Drei Säulen für Compliance

Multi-Cloud-Management für regulierte Unternehmen

Cloud-Computing stellt regulierte Unternehmen vor Herausforderungen. Richtig komplex wird es, wenn Cloud-Grenzen zu überwinden sind. Worauf es dann beim Multi-Cloud-Management ankommt.

Gesetzliche Vorgaben erschweren Banken, Versicherungen und anderen besonderen Regulierungen unterliegenden Unternehmen den Weg in die Cloud. Sie müssen noch stärker als andere auf die Compliance der geplanten Infrastruktur achten. Diese muss auch eventuellen Überprüfungen standhalten – vor allem hinsichtlich des Schutzbedürfnisses der zu verarbeitenden Daten. Noch komplizierter wird es, soll die Infrastruktur sowohl den On- als auch den Off-Premises-Betrieb in Private-, Hybrid- oder Public-Cloud-Szenarien beherrschen. Dazu benötigen Finanzdienstleister eigene Cloud-Plattformen auf Linux- oder Windows-Servern, Microservice-orientierte Anwendungsumgebungen auf Basis von Kubernetes und Containern sowie den Zugang zu Public Clouds der Hyperscaler.

Multi-Cloud-Management bezieht sich daher bei regulierten Unternehmen nicht allein auf Prozesse und Tools, die Workloads in mehreren Public Clouds steuern, überwachen und schützen. Es bezieht sich auch auf die on Premises betriebenen, speziell für den Finanzdienstleistungssektor entwickelten Community-Clouds für die Enterprise-IT und containerbasierte Anwendungen, über die das Gros der IT-Workloads läuft.

Multi-Cloud für regulierte Umgebungen

Wie diese Anforderungen technisch und organisatorisch umgesetzt werden können, zeigt sich am Beispiel der Plattform und der Verfahren von Finanz Informatik Technologie Service (FI-TS), einem auf den Finanzsektor spezialisierten IT-Dienstleister. Mit einer Drei-Säulen-Cloud-Strategie hat er Umgebungen und Verfahren entwickelt, mit denen Banken und Versicherungen neueste Cloud-Technologien nutzen und dabei die aufsichtsrechtliche Compliance sowie eine hohe IT-Sicherheit wahren können.

Die erste Säule, die Finance Cloud Enterprise, gewährleistet einen regulatorisch konformen Betrieb vorhandener Systeme. Als Bestandteil einer Community-Cloud für Banken und Versicherungen bietet sie Zugang zu „Managed Infrastructure as a Service“, das heißt zu virtuellen Maschinen beziehungsweise Infrastructure as a Service (Iaas) in Form von Windows- und Linux-Instanzen mit einem Betriebsanteil (Managed Services) sowie „Platform-as-a-Service“-Produkten, konkret MS-SQL-, Oracle- und DB2-Datenbanken.

Alle Instanzen dieser Cloud betreibt FI-TS in zwei räumlich getrennten Rechenzentren – auf aktueller x86-Hardware in einem symmetrischen Aufbau über die Rechenzentren hinweg. Als Hypervisor dient VMware ESXi 7 inklusive Management über ein zentrales vCenter. Der Storage der VMs wird über die Standorte synchron gespiegelt und mit einem NetApp A700 Metrocluster via NFS bereitgestellt.

Zentraler Aspekt ist das nahtlose Einfügen der Plattform in die Bestandsarchitektur der Finanzdienstleister. Für Nutzer ist jederzeit transparent, ob eine VM in der Bestandswelt oder in der Cloud-Umgebung bereitgestellt wird. Windows-VMs werden beispielsweise direkt in die ADs des Kunden aufgenommen. Das gilt für den Fall, dass er mehrere ADs bei FI-TS, ein AD bei einem anderen Dienstleister oder eine Mischform betreibt. Weiter lässt sich die Finance Cloud Enterprise in die individuellen Netzkonzepte der verschiedenen Institute integrieren. FI-TS stellt nicht nur VMs bereit, sondern übernimmt auch den Betrieb und das Sicherheitsmanagement der Betriebssysteme.

