Bild: Fotolia

Dossier
Hybrid Cloud

In Kooperation mit **Netapp**

Die Cloud für die Zukunft rüsten

gsa. Die Cloud wird erwachsen, die Phase der Early Adopters ist vorüber. Nach Erhebungen der Synergy Research Group kletterte der Gesamtumsatz der führenden Anbieter im Segment Private and Hybrid Cloud im Verlauf eines Jahres um 45 Prozent. Wichtige Treiber sind die Digitalisierung von Geschäftsprozessen und Megatrends wie Big Data/Analytics und Mobile. Immer mehr Daten werden generiert, bearbeitet und verwaltet. Einige liegen im Rechenzentrum des Unternehmens, andere auf den Servern öffentlicher Cloud-Dienste. Das steigert die Anforderungen an die Architektur. Dank Storage-Trends wie «Flash statt Festplatten» im primären Storage und «Back-up-to-Disk statt Tape» wird die Geschwindigkeit, mit der Workloads verarbeitet werden, in den nächsten Jahren deutlich steigen. Es steigen aber auch die Erwartungen an IT-Verantwortliche. Anwender im Business und Kunden wollen auf Daten umgehend zugreifen können. Technologien wie Deduplizierung, optimiertes Loadbalancing und moderne Datenverschlüsselung sind praktische Lösungen. Doch wer in den nächsten Jahren mit den Entwicklungen im Cloud Computing Schritt halten möchte, sollte ein ganzheitliches Konzept entwickeln – wie das der Data Fabric. Sie ermöglicht CIOs, Architekturen aufzubauen, die heterogene Cloud-Dienste nahtlos integrieren, das Management von Daten vereinfacht und die Sicherheit nicht vernachlässigt.

Datenmanagement und -kontrolle in hybriden Cloud-Umgebungen

Im Hinblick auf die Datensicherung ist Vertrauen zentral, besonders wenn diese ausgelagert wird. Beim Thema Datensicherung besteht jedoch nach wie vor eine gewisse Risikobereitschaft. Viele Unternehmen weisen eine hohe Abhängigkeit von ihren operativen Daten aus. Ohne diese Daten könnten viele Organisationen ihre Prozesse nicht mehr in der gewohnten Art und Weise weiterführen. Ein möglicher Weg führt dabei in die Cloud.

DER AUTOR

Christoph Schnidrig
Leiter Systems Engineering, Netapp

Die Zeiten sind vorbei, in denen sich IT-Abteilungen nur auf ihre eigenen Rechenzentren für die Bereitstellung von Services konzentriert haben. Heute existiert eine grosse Zahl von Möglichkeiten bei der Wahl von Services. Oftmals stellt sich auch die Frage: make or buy? Die Wahlfreiheit bietet viele Vorteile. Einerseits ist die überaus einfache Skalierbarkeit zu erwähnen, die es ermöglicht, dass zu jedem Zeitpunkt lediglich die wirklich genutzten Ressourcen im Zugriff sind. Entsprechend fällt eine kostspielige Überdimensionierung komplett weg, und Spitzenzeiten müssen nicht mehr im Vorfeld eingeplant werden. Andererseits können geplante und nicht geplante Ausfallzeiten verringert werden.

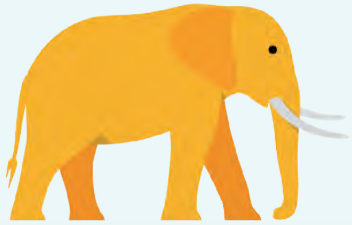
Da die Infrastrukturen von Cloud-Umgebungen in höchstem Masse standardisiert und automatisiert werden, bleibt eine Grosszahl von menschlichen Fehlern aus. Darüber hinaus können die Infrastrukturen solcher Cloud-Umgebungen vollständig transparent gewartet werden. Ein weiterer Vorteil, der durch die wachsende Anzahl der Serviceanbieter entsteht, sind Preisoptimierungen. Infolgedessen findet ein rascher Wandel der IT-Landschaften zu gemischten – eben hybriden – Umgebungen statt. Dabei wandeln sich die internen IT-Abteilungen von reinen Leistungserbringern zu Brokern von IT-Services – von den eigenen und den extern eingekauften.

