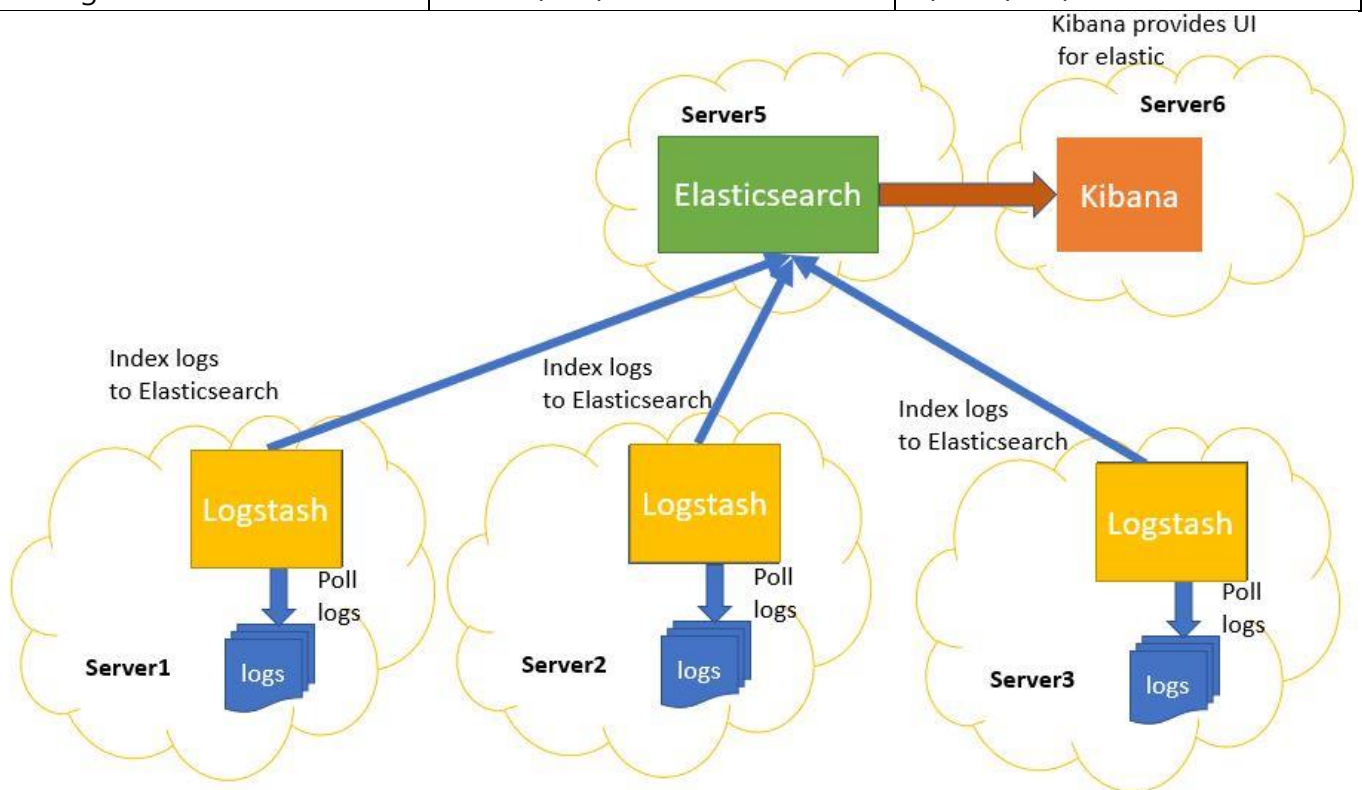
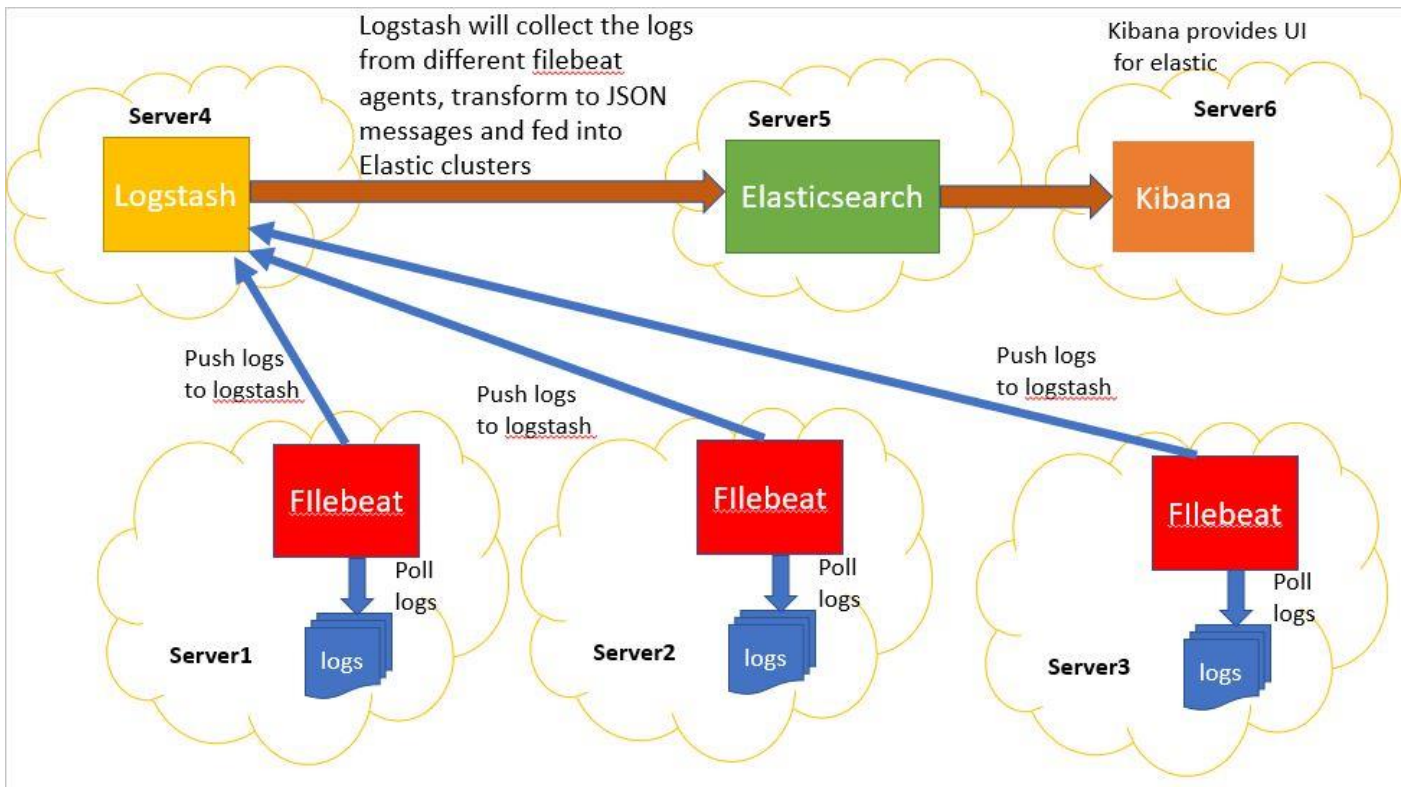


