Zettaset & Red Hat OpenShift Container Platform

Red Hat Software Partner

Zettaset

Introduction

Application binaries can be packaged in different formats and ways for different delivery methodologies such as to run on ; bare metal servers, virtual machines and/or containers. Each of these approaches has their own strengths and weaknesses by means of performance/cost, life cycle management , portability and security.

Key Features

- Provides real-time data protection
- High performance with near zero impact
- Container storage separation
- Direct integration with Kubernetes
- Automated encryption policy management
- No changes to your existing processes

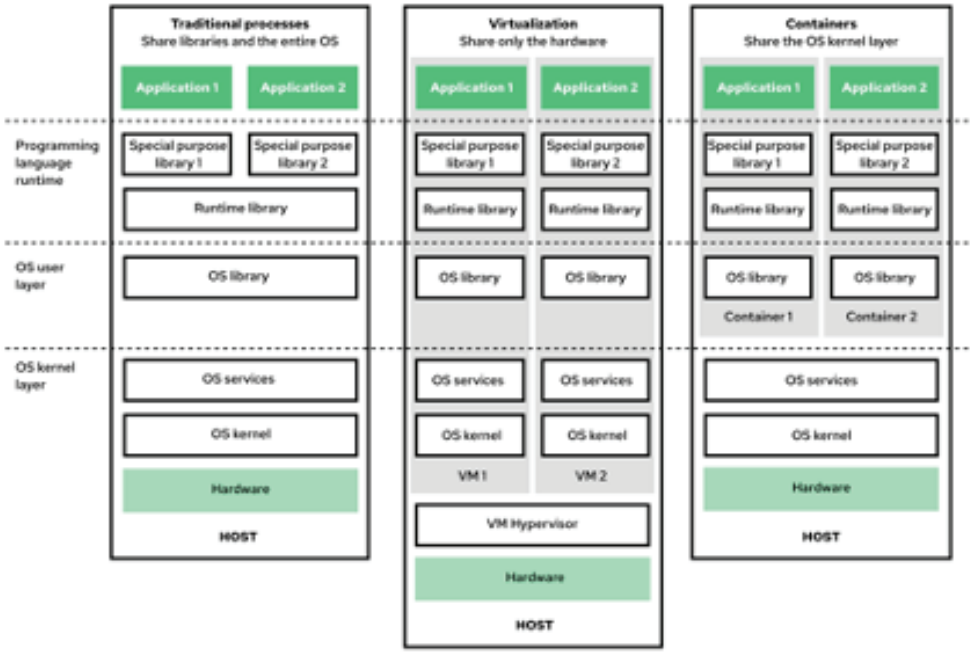


Figure-2 Application Packaging & Delivery Pillars

Red Hat OpenShift Container Platform (OCP) enables application developers to deliver their work either as docker containers and/or virtual machine encapsulation on the same deployment platform. Zettaset OpenShift Security Solution delivers on the promise of container data security in the same way that Red Hat delivers the stable, consistent, and supported base that organizations need to get applications out the door faster.

Protecting data that's stored and used in multi-tenant container environments is required – and Zettaset's software-defined encryption makes it simple. With Zettaset, OpenShift users can flexibly protect container data across any on-premises, cloud, or hybrid deployment with fast and transparent encryption that has a negligible[2] effect on performance, enabling them to:

- Confidently focus on driving innovation quickly
- Dramatically reduce the risk of potential breaches and data theft
- Ensure developers are no longer required to make security decisions
- Create a smooth plan for the transition to DevSecOps

