Engineer

AWS

die Cloud-Plattform von Amazon

Was es ist

AWS steht für Amazon Web Services, Amazons Geschäft mit stunden- und gigabyteweise vermieteter Rechenleistung: virtuelle Server, Dateispeicher, verwaltete Datenbanken, private Netze, Warteschlangen und viele weitere Dienste. Sie werden über eine API eingeschaltet und einem Konto berechnet. Amazon verkauft dies seit 2006. Zwei bekannte Dienste erklären viel vom Rest: Amazon EC2 vermietet virtuelle Maschinen, bei AWS Instanzen genannt. Amazon S3 speichert Dateien als Objekte in Behältern namens Buckets.

Nach der NIST-Definition ist AWS eine öffentliche Cloud. Wer eine Zahlungskarte besitzt, kann ein Konto öffnen. Ressourcen erscheinen binnen Minuten, jede Sekunde und jedes Gigabyte werden gemessen. Übliche Alternativen sind Microsoft Azure und Google Cloud mit ähnlichen Bausteinen unter anderen Namen. Eine EC2-Instanz entspricht einer virtuellen Maschine in Azure oder einer Instanz von Compute Engine in Google Cloud.

Jede Ressource hat einen bestimmten Ort. AWS ist in Regionen aufgeteilt, die jeweils so ausgelegt sind, dass sie von den anderen isoliert sind. Jede enthält mehrere Availability Zones. Eine Zone besteht aus einem oder mehreren getrennten Rechenzentren mit redundanter Stromversorgung, Netzwerktechnik und Konnektivität und ist physisch von anderen Zonen ihrer Region getrennt. Ressourcen entstehen in einer Region, häufig in einer einzelnen Zone. Teams wählen den Ort anhand von Latenz, Recht und Preis.

Der gesamte Zugriff läuft über AWS Identity and Access Management, kurz IAM. Ein Konto beginnt mit einem Root-Nutzer, der alles darf. IAM ergänzt Nutzer, Gruppen, Rollen und Richtlinien, die festlegen, welcher API-Aufruf unter welchen Bedingungen an welcher Ressource erlaubt ist. Die meisten AWS-Sicherheitsfragen erweisen sich als Fragen zu diesen Richtlinien.

Das Konzept für eine Entscheidung nutzen

Nutzen Sie „Was ist AWS?“ für eine konkrete Entscheidung. Wir können helfen, das Konzept mit dem System in Verbindung zu bringen, das Sie entwickeln oder einkaufen. Server werden nach dem tatsächlichen Bedarf dimensioniert und in die Cloud oder aus ihr heraus verlagert — die monatlichen Kosten stehen vorher fest.

Unsere Leistungen entdecken Kontakt aufnehmen →

Die Annahmen hinter dem Begriff prüfen

Nutzen Sie die Erklärung und die verlinkten Arbeiten, um Fragen für Ihr Projekt zu formulieren. Wir können die Annahmen gemeinsam mit Ihnen prüfen, bevor ein Werkzeug ausgewählt wird. 20 Docker-Apps auf Google Cloud und AWS betrieben — 20 bereitgestellte und überwachte Containeranwendungen

20 Docker-Apps auf Google Cloud und AWS betrieben Kontakt aufnehmen →

Warum es wichtig ist

Teams wählen AWS wegen der Breite. Ein Produkt mit verwaltetem PostgreSQL, Warteschlange, Content Delivery Network, Objektspeicher und Containerlaufzeit kann alles über eine Rechnung, ein Identitätssystem und ähnlich aufgebaute Dokumentation erhalten. Diese Breite hat einen Preis. Jeder Dienst hat eigene Preisdimensionen, Grenzen und einen eigenen Bereich der IAM-Richtliniensprache. Wer zehn Dienste übernimmt, pflegt zehn kleine Integrationen mit Amazons Schnittstellen. Ein späterer Ausstieg muss jede ersetzen.

