로그 수집기 배포 구조 v1.0

namespace.yaml

```
apiVersion: v1
kind: Namespace
metadata:
  name: logging
```

- logging이라는 이름의 namespace를 생성한다.
- 로그 수집기 인스턴스들은 logging namespace를 사용한다.
- 리소스 분리를 위한 것으로, 로그 수집 범위와는 상관없다.

logstash-config

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: logstash-config
  namespace: logging
data:
  logstash.conf: |
    input {
      beats {
        port => 5044
      }
    }
    output {
      elasticsearch {
        hosts => ["http://elasticsearch.logging.svc.cluster.local:9200"]
        index => "logstash-%d-%%{+YYYY.MM.dd}"
      }
    }
```

- logstash 컨테이너에서 사용할 config 설정 내용을 사전 정의해 둔 파일이다.
- Beats 프로토콜을 사용해서 Filebeat로부터 5044포트를 통해 로그를 수신한다.
- logstash-%d-%%{}
  - %d에는 프로젝트 id가 들어간다.
  - %%는 java 문자열에서 %로 취급된다.
- Elasticsearch에서 인덱스명 logstash-projectId-YYYY.MM.dd 형식으로 조회 가능하다.
- 현재 Elasticsearch는 "http://elasticsearch.logging.svc.cluster.local:9200"로 클러스터 내 로컬 Elasticsearch로 지정돼 있는데, 이후 Elasticsearch 도메인이 결정되면 수정해야 한다.

logstash.yaml

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: logstash
  namespace: logging
spec:
  replicas: 1
  selector:
    matchLabels:
      app: logstash
  template:
    metadata:
      labels:
        app: logstash
    spec:
      containers:
      - name: logstash
        image: docker.elastic.co/logstash/logstash:7.17.9
        ports:
        - containerPort: 5044
        volumeMounts:
        - name: config-volume
          mountPath: /usr/share/logstash/pipeline/
      volumes:
      - name: config-volume
        configMap:
          name: logstash-config

---
apiVersion: v1
kind: Service
metadata:
  name: logstash
  namespace: logging
spec:
  ports:
  - port: 5044
    targetPort: 5044
  selector:
    app: logstash
```

Deployment

- pod수 : 1개 - 단일 레플리카
- logstash 컨테이너 내에 /usr/share/logstash/pipeline에 logstash-config.yaml 파일 설정 내용 마운트

Service

- port : 클러스터 내부에서 접속할 포트
- targetPort : 실제 컨테이너 포트
- 클러스터 내부에서 logstash.logging.svc.cluster.local:5044 형식으로 접근할 수 있게 된다.

filebeat-config.yaml

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: filebeat-config
  namespace: logging
data:
  filebeat-config.yaml: |
    filebeat.inputs:
    - type: log
      paths:
        - /var/log/*.log
      scan_frequency: 5s
      ignore_older: 1h # 1시간 이후 것은 무시
      close_inactive: 5m

    output.logstash:
      hosts: ["logstash.logging.svc.cluster.local:5044"]
      # logstash로 로그 전송. logging :네임스페이스, 5044 기본 포트.
```

- filebeat 컨테이너에서 사용할 config 설정 내용을 사전 정의해 둔 파일이다.
- 로그 수집 대상은 /var/log/*.log이다.
- 5초마다 변경 사항을 스캔한다.
- 1시간보다 오래된 로그는 무시한다.
- Logstash 서비스인 logstash.logging.svc.cluster.local:5044로 보낸다.

filebeat.yaml

```
apiVersion: apps/v1
kind: DaemonSet # 클러스터의 모든 노드에 Filebeat를 배포하기 위해 사용
metadata:
  name: filebeat
  namespace: logging
spec:
  selector:
    matchLabels:
      app: filebeat
  template:
    metadata:
      labels:
        app: filebeat
    spec:
      containers:
      - name: filebeat
        image: docker.elastic.co/beats/filebeat:7.17.9
        args: [
          "-c", "/etc/filebeat.yaml",
          "-e"
```

```
        ]
        volumeMounts:
        - name: config
          mountPath: /etc/filebeat.yaml
          subPath: filebeat-config.yaml
        - name: shared-logs
          mountPath: /var/log
        securityContext:
          runAsUser: 0
      volumes:
      - name: config
        configMap:
          name: filebeat-config
      - name: shared-logs
        hostPath:
          path: /var/log
```

- DaemonSet으로 지정해서 클러스터 내 모든 노드에서 로그를 수집한다.
- 볼륨 마운트
  - 컨테이너 내부 /etc/filebeat.yaml
    - 여기에 filebeat-config.yaml의 config 내용을 적용한다.
  - /var/log