Hewlett Packard Enterprise

Broschüre

SCHÜTZEN SIE IHRE CONTAINER MIT HPE UND KASTEN K10 VON VEEAM

Flexibler, granularer und hybrider Schutz für Container der Enterprise-Klasse

WAS FÖRDERT DIE ANNAHME VON CONTAINERN?

Die Annahme der Containertechnologie nimmt in überraschendem Maße zu.[1]
Diese Zunahme begründet sich mit der Einfachheit, mit der containerisierte Anwendungen portiert und in verschiedenen Umgebungen eingesetzt werden können. Container verpacken die Anwendungen mit nahezu allem, was sie zur Ausführung benötigen (Konfigurationsdateien, Abhängigkeiten usw.), und isolieren sie für die Bereitstellungsumgebung, wodurch containerisierte Anwendungen problemlos in einer Vielzahl von Umgebungen ausgeführt werden können: lokale Desktops, virtuelle und physische Server, Entwicklungs-, Test- und Produktionsumgebungen sowie private oder öffentliche Clouds.

Ein weiterer Vorteil von Containern ist, dass physische Server eine größere Anzahl von ihnen als virtuelle Maschinen hosten können. Da jeder Container den Zugriff auf den Betriebssystemkern des Hosts teilt, benötigt er viel weniger Platz als eine entsprechende virtuelle Maschine auf einem physischen Server. Die Durchschnittsgröße eines Containers liegt unter einhundert Megabytes, virtuelle Maschinen haben leicht eine Größe, die in Gigabytes gemessen wird.

Schließlich haben sich Anwendungsfälle für Container auf die künstliche Intelligenz (KI) und Analyseanwendungen ausgeweitet. Container werden zum Standard für die Erstellung und Bereitstellung von Modellen für maschinelles Lernen (ML), die Erstellung von Echtzeit-Analyse-Pipelines und die Ausführung von Batch-Analysen und ETL-Aufgaben (Extrahieren, Transformieren, Laden). Ihre Portierbarkeit über verschiedene Umgebungen hinweg macht Container zum perfekten Vehikel für die Verwaltung des gesamten Lebenszyklus von KI-/ML-Modellen und im Übrigen fast jeder Analyseanwendung. Durch die massive Annahme von Containern für Anaytik und KL-/MI-Anwendungen entsteht ein Bedarf an zustandsabhängigen Anwendungen, die große Datenmengen nutzen und generieren und daher persistenten Datenspeicher benötigen.

Warum müssen containerisierte Anwendungen geschützt werden?
Es gibt viele Anwendungsfälle für die Sicherung und Wiederherstellung von Container-Umgebungen wie Kubernetes und den damit verbundenen Anwendungen:

- Wiederherstellung von zustandsabhängigen Anwendungen von Ausfällen bis zu Katastrophen
- Replikation zur Schaffung einer neuen Entwicklungsinitiative oder der Migration zwischen Test/Dev und Produktion
- Der Schutz beginnt vor den Tätigkeiten des Container-Lebenszyklus
- Einfache Konsolidierung von Container-Clustern zur Verringerung der Ausbreitung von Clustern

Anforderungen des Containerschutzes
Die Herausforderung beim Schutz von containerisierten Anwendungen besteht in der Verwaltung ihrer dynamischen Bereitstellung. Eine vollständige Lösung muss die folgenden Aufgaben übernehmen:

- **Implementierung nahtloser Betriebsabläufe und Richtlinien in lokalen und Cloud-Umgebungen.** Die Bereitstellung von Containern kann On-Premises, die Cloud und sogar Multicloud-Umgebungen umfassen. Sicherung und Wiederherstellungsvorgänge müssen diese Flexibilität reflektieren.
- **Sicherung und Wiederherstellung auf der Ebene eines einzelnen Containers (und seiner Daten).** Es liegt in der Natur der Sache, dass Container nicht mit physischen Servern oder virtuellen Maschinen verbunden sind. Der Schutz muss anwendungsorientiert sein und alle Teilkomponenten der Anwendung (Daten und Metadaten) erfassen, um eine Wiederherstellung zu ermöglichen.
- **Beibehaltung der Schutzgranularität.** Kubernetes-Cluster müssen mit verschiedenen Granularitätsebenen gesichert werden können, einschließlich Cluster-, Namespace-, Label-Selector-, Anwendungs- und Persistent-Volume-Ebene.
- **Automatische Wiederherstellung.** Für die Verwaltung großer Containerumgebungen muss eine Komplettlösung die vollautomatische Wiederherstellung von Anwendungen beinhalten.
- **Ausführung datenorientierter Aufgaben.** Eine Lösung muss branchenübliche Container Storage Interface (CSI)-Treiber, wie den HPE CSI-Treiber für Kubernetes, nutzen, um dynamische Bereitstellung, Snapshots, Klone und Wiederherstellungen durchzuführen.

