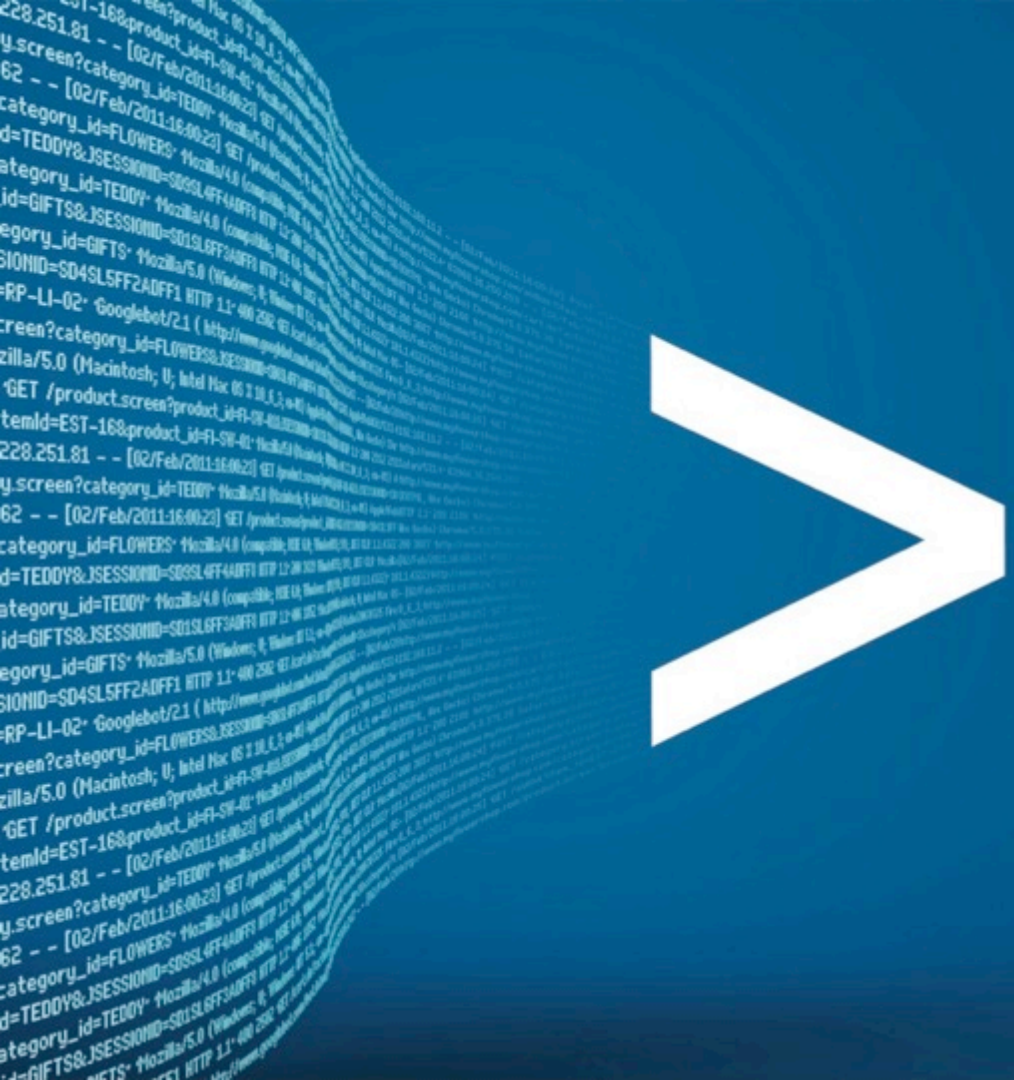


Splunk Enterprise 6.3 새로운 기능

스플렁크 코리아

2015.09.29

splunk>

스플렁크 6.3 새로운 기능

향상된
성능 및 확장성

두배 이상 향상된
성능으로 TCO 절감

향상된
분석 및 시각화

대규모 데이터셋의
분석이 더 용이

대용량
이벤트 수집기

데브옵스/사물 인터넷 규모
의 데이터 지원

엔터프라이즈급
플랫폼

엔터프라이즈급
요구사항의 수용

다양한 요구사항을 수용하도록 기능 및 성능 개선!

