Per Point & Click in die Cloud

Globales Multicloud-Netz als Service

Uwe Scholz

Während Unternehmen im Computing- und Storage-Umfeld heute ganz selbstverständlich auf Cloud-Services zurückgreifen, stellt sich dies im Netzbereich deutlich anders dar. Ein globales On-Demand-Netz auf Basis einer weltweit verteilten virtuellen Infrastruktur soll nun die Implementierung und den Betrieb von Multicloud-Netzen erheblich vereinfachen.

Mit der Einführung der Cloud haben sich Rechen- und Speichersysteme über Virtualisierung und Automatisierung hinaus zu As-a-Service-Angeboten entwickelt. IT-Architekten und -Ingenieure konzentrieren sich nun auf die Auswahl der Serviceattribute, die sie konsumieren möchten, wie z.B. die Berechnung von Instanzen und Speichervolumen, anstatt sich um Implementierungsdetails zu kümmern. Die Komplexität wurde eliminiert, und Cloud Computing ist zu einer tragenden Säule für Computing- und Storage-Anwendungen geworden.

Im Gegensatz dazu hat das Netz (sowie seine Dienste) weder einen ähnlichen Transformationsprozess durchlaufen, noch arbeitet es in echter Übereinstimmung mit der Cloud. Der Aufbau eines Netzes für die Cloud ist mit den folgenden zentralen Herausforderungen verbunden:

- langsame Reaktionszeit auf die Bedürfnisse von Unternehmen und Anwendern aufgrund unzureichender Erfahrung mit Cloud-Netzen und zunehmender Komplexität der Vernetzung;
- blinde Flecken bei Sichtbarkeit und Governance aufgrund unterschiedlicher Cloud-Architekturen und das Fehlen eines einzigen Kontrollpunktes;
- hohe Gesamtbetriebskosten (TCO – Total Cost of Ownership) aufgrund von eigenen Leistungen bei der Implementierung sowie eines komplexen Netzbetriebes.

Hinzu kommt, dass Unternehmen mehr und mehr Multicloud- und Hybridcloud-Strategien verfolgen, wobei der Workload nun nicht auf einen oder zwei, sondern auf mehrere öffentliche Cloud-Dienste verteilt wird. Es ist folgerichtig, dass viele Unternehmen vor Problemen stehen, wenn sie versuchen, das komplexe Geflecht von Endpunkten miteinander zu verknüpfen. Auf individueller Basis lassen sich Cloud-Dienste relativ einfach bereitstellen. Aber mehrere Clouds auf eine kohärente, verwaltbare und sichere Weise miteinander zu verbinden, ist eine ganz andere Sache.

Multicloud-Strategien auf dem Vormarsch

Eine neue Kategorie auf dem Markt für Unternehmensnetze verspricht, hier Abhilfe zu schaffen. Bei der „Netz-Cloud" geht es darum, ein konsistentes und dramatisch vereinfachtes Netzkonzept für On-Premise-, Cloud- und Multicloud-Umgebungen mit integrierten Netz- und Sicherheitsdiensten sowie vollständiger operationeller Transparenz und Verwaltung anzubieten. Ziel ist es, die Notwendigkeit des Aufbaus eines Netzes zu eliminieren und es stattdessen als Service zur Verfügung zu stellen.

Basis für dieses Konzept bildet ein globales On-Demand-Multicloud-Netz, beispielsweise die Alkira Cloud Service Exchange (CSX). Sie stellt eine weltweit verteilte virtuelle Infrastruktur von Cloud Exchange Points bereit. Dabei handelt es sich um Points of Presence mit einem kompletten Routing-Stack sowie umfassenden Netzservicefunktionen. Sie ermöglichen es dem Anwender, sich standortnah mit ihren Cloud-Instanzen zu verbinden. Auf diese Weise können Rechenzentren, lokale Standorte, Zweigstellen oder Homeoffices mit jeder beliebigen Cloud verknüpft werden. Das Unternehmen muss nur einmal eine Verbindung zu seinem Netz herstellen, um Zugang zu allen Clouds zu erhalten, ohne dass dazu ein zusätzliches Engineering nötig wird. Die Komplexität der unterschiedlichen Handhabung der verschiedenen Cloud-Anbieter wird auf

Uwe Scholz ist freier Journalist in Berlin

diese Weise vom Benutzer weg abstrahiert.

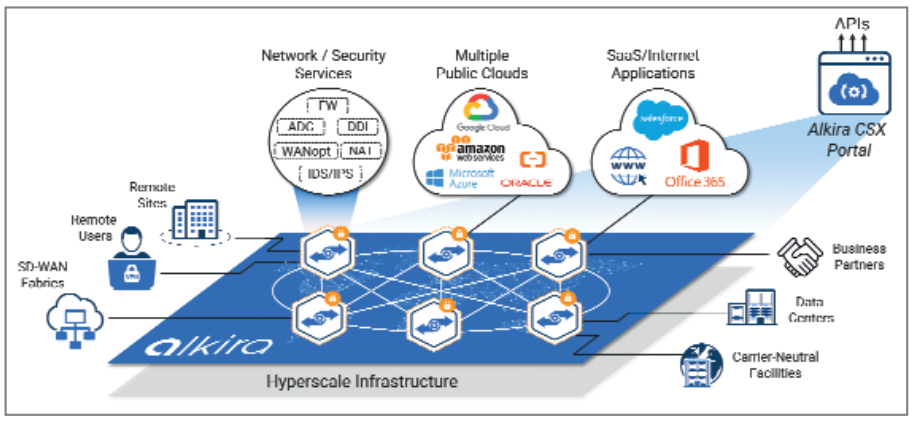
Point-and-Click-Provisionierung

Um ein Netz aufzusetzen, stellt das System eine Landkarte bereit, auf der die existierenden Cloud Exchange Points geografisch verzeichnet sind. Per Point and Click wird der nächstliegende Exchange Point ausgewählt und mit der Cloud-Instanz verbunden, wobei derzeit AWS VPCs, Microsoft Azure VNets und Google Cloud Platform VPCs unterstützt werden. Einmal verbunden, können alle Instanzen sofort über die Service Exchange miteinander kommunizieren.

