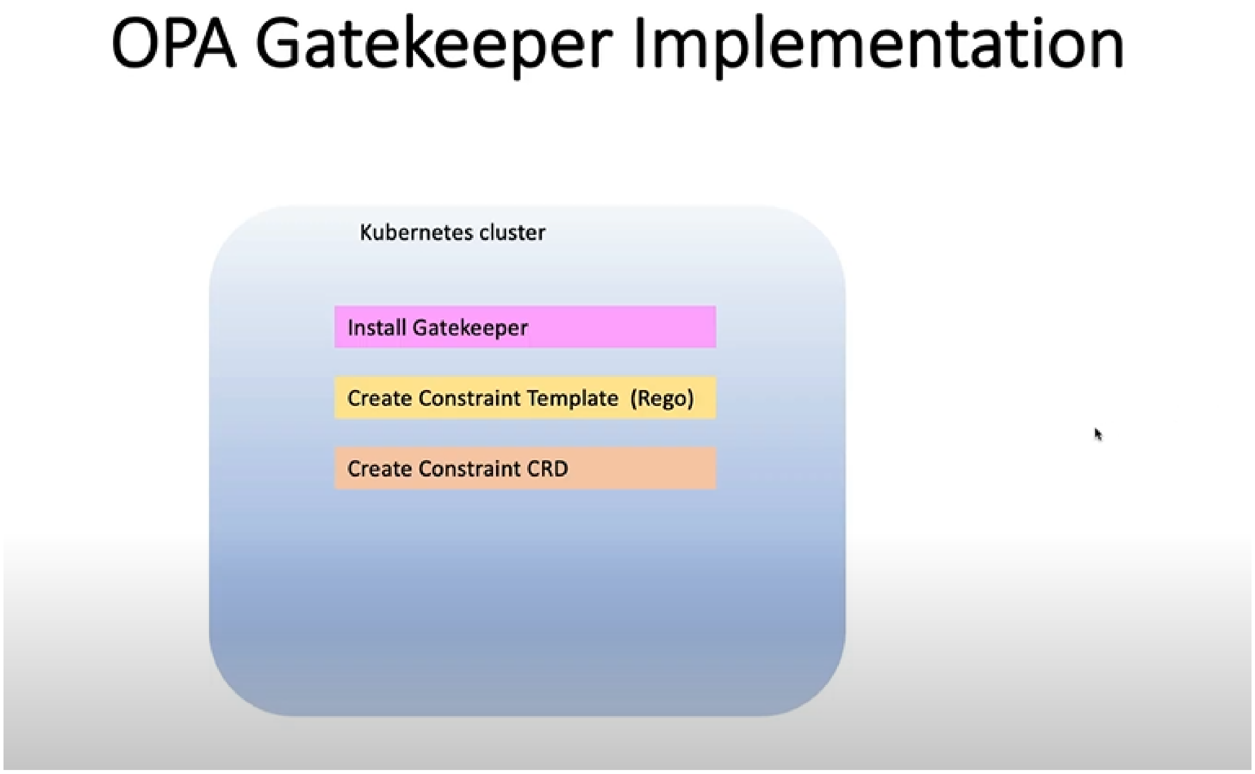
block - loadbalancer services

An OPA policy that enforces a `block-loadbalancer-services` rule in Kubernetes is a policy that is designed to prevent the creation or updating of Kubernetes Services that use the `LoadBalancer` type.

The `LoadBalancer` type is a type of Kubernetes Service that creates an external load balancer in the cloud provider's network. This type of Service is typically used to expose an application to the internet or other external networks. However, this can also be a security risk if not properly configured or if the Service is unnecessary.

The OPA policy enforces the `block-loadbalancer-services` rule by evaluating Kubernetes Service requests against the policy. If the Service request includes a `LoadBalancer` type, the policy will deny the creation or updating of the Service.