스플렁크 6.3 새로운 기능

향상된
성능 및 확장성

- 2x 검색 및 인덱싱 속도
- 20-50% 수용 능력 증가
- 20%+ TCO 절감

두배 이상 향상된 성능으로 TCO 절감

향상된
분석 및 시각화

대규모 데이터셋의 분석이 더 용이

대용량
이벤트 수집기

데브옵스/사물 인터넷 규모의 데이터 지원

엔터프라이즈급
플랫폼

엔터프라이즈급 요구사항의 수용

다양한 요구사항을 수용하도록 기능 및 성능 개선!

성능, 확장성, TCO의 폭발적 향상

CPU 자원을 최대로 활용하는 수직적 확장성(Vertical Scaling)

검색 성능
2x 향상된 실행 속도

인덱싱 속도
2-4x 데이터 수집 성능

지능형 작업 관리자
25%+ 작업 수용력 향상

전체 시스템 가용성
20-50% 향상

- 검색 및 보고서 실행 속도 향상
- 더 큰 데이터셋에 대한 적재 및 분석
- 최적화된 자원 활용도
- TCO 20% 이상 절감

스플렁크 엔터프라이즈 6.2와 비교한 수치이며 정확한 성능 향상율은 적용된 부하, 설정, 가용 처리 용량 등에 따라 달라질 수 있음.

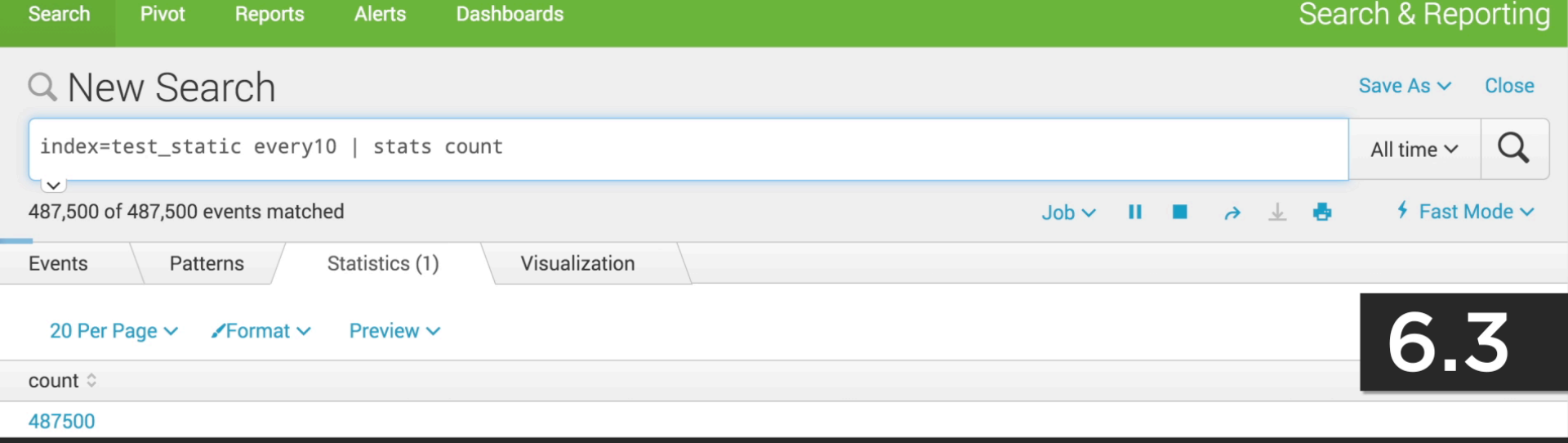
“폭발적 향상”의 의미는?

