Ihr Weg zu Resilienz mit Veeam Kasten

Eine Roadmap für Ihre ersten 100 Tage und darüber hinaus

Dieser Leitfaden unterstützt IT-Administratoren bei der Bereitstellung, Konfiguration und Operationalisierung von Veeam Kasten *for Kubernetes*. Unabhängig davon, ob die Installation über Helm oder den Marketplace erfolgt, ist der Bereitstellungsprozess darauf ausgelegt, schnell, sicher und leicht zugänglich zu sein. Bis zum Tag 100 verfügen Sie über eine Kubernetes-native Backup-Umgebung mit externen, unveränderlichen Exporten, die in Ihre Toolsets und Anwendungen integriert sind, sowie über ein dokumentiertes Wiederherstellungs-Runbook.

100-Tage-Reise

PHASE 1 **Grundlage** **Tage 1-14**	**PHASE 2** **Grundlagen absichern** **Tage 15-45**	**PHASE 3** **Optimierung & Härtung** **Tage 46-75**	**PHASE 4** **Mehrwert nachweisen** **Tage 76-100**
M1: Dimensionierung und Planung	M4: Zentrales Management	M7: Observability-Integration	M10: Wiederherstellungstests
M2: Veeam Kasten bereitstellen	M5: Anwendungsbewusste Verarbeitung	M8: Verbesserte Resilienz	M11: Dokumentation und Reporting
M3: Erste Backup-Jobs	M6: Best Practices für Richtlinien	M9: Abdeckungslücken schließen	M12: laufende Hygiene

Roadmap Auf einen Blick

Phase	Name	Zeitrahmen	Fokus
PHASE 1	Grundlage	Tage 1-14	Umgebung planen, Veeam Kasten bereitstellen und erste Backup-Jobs ausführen
PHASE 2	Die Grundlagen Absichern	Tage 15-45	Zentralisierte Verwaltung, anwendungsbewusste Verarbeitung und Best Practices für Richtlinien.
PHASE 3	Optimieren und absichern	Tage 46-75	Beobachtbarkeit, Resilienz und DR sowie das Schließen von Abdeckungslücken.
PHASE 4	Mehrwert nachweisen	Tage 76-100	Wiederherstellungstests, Dokumentation und fortlaufende Backup-Hygiene.

Verwenden dieser Anleitung

Tage dienen als Orientierung, sind aber keine verbindlichen Fristen. Kleine Umgebungen können Phase 1 auf eine Woche komprimieren, während komplexe Umgebungen Phase 3 verlängern können.

Jeder Meilenstein baut auf dem vorherigen auf, daher wird empfohlen, die Schritte der Reihenfolge nach zu befolgen.

Infokästen im gesamten Text heben Entscheidungspunkte, Architekturoptionen und häufige Fallstricke hervor, die es zu berücksichtigen gilt.

Inhalte

PHASE 1 • Tage 1-14

Grundlage

Ziel: Dimensionierung der Infrastruktur, Bereitstellung und Schutz der ersten Workloads.

Meilenstein 1: Dimensionierung und Planung

Bevor Sie irgendetwas bereitstellen, nehmen Sie sich Zeit für die Planung. Die meisten Schwierigkeiten bei der Bereitstellung einer stabilen und gut geschützten Umgebung lassen sich vermeiden, wenn diesem Schritt die gebührende Aufmerksamkeit gewidmet wird.

Workload-Inventar

- Dokumentieren Sie die Gesamt-Workload und die Anzahl der virtuellen Maschinen (VMs), die Kapazitäten (z. B. Volumegröße/Dateianzahl) sowie die geschätzte tägliche Änderungsrate.
- Identifizieren Sie Ihre kritischsten Workloads. Diese bestimmen Ihre Zielvorgaben für Recovery Point Objective (RPO) und Recovery Time Objective (RTO).
- Notieren Sie alle Datenbanken und Workloads, die von einer anwendungsspezifischen Verarbeitung profitieren könnten.

Dimensionierung und Bereitstellungsplanung für Veeam Kasten

- Veeam Kasten hat nur minimale Systemanforderungen und die Standardwerte sind in der Regel ausreichend.
- Wählen Sie Ihre Bereitstellungsmethode aus: entweder Marketplace/Operator (empfohlen, sofern möglich) oder Helm. Bei Bedarf ist es möglich, die Methode nach der Installation zu wechseln.
- Prüfen Sie, ob Ihre Kubernetes-Version mit der neuesten Version von Veeam Kasten kompatibel ist. Ist dies nicht der Fall, müssen Sie entweder zunächst ein Upgrade durchführen oder eine ältere Version verwenden.
- Bestimmen Sie, ob diese Umgebung durch ein Air-Gap getrennt ist. Falls ja, müssen die Veeam Kasten Images möglicherweise in ein lokales, offline verfügbares Registry über den Marktplatz Ihres Anbieters gepusht werden oder unser Registry freigeschaltet werden.
- Die Planung Ihres Backup-Netzwerks durch die Isolierung des Backup-Traffic auf ein dediziertes VLAN ist eine Sicherheits-Best Practice und mit Kubernetes je nach Ihrem CNI möglich.

