

匹配对应文件名

2025-06-06_00 → Log_filebeat-server_2025-06-06_00-00-00.parquet

`fault_start_time` `faultl_end_time` \longrightarrow log1 | log2 | log3 | log4 | log5 | log6
 time2 time5 time1 | time2 | time3 | time4 | time5 | time6

error: db connection failed
info: user logged in
ERROR: file upload failed

只保留error日志

error: db connection failed
ERROR: file upload failed

`..., time_Beijing, k8_pod, k8_node_name, message, ...`
 ↓ 提取关键列
`time_Beijing, k8_pod, k8_node_name, message`

[2025-06-05T16:10:02Z] error: db connection failed
↓ Drain提取模板
[ISO_TIMESTAMP] error: db connection failed

[2025-06-06T16:10:02Z] error: db connection failed [ISO_TIMESTAMP] error: db connection failed
[2025-06-06T16:11:02Z] error: db connection failed [ISO_TIMESTAMP] error: db connection failed
[2025-06-06T16:12:03Z] error: file upload failed [ISO_TIMESTAMP] error: file upload failed

↓

[2025-06-06T16:10:02Z] error: db connection failed [ISO_TIMESTAMP] error: db connection failed
出现次数: 2
[2025-06-06T16:12:03Z] error: file upload failed [ISO_TIMESTAMP] error: file upload failed
出现次数: 1

tme_beijing, k8_node_name, k8_pod, message, occurrence_count
 ↓ 名字映射&从pod_name提取service_name
 Time_Beijing, node_name, service_name, pod_name, message, occurrence