



DATADOG

Datadog In-depth Session (Day 1)
2:00 PM에 시작합니다!

SKT 2 days 교육 일정

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

시간	Day2
14:00 ~ 14:50 (이성욱 부장)	Application Performance Monitoring (Back End) <ul style="list-style-type: none">- 개요 및 설명- 설치 및 구성 방법- 최적화 사용 방안- Q&A
14:50 ~ 15:00	Break
15:00 ~ 15:50 (정영석 부장)	Real User Monitoring (Front End) <ul style="list-style-type: none">- 개요 및 설명- 설치 및 구성 방법- 최적화 사용 방안
15:50 ~ 16:00	Break
16:00 ~ 17:00	Q&A Session

Datadog Overview

- 기본 소개 및 전체 제품 구성 안내
- 기본 비용 체계
- 계정 접속 및 ORG 구성/권한

Datadog 제품 구성



Datadog 제품 구성



Datadog은 SaaS기반의 통합 모니터링 플랫폼으로 다음의 가치를 추구합니다

- 최소한의 운영 인력으로 모니터링에 필요한 데이터를 손쉽게 수집
- 운영, 개발, 보안 및 기획팀 사이의 원만한 협업 (같은 데이터를 보며 커뮤니케이션)
- 이슈 분석 시간을 최소화

Datadog 기본 비용 체계

Real-Time Unified Data Platform

Infrastructure Monitoring

Hosts / Clouds / VMs
Containers
Processes
Serverless
IoT

APM

Distributed Tracing
Tracing without Limits™ 2019
Continuous Profiler 2020
Deployment Tracking 2020
Database Monitoring

Log Management

Logging without Limits™

Synthetic Monitoring

Security Platform

Security Monitoring 2019
Security Posture Management 2020
Workload Security 2020

Network Monitoring

Network Performance
Network Device 2020

Incident Management

Real User Monitoring

Error Tracking

Infrastructure 과금 단위

- 호스트 수
- 컨테이너 수 (호스트 하나당 10개 컨테이너 무료 포함)
- ECS Fargate는 Task 수
- EKS Fargate는 Pod 수

ADD-ONS

AWS Fargate (serverless containers) \$1 per task \$1 per task

IoT Device Monitoring \$5 per device \$5 per device

Infrastructure

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

Free

\$ 0

Pro

\$ 15

Per host, per month*

Enterprise

\$ 23

Per host, per month*

Core collection and visualization features

- Discussion group supported
- 1-day metric retention
- Up to 5 hosts

Centralize your monitoring of systems, services, and serverless functions

- 450+ integrations
- Out-of-the-box dashboards
- 15-month metric retention

Advanced features and administrative controls

- Machine learning-based alerts
- Live Processes
- Premium support

*Billed annually or \$27 on-demand 100 host minimum

Datadog 기본 비용 체계

Real-Time Unified Data Platform

Infrastructure Monitoring

Hosts / Clouds / VMs

Containers

Processes

Serverless

IoT

APM

Distributed Tracing
Tracing without Limits™ 2019
Continuous Profiler 2020
Deployment Tracking 2020
Database Monitoring

Log Management

Logging without Limits™

Synthetic Monitoring

Security Platform

Security Monitoring 2019
Security Posture Management 2020
Workload Security 2020

Network Monitoring

Network Performance
Network Device 2020

Incident Management

Real User Monitoring

Error Tracking

Serverless 과금단위

- Lambda 호출 수



Serverless

Monitor, detect, and resolve bottlenecks and errors

STARTING AT

\$ 5

Per million invocations, per month*

START FREE TRIAL

Real-time serverless metrics

15-month metric retention

Trace function invocations

Out-of-the-box Service Map

Connect traces across hosts and functions

150k Indexed Spans and 5 custom metrics included

*Billed annually or \$7.20 on-demand. See [docs](#) for more information

Datadog 기본 비용 체계

Real-Time Unified Data Platform

Infrastructure Monitoring

- Hosts / Clouds / VMs
- Containers
- Processes
- Serverless
- IoT

APM

- Distributed Tracing
- Tracing without Limits™ 2019
- Continuous Profiler 2020
- Deployment Tracking 2020
- Database Monitoring

Log Management

- Logging without Limits™

Synthetic Monitoring

- Security Platform
 - Security Monitoring 2019
 - Security Posture Management 2020
 - Workload Security 2020

Incident Management

- Real User Monitoring
- Error Tracking

APM 과금단위

- 호스트 수
- AWS Fargate는 Task 수
- EKS Fargate는 Pod 수
- Indexed span (호스트 당 1M indexed span 무료제공)
 - 초과시 1 Million span 당 약 \$1.7 과금 (15-day retention 기준)
- Ingested span (호스트 당 150 GB 무료제공)
 - 초과시 \$0.10/GB



APM & Continuous Profiler

End-to-end distributed tracing with no sampling
and always-on production code profiling

APM

STARTING AT

\$ 31

Per host, per month*

Monitor every service, every code deployment, and every request

- Correlate traces with metrics, logs, processes, network data, and more
- 15-minute live search & analytics
- 15-day historical search & analytics
- 15-month metric retention

*Billed annually or \$36 on-demand

APM & Continuous Profiler

STARTING AT

\$ 40

Per host, per month*

Optimize code performance in production with minimal overhead

- Everything included in APM
- Code level visibility for every request
- Optimize bottlenecks in your code to reduce resource consumption and cloud costs
- Actionable insights with automatic code analysis

*Billed annually or \$48 on-demand

Datadog 기본 비용 체계

Real-Time
Unified Data Platform

Infrastructure
Monitoring

Hosts / Clouds / VMs
Containers
Processes
Serverless
IoT

APM

Distributed Tracing
Tracing without Limits™ 2019
Continuous Profiler 2020
Deployment Tracking 2020
Database Monitoring

Log Management

Logging without Limits™

Synthetic Monitoring

Security Platform

Security Monitoring 2019
Security Posture Management 2020
Workload Security 2020

Incident Management

Real User Monitoring

Error Tracking

Database Monitoring

Surface slow performing queries and optimize application performance

STARTING AT

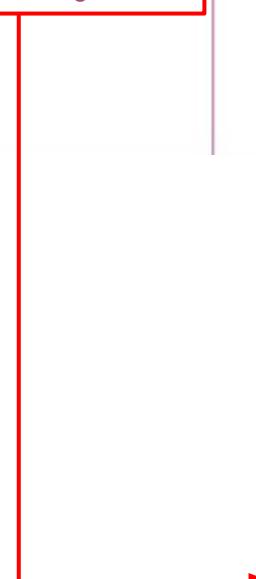
\$ 70

Per database host, per month*

START FREE TRIAL

DB Monitoring 과금단위

- 호스트 수



Track normalized query performance trends using database-generated metrics

Correlate query performance with database infrastructure metrics

Access all of your database insights, database hosts, clusters, and applications

Extract valuable data without compromising database security

*Billed annually or \$84 per host on-demand

Datadog 기본 비용 체계

Real-Time Unified Data Platform

Infrastructure Monitoring

Hosts / Clouds / VMs
Containers
Processes
Serverless
IoT

APM

Distributed Tracing
Tracing without Limits™ 2019
Continuous Profiler 2020
Deployment Tracking 2020
Database Monitoring

Log Management

Logging without Limits™

Synthetic Monitoring

Security Platform

Security Monitoring 2019
Security Posture Management 2020
Workload Security 2020

Network Monitoring

Network Performance
Network Device 2020

Incident Management

Real User Monitoring

Error Tracking

Log Management

Analyze and explore log data in context with flexible retention

Ingest

STARTING AT
\$ 0.10

Per ingested or scanned GB, per month*

Ingest, process, live tail, and archive all logs

- Enrich and structure log data
- Parse on ingestion
- Generate log-based metrics
- Self-hosted archives, with the option to rehydrate
- Dynamic index routing

Retain or Rehydrate

15-DAY RETENTION ▾
\$ 1.70

Per million log events per month*

Retain logs based on their value and rehydrate from archives on-demand

- Define log retention based on tags or facets
- Simplified pricing based on retention for better cost control
- Log patterns and analytics
- Log Rehydration™ for audits and historical analysis

*Per GB of uncompressed data ingested for processing, or compressed data scanned for rehydrating.

Log 과금단위

- 인덱싱(Retain)한 로그 수 (검색을 위해서는 로그 인덱싱 필요)
- 인덱싱을 하지 않을 경우 Ingest 비용 과금

Datadog 기본 비용 체계

Real-Time
Unified Data Platform

Infrastructure
Monitoring

Hosts / Clouds / VMs
Containers
Processes
Serverless
IoT

APM

Distributed Tracing
Tracing without Limits™ 2019
Continuous Profiler 2020
Deployment Tracking 2020
Database Monitoring

Log Management

Logging without Limits™

Synthetic Monitoring

Security Platform
Security Monitoring 2019
Security Posture Management 2020
Workload Security 2020

Incident Management

Real User Monitoring

Error Tracking

Synthetic Monitoring

API and Browser Tests for proactive, end-to-end visibility

API Tests

STARTING AT

\$ 5

Per ten thousand test runs, per month*

Proactively monitor site availability

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

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 \$7.20 on-demand

*Billed annually or \$18 on-demand

Synthetic 과금단위

- Synthetic 테스트가 실행된 수

Datadog 기본 비용 체계

Real-Time Unified Data Platform

Infrastructure Monitoring

Hosts / Clouds / VMs
Containers
Processes
Serverless
IoT

APM

Distributed Tracing
Tracing without Limits™ [2019]
Continuous Profiler [2020]
Deployment Tracking [2020]
Database Monitoring

Log Management

Logging without Limits™

Synthetic Monitoring

Security Platform

Security Monitoring [2019]
Security Posture Management [2020]
Workload Security [2020]

Incident Management

Real User Monitoring

Error Tracking

Security Monitoring

Detect and investigate security threats in real time

STARTING AT

\$ **0.20**

Per GB of analyzed logs, per month*

START FREE TRIAL

Out-of-the-box and custom detection rules

Threat detection across all ingested data, regardless of retention

Security signals explorer and analytics

15-month retention of security signals

*Billed annually or \$0.30 on-demand

Security Monitoring 과금 단위

- Security 검사가 진행된 **로그의 GB 양**

Datadog 기본 비용 체계

Real-Time Unified Data Platform

Infrastructure Monitoring

Hosts / Clouds / VMs
Containers
Processes
Serverless
IoT

APM

Distributed Tracing
Tracing without Limits™ 2019
Continuous Profiler 2020
Deployment Tracking 2020
Database Monitoring

Log Management

Logging without Limits™

Synthetic Monitoring

Security Platform

Security Monitoring 2019
Security Posture Management 2020

Workload Security 2020

Network Monitoring

Network Performance
Network Device 2020

Incident Management

Real User Monitoring

Error Tracking

Cloud Security Posture Management

Continuous configuration audits across cloud accounts,
hosts, and containers

STARTING AT

\$ 7.50

Per host, per month*

START FREE TRIAL

Configuration rules for cloud, containers, and kubernetes

Visibility into your configuration status at any given point in time

Notify and alert on new misconfigurations

CIS, PCI-DSS, HIPAA, GDPR, and other standards

*Billed annually or \$9 on-demand

Security Posture Monitoring 과금단위

- Security Posture 검사되고 있는 호스트 수

Datadog 기본 비용 체계

Real-Time Unified Data Platform

Infrastructure Monitoring

Hosts / Clouds / VMs
Containers
Processes
Serverless
IoT

APM

Distributed Tracing
Tracing without Limits™ 2019
Continuous Profiler 2020
Deployment Tracking 2020
Database Monitoring

Log Management

Logging without Limits™

Synthetic Monitoring

Security Platform

Security Monitoring 2019
Security Posture Management 2020
Workload Security 2020

Incident Management

Real User Monitoring

Error Tracking

Cloud Workload Security

Real-time threat detection across hosts and containers

STARTING AT

\$ 15

Per host, per month*

START FREE TRIAL

Detect threats to your hosts and containers in real-time

Deep file & process activity monitoring

Performant, in-kernel, eBPF-powered analysis

Easy setup with the unified Datadog agent

*Billed annually or \$18 on-demand

Workload Security 과금단위

- 검사되고 있는 **호스트 수**

Datadog 기본 비용 체계

Real-Time Unified Data Platform

Infrastructure Monitoring

Hosts / Clouds / VMs
Containers
Processes
Serverless
IoT

APM

Distributed Tracing
Tracing without Limits™ 2019
Continuous Profiler 2020
Deployment Tracking 2020
Database Monitoring

Log Management

Logging without Limits™

Synthetic Monitoring

Security Platform

Security Monitoring 2019
Security Posture Management 2020
Workload Security 2020

Incident Management

Real User Monitoring

Error Tracking

Network Monitoring

Monitor devices and traffic flows for complete network visibility

Network Performance Monitoring

STARTING AT

\$ 5

Per host, per month*

Understand network traffic patterns and search with tags

- Visualize flows on the network map
- Slice-and-dice traffic by host, process, container, service, AZ, and more
- Analyze system-wide DNS performance

Network Device Monitoring

STARTING AT

\$ 7

Per device, per month*

Monitor the health and performance of on-premise network devices

- Out-of-the-box metrics collected from switches, routers, firewalls and more
- Visualize interface bandwidth and utilization, disk, fan, and other hardware health
- Comprehensive and customizable alerts

Network Performance Monitoring 과금단위

- 호스트 수

Network Device Monitoring 과금단위

- Network 장비 수

*Billed annually or \$7.20 on-demand

*Billed annually or \$10.20 on-demand

Datadog 기본 비용 체계

Real-Time Unified Data Platform

Infrastructure Monitoring

Hosts / Clouds / VMs
Containers
Processes
Serverless
IoT

APM

Distributed Tracing
Tracing without Limits™ 2019
Continuous Profiler 2020
Deployment Tracking 2020
Database Monitoring

Log Management

Logging without Limits™

Synthetic Monitoring

Security Platform

Security Monitoring 2019
Security Posture Management 2020
Workload Security 2020

Network Monitoring

Network Performance
Network Device 2020

Incident Management

Real User Monitoring

Error Tracking

Incident Management

Fully integrated incident management in-app

STARTING AT

\$ 20

Per user, per month*

START FREE TRIAL

Detect, triage, and track incidents with no context-switching

Assess severity and pull in relevant teams and resources

Collaborate directly in-app and across your favorite communication tools

Track incidents across an intuitive timeline and generate postmortems

*Billed annually or \$30 on-demand

Incident Management 과금단위

- Incident Management 사용한 Active User 수

Datadog 기본 비용 체계

Real-Time Unified Data Platform

Infrastructure Monitoring

Hosts / Clouds / VMs
Containers
Processes
Serverless
IoT

APM

Distributed Tracing
Tracing without Limits™ 2019
Continuous Profiler 2020
Deployment Tracking 2020
Database Monitoring

Log Management

Logging without Limits™

Synthetic Monitoring

Security Platform

Security Monitoring 2019
Security Posture Management 2020
Workload Security 2020

Network Monitoring

Network Performance
Network Device 2020

Incident Management

Real User Monitoring
Error Tracking

Real User Monitoring

Measure end-to-end user experience on web and mobile applications

STARTING AT

\$ 15

Per 10k sessions, per month*

START FREE TRIAL

Identify, troubleshoot and resolve performance issues

Collect and track application errors and crashes with Error Tracking

Automatically link frontend requests to backend APM traces

*Billed annually or \$18 on-demand

Real User Monitoring 과금단위

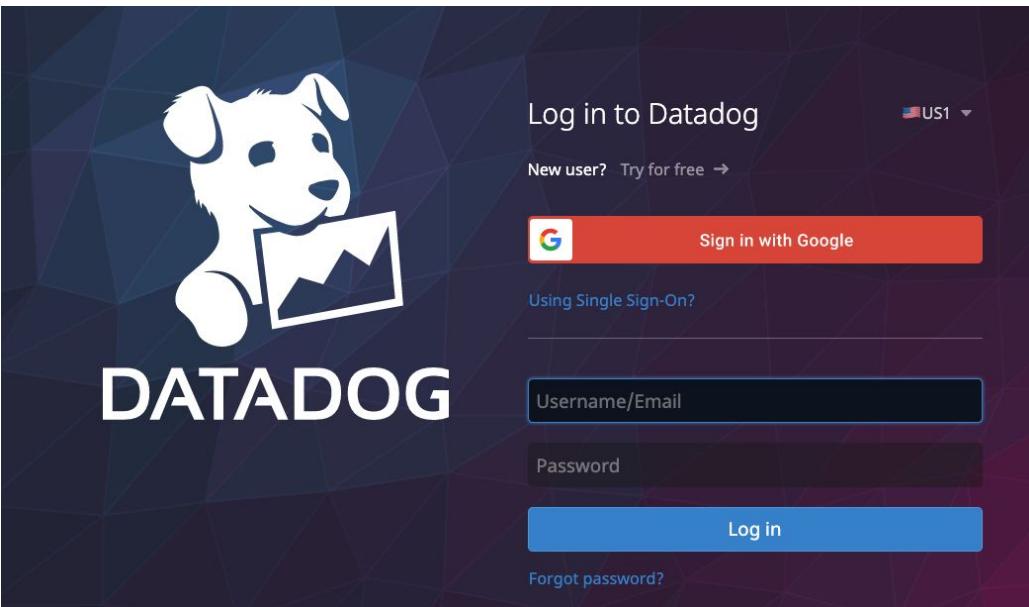
- 사용자 세션 수 (접속 사용자 별로 세션이 생성됨)

비용 걱정 없이 사용 가능한 부분

- Dashboard 생성
- Dashboard Public Share
- Dashboard 조회
- Datadog 사용자 수 (Incident Management Product 제외)
- 알람 생성
- 알람 트리거
- Datadog API 호출
- Notebook 생성 및 사용 (저장된 메트릭을 이용하여 이슈 분석 노트를 만들수 있는 기능)
- 450+ Integration을 통한 메트릭 수집은 대부분 추가 비용이 없습니다.
 - AWS, Azure 과 같이 Host가 탐지되어 메트릭을 수집하는 부분은 Host 과금이 있습니다.
 - Redis, Kafka 와 같은 Integration은 추가 비용없이 메트릭 수집이 됩니다

Datadog 계정 접속

1. ID/PW를 이용한 로그인



2. SSO 계정 연동을 이용한 로그인

- SAML을 지원하는 SSO 솔루션 연동 가능
- SSO 연동 솔루션 예
 - Active Directory
 - Auth0
 - Azure
 - Google
 - NoPassword
 - Okta
 - SafeNet
 - AWS SSO
- 부가 기능
 - SAML Attribute를 Datadog Role에 연동
 - Just in time provisioning (SSO 로그인 시 자동으로 Datadog 계정 생성)
 - SAML Strict (SSO를 통해서만 로그인 하도록 강제 설정)

Datadog 계정 전환

292926 Jacky's sandbox |  datadog.jacky@gmail.com

APM Services 1h Past 1 Hour View All →

Search services env:prod service:*

★ TYPE SERVICE	REQUESTS
  demo	< 0.1 req/s

Watchdog 2d Past 2 Days

datadog.jacky@gmail.com
292926 Jacky's sandbox

Log Out

Settings

Plan & Usage

Configure SAML

SWITCH ORGANIZATION

Filter organizations

AWS Summit 2021 - demo

APPEARANCE

Theme Light Dark System

Ctrl+Opt+D

Go to... Watchdog Events Dashboards Infrastructure Monitors Metrics Integrations APM CI BETA Notebooks Logs Security UX Monitoring Contact Support Help Team

hasn't detected any unusual behavior for env:prod and service:*

다수의 Datadog Account(Org)에 소속되어 있을 경우 설정 ⇒ SWITCH ORGANIZATION을 통해 전환 가능

Finish your APM Setup

9% Complete

Watch APM intro video 6 mins

Show More

Dashboards View All →

- ZooKeeper - Overview (cloned)
- VPC Flow Dashboard(Log기반)
- Kafka Cluster Monitoring
- Kafka - Overview (cloned)
- Kafka - Overview
- Jacky's Dashboard Wed, May 26, 10:
- Jacky's Dashboard Wed, May 26, 10:
- Host Overview 대시보드
- AWS VPC Flow Timeboard
- APM Traces - Estimated Usage

Datadog 접근 권한(기본 ROLE)

사용자 초대하는 화면에서 보시면.. (Team ⇒ Invite Users)

Invite Users

Invite users by email and assign them roles below.

Emails

Enter one or more valid email addresses separated by whitespace, ',', or ':'

Assign roles to users

Select roles

- Datadog Admin Role
- Datadog Read Only Role
- Datadog Standard Role

The diagram illustrates the mapping of Datadog roles to their corresponding permissions. Red lines connect the 'Datadog Admin Role' to the first four permissions. Orange lines connect the 'Datadog Read Only Role' to the next two permissions. Blue lines connect the 'Datadog Standard Role' to the last three permissions.

- Billing(사용량) 페이지 접근
- 사용자 관리
- API Key 관리
- + Standard User의 기능 포함
- Datadog에서 모든 기능에 대해 볼 수 있는 권한만 제공.
- 수정 불가
- Datadog에서 제공하는 모든 기능에 대해 생성 및 사용 가능

Datadog 접근 권한(Custom ROLE)

Custom Role을 통해 세밀한 권한 제어가 가능합니다

참고

- support@datadoghq.com 으로 다음과 같이 보내주시면 됩니다.
Subject: Enable custom roles

Please enable custom roles in our account. The organization name is XXX.

