Ubuntu Filebeat 연동

Ubuntu 20.04 설치

1-1. 이미지 다운로드

Docker CLI 설치 후, cmd 창에서 아래의 명령어로 우분투 20.04 버전 이미지를 다운로드한다.

```
docker pull ubuntu:20.04
```

다운로드 확인

아래 명령어를 통해, 다운 받은 이미지를 확인할 수 있다.

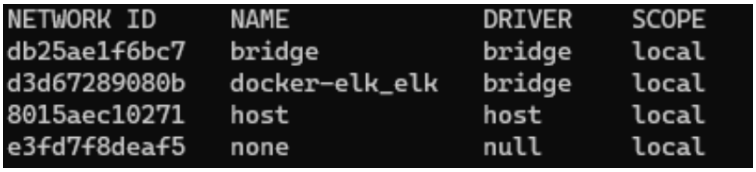
```
docker images
```

1-2. Ubuntu 20.04 컨테이너 생성

1) docker network 확인

현재 네트워크 목록 확인

```
docker network ls
```

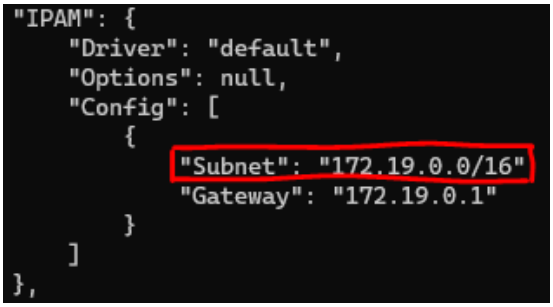


NETWORK ID	NAME	DRIVER	SCOPE
db25ae1f6bc7	bridge	bridge	local
d3d67289080b	docker-elk_elk	bridge	local
8015aec10271	host	host	local
e3fd7f8deaf5	none	null	local

2) docker network 상세 정보 확인

docker network inspect 명령어를 이용하면 네트워크의 자세한 정보를 살펴볼 수 있다.

```
# docker network inspect 네트워크NAME

docker network inspect docker-elk_elk
```



- "Containers": { } 를 보면 logstash, kibana, elasticsearch 각각에 대한 IP Address를 확인할 수 있다.

앞서 docker-elk를 구축하면서 bridge 네트워크 구조를 통해 elasticsearch, logstash, kibana 각각이 연결되어 docker-elk 컨테이너가 생성되었는데 ubuntu도 해당 bridge에 연결할 것이다.

Ubuntu 20.04(linux-ubuntu) 컨테이너 생성

```
docker run -it --name linux-ubuntu ubuntu:20.04 /bin/bash
```

컨테이너에 network 할당하기

Docker Network 관련 설명 블로그: https://captcha.tistory.com/70?category=830258

```
# docker network connect 브릿지이름 컨테이너이름

docker network connect docker-elk_elk linux-ubuntu

docker attatch linux-ubuntu
```

====================== 여기부터 시작 ======================

ELK syslog 연동 (with Ubuntu, filebeat, logstash)

1. Ubuntu 실행

```
docker run -it --name linux-ubuntu ubuntu:20.04 /bin/bash
```

2. Filebeat 설치

- 참고 블로그: [Filebeat+ELK 7.5] 로그 모니터링 서버 구축 (설치부터 설정까지)

필요한 것들 미리 설치

```
apt update

apt install curl -y

apt install vim -y

apt install systemd
6 69
```

이건 보류

```
apt install net-tools
```

Test 해보기

[Windows] 자신의 IP 확인

```
ipconfig
```

[Ubuntu]

```
curl 자신의IP:9200
```

제대로 응답을 받았다면 OK

Filebeat 다운로드

```
curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.15.0-amd64.deb

dpkg -i filebeat-7.15.0-amd64.deb
```

Filebeat : /etc/filebeat 경로에 설치됨

Filebeat 설정 : `/etc/filebeat/filebeat.yml`

```
vi /etc/filebeat/filebeat.yml
```

기존에 입력된 내용에서 주석처리된 부분을 해제하거나 ip수정, enabled: false → true 변경하는 내용이 전부임. (해당 하는 위치 수정)

```
# ============================== Filebeat inputs ===============================
filebeat.inputs:
- type: log
  enabled: true
```

```
  paths:
    - /var/log/*.log

# ========================================== Filebeat modules ==========================================
filebeat.config.modules:
  path: ${path.config}/modules.d/*.yml
  reload.enabled: true

# ============================================== Dashboards ============================================
setup.dashboards.enabled: true


# ============================================== Kibana ================================================
setup.kibana:
  host: "Kibana가 설치된 서버IP:5601"
#       (ipconfig로 확인한 내 windows ip 입력)

# ========================================== Elasticsearch Output ==========================================
# 이 부분 주석처리 해주기
#output.elasticsearch:
  #hosts: ["localhost:9200"]

# ========================================== Logstash Output ===========================================
# 여기 주석 풀고 IP 수정
output.logstash:
  hosts: ["Logstash가 설치된 서버IP:5044"]
#       (ipconfig로 확인한 내 windows ip 입력 - Kibana에서 입력한 host와 동일)
```

Filebeat 모듈 설정

```
# 현재 설정된 파일비트 modules 리스트 확인
filebeat modules list

# logstash 모듈 enable
filebeat modules enable logstash

# (이건 필수인지 잘 모르겠다 - nginx를 사용하여 로그를 수집하는 경우)
filebeat modules enable system nginx
```

Filebeat 초기화 설정

```
# -e: 디버깅 모드
filebeat setup -e
```

시스템 등록

```
systemctl enable filebeat.service

systemctl start filebeat.service

systemctl status filebeat.service
```

