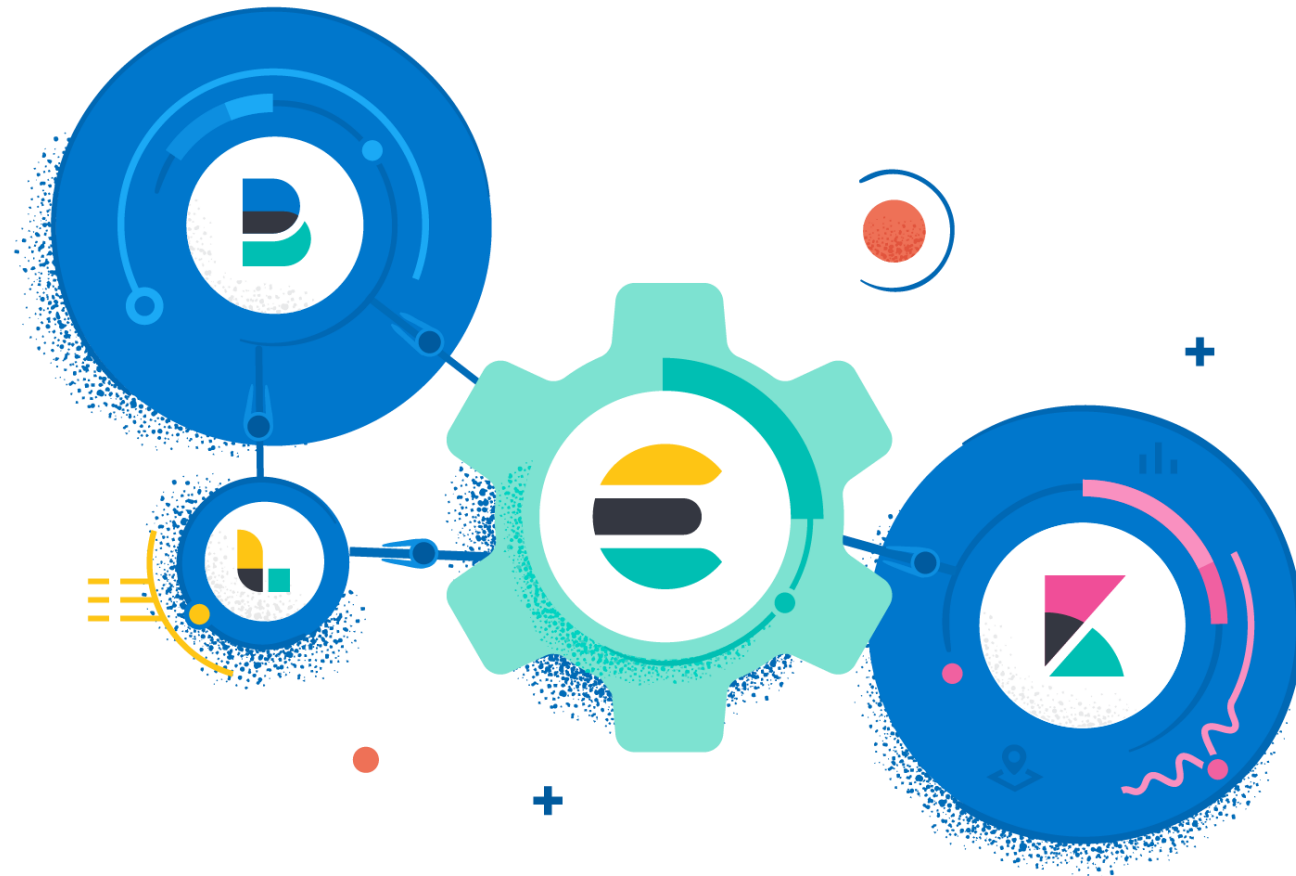


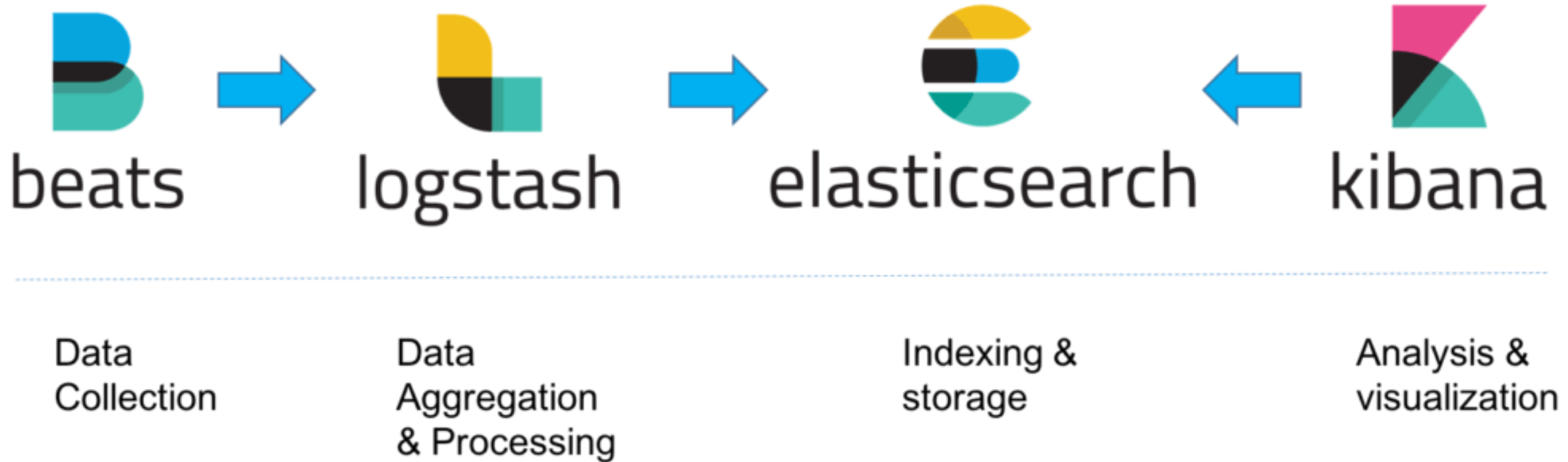
빅데이터 검색엔진 Elastic Stack



Elastic Stack

Elasticsearch, Logstash, Kibana 세가지 오픈 소스 프로젝트가 ELK Stack이라는 명칭으로 서비스가 제공되었고 여기에 Beats를 도입하여 Elastic Stack이라고 합니다.

<https://github.com/elastic>



Elasticsearch

아파치 루씬 기반의 Full Text 검색이 가능한 오픈소스 분석엔진입니다.
