

Technology Watch

Technology

8 October 2026 – Cadence: Bi-weekly (Tuesday and Thursday)

Executive Summary & Topic of the Day

OpenShift Data Foundation (Rook-Ceph): software-defined storage, CSI and per-tenant encryption

Storage is the most underestimated layer of Platform Engineering. ODF industrialises Rook-Ceph on Kubernetes, exposes CSI StorageClasses (ceph-rbd, cephfs) and enables per-PV encryption with HashiCorp Vault as KMS: one key per tenant, one cryptographic boundary per namespace, a sovereign foundation for enterprise AI.

1. Scope

Watch family: 2. Jobs, Skills & Technologies (Qualiopi indicator 24).

Execution cadence: Bi-weekly (Tuesday and Thursday at 08:30).

Distribution: [Aperta Web Radar \(EN\)](#) — [LinkedIn Aperta Scientia](#) — [X @ApertaScientia](#).

2. Topic of the Day — Article Published on the Web Radar

On a Kubernetes platform you size the CPU, cap the memory, watch network latency — and then you discover the real problems the day a PersistentVolumeClaim stays **Pending**. Storage is the most underestimated layer of Platform Engineering: it decides resilience, portability and, increasingly, compliance. On OpenShift that layer has a name: **OpenShift Data Foundation (ODF)** — the operator that turns raw disks into a **Ceph** cluster consumable through the Kubernetes API.

1. ODF: a Ceph cluster governed by an operator

ODF does not invent storage: it industrialises **Rook**, the operator that deploys and reconciles **Ceph** on Kubernetes (see the [Rook Ceph documentation](#)). Three daemon families form the core:

- **MON (Monitor)** — holds the *cluster map* (topology, OSD state, placement groups); the MON quorum is the cluster's single point of decision.
- **MGR (Manager)** — exposes metrics, the dashboard and administration modules.
- **OSD (Object Storage Daemon)** — one process per disk: it stores the actual data, replicates and repairs.

Where a classic SAN demands a dedicated storage administrator, ODF exposes **Kubernetes CRDs**: you declare a **StorageCluster**, Rook converges the real state. It is the same declarative contract as the rest of the platform — and therefore the same GitOps pipeline.

2. One cluster, three consumption interfaces

Ceph storage is exposed to the cluster through **CSI drivers** that dynamically provision volumes:



- **ocs-storagecluster-ceph-rbd** — **RBD block** volumes (RADOS Block Device), **RWO** (ReadWriteOnce) access. The default choice for databases, application state and *StatefulSets*.
- **ocs-storagecluster-cephfs** — **CephFS**, a shared filesystem with **RWX** (ReadWriteMany) access. Essential for volumes shared by several Pods (build artefacts, models, pipelines).
- **S3 / Object Storage via NooBaa (Multicloud Object Gateway)** — an S3-compatible API for backups, *data lakes* and training backends.

From the platform's point of view these are standard **StorageClasses**: a PVC plus a class name, and CSI provisions the volume. That abstraction is what makes storage portable — and testable in CI like any other manifest.

3. Encryption: two granularities, one key decision

This is where ODF outgrows the black-box SAN. Ceph encryption relies on a **two-key envelope**: each volume has a **DEK** (Data Encryption Key) that encrypts the data, itself encrypted by a **KEK** (Key Encryption Key) held by an external **KMS**. ODF integrates with **HashiCorp Vault** as that KMS. Two levels coexist:

- **Cluster-wide encryption** — all data at rest is encrypted, under a single policy. This is the baseline, described step by step in the [Red Hat Developer Blog](#) article [OpenShift Data Foundation and HashiCorp Vault securing data](#).
- **Per-PV (StorageClass) encryption** — often **insufficient** in multi-tenant environments: compliance may require a **distinct key per project, tenant or sensitivity level**.

