2. ELK Config 정보 -1

ELK Stack Config Value 설명

1. Filebeat Config 정보
    1. filebeat Log Config 값

설정값	설 명	기본값
paths	수집할 경로	/var/lo essage /home ssage /var/lo ecure
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	10485 (10MB

설정값	설 명	기본값
json	json포맷으로 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 json키를 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 harverster 도 종료 .	true
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

설정값	설 명	기본값
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

* harvester : 각 파일을 한줄씩 읽기 위해 파일을 열고 , 읽고 , 닫는 행위

2. Logstash Config 정보

1. logstash config 설정정보

1. logstash에는 input / filter / output 단위로 Config 설정 가능
2. input : 로그를 수집하는 방법 (syslog, file, http, udp, snmp, s3 등등 가능), sincedb파일 (inode, device numeber, file offset 저장)에 기록하여 logstash가 재시작 되는 경우 sincedb에 저장된 값 을 참고해서 중단된 시점부터 다시 로딩
3. filter : 수집된 로그를 Elasticsearch로 보내기 위해 로그 데이터 포맷 변환
4. output : 정제한 로그데이터를 외부로 보내는 설정

2. Input - File Config 값

설정값	설 명	기본값
check_archive_validity	압축된 파일을 처리하기전 유효성 검사	false
close_older	마지막으로 읽은 후 파일을 닫는 시간	3600(초
delimiter	줄 넘어가는 구분 기호	\n

discover_internval	path에서 지정한 새파일 검색 옵션 stat_interval의 배수 (ef. stat_interval이 500이면 500 x 15 = 7.5 7.5초마다 새 파일을 검색 함)	15 (초)
exclude	path에서 directory 로 설정했을때 특정 파일을 제외해야 할 경우	-
exit_after_read	읽기 전용으로 파일을 읽을때 (파일내용이 변경되지 않는 상황에서 사용) true로 설정하면 파일 검색 비활성화 (프로세스 시작될때 디렉토리에 있는 파일만 읽고 , 파일 처리 후 수정된 경우 새로 추가된 항목만 로딩)	false
file_chunk_count	다음 파일로 이동하기 전에 각 파일에서 읽은 chunk 수를 설정 . file_check_count = 32, file_chun_size 32로 할 경우	461168 427387 903
file_chunck_size	디스크에서 block 혹은 chunk 단위로 읽을때 chunk에서 값 추출 .	
file_complete_action	read 모드인 경우 파일을 모두 읽었을때 수행하는 작업 (delete, log, log_and_delete 중 선 택)	delete
file_completed_log_path	file_complete_action 수행 후 기록할 파일 경로	
file_sort_by	pah에 설정된 경로의 파일들의 정렬 기준 (last_modified, path 중 선택)	last_mo d
file_sort_direction	file_sort_by에 정의된 정렬 기준에 따라 오름차순 혹은 내림차순 설정 (asc, desc 중 선택) * 가장 오래된 데이터를 먼저 불러와야 할 경우 last_modified + asc로 정의하면 됨 .	asc
ignore_older	지정된 기간 (초)이전에 마지막으로 수정된 파일이 있어도 해당파일은 skip 처리 . 단 , skip된 파일이 이후에 수정되면 데이터 로딩	- (설정할 경우 초단위로 설정
max_open_files	한번에 사용할 수 있는 file handler 갯수 (커널에 설정된 max_open_files 갯수 초과 설정 불 가)	4096
mode	파일을 읽어올때 사용하는 방식 (tail, read 중 선택) read에서만 사용할 수 있는 옵션 : ignore_older, file_completed_action, file_completed_log_path tail에서만 사용할 수 있는 옵션 : start_postion, close_older	tail
path	파일을 읽어들일 경로 설정	

- delete : 파일 삭제

- log : 파일 내용이 file_completed_log_path에 정의한 경로로 저장
- log_and_delete : file_completed_log_path에 정의한 경로로 저장 후 파일 삭제

