Pod Security Standards

A Much Simpler Admission Controller

Pod Security Standards

Pod Security Standards act on the same controls as Pod Security Policies, but don't let you choose which controls to apply with the same granularity.

Instead, there are three pod security standards:

- Privileged : no restrictions – allows any pod specification to run.
- Baseline : minimal restrictions – allows pods without a SecurityContext to run.
- Restricted : best practice restrictions

Pod Security Standard: Privileged

The "privileged" pod security standard is entirely unrestricted.

This standard permits known privilege escalations, like running pods with:

- Privileged containers
- hostPath volumes
- All root capabilities

Pod Security Standard: Baseline

The "baseline" pod security standard blocks known privilege escalations. It blocks:

- Privileged containers
- Using the host's Network, PID, and IPC kernel namespaces
- hostPath volumes
- hostPort and hostIP use
- running a pod without an AppArmor profile on AppArmor-capable nodes
- running a pod with a non-standard SELinux profile on SELinux-capable nodes
- mounting /proc
- deactivating the node's default seccomp filter
- using sysctl settings that are namespaced outside the pod

Pod Security Standard: Restricted

The "restricted" pod security standard uses best practices, but cannot be more specific.

It enforces all the controls from the "baseline" pod security standard and adds:

- Volume type restriction to a specific allow list
- Set-UID and Set-GID binaries not honored (allowPrivilegeEscalation must be false)
- Containers must run as a non-root user
- Seccomp must use either the RuntimeDefault or a profile from the node filesystem.
- All root capabilities must be dropped, though NET_BIND_SERVICE is permitted.

Applying Pod Security Standards

You apply pod security standards to entire namespaces, instead of users or service accounts.

```
apiVersion: v1
kind: Namespace
metadata:
   name: my-privileged-namespace
   labels: pod-security.kubernetes.io/enforce: privileged
   pod-security.kubernetes.io/enforce-version: latest
```