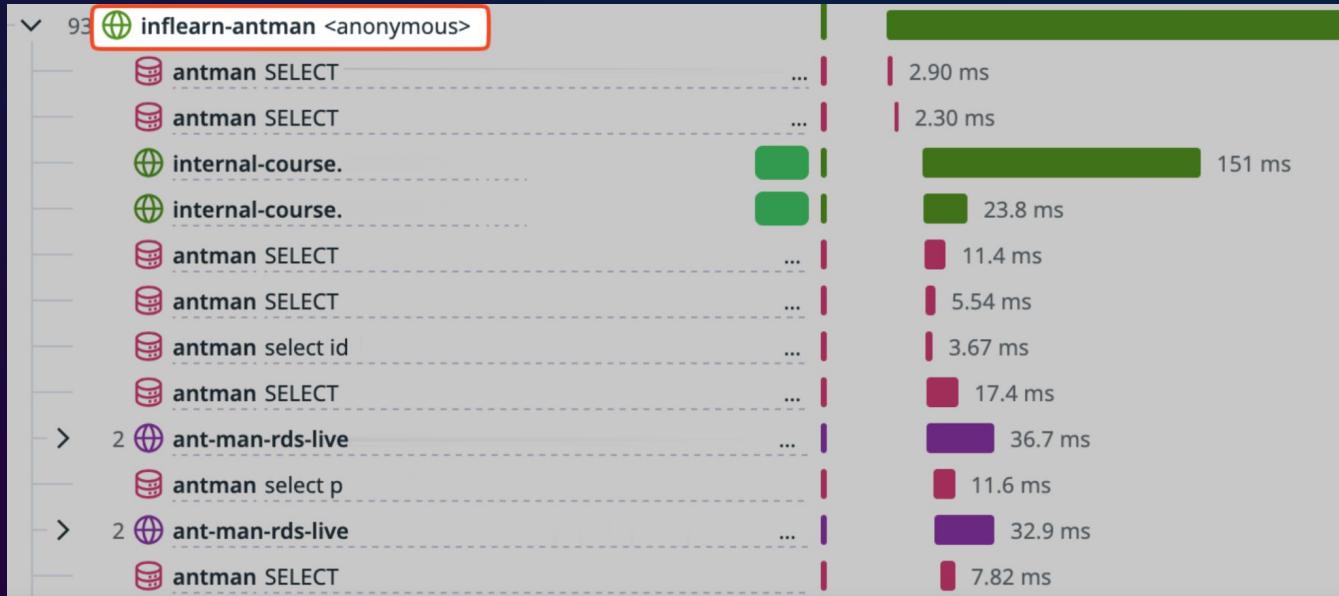
장애가 발생했는데 원인을 모르겠어요.

- 서비스 성장에 따라 같이 빈번해지는 장애와 오류
- 장애 원인을 분석하기 위한 분석 및 모니터링 도구의 부재
- AWS CloudWatch Log와 Alarm만으로는 다양한 장애의 원인을 제때 파악하고 대응하기 어려움



# Datadog을 선택한 이유

- 당시 Node.js 를 가장 잘 지원
  - 익명(anonymous) 함수에 대해  
자동 span 유일하게 지원



# Datadog 첫 날

2021년 7월 22일 ▾

 **조슈아 (DEV)** 15:26  
APM 트레이스 배포하고 정상 동작 중입니다.  
메트릭이랑 로그 통합하기 전에  
개발 파트 가이드용으로 트레이스 사용 문서 작성하고  
안내할까요? (+ 개발파트원 데이터독 회원 가입)

 **향로 (CTO)** 15:37  
네 가이드 문서가 있어야 할 것 같아요.  
다들 APM이 처음이셔서

 **조슈아 (DEV)** 15:38  
옙

1 

넵! 2  2021년 7월 22일 ▾

 **조슈아 (DEV)** 15:54  
[@p-dev](#) Datadog 서비스에 초대드릴 예정입니다. 이  
메일로 초대장이 발송될 거에요.  
회원 가입 후 이름을 슬랙 형식으로 입력해주세요~

넵! 1 

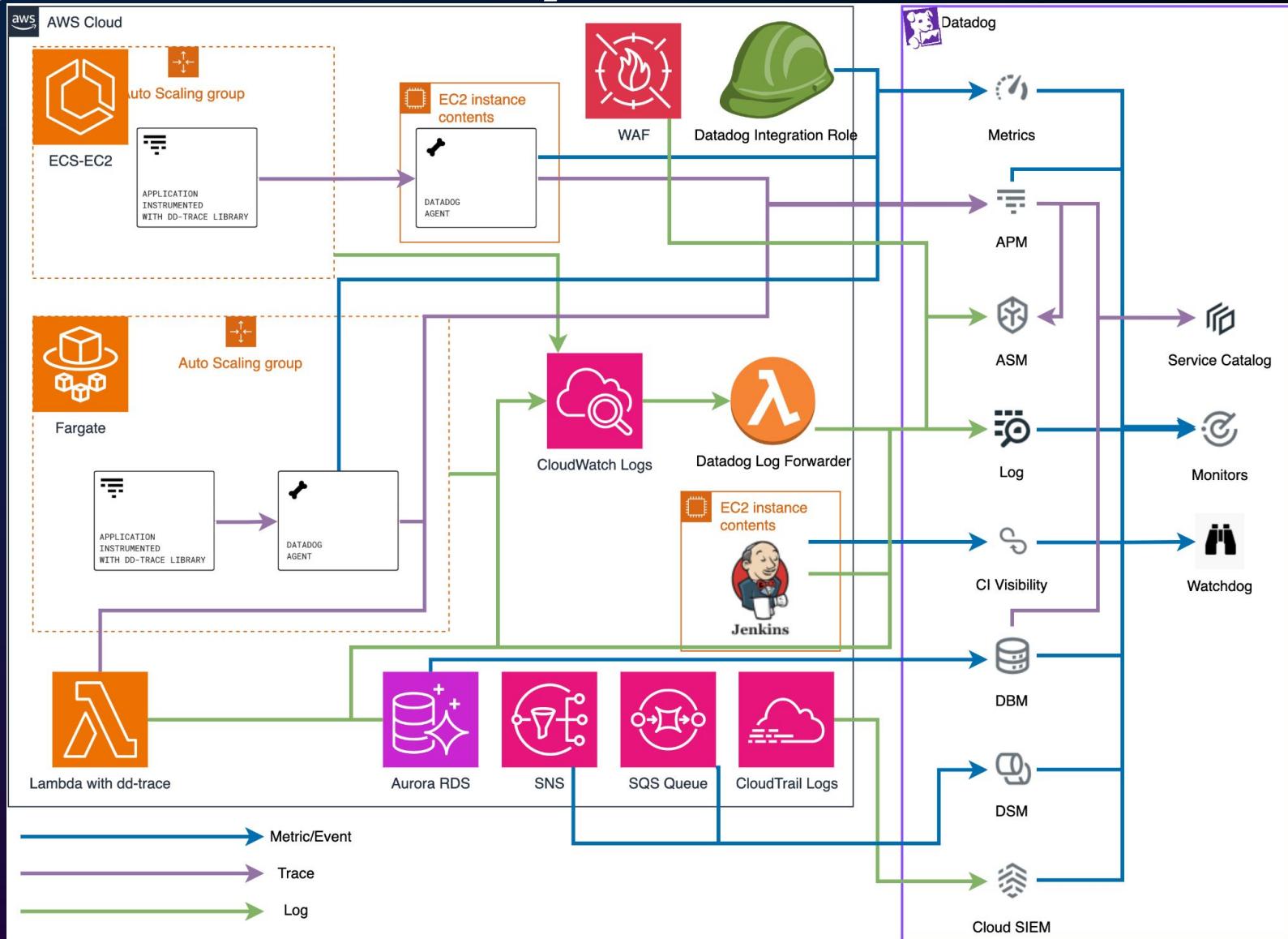
 **3개의 댓글** 4년 전 마지막 댓글



# 잘 사용하고 있는 Datadog 제품 활용 사례



# Datadog Observability Architecture



# APM과 Log

다들 너무 잘 쓰고 계실 것이라 생각합니다.  
따라서...

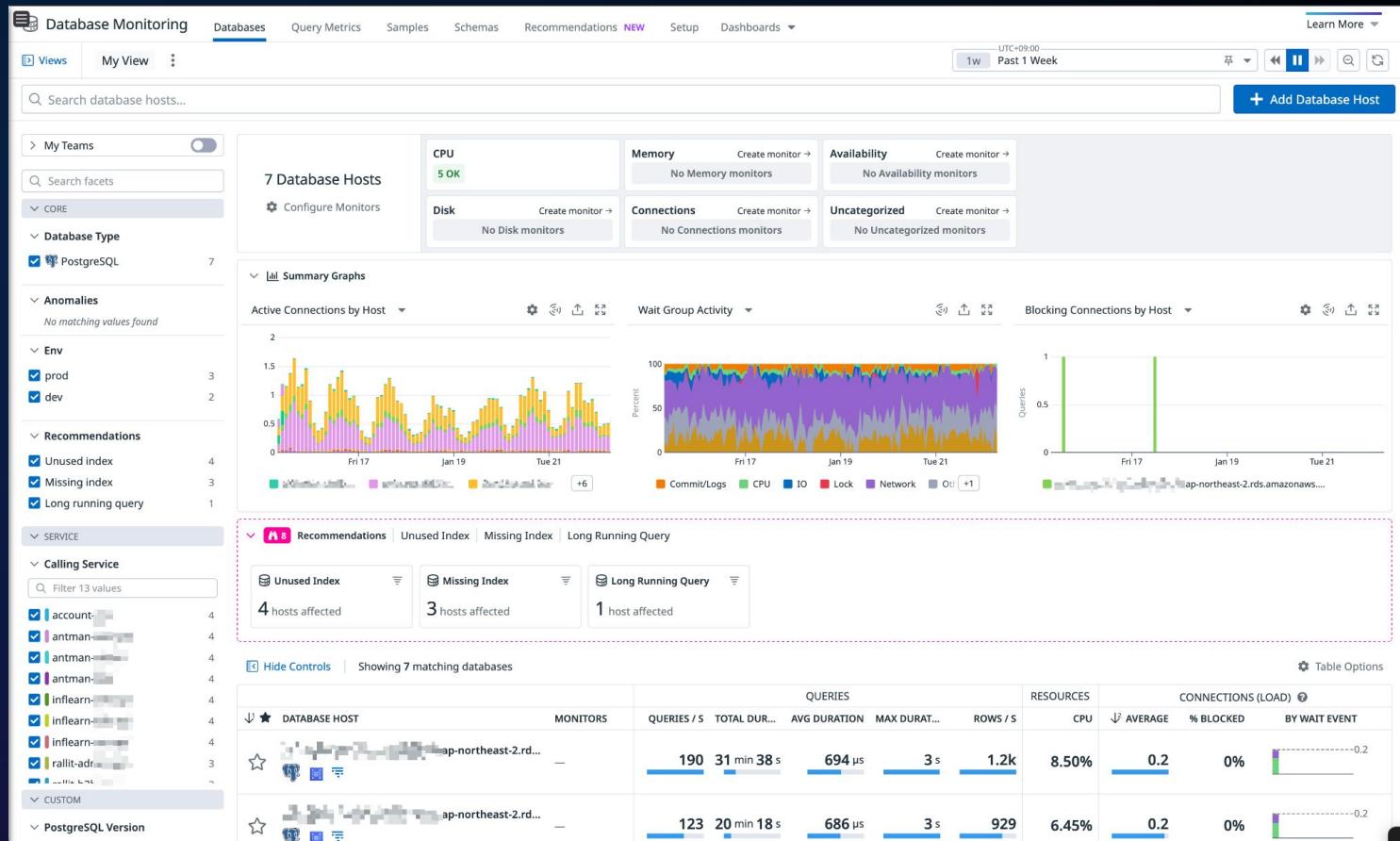
# SKIP

APM과 Log는 발표 후반부의 **Datadog** 잘 써보기에서 등장합니다.



