BigEye

차세대 빅데이터 플랫폼

BigEye

㈜넷크루즈는 빅데이터 기반 로그 및 네트워크 관리·분석 원천 기술을 동시에 보유한 국내 유일의 소프트웨어 업체로서 대용량 로그와 네트워크 패킷 수집·분석의 노하우 및 최신 기술을 적용하여 효율적인 빅데이터 관리 및 분석 환경을 제공합니다.

㈜넷크루즈의 차세대 빅데이터 플랫폼 **BigEye(빅아이)**는 로그 통합관리 구축경험을 통한 데이터 관리 노하우와 빅데이터 처리 분야의 최신 기술이 적용된 통합로그관리 솔루션입니다.
고객사의 시스템 구성 환경 및 규모에 따라 단독형, 분산형, 계층형 아키텍처를 유연하게 구성하여 안정적인 성능과 데이터 안정성을 보장하며, 저장된 데이터에 대해 손쉬운 분석을 위한 시각화 도구를 지원하여, 효율적인 데이터 관리가 가능합니다.

netcruz

차세대 빅데이터 플랫폼 기반의 통합로그

전통적인 "저장" 중심의 로그 관리 시스템에서 진화하여 **대용량 데이터를 실시간으로 활용하는 "분석"중심의 지능형 시스템**으로서 보안, 장애관리, 보안, 기획 등 다양한 분야에 Insight 를 제공하도록 지능화 된 시스템 입니다.

BigEye의 구성

빅데이터 플랫폼 기반의 유연한 확장(Scale-Out)이 가능합니다.

고객은 넷크루즈의 Built-On Component Structure를 통하여 자신의 상황과 로드맵에 맞추어 단계별로 필요한 영역의 시스템만 구성을 할 수 있으며, 필요에 따라 향후 SIEM(통합보안관제) , PIS(개인정보통합관리), NSA(네트워크 상황 인지 및 분석) 등 어떠한 형태의 Component라도 손쉽게 확장 및 통합이 가능합니다.

nML
(Machine Learning)

nSIEM
(Security Information & Event Management)

nPIS
(Personal Information Security)

nNSA
(Network Situational Awarness)

BigEye
Data 수집/저장 및 분산 처리
(정형 및 비정형 데이터, 네트워크 패킷 등)

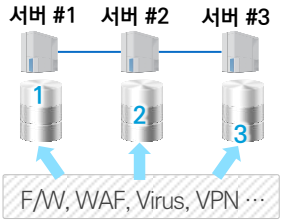
항목		사양	비고
소프트웨어	운영체제	CentOS 7.4 (64-bit)	
하드웨어	CPU	2.2GHz 10Cores * 2ea	
	메모리	128GB	
	디스크	OS : 600GB * 2ea (RAID1)	데이터 저장 공간은 일 로그량 * 보관기간에 따라 별도 산정

※ H/W 사양은 고객사 상황에 따라 변경 될 수 있음

BigEye의 주요 특징

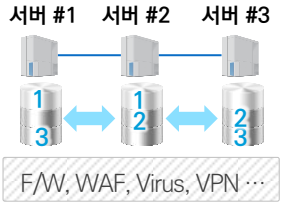
High Performance& High Availability
빅데이터 기반기술 적용

업계 최고 로그 수집 성능 40만 EPS 및
100GB 로그에 대해 1초 이내 검색결과 제공합니다.



1 분산 처리

빅데이터 분산 처리 엔진을 통한 분산 수집/저장 및 검색/분석으로 실시간 데이터 처리 및 신속한 분석



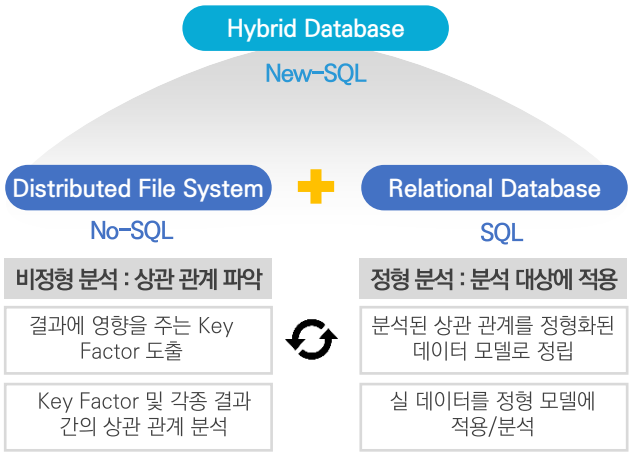
2 동기화 및 밸런싱

수집서버 별 데이터 동기화 및 밸런싱 과정을 통한 고가용성 확보

발생 로그 : 1 2 3

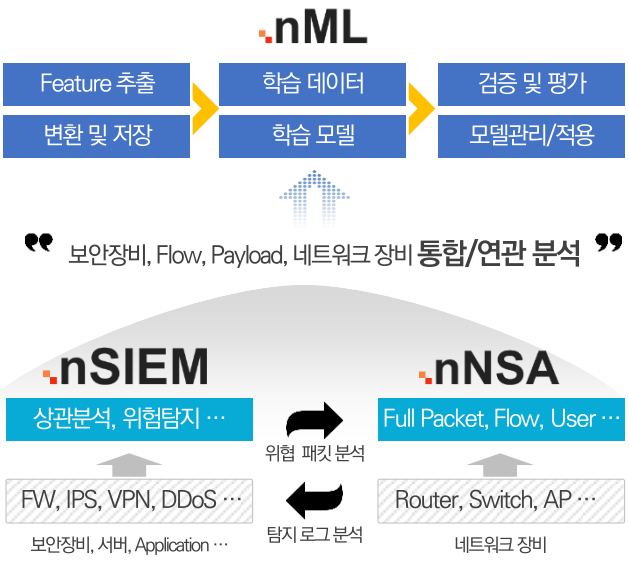
Hybrid Database
SQL과 No-SQL 모두 지원

단일 플랫폼 내에서 동일 데이터로 비정형/정형 분석을 상호 보완적으로 운영함으로써 정합성 확보하였습니다.



