

Kubernetes Data Protection WG Deep Dive

Dave Smith-Uchida & Xing Yang (Broadcom)



Agenda

- Motivation
- Who are involved
- Projects
  - Backup Repository - COSI
  - Snapshot Topology
  - Changed Block Tracking (CBT)
  - Consistent Group Snapshot
  - Volume Replication
- Whitepapers
  - Best Practices for Kubernetes Applications for Data Protection
  - Kubernetes Cyber Recovery White Paper
    - Deep dive on Cyber Recovery
- How to get involved

Motivation

KubeCon CloudNativeCon North America 2026

Day 1 is well supported

- Persistent volume operations
- Workload APIs: Deployment, StatefulSet, ...

Stateful workloads are moving to Kubernetes

- Rapid iteration and agile deployment
- Built-in scalability
- Portability

Day 2 data protection is still limited

GitOps (Flux, Argo CD) recreates manifests, but not:

- Secrets, ConfigMaps and other sensitive data
- Data stored in persistent volumes

Goal: Kubernetes-native building blocks for Day-2 data protection

Who are involved

KubeCon CloudNativeCon North America 2026

Companies supporting this initiative

Arrikto

Catalogic Software

Cohesity (Veritas)

COMMVAULT

DATACORE (MayaData)

DELL Technologies

Druva

Google

HPE

IBM

LINBIT

LinkedIn

Microsoft

mongoDB

NetApp

portworx by Pure Storage

Red Hat

Rubrik

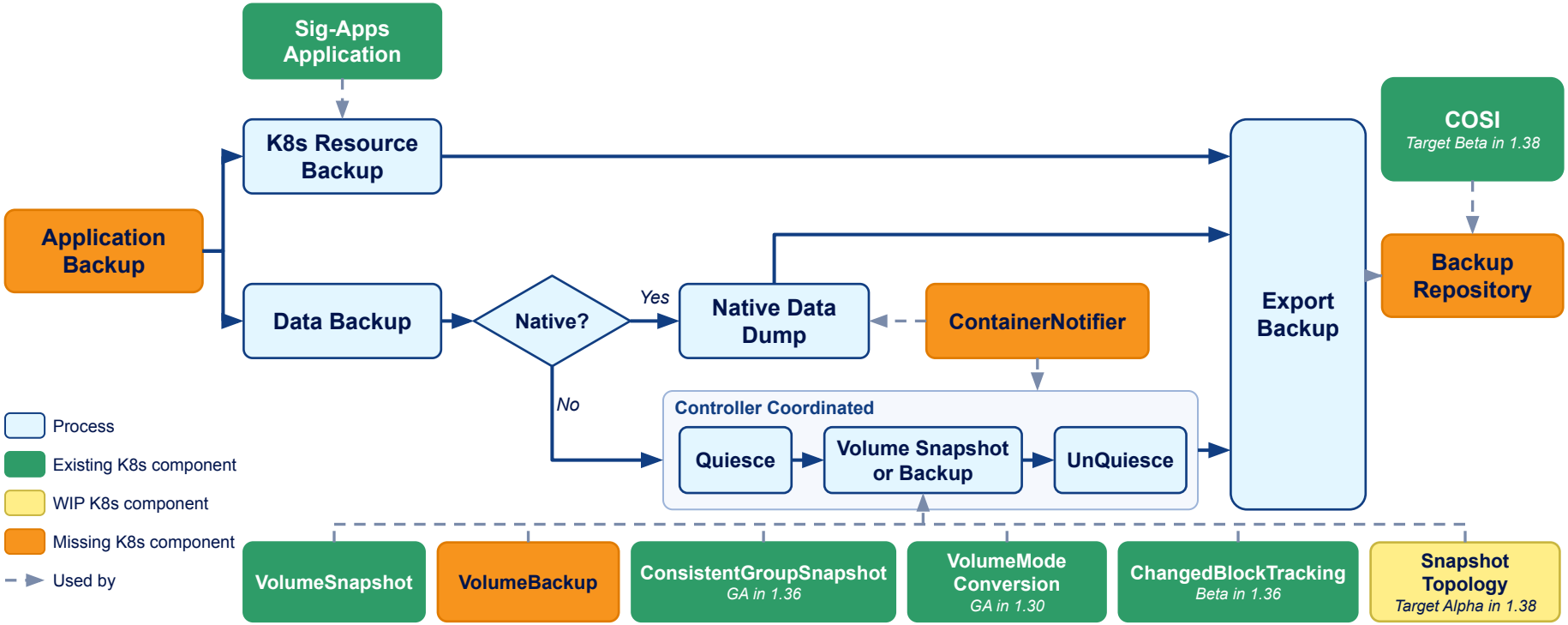
SUSE

TRILIO

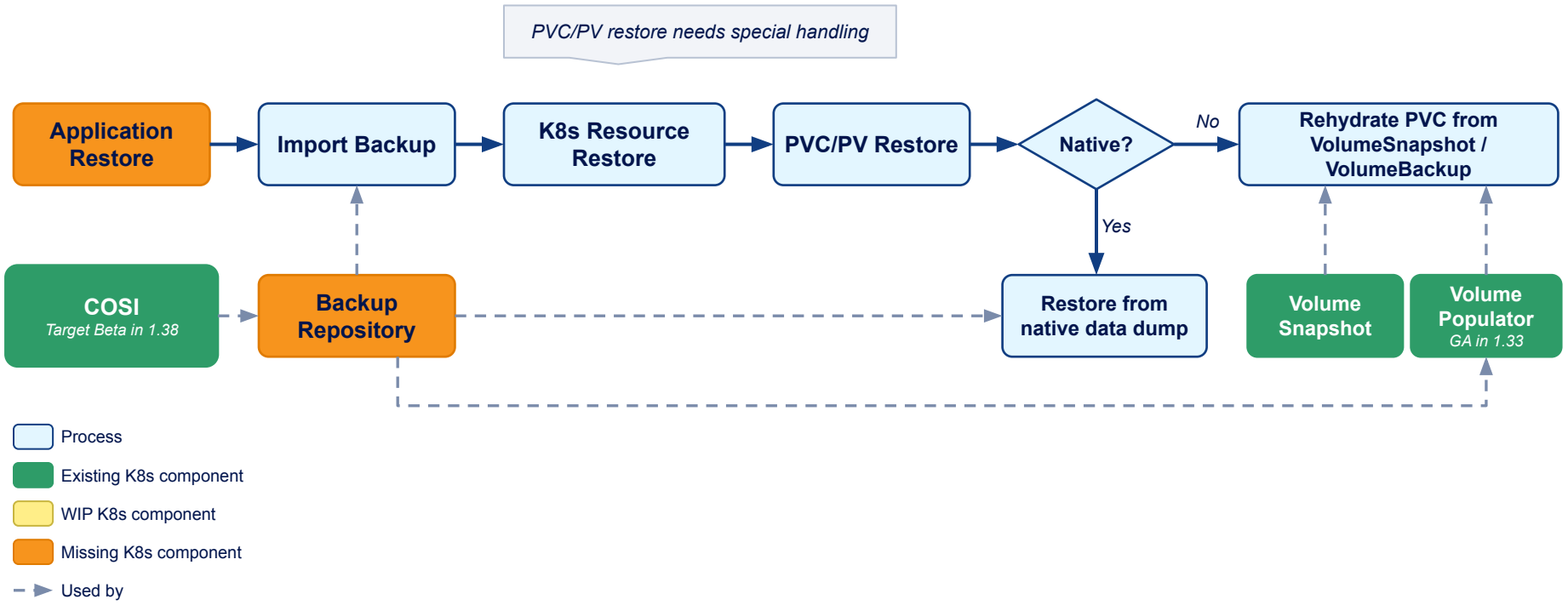
VEEAM (Kasten)

vmware by Broadcom

Backup


Sig-Apps Application
K8s Resource Backup
Application Backup
Data Backup
Native?
Yes
No
Native Data Dump
ContainerNotifier
Controller Coordinated
Quiesce
Volume Snapshot or Backup
UnQuiesce
Export Backup
COSI
Target Beta in 1.38
Backup Repository
Process
Existing K8s component
WIP K8s component
Missing K8s component
Used by
VolumeSnapshot
VolumeBackup
ConsistentGroupSnapshot
GA in 1.36
VolumeMode Conversion
GA in 1.30
ChangedBlockTracking
Beta in 1.36
Snapshot Topology
Target Alpha in 1.38

