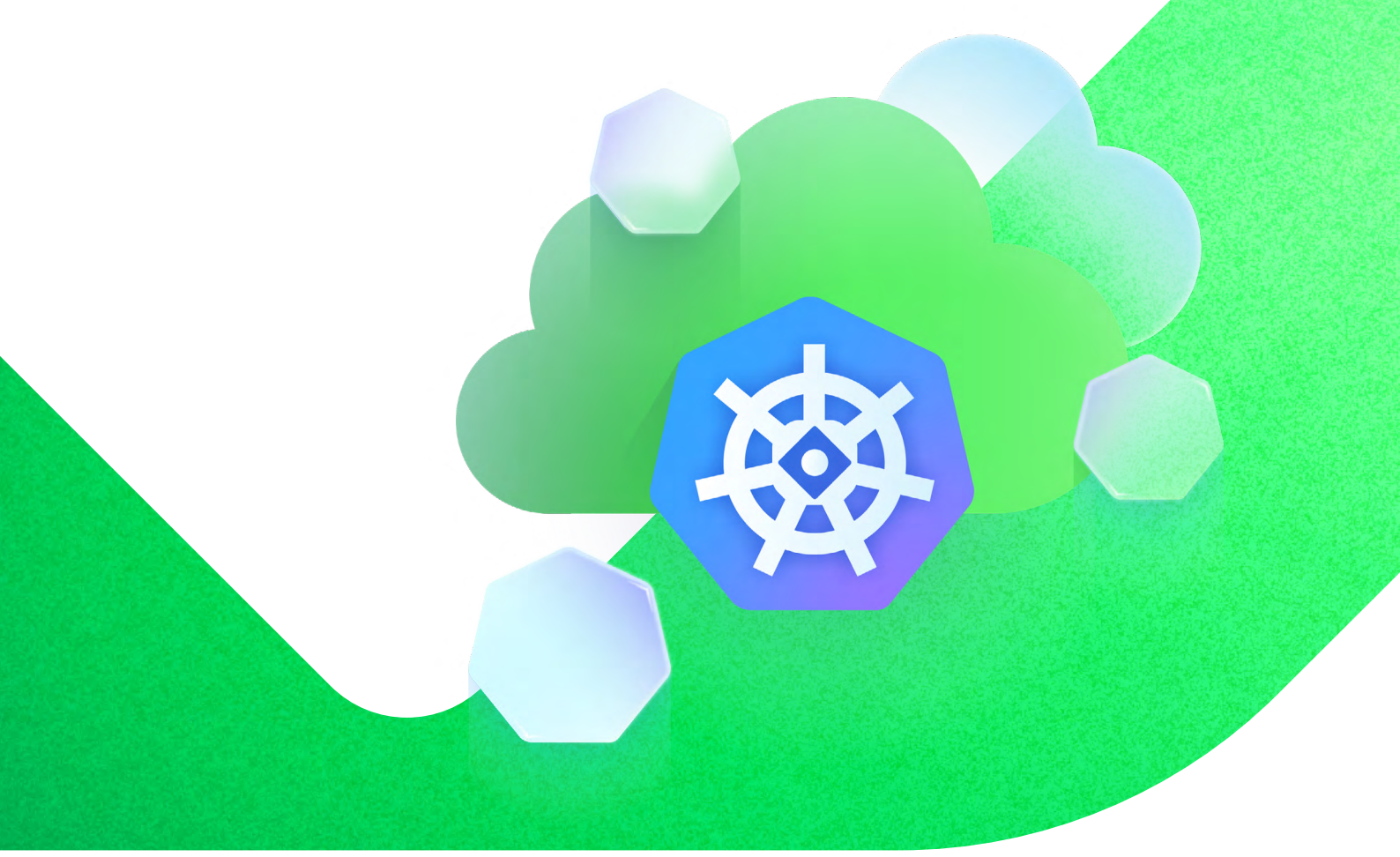
# 5 Best Practices für Kubernetes Backup

## Umgang mit Ihren Anforderungen bezüglich Datensicherung und -verwaltung



# Inhalt

# Executive Summary

**Veeam®, der weltweit führende Anbieter von Lösungen für Datensicherung und Ransomware-Wiederherstellung, unterstützt seine Kunden bei der Sicherung und Verwaltung all ihrer cloudbasierten, virtuellen und physischen Workloads. Veeams Lösung umfasst jetzt auch containerisierte Workloads mit Veeam Kasten *for Kubernetes*. Die Veeam Data Platform hilft Ihnen dabei, die in diesem White Paper beschriebenen Best Practices umzusetzen, um die Anforderungen an die cloudbasierte Datensicherung von Unternehmen zu erfüllen.**

Unternehmen setzen verstärkt auf Anwendungen, die auf der Cloud und auf Microservices basierende Architekturen nutzen — ein Fortschritt gegenüber den bisherigen starren Modellen und virtualisierten Ansätzen. Kubernetes hat sich inzwischen zur wichtigsten Container-Orchestrierungsplattform entwickelt. Parallel zur Einführung von Containern werden neue organisatorische Ansätze (in der Regel als DevOps oder ITOps bezeichnet) zügig eingeführt, bei denen die Rollen der Softwareentwicklung und des IT-Betriebs „kombiniert" werden, um bei gleichbleibender Qualität eine höhere Agilität zu erreichen. In einer solchen Umgebung haben Entwickler mehr Spielraum bei der Auswahl ihrer Tools und nehmen größeren Einfluss auf die Abläufe.

Der Wert von Daten, dem wichtigsten Kapital eines jeden Unternehmens, hat mit der weit verbreiteten Einführung von Kubernetes weiter zugenommen, da die Stacks für künstliche Intelligenz und maschinelles Lernen auf Kubernetes bereitgestellt werden. Diese Informationen und die damit verbundenen Software-Ressourcen sind aber Ziel von Hackerangriffen, die oft verheerende Auswirkungen haben. Auch die Sorge um den Datenschutz hat zu strengen Vorschriften geführt. Zusammengenommen haben diese Faktoren dazu geführt, dass die Datensicherung für IT-Teams zur Priorität geworden ist und vier verschiedene betriebliche Anwendungsszenarien umfasst: Backup und Wiederherstellung, Disaster Recovery, Anwendungsmobilität und Schutz vor Ransomware.

Auch Betriebsteams, die Infrastruktur und Anwendungen verwalten, arbeiten nicht in einer statischen Welt. Die zu verwaltenden cloudbasierten Umgebungen sind dynamisch und komplex. Die Teams müssen eine unterschiedliche Mischung aus traditionellen, virtualisierten und containerisierten Workloads unterstützen, die auf der Nutzung verschiedener Datenservices basieren, einschließlich relationaler und NoSQL-Datenbanken. Ihre Bereitstellungen können sich auf lokale und auch auf mehrere Cloud-Umgebungen verteilen und stützen sich oft auf eine Reihe von Speicherlösungen verschiedener Anbieter. Jede in diesen Umgebungen bereitgestellte Datenmanagement-Lösung muss die Anforderungen von Bedienern und Entwicklern in Einklang bringen, indem sie auf den operationellen Teil fokussiert und entwicklerfreundlich ist.

Kubernetes trägt weiter zum Wandel der IT-Landschaft bei, da es sich grundlegend von Plattformen unterscheidet, die auf früheren Technologien basieren. Dementsprechend ist ein anderer Backup-Ansatz erforderlich, den wir als Kubernetes-basiertes Backup bezeichnen. Es gibt sieben Gründe, warum Kubernetes-basierte Backups wichtig sind.

# 7 Gründe, warum Kubernetes-basierte Backups wichtig sind:

1

## Kubernetes-Bereitstellungsmuster

Die Kubernetes-Plattform unterscheidet sich grundlegend von früheren Computing-Infrastrukturen. Es erfolgt keine Zuordnung von Anwendungen zu Servern oder VMs. Eine Backup-Lösung muss dieses native Architekturmuster von Kubernetes verstehen und mit kontinuierlichen Veränderungen umgehen können.

2

## DevOps und „Shift Left“

Schnelle Anwendungsentwicklungs- und Bereitstellungszyklen sind in Kubernetes-Umgebungen die Regel. Folglich sollten Backup-Lösungen also anwendungs- und nicht infrastrukturorientiert sein.

3

## Herausforderungen für Kubernetes-Bediener

Der Betrieb erfordert Benutzerfreundlichkeit, um für IT-Teams die Einführung von Kubernetes-Bereitstellungen im Produktionsprozess zu beschleunigen. Dabei ist eine Backup-Lösung mit CLI-Zugang und übersichtlicher API sowie einem leistungsstarken und dennoch benutzerfreundlichen Dashboard von entscheidender Bedeutung.

4

## Skalierung der Anwendung

Kubernetes-basierte Microservices bestehen aus Hunderten einzelnen Komponenten mit unabhängigen Lebenszyklen, die nur für Kubernetes sichtbar sind. Ein Kubernetes-nativer Ansatz für Backups, bei dem Anwendungen als Unit of Atomicity für konsistenten Betrieb beibehalten werden, ist dabei unumgänglich.

5

## Datenschutzrisiken

Sich ausschließlich auf die Hochverfügbarkeit und die Replikationsfähigkeiten zu verlassen, kann zur Beschädigung von Daten oder zu katastrophalem Datenverlust führen. Unternehmen benötigen deshalb eine Backup-Lösung, die eine Vielzahl von Kubernetes-Anwendungen und Bereitstellungsmethoden unterstützt.

6

## Sicherheit

Die Kubernetes-Sicherheitsfeatures verhindern nicht nur von außerhalb des Clusters den Zugriff auf interne Anwendungskomponenten und ihre zugehörigen Datenservices, sondern auch über andere nicht vertrauenswürdige Anwendungen. Eine gut strukturierte native Backup-Lösung für Kubernetes, die in die Kubernetes-Konsole integriert werden kann, gewährleistet konsistente Sicherheitsvorgänge.

