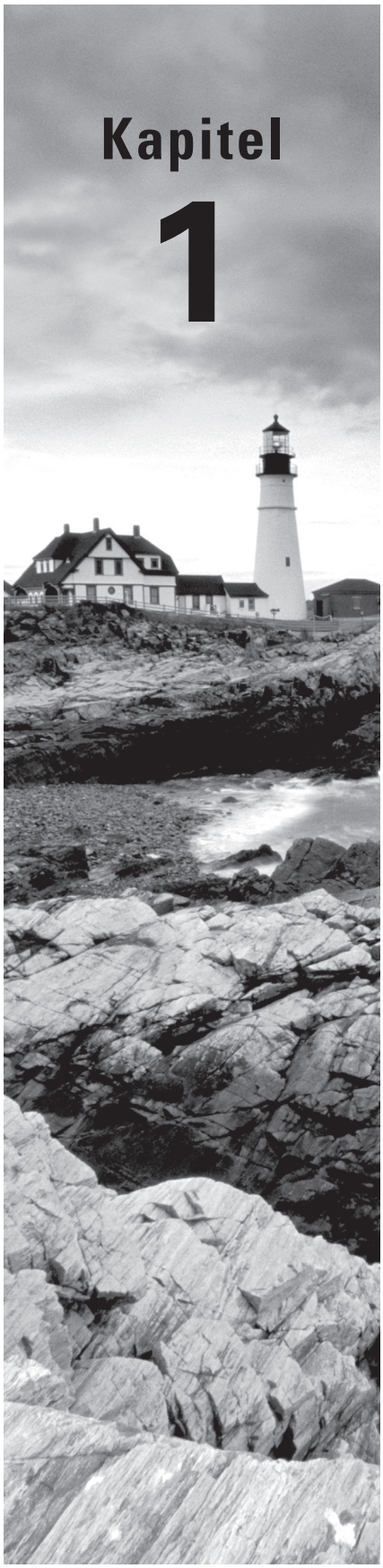
Zentrale AWS-Services



Kapitel

1

Einführung in Cloud-Computing und AWS

Wichtige technologische Innovationen und Entwicklungen spielen sich heute zumeist in der Cloud ab. Bei der Auswahl einer Plattform für geschäftliche und institutionelle Workloads entscheiden sich dabei viele Unternehmen und Einrichtungen für Amazon Web Services (AWS). Ein erfolgreicher AWS Solutions Architect benötigt ein klares Verständnis der Cloud und der Funktionsweise von AWS.

Um Ihnen diese allgemeineren Zusammenhänge zu verdeutlichen, widmet sich dieses Kapitel zunächst sehr grundlegenden Fragestellungen:

- Wie unterscheidet sich Cloud-Computing von anderen Anwendungen und Client-Server-Modellen?
- Auf welche Weise stellt die AWS-Plattform sichere und flexible virtuelle vernetzte Umgebungen für Ihre Ressourcen bereit?
- Wie gewährleistet AWS eine so hohe Servicezuverlässigkeit?
- Wie können Sie Ihre AWS-Ressourcen in Anspruch nehmen und verwalten?
- Wo finden Sie Handbücher und Hilfe für Ihre AWS-Bereitstellungen?

Cloud-Computing und Virtualisierung

Das technologische Fundament aller Cloud-Lösungen ist die Virtualisierung. Wie in Abbildung 1.1 dargestellt, können mittels Virtualisierung die Hardwareressourcen eines einzelnen physischen Servers in kleinere Einheiten aufgeteilt werden. Dieser physische Server könnte also mehrere virtuelle Maschinen hosten, die jeweils ihr komplett eigenes Betriebssystem ausführen, einschließlich eigenem Arbeitsspeicher, Massenspeicher und Netzwerkzugang.

Die Virtualisierung sorgt für deutlich mehr Flexibilität: Ein virtueller Server kann in wenigen Sekunden bereitgestellt, für eine exakt bestimmbare Zeitspanne ausgeführt und dann wieder heruntergefahren werden. Die freigegebenen Ressourcen stehen sofort wieder für andere Workloads zur Verfügung. Ein so dichtes Verfahren sorgt für eine optimale Ausnutzung Ihrer Hardware und erleichtert die Erzeugung von Test- und Sandbox-Umgebungen.

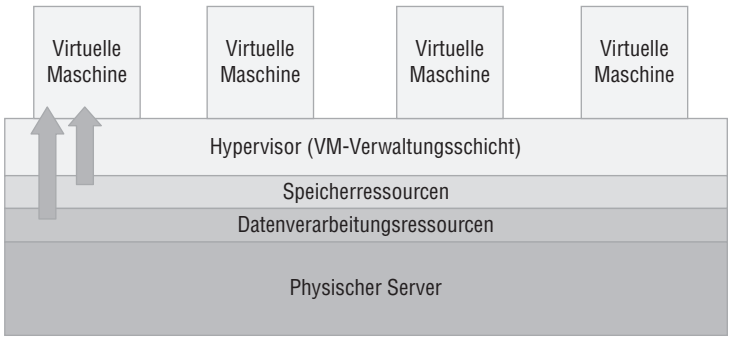


ABBILDUNG 1.1: Ein physischer Server dient als Host für mehrere virtuelle Maschinen.

Cloud-Computing-Architektur

Bekannte Cloud-Computing-Anbieter wie AWS verfügen über riesige Serverfarmen mit Hunderttausenden Servern, Datenlaufwerken und der nötigen Netzwerkverkabelung. In einer sorgfältig eingerichteten virtualisierten Umgebung kann ein virtueller Server sich aus den verfügbaren Ressourcen Arbeits- und Massenspeicher, Rechenzyklen und Netzwerkbandbreite so effizient wie möglich zusammensuchen.

