

Connecting Clouds in a Multicloud Strategy

Research on a Multicloud Approach and Practical Implementation

Lorenzo ELIAS
Student Bachelor Electronics-ICT – Cloud & Cyber Security

Voorwoord

Ik ben Lorenzo Elias, student aan Thomas More in Geel en volg een bacheloropleiding Elektronica-ICT met een specialisatie in Cloud & Cyber Security. Met oprechte dankbaarheid voor alle kennis en ervaringen die ik tijdens mijn studie heb opgedaan, presenteer ik met trots dit onderzoek.

Ter afsluiting van mijn academische carrière liep ik 18 weken stage bij Cegeka in Hasselt, binnen het Network & Security-team. Cegeka is een toonaangevende Europese leverancier van IT-oplossingen met een sterke focus op innovatie en digitale informatie. Dit onderzoek markeert niet alleen het einde van mijn studententijd, maar ook het begin van een nieuw hoofdstuk vol kansen en uitdagingen. Tijdens mijn stage werkte ik aan de technische en strategische aspecten van multicloudstrategieën. Met volle inzet en enthousiasme onderzocht ik de verschillen tussen grote cloudproviders en ontwikkelde ik een proof of concept (PoC) voor een volledig geïntegreerde multicloudomgeving. Het doel was niet alleen om te begrijpen hoe dergelijke architecturen gebouwd kunnen worden, maar ook om te evalueren wanneer en waarom ze de moeite waard zijn om te implementeren in reële bedrijfscontexten.

Bij Cegeka had ik het voorrecht omringd te zijn door een toegewijd en inspirerend team. De steun en begeleiding gaven me de ruimte om professioneel te groeien. Ondanks de druk die zo'n project soms met zich meebrengt, zoek ik altijd naar uitdagingen die me de kans geven mijn eigen grenzen te verleggen. Mijn nieuwsgierigheid, passie en doorzettingsvermogen hielden me gefocust en gemotiveerd om het best mogelijke resultaat te behalen.

Ik wil graag mijn oprechte dank uitspreken aan mijn mentoren, met name Toon Vanoeteren, Dirk Stegen en Jan Weyens. Toon heeft me vanaf het begin begeleid en was altijd beschikbaar voor feedback en advies. Jan en Dirk, mijn stagebegeleiders, moedigden me aan om zelfstandig te werken en kritisch te denken. Ik wil ook het hele Network & Security-team bedanken voor de gastvrijheid en het creëren van een omgeving waarin ik mezelf kon zijn. Dankzij dit team voelde Cegeka meer dan alleen een werkplek; het voelde als een plek waar ik echt thuishoorde.

Terugkijkend op mijn tijd bij Thomas More en Cegeka voel ik een diepe waardering. Deze ervaring heeft mijn passie voor de IT-wereld bevestigd en de basis gelegd voor de professional die ik wil worden.

Lorenzo Elias

Abstract

Dit proefschrift onderzoekt hoe een multicloudomgeving kan worden geïmplementeerd en onder welke omstandigheden een dergelijke strategie gerechtvaardigd is. Naast een theoretische vergelijking van de technische en strategische verschillen tussen platforms, is een proof of concept (PoC) ontwikkeld om de technische haalbaarheid aan te tonen van de integratie van meerdere cloudproviders, zoals Azure en OCI, en deze veilig te verbinden met een on-premises datacenter met behulp van site-to-site VPN-tunnels. De opstelling maakt gebruik van hub-and-spoke-netwerken, firewallclusters en aangepaste routing. Hoewel een multicloudopstelling voordelen biedt zoals flexibiliteit en workloadoptimalisatie, toont dit onderzoek ook aan dat multicloud nooit de standaard mag zijn, maar een bewuste strategie moet zijn, gedreven door duidelijke zakelijke of technische behoeften. De resultaten tonen een verhoogde complexiteit en verborgen kosten aan. In veel gevallen maken deze factoren multicloudopstellingen duurder dan single-cloudopstellingen. In specifieke scenario's, zoals compliancevereisten, workloadspecialisatie of klantgedreven eisen, kan een multicloudstrategie echter een geldige en strategische keuze zijn. Dit project draagt bij aan de interne expertise van Cegeka en biedt praktische inzichten voor organisaties die een multicloudaanpak overwegen. Voor dergelijke organisaties biedt het ontwikkelen van multicloudexpertise een concurrentievoordeel, waardoor ze een bredere klantenbasis kunnen ondersteunen en nieuwe commerciële kansen kunnen ontsluiten.

Inhoudsopgave

INLEIDING _____ **FOUT! BLADWIJZER NIET GEDEFINIEERD.**

1. CLOUDOMGEVINGEN _____ **9**

1.1. Geschiedenis en marktaandeel van cloudproviders _____ 10

1.2. Definitie van een multicloudomgeving _____ 11

2. VERSCHILLENDE CLOUDPROVIDERS _____ **12**

2.1. Globale infrastructuur en terminologie _____ 12

2.2. Diensten _____ **Fout! Bladwijzer niet gedefinieerd.**

2.3. Sterke punten en gespecialiseerde diensten _____ 14

2.4. Identiteits- en toegangsbeheer (IAM) _____ 15

2.4.1. IAM in AWS _____ 16

2.4.2. IAM in Azure _____ 16

2.4.3. IAM in OCI _____ 16

3. MULTICLOUDSTRATEGIEËN _____ **17**

3.1. Voordelen en uitdagingen van een multicloudstrategie _____ 17

3.2. Gerechtvaardigde gebruiksgevallen _____ 18

3.2.1. Gebruiksscenario 1: Specialisatie van werklasten over providers heen _____ 19

3.2.2. Gebruiksscenario 2: Bedrijfsfusies en klantbeperkingen _____ 19

3.2.3 Gebruiksscenario 3: Klant- of nalevingsgestuurde platformscheiding _____ 19

3.3. Wanneer multicloud niet gerechtvaardigd is _____ 19

3.4. Kostenoverwegingen _____ 20

3.4.1. Scenario 1: Multicloud- _____ 20

3.4.2. Scenario 2: Single Cloud-implementatie _____ 21

3.4.3. Kosteninterpretatie en bredere overwegingen _____ 22

4. BEWIJS VAN CONCEPT _____ **25**

4.1. Infrastructuuroverzicht _____ 25

4.2. Infrastructuur in Azure _____ 27

4.2.1. VNets en subnetten _____ 27

4.2.2. FortiGate-clusterconfiguratie _____ 28

4.2.3. Loadbalancer _____ 28

4.2.4. Azure VPN Gateway en VPN-connectiviteit _____ 29

4.2.5. Routing en peering _____ 29

4.3. Infrastructuur in OCI _____ 30

4.3.1. VCN's, subnetten en FortiGate Cluster _____ 31

4.3.2. VPN-connectiviteit en DRG _____ 31

4.3.3. Routing en VCN-peering _____ 31

4.4. Bewijs van implementatie _____ 31

4.4.1. Connectiviteit in Azure _____ 32

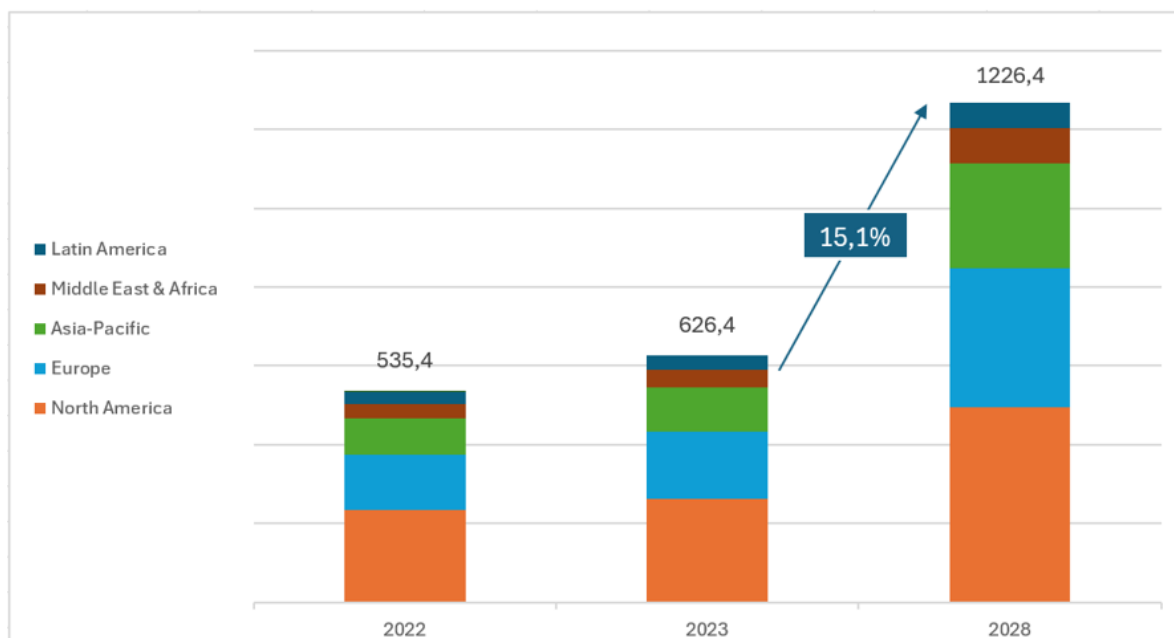
4.4.2. Connectiviteit in Azure met internet _____ 32

4.4.3. Connectiviteit tussen Azure en het datacenter	33
4.4.4. Connectiviteit tussen OCI en Azure	34
4.4.5. Connectiviteit in OCI	35
5. CONCLUSIE	36
REFERENTIELIJST	38
BIJLAGEN	41

Inleiding

Cloud computing onderscheidt zich van eerdere computermodellen doordat het niet alleen het delen van resources mogelijk maakt, maar ook elasticiteit, schaalbaarheid, selfservice provisioning en gecentraliseerd beheer biedt. Deze mogelijkheden stellen organisaties in staat efficiënter te werken, kosten te verlagen en de flexibiliteit te vergroten. In plaats van grote initiële kapitaaluitgaven kunnen bedrijven werken volgens het pay-as-you-go-model, waarbij ze alleen betalen voor wat ze gebruiken. Dit vermindert financiële risico's en biedt meer mogelijkheden voor innovatie en schaalbaarheid, omdat bedrijven de vrijheid hebben om te innoveren zonder beperkingen aan hun infrastructuur (Susnjara & Smalley, 2025). Naast kostenbesparingen verbetert de adoptie van de cloud de samenwerking, omdat medewerkers vrijwel overal toegang hebben tot gegevens en applicaties. Gezien de groeiende behoefte aan flexibiliteit, snelheid en veerkracht in de huidige IT-sector en andere sectoren, is de cloud een fundamenteel element geworden in de strategieën van organisaties. In het huidige bedrijfslandschap is de vraag niet langer of er naar de cloud moet worden overgestapt, maar wat er moet worden verplaatst en hoe dit het beste kan worden gedaan (Google Cloud, sa).

