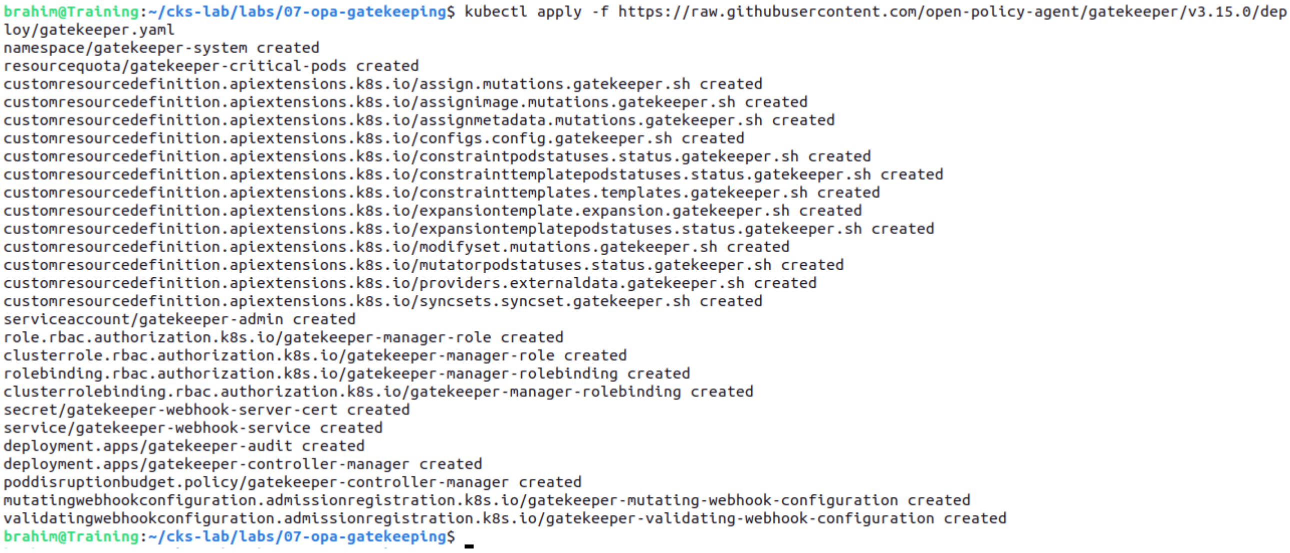
Lab07 - OPA Gatekeeping for Pods

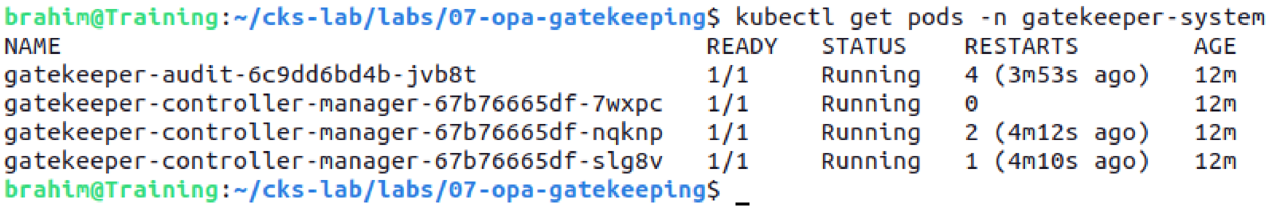
Your organization decides to introduce and enforce policies for Pods. You will create an Object Policy Agent (OPA) constraint and then verify the correct enforcement.

1. **Install the OPA gatekeeper objects with the version 3.15. Refer to the [OPA gatekeeper installation documentation](https://open-policy-agent.github.io/gatekeeper/website/docs/install/).**



