



로그 수집 (ELK)

이노베이션 아카데미
인턴 장준영

01.로그를 수집하는 이유

개발 영역

- 버그 혹은 크래시율 수집 및 상시 트래킹
- 이슈 발생 후 롤백 및 대응 등에 대한 판단의 근거로 활용
- 특정 기능에 대한 사용성 진단

마케팅 영역

- 마케팅 채널별 ROI 진단 및 비용 최적화
- 배너/프로모션/이벤트 효과 측정
- 유저 Segmentation, Targeting

기획/디자인 영역

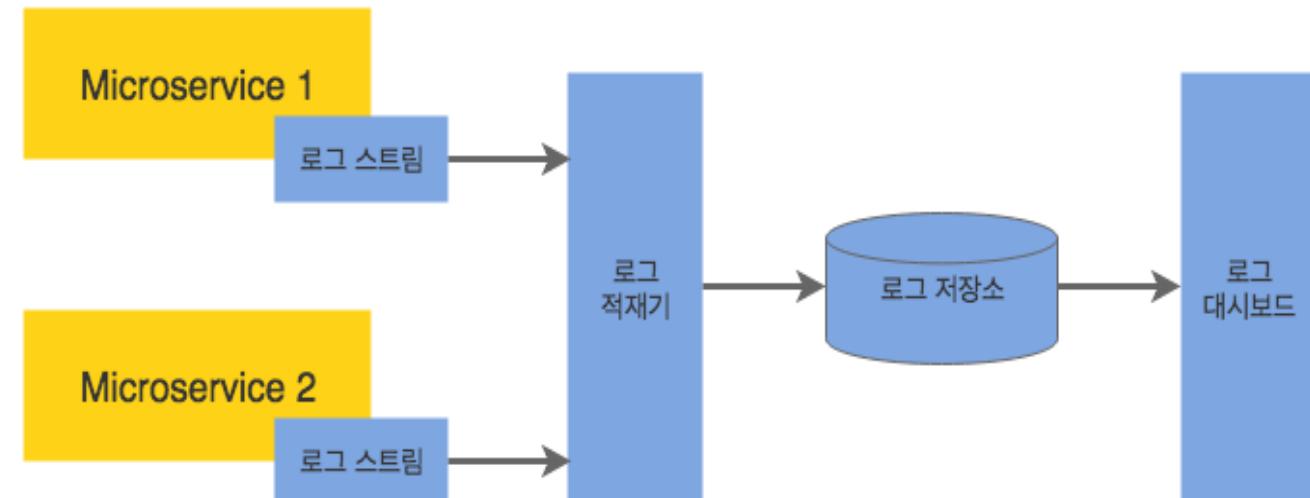
- 시나리오/기능/디자인에 대한 성과 측정 및 개선 (A/B 테스트)
- 유저 Journey 경로 분석 및 이탈 구간 개선 (UX/UI 최적화)
- 유저 Persona 구축 (with 리서치) 및 신규 기능 Ideation



02. 로그를 수집하는 방법

· 중앙 집중형 로깅

- 로그 스트림: 로그 생성자가 만들어내는 로그 메세지의 스트림
- 로그 적재기: 로그 메세지를 여러 다른 종단점으로 메세지를 전송
Ex) **Logstash**, Fluentd
- 로그 저장소: 로그 메세지를 저장을 위한 대용량 데이터 저장소
Ex) HDFS, **Elasticsearch**, NoSQL
- 로그 대시보드: 로그 분석 결과를 시각화함
Ex) **Kibana**, Graphite



03. ELK란?



영어사전 단어·숙어 1-5 / 196건

[elk](#) 미국·영국 [elk] 영국식

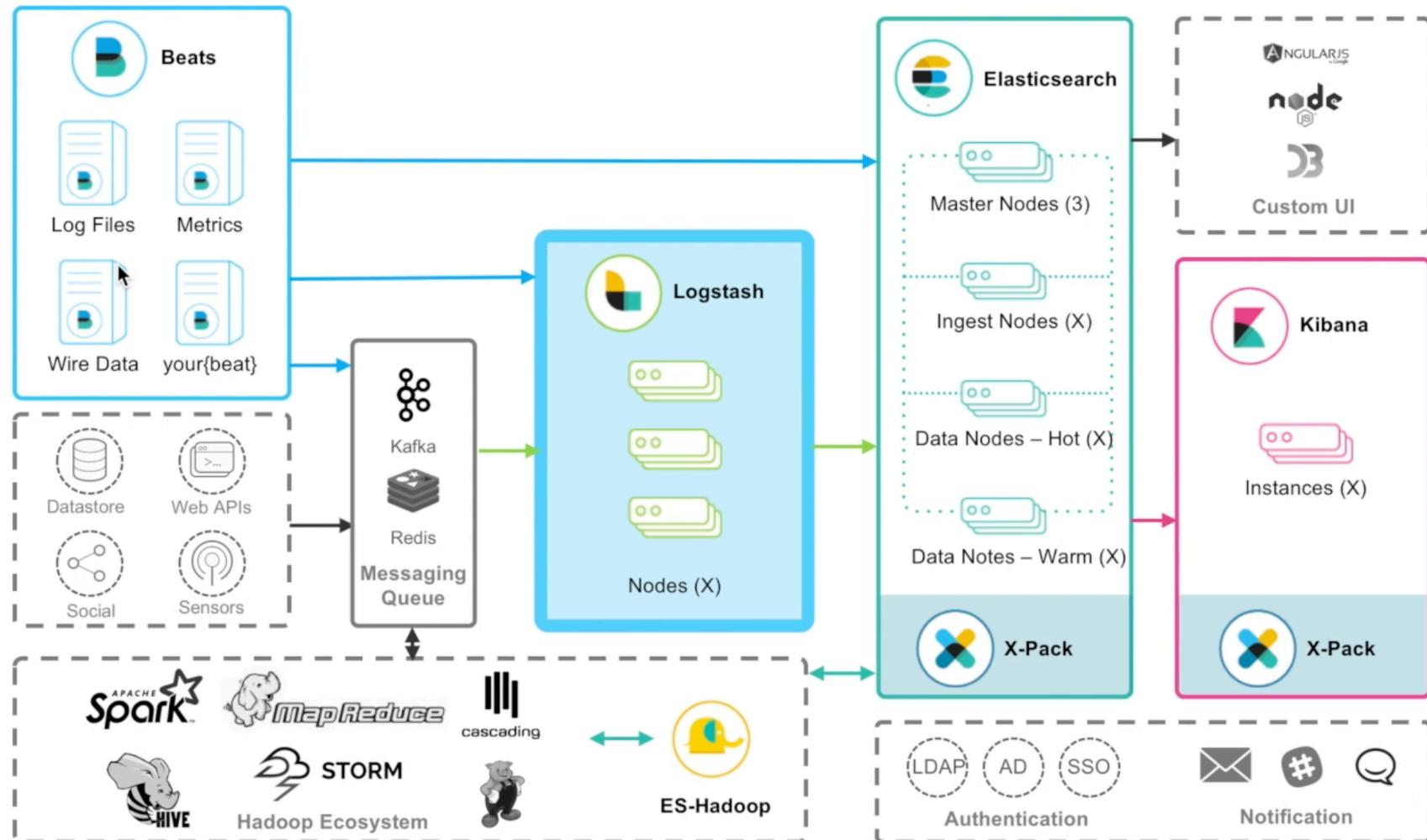
1. 엘크(북 유럽이나 아시아에 사는 큰 사슴. 북미에서는 moose라고 함)
2. = wapiti
3. 엘크스회(the Benevolent and Protective Order of Elks) 회원



