

Cloud-Dienste: Anspruch und Realität von Cloud-Service-Brokern

29.10.2021 08:00 Uhr Christoph Puppe



Cloud-Service-Broker fassen Cloud-Dienste anderer Anbieter zusammen und bieten Kunden zusätzlichen Service. Herausforderung ist die Komplexität von Multi-Clouds

Wer seinen Cloud-Bedarf bei mehreren Anbietern deckt, kann zumindest theoretisch das Risiko eines Vendor Lock-in reduzieren. Vor diesem Hintergrund sind oder waren Cloud-Service-Broker (CSB) die Idee, dass man Cloud-Dienste weiterverkaufen kann, sie also als Value-added Reseller in einem eigenen Kiosk zusammenfasst und Kunden so einen zusätzlichen Service bietet. Multi-Cloud-Umgebungen sind allerdings komplex und die Cloud-Anbieter selbst entwickeln sich so schnell, dass es kaum möglich ist, die ursprüngliche Idee umzusetzen.

Multi-Cloud-Management ist daher aktuell eher bei den Firmen selbst zu finden, und es gibt auch entsprechende Werkzeuge, die zumindest die Verwaltung mehrerer Anbieter erlauben. Allerdings können sie selten alle Dienste der Anbieter verwalten. Auch erlauben nur wenige Cloud-Anbieter das Steuern der Konkurrenz aus der eigenen Plattform heraus.

MEHR ZUM THEMA MULTI-CLOUD



Multi-Cloud-Management für regulierte Unternehmen [1]

Vorteile und strategische Überlegungen zum Einsatz der Multi-Cloud [2]

Multi-Cloud: Cloud-Dienste effizient, sicher und zuverlässig vernetzen [3]

Multi-Cloud-Betrieb: Einfacher mit TOSCA 2.0 [4]

Cloud-Management-Werkzeuge im Vergleich [5]

Unternehmens-IT: Hosted Managed Services im Einsatz [6]