7

## Partnerintegrationen

Polyglot Persistence, bei der mehrere Datenservices innerhalb derselben Anwendung genutzt werden, fiel zeitlich dem Wachstum von Kubernetes zusammen. Dabei entscheidend ist eine Backup-Lösung mit Workload-Wissen zur Auswahl der E/A-Befehle, die am besten für Anwendungsanforderungen geeignet sind, sowie die Interoperabilität mit dem Rest des cloudbasierten Infrastruktur-Ökosystems.

> "Im Rahmen unserer Evaluierung stellte Enterprise Strategy Group fest, dass [Veeam Kasten] die Datensicherung und Wiederherstellung Funktionalitäten für Kubernetes Anwendungen erfüllen kann. Wir haben dies untersucht, indem wir verglichen haben, wie herkömmliche Lösungen und [Veeam Kasten] vier wichtige Anwendungsfälle abdecken: Backup und Wiederherstellung, Disaster Recovery, Mobilität von Anwendungen und Schutz vor Ransomware. [Veeam Kasten] ist für diese Anwendungsfälle besser geeignet, wenn es um zustandsbehaftete und containerisierte Anwendungen auf Kubernetes geht, da die Plattform anwendungsspezifisch und anwendungskonsistent ist. Da herkömmliche Lösungen VM-zentriert sind, kann die Datensicherung für Kubernetes-Anwendungen ineffektiv, ineffizient und unvollständig sein."

**Technisches White Paper: Die Mythen über die Datensicherung mit Kubernetes aufklären**
ESG, April 2024

Basierend auf den Erfahrungen unserer Kunden und unter Berücksichtigung der oben genannten Schlüsselfaktoren, die besondere Aufmerksamkeit verlangen, sind wir zu den folgenden **fünf Best Practices für Backups in Kubernetes** gelangt:

## Architektur

Die zum Schutz von Kubernetes-Anwendungen verwendete Plattform muss automatisch alle Anwendungskomponenten erkennen, die in Ihrem Cluster ausgeführt werden, und dabei die Anwendung als Unit of Atomicity behandeln. Die Anwendung muss den Status bezüglich Speicher-Volumes, Datenbanken (NoSQL/relational) sowie Konfigurationsdaten in Kubernetes-Objekten wie ConfigMaps und Secrets umfassen.

## Wiederherstellbarkeit

Die Plattformen für die Datensicherung müssen es Ihnen ermöglichen, die gewünschten Komponenten der Anwendung am gewünschten Ort wiederherzustellen. Sie sollten zudem über die Granularität verfügen, nur bestimmte Anwendungen wiederherstellen zu können, z. B. das Datenvolumen. Der Ansatz muss die Wiederherstellung einfach und leistungsstark gestalten, indem Sie die passende Point-of-Time-Kopie der Anwendung auswählen können.

## Betrieb

Es sollte sichergestellt werden, dass eine Kubernetes native Backup-Plattform in großem Maßstab eingesetzt werden kann, Betriebsteams die Workflow-Funktionalitäten bietet, die sie benötigen, und Compliance und Monitoring Anforderungen erfüllt. Bediener sollten Anwendungsentwicklern Self-Service-Funktionalitäten zur Verfügung stellen können, ohne dass dafür den Anwendungscode oder die Bereitstellung ändern zu müssen.

## Sicherheit

Es müssen Kontrollmechanismen für Identitäts- und Zugriffsverwaltung und rollenbasierte Zugriffskontrolle (RBAC/Rollenbasierte Zugriffssteuerung) implementiert werden. RBAC/Rollenbasierte Zugriffssteuerung ermöglicht es verschiedenen Personas innerhalb eines Betriebsteams, häufige Aufgaben wie Monitoring bei geringstmöglichem Zugriff zu erledigen. Verschlüsselung bei der Speicherung und während der Übertragung müssen stets implementiert werden, um sicherzustellen, dass die Daten sicher bleiben, wenn sie die Compute-Umgebung verlassen haben.

## Mobilität

In einer Multi-Hybrid-Cloud-Welt muss eine cloudbasierte Datenmanagement-Plattform mehrere Distributionen flexibel unterstützen können und Funktionalitäten bieten, die eine Portierbarkeit von Workloads und Anwendungen über alle unterschiedlichen Umgebungen hinweg ermöglichen. Mobilität und Migration von Kubernetes-Anwendungen stellen die kollektiven Funktionalitäten dar, die für verschiedene Anwendungsfälle erforderlich sind, darunter die Wiederherstellung von Anwendungen, sowie das Klonen und die Migration von Containern.

# Kapitel 1. Einleitung

## 1.1 Moderne IT-Umgebungen

Die Cloud Native Computing Foundation stellte in ihrer jährlichen Umfrage im Jahr 2023 fest, dass der cloudbasiert Ansatz unbestrittene als Infrastruktur der globalen Technologie gilt[1]. IT-Teams haben mit Hochdruck daran gearbeitet, bestehende Anwendungen zu refaktorisieren und cloudbasierte Architekturen als neuen Standard für Entwicklungen zu etablieren. Die Annual Survey von 2023 ergab, dass 66 % der Anbieter und Verbraucher Kubernetes in der Produktion einsetzen und 18 % es einer Bewertung unterzogen. Dieses Ergebnis zeigt, dass Kubernetes weiterhin die De-facto-Container-Orchestrierungsplattform ist, wobei insgesamt 84 % entweder in der Produktion eingesetzt oder diesbezüglich bewertet werden. Das entspricht einer Steigerung von 4 % gegenüber den Ergebnissen des Vorjahres.

**84 %**

**der Anbieter und Verbraucher nutzten Kubernetes im Jahr 2023 in der Produktion oder bei der Bewertung**

Laut einer aktuellen Umfrage von ESG Research[2] nutzen derzeit mehr als 47 % der Entscheidungsträger aus verschiedenen Branchen Container in ihren Produktionssystemen. Darüber hinaus haben weitere 35 % der Unternehmen ihre Absicht bekundet, innerhalb der nächsten 12 Monate Container Technologien einzuführen. Im Jahr 2024 werden voraussichtlich 82 % aller Unternehmen Container einsetzen. In Anbetracht der Ergebnisse bezüglich der weit verbreiteten Einführung der Kubernetes-Container-Technologie steht zu erwarten, dass etwa zwei Drittel der in Produktionsumgebungen genutzten Container auf Kubernetes basieren werden.

**82 %**

**der Unternehmen werden 2024 Container einsetzen**

Neben dieser technologischen Entwicklung ist auch ein Wandel der Organisations- und Prozessansätze bei den IT-Teams zu beobachten. Diese werden in der Regel als DevOps oder ITOps bezeichnet und spiegeln eine neuere, agilere Arbeitsweise wider, bei der Entwickler mehr Freiheit bei der Auswahl ihrer Tools bekommen und eine größere Rolle bei operativen Fragen spielen. Die Denkweise hat sich weiterentwickelt, ebenso wie die Messgrößen, auf die sich die Teams konzentrieren — wobei Metriken wie Code-Release-Zeit, Häufigkeit der Bereitstellung, Zeit bis zur Wiederherstellung und Fehlerrate bei Änderungen stärker berücksichtigt werden.

[1] CNCF Jahresumfrage 2023, Cloud Native Computing Foundation, 9. April 2024

[2] "Measuring the Current State and Momentum in the Enterprise Market for Kubernetes Protection", Enterprise Strategy Group, Christophe Bertrand, April 2023

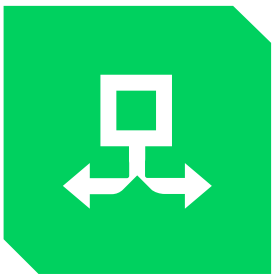
## 1.2 Daten sind ein wertvollstes Gut

Nicht nur haben sich IT-Teams und ihre Organisations-philosophie weiterentwickelt — die IT ist mittlerweile auch zu einem noch wichtigeren Faktor geworden, um sich Wettbewerbsvorteile zu verschaffen. Es sind völlig neue und extrem erfolgreiche Unternehmen hervorgegangen, die sich auf den effektiven und neuartigen Einsatz von IT stützen. Ausschlaggebend dafür sind die verbesserte Verfügbarkeit von skalierbaren Computing-, Netzwerk- und Speicherressourcen, das Wachstum von und der Zugriff auf Daten und außerdem die Einführung von fortschrittlichem maschinellen Lernen und künstlicher Intelligenz. Das beispiellose Wachstum von Daten, die Fähigkeit eines Unternehmens, aus diesen Daten einen Wert zu schöpfen, ständige Angriffe auf IT-Systeme durch staatliche und nichtstaatliche Akteure und die Notwendigkeit, strenge Vorschriften zum Schutz der Privatsphäre und der Datensicherung einzuhalten — dies hat alles dazu geführt, dass Unternehmensdaten als kritische Vermögenswerte erachtet werden, die unbedingt geschützt werden müssen. Alle zugrunde liegenden Datenbestände und der zugehörige Code müssen gegen böswilligen und versehentlichen Verlust oder Korruption geschützt werden.

## 1.3 Was das Betriebsteam beachten muss

Typische IT-Umgebungen in modernen Unternehmen sind keine statischen Gebilde mit festen, standardisierten Bereitstellungen eines einzigen Anbieters. Der Druck, Kostenstruktur und Effizienz durch die Einführung neuer Technologien kontinuierlich zu verbessern, gepaart mit Unternehmensveränderungen wie Fusionen und Übernahmen und der Notwendigkeit, sich ständig ändernde gesetzliche Vorschriften einzuhalten — dies alles führt zu einer höchst dynamischen Situation, die von Betriebsteams nicht nur berücksichtigt, sondern sogar als Status quo angenommen werden muss.