Beats란 무엇인가?

	Logstash	Beats
Resource(CPU와 RAM) 소모	무거움	가벼움
Input, output	많음	적음 Input: file, TCP/UDP, stdin Output: logstash, elasticsearch, kafka, redis, file
Filter	가능	제한적
Buffering	많은 메모리	적은 메모리



→Logstash의 기능



→Beats의 기능 = log 분석

모든 Beats는 오픈소스이며 아파치 라이선스를 가지고 있다.

모든 Beats는 각자마다 사용방법이 다르다.

모든 Beats는 데이터 수집과 엘라스틱서치에 데이터 적재 기능을 원활히 할 수 있도록 도와준다.

Beats의 종류

●Filebeat

Filebeat는 시스템에서 파일을 읽도록 설계되었습니다. 특히 시스템 및 응용 프로그램 로그 파일에 유용하지만 Elasticsearch에 인덱싱하려는 **모든 텍스트 파일**에 사용할 수 있습니다. 로깅의 경우 다양한 서버 및 VM에서 읽은 다음 중앙 Logstash 또는 Elasticsearch 인스턴스로 전송하여 로그 및 파일을 효율적으로 중앙 집중화할 수 있습니다. 또한 파일비트는 MySQL, Apache, NGINX 등으로부터 일반적인 로그 파일 형식을 수집하기 위한 "모듈"을 포함함으로써 구성 프로세스를 용이하게 한다. 이러한 모듈은 파일비트 구성을 단일 명령으로 줄입니다.

