What is a Secret?

A Secret is an object that contains sensitive data, like passwords, OAuth tokens, or SSH keys.

Secret YAML Definition Example

Here's an example of a Secret defined in YAML, storing a username and password.

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: my-secret
type: Opaque
data:
  username: bXl1c2Vy  # base64 encoded value of 'myuser'
  password: bXlwYXNzd29yZA==  # base64 encoded value of 'mypassword'
```

Using Secrets in Pods
1. As Environment Variables

You can inject the keys in a Secret as environment variables inside a Pod.

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: mypod
spec:
  containers:
    - name: mycontainer
      image: nginx
      envFrom:
        - secretRef:
            name: my-secret
```

💡 Explanation: This makes the keys username and password from the my-secret Secret available as environment variables inside the mypod container.

2. As Volumes

You can mount the Secret as a volume to make its keys available as files in the container.

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: mypod
spec:
  containers:
    - name: mycontainer
      image: nginx
      volumeMounts:
        - name: secret-volume
          mountPath: /etc/secrets  # Secret files will be mounted here
  volumes:
    - name: secret-volume
      secret:
        secretName: my-secret
```

Secrets commands

```
# 1. Create a Secret from a literal key-value pair
kubectl create secret generic <secret-name> --from-literal=<key>=<value>

# 2. Create a Secret from a file
kubectl create secret generic <secret-name> --from-file=<key>=<file-path>

# 3. Create a Secret from a directory
kubectl create secret generic <secret-name> --from-file=<directory-path>

# 4. Apply a Secret from a YAML file
kubectl apply -f secret.yaml

# 5. List all Secrets in the current namespace
kubectl get secrets

# 6. Get detailed information about a specific Secret
kubectl describe secret <secret-name>

# 7. Edit a Secret (open the editor to modify it)
kubectl edit secret <secret-name>

# 8. Delete a Secret
kubectl delete secret <secret-name>

# 9. Get the content of a Secret in YAML format
kubectl get secret <secret-name> -o yaml

# 10. Decode a base64 value from a Secret
echo "<base64-encoded-value>" | base64 --decode
```