

Veeam Kasten — Anwendungsfall

Moderne Virtualisierung mit Veeam Kasten

Geschäftliche Herausforderung

Viele Unternehmen setzen auf containerisierte Umgebungen, um Anwendungen schneller bereitzustellen, und prüfen Alternativen zu traditionellen Plattformen wie VMware, um mehr Flexibilität und Kosteneffizienz zu erreichen. Diese Umstellung erfordert die Optimierung der bestehenden virtualisierten Infrastruktur, während gleichzeitig neue cloudnative Architekturen eingeführt werden. IT-Teams müssen hybride Umgebungen verwalten, herkömmliche Systeme integrieren und den Datenschutz gewährleisten. Das Gleichgewicht zwischen diesen Prioritäten ist der Schlüssel zur Förderung von Innovation, zur Maximierung von Ressourcen und zur Zukunftssicherheit der IT in einer sich schnell entwickelnden Landschaft.

Willkommen in der Ära der modernen Virtualisierung

In der schönen neuen Welt der modernen Virtualisierung, in der VMs neben containerisierten Anwendungen auf Kubernetes laufen, müssen Kunden alle ihre virtualisierten Anwendungsdaten vom ersten Tag an effektiv schützen und gleichzeitig Innovation für die Zukunft voranbringen. Moderne Virtualisierung (MV) ermöglicht VMs auf Kubernetes-Plattformen (z. B. Red Hat OpenShift Virtualization und SUSE Virtualization), damit sie parallel zu Containern betrieben werden, wobei alle über eine zentrale Kontrollebene verwaltet werden. Unternehmen setzen moderne Virtualisierung ein, um Lizenzierungsrisiken und Kosten zu senken, Betriebsabläufe zu vereinheitlichen, die Sicherheit zu stärken und Anwendungen zu modernisieren, ohne dabei die Betriebskontinuität oder die Datensicherheit zu gefährden. Zu den Risiken, die mit diesem Übergang in die neue Welt der Virtualisierung einhergehen, zählen Migration und Ausfallzeiten, Tool-Fragmentierung über verschiedene Umgebungen hinweg, Lücken im Ransomware-Schutz sowie komplexe Compliance- und Sicherheitsanforderungen.

Das Wertversprechen von Veeam Kasten

Um den Datenschutz in der modernen Virtualisierung zu unterstützen, bietet Veeam Kasten eine einheitliche, Kubernetes-native Lösung für sowohl containerisierte Anwendungen als auch KubeVirt-basierte VMs. Es bietet konsistentes, richtliniengesteuertes Backup, Disaster Recovery (DR), Anwendungsmobilität und Unveränderlichkeit über lokale, Cloud- und Edge-Umgebungen hinweg.

Zukunftssichere Resilienz für VMs und Container

Einheitlicher Schutz für VMs und Container

- Sichern Sie sowohl Kubernetes-Anwendungen als auch KubeVirt virtuelle Maschinen mit einheitlichen Richtlinien.
- Reduzieren Sie Risiken und stellen Sie Konsistenz mit anwendungsspezifischen Backups sicher.
- Vereinfachen Sie den Schutz, während Sie Ihre Anwendungen modernisieren.

Disaster Recovery und clusterübergreifende Mobilität

- Schnelle Wiederherstellung oder Migration von Anwendungen — von lokal über Edge bis in die Cloud.
- Optimieren Sie Test/Dev, Upgrades und Disaster Recovery (DR) mit minimalem manuellen Aufwand.
- Sichern Sie die Business Continuity in dynamischen und komplexen Umgebungen.

Ransomware-Resilienz und Unveränderlichkeit

- Schützen Sie Backups vor Ransomware-Bedrohungen mit Object-Lock-Immutability.
- Erzwingen Sie Sicherheit durch den Zugriff nach dem Prinzip der geringsten Rechte und auditierte Workflows.
- Stellen Sie Backups auch nach Cyber-Vorfällen zuverlässig wieder her.