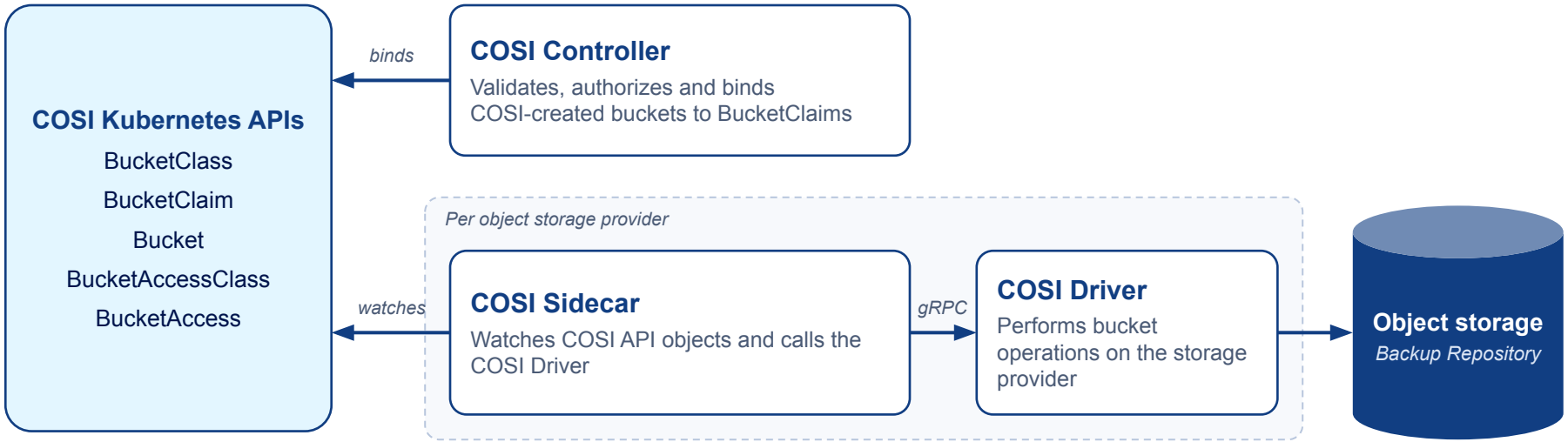
Restore


PVC/PV restore needs special handling
Application Restore
Import Backup
K8s Resource Restore
PVC/PV Restore
Native?
No
Yes
Rehydrate PVC from VolumeSnapshot / VolumeBackup
COSI
Target Beta in 1.38
Backup Repository
Restore from native data dump
Volume Snapshot
Volume Populator
GA in 1.33
Process
Existing K8s component
WIP K8s component
Missing K8s component
Used by

Backup Repository

KubeCon CloudNativeCon North America 2026

Container Object Storage Interface (COSI) provides a standard way to provision and consume object storage in Kubernetes. It can back a Backup Repository such as an object store.

