롤 vs. 클러스터 롤

앞서 설명한 것처럼 롤과 롤 바인딩은 네임스페이스에 한정되는 오브젝트입니다. 따라서 롤은 포드, 서비스, 디플로이먼트 등과 같이 네임스페이스에 한정된 오브젝트에 대한 권한을 정의하기 위해 사용할 수 있습니다. 그렇지만 지금까지 다뤘던 오브젝트 중에는 노드(nodes), 퍼시스턴트 볼륨 등과 같이 네임스페이스에 종속되지 않는 오브젝트도 존재합니다.

물론 클러스터 수준의 오브젝트들에 대한 접근 권한은 서비스 어카운트에 기본적으로 설정돼 있지 않습니다. 이전에 생성해 뒀던 alicek106 서비스 어카운트로 노드의 목록을 출력해 보면 cluster scope의 리소스를 사용할 수 없다는 에러가 출력됩니다. 이와 유사하게 모든 네임스페이스의 리소스를 출력하는 명령어 또한 에러를 출력합니다.

```
$ kubectl get nodes --as system:serviceaccount:default:alicek106
Error from server (Forbidden): nodes is forbidden: User "system:serviceaccount:default:alic
ek106" cannot list resource "nodes" in API group "" at the cluster scope

$ kubectl get services --as system:serviceaccount:default:alicek106 --all-namespaces
Error from server (Forbidden): services is forbidden: User "system:serviceaccount:default:alic
ek106" cannot list resource "services" in API group "" at the cluster scope
```

이런 경우에는 롤 대신 클러스터 롤을 사용할 수 있습니다. 클러스터 롤이라는 이름이 나타내는 것처럼 클러스터 롤은 클러스터 단위의 리소스에 대한 권한을 정의하기 위해 사용합니다. 이번에는 노드의 목록을 출력하기 위한 클러스터 롤을 생성해 보겠습니다. 아래의 내용으로 YAML 파일을 작성합니다.

예제 10.3 chapter10/nodes-reader-clusterrole.yaml

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  namespace: default
  name: nodes-reader
rules:
- apiGroups: [""]
  resources: ["nodes"]
  verbs: ["get", "list"]
```

클러스터 롤의 YAML 파일은 이전에 생성했던 롤의 내용과 크게 다르지 않습니다. kind가 ClusterRole로 설정됐다는 점을 제외하면 다른 부분은 거의 같습니다. resources 항목에 nodes를,