

filebeat日志收集配置手册

机器是否有正在运行的 filebeat ?

一、修改添加配置文件

- 1.修改主配置文件，位置：/opt/filebeat/filebeat.docker.yml
- 2.添加日志输入配置文件
- 3.应用日志格式，可以按需求修改上边的multiline.pattern配置

二、重启filebeat

机器是否有正在运行的 filebeat ?

- 1.无：联系 高金山QQ：207879337 进行安装
- 2.有：按以下步骤进行接入

一、修改添加配置文件

1.修改主配置文件，位置：/opt/filebeat/filebeat.docker.yml

```
1      #设置es索引名，test为测试环境
2      - index: "test-服务名称-%{+yyyy.MM.dd}"
3        when.contains:
4          tags: "test-服务名称"
```

YAML

复制代码

根据自己的服务名，修改如上配置，并追加到下图位置

```
# ----- Elasticsearch Output -----
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["192.169.5.100:9200"]
  indices:
# ----- 5g-os-console索引配置 -----
- index: "test-5g-os-console-%{+yyyy.MM.dd}"
  when.contains:
    tags: "test-5g-os-console"
# ----- 5g-os-api索引配置 -----
```

2.添加日志输入配置文件

- ①创建文件 xxx.yml，路径：/opt/filebeat/inputs.d/
- ②添加如下配置

```

1 # ----- 5g-os-console日志 -----
2 - type: log
3   enabled: true
4   paths:
5     - /日志源文件路径/all.log
6   # 正则表达式, 用于匹配日志
7   multiline.pattern: '^[0-9]{4}-[0-9]{2}-[0-9]{2} [0-9]{2}:[0-9]{2}:[0-9]{2}.*--- \['
8   multiline.negate: true
9   multiline.match: after
10  # tags内容必须和上面es配置下的tags一致, 否则收集不到
11  tags: ["test-服务名称"]
12  # fields下的字段在json中置顶
13  fields_under_root: true
14  fields:
15    # 这里添加level字段, debug会在处理器中截取日志里的日志级别替换掉
16    level: debug

```

下图标注了需要修改的位置

```

1 # ----- 5g-os-console日志 -----
2 - type: log
3   enabled: true
4   paths:
5     - /日志源文件路径/all.log
6   # 正则表达式, 用于匹配日志
7   multiline.pattern: '^[0-9]{4}-[0-9]{2}-[0-9]{2} [0-9]{2}:[0-9]{2}:[0-9]{2}.*--- \['
8   multiline.negate: true
9   multiline.match: after
10  # tags内容必须和上面es配置下的tags一致, 否则收集不到
11  tags: ["test-服务名称"]
12  # fields下的字段在json中置顶
13  fields_under_root: true
14  fields:
15    # 这里添加level字段, debug会在处理器中截取日志里的日志级别替换掉
16    level: debug

```

日志绝对路径, all.log也可以用*.log匹

3.应用日志格式, 可以按需求修改上边的multiline.pattern配置

①“日期 日志级别 [, ” 开头

```

2021-08-23 16:15:00.070 INFO [06aaa7d084f3e2d0,06aaa7d084f3e2d0,true] 1 --- [MONITOR-CLI-1] c.m.t.s.SearchTp1ManufacturerTask

```

正则: '^[0-9]{4}-[0-9]{2}-[0-9]{2} [0-9]{2}:[0-9]{2}:[0-9]{2}.* \[,'

②“日期 日志级别 容器号 --- [” 开头

```
2021-08-23 16:29:57.371 INFO 1 --- [Druid-ConnectionPool-Destroy-1408279755] p6spy  
Execute SQL: SELECT 1 FROM DUAL
```


正则: `^[0-9]{4}-[0-9]{2}-[0-9]{2} [0-9]{2}:[0-9]{2}:[0-9]{2}.*--- \[`

③其他格式日志，按需修改正则表达式，可能会出现日志级别匹配错误问题，联系维护人解决

二、重启filebeat

```
1 docker restart filebeat
```

Shell

 复制代码