분산 시스템 대용량 데이터 수집기술 연구

이동혁*, 정남준*, 김동욱*, 홍수빈*
한국전력공사 전력연구원*

A Study on Distributed System Large-capacity Data Collection Technology

Dong-Hyuk Lee*, Nam-Joon Jung*, Dong-Wook Kim*, Su-Bin Hong*
KEPCO Research Institute*

Abstract - IT서비스의 보편화에 따라 기업의 정보시스템 규모는 대형화되고 있으며, 시스템 운영에 필요한 솔루션의 다양성이 강화되고 있다. 단일 독립형 서버 형태에서 여러 도메인 분야의 서비스 처리를 위한 다수의 시스템으로 구성되는 분산형 구조로 발전하면서 가용성과 성능 관리 측면에서의 복잡성이 심화되고 있다. 이러한 분산환경 시스템에서의 성능 저하와 장애 발생은 조직의 최적운영과 고객 신뢰도 저하를 촉발하게 되는 요인이다. 기업에서는 시스템의 이상 현상을 적기에 발견하고 원인분석 및 조치 하기 위해 비즈니스 서비스 처리 과정인 워크플로우(Workflow)에 포함된 모든 SW솔루션과 HW에서 생성된 비즈니스 처리 정보(이벤트, 로그)들을 수집하여 대응방안을 수립할 필요성이 있다. 본 논문에서는 이러한 분산 시스템의 특징과 기업의 사례를 통해 대용량 데이터 수집 기술의 특징을 분석하고 대표적인 기술인 ELK(ElasticSearch, Logstash, Kibana) Stack을 활용하여 대용량 데이터 수집 시스템을 설계하는 방안을 제시하고자 한다.

1. 서 론

최근 디지털 환경의 급속한 성장과 함께 기업의 정보시스템 규모는 단일 독립형 서버에서 분산형 또는 클라우드 환경으로 통합운영 되고 있는 추세이다. IT 시장 조사 기관인 가트너에 따르면 2019년 전 세계 분산 클라우드 시장규모는 2,143억 달러이고, 2022년에는 3,312억 달러에 이를 것이라고 한다. 또한, 기업의 3분의 1 이상의 기업들이 클라우드 도입 및 구축에 대한 투자를 우선순위로 두고 있어 2022년까지 클라우드 서비스에 대한 성장 규모는 전체 IT서비스 성장세의 3배에 달할 것으로 예상하였다[1]. 그러나 다수의 HW와 SW의 구성된 분산 시스템은 복잡성 심화를 야기 할 수 있고 자칫 성능 저하 및 장애로 이어져 기업시장가치에 상당한 악영향을 미칠 수 있다[2]. 기업은 이러한 문제를 사전에 발견하고 예방하기 위해서 분산 업무 시스템에서의 자신들의 업무환경에 맞는 대용량 데이터 수집 기술을 확보할 필요성이 있다.

2. 본 론

2.1 분산 시스템

2.1.1 분산 시스템의 특징

분산 시스템은 독립적인 여러 대의 컴퓨터가 모여있고, 사용자 입장에서는 그 컴퓨터 집합이 하나처럼 인식되는 특징이 있다. 이는 중앙 집중형 시스템과는 달리 다수의 컴퓨터가 동일한 테스크를 분산 처리하기 위해 네트워크상에서 서로 통신하며 협력한다는 것이다. 중앙 집중형 시스템의 장애 지점과 병목 현상을 제거하여 시스템의 안전성 및 성능을 개선할 수 있고 개별 노드의 용량을 늘려 수평/수직적으로 손쉽게 확장할 수 있어 광범위한 부하를 처리할 수 있는 장점이 있다[3]. 하지만 작업 노드의 분산과 광범위한 확장성은 업무 시스템의 복잡성을 심화하여 시스템의 모니터링 및 유지관리가 어려워지는 문제를 초래하기도 한다.