All Data Coverage
로그 및 네트워크 패킷 분석 지원

인프라 전반의 보안 위협에 대한 가시성 확보를 위해 로그와 네트워크 패킷 분석을 지원합니다.



Data Smart Handling
로그 파싱 및 태깅 작업 편의성 제공

샘플로그 등록 및 필드 구분 기능과 사용자 정의 필드 생성 기능으로 분석의 편의성을 제공합니다.

1 Smart Parser

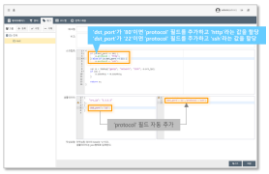
원본 로그 패턴 자동 인식 / 분할

샘플 로그만으로 필드를 구분하여 새로운 패턴의 로그 수집 시 신속하고 편리한 분석 기반 제공

미리 정의 된(Pre-defined) 정규식을 통해, 로그 데이터 자동 인지

비정형 로그 또는 이벤트 데이터를 정형화 된 데이터로 변경

2 Smart Tagging



Data Enrichment (Data → Information)

원본 로그에 대한 사용자 정의 추가 필드 생성으로 분석에 필요한 정보를 원시 로그에 간단히 자동 변환 및 추가

운영환경에 따라 최적의 성능 및 결과를 위한 태깅 기능 제공

필터를 통해 1차로 정규화 된 후, 사용자가 설정한 태깅 함수 적용 (필드 추가/삭제/변경)

BigEye의 주요 기능

구분	내용
로그수집 및 저장	실시간 원본로그 수집 및 압축저장, 암호화 등의 과정을 통해 효율적인 로그관리 환경을 제공합니다.
로그수집 현황 관리	실시간 로그 수집현황(건수, Size, EPS 등) 및 소스 별 로그 내용 확인을 위한 상황판을 제공합니다.
로그 무결성 관리	수집 로그의 무결성 훼손 여부를 실시간으로 체크하여 로그관리의 안정적인 운영을 보장합니다.
편리한 로그 검색	SQL 쿼리문법을 적용하여 유연한 검색이 가능하며, 즐겨찾기, 도움말 등의 편의기능을 제공합니다.
이벤트 관리	탐지조건, 소스유형, 임계치 등을 설정하여 이벤트 발생 룰의 관리기능을 제공합니다.
Agent 중앙관리	Agent의 관리(업데이트, Roll Back, 재시작 등)의 편의성을 위해 원격 중앙관리 기능을 제공합니다.
사용자 정의 기능	사용자 정의 보고서, 대시보드 등의 기능을 통해 고객사에 최적화된 관제환경 구성이 가능합니다.
기타 부가기능	서버 OS 취약점 진단 및 조회기능, 터미널 접속이력(로그인, 명령어 실행 등) 모니터링이 가능합니다.

기존 제품의 한계점

데이터 분산 처리 미지원	다수 서버 구성시 비효율적 활용 (1개 서버의 처리 성능에 의존)
	서버 증설시 별도의 구축 및 연동 작업 필요
데이터 동기화 및 밸런싱 미지원	별도 이중화 미 구성시 장애 발생시 시스템 사용 불가
	장애 발생시 손실 데이터 복구 불가
수집 영역의 한계	Network Packet 수집 불가 (Log 형식만 수집 가능)
	수집 대상별 버퍼 영역(MMAP)의 한계
표준 SQL 미지원	고급 데이터 검색이나 분석시 별도의 자체 쿼리 문법 학습 필요
	SQL을 지원하는 3rd Party 솔루션 연계 불가

BigEye의 주요 개선 사항

구분	기능설명	기존 제품	BigEye
구성	운영 체제	Linux	Linux
	데이터 저장소	SQL Lite	Elastic Search
	구성 정보 저장소	PostGresql	Elastic Search
	운용 방식	수집 대상별 서버 지정	수집 대상별 클러스터 지정
수집 및 저장	데이터 분산 수집 및 저장	X	○
	데이터 동기화 및 밸런싱	X	○
	수집 대상별 버퍼 용량 무제한	X	○
	Network Packet 수집 및 저장	X	○
검색 및 분석	표준 SQL 지원	X	○
	Non-SQL 지원	O	○
	Network Flow 및 Payloade 분석	X	○
	Log 및 Network Packet 연관 분석	X	○
	데이터 분산 검색 및 분석	X	○
	Clustered CEP : 실시간 메모리 분산 처리	X	○
관리 및 편의	Smart Parser : 원본 로그 패턴 자동 인식 / 분할	X	○
	Smart Tagging : 편리한 Data Enrichment (Data → Information)	X	○
	Smart Add : 단순 서버 증설만으로 분산 클러스터 환경 구성	X	○

BigEye Upgrade 기대 효과

수집 및 검색 속도 극대화
By 분산 처리

필요한 모든 데이터 수집
By Log 및 Network Packet 수집

시스템 고 가용성 확보
By 데이터 동기화 및 밸런싱

정형 및 비정형의 고급 분석 지원
By SQL 및 No-SQL 단일플랫폼 지원

netcruz (주)넷크루즈
서울특별시 구로구 디지털로 33길 12 (구로동) 우림이비즈센터 2차 1008호 TEL : 02-869-4123 FAX : 02-869-5123 www.netcruz.co.kr