Innovation Academy

03. ELK란?

The Journey of an Event



Innovation Academy

번외. ELK 왜 알아야 하는가?

saramin 직업별

지역별 직업별 HOT100 큐레이션 공채 기업연구소 짜검색 ELK  로그인하세요 회원가입

직업별

경영·사무
영업·고객상담
IT·인터넷
디자인
서비스
전문직
의료
생산·제조
건설
유통·무역
미디어

직업별(직종)

경력 선택 ▾ 학력 선택 ▾

직업 선택  지역 선택  검색어 입력  상세조건 

직업(직종)명 입력 

나의 검색/메일관리 

주요기업 합격자소서 확인 



Innovation Academy

번외. ELK 왜 알아야 하는가?

티몬

채용공고
검색 개발자

티몬의 쇼핑타임을 이끌어갈 인재를 찾습니다.

IT

담당업무

검색 개발자

- 티몬 검색서비스 개발
- 검색 서비스 관련 API 개발 및 운영
- 검색 서비스 관련 어드민 개발 및 운영
- 티몬 검색 자연어 처리 개발

자격요건

- 학력/전공 : 무관
- 경력/연차 : 관련 경력 3년 이상
- Git 사용 경험자
- Java 및 Spring 환경에서 개발 경험이 있으신 분
- Maven 활용 경험이 있으신 분

제출서류

- 온라인 입사 지원서

제출방법

- 온라인 입사 지원서 작성 및 최종 입사지원

유의사항

온라인 입사지원서 작성 후 최종 입사지원 버튼을 누르지 않으면 접수되지 않습니다. 최종 입사지원 후에는 입사 지원서 수정이 불가능니 유의하시기 바랍니다.

▶ **비데이터 로그 수집 및 분석 시스템 개발 경험자 (Fluentd, ELK, Kafka, Spark 등)**

모집부문

위메프

모집부분	담당업무	자격요건 및 우대사항	인원
SE	<ul style="list-style-type: none">- 개발/배포/운영 과정을 개선할 수 있는 플랫폼 개발 및 운영- 서비스의 신뢰성, 신속한 개발을 지원하는 플랫폼 확보- Cloud native 환경에서 빌드/테스트/배포 자동화- 서비스 및 인프라 자원 시스템 구축 및 운영- 서비스 및 인프라 로깅, 모니터링 시스템 구축 및 운영- MSA 환경에서의 configuration management	<p>[자격요건]</p> <ul style="list-style-type: none">- 5년이상 AWS 클라우드 아키텍처 구성 및 운영 경험이 있으신 분- 코드로 개발 플랫폼 환경을 구축하고 운영 경험이 있으신 분- php, java 중 하나에 능숙하신 분- AWS 환경에서 CI/CD 구축 및 운영 경험이 있으신 분- Docker/Container 기반의 서비스 운영환경에 이해가 높으신 분- 대규모의 분산환경에서 ELK 기반 logging, metric <p>[우대사항]</p> <ul style="list-style-type: none">- ISMS 대응 시스템 환경 및 운영 경험이 있으신 분- 컨테이너 기반의 플랫폼 환경 구축 및 운영을 해보신 분- 동시 접속량이 많은 서비스를 위한 분산 처리 아키텍처에 대한 경험이 많으신 분- 성능 최적화와 운영 자동화를 위한 지속적인 노력을 하시는 분- 원활한 커뮤니케이션 스킬을 갖추신 분 <p>[전형절차]</p> <ul style="list-style-type: none">- 서류전형 > 1/2차면접> 레퍼런스 > 최종합격	0명



번외. ELK 왜 알아야 하는가?

쿠팡

[쿠팡페이] System Engineer 채용 - Fintech Infra

✓ 모집부문 및 상세내용

자격요건

System Engineer 경력 8년 이상

Python, Shell 프로그래밍 및 REST API 활용 경험

Ansible 을 활용한 Infrastructure as Code 구현 가능 및 경험

클라우드(Public/Private), On-Premise 인프라(시스템) 아키텍처 설계/구축/운영 경험

스토리지/백업(VTL, PTL) 구축 및 운영, 장애처리 경험

서버 표준화 및 보안 정책 적용 경험

H/W 벤치마크 및 POC, 성능 관리 경험

RDBMS 운영 경험

인프라 모니터링 구축/운영 경험(zabbix, elk, grafana)

LDAP/DNS 구축/운영

카카오 게임즈

카카오게임즈는 카카오의 게임 전문 자회사로서, PC와 모바일, VR 등의 플랫폼을 아우르며 다양한 장르의 게임을 국내외 게임 시장에 서비스하는 글로벌 멀티플랫폼 게임 기업입니다.
일상의 모든 것이 게임이 되는 카카오게임즈에서 함께 끊임없이 도전하고 새로운 즐거움을 만들어 갈 크루를 찾고 있습니다.

◆ 직원 유형

정규직

◆ 조직소개

광고플랫폼팀에서는 카카오톡에서 진행하는 게임 광고의 효율 증대를 위한 광고 상품 서비스 개발을 진행하고 있으며 카카오톡, 광고주의 게임서버 등 연계서비스들과 주고받는 데이터를 안정적이고 신속하게 처리하는 시스템 개발 등 신규 서비스/플랫폼을 개발하며 다같이 성장하는 경험을 할 수 있습니다.

