



Microsoft Azure

Aufbau von hybriden Infrastrukturdiensten

inkl. Windows virtual Desktop



**Das Handbuch
für IT-Systemarchitekten, Berater
und Administratoren**

Vorwort

Als Microsoft Ende 2008 die ersten Pläne zum Aufbau einer eigenen Cloud Plattform veröffentlichte, konnte ich ehrlich gesagt mit dem Thema gar nichts anfangen. Zu jener Zeit war ich schon einige Jahre Infrastruktur Solution Architect. Mein Fokus lag ganz klar auf der Planung und dem Aufbau von on-premises Infrastrukturmgebungen sowie dem Lösungsdesign zur zentralen Bereitstellung von virtuellen Arbeitsplätzen mit Hilfe von Citrix Technologien.

Anfang 2010 war es dann soweit - die Azure Plattform wurde veröffentlicht und die ersten IaaS und PaaS Dienste standen zur Verfügung. Nach den ersten Versuchen und einem vorsichtigen Herantasten an die neuen Möglichkeiten hielt sich allerdings bei mir persönlich die Begeisterung nach wie vor in Grenzen. Ich konzentrierte mich weiterhin auf meine Kernkompetenzen und gehörte zu den typischen Vertretern der Fraktion „zu schwerfällig, zu kompliziert und zu teuer“. Ich weiß nicht mehr genau, warum ich so eine Abneigung gegen die Azure Cloud hatte - aber wahrscheinlich war auch ein wenig Angst und Unsicherheit dabei, da diese Technologie doch meine gesamte Erfahrung und mein Wissen in Frage stellen könnte (das dachte ich zumindest).

Mit der Einführung des Azure Resource Managers (ARM) im Jahr 2015 sollte sich dann alles schlagartig ändern. Die Provisionierung von Ressourcen wurde vereinfacht, die Funktionalität gefühlt täglich erweitert, die Preise wurden immer attraktiver und das Office365 Angebot hatte mittlerweile Cloud-Services zu einem gewissen Grad

etabliert. Damit waren die Vorteile vor allem im KMU-Umfeld nicht mehr von der Hand zu weisen. Die Anzahl von Projektanfragen stieg steil an und innerhalb kürzester Zeit wurden klassische Infrastruktur-Projekte mit hybriden IaaS / PaaS und vor allem SaaS Technologien - allen voran natürlich die Office365 Klassiker Exchange Online / SharePoint Online und OneDrive for Business - geplant und aufgebaut.

Und was soll ich sagen, innerhalb kürzester Zeit habe ich begonnen, mich wohl zu fühlen. Ich habe rasch erkannt, dass die Möglichkeiten der Nutzung von Azure Services fast unbegrenzt sind und mir als Solution Architect neue Lösungen und Techniken zur Verfügung standen. Mit geringem Aufwand konnten beeindruckende Hybrid-Lösungen aufgebaut werden und es eröffnete Kunden komplett neue Ansätze zur sicheren, stabilen und effizienten Bereitstellung ihrer IT-Anforderungen. In den letzten Jahren durfte ich einige sehr große hybrid-Designs erstellen und ich habe zahlreichen Kunden auf ihrem Weg in die Azure Cloud begleitet. Bei sehr vielen Vorträgen und Trainings musste ich allerdings erkennen, dass ein Großteil der Probleme und Ängste der Kunden heute auf ein falsches Verständnis der Technologien oder ein falsches Basis-Infrastrukturkonzept zurückzuführen sind. Diese Erkenntnisse haben mich dazu bewegt, das vorliegende Buch zu verfassen. Es soll IT-Systemarchitekten, Beratern und Administratoren gleichermaßen dabei helfen, die benötigte Azure Infrastruktur zu planen und aufzubauen!

Einen besonderen Dank möchte ich auch in diesem Buch meiner wunderbaren Frau aussprechen. Durch ihre bedingungslose Unterstützung und ihr einzigartiges Wesen ist es mir möglich, Träume zu leben und meine Ziele zu erreichen.

Göran August Eibel

Enterprise Solution Architect & Technology Evangelist @

<https://www.gecon.at>

Übersicht

Abschnitt I - Grundlagen Azure Infrastruktur

- Bereitstellungsarten in der Cloud - IaaS / PaaS / SaaS
- Azure Ressourcen-Management
- Azure Networking / NSGs und Traffic-Management
- Azure Storage und HA-Optionen
- Azure Virtual Machines
- Azure Active Directory und AD-Connect
- Ausgewählte Azure PaaS Services

Abschnitt II - Aufbau einer hybriden Infrastruktur

- Schritt-für-Schritt Anleitung zum Aufbau einer hybriden Basisinfrastruktur
- Konfiguration von virtuellen Netzen und Subnetzen
- Verbindungsaufbau mit Hilfe der Azure Gateway Services
- Erweitern der on-premises Active Directory Domain Services Strukturen
- Aufbau und Integration einer AD Federation Umgebung inkl. Load-Balancer
- Einrichten von Storage Accounts inkl. Azure File-Share und Azure File-Sync
- Verwendung von Scale-Sets und Monitoring-Services

