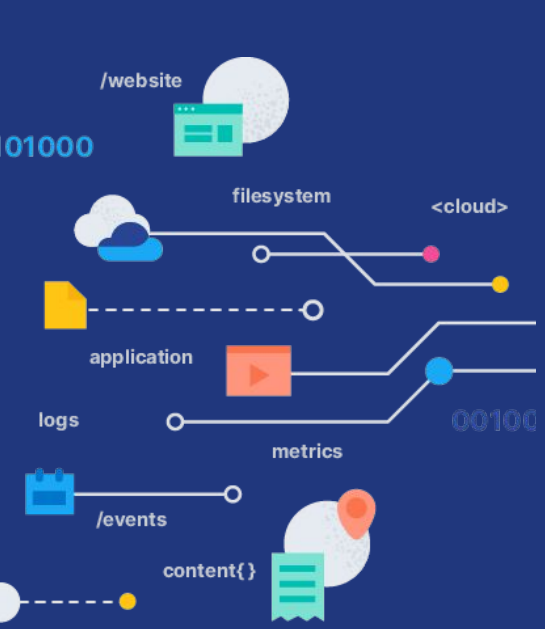
옵저버빌리티 - **APM** 기능 소개

End to End Observability with Elastic APM

Astin Choi
Solutions Architect

엘라스틱 플랫폼



엔터프라이즈 검색

옵저버빌리티

보안

키바나
탐색, 시각화, 대시보드

엘라스틱서치
저장, 검색, 분석

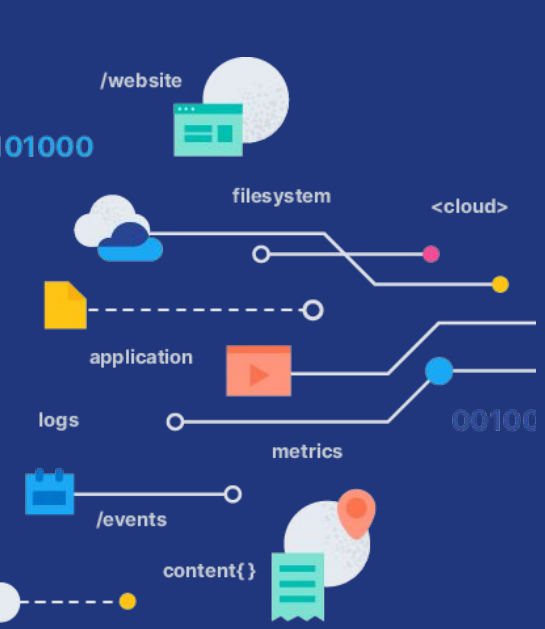
인테그레이션
연결, 수집, 알림

퍼블릭 클라우드

하이브리드

온-프렘

엘라스틱 플랫폼



엔터프라이즈 검색

옵저버빌리티

보안

키바나
탐색, 시각화, 대시보드

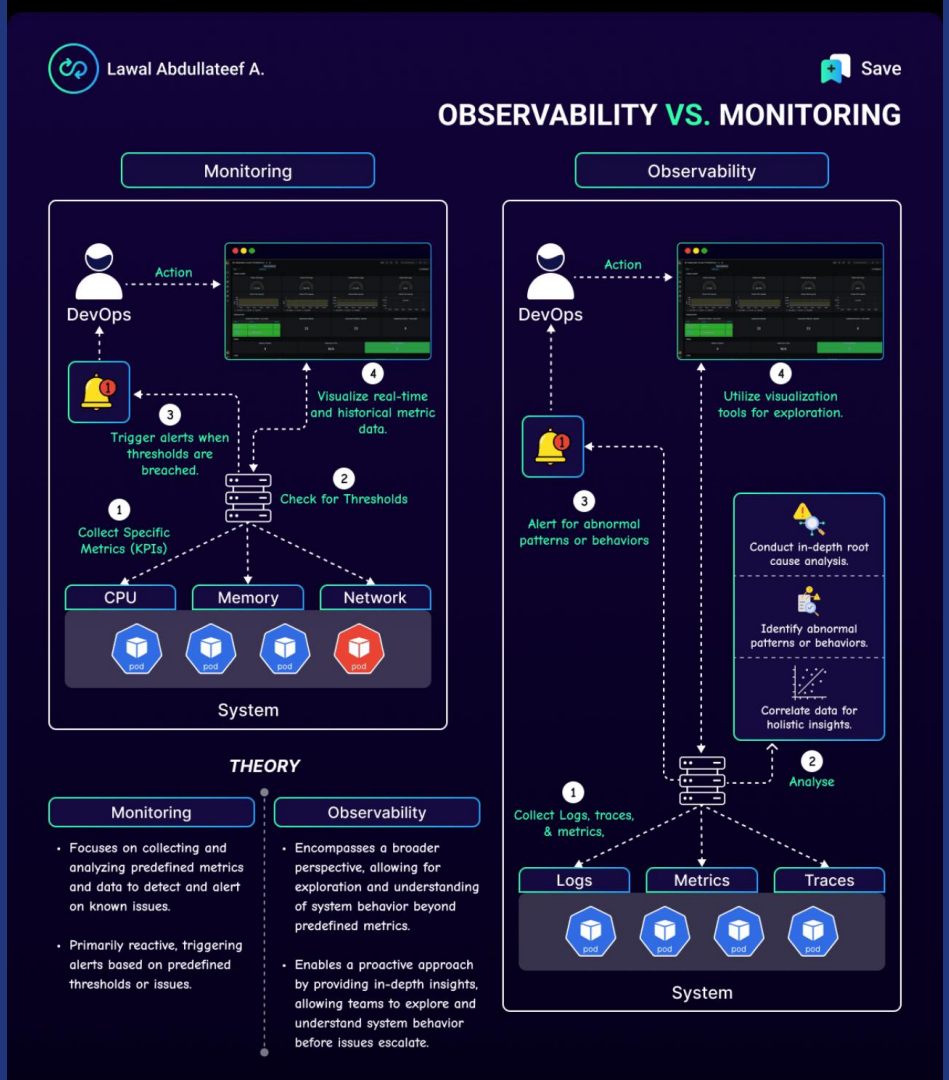
엘라스틱서치
저장, 검색, 분석

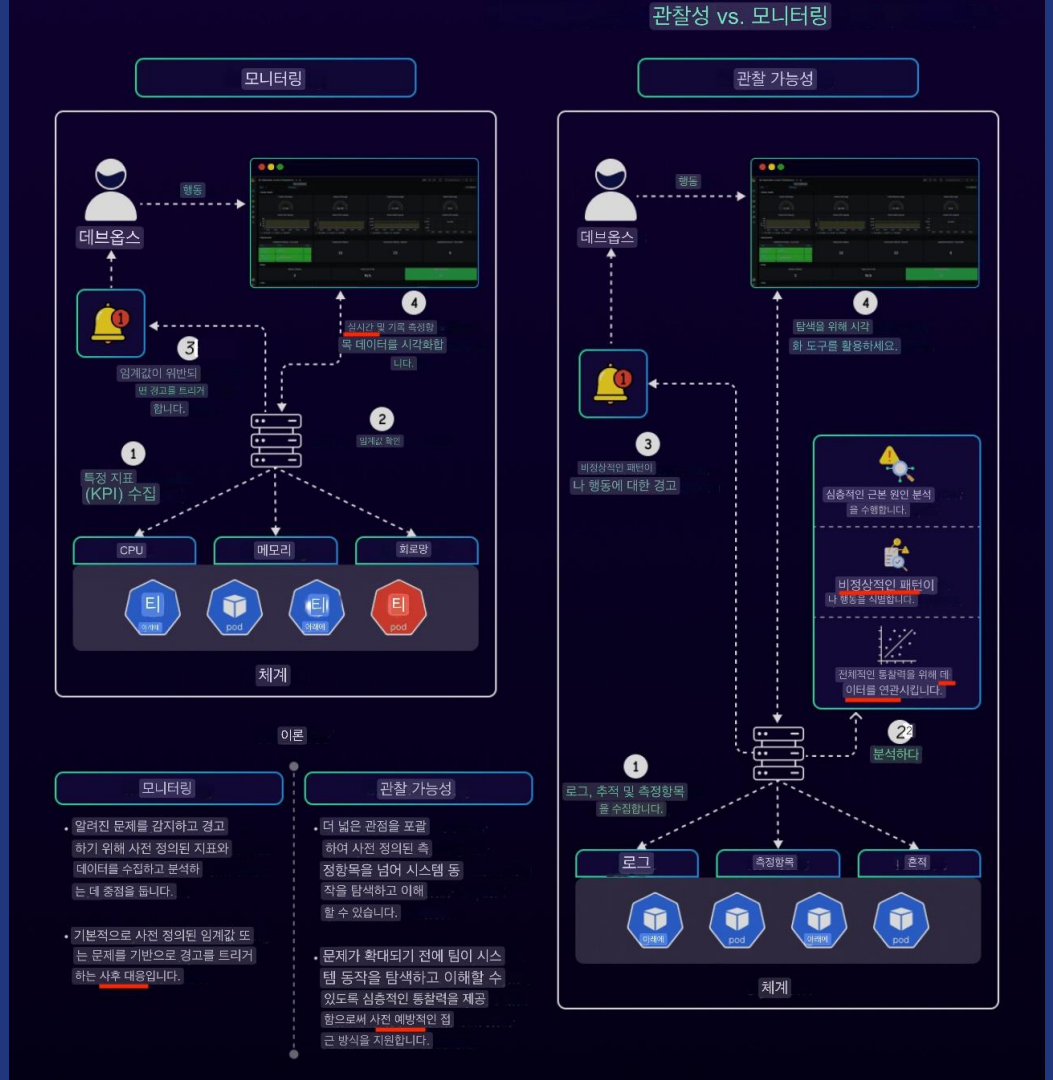
인테그레이션
연결, 수집, 알림

퍼블릭 클라우드

하이브리드

온-프렘


Lawal Abdullateef A.
Save
OBSERVABILITY VS. MONITORING
Monitoring
Observability
Action
DevOps
Visualize real-time and historical metric data.
Trigger alerts when thresholds are breached.
Check for Thresholds
Collect Specific Metrics (KPIs)
CPU
Memory
Network
pod
System
Utilize visualization tools for exploration.
Alert for abnormal patterns or behaviors
Conduct in-depth root cause analysis.
Identify abnormal patterns or behaviors.
Correlate data for holistic insights.
Analyse
Collect Logs, traces, & metrics,
Logs
Metrics
Traces
THEORY
Monitoring
Focuses on collecting and analyzing predefined metrics and data to detect and alert on known issues.
Primarily reactive, triggering alerts based on predefined thresholds or issues.
Observability
Encompasses a broader perspective, allowing for exploration and understanding of system behavior beyond predefined metrics.
Enables a proactive approach by providing in-depth insights, allowing teams to explore and understand system behavior before issues escalate.


관찰성 vs. 모니터링
모니터링
관찰 가능성
데브옵스
행동
1
특정 지표
(KPI) 수집
2
임계값 확인
3
임계값이 위반되
면 경고를 트리거
합니다.
4
실시간 및 기록 측정항
목 데이터를 시각화합
니다.
CPU
메모리
회로망
pod
체계
데브옵스
행동
3
비정상적인 패턴이
나 행동에 대한 경고
4
탐색을 위해 시각
화 도구를 활용하세요.
심층적인 근본 원인 분석
을 수행합니다.
비정상적인 패턴이
나 행동을 식별합니다.
전체적인 통찰력을 위해 데
이터를 연관시킵니다.
2
분석하다
1
로그, 추적 및 측정항목
을 수집합니다.
로그
측정항목
흔적
pod
체계
이론
모니터링
• 알려진 문제를 감지하고 경고
하기 위해 사전 정의된 지표와
데이터를 수집하고 분석하
는 데 중점을 둡니다.
• 기본적으로 사전 정의된 임계값 또
는 문제를 기반으로 경고를 트리거
하는 사후 대응입니다.
관찰 가능성
• 더 넓은 관점을 포괄
하여 사전 정의된 측
정항목을 넘어 시스템 동
작을 탐색하고 이해
할 수 있습니다.
• 문제가 확대되기 전에 팀이 시스
템 동작을 탐색하고 이해할 수
있도록 심층적인 통찰력을 제공
함으로써 사전 예방적인 접
근 방식을 지원합니다.

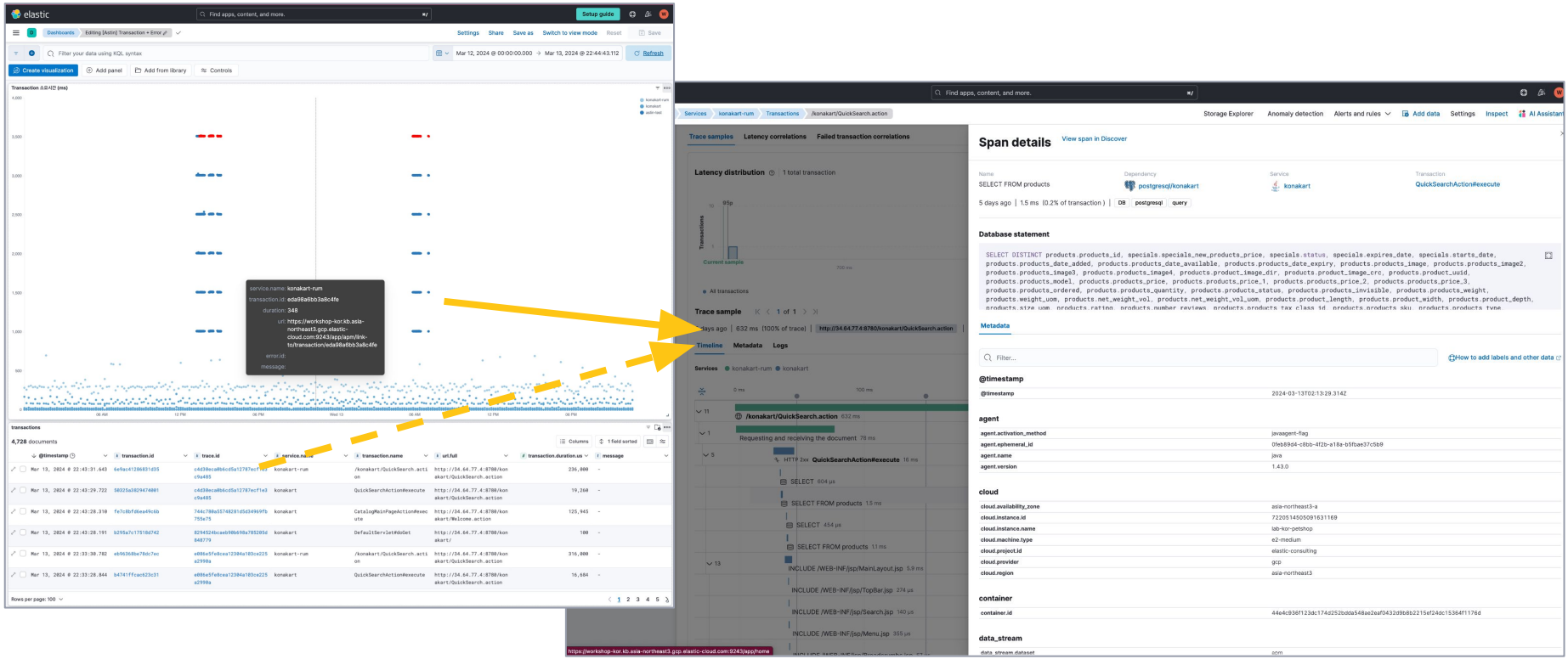
엘라스틱 옵저버빌리티

한 플랫폼, 한 데이터 저장소에서 모두 해결

elastic

사례

S전자 - 실시간 트랜잭션 스캐터플롯



BCR Gates Open
(last 10 minutes)