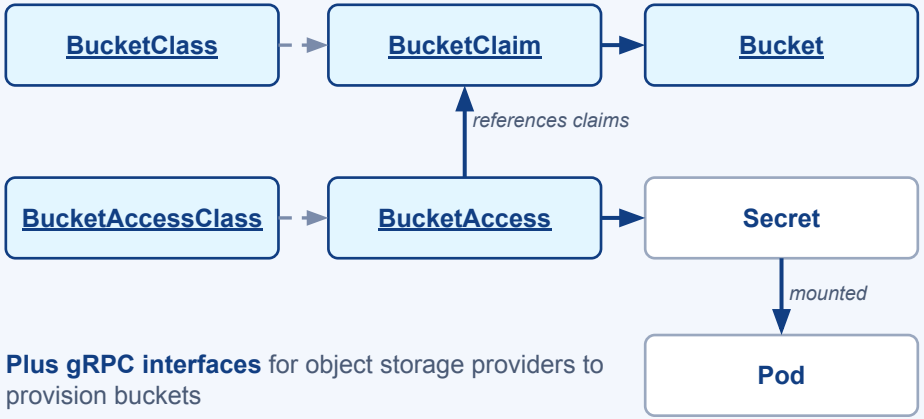


Backup Repository

KubeCon CloudNativeCon North America 2026

v1alpha2 in K8s 1.37 · Targeting Beta in 1.38

COSI Kubernetes APIs



Plus gRPC interfaces for object storage providers to provision buckets

Notable v1alpha2 changes

Multi-bucket access

A BucketAccess can now request access to multiple BucketClaims

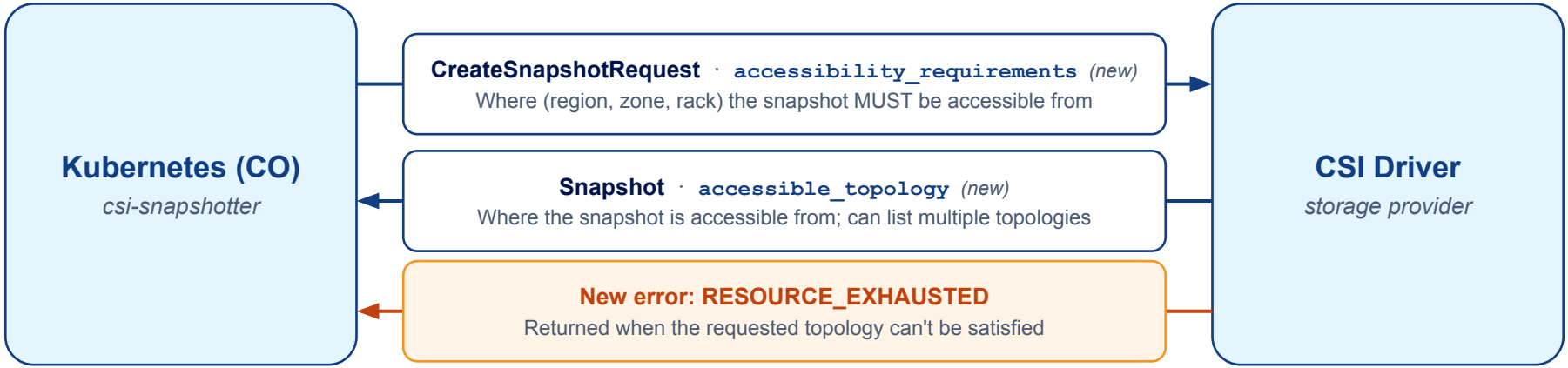
BucketAccessModes

Access	ReadWrite	WriteOnly	ReadOnly
Data	ObjectData	ObjectMetadata	BucketMetadata

Snapshot Topology CSI Specification

KubeCon CloudNativeCon North America 2026

Applies to CSI drivers whose snapshots aren't accessible from every zone or region



New plugin capability `SNAPSHOT_ACCESSIBILITY_CONSTRAINTS`
The driver advertises that snapshots may not be equally accessible from all topologies

If the driver returns no topology, the CO may assume the snapshot is accessible everywhere.

Snapshot Topology in Kubernetes

KubeCon CloudNativeCon North America 2026

Feature gate VolumeSnapshotTopology · Targeting Alpha in K8s 1.38

Adds topology to snapshots

VolumeSnapshotClass · `allowedTopologies` *(new)*
Passed to the driver as accessibility_requirements

↓

CSI Driver

↓ *accessible_topology*

VolumeSnapshotContent · `spec.nodeAffinity` *(new)*
Set by csi-snapshotter from accessible_topology; admins set it by hand for static snapshots

Enforces it when restoring volumes

Depends on the StorageClass volumeBindingMode

`WaitForFirstConsumer`

snapshot-topology-webhook

Mutating: adds the snapshot's nodeAffinity to the pod
Topology not known yet: pod waits on a scheduling gate
Validating: rejects a selected-node the snapshot can't be restored on
In external-snapshotter; uses the default scheduler