!!! 만약 systemctl 명령어 실행 시, 다음과 같은 에러가 난다면 아래 명령어로 실행

```
System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down
```

```
/etc/init.d/filebeat start

ps -a
```

filebeat 구동이 확인되면 설치 완료

docker-elk 를 설치한 windows 경로로 가서 cmd 실행

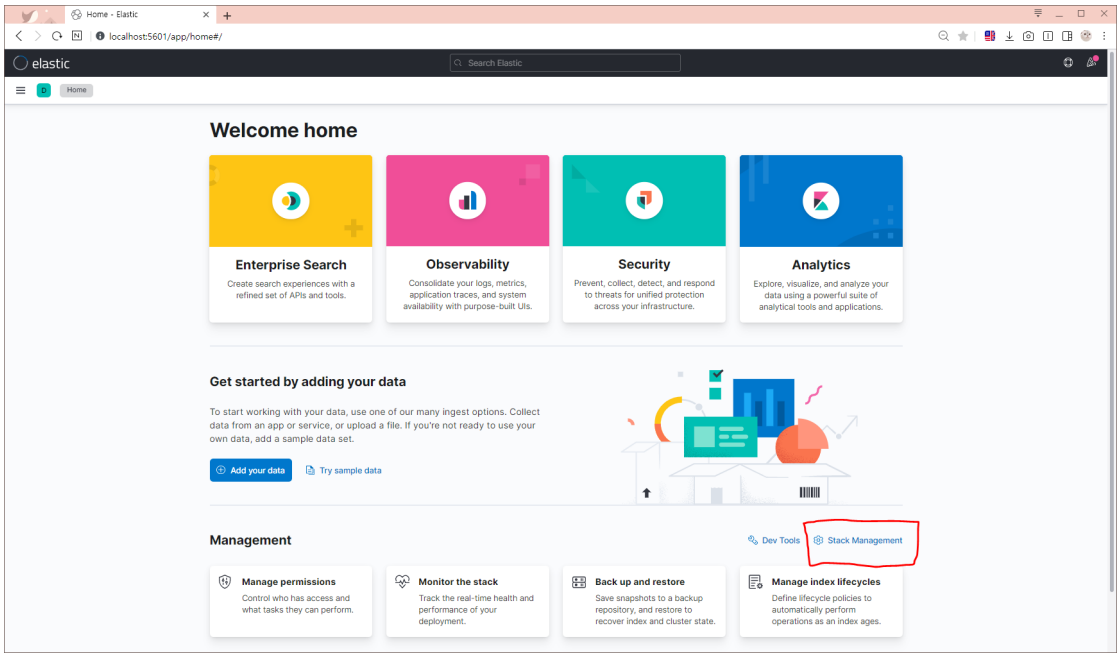
```
docker-compose build

docker-compose restart
```

3. Kibana 설정

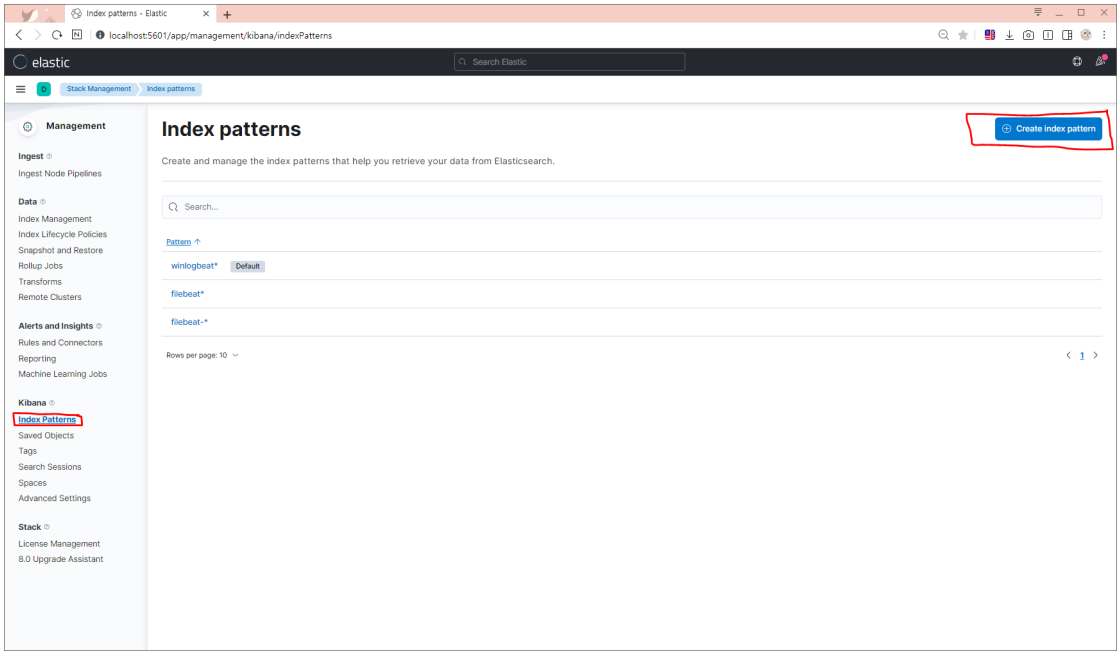
여기서부터는 Winlogbeat 설정했을 때와 동일함

Index Pattern 생성

1. 브라우저에서 Kibana 접속 - **Stack Management**



2. Kibana > Index Patterns에서 **Create Index Pattern**



3. Name: filebeat* 입력, Timestamp field: timestamp 선택

Analytics > Discover 가서 수집된 filebeat 로그 확인

컨테이너(linux-ubuntu)에 접속하기

```
docker exec -it linux-ubuntu /bin/bash
```