97% (519) Accepted | 3% (18) Rejected

PAX Count
(last minute)

2 PAX In | 45 PAX Out

BCR Scans
(last hour)

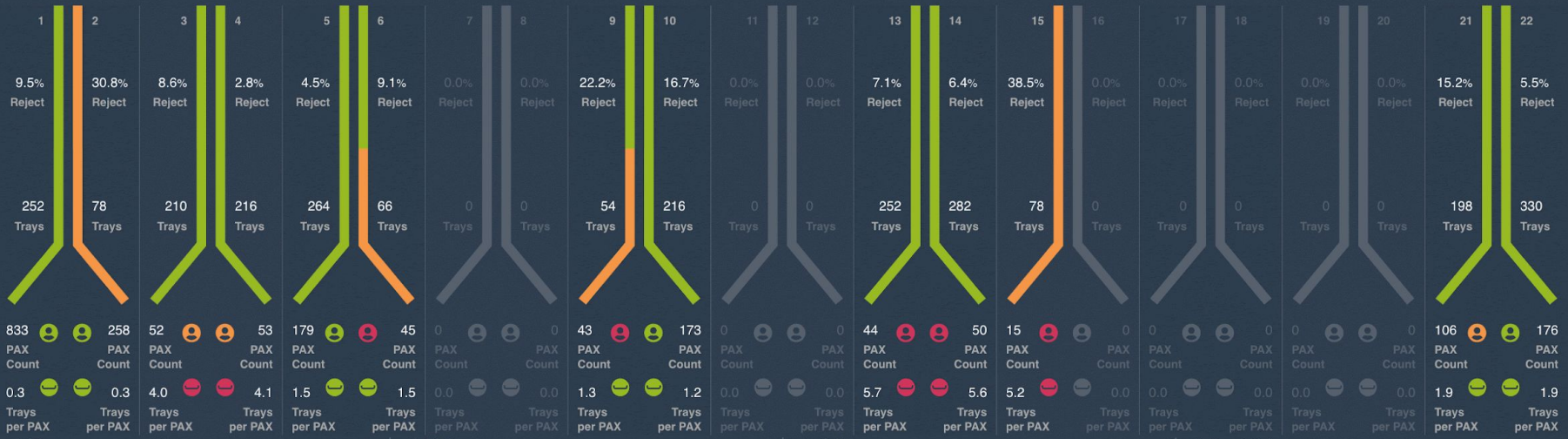
IDL Occupancy
(last 5 minutes)

3241 People

Projected Queue Time
(next minute)

8:44 minutes BCR to Load | 2:39 minutes Load to Exit | 11:23 minutes Total

Lane Usage
(projected hour)



13 Lanes Open

156 Average PAX Count

192 Average Tray Count

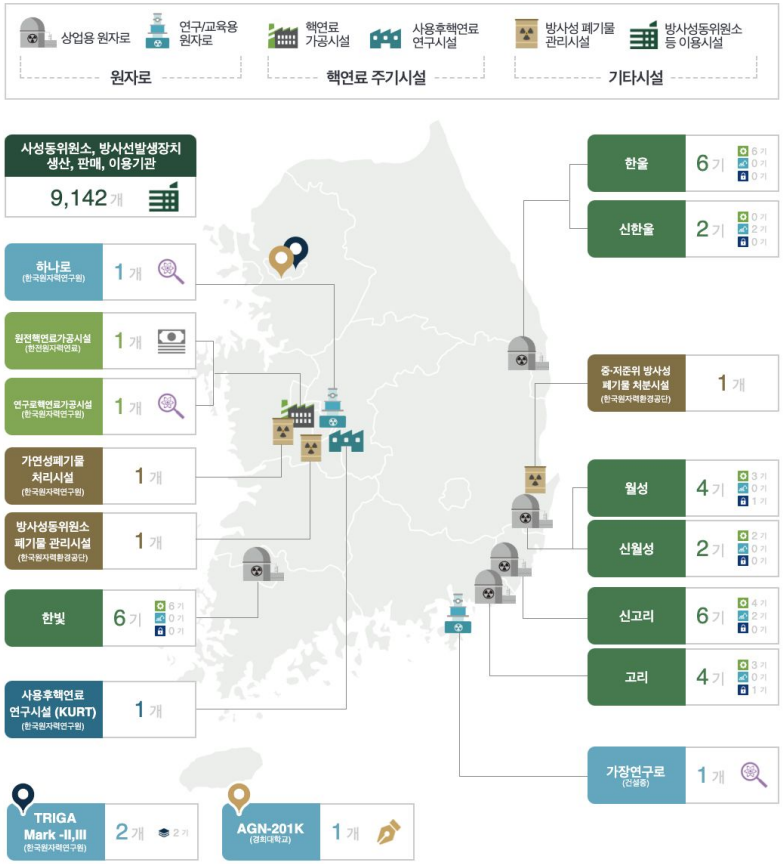
10.1% Average Tray Reject Rate

The information in this dashboard is sample data only

MAG London Stansted Airport

대한민국 원자력·방사선 안전규제 주요현황

2021년 국내 원자력 및 방사선 규제대상 시설·기관 현황



원자력안전규제기관 한눈에 보기

* 출처 : (산하기관 인력, 예산) 공공기관 경영정보 공개시스템(alio.go.kr) 기관별 2021년 2분기 보고서(2021년 6월)
(원안위 인력) 원자력안전위원회와 그 소속기관 직제 시행규칙(2021년 3월)
(원안위 예산) 원자력안전위원회 2021년도 예산 및 기금운용계획(2020년 12월)

해외 주요국

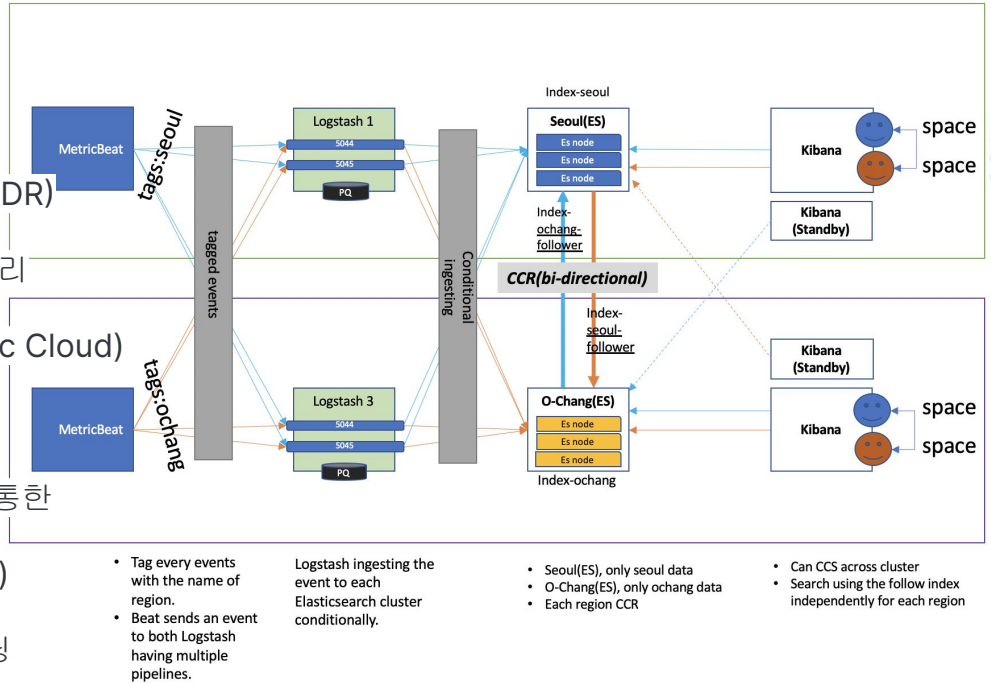
	미국	프랑스	일본	캐나다
예산	약 8억 4400만 달러 (한화 약 9,541억원)	약 6,577만 유로 (한화 약 881억원)	약 728억 엔 (한화 약 7,406억원)	약 1억 4,375만 캐나다 달러 (한화 약 1,311억원)
인력	2,868 FTE	529명	1,089명	913 FTE

elastic

기상청

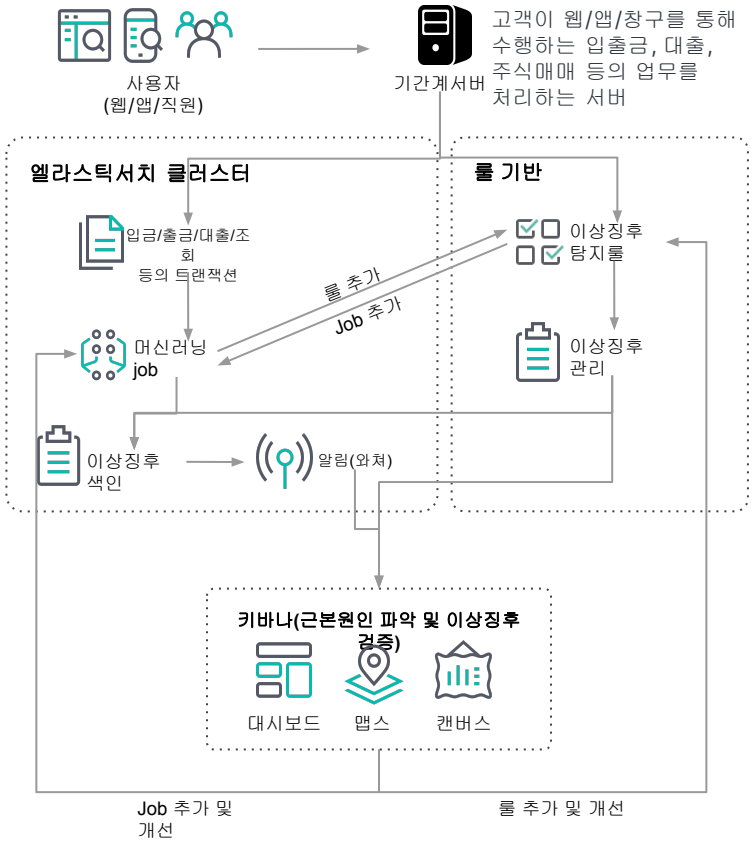
기상청

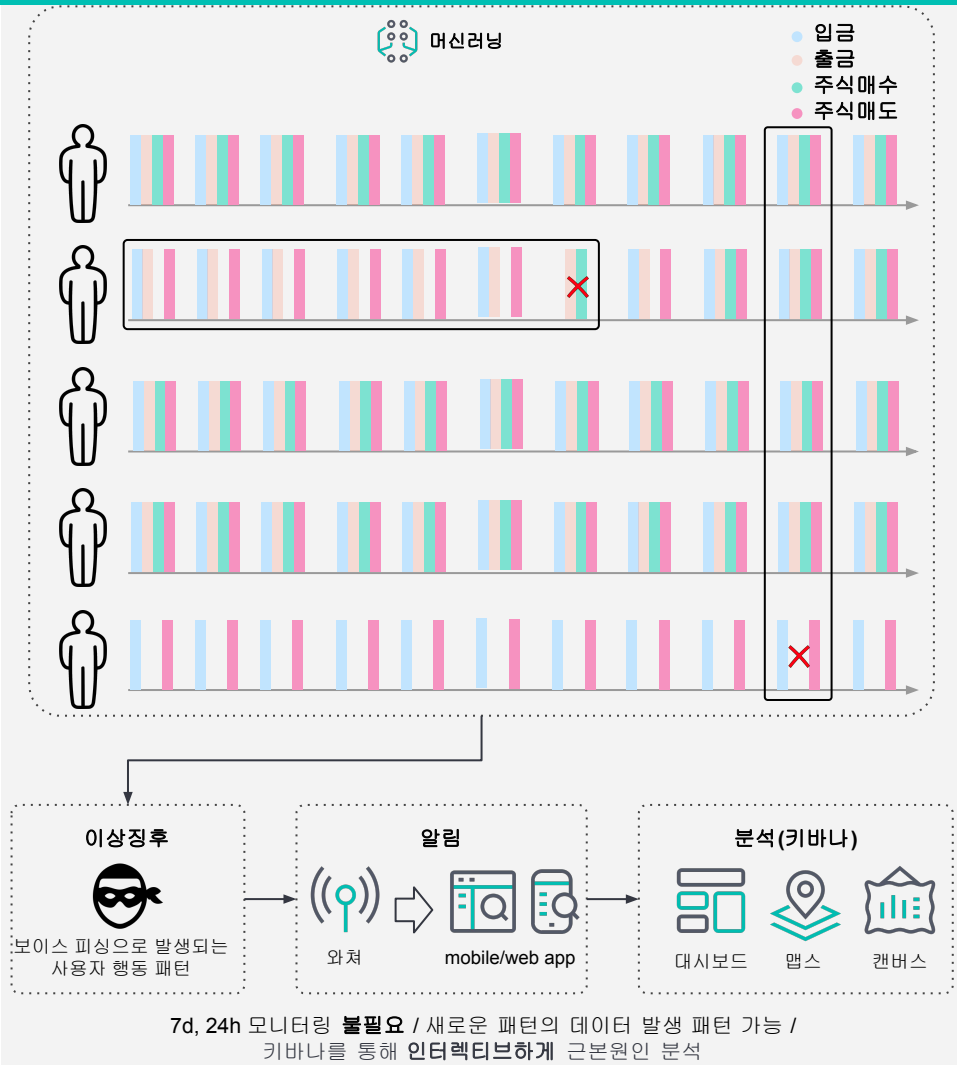
- 서울/오창 데이터 센터 인프라 모니터링
- 800여대 이상의 인프라 로그 실시간 수집
- CCR 기능을 통한 실시간 로그 Sync (Active DR)
- Ingest Manager 를 통한 수집 Agent 원격관리
- Hybrid 환경 (On-prem/Private Cloud/Public Cloud) 통합 모니터링
- Index Lifecycle Management 기능 적용을 통한 데이터 관리 (Hot/Warm/Cold Architecture)
- Drill down 기능을 통한 통합 인프라 모니터링



elastic

S증권





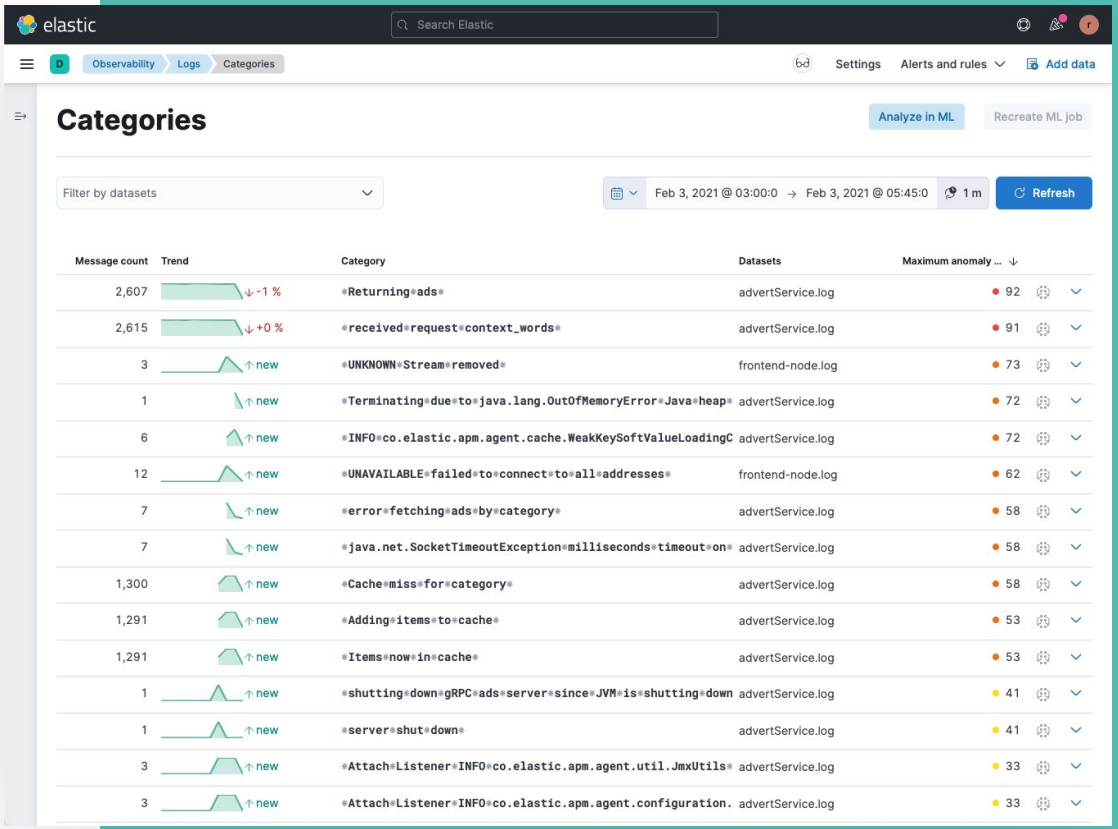
7d, 24h 모니터링 **불필요** / 새로운 패턴의 데이터 발생 패턴 가능 /
키바나를 통해 **인터렉티브하게** 근본원인 분석

