Einführung

Durch die Deutsche Verwaltungscloud (DVC) ergeben sich notwendige Fähigkeiten, die von den IT-Dienstleister in der öffentlichen Verwaltung im Bereich der Services, Betriebsmodelle und IT-Architektur erbracht werden sollen. In diesem Dokument wird das Zusammenspiel zwischen Cloud-Service-Anbietern, den Cloud-Service-Kunden, dem Cloud-Service-Portal (CSP) und den Netzwerk-Service-Anbietern beschrieben, sowie die technologischen Möglichkeiten, die durch den Einsatz von DevOps Praktiken geschaffen werden, die es den Dienstleistern ermöglichen, agiler und flexibler zu sein, um eine sichere und skalierbare benutzerorientierte Cloud-Erfahrung zu gewährleisten.

Anwendungsorientiertes Multi-Cloud-Design

Multi-Cloud Umsetzung der Deutschen-Verwaltungs-Cloud

Befähigung der Cloud-Service-Anbieter

Welche Services und Schnittstellen müssen Cloud-Service-Anbieter bereitstellen, um ihre Rechenzentrum-Services als Cloud-Services anbieten zu können?

Die Cloud-Service-Anbieter in der Deutschen Verwaltungscloud (DVC) werden ihre Services über ein Cloud-Service-Portal (CSP) zur Verfügung stellen, um den Kunden einen einfachen Zugang zu den verschiedenen Cloud-Services zu ermöglichen. Kunden können entweder direkt über das CSP oder indirekt über einen Cloud-Service-Vermittler auf die Services zugreifen, diese bestellen und nutzen. Das CSP bietet den Kunden eine zentrale Anlaufstelle für den Zugriff auf Cloud-Services und ermöglicht es den Anbietern, ihre Services über eine gemeinsame Plattform zu präsentieren. Kunden können auf diese Weise schnell und einfach zwischen den verschiedenen Cloud-Services wählen, die von den Anbietern in der DVC bereitgestellt werden. In Figure 1 sind links oben die Konsumenten und rechts oben die Anbieter dargestellt. In der Mitte das CSP stellt die Verbindung beider da und stößt die Business Prozesse bei den Cloud-Service- und Netzwerk-Service Anbietern an, die zur Bereitstellung des Services benötigt werden.

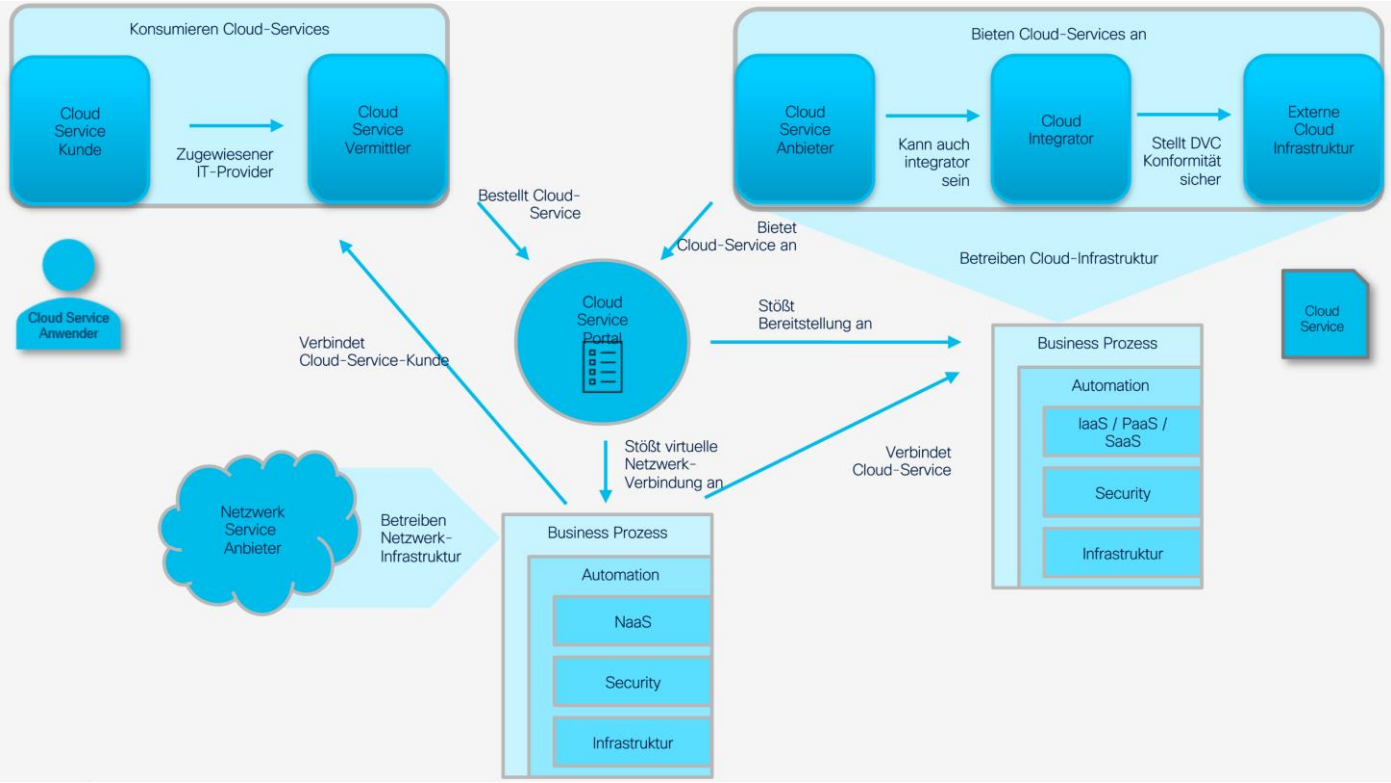

Figure 1.
DVC-Landschaft durch Zusammenspiel der Cloud-Service-Anbieter und Netzwerk-Service-Anbieter

Um sicherzustellen, dass Cloud-Services innerhalb kürzester Zeit (Minuten statt Monate) zur Verfügung stehen, ist es wichtig, dass die Plattformbetreiber im Voraus ausreichende Kapazitäten bereitstellen. Die schnelle und effektive Bereitstellung der Services erfordert ebenfalls, dass die notwendigen Schritte für die Bereitstellung einer Produktions- oder Entwicklungsumgebung (IT-Systeme bestehend aus Computer, Storage, Network) ohne manuelle Implementierungsschritte in einem vordefinierten Business-Prozess ausgeführt werden.

