02-filebeat-rbac.yml 이해

- RBAC(Role based access control)
- Filebeat가 쿠버네티스 클러스터 내에서 정상적으로 동작하기 위한 허가증을 발급하는 과정입니다.

```yaml
apiVersion: v1
kind: ServiceAccount # ServiceAccount 종류의 리소스를 만듭니다.
metadata:
  name: filebeat # 이름을 "filebeat"로 지정합니다.
  namespace: logging # logging 네임스페이스 내에 만듭니다.
```

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: filebeat
rules:
  - apiGroups: [""] # ""는 core API group을 지칭합니다.
    resources:
      - namespaces
      - pods
      - nodes
    verbs:
      - get
      - watch
      - list
```

> filebeat라는 이름의 ClusterRole, 즉 "클러스터 전체에 적용되는 역할(권한 묶음)을 정의합니다.

- kind: ClusterRole
    - 특정 네임스페이스가 아닌, 클러스터 전체에 적용되는 권한을 정의합니다.
- rules: 어떤 권한을 가질지 구체적으로 명시합니다.
    - resources : 네임스페이스, 파드, 노드 정보에 접근할 수 있습니다.
        - Filebeat는 해당 정보를 바탕으로 로그에 이 로그는 어떤 파드에서 발생했고, 그 파드는 어떤 노드에 있는지 등의 메타데이터를 추가할 수 있습니다.
    - verbs : 위 리소스들에 대해 조회 (get, list), 변경 사항을 감시할 수 있는 행동 권한을 부여합니다.

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: filebeat
subjects:
  - kind: ServiceAccount
    name: filebeat
```

```
    namespace: logging
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: filebeat
```

> ClusterRoleBinding: '누구에게 권한을 줄 것인가?'를 정하기 위해 사용합니다.

- ClusterRole을 특정 대상에게 Binding해주는 역할을 수행합니다.
- kind: ClusterRoleBinding
    - ClusterRole을 특정 주체(subject)에게 연결합니다.
- subjects: 권한을 부여받을 대상을 지정합니다.
    - kind: ServiceAccount: 파드와 같은 프로그램이 사용하는 "서비스 계정"에게 권한을 줍니다.
    - name: filebeat: logging 네임스페이스에 있는 filebeat라는 이름의 서비스 계정을 지정합니다.
- roleRef: 연결할 역할을 지정합니다.
    - kind: ClusterRole: ClusterRole 종류의 권한을 연결합니다.
    - name: filebeat: 위에서 정의한 filebeat라는 이름의 ClusterRole을 지정합니다.

> Filebeat만을 위한 전용 filebeat 서비스 계정을 만들어서 권한을 부여합니다.

- ServiceAccount 개념

1. User Account
    - kubectl 명령어를 직접 사용하는 개발자나 관리자입니다.
2. Service Account
    - 클러스터 안에서 실행되는 파드(Pod)나 애플리케이션이 사용하는 계정입니다.