Helm VS Marketplace

Helm: Dies ist die flexibelste Lösung und mit allen Kubernetes-Distributionen kompatibel.

Marktplatz/Operator: Der Bereitstellungs- und Upgrade-Zyklus ist einfacher und unterstützt dieselben Parameter für die Anpassung wie Helm. Es wird zudem häufig in Verbindung mit Red Hat OpenShift eingesetzt.

Der Kompromiss: Es kann zu Verzögerungen beim Erhalt neuen Versionen über den Marktplatz kommen. Updates sind auf Helm sofort verfügbar, doch Anbieter im Marketplace verzögern neue Versionen häufig um einen oder mehrere Tage, um Validierungstests durchzuführen.

Workload-Speicherarchitektur

- **Speicher mit Snapshot-Fähigkeit:** Veeam Kasten ist mit virtuell jedem CSI-Speichertreiber kompatibel, der Snapshots unterstützt, sowie mit direkten Speicherintegrationen.
- **Andere Speicher (z. B. generisches NFS, lokale Festplatte usw.):** Veeam Kasten kann diese Workloads zwar weiterhin schützen, doch das Fehlen einer echten Snapshot-Fähigkeit beeinträchtigt die Zuverlässigkeit und Leistung der Backups. Wir empfehlen Ihnen nachdrücklich ein Upgrade auf Volumes mit Snapshot-Funktionalitäten; aber GSB oder NFS tar könnten verwendet werden, sofern Sie deren inhärente Einschränkungen akzeptieren.

Backup-Speicherarchitektur: Überblick über die Optionen

Ihre Wahl des Speicher bestimmt die Resilienz und Verfügbarkeit Ihrer Backup-Daten. Hier finden Sie einen allgemeinen Überblick über die Vor- und Nachteile der einzelnen Arten von Backup-Speicher, die Sie als Standortprofil konfigurieren können.

Veeam Kasten + Veeam Vault

Snapshots werden über Veeam Vault in externen und logisch durch ein Air-Gap getrennten, unveränderlichen Objektspeicher exportiert. Es sind keine fortgeschrittenen Konfigurations- oder Wartungsmaßnahmen erforderlich.

Veeam Kasten + Veeam Backup & Replication Repository

Snapshots werden in die von Veeam Backup & Replication verwaltete Infrastruktur exportiert, einschließlich Veeam Hardened Repositorys und Scale-out Backup Repositorys (SOBRs). Der Blockmodus ist erforderlich. **Hinweis:** Bei Versionen vor 9.x ist zudem ein kleines zusätzliches Standortprofil (Vault/Object/NFS/CIFS) für Metadaten erforderlich.

Veeam Kasten + Objektspeicher

Snapshots werden in einen Objektspeicher (z. B. S3, Cloud) exportiert, der so konfiguriert sein sollte, dass er sich an einem externen Standort befindet und unveränderlich ist.

Veeam Kasten + NFS/CIFS

Snapshots, die direkt nach NFS/CIFS exportiert werden, sind in der Regel nicht unveränderlich, selbst auf WORM-fähigen Geräten, da hierfür eine Versionsverwaltung erforderlich wäre. Diese Option wird vollständig unterstützt, jedoch nur empfohlen, wenn Sie zusätzlich über unveränderliche Duplikate oder Kopien an einem externen Standort verfügen.

Veeam Kasten + mehrere Standortprofile

Snapshots werden an mindestens zwei Speicherorte exportiert. Bei korrekter Umsetzung unter Verwendung mindestens einer unveränderlichen Option kann dies der widerstandsfähigste Ansatz sein. **Hinweis:** Versionen vor 9.x erfordern mehrere Richtlinien, wobei pro Richtlinie ein Standortprofil verwendet wird.

Speichermodi bestimmen die Funktionalitäten.

Je nach Art Ihres Speichers stehen Ihnen möglicherweise die folgenden Optionen zur Verfügung:

Volume-Modus: Datei oder Block. Beide sind mit Veeam Kasten kompatibel (z. B. Ceph FS oder RBD).

Exportmodus: Datei oder Block. Beides ist mit Veeam Kasten möglich.