(서포트팀에서 Admin 인지 확인 후 활성화 진행해드립니다)
- Enterprise 라이센스 기능으로 라이센스 정책에 따라 향후 사용이 제한될 수 있습니다.

2 Permissions

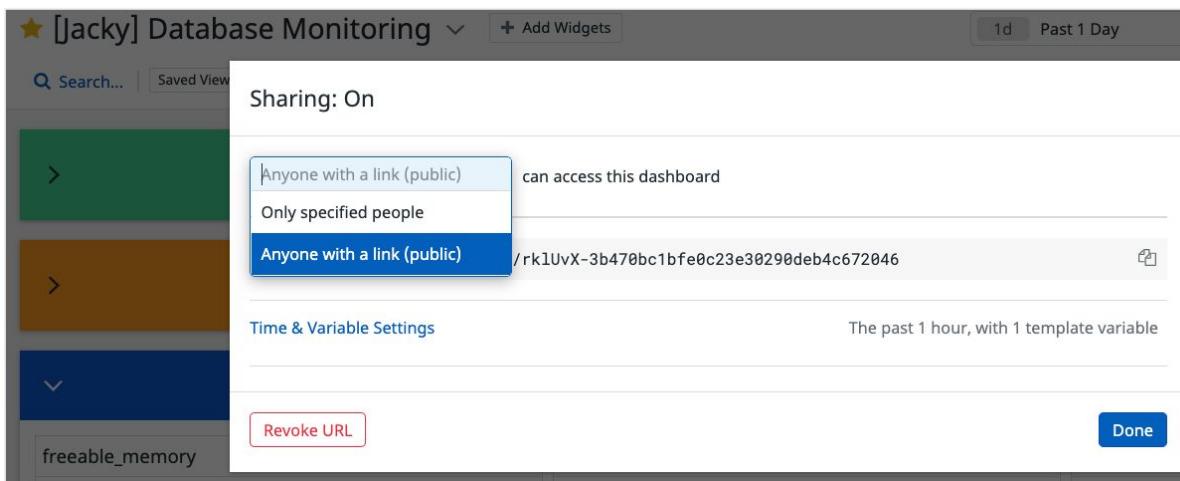
	Privileged Access	Standard Access	Read Only Access
This permission gives you the ability to view and edit components in your Datadog organization that do not have explicitly defined permissions. This includes Notebooks, Events, and other non-Account Management functionality.			
Additional Permissions			
Logs	read	write	other
Logs Read Index Data	<input type="checkbox"/>	.	.
Logs Modify Indexes	.	<input type="checkbox"/>	<input type="checkbox"/>
Logs Live Tail Access	<input type="checkbox"/>	.	.
Logs Write Exclusion Filters	.	<input type="checkbox"/>	.
Logs Write Pipelines	.	<input type="checkbox"/>	<input type="checkbox"/>
Log Write Processors	.	<input type="checkbox"/>	.
Logs Archives	<input type="checkbox"/>	<input type="checkbox"/>	.
Logs Public Config API	.	.	<input type="checkbox"/>
Log Generate Metrics	.	.	<input type="checkbox"/>
Logs Read Data	<input type="checkbox"/>	.	.
Logs Historical View	.	<input type="checkbox"/>	.
Logs Facets	.	<input type="checkbox"/>	.
Dashboards	read	write	other
Dashboards	<input checked="" type="checkbox"/>	<input type="checkbox"/>	.
Dashboards Share	.	.	<input type="checkbox"/>
Monitors	read	write	other
Monitors	<input checked="" type="checkbox"/>	<input type="checkbox"/>	.
Monitors Manage Downtimes	.	.	<input type="checkbox"/>
Security Monitoring	read	write	other
Detection Rules	<input type="checkbox"/>	<input type="checkbox"/>	.
Security Signals	<input type="checkbox"/>	<input type="checkbox"/>	.
Security Filters	<input type="checkbox"/>	<input type="checkbox"/>	.
Access Management	read	write	other
Invite User	.	.	<input type="checkbox"/>
Access Management	.	.	<input type="checkbox"/>
Service Accounts	.	<input type="checkbox"/>	.
Data Scanner	<input type="checkbox"/>	<input type="checkbox"/>	.

Datadog 접근 권한

Datadog 계정 초대 없이 Dashboard만 공유하고 싶은 경우라면?

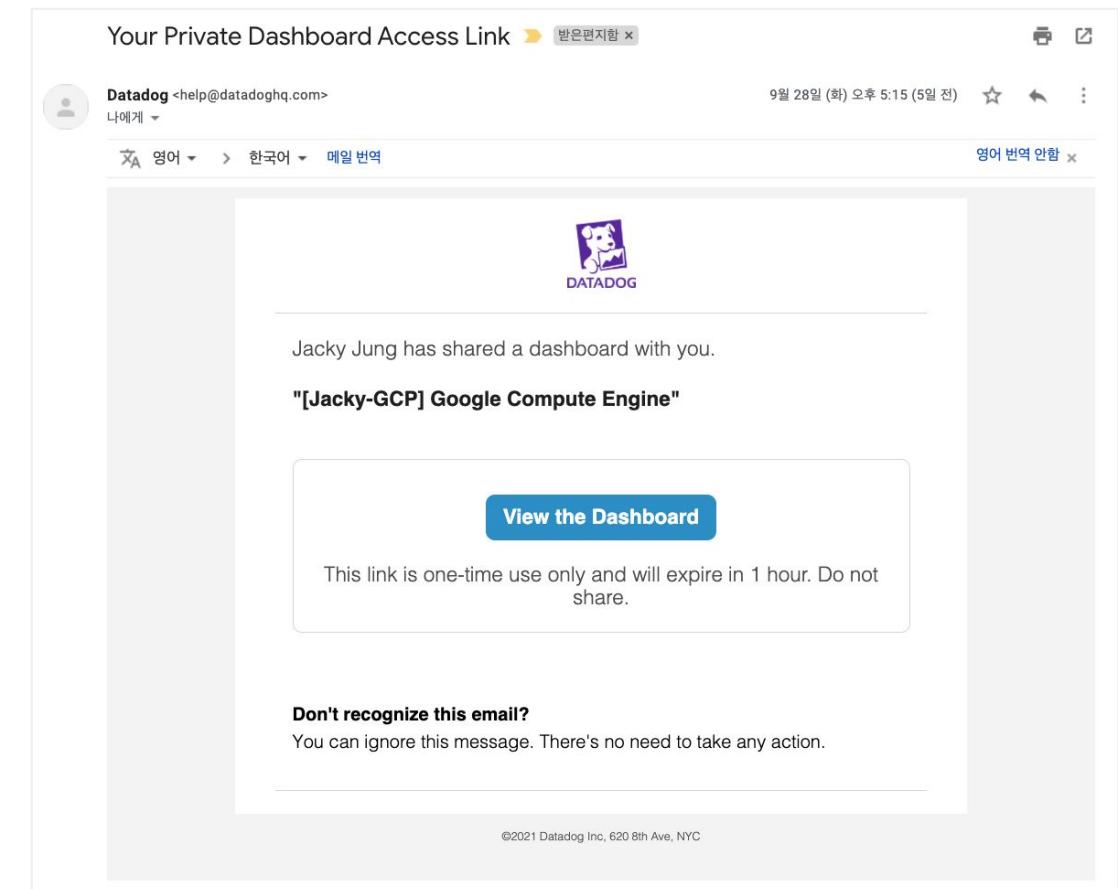
1. Dashboard를 Public share하여 URL을 통해 볼 수 있도록 제공

- Dashboard 화면 ⇒ 설정 ⇒ Configure Sharing 선택



2. Public Share가 보안상 우려가 된다면 Email 기반 인증 share를 활용

- One time Link를 이용해 담당자에게 안전하게 Dashboard 공유 가능



Infrastructure Monitoring

- 개요 및 설명
- 설치 및 구성 방법
- 최적화 사용 방안

1. Infrastructure Monitoring 개요

운영 엔지니어로부터 어떤 모니터링 니즈가 있을까요?

1. Host의 시스템 메트릭 수집

- CPU/Memory/Network/Disk

2. Process Monitoring

- 개별 Process에 대한 모니터링

3. Public Cloud에 대한 가시성 확보

- AWS/Azure/GCP 의 메트릭 수집
- Ex) Loadbalancer, PaaS DB, CDN 등

4. Container Orchestration 환경에서의 상태 메트릭 수집

- Container 시스템 자원
- K8S, EKS, AKS, GKE, ECS

5. 운영중인 솔루션의 Key Metric 수집

- K8S, Redis, NGINX, mysql 등

Q1. 다음의 운영 환경에서 Datadog은 무엇에 대해 과금을 할까요?
(선착순 두분께 Chat에 정답을 올려주신 분께 티셔츠를 제공해 드립니다)

1. EC2 100대 운영
2. EKS 클러스터 10대의 노드에 컨테이너 90개 정도 운영
3. 10개의 Fargate Task 운영
4. RDS 5대 운영
5. ALB 10대 운영

AWS 연동을 통해 EC2, RDS, ALB 메트릭을 수집하고, 각 Host와 Fargate Task에 Datadog 연동을 했을 때 어떤 항목에 과금을 할까요?

※) RDS 5대, 10대, Fargate 10대, ALB 10대, Container 90개

1.1 Host의 시스템 메트릭 수집

Integration ⇒ Agent ⇒ OS 선택하면 상세 가이드가 보입니다 ([링크](#))

- 모니터링을 희망하는 호스트에 아래 보이는 싱글라인 커맨드 이용해 Agent 설치 (바이너리 다운로드, 서비스 등록, 서비스 시작 진행)

Integrations Marketplace Developer Platform APIs Agent Embeds Enrichment Tables

See instructions for [Agent 6](#) or [Agent 5](#) instead

Agent 7 Installation Instructions

Installing on Amazon Linux

The Datadog Agent has x86_64 and arm64 (ARM v8) packages. For other architectures, use the [source install](#).

New installation

1 Use our easy one-step install.

```
DD_AGENT_MAJOR_VERSION=7 DD_API_KEY=[REDACTED] DD_SITE="datadoghq.com" bash -c "$(curl -L https://s3.amazonaws.com/dd-"
```

This will install the YUM packages for the Datadog Agent and will prompt you for your password.
If the Agent is not already installed on your machine and you don't want it to start automatically after the installation, just prepend `DD_INSTALL_ONLY=true` to the above script before running it.

Go to... Watchdog Events Dashboards Infrastructure Monitors Metrics Integrations

Overview Mac OS X Windows Debian Ubuntu Amazon Linux CentOS/Red Hat Fedora SUSE

참고 사항

- 업데이트를 희망하실 경우 동일 커맨드를 다시 실행하면 업데이트가 진행됩니다 (설정 파일은 그대로 유지)
- 마이너 버전에 대해 지정을 희망할 경우 `DD_AGENT_MINOR_VERSION` 옵션을 지정하여 실행합니다. ([Datadog agent version 참고](#))
- S3(s3.amazonaws.com)에 대해 https 접근이 불가능할 경우 인스톨 바이너리를 받아올 수 없어 Agent 설치가 불가능합니다
- 폐쇄망의 경우 바이너리를 Datacenter에 다운로드 받아 패키지 설치를 진행합니다 ([Package repo 참고](#))

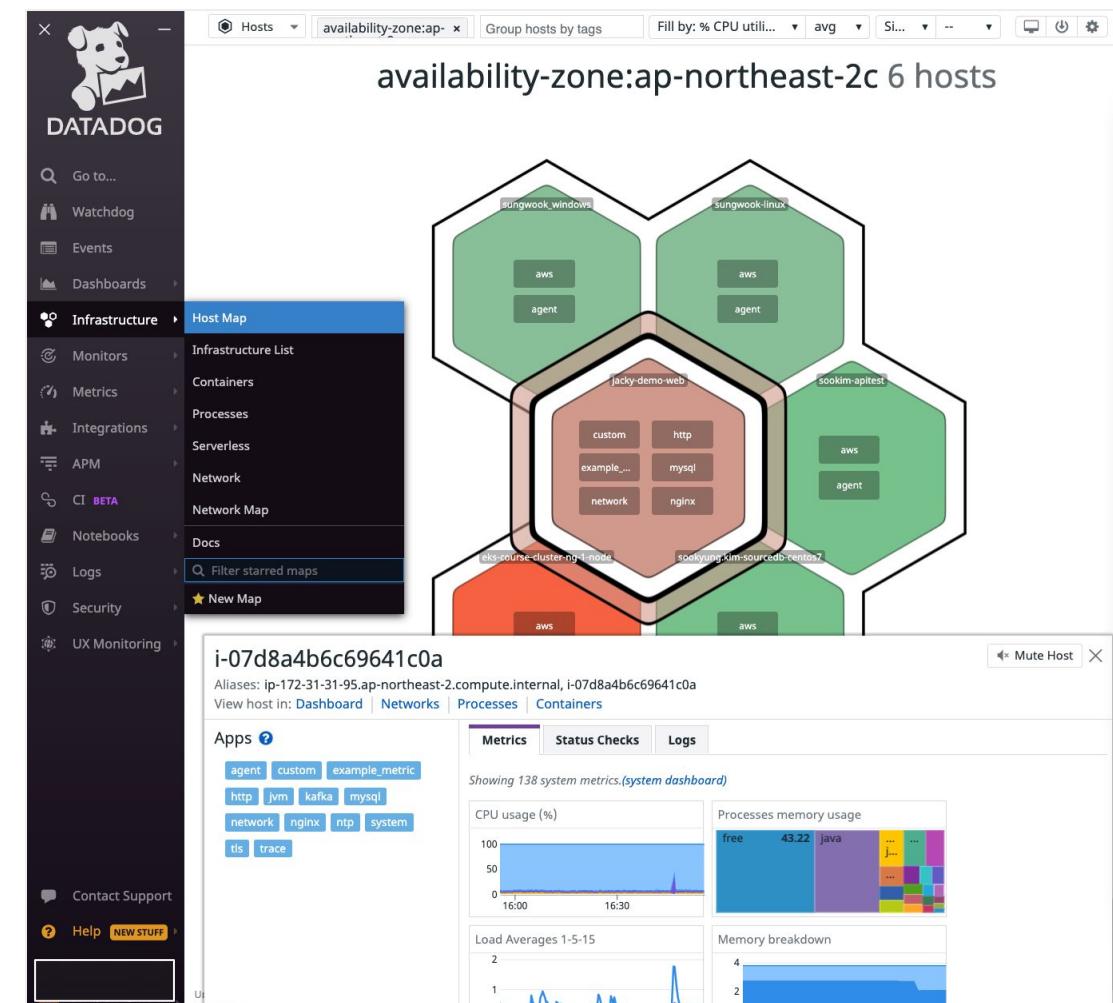
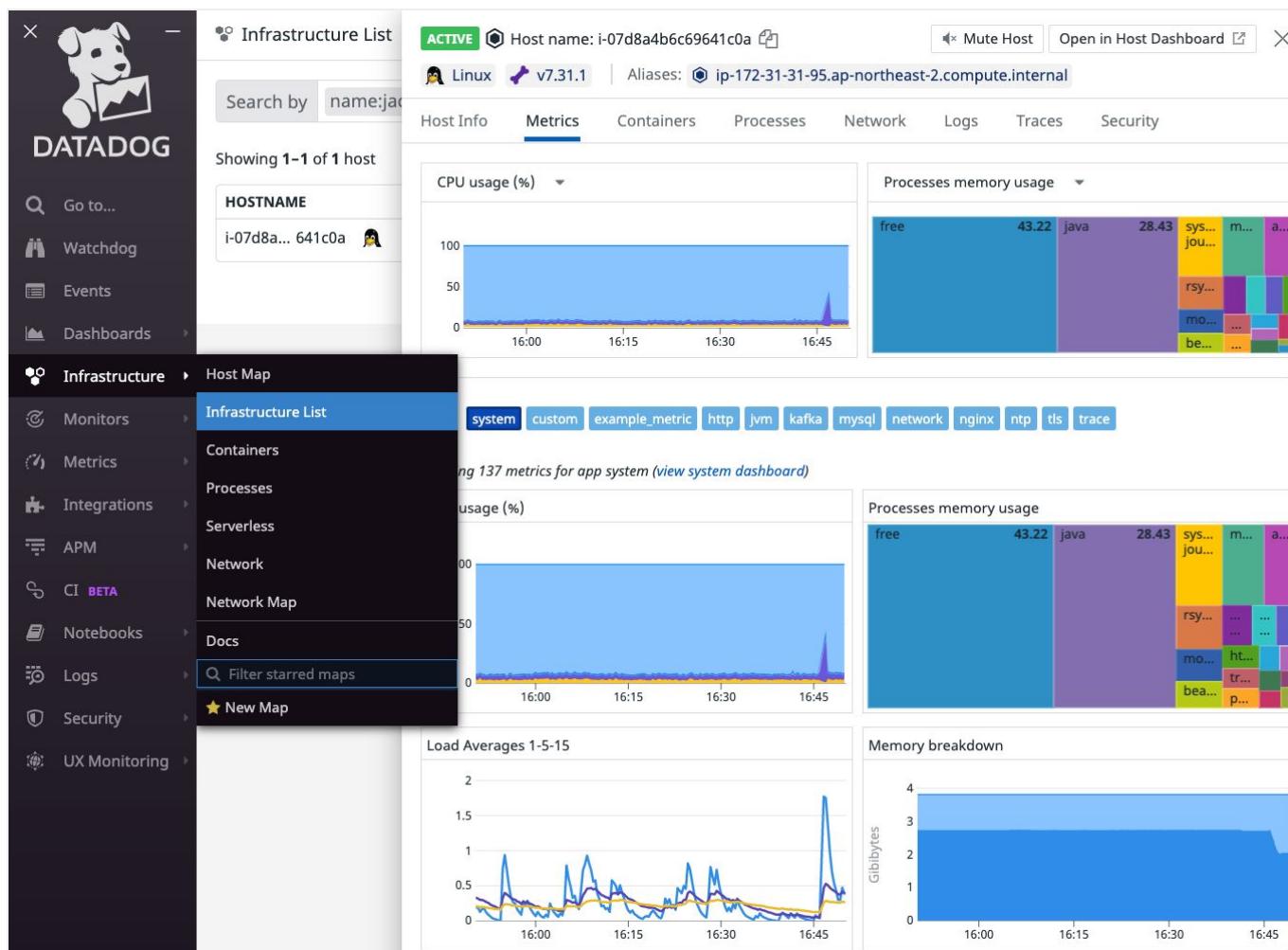
1.2 Host의 시스템 메트릭 (Agent 설치 후)

1) Infrastructure ⇒ Infrastructure List 를 통해 호스트 UP 확인

- 호스트에 대한 CPU, Memory, Disk, Network 등의 사용량에 대해 확인 가능
- Open in Host Dashboard를 통해 Time window 조정하여 메트릭 확인 가능
- 이후 로그, APM, NPM 등에 대해 연동시 각 Tab에서 연계 확인 가능

2) Infrastructure ⇒ Hostmap

- 각 호스트는 육각형으로 표현되고 메트릭 수치에 따라 다른 색으로 표시
- 어떤 호스트에서 리소스 사용량이 높은지 확인 후 디테일한 연동 메트릭 확인 가능



1.3 Host의 시스템 메트릭 리스트 및 Data point 확인

Metrics ⇒ Summary 를 통해 메트릭 리스트 및 tag 확인

- system.* 네임스페이스에 다양한 시스템 메트릭 수집 확인
- 함께 수집된 Tag 와 타임시리즈 그래프 확인

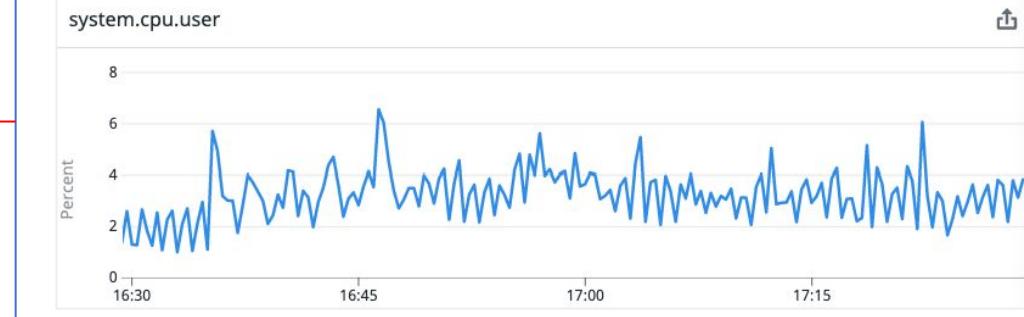
Q2. 여기보이는 system.* 메트릭은 몇 달 보관이 될까요? (선착순 티셔츠1)

정답: Datadog에 Metric 형태로 보관되는 정보는 15개월 유지가 됩니다

The screenshot shows the Datadog Metrics Summary page. On the left, the navigation bar has 'Metrics' selected under 'Metrics'. The main area displays a table of metrics under the heading 'All metrics reporting across your infrastructure in system'. One row is highlighted with a red box, showing 'system.io.r_s' as the metric name. A red arrow points from this row to the 'system.cpu.user' metric detail page on the right. The 'system.cpu.user' page shows details like 'DISTINCT METRICS REPORTED: 7', 'HOSTS: 6', and 'TAG VALUES: 28'. It also lists 'Metadata' and 'Tags' sections. The 'Tags' section is highlighted with a red box, showing a table of tag keys and their values. A red arrow points from this table to the 'Metric Explore' graph on the far right.