- 최근에 수정된 날짜 기준으로 정렬

- 파일명 기준으로 정렬

- read모드 : 지정된 파일의 전체내용을 처리
- tail모드 : 변경된 파일의 내용을 추적해서 처리 . 대상파일이 복사 &붙여넣기 된 경우 새파 일로 인식하고 처음부터 읽어옴

sincedb_clean_after	마지막 timestamp 정보가 있는데 , 해당 설정값 동안 추적된 파일에서 변경사항이 없으면 sincedb에서 읽어들이지 않음	2(일단위
sincedb_path	디스크에 기록된 sincedb 파일 위치 (파일경로로 설정)	<path. > /plugin uts/file
sincedb_write_interval	모니터링할 로그파일의 현재 위치를 사용하여 DB에 쓰는 주기	15(초단위
start_postion	logstach가 처음으로 파일 읽기 시작하는 위치 (beginning, end 중 선택)	end
start_interval	파일이 수정되어 있는지 확인하기 위한 빈도	1 (초단위

3. Input - beat Config 값

설정값	설 명	기본값
add_hostname	7.0.0부터는 미사용	
cipher_suites	암호화할 리스트	1) 참고
client_inactivity_time out	클라이언트가 설정값동안 통신이 없으면 종료	60 (초
ecs_compatibility	ECS; Elastic Common Schema 호환성 (dislabled, v1 중 선택)	disab
host	수신대기할 IP	0.0.0
include_codec_tag	벤더사 정보 없음	true
port	수신할 포트	tcp/5

ssl	이벤트 전송시 암호화 전송	false
ssl_certificate	ssl 사용시 사용할 인증서	
ssl_certificate_authorities	ssl 사용시 인증서 유효성 검사	[]
ssl_handshake_time out	SSL handshake	1000 밀리초 단)
ssl_key	SSL사용시 사용할 SSL 키 (PKCS8 키여야 함)	
ssl_key_passphrase	SSL 사용시 ssl key 패스워드	
ssl_verify_mode	SSL 사용시 클라이언트 정보 확인 (none, peer,force_peer 중 선택)	none
ssl_peer_metadata	이벤트의 메타데이터를 인증서에 저장, ssl_verify_mode에서 force_peer로 설정되어 있어야 함	false
tls_max_version	SSL사용시 사용할 최대 인증서 버전	1.2
tls_min_version	SSL사용시 사용할 최소 인증서 버전	

- o disabled : ECS호환 템플릿 미사용
- o v1 : Elastic Common Schema V1과 호환되는 값 제공 (pipeline.ecs_compatibility 활성화 시 해당값 사용)
- o none : 클라이언트에게 인증서 제공 요청하지 않음
- o peer : 서버가 클라이언트에게 인증서 제공하도록 요청
- o force_peer : peer와 동일하나 , 클라이언트가 인증서를 제공하지 않는 경우 연결 종료

```
1) cipher_suites list :
java.lang.String[TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,


TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256]@459cfcca
```

4. output - Elasticsearch Config값

설정값	설 명	기본값
action	프토로콜에 영향받지 않는 작업 .	index
api_key	elasticsearch api 키를 사용해서 인증 . 해당 기능을 사용하려면 ssl 옵션이 활성화 되 어 있어야 함	
bulk_path	추가 확인필요	
cacert	ssl 구성을 위한 .cert 혹은 pem 파일 경로	
cloud_auth	elastic cloud 클라우드 인증문자열	
cloud_id	elastic cloud 웹콘솔 id	
doc_as_upsert	document_id가 elasticsearch에 없으면 새문서 생성	
document_id	인덱싱할 문서 ID,	
ecs_compatibility	ECS; Elastic Common Schema 호환성 (dislabled, v1 중 선택)	disabled
failure_type_logging_whitelist	로깅하지 않을 elasticsearch 오류값 설정	
custem_headers	각 요청에서 전송된 헤더로 키 /값 세트를 elasticsearch 노드로 전달할때 사용	
healthcheck_path	head 요청이 전송될때 백그라운드에서 서비스 요청에 적합하기 전에 확인	
hosts	원격 인스턴스의 호스트 설정	127.0.0.1
http_compression	http 요청시 gzip 압축 활성화	false
ilm_enabled	Index Lifecycle Management(ilm) 활성화 시 사용 (elasticsearch cluster 6.6.0, 기본 라이선스 이상 설치되어 있어야 함 (true, false, auto중 설정)	auto
ilm_pattern	ilm을 사용하기 위해 인덱스를 생성하기 위한 패턴 (패턴은 인덱스이름에 상관없이 0 으로 채워진 6자리 문자열)	now/d - 000
ilm_rollover_alias	ilm을 사용하기 위해 관리되는 인덱스 별칭	ecs_compat y에 따라 다름

