



옵저버빌리티 - APM and AI

End to End Observability /w Elastic APM

Astin Choi

Solutions Architect

2024-02

엘라스틱서치 플랫폼



엘라스틱서치 플랫폼





부엌에 있는 재료로 볶음밥을 만들려면 어떻게 해야하나요?



부엌에 있는 재료로 볶음밥을 만들려면 다음과 같이 진행할 수 있습니다. 볶음밥은 다양한 재료를 활용하여 맛을 조절할 수 있는 요리로, 계 재료를 조절할 수 있습니다.



생성형 AI는 "세상"에 대해 알고 있지만, "개인"에 대해서 알지 못함

재료:

- 밥 (1~2 그릇)
- 달걀 (2개)
- 식용유 (2~3 큰술)
- 마늘 (다진 마늘 1큰술)
- 양파 (다진 양파 반 개)
- 당근 (다진 당근 반 개)
- 양송이 버섯 (다진 양송이 버섯 약간, 선택사항)
- 소금 (적당량)
- 후추 (적당량)
- 간장 (1~2 큰술)
- 참기름 (1큰술)
- 김 또는 파 (장식용, 선택사항)




준비 단계:

1. 밥을 미리 밥솥이나 냄비에서 지어 둡니다. 밥은 너무 촉촉하지 않고 약간 건더기



스팸과 냉동 야채가 있어요!



스팸과 냉동 야채를 활용하여 맛있는 스팸 볶음밥을 만들어보는 것은 좋은 아이디어   
어입니다. 아래는 스팸 볶음밥을 만드는 간단한 레시피입니다.

재료:

- 밥 (2 그릇 정도, 미리 지어 둔 차가운 밥이 좋습니다.)
- 스팸 (1캔)
- 냉동 야채 (당근, 양파, 녹색 고추 등, 야채 종류는 선택사항)
- 식용유 (2~3 큰술)
- 마늘 (다진 마늘 1큰술)
- 소금 (적당량)
- 후추 (적당량)
- 간장 (1~2 큰술)
- 참기름 (1큰술)
- 김 또는 파 (장식용, 선택사항)

요리 단계:

1. 큰 프라이팬을 중불로 예열합니다.
2. 스팸을 적당한 크기로 잘라서 팬에 넣고 노릇하게 볶아줍니다. 추가적으로 기름이 필요하면 스팸을 볶을 때 기름을 조금 더 두어도 됩니다.
3. 스팸이 볶아질 때, 다른 팬에 식용유를 두르고 다진 마늘을 볶아 향을 내줍니다.
4. 마늘이 은은하게 향이 나면 냉동 야채를 넣고 볶아줍니다. 야채가 해동되고 익을 때까지 볶아주세요

컨텍스트를 제공하면 생성형 AI는
좋은 성능을 발휘함

생성형AI /w 컨텍스트

🔍 부엌에 있는 재료로 볶음밥을 만들려면 어떻게 해야하나요?

부엌에 있는 재료로 볶음밥을 만들려면 어떻게 해야하나요?
0.95 | 스팸
0.95 | 냉동 야채



검색 쿼리로 질문

엘라스틱서치로 시멘틱 벡터 검색을 통해 데이터에 대한 컨텍스트를 찾음

엘라스틱서치

쿼리와 가장 관련성이 높은 데이터



0.95 | 스팸
0.95 | 냉동 야채
0.20 | 피클
0.10 | 베이킹 소다

스팸과 냉동 야채를 활용하여 맛있는 스팸 볶음밥을 만들어보는 것은 좋은 아이디어입니다. 아래는 스팸 볶음밥을 만드는 간단한 레시피입니다.

재료:

- 밥 (2 그릇 정도, 미리 지어 둔 차가운 밥이 좋습니다.)
 - 스팸 (1캔)
 - 냉동 야채 (당근, 양파, 녹색 고추 등, 야채 종류는 선택사항)
 - 식용유 (2~3 큰술)
 - 마늘 (다진 마늘 1큰술)
 - 소금 (적당량)
 - 후추 (적당량)
 - 간장 (1~2 큰술)
 - 참기름 (1큰술)
 - 김 또는 파 (장식용, 선택사항)
- ...

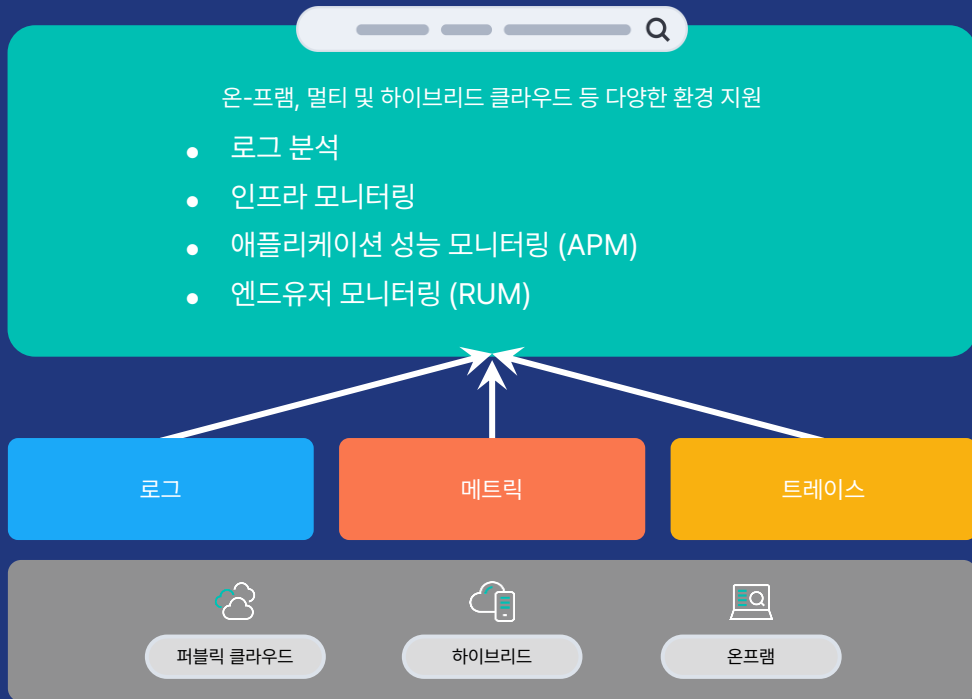
Elastic CEO 및 총괄 매니저 사례 인터뷰
events.elastic.co/gaielasticsearchkorea

엘라스틱서치 플랫폼



엘라스틱 옴저버빌리티

한 플랫폼, 한 데이터 저장소에서 모두 해결





데이터 수집

엘라스틱서치 플랫폼




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

Integrations


Choose an integration to start collecting and analyzing your data.

[Browse integrations](#) **Installed integrations**




Web crawler

Add search to your website with the Enterprise Search web crawler.



Elastic APM

Monitor, detect, and diagnose complex application performance issues.



Elastic Defend

Protect your hosts and cloud workloads with threat prevention, detection, and deep security data visibility.

All categories 320

Search for integrations

<p>AWS 31</p> <p>Azure 25</p> <p>Cloud 61</p> <p>Communications 3</p> <p>Config management 2</p> <p>Containers 8</p> <p>CRM 1</p> <p>Custom 27</p> <p>Database 33</p> <p>Elastic Stack 19</p> <p>Enterprise search 6</p>	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>1Password</p> <p>Collect logs from 1Password with Elastic Agent.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>AbuseCH</p> <p>Ingest threat intelligence indicators from URL Haus, Malware Bazaar, and Threat Fox feeds with Elastic Agent.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>ActiveMQ Metrics</p> <p>Collect metrics from ActiveMQ instances with Metricbeat.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>ActiveMQ Logs</p> <p>Collect and parse logs from ActiveMQ instances with Filebeat.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>AlienVault OTX</p> <p>Ingest threat intelligence indicators from AlienVault Open</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>Akamai</p> <p>Collect logs from Akamai with Elastic Agent.</p> </div>	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>Aerospike Metrics</p> <p>Collect metrics from Aerospike servers with Metricbeat.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>Amazon CloudFront</p> <p>Collect Amazon CloudFront logs with Elastic Agent</p> </div> <div style="border: 1px solid #ccc; padding: 5px;"> <p>Amazon DynamoDB</p> <p>Collect Amazon DynamoDB metrics with Elastic Agent</p> </div>
---	---	--

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, 확장을 한번에
할 수 있음

에이전트 설정 -> UI로 가능

데이터 수집이  만큼 쉬움

BEFORE

```
1 ##### filebeat Configuration Example #####
2
3 # This file is an example configuration file highlighting only the most common
4 # options. The filebeat.reference.yml file from the same directory contains all the
5 # supported options with more comments. You can use it as a reference.
6 #
7 # You can find the full configuration reference here:
8 # https://www.elastic.co/guide/en/beats/filebeat/index.html
9
10 # For more available modules and options, please see the filebeat.reference.yml sample
11 # configuration file.
12
13 # ===== Filebeat inputs =====
14
15 filebeat.inputs:
16
17 # Each - is an input. Most options can be set at the input level, so
18 # you can use different inputs for various configurations.
19 # Below are the input specific configurations.
20
21 - type: log
22
23 # Change to true to enable this input configuration.
24 enabled: false
25
26 # Paths that should be crawled and fetched. Glob based paths.
27 paths:
28   - /var/log/*.log
29   #- c:\programdata\elasticsearch\logs\*
30
31 # Exclude lines. A list of regular expressions to match. It drops the lines that are
32 # matching any regular expression from the list.
33 #exclude_lines: ['^DBG']
34
35 # Include lines. A list of regular expressions to match. It exports the lines that are
36 # matching any regular expression from the list.
37 #include_lines: ['^ERR', '^WARN']
38
39 # Exclude files. A list of regular expressions to match. Filebeat drops the files that
40 # are matching any regular expression from the list. By default, no files are dropped.
41 #exclude_files: ['.gz$']
42
```



