



**Protect Kubernetes
applications with Veeam
Kasten, HPE Alletra Storage
MP X10000 and HPE
Morpheus Enterprise Software**



Introduction

Kubernetes adoption and modernization initiatives are driving enterprises toward platforms that combine orchestration, persistent storage, and data protection. This technical brief describes a validated architecture that brings together HKS (HPE's CNCF-compliant Kubernetes distribution), HPE Alletra Storage MP block and object storage, and Veeam Kasten to deliver end-to-end Kubernetes application protection—from snapshot-based local backup through cross-site application mobility.

Solution Overview

HPE Morpheus Enterprise Software provides unified lifecycle management across on-premises

and cloud environments. As shown in Figure 1, Kasten and the HPE CSI Driver for Kubernetes integrate Kubernetes with HPE Alletra Storage MP B10000, enabling dynamic provisioning, snapshots, and persistent volume management for stateful workloads. Veeam Kasten adds Kubernetes-native backup and mobility, capturing application metadata, persistent data, and custom resources. When paired with HPE Alletra Storage MP X10000 as an S3-compatible object store target, Kasten enables durable, off-cluster backup exports. Together, these components form an enterprise-grade platform for deploying, protecting, and restoring Kubernetes applications across clusters. This brief demonstrates a cross-site restore workflow as an example.

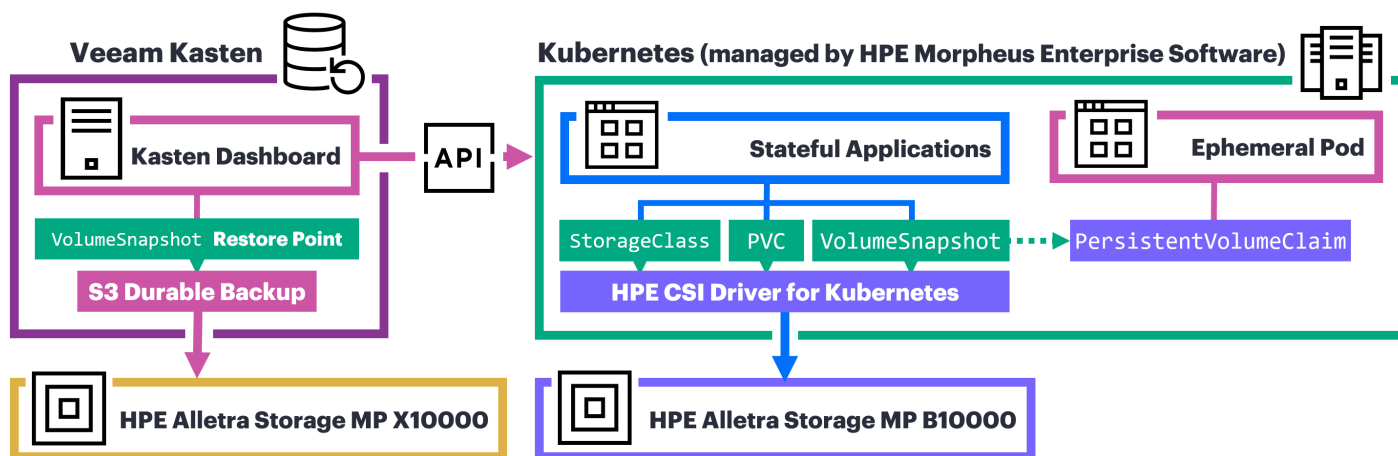


Figure 1. HPE Alletra Storage MP X10000 data protection flexibility

Solution components

Component	Role
HPE Morpheus Enterprise Software	Cloud management platform providing KVM-based virtualization (HVM) and Kubernetes cluster provisioning and lifecycle management.
HPE HKS	CNCF-compliant Kubernetes distribution deployed and managed by Morpheus. Two clusters are used in this brief: one in Colorado and one in California.
HPE CSI Driver for Kubernetes	Standards-based CSI driver connecting Kubernetes to HPE Alletra Storage MP B10000 for dynamic provisioning, snapshots, and clones via iSCSI/FC/NFS.
HPE Alletra Storage MP B10000	High-performance block/file storage providing persistent volumes and array-based snapshots for Kubernetes workloads.
HPE Alletra Storage MP X10000	Scale-out object storage exposing an S3-compatible interface. Serves as the durable, off-cluster backup target for Kasten restore points.
Veeam Kasten K10	Kubernetes-native data management platform providing policy-based backup, recovery, and application mobility across clusters and clouds.

