Implementing a Mutating Admission Webhook

Learn how to implement a mutating admission webhook service.

We'll cover the following

Implement a mutating admission webhook service

A mutating admission webhook service is a web server, because the `kube-apiserver` invokes it through HTTPS `POST` requests. Now, let's implement such a service step by step.

Step 1: Write a simple HTTP server

Let's write a simple HTTP server at the path `/mutate` over port `443`. It adds labels for Pods. Below is the development environment in which we can add and modify our programs. We can click the "Run" button to initialize it.

main.go

Search in directory...

/
- ca.pem
- go.sum
- go.mod
- webhook-deploy.yml
- webhook-config.yml
- Dockerfile
- main.go

```
1  package main
2
3  import (
4      "encoding/json"
5      "flag"
6      "fmt"
7      "io/ioutil"
8      "log"
9      "net/http"
10
11     "github.com/snorwin/jsonpatch"
12     admissionapi "k8s.io/api/admission/v1"
13     corev1 "k8s.io/api/core/v1"
14     metav1 "k8s.io/apimachinery/pkg/apis/meta/v1"
15 )
16
17 var (
18     podResource = metav1.GroupVersionResource{Version: "v1", Reso
19 )
20
21 func admit(admissionReq *admissionapi.AdmissionRequest) (admissio
22     admissionResp = &admissionapi.AdmissionResponse{}
23     // Copy uid from tr.Request
24     admissionResp.UID = admissionReq.UID
25
```

```
26      var err error
27      defer func() {
28          // If the handler returned an error, incorporate the erro
29          if err != nil {
30              admissionResp.Allowed = false
31              admissionResp.Result = &metav1.Status{
```

Mutating admission webhook

In a real-world scenario, we only need to replace the mock code in the function `admit()` (**line 21** in `main.go`) with our actual business logic. In the demo above, we're handling `pods`, and other resources can be handled as well if we've set matching rules in `MutatingAdmissionConfiguration`.

One of the notable qualities of good admission controllers is their capability for easy diagnostics. So, when rejecting a request, we should return an error with precise or detailed information about the denial reasons or suggested solutions, as shown in the code widget above. We reject the requests if we failed to patch the `pods` and return a hint message.

The rest of the code (**lines 78–127** in `main.go`) is a simple HTTP handler that handles requests from the `kube-apiserver` and deserializes the payloads, which are expected to be an `AdmissionReview` object in JSON format, and then sends the mutating result back.

Another notable thing is that, after we finish handling the `AdmissionReview`, we should not forget to set `Response.UID`, which matches `Request.UID`.

Step 2: Generate and use the certificates (optional)

This section can be skipped, because we've packed all the needed certificates into our prebuilt container image. However, if you want to know more about the detailed steps, follow the instructions below.

In production environments, the `kube-apiserver` uses the CA certificate to visit our admission webhooks, which are serving securely with HTTPS.

Now, let's create some certificates for safe serving. Run the following commands in the terminal above.

```
1  echo '{"CA":{"expiry": "87600h","pathlen":0},"CN":"CA","key":{"algo":"rsa","size":2048}}' | cfssl gencer
2  echo '{"signing":{"default":{"expiry":"87600h","usages":["signing","key encipherment","server auth","cl
3  export ADDRESS=localhost,mutating-admission-demo.kube-system.svc
4  export NAME=server
5  echo '{"CN":"'$NAME'","hosts":[""],"key":{"algo":"rsa","size":2048}}' | cfssl gencert -config=ca-config
```

Generate keys and certificates for secure serving

Now, we should have `ca.pem`, `server.pem`, and `server-key.pem` in our directory.

Here, we generate a self-signed certificate with the `CN` field set to `mutating-admission-demo.kube-system.svc`. We're going to run this service in Kubernetes, which is the endpoint that we want to expose. The DNS name `mutating-admission-demo.kube-system.svc` indicates that there's a `Service` named `mutating-admission-demo` running in the namespace `kube-system`.

Step 3: Build and deploy it

We've already built an image `dixudx/pwk:mutating-admission-webhook`. If you want to build one on your own, run the following command in the terminal above:

```
1  docker build -t dixudx/pwk:mutating-admission-webhook ./
```

Build a container image

After the image has been built successfully, we can deploy the webhook in Kubernetes. Now, let's run the following commands in the terminal above:

```
1  kubectl apply -f /usercode/webhook-deploy.yml
```

Deploy the webhook

Now, we run the following commands to make sure the Pods are running healthily:

```
1  kubectl get pod -n kube-system | grep mutating-admission-demo
```

Check our demo Pods

The output will be as follows:

```
1  mutating-admission-demo-6488cdcccc-8jzzz   1/1     Running   0          33s
2  mutating-admission-demo-6488cdcccc-d9g4f   1/1     Running   0          33s
3  mutating-admission-demo-6488cdcccc-xkx2v   1/1     Running   0          33s
```

Our running demo Pods

Then, we declare `MutatingWebhookConfiguration` in the `kube-apiserver`.

```
1  CABUNDLE=`base64 -w 0 ca.pem` envsubst < /usercode/webhook-config.yml | kubectl apply -f -
```

Apply the mutating webhook configuration

In order to let our static `kube-apiserver` Pod access the webhook service with the DNS name `mutating-admission-demo.kube-system.svc`, we need to export the DNS record as follows. We can run it in the terminal above.

```
1  echo "$(kubectl get svc -n kube-system mutating-admission-demo | grep -v NAME | awk '{print $3}') mutat
```

Add a DNS record

In this lesson, our `kube-apiserver` is running as a static Pod, whose lifecycle is managed by the `kubelet`. We only need to update the `kube-apiserver` manifest file, and then the `kubelet` will be notified of the change and restart it later. Then, the `kube-apiserver` can take effect on these DNS updates. In the terminal above, we can take the steps shown below:

```
1  docker ps -a | grep apiserver | grep -v "pause" | awk '{print $1}' | xargs docker rm -f
```

Enable webhook authentication in the kube-apiserver

Step 4: Test it

Let's do some tests to see if our mutating admission webhook `mutating-admission-demo.kube-system.svc` takes effect during the creation of Pods.

```
1  kubectl run a-mock-app --image=nginx:1.23
```

Construct a Pod for testing

The command above will create a Pod with the name `a-mock-app`. Let's run it in the terminal above to see what happens.

```
pod/a-mock-app created
```

The Pod `a-mock-app` is created successfully. Now, let's check its labels by running the command below in the terminal above:

```
1  kubectl get pod a-mock-app -o yaml | grep -C 5 labels
```

Check the labels of the Pod

The output will be as follows:

```
 1  apiVersion: v1
 2  kind: Pod
 3  metadata:
 4    creationTimestamp: "2022-08-17T13:32:20Z"
 5    labels:
 6      my-label-mock: test
 7      run: a-mock-app
 8    name: a-mock-app
 9    namespace: default
10    resourceVersion: "1600"
```

The output

We can see that a new label `my-label-mock=test` has already been injected to the Pod `a-mock-app` by our webhook, which is working as expected.

Ta-da! The mutating admission webhook works!

Back

Mutating Admission Webhooks

Next

Quiz on Admission Control