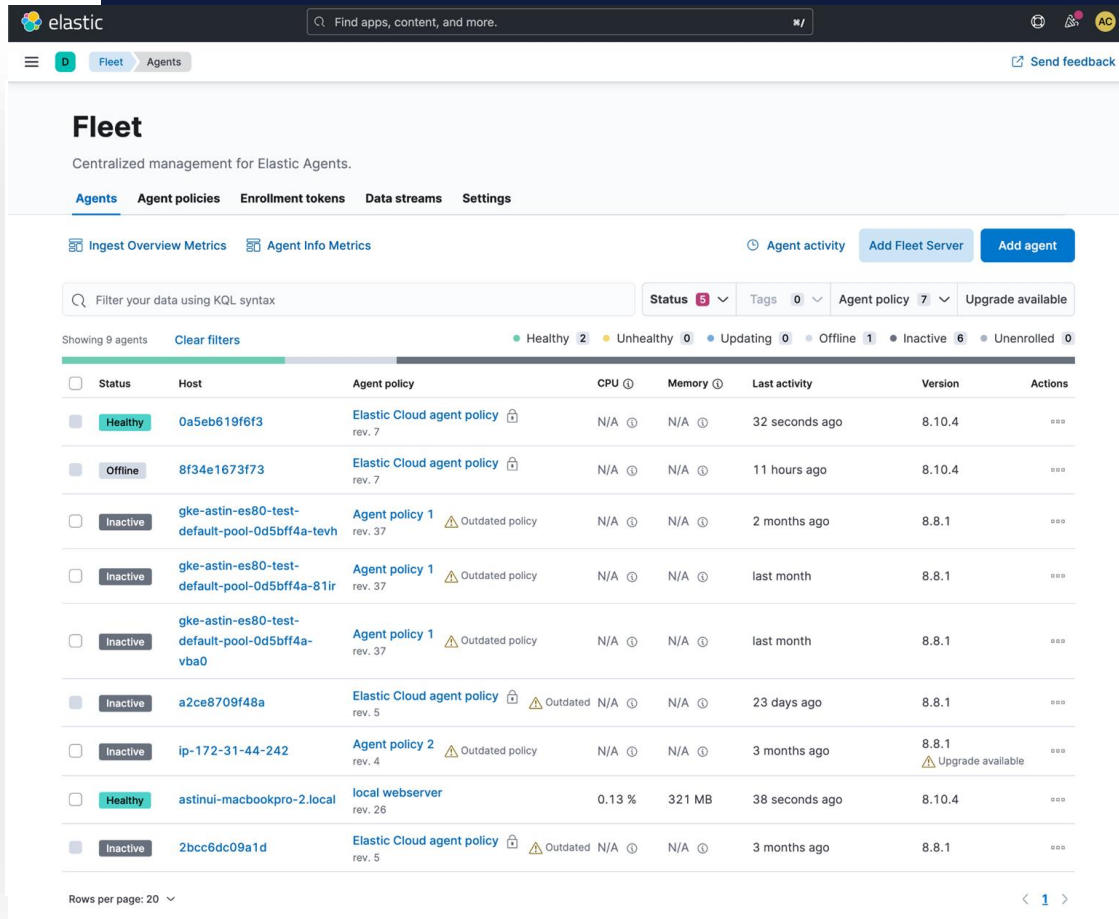
NOW

 Collect logs from Nginx instances

 Collect metrics from Nginx instances

중앙 에이전트 관리 (Fleet)

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



The screenshot displays the Elastic Fleet management interface. At the top, there's a search bar and navigation tabs for 'Agents'. Below this, the 'Fleet' section is titled 'Centralized management for Elastic Agents.' and includes sub-tabs for 'Agents', 'Agent policies', 'Enrollment tokens', 'Data streams', and 'Settings'. A summary bar shows 'Ingest Overview Metrics' and 'Agent Info Metrics', along with 'Agent activity' and buttons for 'Add Fleet Server' and 'Add agent'. A filter bar allows searching with KQL syntax and shows counts for 'Status' (6), 'Tags' (0), 'Agent policy' (7), and 'Upgrade available'. A status bar indicates 'Showing 9 agents' with a legend for 'Healthy' (2), 'Unhealthy' (0), 'Updating' (0), 'Offline' (1), 'Inactive' (6), and 'Unenrolled' (0). The main table lists agents with columns for Status, Host, Agent policy, CPU, Memory, Last activity, Version, and Actions.

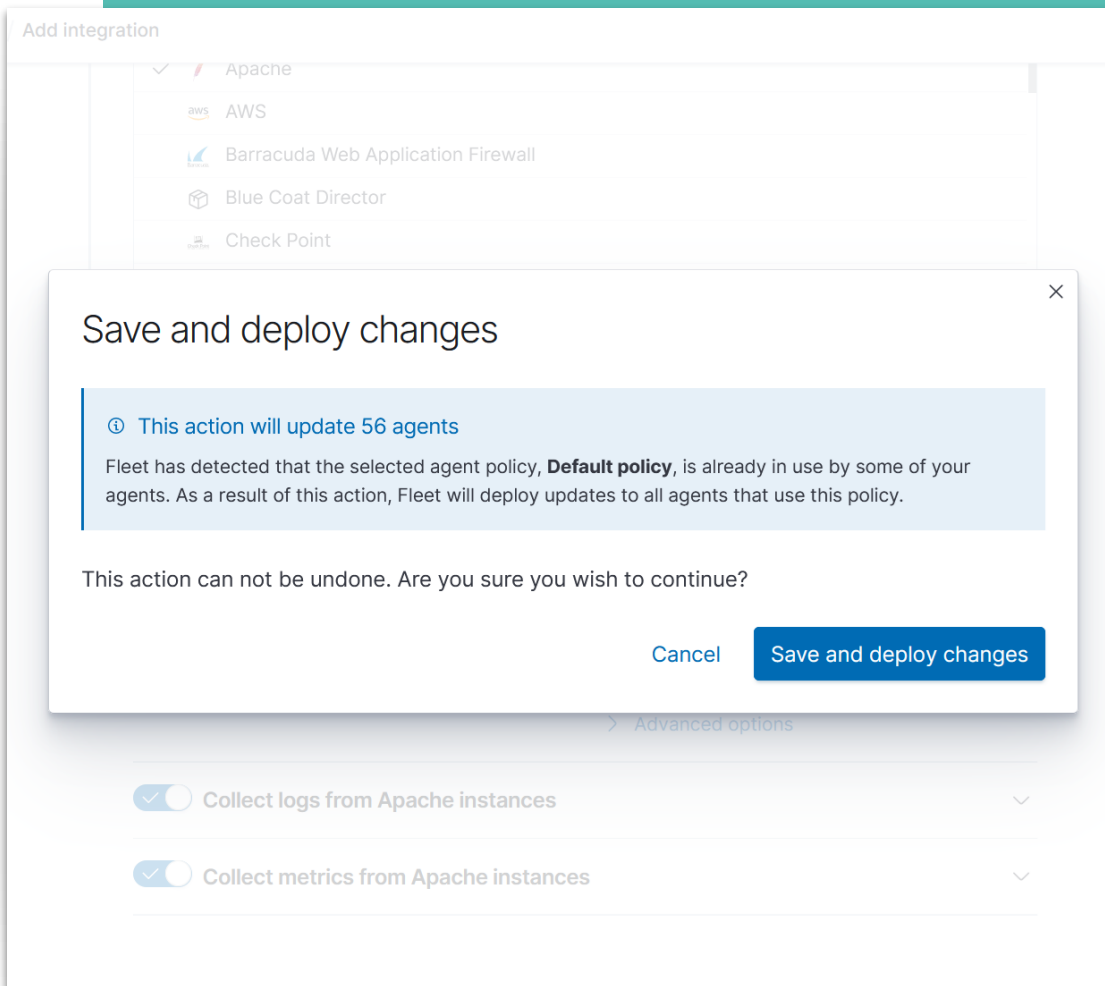
Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
Healthy	0a5eb619f6f3	Elastic Cloud agent policy rev. 7	N/A	N/A	32 seconds ago	8.10.4	...
Offline	8f34e1673f73	Elastic Cloud agent policy rev. 7	N/A	N/A	11 hours ago	8.10.4	...
Inactive	gke-astin-es80-test-default-pool-0d5bff4a-tevh	Agent 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

Elastic Observability

클릭 한 번으로 모두 업데이트

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



The screenshot displays the 'Add integration' dialog in the Elastic Observability interface. A modal window titled 'Save and deploy changes' is overlaid on top, providing a warning and confirmation for the update action.

