OracleDB + ELK

개요

- Oracle DB와 ELK Stack간의 직접적인 통신

Data Flow

```
  Oracle DB
      |
      |
      V
   Logstash      1. Oracle DB에 접속, 쿼리한 데이터를 필터링
      |
      |
      V
Elasticsearch    2. 저장
      |
      |
      V
    Kibana       3. 모니터링
```

환경

Tool	Version
Windows	10
Docker	18.09.2
Docker-compose	1.23.2
ElasticSearch	7.2.0
Logstash	7.2.0
Kibana	7.2.0

1. ELK Install (Docker)

```
docker pull docker.elastic.co/elasticsearch/elasticsearch:7.2.0
docker pull docker.elastic.co/logstash/logstash:7.2.0
docker pull docker.elastic.co/kibana/kibana:7.2.0
```

2. Logstash config

- logstash.conf 수정

(ojdbc6.jar는 다운로드 후, logstash/logstash-core/lib/jars 에 넣어줘야함!)

ojdbc6 다운로드 링크

아래 .conf는 logstash container 내부에서 수정하거나, 로컬에서 수정 한 후 volume mount

```
# logstash.conf

input {
  jdbc {
    jdbc_driver_library => "/usr/share/logstash/config/ojdbc6.jar"
    jdbc_driver_class => "Java::oracle.jdbc.driver.OracleDriver"
    jdbc_connection_string => "jdbc:oracle:thin:@${DB_IP}:${PORT}/${DB_NAME}"
    jdbc_user => ${DB_ID}
    jdbc_password => ${DB_PW}
    statement => ${QUERY}
    use_column_value => true
    tracking_column => idx
    schedule => "* * * * *"
  }
}

filter {
#  filter ex)
#  date{
#    match => ["pick_req_inte", "yyyyMMddHHmmss"]
#  }
}

output {
  elasticsearch {
    hosts => ["http://${ELASTIC_IP}:${PORT}"]
    index => "${INDEX__NAME}"
  }

  stdout {
    codec => rubydebug
  }
}
```

3. Create docker-compose.yaml

- lgcns-logstash:latest : logstash.conf를 수정 후 commit 한 logstash image

```
version: '2.2'

services:
  logstash:
    image: lgcns-logstash:latest
    container_name: logstash
```

```
    command: ./bin/logstash -f /usr/share/logstash/config/logstash.conf
    ports:
      - 5044:5044
      - 9600:9600

  elasticsearch:
    image: docker.elastic.co/elasticsearch/elasticsearch:7.2.0
    container_name: elasticsearch
    environment:
      - node.name=elasticsearch
      - cluster.initial_master_nodes=elasticsearch
    ports:
      - 9200:9200

  kibana:
    image: docker.elastic.co/kibana/kibana:7.2.0
    container_name: kibana
    environment:
      ELASTICSEARCH_URL: http://${ELASTIC_IP}:${ELASTIC_PORT}
      ELASTICSEARCH_REQUESTTIMEOUT: 60000
    ports:
      - 5601:5601
```