Bare-Metal-basierte Cloud-Plattform

Die zweite Säule ist eine Plattform für Microservice-Architekturen: Finance Cloud Native. Dort steht Kubernetes als Cloud-Service bereit. Dedizierte Serverhardware für den Betrieb von Kubernetes-Clustern wird vollautomatisiert und API-gesteuert provisioniert. Zur Serverbereitstellung dient die selbst entwickelte Open-Source-Software metal-stack (metal-stack.io). Sie verfügt über Schnittstellen zum Cloud-Provider-Interface in Kubernetes und zum Kubernetes-Cluster-Manager SAP Gardener. Damit lassen sich sämtliche Skalierungs- und Automatisierungsfunktionen nutzen. Sobald Kubernetes erkennt, dass keine ausreichenden Ressourcen zur Verfügung stehen, reserviert es automatisiert innerhalb weniger Minuten zusätzliche Worker-Nodes.

Die Kubernetes-Services setzen auf die von der Cloud Native Computing Foundation (CNCF) veröffentlichten Versionen, Calico dient als Netzwerk-Provider, MetalLB als Loadbalancer, CSI-Provider für lokalen Storage und zentralen Netzwerkspeicher. Die Dienste sind so konfiguriert, dass sie sich ebenfalls über die Kubernetes-API verwalten lassen.

Eine der wenigen Architekturkomponenten, die nicht auf Open Source aufbauen, ist das zentrale Storage-System des Storage-Spezialisten Lightbits Labs. Die Orchestrierung persistenter Volumes in Kubernetes ist per CSI-Treiber in metal-stack integriert. Jedes Rechenzentrum verfügt damit knotenunabhängig über einen zentralen Block-Storage. Über das Kubernetes-Deployment werden automatisiert Volumes mit der jeweils benötigten Kapazität angelegt und an die Container angebunden. Das erfolgt per NVMe-over-TCP mit Bandbreiten bis zu 25 GBit/s je Worker-Node.

Die dritte Säule der Cloud-Strategie, die Finance Cloud Public Integration, eröffnet für Banken und Versicherungen den regulationskonformen Zugang zu Angeboten der Hyperscaler. Um diese für Kunden nutzbar zu machen, fungiert FI-TS als zentraler Serviceprovider für Public-Cloud-Services. Den Zugang zu den Hyperscaler-Angeboten stellt der Provider über eine Cloud Landing Zone bereit. Dabei berücksichtigt er Complianceanforderungen, etwa hinsichtlich der Aspekte Hybrid Connectivity, Tenant und Identity Management über Verzeichnisdienste wie AD, Multi-Faktor-Authentifizierung, Key Management, Conditional Access, Role-based Access Control, Logging, Monitoring, SIEM, Automation, DevOps, Cost Management und Risikomanagement.

Das Multi-Cloud-Management mehrerer Hyperscaler ist dabei Bestandteil eines umfassenden Managed-Service-Konzeptes. Es schließt in einem gestuften Servicemodell Leistungen ein wie Monitoring, Security und Access Manage-

ment, Netzwerkintegration, Accounting und Regulatorik.

Für das Accounting hat FI-TS als Abrechnungsplattform für Public-Cloud-Leistungen in Go ein Billing-Modul samt API entwickelt. Die Software sammelt die Billing-Records der Hyperscaler ein, bereitet sie auf und leitet sie in einem Hyperscaler-unabhängigen Format an das SAP-SD-System weiter.

Management für regulierte Bereiche

Für Community-Clouds und Public Clouds existieren noch keine vollumfänglichen Multi-Cloud-Management-Tools, die out of the box funktionieren. Aus betrieblicher, technischer und regulatorischer Sicht ist es daher erstrebenswert, einheitliche Prozesse und Tools über alle Cloud-Plattformen hinweg zu implementieren. Das vermeidet Schnittstellenverluste und erleichtert gleichzeitig das einfache und einheitliche Umsetzen regulatorischer Vorgaben.

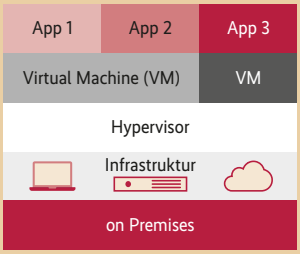
Dem steht der hohe Integrationsaufwand für das Einbinden verschiedener Cloud-Plattformen in eine einheitliche Tool- und Prozesslandschaft gegenüber. Darüber hinaus können spezifische Vorteile von Managementansätzen einzelner Cloud-Plattformen durch eine zu hohe Abstraktion verloren gehen. Zudem kann das Festhalten an den Betriebsweisen unter Umständen die in der Cloud möglichen beschleunigten Release- und Deployment-Verfahren ausbremsen.