◆ 업무내용

- JAVA, Spring framework를 기반으로 광고 사업을 위한 상품을 개발, 운영
- 대용량 트래픽의 효율적 대응을 위해 RDBMS부터 NoSQL DB, Cache, MQ 등 적합한 기술을 검토하고 기존서비스 개선
- AWS의 여러 Feature를 활용하여 유연하고 탄력적인 시스템 아키텍처를 설계
- 안정적인 서비스 운영과 신속한 장애 대응을 위해 Prometheus, Grafana, ELK, Sentry 등 모니터링 시스템 구축 및 운영
- GCD와 Ansible을 활용한 시각적 통합과 자동화를 놓친 때는 개발과 DevOps를 결합
- 자유로운 분위기 속에서 새로운 기술이나 아이디어를 도입하기 위해 다양한 개발적 시도

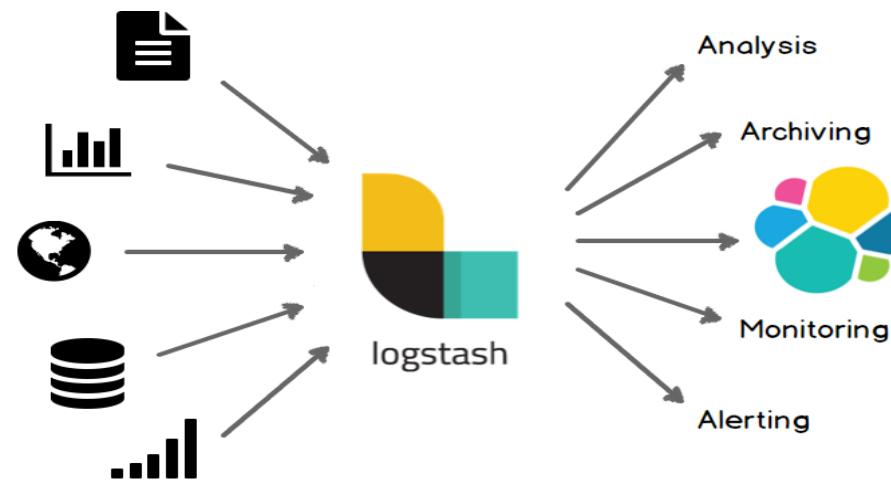


Innovation Academy

03. ELK란?

1) Logstash

- 실시간 파이프라인 기능을 가진 오픈소스 데이터 수집 엔진(Data flow 엔진)
- 다양한 데이터 접근 자원
- 서로 다른 소스의 데이터를 탄력적으로 통합하고 사용자가 선택한 목적지로 데이터를 정규화
- Elasticsearch 및 Kibana 시너지 효과를 발휘



03. ELK란?

1) Logstash 내부 파이프 라인

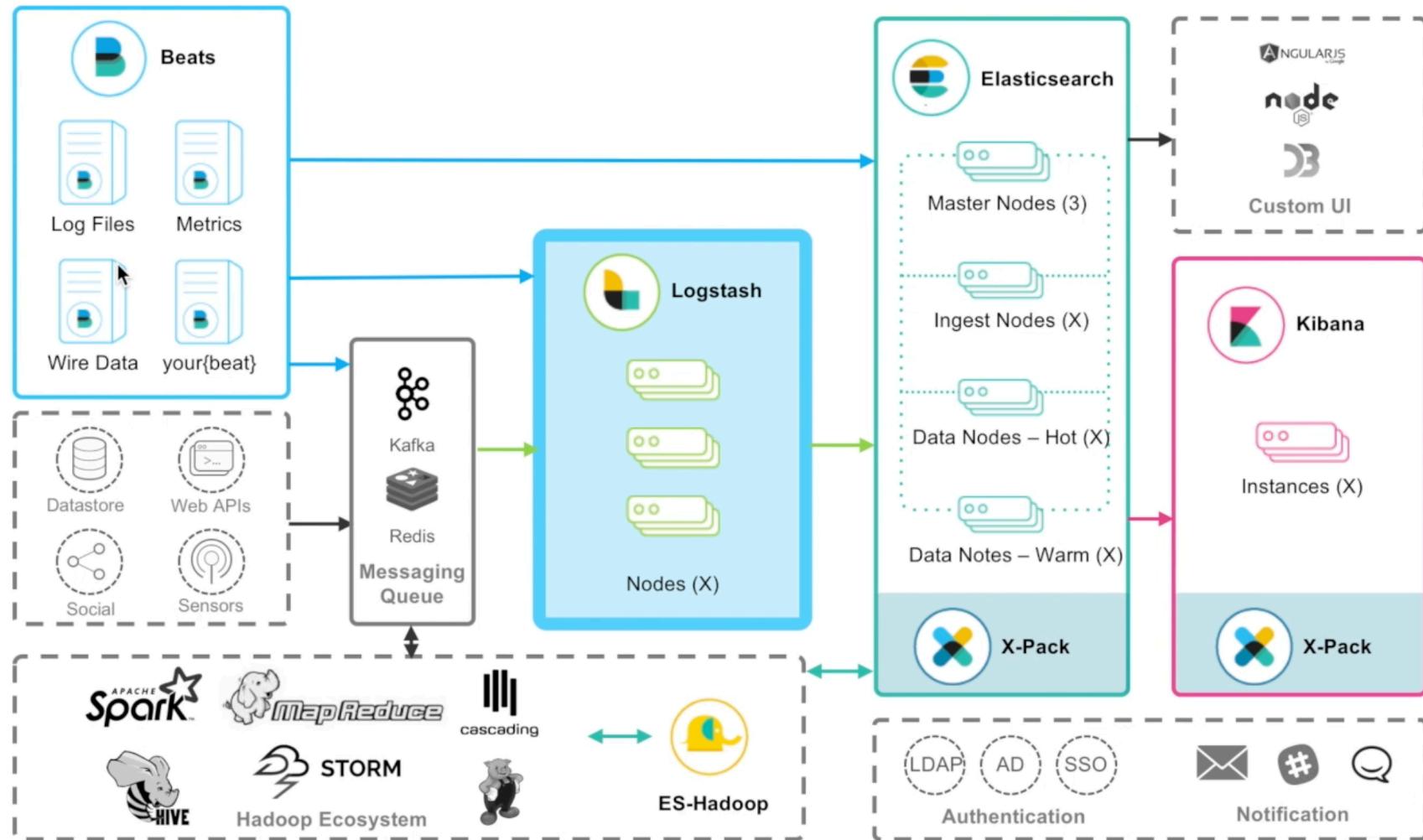


- **input**: 데이터가 유입되는 근원지 (어떤 것을 받을 것인지?)
 - HTTP REQUEST, Syslog, beats 등
- **filter**: 데이터에 변형을 가함 (log 파싱, 태그 추가)
 - log 파싱, 태그 추가 등
- **output**: 데이터를 전송할 목적지
 - s3, elasticsearch 등



03. ELK란?

The Journey of an Event



Innovation Academy

03. ELK란?

2) ElasticSearch

- 오픈소스 풀텍스트 검색 및 분석 엔진
- 방대한 양의 데이터를 신속하게, 거의 실시간으로 저장, 검색, 분석할 수 있도록 지원
- 가장 대중적인 엔터프라이즈 검색 엔진 Ex) Netflix, GitHub, Facebook
- (내부 구조나 동작 원리는 추후에 따로 설명하겠습니다.)