**Jede gewählte Management-Lösung muss mit folgenden Komponenten kompatibel sein:**



**Vielfalt**

**Skalierung**

**Veränderungsrate**

### 1.3.1 Mehrere Workloads

Anwendungsarchitekturen haben in den letzten Jahren einen rasanten Wandel durchgemacht: von monolithischem Design auf Bare Metal über virtualisierte Anwendungen in Hypervisoren, bis hin zu containerisierten Anwendungen, die auf Microservice-Architekturen basieren und oft selbst auf einer virtualisierten Infrastruktur betrieben werden. Die meisten Unternehmen mit IT-Betrieb ab einer gewissen Größenordnung können sinnvollerweise allerdings nicht erwarten, dass alle Anwendungen am gleichen Punkt des Entwicklungsspektrums stehen. Stattdessen ist das am häufigsten beobachtete Muster, dass Anwendungen das gesamte Spektrum abdecken.

**Das Ziel**

Sollte es sein, eine Lösung für die Datensicherung zu nutzen, die diese Vielfalt abdeckt, aber dennoch Refaktorisierung und Neuentwicklung unterstützt, und so die Vorteile von cloudbasierten Anwendungen bietet, einen einfachen Umstiegsweg für herkömmliche Anwendungen ermöglicht und Kosten für das Management der vielfältigen Umgebung einspart.

### 1.3.2 Multi-Umgebungen

Wie bei Anwendungen findet man auch bei Bereitstellungsumgebungen häufig eine Mischung aus lokalen und cloudbasierten Lösungen. Es ist nicht ungewöhnlich, dass Unternehmen bei der Anwendungsbereitstellung einen Hybrid- und Multi-Cloud-Ansatz verfolgen. Bei der Nutzung von verwalteten Kubernetes-Anwendungen oder der Bereitstellung von Kubernetes-Workloads in verschiedenen Clouds unterscheiden sich Kubernetes-Distributionen in der Regel auch in Bezug auf proprietäre Erweiterungen und unterstützte Features.

### 1.3.3 Multi-Daten-Services

Auch bei den Datendiensten, die den Anwendungen zugrunde liegen, gibt es typischerweise eine große Vielfalt. Entwickler wählen die Datendienste aus, die die Anforderungen der jeweiligen Aufgabe am besten umsetzen können. Oft kommen auch mehrere Datendienste innerhalb derselben Anwendung zum Einsatz. Dies führt zu einer polyglotten Mischung aus Software-as-a-Service (SaaS)-Angeboten, Managed Services, relationalen Datenbanken, NoSQL-Systemen, Nachrichtenwarteschlangen und mehr.

### 1.3.4 Vielfältige Speicher-Anbieter

Die Ebene der Speicherinfrastruktur ist eine weitere Dimension mit großer Vielfalt. Teams in hybriden Umgebungen nutzen nicht nur lokalen Speicher und Speicher von Cloud-Anbietern, sondern je nach Bedarf auch unterschiedliche Speichertypen und das möglicherweise auch innerhalb eines einzigen Kubernetes-Clusters. Darüber hinaus wird der Speicher selbst lokal typischerweise von verschiedenen Anbietern (Dell EMC, HP usw.) bezogen, die jeweils ihre eigenen Management-Tools und -Frameworks mitbringen.

# Kapitel 2. Kubernetes-basierte Backups sind wichtig

Backup ist eine seit langem etablierte Disziplin mit einer Vielzahl von Lösungen, um die Anforderungen großer und kleiner Benutzer zu erfüllen. Bei der Sicherung und dem Schutz von Kubernetes-Anwendungen gibt es bestimmte Gründe, warum der Einsatz einer Kubernetes-basierten Backup-Lösung absolut entscheidend ist. Im E-Book „7 wichtige Gründe für Kubernetes-basierte Backups“ wird ausführlich auf diesen Aspekt eingegangen. Weiter unten finden Sie eine Zusammenfassung als Kontext.

## 2.1 Kubernetes-Bereitstellungsmuster

Die Kubernetes-Plattform unterscheidet sich grundlegend von früheren Computing-Infrastrukturen. Es gibt keine Zuordnung von Anwendungen zu Servern oder VMs — Kubernetes verwaltet die Distribution der Anwendungskomponenten auf den Servern, wobei die Anwendungen möglicherweise auch zusammengelegt werden. Herkömmliche Backup-Systeme sind kaum in der Lage, den Zustand einer bestimmten Anwendung übersichtlich zu erfassen.

## 2.2 DevOps und „Shift Left“

Die DevOps-Philosophie, die parallel mit Kubernetes eingeführt wurde, überlässt Entwicklern die Kontrolle über Infrastruktur und Bereitstellung (bekannt als "Shift Left"). Backup-Systeme müssen nicht nur in die von den Entwicklern verwendeten CI/CD-Tools integriert werden, sondern auch automatisch Anwendungen erkennen und absichern, die demnächst online gehen. Dabei sollten sie für die Entwickler transparent sein und auch Kubernetes-basierte APIs verwenden, mit denen die Entwickler vertraut sind. Folglich sollten Backup-Lösungen also anwendungs- und nicht infrastrukturorientiert sein.

## 2.3. Herausforderungen für Kubernetes-Bediener

Teams mit einem vSphere- oder Linux-Hintergrund, die zu Kubernetes wechseln wollen, profitieren von einer Plattform, die tief in Kubernetes integriert ist und ihre inhärente Komplexität nicht zu Tage treten lässt. Die vielen Ressourcen zu ignorieren, ist dabei allerdings keine Option, denn sich beim Backup auf Infrastrukturfestplatten und -volumes zu verlassen, führt zu fehleranfälligen Wiederherstellungsprozessen und letztlich zu längeren Wiederherstellungszeiten.

## 2.4 Skalierung der Anwendung

Im Container-Paradigma kann eine einzelne Anwendung, die früher nur aus einigen wenigen VMs bestand, mittlerweile Hunderten speziellen Kubernetes-Ressourcen entsprechen. Betrachtet man dabei alle Anwendungen in einem Cluster, kann das zu einer überwältigenden Anzahl von Komponenten führen, die ohne eine auf Kubernetes basierende Datensicherungsplattform zu verwalten sind. Außerdem sind Kubernetes und cloudbasierte Anwendungen so konzipiert, dass sie je nach Auslastung mitskalieren. Die Backup-Plattform muss fähig sein, auf diese Anwendungsskalierung in den typischerweise verwendeten Multicluster-Umgebungen effektiv zu reagieren.

## 2.5 Datenschutzlücken

Ob in der Cloud oder lokal, der zugrunde liegende Speicher ist nicht ausfallsicher: Selbst das kampferprobte EBS von AWS wirbt mit einer Failure Rate, die nicht bei null liegt. Außerdem sind lokale Volume-Snapshots möglicherweise nicht vor Hardwareausfällen geschützt und das Löschen eines Volumes führt typischerweise gleichzeitig und automatisch zur Löschung aller zugehörigen Snapshots.

## 2.6 Sicherheit

Kubernetes bietet mehrere Sicherheitsfeatures und um deren Effektivität nicht zu beeinträchtigen, ist es wichtig, dass eine Backup-Lösung auf Kubernetes basiert und in die Kubernetes-Konsole integriert ist. Da Entwickler mittlerweile immer mehr Verantwortung für die Infrastruktur übernehmen („ITOps"-Modell), ist es wichtig, einen genau abgestimmten, rollenbasierten und auf Bereiche abgestimmten Zugriff mit den gleichen Rollen und Tools zu ermöglichen, die bei Kubernetes zum Einsatz kommen, anstatt zusätzliche Rollenmanagement-Systeme zu nutzen, die zu mehr Komplexität führen. Damit der Ansatz von Kubernetes, die Verschlüsselung an Speicher- und Backup-Plattformen zu delegieren, gut funktioniert, muss das Backup-System in der Lage sein, die Kubernetes-Zertifikatsverwaltung zu verstehen, mit speicherintegrierten Schlüsselmanagement-Systemen (KMS) zusammenzuarbeiten und kundenseitig verwaltete Verschlüsselungsschlüssel (CMEKs) über die Secrets-Benutzeroberfläche von Kubernetes zu unterstützen.

## 2.7 Partnerintegrationen

Die Verwendung von Polyglot Persistence in Kubernetes Umgebungen erfordert den Einsatz einer Backup Plattform, die die Beziehungen zwischen den verschiedenen Datendiensten anhand der Kubernetes Metadaten ableiten kann. Eine solche Backup-Lösung kann diese Beziehungen und ihr Verständnis der Workloads nutzen, um eine konsistente Kopie des gesamten Stacks von Anwendungen zu erstellen. Die Backup-Lösung muss auch gut zu den übrigen Kubernetes Cloud nativen Tools passen, die das Betriebsteam z. B. für Monitoring, Benachrichtigungen, Zugriffskontrolle (Kubernetes APIs), Protokollierung und Auditing verwendet.

# Kapitel 3. Anwendungsszenarien für die Datensicherung

Nachdem wir nähergebracht haben, warum ein Kubernetes-natives Backup so wichtig ist, und bevor wir uns mit den Best Practices für Kubernetes-Backup beschäftigen, wollen wir kurz die wichtigsten Anwendungsszenarien im Zusammenhang mit Backups beleuchten.

