Implementing OPA Gatekeeper Policies in Kubernetes

# Step-by-Step Guide

## 1. Install OPA Gatekeeper on Kubernetes

Use the official Gatekeeper manifests to install it:  
  
kubectl apply -f https://raw.githubusercontent.com/open-policy-agent/gatekeeper/release-3.12/deploy/gatekeeper.yaml

## 2. Create a ConstraintTemplate to Restrict "latest" Image Tags

Save the following YAML as deny-latest-tag-template.yaml and apply it:  
  
apiVersion: templates.gatekeeper.sh/v1beta1  
kind: ConstraintTemplate  
metadata:  
 name: k8sdenylatesttag  
spec:  
 crd:  
 spec:  
 names:  
 kind: K8sDenyLatestTag  
 targets:  
 - target: admission.k8s.gatekeeper.sh  
 rego: |  
 package k8sdenylatesttag  
  
 violation[{"msg": msg}] {  
 container := input.review.object.spec.containers[\_]  
 endswith(container.image, ":latest")  
 msg := sprintf("Container image '%s' uses the 'latest' tag, which is not allowed.", [container.image])  
 }

## 3. Create a Constraint to Enforce the Above Template

Save the following YAML as deny-latest-tag.yaml and apply it:  
  
apiVersion: constraints.gatekeeper.sh/v1beta1  
kind: K8sDenyLatestTag  
metadata:  
 name: deny-latest-tag  
spec:  
 match:  
 kinds:  
 - apiGroups: [""]  
 kinds: ["Pod"]

## 4. Create a Template to Enforce Resource Limits

Save this YAML as k8srequiredresources-template.yaml:  
  
apiVersion: templates.gatekeeper.sh/v1beta1  
kind: ConstraintTemplate  
metadata:  
 name: k8srequiredresources  
spec:  
 crd:  
 spec:  
 names:  
 kind: K8sRequiredResources  
 targets:  
 - target: admission.k8s.gatekeeper.sh  
 rego: |  
 package k8srequiredresources  
  
 violation[{"msg": msg}] {  
 container := input.review.object.spec.containers[\_]  
 not container.resources.requests.cpu  
 msg := "CPU requests must be specified."  
 }  
  
 violation[{"msg": msg}] {  
 container := input.review.object.spec.containers[\_]  
 not container.resources.limits.memory  
 msg := "Memory limits must be specified."  
 }

## 5. Create Constraint to Enforce Resource Requests/Limits

Save the following YAML as k8srequiredresources.yaml:  
  
apiVersion: constraints.gatekeeper.sh/v1beta1  
kind: K8sRequiredResources  
metadata:  
 name: container-must-have-resources  
spec:  
 match:  
 kinds:  
 - apiGroups: [""]  
 kinds: ["Pod"]

Apply all configurations using kubectl apply -f <filename>.