

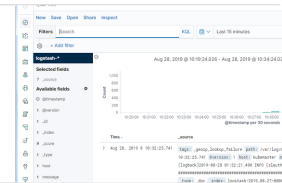
# ELK system

## ▼ Data Architecture (ELK Stack)자료

<https://velog.io/@shinychan95/Elasticsearch-기본-개념-및-특징-정리>

[ELK+Redis] Elasticsearch + Logstash + Kibana + Redis + SpringSleuth를 활용한 로그 추적 시스템 구축  
본 포스팅에서는 제목에서 명시한 바와 같이 ELK + Redis + SpringSleuth를 활용한 마이크로서비스 로그 추적 시스템 구축 방안에 대해 살펴보겠습니다. 이미 수많은 포스팅에서 ELK + Redis / SpringBoot + Sleuth + Zipkin에 대한 가이드가 있었지만, 이 모든 모듈을 활용하여 종합 로그 추적 시스템을 구축하는 포스팅을 찾지 못해 포스팅을 쓰게 되었습니다.

https://waspro.tistory.com/535



ELK+ Redis + SpringSleuth Log 추적 시스템

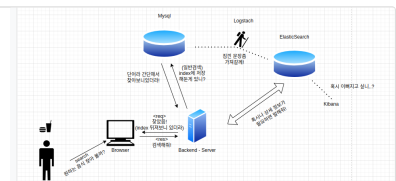
<https://soyoung-new-challenge.tistory.com/58>

MySQL ~ Logstash → ES

### Search Process

수업 시간 때 만든 ELK Stack을 통한 검색 프로세스에 대한 파이프라인을 만들었는데 부족한 부분이 많이 보인다...(Redis를 집어넣지 못했다) 원래라면 MySQL자리에 Redis가 있어야 하고 백엔드 서버와 Logstash 사이에 MySQL이 들어와서 데이터를 저장하고 Logstash에 데이터를 폴링(polling)하는 역할을 집어 넣어줬

https://velog.io/@hanoo2/Search-Process

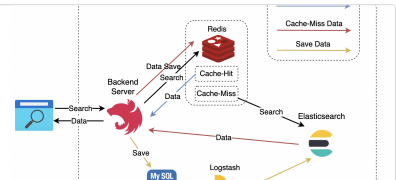


검색 프로세스

### Search Process

서비스를 운영할 때, Client가 원하는 데이터를 찾을 때 DB에 저장되어 있는 Data를 찾아서 제공해야 합니다. Data와 요청이 많아질수록 검색 속도는 점점 느려지게 됩니다. 이러한 문제를 극복하고, 더 빠른 속도로 검색 결과를 제공하기 위해서 여러가지 다른 특성을 지닌 DB를 조합하여 성능을 향상시킬 수 있습니다.

https://velog.io/@jhyeom1545/Search-Process



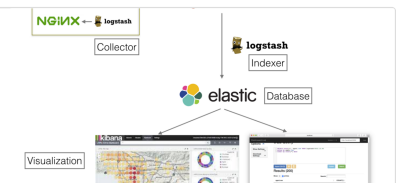
검색 프로세스 2

### ELKR (ElasticSearch + Logstash + Kibana + Redis) 를 이용한 로그분석 환경 구축하기

큰 서비스들을 운영하는 회사들은 자체적인 로그 수집, 정제, 분석 솔루션들을 가지고 있거나 자체적으로 대용량 ES Cluster, Hadoop Cluster 등을 운영합니다. 하지만 초기 스타트업은 한치앞을 내다 볼 수 없기때문에 최소 비용으로 최대의 효과를 낼 수 있는 여러 오픈소스들을 조합하여 잘 사용해야 합니다.

https://medium.com/chequer/elkr-elasticsearch-logstash-kibana-redis-%EB%A5%BC-%EC%9D%B4%EC%9A%A9%ED%95%9C-%EB%A1%9C%EA%B7%B8%EB%B6%84%EC%84%9D-%ED%99%98%EA%B2%BD-%EA%B5%AC%EC%B6%95%ED%95%98%EA%B8%B0-f3dd9d9ae622

ELK + Redis 로그분석 환경 구축



### (3) ELKR (ElasticSearch + Logstash + Kibana + Redis) 로그 분석 시스템

Loggly나 Splunk 같은 유료 로그 매니지먼트 서비스나 자체 로그 분석 시스템을 만들어서 사용하려면 적지 않은 시간과 비용이 들어간다. ElasticSearch, Redis 등 오픈소스 툴을 사용하여 스케일링이 가능한 로그분석 시스템을 만들어 보자. 시스템의 구성은 다음과 같다: Nginx, Apache, Tomcat 등 웹 서버에서 발생하는

http://blog.plura.io/?p=3363



ELK + redis 구축

#### kodol

<https://www.elastic.co/kr/> 오픈소스 검색 및 분석· Elasticsearch | Elastic Elasticsearch 시작하기 실시간 데이터 분석과 검색을 경험해 보세요. [www.elastic.co](http://www.elastic.co) Elasticsearch 는 실시간 검색엔진이라 익숙만 하다면, 검색엔진 도입으로 아주 좋은것 같다. Elasticsearch 에서 제공하는 유틸중에 유용한 도구도 많은것 같

🔗 <https://kodol.tistory.com/18>



#### 데이터 집계, 변환, 저장

오픈소스 서버의 데이터 처리 파이프라인인 Logstash는 다양한 소스에서 동시에 데이터를 수집하여 변환한 후 자주 사용하는 저장소로 전송합니다. (여기서 말하는 저장소는 당연히 Elasticsearch입니다.)

ELK + Mysql + Redis

<https://velog.io/@yjin/ELK-스택>

<https://www.elastic.co/kr/blog/how-to-keep-elasticsearch-synchronized-with-a-relational-database-using-logstash>

<https://velog.io/@broccoliindb/mysql-데이터를-elasticsearch로-검색하기>

<https://github.com/sherifabdnaby/elastdocker/blob/main/docker-compose.yml>

Test 용 post 임시 쿼리

```
INSERT INTO salespost (salespostid, content, title, username)
VALUES (1, 'Jim sold a pencil', 'SOLD PENCIL', 'Jim Carrey');
INSERT INTO salespost (salespostid, content, title, username)
VALUES (2, 'Mike buy a board', 'BUY BOARD', 'Mike Myers');
INSERT INTO salespost (salespostid, content, title, username)
VALUES (3, 'Bryan give free tickets', 'FREE TICKETS', 'Bryan Adams');

INSERT INTO boardpost (boardpostid, content, title, username)
VALUES (4, '에어팟 프로 32만원에 팝니다', '에어팟 프로', 'Jim Carrey');
INSERT INTO boardpost (boardpostid, content, title, username)
VALUES (5, '갤럭시 탭 프로 29만원에 팝니다', '갤럭시탭', 'Mike Myers');
INSERT INTO boardpost (boardpostid, content, title, username)
VALUES (6, '택자 무료나눔합니다', '택자 무료나눔', 'Bryan Adams');

ALTER DATABASE btree_project CHARACTER SET = utf8mb4 COLLATE = utf8mb4_unicode_ci;
ALTER TABLE salespost CONVERT TO CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;
alter table 테이블명 modify 컬럼명 varchar(사이즈);
```

당근마켓 Crawling

Search Server