## 3.1 Backup und Wiederherstellung

Natürlich ist der erste Anwendungsfall beim Thema Backup der Schutz vor versehentlichem oder böswilligem Datenverlust oder -beschädigung. Dazu gehört das regelmäßige Speichern von Kopien der relevanten Informationen, damit im Bedarfsfall eine entsprechende Kopie wiederhergestellt werden kann. Traditionell verfolgen IT-Teams einen Ansatz, bei dem sie vollständige Backups (vielleicht wöchentlich) und häufigere Teilbackups erstellen. Neben der Bestätigung, dass ein Backup erfolgreich erstellt wurde, sind weitere Faktoren von Interesse, z. B. wie lange das Backup gedauert hat (während das Backup läuft, kann die Leistung der Anwendung eingeschränkt sein) und wie viel Speicherplatz das Backup beansprucht hat (Lösungen mit effektiver Deduplizierung und Komprimierung führen zu geringeren Speicherkosten). In modernen Computing-Umgebungen können Backups häufiger erstellt werden, wenn ausgewählte und zustandsbehaftete Datensicherung auf einen nahezu kontinuierlichen Rhythmus eingestellt sind. Neben dem Schutzaspekt können Backups oder „Snapshots“ auch für Test- und Entwicklungszwecke genutzt werden, d. h. man kann ein Snapshot der Produktionsdaten erstellen und es in einer getrennten Umgebung wiederherstellen, um dort Entwicklungs- oder Leistungstests durchzuführen. Es gibt unterschiedliche Ansätze zur Datensicherung. Bei der Erwägung, eine Backup-Strategie einzuführen, ist es sinnvoll, auch das Konzept der Konsistenzebenen zu in Betracht zu ziehen. Die verschiedenen Ansätze legen verschiedene Schwerpunkte: Sie sind entweder speicherzentriert, speicherzentriert, aber mit Service Hooks für Datenservices, datenservicezentriert oder anwendungszentriert. Weitere Einzelheiten zu diesen Konsistenzebenen finden Sie im Artikel „Flavors of Data Management in Kubernetes“[3].

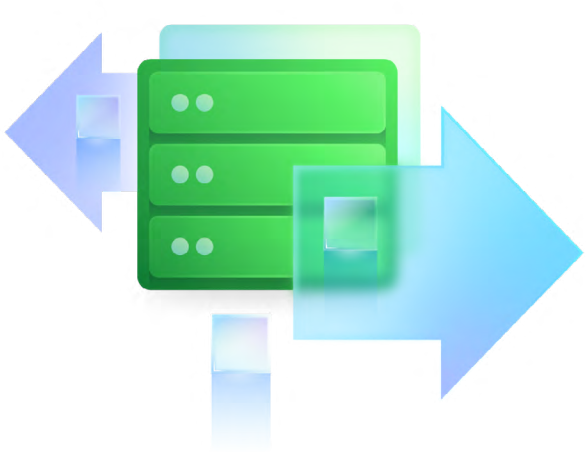
[3] Quelle: „Flavors of Data Protection in Kubernetes“, TFIR, Guarav Rishi, 28. Oktober 2019

## 3.2 Disaster Recovery

Disaster Recovery ist das zweite Anwendungsszenario und bezieht sich auf Szenarien im Falle eines lokalen Ausfalls (z. B. aufgrund eines Brandes oder einer Überschwemmung oder längerer Strom- oder Netzwerkausfälle), der so gravierend ist, dass der Betrieb an einem anderen Standort fortgesetzt werden muss. Für die Nutzung an einem alternativen Standort müssen der gesamte Anwendungs-Stack sowie die zugehörigen Daten zur Verfügung gestellt werden. Neben den Kosten gehören bei Disaster Recovery in der Regel der Wiederherstellungsziel (RPO) (d. h. wie aktuell die Daten sind und wie viel Datenverlust toleriert werden kann) und die Wiederherstellungszeit (RTO) (d. h. wie lange es dauert, bis die Wiederherstellungsumgebung betriebsfähig ist) zu den wichtigsten Erwägungen. Teams müssen diese Aspekte bei der Entscheidung berücksichtigen, welche Art von Datensicherungsmanagement-Plattform für ihre geschäftlichen Anforderungen geeignet ist.

## 3.3 Mobilität von Anwendungen

Unter Anwendungsmobilität versteht man die Möglichkeit, eine Anwendung von einer Umgebung in eine andere zu migrieren, z. B. zwischen Clustern, Regionen, Kubernetes-Distributionen, lokal in die Cloud oder sogar von einer Cloud in eine andere. Solche Verschiebungen können erforderlich werden, wenn ein Unternehmen seine bevorzugte Technologieplattform ändert, Kosten optimiert oder sich neue Geschäftsanforderungen ergeben. Es kann auch wünschenswert sein, eine Anwendung auf einer anderen Plattform wiederherzustellen. Dieses Anwendungsszenario umfasst auch die Anforderungen, die sich aus der Notwendigkeit eines Upgrades von einem Stack zum anderen ergeben (z. B. ein Upgrade von OpenShift 3.x auf OpenShift 4.x). Sollte Mobilität nötig sein, bedarf es starker Unterstützung, um die vielen Unterschiede zwischen den Quell- und Zielumgebungen zu bewältigen — dass die Zielumgebung möglicherweise nicht über das gleiche Speichersystem verfügt, ist dabei nur ein Beispiel. Teams, die vor einem solchen Anwendungsszenario stehen, achten darauf, dass die Lösungen folgende Möglichkeiten bieten: Ermöglichen von Daten- und Anwendungstransformationen von der Quelle zum Ziel, während sich zugrunde liegende Kubernetes-Spezifikationen, Computer- und Speicherinfrastrukturen ändern können (z. B. dass die Plattform richtlinienbasierte Operationen zur transparenten Änderung von Anwendungs-spezifikationen im laufenden Betrieb ermöglicht).



## 3.4 Schutz vor Ransomware

Beim Schutz vor Ransomware handelt es sich um die Fähigkeit, Daten und Anwendungen im Fall eines Cybersecurity-Angriffs, der zu Ransomware-Forderungen führen könnte, zu schützen. Im einfachsten Fall sind regelmäßige Backups von Anwendungen, kritischen Daten und Konfigurationen unerlässlich. So gewährleisten sie eine schnelle Wiederherstellung im Falle eines Angriffs. Mithilfe des Prinzips der geringsten Berechtigungen können unnötige Zugriffe beschränkt und damit die potenziellen Auswirkungen einer Datenschutzverletzung minimiert werden. Ein kontinuierliches Monitoring des Systemverhaltens hilft dabei, Anomalien frühzeitig zu erkennen, während rechtzeitiges Patchen und Updates von sowohl Kubernetes-Clustern als auch von Schutzsystemen die allgemeine Ausfallsicherheit stärkt. Durch die Implementierung einer Netzwerksegmentierung kann die Ausbreitung eines Ransomware-Angriffs innerhalb einer Umgebung eingedämmt werden. Darüber hinaus kann eine Schulung der Mitarbeiter über die Best Practices bei der Sicherheit und die Einführung von Praktiken wie Konsistenz und Beobachtbarkeit in DevOps die Fähigkeit der Mitarbeiter verbessern, schnell und effektiv auf potenzielle Bedrohungen zu reagieren und diese zu erkennen.

# Kapitel 4. Best Practices

Wenn wir über Backups im traditionellen Sinne nachdenken, erwarten wir, dass wir in einer Kubernetes-Umgebung dazu in der Lage sein wollen, Container sichern und wiederherstellen zu können, aber das ist nicht so wichtig wie unveränderliche Container-Backups. Der Schutz des gesamten Anwendungsstatus ist in einer Kubernetes-Umgebung das eigentliche Ziel eines Backups. Das Ziel kann man sich vorstellen, ein Rezept zu erstellen, das die Komponenten und Dienste, die die Anwendung benötigt, bis ins kleinste Detail beschreibt, und einen Snapshot der persistenten Daten zu erstellen und alles zusammen zu speichern. Im Idealfall geschieht dies in einer Fehlerdomäne, die sich vom Kubernetes-Cluster unterscheidet. In diesem Fall würde man bei einer Wiederherstellung dem Rezept folgen, um die persistenten Daten wiederherzustellen und dann die Anwendung und die zugehörigen Services zu installieren und zu konfigurieren, um den normalen Betrieb wiederaufnehmen zu können.

Wenn traditionelle Unternehmen damit beginnen, Container in der Produktion und im großen Maßstab einzuführen, werden herkömmliche monolithische Anwendungen „containerisiert“ oder migriert, um ihre Bereitstellung einfacher zu gestalten. Der Wandel solcher traditioneller Anwendungen zieht neue Erwägungen nach sich, z. B. wie Workloads im Notfall geschützt und wiederhergestellt werden können. Solche Anwendungen enthalten üblicherweise Stateful-Konfigurationen, die wiederhergestellt werden müssen. Zu den Stateful-Daten gehören dabei nicht nur Daten, die von der Anwendung gespeichert werden (z. B. Tabellen in einer Datenbank). Dazu gehören auch zur Anwendungskonfiguration zugehörige Daten (Secrets, TLS-Zertifikate usw.), die im Falle eines Ausfalls nicht wiederhergestellt werden, indem man die Anwendung einfach erneut bereitstellt. Diese Anforderungen bringen einzigartige Herausforderungen für die Sicherung und Wiederherstellung von Workloads mit sich. Als Container-Plattformen hauptsächlich mit Stateless-Workloads genutzt wurden, konnten Anwendungen in der Regel schnell hochgefahren, zerstört und bei Bedarf erneut bereitgestellt werden. Da die Einführung von Containern mittlerweile aber sowohl Stateful- als auch Stateless-Anwendungen umfasst, war der Bedarf an einer soliden Backup-Lösung nie größer.