Eine Cloud-Computing-Plattform bietet bedarfsgerechten Self-Service-Zugriff auf zusammengelegte Datenverarbeitungsressourcen, deren Nutzung gemessen und nach Verbrauch abgerechnet wird. Cloud-Computing-Systeme erlauben präzise Abrechnungsmodelle – nicht selten wird der stündliche Verbrauch bis auf den Bruchteil eines Cents genau beziffert.

Cloud-Computing-Optimierung

Die Cloud eignet sich so hervorragend für viele wichtige Workloads, weil sie nicht nur skalierbar und flexibel, sondern oft auch deutlich kostengünstiger ist als herkömmliche Alternativen. Um eine effektive Implementierung und Bereitstellung zu gewährleisten, sind drei Aspekte zu beachten, die nachfolgend erläutert werden.

Skalierbarkeit

Eine skalierbare Infrastruktur kann eine unerwartet hohe Inanspruchnahme Ihrer Anwendung effizient bewältigen, indem sie automatisch weitere Ressourcen hinzufügt. Zumeist bedeutet dies, dass die Anzahl Ihrer laufenden virtuellen Maschinen (bei AWS auch Instanzen bzw. *Instances* genannt) dynamisch erhöht wird (siehe Abbildung 1.2).

AWS bietet einen Skalierungsdienst (AWS Auto Scaling), mit dem Sie ein Systemabbild definieren, das dann bei steigendem Ressourcenbedarf sofort und automatisch repliziert und zum Starten mehrerer Instanzen genutzt werden kann.

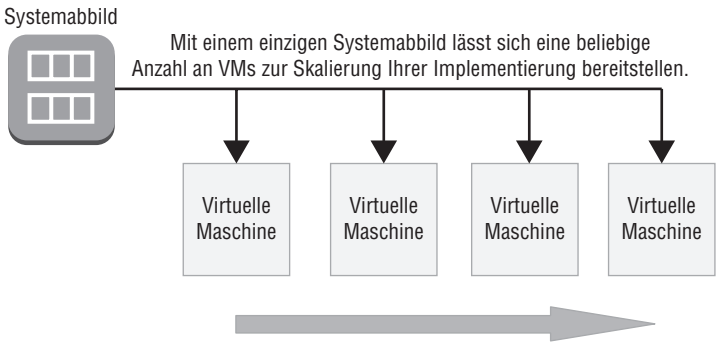


ABBILDUNG 1.2: Kopien eines Systemabbilds werden neuen virtuellen Maschinen bei ihrem Start zugewiesen.

Elastizität

Ähnlich wie die Skalierbarkeit ermöglicht es auch die Elastizität einer Infrastruktur, besser auf einen wechselhaften Ressourcenbedarf zu reagieren. Doch während die Systemabbilder in einer skalierbaren Umgebung bei steigender Nachfrage zur Erhöhung der Kapazität genutzt werden, sorgt eine elastische Infrastruktur für eine automatische *Verringerung* der Kapazität, sobald die Nachfrage wieder sinkt. So lassen sich die Kosten im Zaum halten, weil Ressourcen nur bei tatsächlichem Bedarf genutzt werden.

Kostenmanagement

Die bessere Kontrolle über das IT-Budget beim Cloud-Computing ergibt sich aus der präziseren Verwaltung Ihrer verwendeten Ressourcen, aber auch aus der Umstellung Ihres Kostenmodells, das nun nicht mehr die Investitionskosten (CapEx), sondern die Betriebskosten (OpEx) in den Mittelpunkt rückt.

In der Praxis heißt dies, dass Sie nicht länger mehrere tausend Euro für jeden neuen Server vorstrecken müssen, von den zugehörigen Kosten für Strom, Kühlung, Sicherheit und Rack-Einheiten ganz zu schweigen. Stattdessen werden Ihnen kleinere inkrementelle Beträge in Rechnung gestellt, solange Sie Ihre Anwendung betreiben.

Auf lange Sicht sind die Cloud-Betriebskosten zwar nicht unbedingt niedriger als die Kosten während der gesamten Nutzungsdauer einer vergleichbaren Implementierung im Rechenzentrum, aber das Risiko durch hohe Investitionen bei ungewissen Zukunftsaussichten fällt weg. Falls sich ändernde Bedürfnisse später einmal neue Hardware erforderlich machen, stellt AWS die neue Lösung in Minutenschnelle bereit.

Mit dem AWS-Gesamtbetriebskostenrechner können Sie sich einen besseren Eindruck von den zu erwartenden Kosten und Einsparungen verschaffen: `https://aws.amazon.com/de/tco-calculator/`. Das Tool ermöglicht einen sinnvollen Vergleich der Kosten Ihres derzeitigen Rechenzentrums mit denen der Cloud-Computing-Umgebung von AWS.

Die AWS-Cloud

In der AWS-Konsole tauchen regelmäßig neue, innovative Services auf. Der Versuch, mit diesem Angebot Schritt zu halten, führt nicht selten zu Frust. Als Solutions Architect sollte Ihre Aufmerksamkeit aber ohnehin lieber den zentralen Servicekategorien gelten. Dieser Abschnitt stellt daher die Kategorien kurz vor (Tabelle 1.1) und liefert dann einen ebenso kurzen Überblick der wichtigsten Services (Tabelle 1.2). Im weiteren Verlauf des Buches lernen Sie diese (und andere) Services natürlich noch genauer kennen. Für den Moment sollen Ihnen die folgenden kurzen Definitionen aber erst einmal den Einstieg erleichtern.

