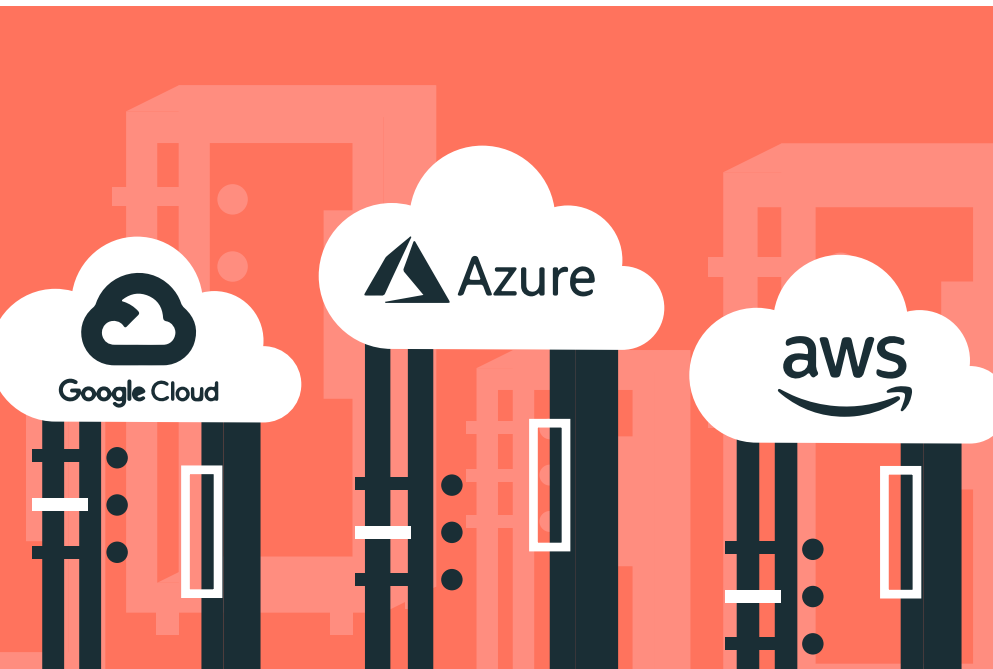




Selbst gehostete Full-Service-Cloud

Die Automatisierungsfunktionen und den Komfort der Public Cloud im eigenen RZ? Das versprechen Microsoft und Google mit ihren um Cloud-Dienste erweiterten Kubernetes-Distributionen.

Von Christoph Puppe

■ Vor fünfzehn bis zwanzig Jahren wurden Milliarden mit dem Versprechen umgesetzt, die Effizienz der Serververwaltung durch RZ-Automatisierung zu steigern. Aber nur die größten Firmen hatten die Kapazitäten, ihre Serverfarmen von der Manufaktur zu Fabriken mit Großserienfertigung umzubauen. Cloud war und ist die Antwort auf dieses Dilemma –

aber wer will wirklich alle Prozesse und Daten auf Hardware außerhalb der eigenen Kontrolle auslagern?

Der Verlust dieser Kontrolle, Abhängigkeit vom Anbieter, Datenschutz und die weiteren Risiken durch die Milliarden Zeilen Code der Cloud-Ressourcenmanager sind gewichtige Gründe, Cloud zu vermeiden. Aus dieser Betrachtung ergibt

sich schnell der Gedanke, zur ursprünglichen Idee zurückzukehren und mit den in der Cloud entwickelten Mechanismen das eigene RZ zu automatisieren.

Connected oder Air-gapped

Mit ihren Hybrid-Cloud- und Self-hosted-Air-Gap-Angeboten wollen die größten CSPs Kunden das Beste aus beiden Welten liefern und so die Versprechen von vor zwei Jahrzehnten einlösen. So sollen die im Artikel „Cloud-Service-Broker – Anspruch und Realität“ [1] betrachteten Azure ARC, AWS Outpost und Google Anthos mit Distributed Cloud im RZ der Kunden diesen die gleichen Vorteile wie im fremden RZ bringen. Endlich die eigenen Daten wieder im eigenen Keller! Latenzen und Kosten sinken, die Industriesteuerung hat den direkten Draht zum Container, Datenschützer und Geheimschutzbeauftragte sind zufrieden, weil Staatsgeheimnisse und personenbezogene Daten nicht aus Drittstaaten erreichbar sind.

Technisch ähneln sich dabei alle Lösungen sehr stark: Es wird entweder selbst gekaufte oder vom Anbieter gelieferte Hardware im eigenen Rechenzentrum aufgestellt und die Verwaltung übernehmen die Ressource Manager der Hyperscaler. Damit ist die Datenhoheit nominell zwar wieder beim Kunden, aber die Verwaltung erfolgt von außen. Ob man nun einen Dienstleister, Service-Now, Solarwinds oder einen anderen Anbieter damit beauftragt oder dies den Hyperscalern überträgt, ist kein großer Unterschied. Souverän sein und Kontrolle haben ist allerdings etwas anderes.