# Database Monitoring (DBM)

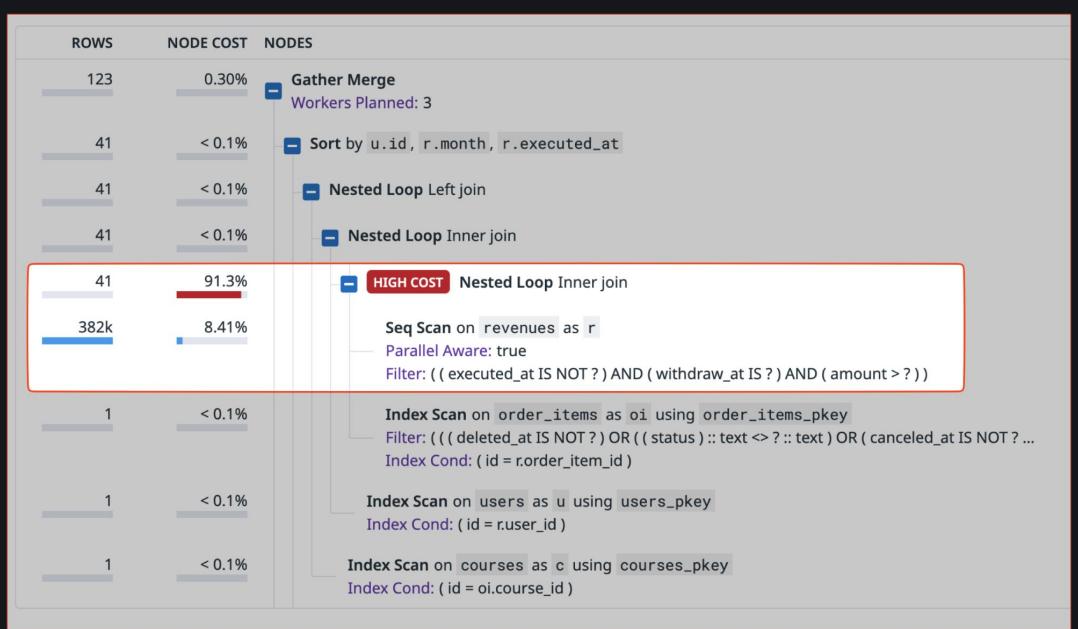
- 디비의 성능을  
끌어올리는 것에 집중된  
서비스
- 스키마 뷰어, 쿼리 메트릭,  
쿼리 샘플링, index 생성  
추천 등 다양한 기능 제공
- APM과 연동



# Database Monitoring (DBM)

## 활용 사례 1 - Query Explain Plan

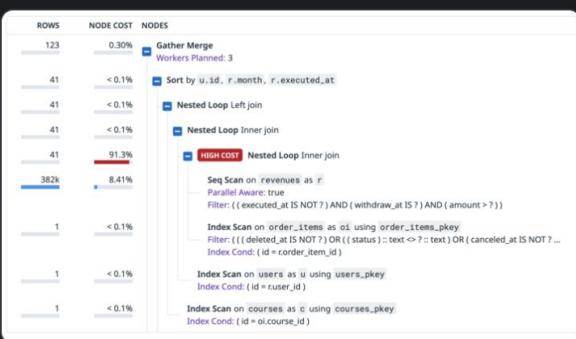
- 실제 실행된 쿼리 대상으로 explain plan을 제공하여 쿼리가 느린 이유를 식별

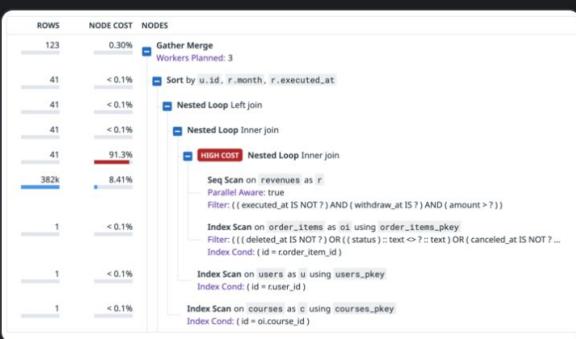


 **후리 (DEV)** 2024년 4월 9일 13:19  
정산 이후 취소된 건 (회수대상) 조회 쿼리입니다.  
평소엔 이렇게 오래걸리지 않았는데,,,;

 **조슈아 (DEV)** 2024년 4월 9일 13:34  
IO 웨이팅이 걸린 것으로 보입니다. writer 디비에 쿼리를 실행하셨는데 아마 다른 쓰기 작업 때문에 자연 걸린거 같아요. select 쿼리는 가급적 reader 디비에서 실행하시면 좋을거 같습니다.

2024-04-09-13-26-54.png ▾



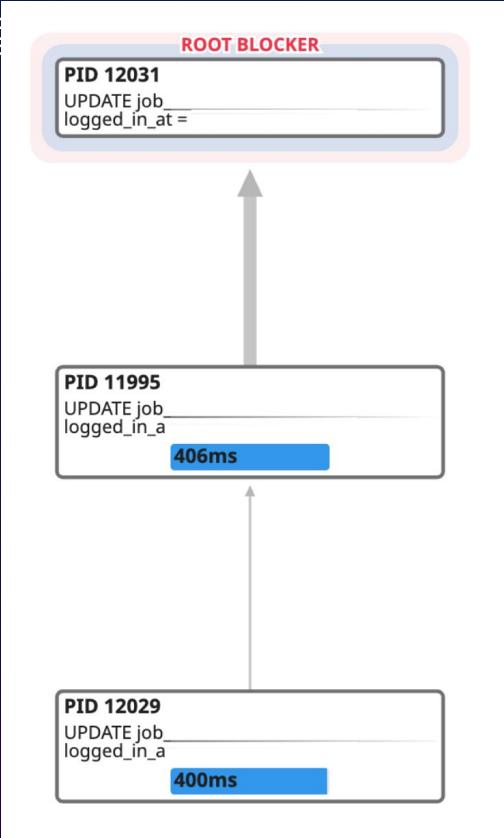




# Database Monitoring (DBM)

## 활용 사례 2 - Lock race condition 식별

- DBM의 Blocking Activity 기능으로 락 경쟁 상태를 식별



향로 (CTO) 2024년 9월 9일 14:48  
@c-rallit-be 나중에 시간되실때 왜 commit이 한번씩 1초이상걸리는지 한번 찾아봐주시면 좋을것같아요.  
1초가 긴 시간은 아닌데 빈도수가 꽤 높은것 같아서요.  
DB 스펙도 이젠 T 시리즈가 아닌데도...

우드 (DEV) 2024년 9월 9일 14:53  
추측하기로는 jobSeeker를 업데이트하는 세션 API가 많이 호출되기도 하고,  
jobSeeker 업데이트 자체가 워낙 많은 곳에서 이루어지다보니까 [요거](#)랑 비슷하게 락이 잡혀서 그런 것 같습니다.  
간헐적으로 발생하는 슬로우쿼리들도 이와 관련된 것이 아닐까 싶어요 (편집됨)

@하루 (DEV) 이번에 발생한 슬로우쿼리는 동일한 쿼리가 0.004초 간격으로 3번 발생했다는 특  
징이 있는데요. 1월 1일에도 비슷한 상황에서 3개의 쿼리가 기록되어 있어 확인을 해보니 락  
경쟁 상황이 발생했던것 같습니다. ([링크](#))

- PID12031이 Network - ClientRead로 인한 슬로우우가 발생함
- PID11995 가 PID12031이 끝날 때까지 기다림 (Wait event: transactionid)
- PID12029 가 PID11995가 끝날 때까지 기다림 (Wait event: tuple)

연속적 락이 걸리는 상황

Network로 인한 지연은 간헐적으로 발생하는 wait event 인데, 지연이 발생하는 시점에 락이  
걸려있는 쿼리들이 여러 개 있는 상황은 부자연스러워보입니다. 왜 동일한 리소스(튜플)를 거  
의 동시에 접근하게 됐는지 원인 파악이 필요해보입니다. (편집됨)

3개 파일 ▾

RESOURCE

- backend-postgres UPDATE job\_seeker SET ...

HOST

- prod-rallit-rds-4.cyhy...  
prod-rallit-rds-4.cyhy...  
prod-rallit-rds-4.cyhy...

ROOT BLOCKER

- PID 12031 UPDATE job\_seeker SET ...
- PID 11995 UPDATE job\_seeker SET ...
- PID 12029 UPDATE job\_seeker SET ...



# Database Monitoring (DBM)

## 활용 사례 3 - Index 생성 추천

- Index를 타지 않는 쿼리가 지속적으로 발생하는 경우 해당 쿼리를 분석하여 Index 생성을 추천

The screenshot shows the Datadog Query Insights interface with the title "Query Insights | Index Recommendation". It displays three separate recommendations, each with a yellow "INDEX RECOMMENDATION" button and a "CREATE INDEX" SQL command. The first recommendation is for a table with columns [redacted] and the command is:

```
CREATE INDEX comments_user_[redacted]
```

The second recommendation is for a table with columns [redacted] and the command is:

```
CREATE INDEX comments_user_[redacted]
```

The third recommendation is for a table with columns [redacted] and the command is:

```
CREATE INDEX comments_user_[redacted]
```



