KCT
통합 Management
시스템 구축

2014.3.26

㈜ 엠앤엘솔루션

목차

- 추진방향
- 하드웨어 내역 및 규격
- 기능소개
- 구축사례
- 기대효과 및 예상 리스크
- 예상 구축 금액
- 유지보수 계획

1. 추진방향

splunk>

MNL SOLUTION

KCT 內 통합 Management를 구축하기 위한 추진방향

- **운영 편의성 제공 및 운영관리 커버리지 확대**
  분산된 로그 데이터(40GB/일) 및 IT 인프라 상태정보를 한 곳으로 수집/분석함으로써 운영 편의성을 제공
  기존 망 관리/운영지원 시스템이 관리/감시하지 못했던 관리음영 해소

- **효율적인 자원운용 유도**
  다양한 IT인프라자원 (서버, 네트워크 장비 등)을 모니터링 함으로써 효율적인 자원 운용을 유도

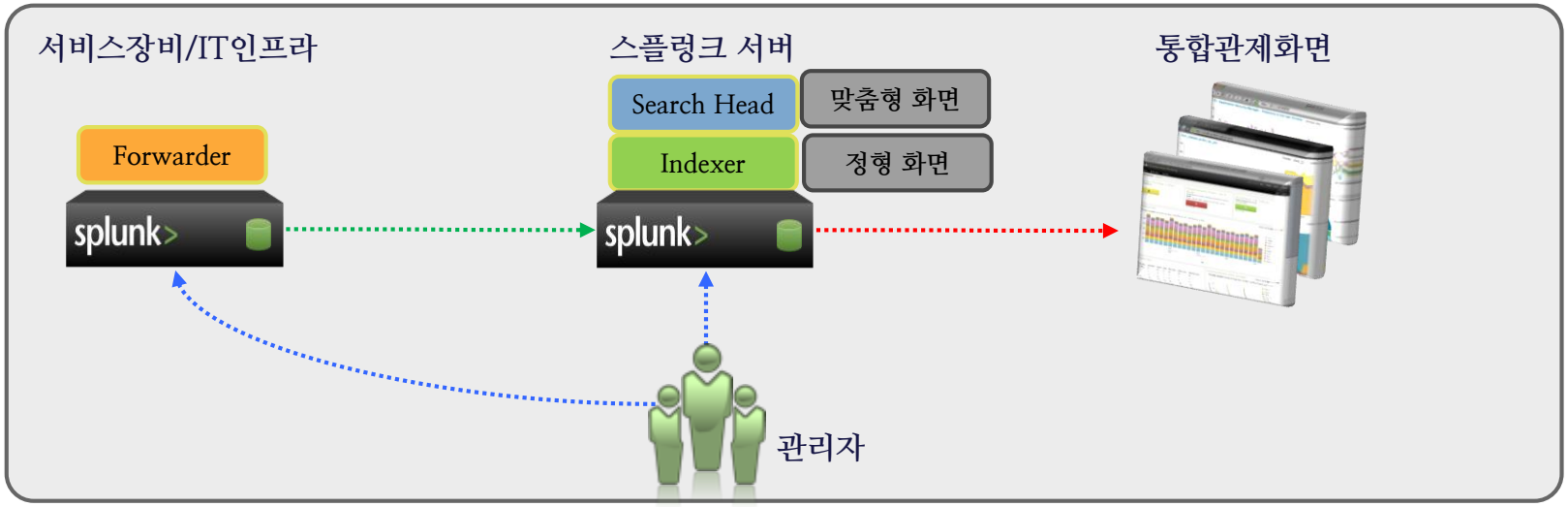
- **통합 모니터링 체계 구축**
  다양한 계층의 로그들 간, 상관 분석을 통하여 사전장애징후 감지 및 사후장애 원인분석
  사고 발생 시 신속히 후속 조치할 수 있는 통합 모니터링 체계를 구축

→ **통합 모니터링 및 실시간 분석도구 도입 필요성 (“스플렁크” 도입)**
다양한 HW, SW 모니터링 도구 혼재 => 통합적인 모니터링/감시체계 환경구축 필요
제한적 모니터링 및 폐쇄적 데이터분석 환경 => 즉각적인 분석/대고객지원, 보고서작성 필요

KCT 內 통합 Management를 구축하기 위한 추진(안)

- **고객환경분석. 전문가 컨설팅 진행**
  스플렁크 코리아/기술총판 등과 협력을 통한 고객환경 및 데이터 분석
  데이터 상관관계(correlation) 도출
  스플렁크 도입/설계로 고 가용성, 고 신뢰성, 상황적응형 Management 시스템 제안

- **IT 통합관제 관련 전문 개발인력 투입**
  정형화(Formal)된 통합관제 감시/모니터링 화면 개발과
  신규 이슈 발생 시, 사용자 맞춤형 화면 구성이 가능하도록 빠른 관제환경 개발
  이종 데이터 (ill defined data) 수신 시, 쉽게 이를 수집/분석/시각화하도록 프레임워크 개발



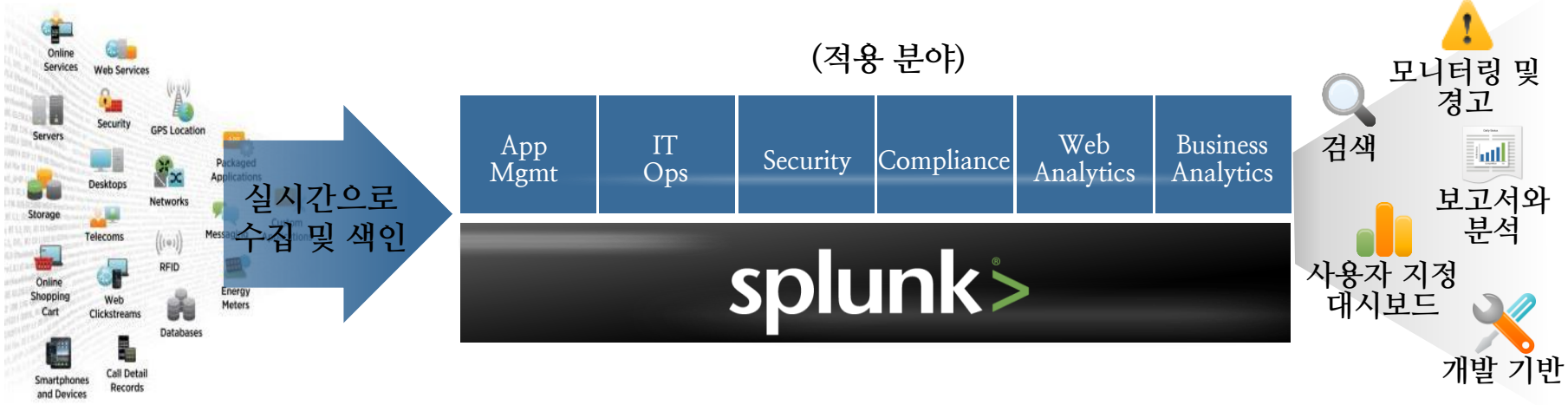
구축 時 도입할 스플렁크(splunk)에 대한 소개

- 전세계적으로 가장 널리 사용되는 상용 "Big Data" 솔루션

12,000+ Servers	27,000+ Hosts	900+ Source Types	227,000 Sources
22 Indexers, 9 Search heads		> 6TB per day indexed	
20+ Different Solutions for RCA		All Migrated to Splunk in 3 Months	

16TB/day zynga	6TB/day LinkedIn	6TB/day Expedia
2.5TB/day Bank of America		1.5TB/day intuit
1TB/day comcast	Time Warner Cable	The University of Texas at Austin
viacom	metroPCS	salesforce.com

- "Big Data"는 모두 컴퓨터 데이터에서 시작, 스플렁크는 컴퓨터의 데이터를 수집하고 분석



구축 時 도입할 스플렁크(splunk)에 대한 소개

• 다양한 원본데이터 유형 지원

– Forwarder (데이터 수집 Agent)

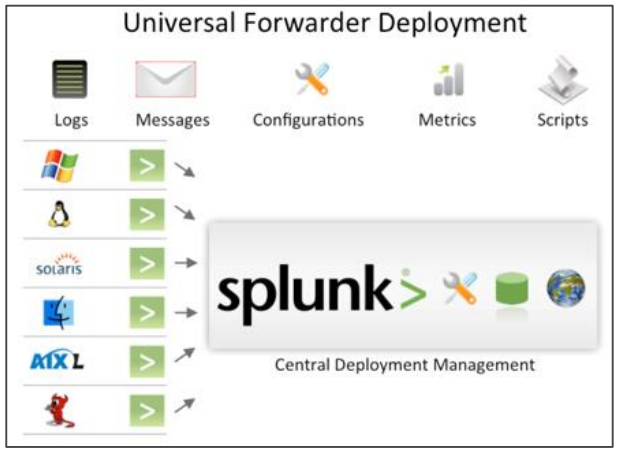
Splunk의 데이터 수집기로는 Universal, Heavy, Light Forwarder 세가지 종류가 제공.
고객의 다양한 로그 수집 요구조건을 수용하기 위해 만들어진 범용 데이터 수집 Agent

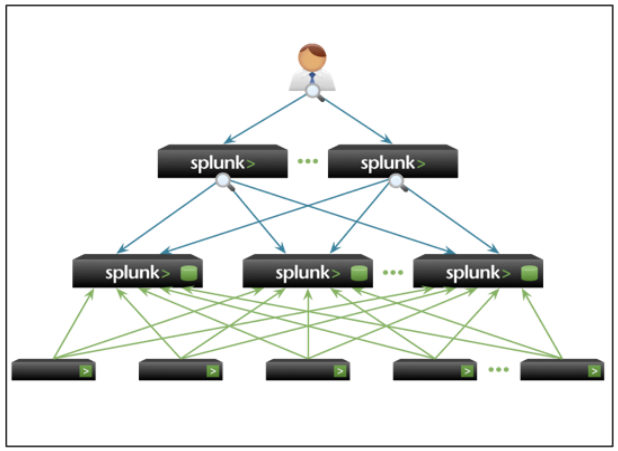
– 다양한 OS지원 (Windows, Linux, Solaris, AIX, Mac OSX 등 범용 OS 지원)

– 다양한 수집 요구조건 수용

– Circular하게 순환하는 형태의 로그 파일, 특정 폴더하의 모든 데이터, OS상에서
주기적인 스크립트의 실행 결과, Configuration File의 변경내역 등 다양한 상황에
유연하게 적용될 수 있도록 설계/개발.

– Heavy Forwarder의 경우, 수집단에서 데이터를 필터링 하는 등 다양한 작업 수행





• 확장 및 분산이 용이한 구조

– 분산구조로 쉬운 확장이 가능

Splunk는 Query를 실행하는 Search Head,

데이터를 저장하는 Indexer,

데이터를 수집하는 Forwarder등을 필요에 따라 분산 배치 가능

(데이터 저장 용량은 Indexer node를 늘려 손쉽게 확장)

구축 時 도입할 스플렁크(splunk)에 대한 소개

- 안정성

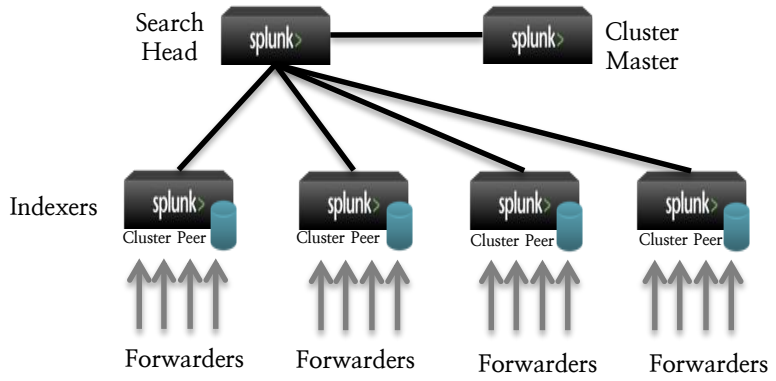
– Splunk Cluster

가장 최신 버전인 Splunk 5.x 부터는 Index node Clustering 기능 제공

한가지 데이터를 여러 node에 중복 저장하여, 디스크 장애나 node 장애에 대처 가능

원본 데이터의 중복 Copy 수는 Replication Factor,

인덱스 정보의 중복 Copy수는 Search Factor로 필요에 따라 지정.