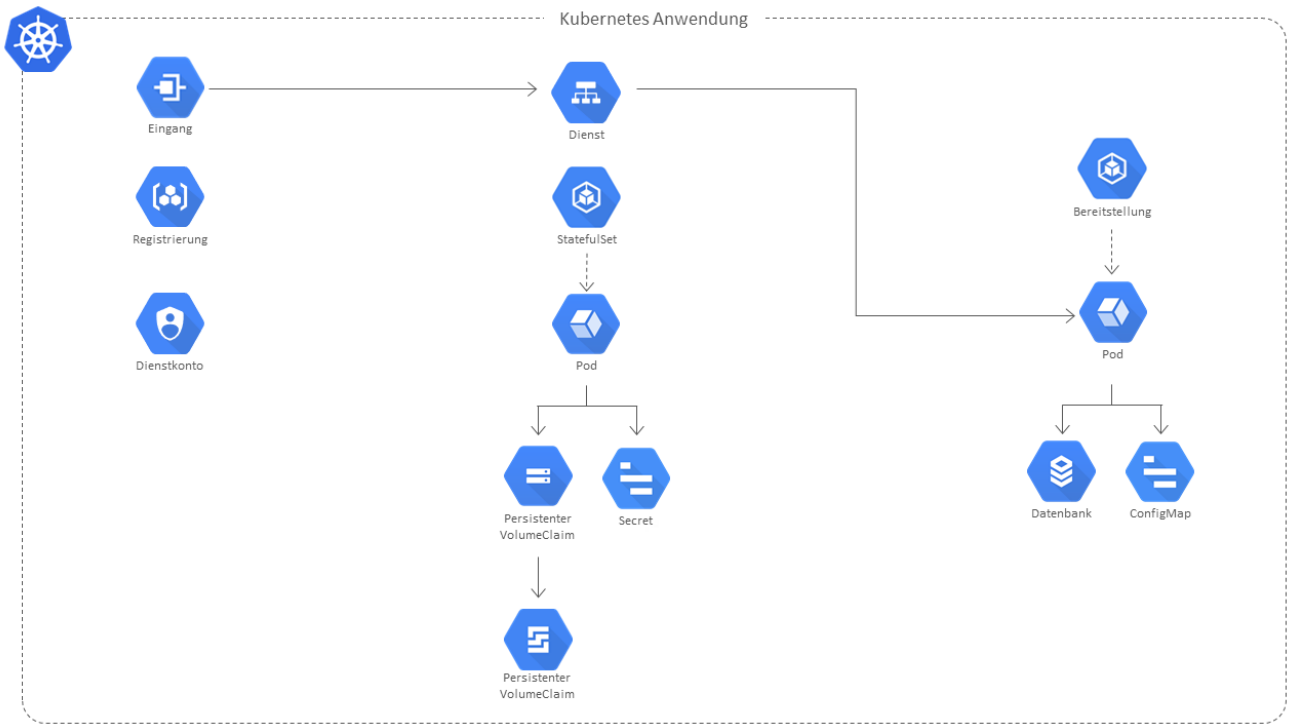
Während der Schutz von geschäftskritischen Daten im Vordergrund steht, ist es ebenso wichtig, sicherzustellen, dass die Daten mit der richtigen Konsistenz erfasst werden. Aus technischer Sicht stehen Überlegungen zu ausfallkonsistenten und anwendungsspezifischen Backups nach wie vor an erster Stelle. Für die meisten Workloads ist ein ausfallsicheres Backup oder ein Snapshot ausreichend, aber für Workloads mit regelmäßigen Änderungen, wie z. B. bei Datenbanken, müssen wir sicherstellen, dass wir ein konsistentes auf einen bestimmten Zeitpunkt bezogenes Backup erstellen, um Datenkorruption zu vermeiden — selbst in der containerisierten Infrastruktur.

Da die Einführung von Kubernetes auf Skalierbarkeit und einfache Bereitstellung abzielt, ist die Automatisierung für jedes in der Umgebung des Containers eingesetzte Management-System letztlich eine der entscheidenden Komponenten. Bei Betrachtung von Backup-Lösung sehen wir, dass herkömmliche Backup-Produkte Schwierigkeiten dabei haben, mit der echten dynamischen Skalierung der Kubernetes-Infrastruktur zusammenzuarbeiten oder sich in diese zu integrieren. Eine Backup-Lösung ist nötig, die sich nicht nur in die Kubernetes-APIs integriert und sie nutzt, sondern diese APIs auch erweitern kann und größere Automatisierungsintegration bietet. Die Bereitstellung einer Backup-Plattform als natives containerisiertes System, das mit Kubernetes funktioniert, wäre die ideale Option und besser als ein traditioneller „Backup-Server“, der in einer anderen Umgebung betrieben wird und separat gemanagt werden muss.

In diesem Abschnitt diskutieren wir die Best Practices und Empfehlungen für die Implementierung einer Kubernetes-fähigen Backup-Lösung sowie die Voraussetzungen für eine erfolgreiche Backup Strategie, die sich gleichzeitig einfach und flexibel an diese sich schnell weiterentwickelnden Cloud nativen Ökosysteme anpassen lässt.

## 4.1 Architektur

Bei der Implementierung einer Backup-Strategie zum Schutz von Kubernetes-Workloads ist es entscheidend, detaillierte Kenntnisse darüber zu haben, wie Kubernetes funktioniert. Dieses Whitepaper soll die Kubernetes Architektur nicht im Detail beschreiben, sondern helfen, besser zu verstehen, wie eine Backup Strategie implementiert werden sollte. Hierfür müssen einige Komponenten näher betrachtet werden.



Im obigen Diagramm sehen wir ein Beispiel für eine typische Kubernetes Anwendung. Sie besteht aus Pods, Diensten, Zertifikaten, Secrets, persistenten Volumes und anderen Komponenten. Wir haben festgestellt, dass produktive Anwendungen im Durchschnitt aus Hunderten solcher Komponenten bestehen. Angesichts dieser Erwägungen ist es wichtig, die richtigen Lösungen zu finden, um nicht nur Daten zu schützen und wiederherzustellen, sondern auch diese internen Komponenten — und das in großem Maßstab.

Sobald wir eine Backup-Plattform in Kubernetes implementiert haben, kann die Lösung über den API-Server automatisch als Schnittstelle mit der Kubernetes-Konsole fungieren. Diese Integration kann nicht nur zur Erkennung der Kubernetes Anwendungen verwendet werden, die auf dem Cluster ausgeführt werden, sondern bezieht auch die zugrunde liegenden Computing-, Netzwerk- und Speicher Infrastruktur-Umgebungen mit ein.

In ersten Schritt wird die Integration genutzt, um die Beziehung zwischen Speicher und Anwendungen zu ermitteln und dann den besten (effizienten, performanten, konsistenten) Weg zu finden, um die auf persistenten Volumes gespeicherten Anwendungsdaten zusammen mit den zugehörigen Anwendungsressourcen zu erfassen. Die nächste Erwägung betrifft den Speicherort von Backup-Daten, einschließlich innerhalb des Speichersystems für schnelle Wiederherstellung oder bei großen Cloud-Anbietern in Abhängigkeit von dauerhaften Snapshots. In den meisten Fällen werden die Backup-Daten aber im Objektspeichersystem einer anderen Ausfalldomäne gespeichert. Das kann sogar auf Georeplikation für Disaster Recovery ausgeweitet werden.

Bei der Integration von Speicher in Kubernetes sind mehrere wichtige Bereiche zu berücksichtigen. Speicher in Kubernetes wird als persistente Volumes dargestellt, die zur Nutzung durch Anwendungscontainer bereitgestellt werden. Neben der Anwendungskonfiguration gehören diese Volumes zu den wichtigsten Geschäftsdaten, die geschützt werden müssen. Auch sollte erwogen werden, wo diese Daten gespeichert sind.

**Solle sie in einem lokalen Blockspeicher aufbewahrt werden?**

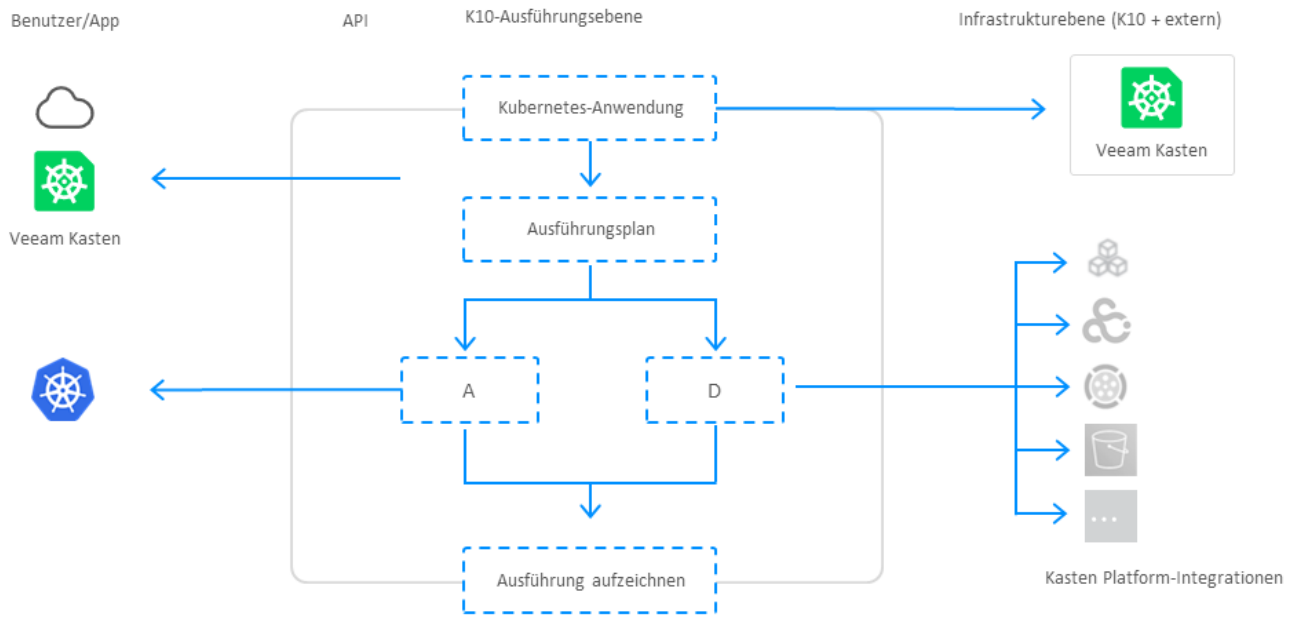
Wenn Kubernetes in einer lokalen Umgebung läuft oder außerhalb des Standorts betrieben wird, sollten Sie über eine Objektspeicherplattform wie Amazon S3 oder Microsoft Azure Blob Storage nachdenken. Bei der Implementierung einer erfolgreichen Datensicherungsstrategie ist es entscheidend, flexibel zu bleiben und leichte Bedienbarkeit bei der Auswahl von Sekundär-speichern für Backup-Daten zu beachten.