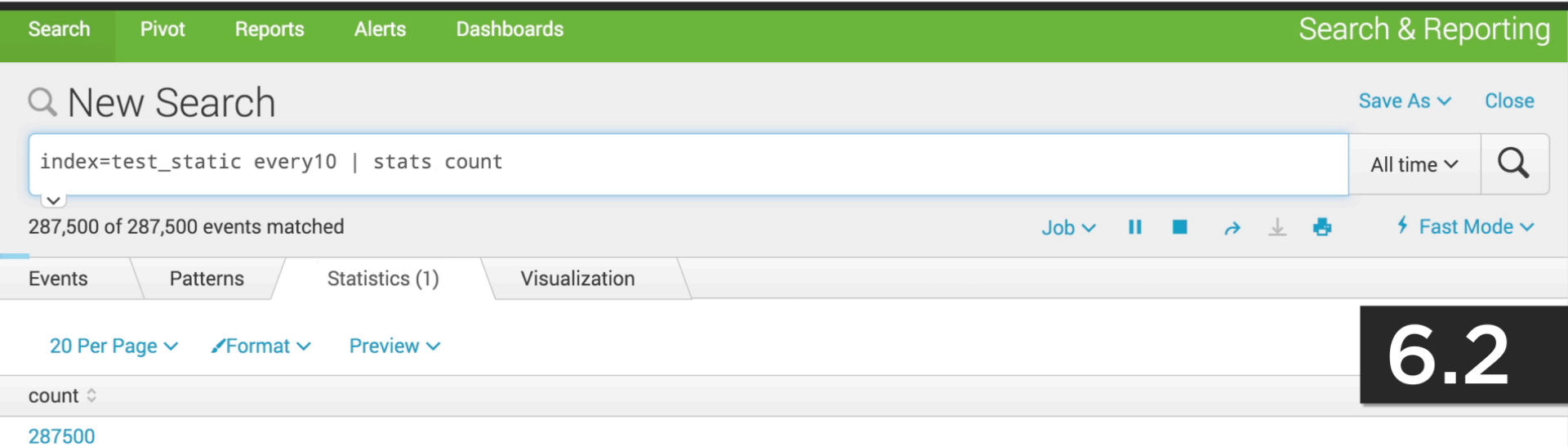
스플렁크 6.3 vs. 스플렁크 6.2

- 중요한 보고서(저장 검색)의 실행 시간이 ¼까지 단축됩니다.
- 데이터 인덱싱에 필요한 하드웨어가 20% 감소됩니다.
- 분석을 위해 데이터를 적재하는 시간이 ½까지 감소합니다.

스플렁크 6.3 vs. 스플렁크 6.0

- 2013년 대비 스프렁크 확장에 필요한 비용이 50%이상 감소합니다.
- 신규 구축시 필요한 하드웨어가 2013년 대비 1/3로 감소합니다.
- 스플렁크 구축을 위해 2013년 대비 ½의 비용으로 가능합니다.


Search
Pivot
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Close
index=test_static every10 | stats count
All time
487,500 of 487,500 events matched
Job
Fast Mode
Events
Patterns
Statistics (1)
Visualization
20 Per Page
Format
Preview
count
487500
6.3


Search
Pivot
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Close
index=test_static every10 | stats count
All time
287,500 of 287,500 events matched
Job
Fast Mode
Events
Patterns
Statistics (1)
Visualization
20 Per Page
Format
Preview
count
287500
6.2

1.1 수직적 확장성(Vertical Scaling) : 검색 및 보고서

- 하나의 검색 실행에 다수의 CPU 코어를 동원하여 더 빠른 검색 결과를 제공
- 일반적으로 “배치(batch)” 형태의 검색 또는 보고서는 통상 2배 이상 빨라짐
- 별도의 추가 시스템 없이 검색 성능을 최적화

최소 2배 이상 향상된 검색 실행 속도

1.2 수직적 확장성(Vertical Scaling) : 데이터 인덱싱

- 다수의 CPU 코어를 활용하여:
  - 데이터 적재 능력의 향상
  - 대규모 데이터의 수집(Ingest) 속도 2배 이상 향상
- 새로운 아키텍처 가이드라인 또한 기존의 250GB에서 인덱서당 하루 300GB로 증가 (범용 서버 기준)

더 적은 수의 인덱서로 더 많은 데이터 수집

1.3 수직적 확장성(Vertical Scaling) : 포워더

- 6.2에서는 데이터 수집에 4코어 이상 사용하기 위해 다수의 인스턴스를 설치하고 관리해야 했음
- 6.3에서는 하나의 스플렁크 인스턴스로 다수의 코어를 활용할 수 있음
  - 예. 16코어 시스템의 경우 기존 대비 4x 수집 성능 제공