- 다양한 분석기능

– 실시간/초고속 검색 엔진 제공

Splunk의 Map/Reduce Architecture기반의 실시간 검색엔진은 초고속 검색 속도를 제공하며 간단한 검색창을 통해 시간조건을 검색하고 논리적, 반복적,문자열, 와일드카드, 검색 필터 등의 검색이 가능 하며, 실시간으로 수집되는 스트리밍에 대한 검색을 제공함으로써 통합적인 데이터 검색이 가능.

– 실시간 장애/Event 현황 탐지 및 분석

Splunk의 실시간 데이터 처리 기능과 강력한 검색기능을 조합하여, 서버 종류/고객사/이벤트의 등급/서비스 종류 別 다양한 차트와 알람, 그리고 대시보드를 생성이 가능.

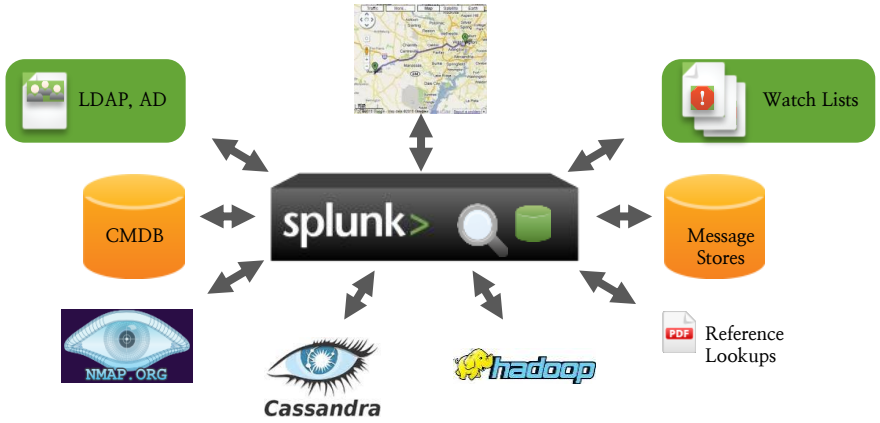
– 다양한 함수 제공

다양한 함수 및 검색 명령어 활용이 가능 (참조: http://docs.splunk.com/Documentation/Splunk/latest/SearchReference/ListOfSearchCommands)

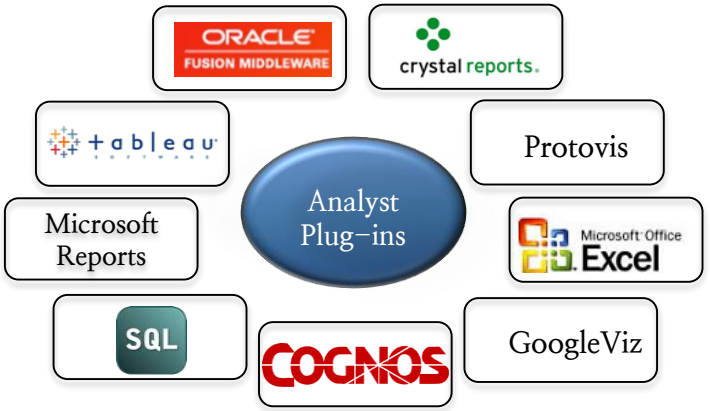
이를 통한 데이터 분석/요약 및 통계 지표 산출이 가능

구축 時 도입할 스플렁크(splunk)에 대한 소개

- 다양한 외부데이터베이스 및 BI/분석 툴과 연계 가능



연동 가능한 데이터베이스 유형

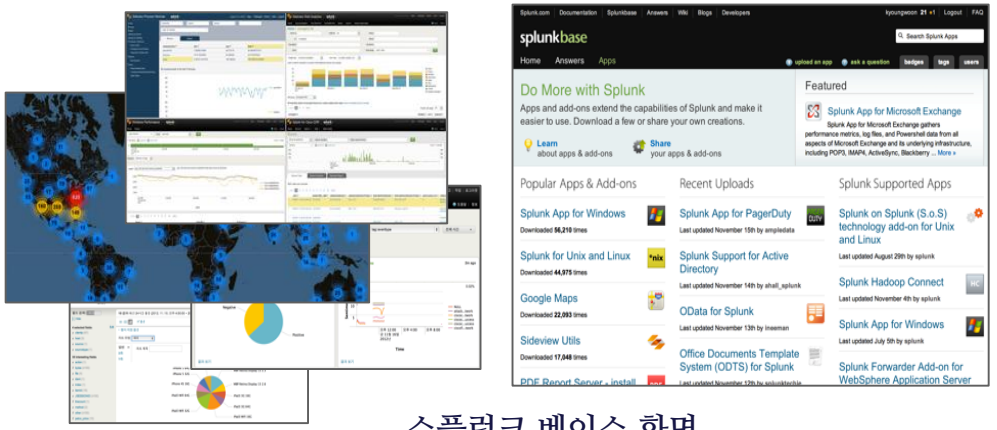


연동 가능한 BI/분석 툴

- 사용하기 쉬운 분석환경 지원

– 다양한 Splunk App UI들을 통한 인터랙티브한 분석 가능

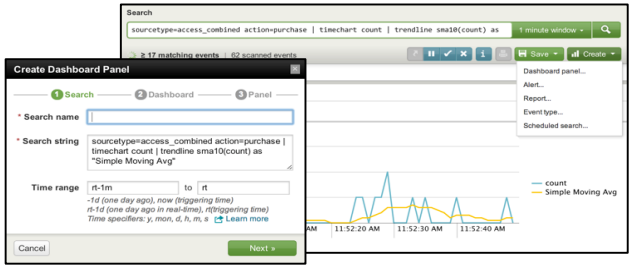
Splunk에 설치되어 있는 기본 App 뿐만아니라 , Splunkbase(http://www.splunkbase.com)의 다양한 무료 앱 및 컴포넌트들을 이용해서, 긴 개발기간 없어도 다양한 응용 분석환경을 제공



스플렁크 베이스 화면

구축 時 도입할 스플렁크(splunk)에 대한 소개

- 강력한 가시화 (Visualization)



– 위저드 형식의 대시보드 생성

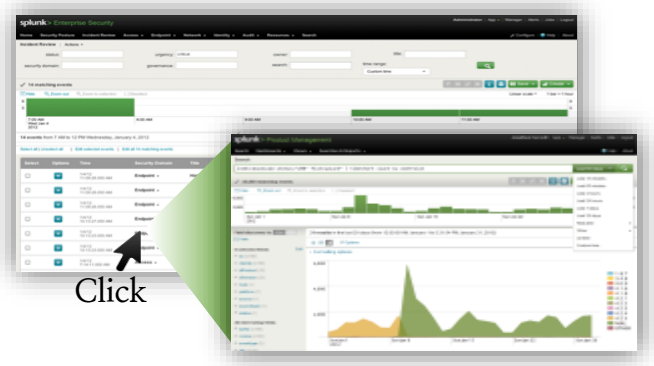
웹 인터페이스를 통해 간단히 대시보드 만드는 기능을 제공.

사용자의 Query를 즉시 Visualization 시키고, 이 결과를 위저드에서 간단히 세 단계의 설정을 거쳐 손쉽게 대시보드를 생성

– 다양한 Chart-Type 제공

기본 built-in 된 다양한 차트 외, Splunk APP을 통해서 무료로 손쉽게 Google Map등의 다양한 Visualization을 추가 가능.

또한, REST API를 이용하면 3rd Party 차트 라이브러리도 연동할 수 있습니다



– Dynamic Drill-down (root cause 추적을 위한)기능 제공

대시보드 사용자가 이상 징후를 포착하거나 추가 ad-hoc 분석을 원할 때, Drill-down기능을 제공하여, 빠르고 손쉬운 분석이 가능하도록 지원.

하나의 차트나 표에서 클릭하여 심층 분석이 가능한 보다 Detail 한 차트로 연결.

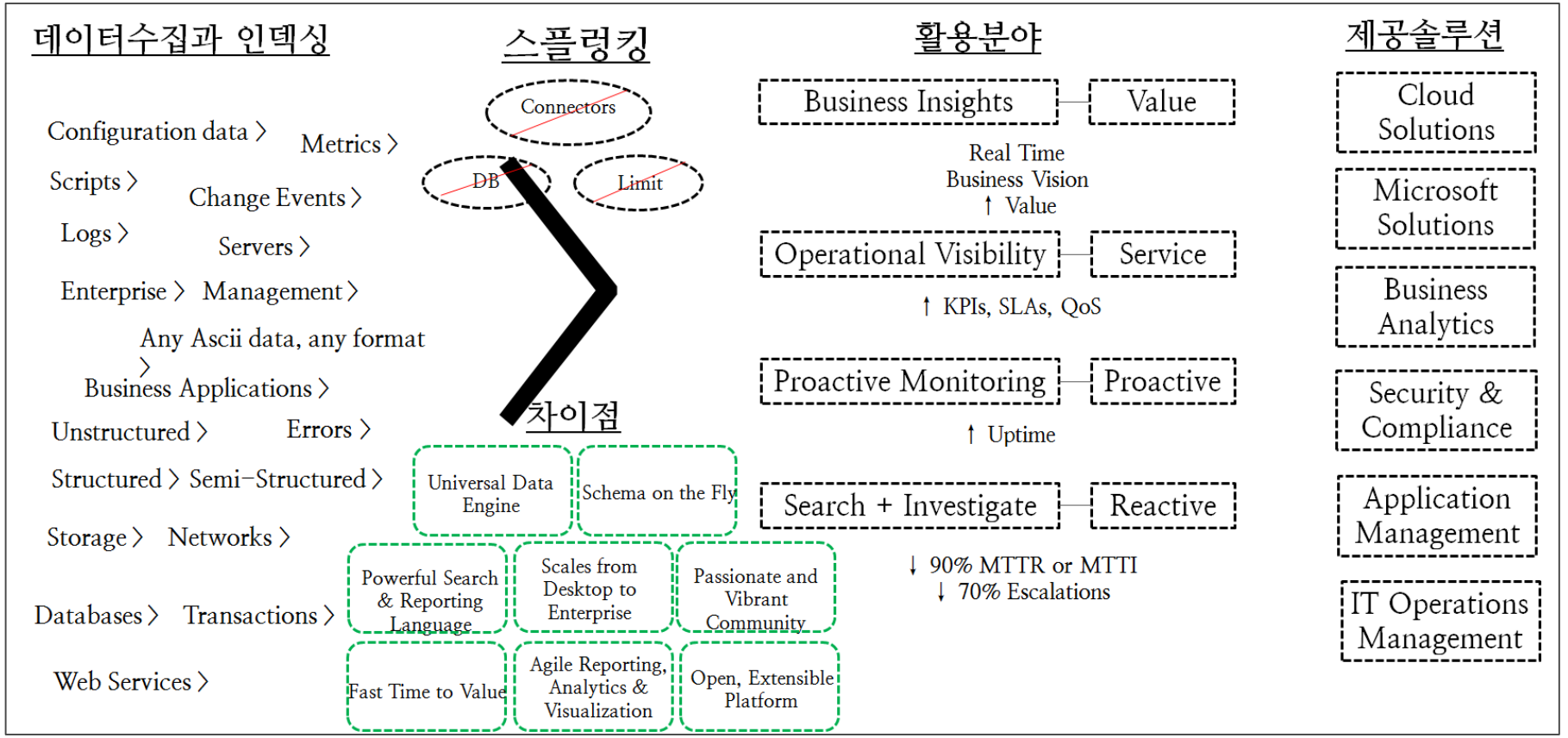
또한, 사용자 요구에 맞게 Customize 가능.

구축 時 도입할 스플렁크(splunk)에 대한 소개

- 他 “Big data” 엔진과의 차별성

– 커넥터/데이터베이스 부재. 비정형데이터 여부에 따른 수용제약 및 물리적/논리적 확장에 제약 없음.