Quelle: FI-TS

Drei-Säulen-Cloud-Strategie

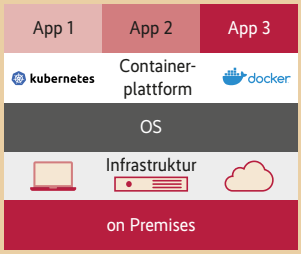
FI-TS Finance Cloud Enterprise

- schnelle Bereitstellung von Ressourcen
- standardisiert und automatisiert
- Sicherheit durch Hypervisor
- taggenaues Pay-per-Use
- Windows, Linux, Datenbank, Middleware



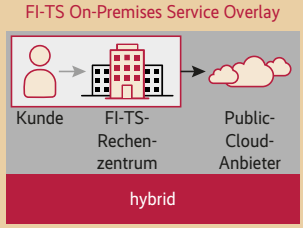
FI-TS Finance Cloud Native

- schnelle Bereitstellung von Ressourcen
- standardisiert und automatisiert
- Sicherheit durch Metal as a Service
- stundengenaues Pay-per-Use
- Container (Kubernetes), Streaming (Apache Kafka)



FI-TS Finance Cloud Public Integration

- Integration großer Public-Cloud-Provider in das digitale Ökosystem von FI-TS
- FI-TS übernimmt die Rolle des Service-Orchestrators
- compliant, standardisiert und transparent



Vor diesem Hintergrund wurde für das Management der Cloud-Umgebungen von regulierten Banken und Versicherungen eine dreistufige Vorgehensweise etabliert. Die umfasst das Aufsetzen und Nutzen

- unternehmensweit einheitlicher Prozesse und Tools;
- cloudübergreifender Prozesse und Tools;
- cloud- oder sogar Hyperscaler-spezifischer Prozesse und Tools.

Einheitliche Prozesse und Tools

Die Kategorie der unternehmensweit einheitlich eingesetzten Prozesse und Tools eignet sich besonders für klassische Betriebsprozesse wie das Incident-, Problem- und Change-Management, betriebswirtschaftliche Aufgaben wie Accounting und Faktura-Management oder regulatorische Anforderungen.

So setzt FI-TS beispielsweise zum Umsetzen seiner plattformübergreifenden Security-Strategie auf eine einheitliche technische Basis für das Security-, Incident- und Event-Management (SIEM). Sowohl die internen Cloud-Systeme und Infrastrukturkomponenten als auch die in einer Public Cloud bereitgestellten Services erfasst der Provider in der einheitlichen Log-, Monitoring- und Reporting-Plattform Splunk.

Auf dieser Grundlage lassen sich Sicherheitsrichtlinien einheitlich überwachen. Zudem kann er verschiedene Events auf unterschiedlichen Cloud-Plattformen korrelieren. Wird beispielsweise ein Security Incident durch einen Angreifer erkannt, können die Sicherheitsverantwortlichen im zentralen SIEM über alle Cloud-Plattformen hinweg prüfen, ob es zum Lateral Movement gekommen ist, also ob der Angreifer sich zwischen den Plattformen bewegen konnte. Dabei werden Muster und Korrelationen zwischen den verschiedenen Plattformen und Technologien ausgewertet.

Auch das Identity and Access Management (IAM) ist mit unternehmensweit einheitlichen Prozessen und Tools umgesetzt. Somit kann sich jeder User überall mit dem gleichen Log-in anmelden, egal ob auf einer externen Website, einem

Finance-Cloud-Enterprise-Server oder bei SaaS-Angeboten wie Teams. Über die plattformübergreifend eingesetzte IAM-Software Garancy Identity Manager verwaltet der Provider Rollen und Rechte. Toxische Rechtekombinationen beziehungsweise Separation-of-Duties-Konflikte (SoD-Konflikte) lassen sich damit auch über Cloud-Plattform-Grenzen hinweg erkennen und vermeiden – ein aus regulatorischer Sicht wesentlicher Aspekt.

Ein weiteres Beispiel für die unternehmensweit einheitlichen Tools und Prozesse ist das Key-Management-System (KMS) für verschlüsselbare Hyperscaler-Services. Der Provider übernimmt als neutraler Dritter das Schlüsselmanagement für die Datenverschlüsselung.

Als Software zum Generieren der Keys für die kryptografische Verschlüsselung von Daten und Authentifizierungen sowie für deren Management (verteilen, speichern beziehungsweise vernichten) kommt HashiCorp Vault zum Einsatz. Das stellt sicher, dass der Schlüssel jederzeit unter der eigenen Kontrolle bleibt, was vor allem bei Public-Cloud-Angeboten wichtig ist.