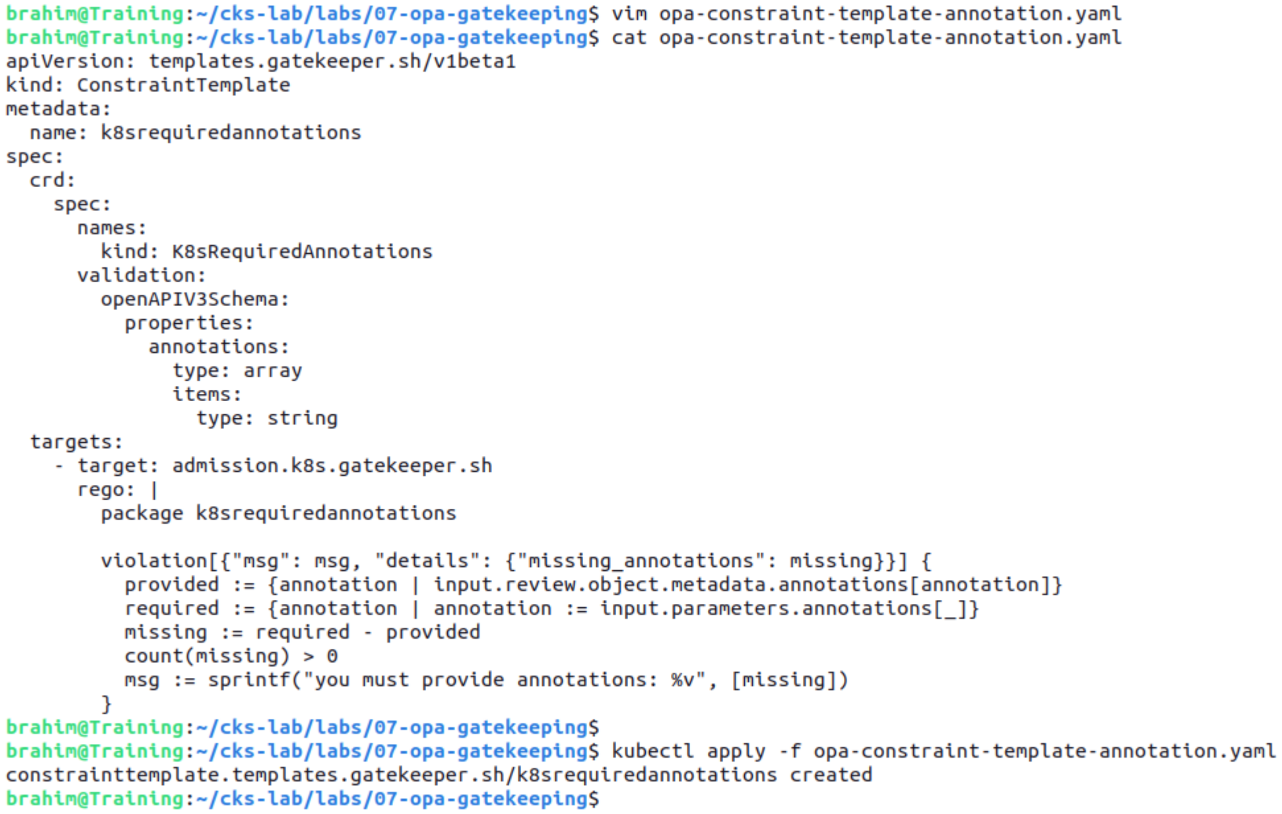
```
brahim@Training:~/cks-lab/labs/07-opa-gatekeeping$ kubectl apply -f https://raw.githubusercontent.com/open-policy-agent/gatekeeper/v3.15.0/dep
loy/gatekeeper.yaml
namespace/gatekeeper-system created
resourcequota/gatekeeper-critical-pods created
customresourcedefinition.apiextensions.k8s.io/assign.mutations.gatekeeper.sh created
customresourcedefinition.apiextensions.k8s.io/assignimage.mutations.gatekeeper.sh created
customresourcedefinition.apiextensions.k8s.io/assignmetadata.mutations.gatekeeper.sh created
customresourcedefinition.apiextensions.k8s.io/configs.config.gatekeeper.sh created
customresourcedefinition.apiextensions.k8s.io/constraintpodstatuses.status.gatekeeper.sh created
customresourcedefinition.apiextensions.k8s.io/constrainttemplatepodstatuses.status.gatekeeper.sh created
customresourcedefinition.apiextensions.k8s.io/constrainttemplates.templates.gatekeeper.sh created
customresourcedefinition.apiextensions.k8s.io/expansiontemplate.expansion.gatekeeper.sh created
customresourcedefinition.apiextensions.k8s.io/expansiontemplatepodstatuses.status.gatekeeper.sh created
customresourcedefinition.apiextensions.k8s.io/modifyset.mutations.gatekeeper.sh created
customresourcedefinition.apiextensions.k8s.io/mutatorpodstatuses.status.gatekeeper.sh created
customresourcedefinition.apiextensions.k8s.io/providers.externaldata.gatekeeper.sh created
customresourcedefinition.apiextensions.k8s.io/syncsets.syncset.gatekeeper.sh created
serviceaccount/gatekeeper-admin created
role.rbac.authorization.k8s.io/gatekeeper-manager-role created
clusterrole.rbac.authorization.k8s.io/gatekeeper-manager-role created
rolebinding.rbac.authorization.k8s.io/gatekeeper-manager-rolebinding created
clusterrolebinding.rbac.authorization.k8s.io/gatekeeper-manager-rolebinding created
secret/gatekeeper-webhook-server-cert created
service/gatekeeper-webhook-service created
deployment.apps/gatekeeper-audit created
deployment.apps/gatekeeper-controller-manager created
poddisruptionbudget.policy/gatekeeper-controller-manager created
mutatingwebhookconfiguration.admissionregistration.k8s.io/gatekeeper-mutating-webhook-configuration created
validatingwebhookconfiguration.admissionregistration.k8s.io/gatekeeper-validating-webhook-configuration created
brahim@Training:~/cks-lab/labs/07-opa-gatekeeping$ _
```