주요 기능

Elastic Observability

로그 분석

- 하이브리드 클라우드를 위한 확장 가능한 중앙 집중식 로그 모니터링
- 로그 분류와 머신 러닝을 기반으로 한 로그 패턴 분석 및 이상 징후 탐지
- 클러스터 통합 검색을 통한 강력한 로그 검색 지원
- 데이터 계층을 통해 성능과 스토리지를 효율적으로 최적화

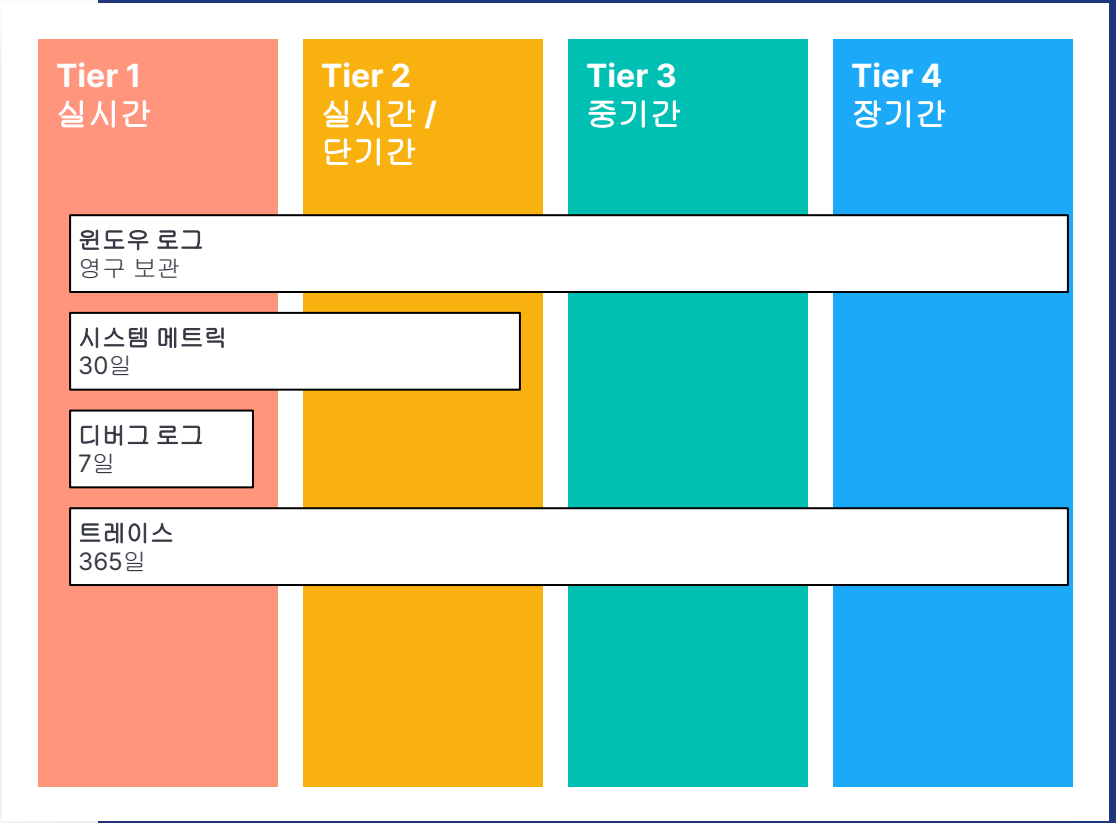


비용 효율적인 데이터 보관 /w data tiers

비용 효율적인 데이터 보관

데이터 종류별로 사용자 정의 가능

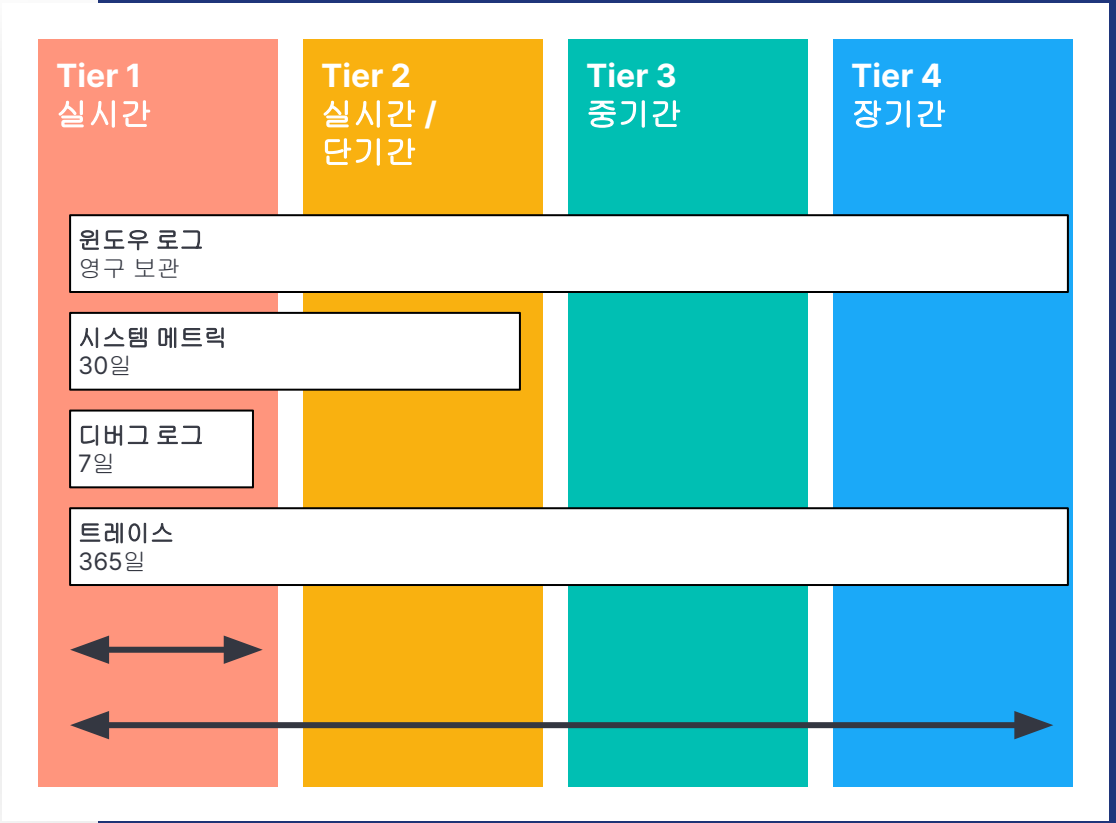
- 데이터를 계층 이동시 소스별로 사용자 정의 가능
- 보관 주기 무제한



끊김없는 검색

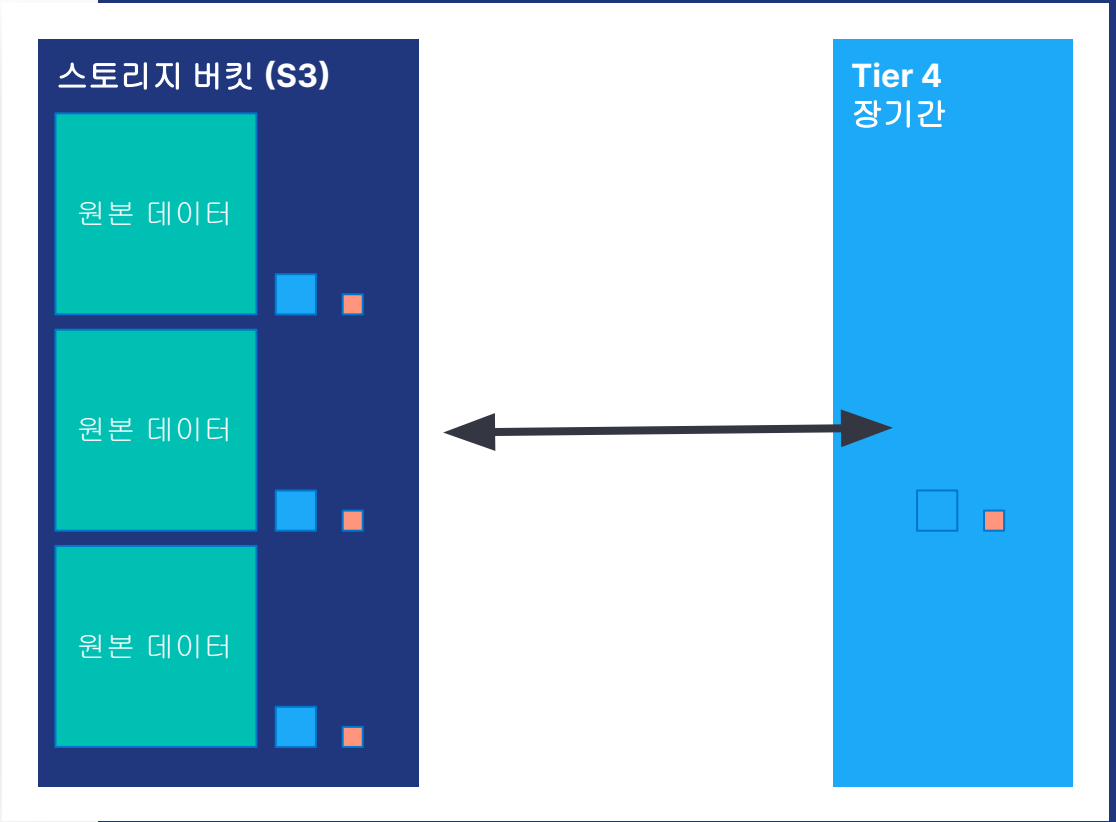
별도 수동 작업 없이

- 전체 데이터에 대한 동일 UX
- 복원 불필요



효율적인 과거 데이터 검색

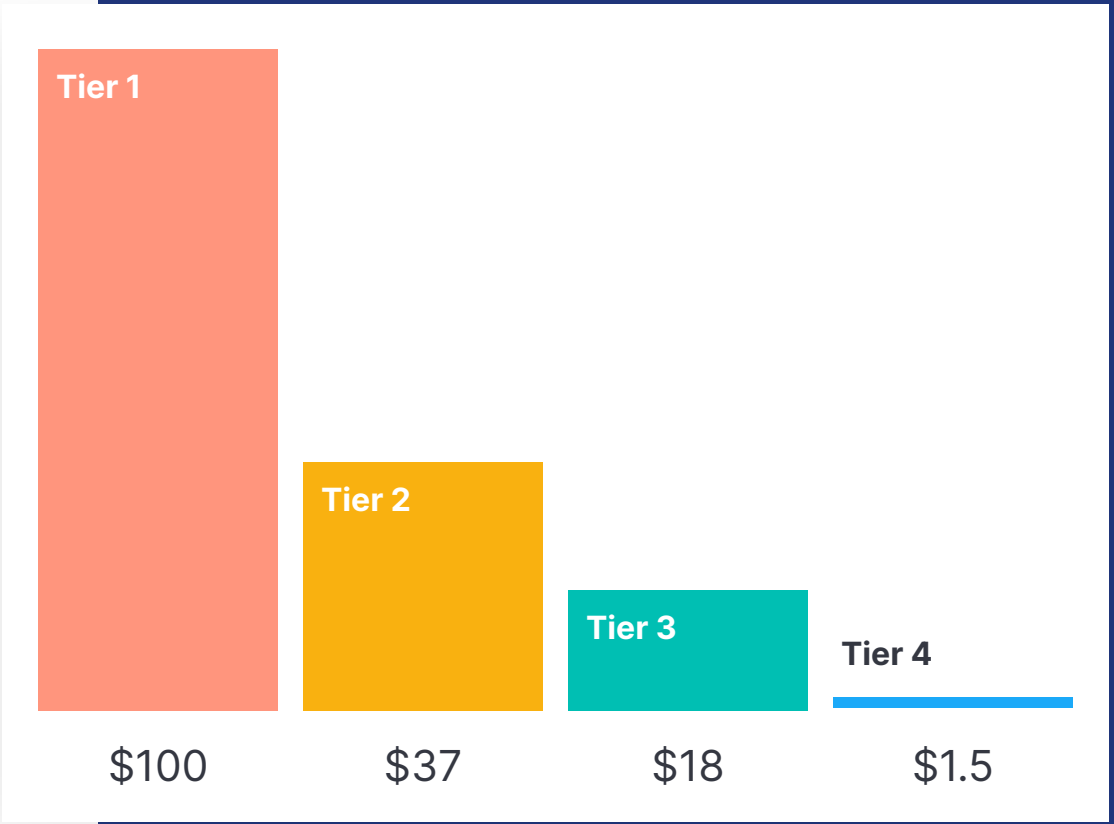
- 필요한 데이터만 로딩
- 로컬 캐시
- 복원 작업 혹은 수동 개입 불필요
- 다른 접근 방식에 비해 빠른 쿼리 성능
- 하드웨어 비용 감소
- 오브젝트 스토리지 API 비용 감소
- 데이터 전송 비용 감소