Herausforderung bei der Verwaltung von Daten in hybriden Cloud-Umgebungen

Während der Wille und der Trend zur verstärkten Nutzung von Hybrid Clouds gegeben ist, entstehen in der Praxis Herausforderungen sowie Probleme bei der Umsetzung. Zum einen gibt es enorme Probleme beim Datenmanagement, wenn Daten im lokalen Rechenzentrum und in der Cloud gespeichert werden. Insbesondere das Verschieben von Daten – liegen doch die allermeisten Daten noch ausserhalb der Cloud – ist zeitaufwändig und komplex. Dazu kommt, dass verschiedene Cloud-Anbieter unterschiedliche und oftmals inkompatible Plattformen betreiben. Daten haben nur dann einen Wert, wenn sie zum richtigen Zeitpunkt am richtigen Ort verfügbar sind. Des Weiteren muss sichergestellt werden, dass alle Daten entsprechend gesichert werden. Aktuelle Fälle von Cloud-Service-Providern, die ihren Dienst kündigen und den Kunden lediglich ein paar Wochen für das Kopieren von Daten gewähren, zeigen die Wichtigkeit auf, Daten jederzeit gesichert zu haben. Zum anderen ergeben sich unterschiedliche Kombinationen von Infrastruktur, Rechen- und Storage-Ressourcen in der Cloud und im eigenen Rechenzentrum (RZ). Daten in dieser Ressourcenmischung zu speichern und zu verwalten, ist eine sehr grosse Herausforderung. In hybriden Clouds können Rechenleistungen oder Applikationen relativ einfach auslagert werden. Sobald diese jedoch Daten generieren, sind die Sicherung und Kontrolle problematisch. Daraus resultiert ein Mangel an Kontrolle, wenn die Daten aus dem eigenen RZ weg sind. Zwangsläufig rücken Themen wie Datensicherheit, Daten Governance und die anbieterabhängigen Service Level ins Zentrum der Überlegungen.

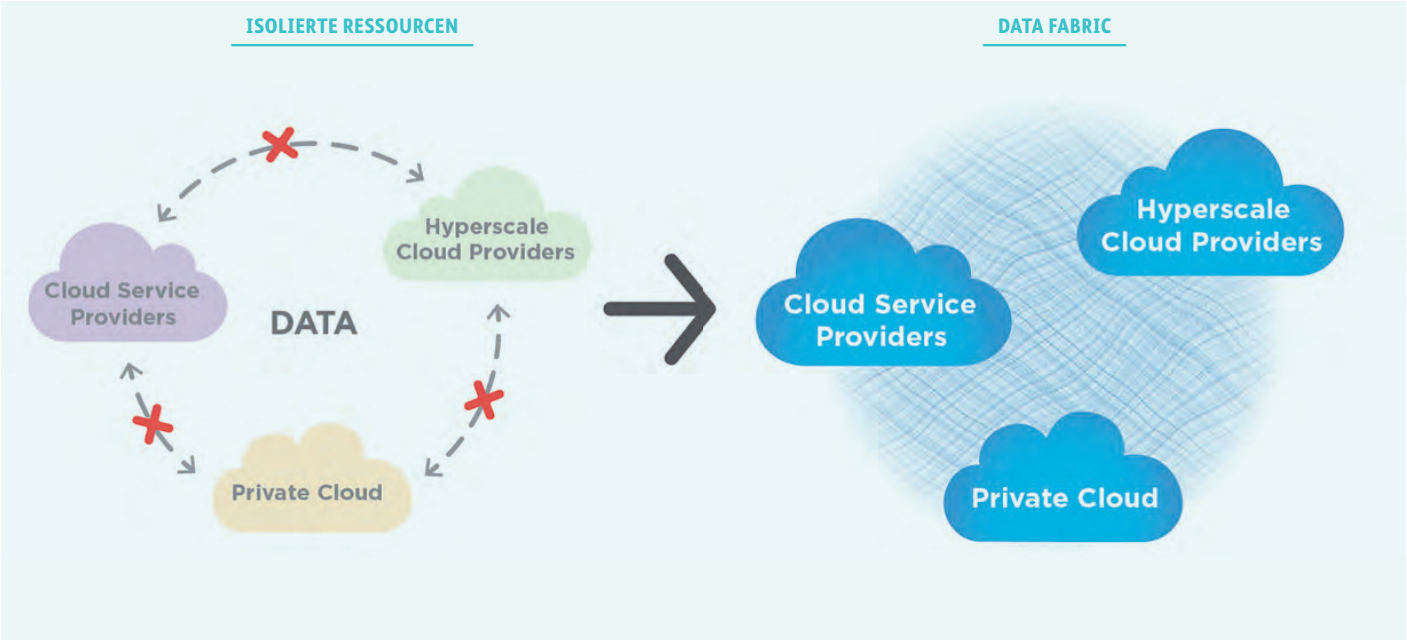
RECHENRESSOURCEN SIND AGIL. DATEN NICHT.

Daten haben nur dann einen Wert, wenn sie zum richtigen Zeitpunkt am richtigen Ort verfügbar sind. Daten lassen sich aber nicht so agil handhaben wie Compute-Leistung.