Sobald alle rechtlichen und kommerziellen Vorgaben innerhalb der DVC für die Erbringung des Cloud-Service des Cloud-Service-Kunden erfüllt sind, startet der Prozess der automatisierten Bereitstellung der Ressourcen. Dieser Prozess wurde zuvor von den verschiedenen Expertenteams des Cloud-Service-Anbieters entwickelt, getestet und bereitgestellt.

Im DevOps Betriebsmodell entwickeln die Teams in enger Zusammenarbeit zwischen Entwicklung und Betrieb ständig neue Services und verbessern bestehende. Nur in diesem Dreiklang zwischen klar definierten Cloud-Services, skalierbarer Infrastruktur und gelebtem DevOps können die Cloud-Service-Anbieter dem Cloud-Service-Kunden ein ähnliches Nutzererlebnis bieten, wie beispielsweise in der Public-Cloud der Hyper-Scaler.

Definition von Cloud-Services

Um standardisierte Cloud-Services bei allen Cloud-Service-Anbietern zu schaffen, ist es wichtig, dass ein Cloud-Service durch eine allgemein akzeptierte Programmierschnittstellen-Definition (Application Programming Interface, API) festgelegt wird. Das zentrale CSP muss beim Anbieten von Services (z. B. Container, Netzwerk, Infrastruktur) eine klare Erwartung an den gelieferten Service und die Fähigkeiten rund um diesen Service festlegen.

Das bedeutet, dass sich der dezentrale Cloud-Service-Anbieter an eine vom CSP festgelegte API-Definition halten muss. Die Cloud-Services sind daher im Cloud-Service-Portal klar definiert und können von den Cloud-Service-Kunden bestellt werden. Bei der Bestellung eines Cloud-Services wird aus dem Cloud-Service-Portal ein Business Prozess per API beim Cloud-Service-Provider zur Initialisierung angestoßen. Die Ausführung der Prozessschritte wird dem Cloud-Service-Kunden direkt angezeigt, und wenn alle Schritte erfolgreich abgeschlossen sind, wird der Zugang zum Cloud-Service bereitgestellt. Der Zugang zum Service würde über einen dezentralen Zugang zum Cloud-Service erfolgen. Dies erfordert eine vollständige Automatisierung der Bereitstellung von IT-Ressourcen, Softwarekomponenten und des Netzzugangs vom Cloud-Service-Kunden zum Cloud-Service-Anbieter.

Im Unterschied zu derzeitigen Rechenzentrum-Services der IT-Dienstleister müssen die Cloud-Service-Anbieter für die Bereitstellung und den Zugang zu den Cloud-Services also eine Technologie-Domänen übergreifende Automatisierung zur Verfügung stellen. Die Experten aus der Infrastruktur (Computer, Storage, Network), der Software-Entwicklung und des Betriebs stellen die notwendige Integration der verschiedenen Bestandteile des Cloud-Services durch APIs zur Verfügung. Kontinuierlich werden die Prozesse zur Provisionierung optimiert.

Die Verfügbarkeit der Cloud-Services muss durch die Sichtbarkeit der einzelnen Service-Bausteine von den Cloud-Service-Anbietern ständig nachgewiesen werden. Technologieübergreifende Reports in Echtzeit zeigen dem Cloud-Service-Kunden die Qualität der zugelieferten Services.

Die Sicherheit der Service-Kette, vom Bildschirm des Bürgers und des Sachbearbeiters bis zum Abschluss des Verfahrens, muss von den Cloud-Service-Anbietern in den Bereichen ihrer Verantwortung gewährleistet werden. Für diese geteilte Verantwortung von Cloud-Services brauchen die unterschiedlichen Organisationen einen abgestimmten Rahmen zur ständigen Kontrolle aller sicherheitsrelevanten Mechanismen. Für die konsistente Implementierung in den Sicherheitsbausteinen und für eine schnelle Reaktionsfähigkeit der Sicherheitsplattform auf Sicherheitsvorfälle ist eine durchgehende Automatisierung der IT-Sicherheitsplattform notwendig.

Einbindung von mehreren Cloud-Service-Anbietern

Wie müssen Cloud-Service-Anbieter verbunden werden, um die gewünschte Wechselfähigkeit zwischen Cloud-Service-Anbietern zu erreichen?

Die Cloud-Föderation im DVC-Kontext bezieht sich auf die Zusammenarbeit zwischen vielen föderalen Cloud-Service-Anbietern, um Cloud-Service-Kunden und Anwendungsentwicklern den nahtlosen Zugriff und die Nutzung von Ressourcen und Services von mehreren Cloud-Service-Anbietern zu ermöglichen, als ob sie Teil einer einzigen Cloud wären. Diese Zusammenarbeit kann den Kunden, den Service-Anbietern und der Gemeinschaft erhebliche Vorteile bieten.

Die Hauptziele einer Multi-Cloud-Architektur sind:

1. Verbesserte Flexibilität und Skalierbarkeit
2. Erhöhte Widerstandsfähigkeit und Verfügbarkeit
3. Erhöhte Sicherheit
4. Reduzierte Kosten
5. Verbesserte Innovation
6. Verbesserte Interoperabilität

7. Geringere Komplexität

Die Kernkomponenten für einen erfolgreichen Cloud-Verbund sind:

- Verteilte Cloud-Instanzen, die auf der Grundlage des im folgenden Abschnitt erläuterten Infrastructure-As-Code-Konzepts arbeiten können.
- Konsistente und nahtlose Netzwerkkonnektivität, einschließlich Zugangs- und Sicherheitsrichtlinien, wie im Abschnitt Multi-Cloud Netzwerk Architektur beschrieben.
- Datenaustauschstandard, wobei wir EDC und IDSA als die führenden Initiativen auf dem Markt ansehen, die sich langfristig an der SIMPL-Initiative der EU-Kommission orientieren.
- Katalog der Cloud-Services, als einziger Zugangs- und Validierungspunkt; ein Modell, das man in Betracht ziehen könnte, wäre die Gaia-X Federated Services Architektur.

Die Cloud-Föderation bietet viele Vorteile für Kunden, Service-Anbieter und die DVC-Gemeinschaft insgesamt. Sie kann Flexibilität, Belastbarkeit, Sicherheit, Innovation, Wettbewerb und Interoperabilität verbessern, sowie Kosten und Komplexität reduzieren. Durch Zusammenarbeit und gemeinsame Nutzung von Ressourcen können Cloud-Anbieter ein robusteres und effizienteres Cloud-Ökosystem schaffen, von dem alle Beteiligten profitieren.

