**Logstash Setup and Configuration**

**Note:** Logstash is always configured on a single node. It’s just a mediator, so doesn’t require cluster capabilities but it is always better to assign good computation capabilities.

$  sudo apt-get update

$  sudo apt-get install default-jdk

$  java -version

$  wget <https://artifacts.elastic.co/downloads/logstash/logstash-6.2.2.tar.gz>

$  sudo tar -xzf logstash-6.2.2.tar.gz

$  cd logstash-6.2.2/

$  sudo vi **sample.conf**

$ ./bin/logstash -f **sample.conf** (if .conf file is located somewhere else, then give full path to the file)

These configuration needs to be written in a ***.conf*** file. For example: **sample.conf**

**... (configurations are given ahead)**

Use the following to get mysql java connector required for logstash conf file:

$ wget <https://dev.mysql.com/get/Downloads/Connector-J/mysql-connector-java-5.1.46.tar.gz>

1. **Logstash configuration for fetching data from RDS SQL to elastic cloud**:

input {

jdbc{

jdbc\_connection\_string=> "jdbc:mysql://tidyquant-mysql.ctzkiiqc8r0v.ap-south-1.rds.amazonaws.com:3306/San\_Francisco\_Crime\_Classification"

jdbc\_user=> "tidyquant"

jdbc\_password=> "tidyquant"

jdbc\_driver\_library=> "/home/ubuntu/mysql-connector-java-5.1.46/mysql-connector-java-5.1.46-bin.jar"

jdbc\_driver\_class=> "com.mysql.jdbc.Driver"

statement => "SELECT \* FROM test limit 1000"

}

}

output {

elasticsearch {

hosts => "https://b8bd4f06269136f164b670ae8c497567.us-east-1.aws.found.io:9243"

user => "elastic"

password => "eGlSf27hAeYT9k8x8xDDNHVj"

index => "test\_logstash"

document\_type => "test\_mapping"

}

stdout {

codec => rubydebug

}

}

1. **Logstash configuration for fetching data from S3 to elastic cloud:**

input{

s3 {

bucket => "tidyquant-pipeline-test"

access\_key\_id => "AKIAJUEDFWZNW2NYVJXQ"

secret\_access\_key => "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"

}

}

filter{

grok {

match => {"message" => "%{COMBINEDAPACHELOG}"}

}

date {

match => [ "timestamp", "dd/MMM/yyyy:HH:mm:ss Z"]

}

}

output {

elasticsearch {

hosts => [ "https://b8bd4f06269136f164b670ae8c497567.us-east-1.aws.found.io:9243" ]

user => "elastic"

password => "eGlSf27hAeYT9k8x8xDDNHVj"

index => "s3\_logstash"

document\_type => "s3\_mapping"

}

stdout {

codec => rubydebug

}

}