

Pod Security Admission Webhook

This directory contains files for a *Validating Admission Webhook* that checks for conformance to the Pod Security Standards. It is built with the same Go package as the [Pod Security Admission Controller](#). The webhook is suitable for environments where the built-in PodSecurity admission controller cannot be used.

For more information, see the [Dynamic Admission Control](#) documentation on the Kubernetes website.

Getting Started

The webhook is available as a Docker image that lives within the SIG-Auth container registry. In addition to the `Dockerfile` for the webhook, this directory also contains sample Kubernetes manifests that can be used to deploy the webhook to a Kubernetes cluster.

Configuring the Webhook Certificate

Run `make certs` to generate a CA and serving certificate valid for `https://webhook.pod-security-webhook.svc`.

Deploying the Webhook

Apply the manifests to install the webhook in your cluster:

```
kubectl apply -k .
```

This applies the manifests in the `manifests` subdirectory, creates a secret containing the serving certificate, and injects the CA bundle to the validating webhook.

Configuring the Webhook

Similar to the Pod Security Admission Controller, the webhook requires a configuration file to determine how incoming resources are validated. For real-world deployments, we highly recommend reviewing our [documentation on selecting appropriate policy levels](#).

Contributing

Please see the [contributing guidelines](#) in the parent directory for general information about contributing to this project.