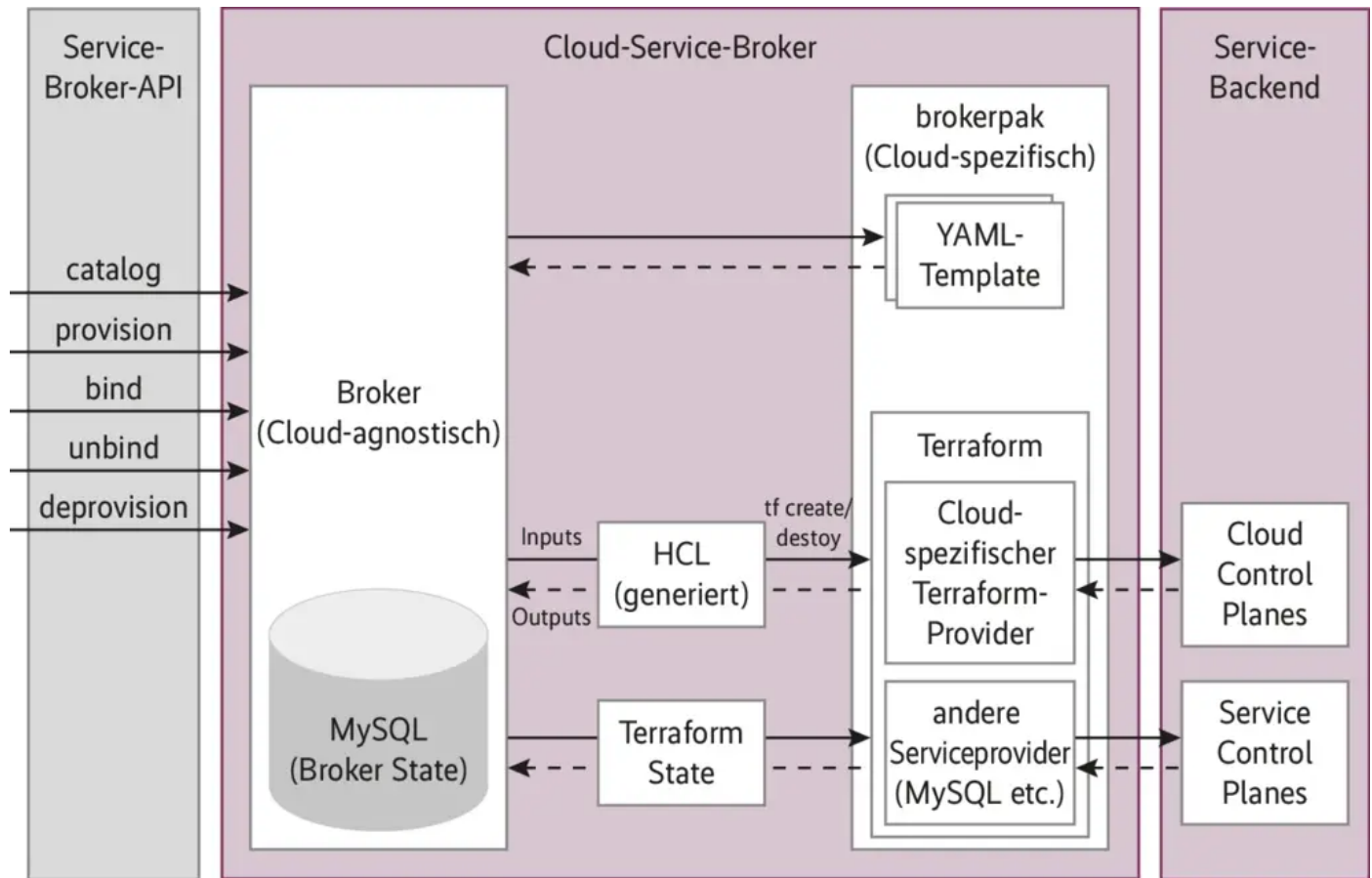
Übersicht Compliance Management: Tools für die Cloud und Schwachstellenscanner [7]

Mehr Angebote finden sich da bei der Verwaltung der eigenen IT-Landschaft mit den Werkzeugen der Cloud. Google Anthos, AWS Outpost und Azure Arc sind die drei dominierenden Werkzeuge für diese Sparte. Auch das Feld der Multi-Cloud-fähigen Managementansätze ist mittlerweile sehr groß.

IX-TRACT

- Ein Multi-Cloud-Ansatz kann Kunden helfen, einen Vendor Lock-in zu vermeiden.
 - Ein Weg dorthin sind Cloud-Service-Broker, die Cloud-Dienste von Drittanbietern zusammenfassen und weiterverkaufen.
 - Angesichts der rasanten technischen Weiterentwicklung scheinen Cloud-Service-Broker als Produkt aber nicht mehr relevant.
 - Aktuelle Angebote für Multi-Cloud-Management enthalten nur Standarddienste.
-