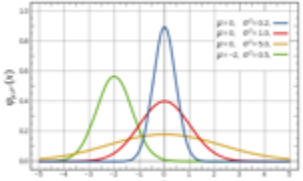
간소화된 포워더 관리

1.4 지능형 작업 관리자(Job Scheduling)

- 더 효율적이고 간소화된 스케줄링
- 작업 내역을 자동으로 분석하여 스케줄링
- 자원 상태를 최적화하여 미실행(skipped search) 최소화
- 특정 시간에 실행되어야 하는 검색의 실행 보증 지원

작업 관리자

작업 항목의 부드러운 할당



스케줄 검색 수용 능력 25% 향상

스플렁크 6.3 새로운 기능

향상된 성능 및 확장성

- 2x 검색 및 인덱싱 속도
- 20-50% 수용 능력 증가
- 20%+ TCO 절감

두배 이상 향상된 성능으로 TCO 절감

향상된 분석 및 시각화

- 이상치 검출
- 지리공간형 시각화
- 단일 값 디스플레이

대규모 데이터셋의 분석이 더 용이

대용량 이벤트 수집기

데브옵스/사물 인터넷 규모의 데이터 지원

엔터프라이즈급 플랫폼

엔터프라이즈급 요구사항의 수용

다양한 요구사항을 수용하도록 기능 및 성능 개선!

개선된 분석 및 시각화

다양한 분석 및 시각화 요소 추가

이상치 검출
(Anomaly Detection)

지리공간형 시각화
(Geospatial Visualization)

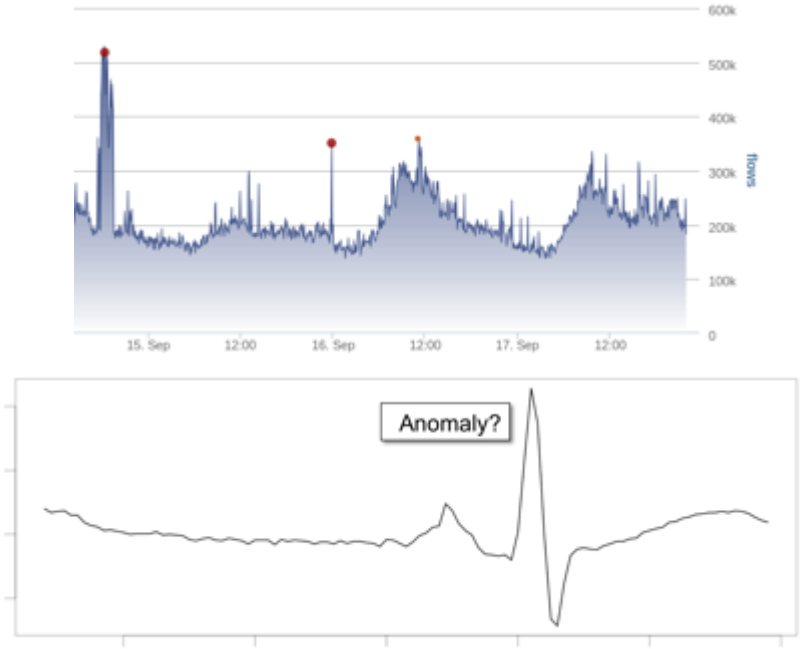
단일 값 디스플레이
(Single Value Display)

- 표준 점수(Z-Score), IQR, 히스토그램 등의 방법론을 검색 명령어에 통합
- 사용자 설정이 가능한 지리적 시각화 기능 추가
- 다양한 컨텍스트 정보를 보여주는 개선된 단일 값 패널 디스플레이

2.1 이상치 검출(Anomaly Detection)