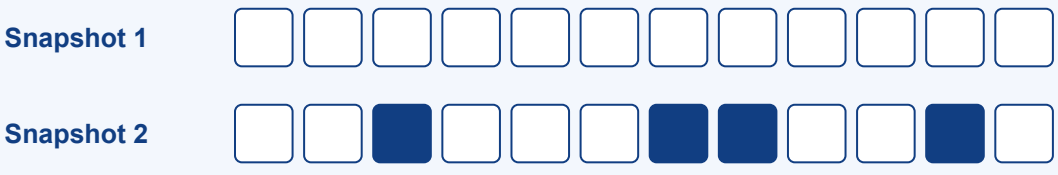
`Immediate`

external-provisioner

Intersects the snapshot's nodeAffinity with the StorageClass allowedTopologies

Changed Block Tracking (CBT) API

Beta in K8s 1.36



Same persistent volume, two points in time

`GetMetadataDelta`

Changed blocks only
Back up just what changed

Vendor agnostic

Standard Kubernetes APIs

Efficient

Identify changed blocks between two snapshots of the same persistent volume

Incremental

Incremental volume backup

Decoupled

Decouple the backup system from the storage system

SnapshotMetadata CSI Specification

KubeCon CloudNativeCon North America 2026

Storage providers should implement a new CSI service and RPCs in their CSI drivers to support CBT

