ELK

분석 및 저장 기능을 담당하는 ElasticSearch, 수집 기능을 하는 Logstash, 이를 시각화하는 도구인 Kibana의 앞글자만 딴 단어이다. ELK는 접근성과 용이성이 좋아 최근 가장 핫한 Log 및 데이터 분석 도구

1) ElasticSearch
- ElasticSearch는 Lucene 기반으로 개발한 분산 검색엔진으로, Logstash를 통해 수신된 데이터를 저장소에 저장하는 역할을 담당
- 데이터를 중심부에 저장하여 예상되는 항목을 검색하고 예상치 못한 항목을 밝혀낼 수 있다.
- 정형, 비정형, 위치정보, 메트릭 등 원하는 방법으로 다양한 유형의 검색을 수행하고 결합할 수 있다.

2) Logstash
- 오픈소스 서버측 데이터 처리 파이프라인으로, 다양한 소스에서 동시에 데이터를 수집하고 변환하여 stash 보관소로 보낸다.
- 수집할 로그를 선정해서, 지정된 대상 서버(ElasticSearch)에 인덱싱하여 전송하는 역할을 담당하는 소프트웨어

3) Kibana
- 데이터를 시각적으로 탐색하고 실시간으로 분석 할 수 있다.
- 시각화를 담당하는 HTML + Javascript 엔진이라고 보면 된다.

- 자동 실행

자동 실행

```
#!/bin/sh

echo "\n\n"
echo "########################################"
echo "########## CHECK ELK  START ! ###########"
echo "########################################"

cd /app/elasticsearch-7.4.1/
elasticsearchcheck=`ps -ef | grep  elasticsearch | awk '{print ($2)}' | wc -l`
if [ $elasticsearchcheck -gt 1 ]
then
   echo "Already Elasticsearch started !"
else
   echo "Start ElasticSearch !"
   /app/elasticsearch-7.4.1/startup.sh
fi

cd /app/kibana-7.4.1-linux-x86_64/
kibanacheck=`ps -ef | grep kibana | awk '{print ($2)}' | wc -l`
if [ $kibanacheck -gt 1 ]
then
   echo "Already Kibana started !"
else
   echo "Start Kibana !"
   /app/kibana-7.4.1-linux-x86_64/startup.sh
fi

cd /app/logstash-7.4.1/
logstashcheck=`ps -ef | grep logstash | awk '{print ($2)}' | wc -l`
if [ $logstashcheck -gt 1 ]
then
   echo "Already Logstash started !"
else
   echo "Start Logstash !"
   /app/logstash-7.4.1/startup.sh
fi

cd /app/
echo "########################################"
echo "############ CHECK ELK END ! ############"
echo "########################################"
echo "\n\n"
```