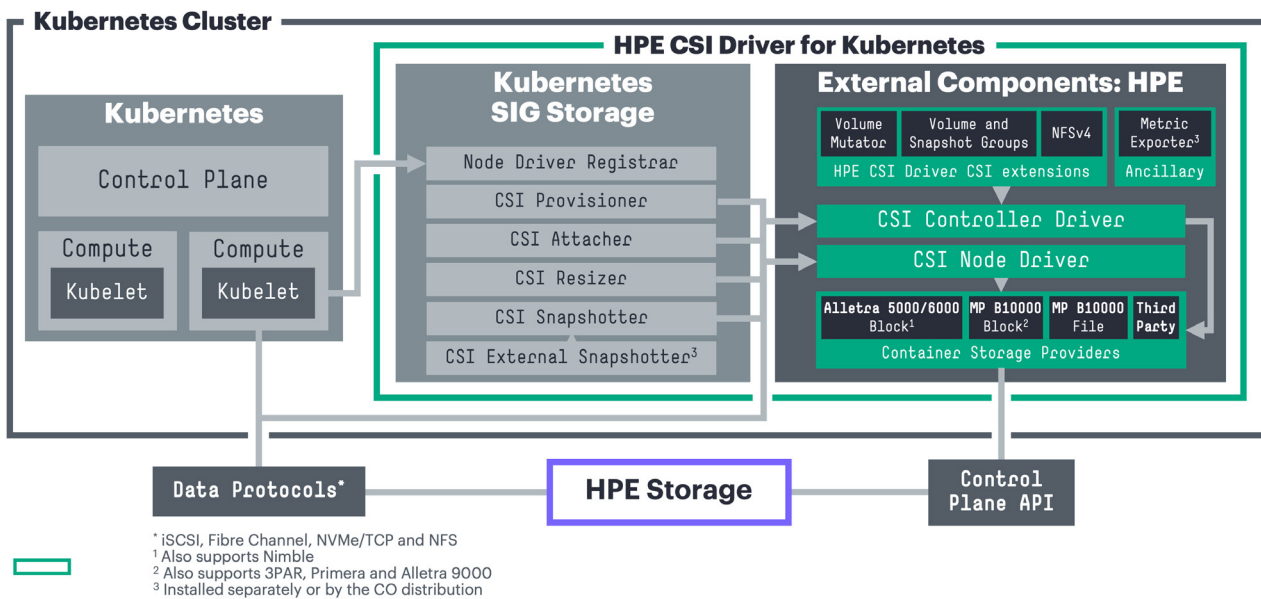


Figure 2. HPE CSI Driver connecting Kubernetes clusters to HPE Alletra Storage MP B10000

How it works

Persistent storage with the HPE CSI Driver for Kubernetes

The HPE CSI Driver for Kubernetes is the standards-based interface between the Kubernetes orchestration layer and HPE Alletra Storage MP B10000. It enables:

Dynamic provisioning — uses a StorageClass to define volume parameters such as protection templates and performance policies. Persistent Volume Claims (PVCs) then automatically provision volumes on the array.

Snapshot and clone operations — The driver supports the Kubernetes VolumeSnapshot API, allowing point-in-time, array-based snapshots and near-instant clones—capabilities that Veeam Kasten leverages directly.

Multi-protocol support — Block (iSCSI/FC) and file (NFS) data paths are supported through a pluggable Container Storage Provider (CSP) architecture.