비용 효율적인 데이터 보관

계층별 데이터 저장 비용

- 지속적으로 비용 감소
- 저렴한 장기 스토리지
- 계층간 유연한 데이터 이동

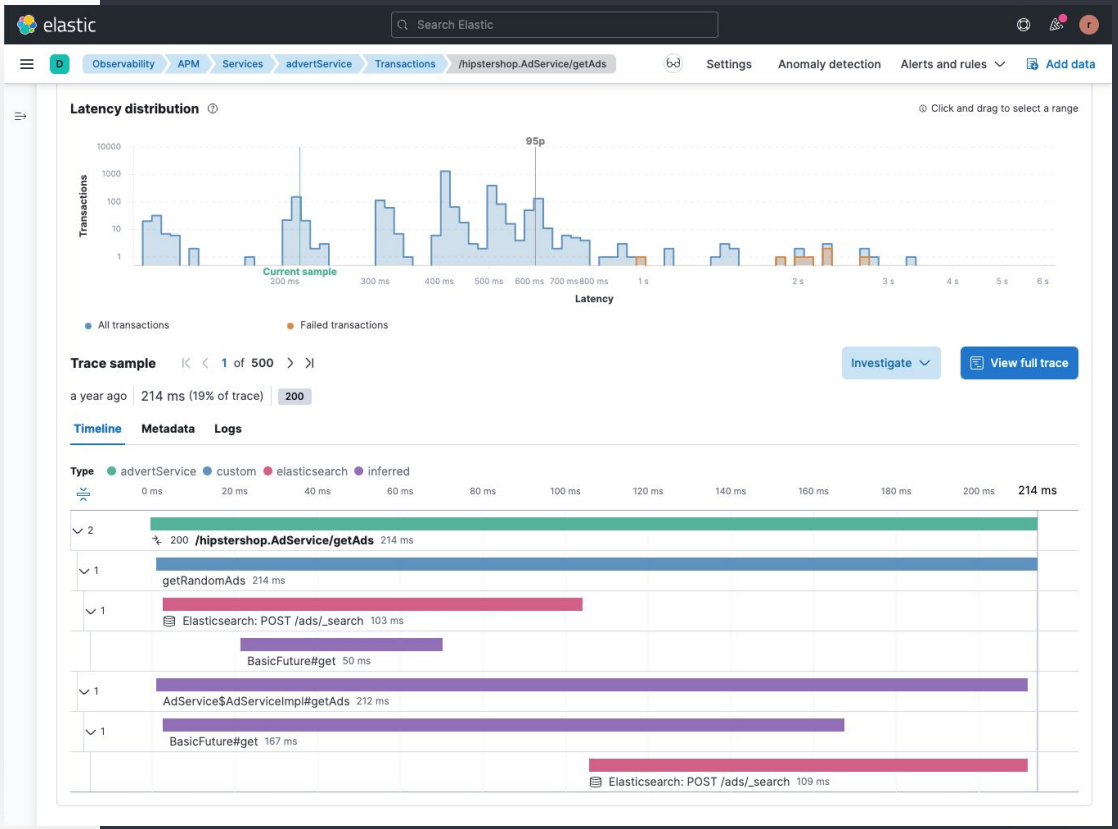


*approximation, data from https://cloud.elastic.co/pricing

Elastic Observability

앱 성능 모니터링 (APM)

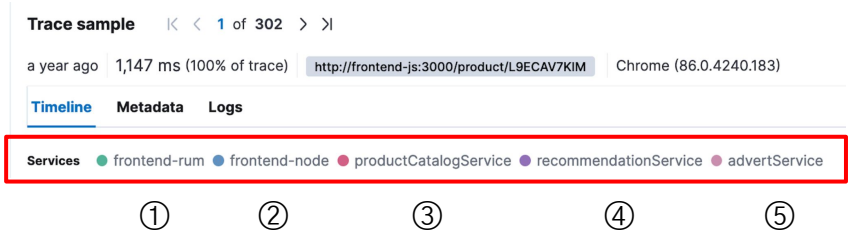
- 엔드투엔드 분산 트레이싱을 통한 코드 품질 향상
- ML 기반 상태 지표와 이상 징후 탐지 기능을 통해 신속한 문제 해결
- 상관 관계 분석을 통해 속도 저하 및 에러 근본 원인 식별
- OpenTelemetry와 엘라스틱 에이전트를 통해 별도의 설정 없이 즉시 사용

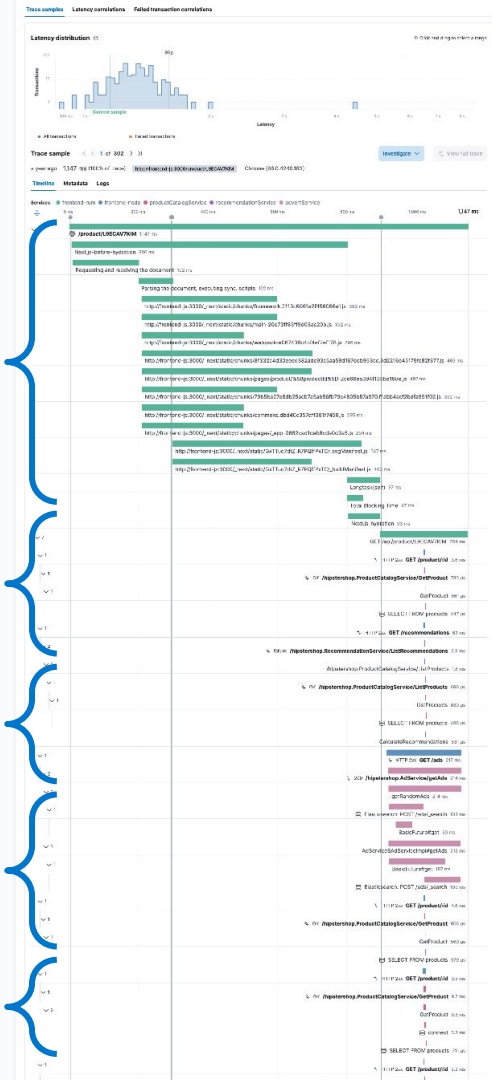


분산 트레이싱으로 End-to-End 분석

여러 서비스 트랜잭션을 하나의 trace.id로 연동

- 사용자 관점에서 하나의 트랜잭션이지만
- MSA 환경에서 다수 서비스로 분리
- 하나의 '분산 트레이싱'으로 분석





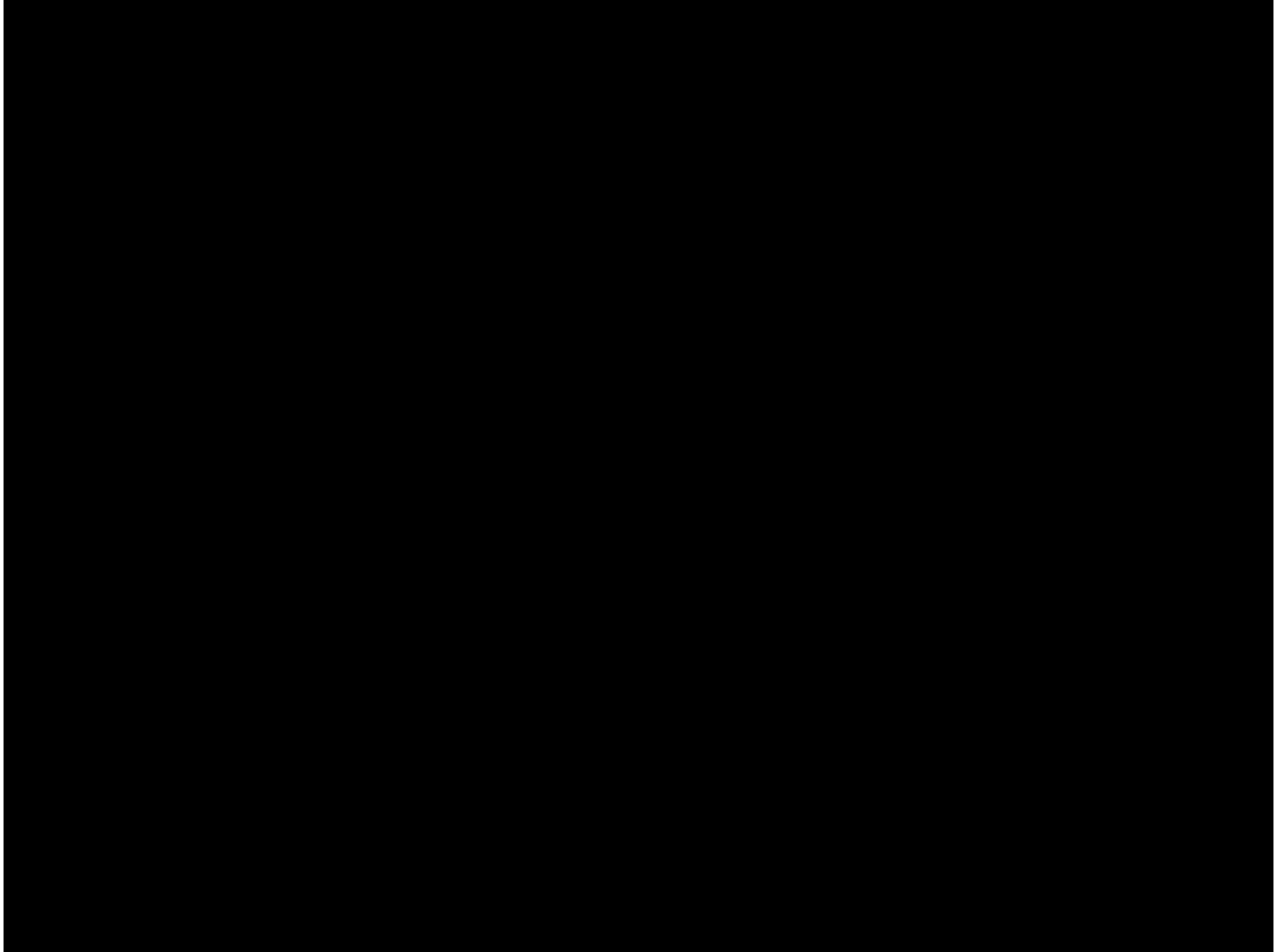
① RUM
Javascript

② 서버사이드 웹
frontend-node(Node.js)

③ 제품 카탈로그 서비스
productCatalogService (Go)

④ 추천 서비스
recommendationService (Python)

⑤ 광고 서비스
advertService (Java)

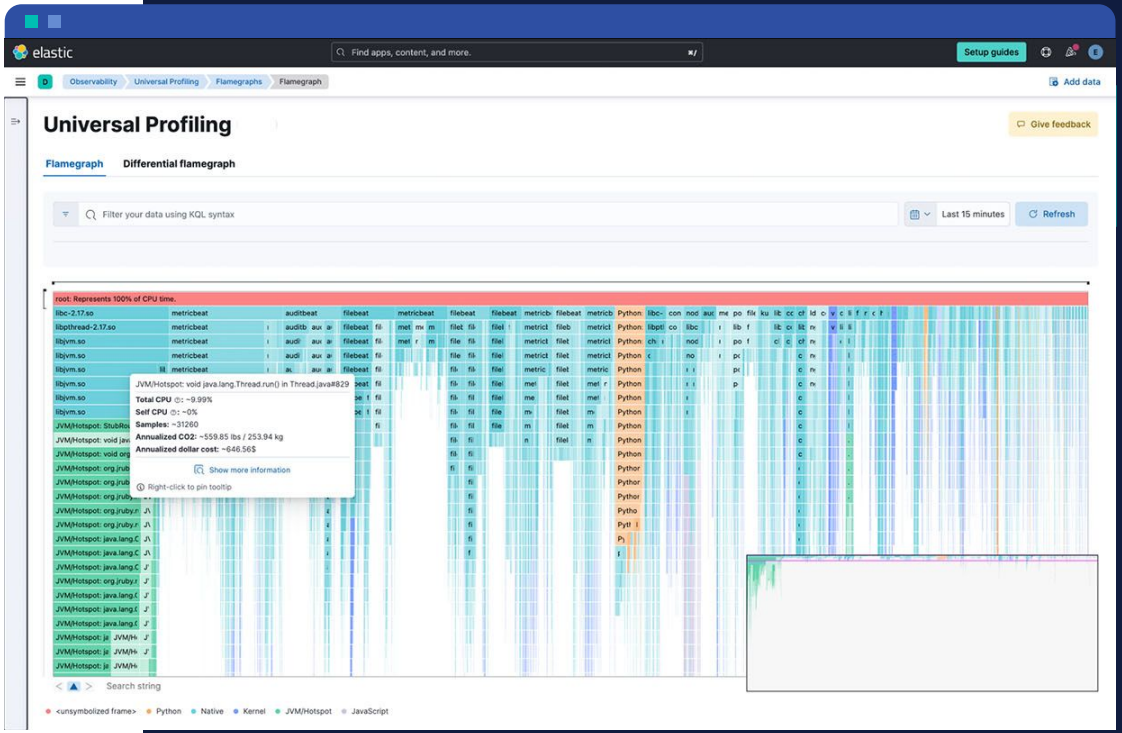


elastic

Elastic Observability

프로파일링

- 다양한 언어와 컨테이너화된 환경 등 전반에서 시스템을 가시화
- 프로덕션 환경에서 낮은 오버헤드로 프로파일링 사용 가능
- 인프라, 앱 등 성능이 나오지 않거나 비효율적인 코드 및 함수 식별
- 컴퓨팅 자원 낭비 제거



elastic

Universal Profiling

Give feedback

TopN functions | Differential TopN functions

Baseline functions

container.name : "cart-service-v1" | Last 15 minutes

Comparison functions

container.name :"cart-service-v2" | Last 15 minutes

Normalize by: Time

Gained overall performance by	Annualized CO2 emission impact	Annualized cost impact	Total number of samples
↑ 53.71%	4.68 lbs / 2.12 kg ↑2.17 lbs / 0.98 kg (53.71%)	$44.1 ↑$20.41 (53.71%)	2,132 ↑987 (53.71%)

	Function	Samples	Self CPU	Total CPU
1	python3.7: lookdict_unicode_nodummy ../Objects/dictobject.c#854	111	5.21%	5.21%
2	python3.7: _PyType_Lookup ../Objects/typeobject.c#3085	97	4.55%	5.21%
3	python3.7: _PyObject_GetMethod ../Objects/object.c#1144	89	4.17%	8.91%
4	Python: flask_route_interest interest.py#31	83	3.89%	62.85%
5	python3.7: _PyEval_EvalCodeWithName ../Python/ceval.c#3946	66	3.10%	7.65%
6	python3.7: frame_dealloc ../Objects/frameobject.c#470	60	2.81%	3.47%
7	Python: __getitem__ os.py#679	59	2.77%	32.97%
8	Python: encode os.py#752	51	2.39%	9.99%

	Function	Samples	Self CPU	Total CPU	Diff
1	python3.7: lookdict_unicode_nodummy ../Objects/dictobject.c#847	70 ↑36.94% rel ↑4.15% abs	7.09% (↓1.89%)	7.29% (↓2.09%)	
2	python3.7: _PyType_Lookup ../Objects/typeobject.c#3074	45 ↑53.61% rel ↑5.27% abs	4.56% (↓<0.01%)	7.19% (↓1.99%)	
3	Python: flask_route_interest interest.py#27	40 ↑51.81% rel ↑4.36% abs	4.05% (↓0.16%)	21.58% (↑41.27%)	↓ 1
4	vmlinux: _raw_spin_unlock_irqrestore vmlinux+0xb6546e	35 ↑16.67% rel ↑0.71% abs	3.55% (↓1.58%)	3.55% (↓1.58%)	↓ 8
5	python3.7: _PyObject_GenericGetAttrWithDict ../Objects/object.c#1235	32 ↑3.03% rel ↑0.10% abs	3.24% (↓1.69%)	8.81% (↓4.26%)	↓ 11
6	python3.7: pymalloc_alloc ../Objects/obmalloc.c#1436	24 ↑46.67% rel ↑2.13% abs	2.43% (↓0.32%)	2.43% (↓0.32%)	↓ 5

