



Red Hat



Data Protection for OpenShift Virtualization with Veeam Kasten





Contents

Overview	3
Why Veeam Kasten for OpenShift?	3
Stateful Cloud-native Applications Require Business Continuity	3
VMs on Kubernetes Makes Application Modernization Easier	3
Red Hat OpenShift Virtualization for VMs	4
Red Hat OpenShift with Veeam Kasten for Freedom of Choice	4
Modernize Applications on Red Hat OpenShift Virtualization	4
Accelerate Veeam Kasten Data Operations on Red Hat OpenShift	5
Enterprise Data Protection with Veeam Kasten and Red Hat OpenShift	5
Install Veeam Kasten Operator Quickly and for Free	6



Overview

Veeam Kasten delivers reliable backup and disaster recovery (DR) for Kubernetes applications and allows virtual machine (VM) and container workloads on traditional infrastructures to operate consistently in modern cloud-native environments.

Why Veeam Kasten for OpenShift?

Built for Kubernetes

Constructed using cloud-native architectural principles, Veeam Kasten provides simplicity via streamlined operations and modern tooling.

Security Everywhere

Comprehensive end-to-end security via enterprise-grade encryption, customer-managed keys, and ransomware protection. Delivers maximum versatility, protecting your data no matter its state or location.

Ease of Use

Quick to deploy and easy to use via a state-of-the-art management interface or cloud-native API. Enables DevOps team agility and reduces the complexity of identifying and protecting system applications.

Stateful Cloud-native Applications Require Business Continuity

Cloud-native application modernization requires the combined efforts of operation and developer teams to adopt stateful workloads -- like VMs and databases -- on Kubernetes. Data protection consists of backup and restores on the cluster, VM exports and imports between clusters for DR and cyber resilience, and securely managing artifacts with policy-based governance.

VMs on Kubernetes Makes Application Modernization Easier

Many teams take an infrastructure-first approach to modernization and "lift and shift" existing applications on VMs to new infrastructure providers. Unfortunately, this costly exercise must be repeated to achieve multi-cloud and hybrid-cloud outcomes. These migrations do not advance to cloud-native infrastructures on Kubernetes either and failed migrations can result in re-patriation of workloads.



VMs are stateful workloads on Kubernetes. VMs hosted on OpenShift Virtualization and protected by Veeam Kasten speed up cloud-native application modernization by solving and improving on traditional application infrastructure, operation, and tooling problems.

Red Hat OpenShift Virtualization for VMs

Red Hat OpenShift Virtualization, a feature of [Red Hat OpenShift](#), allows IT teams to run [VMs](#) alongside containers on the same platform, which simplifies management and improves time to production. By unifying the management and operation of VMs and containers, OpenShift Virtualization reduces operational overhead and drives better alignment between IT operations and development teams. It also maximizes hardware usage, which leads to significant cost savings. Integrating VMs into an OpenShift application platform can provide a consistent environment for application development and deployment. Developers can build, test, and deploy applications faster, which accelerates time to market.

Red Hat OpenShift with Veeam Kasten for Freedom of Choice

Veeam Kasten for Kubernetes DR protects persistent workloads and VMs on Red Hat OpenShift clusters. With Red Hat OpenShift Service on AWS, public-cloud and hybrid-cloud VM application protection becomes easy and secure, since it covers both cloud and on-premises deployments. Migrating VMs between clusters, cloud providers, and OpenShift versions is a DR operation made simple with Veeam Kasten.

With Kasten Transforms, data protection operations between different infrastructure providers can migrate VMs between heterogeneous OpenShift clusters, like from data center to branch office to edge location and back. This solution also enables VM cloning data operations for forensics, troubleshooting, and ransomware recovery.

Modernize Applications on Red Hat OpenShift Virtualization

Certain applications with stringent security or performance requirements can pose challenges for Kubernetes. Due to the shared-resource nature of container hosting on a cluster node, pods may not provide enough isolation for security purposes. Applications may also require elevated security privileges that may be blocked by the provider. Container pods do not expose any tunable kernel resources for performance considerations either.