Add integration

- ✓ Apache
- aws AWS
- Barracuda Web Application Firewall
- Blue Coat Director
- Check Point

Save and deploy changes

④ This action will update 56 agents

Fleet has detected that the selected agent policy, **Default policy**, is already in use by some of your agents. As a result of this action, Fleet will deploy updates to all agents that use this policy.

This action can not be undone. Are you sure you wish to continue?

Cancel **Save and deploy changes**

> Advanced options

- ✓ Collect logs from Apache instances
- ✓ Collect metrics from Apache instances

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

<input type="checkbox"/>	Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
<input checked="" type="checkbox"/>	Healthy	0a5eb619f6f3	Elastic Cloud agent policy rev. 7	N/A	N/A	32 seconds ago	8.10.4	...
<input checked="" type="checkbox"/>	Offline	8f34e1673f73	Elastic Cloud agent policy rev. 7	N/A	N/A	11 hours ago	8.10.4	...
<input type="checkbox"/>	Inactive	gke-astin-es80-test-default-pool-0d5bff4a-tevh	Agent policy 1 rev. 37	N/A	N/A	2 months ago	8.8.1	...
<input type="checkbox"/>	Inactive	gke-astin-es80-test-default-pool-0d5bff4a-81ir	Agent policy 1 rev. 37	N/A	N/A	last month	8.8.1	...
<input type="checkbox"/>	Inactive	gke-astin-es80-test-default-pool-0d5bff4a-vba0	Agent policy 1 rev. 37	N/A	N/A	last month	8.8.1	...
<input checked="" type="checkbox"/>	Inactive	a2ce8709f48a	Elastic Cloud agent policy rev. 5	N/A	N/A	23 days ago	8.8.1	...
<input type="checkbox"/>	Inactive	ip-172-31-44-242	Agent policy 2 rev. 4	N/A	N/A	3 months ago	8.8.1 	...
<input type="checkbox"/>	Healthy	astinui-macbookpro-2.local	local webserver rev. 26	0.13 %	321 MB	38 seconds ago	8.10.4	...
<input checked="" type="checkbox"/>	Inactive	2bcc6dc09a1d	Elastic Cloud agent policy rev. 5	N/A	N/A	3 months ago	8.8.1	...

Rows per page: 20

< 1 >



D

Fleet

Agent policies

Agent policy 1
















[Send feedback](#)[View all agent policies](#)Revision
40Integrations
7Agents
[Add agent](#)Last updated on
Nov 15, 2023Actions 

Agent policy 1

[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	

[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

Description Optional

[Advanced options](#)

Collect logs from System instances [Change defaults](#)

System auth logs (log)
Collect System auth logs using log input

Paths

×

×

[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

×

×

×

[Add row](#)