Befindet sich ein Volume im Blockmodus, können Sie Ihre Snapshots möglicherweise ebenfalls im Blockmodus exportieren. Dies bietet spezielle Features, wie CBT (sofern verfügbar) und Export in ein Veeam Backup & Replication-Repository.

Einsatz von Veeam Backup & Replication + Veeam Infrastruktur Appliance (VIA) als abgesichertes Repository

Für diejenigen ohne vorhandenen unveränderlichen Speicher kann die Integration von Veeam Kasten mit Veeam Backup & Replication und die Bereitstellung von VIA ein sinnvoller Weg sein, um lokale Unveränderlichkeit zu erreichen.

Ein abgesichertes Repository bietet unveränderliche lokale Backups, was bedeutet, dass Ransomware sie während der Aufbewahrung weder verschlüsseln noch löschen kann. Das OS ist gegen unbefugten Zugriff gehärtet und sollte idealerweise auf einem geschützten physischen Server statt auf einer VM ausgeführt werden.

Traditionell erfordert ein abgesichertes Repository die manuelle Installation und Härtung einer Linux-Distribution. VIA beseitigt diese Hürde vollständig, da es pre-hardened ist und über eine bootfähige ISO-Datei bereitgestellt wird. Es kann auch eigenständig auf kompatibler Hardware installiert oder als zertifizierte Appliance bei einem Anbieter erworben werden.

Meilenstein 2: Veeam Kasten bereitstellen

Veeam Kasten bereitstellen

- Verwenden Sie Pre-Flight-Tool, um zu überprüfen, ob die Voraussetzungen erfüllt sind (optional).
- Marketplace/Operator-Methode: Eine detaillierte Anleitung finden Sie hier.
- Helm-Methode: Eine detaillierte Anleitung finden Sie hier.

Dashboard-Zugriff und Authentifizierungsintegration

- Um extern auf das Dashboard zugreifen zu können, fügen Sie einen Ingress oder eine Route zu Veeam Kasten hinzu.
- Es empfiehlt sich die Integration über den Authentifizierungsanbieter IhrerDistribution (z. B. OpenShift Auth), andere Optionen wie eine direkte LDAP-Integration sind jedoch ebenfalls möglich.
- Sobald das Veeam Kasten-Dashboard sichtbar ist, können Sie mit den folgenden Schritten fortfahren.

Infrastruktur mit Veeam Kasten verbinden

- Falls zutreffend (vSphere/Cloud/Sonstiges) fügen Sie ein Infrastrukturprofil für die direkte Speicherintegration hinzu.
- Fügen Sie ein Standortprofil hinzu, um Ihr Backup-Ziel festzulegen.

Meilenstein 3: Erste Backup-Jobs

Backups in Kubernetes-Umgebungen

Storage-Snapshots sind ein leistungsstarkes Feature, das Kubernetes nativ versteht und verwalten kann, sofern sie von Ihrem Storage-Provider unterstützt werden.

Veeam Kasten nutzt diese Funktionalität oder eine direkte Integration, um Snapshots auszulösen, die lokal auf dem Speichergerät gespeichert werden. Veeam Kasten kann diese Snapshots anschließend nutzen, um Daten zuverlässig in ein externes Standortprofil (z. B. NFS, S3, VBR-Repo, Vault usw.) zu exportieren.

Diese Methode ermöglicht ein Höchstmaß an Geschwindigkeit und Konsistenz, während weiterhin Kubernetes-native Features und APIs verwendet werden, um eine maximale Kompatibilität zu gewährleisten.

Was Sie für den Einstieg benötigen

Veeam Kasten, als Kubernetes-native Anwendung, benötigt, dass der Benutzer, der die Installation durchführt, kubectl-Zugriff auf die Zielumgebung, Cluster-Administratorrechte und idealerweise auch Zugriff auf die Verwaltungsoberfläche Ihrer Distribution, sofern vorhanden, hat.

Tipp: Sollten Fehler auftreten, finden Sie Lösungen in unserer Community und auf den KB-Seiten.

- Erfahren Sie mehr über den Schutz von KubeVirt-VMs, sofern dies für Ihre Umgebung zutrifft.
- Erstellen Sie Ihre erste Backup-Richtlinie und weisen Sie Ihr Standortprofil zu.
- Legen Sie zu Beginn eine sinnvolle Aufbewahrungsrichtlinie fest: 1 lokaler Snapshot täglich, mit Exporten zum Standortprofil und jeweils 1 täglicher, 4 wöchentlicher und 3 monatlicher Aufbewahrung.
- Planen Sie den Auftrag so, dass er außerhalb der Stoßzeiten ausgeführt wird, und stellen Sie sicher, dass er sich nicht mit anderen Wartungsfenstern überschneidet.
- Führen Sie den Job bei der ersten Ausführung manuell aus und überwachen Sie ihn bis zum Abschluss.
- Vergewissern Sie sich, dass der Job ohne Warnungen oder Fehler abgeschlossen wurde, bevor Sie mit Phase 2 fortfahren.

