version: '3.5'

# will contain all elasticsearch data.

volumes:

filebeat-data:

services:

# Docker Logs Shipper ------------------------------

filebeat:

image: docker.elastic.co/beats/filebeat:${ELK\_VERSION}

restart: always

# -e flag to log to stderr and disable syslog/file output

command: -e --strict.perms=false

user: root

environment:

ELASTIC\_USERNAME: ${ELASTIC\_USERNAME}

ELASTIC\_PASSWORD: ${ELASTIC\_PASSWORD}

KIBANA\_HOST\_PORT: ${KIBANA\_HOST}:${KIBANA\_PORT}

ELASTICSEARCH\_HOST\_PORT: https://${ELASTICSEARCH\_HOST}:${ELASTICSEARCH\_PORT}

volumes:

- ./filebeat/filebeat.docker.logs.yml:/usr/share/filebeat/filebeat.yml:ro

- /var/lib/docker/containers:/var/lib/docker/containers:ro

- /var/run/docker.sock:/var/run/docker.sock:ro

- filebeat-data:/var/lib/filebeat/data