TAG KEY	COUNT	TAG VALUES
autoscaling_group	1	autoscaling_group:ec2containerservice-jacky-ecs-on-e...
availability-zone	2	availability-zone:ap-northeast-2a availability-zone:ap-northeast-2c
aws-account	1	aws-account:demo
aws	3	aws:cloudformation:logical-id:ecsinstanceasg aws:cloudformation:stack-id:arn:aws:cloudformation:... aws:cloudformation:stack-name:ec2containerservice-j...
cloud_name	1	cloud_name:jacky_vm
description	1	description:this_instance_is_the_part_of_the_auto_scali...
env	2	env:aws-dev env:mymac
iam_profile	1	iam_profile:ecsinstancerole
image	2	image:ami-0d097db2fb6e0f05e image:ami-0f611947480a24c88
instance-type	2	instance-type:t2.small instance-type:t3a.small

- Data point가 정상적으로 쌓이고 있는지 Metric Explore에서 확인 가능



- 원하는 Tag가 잘 수집되었는지 확인 가능 (자동수집 + Custom tag)
- Custom Tag는 /etc/datadog-agent/datadog.yaml 에 아래와 같이 정의 가능

```
## Learn more about tagging: https://docs.datadoghq.com/tagging/
tags:
  - env:aws-dev
  - team:devops
  - service:jacky-springboot-api
#   - <TAG_KEY>:<TAG_VALUE>
```

1.4 Host의 시스템 메트릭을 이용한 알람 설정

Monitor ⇒ New Monitor ⇒ Metric 선택

1) 지원되는 알람 방식

- Threshold Alert: 임계치 기반 알람
- Change Alert: 변화량 기반 알람
- Anomaly Detection: 특이사항 발생시 알람
- Outliers Alert: 서버 그룹중 혼자 사용량이 다른 경우 알람
- Forecast Alert: 예측치에 도달하기 X일 전에 알람이 필요할 경우 사용

2) 알람 생성 절차 (Threshold Alert 기준)

1. 메트릭 설정
2. 어떤 서버군에 적용할지 조건 지정
3. 임계치 설정
4. 알람 메시지 작성 (관련 대시보드와 같이 분석에 도움되는 정보 추가)
5. 수신자 설정 (Email, Slack, Webhook 등)

Manage Monitors Triggered Monitors Manage Downtime

New Monitor / Metric

4h Past 4 Hours

Percent

50
40
30
20
10
0

14:05:00 14:30 15:00 15:30 16:00 16:30 17:00 17:30

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

a Metric system.cpu.user from (everywhere) avg by host Σ [Source](#) [Edit](#) [Advanced...](#)

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

3. Set alert conditions

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

Alert threshold: > 40 (40 %)

Warning threshold: > Optional

Alert recovery threshold: <= Optional

Warning recovery threshold: <= Optional

1.5 메트릭 기반 알람 및 분석 예 (1/2)

1) 알람 조건 설정

4h Aug 4, 5:45 pm – Aug 4, 9:45 pm

Percent

> 50 %

45 % < y < 50 %

alert recovery

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

Metric aws.rds.cpuutilization from (everywhere) avg by dbinstanceidentifier

Trigger a separate alert for each dbinstanceidentifier reporting your metric

3 Set alert conditions

Trigger when the metric is above the threshold at least once during the last 5 minutes for any dbinstanceidentifier

Alert threshold: > 50 (50 %)

Warning threshold: > 45 (45 %)

4 Say what's happening

Include triggering tags in notification title

Edit Preview Markdown Help Use Message Template Variables

[jacky] RDS CPU 사용량이 높습니다.

다음의 Dashboard를 참고하여 확인 바랍니다.

- [Database 대시보드 링크](https://app.datadoghq.com/dashboard/wmd-kgw-9ya/jacky-database-monitoring?from_ts=1628006252161&to_ts=1628092652161&live=true)

- [기존 트러블 슈팅 Notebook 참고 Notebook](https://app.datadoghq.com/notebook/template/9/rfc-title)

@slack-jacky-demo-alert

2) 알람 메시지(Slack)를 통한 이슈 확인

Datadog APP 9:34 AM

Triggered: [jacky] RDS CPU 사용량이 높습니다. on dbinstanceidentifier:jacky-rds-mysql-test

다음의 Dashboard를 참고하여 확인 바랍니다.

- Database 대시보드 링크

- 기존 트러블 슈팅 Notebook 참고 Notebook

@slack-jacky-demo-alert

aws.rds.cpuutilization over dbinstanceidentifier:jacky-rds-mysql-test was > 50.0 at least once during the last 5m.

Metric value: 53.39 (12 kB)

Tags

Notified

dbinstanceidentifier:jacky-rds-mysql-test @slack-jacky-demo-alert

Percent

> 50 %

45 % < y < 50 %

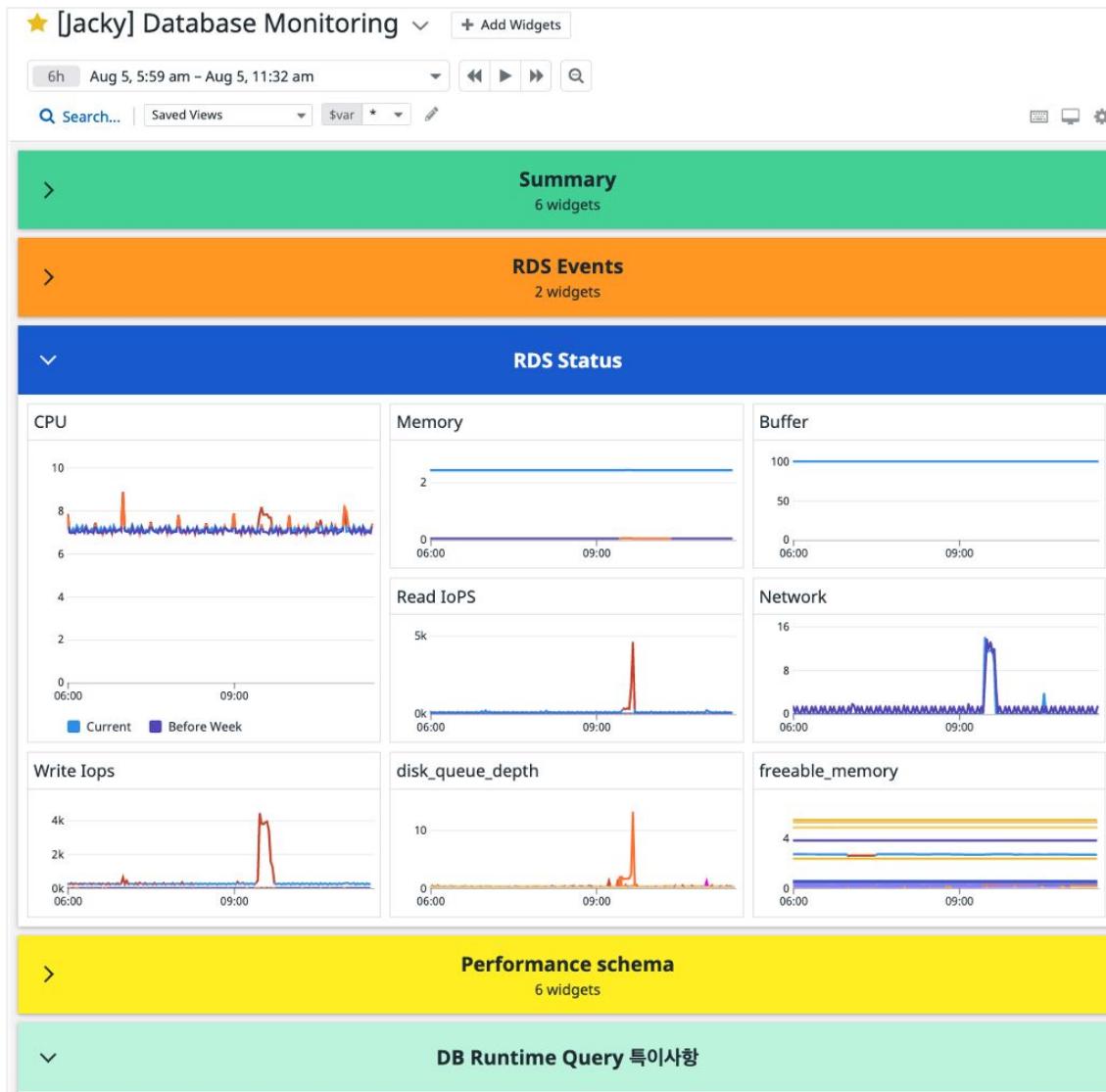
last 5m max: 53.39 %

alert recovery

00:10 00:15 00:20 00:25 UTC

1.5 메트릭 기반 알람 및 분석 예 (2/2)

3) 알람 메시지를 참고하여 연계 대시보드로 넘어와 분석



4) 장애 분석 내용을 Notebook에 정리하여 팀원과 협업

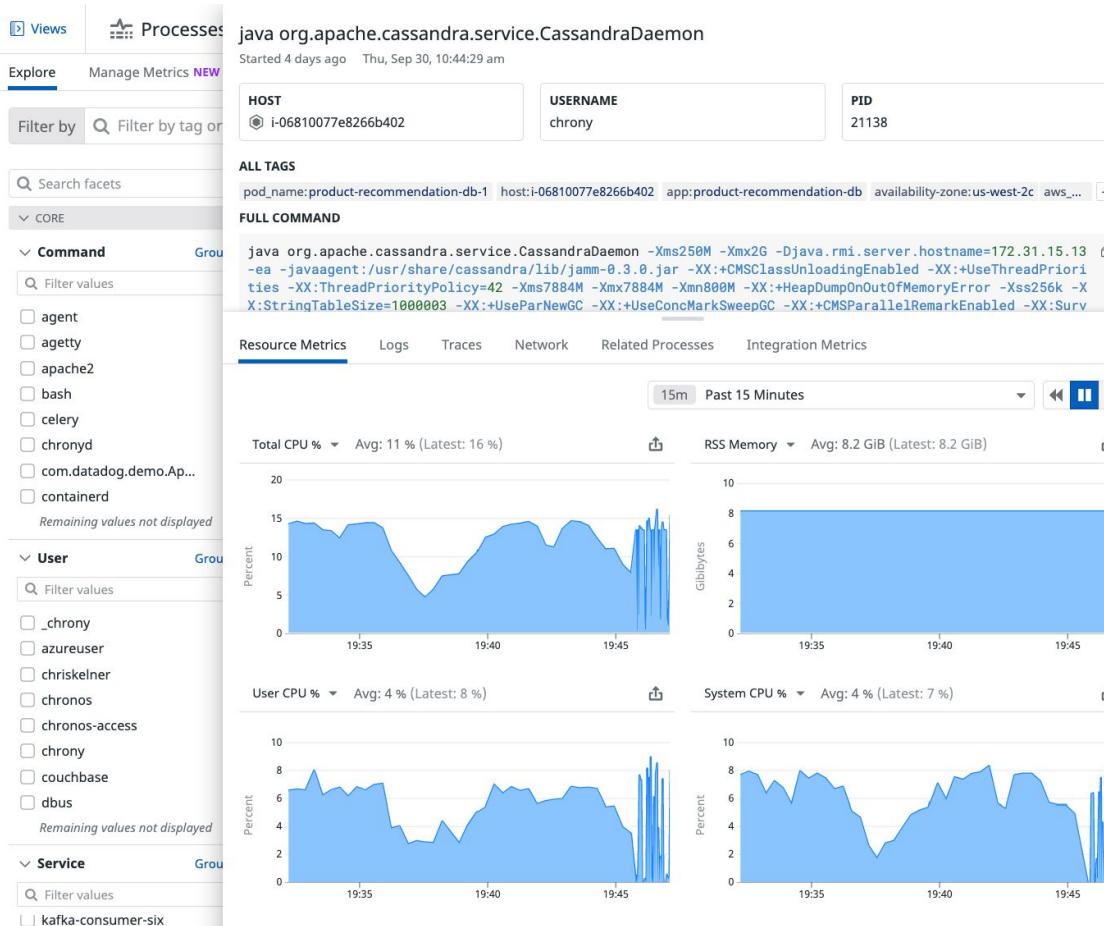


2.1 Process Monitoring 탑

개별 Process에 모니터링을 위해 다음의 2가지 Process Monitoring을 지원합니다

1) Live Process

- 호스트의 모든 Process의 리소스 사용량 및 Tag 수집
- 화면 진입 하면 2초단위 실시간 모니터링 진행
- 수집된 Live Process Data는 36시간 데이터 보관



2) Process Integration

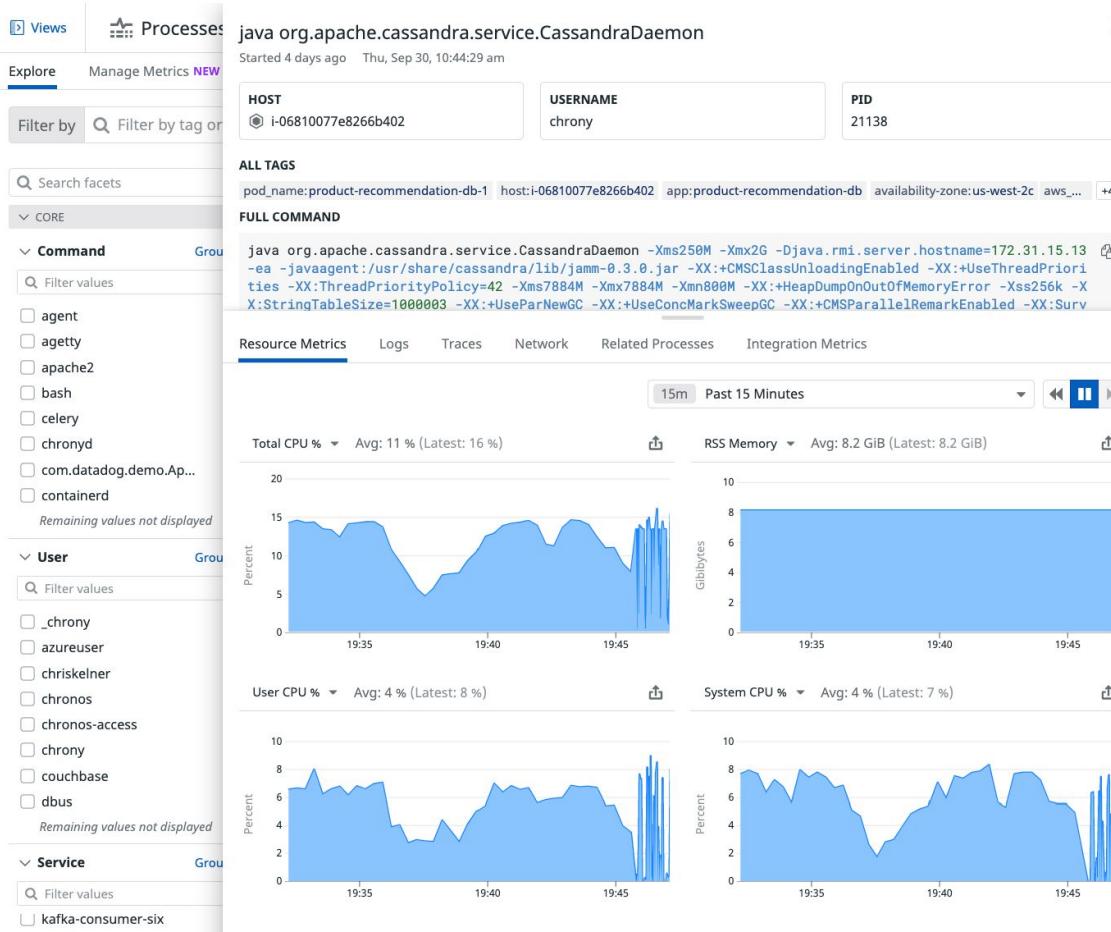
- 원하는 Process에 대해 Datadog 설정 파일에 명시하여 Process 메트릭 수집
- 수집 된 메트릭은 15개월 보관

METRIC NAME
system.processes.number
system.processes.cpu.pct
system.processes.mem.pct
system.processes.mem.rss
system.processes.mem.vms
system.processes.threads
system.processes.mem.real
system.processes.io.read.bytes
system.processes.io.read.count
system.processes.run_time.avg
system.processes.run_time.max
system.processes.run_time.min
system.processes.io.write.bytes
system.processes.io.write.count
system.processes.cpu.normalized_pct
system.processes.io.read.bytes.count
system.processes.io.write.bytes.count
system.processes.open_file_descriptors
system.processes.voluntary_ctx_switches
system.processes.involuntary_ctx_switches
system.processes.mem.page_faults.major_faults
system.processes.mem.page_faults.minor_faults
system.processes.mem.page_faults.children_major_faults
system.processes.mem.page_faults.children_minor_faults

2.2 Process Monitoring 설정

1) Live Process

- 호스트의 모든 Process의 리소스 사용량 및 Tag 수집
- 화면 진입 하면 2초단위 실시간 모니터링 진행
- 수집된 Live Process Data는 36시간 데이터 보관



설정 방법 (centos 예)

- 1) Datadog 설정 파일(/etc/datadog-agent/datadog.yaml)에 다음과 같이 설정

```
process_config:  
  enabled: 'true'
```

- 2) Agent 재시작

```
systemctl restart datadog-agent
```

- 3) 참고 링크

2.2 Process Monitoring 설정

2) Process Integration

- 원하는 Process에 대해 Datadog 설정 파일에 명시하여 Process 메트릭 수집
- 수집 된 메트릭은 **15개월** 보관

The screenshot shows the Datadog Metrics Explorer interface. The search bar at the top right contains the query "system.processes.cpu.pct". Below the search bar, there are sections for "DISTINCT METRICS REPORTED" (3), "HOSTS" (1), and "TAG VALUES" (20). The main content area includes sections for "Configuration", "Metric Type", and "Tags". The "Tags" section lists 15 tag keys, including "availability-zone", "aws-account", "cloud_name", "env", "image", "instance-type", "instance_id", "kernel", "name", "process_name", "region", and "security-group". The "process_name" section highlights three entries: "process_name:java-springboot", "process_name:java_commands", and "process_name:spring_boot_process".

설정 방법 (centos 예)

- 1) Process 설정 파일(/etc/datadog-agent/conf.d/process.d/conf.yaml)에 다음과 같이 설정

```
init_config:  
  
instances:  
  - name: spring_boot_process  
    search_string: ["java"]
```

- 2) Agent 재시작

```
systemctl restart datadog-agent
```

- 3) 참고 링크

3. Public Cloud Integration

Cloud Provider 별 주요 서비스에 대한 Integration을 제공하여 계정 연동만으로 주요 메트릭 수집이 가능합니다

- 메트릭은 Datadog Crawler 기반으로 수집됩니다
- Crawler는 기본 AWS 10분, Azure 5분, GCP 5분 주기로 수집 됩니다
- 필요시 Support(support@datadoghq.com) 팀을 통해 2분, 5분, 10분 등의 주기로 변경이 가능합니다.

AWS Integrations

Azure Integrations

GCP Integrations

3.1 AWS Integration 설정 방법 (Step1)

- Datadog Portal의 AWS Integration [페이지](#)에서
- Automatically Using CloudFormation 선택 후
- 기대 결과
 - 자동으로 Role 생성하는 페이지로 이동

Amazon Web Services Integration

Amazon Web Services (AWS) is a collection of web services that together make up a cloud computing platform.

✓ INSTALLED

Overview Configuration Metrics Collect Logs

This integration is working properly.

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

Datadog uses CloudWatch APIs to monitor your AWS resources every 10 minutes. See the [AWS Integration FAQ](#) for more information.

Enabling the AWS X-Ray Integration increases the amount of Indexed Spans which can impact your bill.

Preferences for all accounts

Silence monitors for expected EC2 instance shutdowns

EC2 automating ?

Limit metric collection by AWS Service

Turning on subintegrations can affect your CloudWatch API usage. See our [AWS FAQ](#) for more info.

ApiGateway
 ApplicationELB
 AppStream
 AppSync
 Athena
 AutoScaling
 Billing
 Budgeting
 CloudFront
 CloudHSM
 CloudSearch
 CodeBuild
 Cognito

AWS Accounts

You have 3 ways to integrate your AWS accounts into Datadog for metric, trace, and log collection. Via Role Delegation you have two options: 1) Use our CloudFormation template to automatically setup the necessary AWS Role (Recommended), 2) Manually create the necessary role and copy the required credentials in the respective form. For GovCloud and AWS China instances, you must use Access Keys. You can find more information on our AWS Integration in our [documentation](#).

Account: New Account

Role Delegation Access Keys (GovCloud or China Only)

Choose a method for setting up the necessary AWS role (we recommend using CloudFormation).

If using the automatic setup, complete the CloudFormation launch process in AWS, and then insert the AWS account ID and generated role name back in this form when completed.

