Kasten by Veeam
Backup, DR e migrazione multi-cloud per Red Hat OpenShift

Danilo Chiavari
Presales Manager, Italy
Veeam Software
Best of Breed Technology Alliance

"Data protection and backup is a necessity for managing Kubernetes at scale across the hybrid cloud. We are pleased to collaborate with Kasten by Veeam so organizations across the globe can use Kasten K1O data management platform with Red Hat OpenShift to rollout, upgrade and protect their cloud-native applications."

Joe Fernandez
VP and GM, Core Cloud Platforms at RedHat
Kasten by Veeam: our Mission

Kasten's **Mission** is tackling Day 2 data management challenges to help enterprises confidently run applications on **Kubernetes**.

- **Backup & Restore**
- **Disaster Recovery**
- **Application Mobility**
Kasten by Veeam: industry recognition

Kasten K10 is a Kubernetes-native, mature solution that’s very suitable for self-hosted, self-managed use cases. It’s architecture scales well and is especially well-suited for edge deployments.

It’s RBAC features and centrally managed policy model are well aligned with large enterprise and self-service requirements.

It’s application-aware data management framework, Kanister, is promising and quickly maturing. It has good support for on-premises repositories.

Enrico Signoretti
Senior Data Storage Analyst, GigaOm
December 2021
Kubernetes Data Protection - Key customer asks

**Kubernetes native**
Automation and workflows in Kubernetes native environments

**Multi-layered consistency**
Consistent data and application resources capture

**Freedom of choice**
Avoid fragmentation and enable deployment flexibility

**DevOps speed & scale**
Shift-left environments and secure self-service
Kasten by Veeam + Red Hat OpenShift
Kasten by Veeam + Red Hat OpenShift

Kasten on Red Hat Marketplace

- Backup and DR for OpenShift
- Flexible purchase options
- Level III certified operator with full lifecycle capabilities (backup, failure recovery / DR)
Kasten by Veeam + Red Hat OpenShift

Kubernetes-native, policy-based protection
How Kasten K10 by Veeam works

Applications as the Operational Unit

- Perform complete application capture
- Abstract underlying infrastructure
- Perform coordinated operations
How Kasten K10 by Veeam works

OCP Cluster

ETCD

CSI

NAMESPACE

RESOURCES

PVs

K10

API

Backup

OBJ
## Application Transforms – Kasten K10 by Veeam

<table>
<thead>
<tr>
<th>Resource</th>
<th>Transform Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress</td>
<td>Change FQDNs</td>
</tr>
<tr>
<td>Service Account</td>
<td>Merge image pull Secrets</td>
</tr>
<tr>
<td>Storage</td>
<td>Change StorageClass</td>
</tr>
<tr>
<td>Registry</td>
<td>Transform registry URLs for applications</td>
</tr>
<tr>
<td>StatefulSets</td>
<td>Transform DNS names, e.g., workload URLs</td>
</tr>
<tr>
<td>Secrets</td>
<td>Filter by label, e.g., Remove TLS secret for auto-regeneration</td>
</tr>
<tr>
<td>OpenShift</td>
<td>Internal updates, e.g., OCP ImageStream tags</td>
</tr>
</tbody>
</table>
Application Transforms – Kasten K10 by Veeam

Test Transform

Operations

Original Resource
Paste a test resource here — JSON or YAML

Transformed Resource
Transform result will be placed here.

Replace
path
"/spec/ports/0/targetPort"
value: 6380
Kasten by Veeam + Red Hat OpenShift

Kasten K10 by Veeam – Main features

**Built for Kubernetes**
Purpose-built for Kubernetes using cloud native architectural principles

**Security Everywhere**
Support for RBAC, OIDC, Token Auth, IAM and industry-standard encryption

**Rich Ecosystem**
Extensive support across the entire stack: select the best tools or infrastructure

**Ease of Use**
State-of-the-art multi-cluster UI; cloud native architecture and API, easy install, extensible
Kasten by Veeam + Red Hat OpenShift

Use case: OpenShift Migration (v3.11 → v4.3)

Integrated reporting & visibility
Kasten K10 by Veeam v5 – What’s new?

Platform Hardening & Ease of Use
- KMS integration for encryption keys management
- Kubernetes native RBAC objects (Roles and Bindings) exposed in UI dashboard

Data Protection Policy Guardrails
- Plugging vulnerabilities by identifying (and fixing) misconfigurations
- Enforceable Policy standards (e.g., RPO, retention, immutability)

Ransomware Attack Detection
- Early detection of potential / impending attack
- AWS S3 or S3-compatible storage supporting S3 Object Lock

Veeam Hardened Linux Repository with immutability
- Comprehensive, end-to-end ransomware protection, from Performance Tier to Capacity Tier
- Next step in VBR data path integration
Thank you

linkedin.com/company/red-hat
youtube.com/user/RedHatVideos
facebook.com/redhatinc
twitter.com/RedHat