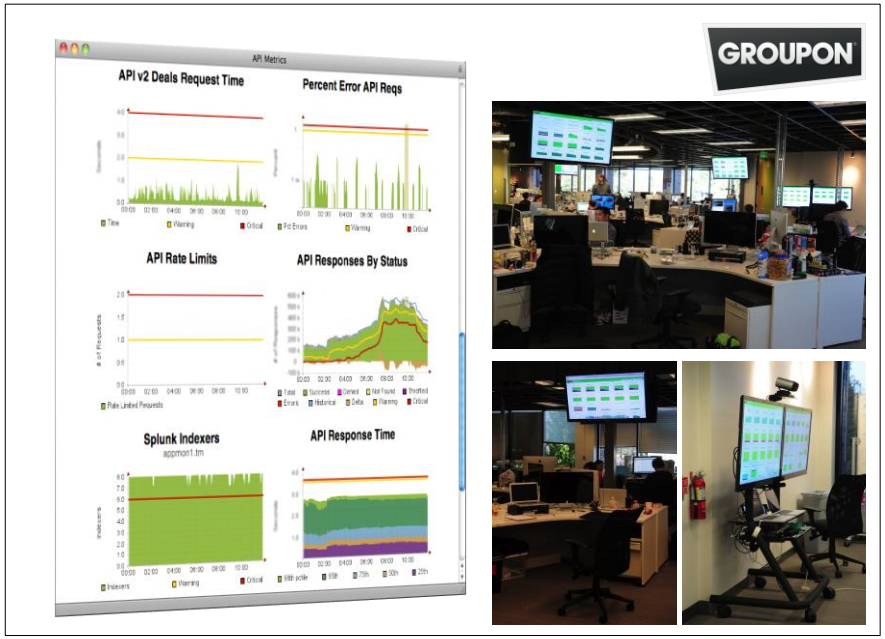
– 통합데이터모델엔진, 스키마리스, 검색엔진, scale-out, 빠른 시장접근성, 가시화, 실 시간성 강화, 오픈/확장 플랫폼 등



구축 時 도입할 스플렁크(splunk)에 대한 소개

- 적용사례
  - 전 세계 4,000 곳 이상의 고객 확보

Reference site



적용사례: 구루폰

2. 하드웨어 내역 및 규격

Splunk S/W 구성

- Forwarder
  - ✓ 데이터를 access할 수 있는 고객의 시스템에 설치되는 컴포넌트
  - ✓ 최소한의 resource를 점유하면서 데이터를 수집 / 전송

- Indexer
  - ✓ 수집된 데이터를 저장하고 인덱스하며, 실제 데이터에 대한 검색이 수행되는 노드
  - ✓ 빠른 응답 속도를 위해서 충분한 Disk I/O 및 CPU 성능이 요구되는 시스템

- Search Head
  - ✓ 고객이 접속하는 웹 환경 제공
  - ✓ 검색 요청이 있을 때 설정된 여러 Indexer노드에 분산 검색을 수행하며 결과 데이터를 취합함
  - ✓ 주로 CPU 및 Memory Intensive한 Job이 수행됨

Splunk S/W 구성

- Search Head를 위한 최소 H/W 사양
  - ✓ Intel 64-bit chip architecture
  - ✓ 4 CPUs, 4 cores per CPU, 2.5~3 GHz per core
  - ✓ 8 GB RAM
  - ✓ 2 x 300 GB, 10,000 RPM SAS hard disks, configured in RAID 0
  - ✓ Standard 1Gb Ethernet NIC, optional 2nd NIC for a management network
  - ✓ Standard 64bit Linux or Windows distribution (Linux recommended)

- 권고 사항
  - ✓ 위에 예시한 H/W는 최소 사양으로, 충분한 성능을 위해서는 상기 System보다 고사양 장비가 필요.
  - ✓ 특정 시점에 검색을 수행하는 1명의 active user 당 최소 1개의 core가 할당 가능하도록 권고.
  - ✓ Saved Search의 수행 또한 active user와 마찬가지로 특정 시점에 1개의 core를 점유할 수 있도록 권고.
  - ✓ Search Head는 CPU를 많이 사용하는 노드 이므로 위 최소 권고 사항보다 충분히 많은 CPU core가 확보 필요.
  - ✓ Search Type에 따라 추가적인 리소스 확보가 필요한 경우가 존재함.

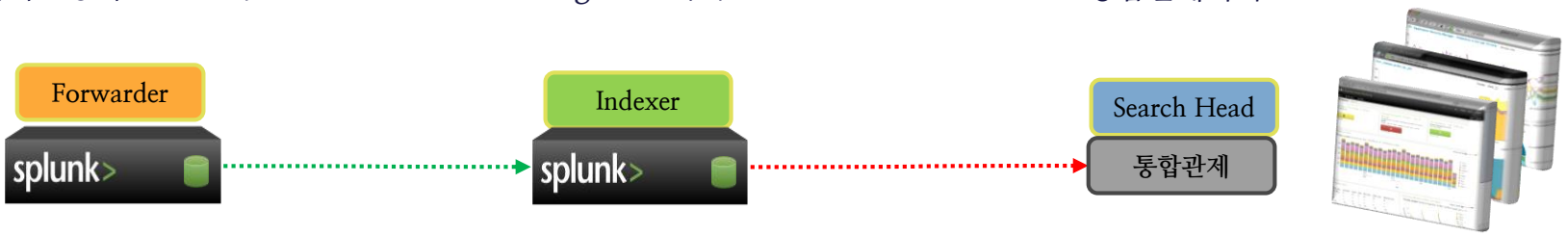
Splunk S/W 구성

- Indexer를 위한 최소 H/W 사양
  - ✓ Intel 64-bit chip architecture
  - ✓ 2 CPUs, 4 cores per CPU, 2.5~3 GHz per core
  - ✓ 8 GB RAM
  - ✓ 최소 1,200 IOPS 이상의 Disk Subsystem (예를 들어 12x300GB, 15,000RPM SAS hard disk, RAID 1+0)
  - ✓ Standard 1Gb Ethernet NIC, optional 2nd NIC for a management network
  - ✓ Standard 64bit Linux or Windows distribution (Linux recommended)

- 권고 사항
  - ✓ 위에 예시한 H/W는 최소 사양으로, 충분한 성능을 위해서는 상기 System보다 고사양 장비가 필요.
  - ✓ local disk로는 cover할 수 없는 많은 용량의 데이터에 대한 빠른 검색 성능이 요구되는 경우 SAN over fiber를 적용 권고.
  - ✓ 일반적으로 Indexer 노드는 bulk read와 disk seek작업이 주로 많습니다. 그러므로 더 많은 disk (more spindles)를 적용하는것이 더 좋은 indexing performance에 효과적
  - ✓ ratio of disks to disk controllers : database server를 구성하는 것과 마찬가지로 높을수록 좋음.

도입 H/W, S/W 내역 및 상세규격 제시

서비스장비/IT인프라 | Big data 서버 | 통합관제서버



Big data 서버 (Splunk Indexer/Header) 1대		
CPU	Intel 2.5GHz 2P12C	
RAM	32GB	
HDD	용량	SAS 900GB * 10
	속도	15000 RPM
	RAID	RAID1 4.5TB x 2EA

통합관제 서버 1대		
CPU	Intel 2.5GHz 2P12C	
RAM	32GB	
HDD	용량	SAS 900GB * 10
	속도	15000 RPM
	RAID	RAID1 4.5TB x 2EA

Big data 서버 (Splunk Indexer/Header)	
개발언어	JAVA, C/C++
DBMS/WAS	Splunk
OS	Linux (Ubuntu)

통합관제 서버	
개발언어	JAVA, C/C++
DBMS	Splunk / MySQL
WAS	Splunk, Apache/Tomcat/Spring/MyBatis
OS	Linux (Ubuntu)

3. 기능소개

splunk>

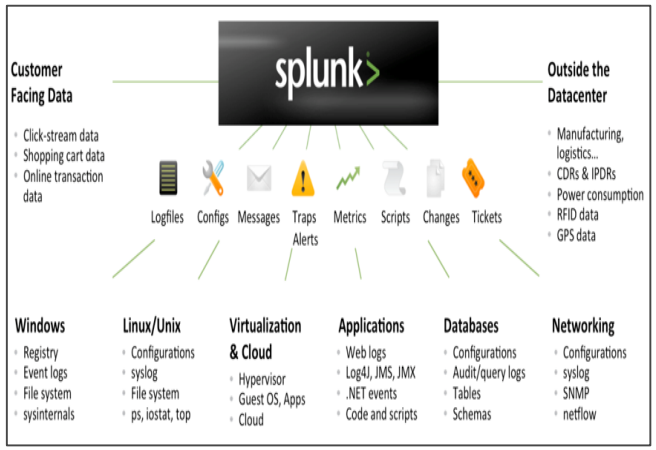
MNL SOLUTION

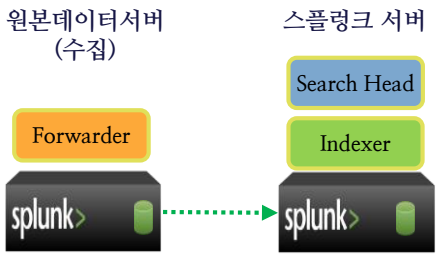
데이터 수집방안: SNMP(Performance, Trap 등), Agent 설치/제어, File (Log, CDR 등)

- **다양한 머신 데이터를 하나의 Universal Indexing 체계를 이용하여 수집**
  Splunk 고유의 Universal Indexing 체계와 Forwarder(유연한 데이터 수집기)를 이용, 다양한 비정형 머신 데이터를 유연하게 수집 가능 (신규 로그를 수집하는 경우에도 별도 Schema나 Agent를 구현할 필요 없음)

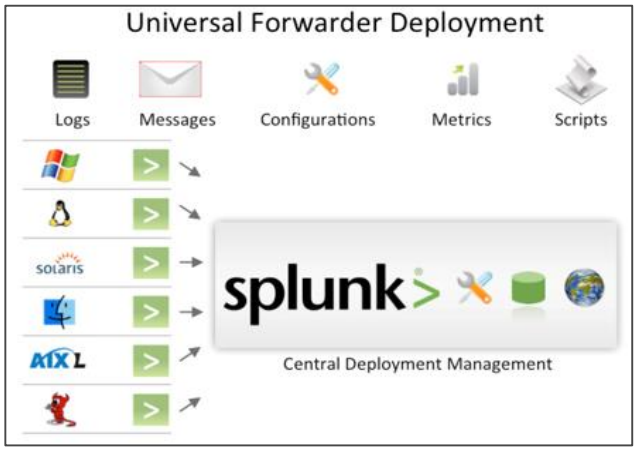
- **SNMP**
  Splunk의 Trap alert 수집기능을 이용하여 Trap 이벤트를 수집. (Trap 주소지정 필요)
  또한 스플렁크 서버에 net-snmp를 설치, 주기적으로 NE로부터 MIB data를 폴링 후, 텍스트 로깅하고 이를 인덱스화

- **Agent 설치/제어 및 파일(Log, CDR)**
  수집대상 서버에 Forwarder를 설치하고, 해당 서버로부터 정책에 의해 파일정보를 수집
  (Agentless 방식도 지원가능: 원격서버접속 및 서버로부터 직접 데이터를 수신하는 방식, 예: syslog, WMI, remote access)





다양한 원본데이터 수집 가능



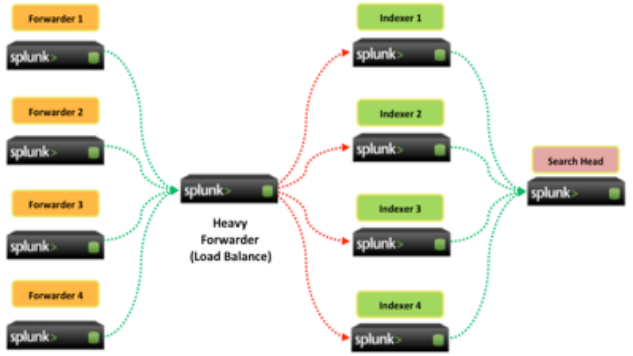
데이터 수집방안

Category	TYPE	Splunk Agent	SSH / TELNET	FTP	NFS/SCP/ RSYNC	TCP/ UDP	DBI / SQL	Script	SNMP
Network	Routers		O			O		O	O
	Switch		O			O		O	O
	Firewall		O			O		O	O
Servers	Linux	O	O	O	O			O	O
	AIX	O	O	O	O			O	O
	Solaris	O	O	O	O			O	O
	Windows	O	O	O	O			O	O
	MAC	O	O	O	O			O	O
	TANDEM		O	O	O			O	O
	TRU64		O	O	O			O	O
	AS400		O	O				O	O
	Mainfreme		O	O				O	
Database	Oracle	O	O	O	O		O	O	
	Informix	O	O	O	O		O	O	
	Sybase	O	O	O	O		O	O	
	Mysql	O	O	O	O		O	O	
	MS SQL	O	O	O	O		O	O	
Applications	apache	O	O	O	O			O	
	Weblogic	O	O	O	O			O	
	Websphere	O	O	O	O			O	
	SAP	O	O	O	O			O	
	Custom App	O	O	O	O			O	

