



Beats & X-Pack

오늘의 학습내용

- 데이터 수집
- Beats 제품군
- X-Pack

▲ 데이터수집

■ 데이터 수집

❖ 데이터 수집 플로우

데이터 소스 선정

- 분석 목적에 따라 데이터 소스를 선정
- 수집 가능 여부 점검 및 세부 목록 작성

세부 계획 수립

- 데이터 소스별 데이터 소유 기관 점검 (데이터 소유권 및 개인정보)
- 소스별 데이터 유형 및 특징 분석
- 수집 기술과 수집 주기 선정

수집 시행

- 사전 테스트 → 수집 진행 → 유출방지 및 업무 지침
- 장애점검/품질향상

▶ 데이터수집

■ 데이터 수집

❖ 데이터 수집 기술

Crawling	- SNS, 뉴스, 웹 정보 등 웹상에서 제공되는 문서 및 정보 수집
FTP	- TCP/IP 프로토콜을 활용하는 인터넷 서버로부터 파일 송수신
Open API	- 서비스, 정보, 데이터 등을 이용할 수 있는 Open API 기반 수집
RSS	- Really Simple Syndication - XML 기반 콘텐츠 배급 프로토콜
Streaming	- 인터넷 기반 음성, 오디오, 비디오 데이터 실시간 수집
Log Aggregator	- 웹 서버 로그, 웹 로그 등 각종 로그 데이터 수집
RDB Aggregator	- RDBMS의 정형 데이터를 HDFS나 NoSQL 전송

◆ Beats 제품군

■ Elastic Beats

- ❖ Elastic Beats는 데이터를 편리하게 Elasticsearch Service로 전송할 수 있게 해주는 경량 데이터 수집기 세트
- ❖ IoT 장치, 에지 장치 또는 포함된 장치 등 하드웨어 리소스가 제한되어 있는 장치에서 데이터를 실행하고 수집 가능
- ❖ Beats는 리소스를 많이 사용하는 데이터 수집기를 실행해야 할 필요 없이 데이터를 수집해야 하는 경우 이상적
- ❖ 네트워크로 연결된 모든 장치에서 이런 종류의 전반적인 데이터 수집을 하면 시스템 전체에 걸친 문제와 보안 사고를 신속하게 탐지하여 대응

◆ Beats 제품군

■ Beats 제품군 I

Filebeat

- 파일 형식으로 제공되는 소스로부터 데이터를 읽고, 전처리하고, 수집
- 모든 종류의 년바이너리 파일 형식이 지원
- Filebeat는 TCP/UDP, 컨테이너, Redis, Syslog 등 수많은 다른 데이터 소스를 지원
- 풍부한 모듈 덕분에 Apache, MySQL, Kafka 등과 같은 일반적인 애플리케이션을 위한 로그 형식 수집과 구문 분석 가능

Metricbeat

- 시스템과 서비스 메트릭을 수집하고 전처리
- 시스템 메트릭에는 프로세스 실행에 대한 정보와 CPU / 메모리 / 디스크 / 네트워크에 대한 정보가 포함
- 모듈은 Kafka, Palo Alto Networks, Redis 외에도 여러 가지를 포함한 수많은 다른 서비스로부터 데이터를 수집하기 위해 제공

◆ Beats 제품군

■ Beats 제품군 II

Packetbeat

- 라이브 네트워크 데이터를 수집하고 전처리
- 애플리케이션 모니터링과 보안, 네트워크 성능 분석 등이 활성화
- Packetbeat는 HCP, DNS, HTTP, MongoDB, NFS, TLS 등의 프로토콜을 지원

Winlogbeat

- 애플리케이션 이벤트, 하드웨어 이벤트, 보안 및 시스템 이벤트 등 Windows 운영 체제로부터 이벤트 로그를 캡처하는 작업을 수행
- Windows 이벤트 로그로부터 제공되는 방대한 정보는 수많은 사용 사례에 대해 유용하게 사용

◆ Beats 제품군

■ Beats 제품군 III

Auditbeat

- 중요한 파일에 이루어지는 변경사항을 탐색하고 Linux Audit Framework로부터 이벤트를 수집
- 여러 다른 모듈이 배포를 용이하게 해주며, 이것은 대부분 보안 분석 사용 사례에서 사용

Heartbeat

- 검색을 사용해 시스템과 서비스의 가용성을 모니터링
- Heartbeat는 따라서 인프라 모니터링과 보안 분석 등과 같은 수많은 시나리오에서 유용
- 지원되는 프로토콜은 ICMP, TCP, HTTP