Figuur 1 illustreert de geschatte groei van de wereldwijde markt voor cloudcomputing, met een verwachte groei van \$ 626,4 miljard in 2023 naar \$ 1.266,4 miljard in 2028, wat zou resulteren in een samengestelde jaarlijkse groei (CAGR) van 15,1%. Deze groei wordt gedreven door de toenemende acceptatie door bedrijven, omdat ze hun kosten willen verlagen en tegelijkertijd de algehele efficiëntie willen verhogen en een concurrentievoordeel willen behalen. Daarnaast beïnvloeden macro-economische factoren zoals verstoringen in de toeleveringsketen en evoluerende regelgeving op het gebied van gegevensbescherming investeringsstrategieën, waardoor de wereldwijde acceptatie van cloud computing verder wordt versneld (Brophy, 2025).



Figuur 1 Verwachte CAGR van de wereldwijde cloud computing-markt

Opmerking. Bewerkt naar "Cloud Computing Market", door MarketsandMarkets, 2023, MarketsandMarkets. <https://www.marketsandmarkets.com/Market-Reports/cloud-computing-market-234.html>

Multicloud is een cloudcomputingstrategie die verschillende potentiële voordelen kan bieden. In deze zogenaamde multicloudstrategie kunnen organisaties in hun behoeften voorzien door diensten van verschillende cloudproviders te combineren. De strategie wil zich baseren op het optimaliseren van de prestaties op workloads, het vergroten van de flexibiliteit en het beperken van het risico van afhankelijkheid van één leverancier. Het gebruik van een multicloudomgeving moet echter een weloverwogen keuze zijn. Naast de vele voordelen die deze strategie biedt, kan een multicloudomgeving ook nadelen hebben.

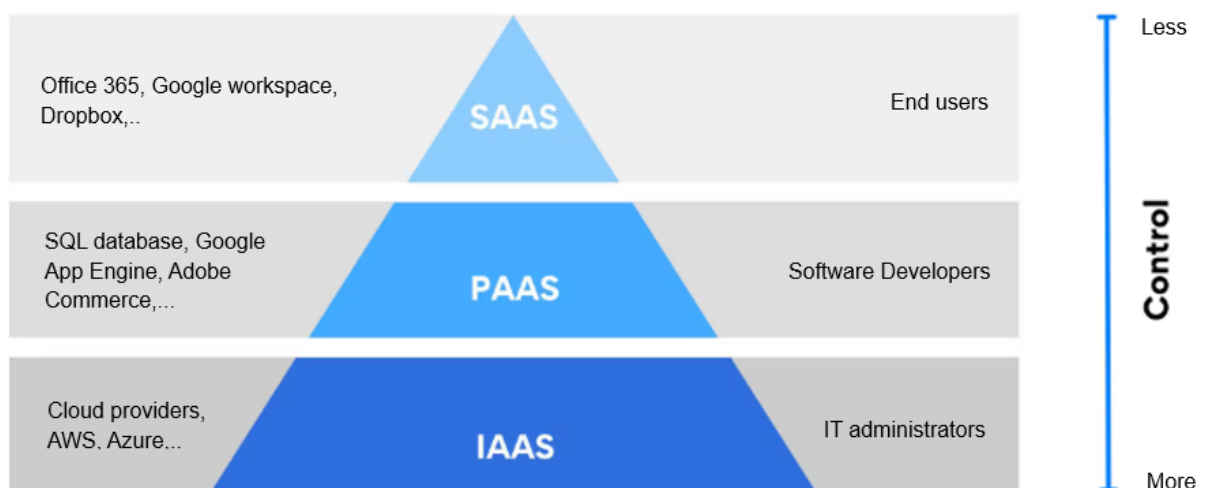
Dit proefschrift onderzoekt hoe een multicloudomgeving kan worden geïmplementeerd en onder welke omstandigheden een dergelijke aanpak gerechtvaardigd is. Het onderzoek onderzoekt en vergelijkt de belangrijkste diensten die worden aangeboden door toonaangevende cloudproviders, met name Amazon Web Services (AWS), Microsoft Azure en Oracle Cloud Infrastructure (OCI). Daarnaast ligt de focus op het identificeren welke van deze diensten essentieel zijn voor de implementatie van een multicloudarchitectuur. Elke cloudprovider wordt ook individueel beoordeeld om zijn specifieke sterke punten te benadrukken. Naast de theoretische analyse wordt een proof of concept (PoC) ontwikkeld, waarbij de nadruk ligt op de interconnectiviteit tussen de verschillende cloudplatformen. Hoewel AWS deel uitmaakt van het technische onderzoek, is het vanwege technische en tijdsbeperkingen niet opgenomen in de PoC. De cloudomgevingen in de PoC zullen hun eigen hub-and-spokesarchitectuur hebben. Daarnaast omvat de opstelling firewallclusters, private en publieke connectiviteit en site-to-site VPN-connectiviteit. Dit onderzoek beoogt bij te dragen aan de interne kennisbasis van Cegeka door verschillende cloudproviders te vergelijken, multicloud use cases te verkennen en de technische componenten te identificeren die nodig zijn voor dergelijke omgevingen.

1. Cloudomgevingen

Voordat we ingaan op specifieke cloudproviders of multicloudomgevingen, is het belangrijk om de bouwstenen van cloudcomputing te begrijpen. Twee essentiële concepten worden gebruikt wanneer een organisatie de cloud benadert: de manier waarop omgevingen worden geïmplementeerd (implementatiemodellen genoemd) en het niveau van de services die in de cloud worden aangeboden (servicemodellen genoemd). Samen definiëren deze termen hoe cloudinfrastructuur wordt gestructureerd en beheerd.

Afhankelijk van de vereiste mate van controle, beveiliging en flexibiliteit kunnen organisaties kiezen uit verschillende implementatiemodellen. Over het algemeen worden deze onderverdeeld in drie modellen. Ten eerste is er de publieke cloud, waar IT-bronnen zoals rekenkracht en opslag worden geleverd door externe leveranciers zoals AWS, Azure of OCI. De services zijn toegankelijk via internet, waarbij meerdere klanten dezelfde onderliggende infrastructuur delen in geïsoleerde omgevingen. Daartegenover staat de private cloud, waar een omgeving is toegewezen aan één organisatie. Deze kan on-premises of door een externe leverancier worden gehost en biedt meer controle over netwerken, beveiliging en compliance, wat vaak belangrijk is voor bedrijven die met gevoelige gegevens werken. Tussen de voorgaande modellen bevindt zich de hybride cloud, die publieke en private omgevingen combineert. Deze maakt het mogelijk om workloads tussen beide te verplaatsen, wat meer flexibiliteit en schaalbaarheid biedt (Microsoft, 2025).

Naast implementatiemodellen wordt cloudcomputing gedefinieerd door de bijbehorende servicemodellen: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) en Software as a Service (SaaS). Zoals weergegeven in Figuur 2, biedt IaaS infrastructuur zoals servers en opslag, waarbij de klant verantwoordelijk blijft voor de besturingssystemen, applicaties en data die erop draaien. PaaS biedt vaak een beheerde omgeving waarin ontwikkelaars applicaties kunnen bouwen en implementeren zonder dat ze de onderliggende infrastructuur hoeven te beheren. SaaS levert daarentegen volledig beheerde applicaties, zoals Microsoft 365 of Google Workspace, waarbij de provider alles afhandelt, van hosting tot updates en beveiliging (IBM, 2021).

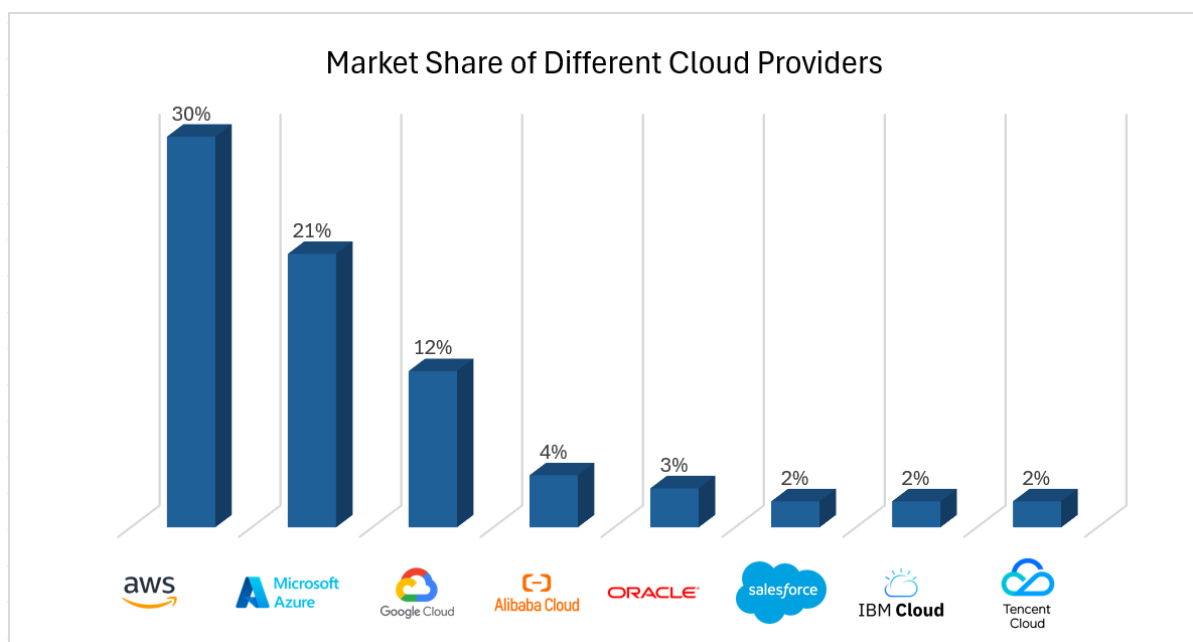


Figuur 2 Cloud Service Modellen: SaaS, PaaS, IaaS vergeleken

Opmerking. Geïnspireerd op "IaaS vs PaaS vs SaaS: Explaining the Key Differences", door A. Dua, 2024, Turing. <https://www.turing.com/blog/iaas-vs-paas-vs-saas-key-differences>

1.1. Geschiedenis en marktaandeel van cloudproviders

AWS werd opgericht in 2006, toen Amazon ontdekte dat het lastig was, en nog steeds is, om IT-infrastructuur te provisionen en te beheren, wat hun getalenteerde teams afleidde van daadwerkelijk innoveren. Amazon wilde de IT-infrastructuur volledig heroverwegen, zodat iedereen toegang zou hebben tot dezelfde kracht van cloud computing als 's werelds grootste bedrijven. Het begon met fundamentele diensten zoals Amazon Simple Storage Service (S3 Buckets), waarmee individuen en organisaties hun gegevens op een kosteneffectieve manier konden opslaan en beheren. Ze boden ook de Elastic Computing Instance (EC2) aan, schaalbare virtuele servers in de cloud, waarmee gebruikers applicaties konden draaien door instances te starten met het gekozen besturingssysteem (OS), CPU, geheugen, opslag en netwerkcapaciteit. AWS won snel aan populariteit vanwege hun schaalbaarheid en pay-per-use prijsmodellen en groeide uit tot een wereldwijd toonaangevend cloudplatform. Tegenwoordig heeft AWS naar schatting een marktaandeel van 30%, zoals weergegeven in Figuur 3, waarmee het de grootste aanbieder is in de wereldwijde cloud computing-industrie (AWS, 2025).