   - Ensure that the OPA gatekeeper objects transition into the "Running" status.



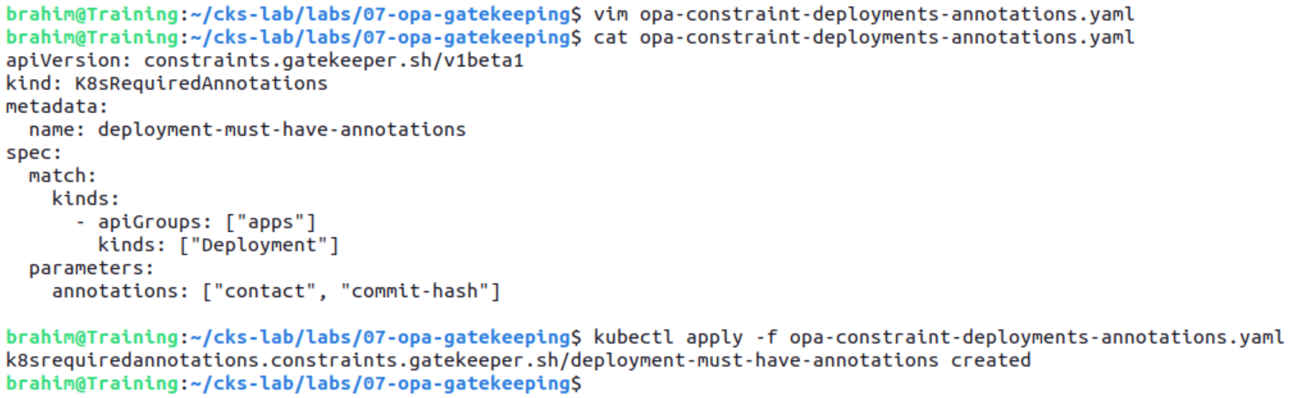
```
brahim@Training:~/cks-lab/labs/07-opa-gatekeeping$ kubectl get pods -n gatekeeper-system
NAME                                             READY   STATUS    RESTARTS        AGE
gatekeeper-audit-6c9dd6bd4b-jvb8t                1/1     Running   4 (3m53s ago)   12m
gatekeeper-controller-manager-67b76665df-7wxpc   1/1     Running   0               12m
gatekeeper-controller-manager-67b76665df-nqknp   1/1     Running   2 (4m12s ago)   12m
gatekeeper-controller-manager-67b76665df-slg8v   1/1     Running   1 (4m10s ago)   12m
brahim@Training:~/cks-lab/labs/07-opa-gatekeeping$ _
```

2. **Inspect the OPA constraint template in the already existing file `opa-constraint-template-annotation.yaml`. Create the object.**