Data

Compute



Eine Data Fabric für eine nahtlose Integration von Hybrid Clouds

Damit diesen Herausforderungen begegnet werden kann, braucht es ein einheitliches Rechenzentrum und ein überspannendes Datenmanagement. Unabhängig davon, wo gerade Daten für Testzwecke geklont, gesichert oder restored werden müssen, sollen dieselben Prozesse und Tools greifen. Die gewonnene Effizienz in der Infrastruktur wird sonst schnell wieder durch einen erhöhten Managementbedarf zunichte gemacht. Zudem müssen Daten von verschiedenen Umgebungen effizient zusammengeführt werden können.

Nutzer sind gut beraten, wenn sie die Daten in mehrere unabhängige Infrastrukturen verteilen (etwa Produktion inhouse, Dev/Test bei einem Cloud-Anbieter und Back-up bei einem anderen). Damit dies möglich wird, braucht es zusätzlich zum globalen Datenmanagement eine einheitliche Datenübertragung. Dadurch können die Daten effizient und einfach transportiert werden. Der Transport in eine Cloud ist im Normalfall ohne Kosten verbunden. Die umgekehrte Richtung ist jedoch oft mit teilweise signifikanten Kosten verbunden. Folglich sollte der Transport der Daten auf beide Seiten umkehrbar sein, um lediglich Änderungen und somit ein Bruchteil des Gesamtvolumens wieder aus der Cloud transferieren zu müssen.

Datenkontrolle im Griff behalten

Überlegungen bezüglich unbefugten Zugriffs auf die Daten müssen immer wieder unternommen werden. Dies ändert sich bei Cloud-Lösungen nicht grundlegend. Was sich jedoch ändert ist, dass sich die physikalische Infrastruktur nicht mehr in den eigenen Räumlichkeiten und auch nicht unter eigener Kontrolle befindet.

Ein Cloud-Anbieter hätte somit die Möglichkeit zum Datenabgriff. Dazu gibt es jedoch grosse juristische Regelwerke, die vermehrt den Anforderungen genügen. Man hört auch öfter: «Wenn Cloud-Anbieter XYZ ein Datenleck hat, ist er weg vom Markt.» Spätestens nachdem der Europäische Gerichtshof das Aus für «Safe Harbor» verkündet hat, entfällt jedoch die prominenteste Lösung dieses datenschutzrechtlichen Problems. Eine Übermittlung von Daten in eine Cloud bedarf stets einer rechtlichen Legitimation. Gerade beim Problem der Übermittlung in unsichere «Drittstaaten», wie die USA vonseiten der EU in datenschutzrechtlicher Hinsicht eingestuft wurde, hatten die meisten Anbieter bisher hauptsächlich auf die nun hinfällige «Safe Harbor»-Selbstzertifizierung gesetzt. Entsprechend sind Lösungen gefragt, die diese Probleme adressieren. Die Verschlüsselung der Daten ist hier als Variante zu nennen. Dabei werden die Daten vor der Sicherung respektive dem Transport in eine Cloud verschlüsselt. Somit wird die Einsicht der Daten während des Transports oder für den Cloud-Anbieter verhindert. Andere Lösungen transportieren die Daten gar nicht erst in eine Cloud, sondern in ein Rechenzentrum neben einer solchen. Dazu wird eine dedizierte Infrastruktur genutzt, über die man die totale Kontrolle hat. Die Cloud wird dann lediglich für die Netzwerk- und Rechenressourcen genutzt. So erhält der Nutzer alle Möglichkeiten einer Cloud mit gleichbleibender Datenkontrolle.

Fazit

Hybrid Clouds sind zweifelsohne die IT-Infrastrukturen der Zukunft. Services werden dort bezogen, wo sie am effizientesten und kostengünstigsten erbracht werden können. Die Kombination der verschiedenen Services und Anbieter ist ein grosses Problem. Daten können nicht einfach herumgeschoben werden. Netzwerkbandbreiten, inkompatible Infrastrukturen und Transferkosten machen da einen Strich durch die Rechnung. Hinzu kommen weitreichende Überlegungen zur Sicherheit und Kontrolle der Daten. Vorsicht ist auch dort geboten, wo die Daten generiert werden. Eine Data Fabric mit einem einheitlichen Datenmanagement und einer gleichartigen Datenübermittlung ermöglicht überhaupt erst eine Hybrid Cloud, in der sich Daten frei und sicher bewegen können.

Der Ansatz der Data Fabric hilft IT-Spezialisten, Cloud-Infrastrukturen reibungslos zu verwalten.

« Hybrid Clouds sind zweifelsohne die IT-Infrastrukturen der Zukunft.»

Christoph Schnidrig

Dossier online
auf www.netzwoche.ch
Webcode 6872

«Mit homogenem Datenmanagement kommen Sie sicher in die hybride Cloud»

Christoph Schnidrig ist Leiter Systems Engineering bei der Schweizer Niederlassung des Storage-Spezialisten Netapp. Im Interview erläutert er, warum bestimmte Cloud-Trends in der Schweiz den Nerv von IT-Verantwortlichen treffen. Ausserdem erklärt Schnidrig, was es beim Aufbau hybrider Cloud-Umgebungen zu beachten gilt. Interview: George Sarpong

«Back-up-as-a-Service scheint den Nerv der Zeit zu treffen.»