Figuur 3 Marktaandeel van verschillende cloudproviders

Opmerking. Geactualiseerd naar "Cloud Infrastructure Market: Amazon en Microsoft blijven koploper in de wereldwijde cloudmarkt", door F. Richter, 2025, Statista. <https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/>

Na het vroege succes van AWS begonnen andere technologiegiganten hun eigen cloudplatformen te bouwen. Microsoft lanceerde Azure in 2010 en betrad de markt met een sterke focus op zakelijke klanten. Dankzij de soepele integratie met bestaande Microsoft-producten, zoals Active Directory, Office 365 en Windows Server, werd Azure al snel een logische keuze voor organisaties die al in het Microsoft-ecosysteem zaten. De ondersteuning voor hybride cloudomgevingen maakte het vooral aantrekkelijk voor bedrijven die de overstap maakten van traditionele on-premises infrastructuur naar cloudomgevingen. Hierdoor veroverde Azure de op één na grootste positie in de cloudmarkt, met een geschat marktaandeel van 21% eind 2024 (Abandy, 2022).

Ondertussen volgde OCI een meer gespecialiseerd traject. OCI, dat enkele jaren later, in 2016, werd gelanceerd, had niet de ambitie om direct te concurreren met AWS of Azure qua servicebreedte. Oracle richtte zich in plaats daarvan op prestaties, kostenefficiëntie en een veilige infrastructuur, en positioneerde zichzelf als hét platform voor high-performance workloads en grootschalige bedrijfsdatabases, met name Oracles eigen databaseproducten. OCI is vooral aantrekkelijk in sectoren waar prestaties per core, voorspelbare prijzen of optimalisatie van databaselicenties cruciaal zijn. Hoewel het wereldwijde marktaandeel bescheiden blijft, geschat op 3%, heeft OCI terrein gewonnen door strategische partnerschappen, zoals de directe verbinding met Azure, en wordt het steeds vaker overwogen in multicloudstrategieën voor specifieke, veeleisende workloads (Gartner et al., 2024).

Zoals in dit hoofdstuk wordt aangetoond, heeft elke cloudprovider een eigen weg bewandeld om zijn huidige marktpositie te bereiken. AWS loopt voorop met een voorsprong als pionier en een uitgebreid dienstenportfolio, Azure profiteert van zijn sterke enterprise-integratie en OCI legt de nadruk op prestatie- en kostenoptimalisatie. Marktaanwezigheid alleen bepaalt echter niet welke provider het meest geschikt is voor specifieke use cases. In het volgende hoofdstuk wordt een diepgaandere vergelijking gemaakt tussen de providers, wat betere inzichten oplevert die de basis vormen voor de multicloud PoC die later in dit proefschrift wordt besproken.

1.2. Definitie van een multicloudomgeving

Een multicloudomgeving verwijst naar het gebruik van cloudservices van twee of meer verschillende cloudproviders binnen één organisatie. In plaats van afhankelijk te zijn van één leverancier voor alle infrastructuur-, database- of softwareservices, kunnen organisaties meerdere cloudplatforms, zoals AWS, Azure en OCI, parallel implementeren. Deze aanpak kan grote voordelen bieden, die worden uitgelegd in hoofdstuk 3, Multicloudstrategieën. Multicloudomgevingen kunnen verschillende vormen aannemen, afhankelijk van de behoeften van de organisatie, hoe de cloudplatforms worden gebruikt en of ze met elkaar verbonden zijn (Chen, 2025).

Eén optie is een geïsoleerde multicloudomgeving, waarbij elk cloudplatform wordt gebruikt voor specifieke workloads, maar de omgevingen technisch niet met elkaar verbonden zijn. Een organisatie kan bijvoorbeeld Azure gebruiken voor haar Microsoft-applicaties en OCI voor het hosten van Oracle-databases. In dit geval werken de platforms onafhankelijk van elkaar en worden er geen gegevens of services tussen hen uitgewisseld (Bell, 2019).

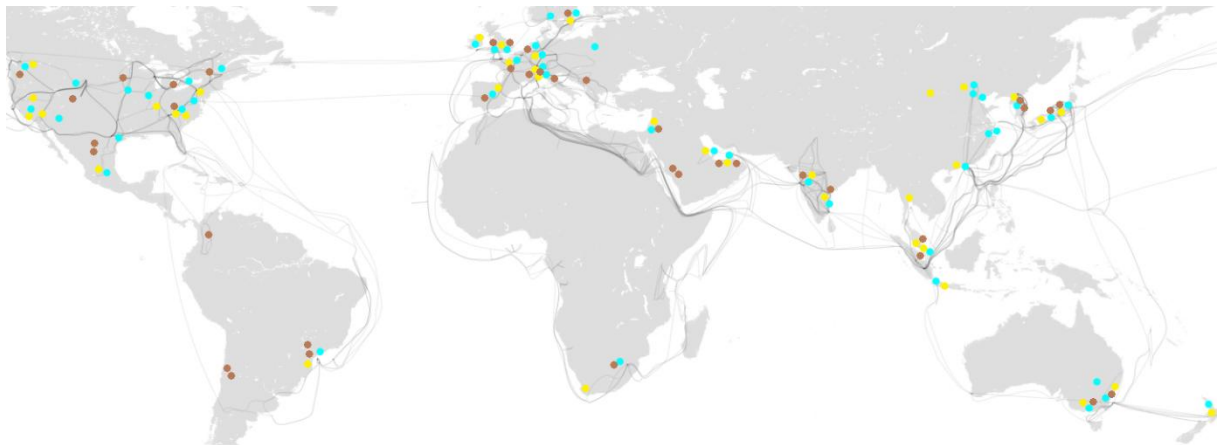
Multicloudomgevingen kunnen ook gebruikmaken van een geïntegreerde multicloudarchitectuur, waarbij meerdere cloudomgevingen technisch met elkaar verbonden zijn, meestal via VPN-tunnels. Dit maakt veilige communicatie en gegevensuitwisseling tussen de omgevingen mogelijk. Deze vorm van multicloud maakt het mogelijk om workloads of andere services over meerdere omgevingen te verdelen. In de praktijk betekent dit dat meerdere servicemodellen, zoals IaaS of PaaS, naast elkaar in dezelfde omgeving kunnen bestaan. Hoewel dit toegevoegde waarde kan bieden, introduceert het ook complexiteit (F5, sa).

2. Verschillende cloudproviders

In een single-cloudscenario is het relatief eenvoudig om de terminologie van een provider te begrijpen. In multicloud-opstellingen, zoals die in dit proefschrift, is het echter essentieel om te begrijpen hoe vergelijkbare concepten verschillend worden geïmplementeerd. De fundamentele elementen worden in de volgende paragrafen verder onderzocht, waarbij elke cloudprovider gedetailleerder wordt geanalyseerd op basis van hun unieke kenmerken en hoe ze zijn toegepast in de PoC die voor dit proefschrift is ontwikkeld.

2.1. Wereldwijde infrastructuur en terminologie

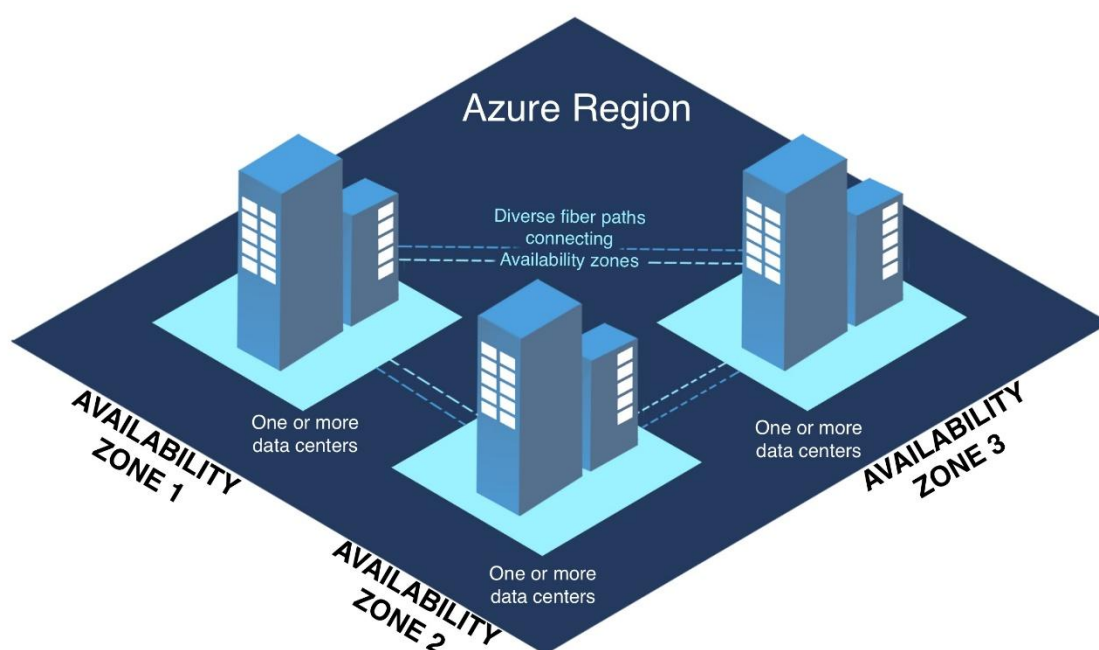
In het snel evoluerende landschap van cloudcomputing is een handvol cloudproviders uitgegroeid tot wereldleiders in de miljardenindustrie. In dit proefschrift gaan we dieper in op drie van hen: Amazon Web Services, Microsoft Azure en Oracle Cloud Infrastructure. Omdat de providers ernaar streven het grootste marktaandeel te verwerven, moeten ze concurrerend zijn. Daarom biedt elk platform een breed scala aan diensten aan, verspreid over infrastructuur-, platform- en softwarelagen. Hoewel alle drie hetzelfde fundamentele doel dienen, namelijk het leveren van schaalbare en on-demand computing resources, verschillen ze in focus, marktpositionering en ecosysteemintegratie. Om hun aanwezigheid in de markt te versterken en toegang tot diensten met lage latentie te garanderen, investeren cloudproviders fors in het uitbreiden van hun geografische aanwezigheid. Figuur 4 illustreert de aanwezigheid van regio's wereldwijd, van AWS (geel), Azure (blauw) en OCI (bruin). Belangrijk om op te merken is dat dit alleen de regio's aangeeft, en niet de datacenters daarbinnen, aangezien de ene provider meerdere datacenters in één regio kan hebben, terwijl een andere er slechts één heeft.



