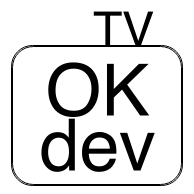
<https://okdevtv.com/mib/elk/elk5>

**[[](https://okdevtv.com/)OKdevTV](https://okdevtv.com/)**

**ELK**

* Elasticsearch + Logstash + Kibana
* Elasticsearch는 Apache의 Lucene을 바탕으로 개발한 실시간 분산 검색 엔진이며,
* Logstash는 각종 로그를 가져와 JSON형태로 만들어 Elasticsearch로 전송하고,
* Kibana는 Elasticsearch에 저장된 Data를 사용자에게 Dashboard 형태로 보여주는 솔루션이다. 
* <http://elastic.co> 사이트 오픈소스 제품

**장점**

* Google Analytics(GA)의 데이터로 사이트 접속 통계를 구할 경우 원하는 대로 데이터를 획득하기 어렵다.
* 자체 서버의 모든 로그를 100% 수집할 수 있기 때문에 데이터에 대한 신뢰성이 높다.
* 파라미터 값별로 통계를 볼 수 있기 때문에 정확한 데이터 분석이 가능하다.
* 검색엔진(lucene)이 포함되어 있어, 빠르게 데이터를 검색할 수 있다.
* 모두 오픈소스이며 자유롭게 사용이 가능하다.

**사전 준비**

* 로그수집 서버(AWS 추천)
  + aws 접속 key가 있는 경우
  + 윈도우에서 git bash 추천(<http://git-scm.com>). putty 접속보다 쉬움
* 리눅스 서버 CentOS 또는 Ubuntu
* Java 1.8 이상

**nginx 설치(샘플용)**

* [nginx 설치](http://okdevtv.com/mib/nginx/nginx)

**jdk 1.8**

sudo yum remove java-1.7.0-openjdk.x86\_64 -y

sudo yum install java-1.8.0-openjdk-devel.x86\_64 -y

[install](https://okdevtv.com/mib/java)

**system env**

sudo vi /etc/security/limits.conf

ec2-user hard nofile 65536

ec2-user soft nofile 65536

ec2-user hard nproc 65536

ec2-user soft nproc 65536

sudo vi /etc/rc.local

echo 1048575 > /proc/sys/vm/max\_map\_count

sudo sysctl -w fs.file-max=65536

cat /proc/sys/fs/file-max

sudo reboot 0

**AWS 포트 설정**

* EC2 Security Groups
* 외부 접근 포트 추가(inbound)
  + http(80)
  + elasticsearch(9200)
  + kibana(5601)

**설치**

* Elasticsearch
* Kibana
* Logstash (FluentD로 대치 가능)
* 버전을 맞춰서 작업하는 것이 좋지만, 최신 버전으로 작업해도 동작함(2016/04/03 현재)
* Elasticsearch와 Kibana는 권장 버전을 맞춰야 함
* 설치 위치 /opt/ 또는 ~/local/ 권장

**Elasticsearch 설치**

mkdir ~/local

cd ~/local

wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-5.1.1.tar.gz

tar xvfz elasticsearch-5.1.1.tar.gz

ln -s elasticsearch-5.1.1 elasticsearch

cd elasticsearch

vi config/elasticsearch.yml

# `# network.host: 192.168.0.1`의 주석을 풀고 `network.host: 0.0.0.0`으로 변경

# 모든 IP에서 접근 가능

bin/elasticsearch -d

# 데몬(백그라운드)로 실행. 옵션 -d를 빼면 터미널 접속해 있는 동안만 실행

* 실행 확인
* curl -i http://localhost:9200/

**Kibana 설치**

cd ~/local

wget https://artifacts.elastic.co/downloads/kibana/kibana-5.1.1-linux-x86\_64.tar.gz

tar xvfz kibana-5.1.1-linux-x86\_64.tar.gz

ln -s kibana-5.1.1-linux-x86\_64 kibana

cd kibana

* copy ip address, private ip needed
* ifconfig | grep inet
* inet addr:172.31.10.233 Bcast:172.31.15.255 Mask:255.255.240.0

vi config/kibana.yml

#server.host: "localhost"

