다보리 - ElasticDB 운영 서버 [

- 1. Elasticsearch과 Kibana 개념 정리
    - Elasticsearch(ElasticDB) 개념
    - Kibana 개념
- 2. Elastic 서버 설치 전 설정 방법
    - Elasticsearch와 Kibana 설치 방법
    - Elsticsearch, Kibana 설정 가이드
- 3. Elasticsearch 서버 설치 방법
    - 서버 접속 방법
    - 서버 설치 방법
- 4. Elasticsearch 계정 생성
    - Elastic 사용자 계정 생성 방법

1. Elasticsearch Kibana

1. Elasticsearch과 Kibana 개념 정리

Elasticsearch(ElasticDB) 개념

1. Elasticsearch란?

Elasticsearch는 분산형 검색 및 분석 엔진으로 데이터를 분산 관리하고 빠르게 검색할 수 있는 기능을 제공함. 여러 서버를 연결해 클러스터를 구성하는 것이 특징이며, 주로 대량의

주로 로그 분석, 실시간 검색, 위치 기반 데이터 검색 등에서 널리 사용됨

2. Elasticsearch 주요 개념

1-1 노드(서버)

- Elasticsearch 클러스터를 구성하는 개별 서버 또는 인스턴스를 의미함
- 하나의 Elasticsearch 인스턴스를 실행하면, 그 인스턴스가 하나의 노드로 동작
- 노드는 각각 데이터 저장, 검색 요청 처리 등의 역할을 수행하며 신속한 검색을 제공

1-2 클러스터

- 클러스터는 Elasticsearch에서 여러 노드가 모여 하나의 시스템처럼 작동하는 집합을 의미함
- 문서, 인덱스, 샤드, 복제본을 생성하고 관리하는 전체 시스템을 의미함

2-1 문서

- 기본 데이터 단위로, JSON 형식으로 저장
- 하나의 문서는 사용자 정보나 제품 데이터 같은 개별 데이터

2-2 인덱스

- 문서들의 집합체로 여러 문서가 모여 하나의 인덱스를 형성
- 인덱스를 사용하여 데이터를 빠르게 검색하고 관리 가능

2-3 샤드

- 데이터가 많아질 경우 하나의 서버에 모든 데이터를 담을 경우 부하가 심해짐
- 샤드를 이용하여 인덱스를 여러 서버에 나누어 저장하는 기능을 제공
- 인덱스가 샤드로 나뉘어있어도 데이터를 검색하는 데 문제가 없으며, 검색 속도가 더 빨라짐
- Elasticsearch는 백그라운드에서 각 샤드에 분산된 데이터를 자동으로 모아서 결과를 하나의 인덱스처럼 보여줌
- 물리적으로는 여러 서버에 샤드(문서 단위로) 분산 되어 있지만 논리적으로는 모든 샤드들이 하나의 인덱스를 구성함

2-4 복제본

- Elasticsearch는 인덱스를 생성할 때 기본적으로 샤드의 복제본이 하나씩 자동으로 생성됨

복제본 샤드는 원본 샤드와 동일한 데이터를 가지고 있으므로 읽기 요청을 복제본에도 분산할 수 있어 읽기 속도가 빨라지며 고가용성을 보장함. 하나의 샤드에는 기본 데이터만 있고, 각 노드에 샤드 복제본을 만들어 서버 장애가 발생해도 복제본을 통하여 데이터를 유지할 수 있어서 안정성이 높아짐

1. Elasticsearch과 Kibana 개념 정리

Kibana 개념

Kibana란?

Elasticsearch 데이터의 시각화를 위한 도구이며 Elasticsearch에 저장된 데이터를 쉽게 검색, 분석하고 차트, 그래프, 웹 등 다양한 형태로 시각화하여 사용자는 Elasticse