Figuur 4 Aanwezigheid van regio's over de hele wereld: AWS, Azure en OCI

Opmerking. Geïnspireerd op "Microsoft Datacenters", door Microsoft, 2025, Microsoft. <https://datacenters.microsoft.com/globe/explore?view=map>; en "AWS Global Infrastructure", door AWS, 2025, AWS Amazon. <https://aws.amazon.com/about-aws/global-infrastructure/>; en "Public Cloud Regions", door Oracle, 2025, Oracle. <https://www.oracle.com/be/cloud/public-cloud-regions/>

Hoewel elke cloudprovider zijn eigen terminologie en interne structuur gebruikt, is de basisarchitectuur grotendeels hetzelfde. Ondanks de naamgevingsverschillen blijft het kernconcept hetzelfde: cloudinfrastructuur is wereldwijd gedistribueerd en logisch gesegmenteerd om schaalbaarheid, fouttolerantie en lage latentie te bieden. Ter illustratie van deze structuur laat Figuur 5 zien hoe Azure een regio organiseert. Elke Azure-regio bestaat uit ten minste één, maar vaak meerdere beschikbaarheidszones. Een beschikbaarheidszone in Azure vertegenwoordigt een geografische locatie waar een of meer datacenters zich kunnen bevinden, elk met eigen stroomvoorziening, koeling en netwerk. De datacenters zijn met elkaar verbonden via snelle glasvezelnetwerken. Hoewel de exacte implementatie kan verschillen, bieden alle cloudproviders de mogelijkheid om kritieke services over meerdere regio's of zones te implementeren, waardoor continuïteit wordt gegarandeerd, zelfs als één zone uitvalt (Microsoft Learn, 2025).



Figuur 5 Cloudregioarchitectuur met redundantie

Opmerking. Bewerkt naar "Wat zijn Azure-regio's?", door Microsoft Learn, 2025, Microsoft. <https://learn.microsoft.com/en-us/azure/reliability/regions-overview>

Hoewel Figuur 5 visualiseert hoe Azure zijn regio's en beschikbaarheidszones structureert, is het belangrijk om te begrijpen dat dezelfde architectuurprincipes gelden voor alle cloudproviders, alleen de naamgeving is anders. Zo organiseert AWS zijn infrastructuur ook in regio's en beschikbaarheidszones, met vrijwel identieke definities. Elke AWS-regio bevat meerdere beschikbaarheidszones; dit zijn geïsoleerde datacenters met onafhankelijke stroomvoorziening, koeling en netwerken, die met elkaar verbonden zijn via verbindingen met lage latentie (AWS, 2025).

OCI structureert zijn regio's daarentegen met behulp van beschikbaarheidsdomeinen in plaats van beschikbaarheidszones. Elk beschikbaarheidsdomein bestaat doorgaans uit één datacenter, in tegenstelling tot de zones van Azure of AWS, die vaak meerdere datacenters beslaan. De beschikbaarheidsdomeinen van OCI bieden nog steeds foutisolatie en redundantie, maar de fysieke scheiding is meestal minder uitgebreid dan bij concurrenten. Dit ontwerp maakt echter verbindingen met extreem lage latentie en hoge bandbreedte mogelijk tussen beschikbaarheidsdomeinen in dezelfde regio, wat gunstig is voor workloads met hoge prestaties en veel databases (Oracle, 2025).

2.2. Services

Cloudproviders kunnen sterk verschillen in branding, ecosysteemontwerp en platformervaring, maar in essentie bieden ze vergelijkbare servicecategorieën die zijn ontworpen om aan dezelfde basisbehoeften te voldoen. Of het nu gaat om de implementatie van virtuele machines, dataopslag, identiteitsbeheer of databases, AWS, Azure en OCI bieden allemaal een vergelijkbaar scala aan services die de fundamentele onderdelen van de verschillende cloudcomputingmodellen bestrijken.

Hoewel de namen, interfaces en sommige implementatiedetails verschillen, blijft de kernfunctionaliteit consistent. Dit stelt organisaties in staat om cloudarchitecturen te ontwerpen op basis van servicetype, in plaats van providerspecifieke functies, op basisniveau. Pas wanneer men zich verdiept in gespecialiseerde aanbiedingen, prijsmodellen, prestatie-optimalisaties en ecosysteemintegraties, beginnen er betekenisvolle verschillen te ontstaan. Deze verschillen worden in het volgende hoofdstuk uitgelegd. (Oracle, 2024).

Tabel 1 biedt een overzicht van de belangrijkste cloudservicecategorieën en de bijbehorende naamgeving die door elke provider wordt gebruikt.

Tabel 1Belangrijkste cloudservices per provider

Functioneel gebied	AWS	Azuurblauw	OCI
Berekenen	EC2	Virtuele machines	Compute-instanties
Objectopslag	S3	Blob-opslag	Objectopslag
Relationele database	RDS	Azure SQL-database	Autonome database
Containerdiensten	ECS/EKS	Azure Kubernetes-service	OCI Kubernetes-service
Identiteit en toegang	IK BEN	Microsoft Entra-ID	IK BEN

2.3. Sterke punten en gespecialiseerde services

Hoewel de kernfunctionaliteiten van AWS, Azure en OCI vaak op meerdere vlakken overlappen, biedt elke provider ook gespecialiseerde services die hen onderscheiden in de markt. Deze unieke sterke punten kunnen een doorslaggevende factor zijn in multicloudstrategieën, waarbij organisaties selectief de beste mogelijkheden van elk platform benutten om hun workloads te optimaliseren.

AWS wordt al lang erkend als een pionier op het gebied van serverless computing. Het biedt een breed scala aan diensten in vrijwel elk domein, waaronder computing,

kunstmatige intelligentie (AI), databases, opslag, analytics en meer. Dit maakt AWS een perfecte keuze voor startups, maar ook voor grote organisaties zoals productgerichte bedrijven die snel en kostenefficiënt software willen bouwen en schalen. Vanuit technisch oogpunt wordt AWS algemeen erkend als een pionier op het gebied van serverless computing, met AWS Lambda dat zeer schaalbare, event-driven architecturen mogelijk maakt (Barr, 2024). De prijsflexibiliteit en het wereldwijde bereik van AWS kunnen het een goede keuze maken voor organisaties die waarde hechten aan kostenbeheersing en een breed scala aan functies (AWS, 2025).

Azure is sterk gepositioneerd als de natuurlijke keuze voor bedrijven die al ingebed zijn in het Microsoft-ecosysteem. De integratie met Active Directory, Office 365 en Windows Server stelt organisaties in staat hun bestaande infrastructuur met minimale verstoringen uit te breiden naar de cloud. Microsoft presteert ook goed in hybride cloudscenario's, met services zoals Azure Arc die het mogelijk maken om on-premises en multicloudomgevingen te beheren als één uniform platform. Dit maakt Azure vooral aantrekkelijk voor bestaande organisaties die al een grote omgeving in het Microsoft-ecosysteem hebben draaien en hun infrastructuur naar de cloud willen verplaatsen (Krishnakumar, 2025).

OCI richt zich op een specifiek segment van de cloudmarkt: grote ondernemingen met veeleisende backoffice- en dataworkloads, met name bedrijven die al Oracle-software gebruiken. De kracht van OCI ligt in prestatiegeoptimaliseerde, kostenefficiënte infrastructuur, die een uitstekende oplossing kan zijn voor kritieke applicaties zoals ERP, financiële systemen en database-intensieve systemen of applicaties. OCI onderscheidt zich ook door zijn mogelijkheden in bare-metal infrastructuur, vaak tegen lagere kosten dan traditionele hyperscalers. Dit maakt OCI met name aantrekkelijk voor organisaties die op zoek zijn naar voorspelbare prestaties voor interne workloads met beperkte licentievereisten (Oracle, 2024).

2.4. Identiteits- en toegangsbeheer (IAM)

IAM is een cruciale pijler bij het beveiligen van elk cloudplatform. Het definieert hoe gebruikers en systemen zich authenticeren en toegang krijgen tot cloudresources, en hoe deze rechten worden gehandhaafd. Hoewel AWS, Azure en OCI allemaal IAM-oplossingen bieden, verschillen ze aanzienlijk in structuur, terminologie en geïntegreerde opties. Elke cloudprovider dwingt rechten af met behulp van zijn eigen native model, waardoor het praktisch noodzakelijk is om hun platformspecifieke IAM-model te gebruiken om gedetailleerde toegangscontrole te implementeren. Hoewel basisconcepten voor authenticatie en autorisatie consistent zijn, zoals rollen, beleid en groepsgebaseerde toegang, variëren de reikwijdte, structuur en handhavingsmechanismen, met name wanneer het om dynamische rechten gaat (Mishra, 2024).

In multicloudomgevingen wordt dit complexer. Het beheer van identiteiten tussen providers is niet standaard geïntegreerd en federatie tussen IAM-systemen vereist tools van derden of handmatige configuratie. Het beheren van gebruikersidentiteiten op meerdere locaties is inefficiënt en vergroot de kans op configuratiefouten. De belangrijkste conclusie is dat gedetailleerde en veilige toegangscontrole alleen kan worden bereikt door het native IAM-model van elk cloudplatform te implementeren, wat de operationele complexiteit vergroot wanneer er meer dan één provider bij betrokken is (Mishra, 2024).

2.4.1. IAM in AWS

AWS IAM biedt flexibele toegangscontrole via gebruikers, groepen en rollen. Gedetailleerde machtigingen worden gedefinieerd met behulp van JSON-beleid, maar veilig en schaalbaar gebruik vereist volledige implementatie van de native structuur van AWS. Gefedereerde identiteit wordt ondersteund, maar integratie met niet-AWS-systemen is afhankelijk van aanvullende configuratie en externe tools (AWS, sa).

2.4.2. IAM in Azure

Azure gebruikt Entra ID voor identiteitsbeheer, met sterke hybride mogelijkheden dankzij de integratie met on-premises Active Directory. Toegangscontrole wordt afgedwongen met behulp van roltoewijzingen in meerdere bereiken. Hoewel federatie wordt ondersteund, vereist gedetailleerde toegang het volledige gebruik van Microsoft's Entra-framework en IAM-model (Microsoft Learn, 2025).

2.4.3. IAM in OCI

OCI organiseert identiteiten met behulp van tenancies, compartimenten en groepsbeleid in een leesbare syntaxis. Dynamische groepen maken cloud-native toegangscontrole mogelijk, maar gedetailleerde toegangscontrole is nog steeds afhankelijk van het gebruik van OCI-native tools. Gefedereerde identiteit is mogelijk, maar vereist een handmatige configuratie (Oracle, 2023).

3. Multicloudstrategieën

Zoals eerder vermeld, verwijst een multicloudstrategie naar het gebruik van clouddiensten van meerdere cloudproviders binnen één organisatie, gebaseerd op strategische, technische of operationele overwegingen. Het gaat verder dan het incidentele gebruik van verschillende platformen en vertegenwoordigt een doelbewuste architectuurbenadering. Het concept wordt visueel weergegeven in Figuur 6.



Figuur 6 AWS, Azure en OCI: vanuit een multicloudperspectief

Let op. Afbeelding gemaakt door de auteur.

Wanneer een organisatie overweegt haar infrastructuur of workloads naar de cloud te migreren, is de centrale vraag niet alleen *hóe* ze migreert, maar ook *waarheen* ze migreert. Met de toenemende volwassenheid van meerdere cloudproviders wordt de mogelijkheid van een multicloudstrategie steeds relevanter. Het implementeren van een multicloudstrategie is echter geen standaardaanbeveling. Het moet het resultaat zijn van een weloverwogen en goed onderbouwde beslissing, rekening houdend met de technische behoeften, bedrijfsprioriteiten en operationele capaciteit van de organisatie (Google Cloud, sa).

