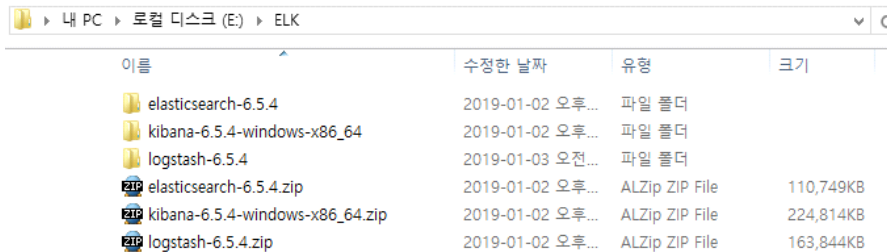


# Window8 ELK 환경구축

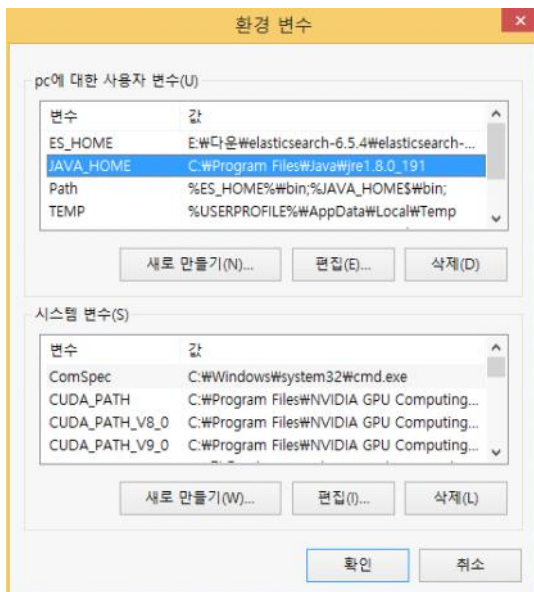
구분	버전	설치링크
Elasticsearch	6.5.4	<a href="https://www.elastic.co/downloads/elasticsearch">https://www.elastic.co/downloads/elasticsearch</a>
Logstash	6.5.4	<a href="https://www.elastic.co/downloads/logstash">https://www.elastic.co/downloads/logstash</a>
Kibana	6.5.4	<a href="https://www.elastic.co/downloads/kibana">https://www.elastic.co/downloads/kibana</a>
Jdk	jdk1.8.0_191 (11버전에서 오류발생)	<a href="https://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html">https://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html</a>



이름	수정된 날짜	유형	크기
elasticsearch-6.5.4	2019-01-02 오후...	파일 폴더	
kibana-6.5.4-windows-x86_64	2019-01-02 오후...	파일 폴더	
logstash-6.5.4	2019-01-03 오전...	파일 폴더	
elasticsearch-6.5.4.zip	2019-01-02 오후...	ALZip ZIP File	110,749KB
kibana-6.5.4-windows-x86_64.zip	2019-01-02 오후...	ALZip ZIP File	224,814KB
logstash-6.5.4.zip	2019-01-02 오후...	ALZip ZIP File	163,844KB

## 0. Java jdk

윈8 기준 : [내컴퓨터 우클릭 속성] -> [고급시스템설정] -> [환경변수] -> 환경변수 설정



JAVA\_HOME : C:\Program Files\Java\jre1.8.0\_191

```
C:\Users\pc>echo %JAVA_HOME%  
C:\Program Files\Java\jre1.8.0_191
```

[cmd에서 환경변수 잡히는지 확인해보자]

## 1. Elasticsearch

설치한 압축파일을 풀고 cmd (관리자권한실행) 후 아래의 경로(bin)에서 elasticsearch.bat 으로 실행

```
관리자: 명령 프롬프트 - elasticsearch.bat
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>e:

E:\>cd E:\ELK\elasticsearch-6.5.4\elasticsearch-6.5.4\bin

E:\ELK\elasticsearch-6.5.4\elasticsearch-6.5.4\bin>elasticsearch.bat
```