Functionbeat

- AWS Lambda와 같은 서버리스 환경 내에서 로그와 메트릭을 수집

X-Pack

X-Pack 개요

- ❖ 보안, 알림, 모니터링, 보고, 그래프 기능, 머신러닝 기능을 설치하기 편리한 단일 패키지로 번들 구성한 Elastic Stack 확장 프로그램
- ❖ X-Pack 구성 요소는 서로 원활하게 연동할 수 있도록 설계되었지만 사용할 기능을 손쉽게 활성화하거나 비활성 가능
- ❖ X-Pack 은 Elasticsearch와 Kibana에 single pack 으로 설치하여 기존 Elastic Stack과 쉽게 통합 가능

X-Pack

X-Pack 개요

- ❖ Security : 사용자/권한 기반의 인증 및 통신 암호화 기능을 제공
- ❖ Alerting : 쿼리 기반의 자동 알림 기능을 제공
- ❖ Monitoring : ES 클러스터의 상태 모니터링 기능을 제공
- ❖ Graph : 관계도 분석 기능을 제공
- ❖ Reporting : Kibana 대시보드를 PDF로 내려 받거나 데이터를 CSV 파일로 저장
- ❖ Machine Learning : 시계열 데이터 기반의 실시간 이상징후 탐지 기능을 제공

X-Pack

X-Pack 개요



X-Pack

Extensions for the Elastic Stack



Security



Alerting



Monitoring



Graph



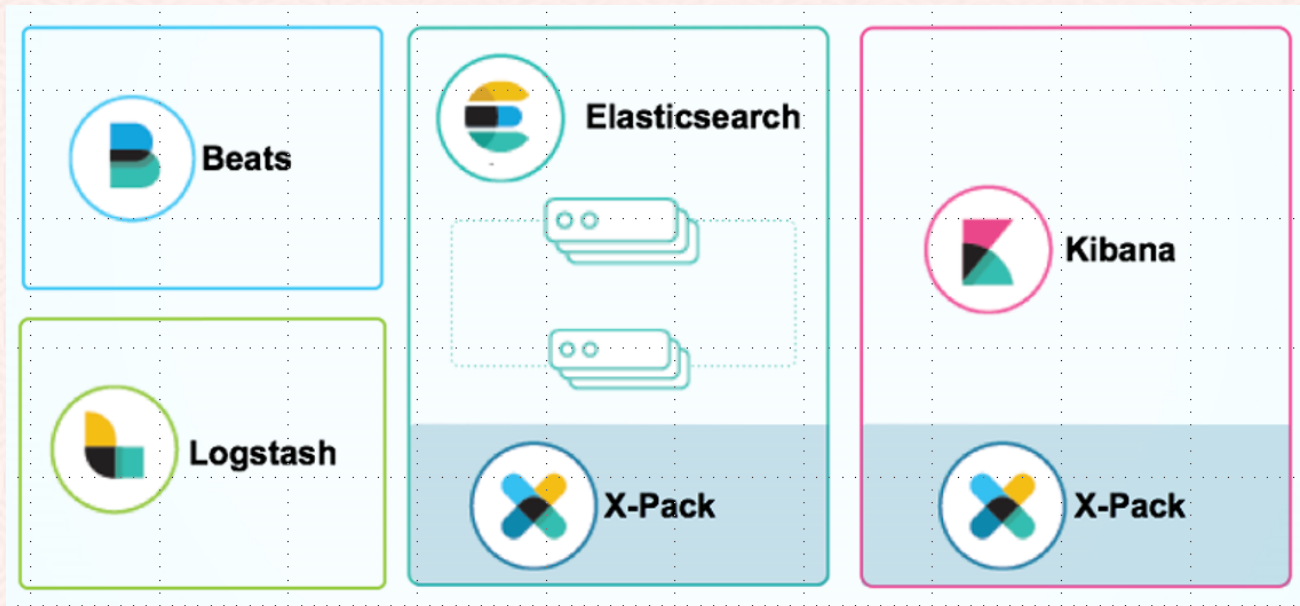
Reporting



Machine
Learning

◆ X-Pack

■ X-Pack 통합



X-Pack


모니터링

- ❖ Elasticsearch, Logstash, Kibana에 install X-Pack할 때 자동으로 Monitoring이 활성화
- ❖ 기본적으로 Elasticsearch의 모니터링 에이전트는 동일한 클러스터 내의 데이터를 색인화
- ❖ Elasticsearch, Logstash, Kibana의 상태 및 성능 모니터링





모니터링


❖ Elasticsearch 클러스터 모니터링

 Clusters
elasticsearch


10 seconds < Last 1 hour >

 Your Trial license will expire on June 1, 2017.