[2]Run-time performance impact is expected to be between 2% and 7%

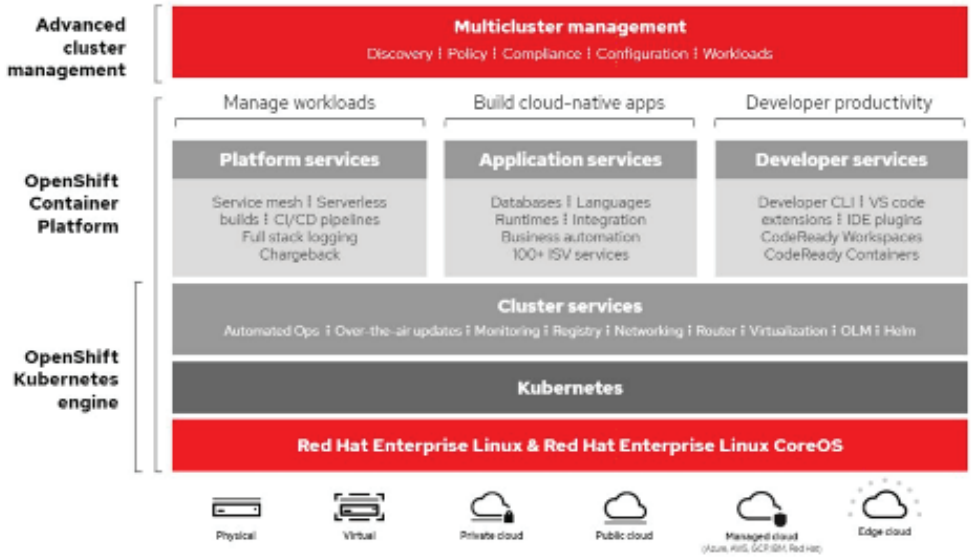
Red Hat
Technology Partner

Red Hat
Certified Technology

"Zettaset delivers on the promise of container data security in the same way that Red Hat OpenShift delivers the stable, consistent, and supported base that organizations need to get applications out the door."

Tim Reilly, CEO, Zettaset

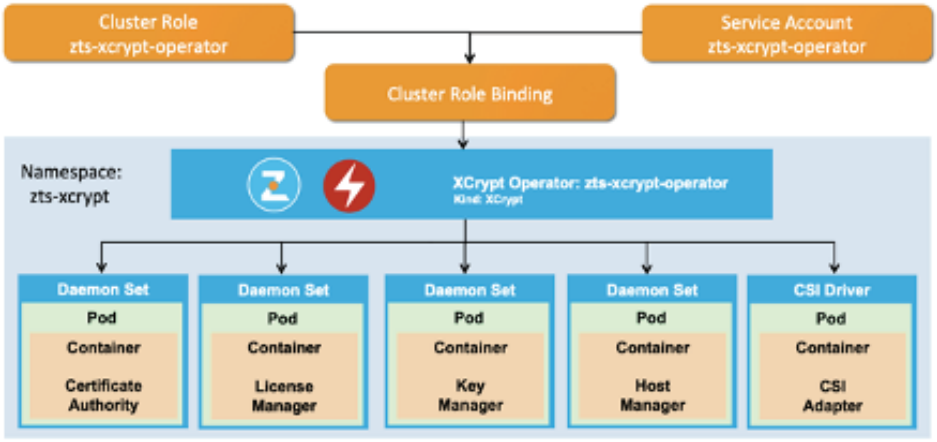
Red Hat OpenShift Container Platform (OCP) is a true multi & hybrid cloud application development, testing, delivery and execution platform with a well-known & accepted as one of the best (and trusted) enterprise operating systems under the hood.



Red Hat OCP has been architected and implemented with enterprise needs in mind for challenging environments , while offering best performance & security , Red Hat OCP enables third party independent software vendors (ISV) to onboard their software as part of the overall solution with Red Hat software portfolio via the marketplace. One of Red Hat's key ISV partners is Zettaset. Zettaset's Red Hat Certified Security Add-On Solution makes it incredibly easy to automate the deployment of software-defined encryption (security at rest) that transparently protects container data throughout your OCP environment.

Solution Architecture

Application developers like to leverage platform abilities to secure their application runtime, the data-in-transit with their application {receiving -> processing & generating -> sending } over network and data stored at rest.



Zettaset XCrypt product suite is a software-only solution that provides transparent high performance data-at-rest and data-in-motion encryption for OpenShift environments with following solution components:

- Zettaset XCrypt Kubernetes Encryption runs natively in OpenShift clusters and provides data-at-rest encryption services backed by the necessary security infrastructure.

- Zettaset XCrypt Kubernetes Encryption enables transparent high-performance data-at-rest encryption for container volumes. By integrating directly into the Kubernetes storage layer via Container Storage Interface (CSI), it is able to provision encrypted storage on demand. By requesting persistent volumes (PV) and persistent volume claims (PVC) of type "Zettaset Encrypted Storage", pods are automatically assigned dedicated encrypted storage with each persistent volume encrypted with its own unique cryptographic key. This level of key granularity enables ultimate data protection and prevents one compromised container from exposing data volumes allocated for other containers in multi-tenant environments.

