DELL Technologies

Solution Brief

Dell Container Storage Modules

Empower your developers with a simple, consistent, integrated, and automated experience for enterprise storage and cloud native stateful applications.

Benefits of Dell CSM

Extend enterprise storage to Kubernetes

Accelerate adoption of cloud native workloads with proven enterprise storage

Empower developers through automation

Reduce development cycles by integrating enterprise storage with existing Kubernetes toolsets

Safely and seamlessly consume storage

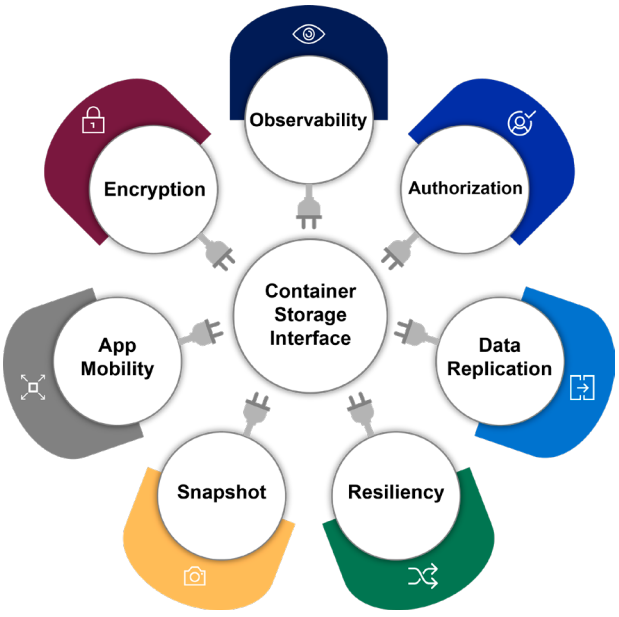
Monitor and secure operations across enterprise storage and DevOps environments

Kubernetes adoption is accelerating, as 90% of surveyed organizations agree that cloud native technology, including Kubernetes, is transforming the way their business operates.[1] However, with 76% of organizations[1] utilizing multiple clouds for their Kubernetes deployments, management requirements across these disparate environments can lead to unexpected challenges. For Kubernetes admins and developers, this means lack of visibility and monitoring, difficulty meeting security and compliance demands, and inconsistent multicloud strategies.

To solve these challenges, enterprises are aligning their developers and IT operations teams, empowering them to design and operate a cloud native organization while meeting business demands and increasing quality outputs. Dell's DevOps solutions help organizations who have these goals in mind, enabling them to use their preferred Kubernetes ecosystem, select a platform suited to their cluster hosting approach, and meet data persistence, storage, and protection requirements.

Container Storage Modules

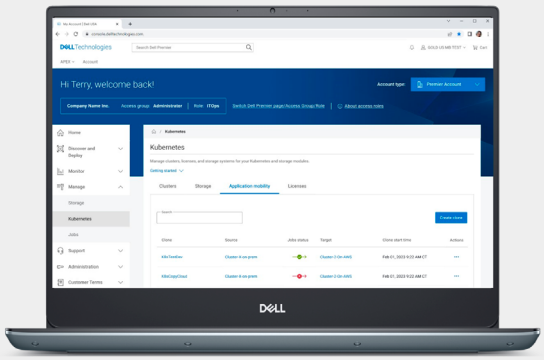
Dell's Container Storage Modules (CSM) bring powerful enterprise storage features and functionality to your Kubernetes running in Dell primary storage arrays, providing easier adoption of cloud native workloads, improved productivity, and scalable operations. Through CSM, your organization can bridge gaps between developers and IT teams with capabilities such as provisioning, snapshotting, replication, observability, authorization, security, app mobility, and resiliency for containerized workloads.



Dell CSM delivers a set of modules that builds on top of the Container Storage Interface (CSI) foundation to deliver unique, powerful storage and enterprise capabilities.

- **Replication:** Easily extend data protection and DR planning to Kubernetes workloads with consistent policy enforcement and user experience.
- **Observability:** Create a single pane management experience for your developers and K8 admins by integrating tools such as Prometheus and Grafana.
- **Resiliency:** Improve application up-time with automatic detection and recovery of node failures.
- **Authorization:** Apply quota and RBAC rules that instantly and automatically restrict a cluster tenant's usage of storage resources.
- **Encryption:** Transparently add host side encryption to a volume, allowing for encryption both at rest and in motion (using familiar external key managers such as HashiCorp Vault).
- **Snapshot:** Build on CSI's point-in-time recovery with additional capabilities such as group/crash consistent snapshots with referential integrity.
- **App Mobility:** Clone stateful application workloads and application data to other Kubernetes clusters (either on-premises or in the cloud) using a single command.

Simply Deployment, Management, and Operations of Dell Container Storage Modules



Dell APEX Navigator for Kubernetes

Dell APEX Navigator for Kubernetes is a unified SaaS-based experience in Dell Premier that simplifies Kubernetes persistence management across multisite environments. With Dell APEX Navigator for Kubernetes, storage admins and DevOps team members can leverage complete storage services management at scale for their Kubernetes ecosystem. This provides them access to advanced data services, through the easy deployment and management of Dell Container Storage Modules.