Ihr erster Wiederherstellungstest: Überspringen Sie diesen Schritt nicht

Bevor Sie zu Phase 2 übergehen, führen Sie eine Wiederherstellung einer nicht kritischen Anwendung durch, um die Wiederherstellbarkeit zu bestätigen.

Sie sind erst dann geschützt, wenn Sie sichergestellt haben, dass Sie wiederherstellen können. Dies dauert nur wenige Minuten und kann tagelange Probleme verhindern.

Lokal VS Export

Denken Sie daran, dass Snapshots nur lokal auf Ihrem Speichergerät gespeichert werden. Das bedeutet:

- Sie sind kein echtes Backup.
- Mehr lokal gespeicherte Snapshots bedeuten mehr verbrauchten Primärspeicher.

Daher ist es wichtig, die Snapshots in ein Standortprofil zu exportieren, bei dem die Aufbewahrungsrichtlinie separat konfigurierbar ist.

Beim Export von Snapshots werden alle Daten automatisch dedupliziert, komprimiert, verschlüsselt und inkrementell gespeichert.

PHASE 2 • Tage 15-45

Die Grundlagen härten

Ziel: Konsistenter Schutz, externe Kopie und Transparenz in Ihrer Umgebung.

Meilenstein 4: Zentrale Verwaltung (MCM)

Multi-Cluster Manager (MCM) ermöglicht zentrale Transparenz und Verwaltung mehrerer Cluster. Auf jedem Cluster wird Veeam Kasten installiert, um die Workloads zu schützen, und die Instanzen können miteinander verbunden werden.

- Sobald ein weiteres Cluster mit Veeam Kasten bereitgestellt wurde, legen Sie eine Kasten-Instanz als Primärinstanz fest und verknüpfen Sie sie mithilfe eines Join-Tokens (Anleitung). Stellen Sie sicher, dass selbstsignierte Zertifikate als vertrauenswürdig markiert sind, um Fehler zu vermeiden.
- Zeigen Sie alle verbundenen Cluster im MCM-Dashboard an.
- Definieren Sie globale Richtlinien und globale Profile, wenn Sie eine konsistente Konfiguration in Ihrer gesamten Umgebung wünschen.
- Fügen Sie Ihren Unternehmenslizenzschlüssel zum primären MCM-Cluster hinzu. Lizenzen werden automatisch an alle anderen Cluster verteilt, ohne dass weitere Konfiguration erforderlich ist.

Meilenstein 5: Anwendungsorientierte Verarbeitung

Durch die anwendungsspezifische Verarbeitung mit Kanister Blueprints wird sichergestellt, dass ausfallsichere Backups anwendungskonsistent oder logisch exportiert werden. Dies ist von entscheidender Bedeutung für Datenbanken wie PostgreSQL, MongoDB, MySQL, Elastic und andere.

- Besprechen Sie Anwendungsanforderungen und Zugriff mit Ihrem Anwendungsteam.
- Suchen Sie nach vorgefertigten Blueprint-Beispielen, die Sie individuell anpassen können, oder erstellen Sie eigene Blueprints.
- Fügen Sie Veeam Kasten den Blueprint hinzu.
- Ordnen Sie den Blueprint den Workloads manuell zu oder erstellen Sie eine Blueprint-Bindung.
- Führen Sie einen Backup- und Restore-Test mit Ihrem Blueprint durch, um die End-to-End-Wiederherstellung der Anwendung zu verifizieren.

Arten von Backups

Ausfallsicher (Standard): Diese Art von Backup erfasst das vollständige Dateisystem zu einem bestimmten Zeitpunkt, in der Regel über Storage-Provider-Snapshots. Dies bietet eine höhere Datenkonsistenz als einfaches Kopieren von Dateien, aber Schreibvorgänge während der Übertragung oder noch nicht gespeicherte Transaktionen könnten dennoch fehlen.

Anwendungskonsistent: Bei dieser Art von Backup wird die Anwendung typischerweise kurzzeitig angehalten, indem die nativen Tools der Anwendung verwendet werden, um sicherzustellen, dass alle Daten auf das Volume geschrieben wurden, bevor der Snapshot erstellt wird.

Logisch: Diese Art von Backup verwendet die nativen Tools der Anwendung, um einen logischen Dump oder Export ihrer Daten als Datei zu erstellen. Dies wird häufig an einen externen Speicherort wie S3 statt auf das Volume selbst gespeichert.