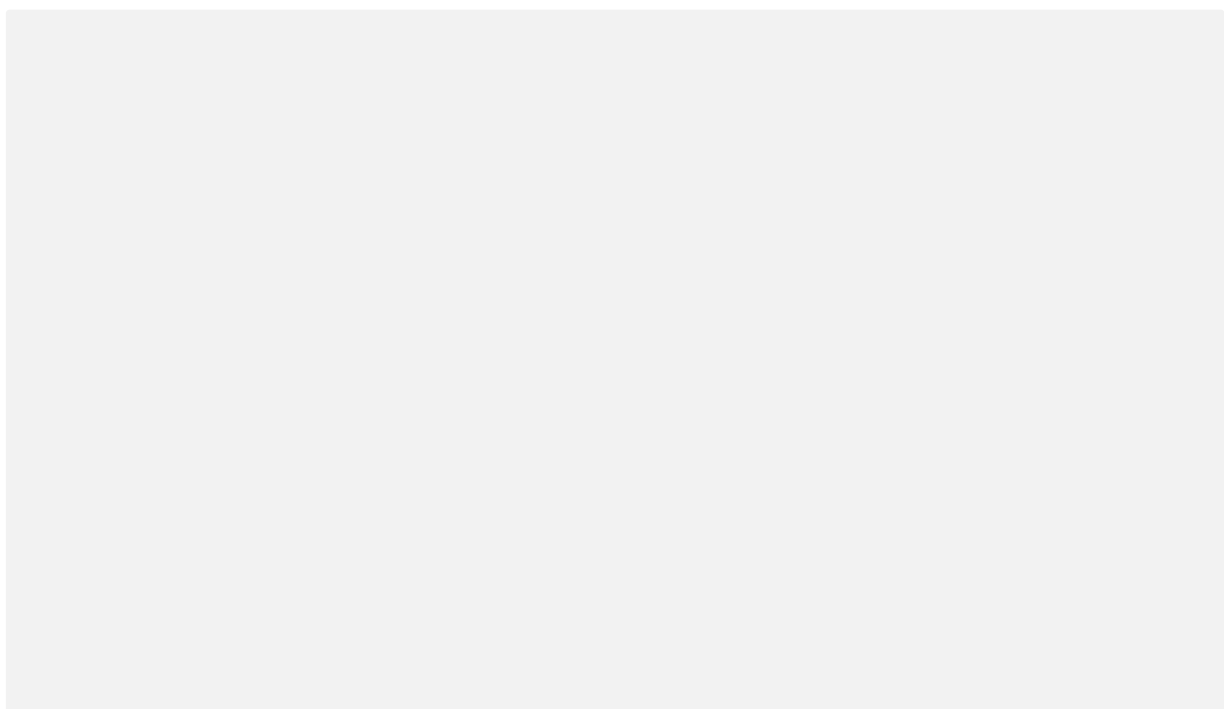
Von den ursprünglichen Hoffnungen ist fast zehn Jahre nach den ersten Veröffentlichungen zum Thema CSB nicht viel übrig geblieben. Die erste Euphorie ist rasch verflogen, denn alle Cloud-Angebote entwickeln sich so schnell, dass es schwierig ist, einen CSB aktuell zu halten. Der Aufwand ist erheblich und die Vorteile für die Kunden nur schlecht darstellbar. Für diese ist es zu einfach, entweder direkt mit den Anbietern zu arbeiten oder selbst die Software zum Multi-Cloud-Management einzusetzen. Accounts beim Anbieter sind schnell erstellt, und so groß ist kein CSB geworden, dass er Mengenrabatte hätte weitergeben können.



Cloud-Service-Broker und Tools fürs Multi-Cloud-Management arbeiten nach sehr ähnlichen Prinzipien, was eine Grafik aus der Dokumentation zu VMware Tanzu für die notwendigen Schnittstellen verdeutlicht.

(Bild: VMware)

Zwar gibt es Marktstudien, die den globalen Markt für diese Dienste bei über 5 Milliarden US-Dollar sehen, aber bei genauerer Betrachtung der Anbieter sind es entweder Beratungshäuser oder Anbieter von Werkzeugen für Multi-Cloud-Management, die die Umsätze machen. Das eigentliche Geschäft eines CSB ist der Einkauf der Dienste und die Vermittlung an die eigenen Kunden. Damit fallen alle Firmen aus der Liste, die nur Software oder Beratung bereitstellen. Sobald der Kunde seine eigenen Accounts bei den Cloud-Anbietern benötigt und von diesen auch die Rechnung erhält, ist es kein CSB mehr.