Cloud-Service-Portal

Das Cloud-Service-Portal fungiert als zentrales Fenster zur Verwaltung und Steuerung der Hybrid Cloud-Infrastruktur und bietet eine verbesserte Kontrolle und Sichtbarkeit in allen Umgebungen. Das Portal bietet eine Vielzahl von Funktionen, die den Prozess der Multi-Cloud-Plattformverwaltung rationalisieren und vereinfachen. Während der gesamte Bereitstellungsprozess automatisiert ist, stellt das Portal die Integration der Unternehmensverfahren sicher. Es bietet eine eingehende Analyse der Nutzung und Nutzungsmuster, Abrechnungsberichte und Ratschläge, während die Sicherheit der Daten gewährleistet wird.

Ein ausgereiftes CSP bietet eine Vielzahl von Funktionen, einige der wichtigsten Funktionen sind hier aufgeführt:

- Selbstverwaltung (Self-Service)
- Dynamic User Interface
- Servicekatalog
- Provisionierung und Automatisierung
- Policy-Driven Orchestration
- DevOps/IaC Integration and Support
- Benutzer-Authentifizierung
- Rollenbasierte Zugangskontrolle
- Delegierung der Kontrolle
- Metering and Show Back
- Advisory
- Operation
- Reporting
- Security

Infrastruktur als Code

Die Standardisierung und Verwendung von "Infrastructure-as-Code" (IaC) ermöglichen ein schnelles automatisiertes Management der IT-Services und Infrastruktur, indem es die Verwaltung von Ressourcen in einer strukturierten und automatisieren Weise ermöglicht. Unter dem Begriff Infrastruktur verstehen wir die IT-Komponenten aus der physikalischen Dimension, also Computer, Netzwerke, Speichersysteme und der IT-

Sicherheit, sowie der logischen Dimension, also Software und Lizenzen zum Management und zur Virtualisierung.

Die Organisationen der IT-Dienstleister werden durch die Anwendung der IaC-Methode zum DevOps Betriebsmodell weiterentwickelt, um das gewünschte Nutzererlebnis zu erzielen. Bei einem DevOps-Modell arbeiten Entwicklungs- und Betriebsteams über den Lebenszyklus von Softwareanwendungen – von der Entwicklung und dem Test über die Bereitstellung bis hin zum Betrieb – zusammen. Durch die Fähigkeiten eines Automation Framework profitieren die Cloud-Service-Kunden und die Cloud-Service-Anbieter selbst.

- **Hohe Transparenz** – Verwaltung der Infrastruktur über die Versionskontrolle, die eine detaillierte Auditierbarkeit der **Änderungen bietet**
- **Minimierung menschlicher Fehler** – Automatisiertes Testen der Infrastruktur auf Schwachstellen oder Fehler mithilfe von Unit-Tests, Integrationstests und Funktionstests
- **Effizienz** – Vermeidung schriftlicher Dokumentation, da der Code selbst den Zustand der Maschine dokumentiert
- **Aufbrechen von Silos in der Organisation der IT-Dienstleister** – Möglichkeit zur Zusammenarbeit bei der Infrastrukturkonfiguration und -bereitstellung

Ein konsistentes Automation Framework bietet einen durchgängigen CI/CD-Workflow zur Bereitstellung logischer Konfigurationen unter Verwendung von Softwarearchiven und geeigneten Tools (z.B. Drone, Jenkins), um die Pipeline mit Eingabevalidierung, automatisierten Tests und Benachrichtigungen zu prozessieren.

Entwicklung eines Automation Framework

Basierend auf unserer Erfahrung in der Softwareentwicklung und vielen praktischen Implementierungen sind folgende Schritte erfolgsversprechend:

- Festlegung der Automatisierungsstrategie, Auswahl der Werkzeuge, Vereinbarung des Ansatzes für IaC
- Auswahl von Anwendungsfällen (User Stories und Use Case) und zugehörigen deklarativen Tasks
- Definition der Anforderungen eines Lösungsdesigns und Implementierungsplans
- Installation und Konfiguration der CI/CD-Pipeline gemäß den bei der Definition der Automatisierungsstrategie, der Anforderungen und des Lösungsdesigns festgelegten Vereinbarung
- Implementierung der definierten Anwendungsfälle (Use-Cases) über sogenannte inhaltlich zu vereinbarende „Automatisierungs-Sprints“

Everything-as-Code

Everything-as-Code (EaC) ist ein Ansatz zur Softwareentwicklung, bei dem Alles als Code behandelt wird - einschließlich Infrastruktur, Konfiguration und Anwendungscode. Dieser Ansatz ermöglicht die Automatisierung und Orchestrierung von Prozessen und die Verwaltung von Ressourcen als Code und sorgt so für Konsistenz und Wiederholbarkeit im Bereitstellungsprozess. Die Cloud-Automation-Plattform (CAP) verwendet IaC, um dem EaC-Paradigma zu folgen.

Dies wird über verschiedene Schichten innerhalb der Architektur erreicht. Die IaC-Schicht, die auf der Service-Schicht sitzt, verwendet CI/CD-Pipelines, um den deklarativen Ansatz zu implementieren. Die IaC-Schicht bietet auch eine North-Bound-API, sodass jede darunter liegende Komponente effektiv abstrahiert und als

Service angeboten werden kann. Die IaC-Schicht kommuniziert mit den Services über ihre jeweilige API.

Die Abstraktion zwischen den Schichten, vom zugrunde liegenden Service über IaC bis hin zur service-übergreifenden Orchestrierungsschicht, ermöglicht es dem Cloud-Service-Anbieter, Einstellungen, die Cloud-Service-Kunden im CSP bestellen können, schrittweise offenzulegen oder einzuschränken. Das Ziel ist, Vorlagen für den Service in IaC als „Rezept“ (wiederverwendbaren Code) zu definieren, die durch benutzer- und umgebungsspezifischen Variablen und aus der Single-Source-of-Truth (SOT) gefüttert werden können.