Automatisierung und agile Day-2-Operationen

- Beschleunigen Sie die Bereitstellung mit operatorbasierter Installation und Helm/GitOps.
- Reduzieren Sie den operativen Overhead durch Multi-Cluster-Management.
- Gewährleisten Sie sichere Abläufe mit RBAC/OIDC und FIPS.

Tiefe und Flexibilität des Ökosystems

- Integrieren Sie CSI-basierten nativen Storage mit lokalem und Cloud-Storage.
- Sorgen Sie mit Kanister Blueprints für umfassenden Datenbankschutz.
- Unterstützen Sie einen vielfältigen Technologie-Stack für echte Modernisierung.

Innovationen freisetzen: Veeam Kasten und führende Plattformen

Plattform	Gemeinsame Lösung/Integration	Universeller Veeam Kasten-Mehrwert
Red Hat OpenShift	Zertifizierter Veeam Kasten-Operator mit tiefer Integration in OpenShift Virtualization, OpenShift Virtualization Engine, und das Sicherheits-Ökosystem von Red Hat. Verfügbar sowohl für lokale Bereitstellungen als auch in Managed-Cloud-Services (z. B. ROSA auf AWS und ARO auf Azure).	Einheitlicher Datenschutz: Eine Lösung zum Schutz von VMs und Containern mit konsistenter, richtliniengesteuerter Sicherung und Wiederherstellung. Resiliente Business Continuity: Backup, DR und Ransomware-Schutz auf Enterprise-Niveau sorgen dafür, dass kritische Anwendungen auch während Ausfällen oder Modernisierungsprojekten verfügbar bleiben. Compliance und Sicherheit: Unveränderlichkeit, Verschlüsselung, und rollenbasierte Zugriffskontrolle (RBAC) vereinfachen Audits und stärken die Cyberresilienz. Hybride und Multi-Cloud-Freiheit: Schützen und verschieben Sie Workloads nahtlos über lokale, Cloud- und Edge-Umgebungen hinweg — ohne Anbieterbindung.
SUSE Virtualization	Native Integration zum Schutz von containerisierten Workloads und VMs, die von SUSE Virtualization verwaltet werden, eng gekoppelt mit Kubernetes für einheitliche Kontrolle.	Modernisieren Sie in Ihrem eigenen Tempo: Führen Sie herkömmliche VMs und neue Container parallel aus und schützen sie auch parallel, während Sie Anwendungen schrittweise modernisieren. Operative Effizienz: Automatisierung, GitOps/CI/CD-Integration und zentralisierte Verwaltung reduzieren Overhead und befähigen Teams. Datenmobilität überall: Vereinfacht Migration von Workloads, Klonen und Failover über verschiedene Umgebungen hinweg, um Innovationen zu beschleunigen.

Moderne Virtualisierungs — Anwendungsszenarien

Migration von Workloads über Clouds hinweg

Da Unternehmen von VMware zu modernen Anwendungsplattformen wechseln, ist ein wichtiger Anwendungsfall das Refactoring oder die Umstellung von herkömmlichen VM-Workloads auf containerisierte, microservicebasierte Architekturen. Anstatt monolithische Anwendungen in VMs auszuführen, ermöglicht Kubernetes die Aufteilung dieser Anwendungen in verwaltbare, skalierbare Container. Dies modernisiert den technischen Stack, reduziert den Overhead und ermöglicht Features wie Auto-Scaling und Rolling Updates. Moderne Anwendungsplattformen können dazu beitragen, diese Lücke zu schließen, indem sie VMs und Container während der Übergangsphase parallel betreiben.

Erhöhte Agilität der Entwickler

Herkömmliche VMware-Umgebungen sind infrastrukturlastig und erfordern eine manuelle Bereitstellung und langsame Bereitstellungszyklen. Kubernetes kehrt dieses Modell um, indem es Self-Service- und API-gesteuerte Plattformen bereitstellt, die DevOps-Teams befähigen. Entwickler können mit Tools wie Helm, GitOps oder ArgoCD Services einrichten, CI/CD-Pipelines ausführen und die Infrastruktur als Code verwalten. Dies reduziert die Abhängigkeiten erheblich und beschleunigt die Release-Geschwindigkeit im Vergleich zu VM-basierten Umgebungen, in denen Änderungen oft langsamere, ticketbasierte Workflows durchlaufen.

