

# 2. ELK Config

## ELK Stack Config Value

### 1. Filebeat Config

#### 1. filebeat Log Config

Config	Default	Value
paths	paths paths	/var/log/message → /home/message /var/log/secure
recursive_glob.enabled	recursive false	true
encoding	W3C false	plain
exclude_lines	exclude_lines	
include_lines	include_lines	
harvester_buffer_size	harvester 16384	16384(16KB)
max_bytes	max_bytes 10485760	10485760(10MB)

参数	类型	默认值
json	son 是否以 json 格式输出 如果为 true，则使用 (keys_under_root, overwrite_keys, expand_keys) 参数 · keys_under_root : 是否以 json 格式输出 · overwrite_keys : 是否覆盖已有的键 · expand_keys : 是否展开键 · add_error_key : json 格式输出时，是否在 error.message 中添加 error.type: json 类型的信息 · message_key : 是否在 json 格式输出时，添加 message_key 键 · document_id : 是否在 json 格式输出时，添加 document_id 键	
multiline	是否以多行格式输出	
exclude_files	path 是否排除指定的文件	
ignore_older	是否忽略比指定时间更早的文件	
close_inactive	是否关闭指定的进程	
close_renamed	是否关闭重命名的文件	
close_removed	是否关闭被删除的文件	true

选项	默认值	说明
close_eof	如果文件在写入时被关闭，则返回 true 如果文件在读取时被关闭，则返回 false (如果文件在写入时被关闭，则返回 true) 如果文件在读取时被关闭，则返回 false )	false
close_timeout	如果文件在写入时被关闭，则返回 true 如果文件在读取时被关闭，则返回 false	0 (无限 )
clean_inactive	inactive 文件在写入时被关闭 如果文件在写入时被关闭，则返回 true	
clean_removed	如果文件在写入时被关闭，则返回 true 如果文件在读取时被关闭，则返回 false 如果文件在写入时被关闭，则返回 true	true
scan_frequency	如果文件在写入时被关闭，则返回 true 如果文件在读取时被关闭，则返回 false	10(秒 )
tail_files	如果文件在写入时被关闭，则返回 true 如果文件在读取时被关闭，则返回 false (rotate 文件 )	false
symlinks	如果文件在写入时被关闭，则返回 true 如果文件在读取时被关闭，则返回 false	false
backoff	如果文件在写入时被关闭，则返回 true 如果文件在读取时被关闭，则返回 false	1(秒 )
max_backoff	如果文件在写入时被关闭，则返回 true 如果文件在读取时被关闭，则返回 false 如果文件在写入时被关闭，则返回 true	10(秒 )
backoff_factor	backoff 文件在写入时被关闭 如果文件在写入时被关闭，则返回 true	2
harvester_limit	如果文件在写入时被关闭，则返回 true 如果文件在读取时被关闭，则返回 false harvester 文件	0 (无限 )