In gleicher Weise können die Remote-Standorte des Unternehmens für den Cloud- und Multicloud-Access angebunden werden. Dabei kann es sich um Homeoffies, Zweigstellen, Datacenter oder ganze Campus handeln. Derzeit werden IPsec, Cisco SD-WAN and AWS Direct Connect als Methoden für die Last-Mile-Konnektivität unterstützt.

Optional können Services wie Firewalls usw. hinzugefügt werden. Zudem besteht die Möglichkeit einer Segmentierung des Netzes. Einmal eingerichtet, umspannen die Segmente das gesamte globale Multicloud-Netz und sorgen für eine durchgängige Isolation. Lokale Standorte, Cloud-Instanzen, Netzservices sowie SaaS-/Internet-Exit-Points werden dazu einem speziellen Segment zugeordnet. Damit kann die Compliance erreicht werden, wenn sensitive Anwendungen in die Cloud verlagert werden.

Die Provisionierung des gesamten globalen Netzes erfolgt dann auf einen Klick. Die Alkira Cloud Service Exchange initialisiert automatisch alle notwendigen Elemente für die zuvor gewählte Konfiguration und startet das Billing. Abhängig vom Umfang des Netzdesigns, also der Zahl der geografischen Standorte, der Public-Cloud-Instanzen und der gewählten Netzservices dauert die Bereitstellung nur wenige Minuten, wobei der Fortschritt mittels Progress-Bar angezeigt wird.



Prinzip der Alkira Cloud Service Exchange (CSX) *(Bild: Alkira)*

Drei Einsatzszenarien

Die Einsatzbereiche der Lösung umfassen drei Szenarien:

- Erstens die Anbindung von Standorten an eine Public Cloud, wobei der Fokus auf einem Hochgeschwindigkeits-Datentransport mit geringer Latenz liegt.
- Zweitens die Verbindung einer Public Cloud mit einer anderen, wobei die CSX automatisch die vom Administrator bereitgestellten Credentials für den jeweiligen Cloud-Betreiber erkennt, um eine Verbindung ohne manuelle Justierung herzustellen.
- Und schließlich die Anbindung von Standorten für Internet- und SaaS-Anwendungen. Der Zugang wird am regional nächstliegenden Internet-Exit-Point bereitgestellt.

Um die Anbindung von lokalen Standorten über das Internet abzusichern, kommen in der Regel Firewalls zum Einsatz. Allerdings führt diese Methode oftmals zu einer hohen Zahl von Firewalls und von zu administrierenden Endpunkten. Die Alkira CSX stellt für die Sicherung der Verbindungen optional Palo Alto Firewalls bereit, die für eine Balance der optimalen regionalen Konnektivität und der erforderlichen Sicherheit Rechnung tragen. Im Vergleich mit einem direkten Internetzugang an jedem lokalen Standort führt diese Methode zu einer deutlichen Verringerung der zu administrierenden Netzelemente.

Die Möglichkeit, Stateful-Firewalls für den Netz-Traffic zu und zwischen Clouds einzusetzen, ist für einen reibungslosen Betrieb unerlässlich. Allerdings müssen Stateful-Firewalls die gesamte bidirektionale Kommunikation überwachen, um die jeweiligen Policies durchsetzen zu können. Dies impliziert jedoch Traffic-Symmetrie. Netze sind aber inhärent asymmetrisch, was insbesondere dann zu Herausforderungen führt, wenn die Firewalls geografisch verteilt sind. Aus diesem Grund nutzt die Cloud Service Exchange ein intelligentes Traffic-Steering, um die Symmetrie über das weltweite Firewall-Netz zu erzielen.

Deutlich verkürzte Einrichtung

Die Firewall-Funktionalität ist Bestandteil eines Servicemarktplatzes, der sukzessive erweitert wird. Er soll künftig weitere netzbasierte Services und Appliances enthalten, die optional eingesetzt werden können.

Die Alkira-Lösung verspricht eine deutlich verkürzte Einrichtung von Multicloud-Netzen, die gewöhnlich Wochen in Anspruch nehmen kann, bis auf wenige Minuten in Übereinstimmung mit den Service-Level-Agreements. Mit ihrer Konzeption eliminiert sie betreiberspezifische Limitierungen durch den Aufbau eines überregionalen Overlay-Netzes einschließlich cloudnativer Routing- und Security-Funktionen. Als On-Demand-Service bietet sie die Elastizität, die Kapazität an den tatsächlichen Bandbreitenbedarf anzupassen. Anwender bezahlen lediglich für die Ressourcen, die sie tatsächlich nutzen. Mittels Firewalls und der Ende-zu-Ende-Segmentierung wird den Anforderungen an Security und Compliance Rechnung getragen. *(bk)*