

Multicloud Management für Finanzdienstleister: Eine permanente Herausforderung

Jede Anwendung benötigt ihre passende Cloud-Umgebung. In der hoch regulierten Finanzwirtschaft gilt dieses Credo wie kaum in einer anderen Branche. Je nach Leistungsschnitt, Modernisierungsgrad und Schutzbedürfnis der zu verarbeitenden Daten laufen Anwendungen in On- und Off-Premise-betriebenen Private, Hybrid oder Public Cloud-Szenarien. Diese Vielfalt ist nötig, um die von Prüfern verlangte Transparenz und Durchgriffsrechte zu gewährleisten. Multicloud-Umgebungen konsistent zu managen ist für regulierte Unternehmen sehr komplex – aber beherrschbar, wenn die gewählte Cloud-Infrastruktur grundlegend darauf ausgelegt ist.

von Dr. Christian Thiel und Gero Skopinski, Finanz Informatik Technologie Service

Banken und Versicherungen nutzen unterschiedlichste Cloud-Plattformen. Für Bestandsanwendungen auf Basis klassischer Technologien nutzen Finanzdienstleister Linux-beziehungsweise Windows-Server-basierte Enterprise-IT-Umgebungen, die einfache Cloud-Prinzipien bieten. Dazu gehören beispielsweise eine schnelle Provisionierung von Maschinen und Services über ein Selfservice-Portal, das vollautomatische Bereitstellen von Datenbanken und Instanzen sowie eine tagesgenaue Abrechnung nach dem Pay-per-use-Modell. Diese Umgebungen sind entsprechend flexibel und eröffnen für nicht Cloud-fähige Kaufsoftware oder Legacy-Anwendungen Möglichkeiten eines modernen IT-Betriebs. Anwendungen können auf diese Plattformen nach dem Lift-and-Shift-Prinzip schnell und einfach migriert werden.



Gero Skopinski, Finanz Informatik Technologie Service

Quelle: Finanz Informatik Technologie Service



Dr. Christian Thiel, Finanz Informatik Technologie Service

Quelle: Finanz Informatik Technologie Service

Für das Entwickeln moderner Anwendungen auf Basis hochskalierbarer Architekturmuster wie Microservices benötigen Banken und Versicherungen eine Cloud Native-Plattform, die On-Premise Kubernetes als Cloud-Service zur Verfügung stellt.

Abgerundet wird die Cloud-Infrastruktur von Finanzdienstleistern durch einen aktiv gemanagten Zugang zu den Public-Cloud-Plattformen großer Hyperscaler wie Google Cloud. Insbesondere die datenschutzrechtlichen und regulatorischen Herausforderungen müssen adäquat adressiert sein, wenn regulierte Finanzdienstleister moderne Lösungsangebote auf Basis von Data Analytics oder Künstlicher Intelligenz (KI) nutzen.

Multicloud Management im regulierten Raum

Banken und Versicherungen benötigen für ihre integrierten Anwendungslandschaften übergreifende Management-Lösungen, mit denen Daten und Workloads plattformübergreifend gesteuert, überwacht und geschützt werden. Multicloud Management bezieht sich bei regulierten Unternehmen daher nicht allein auf übergreifende Prozesse und Tools für verschiedene Public Clouds, sondern umfasst auch die On-Premise betriebenen Community Clouds für die Enterprise IT und Container-basierte Anwendungen. Denn über diese läuft der Großteil der IT-Workloads.

Für das Management von Community Cloud-Plattformen und Public Cloud-Angeboten gibt es keine vollumfänglichen Multicloud Management Out-of-the-Box-Lösungen. Bei der Umsetzung passgenauer Konzepte ist es aus betrieblicher, technischer und regulatorischer Sicht sinnvoll, über alle Cloud-Plattformen hinweg einheitliche Prozesse und Tools zu implementieren. Denn auf diese Weise werden Synergien gehoben, Schnittstellenverluste vermieden und eine einheitliche Umsetzung regulatorischer Vorgaben unterstützt. Dieser Weg ist allerdings mit einem hohen Integrationsaufwand für das Einbinden verschiedener Cloud-Plattformen in eine einheitliche Tool- und Prozesslandschaft verbunden. Zudem besteht die Gefahr, die Vorteile der auf spezifische Cloud-Plattformen abgestimmten Management-Lösungen nicht ausschöpfen zu können.