Innovation Academy

03. ELK란?

Q Elasticsearch는 완전 무료인가요?

&

A Elasticsearch 를 비롯한 Kibana, Logstash, Beats 등 모든 Elastic Stack 제품은 Apache 2.0 라이센스를 따르는 오픈소스이며 기능과 사용 범위에 아무런 제한이 없고 비용이 들지 않습니다.

Q Elasticsearch는 주로 어디에 쓰이나요?

&

A Elasticsearch는 검색엔진이지만 대부분 형태의 데이터를 모두 처리할 수 있어 로그분석, 위치정보 분석 등 다양한 용도로 활용됩니다. 금융, 보안, 게임, 쇼핑, 의료 등 거의 모든 산업 분야에서 사용되고 있으며, 자세한 사례는 <https://www.elastic.co/use-cases> 에서 확인이 가능합니다.

Q Elasticsearch 에서 한글로도 검색이 가능한가요?

&

A 한글을 활용하기 위해서는 한글 형태소 분석기를 별도로 설치해야 합니다. 아리랑, 은전한닢 등의 한글 형태소 분석기의 사용이 가능하며 해당 홈페이지 또는 커뮤니티를 통해 제공받아 설치해야 합니다.



03. ELK란?

Stream Settings Alerts ▾

Search for log entries... (e.g. host.name:host-1)