App Mobility Observability Authentication

Observability Module

CSM Observability delivers a high-level view of storage capacity and performance usage via Grafana dashboards to the Kubernetes users. Kubernetes administrators have insight into CSI Driver persistent storage topology, usage, and performance. Metrics data is collected at a fast rate (<1minute), pushed to the OpenTelemetry Collector, and exported in a format consumable by Prometheus. Topology data related to containerized volumes that are provisioned by a CSI Driver is also captured.

Other capabilities include:

- Storage pool consumption by CSI Driver
- Storage system I/O performance by Kubernetes node
- CSI Driver positioned volume I/O performance
- CSI Driver provisioned volume topology

Replication Module

CSM Replication helps to implement a high availability architecture for business critical applications, a key component of any disaster recovery plan. As such, Kubernetes users can decide that their StatefulApp will use a volume that is replicated on another site. Behind the scenes the replication module is in charge of creating the replicated volume, checking the replication process and mounting the volumes to the workload. In case of a failover / failback, the data replicator will take care or reconfiguring the replication group and remounting the volumes.

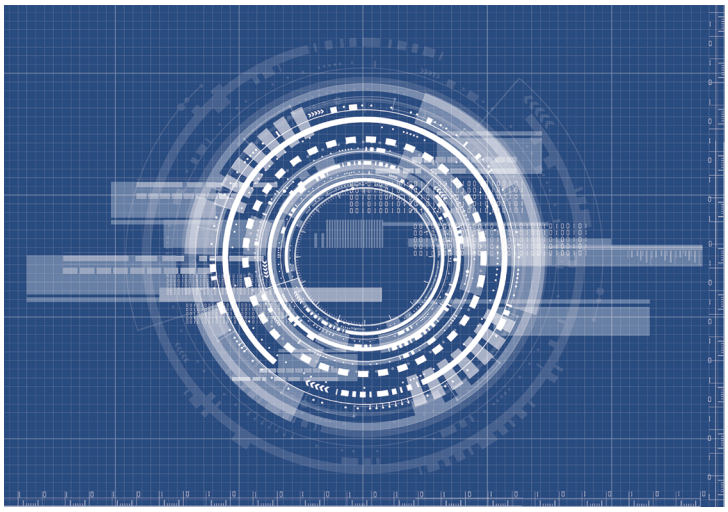
CSM Replication supports both a stretched Kubernetes cluster (one cluster with nodes on the different sites) or replicated Kubernetes cluster (separate clusters on the different sites). This allows you to choose the right disaster recovery plan for your workloads.

Snapshot Module

Snapshot capabilities are part of the CSI plugins for each Dell array and take advantage of state-of-the-art snapshot technology to protect and re-purpose data. In addition to point-in-time recovery, these snapshots are writable and can be mounted for test/dev and analytics use cases without impacting production. Through CSM, a Volumesnapshot group feature is added to the CSI snap shots, delivering additional capabilities such as group/crash consistent snapshots with referential integrity.

Authorization Module

CSM Authorization enables storage administrators to limit and control storage consumption in Kubernetes environments. With this module, storage administrators can apply quota and Role-Based Access Control (RBAC) rules that instantly and automatically restrict cluster tenants' usage of storage resources. The module does this by deploying a proxy between the CSI driver and the storage system to enforce RBAC and usage rules. The access is granted with a token that can be revoked at any point in time, and quotas can be changed on the fly to limit or increase storage consumption from the different tenants.



App Mobility Module

CSM App Mobility allows Kubernetes administrators to clone stateful application workloads and metadata to other Kubernetes clusters using a single command. It leverages native storage array capabilities and open source technologies to copy both application data and metadata to the desired object storage.

CSM App Mobility can be utilized in private and public cloud environments, helping enterprises streamline projects such as bug triage, blue-green deployments, new platform migration, dev/test environment set-up, and more.

Resiliency Module

CSM Resiliency is designed to make Kubernetes applications that utilize persistent storage more resilient to failures. CSM Resiliency uses a pod monitor that is specifically designed to protect stateful applications from various failures. It is not a standalone application, but deployed as a sidecar to Dell's CSI drivers in both the driver's controller pods and the driver's node pods. Deploying CSM Resiliency as a sidecar allows it to make direct requests to the driver through the Unix domain socket that Kubernetes sidecars use to make CSI requests. The module detects node failures (power failure), Kubernetes control plane network failures, and array I/O network failures, in addition to moving the protected pods to properly functioning hardware.

Encryption Module (Available in Tech Preview)

Protecting Kubernetes data is critical, and Dell is dedicated to providing capabilities that can further strengthen our customers' security posture. CSM Encryption accomplishes this by transparently adding host-side encryption to a volume. Through CSM Encryption, enterprises can implement encryption both at rest and in motion for the data in their Dell primary storage using familiar external key managers such as Vault by HashiCorp.

For tech preview, CSM Encryption is available for Dell PowerScale.

Learn more about Dell's Container Storage Module

Contact a Dell Technologies Expert

Read CSM Documentation
Download CSM Software

Join the conversation with #CSM

[1]The State of Kubernetes 2023, presented by VMware. Survey of 752 qualified software development and IT professionals

DELL Technologies