Abschnitt III - Optionale und erweiterte Azure Dienste

- Azure Bastion – Konfiguration und Betrieb
- Einführen von Azure MFA (Multi-Faktor Authentifizierung)
- Nutzung der Azure Monitor Funktionen
- Azure Backup und Funktionen der Recovery Services Vault
- Azure Security Center
- Azure Security Center – Maßnahmen zur Erhöhung der Sicherheit
- Azure Security Center – Prozesse und Management

Abschnitt IV – Windows virtual Desktop

- Definition und Planung eines modernen virtuellen Arbeitsplatzes
- Grundlegende Architektur und Technologien
- Konfiguration einer Azure-basierten WvD Lösung
- Provisionierung von Workplace-Umgebungen
- Anpassungen und Individualisierung
- Applikationsmanagement
- Personalisierung und Zugriff auf den zentralen virtuellen Arbeitsplatz

Inhaltsverzeichnis

Vorwort

Übersicht

Einführung

Aufbau des Buches

1. **Grundlagen**

1.1 Definitionen und Abkürzungen

1.2 Cloud Computing-Typen

 IaaS – Infrastructure as a Service

 PaaS – Platform as a Service

 SaaS – Software as a Service

1.3 Azure Services

 1.3.1 Services für den Aufbau einer hybriden
 Infrastrukturumgebung

1.4 Azure Ressourcen-Management

 Verwaltungsgruppen (Azure Management
 Groups)

 Abonnements (Subscriptions)

 Ressourcengruppen & Ressourcen (Azure
 Resource Groups & Resources)

 1.4.1 RBAC – Role-based Access Control

1.5 Azure Verfügbarkeit

 1.5.1 Availability Sets – Verfügbarkeitsgruppen /
 SLA 99,95%

1.5.2 Availability Zones – Verfügbarkeitszonen /
SLA 99,99%

2. **Azure Networking**

2.1 Grundlagen

2.1.1 Virtual Network – VNET

2.1.2 Service Endpoints

2.1.3 VPN Gateway

2.1.4 ExpressRoute

2.2 Azure Virtual WAN

2.3 Traffic Management

2.3.1 System-Routen und benutzerdefinierte
Routen

2.3.2 Load Balancer

2.3.3 Traffic Manager

2.4 Security

2.4.1 DDoS Protection

2.4.2 Azure NSGs – Network Security Groups

2.4.3 Azure ASGs – Application Security Groups

3. **Azure Storage**

3.1 Storage Account HA-Konfiguration

3.2 Blob Storage

3.2.1 Blob Storage Access Tiers

3.3 Azure Files

3.4 Storage Security

3.4.1 Netzwerkzugriff

3.4.2 Access Keys

4. **Azure VMs**

- 4.1 VM Disks
- 4.2 Zugriff auf VMs
- 4.3 Verfügbarkeit von VMs
 - 4.3.1 Scale Sets

5. **Identity Management**

- 5.1 Azure AD Funktionen
- 5.2 Azure AD Connect und Authentifizierung
 - 5.2.1 Passwort Hash Synchronisation
 - 5.2.2 Pass-Through Authentifizierung
 - 5.2.3 Active Directory Federation
- 5.3 Azure AD – Erweiterte Funktionen
 - 5.3.1 Azure AD Connect Health
 - 5.3.2 Azure MFA
 - 5.3.3 Azure Identity Protection

6. **Azure Monitor**

- 6.1 Monitor & Visualize
- 6.2 Query & Analyze Logs
- 6.3 Setup Alert & Actions

7. **Azure Serverless Computing**

- 7.1 App Service Plan & Web-Apps
- 7.2 Container Services
 - 7.2.1 Azure Kubernetes Service
- 7.3 Azure Data Protection
 - 7.3.1 Azure VM Data Protection