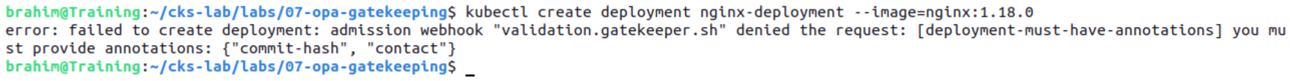
```
brahim@Training:~/cks-lab/labs/07-opa-gatekeeping$ vim opa-constraint-template-annotation.yaml
brahim@Training:~/cks-lab/labs/07-opa-gatekeeping$ cat opa-constraint-template-annotation.yaml
apiVersion: templates.gatekeeper.sh/v1beta1
kind: ConstraintTemplate
metadata:
  name: k8srequiredannotations
spec:
  crd:
    spec:
      names:
        kind: K8sRequiredAnnotations
      validation:
        openAPIV3Schema:
          properties:
            annotations:
              type: array
              items:
                type: string
  targets:
    - target: admission.k8s.gatekeeper.sh
      rego: |
        package k8srequiredannotations

        violation[{"msg": msg, "details": {"missing_annotations": missing}}] {
          provided := {annotation | input.review.object.metadata.annotations[annotation]}
          required := {annotation | annotation := input.parameters.annotations[_]}
          missing := required - provided
          count(missing) > 0
          msg := sprintf("you must provide annotations: %v", [missing])
        }
brahim@Training:~/cks-lab/labs/07-opa-gatekeeping$
brahim@Training:~/cks-lab/labs/07-opa-gatekeeping$ kubectl apply -f opa-constraint-template-annotation.yaml
constrainttemplate.templates.gatekeeper.sh/k8srequiredannotations created
brahim@Training:~/cks-lab/labs/07-opa-gatekeeping$
```

3. Create an OPA constraint object for Deployments that requires two annotations to be specified with the keys `contact` and `commit-hash`.



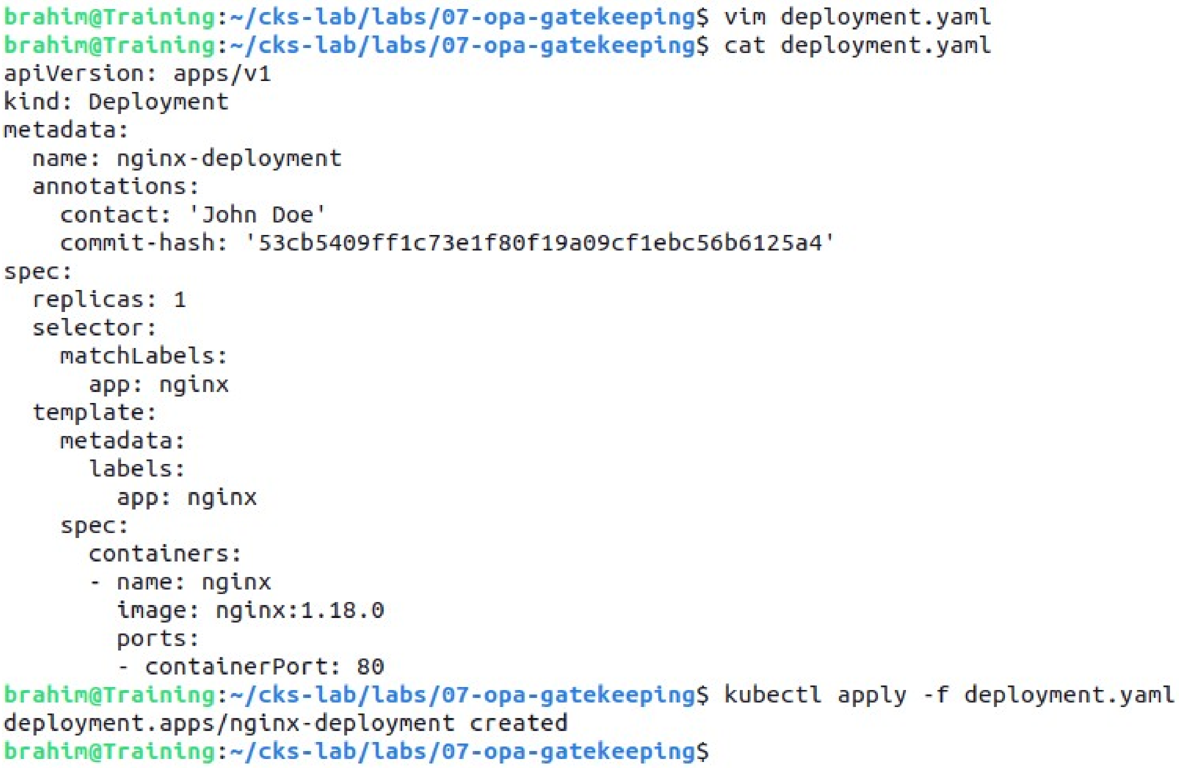
```
brahim@Training:~/cks-lab/labs/07-opa-gatekeeping$ vim opa-constraint-deployments-annotations.yaml
brahim@Training:~/cks-lab/labs/07-opa-gatekeeping$ cat opa-constraint-deployments-annotations.yaml
apiVersion: constraints.gatekeeper.sh/v1beta1
kind: K8sRequiredAnnotations
metadata:
  name: deployment-must-have-annotations
spec:
  match:
    kinds:
      - apiGroups: ["apps"]
        kinds: ["Deployment"]
  parameters:
    annotations: ["contact", "commit-hash"]

brahim@Training:~/cks-lab/labs/07-opa-gatekeeping$ kubectl apply -f opa-constraint-deployments-annotations.yaml
k8srequiredannotations.constraints.gatekeeper.sh/deployment-must-have-annotations created
brahim@Training:~/cks-lab/labs/07-opa-gatekeeping$
```