히스토그램 기반의 이상치 검출을 위한 새로운 SPL 검색 명령어

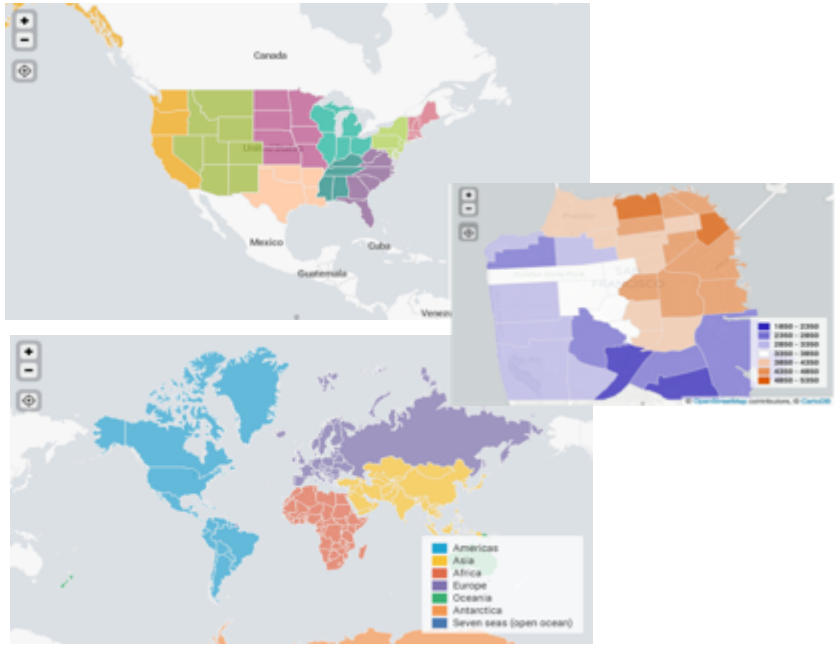
- 완전히 새로운 히스토그램 방식 적용으로 더 정확한 검출 지원
- 하나의 검색 명령어로 세가지 옵션 선택
  (표준 점수(Z-Score), IQR, 히스토그램)
- 기존 ‘outlier’, ‘anomalousvalue’ 명령어 대체



2.2 지리공간형 시각화(Geospatial Visualization)

사용자 설정이 가능한 지리적 시각화 기능의 추가

- 등치 지역도(Choropleth map)를 이용하여 공간 패턴 시각화
- 색상 눈금은 유스케이스 마다 다르게 설정 가능
- 사용자가 정의한 지도 영역 정보 업로드 가능



2.3 단일 값(Single Value) 디스플레이이

다양한 컨텍스트 정보를 보여주는 개선된 단일 값 패널 디스플레이

- 크고 눈에 띄는 색깔로
  멀리서도 한번에 볼 수 있도록 개선
- 최근 추이를 보여주는
  스파크라인(Sparkline) 추가
- 차이 표시자(Delta indicator)로
  직전 상태와의 차이 표시

스플렁크 6.3 새로운 기능

향상된
성능 및 확장성

- 2x 검색 및 인덱싱 속도
- 20-50% 수용 능력 증가
- 20%+ TCO 절감

두배 이상 향상된 성능으로 TCO 절감

향상된
분석 및 시각화

- 이상치 검출
- 지리공간형 시각화
- 단일 값 디스플레이

대규모 데이터셋의 분석이 더 용이

대용량
이벤트 수집기

- HTTP 이벤트 콜렉터
- 개발자 API & SDKs
- 3rd 파티 연동

데브옵스/사물 인터넷 규모의 데이터 지원

엔터프라이즈급
플랫폼

엔터프라이즈급 요구사항의 수용

다양한 요구사항을 수용하도록 기능 및 성능 개선!