Backup workflow

1. A Kasten backup policy runs on a schedule (or on demand).
2. Kasten discovers application objects across target namespaces—Deployments, StatefulSets, ConfigMaps, Secrets, PVCs, and custom resources.
3. Kasten issues a VolumeSnapshot request through the Kubernetes API.
4. The HPE CSI Driver translates the request into an array-level snapshot on the HPE Alletra Storage MP B10000. This is a metadata-only operation and completes in seconds regardless of volume size.
5. Kasten catalogs the snapshot under an App Session—a restore point that captures the complete application state.
6. For durable, off-cluster protection, a subsequent export action streams the restore point to the S3 bucket on the HPE Alletra Storage MP X10000.

Restore workflow

1. The operator selects a restore point in the Kasten dashboard.
2. Kasten creates new PVCs and requests volume clones from the snapshots via the HPE CSI Driver. Clone creation is near-instant (metadata-based).
3. Kasten replays application manifests—recreating Deployments, StatefulSets, ConfigMaps, Secrets, and Services—and binds the cloned volumes to the new PVCs.
4. Pods mount the restored volumes, and Kasten monitors readiness/liveness probes to confirm successful recovery.

HPE Morpheus Enterprise Software

Cloud Management • HKS Cluster Provisioning • Lifecycle Management

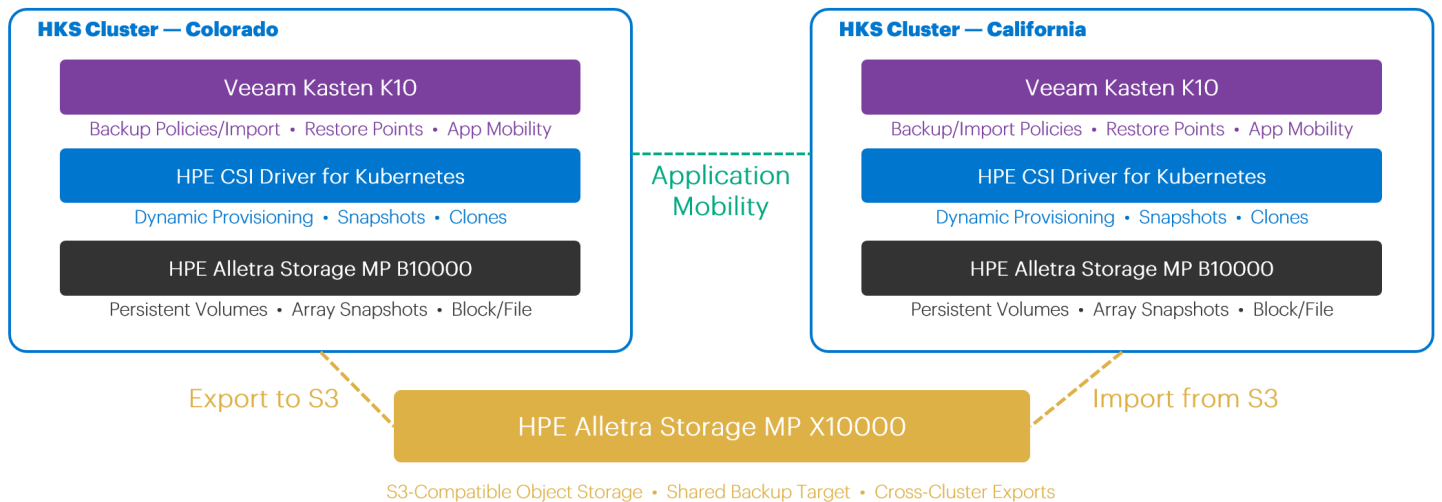


Figure 3. Two HKS clusters with Veeam Kasten and HPE CSI Driver connected via Alletra MP storage

Configuration summary

1. Provision HKS clusters

Deploy Kubernetes clusters through the HPE Morpheus Add Cluster workflow. When deployed with HVM virtual machines, Kubernetes installation is fully automated.