Customize Highlights Last 1 day Show dates Stream live

Jul 23, 2020	event.dataset	Message
15:28:26.000	nginx.access	[nginx][access] 121.135.181.35 - "GET /styleheets/main.css HTTP/1.1" 304 0
15:28:28.000	system.syslog	2020-07-23T06:28:28.535Z#011INFO#011[monitoring]#011log/log.go:145#011Non-zero metrics in the last 30s#011("monitoring": {"metrics": {"beat": {"cpu": {"system": {"ticks": 388, "time": {"ms": 10}}, "total": {"ticks": 1300, "time": {"ms": 17}}, "value": 1300}, "user": {"ticks": 920, "time": {"ms": 7}}}, "handles": {"limit": {"hard": 4096, "soft": 1024}, "open": 12}, "info": {"ephemeral_id": "b5a15397-7fce-453c-b9ff-cdda3e986a64", "uptime": {"ms": 2010069}}, "memstats": {"gc_next": "9623808", "memory_alloc": 8789040, "memory_total": 153740184, "rss": 6963200}, "runtime": {"goroutines": 91}}, "filebeat": {"events": {"added": 37, "done": 37}, "harvester": {"open_files": 4, "running": 4}}, "libbeat": {"config": {"module": {"running": 0}, "reloads": 3}, "output": {"events": {"acked": 37, "batches": 4, "total": 37}, "read": {"bytes": 1623}, "write": {"bytes": 46911}}, "pipeline": {"clients": 10, "events": {"active": 0, "published": 37}, "total": 37}, "queue": {"acked": 37}}}, "registrar": {"states": {"current": 9, "update": 37}}, "writes": {"success": 4, "total": 4}), "system": {"load": {"l": 0.66, "l5": 0.07, "l15": 0.21}, "norm": {"l": 0.66, "l5": 0.07, "l15": 0.21}}})}}
15:28:33.689		121.135.181.35 - [23/Jul/2020:06:28:25 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.89 Safari/537.36"
15:28:33.689		121.135.181.35 - [23/Jul/2020:06:28:26 +0000] "GET /images/ssafy.png HTTP/1.1" 304 0 "http://52.207.287.1/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.89 Safari/537.36"
15:28:33.689		121.135.181.35 - [23/Jul/2020:06:28:26 +0000] "GET /styleheets/main.css HTTP/1.1" 304 0 "http://52.207.287.1/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.89 Safari/537.36"
15:28:54.000	system.syslog	[23210.608669] SGI XFS with ACLs, security attributes, realtime, no debug enabled
15:28:57.000	system.syslog	Started Daily apt upgrade and clean activities.
15:28:58.000	system.syslog	2020-07-23T06:28:58.529Z#011INFO#011[monitoring]#011log/log.go:145#011Non-zero metrics in the last 30s#011("monitoring": {"metrics": {"beat": {"cpu": {"system": {"ticks": 398, "time": {"ms": 9}}, "total": {"ticks": 1320, "time": {"ms": 19}}, "value": 1320}, "user": {"ticks": 900, "time": {"ms": 10}}}, "handles": {"limit": {"hard": 4096, "soft": 1024}, "open": 12}, "info": {"ephemeral_id": "b5a15397-7fce-453c-b9ff-cdda3e986a64", "uptime": {"ms": 2040068}}, "memstats": {"gc_next": "9623808", "memory_alloc": 6299640, "memory_total": 155229584, "rss": 17682432}, "runtime": {"goroutines": 91}}, "filebeat": {"events": {"added": 8, "done": 8}, "harvester": {"open_files": 4, "running": 4}}, "libbeat": {"config": {"module": {"running": 0}, "reloads": 3}, "output": {"events": {"acked": 8, "batches": 3, "total": 8}, "read": {"bytes": 1078}, "write": {"bytes": 1390}}, "pipeline": {"clients": 10, "events": {"active": 0, "published": 8}, "total": 8}, "queue": {"acked": 8}}}, "registrar": {"states": {"current": 9, "update": 8}}, "writes": {"success": 3, "total": 3}), "system": {"load": {"l": 0.03, "l5": 0.12, "l15": 0.35}, "norm": {"l": 0.03, "l5": 0.12, "l15": 0.35}}})}
15:29:28.000	system.syslog	2020-07-23T06:29:28.529Z#011INFO#011[monitoring]#011log/log.go:145#011Non-zero metrics in the last 30s#011("monitoring": {"metrics": {"beat": {"cpu": {"system": {"ticks": 398, "time": {"ms": 3}}, "total": {"ticks": 1330, "time": {"ms": 14}}, "value": 1330}, "user": {"ticks": 940, "time": {"ms": 11}}}, "handles": {"limit": {"hard": 4096, "soft": 1024}, "open": 12}, "info": {"ephemeral_id": "b5a15397-7fce-453c-b9ff-cdda3e986a64", "uptime": {"ms": 2070068}}, "memstats": {"gc_next": "9623808", "memory_alloc": 7655856, "memory_total": 156585800, "rss": 17682432}, "runtime": {"goroutines": 91}}, "filebeat": {"events": {"added": 3, "done": 3}, "harvester": {"open_files": 4, "running": 4}}, "libbeat": {"config": {"module": {"running": 0}, "reloads": 3}, "output": {"events": {"acked": 3, "batches": 2, "total": 3}, "read": {"bytes": 183}, "write": {"bytes": 510}}, "pipeline": {"clients": 10, "events": {"active": 0, "published": 3}, "total": 3}, "queue": {"acked": 3}}}, "registrar": {"states": {"current": 9, "update": 3}}, "writes": {"success": 2, "total": 2}), "system": {"load": {"l": 0.02, "l5": 0.12, "l15": 0.32}, "norm": {"l": 0.02, "l5": 0.12, "l15": 0.32}}})
15:29:58.000	system.syslog	2020-07-23T06:29:58.529Z#011INFO#011[monitoring]#011log/log.go:145#011Non-zero metrics in the last 30s#011("monitoring": {"metrics": {"beat": {"cpu": {"system": {"ticks": 400, "time": {"ms": 5}}, "total": {"ticks": 1340, "time": {"ms": 10}}, "value": 1340}, "user": {"ticks": 940, "time": {"ms": 5}}}, "handles": {"limit": {"hard": 4096, "soft": 1024}, "open": 12}, "info": {"ephemeral_id": "b5a15397-7fce-453c-b9ff-cdda3e986a64", "uptime": {"ms": 2100068}}, "memstats": {"gc_next": "9623808", "memory_alloc": 8574328, "memory_total": 157504272}, "runtime": {"goroutines": 91}}, "filebeat": {"events": {"added": 1, "done": 1}, "harvester": {"open_files": 4, "running": 4}}, "libbeat": {"config": {"module": {"running": 0}, "reloads": 3}, "output": {"events": {"acked": 1, "batches": 1, "total": 1}, "read": {"bytes": 343}, "write": {"bytes": 2519}}, "pipeline": {"clients": 10, "events": {"active": 0, "published": 1}, "total": 1}, "queue": {"acked": 1}}}, "registrar": {"states": {"current": 9, "update": 1}}, "writes": {"success": 1, "total": 1}), "system": {"load": {"l": 0.38, "l5": 0.11, "l15": 0.28}, "norm": {"l": 0.38, "l5": 0.11, "l15": 0.28}}})
15:30:20.000	system.syslog	2020-07-23T06:30:20.691Z#011INFO#011[harvester]#026#011File is inactive: /var/log/auth.log. Closing because close_inactive of 5m(s) reached.
15:30:28.000	system.syslog	2020-07-23T06:30:28.529Z#011INFO#011[monitoring]#011log/log.go:145#011Non-zero metrics in the last 30s#011("monitoring": {"metrics": {"beat": {"cpu": {"system": {"ticks": 410, "time": {"ms": 15}}, "total": {"ticks": 1360, "time": {"ms": 18}}, "value": 1360}, "user": {"ticks": 950, "time": {"ms": 3}}}, "handles": {"limit": {"hard": 4096, "soft": 1024}, "open": 11}, "info": {"ephemeral_id": "b5a15397-7fce-453c-b9ff-cdda3e986a64", "uptime": {"ms": 2130068}}, "memstats": {"gc_next": "9535456", "memory_alloc": 5225080, "memory_total": 158563208}, "runtime": {"goroutines": 86}}, "filebeat": {"events": {"added": 2, "done": 2}, "harvester": {"closed": 1, "open_files": 3, "running": 3}}, "libbeat": {"config": {"module": {"running": 0}, "reloads": 3}, "output": {"events": {"acked": 2, "batches": 1, "total": 1}, "read": {"bytes": 343}, "write": {"bytes": 2512}}, "pipeline": {"clients": 10, "events": {"active": 0, "filtered": 1, "published": 1}, "total": 1}, "queue": {"acked": 2}}}, "registrar": {"states": {"current": 9, "update": 2}}, "writes": {"success": 2, "total": 2}), "system": {"load": {"l": 0.23, "l5": 0.11, "l15": 0.26}, "norm": {"l": 0.23, "l5": 0.11, "l15": 0.26}}})
15:30:58.000	system.syslog	2020-07-23T06:30:58.529Z#011INFO#011[monitoring]#011log/log.go:145#011Non-zero metrics in the last 30s#011("monitoring": {"metrics": {"beat": {"cpu": {"system": {"ticks": 420, "time": {"ms": 8}}, "total": {"ticks": 1370, "time": {"ms: 14}}, "value": 1370}, "user": {"ticks": 958, "time": {"ms: 6}}}, "handles": {"limit": {"hard": 4096, "soft": 1024}, "open": 11}, "info": {"ephemeral_id": "b5a15397-7fce-453c-b9ff-cdda3e986a64", "uptime": {"ms: 2160068}}, "memstats": {"gc_next": "9535456", "memory_alloc": 6576184, "memory_total": 159914312}, "runtime": {"goroutines": 86}}, "filebeat": {"events": {"added": 2, "done": 2}, "harvester": {"open_files": 3, "running": 3}}, "libbeat": {"config": {"module": {"running": 0}, "reloads": 3}, "output": {"events": {"acked": 2, "batches": 2, "total": 2}, "read": {"bytes": 687}, "write": {"bytes": 4026}}, "pipeline": {"clients": 10, "events": {"active": 0, "published": 2}, "total": 2}, "queue": {"acked": 2}}}, "registrar": {"states": {"current": 9, "update": 2}}, "writes": {"success": 2, "total": 2}), "system": {"load": {"l": 0.14, "l5": 0.1, "l15": 0.23}, "norm": {"l": 0.14, "l5": 0.1, "l15": 0.23}}})
15:31:28.000	system.syslog	2020-07-23T06:31:28.529Z#011INFO#011[monitoring]#011log/log.go:145#011Non-zero metrics in the last 30s#011("monitoring": {"metrics": {"beat": {"cpu": {"system": {"ticks": 420, "time": {"ms: 9}}, "total": {"ticks": 1380, "time": {"ms: 18}}, "value": 1380}, "user": {"ticks": 960, "time": {"ms: 9}}}, "handles": {"limit": {"hard": 4096, "soft": 1024}, "open": 11}, "info": {"ephemeral_id": "b5a15397-7fce-453c-b9ff-cdda3e986a64", "uptime": {"ms: 2190068}}, "memstats": {"gc_next": "9535456", "memory_alloc": 7573064, "memory_total": 16091102}, "runtime": {"goroutines": 86}}, "filebeat": {"events": {"added": 1, "done": 1}, "harvester": {"open_files": 3, "running": 3}}, "libbeat": {"config": {"module": {"running": 0}, "reloads": 3}, "output": {"events": {"acked": 1, "batches": 1, "total": 1}, "read": {"bytes": 343}, "write": {"bytes": 2510}}, "pipeline": {"clients": 10, "events": {"active": 0, "published": 1}, "total": 1}, "queue": {"acked": 1}}}, "registrar": {"states": {"current": 9, "update": 1}}, "writes": {"success": 1, "total": 1}), "system": {"load": {"l": 0.08, "l5": 0.09, "l15": 0.21}, "norm": {"l": 0.08, "l5": 0.09, "l15": 0.21}}})