Voor IT-dienstverleners zoals Cegeka kan de vraag "*Welk cloudplatform is het meest geschikt voor deze klant?*" niet in isolatie worden beantwoord. Deze vraag hangt af van een combinatie van factoren zoals workloadvereisten, datapositionering, licentievoorwaarden, integratiebehoeften en flexibiliteit op lange termijn. Alleen wanneer de voordelen van een multicloudomgeving duidelijk opwegen tegen de nadelen, zoals de extra complexiteit en kosten, is een multicloudarchitectuur een verantwoorde keuze.

3.1. Voordelen en uitdagingen van een multicloudstrategie

Een weloverwogen multicloudstrategie biedt organisaties de mogelijkheid om optimaal te profiteren van de sterke punten van meerdere cloudproviders. Door platformen zoals AWS, Azure en OCI parallel te benutten, krijgen organisaties meer flexibiliteit in de implementatie en het beheer van workloads. Deze toegenomen vrijheid levert meerdere voordelen op.

Een van de belangrijkste voordelen is het voorkomen van vendor lock-in. Door workloads over meerdere platforms te verdelen, zijn organisaties minder afhankelijk van het ecosysteem van één provider, waardoor het risico op contractuele of technische beperkingen wordt verminderd. Bovendien maakt multicloud optimale plaatsing van workloads mogelijk: elk cloudplatform heeft zijn eigen specialisaties. De enterprise-integratie van Azure, het brede serviceportfolio van AWS of de prestatiegerichte reken- en databaseservices van OCI stellen organisaties in staat om workloads af te stemmen op de meest geschikte infrastructuur. Een ander belangrijk voordeel is de verhoogde veerkracht. De mogelijkheid om services in verschillende cloudomgevingen uit te voeren, kan de beschikbaarheid en fouttolerantie aanzienlijk verbeteren. Bij uitval van een provider of servicevermindering kunnen workloads overgaan naar een andere provider. De geografische diversificatie kan organisaties ook helpen bij het voldoen aan compliance- en dataprivacyvereisten, zoals de AVG in Europa. Kostenoptimalisatie is een ander belangrijk voordeel. Door prijsmodellen te vergelijken, wat later in dit proefschrift aan bod komt, kunnen organisaties hun kosten effectiever beheersen en voorkomen dat ze onnodig vastzitten aan premium services. Bovendien wordt innovatie versneld door multicloudstrategieën, omdat organisaties toegang krijgen tot een breder scala aan diensten, variërend van machine learning en analyses tot gespecialiseerde opslagaanbiedingen, zonder te hoeven wachten tot één enkele provider hen inhaalt (Teske, 2024).

Ondanks deze vele voordelen brengt de implementatie van een multicloudstrategie verschillende uitdagingen met zich mee. Vanuit technisch perspectief kan het beheer van identiteits-, netwerk-, routerings- en beveiligingsbeleid over meerdere platformen complex zijn. Elke provider gebruikt zijn eigen standaarden, tools en terminologie, wat een uniform gebruik bemoeilijkt. Zonder zorgvuldige planning kan dit leiden tot inefficiëntie, beveiligingslekken en onvoorziene kosten. Zichtbaarheid is ook een veelvoorkomend probleem: monitoring en logging moeten vaak worden gecombineerd met behulp van oplossingen van derden, omdat native tools doorgaans niet over een goede integratie tussen providers beschikken. Dit verhoogt de overhead die gepaard gaat met consistente zichtbaarheid, kostenregistratie en incidentrespons. Bovendien vereist het onderhouden van expertise over meerdere platformen veel bredere vaardigheden binnen IT-teams, wat mogelijk leidt tot hogere trainingskosten. Beveiliging en compliancemanagement worden ook genuanceerder. Het waarborgen van een consistent beveiligingsbeleid over meerdere providers vereist extra aandacht, met name bij toegangscontrole, meerdere firewalls in verschillende cloudomgevingen, encryptiebeleid en auditing. Op dezelfde manier kan de implementatie van Infrastructure-as-Code (IaC), waarbij organisaties cloudomgevingen kunnen opzetten die geautomatiseerd zijn met code, een grotere uitdaging vormen, omdat verschillende platforms specifieke sjablonen en workflows kunnen vereisen (Sasovets & Teres, 2025).

3.2. Gerechtvaardigde gebruiksgevallen

Zoals eerder vermeld, hangt de beslissing om een multicloudstrategie te implementeren af van diverse factoren. Niet elk scenario is gebaat bij een multicloudaanpak en het mag nooit als standaard worden beschouwd. In deze sectie wordt een selectie van representatieve use cases gegeven om te illustreren wanneer een multicloudstrategie toepasbaar is. Deze voorbeelden belichten praktische overwegingen en dienen om de strategische waarde van multicloudstrategieën te demonstreren, die verder gaat dan de technische implementaties.

De besproken use cases bestrijken niet elk mogelijk scenario, maar zijn bedoeld om een relevante set te bieden die aansluit bij de doelstellingen van dit proefschrift. Ze vormen de conceptuele basis voor de PoC die in dit proefschrift is ontworpen en helpen bij het beantwoorden van de vraag wanneer een multicloudstrategie gerechtvaardigd is.

3.2.1. Gebruiksscenario 1: Specialisatie van werklasten over providers heen

Een van de meest voorkomende strategische rechtvaardigingen voor multicloud is functionele specialisatie. Zoals in voorgaande hoofdstukken vermeld, biedt elke cloudprovider unieke services of kostenvoordelen. Zo zijn de databaseservices van Oracle performanter en licentie-efficiënter in OCI, terwijl Azure uitblinkt in applicatiehosting en bedrijfsintegratie met services zoals Microsoft Entra ID. In dergelijke gevallen kan het verdelen van workloads over OCI en Azure leiden tot hogere prestaties en lagere kosten, mits de connectiviteit tussen de platforms beveiligd en bewaakt is. De PoC in dit proefschrift toont aan dat dergelijke communicatie tussen cloudomgevingen technisch haalbaar is met behulp van versleutelde VPN-tunnels en gecentraliseerde inspectie via firewalls, hoewel een dergelijke configuratie ook kan plaatsvinden in een niet-technisch geïntegreerde multicloud (Chen, 2025).

3.2.2. Gebruiksscenario 2: Bedrijfsfusies en klantbeperkingen

In de context van fusies, overnames of IT-standaardisatie kan multicloud een noodzaak zijn. Verschillende bedrijfseenheden hebben mogelijk al fors geïnvesteerd in verschillende cloudplatforms. In plaats van een kostbare en tijdrovende migratie van het ene platform naar het andere te forceren, kunnen organisaties profiteren van een multicloudstrategie door hun omgevingen met elkaar te verbinden en gefaseerde overgangen of cross-cloudcommunicatie mogelijk te maken. Een van de gefuseerde bedrijven kan Azure nodig hebben om redenen van soevereiniteit, terwijl de andere een Oracle-gebaseerde infrastructuur vereist. In dergelijke gevallen profiteren serviceproviders van het aanbieden van multicloudondersteuning om compliant en concurrerend te blijven (Chen, 2025).

3.2.3. Gebruiksscenario 3: Klant- of nalevingsgestuurde platformscheiding

In sommige gevallen dicteren de eisen van klanten het gebruik van specifieke cloudproviders. Een IT-serviceprovider kan bijvoorbeeld een overheidsinstantie bedienen die het gebruik van Azure verplicht stelt vanwege dataresidentie en compliance-normen, terwijl andere klanten de voorkeur geven aan AWS vanwege de flexibiliteit en kosten. De serviceprovider kan beide ondersteunen door applicaties en services te implementeren in de beoogde clouds, zonder ze op infrastructuurniveau te verbinden. Deze configuratie ondersteunt een multi-tenantarchitectuur over meerdere clouds, terwijl omgevingen geïsoleerd blijven om beveiligings-, juridische of contractuele redenen. Toch kwalificeert het nog steeds als een multicloudstrategie vanwege de opzettelijke providersplitsing en het gecoördineerde beheer (Appvia, 2024).

3.3. Wanneer multicloud niet gerechtvaardigd is

Hoewel multicloudstrategieën flexibiliteit en veerkracht kunnen bieden, brengen ze ook architectonische en operationele overhead met zich mee. Er zijn talloze situaties waarin multicloud niet wordt aanbevolen, omdat de risico's groter zijn dan de voordelen, of omdat eenvoudigere alternatieven geschikter zijn. Kleine tot middelgrote organisaties

missen vaak de interne kennis en expertise om meerdere cloudomgevingen goed te beheren en te beveiligen. Elk platform heeft zijn eigen tools, services, configuraties en best practices. Het beheer hiervan vereist gespecialiseerd personeel en constante training. Dus als de workloads van een organisatie efficiënt in één cloud kunnen worden gehost zonder prestatie-, compliance- of servicebeperkingen, dan voegt de introductie van een tweede provider onnodige complexiteit toe.

3.4. Kostenoverwegingen

Hoewel de technische haalbaarheid en strategische doelen van een multicloudarchitectuur duidelijk mogen zijn, blijven kosten een van de meest doorslaggevende factoren bij het bepalen of een dergelijke strategie gerechtvaardigd is of niet. De implementatie van de strategie is niet alleen een technische keuze, maar een fundamentele zakelijke beslissing. Om te illustreren hoe kosten een cloudstrategie kunnen beïnvloeden, presenteert deze sectie een vergelijking tussen een multicloud-implementatie en een single cloud-implementatie. Het scenario is gebaseerd op de praktische context die in dit proefschrift wordt onderzocht, maar het is belangrijk om op te merken dat dit slechts één van de talloze mogelijke configuraties vertegenwoordigt. Cloudprijzen zijn zeer variabel en contextafhankelijk. Factoren die de prijs beïnvloeden, zijn workloadtypen, verkeerspatronen, de selectie van serviceniveaus, het gekozen ondersteuningsniveau en, niet te vergeten, de onderhandelde bedrijfsovereenkomsten. De onderstaande analyse is er niet op gericht om prijsscenario's te generaliseren, maar eerder om het belang te benadrukken van het opnemen van kosten als een belangrijk beslissingscriterium bij elke multicloud-evaluatie (Tata Communications, 2025).

De volgende kostenvergelijkingen zijn gebaseerd op theoretische configuraties met behulp van de officiële prijscalculators van AWS, Azure en OCI. De PoC die voor dit proefschrift is ontwikkeld, betrof de implementatie van virtuele machines puur om de vraag *"Wat is technisch gezien nodig om een multicloudomgeving te implementeren?" te beantwoorden* en om aan te tonen dat interconnectiviteit mogelijk is. Daarom moeten de kostenramingen worden geïnterpreteerd als indicatief en niet als daadwerkelijke gegevens uit een operationele omgeving. De vergelijking is gebaseerd op een vereenvoudigde SaaS-applicatie waarmee eindgebruikers gegevens kunnen indienen via een webinterface en gepersonaliseerde analyses kunnen bekijken in een dashboard. De applicatie omvat een statische frontend, een serverloze backend voor het verwerken van gebruikersinvoer, permanente opslag en een rapportagelaag.

