**پیاده سازی ELK stack بر روی دو سرور**

برای اینکه ما بخواهیم ELK را در دو سرور پیاده سازی کنیم ما باید Elasticsearch ، Logstash و Kibana را در یک سرور و filebeat را در سرور دیگر پیاده سازی کنیم.

در شرکت پروژه­ها بصورت داکری بر روی سرور 192.168.253.76 در حال اجرا می­باشند و هر کدام از کانتینرهای پروژه، log های خود را ذخیره می­کنند.

ما ELK را در سرور 192.168.253.74 پیاده سازی کردیم. حال برای اینکه بخواهیم لاگ فایل­ها را از سرور 76 به سرور 74 انتقال دهیم از filebeat استفاده می­کنیم. filebeat را در سرور 76 پیاده سازی می­کنیم و با توجه به مستندات و فایل­های قبلی که در گروه دواپس در گیت لب وجود دارد، تغییراتی بر روی آن انجام می­دهیم که در زیر این تغییرات توضیخ داده شده است.

آدرس فایل­های قبلی:

http://192.168.251.80:10080/bh-framework/baharan-framework-devops/tree/master/elk-and-filebeats

در فایل docker-compose.yml نیازی به تغییر نیست. اما می­توانیم قسمت مربوط به filebeat را کامنت کنیم تا اجرا نشود.

ما باید پوشه filebeat را که شامل دو فایل filebeat.yml و Dockerfile است را به سرور 76 انتقال دهیم همچنین یک فایل docker-compose.yml نیز ایجاد کنیم که بصورت زیر باشد:

version: '2.2'

services:

filebeat:

build:

context: filebeat/

volumes:

# needed to access all docker logs (read only) :

- "/var/lib/docker/containers:/usr/share/dockerlogs/data:ro"

# needed to access additional informations about containers

- "/var/run/docker.sock:/var/run/docker.sock"

# networks:

# - filebeat

# #depends\_on:

# # - elasticsearch

# links:

# - logstash

# #cpu\_count: 1

cpus: 0.5

mem\_limit: 2G

#networks:

# filebeat:

# driver: bridge

همچنین باید فایل filebeat.yml را تغییرات دهیم که این تغییرات بصورت زیر است:

output.logstash:

hosts: ["logstash:5044"]

اینجا بجای logstash ممکن است localhost هم باشد. در هر صورت باید اینجا آدرس ip سروری که ELK بر روی آن در حال اجرا است را بنویسیم:

output.logstash:

hosts: ["192.168.253.74:5044"]

پس از اینکه این تغییرات را اعمال کردیم docker-compose.yml را up می­کنیم تا با اینکار لاگ­ها را به سرور 74 نتقال دهیم.