Combined with Veeam Kasten, development and operation teams can protect stateful workloads in VMs and containers together on Red Hat OpenShift clusters. By protecting their entire application environment, developers can modernize applications in place and experiment with cloned instances in different namespaces and clusters. This enables many modernization scenarios for persistent applications in VMs, aided by Veeam Kasten data operations:

- Pods and containers may not guarantee enough application security isolation, so VMs on Kubernetes remains a better solution.
- Containers and pods may not guarantee enough application performance, but VMs on Kubernetes enable tunable kernel resources.
- Traditional, monolithic VM applications can be partially or fully refactored alongside neighboring containers in the same namespace, pod, etc. with Kubernetes.



Distributed application VMs --like databases -- require system and/or logical tooling for backup and recovery, since individual VM snapshots cannot capture your entire data domain. Veeam Kasten's blueprint orchestration allows for application-consistent artifacts with full control over application operators, CLIs, and APIs.

Accelerate Veeam Kasten Data Operations on Red Hat OpenShift

Data protection is measured with recovery point objectives and recovery time objectives (RPOs and RTOs), and traditional applications delegate RPO and RTO responsibilities to operations teams and their tools. Unfortunately, these traditional tools often do not work in cloud-native environments, address distributed cloud-native applications, or have significant restrictions. Most data protection tools cannot address the cloud-native and application-consistent backup and restore operations that developers require.

By using the Continuous Integration and Continuous Delivery (CI/CD) capabilities of Red Hat OpenShift Container Platform, organizations can modernize their applications using Veeam Kasten data operations for cloud-native operations. "Day 0" deployment and ongoing "Day 2" maintenance data operations delivered by Veeam Kasten can also be invoked by API or CLI in a CI/CD pipeline.

- Development and testing environments can be populated with real data from vetted production or other backup sources via Veeam Kasten data operations for full fidelity as opposed to synthesized or mock data.
- Cloud-native data protection can become a converged effort of developers and operators, and DR can be configured and tested in pipelines to achieve RPO and RTO goals.
- GitOps can automate deployment, updates, and policy governance to Veeam Kasten as well to help achieve RPOs and RTOs for any VM workload on multiple clusters.
- Data operations can extend to application-consistent backup and recovery for VMs and applications.

Enterprise Data Protection with Veeam Kasten and Red Hat OpenShift

Easily Backup and Restore Applications Anywhere

Automatically capture and protect an entire application stack, including resource definitions, configurations, and underlying data to restore to a known good state. Through Kasten's integration with OpenShift Data Foundation, you can extend compatibility, security, and scalability across environments through policy-driven automation. Manage where and how your backups are securely replicated to off-site storage while enabling near-zero RTOs for your Kubernetes workloads.

Protect Against Ransomware and Prevent Data Loss

Configure policies to automate DR workflows, leverage Kubernetes-native RBAC, and benefit from backup immutability to protect your recovery paths and application data from ransomware attacks.

Veeam Kasten, combined with Advanced Cluster Security (ACS), can provide enhanced visibility, proactive threat detection, and reliable data protection to ensure a resilient and secure environment for Kubernetes, no matter where you run your cloud-native workloads.



Install Veeam Kasten Operator Quickly and for Free

Veeam Kasten is a certified OpenShift operator that is quick and easy to install from the [Red Hat Marketplace](#) and supports flexible licensing. Learn more about the partnership between Red Hat and Veeam and get started today with a free, fully featured version of Veeam Kasten of up to 5 nodes!

About Veeam Kasten

Trusted by the world's largest organizations, [Veeam Kasten](#) delivers secure, Kubernetes native data protection and application mobility, at scale, and across a wide range of distributions and platforms. Proven to recover entire applications quickly and reliably, coupled with its core tenet simplicity, Kasten gives operations and app teams confidence to withstand the unexpected.

→ Learn more: veeam.com

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 develop cloud-native applications, integrate existing and new IT applications, and automate and manage complex environments. [A trusted adviser to the Fortune 500](#), Red Hat provides [award-winning](#) support, training, and consulting services that bring the benefits of open innovation to any industry. Red Hat is a connective hub in a global network of enterprises, partners, and communities, helping organizations grow, transform, and prepare for the digital future.