“ Eine einfache Lösung gibt es daher nicht. Diesen Spagat lösen Banken und Versicherungen, wenn sie Cloud-Services aus einer Hand von Providern beziehen, die ihre Services auf die spezifischen Anforderungen der Finanzwirtschaft abgestimmt haben.”

FI-TS Cloud-Infrastruktur

FI-TS hat Cloud-Service auf Basis dedizierter Server-Hardware für den Betrieb von Kubernetes-Clustern vollautomatisiert und über eine API-Steuerung umgesetzt. In solchen Umgebungen werden beispielsweise Portalanwendungen, digitale Vertriebsplattformen oder Rechenkerne entwickelt, getestet und auch in Produktion genommen.

FI-TS hat zudem für das Nutzen von Services mehrere Hyperscaler ein Tool zur Abstraktion und Umsetzung von Compliance und Accounting-Vorgaben entwickelt. Damit kann der Provider mehrere Hyperscaler über ein einheitliches Management-Framework ansprechen.

Der auf den Finanzsektor spezialisierte IT-Dienstleister, Finanz Informatik Technologie Service (FI-TS), hat dazu beispielweise auf Basis seiner 3-Säulen-Cloud-Strategie konsistente Umgebungen und Multicloud Management-Verfahren entwickelt, mit denen Banken und Versicherungen neueste Cloud-Technologien nutzen und dabei die aufsichtsrechtliche Compliance sowie eine hohe IT-Sicherheit wahren können. Das Management ist dabei dreistufig aufgebaut. Es umfasst:

- unternehmensweit einheitliche Prozesse und Tools,
- Cloud-übergreifende Prozesse und Tools,
- Cloud- beziehungsweise Hyperscaler-spezifische Prozesse und Tools.

3-Säulen-Cloud für die Finanzwirtschaft

Der auf den Finanzsektor spezialisierte IT-Dienstleister Finanz Informatik Technologie Service (FI-TS) hat auf Basis einer 3-Säulen-Cloud-Strategie die FI-TS Finance Cloud entwickelt. Mit dieser können Banken und Versicherungen neueste Cloud-Technologien nutzen und dabei die aufsichtsrechtliche Compliance sowie eine hohe IT-Sicherheit wahren.

Die erste Säule, die so genannte Finance Cloud Enterprise, gewährleistet einen regulatorisch konformen Betrieb von Bestandssystemen. Als integraler Bestandteil einer Community Cloud für Banken und Versicherungen bietet sie Zugang zu „Managed Infrastructure-as-a-Services“. Virtuelle Maschinen beziehungsweise Infrastructure-as-a-Services (IaaS) stehen dabei in Form von Windows- und Linux-Instanzen mit einem Betriebsanteil (Managed Services) sowie „Plattform-as-a-Services“-Produkten zur Verfügung. Der Provider betreibt alle Instanzen in der Finance Cloud Enterprise in zwei räumlich getrennten Rechenzentren. Der wichtigste Vorteil dieser Cloud-Infrastruktur liegt im nahtlosen Einfügen der Plattform in die Bestandsarchitektur der Finanzdienstleister. Die Architektur muss nicht verändert werden.

In der zweiten Säule, der Finance Cloud Native, stellt der Provider in eigenen Rechenzentren Kubernetes als Cloud-Service zur Verfügung. Dazu wird dedizierte Server-Hardware für den Betrieb von Kubernetes-Clustern vollautomatisiert und API-gesteuert provisioniert. Zur Server-Bereitstellung nutzt der Provider die eigens entwickelte Open Source-Software metal-stack ([Webseite](#)). Diese verfügt über Schnittstellen zum Cloud-Provider-Interface in Kubernetes und dem Kubernetes-Cluster-Manager SAP-Gardener.

Autor Gero Skopinski, FI-TS



Gero Skopinski ist Bereichsleiter Cloud Solutions bei Finanz Informatik Technologie Service (FI-TS) ([Webseite](#)). Seit seinem Einstieg 2016 bei FI-TS treibt er die Cloud Strategie des IT-Dienstleisters voran. So ist die aktuelle 3-Säulen-Strategie auf seine Initiative entstanden.

Die dritte Säule der Cloud-Strategie, die Finance Cloud Public Integration, bietet Banken und Versicherungen den regulationskonformen Zugang zu Hyperscaler-Angeboten. Diesen Zugang stellt der Provider über eine Cloud Landing Zone bereit. Dabei berücksichtigt er Compliance-Anforderungen, etwa hinsichtlich der Aspekte Hybrid Connectivity, Tenant-Management und Identity-Management über Verzeichnisdienste wie Active Directory, Multi-Factor-Authentication, Key Management, Conditional-Access, Role Based Access Control, Logging, Monitoring, SIEM, Automation, DevOps, Cost Management und Risikomanagement.