Die zweite Entscheidung betrifft das, was beim Kunden bleibt. AWS veröffentlicht ein Modell geteilter Verantwortung und zieht die Grenze mit zwei Formulierungen: AWS verantwortet die Sicherheit „der“ Cloud, also „Hardware, Software, Netzwerktechnik und Einrichtungen, die AWS-Cloud-Dienste betreiben“. Der Kunde verantwortet die Sicherheit „in“ der Cloud. Die Grenze hängt vom Dienst ab. Auf EC2 patcht der Kunde das Gastbetriebssystem, betreut alle installierten Programme und konfiguriert die Sicherheitsgruppe als vorgelagerte Firewall. Bei S3 oder DynamoDB betreibt AWS Betriebssystem und Plattform. Beim Kunden bleiben Daten, Verschlüsselungsoptionen und die Zugriffsrechte.

Die dritte Entscheidung ist der Preis. Er ist bei AWS eher eine Eigenschaft des Entwurfs als eine später eintreffende Rechnung. Amazons Well-Architected Framework nennt sechs Säulen, an denen eine Workload geprüft werden soll: operative Exzellenz, Sicherheit, Zuverlässigkeit, Leistungseffizienz, Kostenoptimierung und Nachhaltigkeit. Kosten gehören dazu, weil dieselbe Lösung durch Entscheidungen der ersten Woche billig oder teuer wird: Instanzgrößen, Anzahl der Zonen, Datenverkehr aus der Region und verwaltete Dienste anstelle eines Prozesses auf einem einfachen Server.

Wie es in der Praxis aussieht

Auf der Technikseite steht AWS neben Google Cloud als eine der beiden üblicherweise verwendeten Clouds. Azure kommt hinzu, wenn der Kunde bereits dort arbeitet.

Ein Auftrag nutzte beide zugleich: Zwanzig Docker-Anwendungen liefen über Google Cloud und AWS verteilt, darunter R-basierte Analyseanwendungen. Sie wurden in beiden Clouds mit derselben Konfiguration und Überwachung bereitgestellt und gepflegt, damit keine Anwendung zum Sonderfall wurde. Bei Fehlern erfolgte die Fehlersuche mit Podman und die Orchestrierungsdiagnose mit Kubernetes. Die Analyseanwendungen blieben auf beiden Seiten stabil und reproduzierbar im Produktivbetrieb.

Ein anderer Auftrag ging in die Gegenrichtung. Bei einem internationalen Kunden war eine AWS-Umgebung überdimensioniert und um ungenutzte Dienste angewachsen. Die Kosten standen nicht mehr im Verhältnis zum Bedarf. Die Arbeit prüfte die tatsächlich genutzten Dienste, entfernte unnötige, passte die verbleibende Kapazität an und verlagerte Workloads von AWS weg. Diese Infrastrukturänderungen sind die dokumentierte Leistung. Der Nachweis belegt weder ein unter gleichen Bedingungen gemessenes Kostenverhältnis noch eine Produktivitätsmessung oder eine unterbrechungsfreie Migration. Nützlich ist das Beispiel wegen der Methode, eine bestehende Umgebung zu untersuchen und ihren Betrieb am tatsächlichen Unternehmensbedarf auszurichten, nicht als Zusage einer bestimmten Ersparnis.

Beide Beispiele beruhen auf derselben Gewohnheit. Nutzungsabhängige Dienste berechnen alles Eingeschaltete. Ein AWS-Bestand bleibt deshalb gesund, wenn jemand laufend vergleicht, was läuft und was das Unternehmen verwendet.

Wo es schiefgeht

AWS verliert selten Daten oder bleibt lange ausgefallen. Teure Vorfälle beginnen meist im Kundenkonto.

Der Root-Nutzer erledigt die Tagesarbeit. Jedes Konto beginnt mit der eröffnenden E-Mail-Adresse und einem Passwort als Root-Zugang. Dieser hat unbegrenzten Zugriff auf alle Ressourcen und Einstellungen, einschließlich der Kontoschließung. Alltägliche Root-Anmeldung bedeutet, dass ein geleaktes

Passwort alles erreicht. AWS empfiehlt, Root-Zugangsdaten zu schützen, mit Mehrfaktorauthentifizierung zu sichern und für die wenigen nötigen Aufgaben zurückzuhalten. Tägliche Arbeit erfolgt über föderierte Anmeldung und Rollen.