- Zettaset Cryptographic Module runs inside the shared kernel stack of each worker node. Performing cryptographic operations inside the kernel and using AES-256 Native Instructions (NI) that are part of modern chipsets, the overhead of encryption is kept to a minimum. Raw disk I/O benchmarks show between 3% and 7% performance degradation when encryption is introduced.

- Zettaset Key Manager service provides KMIP-compatible key management services, which are specifically suited for managing encryption keys, and are superior to secret management services provided by Kubernetes Secrets. The Key Manager can interoperate with other KMIP-compliant key managers, such as Fornetix Vault Core or Thales/Gemalto Key Secure. The software-based key manager supports virtually unlimited number of cryptographic keys. Its master keys are securely stored in a PKCS#11-compliant Software Security Module (SSM) that can be replaced with any PKCS#11-compliant Hardware Security Module (HSM) for environments that require higher level of key security, a FIPS-certified HSM, or have an existing key management infrastructure.

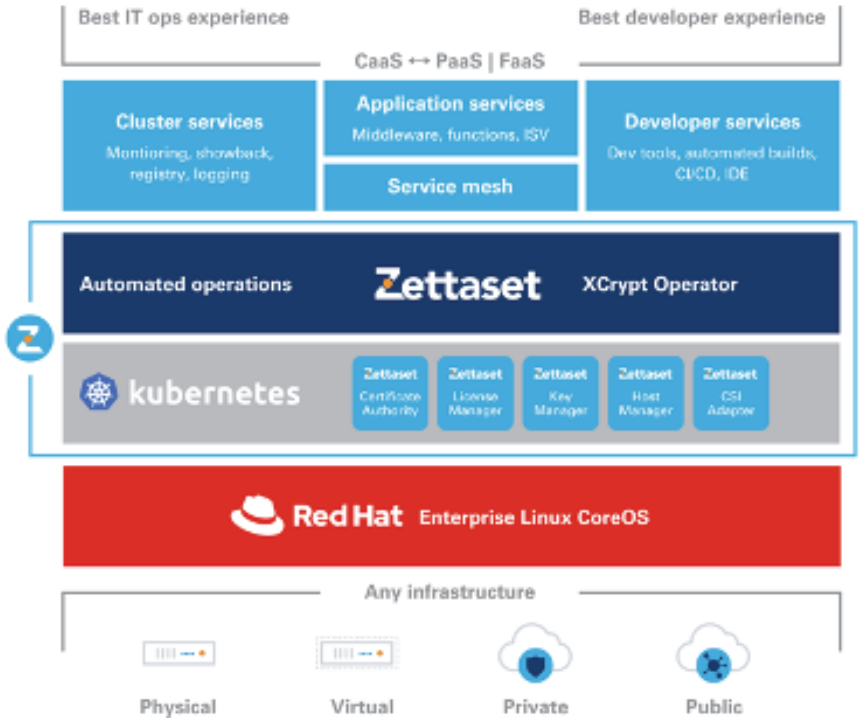


Figure-4 Zettaset XCrypt Kubernetes Encryption in OpenShift

- Zettaset Certificate Authority (CA) service is responsible for establishing infrastructure for secure communication among Zettaset XCrypt components and services. In addition, this service enables several enterprise-oriented security features that allow rapid response to intrusions and compromises. With a single administrative command, a worker node can be securely decommissioned, which will prevent that compromised node from accessing any sensitive information. Also, any persistent volume that is deleted will have its encryption key automatically destroyed on the Key Management server. This will prevent any possibility of data recovery by directly mining storage device data blocks.

- Zettaset Encrypted Storage Manager is a service that is responsible for automated provisioning of encrypted volumes at the request of Kubernetes Container Storage Layer via Container Storage Interface (CSI). Each storage volume is separate from other storage volumes, even if they occupy the same storage device. Each storage volume is encrypted with its own unique cryptographic key, which is securely stored in the Key Manager. Encrypted volumes are only mounted to worker nodes when those volumes are actually in use by one or more containers running on that worker node. Encrypted Storage Manager component also performs storage management to automatically allocate individual storage volumes assembled from one or more available storage units. In addition to managing dedicated storage attached to worker nodes, it is also capable of allocating storage volumes in select Cloud Native Storage systems.