2.1.2 분산 시스템 기업 사례

<표 1>은 전력 산업 분야 어느 한 기업의 영업 및 판매 서비스를 제공하는 시스템의 운영서버 현황이다. 해당 시스템은 검침·요금·수금·고객센터·계통 운영 등의 업무를 관리하기 위하여 구축된 정보 시스템으로, 사용자는 2.7만 명 연계 시스템만 49개에 이른다. 2021년 12월 기준으로 9개 지역본부에서 운영 중이며 1일 약 4천만건의 트랜잭션이 처리되고 있다. 향후 나머지 지역본부까지 확대 시 2배 이상의 데이터가 증가할 것으로 예상된다. 1일 동안의 서버별 트랜잭션 수를 분석해본 결과 WAS(54.9%), Web GIS(19.4%), BPM(17.3%), ESB(8.4%) 순으로 처리되었으며 해당 시스템의 초당 트랜잭션 수는 926 TPS를 처리하는 수준으로 확인되었다.

구 분	용 도	수량
내/외부 모바일 WEB	사용자 업무 접근 환경	7
통합 WAS	온라인 업무 처리	3
배치 Job	EM, Master, Agent, Cosort	15
솔루션	BPMS, BRMS, ETL, 파일관리, Push	11
운영 DB	BPMS(솔루션), 개인정보, 영업 및 배전	12
내/외부 연계	내부/외부 시스템 연계 지원(ESB, Proxy)	10
GIS	Web GIS, EG, Magik중계, Exa-Data	11
모니터링, 백업마스터	시스템 모니터링, 백업 마스터	7
합 계		76

<표 1> 분산 시스템 운영서버 사례

2.2 주요 분산 시스템 데이터 수집기술 특징

2.2.1 Apache Flume(아파치 플럼)

Apache Flume은 대량의 로그 데이터를 수집하여 효율적으로 읽어 들이기 위한 분산 프레임워크이다. 아키텍처는 데이터 소스의 데이터를 다른 저장소로 스트리밍하기 위한 심플한 구조를 가지고 있다. Apache Flume은 데이터 플로우 사이사이에 실패하는 상황에 대해 빠르게 복구하는 복구성에 중점을 두고 있어 대량의 로그 파일을 이동시키는 데 적합하고 유용하다.

2.2.2 Flunetd(플루언트디)

Fluentd는 로그 데이터 수집기로서, 특정 서버에 쌓이고 있는 로그 파일의 경로를 지정하여 로그를 수집할 수 있으며, HTTP, TCP 등의 통신을 하여 Fluentd로 직접 데이터를 전송하는 방식으로도 수집이 가능하다. Fluentd로 전달된 데이터는 Tag, Time, Record(JSON) 형태로 구성된 이벤트로 처리되며 원하는 형태로 다양한 목적지로 전달할 수 있다. Fluentd는 C와 Ruby로 개발되어 일반적으로 더 적은 리소스를 사용하며 데이터 유실을 막기 위해 메모리와 파일 기반의 버퍼(Buffer) 시스템을 가지고 있어 강력한 오류대응 기능을 가지고 있다.

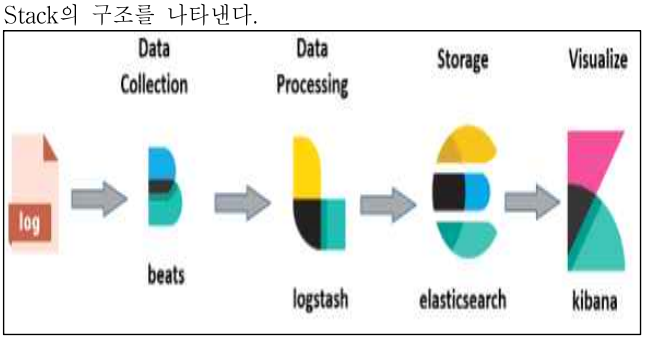
2.2.3 Logstash(로그스태시)