## 4.2 Wiederherstellbarkeit

Die Wiederherstellung ist nicht so einfach wie die Neuerstellung von Kubernetes-Objekten und Speichervolumes. Angesichts der vielen Komponenten und der Komplexität von Kubernetes muss ein Ausführungsplan aufgestellt werden, der zunächst alle Cluster-Abhängigkeiten überprüft, neue Kubernetes-Ansichten der wiederherzustellenden Daten erstellt und die Computing-Infrastruktur und den Kubernetes-Cluster bestimmt, wo die Wiederherstellung initiiert werden soll (z. B. verfügbarkeitszonenübergreifende Wiederherstellung). Sobald der Ausführungsplan zur Wiederherstellung aufgestellt wurde, müssen die Backup-Datenquellen (Objektspeicher, Snapshots, Backups) identifiziert und der Zielspeicher (Neuzuweisung der Speicherklassen, Änderungen der Speicherplattform usw.) vorbereitet werden.

Schließlich muss der Plan bei Bedarf angepasst werden (z. B. Erneuerung von TLS-Zertifizierungen, DNS-Änderungen, Bearbeitung veralteter Secrets usw.). Kubernetes-Anwendungskomponenten müssen aktualisiert werden, um die neuen Speicherressourcen widerzuspiegeln, die im Rahmen der Wiederherstellung erstellt werden.

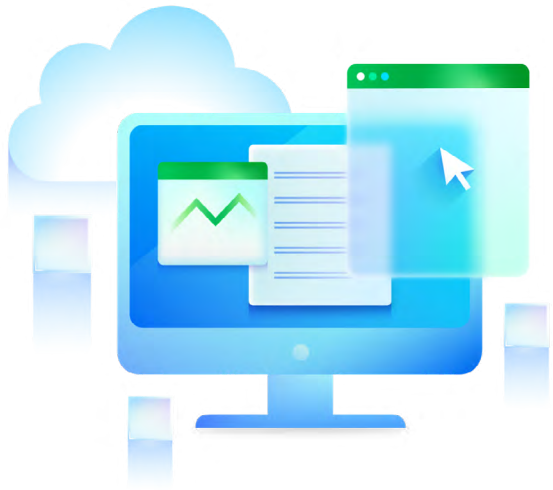
Sobald der Ausführungsplan vorhanden ist, muss die Backup-Plattform in der Lage sein, ihn in entsprechende Kubernetes-API-Aufrufe zu übersetzen, die für die Erstellung der erforderlichen Ressourcen nötig sind (z. B. Erstellung eines Lastausgleichs oder eines neuen Secrets). Dieser Prozess stellt sicher, dass alle erforderlichen Kubernetes-Ressourcen und Microservices, die eine cloudbasierte Anwendung umfassen, mit der ordnungsgemäßen Konfiguration erneut bereitgestellt werden. Das Diagramm unten veranschaulicht den komplexen Prozess der Wiederherstellung.

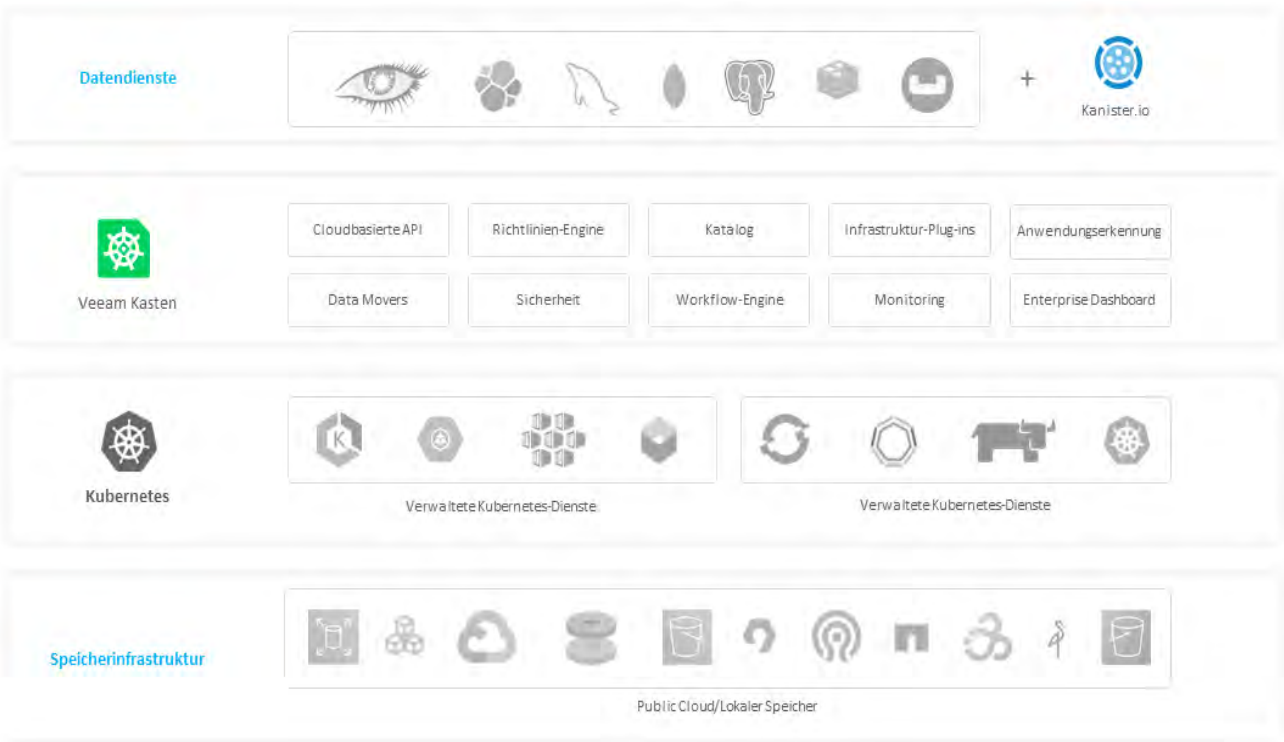


## 4.3 Betrieb

Operative Best Practices stellen in der Regel die größte Herausforderung für Unternehmen dar, insbesondere bei der Implementierung neuer Tools, Dienste und Funktionalitäten für eine äußerst dynamische Infrastruktur. Es sollte sichergestellt werden, dass eine auf Kubernetes basierende Backup-Plattform in großem Maßstab eingesetzt werden kann, Betriebsteams die erforderlichen Workflow-Funktionalitäten bietet und Compliance- und Monitoring-Anforderungen erfüllt. Ein weiterer wichtiger Aspekt sind die Auswirkungen — oder deren Fehlen — auf die Entwickler. Einer der größten Vorteile von Kubernetes besteht darin, dass es Entwicklern eine schnelle und einfache Möglichkeit bietet, Anwendungen bereitzustellen und Upgrades zu implementieren — und das in großem Maßstab. Wenn eine Backup-Plattform diese Anwendungsfälle behindert, werden Entwickler Wege finden, die eingerichteten Prozesse zu umgehen. Entwickler sollten keine Änderungen am Code, beim Erstellen von Paketen, an der Toolchain oder an der Bereitstellung vornehmen müssen. Gleichzeitig sollten die Bediener befähigt werden, Anwendungsentwicklern Self-Service-Funktionalitäten zur Verfügung stellen zu können, wie z. B. die Möglichkeit, ihre eigene Anwendung wiederherzustellen oder die Möglichkeit, den Backup-Betrieb für ihre Datenservices anzupassen und zu erweitern (z. B. Verwendung von benutzerdefinierten oder Datenbankanbieter-Tools, dienstübergreifende Koordinierung und Stilllegung usw.). Darüber hinaus müssen alle Interaktionen der Entwickler mit der Backup-Plattform über die API erfolgen können. Es ist daher von entscheidender Bedeutung, dass jede bereitgestellte Backup-Plattform die Anforderungen sowohl von Container Plattformbetriebsteams als auch von Entwicklern erfüllt.

Bediener sollten sich nicht um die unzähligen Kubernetes-Komponenten kümmern müssen, die zur Anwendung gehören. Die Backup-Richtlinien sollten zum einen vollständig automatisiert sein und zum anderen die Anwendung und keine einzelnen Ressourcen oder die Speicherinfrastruktur adressieren. Die Realisierung der Richtlinie zur konkreten Definition der zu schützenden Anwendungskomponenten sollte erst zum Zeitpunkt ihrer Ausführung erfolgen. So wird sichergestellt, dass alle Komponenten einer Anwendung, die sich rasant ändert, erfasst werden, ohne dass die Richtlinie danach manuell aktualisiert werden muss. In ähnlicher Weise müssen Backup Richtlinien breit angelegt und labelbasiert sein, damit sie neue Anwendungen automatisch erfassen, sobald sie bereitgestellt werden (z. B. Richtlinien, die mit allen Anwendungen übereinstimmen, die MongoDB verwenden oder über das helm Paketverwaltungstool bereitgestellt werden). Dieses Vorgehen erspart Betriebsteams nicht nur die Erstellung manueller Änderungskontrollprozesse, sondern sorgt auch dafür, dass bei der Erstellung und Zerstörung von Anwendungen im großen Maßstab weiterhin alle Compliance-Bedingungen für Backup-SLAs erfüllt werden.