●Metricbeat

이름에서 알 수 있듯이 **Metricbeat는 서버 및 시스템에서 메트릭을 수집하는 데** 사용됩니다. 시스템 및 서비스 통계 전송 전용 경량 플랫폼입니다. 파일비트처럼, 메트릭비트는 리눅스, 윈도우, 맥 OS와 같은 운영 체제, 아파치, 몽고DB, MySQL, nginx와 같은 응용 프로그램으로부터 메트릭스를 수집하기

위한 모듈을 포함한다. Metricbeat는 매우 가볍고 시스템 또는 애플리케이션 성능에 영향을 주지 않고 시스템에 설치할 수 있습니다. 모든 Beats와 마찬가지로, Metricbeat는 자신만의 맞춤 모듈을 쉽게 만들 수 있게 해줍니다.

●Packetbeat

경량 네트워크 패킷 분석기인 **Packetbeat는 네트워크 프로토콜을 모니터링하여 사용자가 네트워크 지연 시간, 오류, 응답 시간, SLA 성능, 사용자 액세스 패턴 등을 감시할 수 있도록** 지원합니다. Packetbeat를 사용하면 데이터가 실시간으로 처리되므로 사용자는 트래픽이 네트워크를 통과하는 방식을 이해하고 모니터링할 수 있습니다. 또한 Packetbeat는 MySQL 및 HTTP를 포함한 여러 애플리케이션 계층 프로토콜을 지원합니다.

●Winlogbeat

Winlogbeat는 윈도우 이벤트 로그의 라이브 스트림을 제공하기 위해 특별히 설계된 도구이다. Windows 이벤트 로그 채널, 로그인 모니터링, 로그인 실패, USB 저장 장치 사용 및 새 소프트웨어 프로그램 설치에서 이벤트를 읽을 수 있습니다. Winlogbeat가 수집한 원시 데이터는 자동으로 Elasticsearch로 전송된 다음 나중에 편리하게 참조할 수 있도록 인덱싱됩니다. Winlogbeat는 보안 강화 톨의 역할을 하며 회사가 윈도우즈 기반 호스트에서 발생하는 모든 것을 말 그대로 감시할 수 있도록 합니다.

●Auditbeat

Auditbeat는 Linux 플랫폼에서 유사한 기능을 수행하며, 전체 사용자 및 프로세스 활동을 모니터링합니다. Auditd 이벤트 데이터가 분석되어 환경 보안 모니터링을 위해 Elasticsearch로 실시간으로 전송됩니다.

●Heartbeat

Heartbeat는 가동 시간 모니터링을 위한 경량 공급자입니다. 기본적으로 ping을 통해 서비스를 모니터링한 다음 분석 및 시각화를 위해 데이터를 Elasticsearch로 전송합니다. 하트비트는 ICMP, TCP 및 HTTP를 사용하여 ping할 수 있습니다. IT는 TLS, 인증 및 프록시를 지원합니다. 효율적인 DNS 확인을 통해 로드 밸런싱 서버 뒤의 모든 호스트를 모니터링할 수 있습니다.

(참고 사이트: <https://sabarada.tistory.com/46> / <https://www.youtube.com/watch?v=WNuWInfWWAg> / <https://www.objectrocket.com/resource/what-are-elasticsearch-beats/>)

(시청하면 좋은 유튜브 자료: <https://www.youtube.com/watch?v=G9B0FJf3xU0> – 영어자료, Auditbeat /

