**Filebeat configuration with path and tomcat module**

add the following code in filebeat.yml file

**Note:** Remember to change the paths according to your tomcat environment.

filebeat.inputs:

## Catalina logs

- type: log

enabled: true

paths:

- /var/log/tomcat9/catalina.\*.log

fields:

codec: plain

type: catalina\_log

##The dissect processor parses the catalina logs by means of a tokenizer

processors:

- dissect:

tokenizer: '%{date} %{time} %{catalina.warnLevel} [%{catalina.method}] %{catalina.class} %{catalina.logMessage}'

field: "message"

##Filebeat processes each log file line-by-line

##However it is possible that a singular Tomcat log entry might contain multiple lines in the form of a Java stack trace

##To preserve the integrity of logs, we define a multiline pattern to process multiline stack traces as a single entry.

multiline.type: pattern

multiline.pattern: '^[[:space:]]+(at|\.{3})\b|^Caused by:'

multiline.negate: false

multiline.match: after

##Localhost Logs

- type: log

enabled: false

paths:

- /var/log/tomcat9/localhost.\*.log

tags: ["localhost\_logs"]

fields:

codec: plain

type: localhost\_log

##The dissect processor parses the catalina logs by means of a tokenizer

processors:

- dissect:

tokenizer: '%{date} %{time} %{tomcatLocalhost.warnLevel} [%{tomcatLocalhost.method}] %{tomcatLocalhost.class} %{tomcatLocalhost.ListenerType}: %{ListenerLog}'

field: "message"

##Filebeat processes each log file line-by-line

##However it is possible that a singular Tomcat log entry might contain multiple lines in the form of a Java stack trace

##To preserve the integrity of logs, we define a multiline pattern to process multiline stack traces as a single entry.

multiline.type: pattern

multiline.pattern: '^[[:space:]]'

multiline.negate: false

multiline.match: after

add the following code in filebeat.yml for template setting

indices:

- index: "tomcat9-catalina-logs-%{+yyyy.MM.dd}"

when.equals:

fields.type: "catalina\_log"

- index: "tomcat9-localhost-logs-%{+yyyy.MM.dd}"

when.equals:

fields.type: "localhost\_log"

- index: "tomcat9-access-logs-%{+yyyy.MM.dd}"

when.equals:

fields.type: "access\_log"

enable Apache module

filebeat modules enable apache

paste the code in to /etc/filebeat/modules.d/apche.yml

**Note:** Remember to change the paths according to your tomcat environment.

# Module: apache

# Docs: https://www.elastic.co/guide/en/beats/filebeat/7.9/filebeat-module-apache.html

- module: apache

# Access logs

access:

enabled: true

var.paths: ["/var/log/tomcat9/localhost\_access\_log.\*.txt"]

##The type:access\_log will help us point these logs to the right direction

input:

processors:

- add\_fields:

target: fields

fields:

codec: plain

type: access\_log

Restart filebeat