8. **Summary - Abschnitt I**

9. **Implementierung einer hybriden Infrastrukturumgebung**

9.1 Übersicht und Reihenfolge der Implementierung

10. **Azure Konto & Tenant**

10.1 Grundlegende Tenant Konfiguration

10.2 Domännennamen und Benutzer

10.3 Azure Policy

10.4 RBAC

11. **Aufbau der Netzwerk-Infrastruktur**

11.1 VNET Konfiguration

11.2 Subnetze

11.2.1 Access Control (IAM) - RBAC

11.3 VPN Gateway Verbindung

11.3.1 Anlegen einer eigenen Active Directory Site für Azure

12. **Aufbau der hybriden Authentifizierungsumgebung**

12.1 Erweitern der on-premises AD Domäne

12.1.1 Installation AZ-DC01

12.1.2 Installation der Windows Server Rollen und Features

12.2 AD Connect

12.2.1 Vorbereitungen

12.2.2 Installation

12.2.3 Benutzerverwaltung

12.3 Active Directory Federation Services

12.3.1 Netzwerkvorbereitungen - NSGs

12.3.2 Availability Set

12.3.3 Installation ADFS

12.3.4 Load Balancer

12.3.5 Installation der ADFS Web Application Proxy Server

12.3.6 Aktivieren des WAP-Zugriffs

12.3.7 Externer Load Balancer für WAP-Service

12.3.8 NSG Konfiguration

12.4 AD-Connect für ADFS konfigurieren

13. **Hybride File-Services**

13.1.1 Speicherkonto

13.2 Erweiterte Storage Account Konfiguration

14. **IaaS Optimierung**

14.1 Azure AD Connect Health

14.1.1 Azure AD Connect Health ADFS

14.2 Scale-Sets

14.2.1 Custom Image - Erstellung eines Master-Images

14.3 Subscription Upgrade

15. **Summary - Abschnitt II**

16. **Azure Bastion**

16.1 Grundlagen

16.2 Implementierung

17. **Azure MFA**

17.1 Grundlagen

17.2 Azure MFA Implementierung

17.3 Advanced MFA-Features

17.3.1 Trusted IPs

17.3.2 Conditional Access Policies

17.3.3 Fraud Alert

- 17.3.4 One-time bypass
- 17.3.5 Identity Protection

18. **Azure Monitoring**

- 18.1 Log Analytics Workspace
 - 18.1.1 Kusto Query Beispiele
- 18.2 Guest OS-Diagnostic
- 18.3 Azure Monitor Alerts
 - 18.3.1 Azure Monitor Actions
- 18.4 Performance Diagnostics

19. **Azure Backup and Site Recovery**

- 19.1 Einrichten der Recovery Services Vault Umgebung
 - 19.1.1 Backup Policies
- 19.2 On-premises Backup

20. **Azure Security Center**

- 20.1 Threat Landscape
 - 20.1.1 Cyber kill chain
 - 20.1.2 Grundlegende Absicherung der Azure Services
- 20.2 Einführung in das Azure Security Center
 - 20.2.1 Security Center Dashboard
- 20.3 Security Policy Management
- 20.4 Erhöhung des Security-Levels
 - 20.4.1 Standard Recommendations
 - 20.4.2 Identity and Access
 - 20.4.3 Weitere Empfehlungen
 - 20.4.4 Single click remediation - Quick Fix!

20.5 Erweiterte Mechanismen zur Erhöhung der Security

20.5.1 Just-in-time access (JIT)

20.5.2 Compliance Report

20.5.3 File integrity monitoring

20.5.4 Adaptive application controls (App whitelisting)

20.6 Alarmierung und Incident-Response Prozess

21. **Summary - Abschnitt III**

22. **22 Digital Workplace - der virtuelle Arbeitsplatz**

22.1 Vorbereitung

22.2 Grundlegende Architektur

23. **Planung der virtual Desktop Umgebung**

23.1 Clients

23.2 Infrastruktur

23.2.1 RD Gateway & WebAccess

23.2.2 Broker & Database

23.2.3 Monitoring & Diagnostic

23.3 Worker

23.3.1 Pool-Typ

23.3.2 Load Balancing

23.3.3 Dynamische Skalierung

23.4 Applikationsmanagement

23.4.1 Hosted Apps

23.4.2 FSLogix - App Masking

23.4.3 MSIX App Attach

23.5 Personalisierung - FSLogix Profile Container

24. **Konfiguration der WvD Umgebung**

24.1 Personal Desktops

24.1.1 Workload Definition

25. **Individuelle pooled Desktops**

25.1 FSLogix Azure File Share

25.2 Custom Image

25.2.1 Personalisierung

25.2.2 Installation und Optimierung der Applikationen

25.2.3 Betriebssystem Optimierung

25.2.4 Master-Image Erstellung

25.3 Image Verwaltung bei pooled Desktops

25.3.1 Aktualisierung des Host Pools

26. **Anpassungen der Workplace Umgebung**

26.1 FSLogix AppMasking

26.1.1 Rule-Set Erstellung

26.2 MSIX App Attach

26.2.1 Vorbereitungen

26.2.2 MSIX Paketierung

26.2.3 Verwendung von MSIX in der WvD Umgebung

27. **Fazit**

Einführung

Die Möglichkeiten der Microsoft Azure Cloud sind gewaltig und verändern die IT-Landschaft nachhaltig. Anfang 2021 umfasst das Produkt- und Technologieportfolio mehr als 600 Services in 60 Regionen mit insgesamt knapp 200 Rechenzentren. Der Aufbau von hoch ausfallsicheren, skalierbaren, modernen und effizienten Lösungen ist nicht nur den großen Unternehmen vorbehalten – jedes moderne IT-Design kann von den Vorteilen der IaaS, PaaS, SaaS und DaaS Lösungen der Microsoft Azure Cloud Umgebungen profitieren.