주로 REST API를 이용해 처리하며, 대량의 데이터를 거의 실시간으로 저장, 검색 및 분석 할 수 있습니다.

Search results for "서울, 한국" (Seoul, Korea) showing hotel listings with filters and details.

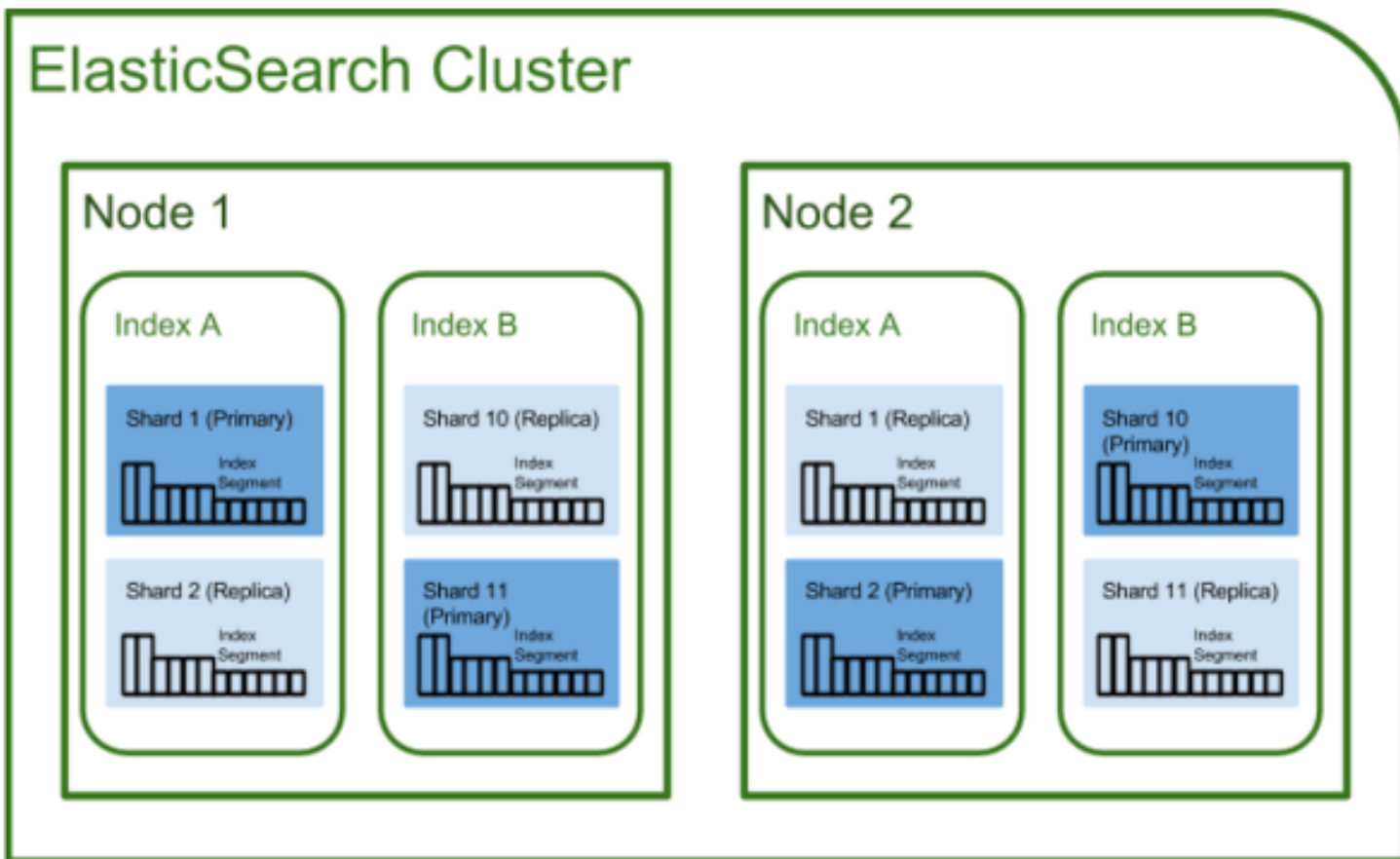
Filters: 검색 결과 좁히기: 3,033개 호텔, 주택 및 아파트. 숙박 시설 이름으로 검색. 인기 필터: 수영장, 아침 식사 포함, 호텔, 주차 포함, 객실 내 욕조. 1박 요금: ₩0 ~ ₩1,000,000+. 숙박 시설 등급: 1, 2, 3, 4, 5. 고객 평점: 0 ~ 10.

