cpl.thalesgroup.com

THALES
Building a future we can all trust

Secure, Compliant Key Management for Red Hat OpenShift Data Foundation Encryption:

Using Thales CipherTrust Manager for centralized key and policy administration

Key Benefits:

- Meet compliance mandates such as PCI DSS, GDPR, and CCPA
- Streamline encryption management with seamless key rotation and data re-keying
- Reduce administration costs with centralized key and policy management
- Optional FIPS 140-2 Level 3 hardware security

The Problem

Container based applications' ephemeral nature promises organizations efficiency, speed, and scale. However, for applications to be of their greatest use as they spin up and down, they must have access to data that persists. Red Hat OpenShift Data Foundation's (ODF) software defined storage for containers tackles this challenge so teams can develop and deploy cloud native applications quickly across clouds while giving them access to the data they need to use. Yet, when it comes to data – particularly sensitive, regulated data – security and privacy compliance become critical topics.

For these scenarios, Red Hat is teaming up with Thales to bring best-in-class security to support enterprises in their OpenShift deployments.

CipherTrust Manager For Red Hat OpenShift Data Foundation

The Solution

Red Hat OpenShift Data Foundation supports cluster-wide encryption for all disks and multi-cloud object gateways to protect data from both physical theft and unauthorized access from namespaces inside the same OpenShift Container Platform (OCP) cluster. When it comes to encryption, best practice and regulatory compliance dictate that organizations separate encryption keys from their encrypted data, and manage these keys throughout their lifecycle in a dedicated key manager. Thales CipherTrust Manager integrates with ODF via the Key Management Interoperability Protocol (KMIP) to meet these security and compliance requirements.

Why Use Thales CipherTrust Manager With Red Hat OpenShift Data Foundation?

Combining Red Hat OpenShift Data Foundation with Thales CipherTrust Manager lets organizations centrally manage the encryption keys securing their persistent sensitive data in alignment with their larger organization-wide key management strategy. Additionally, CipherTrust Manager simplifies an organization's ability to demonstrate their regulatory compliance with the data privacy rules governing their industry.

Centrally Define and Manage Policies to Separate Duties Among Users and Administrators

Administrators can set authentication and authorization policies in CipherTrust Manager that define which users and processes are allowed to access the encrypted ODF data in clear text. Organizations tighten governance of their sensitive data through these controls. Properly tuned policy-based access controls provide an important security layer for organizations subject to mandates that require clear separation of duties between IT and security administrators.

Detailed Logging Functionality for Auditing and Reporting Requirements

CipherTrust Manager records detailed data concerning key status and access in centralized logs that simplify reporting to auditors and regulators. Centralized tracking of key usage and access requests reduces blindspots and improves data security. CipherTrust Manager's reports help to streamline the compliance reporting process while strengthening security around ODF's native encryption keys.

Streamlined, Simplified Encryption Administration

Vendor provided encryption can easily turn into a collection of security silos if not managed well. CipherTrust Manager consolidates Red Hat OpenShift Data Foundation's encryption keys into an easy to use management platform where organizations can manage them along with keys from a wide variety of encryption solutions including: the Thales CipherTrust Data Security Portfolio, self-encrypting drives, tape archives, Storage Area Networks, Cloud Service Provider native encryption, and an ever growing list of vendors supporting the OASIS Key Management Interoperability Protocol (KMIP) standard.

About Thales

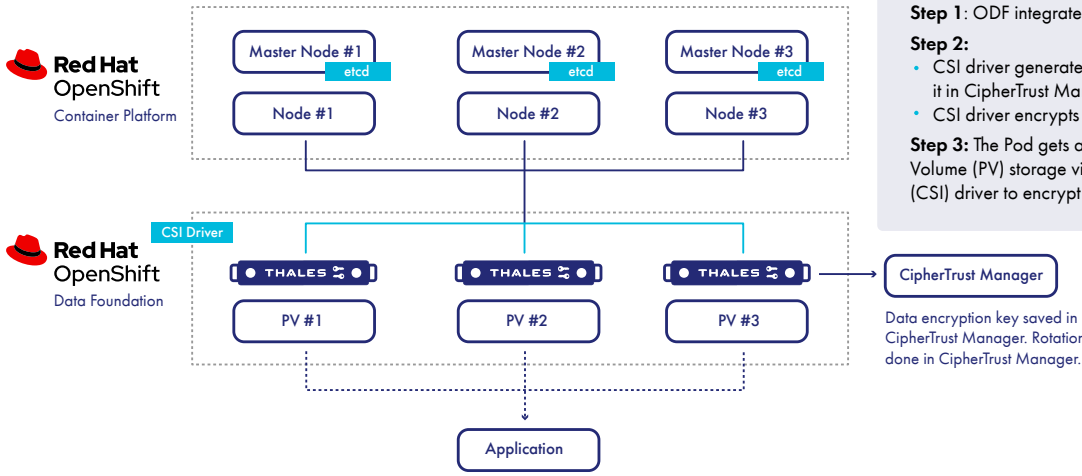
The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

About Red Hat

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers integrate new and existing IT applications, develop cloud-native applications, standardize on our industry-leading operating system, and automate, secure, and manage complex environments. Awardwinning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500. As a strategic partner to cloud providers, system integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future.

For more detailed technical specifications, please visit https://cpl.thalesgroup.com/ or https://www.redhat.com



Step 1: ODF integrates with CipherTrust Manager

Step 2:

- CSI driver generates encryption key in memory and stores it in CipherTrust Manager
- CSI driver encrypts PVs using new encryption key

Step 3: The Pod gets access to the encrypted Persistent Volume (PV) storage via the Container Storage Interface (CSI) driver to encrypt and decrypt the data.

> cpl.thalesgroup.com <

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us