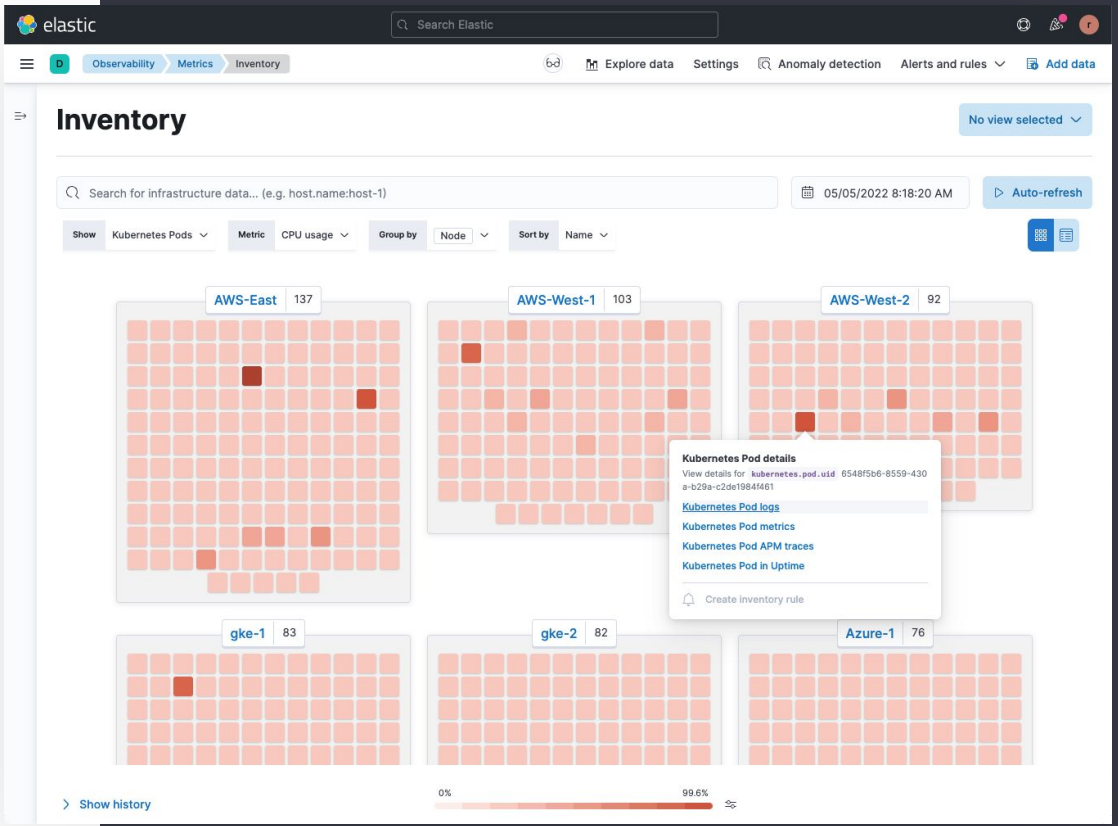
elastic

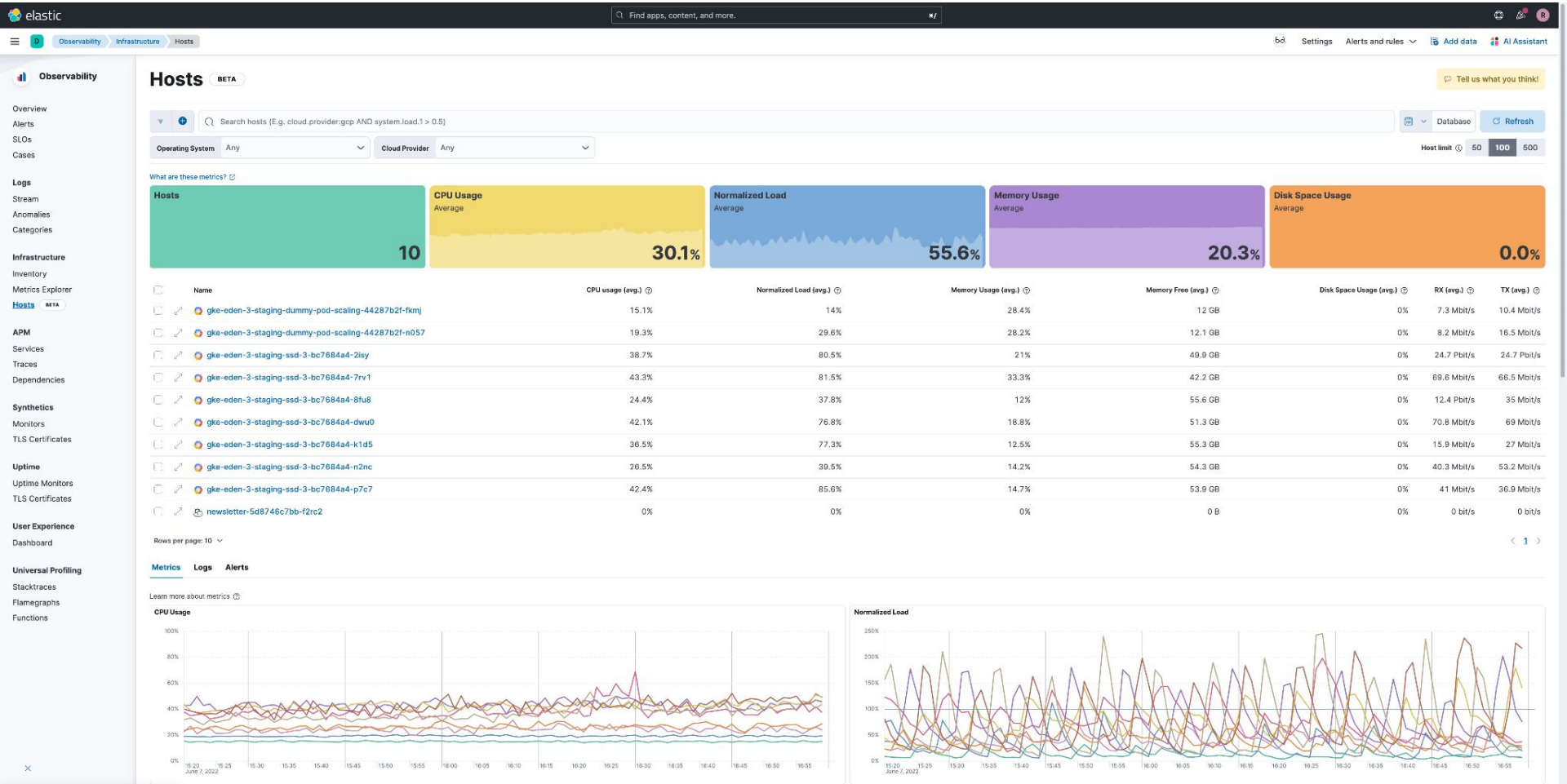
elastic

Elastic Observability

모든 환경에 걸쳐 통합된 가시성

- 온프렘/클라우드 인프라와 3-티어 아키텍처에 대한 인사이트 제공
- AWS, Azure, Google 상에 존재하는 350개 이상의 통합 제공
- Kubernetes (온프렘/클라우드 모두 지원)
- 복잡한 환경에서 문제 원인을 빠르게 찾을 수 있음




elastic
Find apps, content, and more.
Observability
Infrastructure
Hosts
Settings
Alerts and rules
Add data
AI Assistant
Observability
Overview
Alerts
SLOs
Cases
Logs
Stream
Anomalies
Categories
Infrastructure
Inventory
Metrics Explorer
Hosts BETA
APM
Services
Traces
Dependencies
Synthetics
Monitors
TLS Certificates
Uptime
Uptime Monitors
TLS Certificates
User Experience
Dashboard
Universal Profiling
Stacktraces
Flamegraphs
Functions
Hosts
BETA
Tell us what you think!
Search hosts (E.g. cloud.provider:gcp AND system.load.1 > 0.5)
Database
Refresh
Operating System
Any
Cloud Provider
Any
Host limit
50
100
500
What are these metrics?
Hosts
10
CPU Usage
Average
30.1%
Normalized Load
Average
55.6%
Memory Usage
Average
20.3%
Disk Space Usage
Average
0.0%
Name
CPU usage (avg.)
Normalized Load (avg.)
Memory Usage (avg.)
Memory Free (avg.)
Disk Space Usage (avg.)
RX (avg.)
TX (avg.)
gke-eden-3-staging-dummy-pod-scaling-44287b2f-fkmj 15.1% 14% 28.4% 12 GB 0% 7.3 Mbit/s 10.4 Mbit/s
gke-eden-3-staging-dummy-pod-scaling-44287b2f-n057 19.3% 29.6% 28.2% 12.1 GB 0% 8.2 Mbit/s 16.5 Mbit/s
gke-eden-3-staging-ssd-3-bc7684a4-2isy 38.7% 80.5% 21% 49.9 GB 0% 24.7 Pbit/s 24.7 Pbit/s
gke-eden-3-staging-ssd-3-bc7684a4-7rv1 43.3% 81.5% 33.3% 42.2 GB 0% 69.6 Mbit/s 66.5 Mbit/s
gke-eden-3-staging-ssd-3-bc7684a4-8fu8 24.4% 37.8% 12% 55.6 GB 0% 12.4 Pbit/s 35 Mbit/s
gke-eden-3-staging-ssd-3-bc7684a4-dwu0 42.1% 76.8% 18.8% 51.3 GB 0% 70.8 Mbit/s 69 Mbit/s
gke-eden-3-staging-ssd-3-bc7684a4-k1d5 36.5% 77.3% 12.5% 55.3 GB 0% 15.9 Mbit/s 27 Mbit/s
gke-eden-3-staging-ssd-3-bc7684a4-n2nc 26.5% 39.5% 14.2% 54.3 GB 0% 40.3 Mbit/s 53.2 Mbit/s
gke-eden-3-staging-ssd-3-bc7684a4-p7c7 42.4% 85.6% 14.7% 53.9 GB 0% 41 Mbit/s 36.9 Mbit/s
newsletter-5d8746c7bb-f2rc2 0% 0% 0% 0 B 0% 0 bit/s 0 bit/s
Rows per page: 10
1
Metrics
Logs
Alerts
Learn more about metrics
CPU Usage
Normalized Load

elastic

Elastic Observability

통합 환경으로 사일로 제거

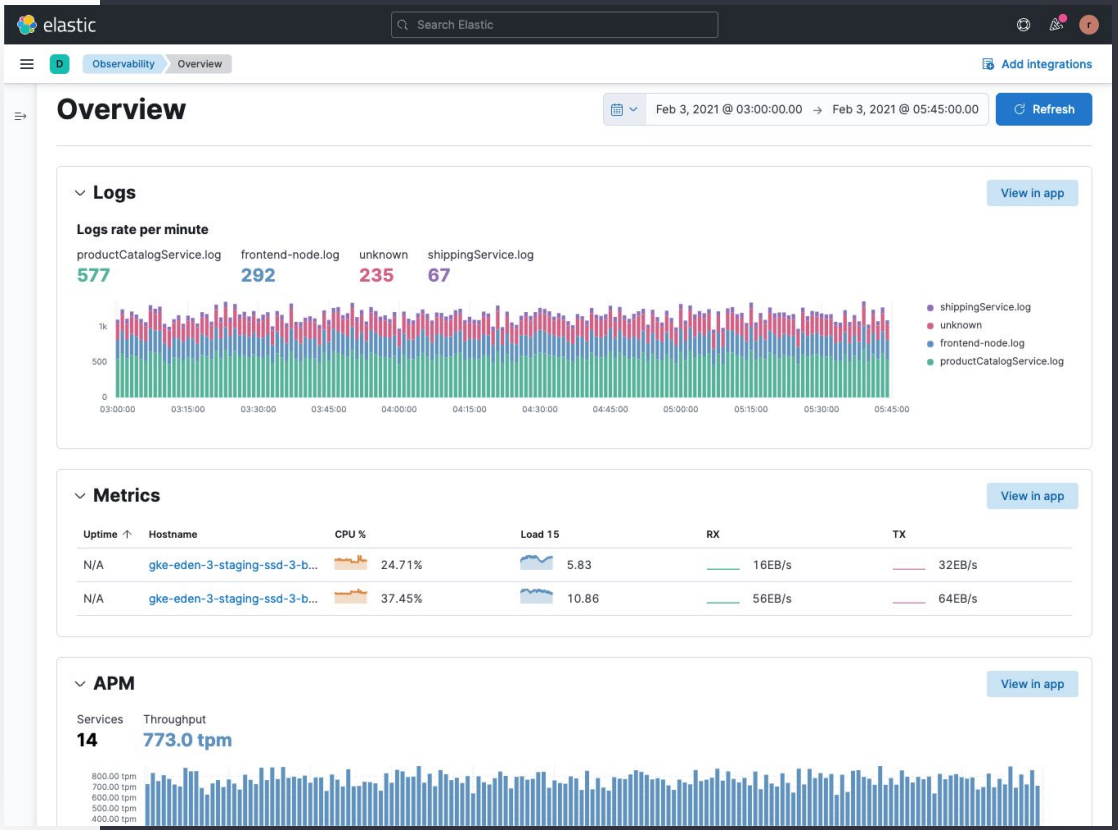
- 모든 비즈니스 및 운영 데이터를 위한 단일 플랫폼
- 메트릭, 로그, 트레이스를 컨텍스트 기반으로 연결해 빠르게 문제 분석
- 업계 유일의 개방형 공통 데이터 모델

```
src:10.42.42.42
client_ip:10.42.42.42
apache2.access.remote_ip: 10.42.42.42
context.user.ip:10.42.42.42
src_ip:10.42.42.42
```