Logstash는 다양한 종류의 로그 데이터를 입출력 및 가공 처리할 수 있는 플러그인 중 하나이다. 서버측 데이터 처리 파이프라인으로서 다양한 소스에서 동시에 데이터를 수집하여 변환한 후 자주 사용하는 저장소로 보낸다. 데이터가 소스에서 저장소로 이동함에 따라 Logstash 필터는 각 이벤트의 구문을 분석하고 명명된 필드를 식별하여 구조를 구성하고, 이를 공통 형식으로 변환 통합하여 분석 시간을 단축할 수 있게 한다.

2.3 ELK를 이용한 분산데이터 수집시스템 설계

2.3.1 ELK Stack 구조 및 구성 요소

ELK Stack은 2.2.3장에서 설명한 로그 수집 파이프라인인 Logstash와 로그 수집 모듈인 Beats, 저장 및 검색 기능을 지원하는 Elasticsearch, 데이터를 시각화하는 Kibana로 구성되어 있는 오픈소스 기반의 데이터 분석 플랫폼이다. <그림 1>은 ELK Stack의 구조를 나타낸다.



<그림 1> ELK Stack 구조

이러한 각 구성요소는 분석에 필요한 모든 유형의 로그에 대해 일련의 작업을 수행하며 다음과 같은 특징이 있다. Beats는 데이터 수집대상인 각 서버에 에이전트 형식으로 설치되는 경량 데이터 수집기이다. 사용하고자 하는 목적에 따라서 개발된 다양한 비트가 존재하며 Logstash와 ElasticSearch에 연계해 광범위한 이벤트 수집이 가능하다. 이렇게 수집된 데이터는 데이터 처리 파이프라인인 Logstash에서 인덱싱 처리와 같은 전처리 과정을 거쳐 지정된 서버에 전송한다. 수신된 데이터는 Apache Lucene 기반의 실시간 분석 검색 엔진인 ElasticSearch에 저장된다. 이 엔진은 정형, 비정형, 위치정보, 메트릭 등 다양한 유형의 실시간 검색을 지원하고 멀티테넌시 기반의 클러스터로 구성할 수 있기 때문에 확장성과 병렬처리가 용이한 장점이 있다[4].

2.3.2 로그 데이터 확보 방안

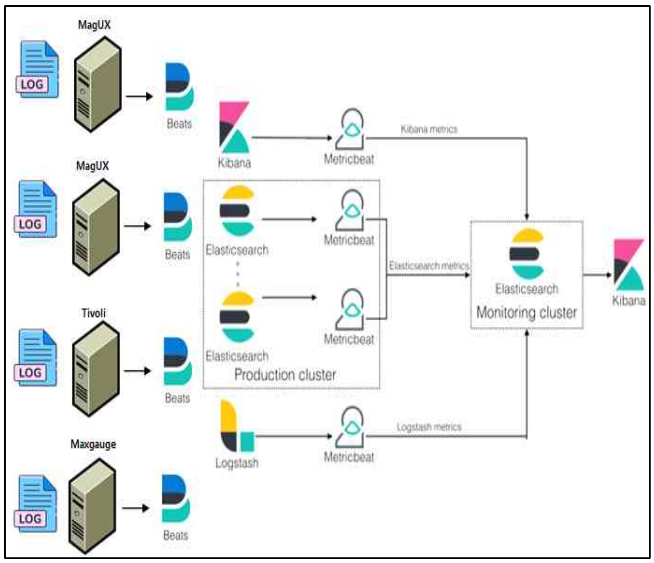
앞서 사례로 설명한 업무 시스템에서의 데이터 수집 대상은 APM(Application Performance Monitoring) 솔루션이 설치된 서버를 기반으로 수집하기로 한다. 광범위한 모든 서버에 데이터 수집기인 Beats 에이전트를 설치하는 것이 아닌 업무 시스템의 성능저하와 장애탐지를 할 수 있는 관제 솔루션이 설치된 서버를 대상으로 한다. <표 2>는 수집 대상으로 선정한 APM 솔루션과 해당 솔루션이 수집하는 주요 데이터 현황이다.