- Zettaset CSI Adapter is responsible for translating Kubernetes Container Storage Interface (CSI) requests into request format that Zettaset Encrypted Storage Manager understands. This component intercepts typical CSI storage management commands. Its master instance is running on Kubernetes Master, and one node instance runs on each worker node.

Complete Zettaset XCrypt Solution can be installed and managed via Kubernetes Native way by an Red Hat OpenShift certified operator which is available via OpenShift Operator Hub. Additionally, all Zettaset container images are based on Red Hat Universal Base Images (UBI) and are certified by Red Hat.

Zettaset XCrypt Solution Resource Footprint

Following are the sizing guidelines and footprint information of Zetaset application/capability on Red Hat OpenShift cluster:

Container	Topology	Image Size	Storage	Memory Use (average/peak)	CPU Use (average/peak)
Certificate Authority	1 per cluster Control Plane Temporal	641MB	N/A	N/A	N/A
Key Manager	2 per cluster Control plane	635MB	5MB +	100MB - 150MB	0.15% - 10%
License Manager	1 per cluster Control plane	637MB	N/A	125MB - 150MB	0.15% - 0.40%
Host Manager	1 per worker node	747MB	10MB	255MB - 430MB	0.25% - 15%

Table-1 Zettaset XCrypt Resource Footprint

Certificate authority server is only required to be running during initial product deployment and when new worker nodes are added or existing/compromised worker nodes are removed from the cluster.

Key Manager storage size will increase as more persistent volumes are created. The increase in storage utilization will be less than 1MB per unique persistent volume.

Peak memory and CPU usage represent bursts in memory and CPU utilization when new persistent volumes are created. In normal operation, CPU and memory utilization are maintained around stated averages.

No additional software and now special configuration is required for application and services containers. Zettaset XCrypt Kubernetes Encryption will not increase resource utilization for those containers.

Key Manager includes active-passive service configuration with automatic key replication to provide high availability for both service and data. It is recommended to use distributed highly available storage for persistent volumes allocated for Key Manager and Host Manager services. If availability of Kubernetes Control Plane is a factor, Key Management services may be located outside of the Kubernetes cluster as long as there is a network communication between the Kubernetes cluster and Key Management services.

The following diagram shows network topology of encryption services provided by Zettaset XCrypt Kubernetes Encryption.

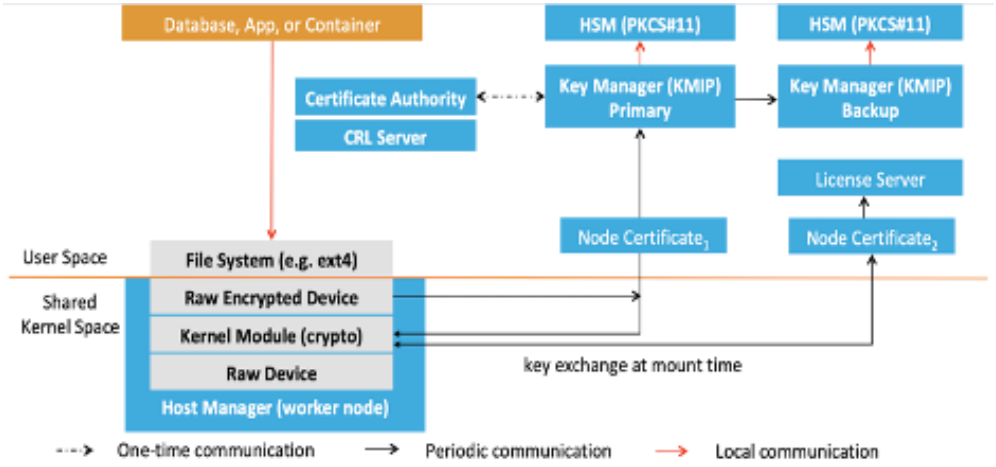


Figure-5 Zettaset XCrypt Kubernetes Encryption Topology and Communication

Many of the performance benefits of Zettaset XCrypt Kubernetes Encryption come from the fact that expensive network communication that includes SSL/TLS connection negotiation occurs infrequently, only when absolutely necessary. These include a one-time communication between the Key Manager and Certificate Authority/CRL service when the Key Manager is starting up as well as key exchange communication when new persistent volume is provisioned or when an existing persistent volume is mounted to a running container.