# Database Monitoring (DBM)

## 주의할 점

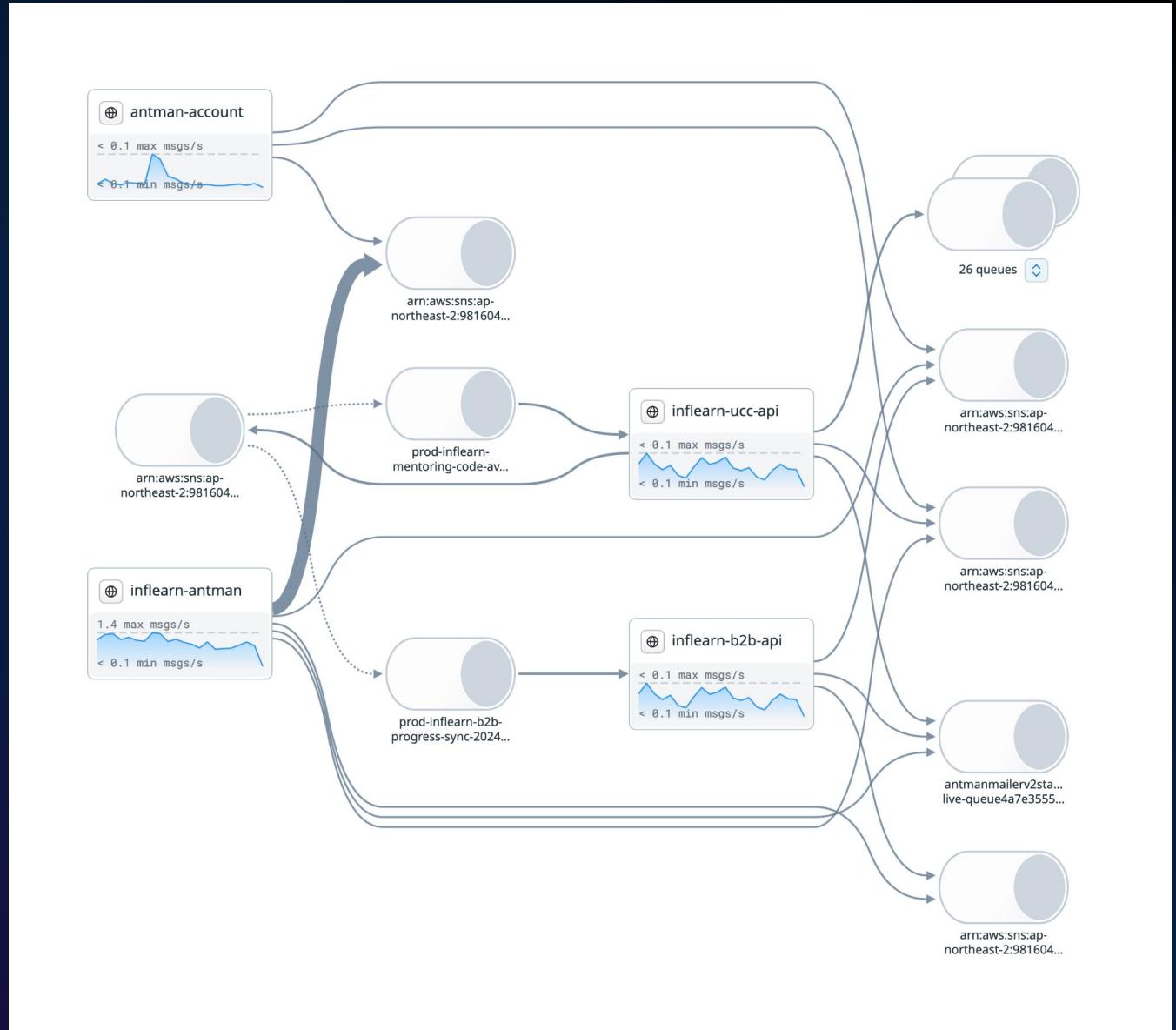
- 실행 중 오류가 발생한 쿼리는 수집되지 않음
  - 오류가 발생한 쿼리는 APM 단에서 확인 필요
- 100% 모든 쿼리가 수집되지는 않음
  - 다만 대표성이 있는 쿼리는 99% 수집된다고 함
- DBM 수집 에이전트는 디비 성능에 영향을 줌
  - CPU: ~1% of the CPU used on average
  - Memory: ~300 MiB of RAM used (RSS memory)
  - Network bandwidth: ~30 KB/s ▼ | 30 KB/s ▲

[https://docs.datadoghq.com/database\\_monitoring/agent/integration\\_overhead/?tab=postgres](https://docs.datadoghq.com/database_monitoring/agent/integration_overhead/?tab=postgres)



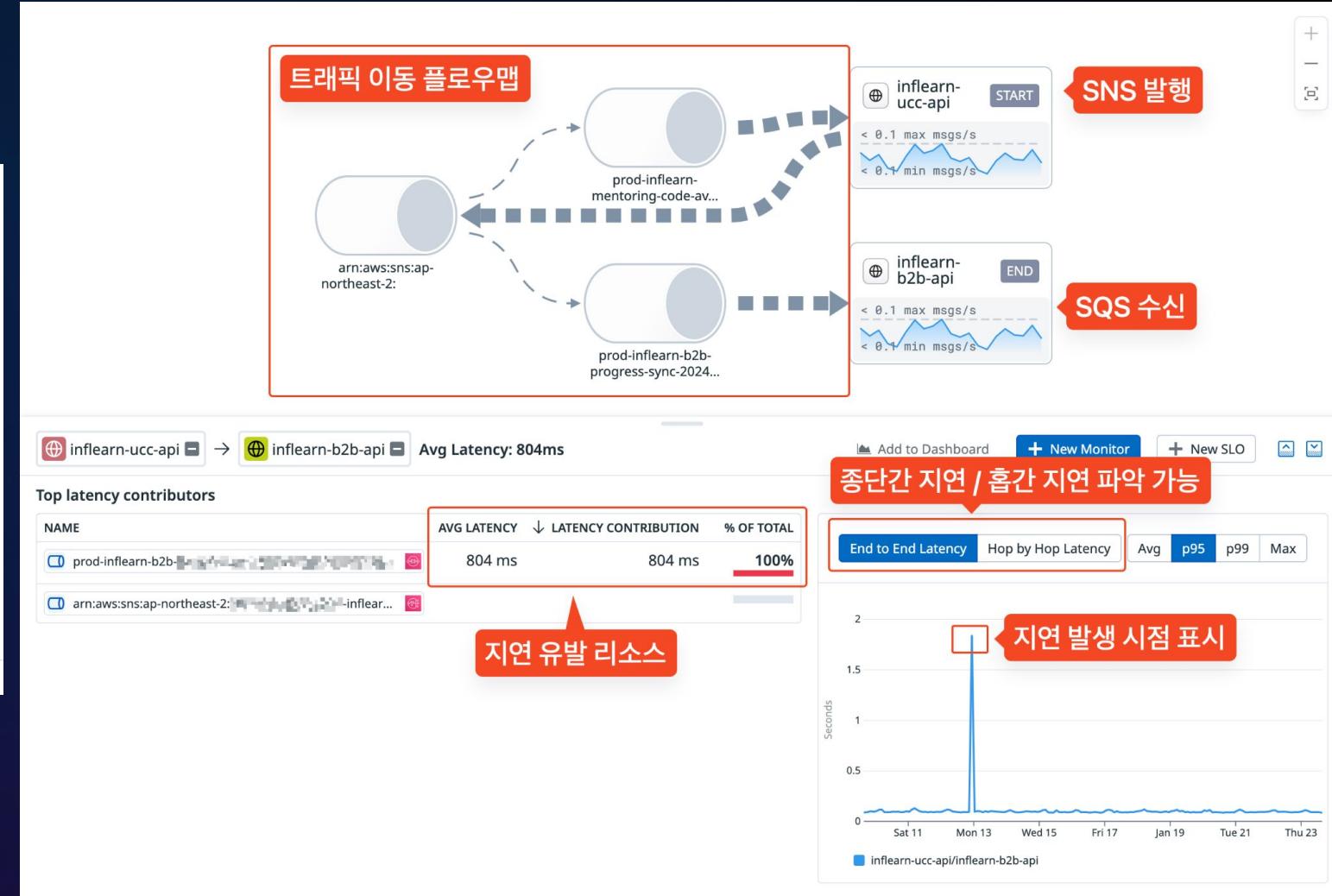
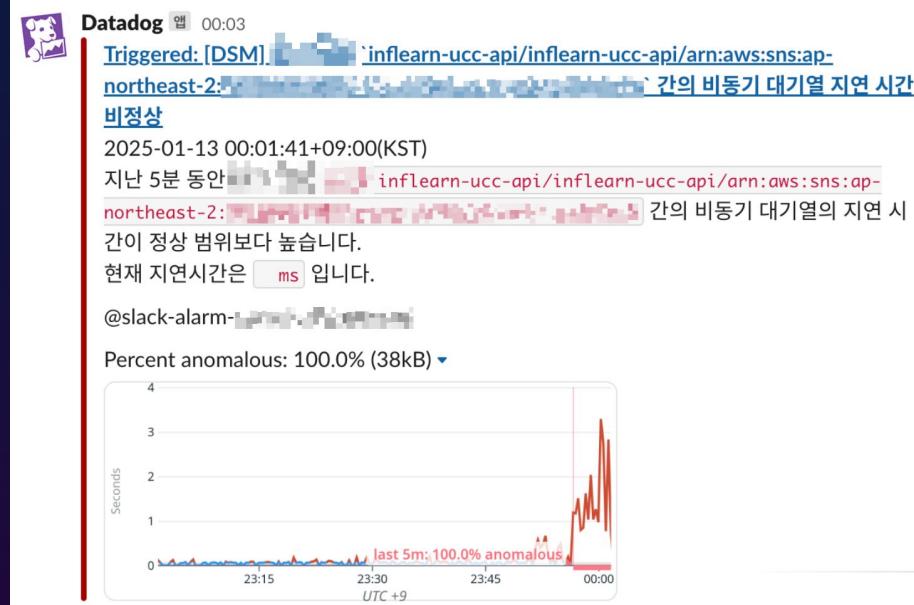
# Data Streams Monitoring (DSM)

- AWS SQS, SNS, Kafka 등 비동기 대기열을 모니터링
- APM으로 확인할 수 없는 비동기 영역에 대한 추적 제공



# Data Streams Monitoring (DSM)

활용 사례 - End to end 지연 식별



# Service Catalog

- 기본적으로 아무 설정 없어도 사용 가능
- Datadog에 연동한 모든 서비스가 표시됨

The screenshot shows the Datadog Service Catalog interface. At the top, there are tabs for 'Explore' (selected), 'Setup & Config', 'Scorecards PREVIEW', and 'Resource Catalog'. Below the tabs is a search bar and a 'Group by' dropdown. The main area has tabs for 'Ownership', 'Reliability', 'Performance', 'Security', 'Costs', and 'Delivery NEW'. On the left, a sidebar shows 'My Teams' (disabled) and a 'Select a Component' section with categories like Systems, Services (88), Datastores, Queues, RUM Apps, External Providers, and Inferred Services. Below this are sections for 'Search facets', 'OVERVIEW', 'Language' (with .NET, Go, Java, Javascript, PHP, Python, Ruby, C++, and All languages checked), and 'Telemetry Type' (with Filter 10 values). The main table lists 88 services, each with a star icon, type (e.g., env:prod), name, scorecard percentage (e.g., 60%, 30%, 40%, 90%), team (e.g., part-devops, part-dev, part-dev, cell-ucc, cell-rallit, cell-rallit, cell-course, cell-b2b, cell-b2b, cell-b2b, cell-auth, cell-auth), on-call status, contact information, repository link, and telemetry icons. A 'Discover services with USM' button and an 'Export as CSV' button are at the top right.

NAME	TYPE	SCORECARDS	TEAM	ON-CALL	CONTACT	REPO	TELEMETRY
inflab-devops-api	env:prod	60%	part-devops				
internal-devops-api.inflearn.com	js env:prod	30%	part-devops				
inflearn-antman-redis	js env:prod	30%	part-dev				
inflearn-antman-postgres	js env:prod	30%	part-dev				
inflearn-antman	js env:prod	40%	part-dev				
inflearn-ucc-api	js env:prod	90%	cell-ucc				
rallit-studio	js env:prod	30%	cell-rallit				
rallit-b2c-api-postgres	js env:prod	30%	cell-rallit				
rallit-b2c-api	js env:prod	40%	cell-rallit				
internal-course.inflearn.com	js env:prod	30%	cell-course				
inflearn-b2b-api	js env:prod	70%	cell-b2b				
antman-b2b-postgres	js env:prod	30%	cell-b2b				
antman-b2b	js env:prod	40%	cell-b2b				
antman-account-redis	js env:prod	30%	cell-auth				
antman-account	js env:prod	40%	cell-auth				



# Service Catalog

## 소유권(Ownership)

소유권탭에서 서비스의 책임자 정보를 확인 가능

1. 담당팀
2. 코드 저장소
3. 서비스 관련 문서
4. 서비스 대시보드

The screenshot shows the Datadog Service Catalog interface for the service **inflab-devops-api**. The **Ownership** tab is selected. The page includes tabs for Reliability, Performance, Security, Costs, and Delivery (with a NEW badge). The **Service Metadata** section displays the schema version (v2.2) and metadata source (UI). Buttons for Edit and Create a Jira ticket are available.