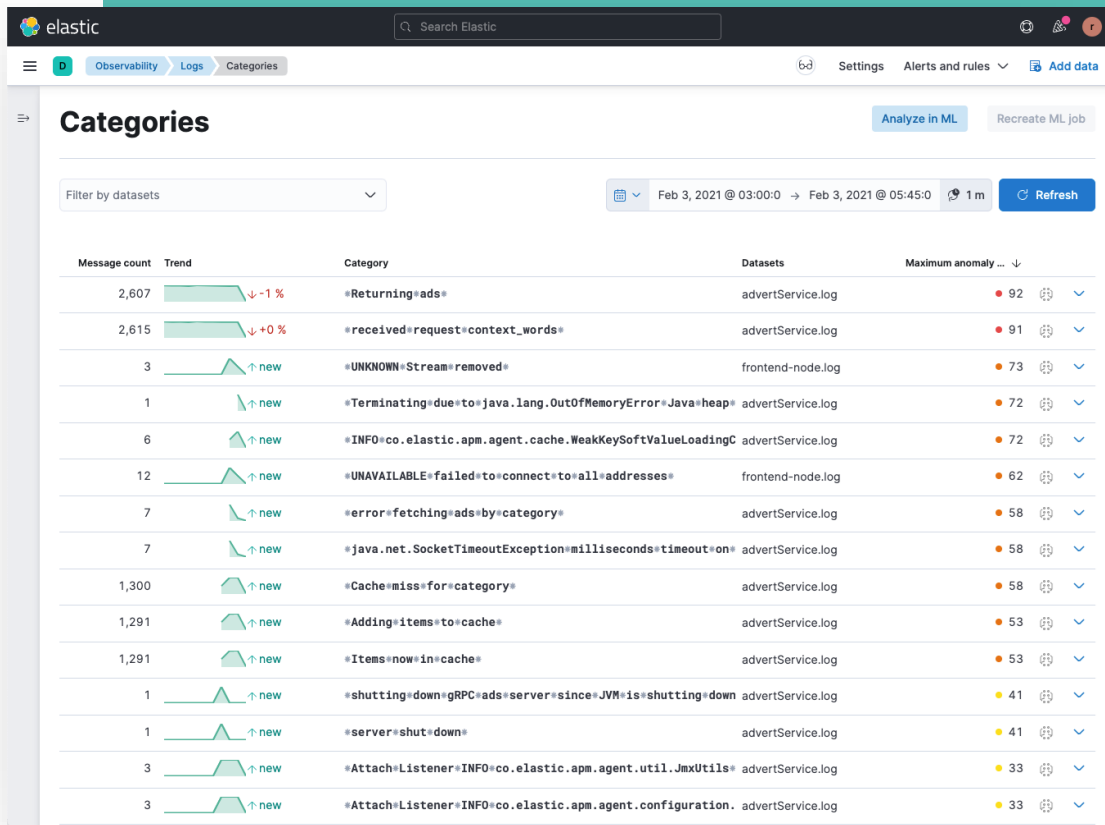
Preserve original event
 ×

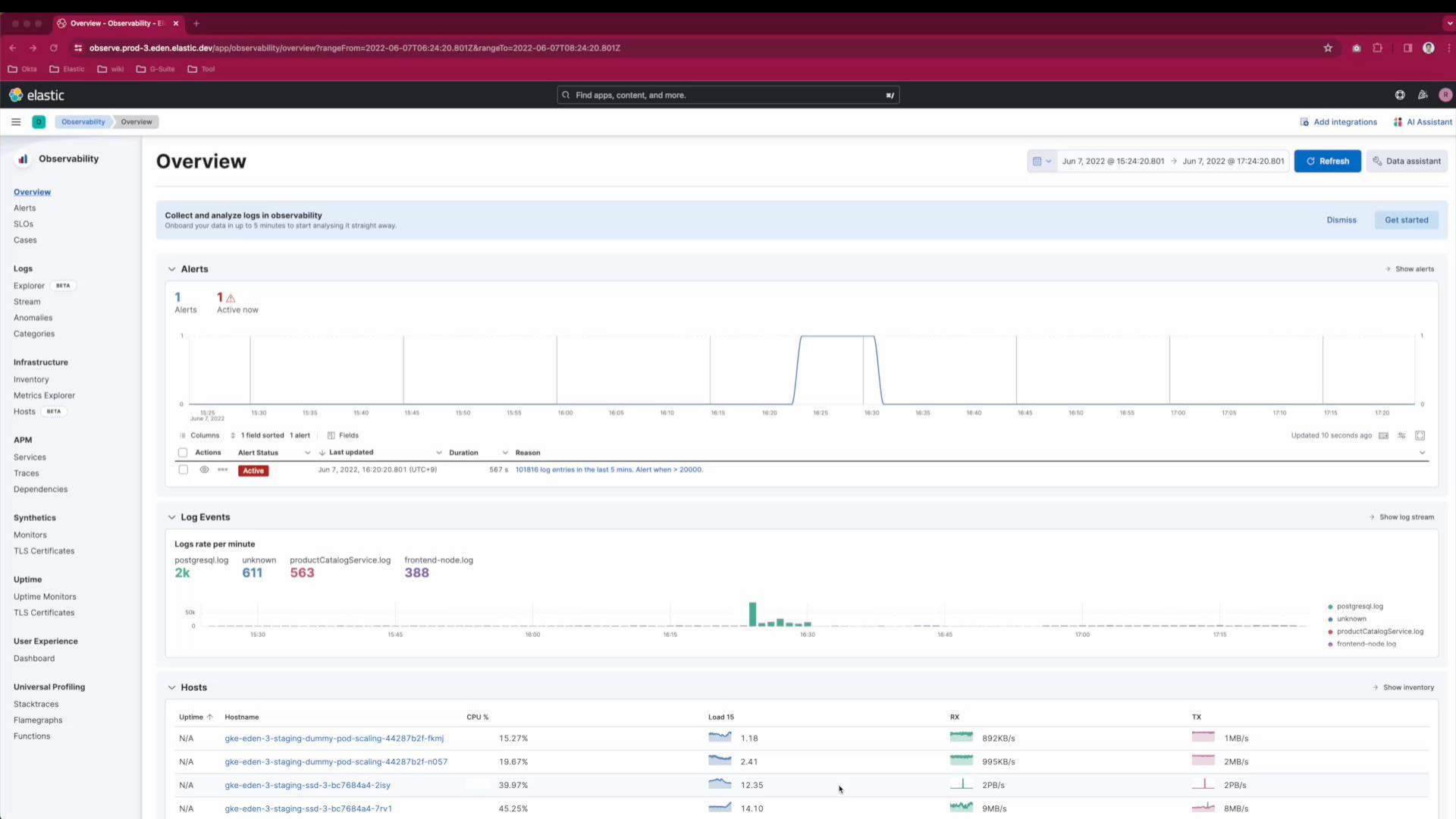


주요 기능

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





Observability

Overview

- Alerts
- SLOs
- Cases

Logs

- Explorer BETA
- Stream
- Anomalies
- Categories

Infrastructure

- Inventory
- Metrics Explorer

APM

- Services
- Traces
- Dependencies

Synthetics

- Monitors
- TLS Certificates

Uptime

- Uptime Monitors
- TLS Certificates

User Experience

- Dashboard

Universal Profiling

- Stacktraces
- Flamegraphs
- Functions

Overview

Jun 7, 2022 @ 15:24:20.801 → Jun 7, 2022 @ 17:24:20.801 Refresh Data assistant

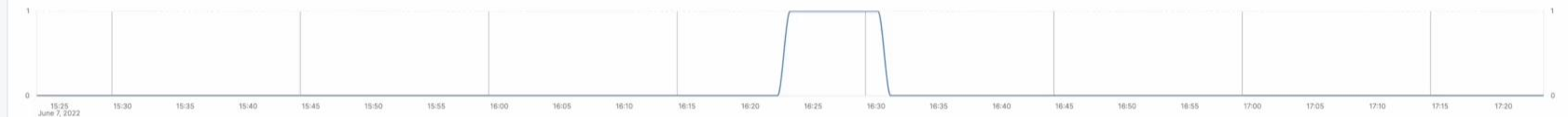
Collect and analyze logs in observability

Onboard your data in up to 5 minutes to start analysing it straight away.

Dismiss Get started

Alerts

1 Alerts 1 Active now



Columns: 1 field sorted 1 alert | Fields

Actions Alert Status Last updated Duration Reason

<input type="checkbox"/>	Active	Jun 7, 2022, 16:20:20.801 (UTC+9)	567 s	101816 log entries in the last 5 mins. Alert when > 20000.
--------------------------	---------------------	-----------------------------------	-------	--

Updated 10 seconds ago

Log Events

Logs rate per minute

postgresql.log 2k unknown 611 productCatalogService.log 563 frontend-node.log 388



Hosts

Uptime ↑	Hostname	CPU %	Load 15	RX	TX
N/A	gke-eden-3-staging-dummy-pod-scaling-44287b2f-fkmj	15.27%	1.18	892KB/s	1MB/s
N/A	gke-eden-3-staging-dummy-pod-scaling-44287b2f-n057	19.67%	2.41	995KB/s	2MB/s
N/A	gke-eden-3-staging-ssd-3-bc7684a4-2isy	39.97%	12.35	2PB/s	2PB/s
N/A	gke-eden-3-staging-ssd-3-bc7684a4-7rv1	45.25%	14.10	9MB/s	8MB/s

비용 효율적인 데이터 보관 /w data tiers

응답 시간

보유기간 (일반 기준)

하드웨어

Tier 1
실시간

Lowest
(밀리초~초)

~7일

SSDs

Tier 2
실시간 / 단기간

Lower
(초)

7~30일

HDDs

Tier 3
중기간

Lower
(초)

30~90일

HDDs

Tier 4
장기간

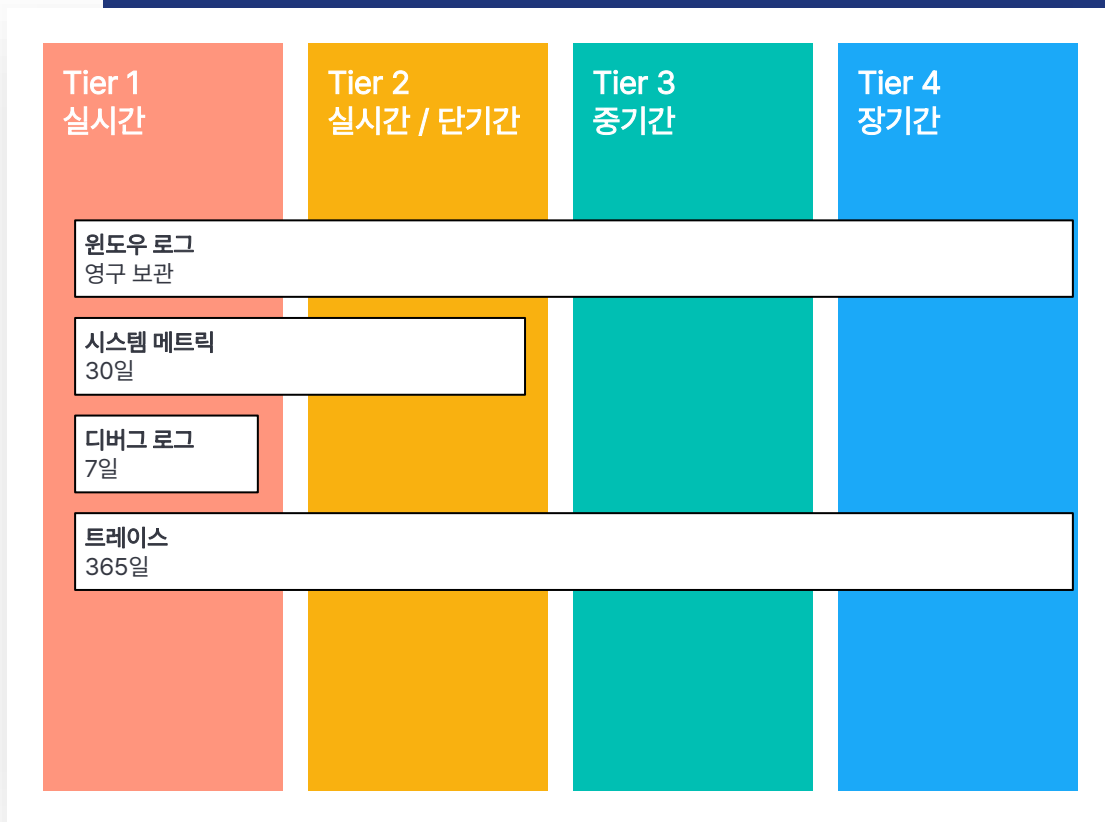
Slowest
(초~분)

90일~

Blob 스토리지 (S3
등)

데이터 종류별로 보관을 자유롭게

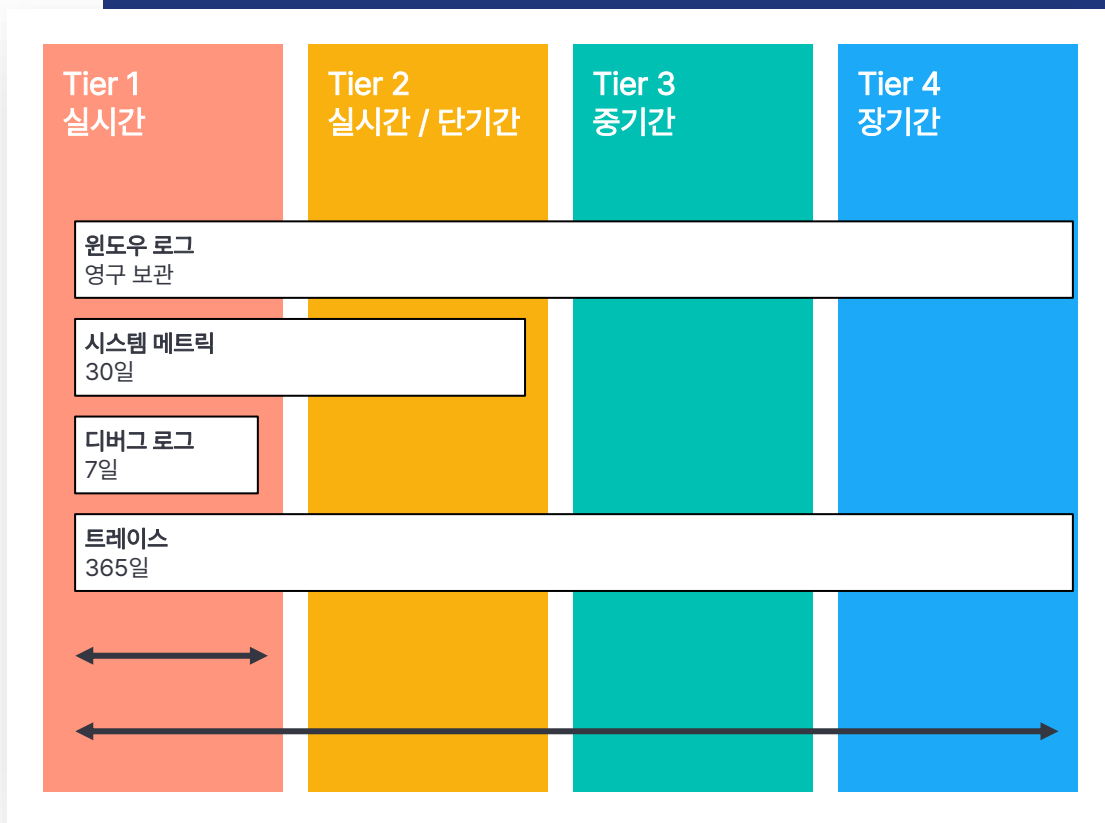
- 데이터를 계층 이동시 소스별로 사용자 정의 가능
- 보관 주기 무제한