4. 실행

- ELK 실행

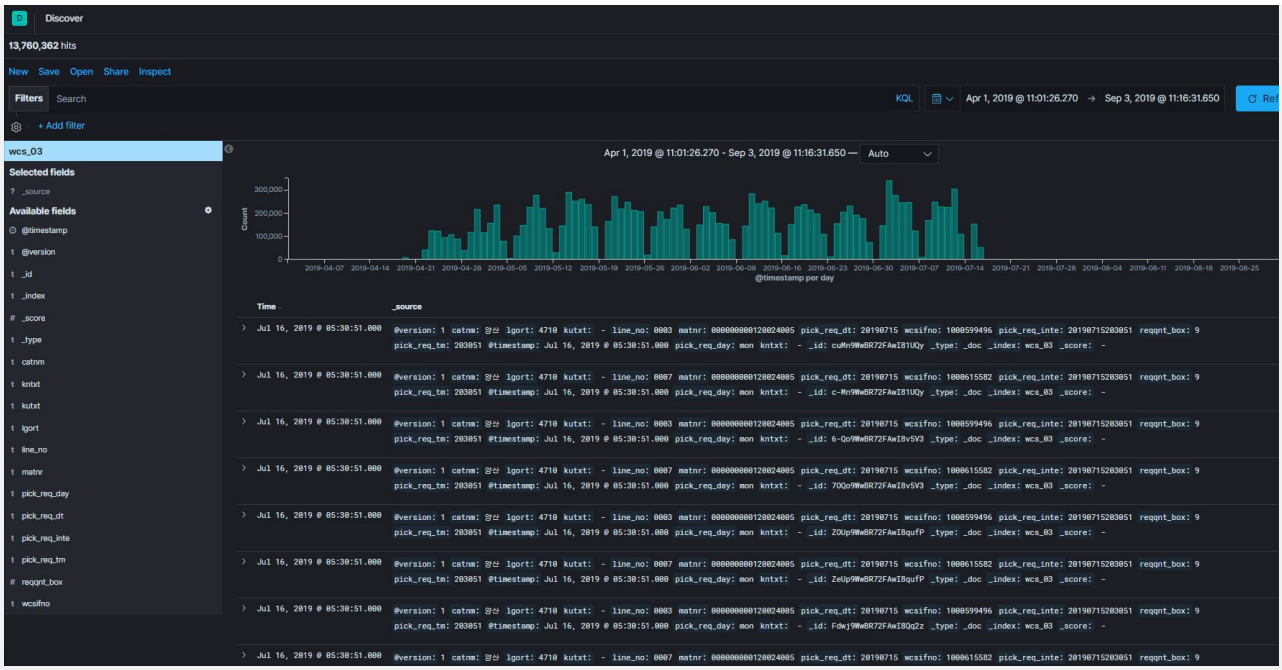
```
# [VR PC]

cd C:\Users\VR\elk
docker-compose up -d
```

- ELK 중지

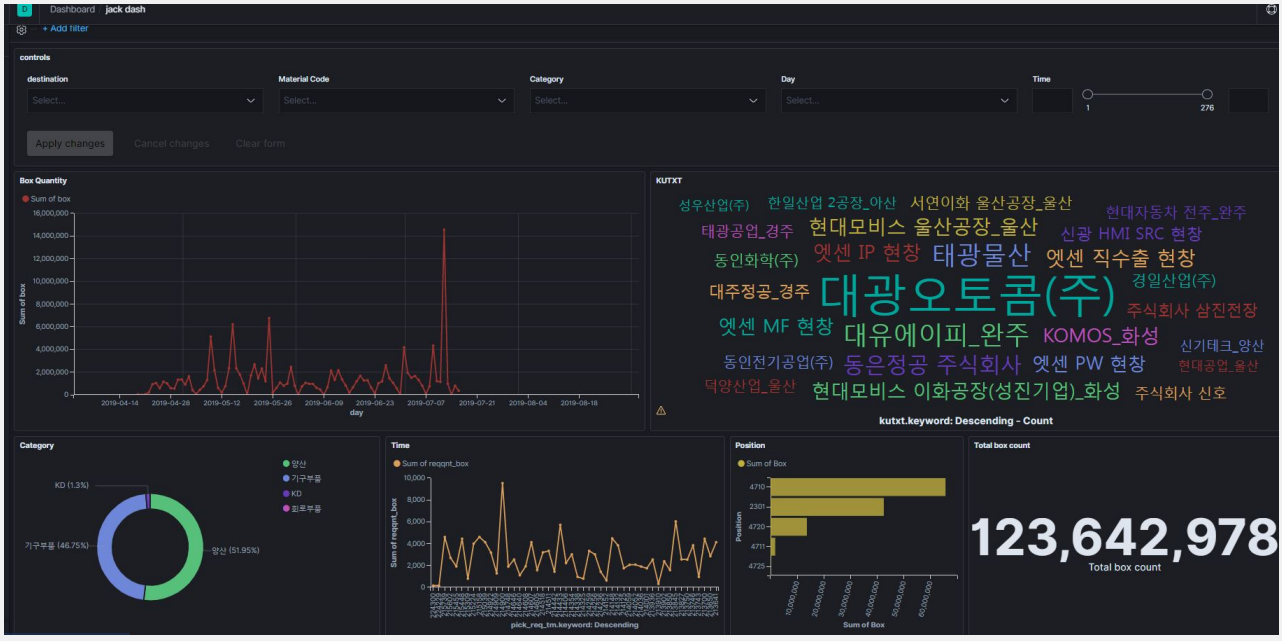
```
cd C:\Users\VR\elk
./elk-down.sh
```

5. 결과

> InputData



Dashboard



기타

- Logstash와 OracleDB의 데이터 통신 주기 확인이 필요

2019-09-03 강재구