The ownership information is organized into four main sections, each highlighted with a red box and numbered 1 through 4:

- TEAM**: Contains the value `part-devops`.
- APPLICATION**: Contains the value `inflab`.
- LIFECYCLE**: Contains the value `active`.
- TIER**: Contains the value `support`.

Below these sections are other service details:

- ON-CALL**: A note about connecting to supported integrations for on-call status, with links to Set Up On-Call, Set Up PagerDuty, and Set Up Opsgenie.
- CODE REPOSITORIES**: Shows a repository named `devops-api`.
- DOCUMENTATION**: Shows a link to the `devops-api API 문서`.
- RUNBOOKS**: A note indicating "Not Provided".
- DASHBOARD LINKS**: A link to the `prod-devops-api` dashboard.
- CONTACTS**: Includes a Slack channel link (`#topic-devops`) and an email address (`part.devops@inflab...`).



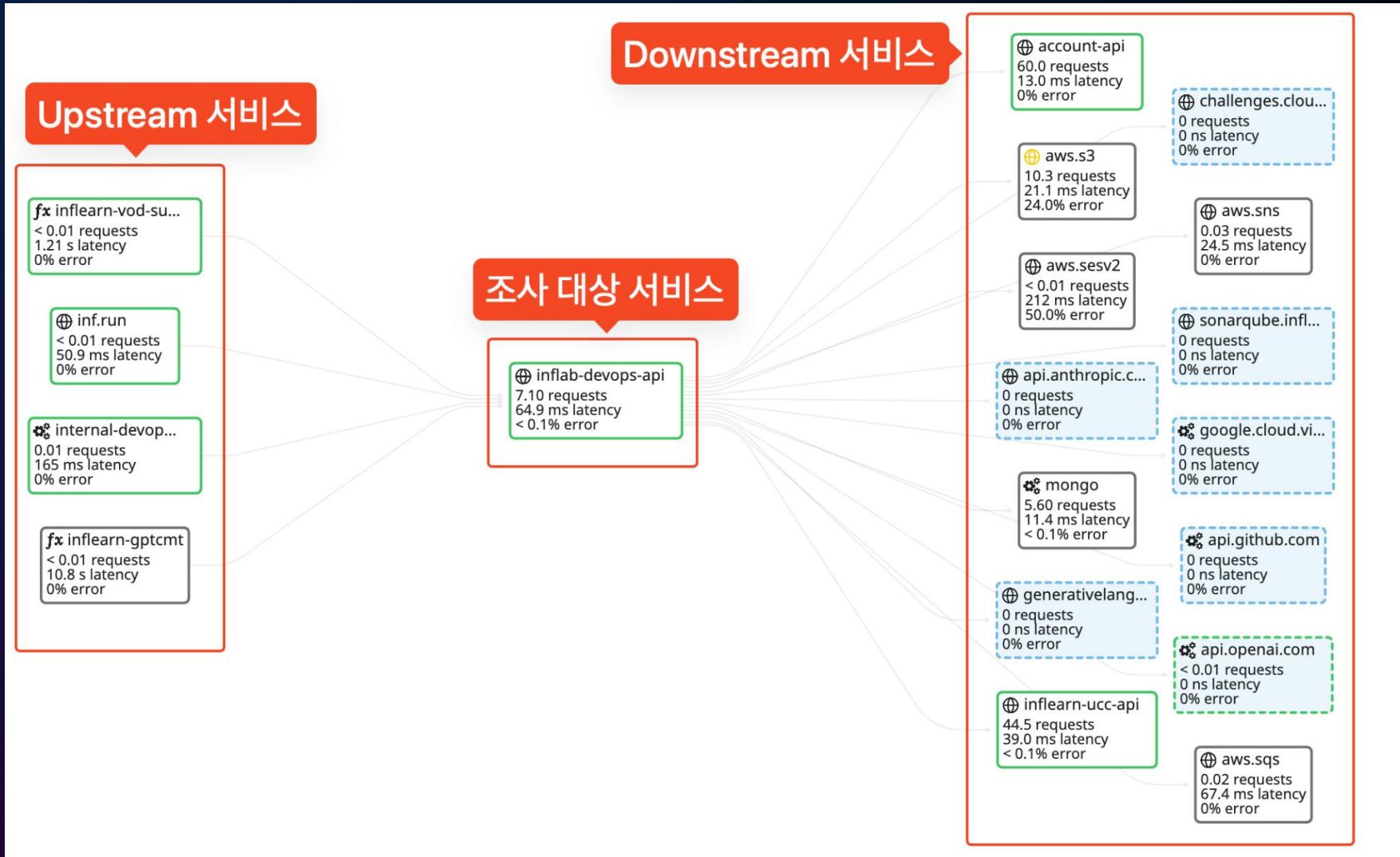
# Service Catalog

## 서비스 맵(Service Map) - Cluster



# Service Catalog

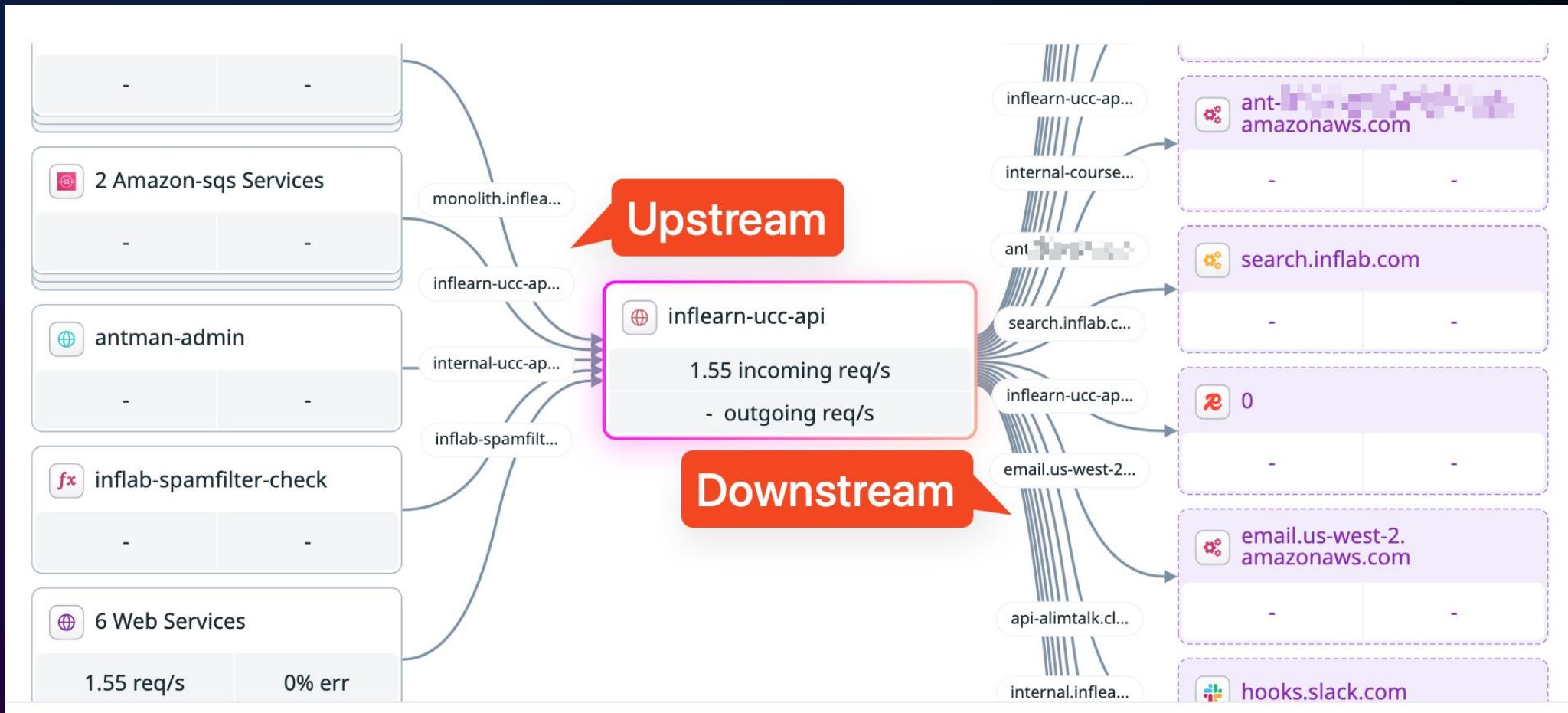
## 서비스 맵(Service Map) - Flow



# Service Catalog

활용 사례 - 서비스 종속성 맵으로 운영 서비스에 대한 큰 그림 그리기

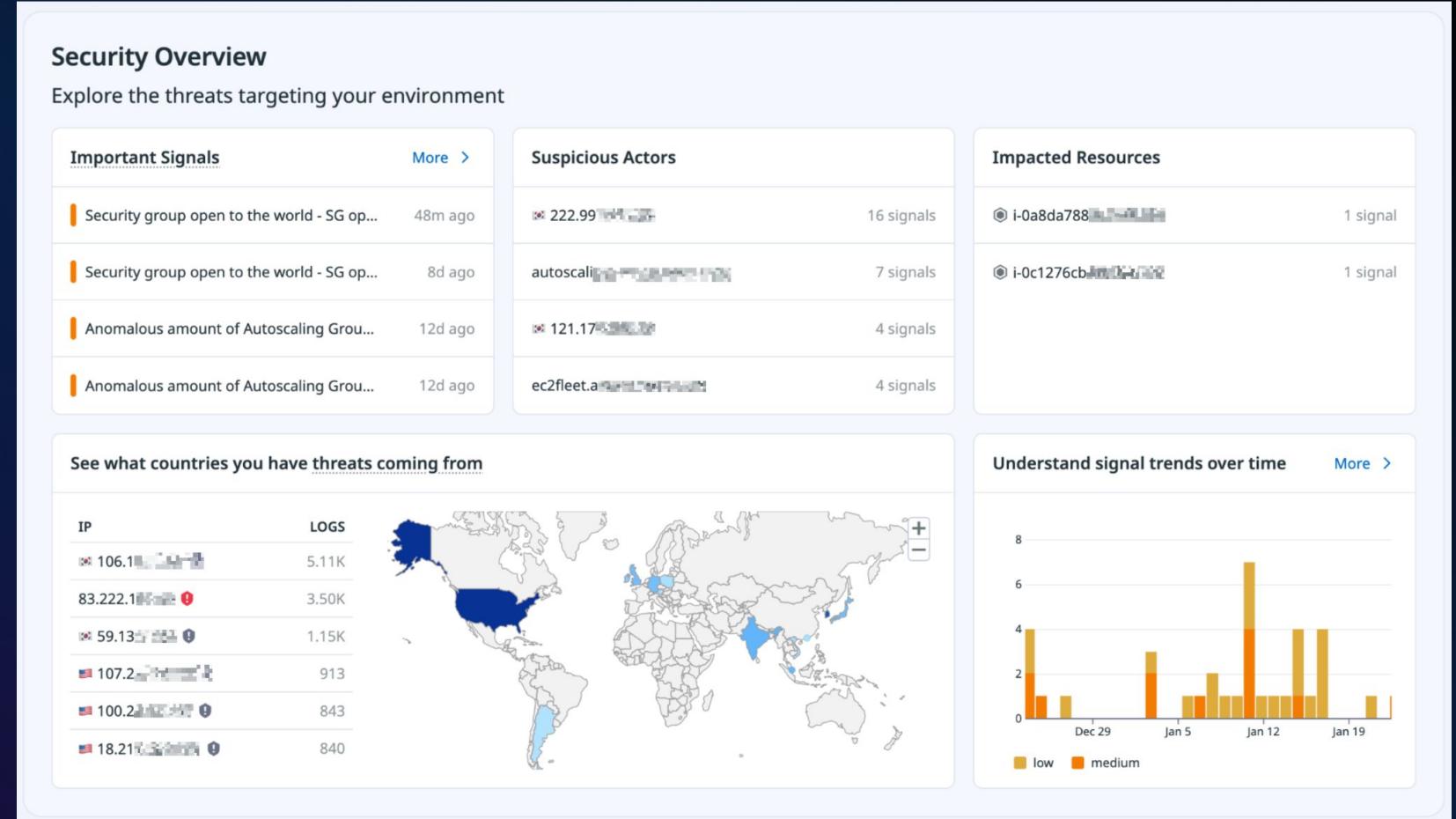
- 서비스의 상하 의존구조를 한 눈에 파악
- 장애 추적시 서비스 종속성 맵을 활용해 신속하게 원인 pin-down