Showing entries until Jul 23, 15:31:28

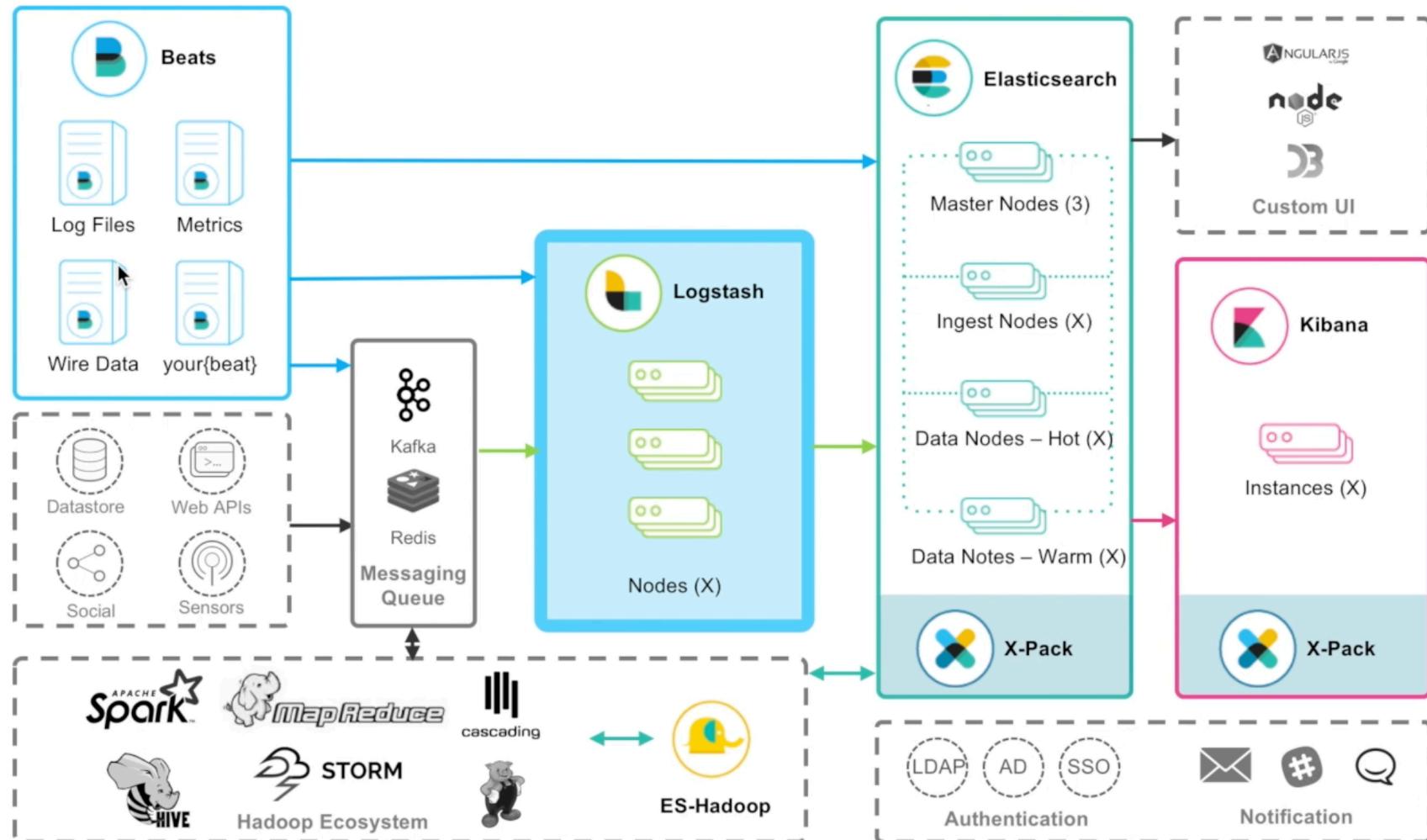
Stream live



Innovation Academy

03. ELK란?

The Journey of an Event



Innovation Academy

03. ELK란?

3) Kibana

- Elasticsearch와 함께 사용하도록 설계된 오픈소스 분석 및 **시각화** 플랫폼
- Elasticsearch에 저장된 데이터를 검색하고 보면서 상호 작용을 수행
- 손쉽게 고급 데이터 분석을 수행하고 다양한 차트, 테이블, 지도의 형태로 데이터를 **시각화**
- 브라우저 기반 인터페이스에서 Elasticsearch 쿼리의 변경 사항을 실시간으로 표시하는 동적 대시보드를 신속하게 생성하고 공유