Blueprints sind leistungsstark und unendlich flexibel. Außerdem können Sie dank der Open-Source-Eigenschaft für jede beliebige Anwendung oder jeden beliebigen Arbeitsablauf einen Blueprint erstellen, falls noch keiner existiert.

Meilenstein 6: Best Practices für Richtlinien

In diesem Meilenstein erstellen Sie zusätzliche Jobs, um alle Ihre Workloads zu schützen und Advanced Einstellungen zu verwenden, um deren Zuverlässigkeit zu gewährleisten.

Best Practices (für die meisten Szenarien)

- Verwenden Sie mehrere Jobs mit Labels, um Anwendungen auszuwählen, anstatt einer Wildcard-Richtlinie, die alles schützt.
- Verwenden Sie VM-basierte Richtlinien anstelle von Namespace-basierten, wenn Sie KubeVirt-VMs schützen.
- Wenn Sie clusterweite Ressourcen sichern möchten, erstellen Sie eine separate Richtlinie für nur diese Backups.
- Definieren Sie ein Backup-Fenster, um sicherzustellen, dass Produktions-Workloads während kritischer Zeiten nicht beeinträchtigt werden.
- Erwägen Sie, Jobs mit gestaffelten Zeitplänen zu planen, um die Leistung zu verbessern.
- Konfigurieren Sie den unveränderlichen Backupschutz.
- Ausschlüsse / Ressourcenfilter (falls erforderlich)
- (Optional) Globale Ressourcen, Richtlinienvoreinstellungen

Weitere Tipps

Bei manuell ausgeführten Aufträgen müssen alle Artefakte manuell entfernt werden, sofern keine Ablaufzeit festgelegt wurde.

Auch wenn der Job mit Ortszeit konfiguriert wurde, werden alle Zeitangaben in UTC umgewandelt und die Zeitpläne der Richtlinien ändern sich nicht für die Sommerzeit.

Überprüfen Sie Ihre Berechnungen! Die Berechnung der Aufbewahrung ist nicht immer offensichtlich. Beispielsweise würden 24 (insgesamt) gespeicherte stündliche Snapshots, die im Abstand von 15 Minuten erstellt werden, nur Snapshots aus einem Zeitraum von 6 Stunden abdecken — nicht 24 Stunden.

PHASE 3 • Tage 46-75

Optimieren und härten

Ziel: Schutzlücken schließen, RTO/RPO verbessern und Transparenz erhöhen.

Meilenstein 7: Observability-Integration

- Aktivieren Sie bei Bedarf die Red Hat ACM Observability-Integration.
- Exportieren Sie Metriken in externe Monitoring-Systeme (z. B. Grafana, Datadog, Thanos, usw.).
- Erstellen Sie Warnmeldungen und Dashboards in Ihren Monitoring-Systemen (Grafana-Beispiel).
- Aktivieren Sie Reporting.

Meilenstein 8: Verbesserte Resilienz und DR

Zu einem Backup aller Workloads sollte auch ein Backup von Veeam Kasten selbst gehören, was mithilfe von Kasten Disaster Recovery (KDR) erreicht werden kann. Dies sollte nicht mit einer DR-Umgebung oder einem DR-Plan verwechselt werden, die je nach erforderlicher Resilienz berücksichtigt werden sollten.

KDR (Backup Ihres Veeam Kasten-Katalogs)

- Aktivieren Kasten DR: Dadurch wird der Veeam Kasten-Backup-Katalog gespeichert, sodass Wiederherstellungen möglich sind, selbst wenn die Kasten-Installation nicht mehr zugänglich ist. Dies ist wichtig, da Veeam Kasten Backup-Dateien nicht eigenständig sind und für die Wiederherstellung den Katalog sowie den Verschlüsselungsschlüssel benötigen.
- Stellen Sie den Kasten DR auf „Lokale Katalog-Snapshots exportieren“ ein und bewahren Sie die folgenden Informationen an einem sicheren Ort auf: Passphrase, Cluster-ID, Details zum KDR-Standortprofil und Anmeldedaten.

DR für Ihre Workloads

- Bestimmen Sie das Maß an Resilienz, das Sie basierend auf Ihren angestrebten RTO/RPO benötigen.
- Sofern eine RTO/RPO von 1+ Tagen akzeptabel ist, könnten Backups und das Neuaufsetzen der Umgebung bei Bedarf eine sinnvolle Lösung sein.
- Wenn RTO/RPOs in Stunden oder Minuten gemessen werden müssen, ist eine sorgfältige Planung unerlässlich. Im Folgenden finden Sie einige Beispiele.