Hybride Cloud hat viele Vorteile und ist in vielen Einsatzszenarien eine gute Lösung. Aber der Lackmustest ist das sogenannte Air Gap: Nur wenn die Distributed Cloud auch ohne Anschluss an den Hersteller und komplett ohne Internetzugang funktioniert, dann ist der Kunde wieder vollständig Inhaber der Daten und Prozesse. Derzeit gibt es zwei Anbieter, die eine Air-Gap-Cloud im Programm haben, die keinen Anschluss an das Internet oder den Hyperscaler benötigt: Azure Stack Hub Disconnected (ASH Disconnected) und die etwas irreführend benannte Google Distributed Cloud Hosted (GDCH).

Google Distributed Cloud Hosted

Eine gemäß der Bekanntgabe der Verfügbarkeit Anfang März dieses Jahres ideale Voraussetzung für die GDCH ist, dass

X-TRACT

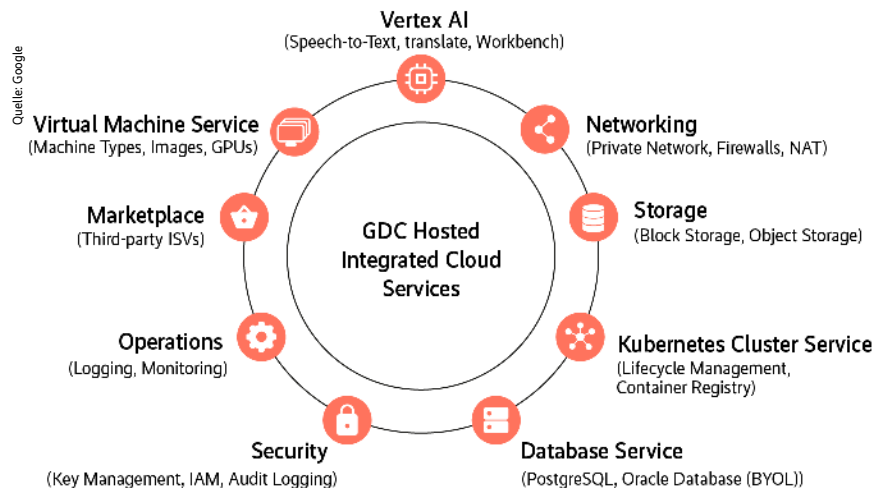
- ▶ Google Distributed Cloud Hosted und Azure Stack Hub Disconnected bieten eine vollständig ohne Internetanschluss betreibbare private Cloud im eigenen Rechenzentrum.
- ▶ Die als Distributed, Self-hosted und Air-Gap-Cloud bezeichneten Produkte wären die Erfüllung des langjährigen RZ-Automatisierungstraums.
- ▶ Die beiden aktuellen Angebote von Google und Microsoft verfügen über einen leider nur sehr eingeschränkten Funktionsumfang.
- ▶ Wer Kubernetes on Premises und Air-gapped betreiben möchte, hat mit diesen Services und den K8s-Distributionen eine große Auswahl.

Kunden mit hoheitlichen Aufgaben mit Staatsgeheimnissen betraut sind, Welt- raumforschung betreiben oder sogenannten „stark regulierte Branchen“ angehören. Das Angebot umfasst mindestens vier Racks, auf denen ein Teil der aus der GCP bekannten Software läuft. Konkrete Kosten für den Betrieb nennt Google nicht, kündigten aber im selben Zug an, man biete Testkonfigurationen ab 300 000 US-Dollar pro Monat an. Leider ist es nicht möglich, das Angebot vorab ohne Kosten auszuprobieren oder anderweitig hinter die Kulissen zu schauen. Die Angaben in diesem Artikel basieren daher auf der öffentlich sichtbaren Dokumentation für die aktuelle Version 1.9.4 (siehe ix.de/zf47).

Immerhin eine Cloud, die Kunden geliefert bekommen. Updates gibt es zwar online, die Administratoren müssen sie dann aber auf Wechselplatten gespeichert hinter das Air Gap tragen. Ubuntu 20.04 LTS ist die Grundlage und kann entweder virtualisiert oder auf Bare Metal laufen. Das Angebot enthält nur wenige der von Google Cloud bekannten Dienste. Hauptsächlich ist GDHC eine Kubernetes-Distribution, die zusätzlich Netzwerk inklusive Firewall, IaaS, Storage, KI (Vertex AI), Schlüsselmanagement, Datenbank (Postgres 1.3 oder Oracle 19) und die Verwaltungsfunktionen für Monitoring, Protokollierung und Sicherheit mitbringt. Immerhin sind ein Terraform-Provider und eine Anbindung an Hardware-Security-Module dabei. In der Cloud sind die Marketplaces für Kunden eine schnelle und einfache Art, Dienstanwendungen zu installieren. Bei Air Gap müssen Kunden die Pakete herunterladen. Wie das genau vor sich gehen soll, schreibt Google jedoch nicht, Apache Spark ist aber schon enthalten.

