2. ELK Config 정보

ELK Stack Config Value 설명

1. Filebeat Config 정보
    1. filebeat Log Config 값

설정값	설 명	기본값
paths	수집할 경로	/var/log/message → /home/message /var/log/secure
recursive_glob. enabled	recursive 패턴으로 확장 기능 활성화	true
encoding	W3C에서 사용하는 인코딩	plain
exclude_lines	로그 전달할때 전송하지 않을 줄 패턴	
include_lines	로그 전달할때 전송할 라인 패턴	모든라인의 데이터 전송
harvester_buffer_size	harvester가 파일을 가지고 올때 사용하는 버퍼크기	16384(바이트 단위)
max_bytes	단일 로그 메시지에 할당하는 최대 크기	10485760(10MB)

설정값	설 명	기본값
json	son포맷으로 작성된 로그를 디코딩할때 사용 (keys_under_root, overwrite_keys, expand_keys 중 하나이상 지정필요) · keys_under_root : 디코딩된 json은 json키 아래배치 · overwrite_keys : 필드 추가시 충돌다는 필드는 덮어쓰기 수행 · expand_keys : 추가 확인필요 · add_error_key : json이 정렬작업시 오류가 발생하면 error.message에 error.type: json키를 추가 · message_key : 라인 필터링 혹은 멀티 라인이 적용되어 있는 경우 json 키를 지정하는 설정 · document_id : 문서 id를 구성	
multiline	멀티라인의 메시지를 처리할때 사용	
exclude_files	path에 정의된 파일중 제외할 파일 리스트 목록	
ignore_older	지정된 시간 범위 이전에 수정된 파일은 전송 제외	
close_inactive	지정된 시간동안 수집되지 않은 경우 파일을 닫음	
close_renamed	파일이름이 변경될때 파일을 닫음	
close_removed	파일이 제거될때 harverster도 종료 .	true

설정값	설 명	기본값
close_eof	파일 끝에 도달하자마자 파일을 닫음 (한번만 작성하고 수시 업데이트시 유용)	false
close_timeout	정해진 시간 초과하면 파일 닫음	0 (비활성화)
clean_inactive	inactive기간 경과하면 파일상태 제거	
clean_removed	마지막으로 읽은 파일이 없는 경우 레지스트리에서 파일정리	true
scan_frequency	지정된 경로에서 새파일을 찾는 빈도	10(초단위)
tail_files	각 파일 끝에서 새파일을 읽기 시작 (rotate적용시 활용가능)	false
symlinks	심볼릭링크된 파일 수집여부	false
backoff	열린파일을 얼마나 크롤링 하는지 확인	1(초단위)
max_backoff	파일이 마지막에 도달한 후 다시 확인하기 전에 대기하는 시간	10(초단위)
backoff_factoer	backoff 시간이 대기하는 시간	2
harvester_limit	하나의 입력에 대해 병렬로 수집하는 최대 harverster 갯수	0 (제한없음)

2.

Revision #1

Created 30 March 2024 01:19:59 by artop0420

Updated 11 November 2024 10:33:23 by artop0420