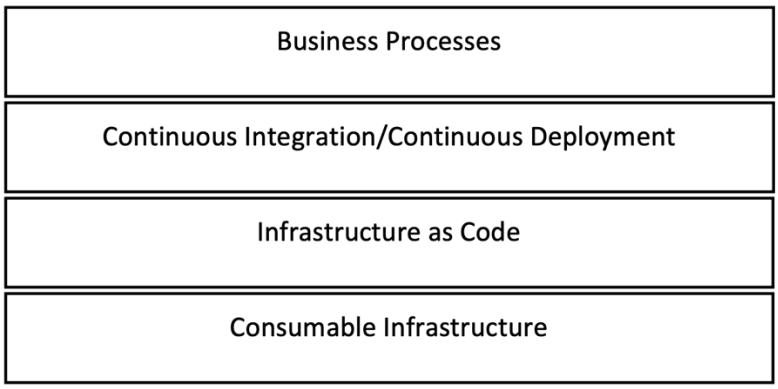

Figure 1: Automatisierung der Services durch DevOps Betriebs- und Entwicklungsmethoden

Da das Datenmodell in der IaC-Schicht herstellerneutral ist, entkoppelt die CI/CD-Pipeline die Implementierung des Datenmodells und die konkrete APIs der jeweiligen Anbieter. So werden Komponenten im Sinne der Souveränität austauschbar, ohne die Implementierung und die Architektur zu beeinträchtigen.

Die Orchestrierungsebene von CAP verwendet die API der Bereitstellungsebene, um komplexe Workflows zu implementieren. Dadurch kann die CAP einen einheitlichen und standardisierten Ansatz für die Verwaltung von Ressourcen über mehrere Clouds hinweg bereitstellen.

Die CAP setzt Best Practices aus der DevOps World für die Orchestrierung, Automatisierung und Bereitstellung von Ressourcen über EaC um. Die CAP verwendet Open-Source-Software zur Automatisierung der Bereitstellung von Ressourcen und bietet eine API und Prozessmodellierungstools für Orchestrierungs-Workflows.

Service Implementierung

Alle Services werden durch Infrastructure-as-Code (IaC) definiert, wobei Variablen rund um die Service-Bereitstellung gesammelt werden von:

- dem Benutzer
- dem Service-Bereitsteller
- der Source-of-Truth (SoT)

Der Anwender bestellt Services über den Servicekatalog, nutzt die bereitgestellten Services und kann benutzerspezifische Variablen definieren. Der Cloud-Service-Anbieter spielt eine Schlüsselrolle und ist für die Verwaltung der Service-Definition verantwortlich, die die Anwender nutzen werden. Der Cloud-Service-Anbieter arbeitet eng mit dem CSP zusammen, um die Vorlagen zu definieren, die den Anwendern im Servicekatalog angezeigt werden. Diese Service-Definition liegt im IaC-Format vor und wird über eine API in

Richtung CSP bereitgestellt. Die Definition gibt vor, welche Implementierungsvariablen benutzerspezifisch und welche umgebungsspezifisch sind. Die SoT hat die Aufgabe, die umgebungsspezifischen Informationen für die Bereitstellung zu verwalten und Informationen über bereitgestellte Services zu speichern.

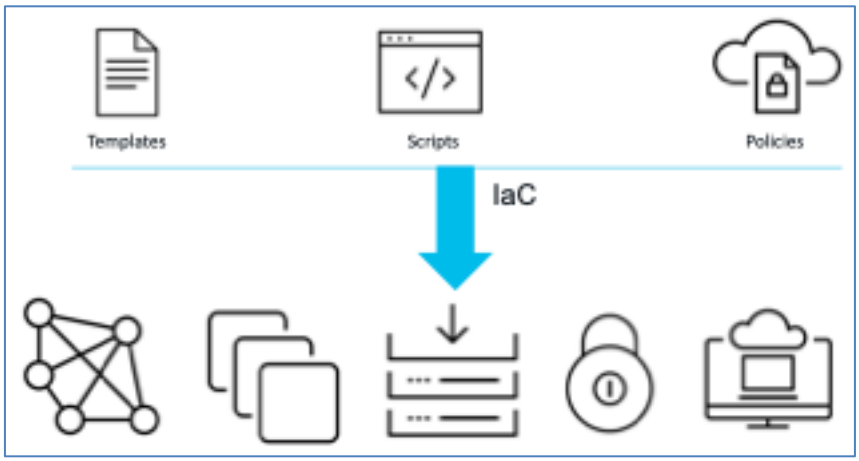

Figure 2: Everything as Code

Alle Services werden durch Infrastructure-as-Code (IaC) definiert, wobei die CAP-Service-bereitstellung durch einen API-Aufruf vom CSP den Business Prozess des Cloud-Service-Anbieters auslöst. Service-Abhängigkeiten werden durch die Integration der Service-Anbieter im CSP orchestriert.

Der Business Prozess speist Benutzervariablen in CI/CD-Pipelines für die Bereitstellung von Ressourcen. Die CI/CD-Pipeline verwenden Open-Source Software zur Automatisierung und IaC in Kombination mit der SoT, um Ressourcen bereitzustellen. Die Daten der SoT fungieren als Zielbeschreibung für die Cloud Plattform-Konfigurationselemente. Alle relevanten Service-Informationen bleiben im SoT bestehen, wie:

- Umgebungswerte für die verschiedenen Infrastrukturkomponenten
- Benutzerspezifische Konfigurationen
- Abrechnungsdaten

Dies wiederum ermöglicht es CAP, IaC sich von den tatsächlichen Konfigurationen zu entkoppeln, indem Blaupausen für IaC-Beschreibungen erstellt und die konkreten Informationen aus dem SoT und der Beauftragung geladen werden. Die modulare Architektur und die CI/CD Pipeline ermöglichen die Implementierung der Network-as-a-Service (NaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) und Container-as-a-Service (CaaS). Jedes Modul hat eine klar definierte API, sodass sowohl das Netzwerk, die Infrastruktur und die Plattform als Service über APIs bereitgestellt werden können. Aufgrund der Erweiterbarkeit von CAP können zusätzliche Services wie Beobachtbarkeit, Security und Service Mesh Management definiert und provisioniert werden.

Dieser Ansatz unterstützt das DevOps Modell, indem die Infrastrukturbereitstellungszeiten in lokalen Rechenzentren auf Minuten reduziert werden. Dadurch ist es möglich, CI/CD-Pipelines zu implementieren, die den gesamten Service-Lebenszyklus von der Entwicklungs-, Staging- und Produktionsumgebung automatisiert bereitstellen. Die abbildungsgleichen Umgebungen können vollständig automatisiert durch die CI/CD-Pipeline und die Informationen aus der SOT erstellt und heruntergefahren werden. Die Business-Prozesse zur Verwaltung der Ressourcen und Services werden in der Orchestration Engine der CAP modelliert und koordiniert. Die Orchestration Engine stellt ein Werkzeug zur grafischen Modellierung dieser und neuer Prozesse bereit, die über eine API genutzt werden. Mit agilen Teams, die die beschriebenen Tools, Prozesse und

DevOps-Methoden konsistent anwenden, wird die Liefergeschwindigkeit aufeinander abgestimmt, um die technischen und geschäftlichen Vorgaben zu erreichen.