Hotel listings include:

- 광고 콘래드 서울 (Conrad Seoul) 5성급. ₩210,000. 여의동. 서울 (ICN-인천국제공항)까지 43km. 서울역까지 5.5km. 9.0 매우 훌륭함. 831개 Hotels.com 고객 이용 후기. 고객's PICK. 수영장, 무료 주차, 반려동물 동반 가능, 스파, 피트니스, 레스토랑.
- 광고 롯데 호텔 월드 (Lotte Hotel World) 5성급. ₩220,000. 송파구 올림픽로 240, 서울특별시, 138-220, 서울특별시. 송파. 서울 (ICN-인천국제공항)까지 58km. 서울역까지 12km. 8.8 훌륭함. 883개 Hotels.com 고객 이용 후기. 무료 주차, 레스토랑, 바, 욕조, 인터넷.
- 서울 신라호텔 (The Shilla Seoul) 5성급. ₩234,000. 중구 동호로 249, 서울특별시, 04605, 서울특별시. 장충동.



Elasticsearch 아키텍처



- 역색인(Inverted Index)을 통한 빠른 검색
- 클러스터 구성을 통한 분산처리 및 고가용성
- Replica를 활용한 데이터 안정성 증대
- Shard 분배를 통한 선형적 확장(scale-out)
- RESTful API 지원
- Schemaless 지원
- 인덱스 기반의 타입 및 색인 방식 설정 지원

Elasticsearch 아키텍처

■ Cluster

- 하나 이상의 Elasticsearch 노드들로 구성된 노드의 집합
- 클러스터는 Elasticsearch 시스템을 구성하는 가장 큰 단위로 독립적으로 운용

■ Node

- 노드는 Elasticsearch가 실행중인 인스턴스

■ Shard

- 데이터를 분산하여 저장하기 위해 Index의 범위를 나눈 것

■ Replica

- 분산 환경에서 데이터의 신뢰성을 높이기 위해 여러 노드에 데이터를 복제하여 저장하는 것

Elasticsearch 논리 아키텍처

■ Document

- 하나의 JSON 오브젝트로 elasticsearch 시스템에서 데이터를 구성하는 최소 단위
- 일반적인 row형 데이터베이스에서 하나의 row에 대응되는 개념

■ Field

- Document를 구성하는 하나의 key-value pair에 해당
- RDBMS의 열(column)에 대응되는 개념
- Elasticsearch는 schema-less 구조이므로, 하나의 Field에 다양한 타입의 데이터를 저장할 수 있음

■ Mapping

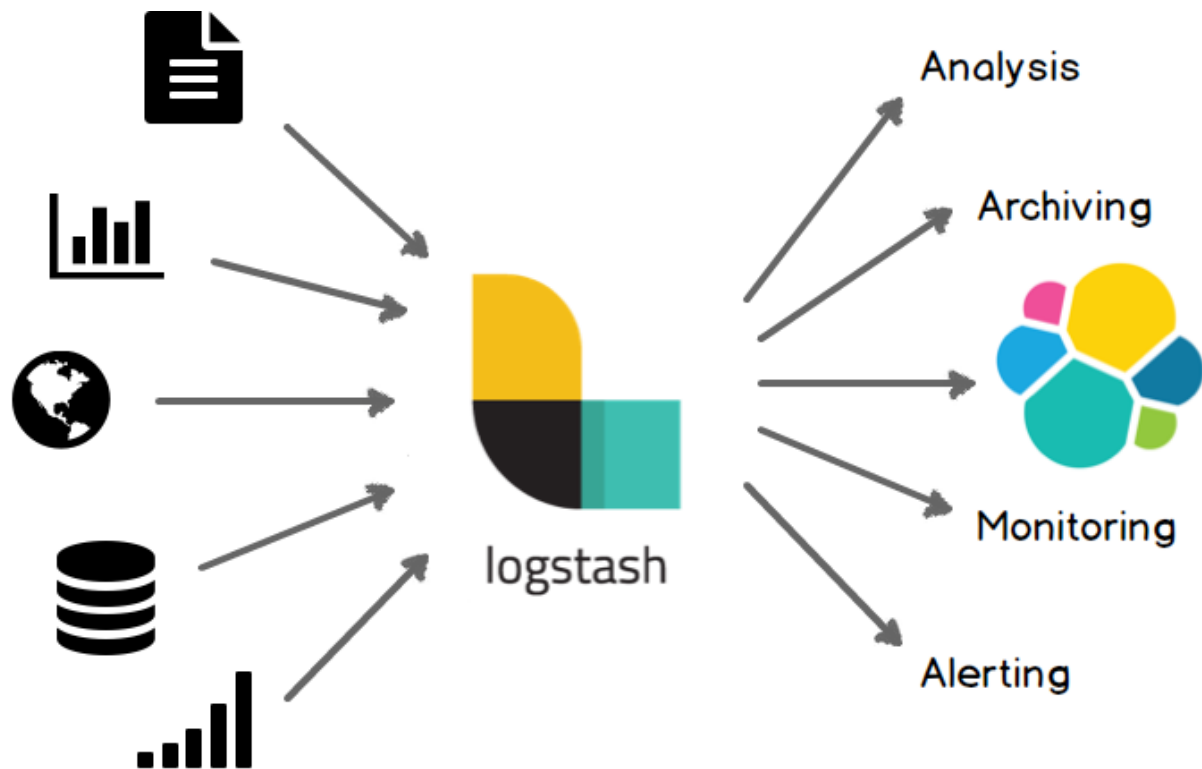
- 하나의 Document를 구성하기 위해 필요한 Field와 Field의 속성, 색인 방법을 정의하는 일련의 과정
- Mapping 과정은 RDBMS에서 스키마를 설계하고 인덱스를 설정하는 과정과 유사