Kibana의 주요 기능

- 데이터 시각화 : 차트, 지도 등 여러 형태의 시각화가 가능하며 데이터를 직관적으로 이해할 수 있음
- 대시보드 : 여러 시각화를 한 곳에 모아 실시간 모니터링 화면을 구성할 수 있어 운영 상태를 파악하는데 유용함
- 검색 및 필터 : Elasticsearch에 저장된 데이터를 검색하고, 특정 필드를 기준으로 필터링하는 기능을 제공
- **Canvas :** 사용자 정의 보고서를 만들 수 있는 도구로, 디자인 요소를 추가한 대시보드를 제작할 수 있음
- **Maps :** 위치 기반 데이터를 지도에 표시할 수 있는 기능을 제공
- **Machine Learning :** Kibana의 Machine Learning 기능을 사용하면 데이터의 패턴을 학습하고, 이상을 감지하면 경고 발생
- **Dev Tools :** Elasticsearch의 쿼리를 테스트하고, REST API를 통해 데이터를 직접 조작할 수 있는 도구
  Elasticsearch와 직접 상호작용 가능

Kibana의 활용 예시

- 로그 모니터링 : 서버 로그 데이터를 Elasticsearch에 저장 후, Kibana 대시보드에서 실시간으로 모니터링 함
- 고객 행동 분석 : 판매 데이터나 사용자 활동 데이터를 시각화하여, 제품 인기도나 특정 사용자 행동 패턴을 분석 가능
- 위치 기반 분석 : 매장별 판매 데이터나 지역별 사용자 활동을 지도 위에 표시하여 트렌드를 파악하고, 마케팅 전략에 활용

2. Elastic □□ □□ □ □□ □□

Elasticsearch와 Kibana 설치 방법

설치 절차

1. Elastic 다운로드 페이지 방문
https://www.elastic.co/kr/downloads/

2. Elasticsearch 다운로드

운영체제에 맞는 버전을 선택하여 다운로드
Linux, Windows, MacOS등 다양한 운영체제의 버전을 제공

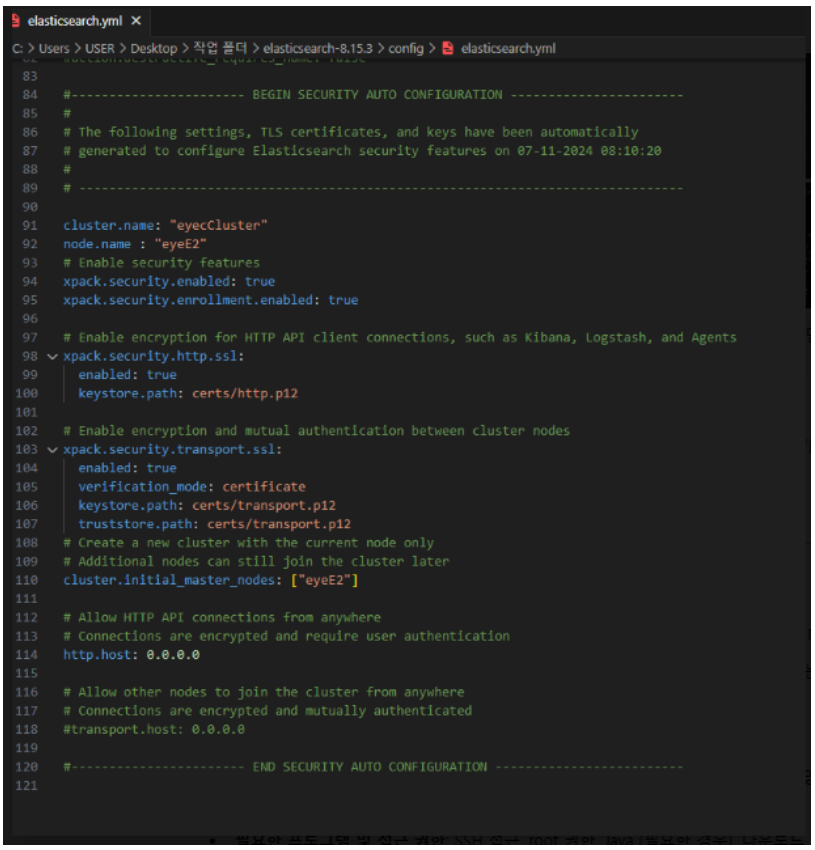
3. Kibana 다운로드
동일한 웹사이트에서 Kibana 다운로드 페이지로 이동하며, 운영체제에 맞는 버전을 다운로드

4. 설치 및 설정 진행
압축을 풀고, 각 소프트웨어에 대한 설정 파일을 수정 (다음 페이지 참고)