구 분	주요 데이터
Intermax	트랜잭션별 소요 시간, 수행 시작/종료 시간, 예외(에러) 내역, 클라이언트 IP 등
MagUX	클라이언트/서버 구간 Round Trip Time, 패킷 전송 완료 소요시간, 응답 지연시간 등
Tivoli	CPU 사용률, 실행 및 실행대기 프로세스 수, 시스템 호출 개수, 사용 가능한 메모리양 등
Maxgauge	수행 쿼리문, 쿼리 수행 시간 및 수행 횟수, 장애 발생 시점 및 내역 등

<표 2> 수집대상 APM솔루션 및 주요 데이터 현황

본 연구에서 수집대상으로 선정한 APM솔루션은 총 4종으로, 트랜잭션 모니터링 솔루션인 Intermax, 네트워크 구간 모니터링 솔루션 Mag-UX, 서버의 CPU, Memory 지표를 활용하여 부하 및 성능지표를 수집하는 Tivoli, DB성능관리 솔루션인 Maxgague가 설치된 서버를 대상으로 로그 데이터를 수집한다.

2.3.3 분산 데이터 로그 데이터 수집 시스템 설계



<그림 2> ELK 기반 데이터 수집 시스템 구성도

수집대상으로 선정된 APM 솔루션이 설치되어 있는 서버 4종을 대상으로 로그 데이터를 수집하기 위한 Beats를 설치하였다. 수집간 서버별 자원 사용량을 확인하기 위해 Metricbeat를 연결한 후 모니터링 클러스터를 구성하여 스택 자원의 활용도를 체크할 수 있도록 설계하였다. 수집된 데이터의 일괄 처리를 위해 Logstash 서버는 하나만을 운영하여 두 개의 분산 노드를 가지는 Elasticsearch에 분산 저장하도록 한다. 노드의 실패 상황에서도 안정적인 동작을 지원하기 위해 노드 구성은 분산 저장을 위한 마스터 노드와 데이터 노드로 이중 구성하였으며 마스터 노드 인덱스의 주 샤드에 이어 복제 샤드를 구성하여 저장하도록 한다. 한 개의 노드에 장애가 발생하더라도 다른 노드에서 데이터 접근이 가능하므로 수집된 데이터의 유실을 방지하고 시스템의 안정성을 높일 수 있다. 이러한 구성은 저 사양의 Logstash(CPU Core 12 ,RAM 8GB) 환경에서 초당 약 2만 TPS의 처리량을 지원하며 이는 앞서 사례로 설명한 업무시스템의 초당 트랜잭션인 926 TPS를 훨씬 능가하는 것을 확인 할 수 있다.

3. 결 론

본 연구에서는 분산 시스템의 특징과 전력 산업 분야의 업무 시스템 사례를 기반으로 ELK Stack을 적용하여 수집 시스템을 설계하는 방안에 대해 연구해 보았다. 본 연구를 기반으로 향후 ELK Stack의 구성요소별 자원 사용량을 분석하여 최대 부하량 및 초당 처리량 등의 성능시험을 진행하여 최적의 데이터 수집 및 처리를 위한 아키텍처를 설계하는 연구를 진행할 계획이다.

[참 고 문 헌]

[1] 백지영, “www.m.ddaily.co.kr/m/m_article/?no=179646”, 2019
[2] 이승재, “IT장애가 기업시장가치에 미치는 영향에 관한 연구”, 한양대학교, p32, 2008,
[3] Kev Zettler “www.atlassian.com/ko/microservice”, 2022
[4]What is the ELK Stack? “www.guru99.com/elk-stack tutoria.html”, 2022