Engineer

AWS

Amazons cloud-platform

Hvad det er

AWS, forkortelse for Amazon Web Services, er Amazons forretning med at udleje computerkraft pr. time og pr. gigabyte: virtuelle servere, fillagring, administrerede databaser, private netværk, køer og et langt katalog af andre tjenester, som alle tændes via ét API og faktureres til én konto. Amazon har solgt det siden 2006. To af de bedst kendte tjenester forklarer meget af resten. Amazon EC2 udlejer virtuelle maskiner, som AWS kalder instanser, og Amazon S3 gemmer filer som objekter i beholdere, der hedder buckets.

Med ordene fra NIST's definition er AWS en offentlig cloud: alle med et betalingskort kan oprette en konto, ressourcer dukker op på få minutter, og hvert sekund og hver gigabyte forbrug bliver målt. AWS bliver typisk sammenlignet med Microsofts Azure og med Google Cloud, der sælger stort set de samme byggeklodser under andre navne. Det, AWS kalder en EC2-instans, er en virtuel maskine i Azure og en Compute Engine-instans i Google Cloud.

Hver ressource i AWS ligger et bestemt sted. Tjenesten er delt op i regioner (Regions), som hver er bygget til at være isoleret fra de andre, og hver region rummer flere tilgængelighedszoner (Availability Zones). En zone er et eller flere separate datacentre med redundant strøm, netværk og forbindelser, fysisk adskilt fra regionens andre zoner. En ressource oprettes i én region, ofte i en enkelt zone, og holdet vælger stedet ud fra latenstid, lovgivning og pris.

Adgangen til det hele går gennem AWS Identity and Access Management, kaldet IAM. En konto starter med en root-bruger, der kan alt, og IAM tilføjer brugere, grupper, roller og politikker, der bestemmer, hvilket API-kald der er tilladt på hvilken ressource og under hvilke betingelser. De fleste spørgsmål om sikkerhed i AWS viser sig at handle om netop de politikker.

Brug begrebet i en beslutning

Brug »Hvad er AWS?« i en konkret beslutning. Vi kan knytte begrebet til det system, I bygger eller køber. Servere dimensioneret efter det, I rent faktisk bruger, flyttet op i skyen eller hjem igen, med den månedlige regning regnet ud først.

Se vores ydelser Kontakt os →

Undersøg antagelserne bag ordet

Brug forklaringen og det tilknyttede arbejde til at formulere spørgsmål til jeres projekt. Vi kan undersøge antagelserne sammen, før et værktøj vælges. Har drevet 20 Docker-apps på Google Cloud og AWS — 20 containeriserede applikationer udrullet og overvåget

Har drevet 20 Docker-apps på Google Cloud og AWS Kontakt os →

Hvorfor det betyder noget

Hold vælger AWS for bredden. Et produkt, der har brug for en administreret PostgreSQL, en kø, et CDN, objektlagring og et sted at køre containere, kan få det hele på én regning og i ét identitetssystem, dokumenteret efter samme mønster. Bredden er også prisen. Hver tjeneste har sine egne prisparametre, sine egne grænser og sit eget hjørne af IAM's politiksprog, og et hold, der tager ti tjenester i brug, vedligeholder derefter ti små integrationer med Amazons grænseflader. At flytte væk senere betyder at erstatte hver eneste af dem.

Den anden beslutning handler om, hvad der bliver hos kunden. AWS beskriver en model for delt ansvar og trækker grænsen med to engelske vendinger: AWS står for sikkerheden »of the cloud«, altså den hardware, software, det netværk og de faciliteter, der kører tjenesterne, og kunden for sikkerheden »in the cloud«. Hvor grænsen går, afhænger af tjenesten. På en EC2-instans opdaterer kunden gæsteoperativsystemet, passer hvert program, der er installeret på den, og konfigurerer dens security group, firewallen foran instansen. På S3 eller DynamoDB kører AWS operativsystemet og platformen, og kunden står tilbage med dataene, valgene om kryptering og de rettigheder, der afgør, hvem der må læse dem.

Den tredje er omkostninger, som i AWS er en egenskab ved designet mere end en faktura, der kommer bagefter. Amazons Well-Architected Framework nævner seks søjler, som en workload skal vurderes ud fra: driftsmæssig ekspertise, sikkerhed, pålidelighed, ydelseseffektivitet, omkostningsoptimering og bæredygtighed. Omkostninger hører med på listen, fordi det samme system kan bygges billigt eller dyrt med valg, der træffes i den første uge: instansstørrelser, antal zoner, hvor meget data der forlader regionen, og hvilke administrerede tjenester der afløser en proces på en almindelig server.

Sådan ser det ud i praksis

På siden om teknologistakken står AWS ved siden af Google Cloud som de to clouds, virksomheden arbejder i som standard, med Azure, hvor en kunde allerede er.

Et forløb brugte begge de clouds på én gang: tyve Docker-applikationer kørte på tværs af Google Cloud og AWS, nogle af dem R-baserede analyseapps. De blev udrullet og vedligeholdt med samme konfiguration og overvågning i begge clouds, så ingen app blev et særtilfælde. Ved fejl gik fejlfindingen gennem Podman og orkestreringsdebugging gennem Kubernetes, og analyseappsene blev holdt stabile og reproducerbare i produktion på begge sider.