Elsticsearch, Kibana □□ □□□

1. Elasticsearch □□

Elasticsearch-8.xx.x/config/elasticsearch.yaml □□ □□

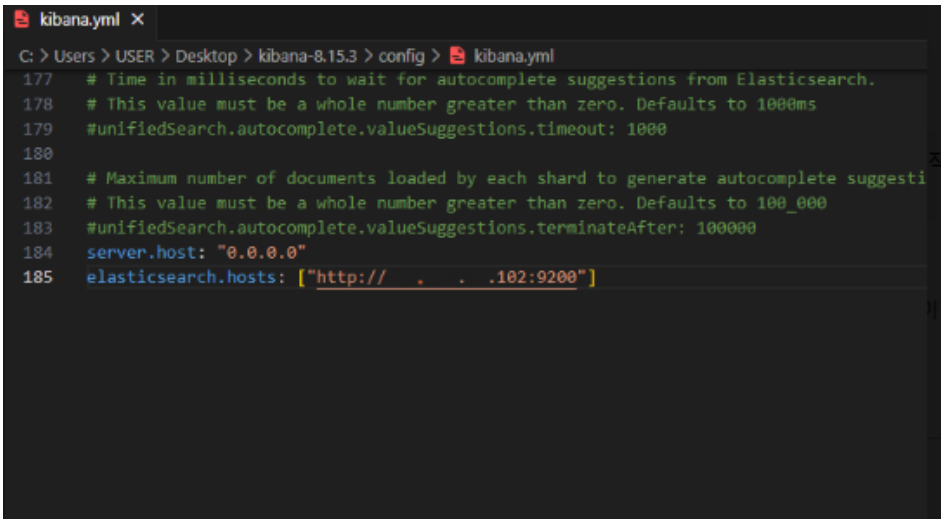


- **cluster.name : "eye"**
- **node.name : "eyeE2"** # □□□□□ □□□ □□□ □□
- **security.enabled : true** # □□ □□ □□□
- **security.http.ssl.enabled : true**
  # Kinaba□ Logstash □□□ □□ □□□□□□ HTTPS□ □□ □□□□ □□□ □ □□□ □□ □□
- **security.transport.ssl.enable : true**
  # □□□□ □□□ □□□□ □□□□ □□□□, SSL□ □□ □□ □□□ □□ # SSL : □
- **keystore.path : certs/transport.p12** # □□ □ SSL □□□ □□
- **truststore.path : certs/transport.p12** # □□□ □ □□ SSL □□□ □□
- **cluster.initail_master_nodes : ["eyeE2"]**
  # □□□□□ □□ □□□ □, □□ □□□ □□□ eyeE2□ □□
  1□□□□□ □□)

- **http:host : 0.0.0.0**
  # □□□□□ □□ IP□ □□□ □ □□□ □□, □□□ □□□□□ □□□□ □□□ □□□ □□□

2. Kibana □□

Kibana/config/kibana.yml □□ □□



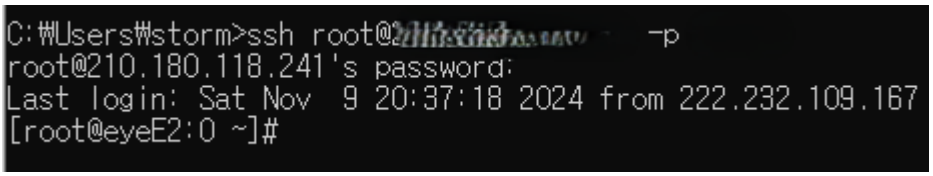
- **server.host : "0.0.0.0"**
  # Kibana□ □□ IP□□ □□ □□□□□ □□□ □□□□ 0.0.0.0□□ □□
- **elasticsearch.hosts : ["http://xxx.xxx.xx.xxx:9200"]**
  # Kibana□ □□□ Elasticsearch □□□ □□□ □□
  # Kibana□ □ □□□ □□ Elasticsearch□ □□□□ □□□□ □□□