⇩

```
source.ip:10.42.42.42
```

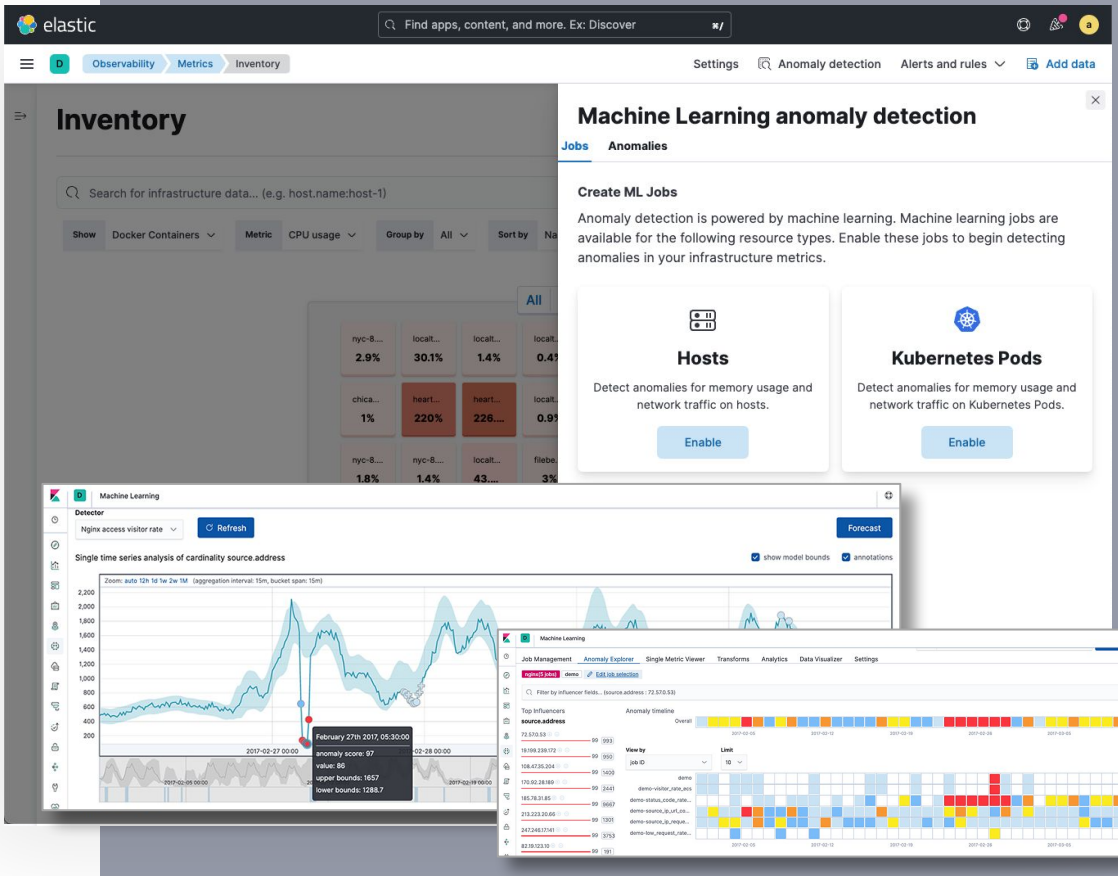
- 다양한 팀이 협업 할 수 있는 환경



Elastic Observability

실행 가능한 인사이트

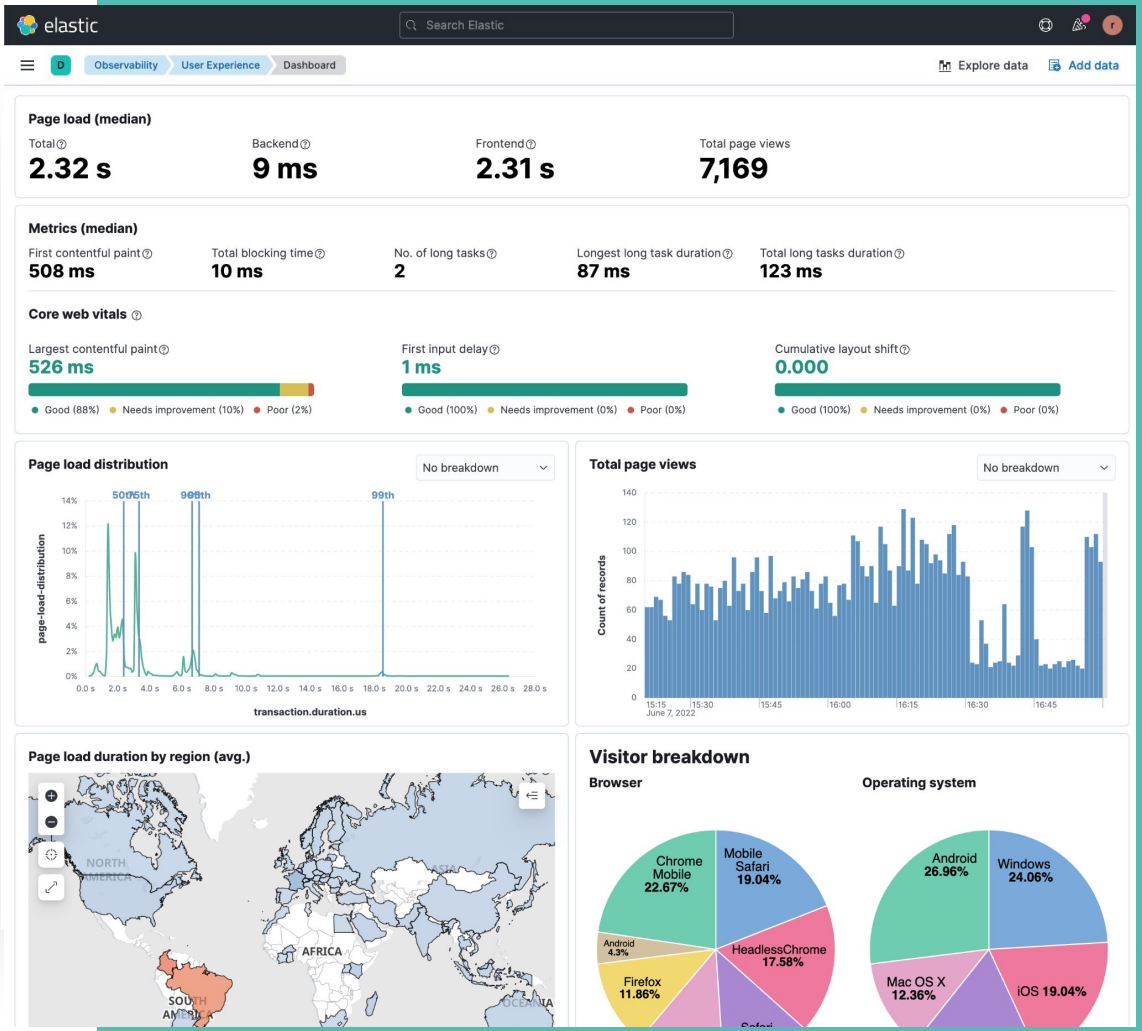
- 코딩이 필요하지 않은 빌트인 머신 러닝
- AI를 기반으로 하는 이상 징후 탐지
- 자동화 된 APM 상관관계 생성으로 편리한 근본 원인 분석
- 강력한 검색을 통한 알려지지 않은 불확실한 일(unknown unknowns) 파악
- MTTD와 MTTR 단축



Elastic Observability

사용자 경험 측정 (RUM)

- 시간의 흐름에 따른 인프라, 애플리케이션 및 비즈니스 동향 추적
- 고객 경험을 측정하고 사용자 여정을 능동적으로 파악
- 프런트엔드에서 백엔드까지 한 번에 추적하여 문제 해결
- SLO 설정, SLI 및 SLA 측정



Error occurrence

View 19 occurrences in Discover.

a few seconds ago | HeadlessChrome (79.0.3945) | customers

Exception stack trace | Metadata

Test CaptureError

webpack:///./src/rum.js in call at line 78

```
73.         featureFlags: ['double-trouble', '4423-hotfix']
74.     }
75. })
76.
77. try {
78.     throw new Error('Test CaptureError')
79. } catch (e) {
80.     apm.captureError(e)
81. }
82.
83.
```

webpack:///webpack/bootstrap b1113b74ced4a8bb4dd9 in this at line 19

```
14.                         l: false,
15.                         exports: {}
16.                 };
17.
18.                 // Execute the module function
19.                 modules[moduleId].call(module.exports, module, module.exports, __webpack_require__);
20.
21.                 // Flag the module as loaded
22.                 module.l = true;
23.
24.                 // Return the exports of the module
```

1 library frame

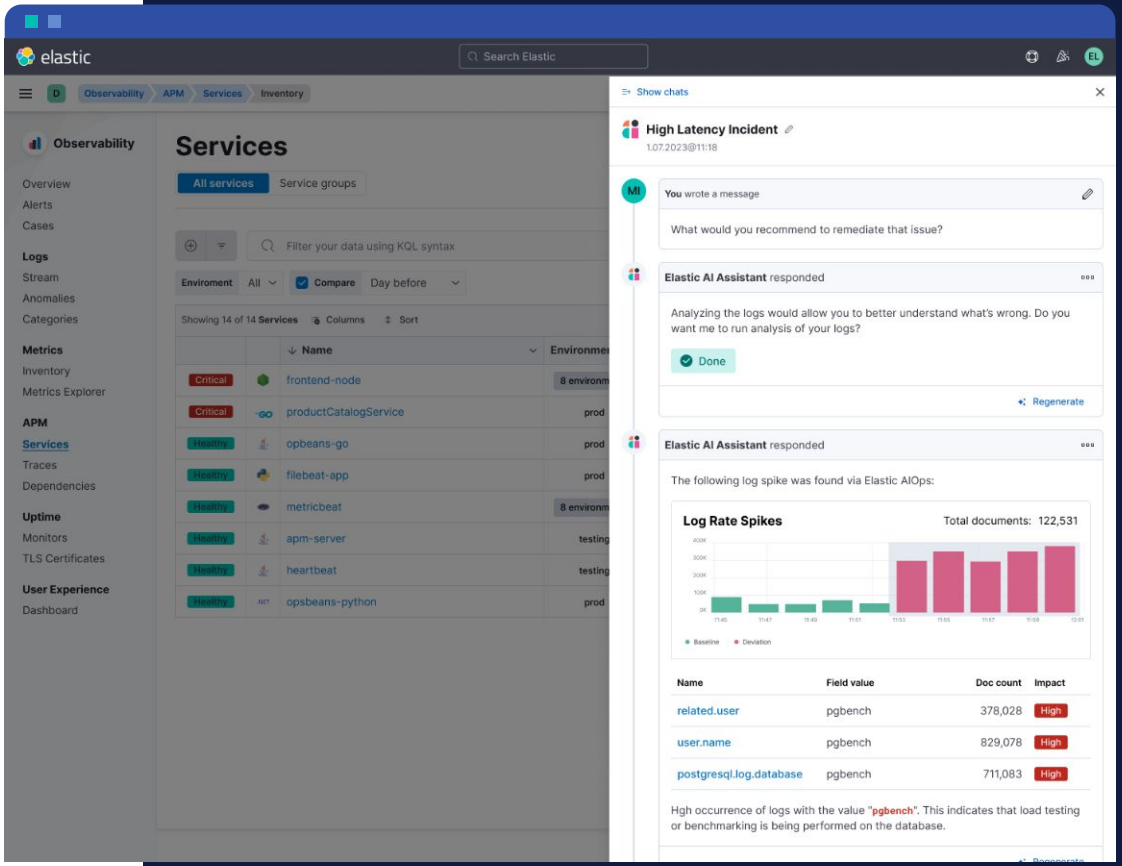
elastic

Elastic Observability

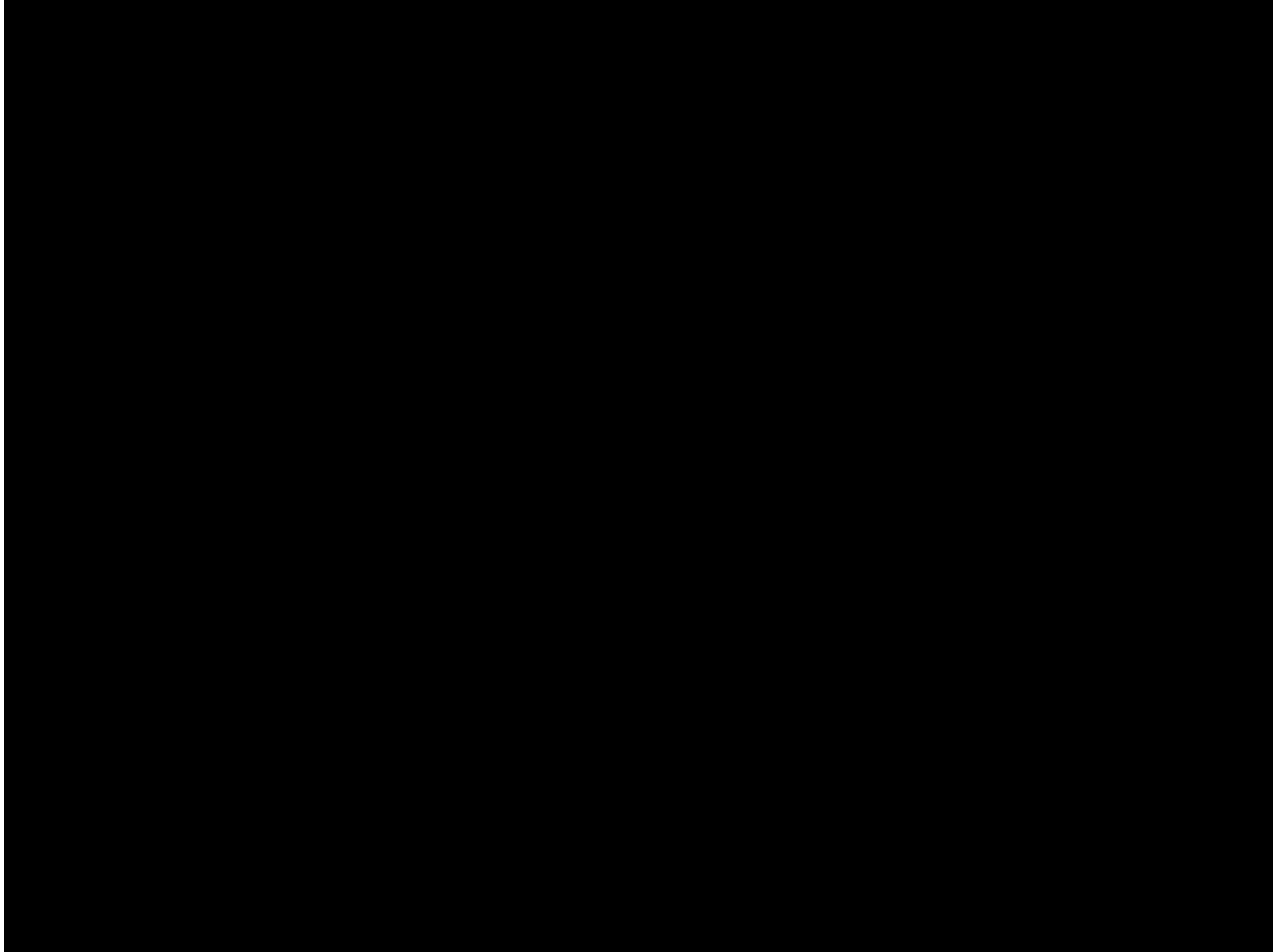
AI 어시스턴트

Powered by ESRE

- 인시던트 관리 및 근본 원인 분석 지원
- 문제를 대화형으로 해결 - 생성형AI
- LLM에 의존하지 않는 개방형 기능
- 컨텍스트 기반으로 신뢰할 수 있는 데이터 제공
- 실제 데이터 기반으로 가이드 (runbook) 제공