4. Create a Deployment that does not define the annotations. What's the behavior?



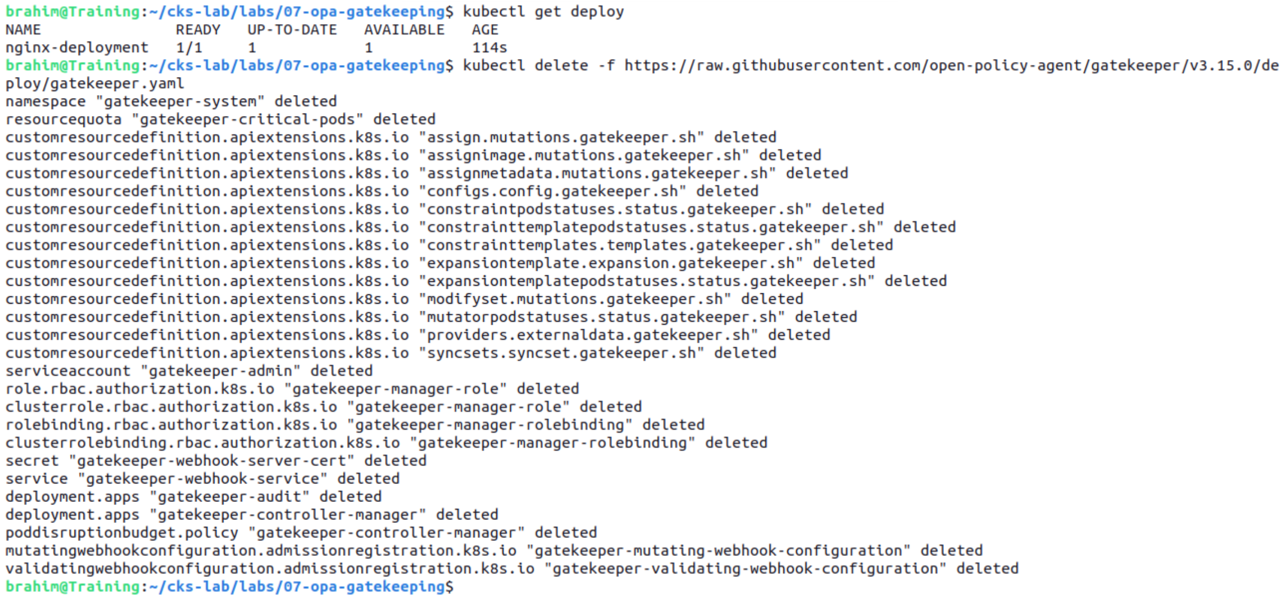
```
brahim@Training:~/cks-lab/labs/07-opa-gatekeeping$ kubectl create deployment nginx-deployment --image=nginx:1.18.0
error: failed to create deployment: admission webhook "validation.gatekeeper.sh" denied the request: [deployment-must-have-annotations] you mu
st provide annotations: {"commit-hash", "contact"}
brahim@Training:~/cks-lab/labs/07-opa-gatekeeping$ _
```

