

# EFK□□□□□

elasticsearch□docker-compose□□

```
version: '3.1'

services:
  elasticsearch:
    image: docker.elastic.co/elasticsearch/elasticsearch:7.6.2
    container_name: elasticsearch
    environment:
      - node.name=elasticsearch
      - discovery.type=single-node
      - bootstrap.memory_lock=true
      - "ES_JAVA_OPTS=-Xms512m -Xmx512m"
      - "ELASTIC_PASSWORD=iyfbvr1EM19jqjq"
      - "xpack.security.enabled=true"
    ulimits:
      memlock:
        soft: -1
        hard: -1
    volumes:
      - ./es_data: /usr/share/elasticsearch/data
    ports:
      - 9200: 9200
```

fluentd k8s□□□

```
---
apiVersion: v1
kind: ServiceAccount
metadata:
  name: fluentd
  namespace: kube-system
---
apiVersion: rbac.authorization.k8s.io/v1
```

```
kind: ClusterRole
```

```
metadata:
```

```
  name: fluentd
```

```
rules:
```

```
- apiGroups:
```

```
  - ""
```

```
  resources:
```

```
    - pods
```

```
    - namespaces
```

```
  verbs:
```

```
    - get
```

```
    - list
```

```
    - watch
```

```
---
```

```
kind: ClusterRoleBinding
```

```
apiVersion: rbac.authorization.k8s.io/v1
```

```
metadata:
```

```
  name: fluentd
```

```
roleRef:
```

```
  kind: ClusterRole
```

```
  name: fluentd
```

```
  apiGroup: rbac.authorization.k8s.io
```

```
subjects:
```

```
- kind: ServiceAccount
```

```
  name: fluentd
```

```
  namespace: kube-system
```

```
---
```

```
apiVersion: apps/v1
```

```
kind: DaemonSet
```

```
metadata:
```

```
  name: fluentd
```

```
  namespace: kube-system
```

```
  labels:
```

```
    k8s-app: fluentd-logging
```

```
    version: v1
```

```
spec:
```

```
  selector:
```

```
    matchLabels:
```

```
      k8s-app: fluentd-logging
```

```
    version: v1
template:
  metadata:
    labels:
      k8s-app: fluentd-logging
      version: v1
  spec:
    serviceAccount: fluentd
    serviceAccountName: fluentd
    tolerations:
      - key: node-role.kubernetes.io/control-plane
        effect: NoSchedule
      - key: node-role.kubernetes.io/master
        effect: NoSchedule
    containers:
      - name: fluentd
        image: fluent/fluentd-kubernetes-daemonset:v1-debian-elasticsearch
        env:
          - name: K8S_NODE_NAME
            valueFrom:
              fieldRef:
                fieldPath: spec.nodeName
          - name: FLUENT_ELASTICSEARCH_HOST
            value: "elasticsearch-logging"
          - name: FLUENT_ELASTICSEARCH_PORT
            value: "9200"
          - name: FLUENT_ELASTICSEARCH_SCHEME
            value: "http"
          # Option to configure elasticsearch plugin with self signed certs
          # =====
          - name: FLUENT_ELASTICSEARCH_SSL_VERIFY
            value: "true"
          # Option to configure elasticsearch plugin with tls
          # =====
          - name: FLUENT_ELASTICSEARCH_SSL_VERSION
            value: "TLSv1_2"
          # X-Pack Authentication
          # =====
          - name: FLUENT_ELASTICSEARCH_USER
            value: "elastic"
```

```

    - name: FLUENT_ELASTICSEARCH_PASSWORD
      value: "changeme"
resources:
  limits:
    memory: 200Mi
  requests:
    cpu: 100m
    memory: 200Mi
volumeMounts:
  - name: varlog
    mountPath: /var/log
# When actual pod logs in /var/lib/docker/containers, the following lines should be
used.
# - name: dockercontainerlogdirectory
#   mountPath: /var/lib/docker/containers
#   readOnly: true
# When actual pod logs in /var/log/pods, the following lines should be used.
- name: dockercontainerlogdirectory
  mountPath: /var/log/pods
  readOnly: true
terminationGracePeriodSeconds: 30
volumes:
  - name: varlog
    hostPath:
      path: /var/log
# When actual pod logs in /var/lib/docker/containers, the following lines should be
used.
# - name: dockercontainerlogdirectory
#   hostPath:
#     path: /var/lib/docker/containers
# When actual pod logs in /var/log/pods, the following lines should be used.
- name: dockercontainerlogdirectory
  hostPath:
    path: /var/log/pods

```

[[ dockercontainerlogdirectory docker]]

kibana[docke-compose]

```

version: '3'
services:

```

```
kibana:
  image: docker.elastic.co/kibana/kibana: 7.6.2
  ports:
    - 5601: 5601
  volumes:
    - ./kibana.yml: /usr/share/kibana/config/kibana.yml
```

kibana

```
#
# ** THIS IS AN AUTO-GENERATED FILE **
#

# Default Kibana configuration for docker target
server.name: kibana
server.host: "0"
elasticsearch.hosts: [ "http://192.168.5.23:9200" ]
xpack.monitoring.ui.container.elasticsearch.enabled: true
elasticsearch.username: elastic
elasticsearch.password: iyfbvr1EM19jqjq
```

---

```
# #1
# 5 2023 03:08:23
# 15 2025 14:56:20
```