4. The multi-tenant case: isolating encryption boundaries per namespace

The [Red Hat Developer Blog](#) article [Enhance data security in OpenShift Data Foundation](#) (15 July 2025) walks through exactly that scenario. By enabling **StorageClass encryption** in the ODF installation wizard, the cluster gains an **additional encrypted StorageClass**:

```
$ oc get sc
NAME                                     PROVISIONER                                RECLAIMPOLICY
ocs-storagecluster-ceph-rbd             openshift-storage.rbd.csi.ceph.com Delete
ocs-storagecluster-ceph-rbd-encrypted (default) openshift-storage.rbd.csi.ceph.com Delete
ocs-storagecluster-cephfs               openshift-storage.cephfs.csi.ceph.com Delete
```

Isolation is built in four moves, each mapped to a Kubernetes primitive:

1. **A Vault role and ACL per tenant** — each namespace gets its own path (`kv/tenant-a/`), hence its own cryptographic boundary.
2. **A ConfigMap inside the namespace** — overrides the CSI configuration to point the volume at the right Vault path.
3. **A dedicated ServiceAccount**, bound to the Vault role through **Kubernetes Auth** (`bound_service_account_namespaces`).
4. **PVCs in the namespace** consuming the encrypted StorageClass — each volume is sealed by the tenant's KEK.

An engineering point that is often missed: **Kubernetes discourages long-lived ServiceAccount tokens** (since v1.22). The right reflex is a **short TTL** in the Vault policy, with automatic rotation through the **TokenRequest API**. The secret no longer lives forever in a Secret; it lives in time.

5. Why this is foundational for AI platforms (AS300)

Storage is not a peripheral *DevOps* topic: it is the substrate of enterprise AI.

- **Distributed training** — datasets must be mounted **RWX** by several workers; CephFS becomes the meeting point for jobs.
- **RAG and vector databases** — a backend such as **Milvus** relies on **RBD** block volumes for its persistent indexes, with CSI snapshots.
- **Model store & registry** — model artefacts and checkpoints are *stateful* volumes: **CSI snapshots and clones** let you version a state without a full copy.
- **Sovereignty** — encryption at rest with keys you control (**Vault KMS**) and internal S3 (**NooBaa**): training data never leaves the perimeter.

3. Curriculum Impact — AS200 & AS300

- **AS200 track (DevOps Platform Engineer — 399h)**: cloud-native storage module — Rook-Ceph architecture (MON/MGR/OSD, placement groups, replication), CSI drivers and dynamic provisioning, RBD (RWO) vs CephFS (RWX) StorageClasses, CSI snapshots/clones, declarative **StorageCluster** deployment through OpenShift GitOps (ArgoCD), PV labelling and access policies.
- **AS300 track (AI Platform Engineer — 399h)**: storage for AI platforms on Red Hat OpenShift AI — RWX dataset mounts for distributed training, RBD persistence backends for vector databases (Milvus/Qdrant) in RAG pipelines, model store and checkpoints versioned through CSI snapshots, per-tenant encryption at rest with Vault KMS for compliance and data sovereignty.
- **Cross-cutting competency validated**: reasoning about an encryption policy (cluster-wide vs per-PV), defining a tenant's cryptographic boundary and automating it with GitOps.

4. Sources & Technical References

- **Red Hat Developer Blog** — *Enhance data security in OpenShift Data Foundation*: <https://developers.redhat.com/articles/2025/07/15/enhance-data-security-openshift-data-foundation> (accessed 2026-10-08)
- **Red Hat Developer Blog** — *OpenShift Data Foundation and HashiCorp Vault securing data*: <https://developers.redhat.com/articles/2025/04/10/openshift-data-foundation-cluster-wide-encryption-hashicorp-vault> (accessed 2026-10-08)
- **Red Hat** — *OpenShift Data Foundation (product page)*: <https://www.redhat.com/en/technologies/cloud-computing/openshift-data-foundation>
- **Red Hat Documentation** — *OpenShift Data Foundation 4.22*: https://docs.redhat.com/en/documentation/red_hat_openshift_data_foundation
- **Rook** — *Rook Ceph Documentation*: <https://rook.io/docs/rook/latest-release/Getting-Started/intro/>
- **Ceph** — *Ceph Documentation*: <https://docs.ceph.com/en/latest/>
- **Kubernetes CSI** — *CSI Developer Documentation*: <https://kubernetes-csi.github.io/docs/>



Contacts & Community:

- **Academic Programs:** learning@apertascientia.io
- **Disability Officer & Student Care:** care@apertascientia.io
- **X (Twitter):** [@ApertaScientia](https://twitter.com/ApertaScientia)
- **Discord Community:** discord.gg/eDJzR5Vk85

Generated by Argos (AGT-002) under the supervision of Sophia (AGT-001). Red Hat, OpenShift and Ansible are trademarks of Red Hat, Inc.