Gerade auch die Ereignisse des Jahres 2020 haben uns allen gezeigt, wie wichtig eine schnelle und stabile Bereitstellung von IT-Services und modernen Arbeitsplatzumgebungen ist. Für Anwender muss der Zugriff auf Dienste unkompliziert und unabhängig von geographischen Standorten erfolgen – der moderne Arbeitsplatz muss zentrale und globale Datendienste nutzen und über das Internet verwaltbar sein. Zum Glück haben schon viele Kunden in den letzten Jahren die Vorteile der Office365 SaaS Dienste erkannt, damit war ein kurzfristiger Ausbau der Dienste (allen voran natürlich Microsoft Teams) für viele Benutzer überhaupt erst möglich.

Aus Sicht der Infrastruktur-Architektur ist die Nutzung der voll-verwalteten SaaS Dienste allerdings erst der Beginn eines kompletten Paradigmenwechsels in den nächsten Jahren. Die on-premises Strukturen und Technologien werden mit entsprechenden Cloud-Services zusammenarbeiten müssen, verschiedene Dienste und

Produkte wird Microsoft auch nur mehr in der Azure Cloud zur Verfügung stellen.

Ich bin der festen Überzeugung, dass es noch einige Jahren dauern wird, bis größere Unternehmen alle IT-Services aus der Cloud beziehen werden. Lokale Infrastrukturen und Datenhaltung werden uns noch lange begleiten, diese müssen sich allerdings nahtlos in die hybride Cloud-Umgebung integrieren. Entscheidend dabei ist allerdings, dass in der Cloud keine Schatten-IT entsteht und sich alle IT-Services als ein großer Verbund aus unterschiedlichen Technologien mit konsistentem Benutzer-, Daten- und Zugriffsmanagement präsentieren. An diesem Punkt soll das vorliegende Buch helfen. Bevor man sich mit den verwalteten Diensten und verschiedenen Plattform- und Software-Services auseinandersetzt, bedarf es einer entsprechenden Vorbereitung der Infrastruktur. Die Azure Umgebung soll sich wie eine geografische Außenstelle im Unternehmen integrieren. Der Netzwerkverkehr muss entsprechend gesteuert werden. Der Zugriff auf Daten und Dienste wird für die Benutzer konsistent und identisch abgebildet, und die Sicherheit aller Informationen muss gewährleistet sein.

Zu oft habe ich in den letzten Jahren festgestellt, dass die Einführung eines vermeintlich unkomplizierten Cloud-Dienstes zu massiven Problemen führte und die Infrastrukturmgebung erneut angepasst werden musste. Viele Kunden haben regelrecht Angst vor neuen Cloud-Diensten, weil sie die Anpassungen und die Neukonfiguration scheuen. In Umgebungen mit einer sauber geplanten Basis-Infrastruktur ist diese Sorge unbegründet. Sobald die hybride Infrastrukturmgebung aufgebaut ist, können neue Dienste und Funktionen mit einer gewissen Leichtigkeit eingeführt werden. Dies ermöglicht eine rasche Konzentration auf neue Produkte und Technologien.

Aufbau des Buches

Das Buch ist in vier Abschnitte unterteilt, welche aufeinander aufbauen. Der erste Abschnitt beschäftigt sich mit den Grundlagen. Der Leser wird die neuen Technologien und Begriffe der Microsoft Azure Infrastruktur Umgebung kennenlernen. Natürlich hat Microsoft das Rad in der Cloud nicht neu erfunden, Grundlagen der IT haben nach wie vor ihre Gültigkeit und müssen auch entsprechend berücksichtigt werden. Es werden Infrastruktur-Technologien und Topologien teilweise neu bzw. angepasst interpretiert. Dies ist an den erweiterten Möglichkeiten und der neuen Definition von Begriffen erkennbar.

Nachdem die Strukturen und Topologien in Abschnitt I grundlegend vorgestellt wurden, gehen wir im Abschnitt II in die Praxis über. Der Aufbau und die Konfiguration einer kompletten hybriden Infrastruktur-Umgebung werden Schritt für Schritt erklärt. Dazu werden wir unser eigenes privates virtuelles Netzwerk in der Azure Cloud definieren und über eine stetige Verbindung mit einer on-premises Microsoft Active Directory Umgebung kommunizieren. Danach stehen die Installation und Konfigurationen der ersten virtuellen Server und die schrittweise Erweiterung des hybriden Data-Centers im Mittelpunkt. Neue Funktionen und Möglichkeiten zur Bereitstellung und Verwaltung von Diensten kommen zum Einsatz. Am Ende von Abschnitt II ist die Umgebung somit für alle möglichen weiteren Schritte in der Cloud optimal vorbereitet.