끊김없는 검색

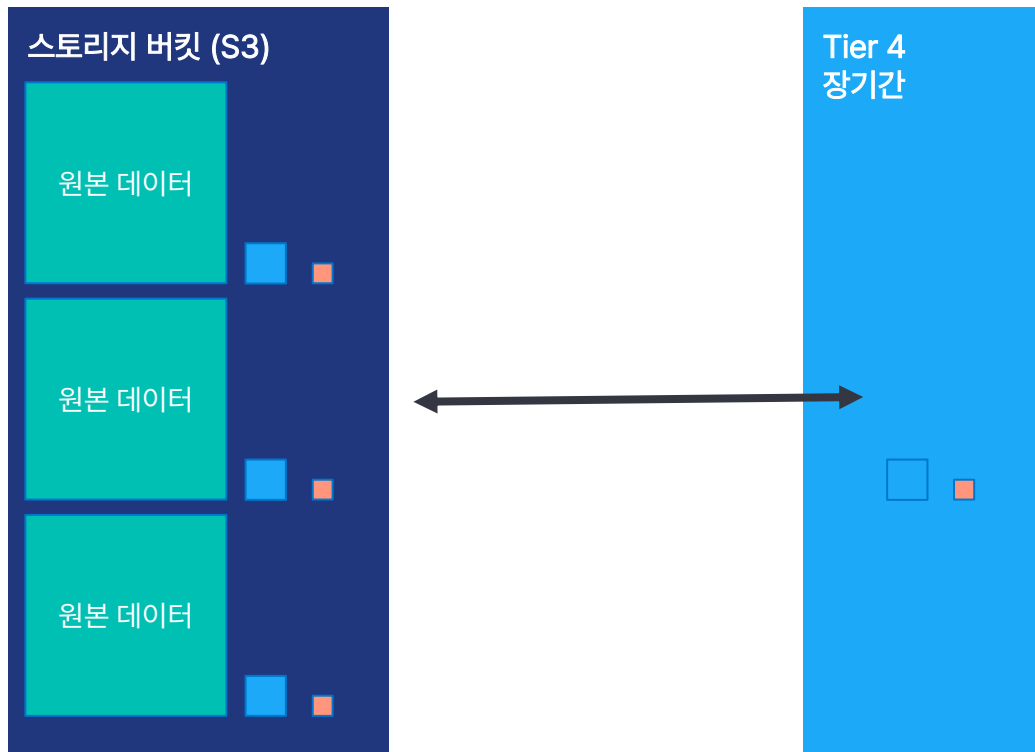
별도 수동 작업 없이

- 전체 데이터에 대한 동일 UX
- 복원 불필요



효율적인 과거 데이터 검색

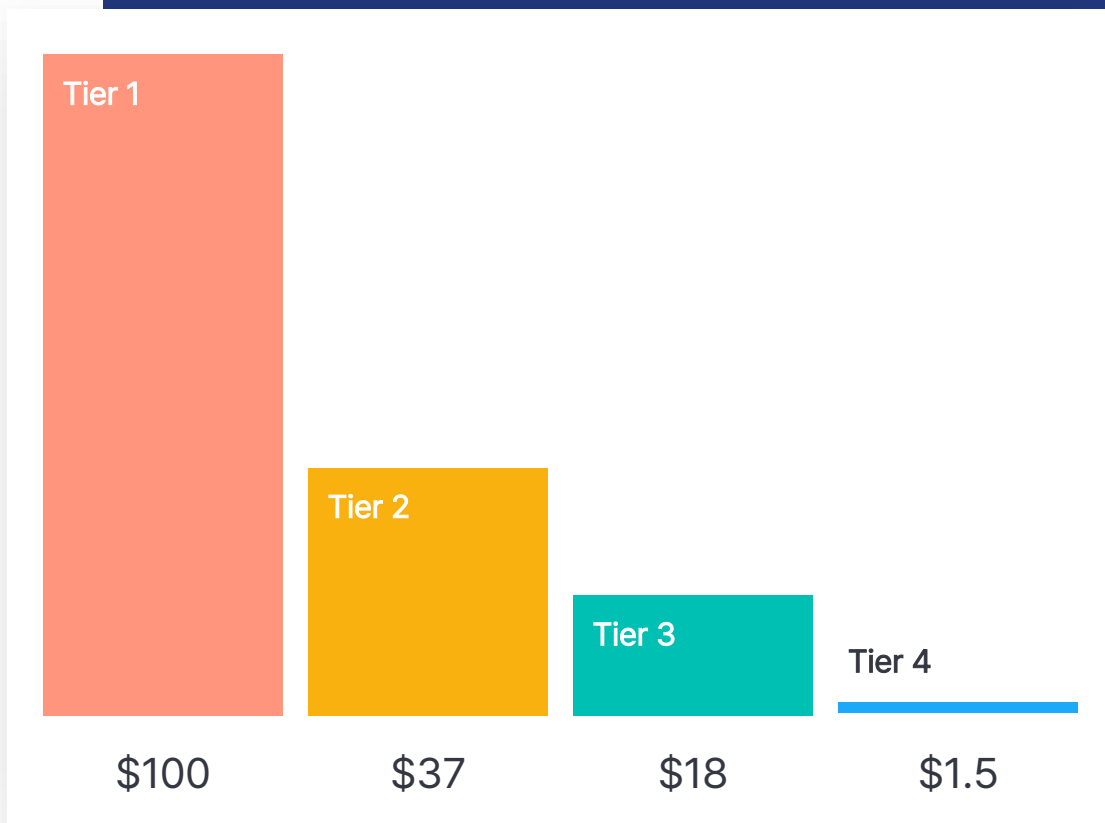
- 필요한 데이터만 로딩
- 로컬 캐시
- 복원 작업 혹은 수동 개입 불필요
- 다른 접근 방식에 비해 빠른 쿼리 성능
- 하드웨어 비용 감소
- 오브젝트 스토리지 API 비용 감소
- 데이터 전송 비용 감소