Beispielkonfigurationen für DR (abhängig von den erforderlichen RTO/RPO-Werten)

- **Ungeschützte Anwendung:** Keine Wiederherstellungspunkte (d.h. keine lokalen Snapshots oder Exporte).

  Ergebnis: Eine Wiederherstellung ist nicht möglich.

- **Nur Export:** Exporte von KDR und exportierte Wiederherstellungspunkte befinden sich in einem externen Standortprofil.

  Ergebnis: Zur Wiederherstellung müssen Sie zunächst eine Kubernetes-Umgebung neu einrichten, Veeam Kasten installieren, den Kasten-Katalog wiederherstellen und anschließend die Anwendungen aus den exportierten Wiederherstellungspunkten wiederherstellen.

- **DR-Umgebung + Import:** Veeam Kasten ist installiert, und es wird regelmäßig eine Import-Richtlinie ausgeführt, um die Wiederherstellungspunkte in einen lokalen Katalog zu importieren.

  Ergebnis: Wiederherstellungspunkte sind an einem sekundären Standort verfügbar und stehen zur Wiederherstellung bereit. Es werden nur minimale Ressourcen verbraucht, bis diese benötigt werden.

- **DR-Umgebung + Import + Wiederherstellung, auf Null skaliert:** Veeam Kasten ist installiert, die Import- und Wiederherstellungsrichtlinie wird regelmäßig ausgeführt, um die Wiederherstellungspunkte in den lokalen Katalog zu importieren und anschließend Anwendungen in die Kubernetes-Umgebung wiederherzustellen. Anschließend werden die Anwendungen wiederhergestellt, aber mit Transforms, die die Replikate aller Workloads auf 0 setzen.

  Ergebnis: Die Anwendungen werden in Kubernetes wiederhergestellt (über Pods, PVs und alle ausgewählten Komponenten). Die Anzahl der Replikate beträgt jedoch 0, sodass — abgesehen vom Speicher — nur minimale Ressourcen verbraucht werden, bis sie benötigt werden.

- **DR-Umgebung + Import + Wiederherstellung, vollständig:** Veeam Kasten ist installiert; die Import- und Wiederherstellungsrichtlinie wird regelmäßig ausgeführt, um die Wiederherstellungspunkte in einen lokalen Katalog zu importieren und anschließend Anwendungen in die Kubernetes-Umgebung wiederherzustellen.

  Ergebnis: Die Anwendungen werden in Kubernetes wiederhergestellt (über Pods, PVs und alle ausgewählten Komponenten), laufen dort genau so, wie sie in der Production liefen, und sind bereit für den vollen Einsatz.

Notfallplanung

Veeam Kasten ist distributionsunabhängig, das heißt, Anwendungen können in jede beliebige Kubernetes-Distribution wiederhergestellt und aus jeder wiederhergestellt werden — sogar zwischen völlig unterschiedlichen Distributionen wie Tanzu zu Azure. Für die Wiederherstellung muss jedoch eine funktionierende Kubernetes-Umgebung vorhanden sein; Kasten kann sich nicht selbst bereitstellen. Erstellen Sie einen geeigneten Notfallplan, damit Sie im Falle eines Vorfalls vorbereitet sind. Testen Sie regelmäßig, ob Ihr Plan Ihre Ziele erfüllt.

Meilenstein 9: Feinabstimmung

- **Überprüfen Sie das Veeam-Kasten-Dashboard:** Behandeln Sie alle ungeschützten Workloads vor allen anderen Optimierungen.
- **Überprüfen Sie die Zeitpläne der Jobs auf Konflikte:** Staffeln Sie die Startzeiten, um Ressourcenkonflikte zu vermeiden.
- Bestätigen Sie, dass alle Backup-Jobs innerhalb Ihres definierten Backup-Fensters abgeschlossen werden.
- **Überprüfen Sie die Compliance des RPO:** Erzeugen alle kritischen Workloads Wiederherstellungspunkte innerhalb Ihres Ziel-Wiederherstellungsfensters?
- Stellen Sie sicher, dass alle Workloads zu mindestens einem unveränderlichen Speicherort exportiert werden.
- Das Aktivieren der Garbage Collection zur Entfernung alter Aktionen kann die Leistung des Katalogs verbessern.
- Testen Sie Ihren Upgrade-Prozess! Neue Veeam Kasten-Versionen werden ungefähr alle zwei Wochen veröffentlicht.

PHASE 4 • Tage 76-100

Wertnachweis und Operationalisierung

Ziel: Wiederherstellbarkeit verifizieren, laufende Systemhygiene etablieren und ROI belegen.

