

Jin's Portfolio

(이진형)

아파치 카프카 개발자 과정(CCDAK) 국내 최초 취득



- 토익 만점 (990점) 3회
- 컴퓨터과학 학사학위 취득
- 컴퓨터과학(정보과학) 석사학위 취득
- 정보처리 기사
- 정보보안 기사 필기합격 (2019)
- 아파치 카프카 개발자 자격증
- 자바개발자 과정 수료 (800시간 교육)

ELKK(Elastic Stack과 Kafka)를 사용하여 모니터링 시스템 설계 및 구축

- Ldap 서버를 시각화 하는 연구 과제
- 혼자서 모든 것을 설계 및 구축



logstash



elasticsearch



kibana

OpenDJ 설치 후 log를
Filebeat으로 수집

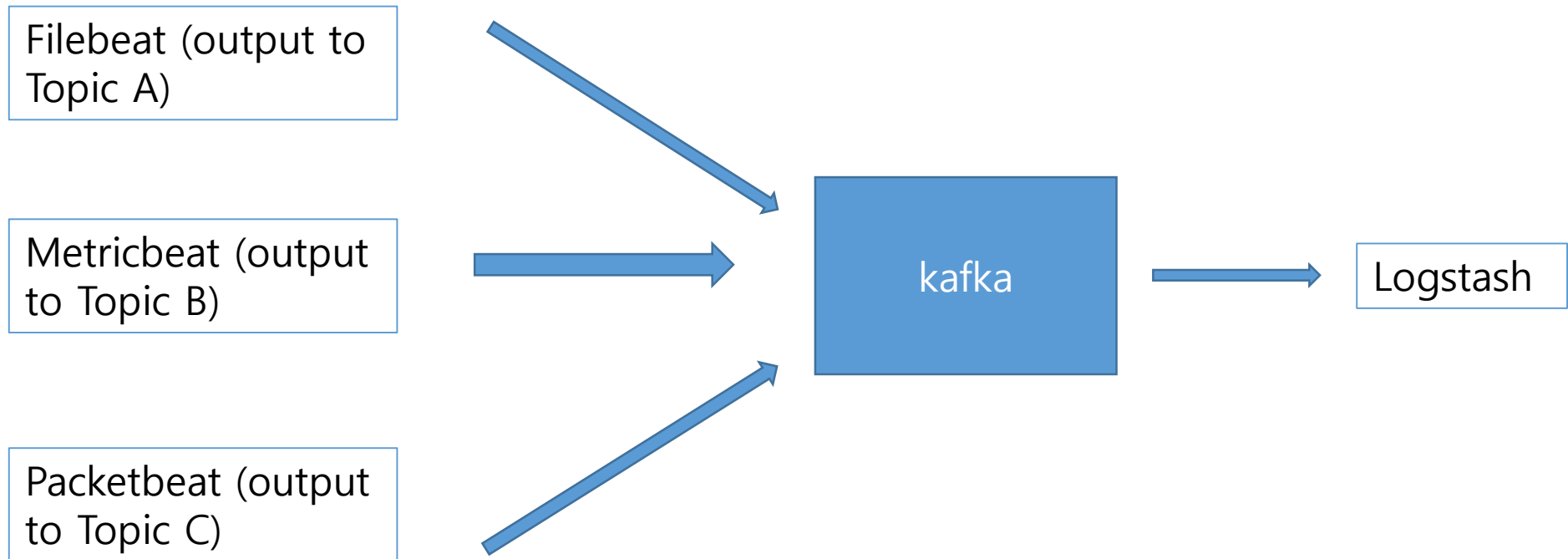
카프카를 거쳐

데이터를 정제,가공 할 수 있는
logstash를 거쳐 (아니면 필요없는
데이터까지 다 저장되어
성능이 떨어짐

DB에 저장 후

멋지게 시각화

시스템 정보
(CPU,
Memory,
disk,
network
bandwidth,
OS정보)를
Metricbeat으로 수집



APM(Application Performance Monitoring)

- Kibana의 APM UI를 통해 애플리케이션 성능 측정
- APM agent와 APM server 설치
- APM server가 Elasticsearch에 데이터를 저장하고 Kibana로 시각화.

APM

Setup Instructions

🔍

Search transactions and errors... (E.g. transaction.duration.us > 300000 AND context.response.status_code >= 400)

📅

▼

Last 24 hours

Show dates

🔄

Refresh

ServicesTraces

Name ↑	Agent	Avg. response time	Trans. per minute	Errors per minute
test	java	9 ms	< 0.1 tpm	0 err.