Kategorie	Funktion
Datenverarbeitung	Diese Services übernehmen in der Cloud quasi die Rolle lokaler physischer Server. Sie bieten erweiterte Konfigurationen, einschließlich automatischer Skalierung, Lastverteilung und sogar serverlose Architekturen (eine Methode zur Bereitstellung von Serverfunktionalität mit sehr geringen Infrastrukturanforderungen).
Netzwerk	Die Services dieser Kategorie sorgen für die Vernetzung Ihrer Anwendungen, die Zugriffssteuerung und erweiterte Remote-Verbindungen.
Speicherung	Diverse Arten von Speicherplattformen erfüllen ein breites Spektrum an Anforderungen – von der sofortigen Zugänglichkeit bis hin zur langfristigen Archivierung.
Datenbanken	Verwaltete Lösungen stehen für Anwendungsszenarien mit verschiedenen Datenformaten bereit: relationale Datenbanken, NoSQL oder Caching.
Anwendungsverwaltung	Überwachen, prüfen und konfigurieren Sie Services und laufende Ressourcen in Ihrem AWS-Konto.
Sicherheit und Identität	Mit diesen Services verwalten Sie die Authentifizierung und Autorisierung, die Verschlüsselung von Daten und Verbindungen sowie die Integration mit Systemen zur Authentifizierungsverwaltung von Drittanbietern.
Anwendungsintegration	In dieser Kategorie finden sich Tools für den Entwurf von entkoppelten, integrierten und API-freundlichen Prozessen zur Anwendungsentwicklung.

TABELLE 1.1: AWS-Servicekategorien

Tabelle 1.2 beschreibt die Funktionen einiger zentraler AWS-Services nach Kategorien sortiert.

Kategorie	Service	Funktion
Datenverarbeitung	Elastic Compute Cloud (EC2)	EC2-Serverinstanzen fungieren als virtuelle Versionen der Server, die Sie sonst in Ihrem Rechenzentrum vor Ort ausführen würden. EC2-Instanzen können mit einem geeigneten Profil (CPU, Arbeitsspeicher, Massenspeicher und Netzwerkschnittstelle) für beliebige Anwendungsanforderungen bereitgestellt werden, sei es als einfacher Webserver oder als Teil eines Clusters aus Instanzen, die zusammen eine integrierte mehrstufige Flottenarchitektur bilden. Da EC2-Instanzen nur virtuell existieren, sind sie deutlich ressourcenschonender und quasi sofort implementierbar.
	Lambda	Serverlose Anwendungsarchitekturen wie die von Amazon Lambda ermöglichen es, reaktionsschnelle öffentliche Services bereitzustellen, ohne dafür rund um die Uhr einen Server laufen lassen zu müssen. Stattdessen lösen bestimmte Netzwerkereignisse (wie Anfragen von anderen Services) die Ausführung einer vordefinierten, codebasierten Funktion aus. Wenn diese Ausführung beendet ist (derzeit nach maximal 15 Minuten), ist auch das Lambda-Ereignis beendet und alle Ressourcen werden automatisch heruntergefahren.
	Auto Scaling	Kopien laufender EC2-Instanzen können als Konfigurationsvorlagen dienen und automatisch gestartet (oder hochskaliert) werden, sobald vorhandene Instanzen den Ressourcenbedarf nicht mehr decken. Sinkt der Bedarf wieder, können ungenutzte Instanzen beendet (oder *herunterskaliert*) werden.
	Elastic Load Balancing	Eingehender Datenverkehr kann zwischen mehreren Webservern verteilt werden, um zu vermeiden, dass Daten an ausgefallene Server geleitet werden oder einzelne Server überlastet sind, während andere Server ungenutzt bleiben.
	Elastic Beanstalk	Beanstalk ist ein verwalteter Service zur abstrahierten Bereitstellung einer Datenverarbeitungs- und Netzwerkinfrastruktur von AWS. Sie müssen einfach nur Ihren Anwendungscode hochladen und Beanstalk startet und verwaltet automatisch alle nötigen Services im Hintergrund.

TABELLE 1.2: Zentrale AWS-Services (nach Kategorie)

Kategorie	Service	Funktion
Netzwerk	Virtual Private Cloud (VPC)	Eine VPC ist eine umfangreich konfigurierbare Netzwerkumgebung, die als Host für Ihre EC2-Instanzen (und RDS-Instanzen) dient. Mit VPC-basierten Tools behalten Sie ein- und ausgehende Netzwerkzugriffe von und zu den Instanzen stets im Blick.
	Direct Connect	Wenn Sie schnelle und sichere Netzwerkverbindungen zu AWS über einen Drittanbieter erwerben, können Sie mit Direct Connect eine dedizierte Verbindung zwischen Ihrem lokalen Rechenzentrum oder Geschäftsstandort und Ihrer AWS-basierten VPC herstellen.
	Route 53	Route 53 ist der DNS-Service von AWS, mit dem Sie die Registrierung von Domains, die Resource-Record-Administration, Routing-Protokolle und Zustandsprüfungen verwalten; die vollständige Integration mit Ihren anderen AWS-Ressourcen ist gewährleistet.
	CloudFront	Amazon CloudFront ist ein verteiltes globales Netzwerk für die Bereitstellung von Inhalten (Content Delivery Network, CDN). Bei ordnungsgemäßer Konfiguration der CloudFront-Distribution werden die Inhalte Ihrer Website an Edge-Standorten rund um die Welt zwischengespeichert, damit Kunden diese Inhalte effizienter und mit möglichst niedriger Latenz abrufen können.
Speicherung	Simple Storage Service (S3)	S3 bietet äußerst vielseitigen, zuverlässigen und kostengünstigen Objektspeicher, der sich hervorragend für die Datenspeicherung und Backups eignet. Der Service wird üblicherweise auch als Teil größerer AWS-Produktionsprozesse genutzt, beispielsweise zum Speichern von Skripten, Vorlagen und Protokolldateien.
	Glacier	Glacier ist eine gute Wahl, wenn Sie riesige Datenarchive langfristig zu niedrigen Kosten speichern möchten und mit Verzögerungen beim Datenabruf von einigen Stunden leben können. Das Lebenszyklusmanagement von Glacier ist eng mit S3 verzahnt.