Innovation Academy

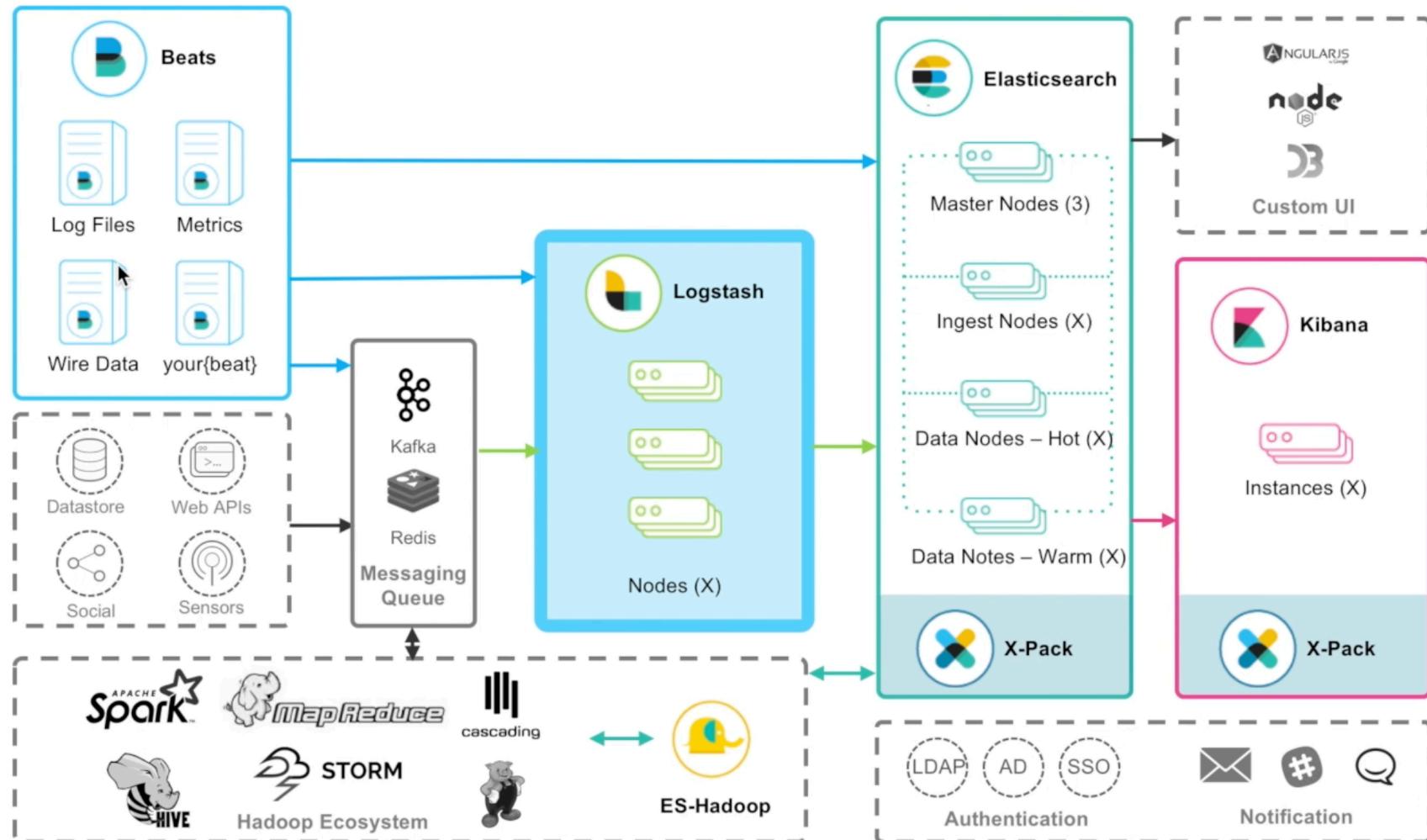
03. ELK란?



Innovation Academy

03. ELK란?

The Journey of an Event



Innovation Academy

03. ELK란?

4) Beats

- Beats는 단일 목적의 **데이터 수집기** 무료 오픈 소스 플랫폼
- Logstash나 Elasticsearch에 데이터를 전송
- 데이터 필터링을 위해서는 Logstash로 데이터를 보내야함



Innovation Academy

03. ELK란?

4) Beats



Filebeat

Real-time insight into log data.

[Download](#)

Packetbeat

Analyze network packet data.

[Download](#)

Winlogbeat

Analyze Windows event logs.

[Download](#)

Metricbeat

Ship and analyze metrics.

[Download](#)

Heartbeat

Ping your Infrastructure.

[Download](#)

Auditbeat

Send audit data to Elasticsearch.

[Download](#)

Functionbeat

Ship cloud data with serverless infrastructure.

[Download](#)

Journalbeat

Analyze Journald logs.

[Download](#)

04. 실습

· 실습 환경

1. nodejs + nginx + beats(Ubuntu)[micro] => 웹 서버

2. ELK (Amazon Linux)[medium] => 로그 수집 서버
(최소사양: 메모리 4GB, 디스크 16GB)

태그 및 속성별 필터 또는 키워드별 검색								
Name	인스턴스 ID	인스턴스 유형	가용 영역	인스턴스 상태	상태 검사	경보 상태	퍼블릭 DNS(IPv4)	IPv4 피
	i-05a4e4dcbe264a1fd	t2.micro	us-east-1e	● stopped	없음			-
	i-064efee69a839ce1d	t2.medium	us-east-1f	● stopped	없음			-



04. 실습

1) Elastic Search 설치(로그 서버)

- <https://www.elastic.co/kr/downloads/elasticsearch>(접속)
- 패키지로 설치할 것인지, wget으로 설치할 것인지는 본인의 선택
- 본인은 yum 패키지 매니저로 설치함



04. 실습

Download Elasticsearch

Want it hosted? Deploy on Elastic Cloud. [Get Started »](#)

Version: 7.8.0

Release date: June 19, 2020

License: [Elastic License](#)

Downloads:

WINDOWS sha.asc	MACOS sha.asc
LINUX X86_64 sha.asc	LINUX AARCH64 sha.asc
DEB X86_64 sha.asc	DEB AARCH64 sha.asc
RPM X86_64 sha.asc	RPM AARCH64 sha.asc
MSI (BETA) sha.asc	

Package Managers:

- Install with [yum, dnf, or zypper](#) 
- Install with [apt-get](#)
- Install with [homebrew](#)



04. 실습

1. Public key install

Download and install the public signing key:

```
rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch
```

2. /etc/zypp/repos.d/ 경로에 아래와 같은 파일 작성 elasticsearch.repo

```
[elasticsearch]
name=Elasticsearch repository for 7.x packages
baseurl=https://artifacts.elastic.co/packages/7.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=0
autorefresh=1
type=rpm-md
```

3. sudo yum install --enablerepo=elasticsearch elasticsearch

4. 설치 완료 !!