## 4.4 Sicherheit

Sicherheit steht an bei jedem Produkt an erster Stelle, das in einer Produktivumgebung eines Unternehmens bereitgestellt wird. Dabei spielt es keine Rolle, ob dies in einer Public Cloud oder in einer lokalen Infrastruktur geschieht. Es müssen Kontrollmechanismen für Identitäts- und Zugriffsverwaltung und rollenbasierte Zugriffskontrolle (RBAC/Rollenbasierte Zugriffssteuerung) implementiert werden. RBAC/Rollenbasierte Zugriffssteuerung verleiht Benutzern und Gruppen bestimmte und oft eingeschränkte Benutzerrechte oder Zugriffsrechte auf die eigentliche Backup-Plattform. Dies ermöglicht es verschiedenen Personas innerhalb eines Betriebsteams, häufige Aufgaben wie z. B. Backup-Monitoring, Sicherstellung der erfolgreichen Backup-Integrität und Durchführung von angeforderten Wiederherstellungen bei so wenig privilegiertem Zugriff wie möglich zu erledigen. RBAC/Rollenbasierte Zugriffssteuerung ermöglicht auch Anwendungsszenarien wie die Erteilung von Entwicklerberechtigungen zur schnellen Wiederherstellung und zum Klonen von Snapshots, gewährt aber nur bestimmten Teammitgliedern Zugriff auf Backups, die an sekundären Speicherorten extern gespeichert sind.

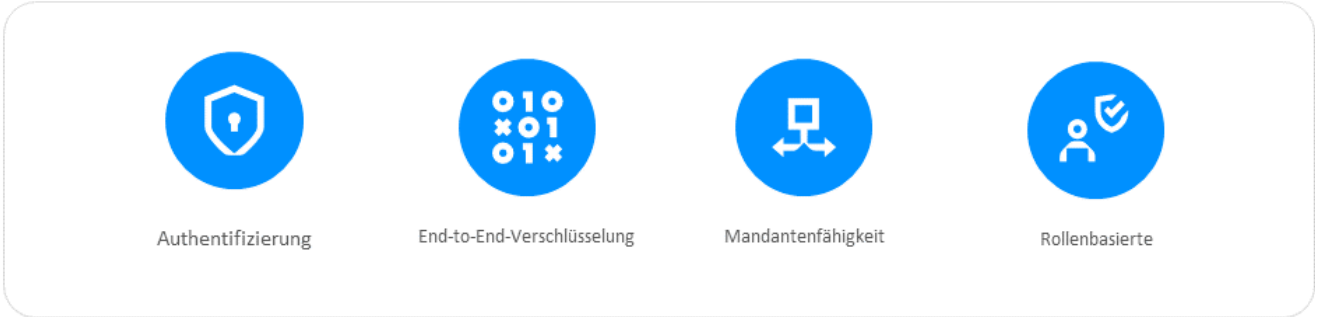
In einer Public Cloud muss eine cloudnative Backup-Plattform neben den oben beschriebenen Sicherheitsanforderungen auch umfassend in das Identity and Access Management (IAM), die Schlüsselverwaltungssysteme (KMS) und die Zertifikatsverwaltung der Cloud integriert werden. Darüber hinaus lässt sich ein echtes auf Kubernetes basierendes Datensicherungssystem in die Authentifizierungslösung des Cloud-Anbieters integrieren (z. B. ODIC, OAuth, Token-Auth. usw.) und dafür braucht es keine zusätzliche Benutzer- oder Gruppenverwaltung, keine neuen Tools oder APIs für RBAC-Richtlinien. Diese Features werden über eine Kubernetes-native CRD-basierte API verfügbar gemacht und sorgen so für eine gut strukturierte, cloudnative Backup-Plattform. Der letzte Aspekt der Sicherheit, der immer implementiert werden muss, ist die Verschlüsselung. Der Schutz der Daten ist von entscheidender Bedeutung, egal ob sie übertragen oder gespeichert werden. Sie müssen sicherstellen, dass die Daten sicher bleiben, sobald sie die Computing-Umgebung verlassen haben.

## 4.4.1 Verschlüsselung während der Übertragung

Beim Verschieben oder Kopieren von Daten zwischen Kubernetes-Clustern oder Speicherumgebungen muss sichergestellt werden, dass die Daten beim Verlassen eines Endpunkts und beim Ankommen an einem anderen verschlüsselt sind. Am Beispiel Objektspeicher: Eine lokale Kubernetes-Anwendungsbereitstellung, die Backups auf AWS S3 auslagern muss, überträgt die Daten normalerweise über eine externe Internetverbindung. Die Backup Plattform muss beim Kopieren über das Internet immer sicherstellen, dass die Daten mit bekannten Protokollen wie TLS verschlüsselt werden.

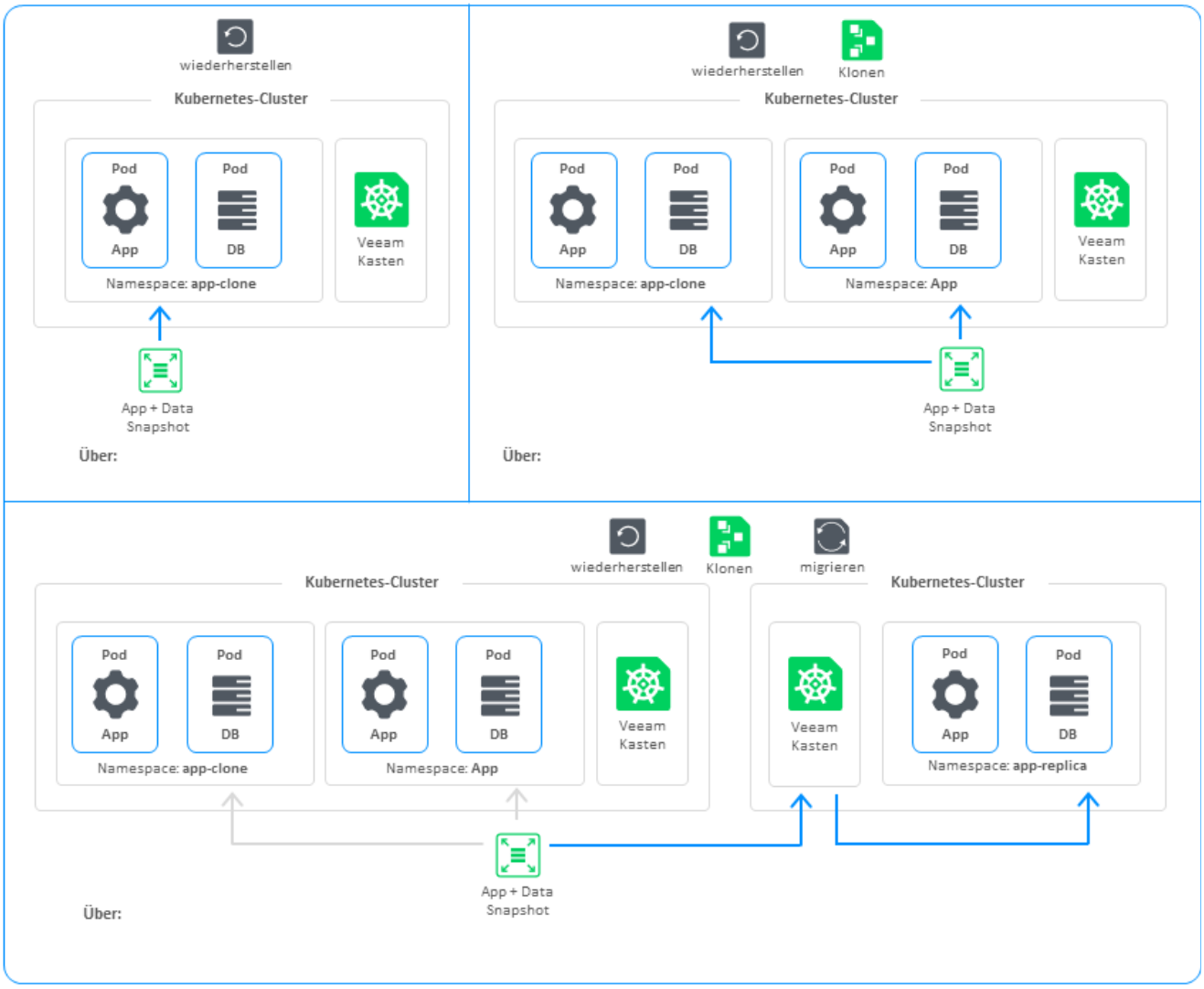
## 4.4.2 Verschlüsselung bei der Speicherung

Um beim obigen Beispiel zu bleiben: Wenn die Daten am Ende an einem Sekundärstandort gespeichert werden, ist es aus Sicherheitsaspekten absolut notwendig, dass diese Daten verschlüsselt sind. Das bloße Implementieren von RBAC/rollenbasierter Zugriffssteuerung und zugehörigen Sicherheitsregeln auf der Steuerungsebene reicht nicht aus, wenn die Daten bei der Speicherung nicht verschlüsselt sind. Die Verwendung bewährter Verschlüsselungsalgorithmen wie AES-256-GCM mit Verschlüsselungsschlüsseln pro Anwendung verhindert versehentliche Datenlecks oder sogar böswilliges Kopieren durch unseriöse Infrastrukturbetreiber oder böswillige externe Entitäten.