Hybrid- und Multi-Cloud-Portabilität

Kubernetes wurde im Hinblick auf Portierbarkeit entwickelt und ist daher ideal für Unternehmen, die von der typischerweise lokalen, an einen Anbieter gebundenen VMware-Infrastruktur zu Hybrid- oder Multi-Cloud-Umgebungen wechseln möchten. Die Umstellung auf moderne Anwendungsplattformen ermöglicht die konsistente Ausführung von Workloads über AWS, Azure, Google Cloud oder lokale Rechenzentren hinweg. Im Gegensatz dazu erfordern VMware-Umgebungen häufig proprietäre Tools und Lizenzierungsmodelle, die diese Flexibilität einschränken. Die deklarativen Konfigurationen und Infrastructure-as-Code-Ansätze von Kubernetes ermöglichen es, Anwendungen unkompliziert neu bereitzustellen oder über verschiedene Umgebungen hinweg zu skalieren. Das ist bei einer herkömmlichen VM-Infrastruktur viel schwieriger.

Kosten- und Ressourcenoptimierung

VMs sind oft mit einem höheren Ressourcen-Overhead verbunden, und jede VM benötigt ihr eigenes OS, ihre eigenen Treiber und ihre eigene Speicherzuweisung. Dies führt zu einer unzureichenden Auslastung der Rechenleistung. Container, die von Kubernetes orchestriert werden, sind weitaus schlanker und können sich denselben OS-Kernel teilen, was sie ideal für Workloads mit hoher Dichte macht. Die Migration von VMware nach Kubernetes kann daher zu erheblichen Kostenersparnissen führen, sowohl im Hinblick auf Hardwareauslastung als auch Lizenzgebühren. Insbesondere da die Lizenzierungskosten für VMware nach der Übernahme durch Broadcom steigen, bietet Kubernetes eine Open Source-Alternative, die kostengünstiger skaliert.

Veeam Kasten — Leistungsstarke Funktionen, einfachere Verwaltung

Feature	So geht's	Mehrwert
Native Wiederherstellung auf Dateiebene	Sie können einzelne Dateien aus PersistentVolumeClaims an jedem Veeam Kasten-Wiederherstellungspunkt sofort auswählen und remote darauf zugreifen, ohne vollständige Volumes oder VMs wiederherstellen zu müssen. Der sichere Zugriff erfolgt über SFTP für den schnellen Abruf von Dateien von jedem Ort aus.	Minimieren Sie Ausfallzeiten und operativen Overhead: Ermöglichen Sie schnelle, gezielte Dateiwiederherstellungen, um Zeit und Ressourcen zu sparen. Unterstützen Sie Ihre Teams dabei, anspruchsvolle Wiederherstellungs-SLAs einzuhalten und das Vertrauen in die Datenresilienz zu stärken.
Automatisierte VM-Schutzrichtlinien	Wenden Sie ganz einfach benutzerdefinierte Sicherungs- und Wiederherstellungsrichtlinien auf einzelne oder Gruppen von KubeVirt-VMs an. Die integrierte Automatisierung erkennt alle abhängigen Ressourcen. Keine manuelle Konfiguration oder Kennzeichnung erforderlich.	Compliance vereinfachen und Risiken verringern: Stellen Sie sicher, dass jede VM den richtigen Schutz erhält, indem manuelle Fehler und Richtlinienlücken reduziert werden. Beschleunigen Sie die Einführung moderner Virtualisierungsplattformen, ohne die Komplexität zu erhöhen.
Optimierte VM-zentrierte Wiederherstellungen	Stellen Sie spezifische VMs wieder her, indem Sie nur die Ressourcen auswählen, die Sie benötigen, wobei Kasten automatisch alle Abhängigkeiten identifiziert. Eliminieren Sie die manuelle Auswahl und Unsicherheiten für eine schnelle, zuverlässige Wiederherstellung.	Beschleunigen Sie die Wiederherstellung, reduzieren Sie die Komplexität: Wiederherstellungen sind einfach und effizient, entlasten IT-Ressourcen und sorgen dafür, dass kritische VMs schnell wieder online sind. Steigern Sie die operative Agilität in dynamischen Umgebungen.
Optionale VM-MAC-Wiederherstellung	Stellen Sie eine kontinuierliche Systemkonnektivität sicher, indem Sie die ursprüngliche Adresse von KubeVirt-VM-Netzwerkadaptern bei der Wiederherstellung beibehalten Vermeiden Sie Netzwerkkonflikte, um die Konnektivität nach der Wiederherstellung sicherzustellen.	Resilienz des Systems verbessern: Stellen Sie die nahtlose Kontinuität und Netzwerkkonsistenz sicher. Minimieren Sie Ausfallzeit und vermeiden Sie den Verlust kritischer Daten.
VM-Dashboard	Vereinfachen Sie den VM-Datenschutz in Kubernetes, indem Sie eine klare, clusterweite Transparenz im Kube Virt-VM-Schutzstatus bieten. Das erhöht die Reaktionsfähigkeit der Admin-Teams beim KubeVirt-Status und ermöglicht die einfachere Analyse von Kubernetes-Konzepten ohne Vorwissen.	Gewinnen Sie tiefe visuelle Einblicke in Kubernetes-VMs: Verringern Sie die Reaktionszeiten für Betriebsteams. Verringern Sie die Komplexität der Verwaltung und Wartung von KubeVirt-Umgebungen.