3. Elasticsearch □□ □□ □□

3. Elasticsearch □□ □□ □□

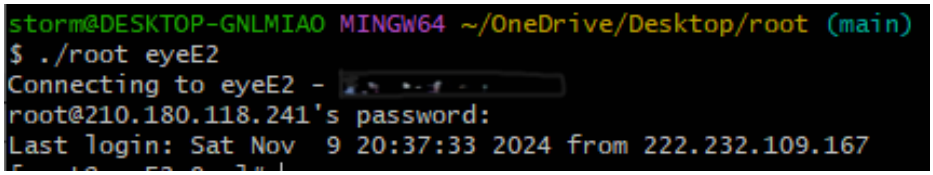
□□ □□ □□

□□ 1. SSH □□



- Window : Git Bash □□, Mac/Linux : □□□ □□ -> ssh (□□□□)@(□□IP) -p (□□) -> □□□□ □□ -> □□ □□

□□ 2. □□□□ □□□ □□ (□□□ □□□□ □□□ □□□ □□)



- Git Bash □□, Mac/Linux : □□□ □□ -> ./(□□ □□) (□□ □□) -> □□□□ □□ -> □□ □□

□□ □□ □□

Elasticsearch□ Kibana□ □□□ □□□□ □□

Elasticsearch



1. Elasticsearch □□□

- □□□ □□ □ -> wget **https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-8.x.x-linux-x86_64.tar.gz**

2. □□ □□

- **tar -xzf elasticsearch-8.x.x-linux-x86_64.tar.gz**

3. Elasticsearch □□

- **cd elasticsearch-8.x.x -> ./bin/elasticsearch**

4. Elasticsearch □□ □□

- **curl -X GET "http://□□_IP:9200"**

Kibana

```
c2-kafka@ubuntu:~/elastic$ wget https://artifacts.elastic.co/downloads/kibana/ki
bana-8.1.0-linux-aarch64.tar.gz
--2022-05-10 13:57:45--  https://artifacts.elastic.co/downloads/kibana/kibana-8.
1.0-linux-aarch64.tar.gz
Resolving artifacts.elastic.co (artifacts.elastic.co)... 34.120.127.130, 2600:19
01:0:1d7::
Connecting to artifacts.elastic.co (artifacts.elastic.co)|34.120.127.130|:443...
 connected.
HTTP request sent, awaiting response... 200 OK
Length: 282907567 (270M) [application/x-gzip]
Saving to: ‘kibana-8.1.0-linux-aarch64.tar.gz’

kibana-8.1.0-linux- 100%[===================>] 269.80M  4.59MB/s    in 70s
```

1. Kibana □□□

- □□□ □□ □ -> wget **https://artifacts.elastic.co/downloads/kibana/kibana-8.x.x-linux-x86_64.tar.gz**

2. □□ □□

- **tar -xzf kibana-8.x.x-linux-x86_64.tar.gz**

3. kibana □□

- **cd kibana-8.x.x -> ./bin/kibana**

4. Kibana □□ □□

- **http://□□_IP:5601 # □ □□□□□ URL□ □□ Kibana□ □□□□ □□□□□ □□□□□ □□**

4. Elasticsearch □□ □□

Elastic 사용자 계정 생성 방법

사용자 계정의 용도
1. Elasticsearch와 Kibana 보안 설정
보안 기능(security.enabled)이 활성화된 환경에서는 Elasticsearch와 Kibana에 접속할 때 사용자 계정이 필요
2. Kibana 로그인에 사용
Kibana URL에 접속하면 로그인 화면이 나타나고, 사용자 계정을 입력하여 접속 가능
3. Elasticsearch API 접근 제어
Elasticsearch API를 사용할 때도 인증된 계정으로 접근해야 함 (권한에 따라 API 접근을 제어)

사용자 생성 명령어
./bin/elasticsearch-users useradd <username> -p <password> -r <role> <username> : 생성할 사용자 이름
<password> : 사용자 비밀번호
<role> : 사용자의 역할 (superuser, kibana_user 등)

사용자 역할과 권한
1. superuser
모든 권한을 가진 최고 관리자 역할
2. kibana_admin
Kibana 설정을 관리할 수 있는 관리자 역할
3. kibana_user

Kibana 대시보드와 시각화 기능을 사용할 수 있는 일반 사용자 역할

4. read-only user (viewer)

읽기 전용 권한을 가진 역할, 데이터 조회만 가능 (변경이나 삭제 x)