<http://127.0.0.1:9200/> 웹브라우저로 작동여부 확인

```
← → ↻ ⓘ 127.0.0.1:9200

{
  "name" : "SoJFBq0",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "_X5E-vW5Q42lfObdw4DQrQ",
  "version" : {
    "number" : "6.5.4",
    "build_flavor" : "default",
    "build_type" : "zip",
    "build_hash" : "d2ef93d",
    "build_date" : "2018-12-17T21:17:40.758843Z",
    "build_snapshot" : false,
    "lucene_version" : "7.5.0",
    "minimum_wire_compatibility_version" : "5.6.0",
    "minimum_index_compatibility_version" : "5.0.0"
  },
  "tagline" : "You Know, for Search"
}
```

## 2. Logstash

원하는 폴더에 압축을 푼다. (단, 경로에 공백이 포함되지 않는 위치에 .. + 한글 경로 없는 곳으로)

ex) "C:\Program Files" --> 공백 포함이라 안됨.

#실행 전 Beats input plugin을 최신으로 업데이트 하자.

- 해당 경로(bin)에서 logstash-plugin update logstash-input-beats

#logstash.conf 파일을 생성해서 bin 디렉토리에 넣어주자.

[logstash.conf]

```
# [Beats input plugin]
# listen on port 5044 for incoming Beats connections
input {
  beats {
    port => 5044
  }
}

# The filter part of this file is commented out to indicate that it is
# optional.
# filter {
#
```

```
# }

# [Elasticsearch output plugin]
# index into Elasticsearch
output {
  elasticsearch {
    hosts => "localhost:9200"
    manage_template => false
    index => "%[@metadata][beat]-%[@metadata][version]-%{+YYYY.MM.dd}"
  }
}
```

#실행해보자. (관리자 권한으로 실행하자) + elasticsearch 커뤄야함.

> logstash.bat -f logstash.conf

```
관리자: 명령 프롬프트 - logstash.bat -f logstash.conf
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>

E:\>cd E:\ELK\logstash-6.5.4\logstash-6.5.4\bin

E:\ELK\logstash-6.5.4\logstash-6.5.4\bin>logstash-plugin update logstash-input-beats
Updating logstash-input-beats
Updated logstash-input-beats 5.1.6 to 5.1.8

E:\ELK\logstash-6.5.4\logstash-6.5.4\bin>logstash.bat -f logstash.conf
```

### 3. Kibana

압축 풀고 cmd에서 실행하면 된다. (관리자 권한으로 실행하자)

```
관리자: 명령 프롬프트 - kibana.bat
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>

E:\>cd E:\ELK\kibana-6.5.4-windows-x86_64\kibana-6.5.4-windows-x86_64\bin

E:\ELK\kibana-6.5.4-windows-x86_64\kibana-6.5.4-windows-x86_64\bin>kibana.bat
log [19:51:56.912] [info][status][plugin:kibana@6.5.4] Status changed from uninitialized to green - Ready
log [19:51:57.049] [info][status][plugin:elasticsearch@6.5.4] Status changed from uninitialized to yellow - Waiting for Elasticsearch
log [19:51:57.052] [info][status][plugin:xpack_main@6.5.4] Status changed from uninitialized to yellow - Waiting for Elasticsearch
log [19:51:57.058] [info][status][plugin:searchprofiler@6.5.4] Status changed from uninitialized to yellow - Waiting for Elasticsearch
log [19:51:57.062] [info][status][plugin:ml@6.5.4] Status changed from uninitialized to yellow - Waiting for Elasticsearch
log [19:51:57.099] [info][status][plugin:tilemap@6.5.4] Status changed from uninitialized to yellow - Waiting for Elasticsearch
log [19:51:57.102] [info][status][plugin:watcher@6.5.4] Status changed from uninitialized to yellow - Waiting for Elasticsearch
log [19:51:57.112] [info][status][plugin:license_management@6.5.4] Status changed from uninitialized to green - Ready
log [19:51:57.114] [info][status][plugin:index_management@6.5.4] Status changed from uninitialized to green - Ready
```

<http://127.0.0.1:5601/> 키바나가 구동하는지 확인해보자.