Veeam Kasten for Kubernetes-Datensicherungs-Plattform

Veeam Kasten ist eine Kubernetes-native Datensicherungs-Plattform, die Operations-Teams in Unternehmen ein benutzerfreundliches, skalierbares und sicheres System für Backup und Wiederherstellung, DR und die Mobilität von Kubernetes-Anwendungen bietet. Mit Veeam Kasten erreichen Teams Kubernetes-native Resilienz bei Ransomware-Angriffen.

Veeam Kasten bietet einen anwendungszentrierten Ansatz und tiefe Integrationen mit relationalen und NoSQL-Datenbanken, Kubernetes-Distributionen und APIs sowie Cloud-Plattformen.

Dies ermöglicht es Teams, jede beliebige Infrastruktur zu wählen und gleichzeitig maximale operative Einfachheit zu erreichen. Richtliniengesteuert und flexibel erweiterbar umfasst Veeam Kasten auch Features wie vollständige Konsistenz, Datenbankintegrationen, automatische Anwendungserkennung, Multi-Cloud-Mobilität sowie eine leistungsstarke webbasierte Benutzeroberfläche.

Anwendungsszenarien für Kubernetes-Datenschutz: Übersicht

Veeam verfügt über ein umfassendes Verständnis von Kubernetes und dessen einzigartigen Herausforderungen bei Backup, Wiederherstellung, DR, Anwendungs-Mobilität, Ransomware-Schutz und moderner Virtualisierung. Veeam Kasten ermöglicht Unternehmen die erfolgreiche und sichere Ausführung von Anwendungen auf Kubernetes.

Mit Veeam Kasten einheitliche Datenresilienz erreichen



Backup und Wiederherstellung

Schützen Sie Ihre Kubernetes-Anwendungen, VMs und deren geschäftskritische Daten zuverlässig und effizient.



Disaster Recovery

Verwalten Sie ganz einfach die externe Replikation von Backups, um geschäftliche Anforderungen und gesetzliche Vorschriften zu erfüllen.



Anwendungsmobilität

Schützen und verschieben Sie Daten ohne Anbieterbindung effektiv dorthin, wo sie benötigt werden.



Schutz vor Ransomware

Sichern Sie Ihre Daten mit proaktiver Bedrohungserkennung, Verschlüsselung und Unveränderlichkeit gegen Risiken ab.



Moderne Virtualisierung

Schützen Sie VMs und Container gemeinsam nahtlos auf Kubernetes.



Weitere Informationen finden Sie unter veeam.com, oder folgen Sie [@Veeam](https://twitter.com/Veeam) auf X.