Automatically Using CloudFormation **Manually**

Remove Account

3.1 AWS Integration 설정 방법 (Step2)

- Datadog API Key 입력 후 Create stack 클릭
- 기대 결과
 - AWS 계정 연동 위한 Role 생성
 - AWS에 적재된 로그 전송위한 Lambda 생성

CloudFormation > Stacks > Create stack

Quick create stack

Template

Template URL
<https://datadog-cloudformation-template.s3.amazonaws.com/aws/main.yaml>

Stack description
Datadog AWS Integration

Stack name

Stack name
datadog

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

Required

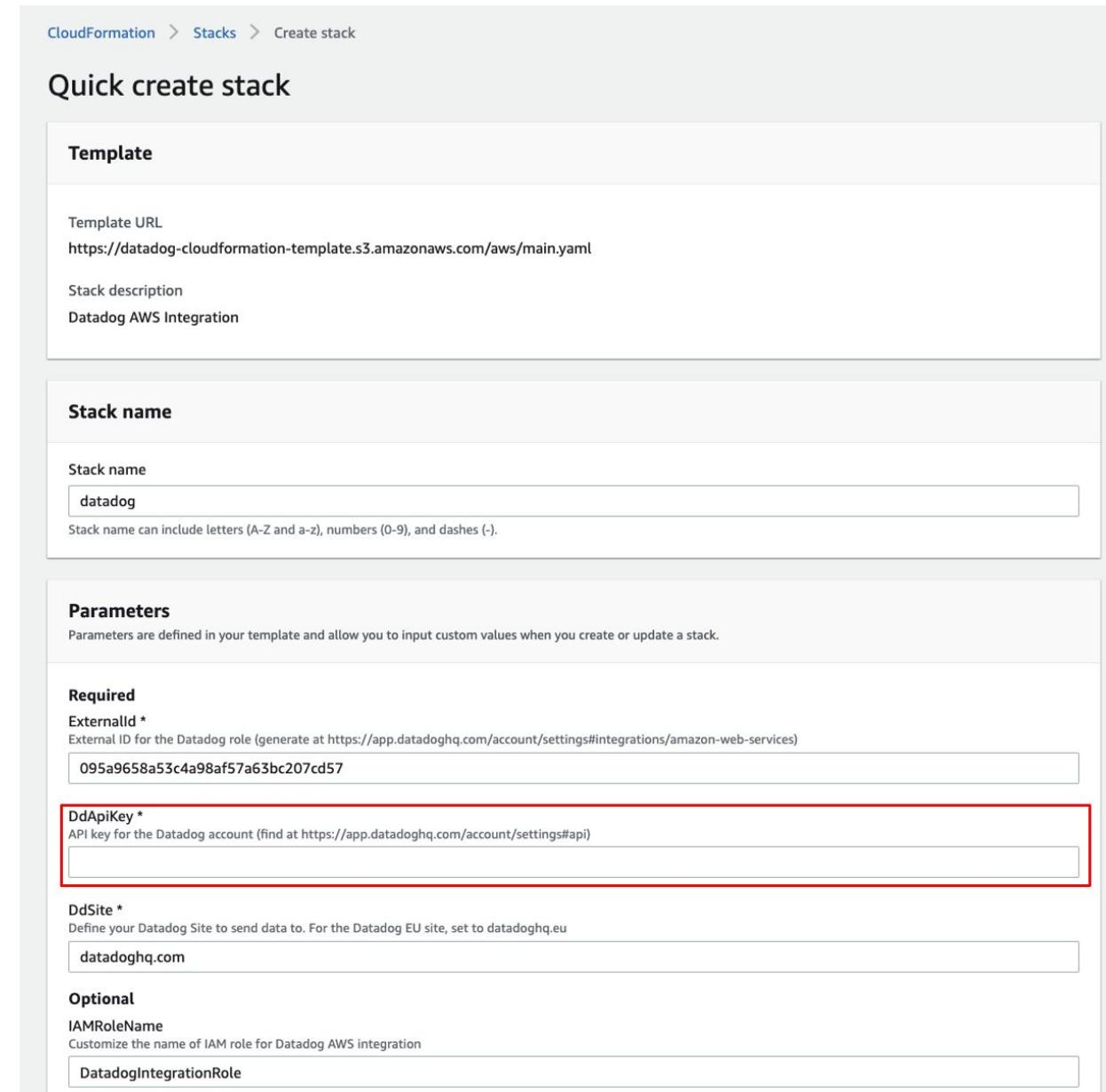
ExternalId *
External ID for the Datadog role (generate at <https://app.datadoghq.com/account/settings#integrations/amazon-web-services>)
095a9658a53c4a98af57a63bc207cd57

DdApiKey *
API key for the Datadog account (find at <https://app.datadoghq.com/account/settings#api>)

DdSite *
Define your Datadog Site to send data to. For the Datadog EU site, set to datadoghq.eu
datadoghq.com

Optional

IAMRoleName
Customize the name of IAM role for Datadog AWS integration
DatadogIntegrationRole



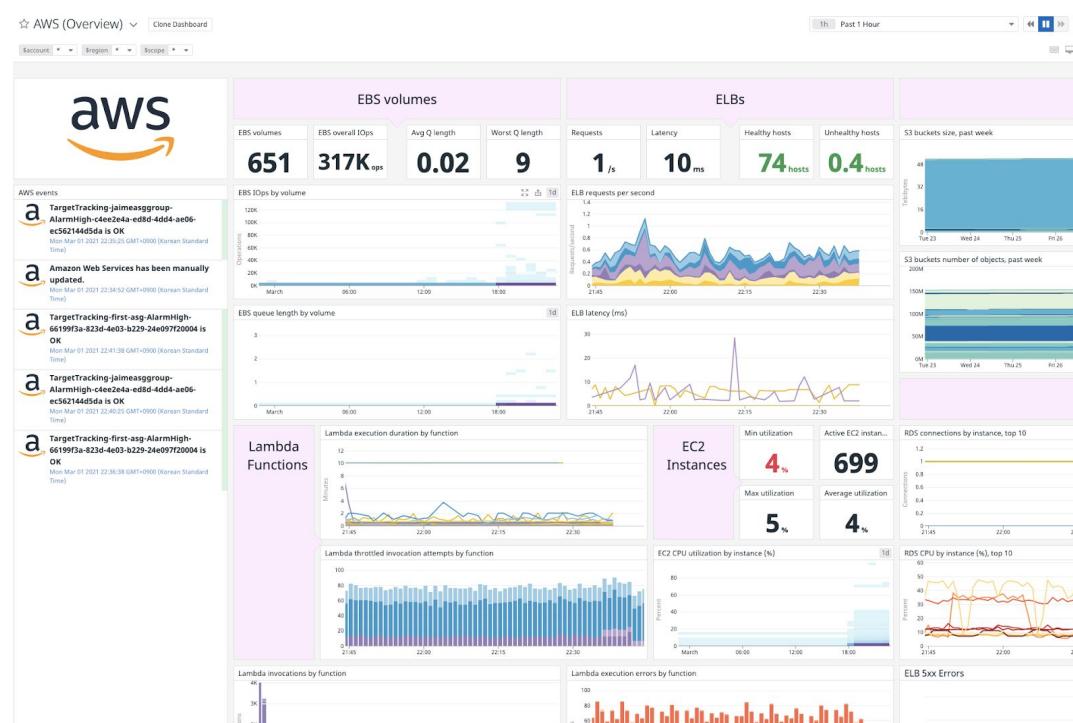
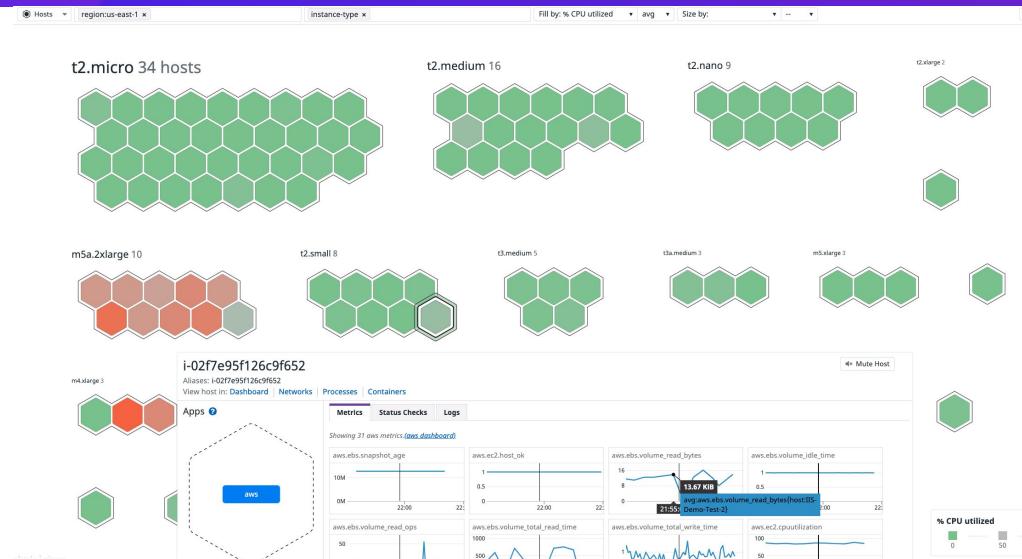
3.1 AWS Integration 설정 방법 (Step3)

- AWS Account ID 입력
- Step 2에서 생성된 Role 입력 후 Update
- 기대 결과
 - AWS 연동 완료
 - 5~10분 후 AWS 대시보드 통해 메트릭 확인

The screenshot shows the Datadog AWS Integration configuration interface. At the top, the AWS logo is displayed with a green 'INSTALLED' button. Below the logo, there are tabs for 'Overview', 'Configuration' (which is selected), 'Metrics', and 'Collect Logs'. A green banner at the top states 'This integration is working properly.' Below this, a note about billing and monitoring frequency is present. On the left, under 'Preferences for all accounts', there are sections for 'Silence monitors for expected EC2 instance shutdowns' (with an 'EC2 automuting' checkbox) and 'Limit metric collection by AWS Service' (with a list of services like ApiGateway, ApplicationELB, CloudFront, etc., many of which have checkboxes). On the right, under 'AWS Accounts', it says you have three ways to integrate AWS accounts into Datadog. It highlights 'Role Delegation' as the recommended method, mentioning CloudFormation support and manual role creation for GovCloud and AWS China instances. It also mentions the use of Access Keys for these regions. Below this, a 'New Account' section is shown with fields for 'AWS Account ID' (containing '123456781234'), 'AWS Role name' (containing 'e.g. DatadogIntegrationRole'), and 'AWS External ID' (containing '095a9658a53c4a98af57a63bc207cd57'). Buttons for 'Generate New ID' and 'Remove Account' are also visible.

3.2 AWS Integration 연동 완료 후

- 다양한 Preset Dashboard가 생성됨
 - EC2
 - EBS
 - ALB
 - RDS
 - 그외 다양한 AWS 서비스
- Clone 후 자유롭게 대시보드 조합 가능



3.3 AWS Integration 연동 Best practice

Silence monitors for expected EC2 instance shutdowns

EC2 automuting

Limit metric collection by AWS Service

Turning on subintegrations can affect your CloudWatch API usage. See our [AWS FAQ](#) for more info.

ApiGateway

ApplicationELB

AppRunner

AppStream

AppSync

Athena

AutoScaling

Billing

Budgeting

CertificateManager

CloudFront

CloudHSM

CloudSearch

CodeBuild

Cognito

Connect

Other options

Collect CloudWatch alarms

Collect custom metrics

You have 3 ways to integrate your AWS accounts into Datadog for metric, trace, and log collection. Via Role Delegation you have two options: 1) Use our CloudFormation template to automatically setup the necessary AWS Role (Recommended), 2) Manually create the necessary role and copy the required credentials in the respective form. For GovCloud and AWS China instances, you must use Access Keys. You can find more information on our AWS Integration in our [documentation](#).

Account: 112560794 Tags: aws_account:1125

Role Delegation Access Keys (GovCloud or China Only)

AWS Account ID: 1125 AWS Role name: DatadogIntegrationRole AWS External ID: ***** Tags: aws_account:1125 Generate New ID

Metric Collection

CloudWatch APIs CloudWatch Metric Streams

Enable or disable metric collection via API for specific namespaces. Metric collection via API is automatically disabled for any namespace sending metrics via streaming.

No namespace collection rules exist for this account.

Add an Account-Specific Namespace Rule

Optionally limit resource collection

to hosts with tag: key:value

to Lambdas with tag: key:value

1. 사용하는 서비스만 메트릭을 수집하도록 체크하세요

- 체크가 되어 있으면 기본적으로 CloudWatch API를 호출합니다

2. AWS Integration과 더불어 Agent도 함께 설치가 권장됩니다

- 둘다 연동해도 1대에 대해서만 과금합니다
- AWS 연동시 AWS에 설정한 Tag 정보도 호스트 모니터링 시 활용이 가능합니다
- Agent는 15초 단위의 정밀한 메트릭이 수집되므로 상세 분석을 위해서는 Agent를 함께 설치가 권장 됩니다.

3. 서비스 성격에 맞춰 AWS Integration 수집 주기를 조절하세요

- Integration 수집 주기는 기본 10분입니다 (RDS 3분)
- PaaS 서비스에 대해 알람 지연을 줄이기 위해서는 AWS Integration 수집 주기를 5분으로 줄일 수 있습니다. (Cloudwatch 비용 증가)
 - 2분도 가능하지만 Cloudwatch 비용 증가 관점에서 권고하지 않습니다

4. 모니터링이 필요없는 호스트는 limit 옵션을 활용해 제외하세요

- tag를 이용하여 EC2 메트릭 수집에서 제외가 가능합니다.
- 기본은 모든 EC2에 대해 수집하는것이므로 불필요하게 모니터링되고 있는 호스트가 있지 않은지 점검이 필요합니다
- 예) datadog_monitor:true tag를 EC2에 넣어 whitelist 기반 관리 가능

4. Container Orchestration 환경에서의 상태 메트릭 수집

1) Kubernetes 환경에서 모니터링이 필요한 부분

1. Cluster Node 리소스 사용량
2. Pod/Container 리소스 사용량
3. Kubernetes Event
4. Application의 Trace 수집
5. Log

수집 방법

- Datadog Agent
- Datadog Trace 라이브러리
- AWS Integration

2) ECS on EC2에서 모니터링이 필요한 부분

1. ECS Cluster 리소스 사용량
2. ECS Service 리소스 사용량
3. ECS Container 리소스 사용량
4. Application의 Trace 수집
5. Log

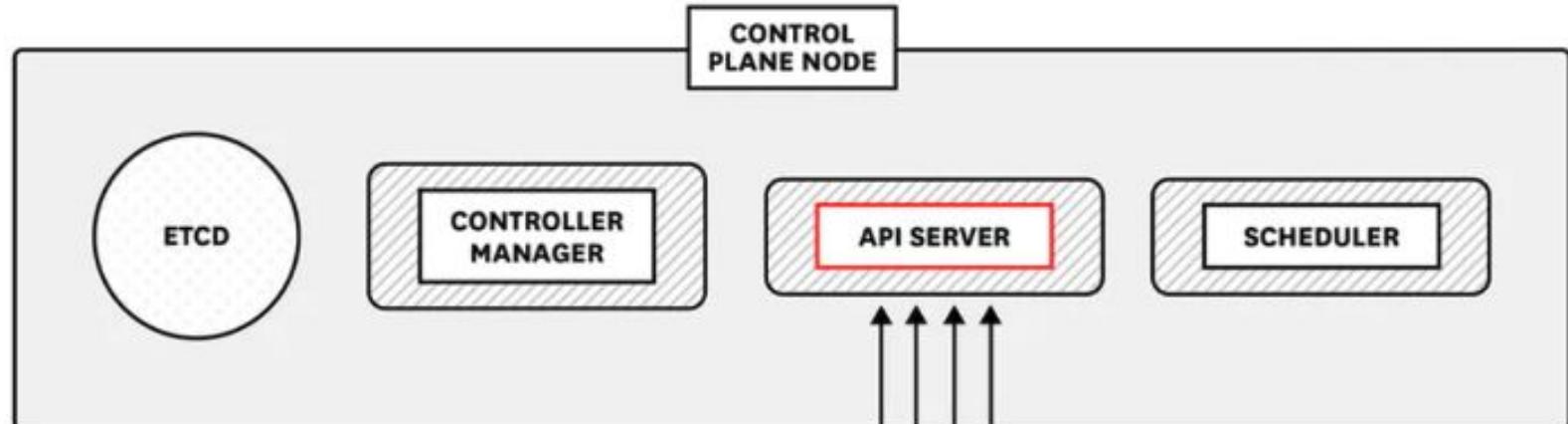
3) ECS on Fargate 모니터링이 필요한 부분

1. Container 리소스 사용량
2. Application의 Trace 수집
3. Log (firelens나 Cloudwatch log를 통해 Datadog으로 수집)

4.1.1 Kubernetes Monitoring 아키텍쳐

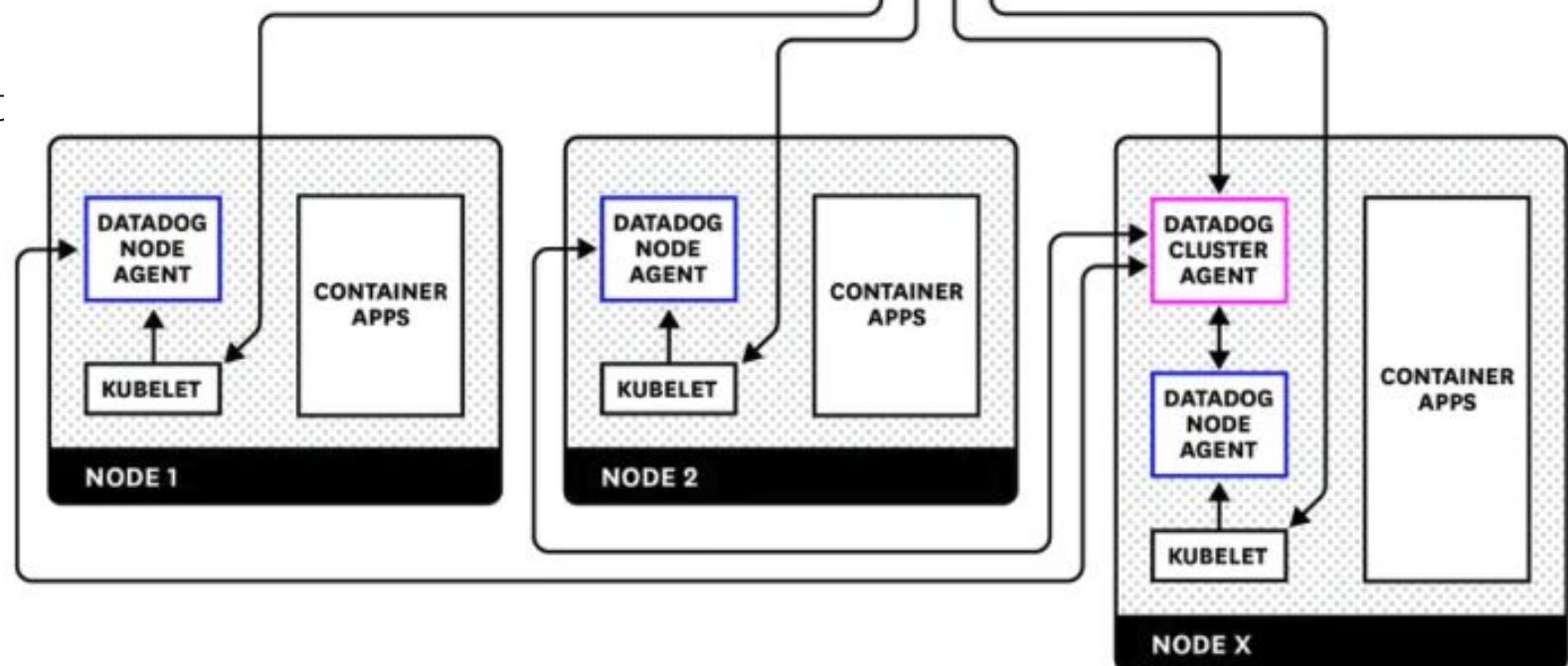
Datadog Node Agent

- ❑ Daemonset으로 배포
- ❑ Node/Pod/Container 메트릭 수집
- ❑ Log 및 APM Trace 수집
- ❑ Kubernetes Event 수집



Datadog Cluster Agent

- ❑ Deployment로 배포
- ❑ API 서버로의 통신을 담당(Node Agent의 요청)
- ❑ HPA에 Custom한 메트릭 사용 지원



4.1.2 Datadog Kubernetes Integration

공식 설치 가이드 페이지

Helm DaemonSet Operator

To install the chart with a custom release name, <RELEASE_NAME> (e.g. datadog-agent):

1. Install Helm.
2. Using the Datadog values.yaml configuration file as a reference, create your `values.yaml`. Datadog recommends that your `values.yaml` only contain values that need to be overridden, as it allows a smooth experience when upgrading chart versions.
3. If this is a fresh install, add the Helm Datadog repo:

```
helm repo add datadog https://helm.datadoghq.com  
helm repo update
```

4. Retrieve your Datadog API key from your Agent installation instructions and run:

- **Helm v3+**

```
helm install <RELEASE_NAME> -f values.yaml --set datadog.apiKey=<DATADOG_API_KEY> datadog/datadog --set targetSystem=<TARGET_SYSTEM>
```

Replace <TARGET_SYSTEM> with the name of your OS: `linux` or `windows`.