index	이벤트로 사용할 인덱스명 , 인덱스를 일별로 분할이 기본값이며 대문자를 사용할 수 없음	ecs compat y에 따라 다 름
keystore	서버에 인증서를 제공하는데 사용되는 키 저장소 (.jks 혹은 .p12)	
keystore_password	keystore의 패스워드	
manage_template	추가 확인필요	
parameters	키 쌍값을 URL문자열로 전달	
parent	하위문서의 경우 상위 ID값	
password	SSL기반의 elasticsearch 클러스터에 인증하기위한 패스워드	
path	Elasticsearch가 설치된 http 경로	

o index : logstash의 이벤트를 인덱싱

o delete : ID값을 기준으로 문서삭제

o create : 문서를 인덱싱 . 이미 인덱싱되어 있는 경우에는 실패

o update : ID값을 기준으로 문서 업데이트

o disabled : ECS호환 템플릿 미사용

o v1 : Elastic Common Schema V1과 호환되는 값 제공 (pipeline.ecs_compatibility 활성화시 해당값 사용)

o true : lifecycle 사용

o false : 미사용

o ECS 활성화시 : ecs- logstash

o ECS 비활성화시 : logstash

o ECS 활성화시 : ecs- logstash-%{+yyyy.MM.DD}

o ECS 비활성화시 : logstash-%{+yyyy.MM.dd}

pipeline	이벤트에 대해 설정항 파이프라인 설정	nil

pool_max	output에 설정된 연결하기 위해 사용하는 최대 연결 수 (너무 낮은 경우 연결이 자 주 열렸다가 닫힘)	1000
pool_max_per_route	output에 설정된 연결하는 동안 필요한 엔드포인트 수	100
proxy	http 통신시 proxy 연결이 필요한 경우 입력	
recurrect_delay	백엔드 통신시 최대 서용하는 retry 횟수	5 (초단위)
retry_initial_interval	retry을 위한 inerval	2 (초단위)
retry_max_interval	최대 retry 를 위한 interval	64 (초단위)
retry_on_conflict	elasticsearch가 업데이틀 위해 시도하는 횟수	1
routing	이벤트 적용을 위해 적용할 라우팅값	
script	스크립트 업데이트 모드에 대한 이름 설정	
script_lang	script사용시 스크립트의 언어 Elasticsearch 6.0 이상에서 인덱싱된 스크립트를 사용 하는 경우 빈문자열로 설정	
script_type	script사용시 변수가 참조하는 유형 . (inline, indexed, file 중 선택)	inline
script_var_name	스크립트에 전달된 변수이름	event
scripted_upsert	true설정시 스크립트는 업데이트	false
sniffing	Elasticsearch에 모든 클러스토 노드 목록을 확인하고 호스트목록에 추가	false
sniffing_delay	sniffing 하기 위한 interval	5 (초 단위)
sniffing_path	스니핑 요청시 사용할 http 경로	
ssl	ElasticSearch클러스터에 SSL / TLS적용시 사용	false
ssl_certificate_verification	SSL 사용시 서버 인증서를 확인하는 옵션	true
template	템플릿 기능사용시 설정할 경로	
template_name	템플릿 이름 지정	ecs compat y에 따라 다 름

template_over write	true로 설정되어 있는 경우 Elasticsearch에 표시된 템플릿을 덮어쓰기	false
timeout	Elasticsearch로 보낸 작업의 시간 제한	60 (초단위)
truestore	서버 인증서 검증을 위한 경로 (.jks 혹은 .p12)	
truestore_pass word	trustore 저장소의 패스워드	
upsert	document_id가 없는 경우 json문자열로 새문서 생성	
user	보안 Elasticsearch 클러스터에 인증하기 위한 사용자 이름	
validate_after_inactivity	keepalived요청 사용시 대기하는 시간	10000 (밀리초단위)
version	인덱싱에 사용할 버전	