# Cloud SIEM

감사로그 중앙집중식 관리 및 위협 탐지

- 감사로그(Audit log)를 실시간으로 분석하여 보안 취약점 및 악의적 공격을 탐지하는 도구



# Cloud SIEM

감사로그 중앙집중식 관리 및 위협 탐지

- 감사로그를 지원하는 다양한 소스를 지원
- 소스별 특화된 위협 탐지 경보 자동 설정

**Security Coverage**  
Explore the rules monitoring your environment

Sources MITRE ATT&CK®

Cloudtrail **INSTALLED** 117 Rules

GCP **INSTALLED** 46 Rules

Gsuite **INSTALLED** 14 Rules

Azure 50 Rules

Github 32 Rules

Github-Telemetry 32 Rules

Microsoft-365 28 Rules

Okta 18 Rules

Slack 16 Rules

Kubernetes 13 Rules

Snowflake 13 Rules

Auth0 11 Rules

Jumpcloud 10 Rules

Windows 10 Rules

524 detection rules found in 61 groups

Filter by Source All

**Cloudtrail**

**AWS IAM AmazonSESFullAccess policy was applied to a group**  
MEDIUM | cloudtrail | DEFAULT | Creation date: Dec 9, 2024, 7:43 pm  
attack TA0004-Privilege-Escalation T1098-Account-Manipulation iaas:aws mitre\_platform:cloud mitre\_platform:iaas

**AWS IAM AmazonSESFullAccess policy was applied to a role**  
MEDIUM | cloudtrail | DEFAULT | Creation date: Dec 9, 2024, 7:43 pm  
attack TA0004-Privilege-Escalation T1098-Account-Manipulation iaas:aws mitre\_platform:cloud mitre\_platform:iaas

**AWS IAM AmazonSESFullAccess policy was applied to a user**  
MEDIUM | cloudtrail | DEFAULT | Creation date: Dec 9, 2024, 7:40 pm  
attack TA0004-Privilege-Escalation T1098-Account-Manipulation iaas:aws mitre\_platform:cloud mitre\_platform:iaas

**Cloud provider activity observed from IP associated with cryptomining** PREVIEW  
MEDIUM | cloudtrail | DEFAULT | Creation date: Nov 27, 2024, 9:41 am  
attack TA0011-Command-And-Control T1071- mitre\_platform:cloud mitre\_platform:iaas tactic:TA0011-command-and-control +1

**Invitation sent to account to join AWS organization**  
HIGH | cloudtrail | DEFAULT | Creation date: Nov 19, 2024, 6:53 pm  
attack TA0005-Defense-Evasion T1535-Unused-Or-Unsupported-Cloud-Regions iaas:aws

**Amazon Bedrock console activity**  
HIGH | cloudtrail | DEFAULT | Creation date: Oct 14, 2024, 6:17 pm  
attack TA0001-Initial-Access T1078-Valid-Accounts mitre\_platform:cloud mitre\_platform:iaas

View All

The screenshot shows a dashboard titled 'Security Coverage' with a sub-section for 'Cloudtrail'. On the left, there's a list of various data sources with their respective rule counts. The 'Cloudtrail' section is expanded, showing five specific alert entries. Each alert includes a severity level (e.g., MEDIUM, HIGH), a timestamp, and a detailed description of the event. A red box highlights the first alert about an AWS IAM policy being applied to a group. The interface also includes filters for 'Source' and 'All' categories.



# Cloud SIEM

## SaaS 감사로그 연동

- AWS CloudTrail
- GCP
- GWS

Active 3 Content Packs

 **CONTENT PACK**  
**AWS CloudTrail**

Monitor security and compliance levels of your AWS operations.

This Content Pack includes:

- 113 Detection Rules
- 1 Dashboard
- AWS Investigator
- Workflow Automation
- Configuration Guide

**✓ ACTIVE**

 **CONTENT PACK**  
**GCP Audit Logs**

Protect your GCP environment by monitoring audit logs.

This Content Pack includes:

- 47 Detection Rules
- 1 Dashboard
- GCP Investigator
- Configuration Guide

**✓ ACTIVE**

 **CONTENT PACK**  
**Google Workspace**

Optimize your security monitoring within Google Workspace.

This Content Pack includes:

- 15 Detection Rules
- 1 Dashboard

**✓ ACTIVE**



# Cloud SIEM

## 활용 사례 1 - 0.0.0.0/32로 오픈된 AWS EC2 보안그룹 탐지

- 실수 또는 임시조치로 인해 발생한 보안 위협에 대해 신속하게 알림

 **Datadog** 앱 1시간 전

`{@recipientAccountId: world} Security group open to the world - SG open to world`

## Goal  
Detect when an AWS security group is opened to the world.

## Strategy  
Monitor CloudTrail and detect when an AWS security group has been created or modified with one of the following API calls:

\* [AuthorizeSecurityGroupIngress][1]

This rule inspects the `@requestParameters.ipPermissions.items.ipRanges.items.cidrIp` array to determine if either of the strings are contained:

\* `0.0.0.0/0`

[자세히 표시](#)



# Cloud SIEM

## 활용 사례 2 - 디비 튜플 암호화에 사용된 KMS 키에 대한 비정상적인 접근 탐지

- 승인되지 않은 AWS 리소스 접근에 대해 즉시 알림
- 빠른 문제 식별 및 대처 가능

 **Datadog** 앱 2024년 3월 12일 13:55  
{@evt.name:Decrypt}.[custom.evt.name:Decrypt].[KMS] 비정상적인 접근 발생:  
-backend

backend에서만 사용되어야 할 KMS 암복호화 키가 비정상적인 접근 방법을 통해 사용되었습니다.

해당 암복호화 키는 정책상 다. -backend ECS 컨테이너에서만 사용되어야 합니다.

악의적 탈취 혹은 개인정보 유출 유무를 점검하십시오.

[View Security Signal](#) · [View Related Logs](#) · [Edit Security Rule](#) · [Manage Notification](#)  
[자세히 표시](#)

---

4개의 댓글

 **제이스 (DEV)** 2024년 3월 12일 13:57  
[REDACTED]에서 Decrypt한 것으로 확인됩니다! 혹시 지난번에 설정한 값이 변경되었는지 확인 하겠습니다

 **제이크 (DEV)** 2024년 3월 12일 14:31  
C.C. [@p-devops](#)

 **제이스 (DEV)** 2024년 3월 12일 14:35  
확인 결과 [REDACTED]에서 [REDACTED] SQS로부터 Message를 가져오는 과정에서 Rallit KMS Key를 사용하는데 지난번에 Rallit KMS Key를 교체하는 작업에서 누락된것으로 확인했습니다. 바로 수정하도록 하겠습니다

 **제이스 (DEV)** 2024년 3월 12일 14:57  
KMS 키 수정 완료했습니다

넵! 1 



# Cloud SIEM

## 활용 사례 3 - CRM 대비를 위한 스케일링 예약 이벤트

- 스케일링 예약 이벤트 감지 시 실시간 알림 발송
- 기존의 수기 공유를 대체

 **Datadog** 앱 13:40

**ECS 스케일링 예약 이벤트 발생 - 예약된 스케일링 동작**

ECS 스케일링 예약 이벤트가 발생했습니다.

- 작업자: [REDACTED]
- 이벤트명: [REDACTED]
- 스케일링 일시: at(2025-01-23T13:46:12)
- 대상: [REDACTED]

[자세히 표시](#)

ECS 스케일링 예약 생성됨

Define search queries for this detection. [Learn More](#)

UTC+09:00 1d Past 1 Day

5  
4  
3  
2  
1  
0 CRM

18:00 21:00 Thu 23 03:00 06:00 09:00 12:00 15:00

default\_zero(count[source:clouptrail @evt.name:PutScheduledAction])

Query put\_schedu 감사로그에서 특정 이벤트 감지

source:clouptrail @evt.name:PutScheduledAction

Count \* group by (everything) roll-up over 0 minutes (no roll-up) sliding window

Preview matching logs

+ Add Query

3 Define Conditions 1 Condition Defined: CRM

4 Describe your Playbook

Use notification variables and Markdown to customize the notifications sent when a signal is generated.

ECS 스케일링 예약 생성됨

Edit Preview

H B I S C < > |

- 이벤트명: \*{{@requestParameters.scheduledActionName}}\*  
- 대상: \*{{@requestParameters.resourceId}}\*  
- 작업자: \*{{@userIdentity.session\_name}}\*  
- 최소수량: \*{{@requestParameters.scalableTargetAction.minCapacity}}\*  
- 최대수량: \*{{@requestParameters.scalableTargetAction.maxCapacity}}\*

Slack 알림 발송 메시지 템플릿

Include triggering group-by values in notification title [Markdown Help](#)



# RUM (Real User Monitoring)

RUM | JS inflearn

DTC10900 1w Past 1 Week

Performance Monitoring Product Analytics Session Replay Error Tracking Sessions Explorer

Summary Optimization Feature Flag Tracking

Analyze your application performance

Revert back to the legacy Summary →

Env All Service All Version All Session Type user Country All Device Type All + Filter

OVERALL PAGE PERFORMANCE Metric: Loading Time

Search page name...

1.21M views

performance: Needs improvement

525.61k views

/course/?/dashboard views

/courses/lecture views

views

performance: Poor

511.52k views

/course/? views

views

performance: Good 171.34k views

/my/courses views

/signin

/users/? /users/?/ courses

/course/? /m... /...

Poor >4s Needs improvement <=4s Good <=2.5s

PERFORMANCE METRICS

Select Page Search View Name...