3. HTTP 이벤트 수집기

수평 확장 가능한 데브옵스(DevOps)및 사물 인터넷(IoT) 데이터 수집 지원

1. 표준 API 및 로깅 라이브러리로 이벤트 데이터 스플렁로에 직접 전달
2. 대표적인 플랫폼 또는 서비스에 통합된 형태로 제공

DevOps & Developers

AWS Lambda

docker

IoT Devices & Applications

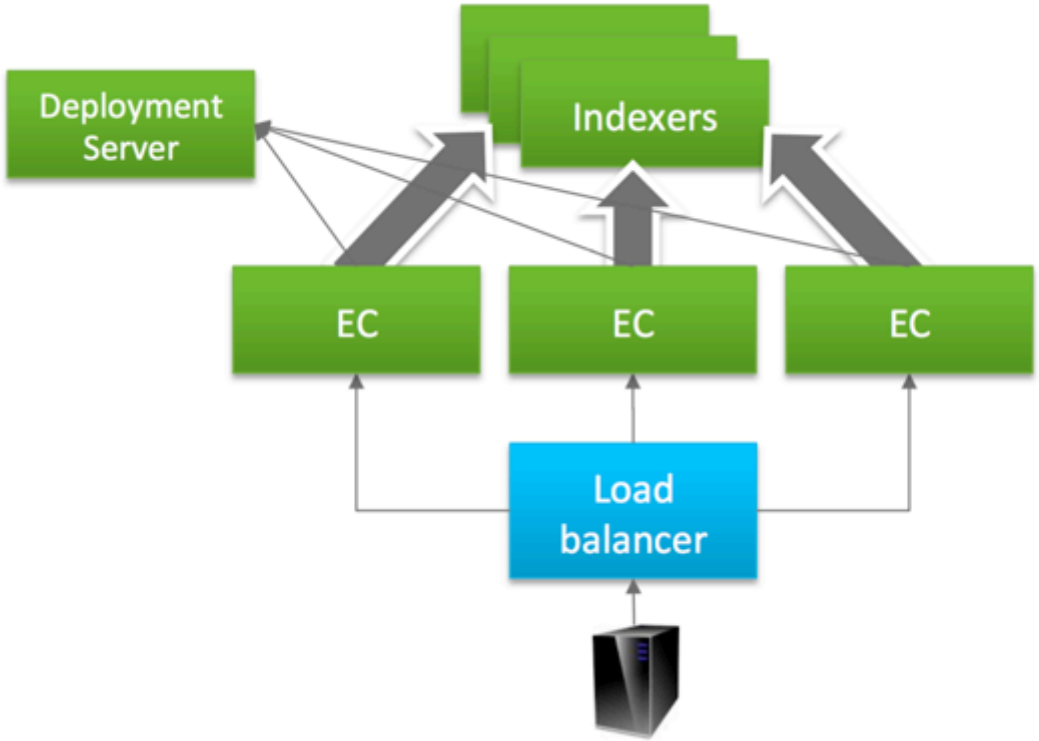
octoblu

xively by LogMeIn

초당 수백만건 규모의 이벤트 수집 지원

3. HTTP 이벤트 수집기

일반 웹 Scaling 기술에 기반한 수집 능력 확장



스플렁크 6.3 새로운 기능

향상된 성능 및 확장성

- 2x 검색 및 인덱싱 속도
- 20-50% 수용 능력 증가
- 20%+ TCO 절감

두배 이상 향상된 성능으로 TCO 절감

향상된 분석 및 시각화

- 이상치 검출
- 지리공간형 시각화
- 단일 값 디스플레이

대규모 데이터셋의 분석이 더 용이

대용량 이벤트 수집기