Abschnitt III zeigt die typischen ersten optionalen Erweiterungen einer modernen hybriden IT-Landschaft. Die sichere Verwaltung der Cloud-Dienste und der damit verbundene abgesicherte administrative Zugriff macht den

Anfang (Azure Bastion). Die Synchronisierung der Active Directory Benutzerkonten in das cloud-basierte Identity-Management Azure AD (wird ebenfalls im Abschnitt II realisiert) ermöglicht nun die Umsetzung des „One-User-One-Identity“ Konzepts für alle Zugriffe. Aus diesem Grund ist es umso wichtiger, diese Identität entsprechend abzusichern - wir werden dazu das PaaS (Platform as a Service) Azure MFA einführen, um eine sichere und unkomplizierte zweistufige Authentifizierung für Benutzer zu etablieren. Nachdem wir die neu aufgebauten Dienste über die Funktionen des Azure Monitors pro-aktiv überwachen können und mit Hilfe von Azure Backup auch gesichert haben, öffnen wir das Kapitel Azure Security. Die Funktionen und Technologien der Azure Security Suite ermöglichen die Absicherung der gesamten Umgebung auf mehreren Ebenen und schützen holistisch gegen die immer häufiger auftretenden Cyber-Security Attacken.

Bei der Planung des Buches habe ich lange überlegt welcher vollumfänglichen Microsoft Cloud Technologie ich hier Platz geben möchte. Lange war geplant, dass in Abschnitt IV der nächste logische Schritt behandelt wird, nämlich die Anbindung und Nutzung der Microsoft 365 Dienste. Nicht nur die Ereignisse des Jahres 2020 haben mich dazu bewegt, diesen Abschnitt dem virtuellen Arbeitsplatz zu widmen. Remote-Working und der sichere und effiziente Zugriff auf den Digital Workplace eines Unternehmens waren schon lange vor dem Jahr 2020 wichtige Themen. In diesem Jahr sind sie allerdings sehr schnell in den Fokus der IT-Verantwortlichen gerückt. Mit dem Windows virtual Desktop (DaaS - Desktop as a Service) steht in der Cloud mittlerweile eine sehr gute Alternative zu klassischen on-premises Desktop-Virtualisierungslösungen zur Verfügung, die wir in Abschnitt IV im Detail betrachten.

Abschnitt I

Grundlagen Azure Infrastruktur

1 Grundlagen

1.1 Definitionen und Abkürzungen

Bevor man sich in die Welt des Cloud-Computings begibt, sollte man sich mit den grundlegenden Begriffen und Definitionen vertraut machen. Dieses Buch ist zwar prinzipiell auf Deutsch geschrieben, auf Grund der besseren Verständlichkeit und üblichen Marktbezeichnungen werden bei manchen Begriffen und Definitionen allerdings die englischen Originalbezeichnungen verwendet.

Active Directory	Microsoft Verzeichnisdienst zur Verwaltung von Domänenobjekten. Active Directory Benutzer, Gruppen und Organisationseinheiten bilden die Basis zur Steuerung und Berechtigung aller Ressourcen.
BYOD	„Bring your own Device“ – Benutzer greifen über eigene private Geräte auf IT-Ressourcen und Daten des Unternehmens zu.
Business Analytics-Tools	Tools, um Daten aus Systemen zu extrahieren und diese zu Analysezwecken in anderen Systemen wie beispielsweise einem Data Warehouse zu integrieren.
BI-Tools	Business Intelligence Tools verarbeiten unstrukturierte Daten aus unterschiedlichen Quellen, um aussagekräftige Trends zu ermitteln.
Cloud	Metapher für ein globales, öffentliches Netzwerk – bei der Public Cloud handelt es sich dabei um das Internet.
Cloud Bursting	Mechanismus zum Verlagern von Ressourcen aus einer privaten Cloud hin zu einer öffentlichen Cloud, wenn die Ressourcenkapazität innerhalb der privaten Cloud nicht mehr ausreicht oder verfügbar ist.
Cloud Computing	Bereitstellen von Computing-Ressourcen wie Rechenleistung, Speicher,

Netzwerkkomponenten und Software über das Internet.

Cloud Computing-Typen

Es gibt grundlegend drei verschiedene Klassifizierungen zur Bereitstellung von Cloud Computing Ressourcen:

IaaS - Infrastructure as a Service

PaaS - Platform as a Service

SaaS - Software as a Service

Elastic Computing

EC beschreibt die Möglichkeit einem Server dynamisch Ressourcen wie Prozessorleistung, Speicher oder Netzwerkressourcen zuordnen zu können.

Grid Computing

Eine Gruppe von verbundenen Computern, um komplexe Operationen gemeinsam durchführen zu können.

Hybrid Cloud

Kombination aus öffentlichen (public) und privaten Cloud-Ressourcen, welche für eine gemeinsame Nutzung von Daten und Systemen verbunden werden.

