1. 서문

ELK Stack → Elastic Stack

Elasticsearch

- Apache 2.0 라이센스로 배포. JAVA로 만들었다.
- 실시간 분석
- 전문 (full text) 검색 : 역파일 색인
- 사용자 관점에서는 JSON 형식의 데이터 전달
- REST API ⇒ http 프로토콜 이용해 어떤 클라이언트라도 연동 O
- 멀티테넌시

Logstash

- 데이터 수집·저장
- 출력 API로 Elastic search 지원
- Elasticsearch의 입력수단
- JRuby : 루비 코드 개발 → 자바 런타임 머신 위에서 돌아감.
- Apache 2.0 라이센스
- 입력 (inputs) → 필터 (filters) → 출력 (outputs)

Kibana

- 시각화 도구
  : Discover, Visualize, Dashboard
  검색 통계 → 화면 만들고 저장·불러오기

Beats

- 파일 내용 수집
- 다른 프로세스 실시간 모니터링

2. 시작하기

elasticsearch download → unzip → bin 디렉토리 하위 elasticsearch.bat

kibana download → unzip → bin 디렉토리 하위 kibana.bat