Kategorie	Service	Funktion
	Elastic Block Store (EBS)	EBS bietet virtuelle Datenlaufwerke zum Hosting des Betriebssystems und der Arbeitsdaten einer EC2-Instanz. Die Laufwerke sind den mit physischen Servern verbundenen Speicherlaufwerken und Partitionen nachempfunden.
	Storage Gateway	Storage Gateway ist ein hybrides Speichersystem, das den Cloud-Speicher von AWS über eine lokale Appliance verfügbar macht. Mit Storage Gateway werden Migrationen, Backups und Prozesse im Rahmen der Notfallwiederherstellung deutlich erleichtert.
Datenbanken	Relational Database Service (RDS)	RDS ist ein verwalteter Dienst, der für Sie eine stabile, sichere und zuverlässige Datenbankinstanz aufbaut. Sie können eine Vielzahl an SQL-Datenbank-Engines auf RDS ausführen, einschließlich MySQL, Microsoft SQL Server, Oracle und Amazon Aurora.
	DynamoDB	DynamoDB kann für schnelle, flexible, hochskalierbare und verwaltete nicht relationale Datenbank-Workloads (NoSQL) eingesetzt werden.
Anwendungsverwaltung	CloudWatch	Keine Implementierung ist komplett ohne irgendeine Form der Überwachung. Und die Erstellung endloser Protokolldateien hat nur dann einen Sinn, wenn auch mal jemand einen Blick auf sie wirft. CloudWatch kann die Leistung von Prozessen und die Auslastung von Ressourcen mithilfe von Ereignismeldungen überwachen. Wenn vorgegebene Schwellenwerte erreicht werden, wird entweder eine Nachricht an Sie gesendet oder eine automatisierte Reaktion ausgelöst.
	CloudFormation	Dieser Service ermöglicht es, mithilfe von Vorlagendateien vollständige und komplexe AWS-Implementierungen zu definieren. Dank der Option, Ihre Nutzung von AWS-Ressourcen durch Skripte zu steuern, fällt es auch leichter, den Startprozess der Anwendungen zu automatisieren, zu standardisieren und zu beschleunigen.

TABELLE 1.2: Zentrale AWS-Services (nach Kategorie) *(Fortsetzung)*

Kategorie	Service	Funktion
	CloudTrail	CloudTrail erfasst Daten zu allen API-Ereignissen in Ihrem Konto. Dieses Protokoll ist nützlich für die Rechnungsprüfung und Fehlersuche.
	Config	Der Config-Service soll das Änderungs- und Compliance-Management für Ihr AWS-Konto unterstützen. Dazu definieren Sie zuerst den gewünschten Konfigurationszustand. Config überprüft sodann fortlaufend, ob zukünftige Zustände dieser Idealkonfiguration entsprechen. Weicht eine Konfiguration zu sehr vom Ideal ab, werden Sie benachrichtigt.
Sicherheit und Identität	Identity and Access Management (IAM)	Mit IAM verwalten Sie die Authentifizierung und den Zugriff durch Benutzer und Programme auf Ihr AWS-Konto. Mithilfe von Benutzern, Gruppen, Rollen und Richtlinien können Sie exakt steuern, wer oder welcher Dienst Ihre AWS-Ressourcen abrufen und in Anspruch nehmen darf.
	Key Management Service (KMS)	KMS ist ein verwalteter Dienst zum Erstellen und Verwenden von Schlüsseln für die Verschlüsselung der Daten, die durch und für Ihre AWS-Ressourcen genutzt werden.
	Directory Service	Für AWS-Umgebungen, die Identitäten und Beziehungen verwalten müssen, bietet Directory Service die Möglichkeit, AWS-Ressourcen mit Identitätsdiensten wie Amazon Cognito und Domänen von Microsoft AD zu integrieren.
Anwendungsintegration	Simple Notification Service (SNS)	SNS ist ein Benachrichtigungsdienst, der die Übermittlung von *Themen* an andere Dienste (z. B. an eine SQS-Warteschlange oder zur Auslösung einer Lambda-Funktion), an Mobilgeräte oder an E-Mail- bzw. SMS-Empfänger automatisiert.
	Simple WorkFlow (SWF)	Mit SWF können Sie eine Reihe von Aufgaben koordinieren, die mit verschiedenen AWS-Services ausgeführt werden sollen oder sogar von nicht digitalen Ereignissen (also von menschlichen Handlungen) abhängen. Wie eine Kombination aus Kleister und Schmiermittel sorgt SWF dafür, dass der Gesamtprozess wie geölt läuft und die einzelnen Bestandteile nicht auseinanderfallen.

Kategorie	Service	Funktion
	Simple Queue Service (SQS)	SQS ermöglicht ereignisgesteuertes Messaging in verteilten Systemen. Die einzelnen Schritte eines umfangreicheren Prozesses können somit entkoppelt, aber gleichzeitig auch koordiniert werden. Die in Ihren SQS-Nachrichten enthaltenen Daten werden zuverlässig zugestellt und erhöhen die Fehlertoleranz von Anwendungen.
	API Gateway	Mit diesem Service erstellen und verwalten Sie sichere und zuverlässige APIs für Ihre AWS-basierten Anwendungen.

TABELLE 1.2: Zentrale AWS-Services (nach Kategorie) *(Fortsetzung)*

Architektur der AWS-Plattform

AWS betreibt rund um die Welt Rechenzentren für seine physischen Server. Da die Standorte so großflächig verteilt sind, können Sie die Latenzzeiten Ihrer eigenen Services im Netz deutlich verkürzen, indem Sie Ihre Workloads in geografischer Nähe der Benutzer ausführen lassen. Zudem wird das Compliance-Management erleichtert, wenn beispielsweise Daten die Grenzen eines bestimmten Rechtssystems nicht verlassen dürfen.