04. 실습

5. Systemd에 서비스 등록 (서버 부팅 시 자동 실행)[optional]

```
sudo /bin/systemctl daemon-reload  
sudo /bin/systemctl enable elasticsearch.service
```

Elasticsearch can be started and stopped as follows:

```
sudo systemctl start elasticsearch.service  
sudo systemctl stop elasticsearch.service
```



04. 실습

2) Kibana, Logstash 설치

- <https://www.elastic.co/kr/downloads/kibana> (kibana 설치)
- <https://www.elastic.co/kr/downloads/logstash> (logstash 설치)
- elasticsearch와 같은 방식으로 설치
- kinana와 logstash는 설치 방법을 생략



04. 실습

3) ELK 파이프라인 연결 (elasticsearch)

- elasticsearch.yml 과 jvm.options를 설정해야함
- find / -name elasticsearch.yml (리눅스 명령어를 사용하면 쉽게 찾을 수 있음)
- find / -name jvm.options(리눅스 명령어를 사용하면 쉽게 찾을 수 있음)



04. 실습

3) ELK 파이프라인 연결 (elasticsearch.yml)

```
# Path to log files:  
#  
path.logs: /var/log/elasticsearch  
"  
# ----- Memory -----  
#  
# Lock the memory on startup:  
#  
#bootstrap.memory_lock: true  
#  
# Make sure that the heap size is set to about half the memory available  
# on the system and that the owner of the process is allowed to use this  
# limit.  
#  
# Elasticsearch performs poorly when the system is swapping the memory.  
#  
# ----- Network -----  
#  
# Set the bind address to a specific IP (IPv4 or IPv6):  
#  
network.host: 0.0.0.0  
"  
# Set a custom port for HTTP:  
#  
http.port: 9200  
"  
# For more information, consult the network module documentation.  
#  
# ----- Discovery -----  
#  
# Pass an initial list of hosts to perform discovery when this node is started:  
# The default list of hosts is ["127.0.0.1", "[::1]"]  
#  
#discovery.seed_hosts: ["host1", "host2"]  
#  
# Bootstrap the cluster using an initial set of master-eligible nodes:  
#  
cluster.initial_master_nodes: "node-1"  
  # ["node-1", "node-2"]  
"  
# For more information, consult the discovery and cluster formation module documentation  
#
```

- elasticsearch의 로그 경로 설정
(elasticsearch 자체의 에러를 찾을 수 있음)
- 인바운드 규칙
- 사용하는 포트 번호
- 노드 설정



04. 실습

3) ELK 파이프라인 연결 (jvm.options)

```
[root@ip-172-31-71-116 ~]# cat /etc/elasticsearch/jvm.options
## JVM configuration

#####
## IMPORTANT: JVM heap size
#####

## You should always set the min and max JVM heap
## size to the same value. For example, to set
## the heap to 4 GB, set:
##
## -Xms4g
## -Xmx4g
##
## See https://www.elastic.co/guide/en/elasticsearch/reference/current/heap-size.html
## for more information
##
#####

# Xms represents the initial size of total heap space
# Xmx represents the maximum size of total heap space

-Xms1g
-Xmx1g

#####
## Expert settings
#####

## All settings below this section are considered
## expert settings. Don't tamper with them unless
## you understand what you are doing
##

#####

## GC configuration
8-13:-XX:+UseConcMarkSweepGC
8-13:-XX:CMSInitiatingOccupancyFraction=75
8-13:-XX:+UseCMSInitiatingOccupancyOnly
```

- ELK가 있는 서버 컴퓨터 사양이 낮다면 jvm.options 파일을 설정



04. 실습

3) ELK 파이프라인 연결 (kibana.yml)

```
# Kibana is served by a back end server. This setting specifies the port to use.  
server.port: 5601  
  
# Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid v  
s.  
# The default is 'localhost', which usually means remote machines will not be able to connect.  
# To allow connections from remote users, set this parameter to a non-loopback address.  
server.host: "0.0.0.0"  
  
# Enables you to specify a path to mount Kibana at if you are running behind a proxy.  
# Use the `server.rewriteBasePath` setting to tell Kibana if it should remove the basePath  
# from requests it receives, and to prevent a deprecation warning at startup.  
# This setting cannot end in a slash.  
#server.basePath: ""
```

- server.host만 실습을 위해 열어놓음
- 나머지는 default 값으로 사용해도 지장 없음

다른 설정 옵션을 보고 싶다면

<https://www.elastic.co/guide/en/kibana/7.8/settings.html> 을 참조



04. 실습

3) ELK 파이프라인 연결 (logstash)

```
→ config cat test.conf
input {
  beats {
    port => "5044"
  }
}
filter {
  grok {
    match => { "message" => "%{COMBINEDAPACHELOG}"}
  }
}

output {
  elasticsearch {
    hosts => ["http://localhost:9200"]
    index => "%{@metadata}[beat]}-%{@metadata}[version]}-%{+YYYY.MM.dd}"
  }
}
```

- input, filter, output 설정
- filter는 공식홈페이지에 미리 정의되어 있는 것이 많음



04. 실습

4) WebServer에 Filebeats 설치

- <https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-installation.html>
- vim /etc/filebeat/modules.d/nginx.yml 를 통해 nginx 설정
- filebeat.yml 수정



04. 실습

4) WebServer에 Filebeats 설치(nginx.yml)

```
- module: nginx
# Access logs
access:
  enabled: true
  var.paths: ["/var/log/nginx/access.log"]
  # Set custom paths for the log files. If left empty,
  # Filebeat will choose the paths depending on your OS.
  #var.paths:

# Error logs
error:
  enabled: true
  var.paths: ["/var/log/nginx/error.log"]
  # Set custom paths for the log files. If left empty,
  # Filebeat will choose the paths depending on your OS.
  #var.paths:
```

~



04. 실습

4) WebServer에 Filebeats 설치(filebeat.yml)

- filebeat.yml의 파일에 있는 output 경로를 설정해줌

```
#----- Elasticsearch output -----
output.elasticsearch:
    # Array of hosts to connect to.
    hosts: ["3.218.67.39:9200"]

    # Optional protocol and basic auth credentials.
    #protocol: "https"
    #username: "elastic"
    #password: "changeme"

#----- Logstash output -----
#output.logstash:
    # The Logstash hosts
    # hosts: ["3.218.67.39:5044"]

    # Optional SSL. By default is off.
    # List of root certificates for HTTPS server verifications
    #ssl.certificateAuthorities: ["/etc/pki/root/ca.pem"]

    # Certificate for SSL client authentication
    #ssl.certificate: "/etc/pki/client/cert.pem"

    # Client Certificate Key
    #ssl.key: "/etc/pki/client/cert.key"
```



05. 결과물

감사합니다

