portworx backup

Portworx Backup 2.7.2

PSA Support

Overview

Pod Security Admission (PSA) is a feature in Kubernetes that enforces security policies during pod creation in a target application cluster. PSA support in Portworx Backup allows various backup related pods and jobs to be run gracefully on PSA set namespaces/clusters. Both PSA (Pod Security Admission) and PSS (Pod Security Standards) are used interchangeably in this document since they implement the same feature in kubernetes. PSA is a non-mutating admission webhook which has replaced the PSP (Pod Security Policy) as an obsolete security feature. PSA replaces the Pod Security Policies feature in Kubernetes, which was deprecated in Kubernetes version 1.21 and removed in 1.25 version. For more information, refer to Pod Security Admission and Pod Security Standards. PSA can be set, either at namespace level or cluster level. For namespace level and cluster level configuration refer to Apply Pod Security Standards at the Namespace Level and Apply Pod Security Standards at the Cluster Level.

PSA allows Kubernetes users to specify security requirements for all pods running in a certain namespace. You can use the following three security levels to specify your requirements:

- `privileged`: an unrestricted policy, which provides the widest possible level of permissions. This policy allows for known privilege escalations.
- `baseline`: a minimally restrictive policy, which prevents known privilege escalations. This policy also allows the default (minimally specified) pod configuration.
- `restricted`: a heavily restricted policy, following the best practices for hardening the current pod.

Each policy contains a set of security requirements a pod (its spec) must comply with. If there are any violations, the pod will not be allowed to run in the given namespace. To enable one of these policies for a namespace, you should label the namespace with an appropriate label. After labeling, the newly created pods will be validated against the specified policy.

You must manage your own namespace. Kubernetes namespaces are often used for isolation of applications or teams, and you can tie the creation or modification of namespaces to internal policies and certifications.

Existing behavior

- Stand-alone volume will not be backed up if a PVC lies in a restricted PSA because the PVC will have files with different UIDs and GIDs and this can cause RD/WR failures.
- Restricted PSP based applications cannot be restored to restricted PSA based namespaces because of multiple configurations, which PSA does not support.
- If the view JSON shows -1 for any UID or GID then either the pod has not defined any UID or it is root.

PSA support in Portworx Backup

Prerequisites

- Cluster where you want to install Portworx Backup should be either Kubernetes Vanilla or RKE2 for PSA support. Refer to Portworx Backup Install prerequisites for more information.
- Namespace where you want to install Portworx Backup and Portworx Enterprise should have PSA mode `privileged`.

Note: You can restore the namespaces you have backed up on your application cluster with Kubernetes version 1.24.x or below only if the namespaces are configured with Pod Security Policies (PSP) mode set to `privileged`.

Limitations

Portworx Backup does not support PSA on the following platforms/environments:

- Cloud and OCP platforms
- Shared PVCs and stand-alone PVCs (without pod)
- KubeVirt Virtual Machines

FAQs

1. **What happens to labels applied on the namespaces after taking backup and restoring it ?**

A. All the PSA labels of the source namespace will be applied to the destination namespace, regardless of the replace policy or any cluster-wide PSA settings. With `replace = true`, if the source cluster and destination namespace have labels with the same key, destination namespace labels will be replaced with source namespace labels.

2. **What happens when the PSA is set at both cluster level and namespace level?**

A. Namespace level PSA setting takes precedence over cluster level setting.

3. **What all clusters will have PSA support?**

A. PSA support is qualified on Vanilla Kubernetes and RKE 2 clusters only.

4. **What does PSA support in Portworx Backup do?**

A. The PSA feature enables KDMP job pods to be adjusted to run smoothly in PSA-restricted environments. If a volume is backed up with a specific UID and GID in a restricted PSA environment, this information will be retained in the `volumeInfo` structure.

5. **What is the expected behavior when we take backup in higher privilege namespace and restore to lower privilege namespace and vice versa?**

A. Backup of an application that was running with higher privilege namespace cannot be restored to a lower privilege namespace, apparently it would fail. However, a backup of an application that was running with lower privilege can be restored to a higher privileged namespace gracefully.