IaaS

Infrastructure as a Service beschreibt ein Cloud Computing Modell bei welchem durch den Cloud-Anbieter die Netzwerk- und Serverinfrastruktur zur Verfügung gestellt werden. Typischerweise übernimmt der Kunde die Verantwortung direkt nach der Installation des Betriebssystems.

KI-Computing

Künstliche Intelligenz (AI - Artificial Intelligence) beschreibt die Fähigkeit eines

Computers menschliche Intelligenz zu imitieren. Mithilfe von Mathematik und Logik kann das Computersystem die Argumentation simulieren, mit der Menschen aus neuen Informationen lernen und Entscheidungen treffen.

Middleware Software zwischen einem Betriebssystem und der Anwendung, um die Kommunikation und Datenverwaltung zu ermöglichen.

PaaS Platform as a Service beschreibt ein Cloud Computing Modell bei welchem neben der Netzwerk- und Serverinfrastruktur auch die gesamte Middleware inkl. Entwicklungs- und Konfigurationsplattform einer Lösung vom Cloud Anbieter verwaltet wird.

Private Cloud Dienste einer Private Cloud sind nicht allen Benutzern über das Internet zugänglich, sondern nur einem eingeschränkten Benutzerkreis. Oft erfolgt die Bereitstellung auch zusätzlich über ein privates, internes Netzwerk.

Public Cloud Dienste einer öffentlichen (public) Cloud werden über das Internet angeboten und sind prinzipiell für jeden Benutzer zugänglich.

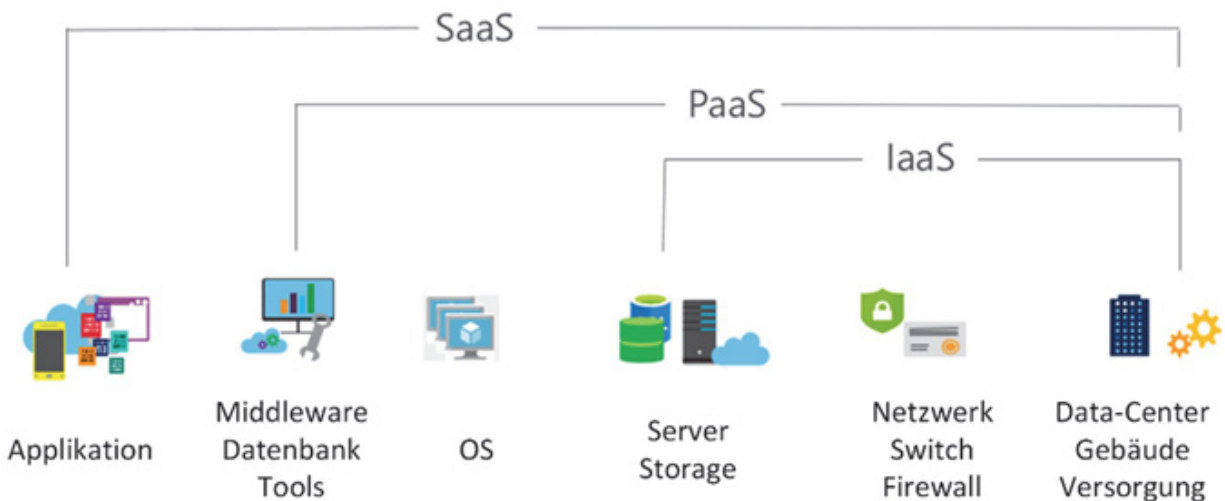
SaaS Software as a Service beschreibt ein Cloud Computing Modell bei welchem bis zu Applikationsschicht einer Lösung alle erforderlichen Ressourcen einer Lösung vom Cloud Anbieter bereitgestellt und verwaltet werden.

Virtualisierung Es wird eine komplett simulierte (virtuelle) Computing-Umgebung bereitgestellt – und keine physische Umgebung. Die virtuellen Treiber agieren unabhängig von der darunterliegenden Hardware.

Zero Touch Deployment Bereitstellung und Konfiguration von Applikationen oder ganzen Systemen ohne Interaktion durch einen Benutzer.

1.2 Cloud Computing-Typen

Abbildung 1.2-1: Darstellung Cloud Computing Typen



IaaS - Infrastructure as a Service

Bei IaaS werden virtuelle Server mit unterschiedlichen, frei konfigurierbaren und dynamisch skalierbaren Leistungsparametern durch die Azure Cloud direkt in einem logischen Verwaltungs- und Abrechnungsbereich (Tenant) des Kunden bereitgestellt. Der Kunde muss sich um die Bereitstellung und Wartung der erforderlichen Hardware inkl. der für den Zugriff auf diese Server benötigte

Infrastruktur (Switch, Router, Firewall usw.) nicht kümmern. Die Verfügbarkeit der Server wird über SLA's (Service Level Agreements) definiert und kann durch optionale Dienste (High Availability -Konfigurationen) individuell erweitert werden.