## 4.5 Mobilität

In den folgenden Diagrammen wird das leistungsstarke Feature der Plattformportierbarkeit veranschaulicht, das von Kubernetes angeboten wird. Mit diesem Feature kann eine Backup-Plattform eine breite Palette von Anwendungsfällen möglich machen. Hierzu gehört die Übertragung von Daten über Namespaces innerhalb desselben Clusters, über verschiedene Speichersysteme, über verschiedene Kubernetes-Cluster, -Distributionen und -Versionen. Es erstreckt sich auch auf Verfügbarkeitszonen innerhalb derselben Region, Überbrückung von Regionen innerhalb derselben Cloud, Verbindung von Cloud- oder Hybridumgebungen und sogar auf die Verknüpfung von Test- und Entwicklungsumgebungen.



Angesichts der vielfältigen lokalen und Cloud-Angebote von Kubernetes ist auch entscheidend, dass eine Lösung für Backup und Datenmanagement Kubernetes-Anwendungen über beliebige Quell- und Zielcluster migrieren kann, die auf stark heterogenen Infrastrukturen laufen können. Wenn Sie beispielsweise einen Workload von Amazon Elastic Kubernetes Service (Amazon EKS) zu Microsoft Azure Kubernetes Service (AKS) migrieren, sehen Sie in jedem Cluster Folgendes:

```
Art: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
       Name: gp2
Bereitsteller: kubernetes.io/aws-ebs
Parameter:
       Art: gp2
       fsTyp: ext4
```

```
Art: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
       Name: managed-premium-retain
Bereitsteller: kubernetes.io/azure-disk
reclaimPolicy:Aufbewahrungs-
parameter:
       storageaccounttype: Premium _ LRS
       Art: Verwaltet
```

Diese verschiedenen Speicherklassen sind nur die Spitze des Eisbergs, was die Unterschiede zwischen den Distributionen angeht, auch wenn diese Distributionen dabei auf der gleichen zugrunde liegenden Kubernetes-Version basieren. Es ist von entscheidender Bedeutung, dass eine Backup-Plattform zuverlässig über verschiedene Distributionen und Infrastrukturen hinweg wiederherstellen und Anwendungs-Backups gleichzeitig automatisch an die neue Wiederherstellungsumgebung anpassen kann.

Bei der Migration von Workloads über Namespaces, Cluster, Regionen und sogar Kubernetes-Distributionen muss eine zuverlässige Backup-Plattform in der Lage sein, alle Abhängigkeiten zwischen Anwendungen zu verstehen und für alle Umgebungen zu übersetzen. Ähnlich wie bei der Planung und Durchführung einer Wiederherstellung in einer cloudbasierten Umgebung ist ein Migrationsplan erforderlich. Dieser muss sicherstellen, dass die Infrastruktur (z. B. Lastausgleich) und clusterweite Abhängigkeiten zwischen Anwendungen verfügbar sind oder in gleichwertige Ressourcen transformiert werden — so realisieren Sie eine erfolgreiche Migration. Nicht nur Container und Speicher-Volumes müssen migriert werden, sondern es müssen auch FQDNs, Secrets und DNS-Adressen bei einer Migration während der Übertragung geändert werden.

# Kapitel 5. Fazit

Im vorherigen Abschnitt wurden die wichtigsten Anforderungen und Empfehlungen für die Implementierung einer Kubernetes Backup-Lösung beleuchtet. Sie lassen sich in folgenden fünf Best Practices zusammenfassen:

**Architektur**

Die zum Schutz von Kubernetes-Anwendungen verwendete Plattform muss automatisch alle Anwendungskomponenten erkennen, die in Ihrem Cluster ausgeführt werden, und dabei die Anwendung als Unit of Atomicity behandeln. Die Anwendung muss den Status bezüglich Speicher-Volumes, Datenbanken (NoSQL/relational) sowie Konfigurationsdaten in Kubernetes-Objekten wie ConfigMaps und Secrets umfassen.

**Wiederherstellbarkeit**

Die Plattformen für die Datensicherung müssen es Ihnen ermöglichen, die gewünschten Anwendungskomponenten am gewünschten Ort wiederherzustellen. Sie sollten zudem über die erforderliche Kontrolle bei der Granularität verfügen, nur bestimmte Anwendungen wiederherstellen zu können, z. B. das Datenvolumen. Der Ansatz muss die Wiederherstellung einfach und leistungsstark machen, indem Sie auch die entsprechende Point-of-Time-Kopie der Anwendung auswählen können.

**Betrieb**

Es sollte sichergestellt werden, dass eine Kubernetes native Backup-Plattform in großem Maßstab eingesetzt werden kann, Betriebsteams die Workflow-Funktionalitäten bietet, die sie benötigen, und Compliance und Monitoring Anforderungen erfüllt. Bediener sollten Anwendungsentwicklern Self-Service-Funktionalitäten zur Verfügung stellen können, ohne dass dafür den Anwendungscode oder die Bereitstellung ändern zu müssen.

**Sicherheit**

Es müssen Kontrollmechanismen für Identitäts- und Zugriffsverwaltung und rollenbasierte Zugriffskontrolle (RBAC/Rollenbasierte Zugriffssteuerung) implementiert werden. RBAC/Rollenbasierte Zugriffssteuerung ermöglicht es verschiedenen Personas innerhalb eines Betriebsteams, häufige Aufgaben wie Monitoring bei geringstmöglichem Zugriff zu erledigen. Verschlüsselung bei der Speicherung und während der Übertragung müssen stets implementiert werden, um sicherzustellen, dass die Daten sicher bleiben, wenn sie die Compute-Umgebung verlassen haben.

**Anwendungsmobilität**

In einer Multi-Hybrid-Cloud-Welt muss eine cloudbasierte Plattform zur Datensicherung mehrere Distributionen flexibel unterstützen können und Funktionalitäten bieten, die eine Mobilität von Workloads und Anwendungen über alle unterschiedlichen Umgebungen hinweg ermöglichen. Mobilitätsfunktionalitäten sind für verschiedene Anwendungsszenarien erforderlich, darunter die Wiederherstellung von Anwendungen, das Klonen und die Migration von Containern. Wenn Sie sich an die Best Practices in dieser Anleitung halten, können Sie Ihren Kunden ein konsistentes und zuverlässiges Angebot bieten, wenn es zu Datenverlust oder -korruption oder sogar zu einem kompletten Ausfall kommt.

Veeam ist eindeutiger Marktführer für Backup-Lösungen für virtualisierte Workloads. Angesichts des fortschreitenden Wachstums von Kubernetes-Anwendungen und -Bereitstellungen bietet Veeam Kasten für Kubernetes die beste Datensicherung und Mobilitätslösung für die Anforderungen, die Unternehmen an eine cloudbasierte Datensicherung stellen. Die Veeam Kasten-Plattform zur Datensicherung wurde speziell für Kubernetes entwickelt und bietet Backup, Wiederherstellung, Disaster Recovery, Mobilität der Anwendung und Ransomware-Schutz für Ihre gesamte Kubernetes-Anwendung unter Berücksichtigung der oben hervorgehobenen Best Practices.

## Veeam Kasten für Kubernetes

Mit der zentralen Plattform von Veeam können Unternehmen ihre Backups modernisieren, den Umstieg auf die Hybrid Cloud beschleunigen und ihre Daten schützen. Unsere Lösungen lassen sich einfach installieren und ausführen, passen sich flexibel in jede Umgebung ein und sind stets zuverlässig. Die größten Unternehmen weltweit vertrauen auf Veeam Kasten. Es bietet sichere, auf Kubernetes basierende Datensicherung und Mobilität von Anwendungen in großem Maßstab und über eine Vielzahl von Distributionen und Plattformen hinweg. Veeam Kasten ist nachweislich in der Lage, ganze Anwendungen schnell und zuverlässig wiederherzustellen und gibt den Betriebs- und App-Teams die Gewissheit, unerwartete Situationen bewältigen zu können.

**Weitere Informationen finden Sie unter:**
veeam.com/kubernetes-native-backup-and-re store

### Über Veeam Software

Veeam®, der Weltmarktführer im Bereich Datenresilienz, ist der Ansicht, dass jedes Unternehmen nach einer Unterbrechung des Geschäftsbetriebs in der Lage dazu sein sollte, den Betrieb mit Gewissheit und der Kontrolle über alle seine Daten wieder aufzunehmen, wann und wo immer diese benötigt werden. Veeam nennt dies maximale Ausfallsicherheit und wir arbeiten kontinuierlich daran, innovative Lösungen zu entwickeln, mit denen unsere Kunden diese Zielvorgabe erreichen. Veeam-Lösungen wurden speziell für die Datenresilienz entwickelt, indem sie Daten-Backup, Datenwiederherstellung, Datenfreiheit, Datensicherheit und Datenintelligenz bereitstellen. Mit Veeam können Verantwortliche im IT- und Sicherheitsbereich darauf vertrauen, dass ihre Anwendungen und Daten in allen Umgebungen in der Cloud, in virtuellen, physischen, SaaS und Kubernetes sicher und jederzeit verfügbar sind. Veeam hat seinen Hauptsitz in Seattle und ist mit Niederlassungen in mehr als 30 Ländern vertreten. Weltweit hat Veeam mehr als 550.000 Kunden, darunter 74 % der Global 2000-Unternehmen, die auf Veeam vertrauen, um einen zuverlässigen Geschäftsbetrieb zu gewährleisten. Maximale Ausfallsicherheit beginnt mit Veeam. Erfahren Sie mehr unter www.veeam.com/de oder folgen Sie Veeam auf LinkedIn @veeam-software und X @veeam.