<https://www.youtube.com/watch?v=WNuWInfWWAg> – 영어자료, Filebeat /

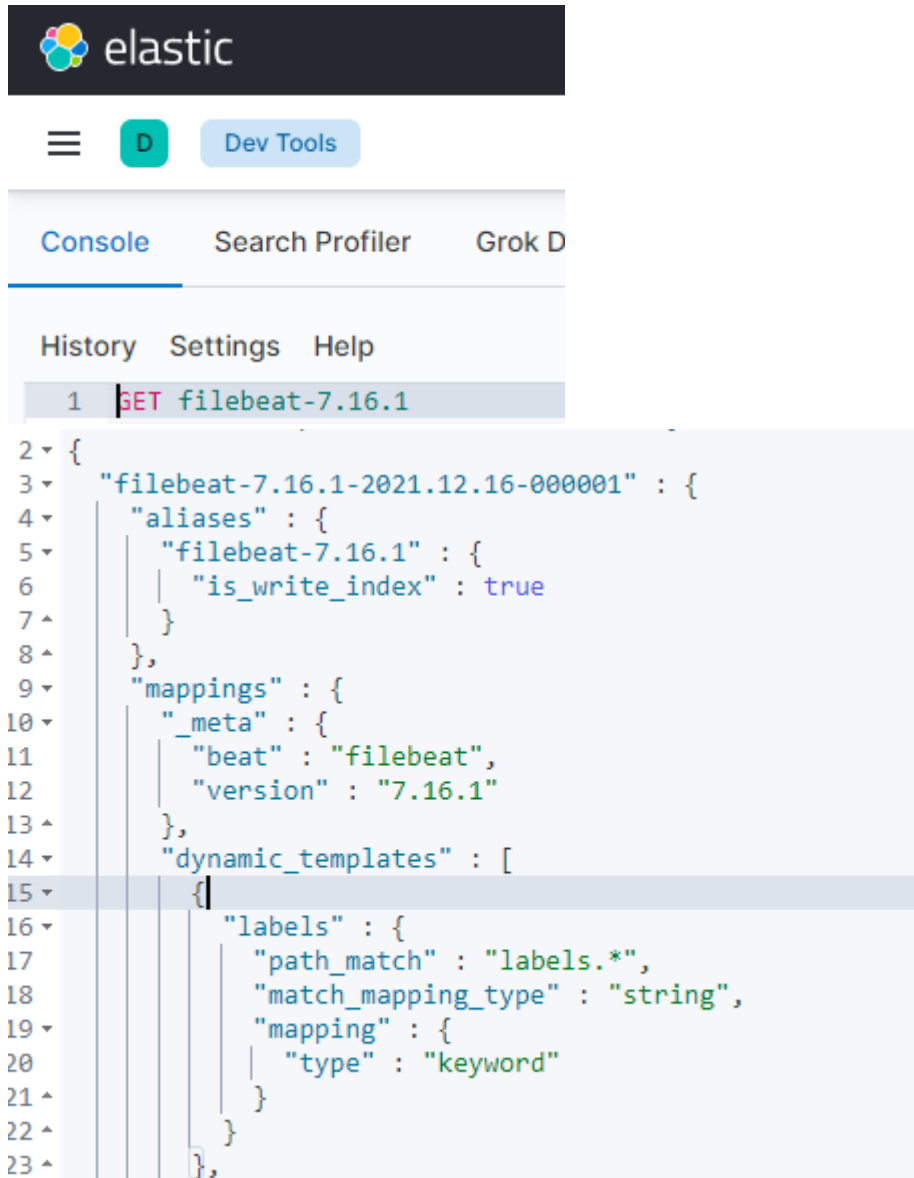
<https://www.youtube.com/watch?v=NeKnHoawKDI> – 한국어자료)

Filebeats 실습

<https://m.blog.naver.com/ksh60706/221729113310>

위 사이트를 똑같이 따라하면 된다. 띄어쓰기를 중요하게 생각하자.

참고로



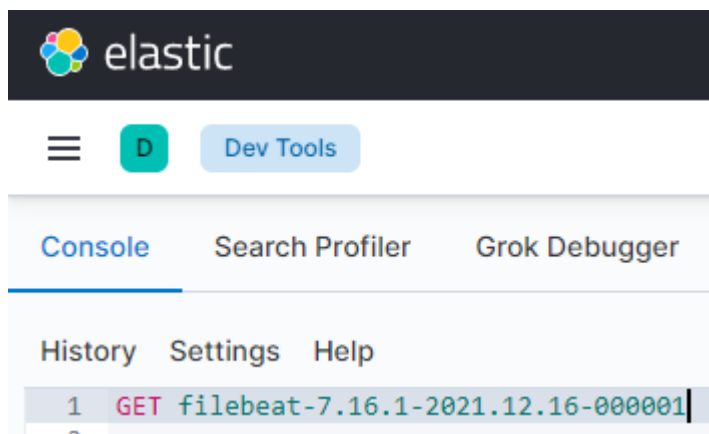
```
elastic

Console Search Profiler Grok D

History Settings Help

1 GET filebeat-7.16.1

2 {
3   "filebeat-7.16.1-2021.12.16-000001" : {
4     "aliases" : {
5       "filebeat-7.16.1" : {
6         "is_write_index" : true
7       }
8     },
9     "mappings" : {
10      "_meta" : {
11        "beat" : "filebeat",
12        "version" : "7.16.1"
13      },
14      "dynamic_templates" : [
15        {
16          "labels" : {
17            "path_match" : "labels.*",
18            "match_mapping_type" : "string",
19            "mapping" : {
20              "type" : "keyword"
21            }
22          }
23        }
24      ]
25    }
26  }
```



```
elastic

Console Search Profiler Grok Debugger

History Settings Help

1 GET filebeat-7.16.1-2021.12.16-000001|
2
```

```

2 {
3   "filebeat-7.16.1-2021.12.16-000001" : {
4     "aliases" : {
5       "filebeat-7.16.1" : {
6         "is_write_index" : true
7       }
8     },
9     "mappings" : {
10      "_meta" : {
11        "beat" : "filebeat",
12        "version" : "7.16.1"
13      },
14      "dynamic_templates" : [
15        {
16          "labels" : {
17            "path_match" : "labels.*",
18            "match_mapping_type" : "string",
19            "mapping" : {
20              "type" : "keyword"
21            }
22          }
23        }
24      ]
25    }
26  }
27 }

```

성공했다!