- o inline : 인라인유형의 스크립트

- o indexed : Elasticsearch에 인덱스된 스크립트 이름

- o file : Elasticsearch의 구성디렉토리에 저장된 이름

- o ECS 활성화시 : ecs- logstash

- o ECS 비활성화시 : logstash

version_type	interval, external, external_gt, external_gte, force 중 선택 interval : 지정된 버전이 저장된 문서의 버전과 동일한 경우에만 인덱스 external, external_gt : 지정된 버전이 저장된 문서의 버전보다 더 높거나 혹은 없는 경우에만 문서를 인덱싱 external_gte : 지정된 버전이 저장된 문서의 버전보다 같더나 높은 버전에만 문서 인 덱싱 (해당방식 사용시 데이터 손실 위험 존재)

5. Filter Config 값

필터종류	사용용도
aggregate	여러이벤트의 정보 집계
alter	mutate필터가 처리하지 않는 필드의 작업 수행
bytes	해당 숫자값으로 구문분석
cidr	네트워크 ip 주소 확인
cipher	이벤트에 암호 적용

clone	이벤트 복사
csv	쉼표 (,)로 구분된 데이터를 개별필드로 구문분석
date	logstash 타임스탬프로 사용하기 위해 날짜를 구문 분석
de_dot	필드이름에서 점을 제거
dissect	구분기호를 사용해서 구조화되지 않은 이벤트 데이터를 필드로 추출
dns	DNS값 설정
drop	모든 이벤트 삭제
elapsed	이벤트 처리 경과시간 계산
elasticsearch	Elasticsearch의 예전 이벤트에서 현재 이벤트로 복사
environment	환경 변수값을 메타 데이터 필드로 저장
extractnumbers	문자열에서 숫자를 추출
fingerprint	일관된 해시값으로 대체하여 필드 처리
geoip	ip주소에 지리정보 추가
grok	구조화되지 않은 이벤트를 필드로 구문분석
http	REST API와의 통합용으로 사용
i18n	필드에서 특수 문자 제거
java_uuid	uuid를 생성하고 이벤트 추가
jdbc_static	추가 확인필요
jdbc_streaming	추가 확인필요
json	json 포맷의 이벤트 구문 분석
json_encode	필드 데이터를 json으로 표현
kv	Key - Value 포맷 구문분석
memcached	memcached의 외부 데이터 통합
metricize	여러 메트릭을 포함하는 이벤트를 분석해서 각 단일 메트릭 / 여러 이벤트로 분석
metrics	메트릭 사용
mutate	추가 확인필요
prune	black / whitelist을 적용할 필드 목록을 기반으로 이벤트 데이터 정리
range	지정된 필드가 설정한 크기 혹은 길이 내에 있는지 확인

ruby	ruby 코드 실행
sleep	작업 대기 시간
split	다중라인의 메시지 혹은 문자열을 각각 이벤트로 분할
syslog_pri	syslog같이 메시지의 우선순위 필드를 구문분석
threats_classifier	보안로그 강화
throttle	이벤트수 제한
tld	기본메시지의 내용을 지정한 내용으로 치환
translate	특정필드의 데이터를 yaml 파일이나 hash로 전환
truncate	정의한 크기보다 큰 필드를 자름
urldecode	암호화된 URL과 필드 정보를 복호화
useragent	에이전트 문자열을 필드로 구문분석
uuid	이벤트에 uuid를 추가
wurfl_device_detection	OS에서 인식한 장치 정보를 로그에 포함
xml	xml을 필드로 구문분석 kSearch / Logstash(FielBeat) / Kibana 아키텍쳐

3. ElasticSearch Config값

설정값	설 명	기본값
path.data	데이터 경로	/var/data/elasticsearch
path.log	로그데이터 경로	/var/log/elasticsearch
cluster.name	클러스터 구성할때 다른노드와 공유할때 사용	elasticsearch
node.name	노드 ID	임의로 생성되는 UUID / 자리
network.host	클러스터 환경에서는 서버 실제 IP로 설정	loopback주소로 설정
discovery.seed.hosts	클러스터 환경에서 연결할 수 있는 노드목록 리스트	
cluster.initial_master_nodes	Elasticsearch 최초 구동시 마스터노드를 설정하기 위한 master 노드 목록	
bootstrap.memory_lock	프로세스 공간을 선언하고 heap memory가 스왑되지 않도록 설정 (해당기능 사용시 true설정)	false
jvm heap	-Xmx, -Xms 설정	