APM

Setup Instructions

🔍

Search transactions and errors... (E.g. transaction.duration.us > 300000 AND context.response.status_code >= 400)

📅

▼

Last 24 hours

Show dates

🔄

Refresh

ServicesTraces

Name	Originating service	Avg. response time	Traces per minute	Impact ↓
GreetingController#greeting	test	9 ms	0.047 tpm	

Transaction duration



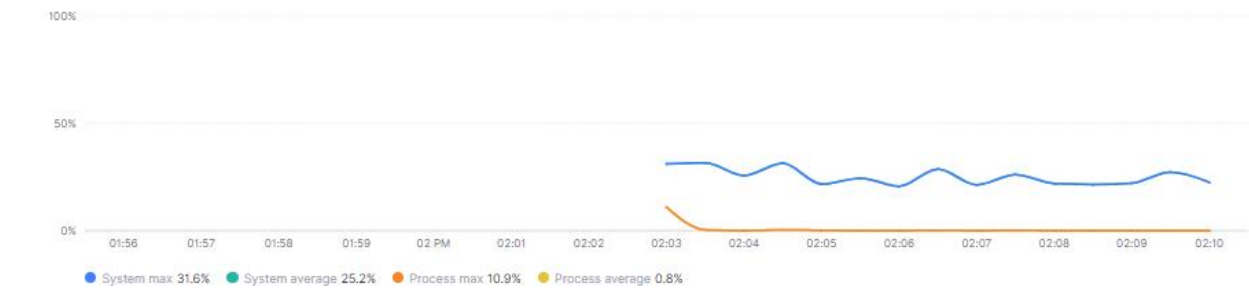
Requests per minute



No errors were found

Try another time range or reset the search filter.

CPU usage



Memory usage



GreetingController#greeting

Search transactions and errors... (E.g. transaction.duration.us > 300000 AND context.response.status_code >= 400)

Last 15 minutes Show dates Refresh



Transaction sample

Timestamp
5 minutes ago (September 4th 2019, 14:07:26.692)

Duration
19 ms

% of trace
100.0%

Errors
None

URL
http://localhost:8080/greeting

Result
HTTP 2xx

User ID
N/A

Actions

View full trace

Timeline

HTTP

Host

Service

Process

Agent

URL

User

Labels

Services

● test

0 ms

2 ms

4 ms

6 ms

8 ms

10 ms

12 ms

14 ms

16 ms

19 ms

HTTP 2xx

GreetingController#greeting

19 ms

request

cookies

JSESSIONID

[REDACTED]

headers

Accept

[

"text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3"

]

Accept-Encoding

[

"gzip, deflate, br"

]

Accept-Language

[

"en-US,en;q=0.9,ko;q=0.8,la;q=0.7"

]

Cache-Control

[

"max-age=0"

]

Connection

[

"keep-alive"

]

Host

[

"localhost:8080"

]

Sec-Fetch-Mode

[

"navigate"

]

Sec-Fetch-Site

[

"none"

]

Sec-Fetch-User

[

"?1"

]

Upgrade-Insecure-Requests

[

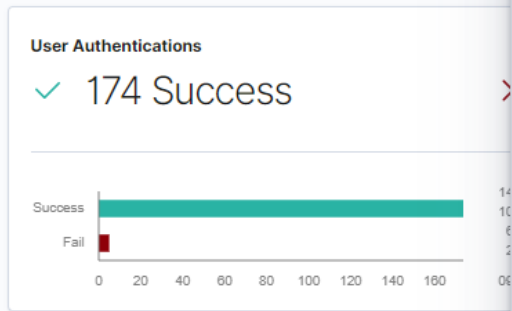
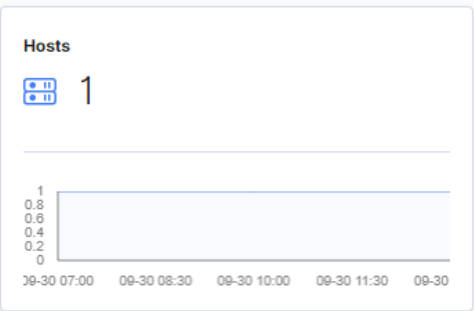
SIEM(Security Information and Event Management)

- 호스트 기반과 네트워크의 기반 데이터를 수집하여 Kibana의 SIEM으로 모니터링
- 감사 로그를 수집하는 AuditBeat와 윈도우 이벤트 로그를 수집하는 Beat, 그리고 네트워크 패킷 관련 데이터를 수집하는 PacketBeat로 데이터 수집

🔍 e.g. host.name: "foo"