Create index pattern

Name

Use an asterisk (*) to match multiple characters. Spaces and the characters , /, ?, " , < , > , | are not allowed.

Timestamp field

✓ Your index pattern matches 2 sources.

filebeat-7.16.1

Alias

filebeat-7.16.1-2021.12.16-000001

Index

Rows per page: 10

Create index pattern

Name

Use an asterisk (*) to match multiple characters. Spaces and the characters , /, ?, " , < , > , | are not allowed.

Timestamp field

✓ Your index pattern matches 2 sources.

filebeat-7.16.1

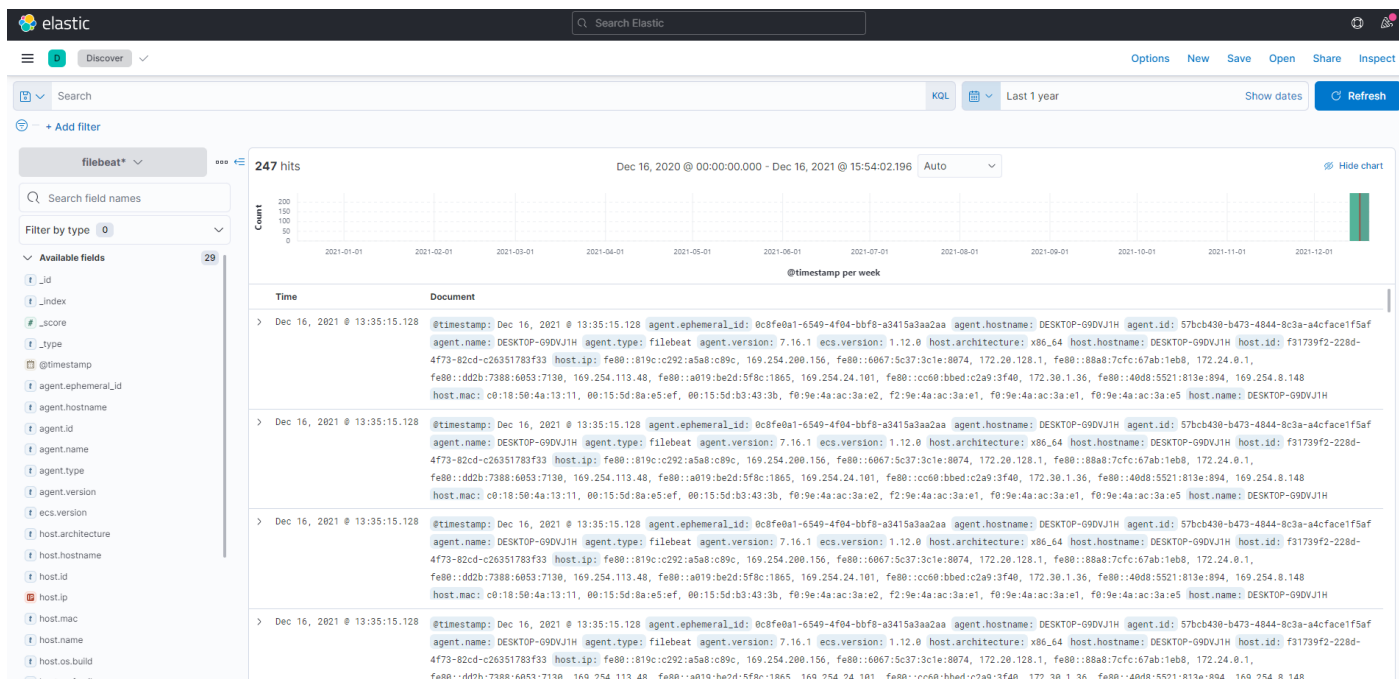
Alias

filebeat-7.16.1-2021.12.16-000001

Index

Rows per page: 10

파일의 log분석기라서 Timestamp field가 여러 개 뜬다.



discover에도 값이 이쁘게 30초 단위로 들어가고 있다.