INTELLIGENTEN, SICH SELBST REGELNDEN DATENSPEICHER MIT HPE NIMBLE STORAGE GENIESSEN

Sammeln Sie neue Erfahrungen beim Datenspeicher – mit einer agilen, schnellen und stets betriebsbereiten Plattform, die alles von VMs über Container bis hin zu Test- und Entwicklungsumgebungen unterstützt und ohne großen Aufwand auch in der Hybrid Cloud eingesetzt werden kann. **Es ist Zeit zum Umsteigen**.

[1] Best Practices for Running Containers and Kubernetes in Production [Best Practices für die Verwendung von Containern und Kubernetes in der Produktion], Gartner, August 2020

Wie HPE und Kasten von Veeam die Anforderungen an den Schutz von Kubernetes Clustern erfüllen
Einem neuen Bericht von Grand View Research, Inc. und anderen Analyseunternehmen zufolge wird der globale Markt für Containeranwendungen bis 2025 voraussichtlich 8,2 Milliarden US-Dollar erreichen und im Prognosezeitraum eine durchschnittliche jährliche Wachstumsrate von 26,5 % verzeichnen.

Topgründe für den Schutz von Containern:
- Wiederherstellung von zustandsabhängigen Anwendungen von Ausfällen bis zu Katastrophen
- Replikation der Umgebung für die Migration einer Test/Dev-Umgebung zur Produktion oder von der Produktion zur Bereitstellung vor einer Aktualisierung
- Einfache Migration von Container-Clustern

Hauptanforderungen für eine Lösung für den Containerschutz:
- Public Cloud und On-Premises sind abgedeckt
- Schutz auf Anwendungsebene
- Automatische Richtlinien
- Hoher Grad an Sicherheit

Die HPE und Kasten von Veeam Lösung für den Containerschutz:
- Vollständige Prüfung, Validierung und Optimierung
- Maximaler Grad an Flexibilität und Granularität für Sicherung und Wiederherstellung von Containern
- Einsatz und Verwaltung in hybriden Umgebungen (Public Cloud und On-Premises)
- Schrittweite Bereitstellung für den Conatinerschutz

HPE UND KASTEN K10 VON VEEAM LÖSUNG

Kasten K10 von Veeam bietet Betriebsteams in großen Unternehmen ein einfach zu bedienendes, skalierbares und sicheres System für Sicherung/Wiederherstellung, Disaster Recovery und Anwendungsmobilität.

Die Kombination aus HPE Datenspeicher und der Kasten K10 von Veeam Plattform bietet End-to-End-Schutz für Kubernetes-Cluster der Enterprise-Klasse, um Container zu sichern, wo immer sie sich befinden (On-Premises, in der Cloud oder hybrid), und sie wiederherzustellen, wo immer sie benötigt werden. Mit dem HPE Complete-Programm bietet Hewlett Packard Enterprise validierte, sofort nutzbare Sicherungs- und Wiederherstellungslösungen aus einer Hand an, die das Risiko reduzieren, die Wiederherstellungsbereitschaft verbessern und gleichzeitig Ihre Daten schützen.

Diese Lösung zum Schutz containerisierter Anwendungen umfasst HPE Hardware, HPE CSI Driver für Kubernetes und Kasten K10 von Veeam Software.

HPE Storage
Die HPE Datenschutzlösung für Kubernetes Cluster enthält diese wichtigen Hardwarekomponenten:

- **HPE Alletra,** eine cloud-native Dateninfrastruktur, hilft den IT-Fachkräften beim Umstieg von ihrer eigenen, von ihnen gewarteten Dateninfrastruktur auf den einfachen Zugriff und die Nutzung der Infrastruktur On-Demand und as-a-Service. HPE Alletra wurde sowohl für traditionelle als auch moderne Anwendungen entwickelt und deckt Workload-optimierte Systeme ab, um hohe architektonische Flexibilität ohne die Komplexität des traditionellen Datenspeichermanagements sicherzustellen. Durch die neue Mobilität von Daten über Clouds hinweg wird das wahre Potenzial der Hybrid Cloud endlich freigesetzt.
- **HPE Primera** bietet die Agilität der Cloud und setzt neue Maßstäbe bei Ausfallsicherheit und Leistung. Durch die integrierte Ausfallsicherheit und unterstützt durch HPE InfoSight ermöglicht es sofortigen Zugriff auf Daten mit einem Datenspeicher, der sich in wenigen Minuten einrichten und transparent aktualisieren lässt sowie as-a-Service bereitgestellt wird.
- **HPE Nimble Storage** kombiniert ein zuverlässiges Systemdesign mit Predictive Analytics, um die höchste gemessene Verfügbarkeit in der Speicherbranche zu erzielen und erstklassigen Support zu bieten. Da Predictive Analytics von Anfang an in die Kernarchitektur integriert ist, kann die Infrastruktur lernen, unabhängig davon, wie lange sie bereits im Einsatz ist.
- **HPE Nimble Storage dHCI** ist eine intelligente Plattform mit der Flexibilität einer konvergenten Infrastruktur und der Einfachheit einer hyperkonvergenten Infrastruktur (HCI). Es disaggregiert Computing und Datenspeicher und integriert hyperkonvergente Steuerung, um Unternehmen die einfache Verwaltung der Infrastruktur in einer flexiblen Architektur zu bieten. Diese Plattform wird mit einem der weltweit sichersten Server, dem HPE ProLiant, und dem sich selbst regelnden Flash-Datenspeicher HPE Nimble Storage erstellt. Sie bietet die Flexibilität, um Rechenleistung und Datenspeicher unabhängig für nicht vorherzusehendes Wachstum und die für geschäftskritische Anwendungen erforderliche Datenresilienz und Leistung zu skalieren.
- **HPE Apollo 4000 Systems mit Scality RING Scalable Storage** ist eine skalierbare, softwaredefinierte Speicherplattform, die auf HPE Apollo 4000 Servern läuft und eine Option für ein Sicherungsziel bietet. Es wurde für Umgebungen mit Mehrfachanwendungen entwickelt, das unstrukturierte Daten in Petabyte-Größe speichern muss.

HPE CSI Driver für Kubernetes
Der HPE CSI-Treiber für Kubernetes ermöglicht die Verwendung eines Container-Storage-Providers (CSP) zur Durchführung von Datenmanagement-Vorgängen auf Speicherressourcen. Die Architektur des CSI-Treibers ermöglicht es Anbietern von Blockspeichern, einen CSP zu implementieren, der der Spezifikation entspricht. Der CSI-Treiber unterstützt das HPE Primärspeicher-Portfolio.

Kasten K10 von Veeam Software
Kasten K10 von Veeam ist eine echte Kubernetes-native Sicherungslösung, die cloud-native Anwendungen und geschäftskritische Daten schützt. Es erfasst und schützt automatisch einen gesamten Anwendungsstapel, einschließlich Ressourcendefinitionen, Konfigurationen und zugrunde liegender Daten. Durch dynamische Richtlinien, die für eigens entdeckte Anwendungen gelten, können Sicherungen im großen Maßstab gemanagt werden. Wenn der Schutz auf Volume-Ebene nicht ausreicht, kann der Workflow um einem Kanister-Blueprint erweitert werden, um anwendungsspezifische Vorgänge anzuwenden. Kasten K10 von Veeam bietet automatisierte Richtlinien, wie Sicherungen an Außenstellen sicher repliziert werden können. Mit widerstandsfähigen, geplanten und On-Demand-Workflows ist die Disaster Recovery für Anwendungen aktiviert.

Mit Kasten K10 von Veeam können ganze Anwendungen zwischen Clouds und On-Premises für Test/Dev, Lastausgleiche und Aktualisierungen bewegt werden. Da keine benutzerdefinierte Skripterstellung erforderlich ist, können Anwendungen mit robusten geplanten und On-Demand Workflows und über Public oder Private Cloud-Infrastrukturen mit nahtloser Datenkonvertierung zwischen Infrastrukturformaten migriert werden. Für eine verbesserte Umgebungsisolation und betriebliche Kontrolle kann die Migration zwischen nicht föderierten Clustern erfolgen. Wenn die Kubernetes-Cluster, die auf HPE Nimble Storage dHCI laufen, Volume-Snapshots und Klone erstellen, orchestriert Kasten K10 von Veeam das Senden von Kopien der Snapshots an das HPE Apollo System mit Scality RING Scalable Storage Sicherungszielen.

FAZIT

Container Plattformen der Enterprise-Klasse bleiben uns erhalten. Die gemeinschaftliche HPE und Kasten K10 von Veeam Lösung zum Schutz containerisierter Anwendungen bietet einzigartige Vorteile:

- Vollständige Prüfung, Validierung und Optimierung
- Maximale Flexibilität und Granularität für Container-Sicherung und -Wiederherstellung
- Einsatz und Verwaltung in hybriden Umgebungen (Public Cloud und On-Premises)

Hewlett Packard Enterprise

© Copyright 2022 Hewlett Packard Enterprise Development LP. Änderungen vorbehalten. Die Garantien für Hewlett Packard Enterprise Produkte und Services werden ausschließlich in der entsprechenden zum Produkt oder Service gehörigen Garantieerklärung beschrieben. Aus dem vorliegenden Dokument sind keine weiterreichenden Garantieansprüche abzuleiten. Hewlett Packard Enterprise haftet nicht für technische oder redaktionelle Fehler oder Auslassungen in diesem Dokument.

a00114798DEE, Rev. 1