[8]

Standards

Das gemeinsame Verwalten mehrerer Anbieter von Cloud-Diensten kann nur mit etablierten Standards funktionieren. Terraform hat sich hier am Markt etabliert, um Dienste einzurichten, zu konfigurieren und auch wieder zu löschen. **In der Registry von terraform.io [9]** fanden sich bei der Recherche für diesen Artikel 1437 Provider, von denen 34 den Status official und 151 den Status verified haben. Die weiteren sind nicht überprüft und die Community hat die Skripte hochgeladen, aber es gibt keine Garantien, dass diese Templates korrekt oder vollständig sind. Um überhaupt in der Registry aufzutauchen, muss der Anbieter über einen Terraform-Dienst verfügen, der die Skripte ausführt und nach ihren Anweisungen Ressourcen erstellt.

Ein weiterer Standard ist YAML als strukturierte Beschreibungssyntax für die gewünschten Dienste. YAML und JSON sind hier oft austauschbar, da sich beide Formate gut eignen, viele Dienste beides akzeptieren und die Konvertierung einfach und verlustfrei möglich ist. Ab YAML 1.2 bezieht sich der Standard auch direkt auf JSON, und somit ist jede JSON-Datei auch eine valide YAML-Datei.

Protokollierung und Überwachung sind leider nicht ganz so gut standardisiert. Für die Überwachung sind "Application Performance Monitoring" (APM) Logs und auch die Prometheus Endpoints zumindest im Cloud Native Stack so weit verbreitet, dass man von einem Standard sprechen kann. Aber viele PaaS-Angebote verfügen nicht über eben diese Endpunkte. Einen Überblick zu APM liefert der Artikel " **Systemmanagement: Marktübersicht Application Performance Monitoring [10]** ".

Protokolldaten liegen zumeist in JSON vor, aber ein definiertes Format, dem sich alle Anbieter mit allen ihren Diensten angeschlossen hätten, existiert hierfür nicht. Wer also Protokolle aus vielen Quellen auswerten muss, wird weiterhin die Daten bei Eingang in ein eigenes Format konvertieren müssen.

Auch bei der Erkennung und Behandlung von Vorfällen ist die Lage sehr unschön. Hier setzt jeder Anbieter seine eigenen Ideen um. Eine standardisierte Schnittstelle, um etwa Ausfälle, Angriffe oder sonstige Probleme des Anbieters auszulesen oder geschickt zu bekommen, würde das Sicherheitsmanagement stark vereinfachen.

Multi-Cloud-Spezialisten

Will man das Feld sortieren, ist es hilfreich, mit den Spezialisten anzufangen. Hierzu zählen die Sicherheitswerkzeuge zur Suche nach fehlerhaften und unsicheren Einstellungen. Diese Tools betrachten nicht nur die großen Public-Cloud-Anbieter, sondern haben auch die On-Premises-Clouds und sonstige IT-Dienste im Fokus. Eine Übersicht findet sich im Artikel "**Übersicht Compliance Management: Tools für die Cloud und Schwachstellenscanner [11]**".

Die großen Public-Cloud-Anbieter, aber auch die selbst betriebenen Cloud-Stack-Dienste wie Kubernetes sind dabei mit ihren APIs für die Verwaltung eine große Hilfe, denn so kann die Überwachung über eine definierte Schnittstelle erfolgen. Der Vorteil dabei: Alle Dienste und ihre Einstellungen sind zugänglich. Bei der herkömmlichen IT ist es oft erforderlich, lokale Agenten für die Analyse von Konfigurationsdateien zu nutzen, und es besteht das Risiko, Server und Dienste zu übersehen. Die Vorteile beim Betrieb von Standards und Schnittstellen machen sich so auch bei den Audits bemerkbar.

Ein weiterer Spezialfall sind Security Operations Center, die die Public-Cloud-Anbieter in den meisten Fällen nur für das eigene Angebot bereitstellen. Aber auch hier ist zu bemerken, dass Multi-Cloud die Zukunft ist oder zumindest von allen als diese angesehen wird. So bietet AWS mit dem Security Hub die Möglichkeit, über weitere Werkzeuge auch die Sicherheit anderer Anbieter zu überwachen. Microsoft geht hier noch einen Schritt weiter und ermöglicht im Azure Security Center das Anbinden an Google Cloud und AWS.