server.host: "172.31.10.233"

bin/kibana

# background run

nohup bin/kibana &

* 실행 확인 http://아이피:5601

**Logstash 설치**

cd ~/local

wget https://artifacts.elastic.co/downloads/logstash/logstash-5.1.1.tar.gz

tar xvfz logstash-5.1.1.tar.gz

ln -s logstash-5.1.1 logstash

cd logstash

* conf 파일 생성

mkdir logconf

vi logconf/nginx.conf

logconf/nginx.conf

input {

file {

path => "/var/log/nginx/access.log"

start\_position => beginning

}

}

filter {

grok {

match => { "message" => "%{COMBINEDAPACHELOG}"}

}

geoip {

source => "clientip"

}

}

output {

elasticsearch {}

stdout {}

}

* logstash 실행
* # test
* bin/logstash -f logconf/nginx.conf -t
* # run
* bin/logstash -f logconf/nginx.conf
* # background run
* nohup bin/logstash -f logconf/nginx.conf &

**Kibana 통계**

**시각화(Visualize)**

* Terms(request.raw, clientip.raw, ...) 또는 Filters(request: "/hello.html", ...) 이용해서 차트 생성
* 테이블, 라인차트, 파이차트, 지도 등 가능
* 만들어진 차트는 저장 가능

**대시보드 만들기**

* 저장된 차트를 한 화면에서 볼 수 있도록 추가, 레이아웃 가능

**part 2**

**Logstash**

* 필드 추가
* field{
* mutate {
* add\_field => {
* "reqs" => "%{request}"
* }
* }
* }
* 분리
* field{
* mutate {
* split => ["reqs", "?"]
* add\_field => { "uri" => "%{reqs[0]}" }
* add\_field => { "req\_uri" => "%{reqs[0]}" }
* # add\_field => { "querystring" => "%{reqs[1]}" }
* }
* }
* 필드 제거
* mutate {
* remove\_field => [
* "reqs",
* "uri"
* ]
* }
* 파라미터 필드 만들기
* filter {
* mutate {
* add\_field => {
* "tmp" => "%{request}"
* }
* }
* if [tmp] =~ "\?" {
* mutate {
* split => [
* "tmp", "?"
* ]
* add\_field => {
* "params" => "%{[tmp][1]}"
* }
* }
* kv {
* field\_split => "&"
* source => "params"
* include\_keys => [ "category", "utm\_source" ]
* prefix => "param\_"
* }
* }
* }
* 또는

# params

if [request] =~ "\?" {

kv {

field\_split => "&"

source => "querystring"

include\_keys => [ "query", "redirectUrl" ]

prefix => "param\_"

}

}

* 이미지 제거
* filter {
* if [message] =~ "^#|\.(css|js|ico|png|xml|jpg|JPG|gif|jpeg|eot\?) " {
* drop {}
* }
* }
* useragent 파싱
* useragent {
* source => "agent"
* }
* timestamp 조정(apache log)
* date {
* match => [ "timestamp", "dd/MMM/yyyy:HH:mm:ss Z" ]
* }
* <https://www.elastic.co/guide/en/logstash/current/plugins-filters-date.html>
* urldecode
* urldecode {
* field => "params"
* }
* to integer
* mutate {
* convert => [ "bytes", "integer" ]
* }

**Kibana**

* 질의어 문법(query syntax)
  + Lucene 검색 엔진의 문법 그대로 사용(<https://lucene.apache.org/core/2_9_4/queryparsersyntax.html>)
* request: "uri"
* 제외 -device : "Spider"

**elasticsearch**

* 데이터 지우기
  + curl -XDELETE http://localhost:9200/logstash\*

**Filebeat with logstash**

* (Optional)
* logstash forwarder(deprecated) 의 경량(lightweight) 버전
* logstash plugin 설치
* cd ~/local/logstash
* ./bin/logstash-plugin install logstash-input-beats
* filebeat 설치

cd ~/local

wget https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-5.1.1-linux-x86\_64.tar.gz

tar xvfz filebeat-5.1.1-linux-x86\_64.tar.gz

ln -s filebeat-5.1.1-linux-x86\_64 filebeat

cd filebeat

# elasticsearch 부분 #으로 주석 처리

# elasticsearch:

#hosts: ["localhost:9200"]