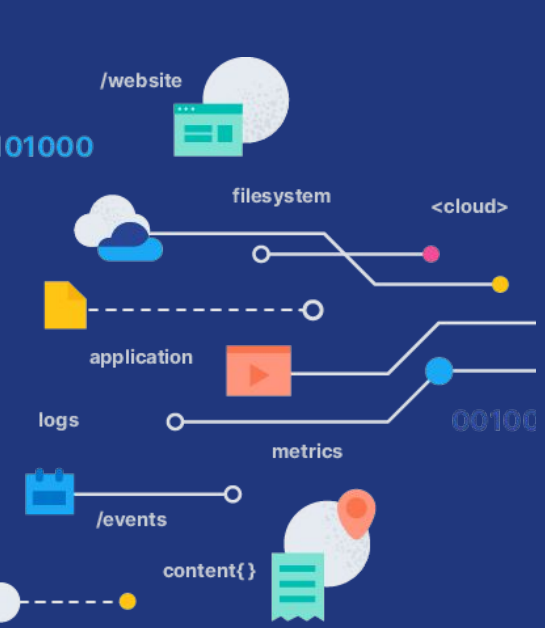
elastic



elastic

데이터 수집

엘라스틱 플랫폼



엔터프라이즈 검색

옵저버빌리티

보안

키바나
탐색, 시각화, 대시보드

엘라스틱서치
저장, 검색, 분석

인테그레이션
연결, 수집, 알림

퍼블릭 클라우드

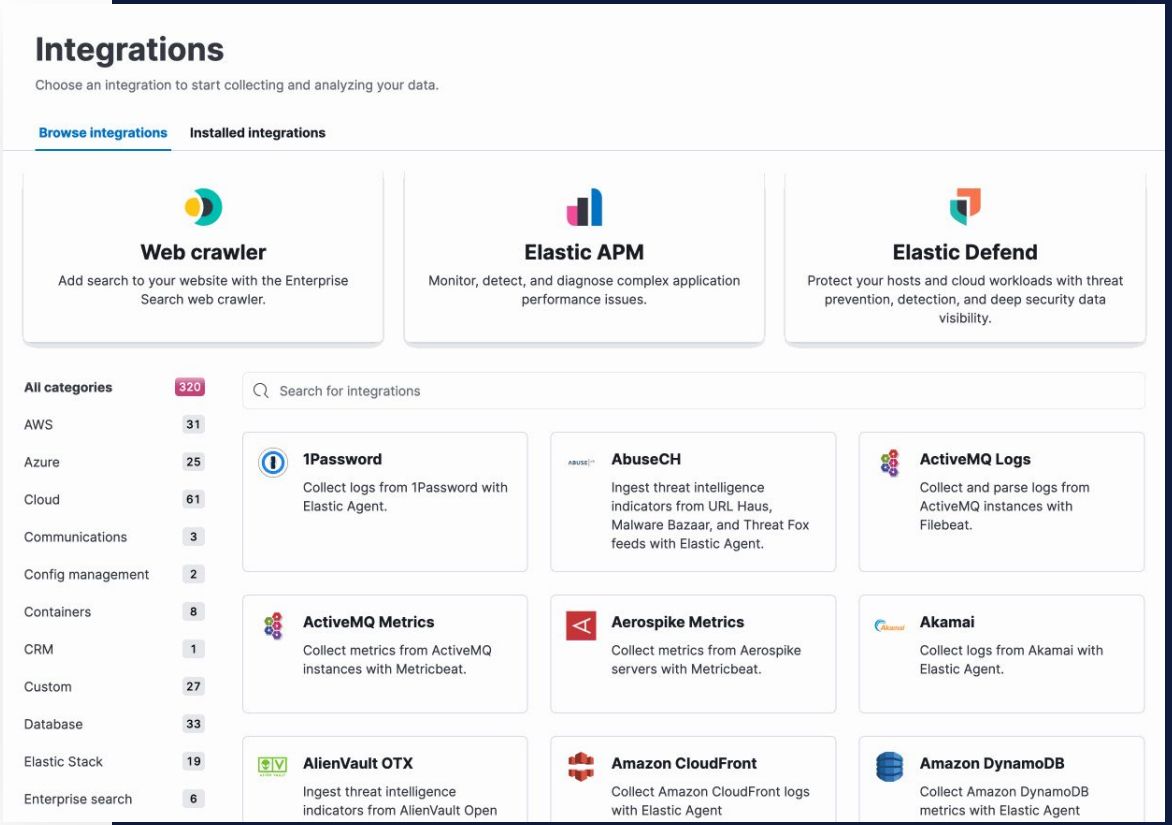
하이브리드

온-프렘

Elastic Observability

간편한 데이터 수집

- 로그, 메트릭, 트레이스 데이터 수집을 한 에이전트에서
- 중앙 에이전트 관리 (Fleet)
  - 수천개의 에이전트 관리
  - 한 번의 클릭으로 에이전트 설정 변경 및 업그레이드
- 대시보드 및 시각화 기능 포함 350개 이상 통합(Integrations) 지원



elastic

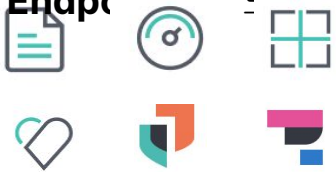
엘라스틱 에이전트

로그, 메트릭, 트레이스, 보안 등을 위한 단일 통합 에이전트
핵심 비츠 에이전트를 내부적으로 조정

BEFORE

ON EVERY HOST:

- **Filebeat** for 로그
- **Metricbeat** for 메트릭
- **APM agent** for 트레이스
- **Packetbeat** for 네트워크
- **Winlogbeat** for 윈도우 데이터
- **Auditbeat** for 감사 데이터
- **Heartbeat** for 업타임
- **Endpoint** for 보안



NOW

ON EVERY HOST:

- **Elastic Agent** for 로그, 메트릭, 트레이스, 업타임, 보안, 윈도우 데이터 등

설치, **설정**, **확장**을 한번에 할 수 있음

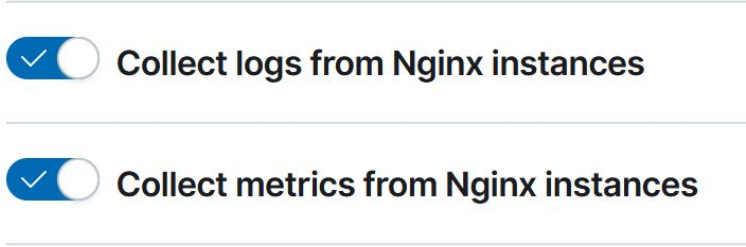
에이전트 설정 → UI로 가능

데이터 수집이 ☑️ 만큼 쉬움

BEFORE

```
###################### Filebeat Configuration Example #########################

# This file is an example configuration file highlighting only the most common
# options. The filebeat.reference.yml file from the same directory contains all the
# supported options with more comments. You can use it as a reference.
#
# You can find the full configuration reference here:
# https://www.elastic.co/guide/en/beats/filebeat/index.html

# For more available modules and options, please see the filebeat.reference.yml sample
# configuration file.

# ============================== Filebeat inputs ===============================

filebeat.inputs:

# Each - is an input. Most options can be set at the input level, so
# you can use different inputs for various configurations.
# Below are the input specific configurations.

- type: log

  # Change to true to enable this input configuration.
  enabled: false

  # Paths that should be crawled and fetched. Glob based paths.
  paths:
    - /var/log/*.log
    #- c:\programdata\elasticsearch\logs\*

  # Exclude lines. A list of regular expressions to match. It drops the lines that are
  # matching any regular expression from the list.
  #exclude_lines: ['^DBG']

  # Include lines. A list of regular expressions to match. It exports the lines that are
  # matching any regular expression from the list.
  #include_lines: ['^ERR', '^WARN']

  # Exclude files. A list of regular expressions to match. Filebeat drops the files that
  # are matching any regular expression from the list. By default, no files are dropped.
  #exclude_files: ['.gz$']
```

NOW



elastic

API 키 사용

최소 권한으로 더 나은 제어

BEFORE

- 비츠에서 아이디/패스워드 입력
- 패스워드 YAML 설정에 저장됨
- 기본 사용자는 슈퍼유저 권한이 있음
- 하나 또는 몇 개의 비밀번호로 모든 비츠 사용

NOW

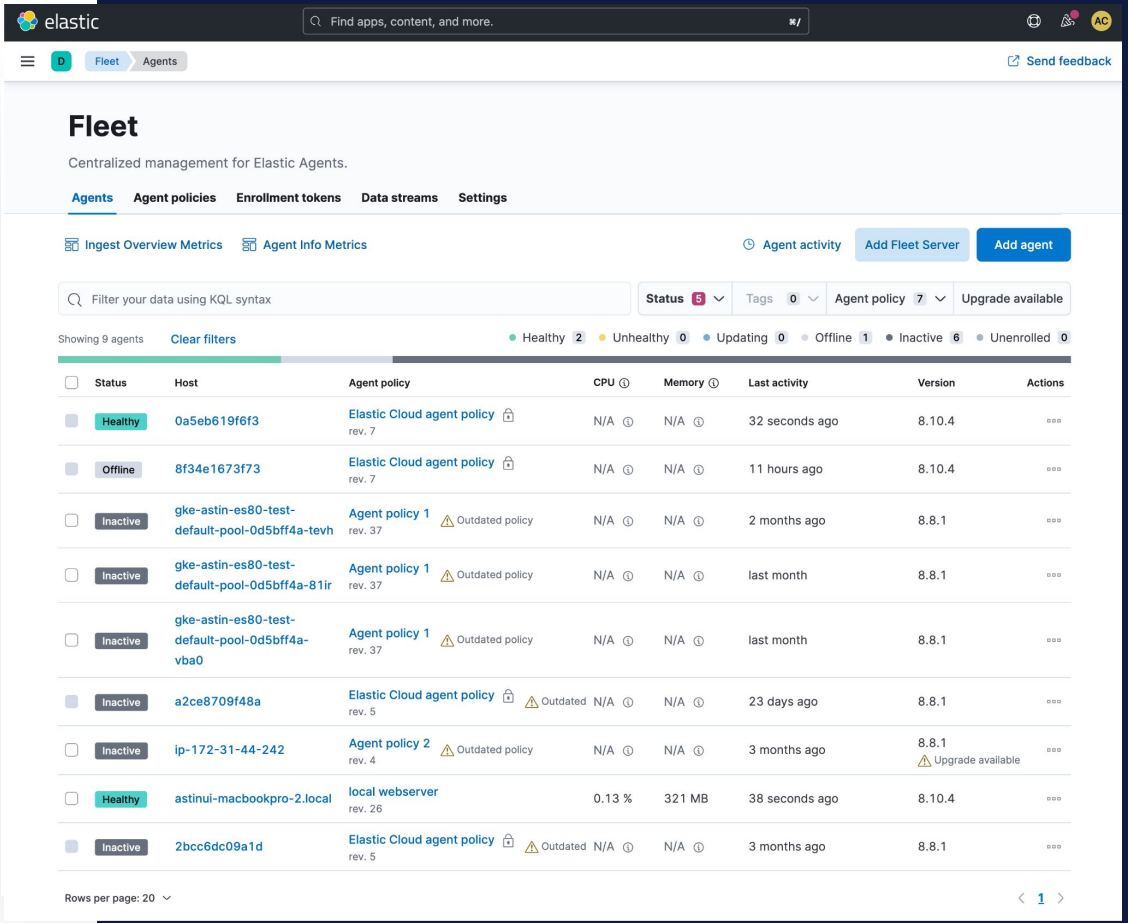
- Fleet 및 엘라스틱서치에 대한 API 키
- Fleet에서 자동으로 키 생성
- 각 에이전트에서 최소한의 권한으로 사용
- 에이전트 당 하나의 키로 쉽게 관리 가능

elastic

Elastic Observability

중앙 에이전트 관리 (Fleet)