Die Rechenzentren befinden sich innerhalb von AWS-Regionen, von denen es derzeit siebzehn gibt (private GovCloud-Regionen der US-Regierung nicht inbegriffen); diese Anzahl nimmt stetig zu. Achten Sie beim Starten neuer AWS-Ressourcen immer darauf, welche Region Sie ausgewählt haben, denn die Preise und Serviceverfügbarkeiten können in den Regionen variieren. Tabelle 1.3 enthält alle nicht behördlichen Regionen mit ihren Namen und Endpunktadressen.

Regionsname	Regionscode	Endpunkt
USA Ost (Nord-Virginia)	us-east-1	`us-east-1.amazonaws.com`
USA Ost (Ohio)	us-east-2	`us-east-2.amazonaws.com`
USA West (Nordkalifornien)	us-west-1	`us-west-1.amazonaws.com`
USA West (Oregon)	us-west-2	`us-west-2.amazonaws.com`
Asien-Pazifik (Mumbai)	ap-south-1	`ap-south-1.amazonaws.com`
Asien-Pazifik (Seoul)	ap-northeast-2	`ap-northeast-2.amazonaws.com`

Regionsname	Regionscode	Endpunkt
Asien-Pazifik (Osaka-Lokal)	ap-northeast-3	ap-northeast-3.amazonaws.com
Asien-Pazifik (Singapur)	ap-southeast-1	ap-southeast-1.amazonaws.com
Asien-Pazifik (Sydney)	ap-southeast-2	ap-southeast-2.amazonaws.com
Asien-Pazifik (Tokio)	ap-northeast-1	ap-northeast-1.amazonaws.com
Kanada (Zentral)	ca-central-1	ca-central-1.amazonaws.com
China (Peking)	cn-north-1	cn-north-1.amazonaws.com.cn
EU (Frankfurt)	eu-central-1	eu-central-1.amazonaws.com
EU (Irland)	eu-west-1	eu-west-1.amazonaws.com
EU (London)	eu-west-2	eu-west-2.amazonaws.com
EU (Paris)	eu-west-3	eu-west-3.amazonaws.com
Südamerika (São Paulo)	sa-east-1	sa-east-1.amazonaws.com

TABELLE 1.3: Auflistung öffentlich zugänglicher AWS-Regionen

Über die Endpunktadressen können Sie innerhalb von Programmcode oder Skripten auf Ihre AWS-Ressourcen zugreifen. Die Endpunkte werden oft um Präfixe wie `ec2`, `apigateway` oder `cloudformation` erweitert, um einen spezifischen AWS-Service anzugeben. Die Adresse sieht also zum Beispiel so aus: `cloudformation.us-east-2.amazonaws.com`. Eine Auflistung aller Endpunktadressen mit Präfixen finden Sie unter `https://docs.aws.amazon.com/de_de/general/latest/gr/rande.html#ec2_region`.

Da der latenzarme Zugriff so wichtig ist, werden bestimmte AWS-Services von designierten Edge-Standorten aus angeboten. Zu diesen Services zählen Amazon CloudFront, Amazon Route 53, AWS Firewall Manager, AWS Shield und AWS WAF. Die vollständige und aktuelle Liste verfügbarer Standorte gibt es unter `https://aws.amazon.com/de/about-aws/global-infrastructure/regional-product-services/`.

Physische AWS-Rechenzentren werden in Ihrem AWS-Konto als sogenannte *Availability Zones* (AZs) aufgeführt. Innerhalb einer Region kann es ein halbes Dutzend solcher AZs geben, die mit Codes der Form `us-east-1a` identifiziert werden.

Zum Organisieren Ihrer Ressourcen aus bestimmten Regionen nutzen Sie Virtual Private Clouds (VPCs). Eine VPC ist im Prinzip ein Adressbereich im Netzwerk, innerhalb dessen Sie Subnetze erzeugen und bestimmten Availability Zones zuordnen können. Bei korrekter Konfiguration ermöglicht diese Architektur das effektive Abschotten von Ressourcen und die dauerhafte Replikation.

AWS-Zuverlässigkeit und Compliance

Wenn Sie Ihren ersten Service starten, sind dank AWS bereits viele wesentliche Anforderungen in Sachen Datenschutz, Rechtsvorschriften und Sicherheit automatisch erfüllt.

AWS hat enorm in die Planung und Ausgestaltung seiner Infrastruktur durch kompetente Experten investiert. Seine hochsicheren und abgeriegelten Rechenzentren, Redundanzschichten und sorgfältig entwickelten Verfahrensprotokolle lassen sich von kleineren Unternehmen nur schwer oder gar nicht replizieren.

Ressourcen auf der AWS-Plattform entsprechen je nach anwendbaren Vorgaben Dutzenden nationalen und internationalen Standards, Frameworks und Zertifizierungen, unter anderem der DSGVO, ISO 9001, FedRAMP und NIST. (Weitere Informationen hierzu finden Sie unter `https://aws.amazon.com/de/compliance/programs/`.)

Modell der gemeinsamen Verantwortung

Die eben genannten Standards und Vorkehrungen beziehen sich natürlich nur auf die zugrunde liegende AWS-Plattform. Wie Sie die AWS-Ressourcen schlussendlich nutzen, obliegt Ihrer Entscheidung und somit auch Ihrer Verantwortung. Hier kommt das Modell der gemeinsamen Verantwortung ins Spiel.

AWS garantiert den sicheren und ununterbrochenen Betrieb seiner Cloud, also seiner physischen Server, Speicherdienste, Netzwerkinfrastruktur und verwalteten Services. Die Kunden von AWS hingegen sind für all das verantwortlich, was *innerhalb* dieser Cloud passiert (siehe Abbildung 1.3). Dies umfasst die Sicherheit und Nutzung installierter Betriebssysteme, den Umgang mit Daten auf Clientseite, die Übertragung von Daten im Netzwerk, die Authentifizierung und Zugriffe von Endbenutzern sowie die Verarbeitung von Kundendaten.

