SECURITY

Security

Pod Security Policies

To automate the enforcement of security contexts, you can define PodSecurityPolicies (PSP). A PSP is defined via a standard Kubernetes manifest following the PSP API schema. An example is presented below.

These policies are cluster-level rules that govern what a pod can do, what they can access, what user they run as, etc.

For instance, if you do not want any of the containers in your cluster to run as the root user, you can define a PSP to that effect. You can also prevent containers from being privileged or use the host network namespace, or the host PID namespace.

You can see an example of a PSP below:

```
apiVersion: policy/v1beta1
kind: PodSecurityPolicy
metadata:
  name: restricted
spec:
  seLinux:
    rule: RunAsAny
  supplementalGroups:
    rule: RunAsAny
  runAsUser:
    rule: MustRunAsNonRoot
  fsGroup:
    rule: RunAsAny
```

For Pod Security Policies to be enabled, you need to configure the admission controller of the controller-manager to contain **PodSecurityPolicy**. These policies make even more sense when coupled with the RBAC configuration in your cluster. This will allow you to finely tune what your users are allowed to run and what capabilities and low level privileges their containers will have.

PSPs have been deprecated, and will be removed in 1.25. The replacement Pod Security Admission is in alpha.

More information can be found in the Kubernetes documentation.

Also, see the PSP RBAC example on GitHub for more details.