K8s 시크릿

특징

- 시크릿은 패스워드, 토큰, 키처럼 보안이 필요한 데이터를 저장하는 데 사용한다. 보안 데이터의 노출 리스크를 줄이기 위해 사용된다. 사이즈는 1MB 미만이어야 한다.
- 서비스 어카운트를 만들면 서비스 어카운트의 토큰을 담은 시크릿이 네임스페이스에 자동으로 생성된다. 해당 토큰은 RBAC 기반의 접근 제어에 사용된다.
- 사용자가 시크릿을 등록하면 파드의 환경 변수나 마운트된 볼륨의 파일을 통해 접근할 수 있다.
- 시크릿은 네임스페이스에 속하며 다른 네임스페이스에서는 읽을 수 없다.
- 시크릿 자체는 암호화와는 직접적인 관계가 없으며 벤더가 제공하는 추가적인 암호화 기능을 사용할 수도 있다
- 파드가 시크릿을 사용하도록 설정했으면 기동하기 전에 시크릿이 존재해야 한다.

시크릿 이용

Base64 인코드

```
$ echo -n 'my_id' | base64
bXlfaWQ=
$ echo -n 'my_password' | base64
bXlfcGFzc3dvcmQ=
```

secret yml

```
apiVersion: v1
kind: Secret
metadata:
  name: db-credentials
type: Opaque
data:
  username: bXlfaWQ=
  password: bXlfcGFzc3dvcmQ=
```

command

```
$ kubectl apply -f db_credentals.yml
```

get secret

```
$ kubectl get secret

NAME                  TYPE                                  DATA   AGE
db-credentials        Opaque                                2      17s
default-token-mwh6r   kubernetes.io/service-account-token   3      4d5h
tls-certificate       kubernetes.io/tls                     2      46h
```

my yml

```
apiVersion: v1
kind: Pod
metadata:
  name: web-apl
spec:
  containers:
  - name: nginx
    image: nginx
    env:
      - name: DB_USERNAME ## 환경 변수
        valueFrom:
          secretKeyRef:
            name: db-credentials ## 시크릿명
            key: username ## 시크릿 키
      - name: DB_PASSWORD ## 환경 변수
        valueFrom:
          secretKeyRef:
            name: db-credentials
            key: password
```

command

```
$ kubectl apply -f reg_secret_env.yml
pod/web-apl created

$ kubectl get po
NAME                       READY   STATUS    RESTARTS   AGE
bustbox                    0/1     Error     0          3h58m
web-apl                    1/1     Running   0          11s
web-php-7b7566bd54-nvm7n   1/1     Running   0          4h6m

$ kubectl exec -it web-apl -- bash -c 'echo $DB_USERNAME, $DB_PASSWORD'
my_id, my_password
```

컨테이너에서 시크릿을 볼륨으로 마운트하는 매니페스트

```
apiVersion: v1
kind: Pod
metadata:
  name: web
spec:
  containers:
  - name: nginx
    image: nginx
    ports:
    - protocol: TCP
      containerPort: 443
    volumeMounts: ## 마운트 정의
    - name: cert-vol ## 시크릿의 볼륨 이름
      mountPath: /etc/cert ## 컨테이너상의 마운트 경로
  volumes: ## 볼륨 정의
  - name: cert-vol ## 시크릿의 볼륨 이름
    secret:
      secretName: www-cert ## 시크릿의 이름
```

관련 문서

- Kubernetes