비용 효율적인 데이터 보관

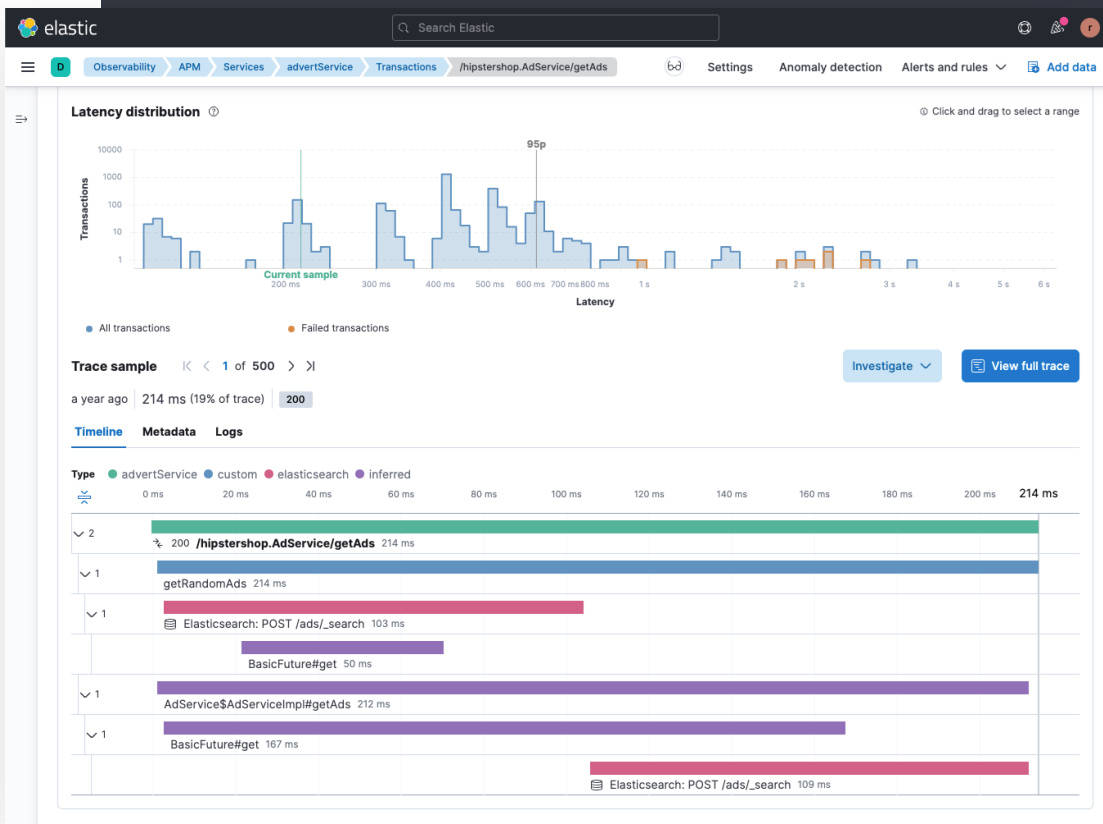
계층별 데이터 저장 비용

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



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



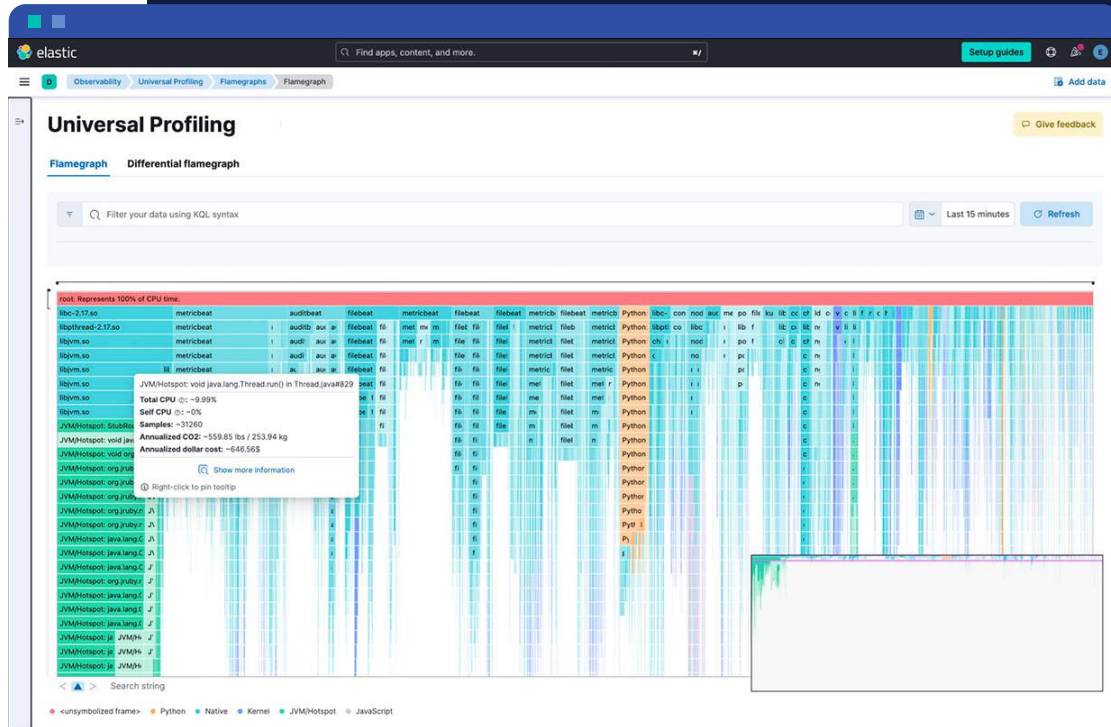
Google

Search Google or type a URL

-  LinkedIn
-  Inbox (103)
-  Elastic
-  Google Drive
-  NAVER
-  Login — Elas...
-  Google Tran...
-  Elastic Cloud
-  네이버
-  Add shortcut

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



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

↑ 53.71%

Annualized CO2 emission impact

4.68 lbs / 2.12 kg

↑ 2.17 lbs / 0.98 kg (53.71%)

Annualized cost impact

\$44.1

↑ \$20.41 (53.71%)

Total number of samples

2,132

↑ 987 (53.71%)

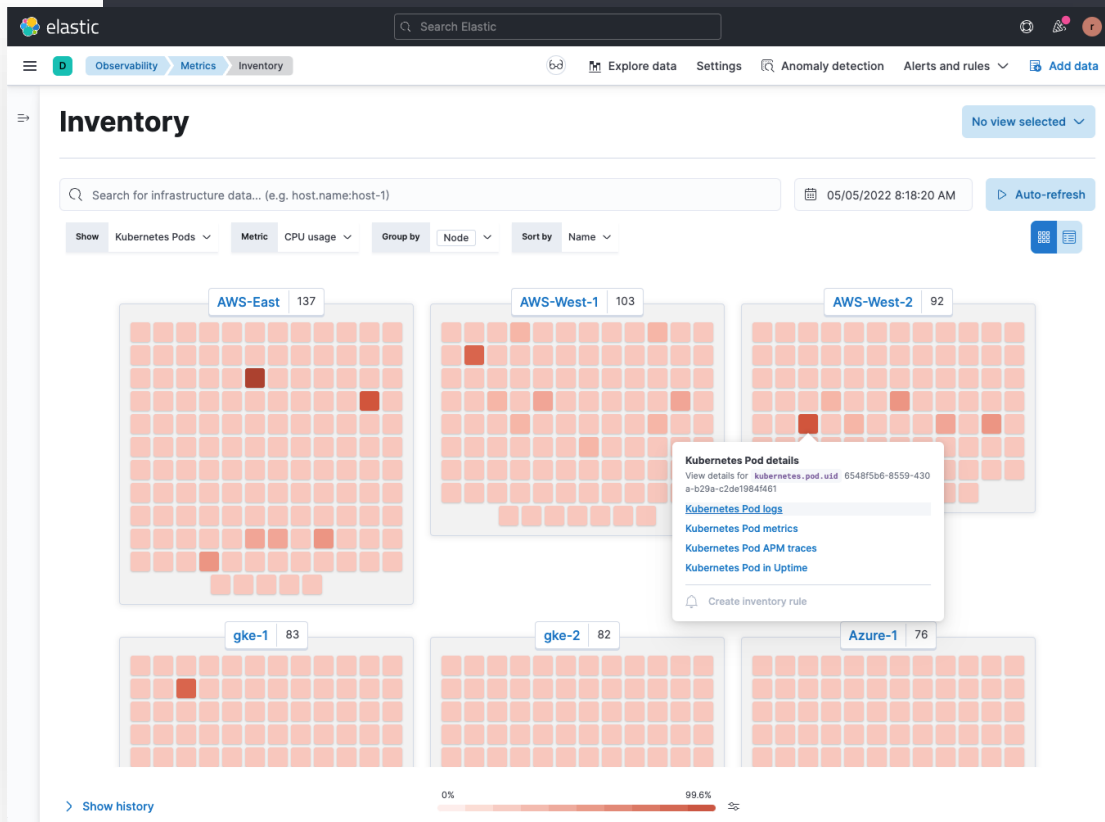
Function	Samples	Self CPU	Total CPU
python3.7: lookdict_unicode_nodummy ../Objects/dictobject.c#854	111	5.21%	5.21%
python3.7: _PyType_Lookup ../Objects/typeobject.c#3085	97	4.55%	5.21%
python3.7: _PyObject_GetMethod ../Objects/object.c#1144	89	4.17%	8.91%
Python: flask_route_interest interest.py#31	83	3.89%	62.85%
python3.7: _PyEval_EvalCodeWithName ../Python/ceval.c#3946	66	3.10%	7.65%
python3.7: frame_dealloc ../Objects/frameobject.c#470	60	2.81%	3.47%
Python: __getitem__ os.py#679	59	2.77%	32.97%
Python: encode os.py#752	51	2.39%	9.99%
python3.7: PyDict_LoadGlobal	50	2.25%	5.25%

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



모든 환경에 걸쳐 통합된 가시성

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



Tell us what you think!

Hosts BETA

Search hosts (E.g. cloud.provider:gcp AND system.load.1 > 0.5)

Operating System: Any Cloud Provider: Any

Host limit: 50 100 500

What are these metrics?

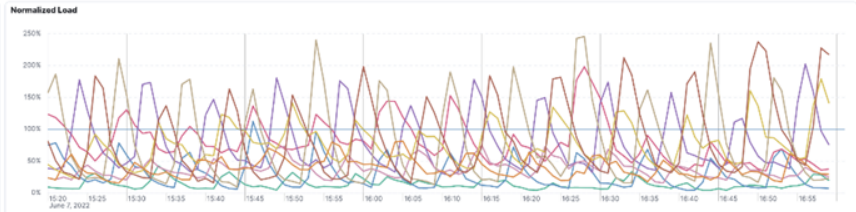
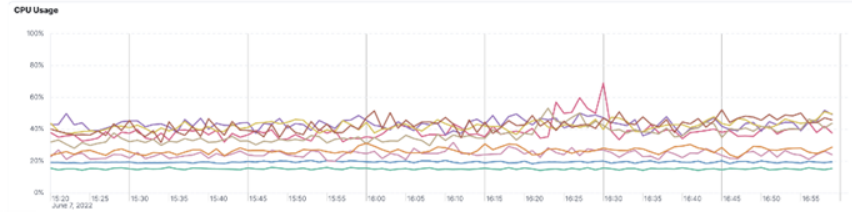


Name	CPU usage (avg)	Normalized Load (avg)	Memory Usage (avg)	Memory Free (avg)	Disk Space Usage (avg)	RX (avg)	TX (avg)
gke-eden-3-staging-dummy-pod-scaling-44287b2f-fkmj	15.1%	14%	28.4%	12 GB	0%	7.3 Mbit/s	10.4 Mbit/s
gke-eden-3-staging-dummy-pod-scaling-44287b2f-n057	19.3%	29.6%	28.2%	12.1 GB	0%	8.2 Mbit/s	16.5 Mbit/s
gke-eden-3-staging-ssd-3-bc7684a4-2lvy	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