Optimize Vitals

Performance Dashboard Optimize Vitals →

Loading Time 4.89

Largest Contentful Paint 6.18% ↗

First Contentful Paint 4.08% ↗

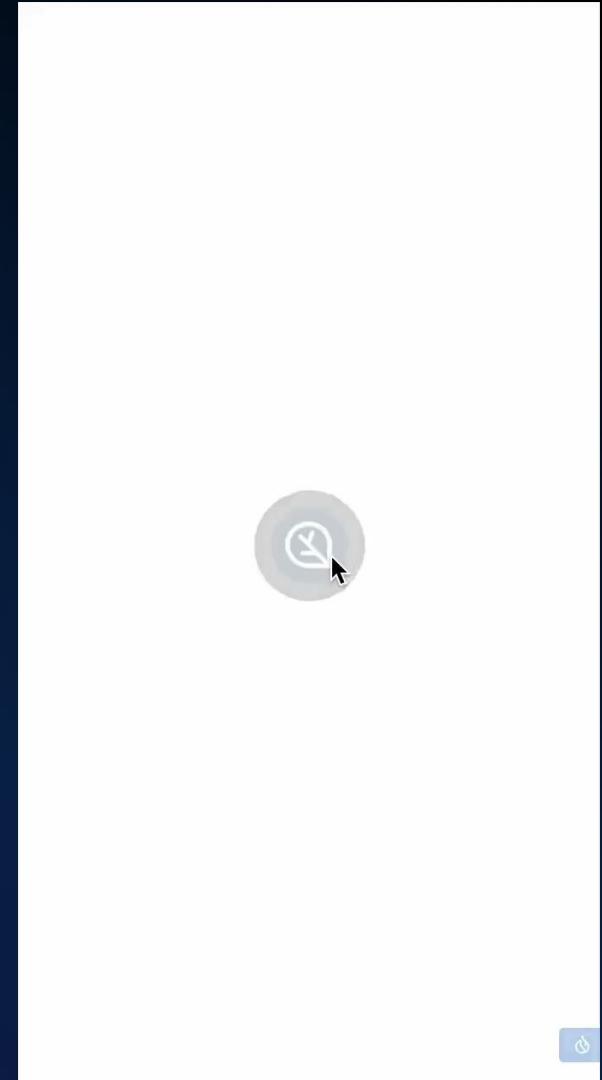
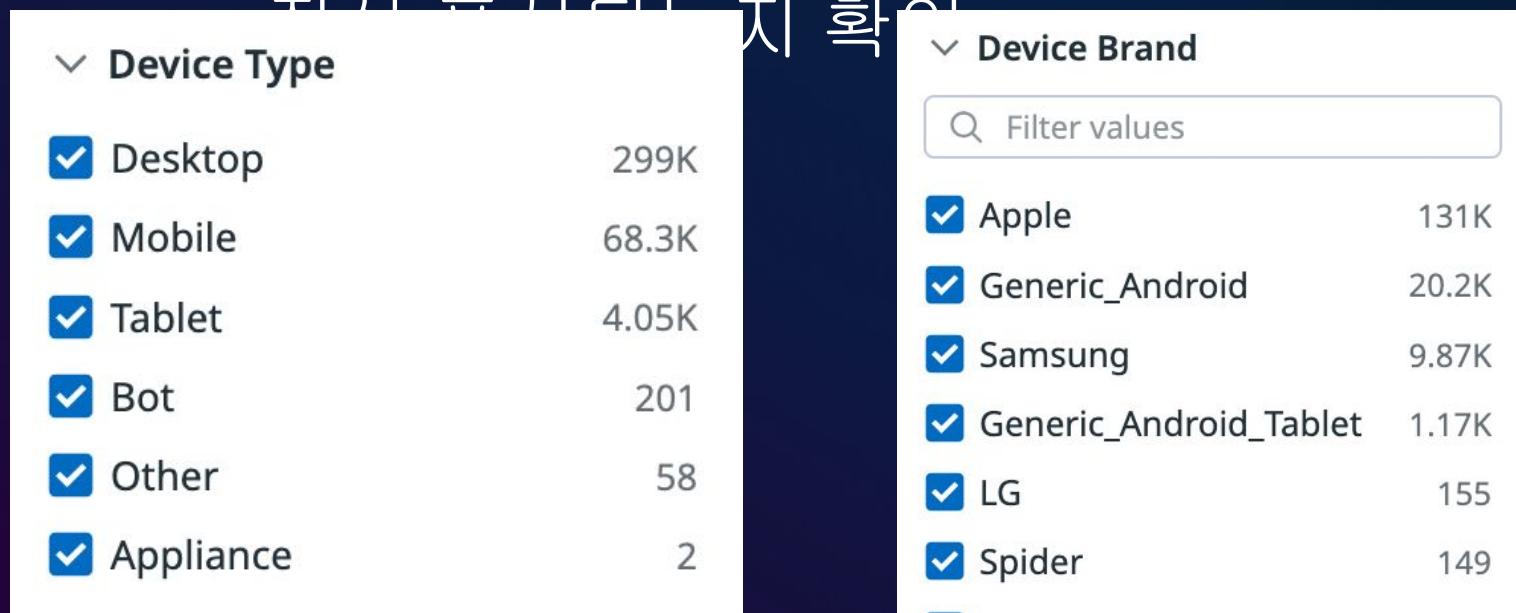
Cumulative Layout Shift -14.79% ↘

Interaction To Next Paint -21.34% ↘

# RUM (Real User Monitoring)

## 활용 사례 - 유저 액션 추적

- UI/UX에서 발생하는 버그 재현에 활용
- 사용자단의 단말마다 UI가 실제로



# Datadog을 잘 써보기



# Datadog을 잘 써 보기

- 적은 비용으로 최대한의 효율 뽑아내기
  - Datadog agent host 수량 최적화
  - Log 비용 최적화
- 자격증명 자동화
  - Google Workspace SAML 연동



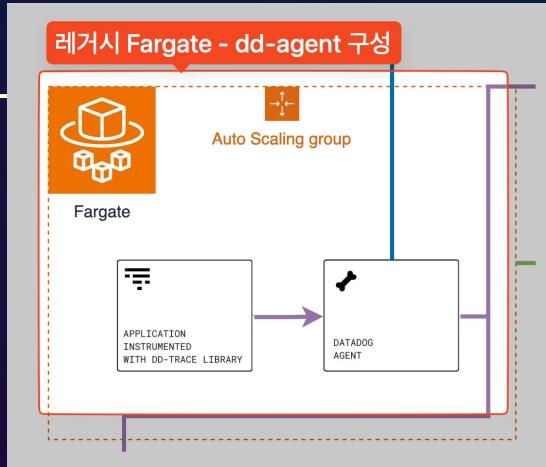
# Datadog agent host 수량 최적화

- Datadog Agent Host 월 비용: \$31~45

- Datadog Fargate\* 컨테이너 월 비용:

\$2.9~3.7

- Agent Host 수 최적화



\*)Fargate: AWS의 Full Managed 컨테이너 서비스

## APM Host 월 비용

APM	APM Pro	APM Enterprise
STARTING AT <b>\$ 31</b> Per host, per month*	STARTING AT <b>\$ 35</b> Per host, per month*	STARTING AT <b>\$ 40</b> Per host, per month*
APM DevSecOps	APM DevSecOps Pro	APM DevSecOps Enterprise
STARTING AT <b>\$ 36</b> Per host, per month*	STARTING AT <b>\$ 40</b> Per host, per month*	STARTING AT <b>\$ 45</b> Per host, per month*

## APM Fargate 월 비용

AWS Fargate

\$2 per task (\$2.90 on-demand)

\$2 per task (\$2.90 on-demand)

10GB span ingestion and 65,000 span retention, averaged across all your APM hosts

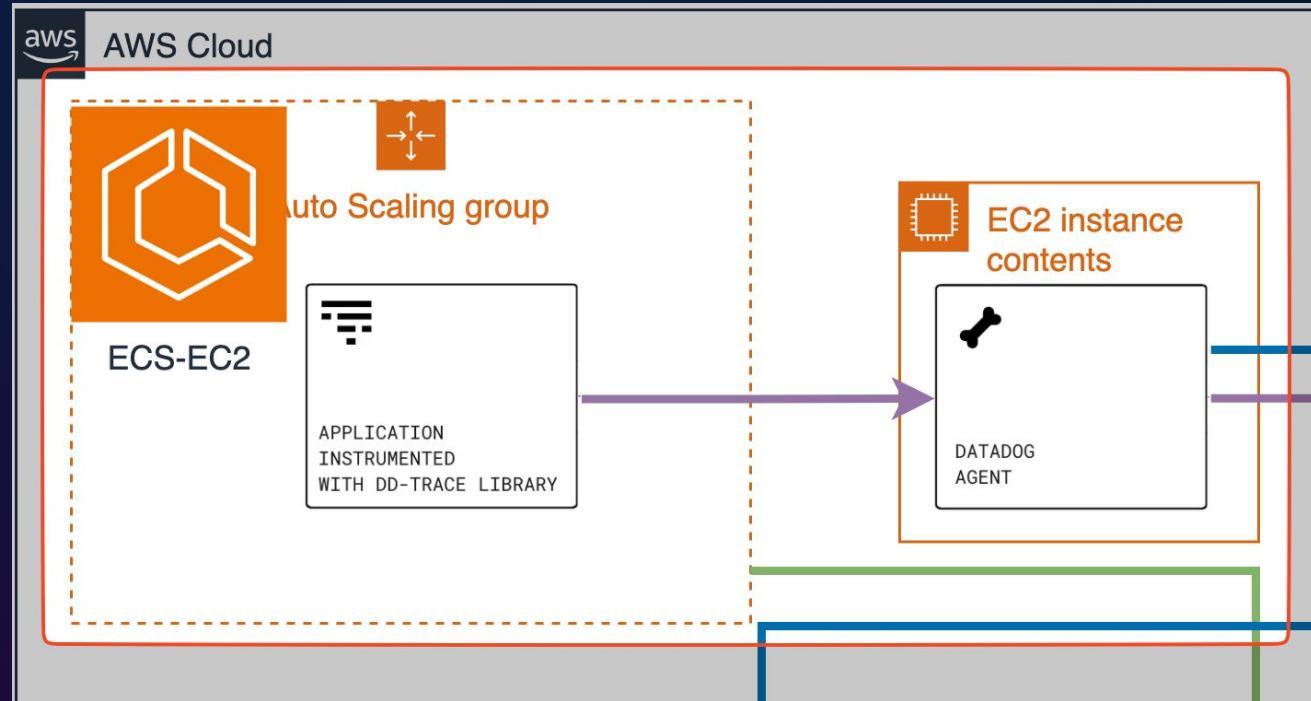
\$2.60 per task (\$3.70 on-demand)

10GB span ingestion and 65,000 span retention, averaged across all your APM hosts, 1 profiled host