데이터 수집방안

- **서비스 운용 중인 서버에 설치되는 Agent는 최소한의 서버자원을 점유**

  Splunk Universal Forwarder는 모니터링 대상 서버자원을 최소로 사용하고 최대한의 데이터를 수집/전송할 수 있도록 설계/개발된 효율적인 모듈임 (국내 도입 前 PoC에서의 측정치: CPU 1%, Mem 1%)



예시: Agent 자원점유율 검증시험

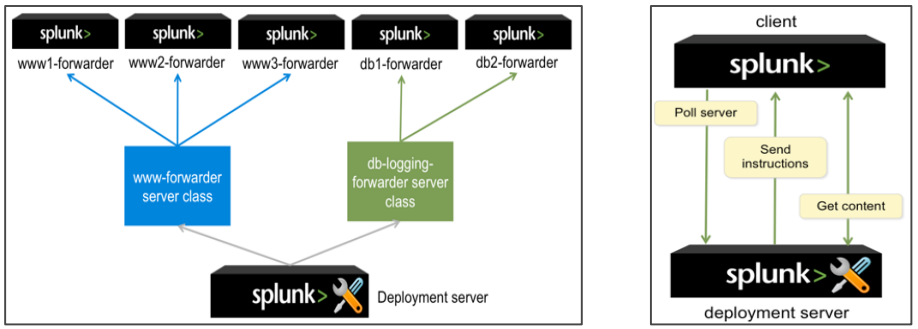
(Test Server)
Universal Indexer : Amazon EC2 m1.xlarge
Load Balancer(Heavy Forwarder) : Amazon EC2 m2.2xlarge
Indexer 4 nodes : Amazon EC2 m2.2xlarge
Search Head : Amazon EC2 m2.2xlarge

(Scenario)
5GB, 10GB, 15GB, 100GB /server /day
1 event size = 328 bytes

(Result)
CPU 점유율 1% 이하
Memory 사용율 1% 이하

- **Deployment 서버를 이용한 중앙에서 Agent를 일괄관리**

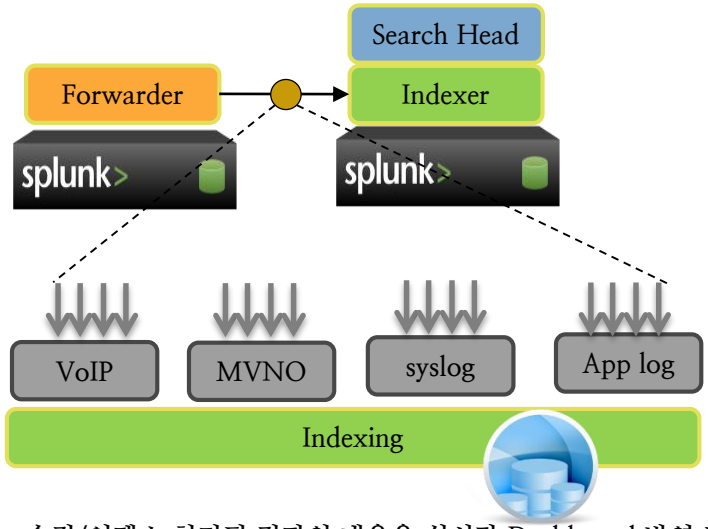
  Deployment 서버를 이용, 분산환경에서 다수의 Forwarder/인덱스 노드 설정을 중앙에서 손쉽게 일괄관리 하는 기능을 제공

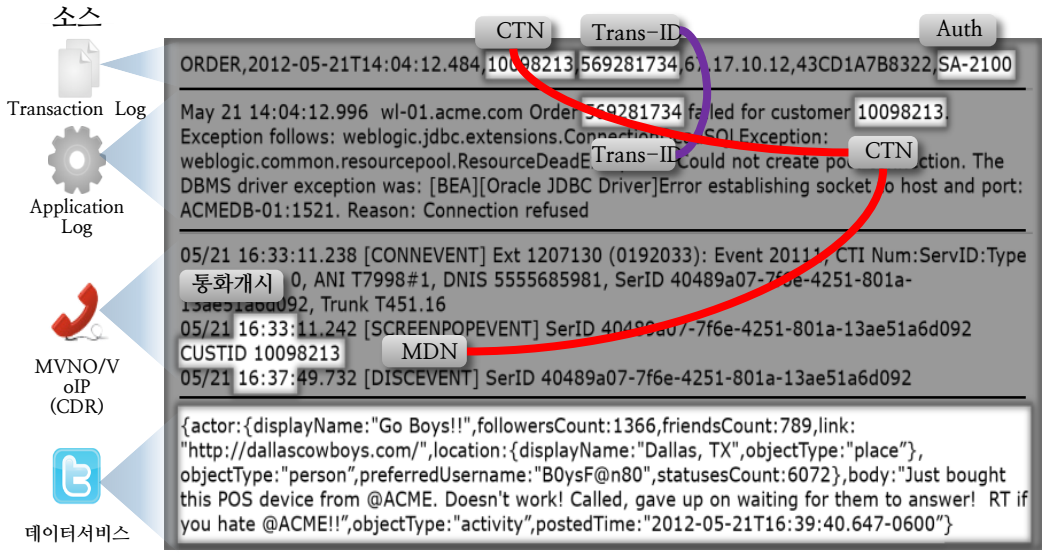


Deployment 서버를 통한 중앙관리

데이터 처리/분석 방안

- **시스템, 고객군, 고객 단위 별 서비스 정보와 연계하여 운용측면의 데이터 제공방안**
  서비스장비와 IT인프라자원에 Forwarder agent를 탑재하고,
  Syslog, Application Log 및 CDR을 수집

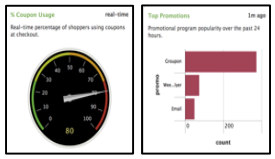


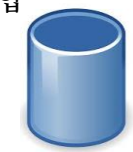


다양한 원본데이터로부터 상관 분석하는 과정

수집/인덱스 처리된 결과의 내용을 실시간 Dashboard 반영 및 통계화 (RDB)
- 5분/30분/1시간/일 별 통계화 및 실시간 반영
- 서비스, 시스템, 가입자 別 별도 레코드로 저장
- 호 시도/성공/실패 수 및 완료율 (VoIP = INVITE~BYE, CDR= open/close/interim)

실시간 검색은 Splunk Search Head를 통해 직접 질의, 기타 통계화는 Splunk 실시간 엔진을 통해서 직접 통계데이터베이스(RDB)에 삽입

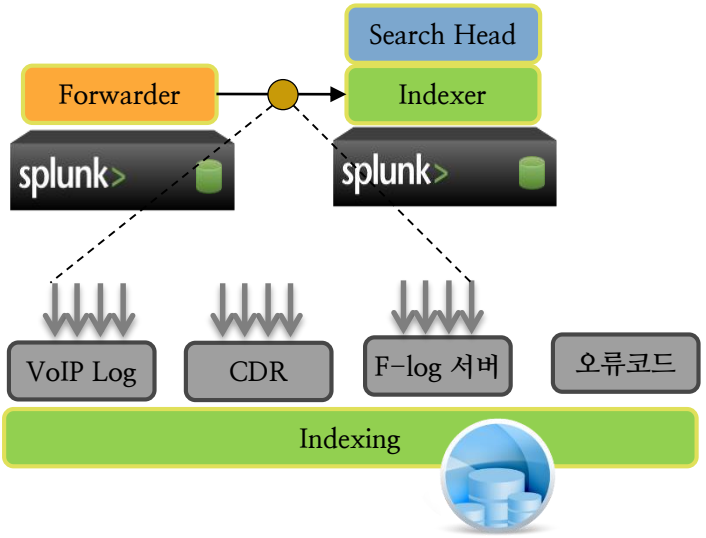


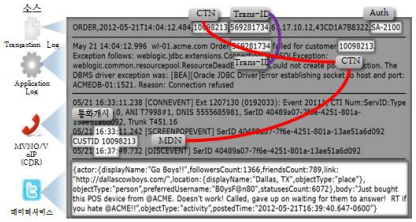


서비스	시스템	시간	CTN	유형
VoIP	GW1	2014032..	010xxxx	INVITE
MVNO	MSC1	2014032..	010xxxx	CDR(o)
-	GW2	2014032..	-	DOWN

데이터 처리/분석 방안

- **불 완료 로그분석을 통한 서비스, 고객, 시스템 단위 데이터 제공방안**
  별도 불 완료 로그서버가 있을 경우, 해당시스템에 Forwarder를 탑재하여 불완료 로그를 수집하거나,
  VoIP (SIP GW/TGW/IBCF) 등의 Application Log와 CDR 저장서버에 Forwarder를 탑재하여 전체로그를 수집함.
  별도 에러코드가 존재할 경우, 이를 파일형태로 저장한 후 인덱스화





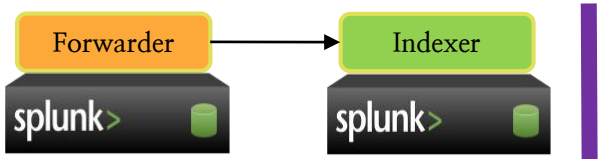
수집/인덱스 처리된 결과의 내용을 실시간 Dashboard 반영 및 통계화 (RDB)
- 5분/30분/1시간/일 별 통계화 및 실시간 반영
- 서비스, 시스템, 가입자 別 별도 레코드로 저장
- 수신된 CDR 내 오류코드 또는 VOIP 트랜잭션 내 오류코드를 인덱스화 한 오류코드 테이블과 매핑하여 분류

실시간 검색은 Splunk Search Head를 통해 직접 질의, 기타 통계화는 Splunk 실시간 엔진을 통해서 직접 통계데이터베이스(RDB)에 삽입

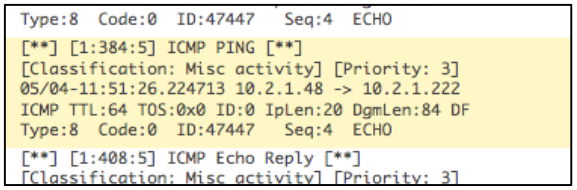
서비스	시스템	시간	CTN	오류코드
VoIP	GW1	2014032..	010xxxx	서버미응답
MVNO	MSC1	2014032..	010xxxx	잔액부족
-	GW2	2014032..	-	시스템다운

데이터 처리/분석 방안

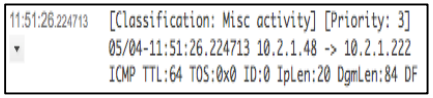
- **실시간 서비스품질, 트래픽 성능감시를 위한 기능 제공방안**
  Splunk는 실시간으로 수집한 데이터를 자동인식한 후, 세분화 후 인덱스 化함
  이후 다양한 조건으로 실시간 데이터 검색이 가능하며,
  이를 이용하여 실시간 서비스품질 및 트래픽 성능 감시가 가능 (예: VoIP RTCP 또는 ICMP RTT 등 자료수집)

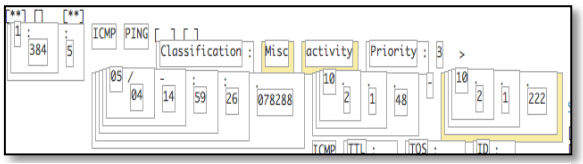


실시간 Dashboard 구성 (조건질의를 이용)

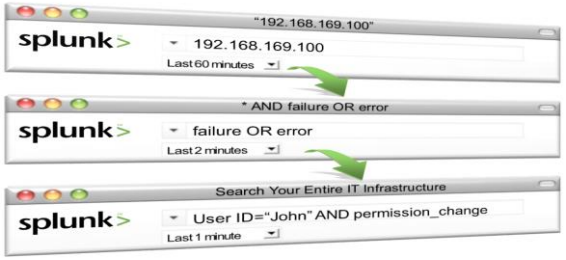


실시간 데이터 자동이벤트 경계식별
(예: 타임스템프자동정규화)

