Der Aufstieg von Kubernetes und die wachsenden Herausforderungen für die Datensicherung

Container gibt es zwar schon seit den 1970er Jahren, aber erst 2013 machte die Software-Firma Docker den Container-Ansatz so richtig populär. Mittlerweile haben Container-Lösungen wie Kubernetes die Art und Weise, wie Anwendungen entwickelt, verwaltet und bereitgestellt werden, grundlegend verändert. Sie ermöglichen es Entwicklern, sich ausschließlich auf die Software-Erstellung und die Bereitstellung von Anwendungen zu konzentrieren. Es ist keine Übertreibung zu sagen, dass Container die Softwareentwicklung revolutioniert haben.

Entscheidet sich ein Unternehmen für den Einsatz von Container-Lösungen, muss es aber auf jeden Fall auch die Datensicherung berücksichtigen. Warum das so ist wird klar, wenn man sich anschaut, was Container sind und wie sie eingesetzt werden. Ein Container ist eine Anwendung, die alle ihre Abhängigkeiten, Bibliotheken und Konfigurationsdateien in einem einzigen Paket bündelt. Diese Bündelung erleichtert das Aufsetzen neuer Container-Instanzen und das nahtlose Verschieben dieser Container von einer Rechenumgebung in eine andere.

Das ist in vielerlei Hinsicht vorteilhaft. Container werden typischerweise dann eingesetzt, wenn Entwickler eine Anwendung von einer Testumgebung, wie z.B. ihrem Laptop, in eine Produktionsumgebung verschieben wollen. Der Einsatz ist auch üblich, wenn von einer physischen Maschine auf eine cloud-basierte virtuelle Maschine migriert wird.

Container sind in vielen verschiedenen Szenarien sehr vorteilhaft, da sie nicht durch Unterschiede in Betriebssystemen, Softwareversionen usw. ausgebremst werden. In der Tat sind sie extrem flexibel und portabel, was sie zu einer natürlichen Ergänzung für viele Cloud-Anwendungen macht. Da sich Computing und Storage sehr stark in die Cloud verlagert haben, werden Container künftig zu einer unverzichtbaren Technologie für jedes moderne Unternehmen.

Container und die Datensicherheit

Doch während Container-Orchestrierungstools wie Kubernetes aufgrund ihrer Skalierbarkeit und Portabilität praktisch sind, können sie bei der Datensicherheit zu Problemen führen. Das hat gleich mehrere Gründe. Zunächst einmal ist eine Kubernetes-Architektur außergewöhnlich dynamisch.

Container werden schnell auf- und ebenso schnell wieder abgebaut, je nach den Zielen und Spezifikationen der Entwickler. Das bedeutet, dass Container im Wesentlichen temporär sind und eine relativ kurze Lebensdauer haben. Mit der Einführung von Containern in immer mehr Unternehmen wird daher die Datensicherheit zu einem immer wichtigeren Thema. Eine wachsende Anzahl von Unternehmen, die Container in ihrer Testumgebung einsetzen, stellt fest, dass während dieser Migration und Bereitstellung unerwartete Dinge mit den Daten passieren können. Eine ordnungsgemäße Datensicherung ist deshalb von besonderer Bedeutung und wird in den kommenden Monaten und Jahren noch wichtiger werden.

Mehr Container bedeuten mehr Daten

Je mehr Unternehmen Container einsetzen, desto mehr Daten werden erzeugt, die gesichert und gespeichert werden müssen. Da Container in der Regel zu Test- und Entwicklungszwecken eingesetzt werden, ist ihre Lebensdauer zumeist kürzer als die Lebensdauer der von ihnen erzeugten Daten. So müssten beispielsweise aus Compliance-Gründen diese Daten auch dann noch gespeichert und geschützt werden, wenn ein bestimmter Container längst außer Betrieb genommen oder zerstört wurde.

Auch gilt zu beachten, dass die Sicherung von Container-Daten kein zeitbasierter Prozess ist, bei dem die Daten alle paar Minuten oder Stunden gesichert werden. Bei Containern ist die Sicherung eher ereignisgesteuert. Wird zum Beispiel ein neuer Container erstellt und nicht das gewünschte Ergebnis erzielt, sollte der Administrator die Möglichkeit haben, schnell zum vorherigen Zustand zurückkehren zu können. An diesem Punkt wird also ein Backup benötigt. Aus all diesen Gründen ist das Backup von Containern ein immer wichtigeres Thema. Obwohl Container so konzipiert sind, dass sie nur dann existieren, wenn sie gebraucht werden, müssen Containerdaten länger erhalten bleiben und letztlich geschützt werden.

Container mit der Datensicherung in Einklang bringen

Unternehmen müssen gleich mehrere Maßnahmen ergreifen, um sicherzustellen, dass ihre Containerdaten erfolgreich gespeichert werden. Zunächst ist es wichtig, die Datenanforderungen für jede einzelne Container-Anwendung zu bewerten. Unternehmen sollten auch sicherstellen, dass es Protokolle gibt, die verhindern, dass Containerdaten unnötig überschrieben werden. Außerdem müssen sich Unternehmen über die Sicherheits- und Zugriffsanforderungen jedes Containers in ihrer Umgebung im Klaren sein.

Die Containerisierung hat der Anwendungsentwicklung einen deutlichen Schub gegeben. Aber Unternehmen müssen sich dabei ernsthafte Gedanken über die Speicherung, Sicherung und den Schutz ihrer Daten machen. Wenn sie das Problem der Datensicherung direkt angehen, können sie die vielen Vorteile der Container-basierten Entwicklung durchaus nutzen und zuversichtlich in die Zukunft blicken.