■ Indices

- 여러 Type의 집합으로 RDBMS에서 Database에 대응되는 개념
- Index는 Shard와 Replica가 이루어지는 최소 단위

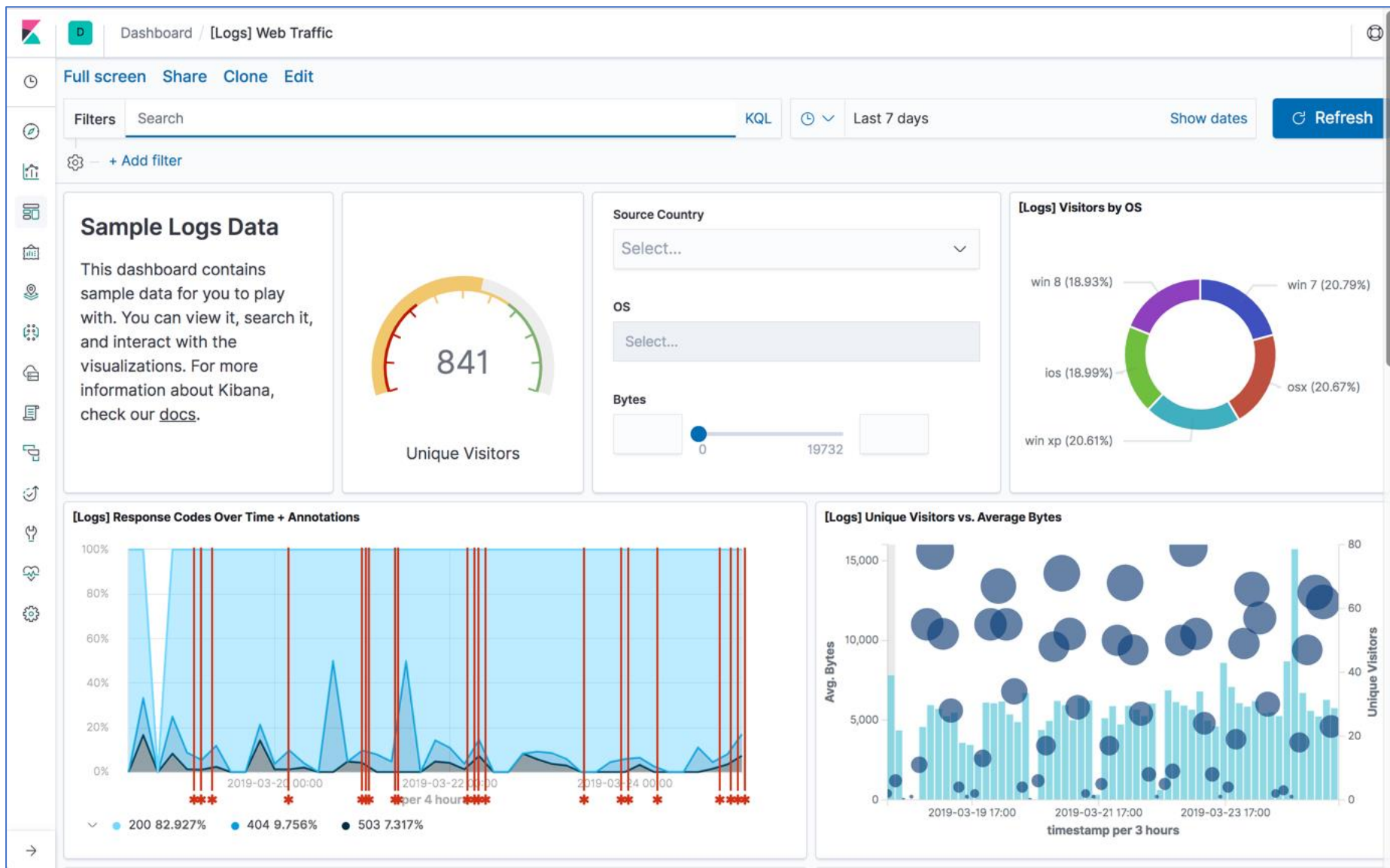
Logstash

다양한 플러그인을 이용하여 데이터 집계 및 보관, 데이터를 처리하며,
파이프라인으로 데이터를 수집하여 필터를 통해 변환 후 Elastic Search로 전송합니다.