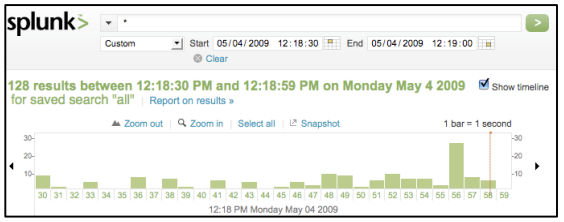




모든 항목을 세분화/인덱스



다양한 조건으로 검색

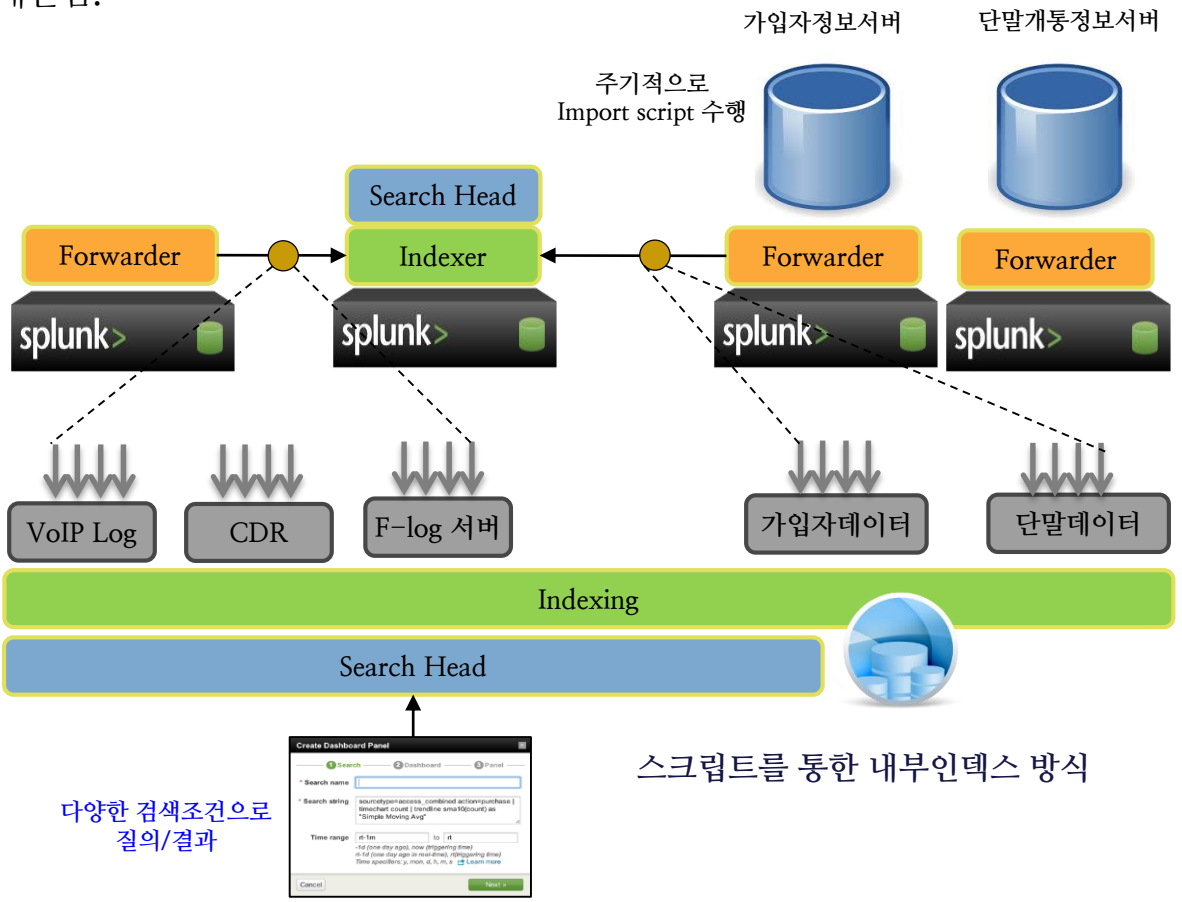


검색결과 조회

데이터 처리/분석 방안

- **가입자 정보 연동을 통한 서비스 상품, 단말기, 고객단위 별 데이터 제공방안**
  가입자정보/단말개통정보 서버와 연동이 가능할 경우,
  실시간 DB링크/커넥트를 통한 방법보다는, 주기적으로 현행화된 가입자/단말정보를 import한 후, Forwarder를 통해 Splunk 서버에 수집/인덱스 처리하는 방법을 제안함.

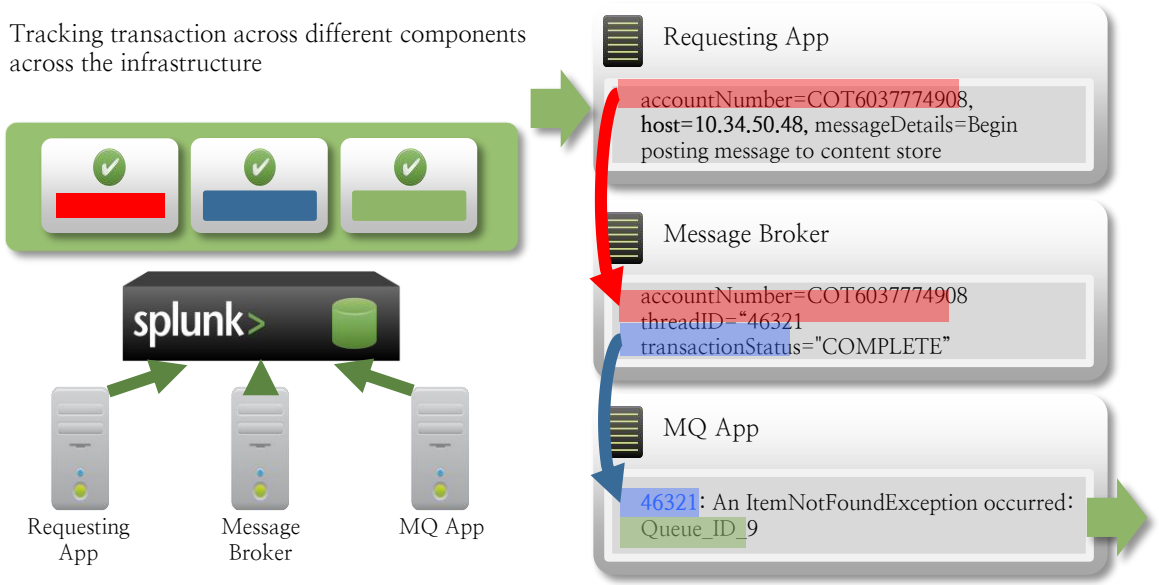
외부 데이터베이스 연동 방식
(하둡 포함)

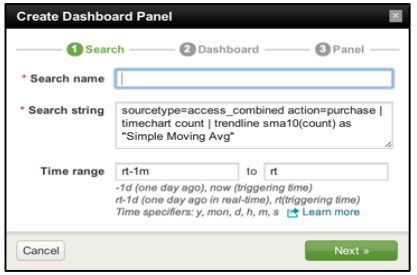


스크립트를 통한 내부인덱스 방식

데이터 처리/분석 방안

- **서비스 및 고객 단위 별 사용이력 정보 실시간 추출 방안**
  Splunk는 수집된 정보를 인덱스화 하는 과정 중에 고유의 Universal Indexing을 수행하게 되며,
  Head 검색/조회 command를 통해 원하는 서비스 별, 고객 별 사용이력의 실시간 trace가 가능함.






```
2014-03-24 11:28:54,301 [WEB] INFO messageType = POST,
messageStatus = INIT, accountNumber = COT6037774908, host =
10.34.50.48, messageDetails = Begin posting message to content store
2014-03-24 11:28:54,322 [WEB] INFO messageType = POST,
messageStatus = TASK, accountNumber = COT6037774908, host =
10.34.50.48, messageDetails = Opening connection to host:
[ www.contentstore.com:80 ]
2014-03-24 11:28:54,397 [WEB] INFO messageType = POST,
messageStatus = TASK, accountNumber = COT6037774908, host =
10.34.50.48, messageDetails = Connection established to host:
[ www.contentstore.com:80 ]
2014-03-24 11:28:54,474 [WEB] INFO messageType = POST,
messageStatus = TASK, accountNumber = COT6037774908, host =
10.34.50.48, messageDetails = Writing message to host:
[ www.contentstore.com:80 ]
<TRANSACTION date="24032014 11:28:54,797" activityCode="1010"
sequenceNumber="100198887" accountNumber="COT6037774908"
threadID="46321" callerID="MAR10209LA" transactionStatus="FAILURE"
result="FATAL" host="10.34.51.91" comment="Invocation of Content API
for sequenceNumber 100198887 failed" >
[03/24/10 11:28:55 UTC] 000000af StorageApi E
com.ibm.wps.policy.commands.StorageApi logExceptionGetPvsProperties
46321: An ItemNotFoundException occurred in method
logExceptionGetPvsProperties. com.ibm.portal.WpsException: 46321: An
ItemNotFoundException occurred in method logExceptionGetPvsProperties.
```

이.기종 분산시스템에서의 E2E Trace/View

데이터 처리/분석 방안

- 기타 전화서비스제공자 기준, 다양한 조건의 사업분석 데이터 종류 제시

– 정적데이터 + 동적데이터 결합을 통한 사업분석 데이터 추출 가능
정적: 고객/가입자 데이터, 개통단말 정보
동적: 고객사용정보 (application log, CDR)

예시)
서울지역 30대 남자가 선호하는 단말유형 <– 기존 가입자/단말정보로 추출 가능한 영역
실제 제공하는 단말화면이 클 경우, 음성/데이터호 ARPU에 영향을 주는 지 여부에 대한 상관도 분석 (개선 가능)
: 상관도가 높을 경우, 단말프로모션이 가능
: CDR에 위치정보가 포함될 경우, 특정지역(존) 요금제도 고려 가능

CTN	시작 시간	Duration	서비스종류	URL
010xxx…	2014032..	180	CS	
010xxx…	2014032..	340	PS	NAVER

CTN	가입자명	성별	요금제	나이
010xxx…	홍길동	1	선불	43

CTN	단말모델
010xxx…	삼성A

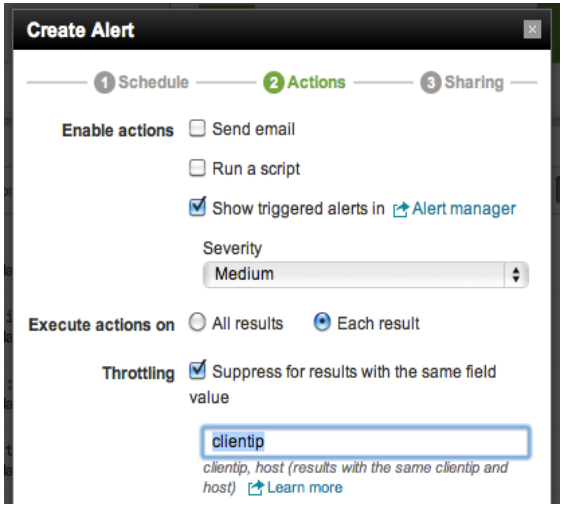
이벤트 처리방안

- 장애 등의 이벤트 표현방법, 임계치 설정 방안

– 유연한 경보체계 제공
다양한 이벤트들을 실시간으로 감지하고 이를 경보로 연결가능.
이벤트의 조건은 과거 데이터 + 실시간 스트림 동일 적용
(여러 원천 데이터가 서로 조합된 형태로 검색/적용)
=> 모니터링, 감시화면에 관련한 가시/가청정보 제공 가능

– E-mail 발송 방식 (옵션)
사용자가 지정한 조건에 부합하는 상황이 발생하였을 때,
이벤트 정보와 관련 내용을 담당자 Email로 전송가능

– 스크립트 수행 (옵션)
경보가 발생하였을 때 Script를 수행하도록 지정하는 기능
이 기능은 특정 상황 발생 時 사람이 개입하지 않고,
시스템이 지정된 동작을 수행하는 용도로도 적용가능