Metrics Logs Alerts

Learn more about metrics



통합 환경으로 사일로 제거

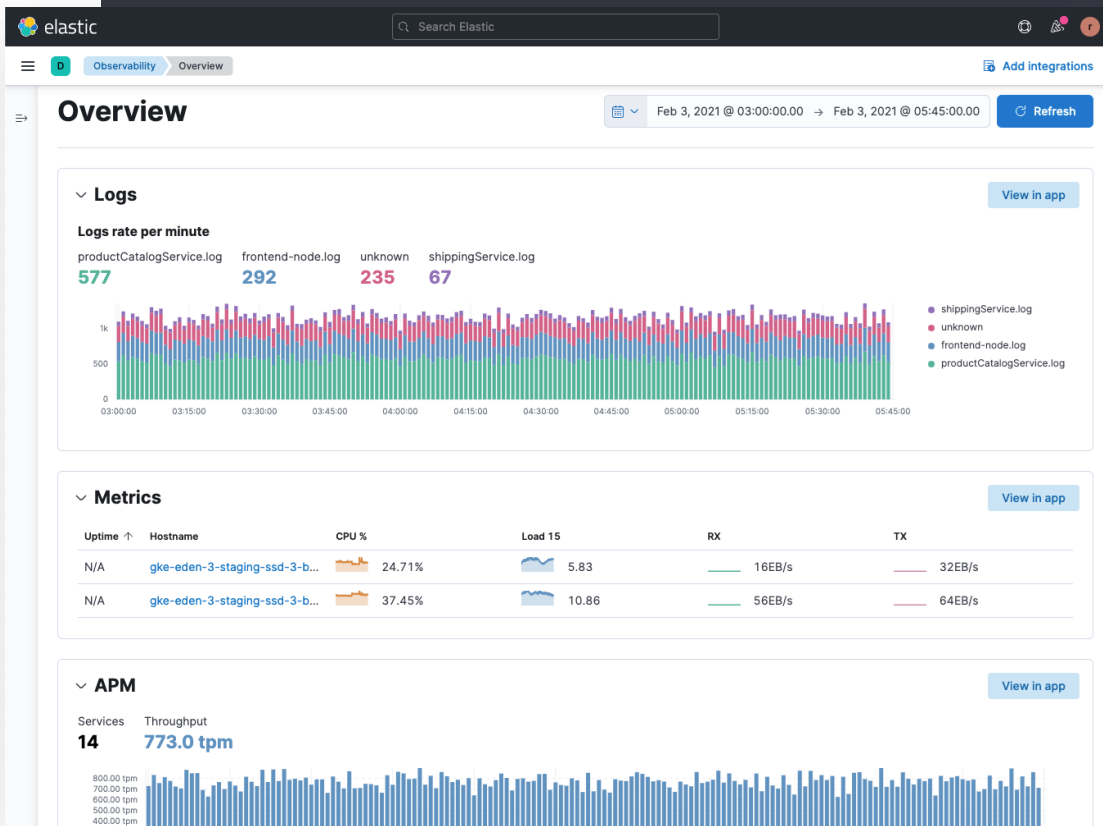
- 모든 비즈니스 및 운영 데이터를 위한 단일 플랫폼
- 메트릭, 로그, 트레이스를 컨텍스트 기반으로 연결해 빠르게 문제 분석
- 업계 유일의 개방형 공통 데이터 모델 (Elastic Common Schema)

```
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
```



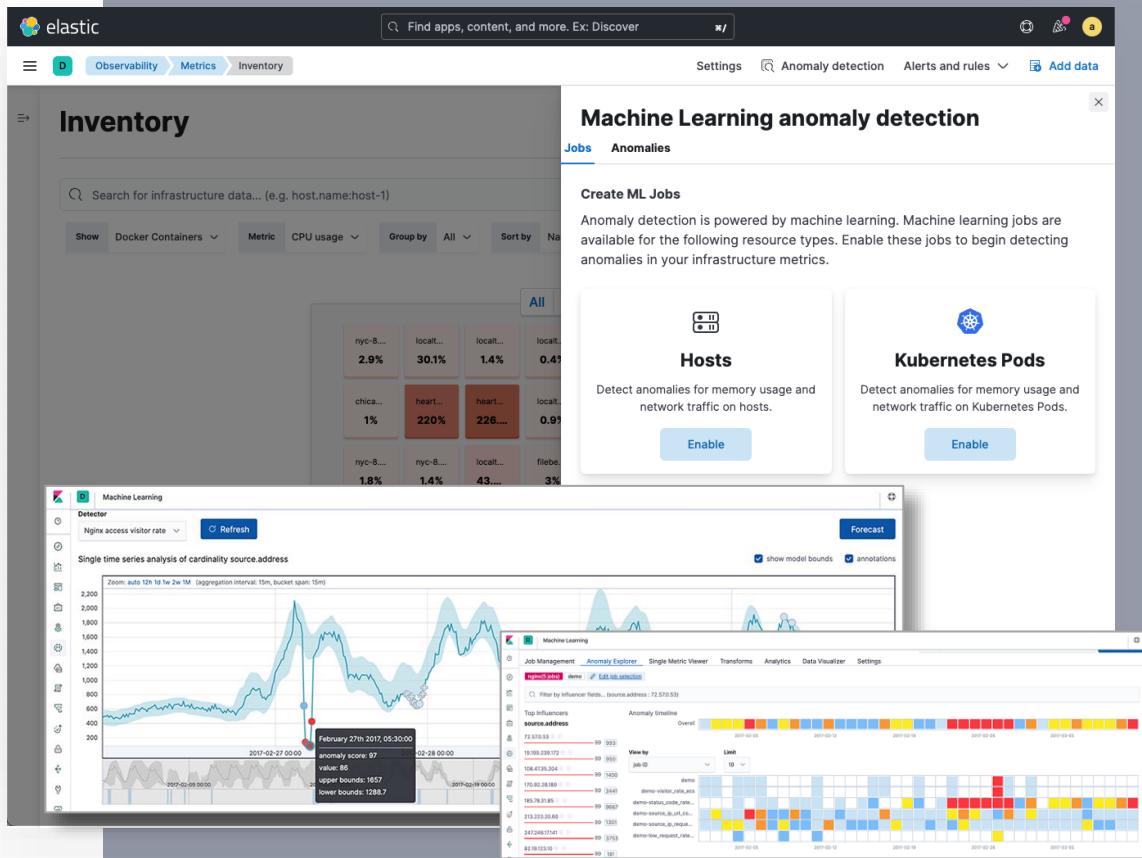
```
source.ip:10.42.42.42
```

- 다양한 팀이 협업 할 수 있는 환경 (ITOps, DevOps, SRE, AppDev)



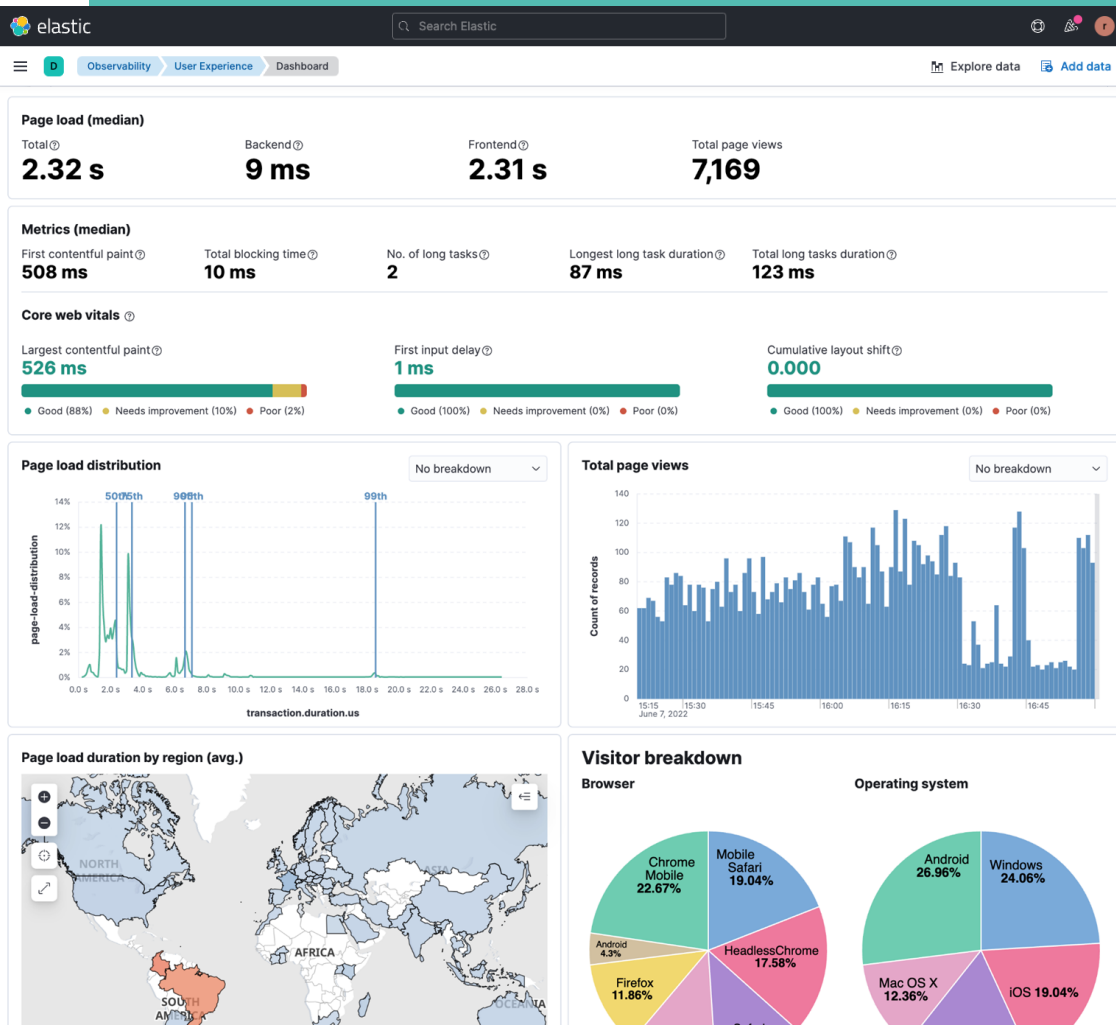
실행 가능한 인사이트

- 코딩이 필요하지 않은 빌트인 머신 러닝
- 시를 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