Implementation:



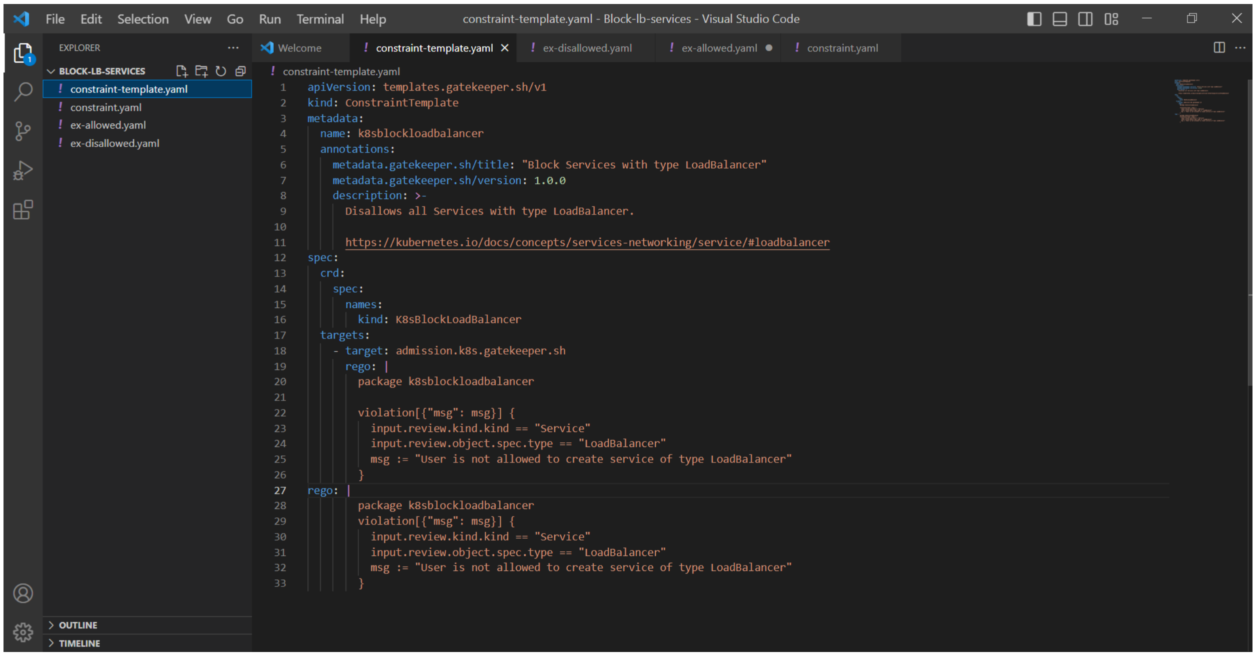
OPA Gatekeeper Implementation

Kubernetes cluster

Install Gatekeeper

Create Constraint Template (Rego)

Create Constraint CRD



```yaml
apiVersion: templates.gatekeeper.sh/v1
kind: ConstraintTemplate
metadata:
  name: k8sblockloadbalancer
  annotations:
    metadata.gatekeeper.sh/title: "Block Services with type LoadBalancer"
    metadata.gatekeeper.sh/version: 1.0.0
    description: >-
      Disallows all Services with type LoadBalancer.

      https://kubernetes.io/docs/concepts/services-networking/service/#loadbalancer
spec:
  crd:
    spec:
      names:
        kind: K8sBlockLoadBalancer
  targets:
    - target: admission.k8s.gatekeeper.sh
      rego: |
        package k8sblockloadbalancer

        violation[{"msg": msg}] {
          input.review.kind.kind == "Service"
          input.review.object.spec.type == "LoadBalancer"
          msg := "User is not allowed to create service of type LoadBalancer"
        }
rego: |
        package k8sblockloadbalancer
        violation[{"msg": msg}] {
          input.review.kind.kind == "Service"
          input.review.object.spec.type == "LoadBalancer"
          msg := "User is not allowed to create service of type LoadBalancer"
        }
```