Eine andere Kategorie von Spezialisten kümmert sich jeweils nur um einen Dienst, aber das bei diversen Public-Cloud-Anbietern. Ein sehr bekanntes Beispiel ist hier das kürzlich von SUSE gekaufte Rancher. Schon immer konnte es Kubernetes-Cluster in AWS erstellen und verwalten. **Seit der Version 2.6 sind nun auch Azure und Google Cloud dazugekommen [12].**

Storage-Angebote sind ein weiteres Beispiel. Kaum ein Hersteller von On-Premises-Storage, dessen Produkte nicht das Backup in diverse Public-Cloud-Dienste anbieten. Manche Anbieter gehen hier auch noch weiter, indem sie selbst in die Cloud gehen und sich als Teil der Hyperscaler vermarkten.

Ein recht großes Marktsegment bilden die im **zitierten Artikel aufgeführten Multi-Cloud-Abrechnungs- und Optimierungswerkzeuge [13]**. Hier sammelt ein Dienstleister oder eine Software auf den eigenen Rechnern die Rechnungen aller Cloud-Dienste ein und analysiert sie. Zumeist ist dabei auch eine Auswertung nach Einsparpotenzialen enthalten.

Generalisten des Multi-Cloud-Managements

Ein sehr weites Feld sind die Multi-Cloud-Management-Generalisten (MCM). Also entweder ein SaaS-Angebot oder eine Software für den On-Premises-Einsatz, die die Verwaltung von Diensten auf mehreren zumeist großen Cloud-Anbietern und den selbst betriebenen Cloud-Stack-Diensten unter einer Oberfläche zusammenfassen.

So wird es für Nutzer relativ einfach, eine aus Public, Virtual Private und Private Cloud bestehende Umgebung zu verwalten. Diesen Generalisten ist gemein, dass sie sich meistens auf die bei allen Anbietern relativ ähnlichen Basisdienste konzentrieren, also auf virtuelle Systeme (IaaS), Datenbanken, Block- oder Objektspeicher (STaaS), Benutzermanagement, Rechnungen, Netzwerke und Kubernetes.

Dinge, durch die sich die Cloud-Anbieter wirklich voneinander differenzieren, wie APIs für KI, Quantencomputing, Data Warehousing, Datenstreaming mit Kafka und anderen Produkten, Quellcodeverwaltung oder generell DevOps und CI/CD, No-Code-Lösungen, spezielle Produkte für Branchen, IoT et cetera, lassen sich üblicherweise nicht über die MCM verwalten. Wer solche Zusatzfunktionen nutzen will, muss dann doch wieder direkt mit dem Cloud-Anbieter interagieren. Auch wer einen kleineren oder lokalen IaaS- oder STaaS-Anbieter bevorzugt, hat mit den MCM kaum eine Chance, da diese zwar alle drei großen Hyperscaler (AWS, Azure und GCP) steuern können, aber nicht den kleinen Hoster von nebenan.

Der Spezialfall unter den Spezialfällen ist sicherlich die Verwaltung der eigenen IT-Systeme unter der gleichen Oberfläche wie die der Virtual Private Cloud. Hier haben Google mit Anthos, AWS mit Outpost und Azure mit Arc ihre Produkte um eine Software **zum Verwalten der On-Premises-IT erweitert [14]**. So lässt sich eine vereinheitlichte Verwaltung der hybriden Cloud erreichen. Zumindest für die oben erwähnten Standarddienste wie IaaS, STaaS, DBaaS und IDaaS ist es praktisch, da dies die Grenzen zwischen dem eigenen Rechenzentrum und der ausgelagerten IT unsichtbar macht.