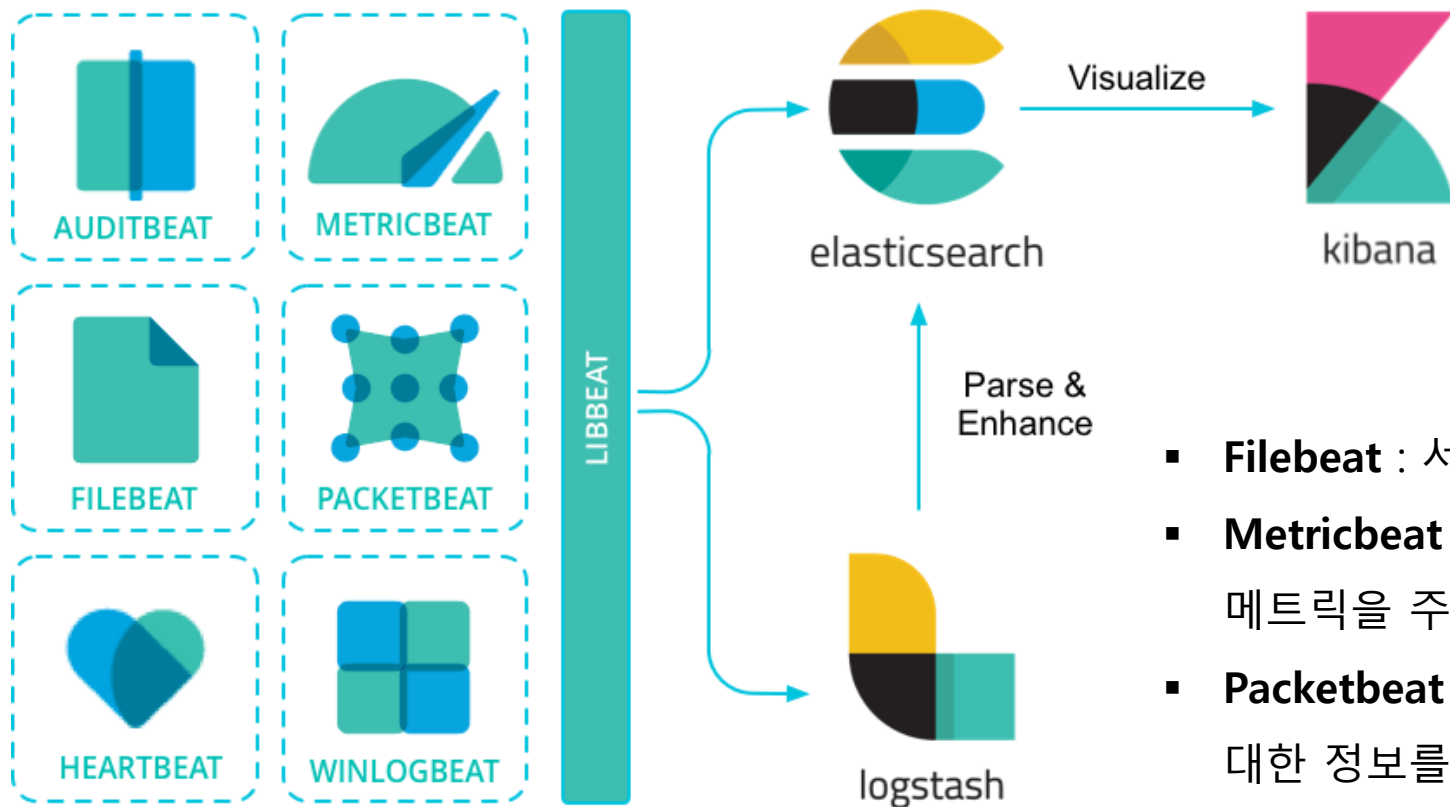
- **입력** : Beats, Cloudwatch, Eventlog 등의
다양한 입력을 지원하여 데이터 수집
- **필터** : 형식이나 복잡성에 상관없이 설정을 통해
데이터를 동적으로 변환
- **출력** : Elastic Search, Email, ECS, Kafka 등
원하는 저장소에 데이터를 전송

Elasticsearch에서 색인된 데이터를 검색하고 시각화 하는 기능을 제공합니다.



Beats

경량 에이전트로 설치되어 데이터를 Logstash 또는 Elastic Search로 전송하는 도구입니다.



- **Filebeat** : 서버에서 로그 파일을 제공
- **Metricbeat** : 서버에서 실행중인 운영 체제 및 서비스에서 메트릭을 주기적으로 수집하는 서버 모니터링 에이전트
- **Packetbeat** : 응용 프로그램 서버간에 교환되는 트랜잭션에 대한 정보를 제공하는 네트워크 패킷 분석기
- **Winlogbeat** : Windows 이벤트 로그를 제공

Elasticsearch 설치

<https://www.elastic.co/kr/downloads/elasticsearch>

Downloads:

↳ [WINDOWS](#) [sha](#) [asc](#)

↳ [MACOS](#) [sha](#) [asc](#)

↳ [LINUX X86_64](#) [sha](#) [asc](#)

↳ [LINUX AARCH64](#) [sha](#) [asc](#)

↳ [DEB X86_64](#) [sha](#) [asc](#)

↳ [DEB AARCH64](#) [sha](#) [asc](#)

↳ [RPM X86_64](#) [sha](#) [asc](#)

↳ [RPM AARCH64](#) [sha](#) [asc](#)

↳ [MSI \(BETA\)](#) [sha](#) [asc](#)

Package Managers:

Install with [yum](#), [dnf](#), or [zypper](#)

Install with [apt-get](#)

Install with [homebrew](#)

Containers:

Run with [Docker](#)