4. Kibana Config 값

분류	설정값	설명	기본값
서버설정	console.enabled	프로세스 실행시	true
서버보안	csp.rules	브라우저에서 불필요하고 안정하지 않은 특정기능을 비활성화	
서버보안	csp.strict	기본적인 CSP규칙을 적용하지 않는 브라우저에 대해 접속 차단	true
서버보안	csp.warnLegacyBrowsers	기본적인 CSP규칙을 적용하지 않은 브라우저접속시 경고메시지 출력 (csp.strict가 true되면 해당 기능은 무효화)	true
elasticsearch 연동	elasticsearch.customHeaders	Elasticsearch로 보낼 헤더이름 및 값	없음
elasticsearch 연동	elasticsearch.hosts	쿼리에 사용할 Elasticsearch URL	http://localhost:9200
elasticsearch 연동	elasticsearch.pingTimeout	Elasticsearch가 ping에 응답할때까지 기다리는 시간	30000(밀리 초단위)
elasticsearch 연동	elasticsearch.requestHeadersWhitelist	Elasticsearch로 보낼 kibana 클라이언트 헤더목록	없음 (헤더 보내지 않음)
elasticsearch 연동	elasticsearch.shardTimeout	elasticsearch가 샤드의 응답을 기다리는 시간 미사용시 0	30000(밀리초 단위)
elasticsearch 연동	elasticsearch.sniffInterval	elasticsearch에서 업데이트된 노드 목록 확인시간	false (밀리초 단위)
elasticsearch 연동	elasticsearch.sniffOnStart	프로세스 시작시 다른서버에 설치된 elasticsearch 를 찾을때 사용	false
elasticsearch 연동	elasticsearch.sniffOnConnectionFault	elasticsearch 연결 오류발생시 elasticsearch 노드목록 업데이트	false
elasticsearch ssl연동	elasticsearch.ssl.alwaysPresentCertificate	elasticsearch에서 인증서 요청시 클라이언트 인증서 전달	false
elasticsearch ssl연동	elasticsearch.ssl.certificate / elasticsearch.ssl.key	PEM으로 인코딩된 클라이언트 인증서와 개인키 경로	false
elasticsearch ssl연동	elasticsearch.ssl.certificateAuthorities	elasticsearch에서 신뢰할 수 있는 인증기간의 인증서 경로	false
elasticsearch ssl연동	elasticsearch.ssl.keyPassphrase	개인키를 복호화시 사용하는 암호	false
elasticsearch ssl연동	elasticsearch.ssl.keystore.path	클라이언트 인증서와 해당 개인키를 포함하는 PKCS#12키 저장소	false