- **Helm v1/v2**

```
helm install -f values.yaml --name <RELEASE_NAME> --set datadog.apiKey=<DATADOG_API_KEY> datadog/datadog
```

Note

1. helm이 현재는 Recommended 설치 방법입니다
2. 다음의 링크를 통해 제가 사용한 샘플 helm chart도 참고하시면 도움이 됩니다
 - https://github.com/JungYoungseok/datadog/blob/master/kubernetes_yaml/values.yaml
 - Metric, Process Monitoring, NPM, Log, APM 활성화

4.1.3 Datadog Kubernetes Integration 실행 예

샘플 helm chart 배포 후 결과 화면(1/3)

```
jacky.jung@COMP11458:~/AWS_Summit_2021|→ helm install -f values.yaml --name datadog-monitoring --set datadog.apiKey=e30d7c5c44c043e4470f --set datadog.appKey=ddacbeaea9022a1d8c930ddb08b0 datadog/datadog
NAME: datadog-monitoring
LAST DEPLOYED: Fri Mar 5 01:59:19 2021
NAMESPACE: default
STATUS: DEPLOYED

RESOURCES:
==> v1/APIService
NAME                                     AGE
v1beta1.external.metrics.k8s.io  0s

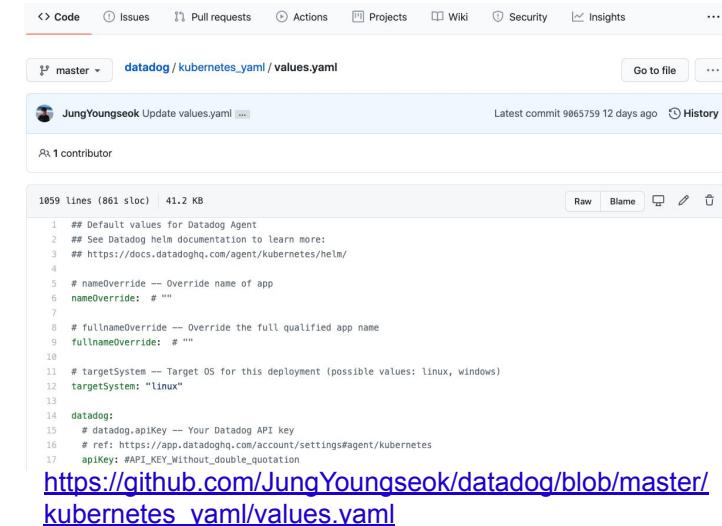
==> v1/ClusterRole
NAME                                     AGE
datadog-monitoring                      1s
datadog-monitoring-cluster-agent          1s
datadog-monitoring-cluster-agent-external-metrics-reader 1s

==> v1/ClusterRoleBinding
NAME                                     AGE
datadog-monitoring                      0s
datadog-monitoring-cluster-agent          0s
datadog-monitoring-cluster-agent-external-metrics-reader 0s
datadog-monitoring-cluster-agent:system:auth-delegator 0s

==> v1/ConfigMap
NAME          DATA   AGE
datadog-monitoring-installinfo           1    1s
datadog-monitoring-security              1    1s
datadog-monitoring-system-probe-config  1    1s

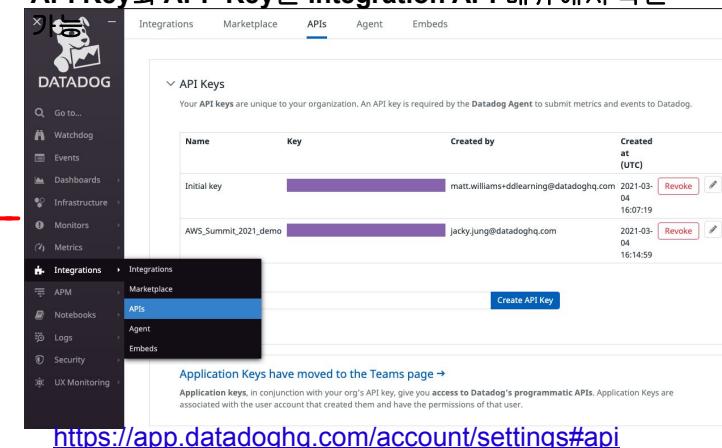
==> v1/DaemonSet
NAME      DESIRED  CURRENT  READY  UP-TO-DATE  AVAILABLE  NODE SELECTOR          AGE
datadog-monitoring  2        2        0       2           0          kubernetes.io/os=linux  0s
```

Helm chart는 아래 sample Chart 사용



The screenshot shows a GitHub repository page for 'datadog / kubernetes.yaml / values.yaml'. It displays the YAML configuration for the Datadog monitoring stack. Key sections include 'datadog' (with API and app keys), 'targetSystem' set to 'linux', and 'integrations' like 'Metrics' and 'Logs'. A link at the bottom points to the original source: https://github.com/JungYoungseok/datadog/blob/master/kubernetes_yaml/values.yaml.

API Key와 APP Key는 Integration API 메뉴에서 확인



4.1.3 Datadog Kubernetes Integration 실행 예

샘플 helm chart 배포 후 결과 화면(2/3)

==> v1/Deployment					
NAME	READY	UP-TO-DATE	AVAILABLE	AGE	
datadog-monitoring-cluster-agent	0/1	1	0	0s	
datadog-monitoring-kube-state-metrics	0/1	1	0	0s	
==> v1/Pod(related)					
NAME	READY	STATUS	RESTARTS	AGE	
datadog-monitoring-79mbn	0/4	Init:0/3	0	0s	
datadog-monitoring-cluster-agent-64cbff9499-qfd6x	0/1	Pending	0	0s	
datadog-monitoring-kube-state-metrics-6d5c7b57b9-j5wdm	0/1	Pending	0	0s	
datadog-monitoring-qrsvg	0/4	Init:0/3	0	0s	
==> v1/RoleBinding					
NAME	AGE				
datadog-monitoring-cluster-agent	0s				
==> v1/Secret					
NAME	TYPE	DATA	AGE		
datadog-monitoring	Opaque	1	1s		
datadog-monitoring-appkey	Opaque	1	1s		
datadog-monitoring-cluster-agent	Opaque	1	1s		
==> v1/Service					
NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
datadog-monitoring-cluster-agent	ClusterIP	10.100.108.7	<none>	5005/TCP	0s
datadog-monitoring-cluster-agent-metrics-api	ClusterIP	10.100.171.206	<none>	8443/TCP	0s
datadog-monitoring-kube-state-metrics	ClusterIP	10.100.105.31	<none>	8080/TCP	0s
==> v1/ServiceAccount					
NAME	SECRETS	AGE			
datadog-monitoring	1	1s			
datadog-monitoring-cluster-agent	1	1s			
datadog-monitoring-kube-state-metrics	1	1s			

4.1.3 Datadog Kubernetes Integration 실행 예

샘플 helm chart 배포 후 결과 화면(3/3)

```
==> v1beta1/ClusterRole
NAME          AGE
datadog-monitoring-kube-state-metrics  1s

==> v1beta1/ClusterRoleBinding
NAME          AGE
datadog-monitoring-kube-state-metrics  0s
```

NOTES:

Datadog agents are spinning up on each node in your cluster. After a few minutes, you should see your agents starting in your event stream:

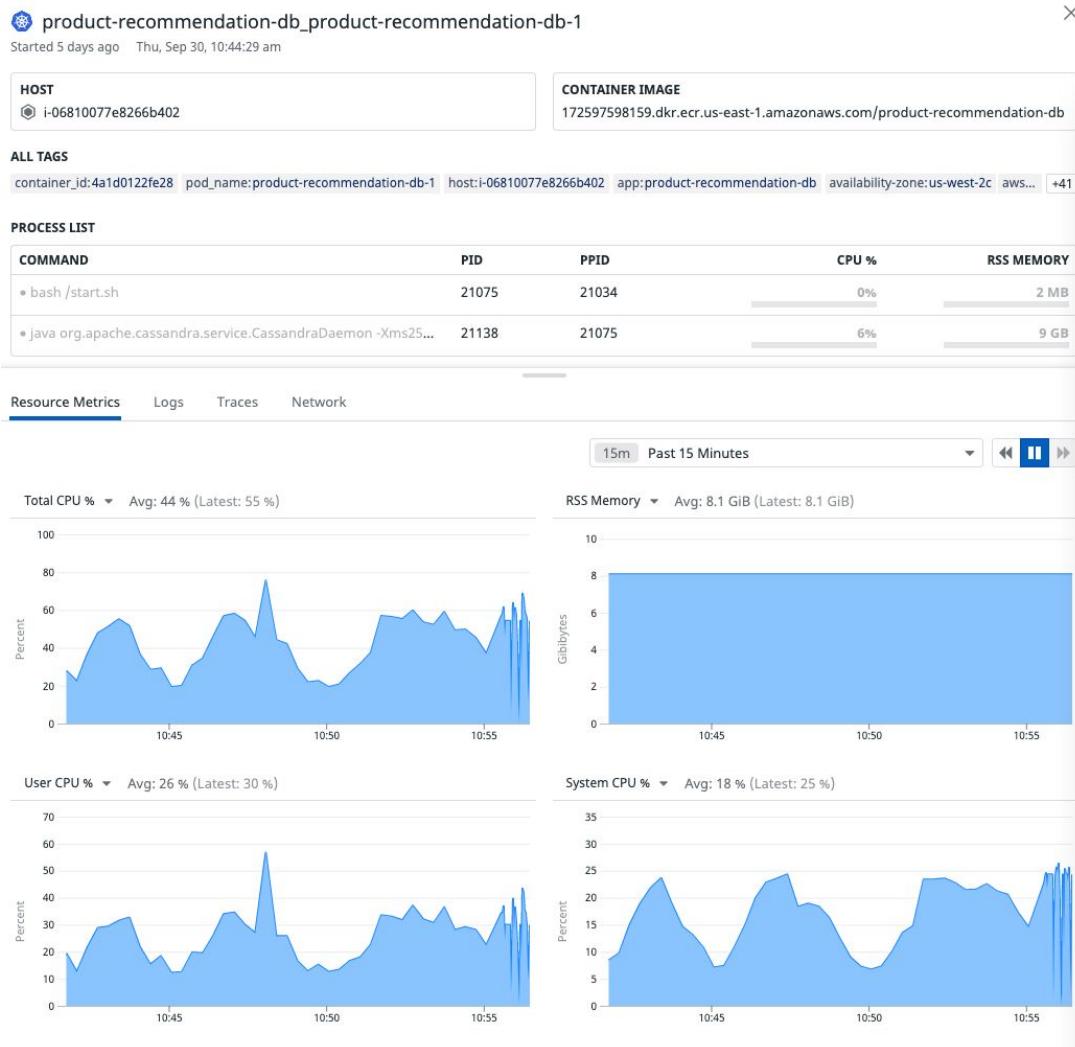
<https://app.datadoghq.com/event/stream>

The Datadog Agent is listening on port 8126 for APM service.

```
[jacky.jung@COMP11458:~/AWS_Summit_2021] => kubectl get pods
NAME                           READY   STATUS    RESTARTS   AGE
advertisements-dcff6b4bd-z7k5r   1/1     Running   0          2d16h
datadog-monitoring-79mbn        4/4     Running   0          4m46s
datadog-monitoring-cluster-agent-64cbff9499-qfd6x  1/1     Running   0          4m46s
datadog-monitoring-kube-state-metrics-6d5c7b57b9-j5wdm  1/1     Running   0          4m46s
datadog-monitoring-qrsvg         4/4     Running   0          4m46s
db-56ct8c59b5-mkjrc            1/1     Running   0          5d1h
deployment-2048-6754c747b4-921lk  2/2     Running   0          2d5h
discounts-5c996dfc49-5k99j       1/1     Running   0          2d16h
frontend-6888f67fcc-xkxsf        1/1     Running   0          3d
store-frontend-6ffffd84-vt8wb      1/1     Running   0          2d16h
[jacky.jung@COMP11458:~/AWS_Summit_2021] =>
```

4.1.4 Kubernetes Integration을 통해 확인할 수 있는 부분 (1/3)

1. Container 레벨 가시성 + Process 정보



2. Pod Level 가시성

The screenshot shows the Kubernetes Pod details page for the pod `ad-auction-2-6969db6b89-2h8kd`. It includes:

- POD STATUS:** RUNNING
- POD DETAILS:** READY: 1/1, RESTARTS: 0, AGE: 5 days, IP: 10.48.10.117, NODE: gke-demo-11287-us-prod-west-pool-2-2b19f4ee-lvjs, NAMESPACE: default, QOS: Burstable.
- TAGS:** app:ad-auction-2, automatic-restart:true, availability-zone:us-west1-b, chart_name:dd-trace-demo, cloud_provider:gcp, cluster_location:us-west1-a, cluster_name:dd-trace-demo, pod-template-hash:6969db6b89, service:ad-auction, tags.datadoghq.com/env:prod, tags.datadoghq.com/service:ad-auction, tags.datadoghq.com/version:74d775d7, team:ads.
- KUBERNETES LABELS:** app:ad-auction-2, chart_name:dd-trace-demo, pod-template-hash:6969db6b89, service:ad-auction, tags.datadoghq.com/env:prod, tags.datadoghq.com/service:ad-auction, tags.datadoghq.com/version:74d775d7, team:ads.
- VIEW RELATED:** Containers
- CONTAINERS:** Shows one container named `ad-auction_ad-auction-2-6969db6b89-2h8kd` in UP status, with 5% CPU usage and 89 MB memory.
- YAML View:** Displays the YAML configuration for the pod.
- Annotations:** ad.datadoghq.com/ad-auction.logs: [{"source": "nodejs", "service": "ad-auction"}]
- Metadata Fields:** Name, Generate Name, Namespace, Uid, Resource Version, Creation Timestamp, Labels, Annotations, Owner References, Managed Fields.
- Spec Fields:** Volumes, Containers, Restart Policy, Termination Grace Period, Dns Policy, Service Account Name, Service Account, Node Name.

4.1.4 Kubernetes Integration을 통해 확인할 수 있는 부분 (2/3)

3. Deployment 레벨 가시성

The screenshot shows the 'Containers' view for Kubernetes Deployments. On the left, there's a sidebar with navigation links for Views, Containers, Clusters, Pods, Deployments (selected), Replica Sets, Services, and Namespace. The main area displays a table of Deployments grouped by kube_cluster_name. Each row contains information like Deployment name, Age, Current/Desired State, Up To Date Status, Available Pods, and Kubernetes Labels. A red box highlights the sidebar and the 'Containers' section of the main table.

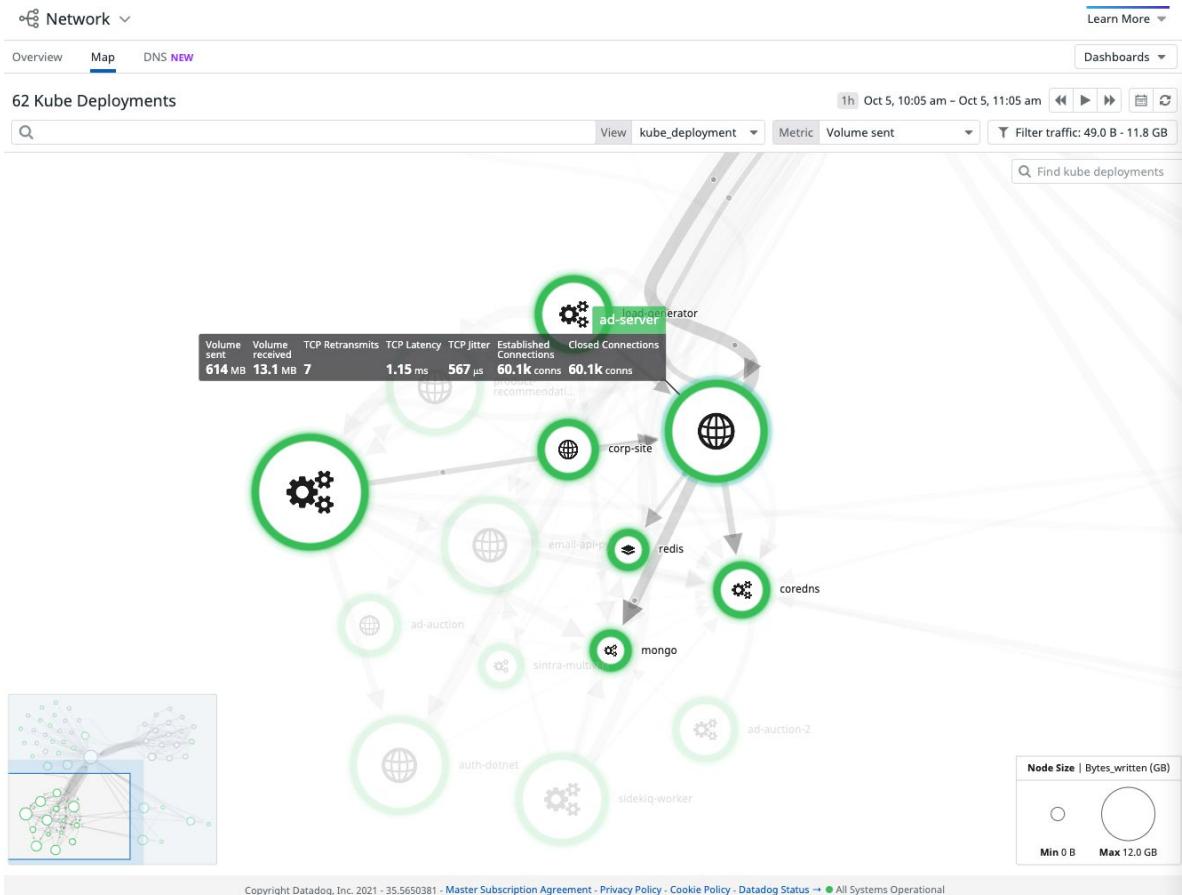
Container, Pod, Node 외에 각 리소스별 View를 제공하여 손쉽게 K8S의 가시성 확보 가능

4. Node 레벨 가시성

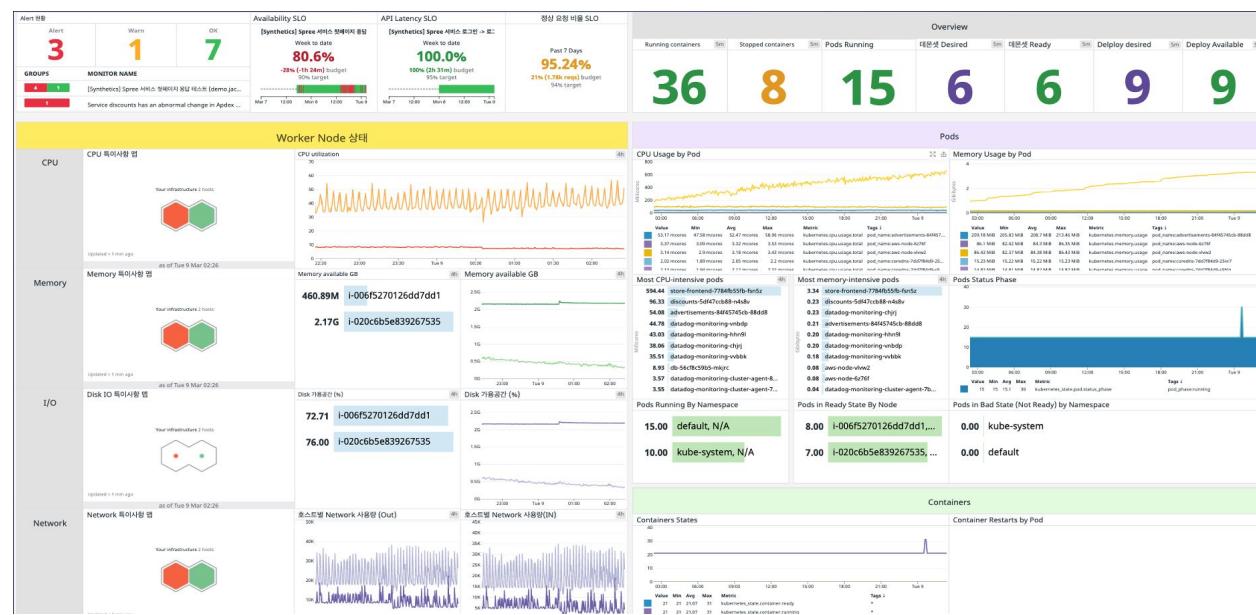
The screenshot shows the 'Containers' view for a specific Node (aks-agentpool-21451434-vmss000000). The top bar includes 'Views', 'Containers' (selected), 'Save', 'Learn More', 'LIVE Oct 5, 10:58 am', and refresh buttons. The main area has tabs for NODE, CONTAINERS, and Metrics. The NODE tab shows detailed information for the node, including Role (agent), Version (v1.19.11), Internal IP (10.240.0.4), Age (2 months), Namespace (None), and Cluster (demo-11287-aks-no...). Below this are sections for TAGS and KUBERNETES LABELS. The CONTAINERS tab shows a list of pods running on the node, with 'Nodes' highlighted in blue. A red box highlights the 'Nodes' section of the sidebar and the 'Nodes' section of the main table.