Elasticsearch 설치

■ jvm.options

- -Xms1g
- -Xmx1g

■ elasticsearch.yml

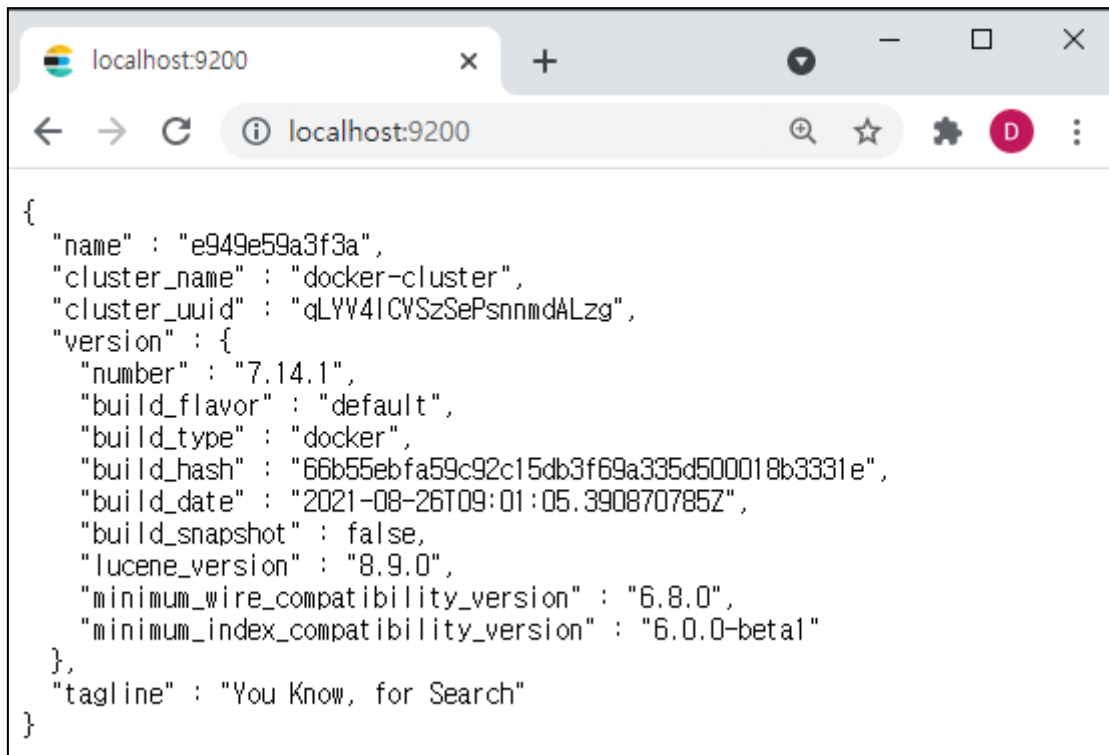
- **xpack.security.enabled: false**
- #network.host: 192.168.0.1
- #http.port: 9200
- #discovery.seed_hosts: ["host1", "host2"]
- #cluster.initial_master_nodes: ["node-1", "node-2"]