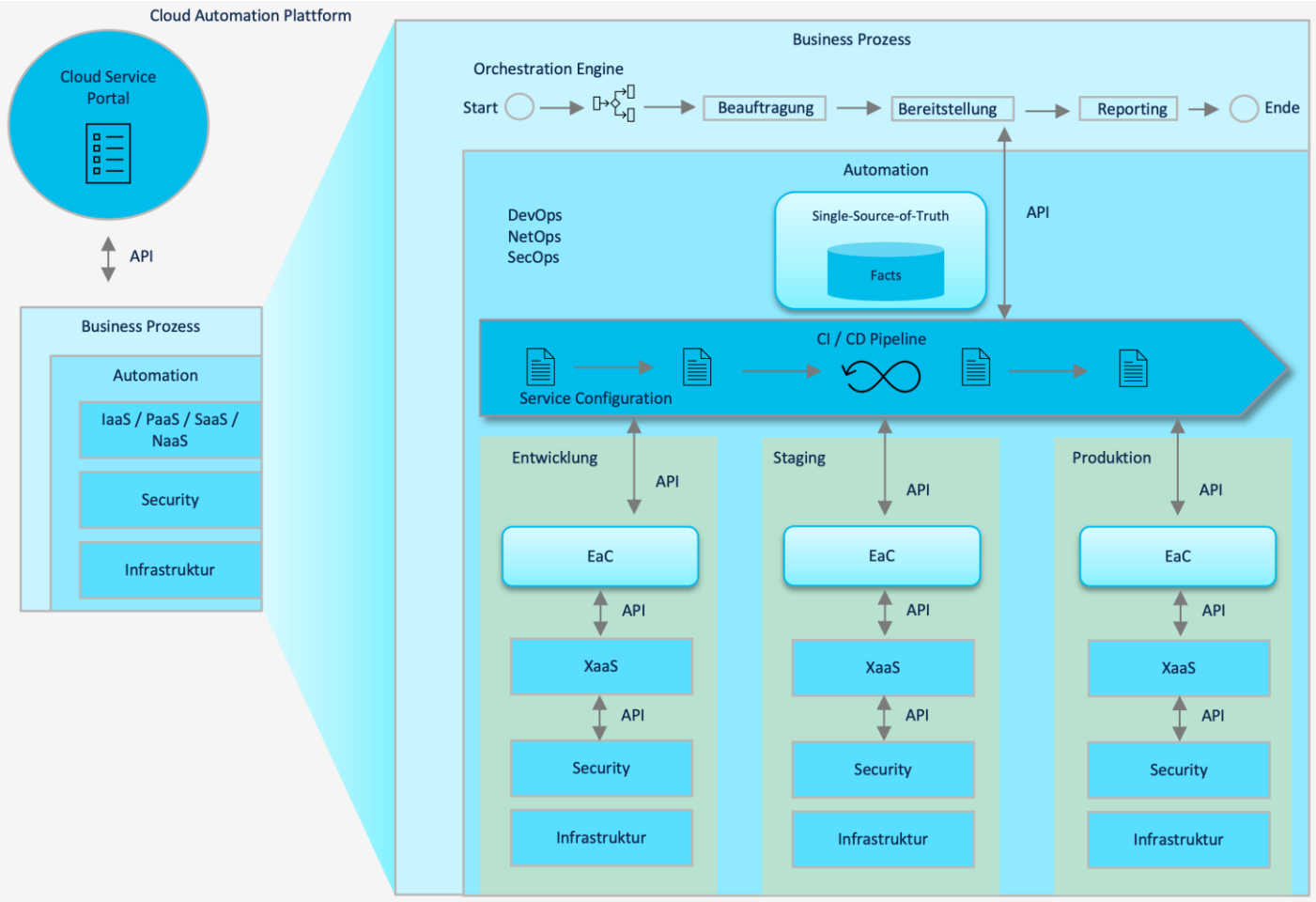

Figure 3: Zukünftige Service- und Betriebskonzepte nach DevOps für Cloud-Service-Anbieter und Netzwerk-Service-Anbieter

Integration des Cloud-Service-Portals und der Cloud-Automation-Plattform

Die beschriebene Orchestration Engine ermöglicht dem Cloud-Service-Anbieter Prozesse zu definieren, die die Grundlage für einen Produktkatalog darstellen. Die folgende Liste zeigt Bereitstellungs-Prozesse, die in der Orchestration Engine umgesetzt werden

- Virtual Machines VMs
- Kubernetes-Cluster
- Container

Neben den Entwickler-orientierten Workflows werden auch Infrastruktur-Workflows für

- Vernetzung
- Sicherheit
- Beobachtung

bereitgestellt.

Jeder dieser Workflows kann wiederverwendet und kombiniert werden, um komplexe Services zu erstellen. Beispielsweise verwendet der Workflow für ein Kubernetes-Cluster Netzwerk- und VM-Workflows, um das Netzwerk vorzubereiten und Controller- und Worker-Knoten für den Kubernetes-Cluster bereitzustellen. Jeder Workflow wird über eine API bereitgestellt. Das CSP nutzt die API, um seinen Cloud-Service-Kunden den Servicekatalog anzubieten. Jeder neue Workflow kann über eine API verfügbar gemacht werden, sodass neue Services zum Servicekatalog hinzugefügt werden können.

Multi-Cloud Netzwerk Architektur Überblick

Wie werden die Netzwerke zur Kopplung mehrerer Cloud-Service-Anbieter und deren Nutzer aufgebaut? Welche zentralen Instanzen sind für den sicheren Betrieb der Netzwerke notwendig?