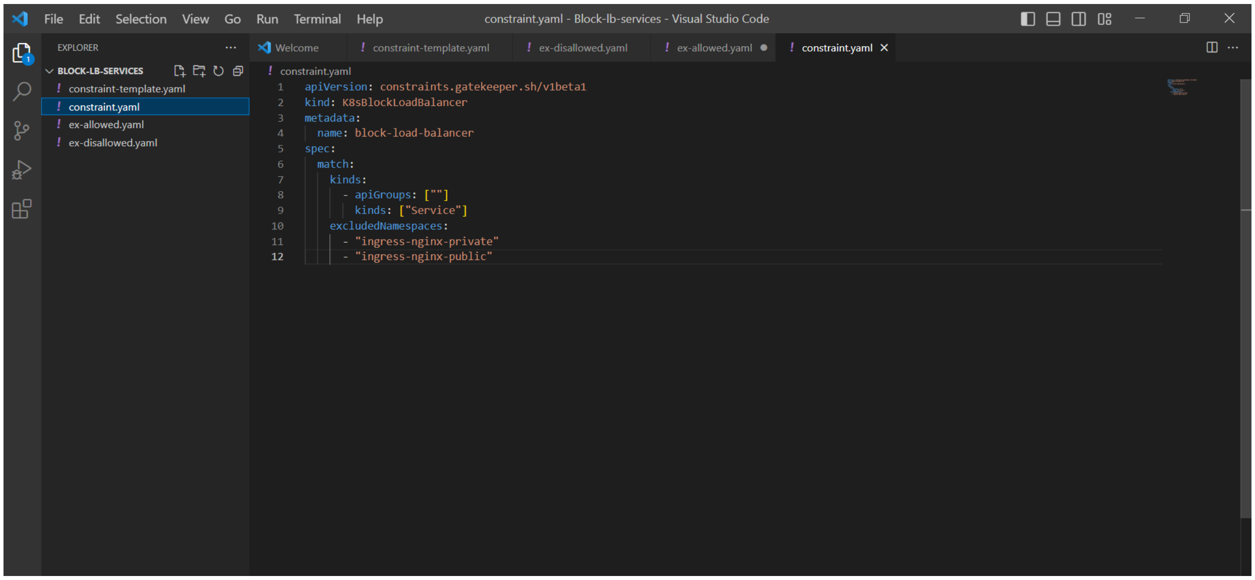
This YAML code describes a Kubernetes Gatekeeper constraint template that is used to enforce a policy that blocks the creation of services with type `LoadBalancer` in a Kubernetes cluster.

The `apiVersion` field specifies the API version for the Kubernetes custom resource definition (CRD) for this constraint template, which is `templates.gatekeeper.sh/v1`. This is the API version used by the Gatekeeper project.

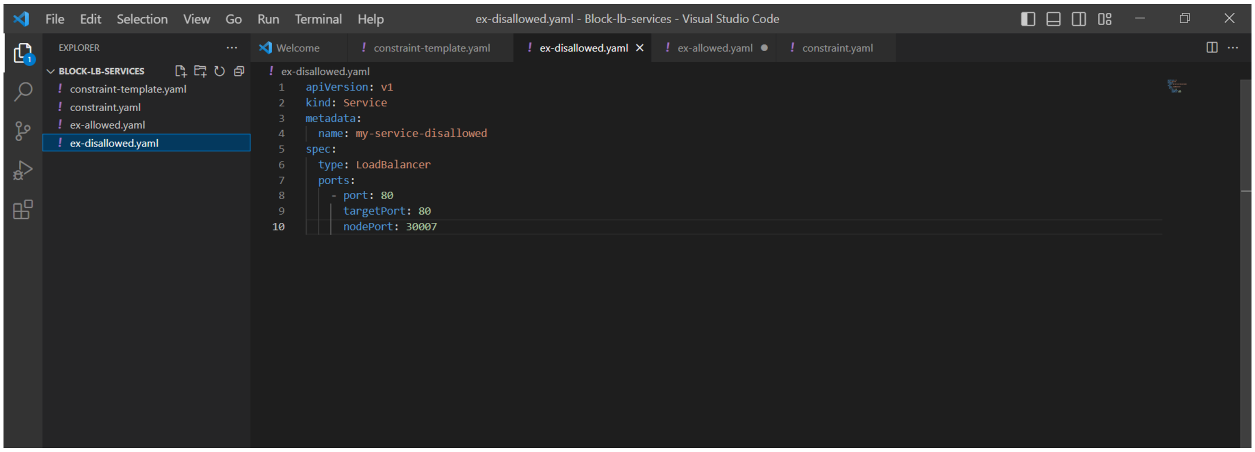
The `kind` field specifies the type of resource, which is `ConstraintTemplate`.

The `metadata` field contains information about the constraint template. The `name` field specifies a name for the constraint template, which is `k8sblockloadbalancer`. The `annotations` field contains metadata about the template, including a title, version, and description.