■ 실행

- cd bin
- elasticsearch

■ 실행 확인

- curl localhost:9200
- <http://localhost:9200/> 접속



```
{
  "name" : "e949e59a3f3a",
  "cluster_name" : "docker-cluster",
  "cluster_uuid" : "qLYV4lCVSZePsnmdALzg",
  "version" : {
    "number" : "7.14.1",
    "build_flavor" : "default",
    "build_type" : "docker",
    "build_hash" : "66b55ebfa59c92c15db3f69a335d500018b3331e",
    "build_date" : "2021-08-26T09:01:05.390870785Z",
    "build_snapshot" : false,
    "lucene_version" : "8.9.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

Kibana 설치

<https://www.elastic.co/kr/downloads/kibana>

Downloads:

↳ [WINDOWS](#) [sha](#) [asc](#)

↳ [MACOS](#) [sha](#) [asc](#)

↳ [LINUX X86_64](#) [sha](#) [asc](#)

↳ [LINUX AARCH64](#) [sha](#) [asc](#)

↳ [DEB X86_64](#) [sha](#) [asc](#)

↳ [DEB AARCH64](#) [sha](#) [asc](#)

↳ [RPM X86_64](#) [sha](#) [asc](#)

↳ [RPM AARCH64](#) [sha](#) [asc](#)

↳ [MSI \(BETA\)](#) [sha](#) [asc](#)

Package Managers:

Install with [yum](#), [dnf](#), or [zypper](#)

Install with [apt-get](#)

Install with [homebrew](#)

Containers:

Run with [Docker](#)

Kibana 설치

■ kibana.yml

- #elasticsearch.hosts: ["http://localhost:9200"]

■ 실행

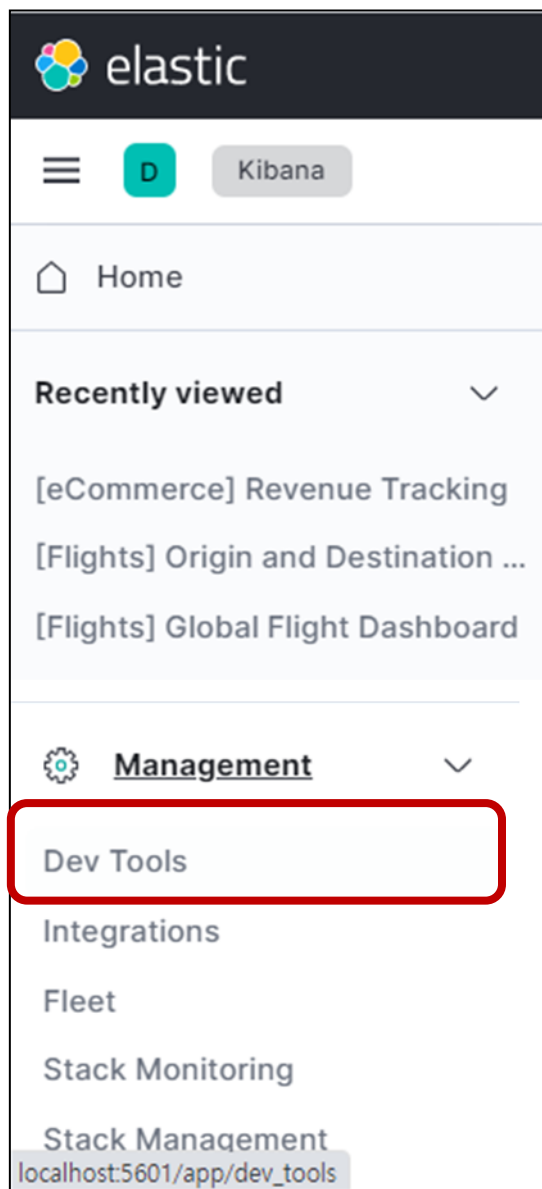
- cd bin
- kibana

■ 사용

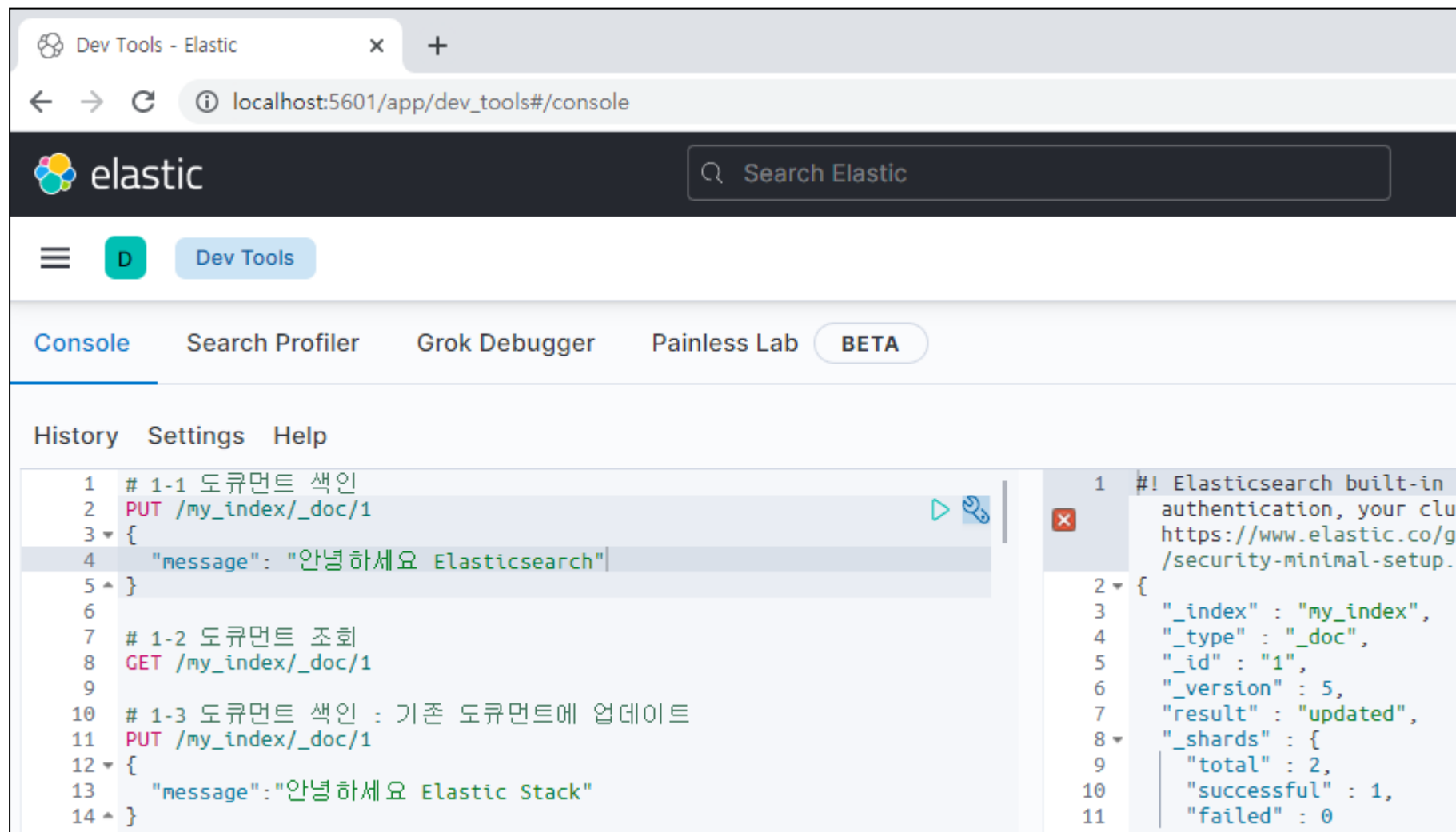
- http://localhost:5601/ 접속

The image displays two screenshots of the Kibana web interface. The left screenshot shows the 'Welcome home' page with a pink banner for 'Observability' and a 'Get started by adding integrations' section. The right screenshot shows the 'Sample data' page with various data visualizations and 'Add data' buttons. A red box highlights the 'Add data' buttons on the right, and a blue arrow points from the 'Try sample data' button in the left screenshot to the 'Add data' buttons in the right screenshot. A red circle with the number '1' is next to the 'Try sample data' button, and a red circle with the number '2' is next to the 'Add data' buttons.

Elasticsearch 실습