Langlebige Zugriffsschlüssel werden offengelegt. Ein Schlüsselpaar funktioniert bis zur Löschung und reist leicht: in Dotfiles eines Laptops, CI-Variablen, Containerimages oder Commits. Die IAM-Empfehlungen beginnen am anderen Ende. Menschen melden sich beim Identitätsanbieter an und bekommen befristete Zugangsdaten. Workloads erhalten sie aus einer IAM-Rolle an ihrer Rechenressource. Wo ein dauerhafter Schlüssel wirklich nötig ist, wird er rotiert. Ungenutzte Schlüssel, Nutzer und Rollen werden entfernt.

Ein Budgetalarm gilt als Bremse. AWS Budgets meldet, wenn tatsächliche oder prognostizierte Ausgaben eine Grenze überschreiten. Die Werte werden bis zu dreimal täglich aktualisiert. Ein Alarm meldet also bereits ausgegebenes Geld; die Ressourcen laufen und kosten weiter. Budgets kann auch handeln, etwa mit einer IAM- oder Service-Control-Richtlinie gegen neue Ressourcen oder an bestimmten EC2- beziehungsweise RDS-Instanzen. Das geschieht nur, wenn die Handlung vorher samt ausführender Rolle konfiguriert wurde.

Alles liegt in einer Availability Zone. Eine Instanz mit einer Platte in einer Zone ist am billigsten und teilt das Schicksal dieses Ortes. Zonen sollen dafür sorgen, dass ein Strom- oder Netzfehler einer Zone die anderen weiterlaufen lässt. AWS empfiehlt die Verteilung auf mehrere. Eine wichtige Datenbank erhält einen Standby in einer zweiten Zone. Die Webschicht erhält Instanzen in mindestens zwei Zonen hinter einem beide umfassenden Load Balancer.

Ein für eine Vorführung geöffneter Bucket bleibt offen. Neue S3-Buckets sperren öffentlichen Zugriff standardmäßig. Eine Bucket-Richtlinie oder Objektberechtigung kann das jedoch in einer Minute ändern. Ein für einen Nachmittag geteilter Link ist ein Jahr später noch öffentlich. S3 Block Public Access auf Konto- oder Organisationsebene überstimmt solche Richtlinien. Aktivieren Sie es, wo kein Veröffentlichungsbedarf besteht, und liefern Sie öffentliche Dateien aus einem dafür gebauten Bucket.

Weiterführende Lektüre

- AWS Documentation — Nutzerleitfäden, API-Referenzen und Anleitungen für jeden Dienst.

- Geteilte Verantwortung — die Sicherheitssäule des Well-Architected Frameworks zu den Zuständigkeiten von AWS und Kunden.
- Die Säulen des Frameworks — sechs Prüfbereiche, darunter Kosten und Zuverlässigkeit.
- AWS-Regionen und Availability Zones — Isolation der Regionen und Zonen sowie Gründe für zonenübergreifende Anwendungen.
- Sicherheitsempfehlungen für IAM — Föderation, Rollen, Mehrfaktorauthentifizierung, Root-Nutzer und geringste Rechte.
- Kostenverwaltung mit AWS Budgets — Budgets für tatsächliche und erwartete Ausgaben, Benachrichtigungen und ausführbare Aktionen.

Glossar

Für Ihre tatsächlichen Rahmenbedingungen auswählen

Beschreiben Sie den Bereitstellungsweg, die Betriebsrisiken und die Bereitschaftsverantwortlichen. Wir können eine Änderung mit Prüfungen, einem Wiederherstellungsweg und klaren Zuständigkeiten abgrenzen.

Preise ansehen Kontakt aufnehmen →

Die Begriffe praktisch nutzbar machen

Fragen Sie, wie „Was ist AWS?“ auf Ihre Organisation zutrifft. Ein konkretes Beispiel aus Ihrem bestehenden System reicht aus, um das Gespräch zu beginnen.

Unsere Leistungen entdecken

welcome@engineer.company +45 50 10 61 84 Kopenhagen, Dänemark

Nehmen Sie diese Seite mit

Kontaktkarte

Mit Sorgfalt und Liebe gestaltet von D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Copyright © 2025 – heute · Engineer ApS · Alle Rechte vorbehalten.

Gedruckt von https://engineer.company/de/glossary/aws/