Cloud-Computing hat in den letzten Jahren enorm an Bedeutung gewonnen und viele Institutionen setzen mittlerweile auf eine Kombination von Cloud-Services und Anbietern um ihren Kunden, die benötigten Services zur Verfügung zu stellen. Allerdings stellt die sichere Vernetzung von mehreren Cloud-Service-Anbietern und deren Nutzern eine technische und organisatorische Herausforderung dar. Auf der technischen Seite müssen neue Konzepte implementiert werden, da klassische Topologien und Regeln in der Cloud Umgebung nicht sinnvoll skalieren. Organisatorisch müssen Verantwortung zwischen Netzwerk-Service-Anbietern und Cloud-Service-Anbietern geklärt und überwacht werden. Kundenspezifische Netzwerke müssen sicher und automatisiert bis in die Cloud-Service-Anbieter bereitgestellt werden. Dazu ist eine Normierung der API und des verwendeten Daten-Modells wünschenswert.

Zur Vereinfachung gehen wir hier nicht auf die Vernetzung innerhalb eines Cloud-Service-Anbieters ein, sondern nur auf die Anbindung an die Kunden-Netze und die Verbindungen zwischen Cloud-Service-Anbietern. Moderne Netze nutzen via Software definierte Technologien in allen Ebenen. Glasfaser ist die Basis für skalierbare Verbindungen. Optische- und Transport-Netze werden immer weiter bis in 400G Coherent-Transceivers integriert. Hier werden die optischen Bauteile (Laser, Receiver, Modulator) und die Digital-Signal-Prozessoren (DSP) in einem Interface zusammengeführt. Neue DWDM-Architekturen stellen auf einer Glasfaser theoretisch 80 Wellenlängen auf DWDM-Systemen mit Bandbreiten von 400G pro Wellenlänge auf IP-Ebene bereit. Auf einer Dark-Fiber steht also ein Vielfaches von 400G Ethernet zur Anbindung von Cloud-Service-Anbietern zur Verfügung.

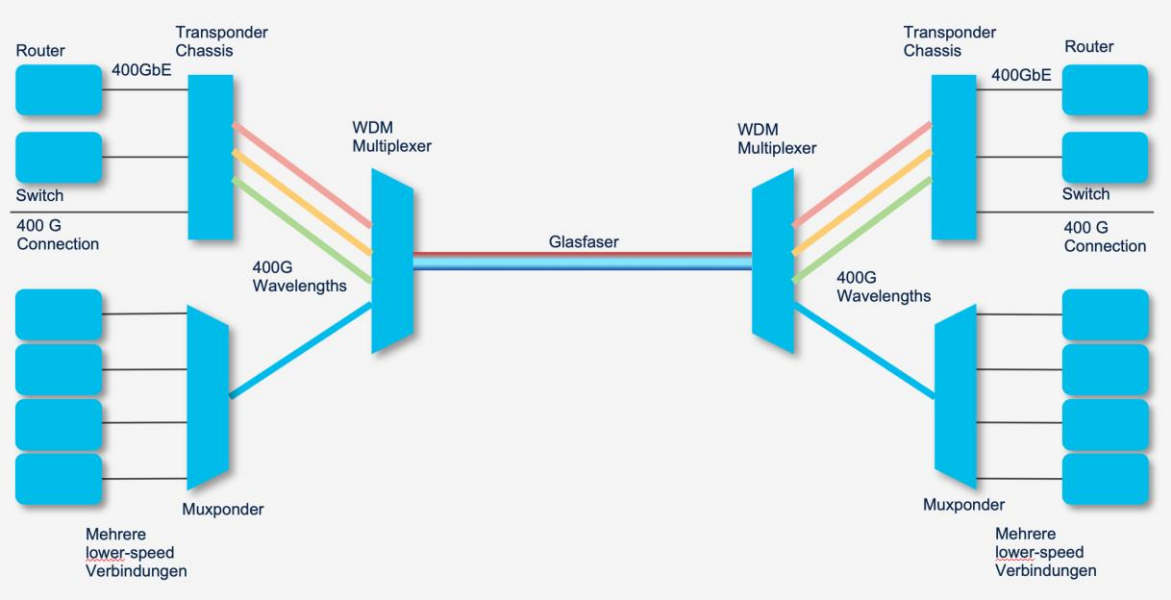

Figure 4: Abbildung Optische Transportnetze

Bei Anbindungen von Cloud-Service-Anbietern ist zu berücksichtigen, wie viele Nutzer in welcher Art und Weise auf welche Service gleichzeitig zugreifen. Abhängig vom verwendeten Service werden für die Netzdimensionierung klassische Überbuchungsmodelle von 1 zu 50 oder höher verwendet. Solch eine Anbindung kann für einfache Web-, Mail- oder Dateiablage-Systeme sinnvoll sein. Moderne Video- oder Echtzeit-Dienste benötigen andere Modelle, da die Servicequalität bei eintretender Überbuchung im ungünstigen Fall für alle Teilnehmer schlechter wird.

Die Verkehrsströme der Services zu erkennen, so früh wie möglich zu klassifizieren und die Anforderungen an die Netzwerke in der Planung zu berücksichtigen, ist bei Cloud Anbindungen besonders wichtig. Im Idealfall geben die Anwendungen das notwendige Transportprofil über die Klassifizierung dem Paket mit auf den Weg und stellen das Verhalten des Netzwerks damit ein.

Ab OSI-Layer 3 stellen Software-Definierte Wide-Area-Netze (SD-WAN) unterschiedliche Transport Verhaltensweisen (Transport-Profile) zur Verfügung. Mit diesen zentral gesteuerten Netzen können dynamisch die Wegeführung, die Bandbreite, die möglichen Verbindungen, die Quality-of-Services (QoS) und die Sicherheitsregeln pro Verkehrsstrom eingestellt werden. Die Endpunkte der spezifischen SD-WAN pro Service und Kunden (SD-WAN Edge) werden innerhalb der Virtual-Private-Cloud der verschiedenen Cloud-Service-Anbieter implementiert.