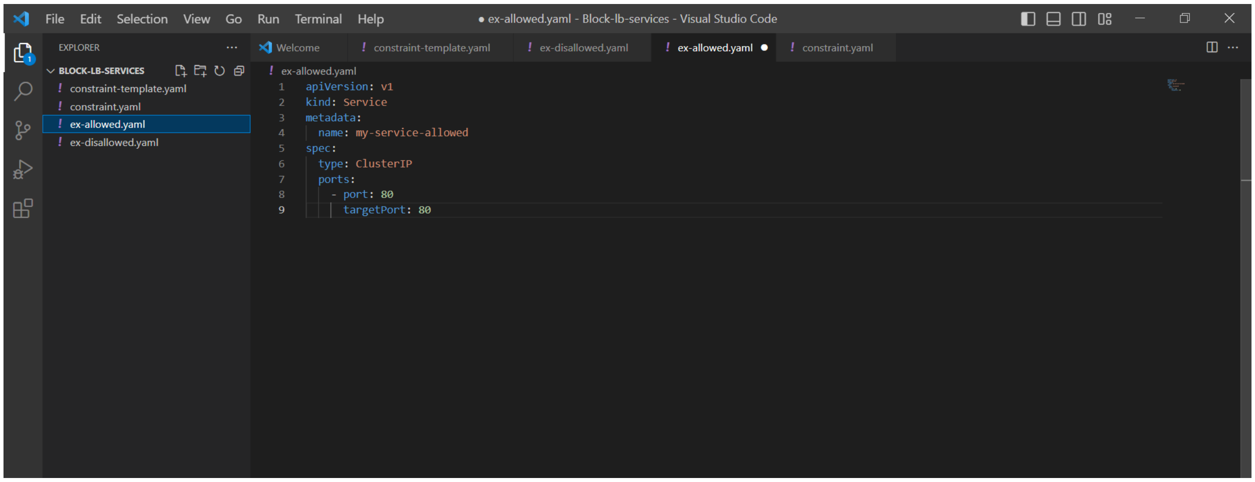
The `spec` field contains the actual policy definition for the constraint template. In this case, it defines a CRD for the policy with a `kind` of `K8sBlockLoadBalancer`. The `targets` field specifies the target of the policy, which is the admission controller for Kubernetes Gatekeeper. The `rego` field contains the actual policy written in the Rego language, which checks whether the incoming service object has a `type` of `LoadBalancer`, and if so, it returns a violation message stating that the user is not allowed to create services of this type.



```yaml
apiVersion: constraints.gatekeeper.sh/v1beta1
kind: K8sBlockLoadBalancer
metadata:
  name: block-load-balancer
spec:
  match:
    kinds:
      - apiGroups: [""]
        kinds: ["Service"]
    excludedNamespaces:
      - "ingress-nginx-private"
      - "ingress-nginx-public"
```