3.4.1. Scenario 1: Multicloud-implementatie

Tabel 2 geeft een gedetailleerd overzicht van de gebruikte cloudcomponenten per provider, samen met hun geschatte maandelijkse kosten (zie Bijlage 4 bij Bijlage 6). De multicloud-opstelling verdeelt services over Azure, AWS en OCI om de specifieke sterke punten van elke provider te benutten. Een webfrontend wordt gehost in AWS met behulp van S3, wat zorgt voor de levering van statische content. Backendlogica wordt uitgevoerd met behulp van AWS Lambda en de API-gateway en verwerkt gebruikersinvoer. Permanente gegevens worden opgeslagen in de autonome database van OCI, die geoptimaliseerd is voor transactionele workloads. Analytische dashboards worden aangeboden via Azure's Power BI embedded, wat zorgt voor een consistente rapportage-ervaring. De verbinding tussen de omgevingen verloopt via site-to-site VPN's en er wordt rekening gehouden met het bandbreedtegebruik.

Tabel 2 Multicloud-kostenoverzicht per component per provider

Onderdeel	Wolk	Dienst	Maandelijke kosten (USD)
Frontend	AWS	S3	\$1,28
Backend/API	AWS	Lambda + API-gateway	\$32,30
VPN + Uitgang	AWS	VPN	\$165,16
Databank	OCI	Autonome DB	\$118,41
Opslag	OCI	Objectopslag	\$1,25
Dashboard	Azuurblauw	Power BI ingebed	\$353,43
VPN-gateway	Azuurblauw	VPN-gateway	\$138,70
Internet-uitgang	Azuurblauw	Bandbreedte	\$72,00
Blob-opslag	Azuurblauw	Klodder	\$5,88
Totale maandelijke kosten			\$888,41

3.4.2. Scenario 2: Implementatie in één cloud

In de analyse van de single-cloud-implementatie wordt een vergelijking gemaakt tussen Azure, AWS en OCI. Om de prijsverschillen tussen de verschillende clouds in dit scenario beter te begrijpen, is dezelfde SaaS-oplossing door alle cloudproviders geprijsd met behulp van de officiële prijscalculators, die te zien zijn in Bijlage 1 bij Bijlage 3.

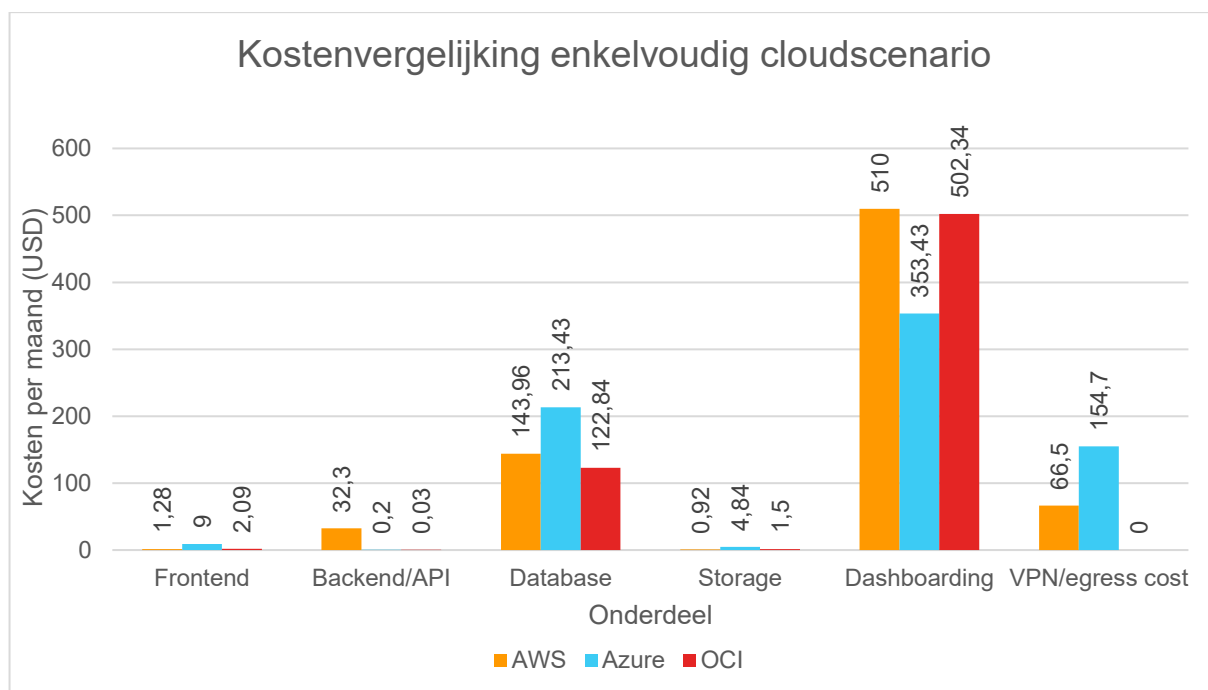
Elk platform werd waar mogelijk geconfigureerd met behulp van gelijkwaardige services. Zo werd AWS Lambda vergeleken met Azure Functions en Oracle Functions, terwijl opslag- en databaseopties werden geselecteerd op basis van standaardconfiguraties en, waar mogelijk, met de 'bring your own'-licentieprijzen.

Figuur 7 Hieronder worden de kosten per component per provider weergegeven voor het gebruik van de oplossing binnen één omgeving. Dergelijke vergelijkingen moeten altijd binnen een bedrijf worden gemaakt bij het selecteren van een cloudprovider, hoewel ze zich mogelijk niet alleen richten op de prijsstelling van services, zoals uitgelegd in hoofdstuk 3.4.3, Kosteninterpretatie en bredere overwegingen.

Sommige services, zoals VPN/uitgaand verkeer, dashboard en database, vertonen sterke verschillen. Deze verschillen worden voornamelijk veroorzaakt door de manier waarop elke provider zijn prijsmodel structureert en de specifieke services die worden gebruikt om dezelfde functies te vervullen. Azure hanteert bijvoorbeeld een prijs voor de VPN-gatewaycomponent, maar er wordt een vast bedrag betaald voor 0 tot 10 site-to-site VPN-tunnels. AWS daarentegen rekent kosten per site-to-site-verbinding. OCI richt zich sterk op kostenoptimalisatie en brengt geen kosten in rekening voor de eerste 10 TB uitgaande data.

De vergelijking illustreert dat, zelfs wanneer ze functioneel vrijwel identiek zijn, de maandelijke kosten van dezelfde cloud-native applicaties sterk kunnen variëren, afhankelijk van de gebruikte provider. Het is echter belangrijk om te onthouden dat deze

waarden theoretisch zijn en uitsluitend gebaseerd op openbare prijscalculators, en dat er geen factureringsgegevens van actief gebruik zijn gebruikt.

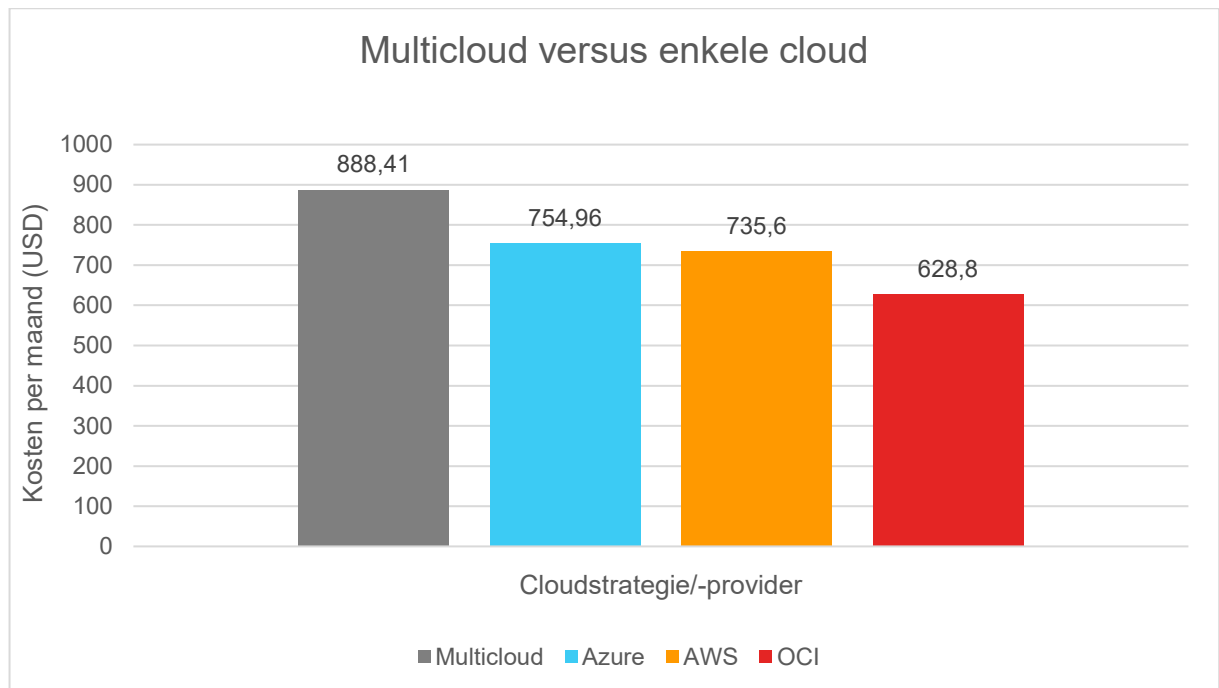


Figuur 7 Kostenvergelijking van componenten in een enkele cloudopstelling

3.4.3. Kosteninterpretatie en bredere overwegingen

Deze sectie gaat verder dan een simpele prijsvergelijking en belicht de onderliggende variabelen waarmee rekening moet worden gehouden bij de evaluatie van multicloud- versus singlecloud-implementaties. Door de theoretische kosten te presenteren naast de factoren die deze beïnvloeden, geeft deze analyse een beter onderbouwde en realistischere conclusie over welke kosten vaak onvoorzien zijn en mogelijk niet direct zichtbaar zijn tijdens de initiële planning.

Figuur 8 hieronder geeft een overzicht van de totale maandelijkse kosten per provider en een multicloudscenario, gebaseerd op een eenvoudige SaaS-applicatie in verschillende architecturen. Het biedt een vereenvoudigde maar informatieve vergelijking van de prijsverschillen afhankelijk van de gekozen cloudstrategie.



Figuur 8 Vergelijking van de maandelijkse kosten in een multicloud- versus singlecloud-opstelling

Hoewel de resultaten op papier duidelijkheid lijken te scheppen, is de werkelijkheid complexer. Cloudkosten zijn geen vaststaand bedrag, maar worden gevormd door een breed scala aan technische, operationele en zakelijke factoren. De prijscalculators die in de analyse zijn gebruikt, geven slechts een deel van het beeld en zijn gebaseerd op de openbare prijsniveaus. Deze weerspiegelen niet de werkelijke zakelijke overeenkomsten of consumptiepatronen.

Een belangrijke factor die wordt uitgesloten en vaak over het hoofd wordt gezien in rekenmachinegebaseerde berekeningen, is personeels- en operationele overhead. Het beheren van meerdere cloudomgevingen verhoogt de complexiteit van de hele omgeving aanzienlijk. Elk platform heeft zijn eigen services, terminologie en tools, waardoor IT-engineers kennis moeten hebben van meerdere omgevingen. Dit betekent dat organisaties fors moeten investeren in training, certificering en mogelijk het aannemen van personeel dat bekend is met verschillende platformen. Organisaties met al ruime ervaring binnen hun IT-teams kunnen minder overhead- en trainingskosten ervaren, terwijl kleinere of minder volwassen IT-organisaties een steile leercurve met bijbehorende kosten zullen ervaren.