CSI Driver

New SnapshotMetadata service

New CSI RPC

`GetMetadataAllocated`

Allocated blocks of a snapshot

New CSI RPC

`GetMetadataDelta`

Changed blocks between two snapshots

New plugin capability `SNAPSHOT_METADATA_SERVICE`

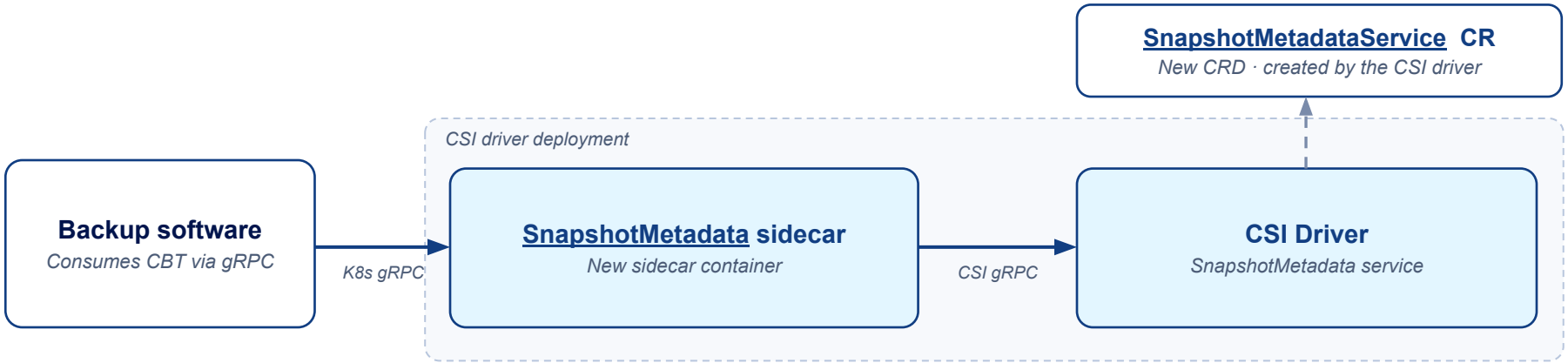
Supports block volumes only

SnapshotMetadata in Kubernetes

KubeCon CloudNativeCon North America 2026

Beta in K8s 1.36

Backup software should adopt these APIs to support CBT



Two Kubernetes SnapshotMetadata gRPC RPCs

Very similar to the CSI SnapshotMetadata service RPCs

`GetMetadataAllocated`

`GetMetadataDelta`

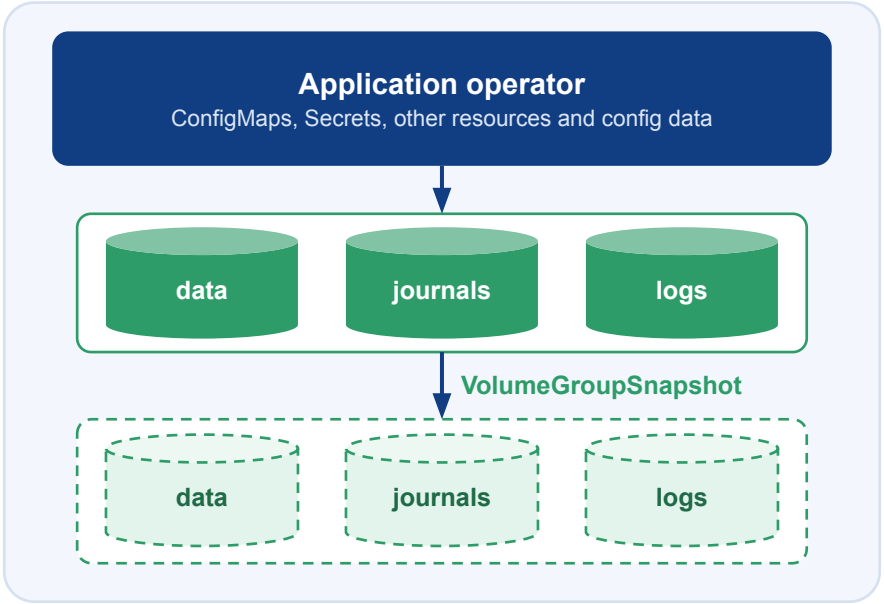
Consistent Group Snapshot

GA in K8s 1.36

Crash consistency
When application consistency is not available or not practical

Write-order consistency
Across multiple volumes in the same group

Better performance



Consistent Group Snapshot - Design

KubeCon CloudNativeCon North America 2026

GA in K8s 1.36

1 Kubernetes APIs

- `VolumeGroupSnapshot`
- `VolumeGroupSnapshotContent`
- `VolumeGroupSnapshotClass`

2 CSI spec changes

New Group Controller Service, with gRPC interfaces to:

- `CreateVolumeGroupSnapshot`
- `DeleteVolumeGroupSnapshot`
- `GetVolumeGroupSnapshot`

3 New controller logic

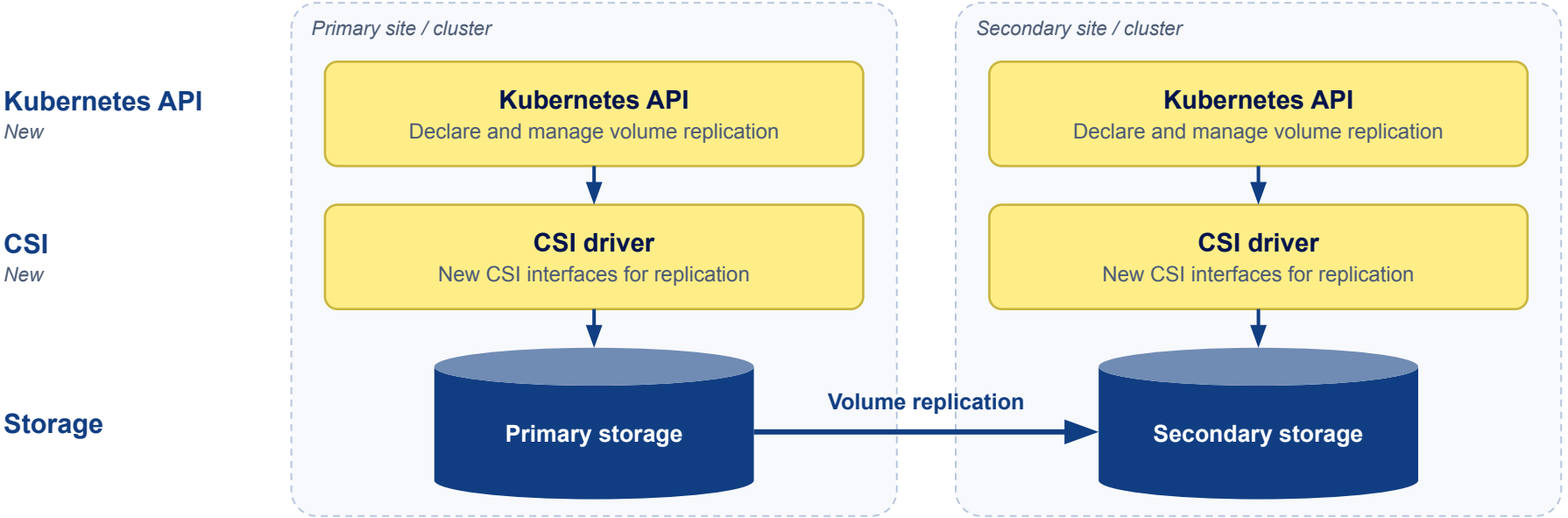
In the Kubernetes CSI components:

- **snapshot-controller**
- **CSI snapshotter sidecar**

Volume Replication

Status: Design / prototyping

Replicating volumes needs new pieces at both layers



KubeCon CloudNativeCon North America 2026

Whitepapers



Kubernetes Data Protection: Best Practices Whitepaper



Kubernetes now has mechanisms for data protection and multiple strategies for ensuring application resiliency including GitOps, backup/restore and remote replication

Protecting an application involves:

- Understanding the resiliency needs of the application
- Selecting the right strategy to meet the resiliency needs
- Making modifications, if necessary to the application to handle the strategy

Whitepaper is under construction, contributors/reviewers are needed!

Currently moving to first draft.

Kubernetes Cyber Recovery White Paper

KubeCon CloudNativeCon North America 2026

"Cyber Recovery" is the process of recovering from a ransomware attack.
This new white paper defines how to prepare for and recover from a ransomware attack.
Key points:

- Cloud native ransomware threat vectors
- Defenses
  - Immutable storage
  - Supply chain lockdown
  - Isolated recovery environments
- Regulatory alignment

Ransomware Attacks

Why is recovering from a ransomware attack harder than usual recovery?

- Adversarial - not hardware failures or human error. Active human threat actors
- Everything can be compromised - control plane and backups must be verified and cannot just be trusted
- Data may appear good but be infected
- Network connectivity must be controlled during recovery to prevent malware activity

Cloud Native Ransomware Threat Vectors

- Erasing safety nets
- Locking up databases
- Snapshot poisoning
- Hidden outbound network communication
- AI accelerated malware

Immutable Storage For Backups

- Threat
  - Ransomware attacks target safety nets - backups
  - Will steal credentials and delete or corrupt snapshots and backups
- Defenses
  - Backup tools must support immutable backups
  - Use "Compliance mode" for production cyber recovery vaults
  - On-prem/self-managed object storage must be secured
  - Airgapped cyber vaults required for best protection
  - Consider offline storage (e.g. tape)

Supply Chain Lockdown

Threat

- Backup management tool elevated permissions used by attackers

Defenses

- Short-lived, dynamic security tokens via OIDC/Identity federation
- Least-privilege, granular RBAC roles for specific namespaces
- Scoped Write-only or Append-only permissions for storage targets

Isolated Recovery Environments

Threat

- Malware reactivates during during recovery

Defenses

- Software airgapping - block all in/out traffic at L3/L4 level
- Forensic investigation & pinhole scanning
- Deterministic promotion or rollback with AI scanner

Regulatory alignment

Standards

- NIST SP 800-209 Storage Infrastructure Security Guidelines
- NIST SP 800-207 Zero Trust Principle
- EU Digital Operational Resilience Act (DORA) & NIS2 Directives

Whitepaper discusses how recommendations map to these standards

Where do we go from here?

- Kubernetes Data Protection: Best Practices Whitepaper is nearing completion
  - Issues and pull requests welcome
  - Working draft is here: https://github.com/dsu-igeek/community/blob/dp-best-practices-wp-10-27-2026/wg-data-protection/data-protection-workflows-white-paper.md
- Kubernetes Cyber Recovery White Paper is under construction.
  - https://docs.google.com/document/d/1ibS-iAUvk3O6XQP0HcwEjFXDzyKPpvote0lQaDZd1w4/edit?usp=sharing

How to get involved



- Home page: https://github.com/kubernetes/community/tree/master/wg-data-protection
- Bi-weekly meeting on Wednesdays at 9am Pacific Time. Meeting recordings available on YouTube.
  - Agenda doc
- Mailing list: https://groups.google.com/a/kubernetes.io/g/wg-data-protection
- Slack channel: #wg-data-protection

KubeCon CloudNativeCon
North America 2026

Thank You

