## 주요 기능

**대시보드**

로그프레소는 위젯을 도킹 배치할 수 있는 대시보드를 제공합니다. 그리드나 차트에 쿼리를 바인딩한 위젯을 배치할 수 있으므로, 사용자가 원하는 데이터와 형태로 대시보드를 구성할 수 있습니다.

**실시간 풀텍스트 인덱싱**

로그프레소는 단일 머신에서 초당 30만건 이상 인덱싱할 수 있는 고성능 실시간 인덱싱 엔진을 탑재하고 있습니다. 일반적인 타사 솔루션과 달리 데이터 수집 즉시 인덱싱되어 풀텍스트 검색 가능한 상태가 됩니다.

**실시간 압축**

로그프레소는 실시간으로 압축 쓰기를 수행합니다. 압축 알고리즘은 선택 가능하며 압축 방식에 따라 대략 1/5에서 1/10 수준의 압축률을 보입니다. 일반적인 일 단위 압축과 달리 부분 압축 및 해제가 가능하므로, 기존에 비해 몇 배의 로그를 검색 가능한 상태로 유지할 수 있습니다.

**실시간 분석 및 경보**

실시간 로그 스트림에 대해 문맥을 이용한 복잡한 연관 분석을 수행할 수 있습니다. 분석 결과에 따라 경보를 발생시키고, 설정된 경보 처리 방식에 따라 단순 로깅을 수행하거나 메일이나 SMS를 통하여 사용자에게 경보를 전달할 수 있습니다.

**실시간 데이터 수집**

로그 파일, 데이터베이스, Syslog, SNMP Trap, 에이전트 기반의 실시간 로그 수집 기능을 내장하고 있습니다. 또한 로그프레소 REST API를 사용하여 로그를 프로그래밍 방식으로 입력할 수 있습니다.

**비정형 데이터 처리**

로그프레소는 기존의 DBMS와 달리 정형화되지 않은 임의의 로그를 받아들일 수 있습니다. 로그는 원본 그대로 유지되고, 쿼리 시간에 파싱되어 가공됩니다. PCAP 등 바이너리 포맷의 경우에도 원본 그대로 유지하고 파서를 통해 필드를 추출할 수 있습니다.

**전용 쿼리 문법**

로그프레소는 유닉스 파이프 메타포의 전용 쿼리 문법을 내장하여 SQL로 처리하기 힘들었던 정규표현식 검색, 필드 추출, 시계열 분석 등을 쉽게 수행할 수 있습니다. 원하는 쿼리 문자열을 뒤에 덧붙이는 방식으로 쉽게 쿼리 결과를 가공할 수 있습니다.

**스크립팅 엔진**

로그프레소는 로그 수집, 파싱, 인덱싱, 실시간 분석, 쿼리 전 영역에 걸쳐 스크립팅 확장을 지원합니다. 현재 파이썬 스크립트를 이용하여 런타임에 스크립트를 적재시킬 수 있으므로, 복잡한 사용자 정의 로직도 별도의 제품 커스터마이즈 없이 사용자가 직접 구현 가능합니다.

**태깅 및 필터링**

실시간으로 원본 로그에 메타데이터를 태깅하거나, 필터링을 수행합니다.

**로그 파서 설정**

테이블 데이터에 대하여 기본으로 적용할 파서를 설정. 원본 로그를 파싱하여 필드를 추출합니다.

**에이전트 연동**

센트리(에이전트)를 사용하여 원격 호스트에서 로그를 수집하거나 실시간으로 모니터링합니다.

**실시간 암호화**

수집된 원본 로그의 전송부터 파일 저장까지 평문을 노출하지 않고 실시간 암호화를 수행합니다.

**예약된 쿼리 경보**

지정된 주기마다 쿼리 실행 후 경보 조건과 일치하면 경보 메일을 전송합니다.

**계정관리**

로그프레소 계정과 테이블 접근 권한을 관리합니다.

**엑셀 연동분석**

엑셀 웹쿼리를 통해 로그프레소 쿼리 결과를 시트에 삽입하고 자동 갱신되도록 설정할 수 있습니다.

**외부시스템 연동**

하둡(HDFS)과 완벽하게 연동하여 사용할 수 있어, 하둡으로 수집한 데이터를 로그프레소를 이용해 빠른 분석이 가능합니다. 또한 각종 상용 RDBMS와 연동하여, RDBMS에 저장한 데이터를 다양하게 분석할 수 있습니다.