2. Prepare an S3 bucket on the HPE Alletra Storage MP X10000

Create a bucket and record the S3 endpoint, bucket name, access key, and secret key. This bucket will be shared across both clusters; Kasten uses a unique prefix per cluster to isolate data.

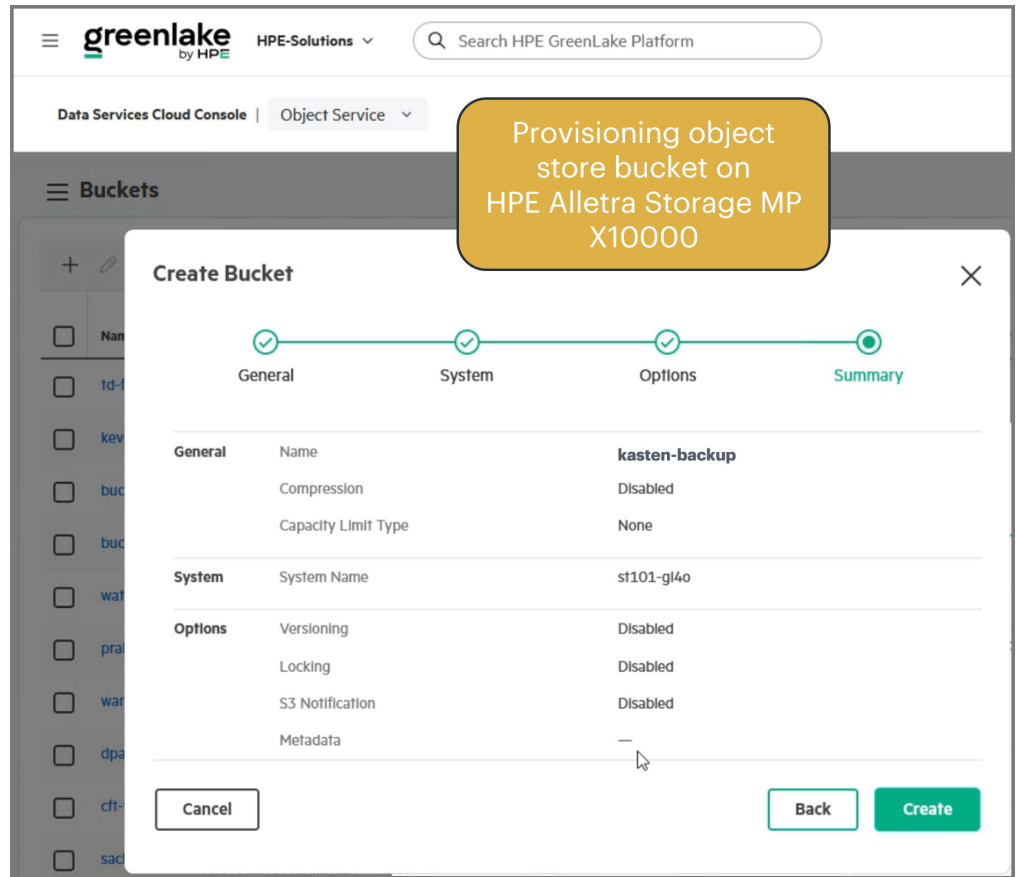


Figure 4. Creating an S3 bucket for Kasten backup on HPE Alletra Storage MP X10000

3. Install and configure the HPE CSI Driver

- **Deploy the driver** — Install via Helm chart from Artifact Hub (hpe-storage/hpe-csi-driver).
- **Create a Secret** — Define a Secret with the Alletra B10000 management IP and credentials.
- **Create a StorageClass** — Reference the Secret and set volume parameters (protection template, performance policy, etc.).
- **Install VolumeSnapshot CRDs** — Deploy the external-snapshotter CRDs and create a VolumeSnapshotClass pointing to the HPE CSI Driver.

4. Install Veeam Kasten

Deploy Kasten via Helm into its own namespace (kasten-io). Supply any required TLS certificates during installation.