Hosts

Last Event: 48 minutes ago



All Hosts

Showing: 1 Host

Name	Last Seen [Ⓢ] ↓
DESKTOP-MOVCIN1	Sep 30, 2019 @ 14:35:10.003

Authentications

Showing: 7 Users

User	Successes	Failures	Last Success
SYSTEM	153	0	3 hours ago
dsm	12	5	3 hours ago
DWM-1	3	0	9 hours ago

✕ ☆

Untitled Timeline

Description

🗨 Notes 0

🔒

📅 Last 24 hours

Show dates

🔄 Refresh

⚙

OR

host.name: "DESKTOP-MOVCIN1" ✕

Drop here to build an OR query

AND Filter

🔍 Filter events

Fields

@timestamp

message

event.category

event.action

host.name

> 📌 🗨

Sep 30, 2019 @ 14:35:10.003

--

network_traffic

network_flow

DESKTOP-MOVCIN1

🕒 0ns

🕒 Sep 30, 2019 @ 14:34:57.523

🕒 Sep 30, 2019 @ 14:34:57.523

86B 1 pkts

ipv6-icmp

1:piJGwae64DKlvYQple95ax0r4t0=

Source

fe80::616d:1aa9:a369:5697

86B 1 pkts

Destination

ff02::1:ff25:f79a

> 📌 🗨

Sep 30, 2019 @ 14:35:10.003

--

network_traffic

network_flow

DESKTOP-MOVCIN1

🕒 0ns

🕒 Sep 30, 2019 @ 14:34:57.523

🕒 Sep 30, 2019 @ 14:34:57.523

86B 1 pkts

ipv6-icmp

1:jW/Vq0SppxpTjVricXAU3+UNPUg=

Source

fe80::391a:b5a6:8125:f79a

86B 1 pkts

Destination

ff02::1:ff69:5697

> 📌 🗨

Sep 30, 2019 @ 14:35:10.003

--

network_traffic

network_flow

DESKTOP-MOVCIN1

🕒 0ns

🕒 Sep 30, 2019 @ 14:34:50.511

🕒 Sep 30, 2019 @ 14:34:50.511

86B 1 pkts

ipv6-icmp

1:EvnqrsQEryvew3HcjDx20zJzi90=

Source

fe80::5d5d:9a17:a026:7bca

86B 1 pkts

Destination

ff02::1:ff22:ce4

> 📌 🗨

Sep 30, 2019 @ 14:35:10.003

--

network_traffic

network_flow

DESKTOP-MOVCIN1

🕒 0ns

🕒 Sep 30, 2019 @ 14:34:50.511

🕒 Sep 30, 2019 @ 14:34:50.511

86B 1 pkts

ipv6-icmp

1:TF88lz9pRoDX9sMdPiXmFyzYLNw=

Source

fe80::5d5d:9a17:a026:7bca

86B 1 pkts

Destination

ff02::1:ffb9:b7ea

> 📌 🗨

Sep 30, 2019 @ 14:35:10.003

--

network_traffic

network_flow

DESKTOP-MOVCIN1

🕒 0ns

🕒 Sep 30, 2019 @ 14:34:50.511

86B 1 pkts

ipv6-icmp

1:xPZIYOc7a+jVpIEbCMv2MDouMCU=

Source

Destination

25 of 29259 Events


Load More

🕒 Updated 1 second ago

Network Events DNS Queries Unique Private IPs

Source IP	Last Domain	Direction	Bytes ↓	Packets	Unique Destination IPs
-----------	-------------	-----------	---------	---------	------------------------

Rows: 10 [Load More](#)



Top DNS Domains?

Showing: 290 Domains

☐ Include PTR Records

naver.com	107	72	3.618KB	10.832KB
-----------	-----	----	---------	----------

Rows: 10 [Load More](#)

[illegible]

AWS

사용해 본 서비스 목록 :

EC2

S3

Redshift

DynamoDB

Lambda

Elastic Beanstalk

Amazon EMR

Amazon Elasticsearch Service

Amazon Managed Streaming for Apache Kafka

CodeStar

CodeCommit

CodeDeploy

CodePipeline

Docker & Kubernetes & CI/CD

- AWS EC2에 미니큐브를 설치 후 helm chart를 이용해 카프카 pod 3, 주키퍼 pod 3으로 데이터 스트리밍 플랫폼 구성
- Docker image 만드는 법 연구 (Monolithic 회사 애플리케이션을 마이크로서비스로 전환 후 컨테이너화 하기 위해서)
- CI/CD 연구중 (DevOps 프로세스 도입으로 개발 생산성 향상을 위해서)

The End.