Et andet forløb gik den modsatte vej. For en international kunde var et AWS-setup blevet overdimensioneret og havde samlet ubrugte tjenester, og omkostningerne var vokset ud af proportion med forretningens behov. Arbejdet gennemgik, hvilke tjenester der blev brugt, fjernede unødvendige tjenester, tilpassede den resterende kapacitet og flyttede workloads væk fra AWS. Det er de leverede infrastrukturændringer, som registreringen beskriver. Den dokumenterer ikke et sammenligneligt omkostningsforhold, en produktivitetsmåling eller en flytning uden driftsforstyrrelser. Eksemplet er nyttigt for metoden til at undersøge det eksisterende setup og ændre det, forretningen har brug for at drive, ikke som et løfte om en bestemt besparelse.

Begge sager handler om den samme vane. En tjeneste med betaling efter forbrug fakturerer for alt, der er tændt, så en AWS-opsætning holder sig sund, når nogen løbende sammenligner det, der kører, med det, forretningen bruger.

Hvor det går galt

AWS mister sjældent data eller er nede længe. De dyre hændelser begynder oftest inde på kundens egen konto.

Root-brugeren klarer dagens arbejde. Hver konto begynder med en root-bruger, den e-mailadresse og adgangskode, der oprettede den, med ubegrænset adgang til alle ressourcer og indstillinger, også til at lukke kontoen. Logger man ind som root til rutineopgaver, når én lækket adgangskode alt. AWS anbefaler at beskytte root-brugerens loginoplysninger, sætte multifaktorgodkendelse på dem og gemme dem til de få opgaver, der kræver dem, mens det daglige arbejde foregår via fødereret login og roller.

Langlivede adgangsnøgler lækker. Et nøglepar virker, indtil nogen sletter det, og det rejser let: ind i dotfiles på en bærbar, i en CI-variabel, i et containerimage, i et commit. IAM's liste over god praksis starter i den anden ende. Mennesker logger ind via en identitetsudbyder og får midlertidige loginoplysninger, og workloads henter midlertidige loginoplysninger fra en IAM-rolle, der er knyttet til den maskine, de kører på. Hvor en langvarig nøgle er uundgåelig, skal den roteres, og nøgler, brugere og roller, der står ubrugte hen, skal fjernes.

En budgetadvarsel bliver taget for en bremse. AWS Budgets sender en besked, når det faktiske eller det forventede forbrug passerer en grænse, og tallene opdateres op til tre gange om dagen, så en advarsel melder om penge, der allerede er brugt. Ressourcerne kører videre og bliver ved med at koste. Budgets kan også udføre en handling, for eksempel anvende en IAM-politik eller en service control policy, der forhindrer, at nye ressourcer oprettes, eller gribe ind over for bestemte EC2- eller RDS-instanser. Det sker kun, når handlingen er sat op på forhånd med en rolle at handle igennem.

Alt står i én tilgængelighedszone. En enkelt instans med en enkelt disk i én zone er den billigste opstilling, og den deler skæbne med det ene sted. Zonerne findes, for at en strøm- eller netværksfejl ét sted lader de andre køre videre, og AWS' dokumentation anbefaler at sprede en applikation over flere. En database, der betyder noget, får en standby i en anden zone, og et weblag får instanser i mindst to, bag en load balancer, der spænder over begge.

En bucket, der blev åbnet til en demo, forbliver åben. Nye S3-buckets blokerer offentlig adgang som standard, men en bucket-politik eller en objekttilladelse kan ændre det på et minut, og et link, der blev delt med en kunde for en eftermiddag, er stadig offentligt et år senere. S3 Block Public Access, sat for hele kontoen eller organisationen, tilsidesætter de politikker. Slå det til overalt, hvor en konto ikke har grund til at offentliggøre filer, og server offentlige filer fra en bucket, der er bygget til formålet.

Læs mere

- AWS Documentation — oversigten over brugervejledninger, API-referencer og vejledninger til hver AWS-tjeneste.
- Shared responsibility — sikkerhedssøjlen i Well-Architected om, hvilke lag AWS sikrer, og hvilke kunden sikrer.
- The pillars of the framework — de seks områder, AWS vurderer en workload ud fra, herunder omkostninger og pålidelighed.

- AWS Regions and Availability Zones — hvordan regioner og zoner er isoleret, og hvorfor en applikation bør spænde over flere zoner.
- Security best practices in IAM — føderation, roller, multifaktorgodkendelse, root-brugeren og mindste privilegium samlet i én liste.
- Managing your costs with AWS Budgets — budgetter for faktisk og forventet forbrug, deres beskeder og de handlinger, de kan udføre.

Ordliste

Vælg ud fra jeres faktiske vilkår

Medbring udrulningsforløbet, driftsrisiciene og dem, der har vagten. Vi kan afgrænse en ændring med kontroller, en vej tilbage og tydeligt ansvar.

Se, hvad det koster Kontakt os →

Gør begreberne praktiske

Spørg, hvordan »Hvad er AWS?« gælder i jeres organisation. Et konkret eksempel fra jeres nuværende system er nok til at begynde samtalen.

Se vores ydelser

welcome@engineer.company +45 50 10 61 84 København, Danmark

Tag denne side med dig

Visitkort

Lavet med kærlighed af D.

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

Copyright © 2025 – nu · Engineer ApS · Alle rettigheder forbeholdes.

Udskrevet fra https://engineer.company/da/glossary/aws/