Christoph Schnidrig

Wie entwickelt sich die Adaption der hybriden Cloud in der Schweiz aus Ihrer Sicht?
Christoph Schnidrig: Das Thema nimmt sowohl bei unseren Partnern wie auch bei den Kunden Fahrt auf. Unsere Partner bauen ihre Hybrid-Cloud-Angebote zum Teil massiv aus. Vor allem Back-up-as-a-Service scheint den Nerv der Zeit zu treffen und bietet wohl auch die kleinste Einstiegshürde. Interessanterweise werden besonders auch Bedenken bezüglich Datensicherheit respektive -hoheit bei sehr grossen Firmen abgebaut.

Was sind die grössten Herausforderungen beim Aufbau hybrider Cloud-Umgebungen?
Zum einen müssen erst einmal Zielsysteme oder Applikationen gefunden werden, die sich in einer hybriden Cloud betreiben lassen. Die starke Verknüpfung von IT-Systemen ist bei der Umsetzung ein grosses Problem. Dann folgen Sicherheitsanforderungen und -bedenken. Man muss prüfen, ob es rechtlich möglich ist, die Daten in eine Public Cloud zu transferieren. Oftmals weiss man dann im Detail gar nicht, um welche Daten es sich nun effektiv handelt. Aus diesem Grund werden dann eher lokale Anbieter im selben Rechtsraum vorgezogen. Zuletzt sind es sicherlich auch technische Herausforderungen. Damit die Netze sicher miteinander verbunden sind, sind umfangreiche Arbeiten und vor allem auch Planung nötig.

Sie schlagen die Verteilung von Daten auf mehrere unabhängige Infrastrukturen vor. Das verkompliziert das Management der Infrastruktur doch eher, als dass es dieses erleichtert. Wo bleibt da der Vorteil der von Ihnen propagierten Hybrid Cloud?
Wir ermöglichen die Verteilung von Daten durch ein homogenes Datenmanagement auf mehrere unabhängige Infrastrukturen. So kann der Kunde immer diejenige nutzen, die ihm gerade die beste Funktion oder den besten Preis bietet. Darüber hinaus kann er so eine sinnvolle Risikoverteilung vornehmen. Wir haben Kunden, die SQL Failover Cluster zwischen Amazon und Azure betreiben. Ins Management unseres cloudübergreifenden Datenmanagements investieren wir seit einigen Jahren viel Zeit und Energie. So unterstützen die heute verfügbaren Tools eine Übersicht und Kontrolle auf einen Blick – egal ob sich die Ressourcen im lokalen Rechenzentrum, in der Cloud A oder in der Cloud B befinden.

Was müssen IT-Verantwortliche beachten, damit Businessanwender Daten zur richtigen Zeit verwenden können?
Es muss einen Datentransportmechanismus geben, der die Daten überhaupt flexibel bewegen kann. Dieser Transportmechanismus muss so flexibel sein, dass sich die Replikation auch einfach umdrehen lässt und vor allem die Daten an der Quelle oder auch am Ziel bearbeitet werden können. Stellen Sie sich vor, dass Sie grosse Datenmengen in eine Public Cloud transferieren. Hineintransferieren kostet in der Regel nichts, hinaus schon. Nun kündigt der Cloud-Anbieter Ihrer Wahl seinen Service, so geschehen kürzlich bei Verizon. Nun müssen Sie Ihre Daten innerhalb von kurzer Zeit wieder aus der Cloud holen. Das ist nicht nur eine Frage der Kosten, sondern auch der verfügbaren Bandbreite. Wenn nun der Transportmechanismus dem bereits Rechnung trägt, transferieren Sie Ihre Daten entsprechend entspannt zum nächsten Anbieter. Oder aber, Sie transferieren die Daten gar nicht in die Cloud, sondern an deren Rand. So müssen Sie keine Daten bewegen, können aber die überaus flexible Rechenleistung beliebiger Clouds nutzen. Diese Lösungen bieten wir heute schon an.

Wie können IT-Verantwortliche Daten in hybriden Cloud-Umgebungen effizient schützen?
Zum einen sollte die Kontrolle der Daten nicht aus der Hand gegeben werden. Das heisst, ein Mechanismus sollte dafür sorgen, dass Sie die Daten entweder kontinuierlich oder auf Abruf an einen zweiten Standort transportieren können. Darüber hinaus bietet sich die Verschlüsselung der Daten an. So kann sichergestellt werden, dass der Cloud-Betreiber vom Zugriff auf die Daten ausgesperrt wird.