Instalando logstash

sudo apt install openjdk-8-jre-headless

```
sudo apt-get update
sudo apt-get install logstash
```

Configurando logstash

sudo nano /etc/logstash/conf.d/logstash.conf

```
input {
        file {
                path => "/home/fernando/access_log“
               start_position => "beginning"
        }
}

filter {
        grok {
                match => { "message" => "%{COMBINEDAPACHELOG}" }
        }
        date {
                match => [ "timestamp", "dd/MMM/yyyy:HH:mm:ss Z" ]
        }
}

output {
        elasticsearch {
                hosts => ["localhost:9200"]
        }
        stdout {
                codec => rubydebug
        }
}
```

Sundog Education Coralogix PROF. FERNANDO AMARAL


Sundog
Education

Coralogix

PROF.
FERNANDO
AMARAL