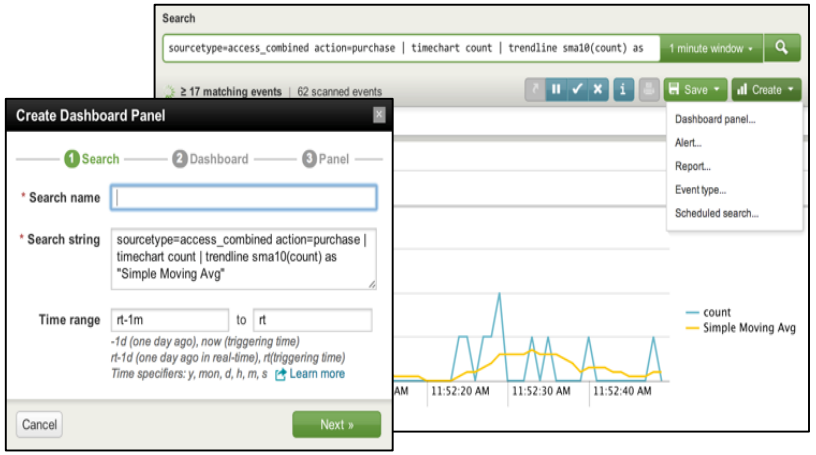


장애이벤트 관리기능

User Interface

- 비 구조적인 로그수집을 통해 비정형화된 UI로 표현할 수 있는 방법제시

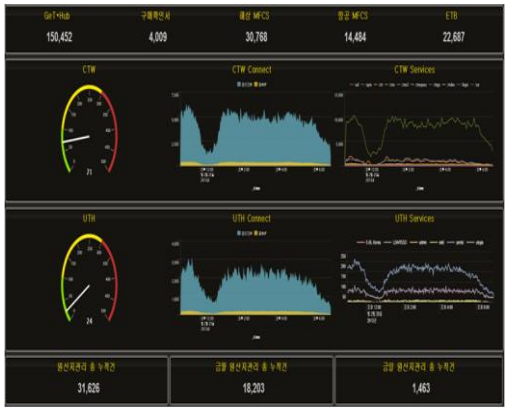
– Dashboard 생성 위자드를 이용하는 방법
Dashboard 생성기를 이용하여
기 수집/인덱스화 된 자료에 검색 문법에 맞춰서 질의 명령어 수행
수행의 결과물로서 다양한 형태의 대시보드 생성이 가능
생성된 Dashboard를 원하는 패널에 부착



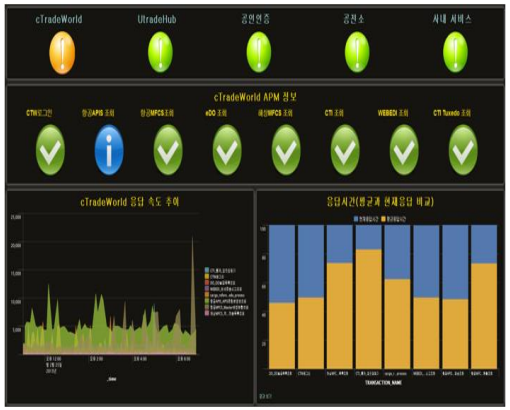
– REST API 연동을 통한 Dashboard 생성
외부 연동차트(예: 크리스탈리포트)의 원천데이터를 Splunk WAS의
URL로 설정하고 REST API를 호출하면,
JSON/XML 형태의 원천데이터가 입수되어 지정한 차트의
UI/UX 표현이 가능함.

User Interface

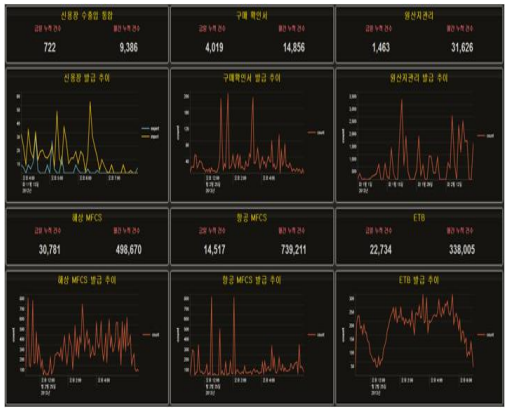
성능감시, 트래픽패턴 및 서비스 상황 등의 통합 UI 구성방안 제시



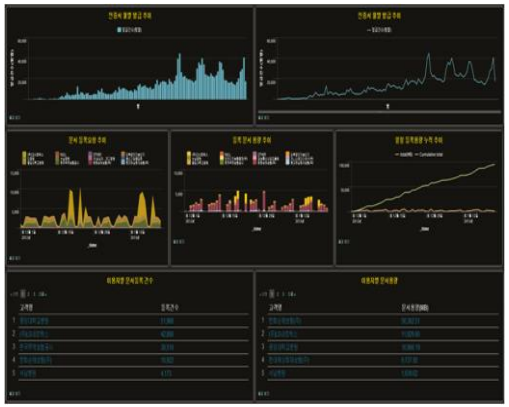
종합현황판



트래픽현황



서비스현황(전체)



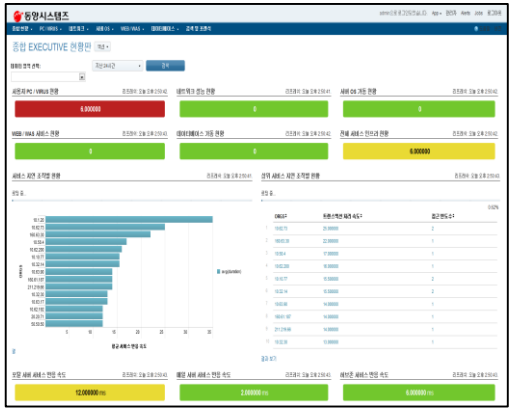
서비스현황(개별)

장애상황

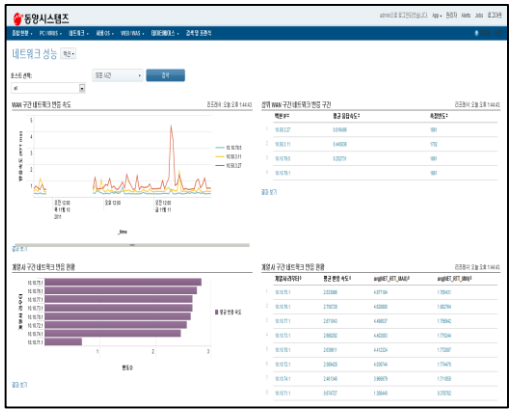
네트워크상황

User Interface

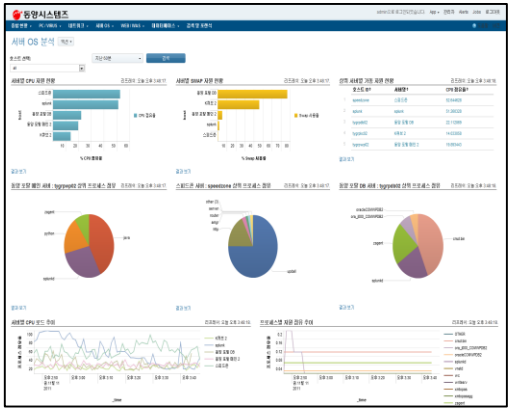
시스템 등의 인프라, 서비스 정보를 구성할 수 있는 구성관리 방안 제시



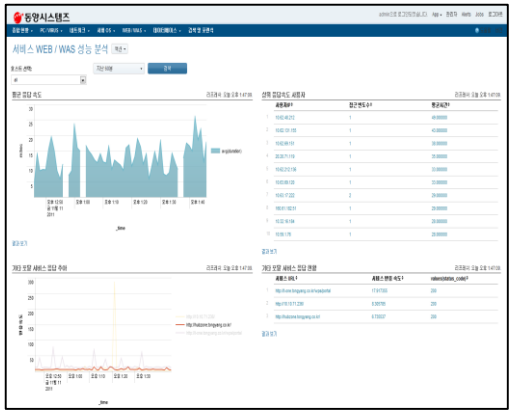
종합현황판



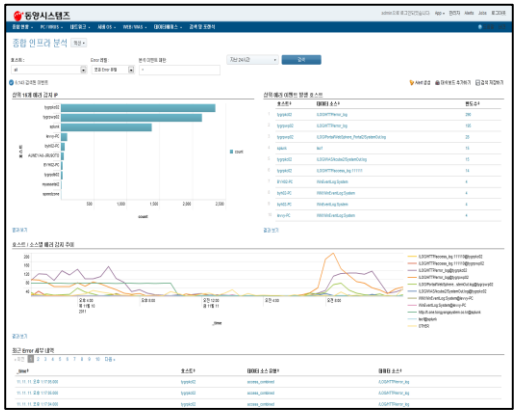
네트워크 성능관리



시스템성능 및 자원관리



서비스 WEB/WAS관리

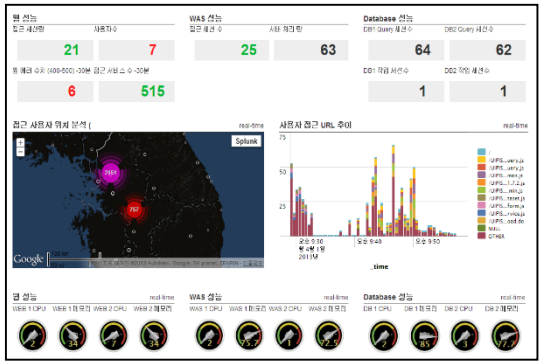


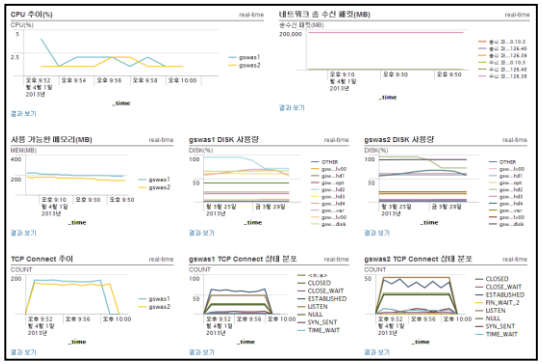
인프라 장애관리

4. 구축사례

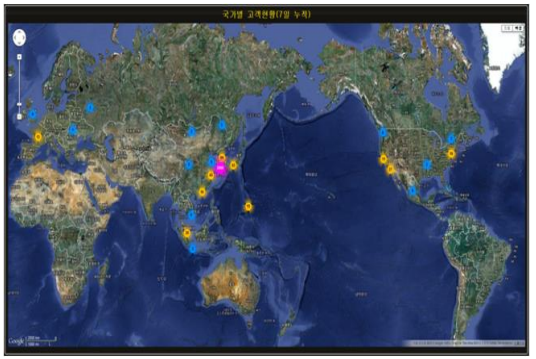
종합상황 인프라(Display) 구축사례

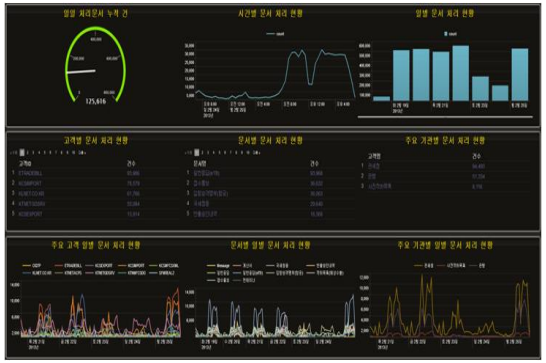
- 증권사, 인프라/서비스 통합관제





- 무역자동화, 인프라/서비스 통합관제





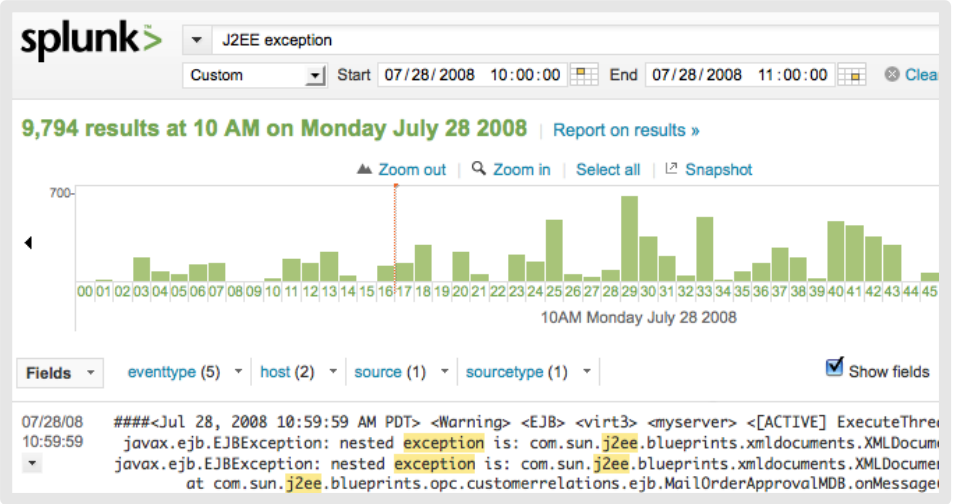
Service Desk 효율성 향상 – vodafone

- Dramatically improve Service Desk Effectiveness

vodafone

"Splunk reduced our escalations by 90% and our problem resolution time by 67%."