4.1.4 Kubernetes Integration을 통해 확인할 수 있는 부분 (3/3)

5. Network Flow 가시성



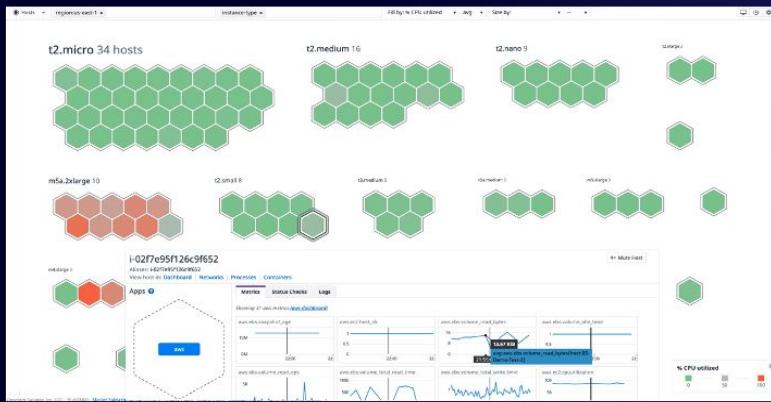
6. Kubernetes 대시보드 샘플



4.1.5 Kubernetes Monitoring Best practice

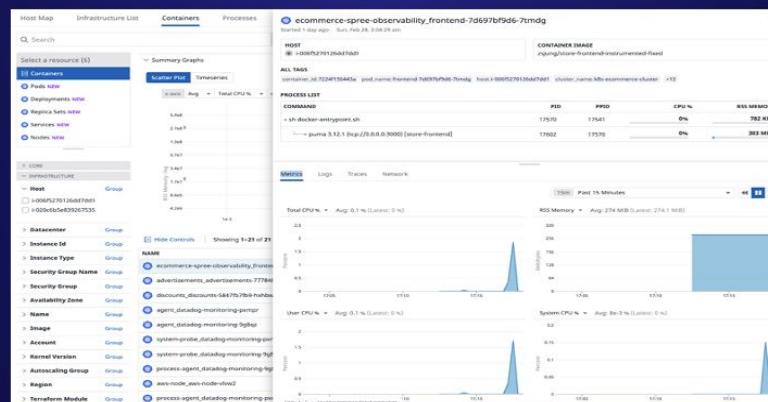
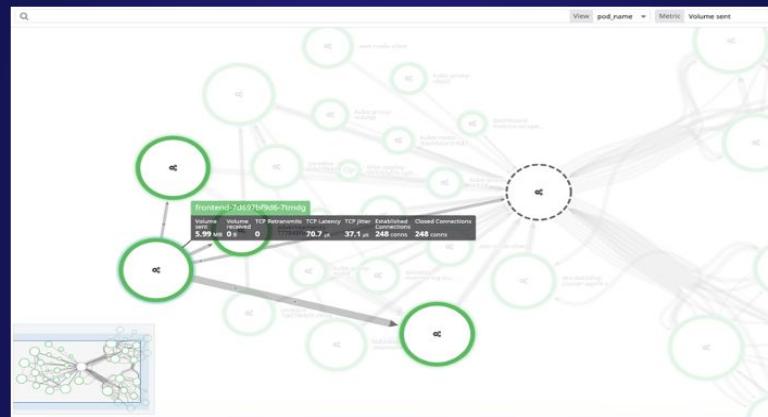
쉽게 FullStack Data를 연동하고 Powerful한 분석 환경을 통해 장애 분석 시간 최소화

1. AWS 계정 연동



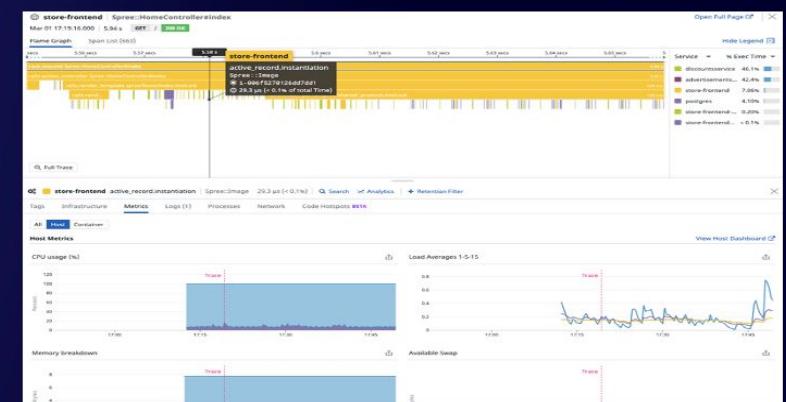
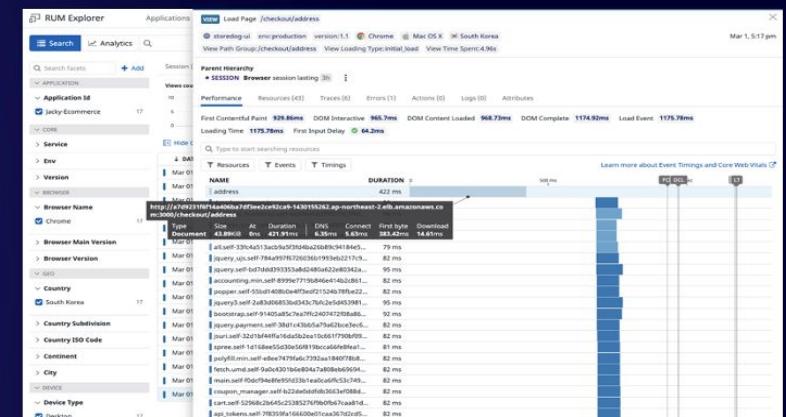
AWS 환경의 리소스를 효과적으로 시각화

2. Helm chart 배포



EKS의 Node/Pod/Container에 대한 가시성 확보

3. Application에 Datadog SDK 연동

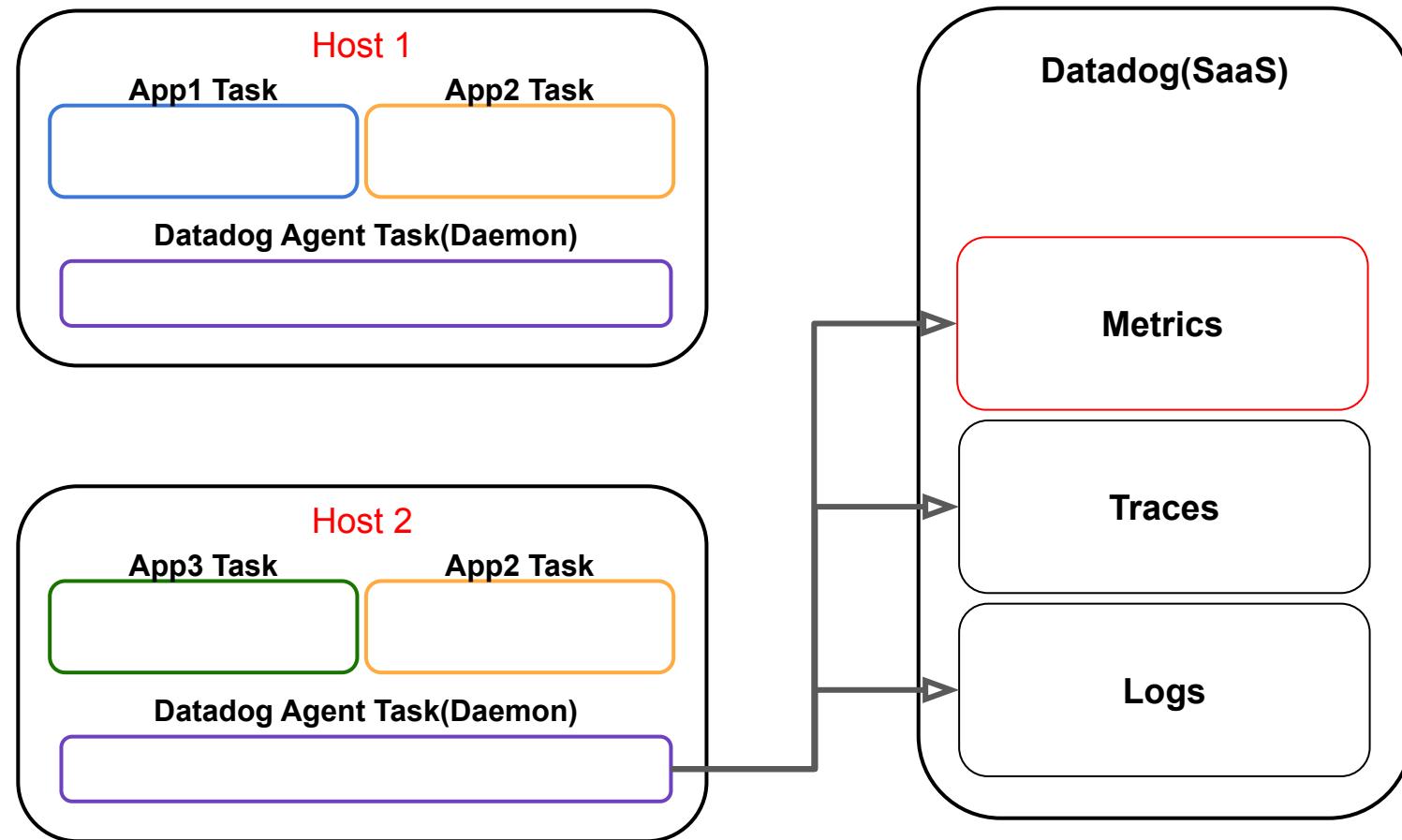


End User부터 Backend까지의 FullStack 가시성 확보

4.2.1 ECS on EC2 메트릭 수집 아키텍쳐

Datadog Agent Task

- ❑ Daemon 서비스로 각 호스트에 배포됨
- ❑ Host내의 Task별 컨테이너 리소스 수집
- ❑ 컨테이너 메트릭 + Trace + Log 수집



4.2.2 ECS on EC2 연동 방법

ECS on EC2 연동 방법 ([링크](#))

1. For Linux containers, download [datadog-agent-ecs.json](#) (datadog-agent-ecs1.json) if you are using an original Amazon Linux 1 AMI). For Windows, download [datadog-agent-ecs-win.json](#).
2. Edit `datadog-agent-ecs.json` and set `<YOUR_DATADOG_API_KEY>` with the Datadog API key for your account.
3. Optionally - Add the following to your ECS task definition to deploy on an [ECS Anywhere cluster](#).

```
"requiresCompatibilities": ["EXTERNAL"]
```

4. Optionally - Add an Agent health check.

Add the following to your ECS task definition to create an Agent health check:

```
"healthCheck": {  
    "retries": 3,  
    "command": ["CMD-SHELL", "agent health"],  
    "timeout": 5,  
    "interval": 30,  
    "startPeriod": 15  
}
```

5. Optionally - If you are in Datadog EU site, edit `datadog-agent-ecs.json` and set `DD_SITE` to `DD_SITE:datadoghq.eu`.

6. Optionally - See [log collection](#) to activate log collection.

7. Optionally - See [process collection](#) to activate process collection.

8. Optionally - See [trace collection \(APM\)](#) to activate trace collection.

9. Optionally - See [network performance monitoring \(NPM\)](#) to activate network collection

10. Execute the following command:

```
aws ecs register-task-definition --cli-input-json <path to datadog-agent-ecs.json>
```

Datadog 기본 task definition json

```
{  
    "containerDefinitions": [  
        {  
            "name": "datadog-agent",  
            "image": "public.ecr.aws/datadog/agent:latest",  
            "cpu": 100,  
            "memory": 512,  
            "essential": true,  
            "mountPoints": [  
                {  
                    "containerPath": "/var/run/docker.sock",  
                    "sourceVolume": "docker_sock",  
                    "readOnly": null  
                },  
                {  
                    "containerPath": "/host/sys/fs/cgroup",  
                    "sourceVolume": "cgroup",  
                    "readOnly": null  
                },  
                {  
                    "containerPath": "/host/proc",  
                    "sourceVolume": "proc",  
                    "readOnly": null  
                }  
            ],  
            "environment": [  
                {  
                    "name": "DD_API_KEY",  
                    "value": "<YOUR_DATADOG_API_KEY>"  
                },  
                {  
                    "name": "DD_SITE",  
                    "value": "datadoghq.com"  
                }  
            ]  
        },  
        "volumes": [  
            {  
                "host": {  
                    "sourcePath": "/var/run/docker.sock"  
                },  
                "name": "docker_sock"  
            },  
            {  
                "host": {  
                    "sourcePath": "/proc/"  
                },  
                "name": "proc"  
            },  
            {  
                "host": {  
                    "sourcePath": "/sys/fs/cgroup/"  
                },  
                "name": "cgroup"  
            }  
        ],  
        "family": "datadog-agent-task"  
    ]  
}
```

요약하면

1. DatadogAgent Task 생성
2. Daemon SERVICE로 등록

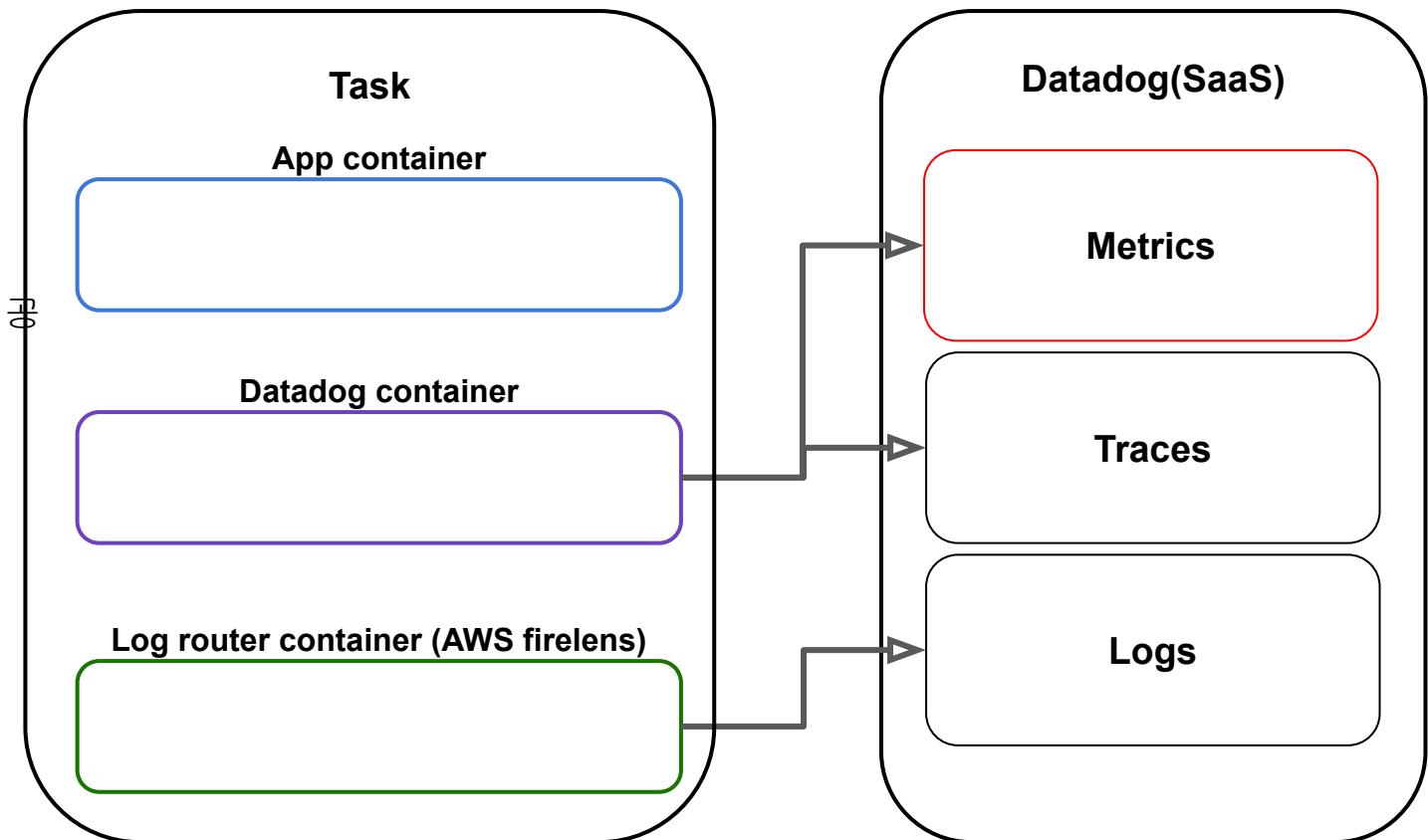
4.3.1 ECS on Fargate 메트릭 수집 아키텍쳐

Datadog container

- ❑ Task내에 sidecar 형태로 배포됨
- ❑ Task내의 container 메트릭 수집
- ❑ Application의 Trace 수집

Log router container

- ❑ Fargate 환경에서 생성되는 로그에 대해 수집
- ❑ AWS firelens에서 Datadog으로 전송할 수 있는 옵션 제공



4.3.2 ECS on Fargate 메트릭 수집 방법

ECS on Fargate 연동 방법 ([링크](#))

AWS CLI

1. Download [datadog-agent-ecs-fargate](#). **Note:** If you are using IE, this may download as gzip file, which contains the JSON file mentioned below.**
2. Update the JSON with a `TASK_NAME`, your Datadog API Key, and the appropriate `DD_SITE` (datadoghq.com). Note that the environment variable `ECS_FARGATE` is already set to `true`.
3. Add your other containers such as your app. For details on collecting integration metrics, see [Integration Setup for ECS Fargate](#).
4. Execute the following command to register the ECS task definition:

```
aws ecs register-task-definition --cli-input-json  
file://<PATH_TO_FILE>/datadog-agent-ecs-fargate.json
```

Datadog 기본 task definition json

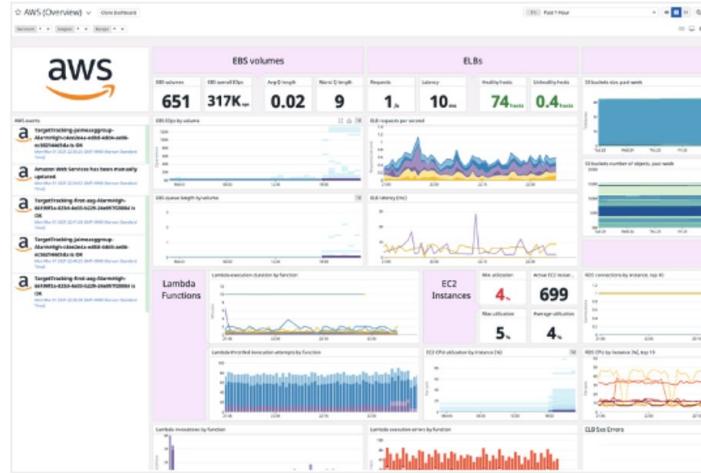
```
{  
    "family": "<TASK_NAME>",  
    "networkMode": "awsvpc",  
    "containerDefinitions": [  
        {  
            "name": "datadog-agent",  
            "image": "public.ecr.aws/datadog/agent:latest",  
            "essential": true,  
            "environment": [  
                {  
                    "name": "DD_API_KEY",  
                    "value": "<YOUR_API_KEY>"  
                },  
                {  
                    "name": "ECS_FARGATE",  
                    "value": "true"  
                }  
            ]  
        },  
        "requiresCompatibilities": [  
            "FARGATE"  
        ],  
        "cpu": "256",  
        "memory": "512"  
    ]  
}
```

요약하면

1. Application task에 datadog-agent 컨테이너가 추가되는 형태입니다
(sidecar)

4.3.3 ECS on Fargate Monitoring Best practice (1/2)

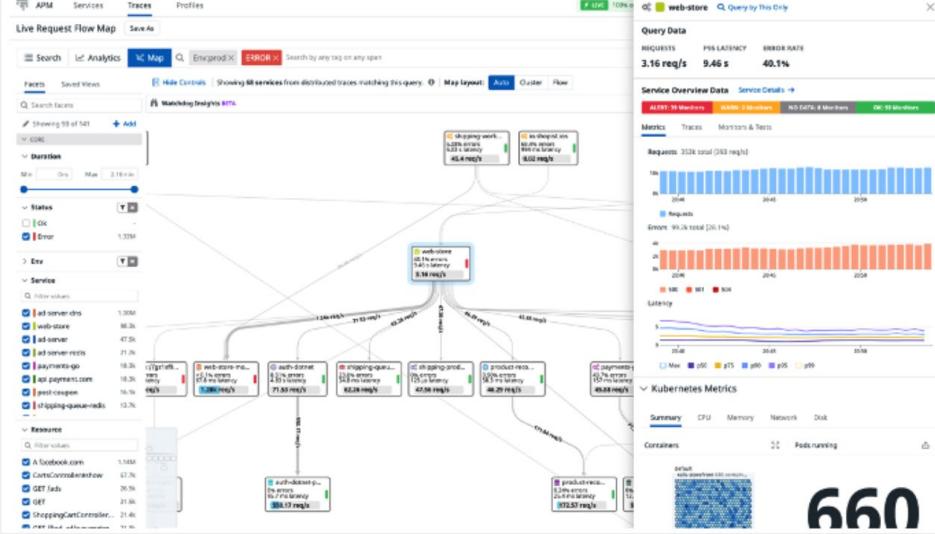
1. AWS 계정 연동 (PaaS 서비스 가시성 확보)