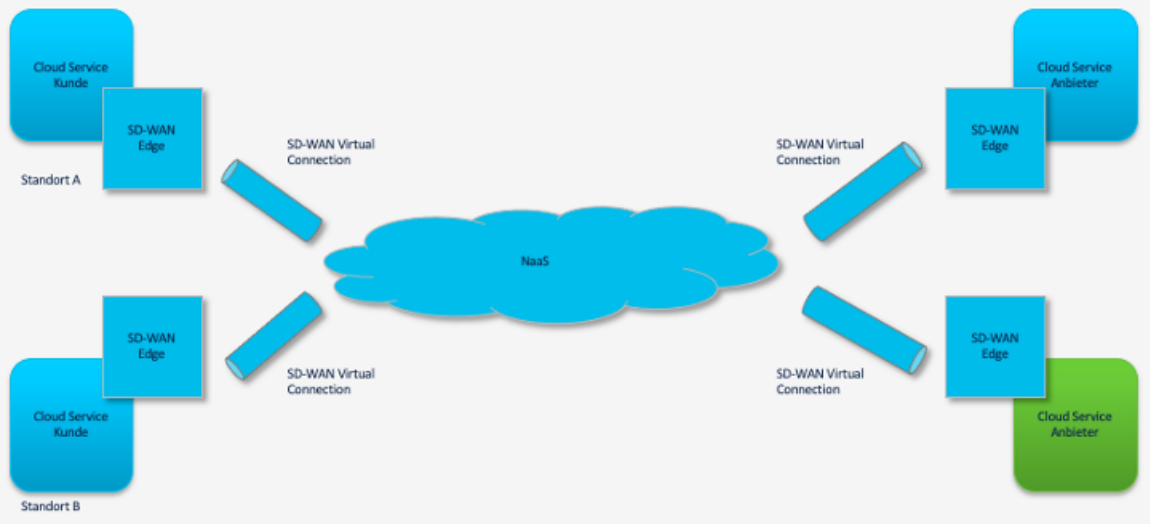

Figure 5: Abbildung Logische Software definierte Netzwerke (SD-WAN) zur Cloud Anbindung

Die Netzwerke werden als Plattform betrieben und als Network-as-a-Service (NaaS) bereitgestellt. Die Kontroller der Optischen-, Transport- und IP-Schichten werden weitestgehend integriert, aufeinander abgestimmt und durch die Orchestrierung der Netzkonfigurationen (siehe IaC) dynamisch angepasst. Diese Änderungen folgen ausschließlich den Mechanismen, die vom jeweiligen Expertenteam zur Verfügung gestellt wurden und werden nur per API angesprochen.

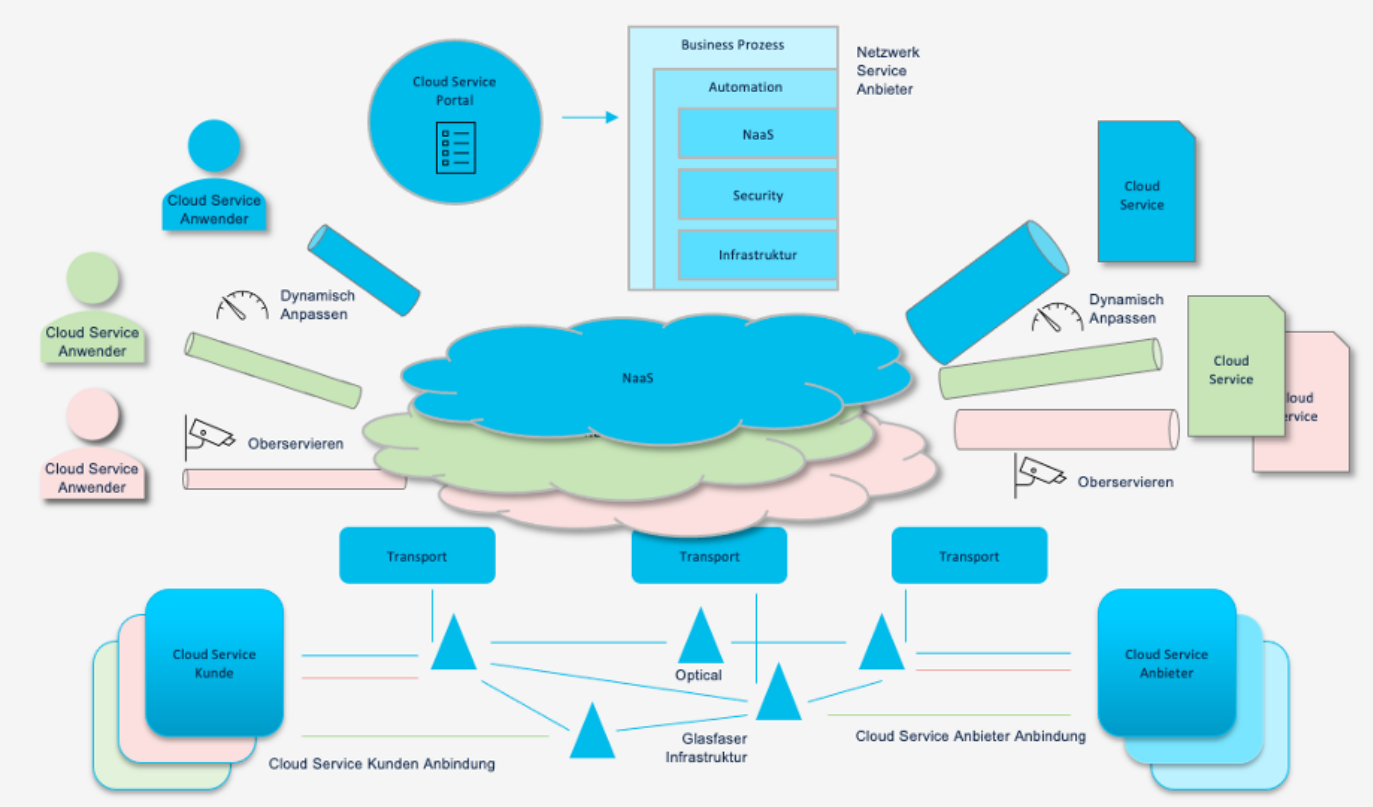

Figure 6: Abbildung Netzwerk-Service-Anbieter Aufbau und Betrieb

Damit die Verkehrs- und Sicherheitsregeln durchgesetzt werden können, ist eine hohe Sichtbarkeit und Überwachung des Netzwerks notwendig. Nur so kann festgestellt werden, welche Services transportiert werden, hinzukommen, ob die bestehenden Regeln durchgesetzt werden und ob es Unregelmäßigkeiten im Zugangsnetz gibt, die Einfluss auf die Nutzungs-Qualität und Sicherheit aller haben.

Durch eine Kombination aus aktiven und passiven Monitoring-Technologien können in Echtzeit Störungen im Netz, Veränderungen von Anwendungsverhalten, Nutzer-Einschränkungen und Beeinflussung der ursprünglichen Ziele der Cloud-Services erkannt werden und durch die tiefgehende Analyse über den gesamten Technologie-Aufbau, von der Glasfaser bis zur Datenbank-Performance im Cloud-Service-Anbieter, schneller behoben werden. Die Cloud-Anbindungen und die Cloud-Services werden aus Sicht des Nutzers überwacht, dazu wird der gesamte Anwendungsfluss über mehrere Cloud-Services und Netzwerk-Services analysiert und steht schon bei der Entwicklung der Anwendung den Entwicklern zur Verfügung. Bestehende Abhängigkeiten von Anwendungen und Services in der Multi-Cloud-Umgebung werden sichtbar gemacht und kontinuierlich überwacht.