Unternehmensweite Prozesse und Tools

Insbesondere für klassische Betriebs-Querschnittsprozesse wie das Incident-, Problem- und Change-Management, aber auch für betriebswirtschaftliche Themen, wie beispielsweise Accounting und Faktura-Management und auch regulatorische Themen, setzt FI-TS in seiner Community Cloud unternehmensweit einheitliche Prozesse und Tools ein. Ein Beispiel dafür ist etwa die plattformübergreifende Security-Strategie, die auf Basis eines plattformübergreifend eingesetzten Security-, Incident- und Event-Management (SIEM)-Tools realisiert ist. Damit kann der Provider seine Sicherheitsrichtlinien zentral überwachen und auch Events auf unterschiedlichen Cloud-Plattformen korrelieren. Ein anderes Beispiel ist das Identity- and Access-Management.

“ Über eine plattformübergreifend eingesetzte Identity- and Access-Management-Lösung managt der Provider nicht nur Rollen und Rechte, sondern ermöglicht auch das plattformübergreifend einheitliche Login von Nutzern.”

Cloud-übergreifende Prozesse und Tools

Der Einsatz von Cloud-übergreifenden Prozessen und Tools im Multicloud Management ist bei FI-TS eng verknüpft mit der Anwendung von DevOps-Prinzipen. Denn diese gewährleisten einheitliche und automatisierte Verfahren bei der Integration und beim Deployment von Anwendungen und Infrastruktur-Komponenten. Das ist beispielsweise beim regulatorisch notwendigen Nachweis der Ressourcennutzung von Hyperscaler-Angeboten wichtig. Da der Provider Public Cloud-Services ausschließlich über eine CI/CD-Pipeline deployed, kann er zu jeder Zeit nachweisen, welche Ressourcen zu welchem Zeitpunkt bei welchem Hyperscaler genutzt wurden.

Cloud-spezifische Tools und Prozesse

Um bei der Entwicklung und im Betrieb keine wesentlichen Informationen zu verlieren beziehungsweise zwischen den Cloud-Plattformen oder zur Legacy-IT keine aufwendige architekturelle Brücke für die Verbindung einsetzen zu müssen, nutzt FI-TS auch plattformspezifische Cloud Management-Prozesse und -Tools. Insbesondere für das Monitoring, das Logging und auch bei technischen Schnittstellen zum Datentransfer zwischen den Plattformen setzt der Provider auf spezifische Lösungen. Bei Bedarf bindet er diese in eine Gesamtlösung ein, wie etwa beim Monitoring und Metering. Hierzu nutzt FI-TS plattformspezifische Lösungen, die im Fall einer Störung volle Transparenz über die Auswirkungen auf den betroffenen Cloud-Plattformen bieten. Um die definierten Alarmierungswege plattformübergreifend und zügig einzuhalten, leitet der Provider dezentral auftretende Störungsalerts an ein Alert- und Event-Management-System weiter und wertet diese zentral aus.

“ *FI-TS hat damit das Multicloud Management in ihrer Community Cloud durchgängig organisiert. Dennoch muss der Provider wie alle Finanzdienstleister auch sein Multicloud Management in den nächsten Jahren immer wieder auf den Prüfstand stellen.*”

Denn die Public Cloud-Provider differenzieren ihre Angebote tendenziell immer stärker. Dies muss synchronisiert werden mit den klassischen Technologien, die auch auf absehbare Zeit fester Bestandteil der IT-Landschaft von Banken und Versicherungen sein werden. Hierfür scheint es auch weiterhin keine Standard-Lösung zu geben, so dass ein ausgewogenes Multicloud Management eine permanente Herausforderung bei der Digitalisierung der Finanzwirtschaft bleiben wird.

Autor Dr. Christian Thiel, FI-TS



Dr. Christian Thiel ist seit Januar 2020 in der Geschäftsführung von FI-TS ([Webseite](#)). Er trägt die Verantwortung für Compliance, Vertrieb, Marketing sowie Architektur- und Produktmanagement. Christian Thiel ist Experte für aufsichtsrechtliche Anforderungen an die IT der Finanz- und Versicherungsbranche und profunder Kenner des Markts.

Dr. Christian Thiel und Gero Skopinski, FI-TS ■

<https://bit.ly/3l0qe5z>