사용자 경험 측정 (RUM)

- 시간의 흐름에 따른 인프라, 애플리케이션 및 비즈니스 동향 추적
- 고객 경험을 측정하고 여정을 능동적으로 파악
- 프론트엔드에서 백엔드까지 한 번에 추적 & 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

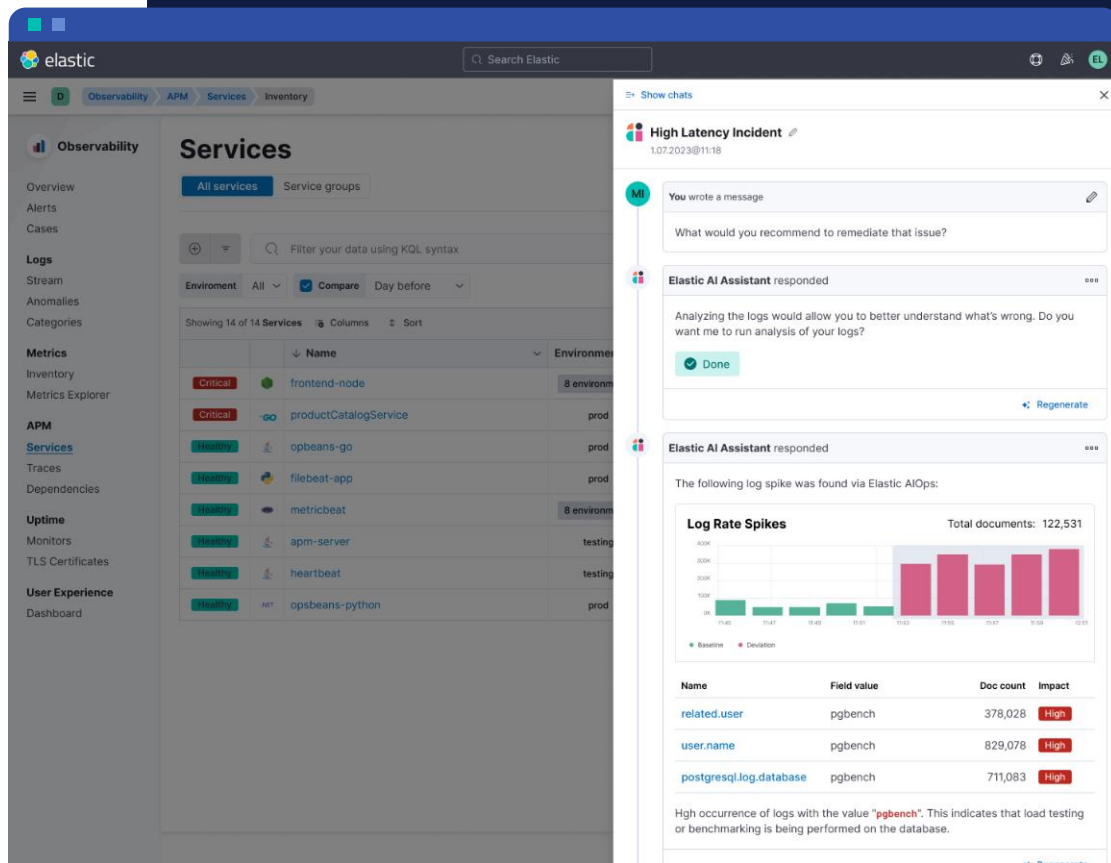
```
14.         l: false,
15.         exports: {}
16.     };
17.
18.     // Execute the module function
19.     modules[moduleId].call(module.exports, module, module.exports, __webpack_require__);
20.
21.     // Flag the module as loaded
22.     module.l = true;
23.
24.     // Return the exports of the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

> 1 library frame

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



The screenshot displays the Elastic Observability dashboard. On the left, a navigation sidebar includes sections for Overview, Alerts, Cases, Logs, Metrics, APM, Services, Traces, Dependencies, Uptime, Monitors, TLS Certificates, and User Experience. The main content area is titled 'Services' and shows a table of 14 services. The table includes columns for Name, Environment, and Status. Services like 'frontend-node' and 'productCatalogService' are marked as 'Critical', while others like 'opbeans-go' and 'metricbeat' are 'Healthy'.

On the right, a chat window titled 'High Latency Incident' is open. It shows a user message asking for remediation recommendations. The Elastic AI Assistant responds, suggesting log analysis and offering to run an analysis. A 'Done' button is visible. Below this, another AI response shows a 'Log Rate Spikes' chart and a table of log entries.

Log Rate Spikes Chart Data:

Time	Baseline	Deviation
11:45	~100	~100
11:47	~100	~100
11:49	~100	~100
11:51	~100	~100
11:53	~100	~300
11:55	~100	~350
11:57	~100	~300
11:59	~100	~350
12:01	~100	~350

Log Entries Table:

Name	Field value	Doc count	Impact
related.user	pgbench	378,028	High
user.name	pgbench	829,078	High
postgresql.log.database	pgbench	711,083	High

High occurrence of logs with the value "pgbench". This indicates that load testing or benchmarking is being performed on the database.

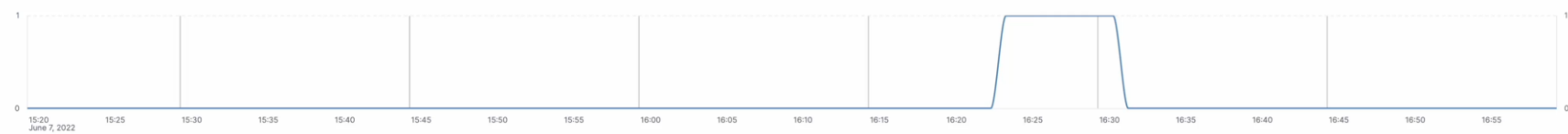
- Observability
- Overview
- Alerts
- SLOs
- Cases
- Logs
- Stream
- Anomalies
- Categories
- Infrastructure
- Inventory
- Metrics Explorer
- Hosts
- APM
- Services
- Traces
- Dependencies
- Synthetics
- Monitors
- TLS Certificates
- Uptime
- Uptime Monitors
- TLS Certificates
- User Experience
- Dashboard
- Universal Profiling
- Stacktraces
- Flamegraphs
- Functions

Alerts

Search alerts (e.g. kibana.alert.evaluation.threshold > 75)

Show all Active Recovered

1 Alerts 1 Active now



Columns 1 field sorted 1 alert Fields

Actions Alert Status Last updated Duration Reason

Active Jun 7, 2022, 16:20:20.801 (UTC+9) 567 s 101816 log entries in the last 5 mins. Alert when > 20000.

Updated 2 seconds ago

무료 14일 트라이얼 elastic.co/cloud/signup 퀵스타트 elastic.co/training/free

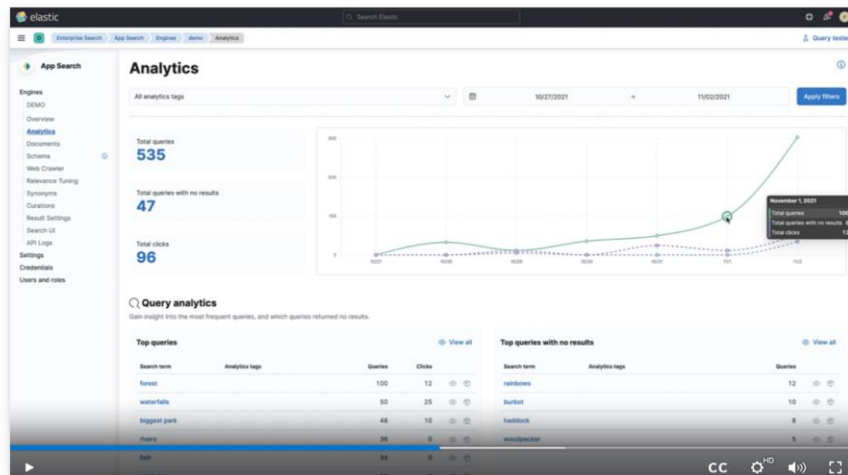
FREE ELASTIC TRAINING

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](#) →





Thank you!