Paulo Carvalho
Director Operations



- Delivered rapid application troubleshooting and quality management of high-margin 3G services
- Enabled rapid error search across Java & J2EE infrastructure
- Provided service desk with required information quickly and improved customer satisfaction level

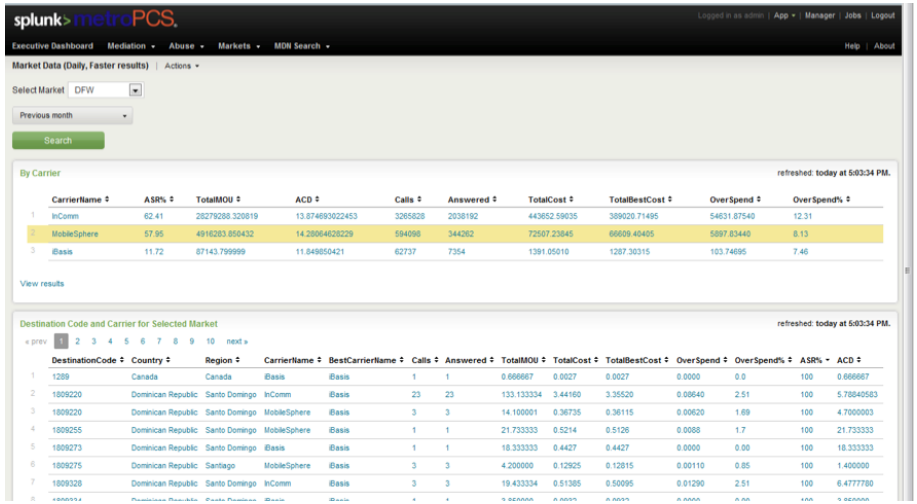
Telecom reference – metroPCS

- Telecom Call Revenue and Cost Analysis

metroPCS
Unlimit Yourself.

"With an implementation time of just a few weeks, Splunk surpassed all ROI expectations and has delivered millions of dollars in savings."

Gregg Woodcock
Corporate Engineering



- Lookup tariff data to calculate cost per call
- Ingest any CDR format and provide ARPU visibility
- Dashboards highlight 'terms of service' abusers

N/W Performance Management – Century Link

– 구축 필요성

급격한 가입자증가에 대한 관리

뛰어난 고객경험 제공

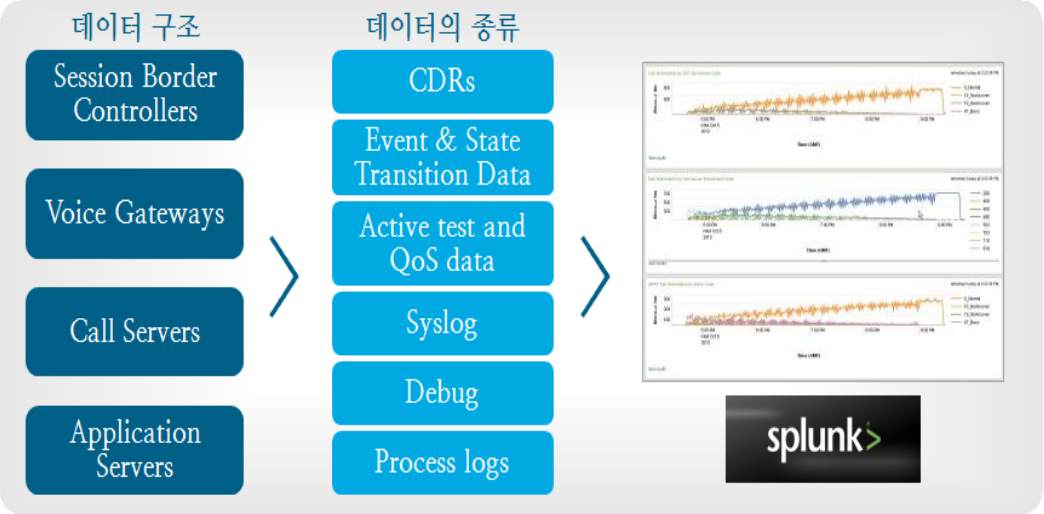
네트워크 운영효율성 향상

성능향상과 동시에 비용절감

네트워크 인프라의 추가수익

네트워크 성능관리
(네트워크데이터에 대한 가시성)

단기: VoIP 서비스에 적용
중기: 전 서비스영역으로 확대



국내 대용량 구축사례

국내 90여개사의 고객들이 Splunk를 사용하고 있으며 적용분야는 IT운영, 보안, application성능관리, 비지니스 분석등 다양한 사례로 실시간 분석 시스템 구축

2TB/day SAMSUNG ELECTRONICS	1.2TB/day HYUNDAI
.5TB/day Hana Financial Group	.3TB/day kt
~.2TB/day CJ O SHOPPING 현대중공업 HyundaiCard LG U+ SAMSUNG 삼성생명 NEXON	

IT 운영관리 proactive 모니터링/business 분석사례 – 삼성전자

- Splunk도입으로 Global service 품질 관리, 보장, 사업현황 실시간 분석

Ch@t ON

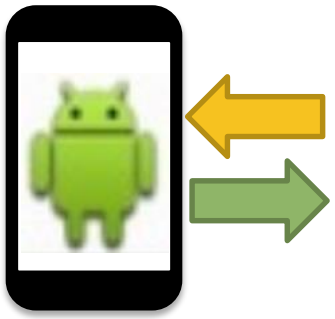
◇ 아이폰용 챗온

Chatting Service

S-Cloud

Multimedia Contents
Sharing Platform

SPP

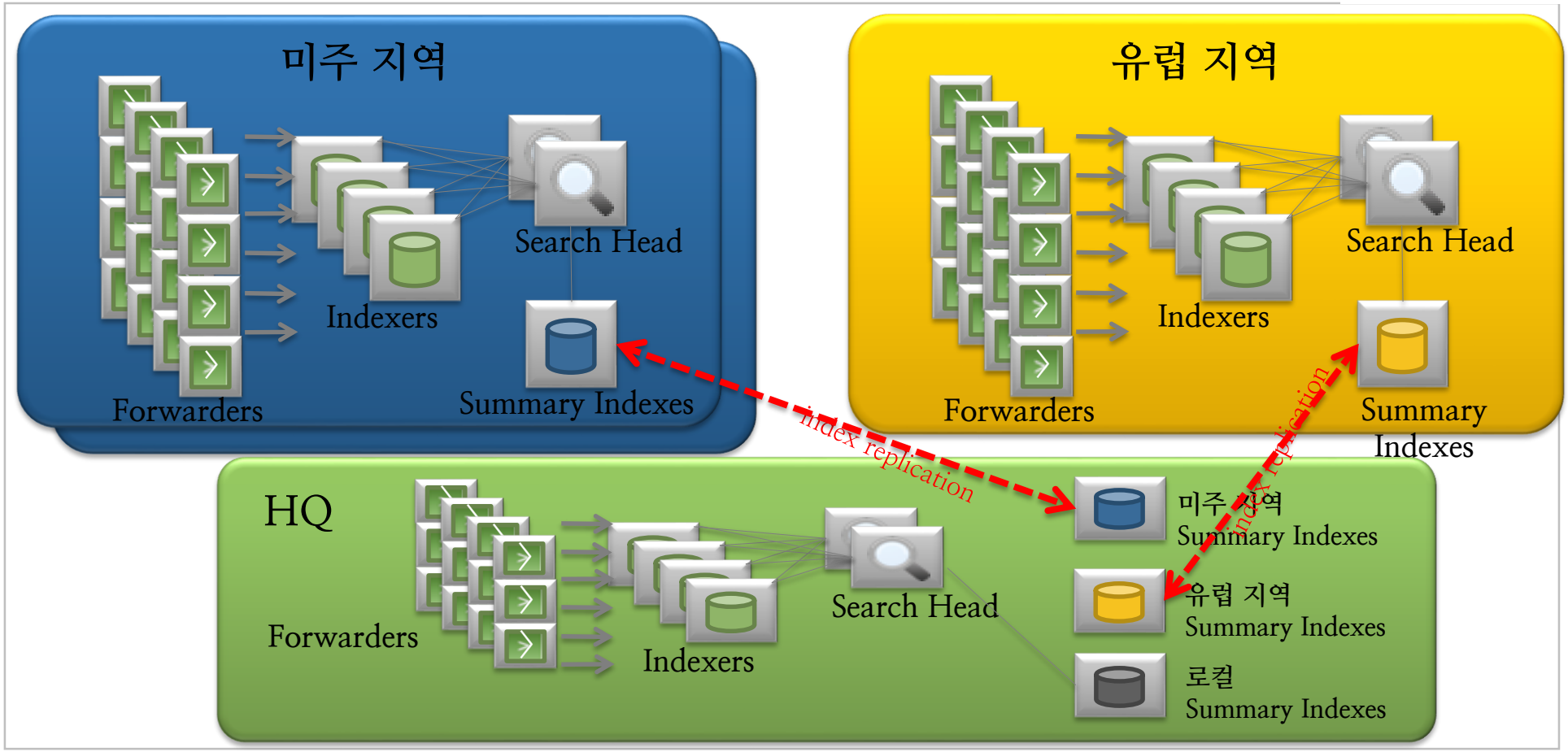


Message
Push Platform

전세계의 Smartphone, tabletPC, SmartTV사용자들을 위한 공통 서비스의 Global service상태 monitoring, 장애 파악 및 실시간 대응, 나아가 판매 현황 추이 등 실시간 파악, 영업 전략 수립

IT 운영관리 proactive 모니터링/business 분석사례 – 삼성전자

- 전세계 지역별 거점 IT Center 개별 운영, 통합 검색 지원



IT 운영관리 proactive 모니터링/business 분석사례 – 삼성전자

- 도입효과 분석

Before

- **장애 분석**
  Global IDC에서 운영되는 network, server, application등에서 발생되는 문제로 인하여 장애 발생시 개별 시스템별로 관리하여 통합분석 불가. 결과적으로 원인 파악없이 종료
- **장애 조치**
  통상 원인 파악이 되지 않는 경우가 많으므로 재기동과 같은 방식으로 장애 조치시간을 줄이는 데 주력.
- **서비스 품질관리**
  서비스 지표의 중요성에 대한 분석이 불가한 상황 하에서 관리해야 할 지표가 확실하지 않아 전체 SLA에 대한 관리에 어려움이 크

After

- **장애 분석**
  장애의 원인이 되는 모든 장비, application등에서 상태를 모니터링할 수 있는 데이터를 실시간으로 수집, indexing하여 장애 시점을 기준으로 각 데이터들간의 상관관계분석을 통해 원인의 체계적 분석 가능
- **장애 조치**
  장애분석에 따라 root cause에 대해서 효과적며 빠른 조치가 가능해져 장애 대응시간을 획기적으로 개선함
- **서비스 품질관리**
  서비스 품질에 관련있는 지표들의 현황에 대해 통찰력을 갖게 됨으로써 서비스 추이에 대한 적극적인 예측이 가능하고 품질개선을 위한 사전 대응이 가능해 짐

IT 운영관리 proactive 모니터링/business 분석사례 – 삼성전자

- 구축 시간 및 운영 인력/비용

Before

- **구축 비용**
  DB, WAS, APM, DW등 많은 종류의 솔루션을 필요로하여 전체 구축비용이 커서 구축을 위한 예산 확보에 어려움이 큼
- **구축 시간**
  다양한 솔루션들을 결합하여 SI성격으로 구축해야 하므로 많은 인력과 시간이 필요함. 최소 20명 이상 6개월이상 소요
- **운영인력/비용**
  많은 이기종 솔루션에 대한 관리인원을 확보해야 하며 전문성확보에 어려움이 큼. 각 솔루션별 전문운영관리인원이 필요하므로 운영비용이 커지는 문제