Meilenstein 10: Wiederherstellungstests

Das einzige Backup, das zählt, ist eines, von dem Sie wiederherstellen können. In Phase 4 weisen Sie mit dokumentierten Beweisen nach, dass Ihre Umgebung die RTO- und RPO-Anforderungen erfüllt.

Granulare und vollständige Wiederherstellungstests

- Testen Sie die vollständige Wiederherstellung eines Namespaces oder eine vollständige VM-Wiederherstellung aus einem Export. Simulieren Sie einen vollständigen Ausfall Ihrer lokalen Umgebung, um Ihre externe Kopie zu validieren.
- Testen Sie die Wiederherstellung von Anwendungsobjekten: Stellen Sie eine Datenbank wieder her und führen Sie Datenbankabfragen durch, um zu überprüfen, ob Ihre Daten intakt sind.
- Testen Sie die Wiederherstellung auf Dateiebene (falls gewünscht): Stellen Sie einzelne Dateien aus einem Export an einem Testziel wieder her.
- Testen Sie Ihren gesamten DR-Plan von Anfang bis Ende, notieren Sie sich alle Punkte, die verbessert werden müssen, und dokumentieren Sie den Prozess ausführlich, sodass sichergestellt ist, dass Ihr Plan und der Zugriff darauf verfügbar sind.
- Erfassen Sie die tatsächlichen Wiederherstellungszeiten und vergleichen Sie diese mit Ihren RTO-Zielen. Dokumentieren Sie die Ergebnisse.

Best Practices für Wiederherstellungstests

Stellen Sie immer auf ein Nicht-Production-Ziel wieder her und überschreiben Sie während eines Tests niemals produktive Workloads.

Dokumentieren Sie, was wiederhergestellt wurde, aus welchem Wiederherstellungspunkt, auf welches Ziel und wie lange es gedauert hat.

Diese Resultate sind Ihr Nachweis der Wiederherstellbarkeit. Bewahren Sie sie für Compliance-Überprüfungen, Audits und Management-Reporting auf.

Beachten Sie außerdem, dass bestimmte Ressourcen (insbesondere NetzwerkServices) innerhalb derselben Umgebung, auch wenn Sie in unterschiedliche Namespaces wiederherstellen, zu Konflikten führen können. Bitte überprüfen Sie Ihre Konfiguration vor der Wiederherstellung, stellen Sie die Daten in einer anderen Umgebung wieder her und/oder verwenden Sie Transforms, um Konflikte zu vermeiden.

Wiederherstellung in unterschiedlichen Umgebungen

Wenn Sie zwischen verschiedenen Standorten, Kubernetes-Distributionen, Plattformen oder in anderen Fällen wiederherstellen, Transforms können verwendet werden, um Ihre Konfiguration bei der Wiederherstellung nahtlos zu modifizieren. Beispielsweise, wenn Sie Netzwerkpfade von Production zu DR umstellen oder Speicherklassen ändern. Es sind keine manuellen Änderungen erforderlich, damit Ihre Wiederherstellungen sofort mit einer angepassten Konfiguration oder in einer neuen Umgebung ausgeführt werden können.

Meilenstein 11: Dokumentation und Reporting

- Aktivieren Sie Reporting, falls noch nicht geschehen.
- Dokumentieren Sie Ihre endgültige Backup-Architektur, einschließlich der Richtlinienliste, der Exportziele, der Zeitpläne und der Aufbewahrungsrichtlinien.
- Überprüfen Sie den Speicherverbrauch von Veeam Vault und bestätigen Sie, dass Ihre Nutzung im Einklang mit Ihrem geplanten Budget steht.
- Archivieren Sie die Ergebnisse der Wiederherstellungstests zusammen mit der Architekturdokumentation.

Meilenstein 12: Eine regelmäßige Systemhygiene etablieren

Bis Tag 100 sollte Ihre Umgebung stabil und vollständig dokumentiert sein. Diese Gewohnheiten sorgen dafür, dass es so bleibt:

- **Wöchentlich:** Überprüfen Sie das Veeam Kasten Dashboard und untersuchen Sie alle fehlgeschlagenen oder gewarnten Jobs, bevor sich diese häufen.
- **Monatlich:** Prüfen Sie die aktuellen Kasten-Releases und aktualisieren Sie regelmäßig.
- **Vierteljährlich:** Führen Sie einen dokumentierten Wiederherstellungstest durch und wechseln Sie dabei jedes Quartal zwischen verschiedenen Workload-Typen.
- **Jährlich:** Überprüfen Sie Ihre Backup-Architektur im Hinblick auf die aktuellen Business-Anforderungen.
- **Vor der Verlängerung:** Überprüfen Sie die Lizenzierungsnutzung in Ihrem Kasten-Dashboard (z. B. insgesamt über MCM oder in jedem Cluster einzeln), um zu bestätigen, dass Sie sich innerhalb Ihres Lizenzumfangs befinden.

