Product use case

Veeam Kasten Use Case

Kubernetes-native Disaster Recovery

DR Planning in the Context of a Modern Compute Infrastructure

Disasters can be natural or man-made, but in the event of any micro or macro calamity, having a plan in place to quickly restore systems is the best method to deal with them. Computing systems are a foundational tenet of businesses, governments, and non-governmental organizations around the world, and disaster recovery (DR) plans are a key measure of preparedness.

Server Backup Does Not Protect Modern Applications

Traditional backup and restore solutions have historically been considered adequate to protect infrastructures that could be affected by disaster. With the rise of more complex computing modalities, like those that rely on virtualized container applications and services, traditional DR methods are no longer adequate protection. Organizations are still dealing with the long tail of digital transformation programs that continue to modernize the foundation of how they conduct operations.

New Tools for Computing Infrastructures

As digital transformation works through business, governmental, and non-governmental organizations, support systems are in flux with respect to how well they can deliver a solution. DR planning for Kubernetes workloads based on a variety of infrastructures is an artifact of modern computing that's currently in-process. Fortunately, tools, companies, and ecosystems are able to address the challenges presented to this in-progress, but foundational aspect of modern-day disaster planning.

Key Veeam Kasten Capabilities

Disaster Recovery Automated Workflows

Veeam Kasten delivers DR for Kubernetes applications with robust scheduled and on-demand workflows that use standard and vendor-specific cluster blueprints. Veeam Kasten's backup platform monitors and tracks backups and service restorations as well.

Automatic Import and Restore

With Veeam Kasten, you can automatically import and restore application changes to a DR cluster when a new application export is generated. Policies provide automated enforcement to help restore operations to align with service-level agreements (SLAs) after an event.

Maintain Multiple Restore-ready Backups

Increasingly, cyber attackers are targeting backup systems as part of cyber incursion. Multi-component container applications with secure backups not only improve application resilience, but elevate protection from single-volume failures and cyber intrusions too.

Product use case

Disaster Recovery for Kubernetes

DR for Modern Applications

- A microservices architecture has many pods, data sources, and deployment variations that are not defined by hardware volumes.
- With backups encrypted and stored offline and offsite locations, chances are improved that cybercriminals cannot affect the resilience of protected Kubernetes applications.
- In the case of polyglot data, each of the application data sources (including configuration, persistent, and temporary data) do not reside in the same physical or virtual space as the application.

Critical Requirements for an Effective Kubernetes DR Solution

- Components can be returned to service in test or production environments, as well as from among clones, encrypted data, and immutable backups.
- If a full application restoration is needed, an ideal Kubernetes backup management solution provides an application blueprint to sequentially restore an application and minimize impact to SLAs.
- Relaunches can be performed directly on an existing virtual platform, or it can be mobilized to an alternative platform, like an, on-premises,public cloud, private cloud, or a hybrid environment.

Disaster Recovery Use Case Scenarios

Ransomware Attack

Ransomware attacks represent slightly more than 10% of cybersecurity breaches, but they can be very costly. A typical attack results in non-ransom costs of over $4.5 million, according to the latest survey by the Ponemon Institute*. With an effective backup and encryption strategy in place, control of offline and offsite data backups can preserve data sovereignty, even in the event of a network breach.

Unintentional Failures

Natural disasters and other unplanned events such as a power outage can significantly disrupt production operations, causing revenue leakage. The ability to automatically restore a service interrupted by a disaster or mobilize a backup to an alternative production-ready environment is one of the main goals of a DR-capable organization.

Malicious Data Loss

Cybersecurity events are not the only source of a security breach — internal sources such as a disgruntled contractor, the supply chain network, or a partner organization with improperly managed access can also present a threat. The ability to protect and preserve data, especially Personally Identifiable Information (PII) of customers, partners, and employees, is of utmost importance. When live information, backup, and in-transit data is encrypted, the probability of a severe data loss and liability is significantly reduced.

Infrastructure or Hardware Failure

Even when a disaster is based on an infrastructure or hardware failure, the consequences can be catastrophic if you're not prepared to deal with recovery. IT groups can find themselves bearing the brunt of the blame if they are not using recovery tools designed for today's complex microservices infrastructure. Creating a copy of a live application or service measures application performance, data usage, and other evaluation techniques with the most current application data set.

*Ponemon Institute, (August 2022), Cost of a Data Breach Report 2022. IBM Security, https://www.ibm.com/reports/data-breach

Product use case

Specification Sheet for Disaster Recovery

Disaster Recovery Key Features	
Security	• FIPS 140-3 including multi-cluster support • Kubernetes-native Roles Based Access Control (RBAC) • Identity Access Management (IAM) • OpenID Connect (OIDC) OAuth 2.0, Framework Azure • Managed identity • Key Management System (KMS) • Token Auth
Policy-based automation	• Declarative policy definitions for separation of concerns • Automatic misconfiguration detection • GFS retention policy
Multi-cluster management at scale	• Large-scale out of the number of clusters • Simultaneous deployment and support • Performance and efficiency maintained at-scale
Generic block mode support	• Present block-based devices to VMs • Support for VMs and containers in production
Transforms library	• TransformSet custom resource (CR)
External integrations for monitoring and alerting	• Pre-integrated with Azure Sentinel, DataDog, Prometheus
User interface	• Out-of-the-box dashboards, metrics, and reports • Up-to-date status indicators for all live applications • Pre-set alarm triggers • Immutable restore point visibility
Re-deployment flexibility	• Cross-cloud portability/restorability (protection from vendor lock-in)

Product use case

Veeam Kasten *for Kubernetes* Data Protection Platform

Veeam Kasten is a Kubernetes-native data protection platform that provides enterprise operations teams with an easy to use, scalable, and secure system for backup and restore, disaster recovery (DR), and application mobility of Kubernetes applications. With Veeam, teams achieve Kubernetes-native resilience against ransomware attacks. Kasten offers an application-centric approach and deep integrations with relational and NoSQL databases, Kubernetes distributions and APIs, and cloud platforms. This provides teams with the freedom to choose any infrastructure they want while achieving maximum operational simplicity. Policy-driven and extensible, Kasten also includes features such as full-spectrum consistency, database integrations, automatic application discovery, multi-cloud mobility, and a powerful web-based user interface.

> "Throughout our evaluation, Enterprise Strategy Group determined that Kasten can deliver the data protection and recovery capabilities required by Kubernetes applications. We examined this by comparing how traditional solutions and Kasten address four major use cases: Backup and restore, DR, application mobility, and ransomware protection."

Dispelling the Myths of Kubernetes Data Protection
ESG 04 2024

Kubernetes Data Protection Use Cases: Summary

Veeam deeply understands Kubernetes and it's unique challenges with regard to backup, restore, DR, application mobility, and ransomware protection. Veeam Kasten helps enterprises successfully run applications on Kubernetes with confidence.

Veeam Kasten Use Cases

Backup & Restore
Protect your cloud native Kubernetes and VM applications, while preserving your business-critical data.

Disaster Recovery
Manage how backups are replicated off-site to meet business and regulatory requirements.

Application Mobility
Move applications between clouds and on-premises for test/dev, load balancing, data management, and upgrades.

Ransomware Protection
Protect your Kubernetes platform during cyberattacks to preserve business continuity.

For more information, visit Veeam.com or follow @Veeam on X.