2. Task내의 Container 메트릭 수집



3. Task내의 Application Trace 수집



- 다양한 Preset Dashboard가 생성됨

- EC2
- EBS
- ALB
- RDS
- 그외 다양한 AWS 서비스

- Clone 후 자유롭게 대시보드 조합 가능

- Sidecar 컨테이너로 배포 되어 컨테이너 메트릭 수집

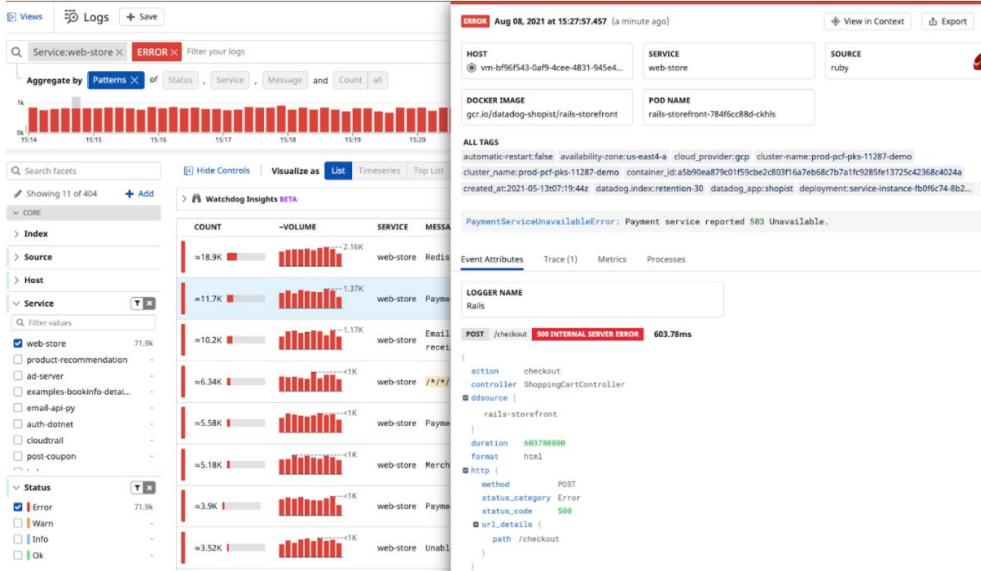
- Tag가 함께 수집되어 Filtering 및 Grouping 가능

- APM을 통해 Application 가시성(trace 확보)

- 분산 트레이싱 환경 구성
- 여러만 별도로 모아 관리 가능 (Error Tracking)
- trace_id를 통해 로그 연계 분석 지원

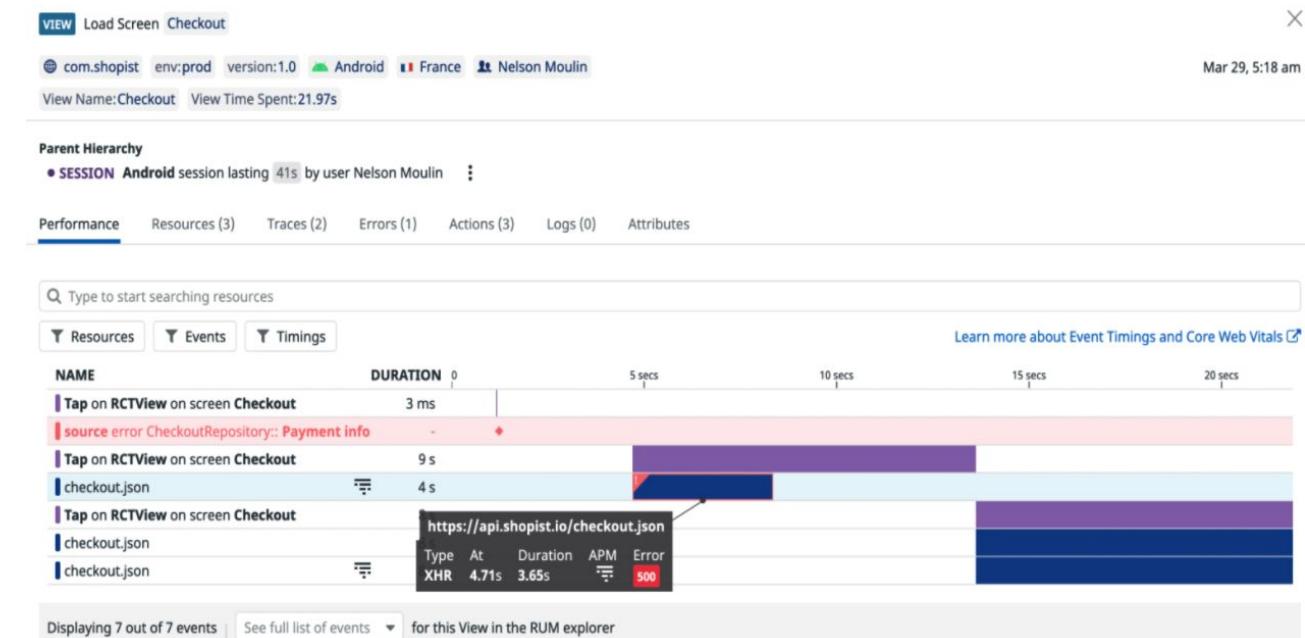
4.3.3 ECS on Fargate Monitoring Best practice (2/2)

4. Application container의 로그 수집



- ❑ firelens를 통해 Datadog으로 로그 전송 기능 지원
- ❑ APM-Log 연계 분석
- ❑ Log 기반 알람 및 대시보드 구성

5. 사용자 관점의 성능 메트릭 수집



- ❑ RUM을 통해 서비스 사용자 성능 메트릭
- ❑ 사용자 부터 Backend까지 FullStack 모니터링 환경 제공
- ❑ Front의 Error Tracking 기능 지원
- ❑ 사용자 관점의 Business 지표 분석 기능 지원

5. 운영중인 솔루션의 Key Metric 수집

요구사항

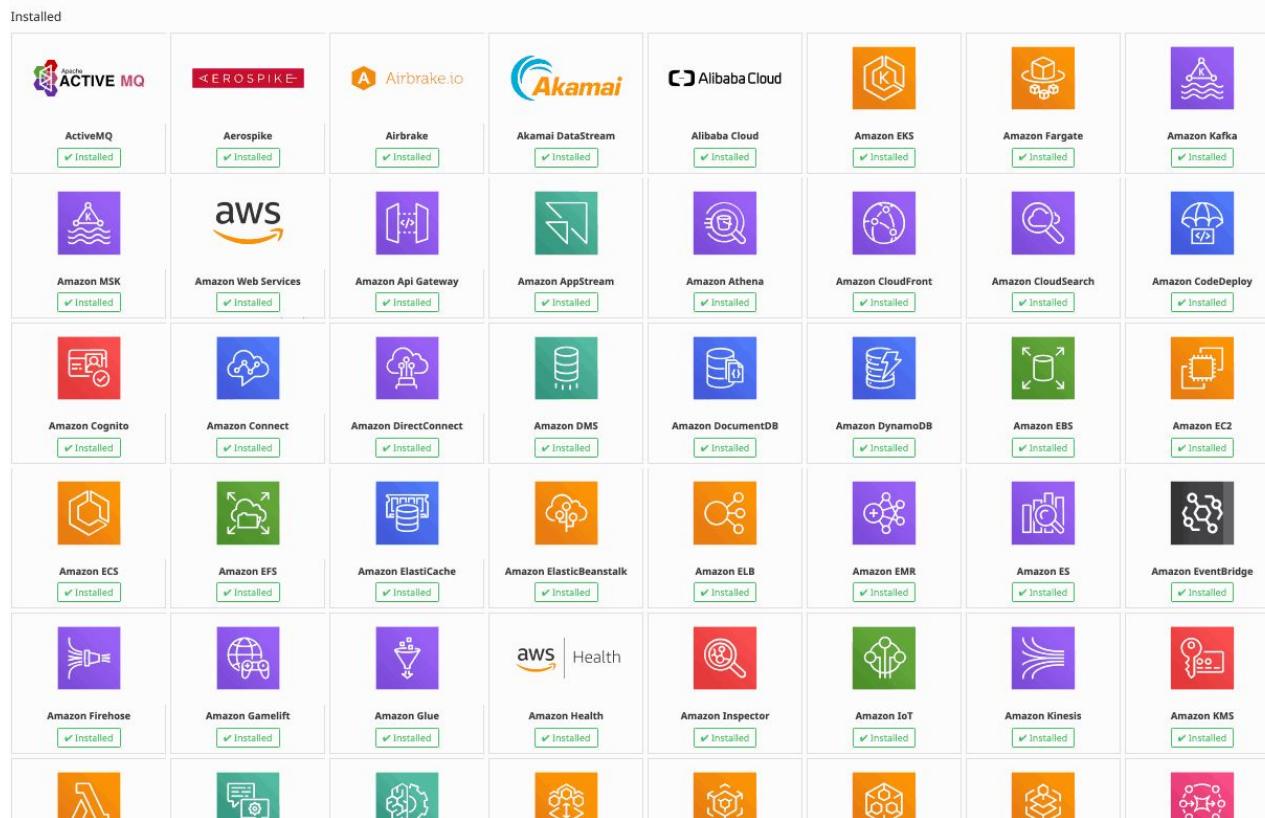
- ❑ Kafka broker의 상태 메트릭 수집 모니터링이 필요합니다 ➔ **kafka integration**
- ❑ Mysql 서버의 performance 정보를 수집하고 싶어요 ➔ **mysql integration**
- ❑ Redis 서버의 상태 모니터링이 필요합니다 ➔ **redis integration**
- ❑ 서비스의 health check API에 대한 availability 와 응답 시간에 대한 레이턴시 측정을 하고 싶어요 ➔ **http check integration**

Datadog으로 지원 가능한가요?

- 450+ 제공되는 Datadog Integration으로 지원 가능합니다
- 별도의 개발 없이 Integration 연동을 통해 Key 메트릭 수집

Q2. Kafka 10개의 노드에 Datadog agent가 설치되어 있는 상황에서 Kafka integration을 하면 추가 비용이 발생하나요? (티셔츠 1)

Q3. http check을 이용해 1달 동안 1만번 테스트가 발생했을 때 추가 비용이 발생하나요? (티셔츠 1)



5.1 Redis Integration 설정 예

1. /etc/datadog-agent/conf.d/redisdb.d/conf.yaml 파일에서 host, port 정보 확인 후 저작

```
init_config:  
instances:  
## @param host - string - required  
## Enter the host to connect to.  
- host: localhost  
## @param port - integer - required  
## Enter the port of the host to connect to.  
port: 6379  
  
## @param username - string - optional  
## The username to use for the connection. Redis 6+ only.  
#  
# username: <USERNAME>  
  
## @param password - string - optional  
## The password to use for the connection.  
#  
# password: <PASSWORD>
```

2. Datadog agent 재시작

```
systemctl restart datadog-agent
```

3. Redis integration 후 수집되는 메트릭 ([참고](#))

Name	Units	Description
redis.active_defrag.hits	operations	Number of value reallocations performed by the active defragmentation process.
redis.active_defrag.key_hits	keys	Number of keys that were actively defragmented.
redis.active_defrag.key_misses	keys	Number of keys that were skipped by.
redis.active_defrag.misses	operations	Number of aborted value reallocations started by the active defragmentation process.
redis.active_defrag.running		Whether active defragmentation is running or not.
redis.aof.buffer_length	bytes	Size of the AOF buffer.
redis.aof.last_rewrite_time	seconds	Duration of the last AOF rewrite.
redis.aof.loading_eta_seconds	seconds	The estimated amount of time left to load.
redis.aof.loading_loaded_bytes	bytes	The amount of bytes to load.
redis.aof.loading_loaded_perc	percent	The percent loaded.
redis.aof.loading_total_bytes	bytes	The total amount of bytes already loaded.
redis.aof.rewrite		Flag indicating a AOF rewrite operation is on-going.
redis.aof.size	bytes	AOF current file size (aof_current_size).
redis.clients.biggest_input_buf		The biggest input buffer among current client connections.
redis.clients.blocked	connections	The number of connections waiting on a blocking call.
redis.clients.longest_output_list		The longest output list among current client connections.
redis.clients.recent_max_input_buffer		The biggest input buffer among recent client connections.
redis.clients.recent_max_output_buffer		The longest output buffer among recent client connections.
redis.command.calls		The number of times a redis command has been called, tagged by 'command', e.g. 'command:append'. Enable in Agent's redisdb.yaml with the command_stats option.

5.2 Redis Integration Dashboard

Redis - Overview ▾ Clone Dashboard

Search... \$scope * \$host *

1d Past 1 Day | High Density Mode |

This dashboard shows latency information and slow query counts that summarize your Redis master's performance.

Our 3-part blog series

How to monitor Redis performance metrics ↗

Collecting Redis metrics ↗

More ▾ More ▾

Hit rate 52 % Blocked clients 192 conn

Redis keyspace 26.45M keys Unsaved chan... 312.05k

Primary link d... (No data)

This metric is only available when the connection between the primary and secondary nodes is active.

Connected clients

Redis has 10,000 client connections available by default, but you can increase it up to 64,000.

Connected replicas

Rejected connections

Keys

Performance Metrics

Latency by Host

T...	M...	Avg	Max	Val
ho...	La...	1.27 ms	40.93 ms	0.74 n
ho...	La...	10.59 ms	93.59 ms	4.72 n
ho...	La...	12.60 ms	59.92 ms	18.80 n
ho...	La...	1.22 ms	4.09 ms	0.82 n

Slowlog

Memory Metrics

Percent Used Memory by Host

T...	M...	Avg	Min	Max
ho...	% ...	—	—	—
ho...	% ...	—	—	—
ho...	% ...	—	—	—
ho...	% ...	—	—	—

Memory usage is a crucial performance factor. If `used_memory > total available system memory`, the OS will begin swapping.

Evictions

Logs

Error Logs

No matching entries found

Try Rehydrating From Archives ↗

All Logs

DATE

- Oct 05 13:16:55.542 Background saving terminated with success
- Oct 05 13:16:52.308 Background saving terminated with success
- Oct 05 13:16:52.202 DB saved on disk
- Oct 05 13:16:50.920 Background saving terminated with success
- Oct 05 13:16:47.043 10000 changes in 60 seconds. Saving...
- Oct 05 13:16:45.944 RDB: 4 MB of memory used by copy-on-write
- Oct 05 13:16:45.924 DB saved on disk
- Oct 05 13:16:45.185 Background saving started by pid 1523945
- Oct 05 13:16:45.164 10000 changes in 60 seconds. Saving...

Latency measures the time between a client request and the server response, and monitoring it enables you to detect issues early.

More ▾

Slowlog

Evictions

Logs

No matching entries found

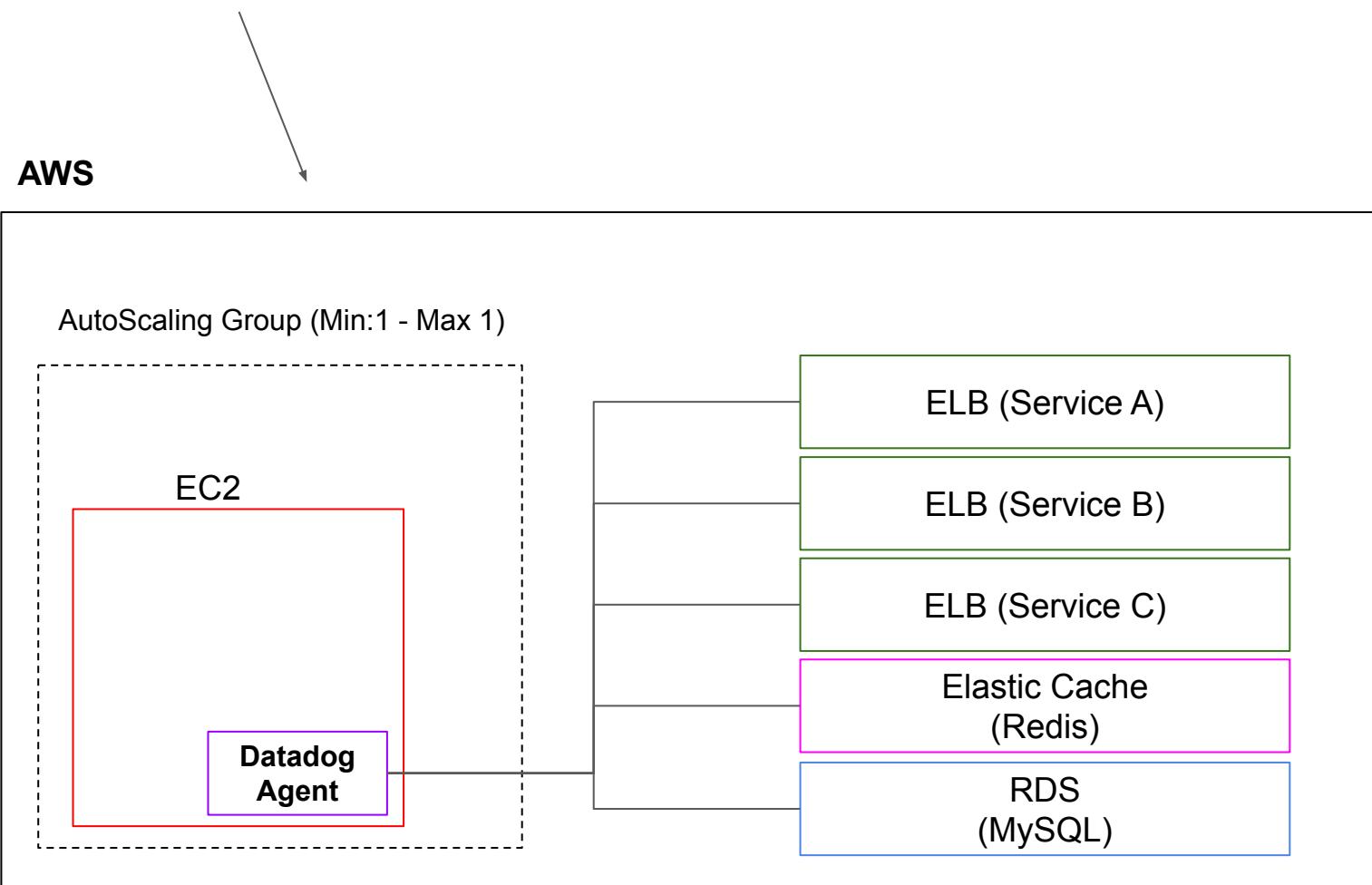
Try Rehydrating From Archives ↗

5.3 Integration Best practice

1. 가급적 다양한 인테그레이션을 활용하여 연계 분석에 활용하세요

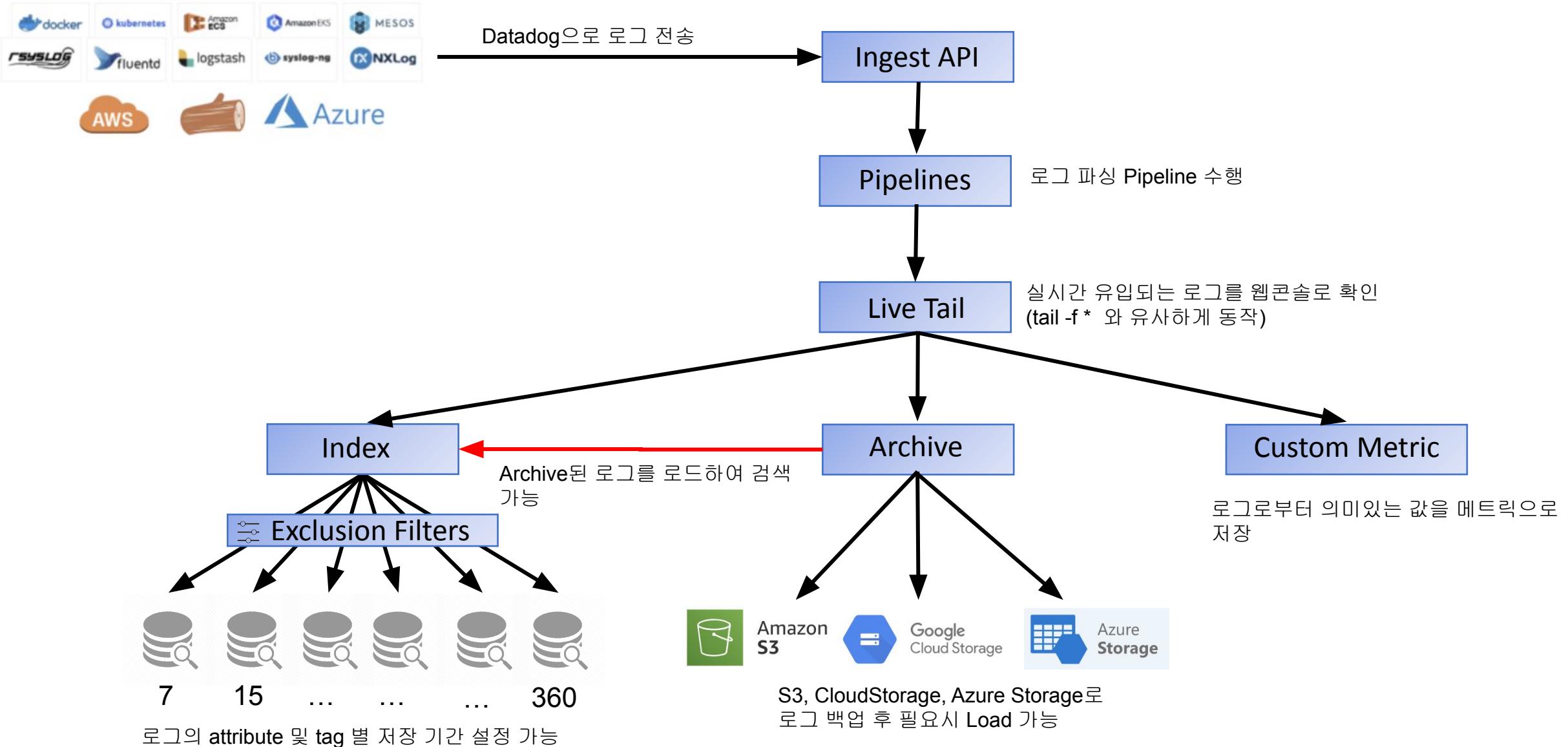
- 다양하게 수집된 메트릭은 머신러닝을 이용한 특이사항 탐지에 사용될 수 있습니다