Nächste Schritte

Sie wünschen weitere Infos?

- Besuchen Sie Veeam University
- Entdecken Sie Success Storys Ihrer Kollegen
- Kontakt mit Customer Success aufnehmen
- Teilen Sie Ihre Geschichte zur Datenresilienz mit Veeam

Anhang: Kurzreferenz

Kernkomponenten: Veeam-Integration

- **Veeam Software Appliance (VSA):** Vorgehärtete Appliance mit vorinstalliertem Veeam Backup & Replication. Als OVA (VM) oder ISO (physisch) bereitstellen. Kann selbst als begrenztes, unveränderbares Repository fungieren oder mit anderen Appliances oder Backup-Speicher, einschließlich dedizierter VIAs, zusammenarbeiten.
- **Veeam Infrastructure Appliance (VIA):** Pre-hardened Appliance, die als dediziertes abgesichertes Repository oder in einer anderen Rolle bereitgestellt wird. Bietet lokale Unveränderlichkeit, ohne dass Linux-Kenntnisse erforderlich sind. Eine Rolle pro Appliance.
- **Veeam Backup & Replication:** Kern-Backup-Engine, die auf dem VSA gehostet wird. Verwaltet Aufträge, Repositorys, Proxys und Wiederherstellungsvorgänge.
- **Scale-out Backup Repository:** Ein logisches Konstrukt, das eine lokale Performance Tier (z. B. VIA) und eine Capacity Tier (z. B. Vault/S3/NFS) in einem einzigen Backup-Ziel vereint.
- **Veeam Vault:** Unveränderbarer Cloud-Objektspeicher für externe Kopien. Es wird von Veeam verwaltet und erfordert kein separates Cloud-Konto.

Schlüsselbegriffe

- **RPO RPO:** Maximal akzeptabler Datenverlust, zeitlich bemessen. Steuert die Häufigkeit des Backup-Zeitplans.
- **RTO:** Maximale akzeptable Ausfallzeit, bevor ein Workload wiederhergestellt werden muss.
- **Unveränderbarkeit:** Backup-Daten, die für eine bestimmte Aufbewahrung weder verändert noch gelöscht werden können. Schützt vor der Verschlüsselung von Backup-Dateien durch Ransomware.
- **Abgesichertes Veeam-Repository:** Ein Linux-basiertes Backup-Repository mit Unveränderbarkeit, die auf OS-Ebene durchgesetzt wird. Wird von VIA einsatzbereit bereitgestellt, ohne dass eine Linux-Administration erforderlich ist.
- **KubeVirt:** Ein Open-Source-Projekt, das es Kubernetes ermöglicht, virtuelle Maschinen (VMs) neben containerisierten Workloads auszuführen und zu verwalten. So können Sie VMs auf Kubernetes-Plattformen wie OpenShift Virtualization und SUSE Harvester ausführen, die durch Veeam Kasten geschützt werden können.
- **Anwendungsspezifische Verarbeitung:** Verarbeitung, die anwendungskonsistente Backups erstellt, was Veeam Kasten durch die Nutzung von Blueprints umsetzen kann.
- **Blueprint:** Kanister-Blueprints sind ein Open-Source-Mechanismus zur Beschreibung benutzerdefinierter Aufgaben für das Datenmanagement auf Anwendungsebene in Kubernetes.

Zusätzliche Ressourcen

- Veeam Help Center
- Veeam-Kundenportal (Herunterladen)
- Veeam Community-Foren
- Veeam KB-Artikel
- Veeam Kasten-Dokumentation
- Kanister Blueprints-Dokumentation

Über Veeam Software

Veeam ist das führende Unternehmen für Daten- und KI-Vertrauen mit dem Anspruch, Organisationen dabei zu unterstützen, ihre Daten und KI vollständig zu verstehen, zu schützen und resilient zu halten, um die sichere Nutzung von KI in großem Umfang zu beschleunigen. Als Marktführer in den Bereichen Datenresilienz und Management der Datensicherheitslage (Data Security Posture Management = DSPM) ist Veeam auf die Konvergenz von Identität, Daten, Sicherheit und KI-Risiko ausgerichtet.

Veeam hat seinen Hauptsitz in Seattle und ist mit Niederlassungen in mehr als 30 Ländern vertreten. Weltweit schützt Veeam über 550.000 Kunden, darunter 82 % der Fortune 500.

Mehr erfahren unter www.veeam.com oder folgen Sie Veeam auf LinkedIn @veeam-software und X @veeam.