 Top Cluster Alerts

 Elasticsearch cluster status is yellow. [Allocate missing replica shards.](#)
May 3, 2017 4:57:58 PM

[View all alerts](#)

 Elasticsearch


Health: ● Yellow

[Overview](#)

Version: 5.4.0
Uptime: 6 hours

[Nodes: 1](#)
Disk Available: 308GB / 465GB (66.22%)
JVM Heap: 41.67% (826MB / 2GB)

[Indices: 12](#)
Documents: 39,653
Disk Usage: 20MB
Primary Shards: 12
Replica Shards: 0


 Kibana

Health: ● Green

[Overview](#)

Requests: 3
Max. Response Time: 39 ms

[Instances: 1](#)
Connections: 4
Memory Usage: 8.52% (122MB / 1GB)

 Logstash

[Overview](#)


Events Received: 4
Events Emitted: 4

[Nodes: 1](#)
Uptime: 2 minutes
JVM Heap: 6.73% (67MB / 990MB)



모니터링


❖ Elasticsearch 노드 모니터링

 **kibana**


Clusters / monitoring-cluster / Elasticsearch

10 seconds ◀ Last 1 hour ▶

Overview Indices Nodes

 Nodes: **1** Indices: **9** Memory: **355MB / 2GB** Total Shards: **17** Unassigned Shards: **8** Documents: **18,775** Data: **9MB** Uptime: **3 hours** Version: **5.2.0**

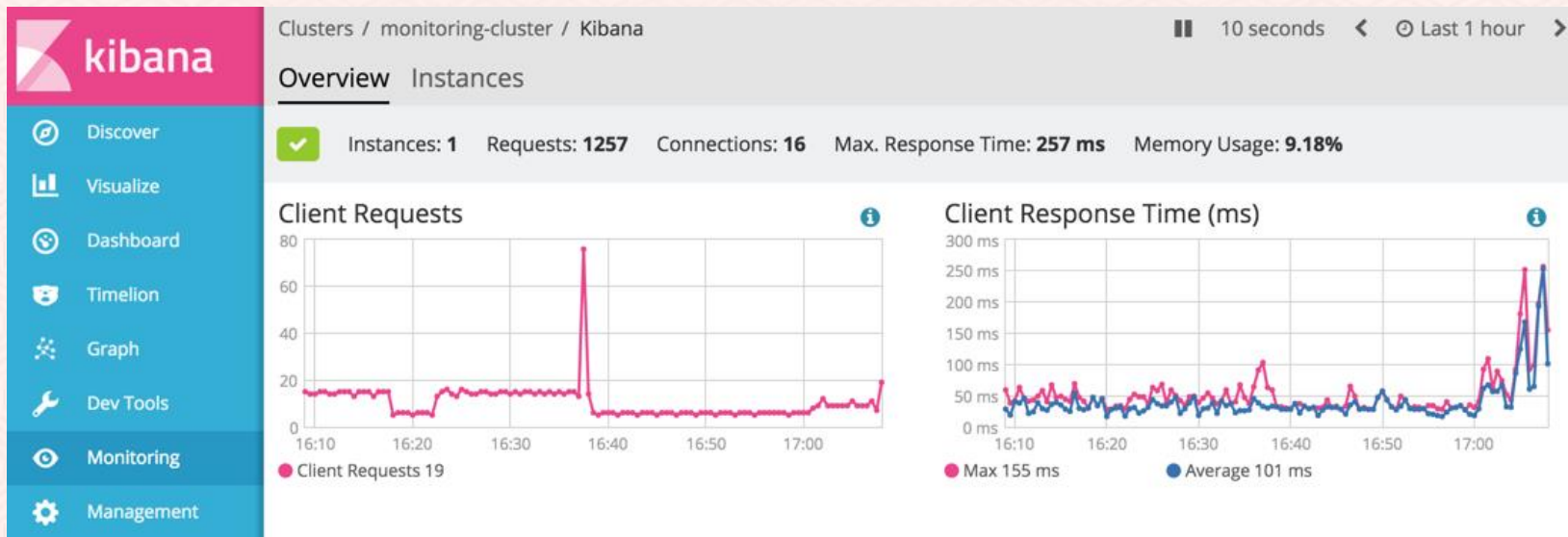
Nodes 1 of 1

Name	Status	CPU Usage	Load Average	JVM Memory	Disk Free Space	Shards
★ u1eT8aY 172.30.0.57:9300		0.33 % ↑ 2 % max 0 % min	0 ↓ 0.27 max 0 min	19 % ↑ 23 % max 14 % min	640.4 MB ↓ 663.7 MB max 640.4 MB min	9



모니터링

❖ Kibana 모니터링





모니터링

❖ Logstash 모니터링