elasticsearch ssl연동	elasticsearch.ssl.keystore.password	지정된 키 저장소를 복호화시 사용하는 암호	
elasticsearch ssl연동	elasticsearch.ssl.truststore.path	elasticsearch에서 신뢰할 수 있는 인증서 구성시 신뢰저장소의 경로	
elasticsearch ssl연동	elasticsearch.ssl.truststore. password	신뢰하는 저장소 복호화시 사용하는 암호	
elasticsearch ssl연동	elasticsearch.ssl.verificationMode	elasticsearch 아웃바운드 SSL/TLS연결시 수신하는 서버 인증서 (full, certificatem none 중 선택) • full : 호스트이름 확인 • certificate : 호스트 이름 사용안함 • none : 인증서 검증 무시	full
elasticsearch 연동	elasticsearch.username	elasticsearch에 기본인증이 설정되어 있는 경우 elasticsearch 사용자 정보	
elasticsearch 연동	elasticsearch.password	elasticsearch 기본인증이 설정되어 있는 경우 elasticsearch 사용자 패스워드	
elasticsearch 연동	enterpriseSearch.host	엔터프라이즈 검색을 위한 인스턴스 URL	
서버설정	interpreter.enableInVisualize	visualize에서 인터프리터 사용여부	true
서버설정	kibana.autocompleteTimeout	elasticsearch의 자동완성 대기시간	1000 (밀리 초단위)
서버설정	kibana. autocompleteTerminateAfter	elasticsearch 자동완성을 생성하기 위해 각 샤딩된 데이터 로그하는 최대 문서수	100000
서버설정	logging.dest	kibana로그 출력시 저장하는 파일	stdout
서버설정	logging.json	로그포맷을 json으로 기록 .	false
서버설정	logging.quiet	true로 설정시 오류메시지를 제외한 모든 로그 출력	false
서버설정	logging.silent	false로 설정시 모든 로그 데이터는 보이지 않음	false
서버설정	logging.timezone	표준시간대 설정	
서버설정	logging.verbose	true시 시스템 사용정보 및 모든 이벤트 로그저장	false
kibana map 설정	map.includeElasticMapsService	Elastic Maps Servive에 대해 연결을 비활성화하려면 설정	true
kibana map 설정	map. proxyElasticMapsServiceInMaps	kibana를 통해 모든 map용 app이 elastic maps service를 요청	false
kibana map 설정	map.regionmap	지도를 시각화 사용시 사용할 레이어 정보	

kibana map 설정	map.regionmap.layers[].attribution	map 사용시 geojson파일의 경로	
kibana map 설정	map.regionmap.layers[].fields[]	map 사용시 레이어에 노출하려면 geojson 기능 속성	
kibana map 설정	map.regionmap.layers[].fields[].description	지도 시각화 구성시 옵션탭 아래에 표시되는 텍스트문구	
kibana map 설정	map.regionmap.layers[].fields[].name	Elasticsearchdp 저장된 데이터와 geojson간 내부 결합시 사용 .	
kibana map 설정	map.regionmap.layers[].name	map 사용시 제공되는 지도설명	
kibana map 설정	map.regionmap.layers[].url	map사용시 geojson파일의 URL	
kibana map 설정	map.tilemap.options.attribution	지도 속성 문자열	
kibana map 설정	map.tilemap.options.maxZoom	최대 확대 수준	10
kibana map 설정	map.tilemap.options.minZoom	최소 확대 수준	1
kibana map 설정	map.tilemap.options.subdomains	서브 도메인 리스트	
kibana map 설정	map.tilemap.url	kibana가 타입맵 시각화시 사용하는 url	
서버설정	newsfeed.enabled	kibana ui알림센터에 뉴스피드 사용 설정	trure
서버설정	path.data	elasticearch에 저장되지 않는 데이터 경로	data
서버설정	pid.file	kibana pid파일 생성 경로	
서버설정	ops.interval	시스템 및 프로세스 성능 메트릭 샘플링 간격 (최소 100이상)	5000 (밀리 초단위)
서버설정	ops.cGroupOverrides.cpuPath	cgroup사용시 cpu 경로 정보	/proc/self/cgroup
서버설정	ops.cGroupOverrides.cpuAcctPath	cgroup사용시 cpuacct 경로 정보	/proc/self/cgroup
서버설정	server.basePath	kibana통신앞에 프록시가 존재하는 경우 kibna 마운트할 경로 server.rewriteBasePath 설정이 되어 있어야 하고 , 경로가 "/"로 마치면 안됨	
서버설정	server.publicBaseUrl	사용자가 kibana에 접속할 수 있는 URL	