- HTTP 이벤트 콜렉터
- 개발자 API & SDKs
- 3rd 파티 연동

데브옵스/사물 인터넷 규모의 데이터 지원

엔터프라이즈급 플랫폼

- 향상된 관리 기능
- 사용자 정의 경고 작업
- 데이터 무결성 보장

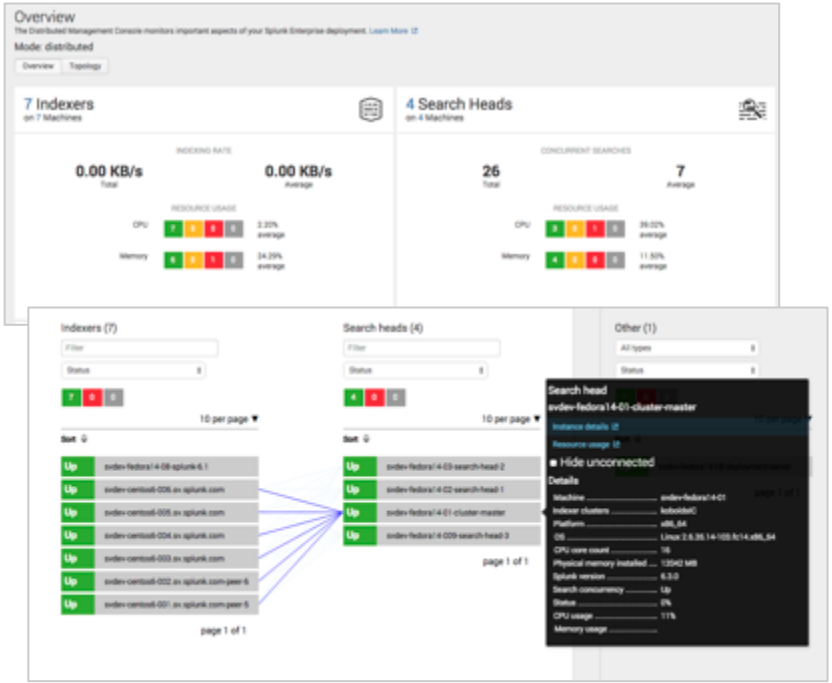
엔터프라이즈급 요구사항의 수용

다양한 요구사항을 수용하도록 기능 및 성능 개선!

4.1 분산 관리 콘솔(DMC) II

새로운 토폴로지 뷰 및 스플렁크 환경 모니터링 기능 추가

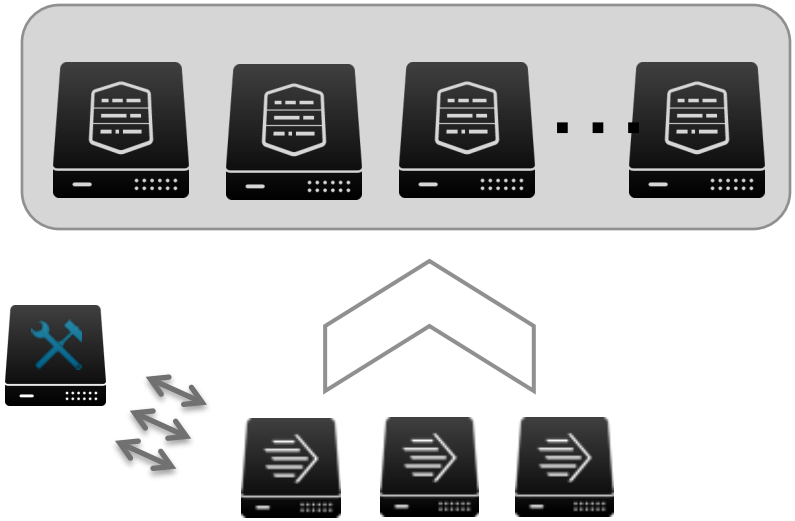
- 검색 헤드/인덱서에 대한 KPI와 성능 메트릭 시각화 제공
- 포워더의 상태와 성능을 모니터링하는 뷰 제공
- 인덱스와 메타데이터 저장소 가동율 모니터링
- 시스템 상태 확인 및 경고 발생



4.2 인덱서 자동 탐지

복잡한 수집 환경에서 포워더 관리 간소화

- 포워더가 접근했던 인덱서 목록을 클러스터 마스터가 유지 및 관리
- 포워더를 일일이 재설정하거나 조작하지 않고 인덱서를 추가 및 삭제 할 수 있음