Azure Stack Hub Disconnected

Das etwas länger am Markt befindliche Angebot für eine Air-Gap-Distributed-Cloud kommt von Microsoft. Der Azure Stack Hub (ASH) lässt sich auch „Disconnected“, das heißt ohne Internetanbindung betreiben. Die drei Optionen Azure Stack, HCI und Edge sind laut Dokumentation und Marketing auch in der Disconnected-Variante enthalten. Für HCI stimmt dies nicht, da die Lizenzverwaltung mindestens zu Beginn der Laufzeit eine Verbindung zu Azure Online benötigt. Bei Edge erfolgt die initiale Installation über das Azure-Portal und danach ist kein zentrales Management der Edges mehr möglich, sondern nur lokal auf den Geräten selbst. ASH Disconnected kann



Nur wenige der weit über 300 verfügbaren Google-Dienste sind auch in der Air-Gap-Variante enthalten.

dies nicht über lokale Netze übernehmen. Das ist eine erhebliche Einschränkung, die die Zweckmäßigkeit sehr zweifelhaft erscheinen lässt. Damit bleibt nur der Azure Stack Hub, der tatsächlich mit Air Gap betreibbar ist.

Wie auch GDHC ist ASH hauptsächlich eine um notwendige Tools für IaaS, Storage, Benutzerverwaltung, Ressourcenmanagement, Schlüsselverwaltung und Administration erweiterte Kubernetes-Distribution. Für das Air Gap listet Microsoft die Funktionen, die eingeschränkt oder nicht zur Verfügung stehen, in der Dokumentation auf und auch für die Edge (ASE) finden sich passende Informationen (siehe ix.de/zf47). Für den Marktplatz hat Microsoft eine Lösung parat: Die Installationsdateien lassen sich per PowerShell-Modul aus dem Online Market in Azure herunterladen und dann in den lokalen ASH importieren. Dass Azure Active Directory nicht nutzbar ist, ist bei Air Gap zu erwarten. Hier muss ein lokaler Active Directory Federations Services Server einspringen.

ASH läuft auf Standardhardware und nutzt – wenig überraschend – Hyper-V. Im Gegensatz zu GDHC beschafft und installiert der Kunde die Serverhardware selbst. Es fallen Lizenzgebühren an und der Support ist entweder über einen Vertriebspartner oder von Microsoft selbst zu beziehen. Für Air Gap ist es notwendig, ein Enterprise Agreement über die installierte Kapazität abzuschließen, da eine Abrechnung nach Nutzung eine Verbindung zu Azure benötigen würde.

Fazit

Die beiden Angebote für die Disconnected, Self-hosted und damit Air-gapped Cloud sind bei genauerer Betrachtung

hauptsächlich Kubernetes-Distributionen, die neben Storage, Verwaltung und einer Datenbank noch einige wenige weitere Dienste wie KI bei Google oder importierte Marketplace-Dienste bei Azure mitbringen. Damit stehen sie nicht so sehr in Konkurrenz zu den Onlinediensten der Hyperscaler, sondern zu den anderen Kubernetes-Distributionen, denn die lassen sich durch die Bank auch Air-gapped installieren.

Der Vorteil für den Anwender ist sicherlich die ausgereifte Verwaltung und dass die jeweiligen Oberflächen denen der Onlineangebote stark ähneln. Aber wer OpenShift, Rancher, Kubermatic oder auch Tanzu kennt, wird diesen Vorteil vielleicht nicht unbedingt so hoch schätzen, wie die wenigen verfügbaren Preisblätter dies erfordern. Leider gibt es wie so oft öffentlich keine Preise. Nur wer ein konkretes Angebot anfordert, erhält hier Einblick. (avr@ix.de)

Quellen

- [1] Christoph Puppe; Cloud-Dienste; Cloud-Service-Broker – Anspruch und Realität; iX 11/2021, S. 110
- [2] Links zu den vorgestellten Angeboten: ix.de/zf47

CHRISTOPH PUPPE



ist Managing IT Security Architect und Auditteamleiter für ISO 27001 nach Grundschutz bei SVA System Vertrieb Alexander GmbH, Mitautor des Grundschutz-Kompendiums und ehemaliger Penetrationstester.