Licentievoorwaarden maken de vergelijking nog ingewikkelder. De meeste providers staan klanten toe hun eigen licentie mee te nemen voor databases, virtuele machines en andere services. Bij andere providers is de licentie inbegrepen in de serviceprijs, afhankelijk van de service. Klanten die Microsoft-technologieën gebruiken, kunnen dus profiteren van Azure Hybrid-voordelen of kortingen op gereserveerde instances. OCI biedt voordelen voor het native uitvoeren van Oracle-workloads en AWS biedt kostenflexibiliteit zonder diverse besparingsplannen. Configuraties in deze vergelijking maakten gebruik van pay-as-you-go-prijzen, wat maximale flexibiliteit biedt, maar wel een hogere prijs heeft. In de praktijk kunnen grote organisaties vaak onderhandelen over aangepaste prijsafspraken of contracten voor vastgelegd gebruik afsluiten die betere prijzen bieden. Bedrijven die grote volumes cloudservices gebruiken, profiteren vaak van betere voordelen die niet tot uiting komen in de standaard prijscalculators. Deze

elementen zijn cruciaal bij het bepalen van de juiste strategie en kunnen een theoretisch kostenverschil veroorzaken ten opzichte van implementaties in de praktijk.

Een andere cruciale variabele is datavolume en dataoverdracht. Het scenario dat voor de vergelijking wordt gebruikt, gaat ervan uit dat er minimaal verkeer tussen services is en dat de datavolumes relatief klein zijn, aangezien alleen uitgaand internetverkeer wordt geschat op 50 GB/maand. In echte implementaties kunnen workloads veel meer data produceren, meer bandbreedte vereisen of frequentere interactie tussen componenten in verschillende clouds vereisen. Dit is met name relevant in multicloudomgevingen waar interne communicatie van workloads mogelijk via site-to-site VPN's moet verlopen, wat vaak kosten voor uitgaand verkeer in meerdere omgevingen genereert. Zelfs intern netwerkverkeer in clouds kan leiden tot onverwachte kosten, zoals uitgaande data tussen regio's of beschikbaarheidszones. Deze dataverplaatsingspatronen zijn zeer scenariospecifiek en kunnen de kosten drastisch verhogen boven de aanvankelijk geschatte kosten.

Elke provider omvat ook bepaalde kosten in het standaardprijsmodel, wat een extra laag onvoorspelbaarheid toevoegt. AWS brengt bijvoorbeeld kosten in rekening voor het gebruik van de NAT-gateway, load balancer-verwerking of verkeer tussen beschikbaarheidszones. Azure kan extra kosten genereren via monitoring- en diagnostische services zoals Log Analytics. OCI omvat relatief grote uitgaande datalimieten, maar wanneer deze drempels worden overschreden, kunnen de kosten snel stijgen. Dit soort kosten is vaak moeilijk te berekenen tijdens de planningsfase, vooral voor organisaties met dynamische of schaalbare workloads.

Uiteindelijk zijn kosten weliswaar een belangrijke factor, maar de operationele doelen en de bedrijfscontext van een organisatie helpen ook bepalen welke strategie de juiste is. Een duurder provider kan nog steeds een betere keuze zijn als deze nauwere integratie, licentievoordelen of een kortere doorlooptijd biedt bij het op de markt brengen van nieuwe diensten. De keuze voor een cloudoplossing mag daarom nooit alleen op basis van kosten worden gemaakt, maar ook in de context van strategische afstemming, servicespecialisatie en organisatorische capaciteit.

4. Bewijs van concept

Het doel van deze Proof was om de praktische implementatie van een technisch geïntegreerde multicloudarchitectuur te verkennen, die Azure en OCI verbindt en tegelijkertijd veilige toegang tot het on-premises datacenter vanuit één cloudprovider garandeert. Deze PoC werd ontworpen in het kader van Cegeka's interne innovatie-initiatieven, gericht op het vergroten van de kennis rond multicloudomgevingen.

Een centrale vereiste was het garanderen van een veilige en betrouwbare netwerkverbinding tussen de cloudomgevingen en een verbinding met het on-premises datacenter. Dit omvatte het configureren van VPN-tunnels, firewallclusters en het ontwerpen van aangepaste routeringspaden om verkeer correct te leiden. De PoC richt zich op connectiviteit en beheer op infrastructuurniveau in een multicloud-opstelling.

De implementatie van de PoC verliep in verschillende fasen, elk gericht op een specifieke cloudomgeving of connectiviteitslaag. Het doel was om de onderliggende infrastructuur stapsgewijs op te bouwen en ervoor te zorgen dat elke cloudomgeving afzonderlijk functioneerde voordat cross-cloud communicatie tot stand werd gebracht.

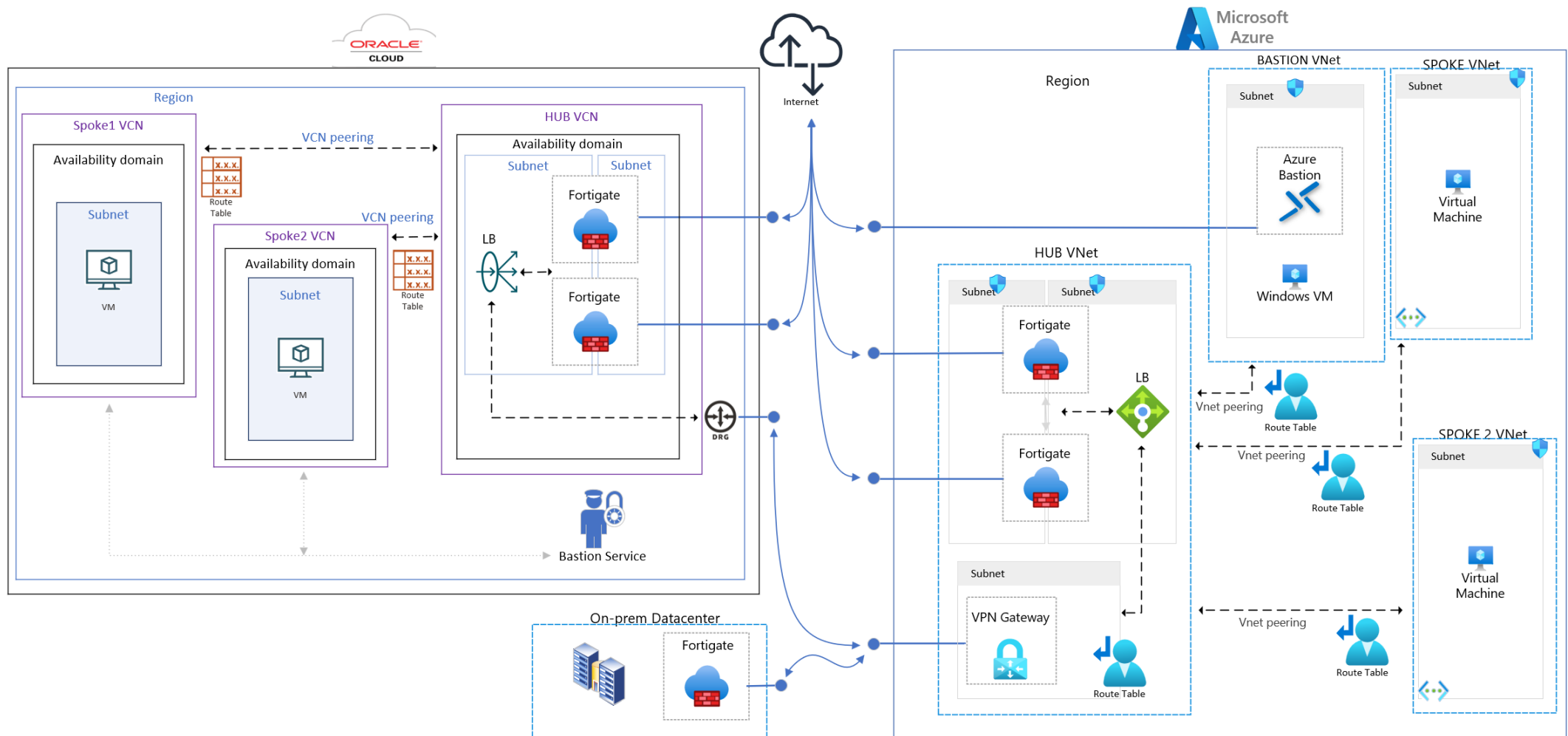
4.1. Infrastructuuroverzicht

De multicloudomgeving die voor deze PoC is ontworpen, bestaat uit twee cloudplatforms, Azure en OCI, die elk een eigen, maar vergelijkbare architectuur hebben. Beide cloudomgevingen volgen een hub-and-spoke-topologie, waarbij het virtuele hubnetwerk of cloudnetwerk fungeert als centraal connectiviteitspunt en de 'spokes' geïsoleerde workloads hosten.

In Azure omvat het hub-VNet een FortiGate-firewallcluster in een active-active-configuratie en een VPN-gateway, terwijl de 'spokes' virtuele machines bevatten die workloads binnen geïsoleerde subnetten kunnen simuleren. Op dezelfde manier werd in OCI een VCN voor de hub aangemaakt, met een FortiGate-firewallcluster met 'spokes' die in verschillende VCN's en subnetten zijn geïmplementeerd.

Om beide cloudomgevingen met elkaar te verbinden, wordt een site-to-site VPN tussen Azure en OCI gebruikt. Met behulp van IPsec-tunnels zorgt deze verbinding voor versleutelde, betrouwbare communicatie tussen de clouds. Daarnaast verbindt een tweede VPN-tunnel Azure met het on-premises datacenter, waardoor connectiviteit van on-premises naar de cloud mogelijk is.