Cloudübergreifende Prozesse und Tools setzt der Provider im Multi-Cloud-Management insbesondere dann ein, wenn DevOps-Prinzipen angewendet werden. Das gewährleistet möglichst einheitliche und automatisierte Verfahren zur Integration und zum Deployment von Anwendungen und von Infrastrukturkomponenten.

Cloudübergreifende Tools und Prozesse

Um die aus regulatorischer Sicht notwendige Dokumentation und Rückverfolgbarkeit personifizierter Zugriffe auf Public-Cloud-Services zu gewährleisten, deployt FI-TS Services nur über eine CI/CD-Pipeline. Dabei verwaltet der Provider die Netzwerke, virtuellen Maschinen, Lastenausgleichsmodule und Verbindungstopologie mithilfe von Infrastructure as Code (IaC). So lässt sich zu jeder Zeit nachweisen, welche Ressourcen zu welchem Zeitpunkt bei welchem Hyperscaler genutzt wurden.

Um mehrere Hyperscaler über ein einheitliches Managementframework ansprechen zu können, hat FI-TS für die Public-Cloud-Integration-Services ein Tool zur Abstraktion und Umsetzung von Compliance- und Accounting-Vorgaben entwickelt. Dazu hat man die CI/CD-Pipeline auf Basis von GitLab um die eigene Software Cloud Generator ergänzt. Mit dieser ebenfalls in Go programmierten Software lassen sich Hyperscaler-Services per IaC deployen. Cloud Generator verwendet YAML-Dateien, in denen Nutzer benötigte Services wie virtuelle Server (IaaS) und SQL-Datenbanken (PaaS) Hyperscaler-unabhängig spezifizieren. Durch die Software stellt der Provider sicher, dass in Public Clouds auf Basis von Terraform-Blueprints nur die Services und Berechtigungen nutzbar sind, die für den jeweiligen Workload erlaubt sind. Auf diese Weise werden beispielsweise Entwicklungs- und Produktionsumgebungen strikt getrennt. Dies ist zur Umsetzung der Compliancevorgaben unbedingt erforderlich.

Cloudspezifische Tools und Prozesse

Cloudspezifische Prozesse und Tools kommen dann zum Einsatz, wenn durch das Vereinheitlichen der Multi-Cloud-Management-Tools zu viele für die Entwicklung und den Betrieb erforderliche Informationen verloren gehen würden oder wenn eine Brücke für die Verbindung zwischen den Cloud-Plattformen oder zur Legacy-IT notwendig ist. Dies betrifft insbesondere Monitoring und Logging sowie das Umsetzen technischer Schnittstellen zum Datentransfer zwischen den Plattformen.

Für das Monitoring und Metering dienen verschiedene Pakete, um im Fall einer Störung volle Transparenz über die Auswirkungen auf den betroffenen Cloud-Plattformen zu erhalten. Bei der Community-Cloud des Providers übernimmt das freie Prometheus das Servicemonitoring und Alerting und das ebenfalls freie Grafana die Visualisierung der Prometheus-Daten. Zur Überwachung der Hyperscaler-Dienste dienen die umfangreichen Monitoringservices der jeweiligen Anbieter. Das Nutzen der Hyperscaler-spezifischen Dashboards stellt sicher, dass im Störungsfall alle bereitgestellten Detailinformationen ausgewertet werden können und keine Spezifika durch eine übergreifende Konsolidierung verloren gehen.

Damit dennoch die definierten Alarmierungswege plattformübergreifend und zügig eingehalten werden, werden die in den Hyperscaler-Plattformen angelegten Störungsmeldungen an das zentrale Alert- und Event-Management-System ZIS weitergeleitet. Im Falle von Sicherheitsvorfällen generiert ZIS automatisch Tickets in der Plattform ServiceNow. (avr@ix.de)

Gero Skopinski
leitet den Bereich Cloud Solutions von Finanz Informatik Technologie Service (FI-TS) und treibt dort seit seinem Einstieg 2016 die Cloud-Strategie des IT-Dienstleisters voran.

Dr. Christian Thiel
ist Geschäftsführer von Finanz Informatik Technologie Service (FI-TS) und verantwortet unter anderem die Themen Compliance, Architektur- und Produktmanagement.