서버설정		server.compression.enabled	모든 http응답에 압축사용여부	true
서버설정		server.compression. referrerWhitelist	kibana 앞에 reverse proxy가 존재하는 경우 referer 헤더를 기반으로 http응답시 압축을 사용여부 (server.compression.enabled가 활성화된 경우 해당값은 무시)	none
서버설정		server.customResponseHeaders	kibana서버에서 클라이언트로 응답보낼 헤더이름 / 값	없음
서버설정		server.host	호스트 설정 (원격연결 허용시 서버 IP주소 입력)	localhost
서버설정		server.keepaliveTimeout	keepalived 대기 시간	120000 (밀리 초 단위)
서버설정		server.maxPayloadBytes	수신서버의 최대 payload크기	1048576 (바이트 단위)
서버설정		server.name	kibana 인스턴스를 시벽하는 이름	hostname
서버설정		server.port	서버에서제공하는 포트	5601
서버설정		server.requestId.allowFromAnyIp	로그에서 요청을 식별하고 Elasticsearch로 전달하기 위해 모든 ip주소가 X- Opaque-ID 헤더를 신뢰하는지 설정	
서버설정		server.requestId.ipAllowlist	X-Opaque-id 헤더를 신뢰하는 IP주소목록	false
서버설정		server.rewriteBasePath	kibaka에서 reverse proxy에서 basepath rewrite하는지 설정	
서버설정		server.socketTimeout	closed 소켓 닫기 전 대기시간	120000 (밀리초단위)
서버 설정	SSL	server.ssl.certificate / server.ssl.key	PEM으로 인코딩된 클라이언트 인증서와 개인키 경로	
서버 설정	SSL	server.ssl.certificateAuthorities	신뢰할 수 있는 인증기간의 인증서 경로	
서버 설정	SSL	server.ssl.cipherSuites	ssl 암호목록	1)SSL 리스트 참고

서버 설정	SSL	server.ssl.clientAuthentication	클라이언트 연결에서 인증서 요청시 사용하는 설정값 • required : 클라이언트가인증서를 제시하지 않는한 연결 거부 • optional : 클라이언트가 인증서가 있는 경우 사용 • none : 클라이언트 인증서 검증 무시	none
서버 설정	SSL	server.ssl.enabled	kibana 접속시 ssl 사용여부	false
서버 설정	SSL	server.ssl.keyPassphrase	신뢰할 수 있는 인증기간의 인증서 경로	
서버 설정	SSL	server.ssl.keystore.path	신뢰할 수 있는 인증기간의 인증서 경로	
서버 설정	SSL	server.ssl.keystore.password	지정된 키 저장소를 복호화시 사용하는 암호	
서버 설정	SSL	server.ssl.truststore.path	신뢰할 수 있는 인증서 구성시 신뢰저장소의 경로	
서버 설정	SSL	server.ssl.truststore.password	신뢰하는 저장소 복호화시 사용하는 암호	
서버 설정	SSL	server.ssl.redirectHttpFromPort	모든 http 요청을 https로 리다이렉션 함	
서버 설정	SSL	server.ssl.supportedProtocols	지원되는 SSL프로토콜	TLSv1.1, TLSv1.2, TLSv1.3
서버보안		server.xsrf.allowlist	API 보호기능 비활성화	enable
서버보안		server.xsrf.disableProtection	ture설정시 kibana에서 사이트 위조방지 기능 비활성화	false
서버보안		status.allowAnonymous	true설정시 미인증사용자 사용불가	false
서버보안		telemetry. allowChangingOptInStatus	고급설정에서 원격 분석 설정 변경 가능	true
서버보안		telemetry.optIn	원격 데이터의 수집가능	true
서버보안		telemetry.enabled	클러스터 통계를 보고시 사용	true
서버보안		vis_type_vega.enableExternalUrls	모든 url을 사용하여 외부 데이터 소스 및 이미지에 액세스 할수 있도록 구성하려면 true 설정	false
xpack 설정		xpack.license_management. enabled	xpack 라이선스 관리 UI사용하지 않으려면 false	true

xpack 설정	xpack.rollup.enabled	xpack 롤업 UI를 사용하지 않으려면 설정	false	true
서버설정	i18n.locale	kibak인터페이스 언어 설정		en

1) SSL리스트 : TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_AES_128_GCM_SHA256 ECDHE-RSA-AES128-GCM-SHA256, ECDHE-ECDSA-AES128-GCM-SHA256, ECDHE-RSA-AES256-GCM-SHA384, ECDHE-ECDSA-AES256-GCM-SHA384, DHE-RSA-AES128-GCM- SHA256, ECDHE-RSA-AES128-SHA256, DHE-RSA-AES1

* CSP ; Content-Security-Policy (https://w3c.github.io/webappsec-csp/ 참고)

Revision #3

Created 2022-07-17 18:32:52 KST by artop0420

Updated 2024-11-11 10:33:23 KST by artop0420