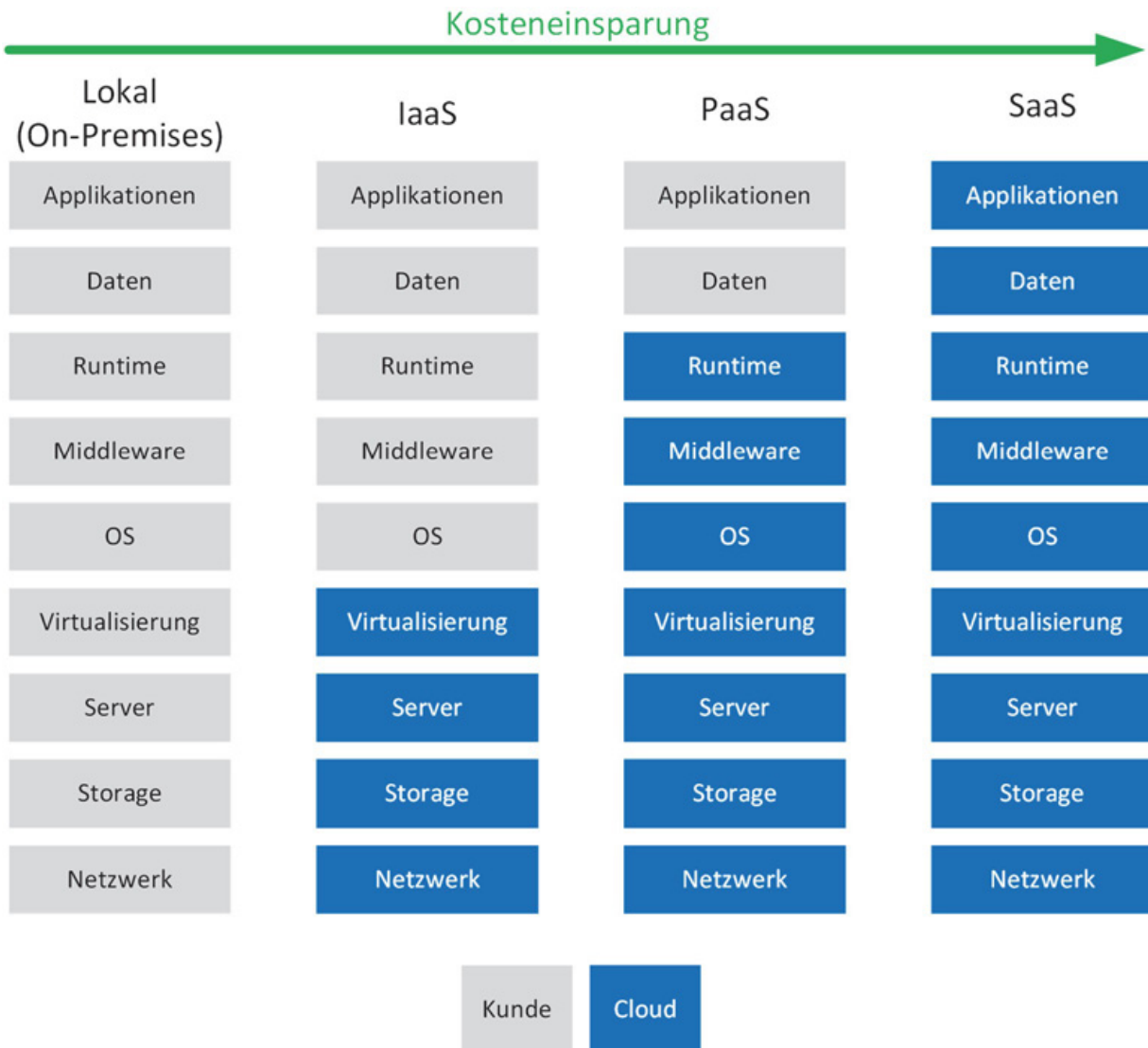
PaaS - Platform as a Service

PaaS Dienste gehen einen Schritt weiter, zusätzlich zur gesamten Hardware inkl. Infrastruktur für den Zugriff über das Internet (Public Cloud) oder dedizierten, abgeschotteten Bereichen (Private Cloud) werden durch die Azure Cloud auch die Verwaltung der gesamten Betriebssystem-Ebene inkl. aller Updates sowie der benötigten Middleware und Runtime-Komponenten des Dienstes übernommen. Ein typisches Beispiel für PaaS in der Azure Cloud sind die Azure SQL Services - die gesamte Bereitstellung und Wartung eines SQL Servers bzw. SQL-Clusters entfällt für den Kunden.