# Datadog agent host 수량 최적화

- Agent Host와 컨테이너 Host 분리
- Agent Host를 6개만 운영



# Datadog agent host 수량 최적화

## 연결 방법

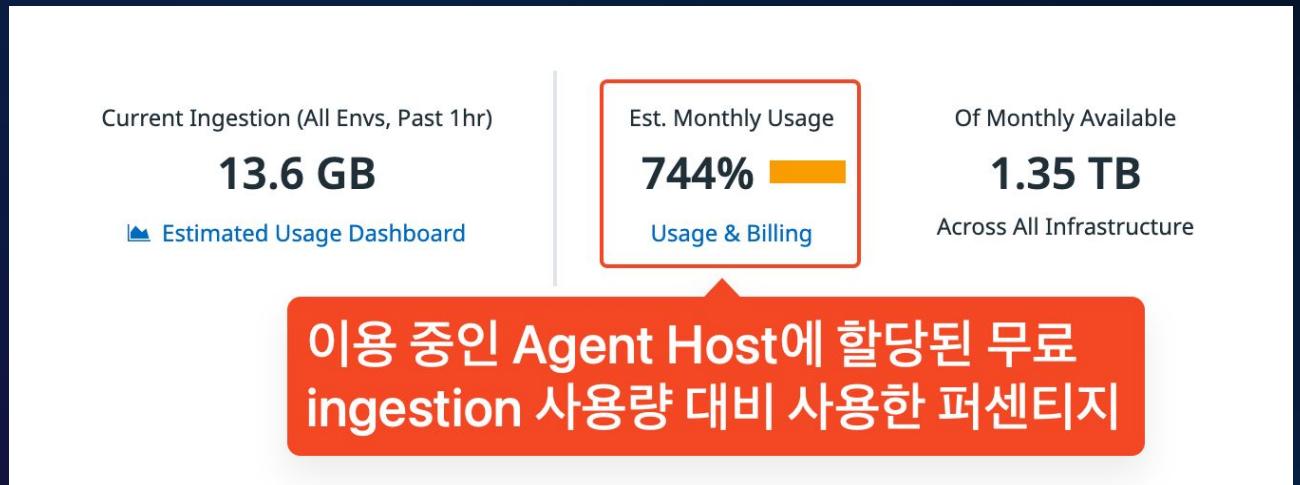
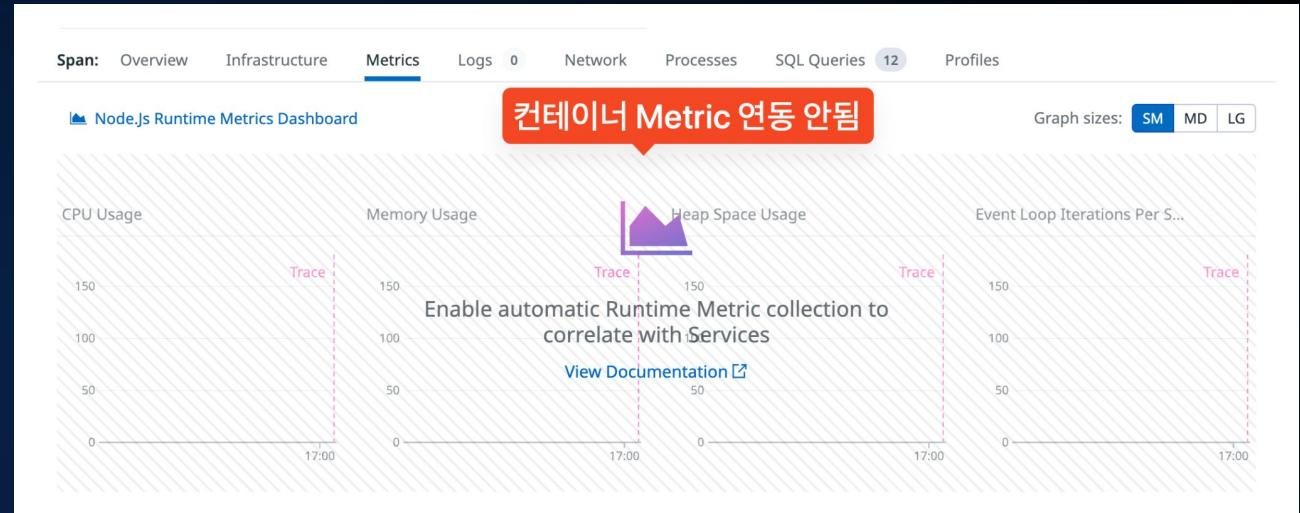
- 각 서비스 컨테이너에 **DD\_AGENT\_HOST**와 **DD\_TRACE\_REPORT\_HOSTNAME** 환경 변수 정의



# Datadog agent host 수량 최적화

## 주의 사항

- Metric 연동 불가
  - AWS 통합의 메트릭 활용 필요
- 별도의 trace ingestion 비용 발생 가능
  - 비용은 Agent Host보다 저렴



# Log 비용 최적화

Index를 사용하여 유형별 Log 리텐션 기간 지정

- Retention: Log 보관 기간
  - 3일 ~ 15개월 다양
- Log 소스의 중요도에 따라 보관 기간 설정 필요

The screenshot shows the Datadog 'Indexes' configuration page. It displays 10 active indexes and their retention settings across different tiers.

STANDARD TIER	FLEX TIER
3 days	—
—	180 days
3 days	—
3 days	180 days
3 days	—

**Indexes** View docs | View Usage Dashboard | Flex Logs Compute Size: Starter + New Index

View All indexes Filter Indexes

10 indexes defined

Index 이름	필터 조건	Log 리텐션 기간
index-vod	host:"/aws/batch/job" service:inflearn-vod-* @aws.s3.bucket:aws-waf-logs-* source:cloudfront source:postgresql source:elb source:amazon-inspector OR service:amazon-inspector source:clouptrail source:cloudwatch *	3 days
index-waf		180 days
index-cloudfront		3 days
index-rds		180 days
index-elb		3 days
index-amazon-inspector		3 days
index-clouptrail		3 days
index-cloudwatch		3 days
main		3 days
index-15		3 days

INDEXES 10 active

FILTERS

Add a new index



# Log 비용 최적화

Index를 사용하여 유형별 Log 리텐션 기간 지정

- Index 분리시 index별 사용량 확인 가능
- 각 Log에 필요한 retention 기간 및 비용을 확인하여 개별 지정 추천

## Index별 로그 사용량 확인 가능

NAME	RETENTION (D)	LIVE INDEXED LOG COUNT	REHYDRATED INDEXED LOG CO...	↓ TOTAL INDEXED LOG COUNT	CONTRIBUTION PERCENTAGE
index-elb	3	524,182,313	0	524,182,313	36.4%
index-cloudfront	3	512,580,380	0	512,580,380	35.6%
index-rds	3	247,175,511	0	247,175,511	17.2%
index-cloudtrail	3	56,996,460	0	56,996,460	3.96%
main	3	52,458,517	0	52,458,517	3.65%
index-cloudwatch	3	44,971,968	0	44,971,968	3.13%
index-amazon-inspector	3	181,452	0	181,452	< 0.1%
index-vod	3	161,086	0	161,086	< 0.1%

## Retention 기간별 Log 요금

Logs - Indexed Log Events	Per 1M indexed logs (3-day retention), per month	\$1.06
Logs - Indexed Log Events	Per 1M indexed logs (7-day retention), per month	\$1.27
Logs - Indexed Log Events	Per 1M indexed logs (15-day retention), per month	\$1.70
Logs - Indexed Log Events	Per 1M indexed logs (30-day retention), per month	\$2.50



# Log 비용 최적화

## Rehydration 활용

- Rehydrate 기능으로 retention 기간이 지난 Log를 다시 Datadog log로 복구 가능
- 복구 범위와 쿼리 조건을 세밀하게 지정하면 비용 절감 가능

Log Forwarding

Archives Forward logs to your Amazon, GCP or Azure cloud storage

Custom Destinations Forward logs to other destinations such as your SIEM provider

6 archives defined [View docs](#)

[+ New Archive](#)

View All archives [Filter Archives](#)

Pipelines **Rehydrate 아카이브 대상 S3 버킷 필터**

ARCHIVES	FILTERS
1 cloudfront	source:cloudfront
2 elb	source:elb
3 waf	@aws.s3.bucket:aws-waf-logs-*
4 cloudwatch	source:cloudwatch
5 rds	source:postgresql
6 default	*

Rehydrate from Archive **Rehydrate할 범위와 index 지정**

1 Set Scanning Range  
Select Time Period UTC+09:00  
1d Jan 21, 6:07 pm – Jan 22, 6:07 pm

Select Archive cloudfront

Archive Size Scan size is unknown - Estimate it to forecast scanning costs.  
[Estimate](#)

2 Set Historical View  
Name Historical Index jan-21-jan-22  
Set Indexing Query **쿼리할 로그 지정**  
Enter your query

Stop Rehydration if Volume Exceeds 300 million

Retain Logs for 3 days

3 Notify Team on Rehydration Completion  
@joshua@inflab.com  
{#is\_success}  
Rehydration from archive {{archive}} from {{from}} to {{to}} filtered by {{query}} has been successfully completed. {{scan\_size}} have been scanned and {{number\_of\_indexed\_logs}} events have been indexed.  
  
Start exploring right away: {{explorer\_url}}  
{#is\_error}  
An error has occurred with the rehydration from archive {{archive}} from {{from}} to {{to}} filtered by {{query}}. {{scan\_size}} have been scanned and {{number\_of\_indexed\_logs}} events have been indexed.  
  
More detailed information here: {{view\_modal\_url}}  
{#is\_error}

**Scan size is unknown - Estimate it above to forecast scanning costs.**

[Cancel](#) [Rehydrate From Archive](#)



# Google Workspace SAML 연동

## IdP를 통한 사용자 연동

- 사용자 자동 Provision으로 효율적인 자격증명 관리
- 회사가 사용하는 IdP (자격증명제공자)로부터 사용자 연동
- 더 이상 이메일 초대는 불필요

NAME	EMAIL	ROLES	LOGIN METHODS
[REDACTED]	[REDACTED]	SAML 연동된 계정 Datadog Standard Role	SAML
[REDACTED]	[REDACTED]	Datadog Standard Role	SAML
[REDACTED]	[REDACTED]	Datadog Admin Role +1	SAML
[REDACTED]	[REDACTED]	Datadog Standard Role	SAML
[REDACTED]	[REDACTED]	Datadog Standard Role	SAML
[REDACTED]	[REDACTED]	Datadog Read Only Role	SAML
[REDACTED]	[REDACTED]	Datadog Standard Role	SAML

Teams 12			
NAME	MEMBERS	LINKS	SERVICES
cell-auth	[REDACTED] +1	[REDACTED]	account antman-account +2
cell-b2b	[REDACTED] +4	[REDACTED]	antman-b2b antman-b2b-postgres +1
cell-course	[REDACTED] +4	[REDACTED]	internal-course.inflearn.com
cell-mobile	[REDACTED] +1	[REDACTED]	
cell-player	[REDACTED] +2	[REDACTED]	
cell-rallit	[REDACTED] +6	[REDACTED]	rallit-b2c-api rallit-b2c-api-postgres +3
cell-search	[REDACTED] +2	[REDACTED]	
cell-ucc	[REDACTED] +6	[REDACTED]	inflearn-header-api inflearn-ucc-api
part-be	[REDACTED] +9	[REDACTED]	
part-dev	[REDACTED] +31	[REDACTED]	inflearn-antman inflearn-antman-postgres +1
part-devops	[REDACTED] +4	[REDACTED]	inflab-devops-api internal-devops-api.inflearn.com
part-fe	[REDACTED] +14	[REDACTED]	



