LogMate

강찬욱, 양승원, 정주연

Overview

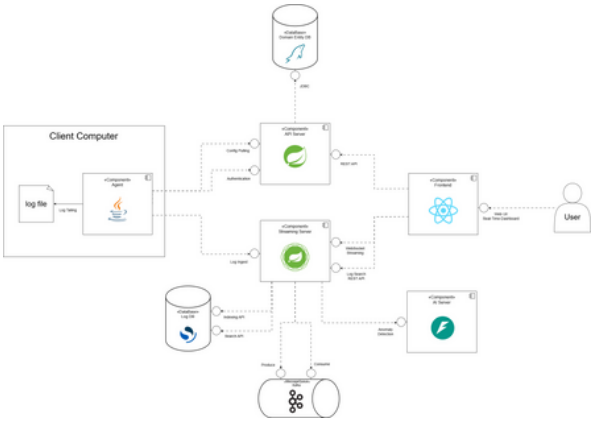
“간단하게 구성하는 로그 모니터링 & AI 분석 서비스”
현재 대부분의 로그 모니터링 솔루션은 전문적인 기술 지식이나 복잡한 인프라 설정이 필요해 초기 도입 시 높은 개발 비용과 시간적 투자가 필요하다는 단점이 존재한다. 본 프로젝트는 이러한 진입 장벽을 해소하고 기술적 배경이 부족한 사용자도 쉽게 활용 가능한 로그 수집 및 AI 기반 분석 SaaS를 제공하여 사용자의 편의성을 극대화하고자 한다.

Problem

현대적 개발 환경에서 로그 모니터링은 필수적인 DevOps 도구입니다. 하지만 실제 운영 단계에서 모니터링 시스템을 관리하고 구축하는 일은 매우 어렵다.

시스템 구축부터 비용, AI 활용까지 진입 장벽이 높고, 솔루션은 파편화되어 있어 로그 관리의 기본조차 접근하기 어렵다.

Architecture



Core Features & Outcomes

1. Zero-Config 기반 즉시 배포 및 자동 로그 수집
   - 설치 직후 별도 초기 설정 없이도 즉시 로그를 수집하고 모니터링 환경을 구성할 수 있다.
   - 다양한 운영 환경에서도 일관된 자동 초기화를 지원하여 DevOps 경험이 없는 사용자도 손쉽게 사용할 수 있다.
2. 실시간 설정 변경(Hot Reload)을 통한 무중단 파이프라인 재구성
   - Tailer, Parser, Filter 등 Agent 파이프라인 요소를 서비스 중단 없이 변경할 수 있다.
   - 변경된 설정은 즉시 반영되며, Agent는 재시작 없이 새로운 파이프라인 구성을 적용한다.
   - 운영 중에도 로그 수집 규칙을 유연하게 조정할 수 있어 장애 대응 및 테스트에 유용하다.
3. 고성능 실시간 로그 스트리밍 처리
   - WebFlux 기반 비동기 구조로 여러 사용자의 동시 스트림 요청을 안정적으로 처리한다.
   - Kafka 기반 메시지 버퍼링을 통해 네트워크 불안정 상황에서도 로그 손실 없이 안정적으로 전달한다.
   - WebSocket을 통해 사용자에게 지연 없이 실시간 로그를 스트리밍하여 즉각적인 모니터링이 가능하다.
4. 장애 복구 및 신뢰성 강화 검증
   - Kafka DLQ(Dead Letter Queue) 구조를 적용하여 예외 상황에서도 로그 유실이 없음을 확인하였다.
   - Exporter → Streaming → Dashboard 흐름에서 재전송 및 재처리가 정상 수행됨을 검증하였다.
5. 오픈소스 프로젝트화 기반 마련
   - 모듈화된 구조 덕분에 parser/filter/storage 플러그인 확장이 용이하여
   - 외부 기여자 참여가 가능한 형태로 아키텍처가 정립되었다.
   - 실제 GitHub 오픈소스 배포를 통해 지속 가능한 생태계 기반을 확보하였다.
6. AI 기반 로그 이상 탐지 (Anomaly Detection)
   - 수집된 로그를 기반으로 머신러닝 기반 이상 탐지 모델(Isolation Forest)을 적용하였다.
   - 탐지된 이상 이벤트는 별도의 점수로 표시되어 대시보드에서 우선적으로 확인할 수 있다.

https://github.com/TEAM-LOGMATE