2. Cloud 환경에서 인스턴스 하나는 모니터링 용도로 PaaS 솔루션 모니터링이나 HTTP Check에 활용하시면 좋습니다



Log Flow

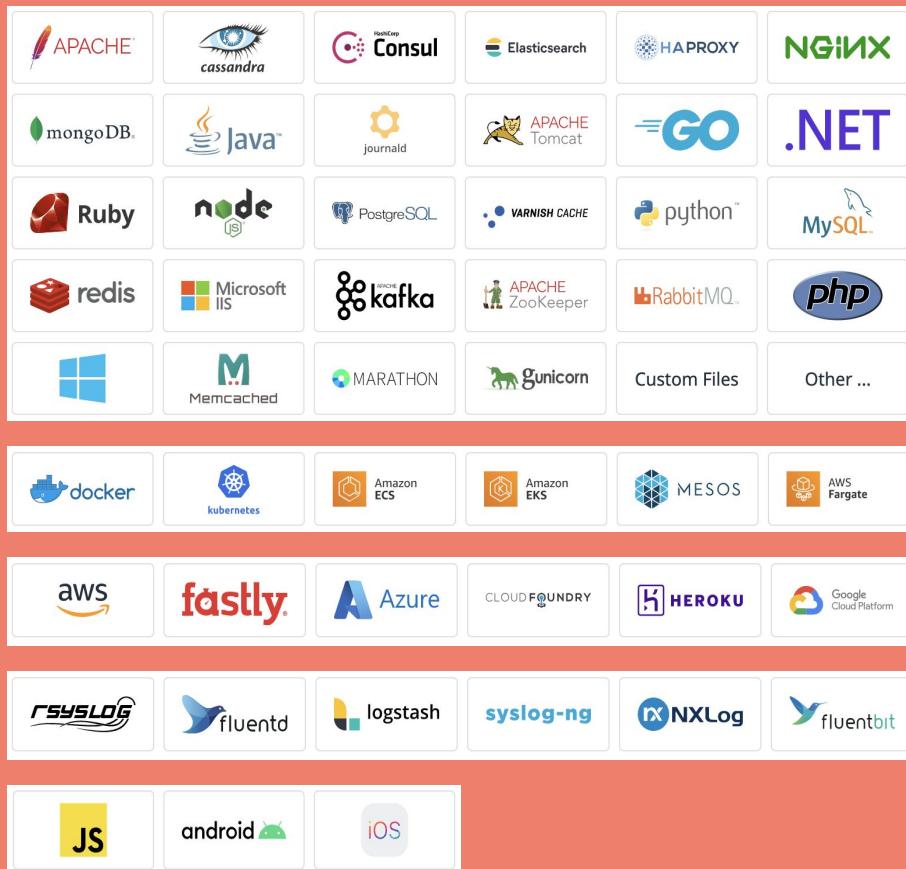
#Datadog Log Flow



Log Features

#Sending Logs to Datadog

다양한 방법을 통한 로그전송



Things To Check

- Filter logs
- Scrub
- multi-line

Sample

logs:

- type: file
path: 로그_경로/server.log
service: myapplication
source: java
log_processing_rules:
 - type: multi_line
name: new_log_start_with_date
pattern: - \d{4}-\d{2}-\d{2}



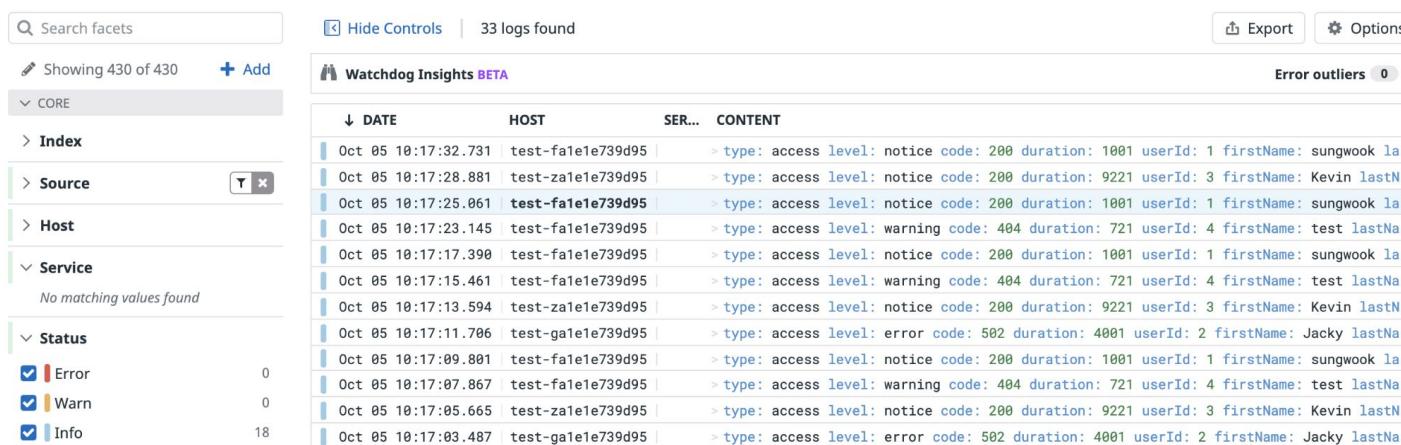
#Sending Logs to Datadog

Sending Logs via API

```
"ddsource": "test",
"ddservice": "test",
"ddtags": "env:staging,user:sungwook",
"hostname": "test-fa1e1e739d95",
"message": "type: access level: notice code: 200 duration: 1001 userId: 1 firstName: sungwook
lastName: lee phoneNumber: 010-1234-5678 emailAddress: AAAAA@datadoghq.com"
}
```

```
***curl -d @$list https://http-intake.logs.datadoghq.com/v1/input -H "Content-Type: application/json" -H "DD-API-KEY: ${API}"
```

Result



The screenshot shows the Watchdog Insights interface with the following details:

- Search facets:** Search bar with placeholder "Search facets".
- Controls:** Hide Controls button, 33 logs found, Export button, Options button.
- Watchdog Insights BETA:** Error outliers 0.
- Facets:**
 - CORE:** Index, Source, Host, Service (No matching values found), Status (Error 0, Warn 0, Info 18).
- Table:** Shows log entries with columns: DATE, HOST, SER..., CONTENT. The first few rows of data are:

DATE	HOST	SER...	CONTENT
Oct 05 10:17:32.731	test-fa1e1e739d95		>type: access level: notice code: 200 duration: 1001 userId: 1 firstName: sungwook la...
Oct 05 10:17:28.881	test-zale1e739d95		>type: access level: notice code: 200 duration: 9221 userId: 3 firstName: Kevin lastN...
Oct 05 10:17:25.061	test-fa1e1e739d95		>type: access level: notice code: 200 duration: 1001 userId: 1 firstName: sungwook la...
Oct 05 10:17:23.145	test-fa1e1e739d95		>type: access level: warning code: 404 duration: 721 userId: 4 firstName: test lastNa...
Oct 05 10:17:17.390	test-fa1e1e739d95		>type: access level: notice code: 200 duration: 1001 userId: 1 firstName: sungwook la...
Oct 05 10:17:15.461	test-fa1e1e739d95		>type: access level: warning code: 404 duration: 721 userId: 4 firstName: test lastNa...
Oct 05 10:17:13.594	test-zale1e739d95		>type: access level: notice code: 200 duration: 9221 userId: 3 firstName: Kevin lastN...
Oct 05 10:17:11.706	test-gale1e739d95		>type: access level: error code: 502 duration: 4001 userId: 2 firstName: Jacky lastNa...
Oct 05 10:17:09.801	test-fa1e1e739d95		>type: access level: notice code: 200 duration: 1001 userId: 1 firstName: sungwook la...
Oct 05 10:17:07.867	test-fa1e1e739d95		>type: access level: warning code: 404 duration: 721 userId: 4 firstName: test lastNa...
Oct 05 10:17:05.665	test-zale1e739d95		>type: access level: notice code: 200 duration: 9221 userId: 3 firstName: Kevin lastN...
Oct 05 10:17:03.487	test-gale1e739d95		>type: access level: error code: 502 duration: 4001 userId: 2 firstName: Jacky lastNa...

#Pipelines

다양한 Pipeline Library 제공

Pipeline Library [?](#)

↑ PIPELINES 196 available | 120 installed FILTERS

Source	Description
ActiveMQ	source:activemq
Adobe Experience Manager	source:adobe.experience.manager
Aerospike ✓	source:aerospike
Airflow	source:airflow
Akamai	source:akamai
Alcide ✓	source:alcide
Ambari ✓	source:ambari
Android logs ✓	source:android
Apache ✓	source:apache
Apache httpd	source:httpd
Apigee	source:apigee
Aqua ✓	source:aqua
Auth0	source:auth0
AWS ALB Ingress Controller ✓	source:aws-alb-ingress-controller
AWS Api Gateway ✓	source:apigateway
AWS CloudFront ✓	source:cloudfront
AWS CloudHSM	source:cloudhsm



Things To Check

- Processor

- Grok parser
- URL parser
- User-Agent parser
- Category processor
- Arithmetic processor
- GeolIP parser
- Lookup processor
- Remapper
- Log date remapper
- Log status remapper
- Service remapper



#Sending Logs to Datadog

Parser 적용 rule ex. %{data::keyvalue(": ")}

Edit Grok Parser: Grok Parser ? X

1 type: access level: notice code: 200 userId: 1 firstName: 성우 lastName: 0이 phoneNumber: 010-1234-5678 emailAddress: AAAAA@datadoghq.com MATCH Need Help?

+ Add

2 Define parsing rules ?

```
rule %{data::keyvalue(": ")}
```

Advanced Settings

✓ 0 Helper Rules, 1 Parsing Rules

rule rule matched. Extraction:

```
{
  "type": "access",
  "level": "notice",
  "code": 200,
  "userId": 1,
  "phoneNumber": "010-1234-5678",
```

Cancel Update

Result

NOTICE Oct 05, 2021 at 10:21:56.489 (a few seconds ago) View in Context Export X

HOST test-fa1e1e739d95 SOURCE test

ALL TAGS datadog.index:retention-7 env:staging source:test user:sungwook

```
type: access level: notice code: 200 duration: 1001 userId: 1 firstName: sungwook lastName: lee phoneNumber: 010-1234-5678 emailAddress: AAAAA@datadoghq.com
```

Event Attributes Trace (0) Metrics Processes

Duration: 1001ms

Attribute	Value
code	200
ddservice	test
duration	1001
emailAddress	AAAAA@datadoghq.com
firstName	sungwook
hostname	test-fa1e1e739d95
lastName	lee
level	notice
phoneNumber	010-1234-5678
type	access
userId	1

#Archives & Rehydrate

저장 & 복원

The screenshot shows the Datadog interface for managing historical views. At the top, there's a sidebar with a dog icon and several navigation links. The main area has three sections:

- Select Archive Type:** Shows options for Amazon S3, Google Cloud Storage, and Azure Storage. The Amazon S3 option is selected.
- Configure Bucket:** Includes instructions to log in to the AWS account, grant Datadog Role write access, and input account, bucket, and path details. It also shows the AWS Account dropdown and a list of historical views.
- Archives View:** Displays a table of historical views with columns for QUERY, # OF EVENTS, and CREATED. Three views are listed as ACTIVE:
 - hadhemi-investigation (service:delancie-crawler_aws i-07301c82594cf93f from Jun 4, ...)
 - vault-us2-010119-080419 (service:acme-consul from Jan 1, 5:57 am - May 8, 6:00 am)
 - muw-logs-may22-23 (service:monitor-upptime-writer from May 22, 10:00 pm - May 2...)

A pink box highlights the "Rehydrate From Archives" button in the Archives view header, and another pink box highlights the "New Historical View +" button.

Things To Check

- Index 없이 사용가능
 - 복원시 Ingest / Index 비용발생
 - Estimate scan size
 - Custom Storage 사용불가
- *약 12GB 테스트시 약 5-10분 소요
(Storage 위치등에 따라 차이발생)



#Log Features Demo



DATADOG

- Go to...
- Watchdog
- Events
- Dashboards
- Infrastructure
- Monitors
- Metrics
- Integrations
- APM
- CI BETA
- Notebooks
- Logs
- Security
- UX Monitoring
- Contact Support
- Help
- Invite Users
- sungwook.lee... Datadog Demo (...)

Live Tail

Filter your logs 

28121 events/s, <1% displayed (refine your query to avoid sampling) 

Live Tail  Pause  Options

DATE	HOST	SERVICE	CONTENT
Oct 01 16:26:51.256	gke-events-alerting-de...	web-store-mongo	> connection accepted from 10.204.11.79:34840 #323028 (948 connections now open)
Oct 01 16:26:50.860	gke-events-alerting-de...	email-api-py	> "POST /api/v1/email/ HTTP/1.1" 201 129
Oct 01 16:26:50.709	i-0afdf6fe28c9a089f	web-store	> MONGODB [138510] mongo:27017 rails_storefront_development.find SUCCEEDED ...
Oct 01 16:26:50.040	gke-demo-11287-us-prod...	web-store-mongo	> (812 connections now open)
Oct 01 16:26:49.690	gke-demo-11287-us-prod...	auth-dotnet	> Deleted expired session with token=EVGH501XMG9702V4X00YXW44
Oct 01 16:26:49.617	gke-us-staging-default...	web-store-mongo	> conn228650: { driver: { name: "PyMongo", version: "3.8.0" }, os: { type: "Linux..."}
Oct 01 16:26:49.292	i-079a86fe62bca52cc	chaos-engineering	> 2021-10-01 07:26:48,263 - rails_generator.py - DEBUG - main_merchant_loop:358 -...
Oct 01 16:26:49.028	gke-demo-dpn-us-west-d...	auth-dotnet	> Found session with token=A30YM9MZDF50YV360FAN71YM
Oct 01 16:26:49.022	gke-us-staging-pool-1...	web-store	> MONGODB [87973] mongo:27017 #11 rails_storefront_development.find STARTED...
Oct 01 16:26:49.018	gke-demo-11287-us-prod...	auth-dotnet	> Deleted expired session with token=PZ4D3I1PXAIU3U8DDHS0WCZJ
Oct 01 16:26:49.941	gke-demo-11287-us-prod...	auth-dotnet	> Checking token for customer=RXJGFLHT149D7C1B8QPN2SDB with session=MDR7GVG9JH533...
Oct 01 16:26:48.844	gke-demo-dpn-us-west-d...	web-store	> MONGODB [26144] mongo:27017 rails_storefront_development.find SUCCEEDED ...
Oct 01 16:26:48.751	gke-events-alerting-de...	web-store	> /rails-storefront/app/controllers/shopping_cart_controller.rb:745: warning: alr...
Oct 01 16:26:48.651	snmp-demo-node-4.c.fet...	snmplabslogs	> 2021-10-01T07:01:37.57 snmpsime: Response var-binds: 1.3.6.1.2.1.6.13.1.4.145.6...
Oct 01 16:26:48.594	i-0afdf6fe28c9a089f	email-api-py	> Response code from SES: 200
Oct 01 16:26:48.320	gke-demo-11287-us-prod...	web-store-mongo	> connection accepted from 10.56.20.168:34800 #417082 (798 connections now open)
Oct 01 16:26:48.282	gke-demo-11287-us-prod...	web-store	> MONGODB [62204] mongo:27017 rails_storefront_development.find SUCCEEDED ...
Oct 01 16:26:48.274	vm-49403541-5fd5-4254-...	web-store	> MONGODB [21492] mongo:27017 #72 rails_storefront_development.count STARTED...
Oct 01 16:26:48.247	gke-demo-11287-us-prod...	shipping-producer	> MONGODB [705154] mongo:27017 #6 rails_storefront_development.find STARTED...
Oct 01 16:26:48.140	gke-demo-11287-us-prod...	auth-dotnet	> Deleted expired session with token=0P708PIW6V72IVKFCGZ3T91X
Oct 01 16:26:48.099	gke-demo-dpn-us-west-p...	auth-dotnet	> Found session with token=KJMJDHP2KQN4Q10ZECZ240KC
Oct 01 16:26:48.035	gke-events-alerting-de...	auth-dotnet	> Found session with token=SOZUQ6JWTJC1Y36IJWCUJJDD
Oct 01 16:26:47.927	snmp-demo-node-3.c.fet...	snmplabslogs	> 2021-10-01T07:01:22.84 snmpsime: Request var-binds: 1.3.6.1.2.1.6.8.0=<, flags...
Oct 01 16:26:47.902	gke-demo-11287-us-prod...	email-api-py	> "GET /api/v1/email/ HTTP/1.1" 200 6166
Oct 01 16:26:47.860	i-002866ca391556841	web-store	> Response from fraud prevention: 200

Log Optimization

#Log Optimization

Logging Without Limits™

- INGEST

Filter Logs

Generate Metrics

- INDEX

로그 중요도별 저장 주기 조정

Set daily quota

사용량에 따른 알람 생성

After

- INGEST

Ingest 비용 절감

로그 저장 없이 특정 패턴 발생시 알람

- INDEX

Access 로그 3일 / Error 로그 15일

Access 로그에 추가 일 100M 제한

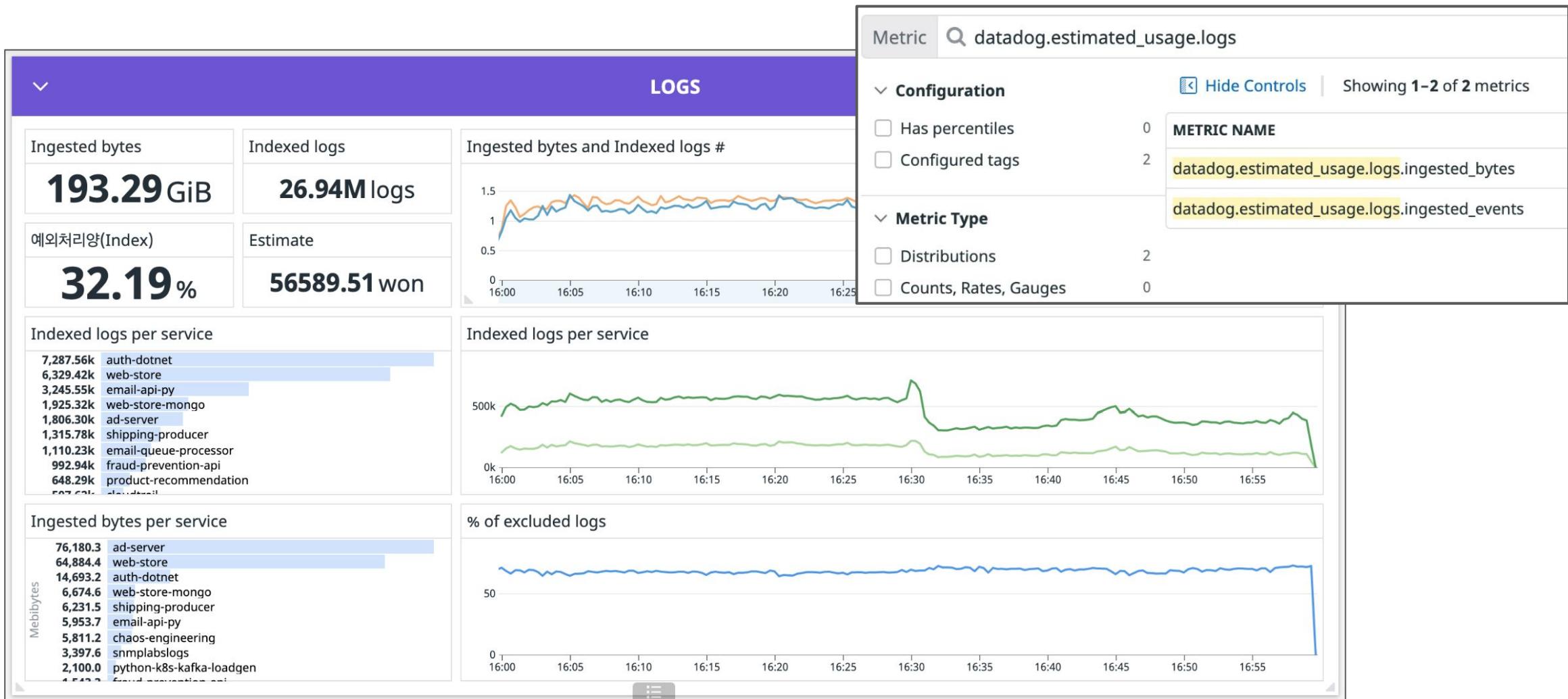
Dashboard 및 알람으로 특이사항 감지

Archive & Rehydrate 기능 활용



#Log Optimization

Metric을 활용한 사용량 모니터링



Q&A

#Quick Review

Q1. Datadog 로그 제품에서 비용 최적화가 가능한 두가지 영역은?

A. INGEST & INDEX 조정을 통해 가능합니다

Q2. Grok Parser processor 사용이 처음입니다. Parse My Logs를 적용해도
파싱이 정상적으로 되지 않습니다

A. Need Help 클릭 혹은 support@datadoghq.com으로 요청