Service-Level-Agreements von AWS

Wenn AWS den sicheren und zuverlässigen Betrieb seiner Cloud »garantiert«, ist damit nicht gemeint, dass *nie* irgendwelche Unterbrechungen oder Sicherheitslücken auftreten werden. Laufwerke können ausfallen, es kann zu Stromausfällen kommen und auch Naturkatastrophen lassen sich nicht durch eine bloße Garantie auf dem Papier abwenden. Falls aber wirklich einmal etwas schiefläuft und die Systemverfügbarkeit unter einem bestimmten Schwellenwert liegt, erstattet AWS dem Kunden seine *direkten* Verluste in Form von Servicegutschriften. Das entschädigt natürlich nicht unbedingt für verlorenes Vertrauen Ihrer eigenen Kunden oder entgangene Geschäfte.

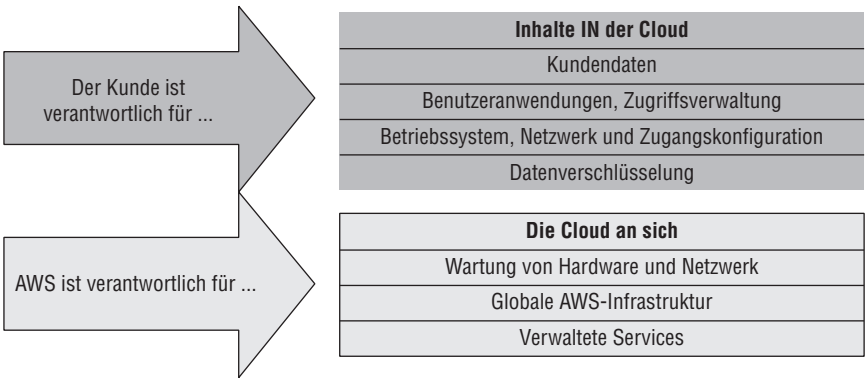


ABBILDUNG 1.3: Das Modell der gemeinsamen Verantwortung von AWS

Der exakte Schwellenwert unterscheidet sich von Service zu Service. Im Service-Level-Agreement (SLA) für AWS EC2 beispielsweise beträgt er 99,99 Prozent, das heißt, Ihre EC2-Instanzen, ECS-Container und EBS-Speicherressourcen dürfen im Monat maximal vier Minuten nicht verfügbar sein.

Bedenken Sie bei Ihrer Planung immer: Es stellt sich nicht die Frage, *ob* ein Service ausfällt, sondern *wann*. Sorgen Sie also dafür, dass Ihre Anwendungen möglichst regional verteilt ausgeführt werden und eine hohe Fehlertoleranz aufweisen. Eventuelle Störungen fallen Ihren Kunden dann meist gar nicht auf.

Die Arbeit mit AWS

Ihre gewählten AWS-Services müssen Sie logischerweise auch auf irgendeine Weise verwalten. Die browserbasierte Managementkonsole bietet Ihnen eine hervorragende Möglichkeit, sich mit den Funktionen des jeweiligen Service und seiner Anwendung in der Praxis vertraut zu machen. Es gibt kaum administrative Aufgaben, die Sie nicht über die Konsole erledigen könnten. Zudem erläutern zahlreiche Visualisierungen und Handbücher die Arbeit. Sobald Sie aber die Funktionen besser beherrschen und auch die Komplexität Ihrer AWS-Implementierungen zunimmt, werden Sie wahrscheinlich immer öfter ohne die Konsole arbeiten.

Die AWS-Befehlszeilen-Schnittstelle (CLI)

Die *AWS-Befehlszeilen-Schnittstelle* (»Command Line Interface«, kurz: CLI) ermöglicht Ihnen die Ausführung komplexer AWS-Funktionen über Ihre lokale Befehlszeile. Wenn Sie den Dreh erst mal raushaben, lassen sich viele Aufgaben deutlich einfacher und effizienter lösen.

Nehmen Sie zum Beispiel an, Sie möchten ein halbes Dutzend EC2-Instanzen starten, um eine Microservices-Umgebung zu erstellen. Jede Instanz übernimmt eine ganz bestimmte Funktion und muss daher mit gewissen individuellen Anpassungen bereitgestellt werden. Es wäre viel zu mühselig und zeitaufwendig, sich durch die ganzen Menüfenster der Konsole zu klicken, erst

recht, wenn diese Aufgabe mehrmals wöchentlich ausgeführt werden muss. Viel einfacher wäre es, den ganzen Prozess in ein simples Skript zu packen, das Sie mithilfe der AWS-CLI über Ihre lokale Befehlszeile oder PowerShell-Schnittstelle ausführen.

Die Installation und Konfiguration der AWS-CLI unter Linux, Windows oder macOS ist kinderleicht; die genauen Schritte dabei hängen von Ihrer Plattform ab. Eine aktualisierte Anleitung finden Sie unter `https://docs.aws.amazon.com/de_de/cli/latest/userguide/cli-chap-install.html`.

AWS-SDKs

Wenn Sie den Zugriff auf Ihre AWS-Ressourcen in Ihren Anwendungscode einbinden möchten, benötigen Sie für Ihre jeweilige Programmiersprache ein passendes AWS Software Development Kit (SDK). AWS bietet derzeit SDKs für neun Sprachen, einschließlich Java, .NET und Python, sowie mehrere SDKs für Mobilgeräte, unter anderem für Android und iOS. Auch für Eclipse, Visual Studio und VSTS gibt es Toolkits.

Eine komplette Übersicht aller Tools für Entwickler steht unter `https://aws.amazon.com/de/tools/` zur Verfügung.

Technische Unterstützung und Ressourcen im Web

Im Leben verläuft nicht immer alles nach Plan – und bei der Arbeit mit AWS auch nicht. Früher oder später werden Sie technische Unterstützung oder Hilfe mit Ihrem Konto benötigen. Zum Glück gibt es ein breites Spektrum an Support-Optionen, die Sie sich frühzeitig genauer anschauen sollten.

