I. 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]:%{logou
tDate}[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