5. Create a Deployment that does define the annotations. What's the behavior?

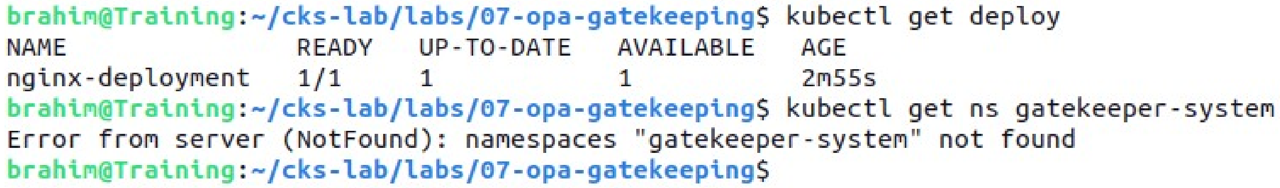


```
brahim@Training:~/cks-lab/labs/07-opa-gatekeeping$ vim deployment.yaml
brahim@Training:~/cks-lab/labs/07-opa-gatekeeping$ cat deployment.yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx-deployment
  annotations:
    contact: 'John Doe'
    commit-hash: '53cb5409ff1c73e1f80f19a09cf1ebc56b6125a4'
spec:
  replicas: 1
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
      - name: nginx
        image: nginx:1.18.0
        ports:
        - containerPort: 80
brahim@Training:~/cks-lab/labs/07-opa-gatekeeping$ kubectl apply -f deployment.yaml
deployment.apps/nginx-deployment created
brahim@Training:~/cks-lab/labs/07-opa-gatekeeping$
```

6. Delete the OPA gatekeeper objects.



```
brahim@Training:~/cks-lab/labs/07-opa-gatekeeping$ kubectl get deploy
NAME               READY   UP-TO-DATE   AVAILABLE   AGE
nginx-deployment   1/1     1            1           114s
brahim@Training:~/cks-lab/labs/07-opa-gatekeeping$ kubectl delete -f https://raw.githubusercontent.com/open-policy-agent/gatekeeper/v3.15.0/de
ploy/gatekeeper.yaml
namespace "gatekeeper-system" deleted
resourcequota "gatekeeper-critical-pods" deleted
customresourcedefinition.apiextensions.k8s.io "assign.mutations.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "assignimage.mutations.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "assignmetadata.mutations.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "configs.config.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "constraintpodstatuses.status.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "constrainttemplatepodstatuses.status.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "constrainttemplates.templates.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "expansiontemplate.expansion.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "expansiontemplatepodstatuses.status.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "modifyset.mutations.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "mutatorpodstatuses.status.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "providers.externaldata.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "syncsets.syncset.gatekeeper.sh" deleted
serviceaccount "gatekeeper-admin" deleted
role.rbac.authorization.k8s.io "gatekeeper-manager-role" deleted
clusterrole.rbac.authorization.k8s.io "gatekeeper-manager-role" deleted
rolebinding.rbac.authorization.k8s.io "gatekeeper-manager-rolebinding" deleted
clusterrolebinding.rbac.authorization.k8s.io "gatekeeper-manager-rolebinding" deleted
secret "gatekeeper-webhook-server-cert" deleted
service "gatekeeper-webhook-service" deleted
deployment.apps "gatekeeper-audit" deleted
deployment.apps "gatekeeper-controller-manager" deleted
poddisruptionbudget.policy "gatekeeper-controller-manager" deleted
mutatingwebhookconfiguration.admissionregistration.k8s.io "gatekeeper-mutating-webhook-configuration" deleted
validatingwebhookconfiguration.admissionregistration.k8s.io "gatekeeper-validating-webhook-configuration" deleted
brahim@Training:~/cks-lab/labs/07-opa-gatekeeping$
```



```
brahim@Training:~/cks-lab/labs/07-opa-gatekeeping$ kubectl get deploy
NAME               READY   UP-TO-DATE   AVAILABLE   AGE
nginx-deployment   1/1     1            1           2m55s
brahim@Training:~/cks-lab/labs/07-opa-gatekeeping$ kubectl get ns gatekeeper-system
Error from server (NotFound): namespaces "gatekeeper-system" not found
brahim@Training:~/cks-lab/labs/07-opa-gatekeeping$
```