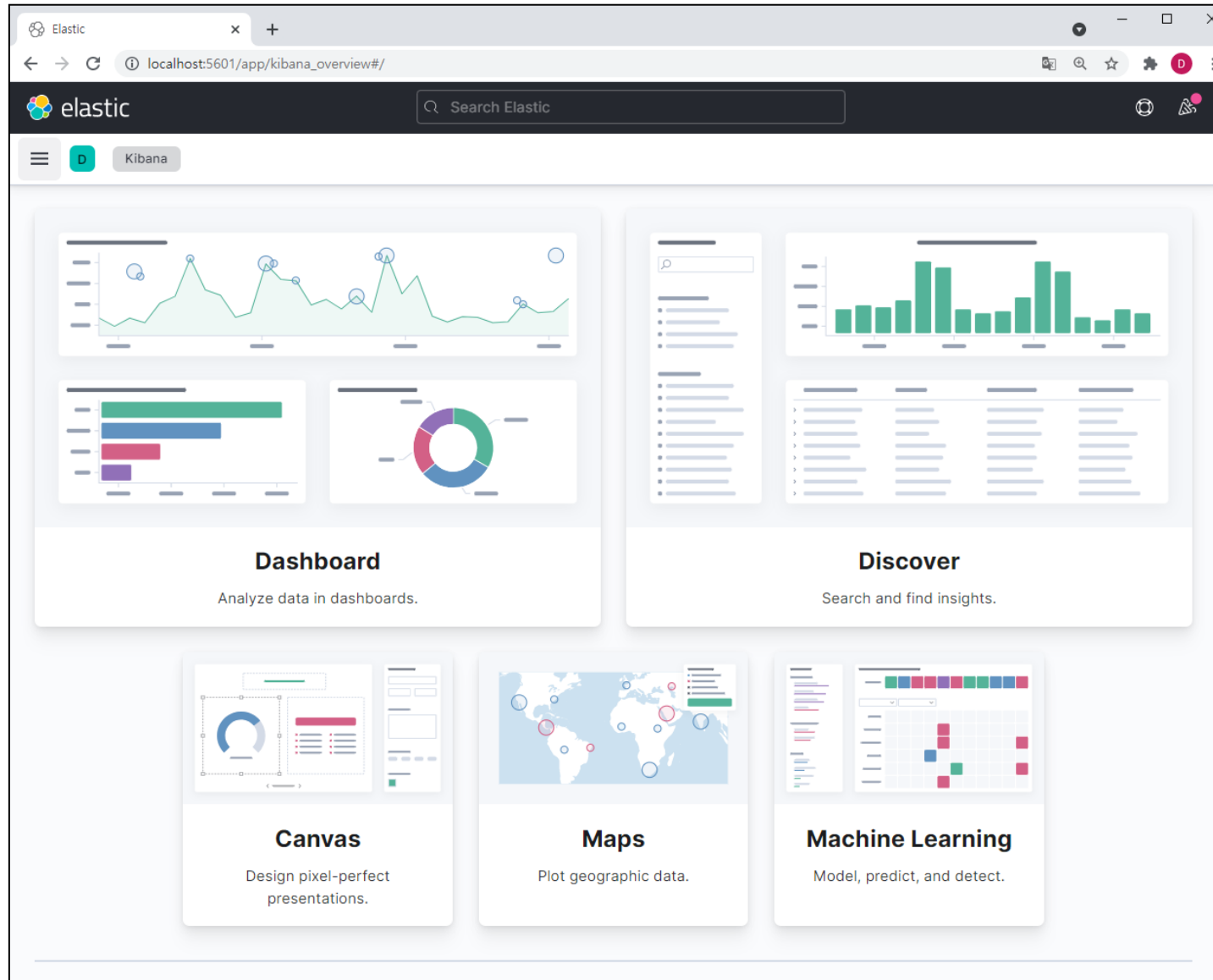
ElasticSearch.txt



<https://www.elastic.co/kr/webinars/getting-started-elasticsearch>

<https://github.com/kimjmin/elastic-demo/blob/master/demos/get-started/elasticsearch-7x.md>

Kibana 실습



ElasticSearch 클러스터 관리도구

<https://chrome.google.com/webstore/detail/multi-elasticsearch-head/cpmmilfkofbeimbmgiclohpodggeheim>

The screenshot displays the Elasticsearch-head Chrome extension interface. At the top, the browser tab is labeled 'elasticsearch-head'. The address bar shows the extension URL: 'chrome-extension://cpmmilfkofbeimbmgiclohpodggeheim/elasticsearch-head/index.html'. The main header area includes the 'Elasticsearch' logo, a dropdown menu for the selected instance ('elasticsearch (http://localhost:9200/) (8.2.3)'), and a yellow status bar indicating 'cluster health: yellow (6 of 11)'. Below the header, there are tabs for 'Overview', 'Indices', 'Browser', 'Structured Query [+]', and 'Any Request [+]'. The 'Cluster Overview' section is active, showing a table of indices with their sizes and document counts. Below this, there is a section for 'Unassigned' and 'Assigned' nodes. The 'Assigned' section shows a node named 'DESKTOP-335KS8C' with a status of '0' for each index.

Index	Size	Docs	Info	Actions
phones	size: 5.07ki (5.07ki)	docs: 5 (5)	Info	Actions
my_stations	size: 6.14ki (6.14ki)	docs: 10 (10)	Info	Actions
my_index_2	size: 7.87ki (7.87ki)	docs: 1 (1)	Info	Actions
my_index	size: 4.60ki (4.60ki)	docs: 5 (5)	Info	Actions
my_geo	size: 5.32ki (5.32ki)	docs: 4 (4)	Info	Actions
kibana_sample_data_ecommerce	size: 4.12Mi (4.12Mi)	docs: 4,675 (4,675)	Info	Actions
.security-7	size: unknown	docs: unknown	Info	Actions
.kibana_task_manager_8.2.3_001	size: unknown	docs: unknown	Info	Actions
.kibana_...	size: unk	docs: unk	Info	Actions

Node	phones	my_stations	my_index_2	my_index	my_geo	kibana_sample_data_ecommerce	.security-7	.kibana_task_manager_8.2.3_001	.kibana_...
Unassigned	0	0	0	0	0	0	0	0	0
DESKTOP-335KS8C	0	0	0	0	0	0	0	0	0

Thank you