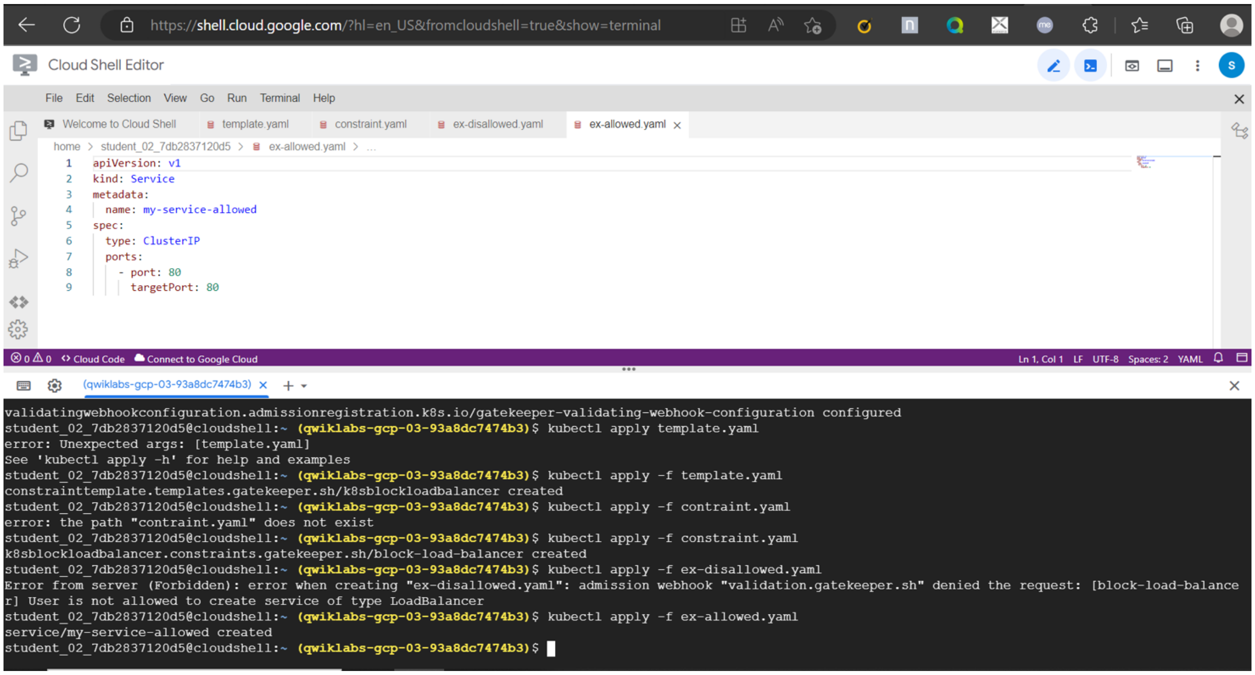


```yaml
apiVersion: v1
kind: Service
metadata:
  name: my-service-disallowed
spec:
  type: LoadBalancer
  ports:
    - port: 80
      targetPort: 80
      nodePort: 30007
```



```yaml
apiVersion: v1
kind: Service
metadata:
  name: my-service-allowed
spec:
  type: ClusterIP
  ports:
    - port: 80
      targetPort: 80
```

Output:



https://shell.cloud.google.com/?hl=en_US&fromcloudshell=true&show=terminal
Cloud Shell Editor
File Edit Selection View Go Run Terminal Help
Welcome to Cloud Shell
template.yaml
constraint.yaml
ex-disallowed.yaml
ex-allowed.yaml
home > student_02_7db2837120d5 > ex-allowed.yaml > ...
0 0 Cloud Code Connect to Google Cloud
Ln 1, Col 1 LF UTF-8 Spaces: 2 YAML
(qwiklabs-gcp-03-93a8dc7474b3)

```yaml
apiVersion: v1
kind: Service
metadata:
  name: my-service-allowed
spec:
  type: ClusterIP
  ports:
    - port: 80
      targetPort: 80
```

```
validatingwebhookconfiguration.admissionregistration.k8s.io/gatekeeper-validating-webhook-configuration configured
student_02_7db2837120d5@cloudshell:~ (qwiklabs-gcp-03-93a8dc7474b3)$ kubectl apply template.yaml
error: Unexpected args: [template.yaml]
See 'kubectl apply -h' for help and examples
student_02_7db2837120d5@cloudshell:~ (qwiklabs-gcp-03-93a8dc7474b3)$ kubectl apply -f template.yaml
constrainttemplate.templates.gatekeeper.sh/k8sblockloadbalancer created
student_02_7db2837120d5@cloudshell:~ (qwiklabs-gcp-03-93a8dc7474b3)$ kubectl apply -f contraint.yaml
error: the path "contraint.yaml" does not exist
student_02_7db2837120d5@cloudshell:~ (qwiklabs-gcp-03-93a8dc7474b3)$ kubectl apply -f constraint.yaml
k8sblockloadbalancer.constraints.gatekeeper.sh/block-load-balancer created
student_02_7db2837120d5@cloudshell:~ (qwiklabs-gcp-03-93a8dc7474b3)$ kubectl apply -f ex-disallowed.yaml
Error from server (Forbidden): error when creating "ex-disallowed.yaml": admission webhook "validation.gatekeeper.sh" denied the request: [block-load-balance
r] User is not allowed to create service of type LoadBalancer
student_02_7db2837120d5@cloudshell:~ (qwiklabs-gcp-03-93a8dc7474b3)$ kubectl apply -f ex-allowed.yaml
service/my-service-allowed created
student_02_7db2837120d5@cloudshell:~ (qwiklabs-gcp-03-93a8dc7474b3)$
```

In the above image tested the constraint by attempting to create a Kubernetes service with a type of LoadBalancer,that resulted in a denial and a message indicating that the user is not allowed to create services of this type.