

2. ELK Config



perplexity 100% AI

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
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	son参数 参数 参数 参数 参数 (keys_under_root, overwrite_keys, expand_keys 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 · expand_keys : 参数 参数 · add_error_key : json 参数 参数 参数 参数 error.message 参数 error.type: json 参数 参数 · message_key : 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	
multiline	参数 参数 参数 参数	
exclude_files	path 参数 参数 参数 参数 参数 参数	
ignore_older	参数 参数 参数 参数 参数 参数 参数 参数	
close_inactive	参数 参数 参数 参数 参数 参数 参数	
close_renamed	参数 参数 参数 参数	
close_removed	参数 参数 harvester 参数 参数 参数 参数	true

이름	타입	기본값
close_eof	이름이 파일 이름인 파일이 닫힐 때 파일의 끝을 나타내는 (파일의 끝을 나타내는 파일의 끝을 나타내는)	false
close_timeout	파일의 끝을 나타내는 파일의 끝을 나타내는	0 (없음)
clean_inactive	inactive이름이 파일 파일의 끝을 나타내는	
clean_removed	파일의 끝을 나타내는 파일의 끝을 나타내는 파일의 끝을 나타내는	true
scan_frequency	파일의 끝을 나타내는 파일의 끝을 나타내는	10(없음)
tail_files	이름이 파일 이름인 파일 이름이 파일 이름인 파일 (rotate이름이 이름이 파일 이름인 파일)	false
symlinks	파일의 끝을 나타내는 파일의 끝을 나타내는	false
backoff	파일의 끝을 나타내는 파일의 끝을 나타내는	1(없음)
max_backoff	파일의 끝을 나타내는 파일의 끝을 나타내는 파일의 끝을 나타내는	10(없음)
backoff_factor	backoff이름이 파일 파일의 끝을 나타내는	2
harvester_limit	파일의 끝을 나타내는 파일의 끝을 나타내는 파일의 끝을 나타내는 harvester	0 (없음)

Revision #2

Created 2024-03-30 01:19:59 KST by artop0420

Updated 2026-02-12 23:03:27 KST by artop0420