- 여러 에이전트를 중앙에서 UI로 관리
- 엘라스틱 에이전트 상태에 대한 빠른 가시성 확보
- 에이전트 설정 및 버전을 원격으로 업데이트

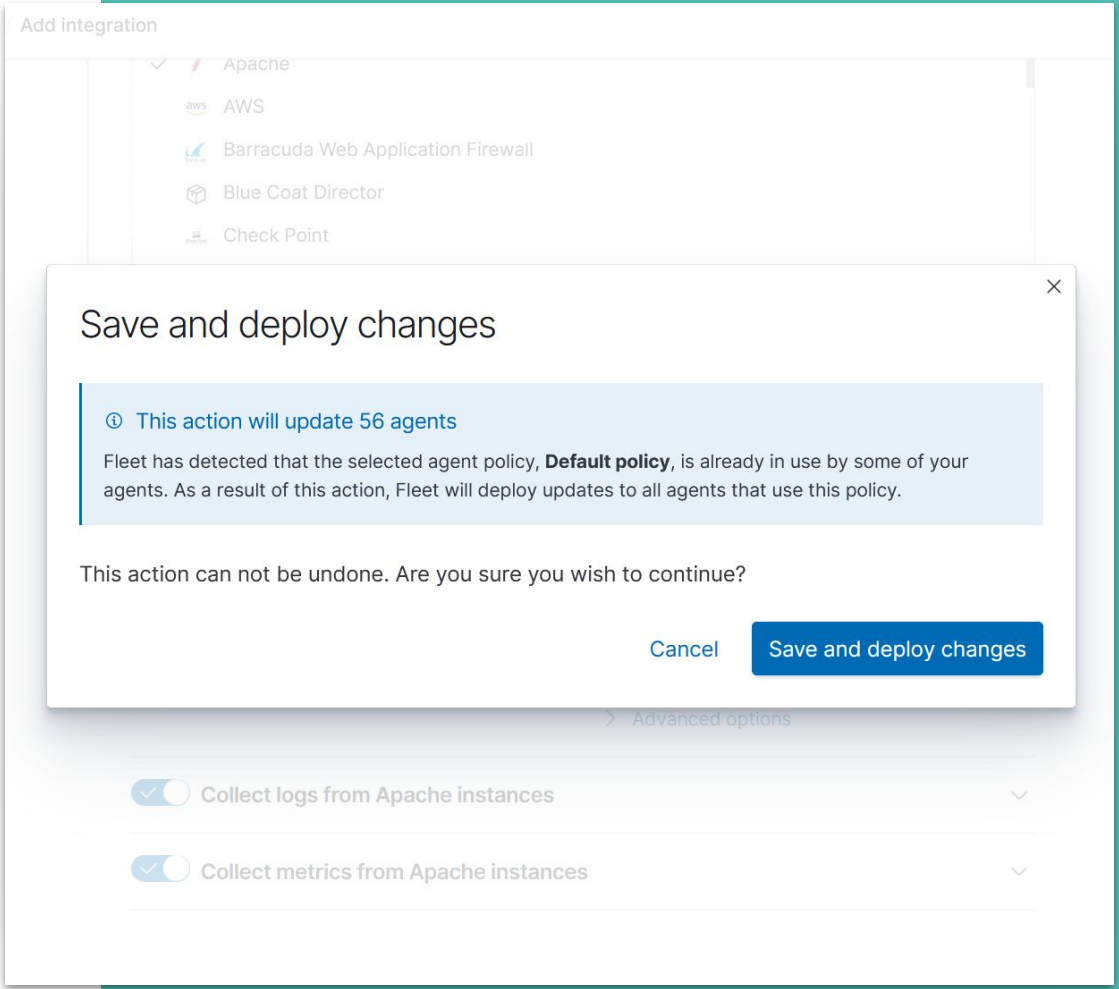


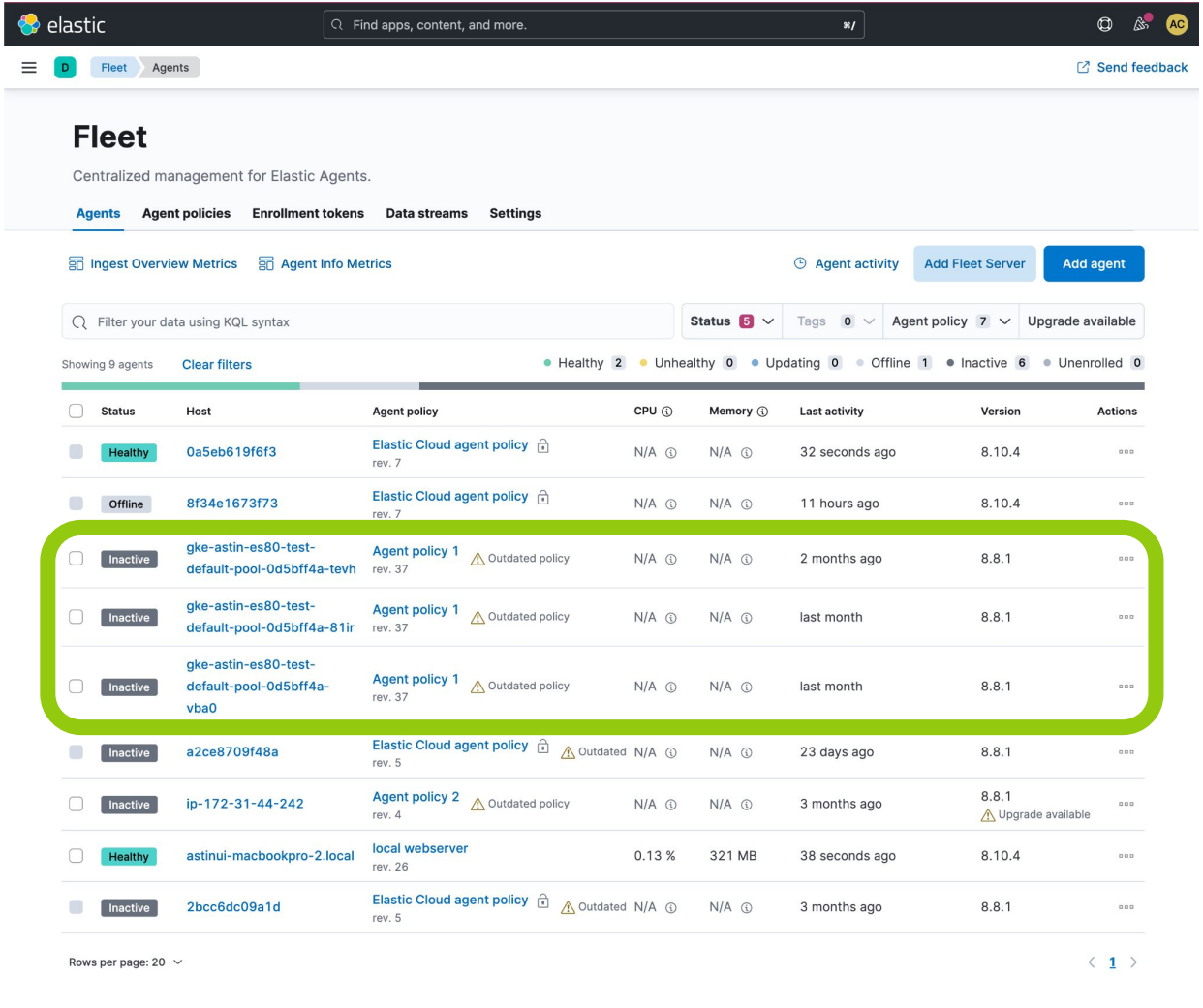
elastic

Elastic Observability

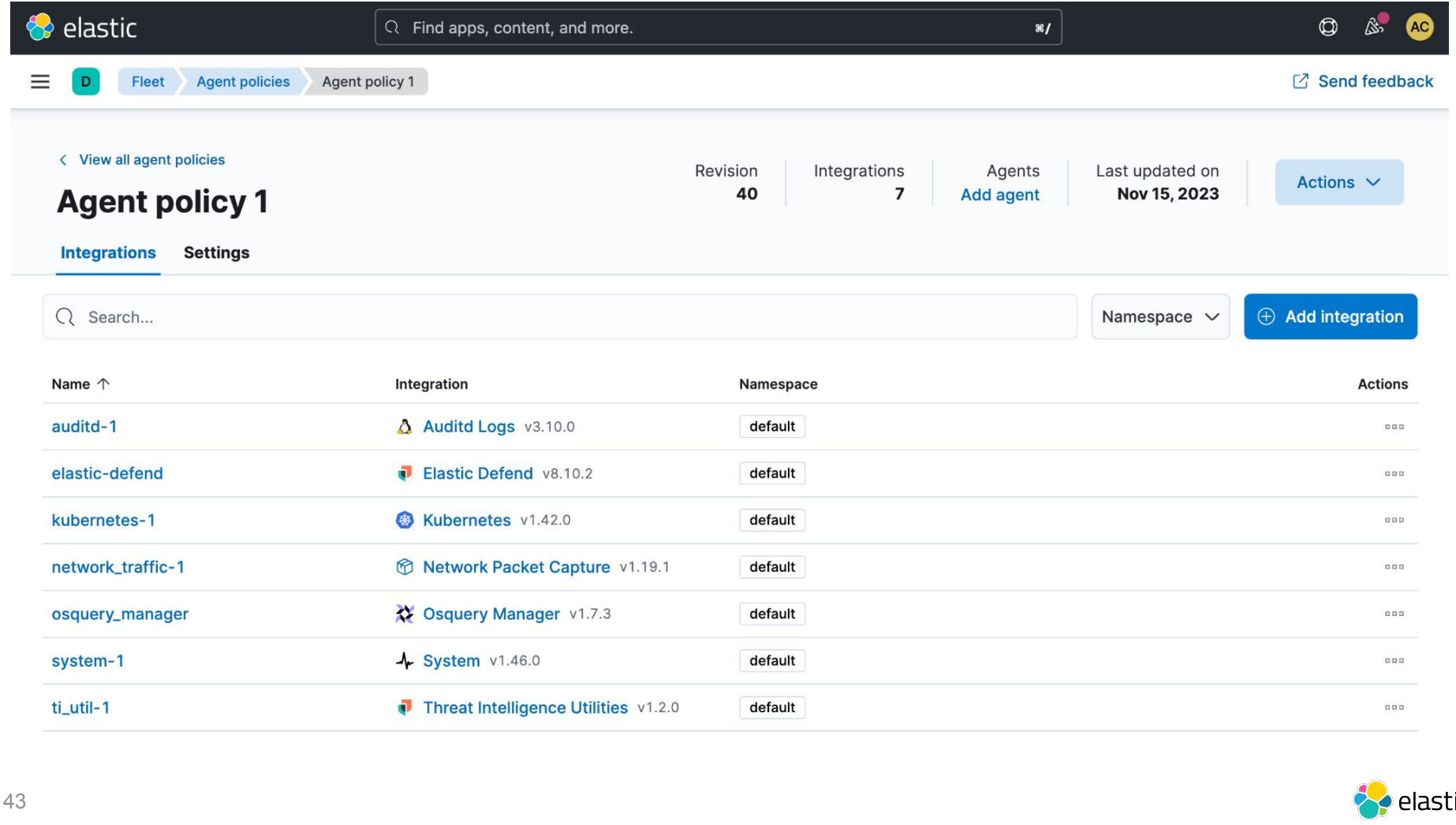
클릭 한 번으로 모두 업데이트

- 클릭 한 번으로 모든 에이전트에서 정책(Policy) 업데이트
- Powershell, Chef, Ansible 등을 사용하는데 드는 시간과 번거로움을 줄여줌

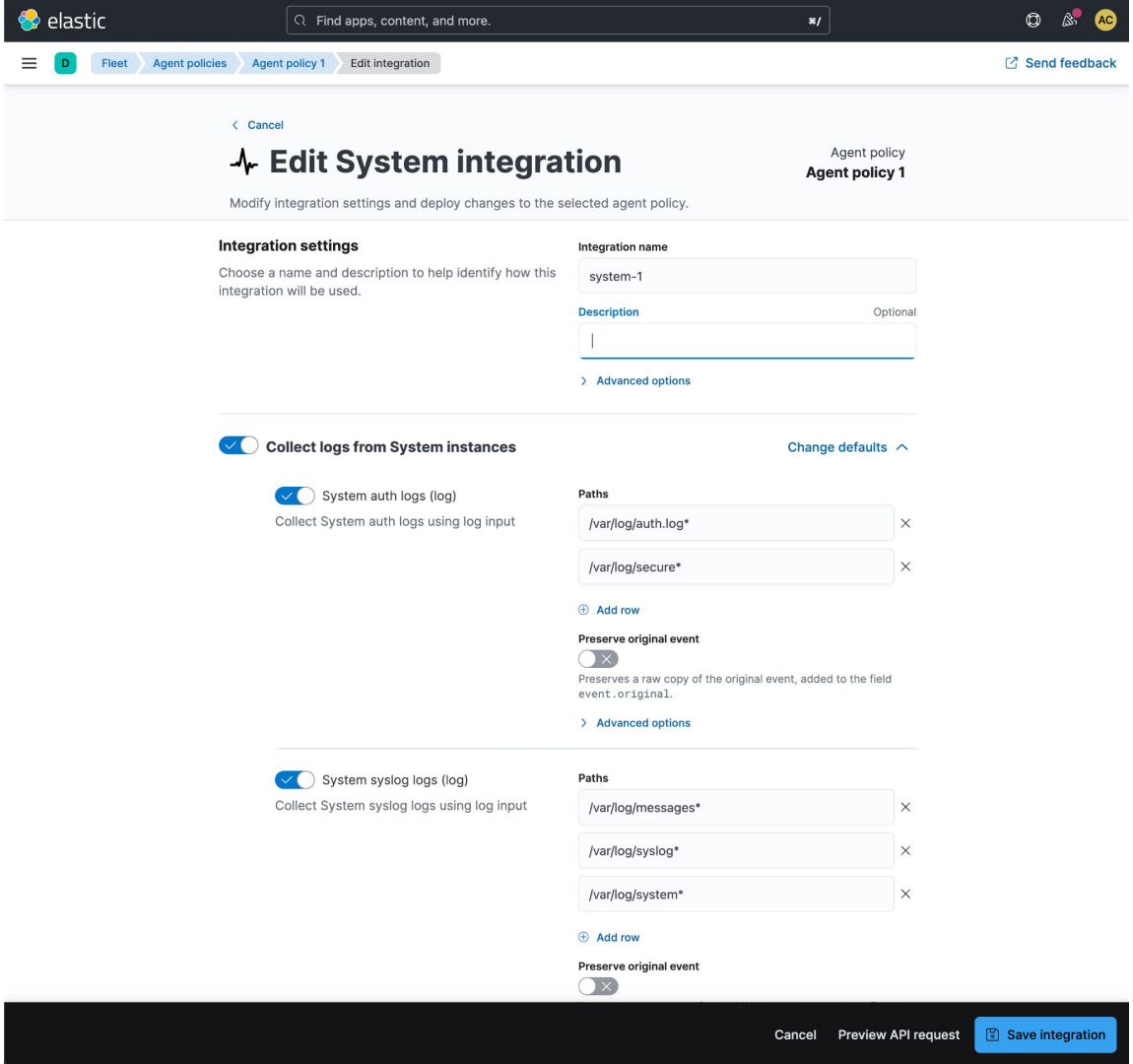



elastic
Find apps, content, and more.
⌘/
AC
D
Fleet
Agents
Send feedback
Fleet
Centralized management for Elastic Agents.
Agents
Agent policies
Enrollment tokens
Data streams
Settings
Ingest Overview Metrics
Agent Info Metrics
Agent activity
Add Fleet Server
Add agent
Filter your data using KQL syntax
Status 5
Tags 0
Agent policy 7
Upgrade available
Showing 9 agents
Clear filters
Healthy 2
Unhealthy 0
Updating 0
Offline 1
Inactive 6
Unenrolled 0
Status
Host
Agent policy
CPU
Memory
Last activity
Version
Actions
Healthy
0a5eb619f6f3
Elastic Cloud agent policy
rev. 7
N/A
N/A
32 seconds ago
8.10.4
Offline
8f34e1673f73
Elastic Cloud agent policy
rev. 7
N/A
N/A
11 hours ago
8.10.4
Inactive
gke-astin-es80-test-default-pool-0d5bff4a-tevh
Agent policy 1
rev. 37
Outdated policy
N/A
N/A
2 months ago
8.8.1
Inactive
gke-astin-es80-test-default-pool-0d5bff4a-81ir
Agent policy 1
rev. 37
Outdated policy
N/A
N/A
last month
8.8.1
Inactive
gke-astin-es80-test-default-pool-0d5bff4a-vba0
Agent policy 1
rev. 37
Outdated policy
N/A
N/A
last month
8.8.1
Inactive
a2ce8709f48a
Elastic Cloud agent policy
rev. 5
Outdated
N/A
N/A
23 days ago
8.8.1
Inactive
ip-172-31-44-242
Agent policy 2
rev. 4
Outdated policy
N/A
N/A
3 months ago
8.8.1
Upgrade available
Healthy
astinui-macbookpro-2.local
local webserver
rev. 26
0.13 %
321 MB
38 seconds ago
8.10.4
Inactive
2bcc6dc09a1d
Elastic Cloud agent policy
rev. 5
Outdated
N/A
N/A
3 months ago
8.8.1
Rows per page: 20
1

elastic


elastic
Find apps, content, and more.
⌘/
AC
D
Fleet
Agent policies
Agent policy 1
Send feedback
View all agent policies
Agent policy 1
Revision
40
Integrations
7
Agents
Add agent
Last updated on
Nov 15, 2023
Actions
Integrations
Settings
Search...
Namespace
Add integration
Name
Integration
Namespace
Actions
auditd-1
Auditd Logs v3.10.0
default
elastic-defend
Elastic Defend v8.10.2
default
kubernetes-1
Kubernetes v1.42.0
default
network_traffic-1
Network Packet Capture v1.19.1
default
osquery_manager
Osquery Manager v1.7.3
default
system-1
System v1.46.0
default
ti_util-1
Threat Intelligence Utilities v1.2.0
default

elastic


elastic
Find apps, content, and more.
⌘/
AC
D
Fleet
Agent policies
Agent policy 1
Edit integration
Send feedback
Cancel
Edit System integration
Agent policy
Agent policy 1
Modify integration settings and deploy changes to the selected agent policy.
Integration settings
Choose a name and description to help identify how this integration will be used.
Integration name
system-1
Description
Optional
Advanced options
Collect logs from System instances
Change defaults
System auth logs (log)
Collect System auth logs using log input
Paths
/var/log/auth.log*
/var/log/secure*
Add row
Preserve original event
Preserves a raw copy of the original event, added to the field event.original.
Advanced options
System syslog logs (log)
Collect System syslog logs using log input
Paths
/var/log/messages*
/var/log/syslog*
/var/log/system*
Add row
Preserve original event
Cancel
Preview API request
Save integration

elastic

무료 **14**일 트라이얼

elastic.co/cloud/signup

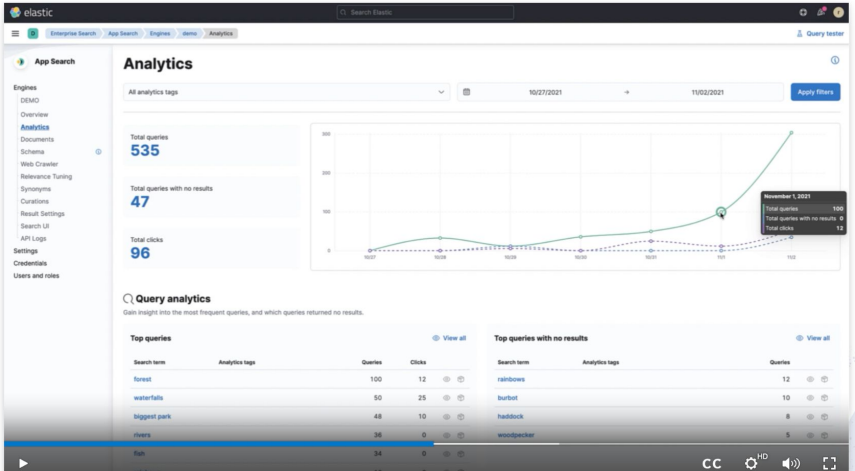
퀵스타트 **elastic.co/training/free**

FREE ELASTIC TRAINING

Enterprise Search Quick Start

In this 3-step Quick Start series, you'll learn about Elastic Enterprise Search: modern, natural search experiences with pretuned relevance for your apps and websites. See how quickly you can get set up, ingest data, discover the search interface, and analyze and tune a search engine for your needs. Topics include what is Elastic Enterprise Search, indexing data into Elastic Enterprise Search, and analyzing and refining search.

Start free trial Read documentation →



elastic

Thank you!