Schon beim Erstellen Ihres neuen AWS-Kontos müssen Sie eine der verschiedenen Support-Stufen auswählen. Welche am besten geeignet ist, hängt von Ihrem Vorhaben und Budget ab.

Support-Stufen

Der Standard-Support, auch als »Basic Support« bezeichnet, ist kostenlos und umfasst einen normalen Kundenservice sowie Handbücher, Whitepaper und ein Forum. Der Kundenservice beantwortet Fragen zur Abrechnung und zu Ihrem Konto.

Die Support-Stufe »Developer« ist ab 29 US-Dollar pro Monat erhältlich und stellt einem einzelnen benannten Kontoinhaber einen Cloud-Support-Techniker zur Seite. Außerdem erhalten Sie allgemeine Empfehlungen und eine schnellere Antwort bei Systembeeinträchtigungen.

Die nächsthöhere Stufe, nämlich »Business«, bietet ab 100 US-Dollar/Monat garantiert schnellere Antworten auf die Anfragen einer uneingeschränkten Anzahl von Benutzern bei Systembeeinträchtigungen, persönliche Unterstützung bei der Fehlersuche und eine Support-API.

Die Stufe »Enterprise« schließlich umfasst alle Leistungen der niedrigeren Stufen plus direkten Kontakt zu AWS Solutions Architects (die Sie beim Entwurf und der Implementierung beraten), zu Ihrem eigenen Technical Account Manager (TAM) und zum sogenannten Concierge Support Team (das Sie beim Wechsel in die Cloud generell begleitet). Bei komplexen,

geschäftskritischen Implementierungen ist so eine geballte Unterstützung natürlich nicht zu verachten – dafür müssen Sie aber auch mindestens 15.000 US-Dollar im Monat hinblättern.

Einen Vergleich aller Support-Stufen finden Sie unter `https://aws.amazon.com/de/premiumsupport/plans/`.

Weitere Support-Ressourcen

Abgesehen vom offiziellen Support gibt es zahlreiche Ressourcen, mit deren Hilfe Sie selbst nach einer Lösung für Ihr jeweiliges Problem suchen können.

- Die AWS-Foren stehen jedem mit gültigem AWS-Konto offen (`https://forums.aws.amazon.com`). Die Foren an sich sind derzeit nur auf Englisch verfügbar; es gibt aber ein Unterforum namens »German Forum«, in dem Sie sich auf Deutsch unterhalten können.
- Die umfangreiche und gut gepflegte AWS-Dokumentation können Sie unter `https://aws.amazon.com/documentation/` durchstöbern (gegebenenfalls müssen Sie im oberen Seitenbereich die Sprache auf Deutsch umstellen).
- Auf der Seite »AWS Well-Architected« (`https://aws.amazon.com/de/architecture/well-architected/`) finden sich allgemeine Informationen und diverse verlinkte Whitepaper und Handbücher mit Empfehlungen für Ihre Cloud-Implementierung.

Zusammenfassung

Cloud-Computing beruht auf dem Konzept der Virtualisierung, bei dem physische Ressourcen effizient in kleinere, flexiblere virtuelle Einheiten aufgeteilt werden. Diese Einheiten werden auf Basis eines »Pay-as-you-go«-Abrechnungsmodells von Unternehmen »angemietet«, um unterschiedlichste Anforderungen vernetzter Anwendungen oder Workflows auf kostengünstige, skalierbare und elastische Weise zu erfüllen.

Amazon Web Services bietet zuverlässige und sichere Ressourcen, die weltweit über eine wachsende Zahl an Regionen und Availability Zones hinweg repliziert und verteilt werden. Die AWS-Infrastruktur wird Branchenempfehlungen und gesetzlichen Vorgaben gerecht, überträgt Ihnen aber im Rahmen des Modells der gemeinsamen Verantwortung die Pflicht, die Rechtmäßigkeit Ihrer Aktivitäten *innerhalb* der Cloud sicherzustellen.

Das immer größere Portfolio an AWS-Services erfüllt quasi jede denkbare Anforderung an digitale Dienste. Die zentralen Services decken die Kategorien Datenverarbeitung, Netzwerk, Datenbanken, Speicherung, Sicherheit und Anwendungsverwaltung ab.

Ihre AWS-Ressourcen verwalten Sie über die Managementkonsole, über die AWS-Befehlszeilen-Schnittstelle (CLI) oder über Code, den Sie mit einem AWS-SDK generieren.

Technischen Support und Hilfe zu Ihrem Konto erhalten Sie im Rahmen verschiedener Support-Stufen sowie in diversen Handbüchern und Foren. Whitepaper und Leitfäden für Benutzer und Entwickler stehen als kostenlose E-Books für Kindle bereit. Sie finden sie unter: `https://www.amazon.de/Amazon-Web-Services/e/B007R6MVQ6/ref=dp_byline_cont_ebooks_1`.

Prüfungsschwerpunkte

Verständnis der AWS-Plattformarchitektur: AWS unterteilt seine Server und Speicherdienste in weltweit verteilte Regionen, die wiederum in Availability Zones gegliedert sind. Diese Unterteilung erlaubt es, Daten innerhalb von AZs oder auch regionsübergreifend zu replizieren, um so die Verfügbarkeit zu verbessern oder um Prozesse und Ressourcen aus Sicherheits- und Compliance-Gründen voneinander abzuschotten. Machen Sie sich diese Vorteile bei Ihren eigenen Implementierungen zunutze!

Verwendung der AWS-Verwaltungstools: Wenngleich Sie sicherlich hin und wieder die browserbasierte AWS-Konsole nutzen werden, lassen sich viele Aufgaben besser über die AWS-Befehlszeilen-Schnittstelle (CLI) und aus Ihrem Programmcode heraus über AWS-SDKs erledigen.

Auswahl einer Support-Stufe: Um eine erfolgreiche Implementierung zu gewährleisten, müssen Sie die richtige Support-Stufe für die konkreten Kundenanforderungen auswählen können. Machen Sie sich daher mit den verfügbaren Optionen gut vertraut!