Fazit und Vergleichstabelle

Cloud-Computing entwickelt sich nach wie vor schnell und viele Ideen der Anfangszeit haben aktuell keine praktische Bedeutung mehr, während sich andere Technologien in einer Geschwindigkeit durchgesetzt haben, die zu Anfang nicht vorstellbar war. Der Trend hier geht daher klar weg vom Cloud-Brokerage hin zur gemeinsamen Verwaltung mehrerer Cloud-Anbieter mit einem Softwaretool, aber ohne einen Zwischenhändler.

Multi-Cloud-Management ist leider immer noch stark auf Standarddienste beschränkt und entschärft so zwar den Vendor Lock-in, aber die interessanten Angebote mit sehr spezialisierten Diensten bleiben außen vor. Hier muss jede Firma selbst entscheiden, ob diese einen ausreichenden Vorteil bieten, dass man sich fest an einen der Anbieter binden möchte, oder ob man lieber darauf verzichtet und auf diese Weise flexibel bleibt.

Vergleichsmatrix Multi-Cloud-Management-Tools

	ActivePlatform Cloud	Anthos	Azure Arc	Cloud Governance	Cloud Management Platform	Cloud Pak for Multicloud Management
Anbieter	ActivePlatform	Google	Microsoft	CloudBolt	Flexera	IBM
Alibaba Cloud				✓	✓	
AWS		✓ (K8s)	✓ (K8s)	✓	✓	✓
Azure	✓	✓ (K8s)	✓	✓	✓	✓
GCP		✓	✓ (K8s)	✓	✓	✓
IBM Cloud				✓		✓
Oracle Cloud				✓		
on Premises		✓	✓ (Server, K8s, SQL- Server)	✓	✓	✓
Technologien						
CloudStack	✓			✓	✓	
Kubernetes		✓	✓	✓	✓	✓
OpenStack			✓	✓	✓	✓
OpenShift				✓		✓
VMware	✓	✓		✓	✓	✓

¹ nur auf der gelieferten Hardware, ² nur Monitoring

(avr [15])

URL dieses Artikels:

<https://www.heise.de/-6233204>

Links in diesem Artikel:

[1] <https://www.heise.de/hintergrund/Multi-Cloud-Management-fuer-regulierte-Unternehmen-6658793.html>

[2] <https://www.heise.de/hintergrund/Multi-Cloud-Management-in-Firmen-Vorteile-ausreizen-mit->

richtiger-Strategie-6657254.html

[3] <https://www.heise.de/hintergrund/Multi-Cloud-Cloud-Dienste-effizient-sicher-und-zuverlaessig-vernetzen-6328498.html>

[4] <https://www.heise.de/hintergrund/Multicloud-Betrieb-Einfacher-mit-TOSCA-2-0-5061885.html>

[5] <https://www.heise.de/ratgeber/Cloud-Management-Werkzeuge-im-Vergleich-4959106.html>

[6] <https://www.heise.de/ratgeber/Unternehmens-IT-Hosted-Managed-Services-im-Einsatz-4937360.html>

[7] <https://www.heise.de/tests/Uebersicht-Compliance-Management-Tools-fuer-die-Cloud-und-Schwachstellenscanner-4989174.html>

[8] <https://www.heise.de/ix/>

[9] <https://registry.terraform.io/browse/providers?tier=partner>

[10] <https://www.heise.de/hintergrund/Systemmanagement-Marktuebersicht-Application-Performance-Monitoring-5057879.html>

[11] <https://www.heise.de/tests/Uebersicht-Compliance-Management-Tools-fuer-die-Cloud-und-Schwachstellenscanner-4989174.html>

[12] <https://www.heise.de/news/Kubernetes-SUSE-Rancher-2-6-verwaltet-auch-Cluster-auf-Azure-und-Google-GKE-6178641.html>

[13] <https://www.heise.de/tests/Uebersicht-Compliance-Management-Tools-fuer-die-Cloud-und-Schwachstellenscanner-4989174.html>

[14] <https://www.heise.de/tests/Kommerzielle-Kubernetes-Distributionen-im-Vergleich-4702602.html>

[15] <mailto:avr@ix.de>

Copyright © 2021 Heise Medien