5. Configure the Kasten location profile

Add an S3-compatible location profile using the endpoint, bucket, and credentials from step 2.

6. Define backup policies

Policy setting	Value
Snapshot frequency	Hourly
Export frequency	Daily
Selection method	By namespace or by label
Snapshot target	HPE Alletra Storage MP B10000 (via CSI snapshots)
Export target	HPE Alletra Storage MP X10000 S3 bucket

The screenshot shows the Veeam Kasten interface for managing policies. The left sidebar contains navigation options like Dashboard, Applications, Restore Points, Virtual Machines, Policies, Presets, Profiles, Location, Infrastructure, Blueprints, Transform Sets, and Get Support. The main content area is titled 'Policies' and includes a 'Create New Policy' button. Below the title is a table of policies with columns for Name, Validation, Resources, Action, Frequency, Last Run Time, and Last Run Status. Two policies are listed: 'k10-disaster-recovery-policy' (Valid, kasten-io, Snapshot, Hourly) and 'prometheus-backup-policy' (Valid, app:prometheus +1, Snapshot + Export, Hourly). The 'prometheus-backup-policy' is highlighted with a blue box, and two arrows point from it to two storage targets: 'HPE Alletra Storage MP B10000' (green box) and 'HPE Alletra Storage MP X10000' (orange box).

Figure 5. Kasten protection policies for snapshot and export to Alletra MP X10000

Cross-site application restore

A key advantage of exporting restore points to S3-compatible object storage is application mobility. Because the HPE Alletra Storage MP X10000 bucket is accessible from both clusters, a restore point created in Colorado can be imported and restored in California.

Demonstration using a Prometheus time-series database

Prometheus is an open-source monitoring and alerting toolkit widely adopted in Kubernetes environments. It collects and stores time-series metrics from cluster nodes, pods, and applications, making it a common workload to protect in production clusters. Prometheus is initially deployed on the Colorado HKS cluster. A Kasten backup policy captures hourly snapshots on the HPE Alletra Storage MP B10000 and performs a daily full export to the S3 bucket hosted on the HPE Alletra Storage MP X10000.

Steps to restore on the California cluster:

1. On the California cluster, create a Kasten **import policy** referencing the same S3 location profile and bucket. Also provide the “config data” string from the protection policy on the Colorado cluster.
2. Kasten discovers the exported restore points from the Colorado cluster.
3. Select a restore point and initiate a restore. Kasten provisions new PVCs (backed by the California-local Alletra B10000), replays application manifests, and brings Prometheus online on the California cluster.

This workflow validates disaster recovery, planned migration, and dev/test cloning use cases without requiring shared storage fabrics between sites.