The advantages of this approach are that time-consuming context switching between kernel space and user space as well as key retrieval operations don't occur nearly as frequently as they would in an infrastructure-based file-level encryption solution. File-level encryption requires switching from kernel space and user space and back as well as key retrieval network operations for every file operation. Consequently, file-level encryption solutions deployed in Kubernetes environments result in very significant performance hit. Zettaset XCrypt Kubernetes Encryption is able to avoid this performance hit due to its advanced Kubernetes-native design.

Solution Key Differentiators

Zettaset XCrypt Kubernetes Encryption for OpenShift provides unified vendor-agnostic and storage-agnostic encryption services for stateful containers and pods no matter which environment the pods run in: on-premise, in the cloud, or hybrid. Thanks to OpenShift Operator implementation, the deployment is simple and fully automated. All container images used as part of the encryption system are certified by Red Hat.

High performance and complete transparency are the hallmarks of Zettaset XCrypt Kubernetes Encryption. Applications will not suffer from performance degradation typically associated with introducing encryption. Users and administrators will not have to change the way they interact with OpenShift clusters to take full advantage of data encryption. No cryptographic knowledge is required to deploy and use Zettaset software. Developers will be able to focus on rapid application development without concerns that arise from dealing with sensitive enterprise data. Simple "point-and-encrypt" policy management enables administrators to focus on the health and performance of OpenShift clusters instead of worrying about where sensitive data might be and which containers may be accessing it. Since encryption services are running within the shared kernel space, there is no need to install any additional software inside application containers.

Zettaset XCrypt Kubernetes Encryption simplifies certification and compliance initiatives for PCI, HIPAA, GDPR, as well as other compliance initiatives by providing data at rest and data in transit encryption. Data encryption is commonly identified as one of the simplest ways to achieve compliance.

Zettaset XCrypt Kubernetes Encryption provides light-weight encryption services and is suitable for deployment in locations where worker nodes are geographically remote to the rest of the Kubernetes cluster.

A self-contained complete encryption solution, Zettaset XCrypt Kubernetes Encryption provides the ultimate protection for enterprise data. It is the last line of defense designed to complement and enhance other security solutions that may focus on integrity of container software stack or on container perimeter security. A software-only solution, it will scale as the container environment scales.

Unique key for each persistent volume ensures that container volumes remain secure and granular approach to encryption allows secure decommissioning of individual volumes as well making sure that volumes are only available when in use. Compared to infrastructure-controlled encryption, such as that provided by Self Encrypting Drives (SEDs), Zettaset XCrypt Kubernetes Encryption provides greater key granularity, automated KMIP-compliant key management, interoperability with other Key Managers, and most importantly, comparable level of application performance and lower Total Cost of Ownership (TCO).

Summary

Multi-tenant application modernization platforms present unique security challenges and introduce multitude of new attack vectors. For example; inside the very same enterprise/corporation different organization groups may be subject to different regulatory compliances for their business verticals, each organization brings their own failure as well as security domain needs that they are responsible for, where they are simply the tenants of the same underlying platform. Therefore, it is critical to implement data security solutions that are designed and developed to work in multi-tenant application platform (Red Hat OpenShift Container Platform) natively and to scale as these platforms scale.

While other types of security software focus on protecting container runtime and software stack, controlling policies, and looking for vulnerabilities, Zettaset XCrypt software suite provides the first and the last line of defense, securing the data - the most valuable commodity of any enterprise - in storage and in motion , all which delivered container natively within Red Hat OpenShift Container Platform.

Learn More about Software-defined encryption with Zettaset

Company: Zettaset Contact: sales@zettaset.com URL: www.zettaset.com

About Zettaset

Zettaset is a leader in data protection and security. Its software-defined encryption solution protects against data theft and can be transparently deployed across all physical and virtual environments. Zettaset's XCrypt products offer high performance encryption that scales efficiently across all types of enterprise infrastructures. The XCrypt Platform simplifies encryption deployment and policy management to achieve the required level of data protection. Whether sensitive data resides on-premise, in the cloud or in hybrid environments, Zettaset encryption is there to secure and defend these critical assets.

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. Award-winning 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.

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

North America
1 888 REDHAT1
www.redhat.com

Europe, Middle East, and Africa
00800 7334 2835
europe@redhat.com

Asia Pacific
+65 6490 4200
apac@redhat.com

Latin America
+54 11 4329 7300
info-latam@redhat.com

redhat.com