# Google Workspace SAML 연동

## GWS SAML 연동 방법

- 참고문서: <https://support.google.com/a/answer/7553768>

Organization Settings ▾

Search

IDENTITY & ACCOUNTS

- Users
- Teams NEW
- Service Accounts

AUTHENTICATION

- Login Methods** (선택)
- SAML Group Mappings

ACCESS

- API Keys
- Application Keys
- Roles
- Client Tokens
- Events API Emails

SECURITY

- Safety Center NEW
- Public Sharing
- OAuth Apps
- Remote Configuration

Organization: Inflab | Log Out

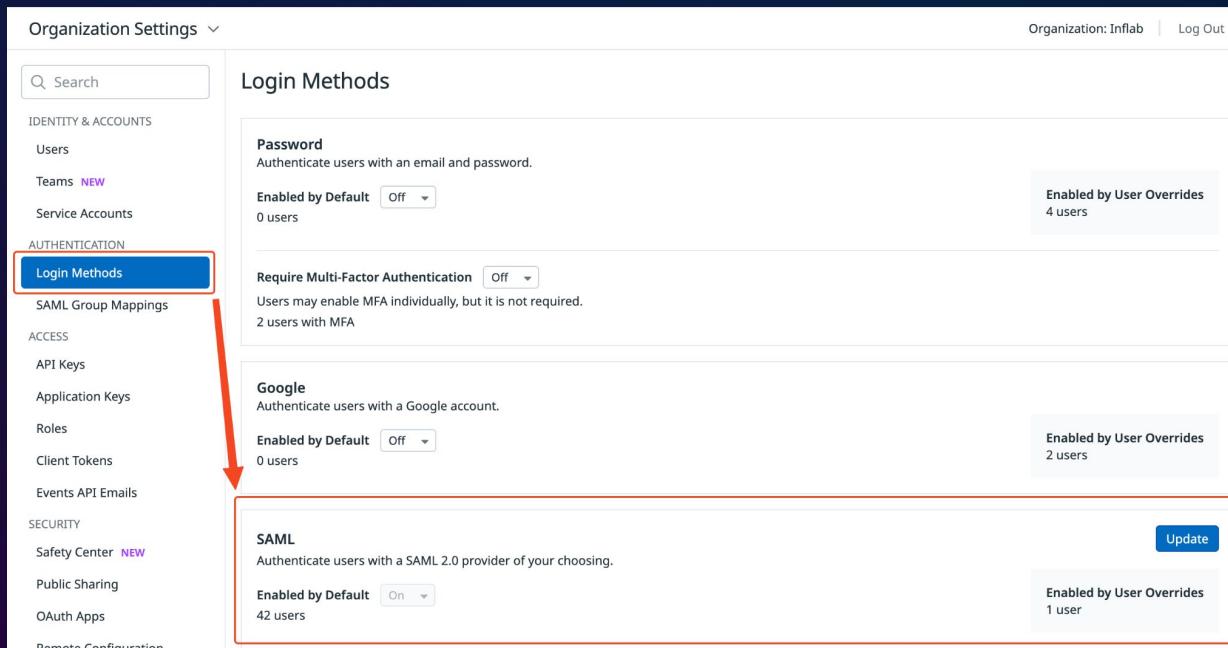
### Login Methods

**Password**  
Authenticate users with an email and password.  
Enabled by Default: Off (0 users)  
Enabled by User Overrides: 4 users

**Require Multi-Factor Authentication**  
Users may enable MFA individually, but it is not required.  
2 users with MFA

**Google**  
Authenticate users with a Google account.  
Enabled by Default: Off (0 users)  
Enabled by User Overrides: 2 users

**SAML**  
Authenticate users with a SAML 2.0 provider of your choosing.  
Enabled by Default: On (42 users)  
Enabled by User Overrides: 1 user



**SAML is enabled**

Valid IdP metadata installed | Replace IdP Metadata

**Datadog Service Provider details**

Datadog supports HTTP-POST binding for SAML 2.0.

자격증명 획득을 위한 정보

Service Provider Metadata	<a href="https://app.datadoghq.com/account/saml/config/94ba7...">https://app.datadoghq.com/account/saml/config/94ba7...</a>
Service Provider Entity ID	<a href="https://app.datadoghq.com/account/saml/metadata.xml">https://app.datadoghq.com/account/saml/metadata.xml</a>
Assertion Consumer Service URL	<a href="https://app.datadoghq.com/account/saml/assertion">https://app.datadoghq.com/account/saml/assertion</a>
Service Provider Details	<a href="https://docs.datadoghq.com/account_management/saml/">https://docs.datadoghq.com/account_management/saml/</a>

**Additional Features**

Identity Provider (IdP) Initiated Login  
 Identity Provider (IdP) Initiated Login

IdP에서 로그인을 허용하는 설정

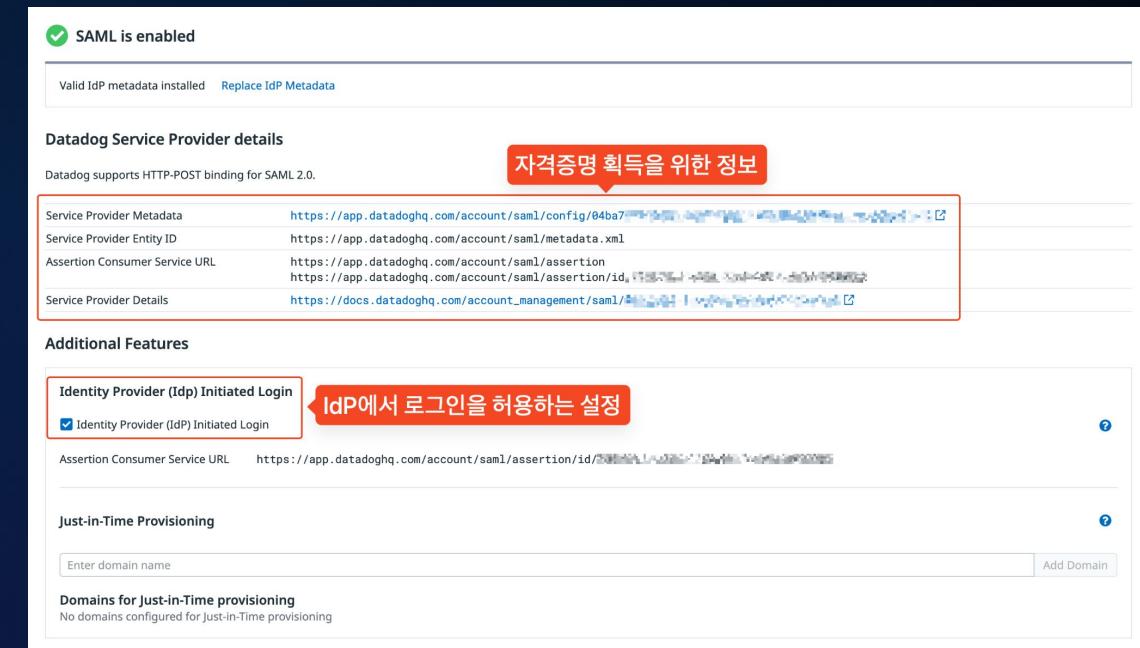
Assertion Consumer Service URL: <https://app.datadoghq.com/account/saml/assertion/id/...>

**Just-in-Time Provisioning**

Enter domain name

Add Domain

Domains for Just-in-Time provisioning  
No domains configured for just-in-time provisioning



# Google Workspace SAML 연동

## GWS 쪽 구성 방법

- 참고문서: <https://support.google.com/a/answer/7553768>

SAML GWS 쪽 구성

Datadog

SAML 로그인 테스트

메타데이터 다운로드

세부정보 수정

앱 삭제

사용자 액세스

선택한 사용자에게 관리 앱을 제공하려면 그룹 또는 조직 단위를 선택하세요. 자세히 알아보기

세부정보 보기

모든 사용자에 사용하도록 설정

서비스 제공업체 세부정보

인증서

Google\_2029-8-6-02228\_SAML2\_0  
(만료일: 2029. 8. 6.)

ACS URL

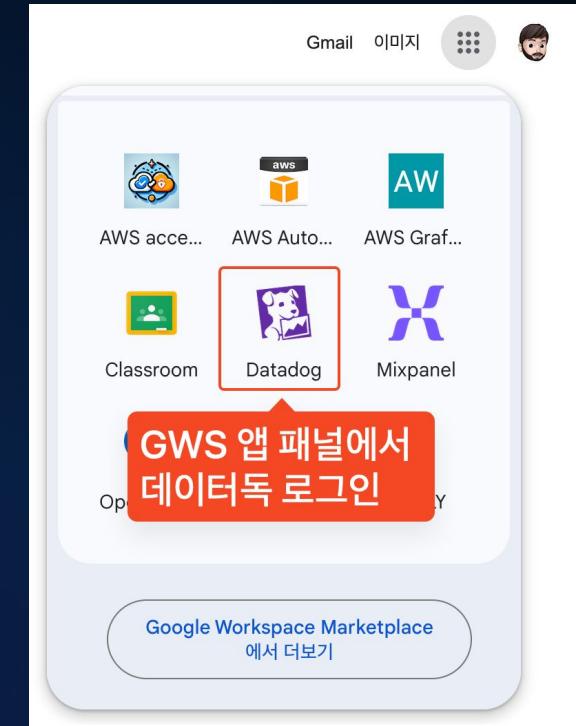
엔티티 ID

https://app.datadoghq.com/account/saml/metadata.xml

SAML 속성 매핑

Google 디렉터리의 사용자 프로필 필드를 SAML 서비스 제공업체 속성에 매핑합니다.

urn:oid:1.3.6.1.4.1.5923.1.1.1.6	urn:oid:2.5.4.4	urn:oid:2.5.4.42
Basic Information > Primary email	Basic Information > Last name	Basic Information > First name
Group membership		
15 groups > group		



# Google Workspace SAML 연동

GWS 그룹 정보로 Datadog 팀 정보에 자동 연동

The screenshot shows the Google Workspace Groups interface. At the top, it displays 'Teams 12'. Below is a table with columns for 'NAME' (team name), 'MEMBERS' (number of members), 'LINKS' (links to other services like account, antman-account, antman-b2b, antman-b2b-postgres, internal-course.infllearn.com, inflearn-header-api, inflearn-ucc-api), and 'SERVICES' (links to inflearn-antman, inflearn-antman-postgres, inflab-devops-api, and internal-devops-api.infllearn.com). A red box highlights the 'GWS와 자동 연동되는 팀 구성' (Automatically synchronized team configuration) section at the top of the table.

## SAML Group Mappings

Team Mappings

Role Mappings

✓ Team Mappings enabled [What are team mappings?](#)

Filter by team or IDP attributes

TEAM	ATTRIBUTE KEY	ATTRIBUTE VALUE
cell-ucc	group	Cell-ucc
part-devops		파트
part-dev		인강의
cell-course		모바일
cell-mobile		랩톱
cell-rallit		-검색엔진
cell-player		개발 백엔드 파트
cell-search		개발 프론트엔드 파트
part-be	group	Cell-auth
part-fe	group	Cell-b2b
cell-auth	group	Cell-계정인증

### Edit Team Mapping

Map a Datadog Team to its key-value pair found in your IDP provider's SAML assertion. Users with these key-value pairs will be added to the teams on login. For further details, see our [docs](#).

Key	Value	Team
group	Cell-ucc	cell-ucc



# Google Workspace SAML 연동

GWS 그룹 정보로 Datadog 역할 자동 부여

## SAML Group Mappings

Team Mappings

Role Mappings

 Role Mappings enabled [What are mappings?](#)

Filter by role or IDP attributes

ROLE	ATTRIBUTE KEY	ATTRIBUTE VALUE
Datadog Admin Role	group	데브옵스 파트
Datadog Standard Role	group	개발 파트
Datadog Read Only Role	group	PM 파트
Datadog Read Only Role	group	프로덕트 디자인 파트

## Edit Role Mapping

Map a Datadog Role to its key-value pair found in your IDP provider's SAML assertion. Users with these key-value pairs will be granted the roles on login. For further details, see our [docs](#).

Key	Value	Role
group	개발 파트	→ Datadog Standard Role

[Cancel](#)

[Save](#)



# Google Workspace SAML 연동

정리

- IdP (자격증명제공자)로부터 사용자 연동
- 사용자의 팀 정보 자동 연동
- 사용자의 역할 자동 부여
- 더 이상 이메일 초대 & 수동 권한 부여 불필요



# 마무리



# Datadog의 많고 다양한 기능 vs 사용자에게 정말 필요한 기능



Datadog 좋아요. 그리고 잘 쓰면 더  
좋아요.



# 질문 답변



# 다음에 또 만나요!

Contact: [joshua@inflab.com](mailto:joshua@inflab.com)

