**FILEBEAT CONFIGURATION**

**Installing filebeat**

sudo apt update

sudo apt install apt-transport-https curl

curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elastic-archive-keyring.gpg

echo "deb [signed-by=/usr/share/keyrings/elastic-archive-keyring.gpg] https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list

sudo apt update

sudo apt install filebeat

**vi /etc/filebeat/filebeat.yml**

filebeat.inputs:

- type: log

paths:

- /var/log/varnish/varnishlog.log

multiline.pattern: '^(<< Request >>|\\*\\* << BeReq >>)'

multiline.negate: true

multiline.match: after

exclude\_lines: ['^End$']

output.elasticsearch:

hosts: ["103.189.88.139:9200"]

index: "varnish-logs-%{+yyyy.MM.dd}"

username: "elastic"

password: "password123!"

setup.template:

name: 'filebeat'

pattern: 'filebeat-\*'

enabled: true

**Command to check if the configuration is right or not**

filebeat test config