# logstash 부분 # 주석 해제

logstash:

hosts: ["localhost:5044"]

# filebeat.yml 내용 중 로그 위치 변경 `/var/log/nginx/\*.log`

* logconf/nginx.conf 파일 변경

input {

beats {

port => 5044

}

}

filter {

grok {

match => [

"message", "%{COMBINEDAPACHELOG}",

"message", "%{COMMONAPACHELOG}"

]

}

geoip {

source => "clientip"

}

}

output {

elasticsearch {

hosts => "localhost:9200"

manage\_template => false

index => "%{[@metadata][beat]}-%{+YYYY.MM.dd}"

document\_type => "%{[@metadata][type]}"

}

}

./filebeat -e -c filebeat.yml

* start shell

echo "nohup ./filebeat -e -c filebeat.yml &" > start.sh

chmod +x start.sh

./start.sh

**ELK with PM2**

* 2G짜리 메모리의 인스턴스에서 ELK를 돌리면 OutOfMemory 때문에 종종 Elasticsearch 또는 Kibana가 죽습니다.
* 고육지책으로 Kibana는 node 기반이기 때문에 pm2로 Kibana가 죽으면 자동으로 살리는 방법입니다.
* download from <http://nodejs.org> and install node.js
* npm install -g pm2
* cd ~/local/kibana
* pm2 start bin/cli
* check kibana status with pm2 list
* pm2 logs path is placed in ~/.pm2/logs

**kibana 인증 with nginx**

sudo vi /etc/nginx/nginx.conf

* server\_name: 아래 kibana 프록시 설정
* auth\_basic "Restricted Access";
* auth\_basic\_user\_file /etc/nginx/htpasswd.users;
* location / {
* proxy\_pass http://localhost:5601;
* proxy\_http\_version 1.1;
* proxy\_set\_header Upgrade $http\_upgrade;
* proxy\_set\_header Connection 'upgrade';
* proxy\_set\_header Host $host;
* proxy\_cache\_bypass $http\_upgrade;
* }
* nginx 재시작
  + sudo service nginx restart
* 5601 포트는 막고 80으로만 접속

**참고**

* Logstash grok patterns
  + <https://github.com/logstash-plugins/logstash-patterns-core/blob/master/patterns/grok-patterns>
* ELKR (ElasticSearch + Logstash + Kibana + Redis) 를 이용한 로그분석 환경 구축하기
  + <http://brantiffy.axisj.com/archives/418>
* 2016 ELK 스택으로 서울시 지하철 대시보드 만들기 *추천*
  + <https://youtu.be/xPjNtd8xUZo>
* EMOCON 2015 F/W ELK 스택을 사용한 서울시 지하철 대시보드 만들기
  + <https://youtu.be/ec-XzM6_CgU>
* ELK 구축하기 1 – LOGSTASH
  + [http://linux.systemv.pe.kr/elk-구축하기-1-logstash/](http://linux.systemv.pe.kr/elk-%EA%B5%AC%EC%B6%95%ED%95%98%EA%B8%B0-1-logstash/)
* [Ubuntu] ELK 설치 및 테스트 하기
  + <http://digndig.kr/ubuntu/449/>
* Splunk 대체 Solution으로서의 ELK Stack
  + <http://blog.embian.com/18>
* How To Install Elasticsearch, Logstash, and Kibana 4 on Ubuntu 14.04
  + <https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-4-on-ubuntu-14-04>
* ELK 프로그래밍 방송 영상
  + <http://bit.ly/okdevtv-elk>
* Logstash Configuration
  + <https://www.elastic.co/guide/en/logstash/current/event-dependent-configuration.html>
* Elasticsearch(Lucene) Query Syntax
  + <https://lucene.apache.org/core/2_9_4/queryparsersyntax.html>
* ELK Kibana 사용법
  + <https://dl.dropboxusercontent.com/u/2385737/Kibana-basic.pdf>
* okky.conf
  + <https://okdevtv.com/md/elk/okky.conf>

[What Else?](https://okdevtv.com/md/list.html)