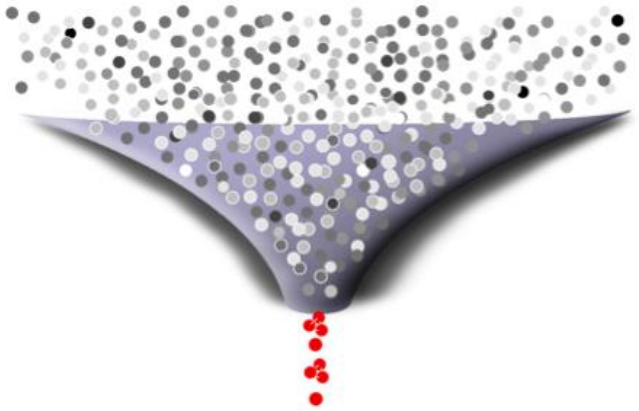
After

- **구축 비용**
  단일 솔루션을 end-to-end구축이 가능하므로 비용의 효율화
- **구축 시간**
  End-to-End 솔루션으로 구축하고 필요한 dash board등의 생성이 간단하여 요구사항분석, 시스템 아키텍처설계 후 구축까지 3개월 소요
- **운영인력/비용**
  운영인력의 관점에서 search processing language 작성과 데이터관리 인력의 최소화로 운영비용을 획기적으로 줄일 수 있음

보안관리 및 침입탐지분석사례 – 현대자동차

- 기존 SIEM솔루션의 취약점을 해결하여 강력한 보안 인프라 구현

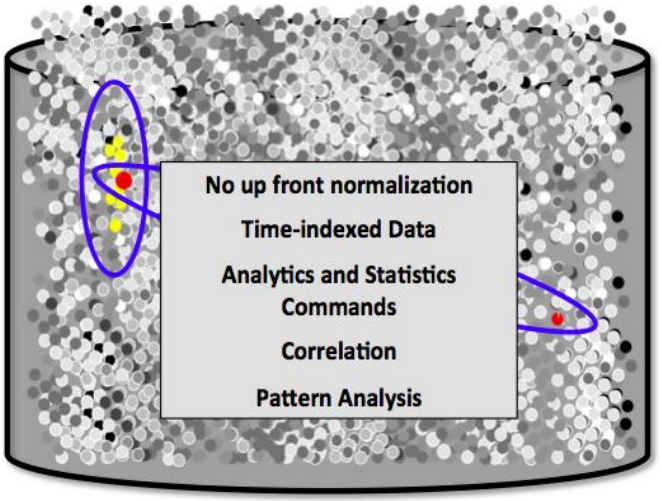
Traditional SIEM



Data Reduction Model

VS.

Splunk

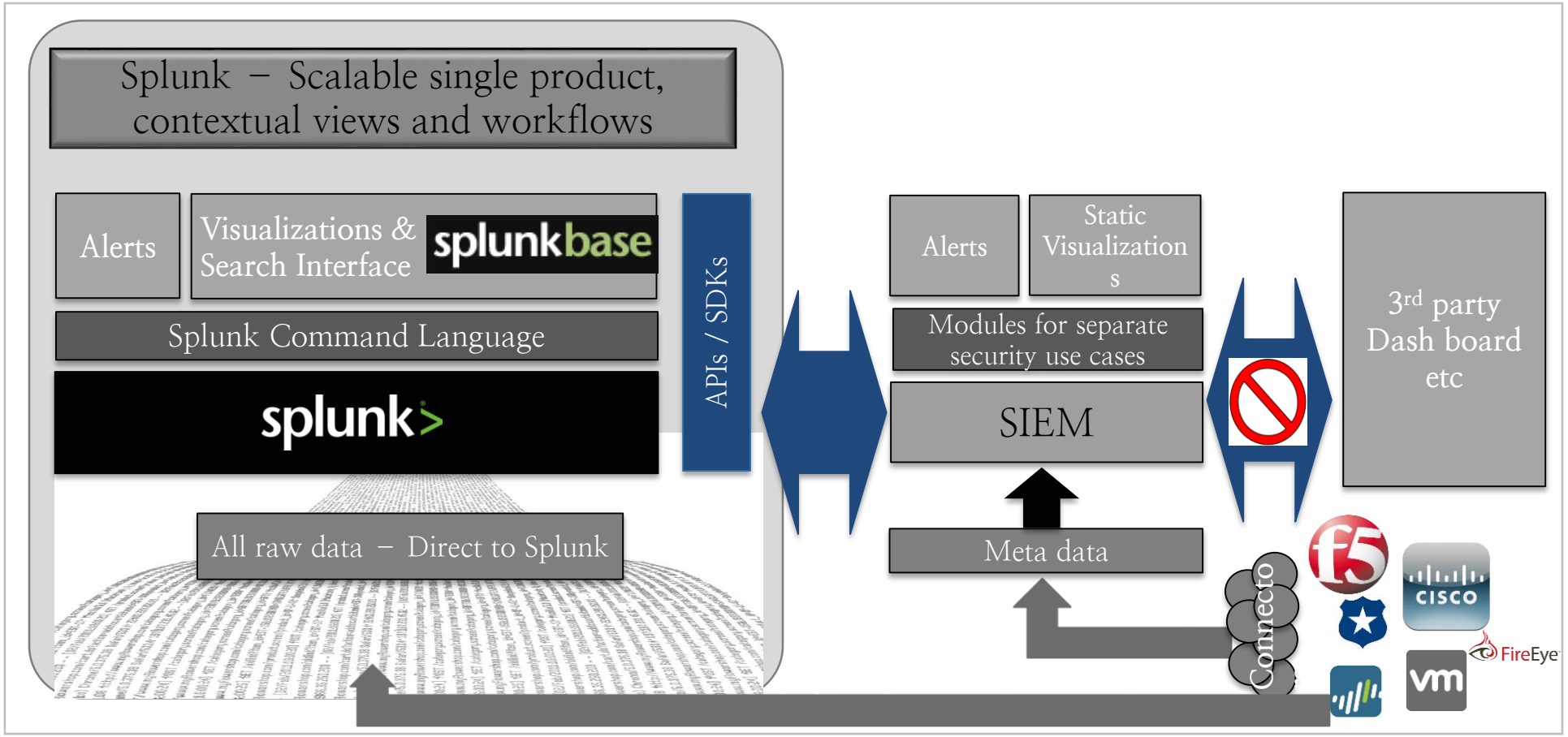


Data Inclusion Model

기존의 전통적인 SIEM제품인 Arcsight를 활용한 전사적 보안운영을 하는 상황에서 data reduction model로 인하여 발생할 수 밖에 없는 보안의 취약점을 극복하기 위해 SIEM제품의 log와 다른 데이터를 함께 분석하여 보안 시스템의 완결성 제고

보안관리 및 침입탐지분석사례 – 현대자동차

- 전통적인 SIEM제품을 활용하는 경우는 Connector개발로 인한 비용과 시간의 제약발생, Splunk는 Agent/Agentless모두 가능하여 비용절감
- 전통적인 SIEM제품의 자체log를 통합 분석가능하며 SDK를 통한 UI통합 가능
- Scalability를 고려한 architecture



보안관리 및 침입탐지분석사례 – 현대자동차

- 다양한 종류의 보안 application, FW, security GW들로 부터 방대한 데이터를 실시간으로 수집, 분석하여 SIEM정보와 통합하는 platform

국내 구축사례


한국의료분쟁조정중재원
Korea Medical Dispute Mediation and Arbitration Agency
증앙선거관리위원회
대한민국해군
REPUBLIC OF KOREA NAVY
SAMSUNG
SAMSUNG SDS
LG U+
하나금융그룹
Hyundai Capital
관세청
KOREA CUSTOMS SERVICE
Hyundai Card
DAUM
KICT 한국건설기술연구원
KFDA 식품의약품안전청
hi-pass
한국도로공사
KISA
한국인터넷진흥원
KISTI 한국과학기술정보연구원
Korea Institute of Science and Technology Information
hynix
KERIS
한국교육학술정보원
olleh ucloud
CJ POWERCAST
kt powertel
MANDO
예금보험공사
KOREA DEPOSIT INSURANCE CORPORATION
한양대학교의료원
HANYANG UNIVERSITY MEDICAL CENTER
kt
기획재정부
MINISTRY OF STRATEGY AND FINANCE
국방과학연구소
Agency for Defense Development
HanbitSoft
한국교직원공제회
THE KOREAN TEACHERS' CREDIT UNION
KIER
한국에너지기술연구원
KOREA INSTITUTE OF ENERGY RESEARCH

5. 기대효과 및 예상 리스크

splunk>

MNL SOLUTION

도입 시 기대효과

도입 時 기대효과

관제 시스템 통합	적은 인력으로 유기적 원인 분석
대용량 데이터(40GB/day) 분산 처리	성능 저하 없음
새로운 시스템을 추가 라이센스 없이 즉시 수용 분석	추가 Agent 없이 즉시 수용 분석
신규 이슈 발생 시 맞춤형 관제 화면 변경	짧은 시간과 작은 비용으로 변경 적용
대용량 로그 파일 50% 데이터 압축	스토리지 비용 절감
추가 비용 없이 파일시스템 변경 이력관리 및 데이터 트랜잭션 관리	내부 보안 위배 추적 관리 가능 (농협사태)
작업 이력 관리	내부 감사 및 사고에 대한 명확한 원인 분석

예상 Risk

- Splunk 전담 담당자 부재

  간단한 교육으로 Splunk Head Search 및 Ad-Hoc Dashboard 생성이 쉽게 가능하지만,

  대부분 고객사 문제로 담당자가 미지정되어, 도입된 장비를 효과적으로 운용하지 못하는 경우가 자주 발생

- 가입자 증가에 따른 라이선스 갱신 이슈

  간단한 교육으로 Splunk Head Search 및 Ad-Hoc Dashboard 생성이 쉽게 가능하지만,

  대부분 고객사 문제로 담당자가 미지정되어, 도입된 장비를 효과적으로 운용하지 못하는 경우가 자주 발생

6. 예상 구축금액

예상 상세 견적

- 상세견적

단위:백만원, VAT별도

구분		모델	대수	단가	공급가
H/W	서버	Intel 2.5GHz 2P12C, 32GB MEM, 4.5TB * 2 HDD	2	18	18
S/W	Splunk	20GB Index volume Lic,	1	186	186
	컨설팅	데이터수집분석 및 컨설팅	2	16	32
	커스터마이즈	Splunk Operational Intelligence App SW Pack	1	40	40
	WAS/Dashboard	Formal Dashboard 개발 (기획/디자인/개발)	15	8	120
합계					396

7. 유지보수 계획

splunk>

MNL SOLUTION

유지보수 및 교육계획

- 유지보수

구분		Y+0	Y+1	Y+2	Y+3
H/W	서버	무상			공급가의 10%
S/W	Splunk	무상	공급가의 18%/년		
	컨설팅	업무량(M/M)에 따라 별도 산출			
	커스터마이즈	업무량(M/M)에 따라 별도 산출			
	WAS/Dashboard	무상	공급가의 12%/년		

- 시스템 교육계획

구분		정기	비 정기
H/W	서버	무상	인수 시 1회 (0.5 일, 집체교육)
S/W	Splunk	정기교육 (1회/월, 교육장)	인수 시 1회 (2일. 집체교육)
	WAS/Dashboard	정기교육 (1회/분기, 지정장소)	인수 시 1회 (1일, 집체교육)

향후 KCT 인프라 증설/추가 時 지원계획

구분		증설/추가
H/W	서버	18백만원/대
S/W	Splunk	아래 인덱스 볼륨 別 라이스센스 참조
	컨설팅	16백만원/월, 업무투입량(M/M) 별도 산출
	커스터마이즈	40백만원 (1.5개월투입기준), 업무투입량(M/M) 별도산출
	WAS/Dashboard	업무투입량(M/M) 별도산출

인덱스 볼륨 사이즈	라이선스가격 (단위: 백만원, 부가세별도)	비고
1GB	32	
2GB	58	
5GB	89	
10GB	130	
20GB	186	
50GB	279	
100GB	356	
200GB	587	
500GB	1123	
1TB	1571	

감사합니다.