4.3 데이터 무결성 보장

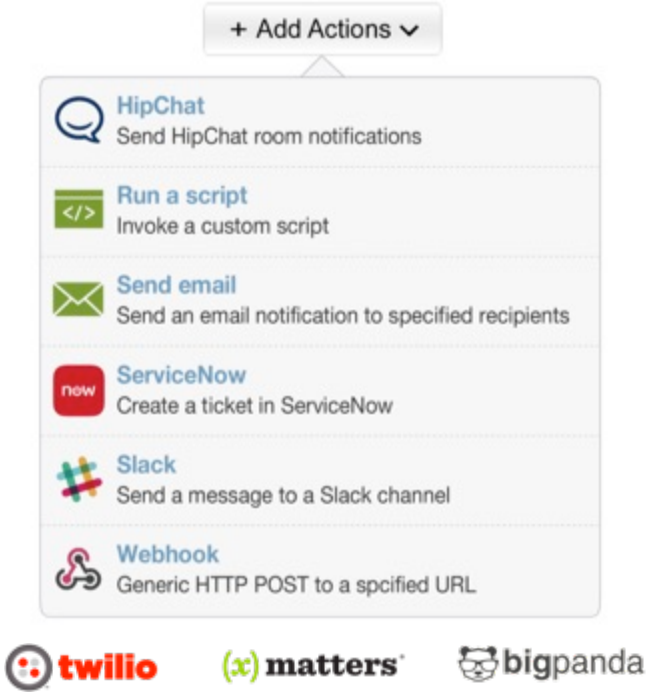
수집된 데이터의 변조 방지를 보장하는 GPG13 규정 기반의 기술적용

- 선택한 인덱스의 데이터에서 해시 시그니처 주기적으로 생성
- 생성 주기는 관리자에 의해 검증
- 데이터가 변조되지 않았음을 보장하여 보안 및 규정 준수 관련 요구사항 만족
- 해시 정보는 보안 검증을 위해 내보내기 가능

4.4 사용자 정의 경고 작업(Alert Action)

스플렁크 경고 기능을 이용하여 작업 흐름을 트리거 또는 자동화

- 외부 애플리케이션을 패키징 방식으로 스플렁크와 통합
- 간편한 관리자/사용자 설정
- 개발자는 경고 작업을 앱으로 빌드, 패키징 및 배포할 수 있음
- 통합 기능을 계속해서 추가할 수 있음



4.5 스플렁크 모바일 엑세스(Splunk Mobile Access)

스플렁크의 데시보드, 경고 및 기타 기능을 아이폰/안드로이드폰에서도 활용

- 데시보드, KPI, 보고서 모니터링
- 실시간 비즈니스/운영 관련 경고 확인
- 의견 개진 및 데이터 공유
- MDM과 SSO 지원
- 더이상 별도의 모바일 엑세스 서버의 구축 필요 없음

기타 추가된 기능들

플랫폼 기능 개선

- 수직적 확장성
- HTTP 이벤트 콜렉션
- 지능형 작업 관리자
- 데이터 무결성 보장
- 사용자 정의 경고 작업
- **검색 헤드 클러스터링 개선**

관리 기능 개선

- 분산 관리 콘솔
- 인덱서 자동 탐지
- 모바일 엑세스 단순화
- **필드 추출 기능 개선**
- **앱 검색 화면 개선**

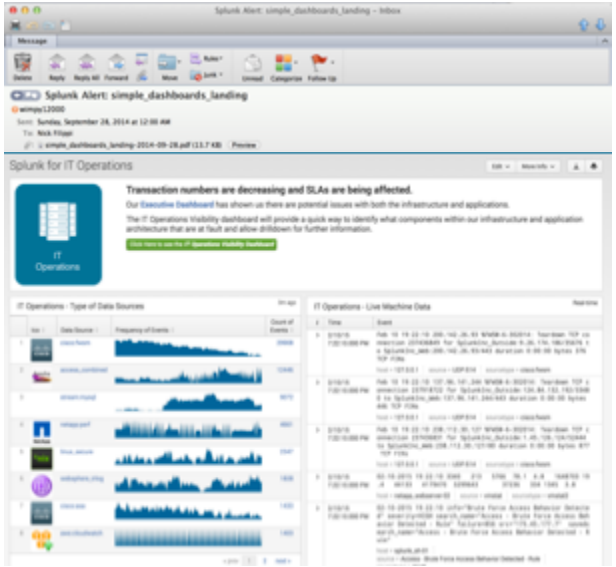
사용자 경험 개선

- 이상치 검출
- 지리공간형 시각화
- 단일 값 디스플레이
- **PDF 생성기 개선**

PDF 기능 개선

PDF 커스터마이징 기능 개선

- header/footer 커스터마이징
- 사용자 로고 삽입
- 스파크라인(Sparkline) 표기 개선
- 파일명 변경



스플렁크 제품별 기능 비교

	Splunk Enterprise	Splunk Cloud	Hunk	Splunk Light
Performance & Scale	Both	Scale	Search	No
HTTP Events	Yes	Yes	No	Yes
Data Visualization	Yes	Yes	Yes	Yes
Alert Action Integration	Yes	Yes	Yes	Future
Data Integrity Control	Yes	Yes	No	Yes
Distributed Mgt Console	Yes	Future	Yes	No

감사합니다.

splunk>