

# 2. ELK Config ??

ELK Stack Config Value

1. Filebeat Config

1. filebeat Log Config

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

参数	参数说明	默认值
json	<p>son参数 参数 参数 参数 参数 (keys_under_root, overwrite_keys, expand_keys 参数 参数 参数 ) · keys_under_root : 参数 json 参数 参数 · overwrite_keys : 参数 参数 参数 参数 参数 参数 · expand_keys : 参数 参数 · add_error_key : json 参数 参数 参数 error.message error.type: json 参数 参数 · message_key : 参数 参数 参数 参数 参数 参数 参数 参数 json 参数 参数 参数 · document_id : 参数 id 参数</p>	
multiline	<p>参数 参数 参数 参数</p>	
exclude_files	<p>path 参数 参数 参数 参数 参数 参数</p>	
ignore_older	<p>参数 参数 参数 参数 参数 参数 参数 参数</p>	
close_inactive	<p>参数 参数 参数 参数 参数 参数 参数</p>	
close_renamed	<p>参数 参数 参数 参数</p>	
close_removed	<p>参数 参数 harvester 参数 参数</p>	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 如果文件在读取时被关闭，则返回 false	
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 )