SaaS - Software as a Service

Bei SaaS wird die gesamte Software direkt über das Internet bereitgestellt, auch die Verwaltung und Sicherung der durch die SaaS Services erzeugten Daten erfolgt durch den SaaS Anbieter. Die Abrechnung bei SaaS Diensten erfolgt typischerweise nach einem Abonnement-Modell, IaaS und PaaS Dienste werden gewöhnlicherweise nach dem „Pay-as-you-use“ Modell verrechnet. Die gesamte Produkt-Suite von Office365 ist ein typischer Vertreter moderner SaaS Lösungen.

Abbildung 1.2-2: Vergleich der Verantwortungsbereiche



- Keinerlei Investitionskosten und insgesamt niedrigere laufende Kosten
- Verbesserte Geschäftskontinuität und dynamische Skalierung
- Verbesserte Stabilität und Notfallwiederherstellung
- Reduzierte Verwaltungsaufwände und Entwicklungsaufwände (PaaS)
- Standardmäßiger ortsunabhängiger und größtenteils endgeräteunabhängiger Zugriff auf alle Ressourcen in der Microsoft Azure Cloud
- Kostengünstige Nutzung ausgereifter Programme und Tools

- Mehrstufiger Sicherheitsansatz inkl. Pro-aktiver Erkennung von Angriffen und Malware durch Einsatz von KI und ML Systemen
- Globale, internationale Compliance Standards sowie länder- und branchenspezifische Voraussetzungen wie ISO 27001, HIPAA, FedRAMP, SOC 1 und SOC 2 oder Australia IRAP, UK G-Cloud und Singapore MTCS werden durch die Azure Cloud erfüllt

1.3 Azure Services

Abbildung 1.3-1: Azure Services Übersicht – Quelle: Microsoft TechNet



Alle aktuell zur Verfügung stehenden Dienste der Azure Cloud zu erläutern, würde den Rahmen dieses Buches sprengen. Daher konzentriert sich dieses Kapitel auf die grundlegenden Service-Strukturen. Auf Dienste, welche für den Aufbau einer hybriden Infrastrukturmgebung zwingend benötigt werden, wird im weiteren Verlauf dieses Buches detailliert eingegangen.

Anfang 2021 stehen über die Microsoft Azure Cloud knapp 600 Dienste zur Verfügung, welche über einen eigenen

Service-Channel bzw. dem Marketplace angeboten werden. Eine Gruppierung dieser Dienste in 22 Kategorien soll die Auswahl erleichtern.

- Analysen** Verschiedene Azure Services zum Sammeln, Analysieren, Verarbeiten und Visualisieren von Daten. Azure DataBricks, PowerBI Embedded und Azure Data Lake Storage gehören beispielsweise zu dieser Kategorie.
- Blockchain** Unterschiedliche Tools und Services zum Erstellen und Verwalten von Blockchain basierenden Anwendungen.
- Compute** Gerade bei Aufbau von Infrastrukturdiensten in der Cloud eine der wichtigsten Kategorien. Hier finden sich die Dienste zur Erstellung von virtuellen Windows oder Linux Computern / Servern, VM Scale-Sets, Azure Dedicated Hosts oder auch Instanzen zur Ausführung von SAP-HANA Workloads in der Azure Cloud.
- Container** Services zur Erstellung und Verwaltung von unterschiedlichen Container-Technologien inkl. Azure Kubernetes Services (AKS) werden in dieser Kategorie angeboten.
- Datenbanken** Vollständig verwaltete Datenbanken und Instanzen in unterschiedlichen technischen Ausprägungen und Funktionen stellen die Dienste in dieser Kategorie zur Verfügung.
- DevOps** Über diese Services kann eine komplette, Cloud-basierte Prozessumgebung zur gemeinsamen Entwicklung und Bereitstellung von Applikationen realisiert werden.

Entwicklungstools

Entwicklung und Verwaltung von Clouduanwendungen, unabhängig von Sprache und Plattform stehen im Fokus dieser Servicegruppe.

Hybrid

Technologien zum Aufbau von hybriden Infrastrukturumgebungen, wie beispielweise Azure ExpressRoute zum Aufbau von hoch performanten und stabilen Netzwerkverbindungen, oder auch das Azure Active Directory zum zentralen Identitätsmanagements findet man in dieser Kategorie.

Identität

Die zentrale Verwaltung von Benutzer- und Geräteidentitäten inkl. dem Schutz von vertraulichen Daten werden von Diensten wie beispielsweise den Azure AD Domain Services oder den Azure Information Protection Services angeboten.

Integration

Tools zur nahtlosen Integration von Cloud-basierten bzw. lokalen Daten und Prozessen finden sich in dieser Kategorie.

IoT

Internet of Things - eine stark wachsende Kategorie mit Services und Tools zur Bewältigung dieser teilweise sehr komplexen Herausforderung.

KI / ML

KI und Machine Learning Services für unterschiedliche Anwendungsfälle stehen hier zur Verfügung. Neben Sprach-, Bild-