Die Auswertung der Überwachung der Verkehrsströme und der Anwendungsverhalten führt mit der Dynamik der Software-Definierten Netze zur Möglichkeit, automatisiert Verbesserung der bestehenden Services durch eine Veränderung der Netzwerk-Services und durch Verschiebung der Ressourcen in andere Cloud-Service-Anbieter durchzuführen. Die Ressourcen können je nach Last dynamisch hoch- oder runtergefahren werden, um Einsparungen, Verbesserung der Performance und der Nutzererfahrung zu erzielen.

Die Informationen zu den Verkehrsströmen der Anwendungen und die Benutzer-Rechte sind in allen Netzebenen zu bewahren und für die Steuerung der Verkehrsströme zu nutzen. Durch Gruppenkennzeichnungen (Group Tags) werden Zugriffsberechtigungen im Netzwerk ausgewertet und unzulässige Verbindungen frühzeitig unterbunden, bevor sie andere Nutzer oder Anwendungen in der

Performance beeinflussen. Diese Metadaten sollen in jedem Netzabschnitt und an den Netz-Übergängen erhalten bleiben.

Bei konsequenter Umsetzung können Engpässe, potenzielle Probleme und Beeinträchtigungen frühzeitig erkannt werden, bevor sie für den Nutzer spürbar werden. Die Umsetzung einer zentralen Rechteverwaltung und das dynamische Zu- und Abschalten von Ressourcen und Services wird durch diese moderne Netzwerkarchitektur ermöglicht.

Realisierung der IT-Schutzziele

Überwachung der Services

Wie können die Multi-Cloud-Services aller beteiligten Cloud-Service-Anbieter in allen Ebenen überwacht werden?

Die Cloud-Services können von unterschiedlichen Cloud-Service-Anbietern an Cloud-Service-Kunden zur Verfügung gestellt werden. Diese Services können Speicher- oder Rechenleistung, aber auch Software und Applikationen umfassen. Die Cloud-Service-Anbieter haben die Möglichkeit ihr eigenes Rechenzentrum, als auch externe Cloud-Provider, sowie Public Cloud Provider einzusetzen. Das kann zu komplexen Abhängigkeiten zwischen Cloud-Service-Kunde, Softwarebetreiber, Netzwerk-Service-Anbieter und Cloud-Service-Anbieter führen.

Für eine hohe Akzeptanz der DVC ist die zuverlässige Verfügbarkeit von Cloud-Services über alle Ebenen und Anbieter hinweg stets zu gewährleisten. Das kann nur durch lückenlose Sichtbarkeit aller beteiligten Service-Bausteine garantiert werden. Die Überwachung der Multi-Cloud-Services muss Ende-zu-Ende, das heißt vom Cloud-Service-Kunden bis zum Cloud-Service-Anbieter, implementiert und umgesetzt sein.

Alle beteiligten Cloud-Service-Anbieter müssen sich mit Service-Level-Agreements (SLA) auf hohe Verfügbarkeiten verpflichten und damit Garantien für die Softwarebetreiber bereitstellen. Dahinter steht die Frage: Wie kann ich als Softwarebetreiber die Qualität meiner Services überwachen, damit die Cloud-Service-Kunden die versprochenen Leistungen erhalten?

Die Softwarebetreiber müssen jederzeit und selbstständig die Möglichkeit haben, die eigenen Services zu überwachen. Dabei steht der proaktive und reaktive Support im Fokus. Einerseits sollten automatische Überwachungs- und Monitoring-Tools zum Einsatz kommen, um proaktiv auf Änderung oder Auffälligkeiten im Netzwerk reagieren zu können. Andererseits muss der Softwarebetreiber die Chance haben, auf Kundenbeschwerden zu reagieren. Der reaktive Support braucht Möglichkeiten für ein Troubleshooting in der gesamten Service-Chain. Die Überwachungsdaten sollten für einen verhältnismäßigen Zeitraum abgelegt und aufbewahrt werden, um vergangene Meldungen zu analysieren.

Ein wichtiger Bestandteil einer umfassenden Sichtbarkeit sind übergreifende Reports in Echtzeit, die die Qualität der Services zeigen. Dabei ist sowohl das Überwachen auf der Applikationsebene und der Netzwerkebene unabdingbar. Die Chancen der Applikationsüberwachung liegen in der Performanceoptimierung, im Fehlermanagement und der Nutzer-Erfahrung. Die Netzwerkebene teilt sich in logische und physikalische Netzwerke auf. Beide Netzwerke müssen überwacht und sichtbar werden, um Ausfällen und Unterbrechungen zügig identifizieren zu können.

Ein zusätzlicher Aspekt der Überwachung ist die Datengrundlage für Optimierungen der Softwarequalität. Eine genaue Analyse der Antwortzeiten einzelner Softwaremodule ermöglicht eine Verbesserung der Softwarequalität und damit eine bessere Nutzung der Hardwareressourcen. Diese Optimierung ist sowohl im Sinne der Cloud-Service-Nutzer und der Nachhaltigkeit.

Die Überwachung von Applikationen sowie Netzwerken über Technologiedomänen und Service-Anbieter hinweg ist ein fundamentaler Baustein einer Multi-Cloud Strategie. Die Sichtbarkeit über den gesamten Technologie-Aufbau führt zu einer effizienteren und zuverlässigeren DVC.

Abkürzungsverzeichnis

API	Application Programming Interface
CaaS	Container-as-a-Service
CAP	Cloud-Automatisierungs-Plattform
CI/CD	Continuous Integration/Continuous Delivery
CSP	Cloud-Service-Portal
DevOps	Development und Operations
DSP	Digital-Signal-Prozessor
DVC	Deutsche Verwaltungscloud
DWDM	Dense Wavelength Division Multiplexing
EaC	Everything-as-Code
IaaS	Infrastructure-as-a-Service
IaC	Infrastructure as Code
NaaS	Network-as-a-Service
PaaS	Platform-as-a-Service
QoS	Quality-of-Service
SD-WAN	Software-Defined Networking in einem Wide Area Network
SLA	Service-Level-Agreements
SoT	Source-of-Truth