1. Install filebeat
   * Download filebeat
     1. <https://artifacts.elastic.co/downloads/beats/filebeat/filebeat->{{ version }}-linux-x86\_64.tar.gz
   * extract tar.gz to your filebeat path
   * create Config directory in filebeat
     1. ../filebeat-{{ version }}-linux-x86\_64/CustomConfig
     2. ../filebeat-{{ version }}-linux-x86\_64/CustomConfig/inputs.d
   * create filebeat.yml in CustomConfig directory

filebeat.config.inputs:

enabled: true

path: ../filebeat-{{ version }}-linux-x86\_64/CustomConfig/inputs.d/\*.yml

output.elasticsearch:

hosts: ["{{ elasticsearch\_host:port}}"]

username: "\*\*\*\*\*\*\*\*"

password: "\*\*\*\*\*\*\*\*"

monitoring:

enabled: true

elasticsearch:

hosts: ["{{ elasticsearch\_host:port}}"]

cluster\_uuid: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

setup.ilm.enabled: false

* + create your project log yml

- type: log

paths:

- {{ log\_path }}

fields\_under\_root: true

scan\_frequency: 3s

idle\_timeout: 3s

pipeline: {{ pipeline\_name }}

processors:

- dissect:

tokenizer: "[userId]:%{userId}[createdDate]:%{createdDate}[loginDate]:%{loginDate}[logoutDate]:%{logoutDate}[sessionId]:%{sessionId}[ip]:%{ip}[device]:%{device}[loginActionType]:%{loginActionType}[content]:%{content}"

field: "message"

target\_prefix: ""

- drop\_event:

when:

has\_fields: ["log.flags"]

* ITIG team will provide “username” , “password” , “cluster\_uuid” , “pipeline\_name” , “elasticsearch\_host:port” . Please pay more attention to whether to fill in the configuration file