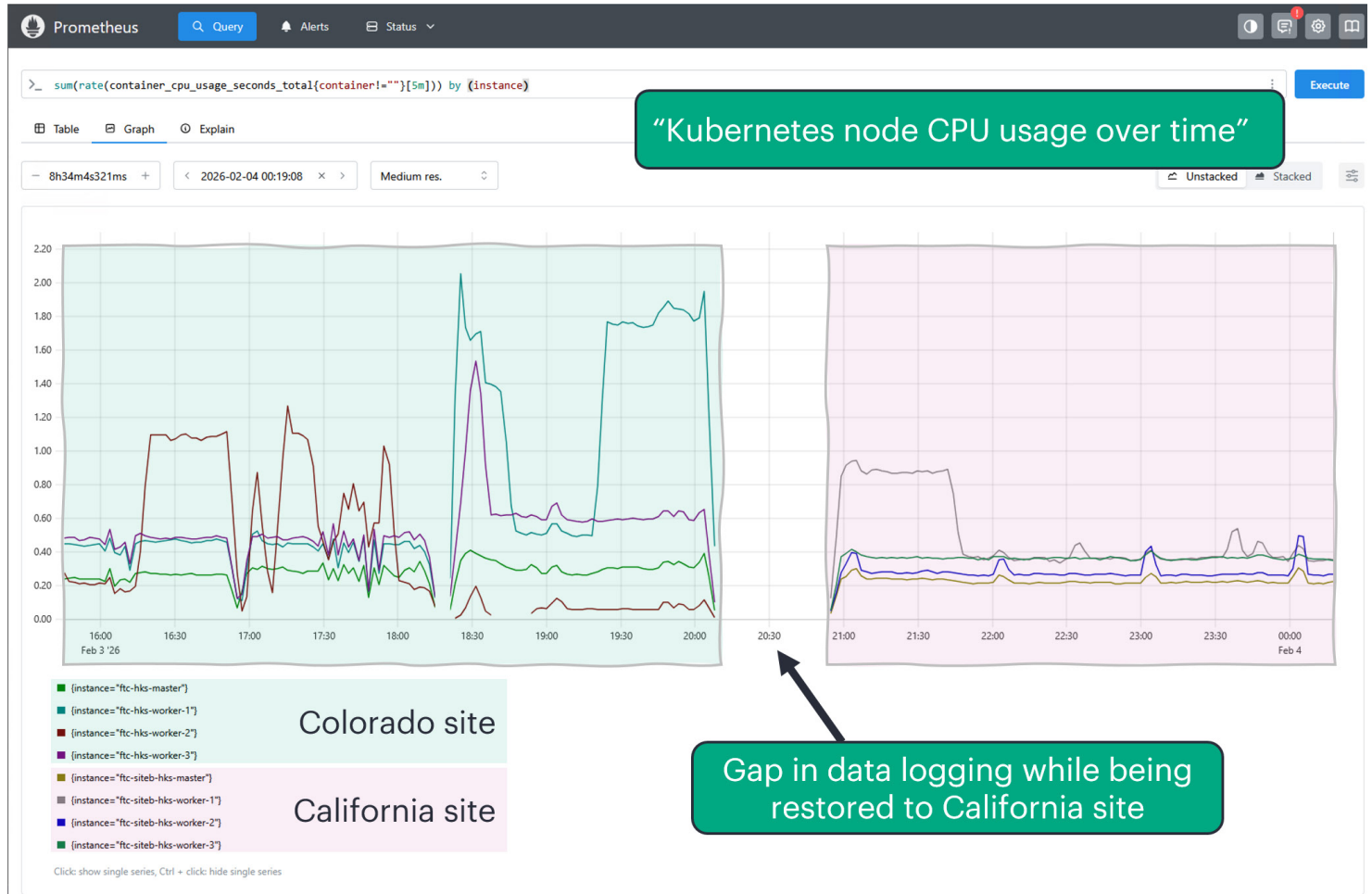


Figure 6. Prometheus CPU metrics across Colorado and California HKS clusters during restore

Conclusion

The combination of HPE Morpheus Enterprise Software, HKS, HPE CSI Driver for Kubernetes, HPE Alletra Storage MP B10000, HPE Alletra Storage MP X10000, and Veeam Kasten delivers an integrated, enterprise-grade platform for Kubernetes data protection. Snapshot-based backups provide rapid, low-impact local recovery, while S3 exports to the Alletra X10000 enable durable off-cluster protection and cross-site application mobility. This architecture allows organizations to standardize on HPE infrastructure for both the compute/storage plane and the backup target, simplifying operations and reducing risk.

Learn more at

[HPE.com/us/en/Alletra-Storage-MP-X10000.html](https://hpe.com/us/en/Alletra-Storage-MP-X10000.html)

[HPE.com/us/en/Morpheus-Enterprise-Software.html](https://hpe.com/us/en/Morpheus-Enterprise-Software.html)

[HPE.com/Storage/Containers](https://hpe.com/Storage/Containers)

[HPE.com/us/en/alliance/Veeam.html](https://hpe.com/us/en/alliance/Veeam.html)

Visit [HPE.com](https://hpe.com)

[Chat now](#)

© Copyright 2026 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

a00157443ENW

HEWLETT PACKARD ENTERPRISE

hpe.com