Übung

ÜBUNG 1.1

Verwenden der AWS-Befehlszeilen-Schnittstelle (CLI)

Installieren und konfigurieren Sie die AWS-CLI auf Ihrem lokalen System (sofern Sie dies noch nicht getan haben) und prüfen Sie die korrekte Funktionsweise, indem Sie sich die derzeit aktiven Buckets in Ihrem Konto anzeigen lassen. Ein Fleißbienchen können Sie sich verdienen, wenn Sie außerdem selbst einen S3-Bucket erzeugen und dann eine einfache Datei oder ein Textdokument von Ihrem Rechner in den neuen Bucket kopieren. Überprüfen Sie in der Browserkonsole, ob die Datei ihr Ziel korrekt erreicht hat.

Als Starthilfe seien hier folgende CLI-Befehle genannt:

```
aws s3 ls
aws s3 mb <bucketname>
aws s3 cp /path/to/file.txt s3://bucketname
```

Testfragen

1. Ihre Entwickler wollen vollständig bereitgestellte EC2-Instanzen ausführen, um die Implementierung ihres Anwendungscodes zu unterstützen, möchten sich dabei aber nach Möglichkeit die manuelle Konfiguration und Inbetriebnahme der nötigen Infrastruktur ersparen. Welchen der folgenden Services sollten sie nutzen?
   - **A.** AWS Lambda
   - **B.** AWS Elastic Beanstalk
   - **C.** Amazon EC2 Auto Scaling
   - **D.** Amazon Route 53

2. Welchen Service würden Sie wählen, um am effektivsten die Latenzzeiten beim Zugriff auf Ihre Anwendungsressourcen über das Internet durch Endbenutzer zu verkürzen?
   - **A.** Amazon CloudFront
   - **B.** Amazon Route 53
   - **C.** Elastic Load Balancing
   - **D.** Amazon Glacier

3. Für welches der folgenden Anwendungsszenarien ist Elastic Block Store am besten geeignet?
   - **A.** Sie benötigen preiswerten und zuverlässigen Speicherplatz für Dateien, auf die Ihre Anwendung zugreifen kann.
   - **B.** Sie benötigen einen sicheren Speicherplatz für Backup-Archive Ihrer lokalen Server.
   - **C.** Sie benötigen eine Möglichkeit, Rechenzyklen nach Bedarf zu buchen, um eine wechselhafte Nachfrage nach Ihrer Anwendung zu bewältigen.
   - **D.** Sie benötigen persistenten Speicher für das Dateisystem, das von Ihrer EC2-Instanz ausgeführt wird.

4. Welches der folgenden Tools eignet sich am besten, um den Zugriff auf Ihre AWS-Services und die Managementkonsole zu steuern?
   - **A.** AWS Identity and Access Management (IAM)
   - **B.** Key Management Service (KMS)
   - **C.** AWS Directory Service
   - **D.** Simple WorkFlow (SWF)

5. Für Daten-Workloads, die mehr Geschwindigkeit und Flexibilität erfordern, als eine klar definierte Struktur bieten kann, empfiehlt sich welcher der folgenden Services?
   - **A.** Relational Database Service (RDS)
   - **B.** Amazon Aurora
   - **C.** Amazon DynamoDB
   - **D.** Key Management Service (KMS)

6. Welcher der folgenden Endpunkte entspricht der Adresse für eine EC2-Instanz in der Region Irland?
   - **A.** `compute.eu-central-1.amazonaws.com`
   - **B.** `ec2.eu-central-1.amazonaws.com`
   - **C.** `elasticcomputecloud.eu-west-2.amazonaws.com`
   - **D.** `ec2.eu-west-1.amazonaws.com`
7. Was ist mit dem Begriff »Availability Zone« in der AWS-Dokumentation gemeint?
   - **A.** Ein isoliertes physisches Rechenzentrum (oder mehrere solcher Rechenzentren) innerhalb einer AWS-Region
   - **B.** Sämtliche Hardwareressourcen innerhalb einer einzigen Region
   - **C.** Ein einzelnes Subnetz, das von Ressourcen innerhalb einer Region genutzt wird
   - **D.** Ein einzelner isolierter Serverraum im Rechenzentrum
8. Mit welchem AWS-Tool können Sie Ihre EC2-Instanzen organisieren und ihre Netzwerkkonnektivität und Zugriffssteuerung konfigurieren?
   - **A.** Load Balancing
   - **B.** Amazon Virtual Private Cloud (VPC)
   - **C.** Amazon CloudFront
   - **D.** AWS-Endpunkte
9. Sie möchten sicherstellen, dass die Anwendung, die Sie mithilfe von EC2- und S3-Ressourcen gerade entwickeln, die Standards Ihrer Branche in Sachen Zuverlässigkeit erfüllt. Wo finden Sie die relevanten Angaben?
   - **A.** Protokolle mit Daten zu bisherigen Systemverfügbarkeiten
   - **B.** AWS Program Compliance Tool
   - **C.** Service-Level-Agreements von AWS
   - **D.** Modell der gemeinsamen Verantwortung von AWS
10. Welches der folgenden Tools würden Sie nutzen, um Ihre AWS-Infrastruktur über Ihre lokale Befehlszeile oder Shell-Skripte zu verwalten?
    - **A.** AWS Config
    - **B.** AWS-Befehlszeilen-Schnittstelle (CLI)
    - **C.** AWS-SDK
    - **D.** AWS-Konsole
11. Ihr Unternehmen benötigt einen direkten Support-Ansprechpartner für die Leiter sowohl Ihres Entwicklerteams als auch Ihrer IT-Abteilung. Welche Support-Stufe benötigen Sie mindestens?
    - **A.** Business
    - **B.** Developer
    - **C.** Basic
    - **D.** Enterprise