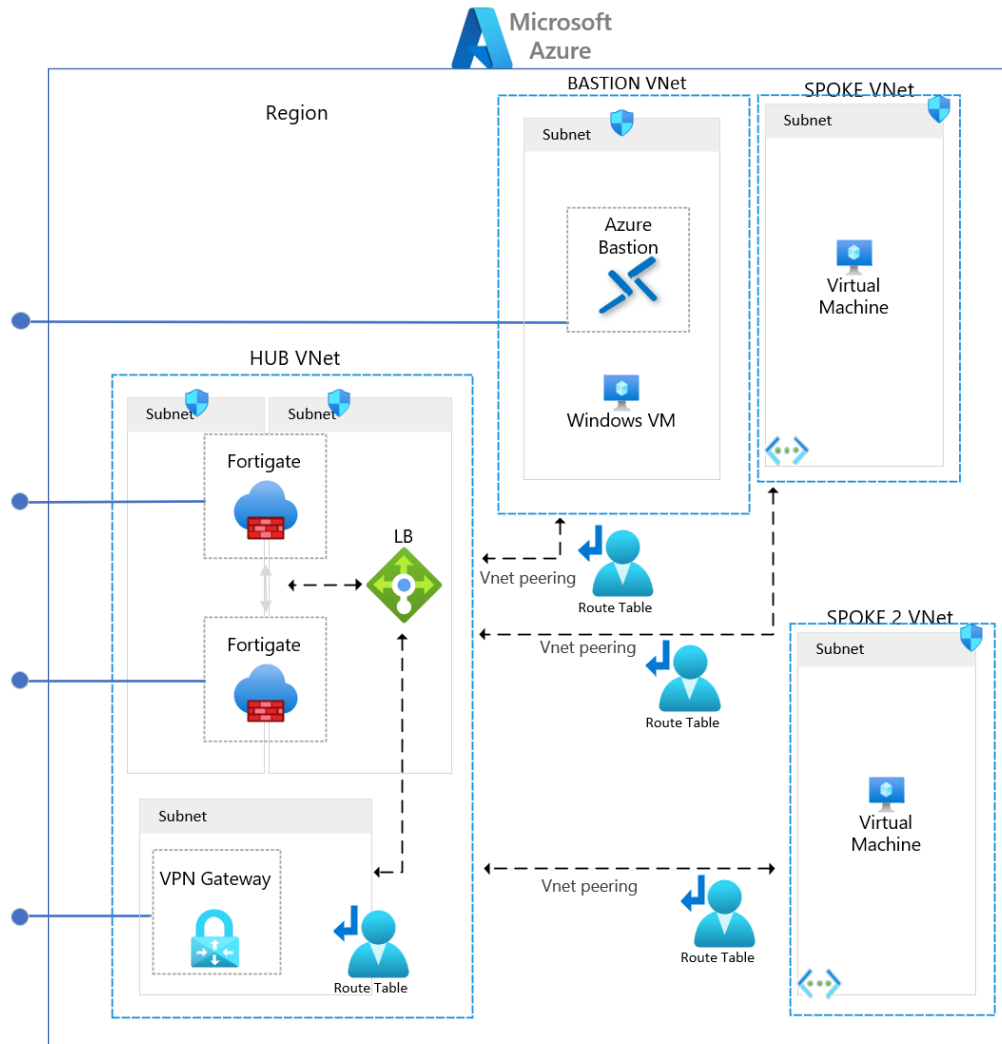
Elk firewallcluster fungeert als primair in- en uitgangspunt in zijn respectievelijke omgeving, en er zijn aangepaste routingstabellen geconfigureerd om al het verkeer, inclusief intern verkeer, via de firewalls te leiden. Figuur 9 illustreert de architectuur op hoog niveau.



Figuur 9 Multicloudarchitectuur tussen Azure en OCI met een verbinding met een on-premises datacenter

4.2. Infrastructuur in Azure

In deze sectie worden het ontwerp en de implementatie van de Azure-omgeving binnen de multicloud PoC beschreven. Zoals weergegeven in Figuur 10. Zoals blijkt uit de implementatie is er sprake van een hub-and-spoke-netwerkmodel, uitgerust met een firewallcluster om het verkeer te controleren en te inspecteren.



Figuur 10 Azure Cloud-architectuur met een hub-and-spokes-model

4.2.1. VNets en subnetten

De Azure-implementatie begon met het creëren van de hub-and-spoke-netwerktopologie. Centraal in de topologie staat het HUB VNet, dat fungeert als centraal communicatiepunt in de omgeving. Binnen dit VNet werden drie subnetten ingericht:

- I. **WAN-subnet:** Ontworpen voor het hosten van interfaces die externe connectiviteit vereisen, zoals de openbare netwerkinterfaces van de FortiGate-firewalls.
- II. **LAN-subnet:** Speciaal voor de interne verkeersstroom tussen Azure-spokes en de firewalls, waardoor beveiligde communicatie wordt gegarandeerd.
- III. **Gateway-subnet:** Een vereist subnet dat de VPN-gateway host die wordt gebruikt voor site-to-site-connectiviteit met OCI en het on-premises datacenter.

Daarnaast is er een apart Bastion VNet geïmplementeerd ter ondersteuning van veilige beheerderstoegang. Dit VNet omvat de Azure Bastion-service, die een veilige verbinding mogelijk maakt met de Windows VM die ook in hetzelfde VNet is geïmplementeerd.

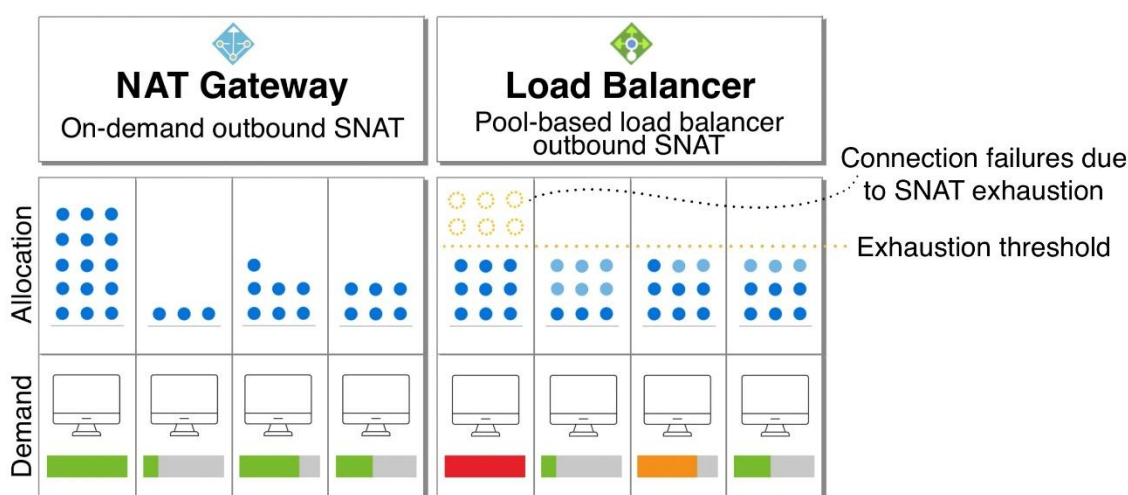
4.2.2. FortiGate-clusterconfiguratie

Een FortiGate-firewallcluster met hoge beschikbaarheid werd geïmplementeerd binnen het HUB VNet om de verkeersinspectie af te handelen. Elke FortiGate-instantie werd geconfigureerd met twee netwerkinterfaces: één interface in het WAN-subnet voor extern verkeer en één interface in het LAN-subnet voor intern verkeer. Deze configuratie maakt centrale inspectie van verkeer tussen spokes, het internet en externe clouds mogelijk. Het cluster zorgt ervoor dat alleen toegestaan verkeer, op basis van beleid, de resources in de cloud bereikt. De active-active configuratie ondersteunt automatische failover, wat zorgt voor hoge beschikbaarheid en redundantie.

4.2.3. Loadbalancer

Om de distributie van verkeer en sessieverwerking mogelijk te maken, werd vóór het cluster een Azure Internal Load Balancer (ILB) geconfigureerd. De ILB ontvangt uitgaand verkeer van interne resources en verdeelt dit over de firewallknooppunten. De regels voor load balancing waren gebaseerd op het bron-IP-adres en -protocol om sessiepersistentie te garanderen. Dit is met name handig voor stateful inspection, waarbij het verkeer van een sessie door dezelfde firewallinstantie moet worden afgehandeld. De ILB speelt een cruciale rol bij het bieden van hoge beschikbaarheid en redundantie. Wanneer een firewall niet meer beschikbaar is, leidt de load balancer het verkeer automatisch om naar de gezonde instantie.

Er is bewust gekozen voor een architectuur die de externe load balancer van Azure niet gebruikt voor binnenkomend verkeer. Deze beslissing was gebaseerd op twee beperkingen: het ontbreken van dynamische poorttoewijzing, zoals weergegeven in Figuur 11, en de afwezigheid van ondersteuning voor Internet Control Message Protocol (ICMP), wat vereist was voor diagnostiek en bereikbaarheidstests in deze PoC.



Figuur 11 Risico op SNAT-uitputting met Azure Load Balancer versus NAT-gateway

Opmerking. Geïnspireerd op "Optimaliseer uw Azure-implementaties voor uitgaande connectiviteit" van Microsoft Learn, 2025, Microsoft. <https://learn.microsoft.com/en-us/azure/load-balancer/troubleshoot-outbound-connection?>

4.2.4. Azure VPN Gateway en VPN-connectiviteit

Om veilige communicatie met externe netwerken mogelijk te maken, is een Azure VPN Gateway geïmplementeerd in het toegewezen subnet. De gateway ondersteunt meerdere VPN-verbindingen die zijn gebruikt. De gateway vormt één verbindingspunt tussen de site-to-site VPN-tunnels en OCI en het on-premises datacenter. Voor deze PoC is gekozen voor site-to-site VPN-tunnels omdat deze zijn ontworpen voor permanente, veilige verbindingen tussen netwerken. Dit sluit aan bij de doelstelling van de PoC om een geïntegreerde multicloud-opstelling te simuleren waarbij onderlinge verbinding centraal staat.

Alternatieven zoals Azure ExpressRoute werden overwogen, maar uiteindelijk niet gebruikt voor deze configuratie. ExpressRoute biedt privéconnectiviteit met hoge doorvoer naar andere netwerken, maar is duurder en daarom niet geschikt voor deze configuratie. Een site-to-site VPN daarentegen biedt een toegankelijke oplossing, vooral in een testomgeving.

De gateway vormt één eindpunt van twee IPSec site-to-site VPN-tunnels, waarvan er één naar OCI gaat en de andere naar het on-premises datacenter. Deze tunnels maken veilige, versleutelde communicatie mogelijk tussen de Azure-omgeving en beide externe netwerken, en vormen een cruciaal onderdeel van een multicloud-opstelling.

Tijdens de implementatie ontstond een extra technische uitdaging door het gebruik van overlappende IP-adresbereiken in het on-premises datacenter en de OCI-omgeving. Beide omgevingen gebruikten identieke netwerkprefixen, wat zou leiden tot routeringsconflicten en onjuiste beleidsafstemming met Azure. Om dit op te lossen, werden NAT-regels toegepast op de VPN-gateway, waardoor binnenkomend verkeer vanuit de on-premises omgeving werd omgezet naar een speciaal, niet-overlappend IP-bereik, zoals weergegeven in Figuur 12.

Name	Type	IP Configuration ID	Mode	Internal Mappings	External Mappings
ONPREM-TO-AZURE	Static		IngressSnat	172.22.20.64/28	192.168.0.64/28
AZURE-TO-ONPREM	Static		EgressSnat	192.168.0.64/28	172.22.20.64/28

Figuur 12 IP-adresvertaalregels tussen Azure en on-premises-omgevingen

4.2.5. Routing en peering

Om verkeer tussen het HUB-VNet en de spoke-VNets mogelijk te maken, werd VNet-peering geconfigureerd met bidirectionele toegang. Elke spoke is gekoppeld aan het HUB-VNet en er is geen peering tussen de spokes. Dit zorgt ervoor dat al het verkeer naar het HUB-VNet wordt geleid, waar inspectie kan plaatsvinden. Om dit te bereiken, werden User Defined Routes (UDR's) geconfigureerd in de routingtabellen van alle bijbehorende subnetten. De UDR's overschrijven de standaardroutes van Azure wanneer ze overlappen. In het geval van deze PoC werden de standaardroutes 0.0.0.0/0 van Azure overschreven, zodat al het verkeer van de spokes naar het IP-adres van de ILB wordt geleid, zoals weergegeven in Figuur 13.

Associated route table: ①

RT-SPOKE-LE-POC

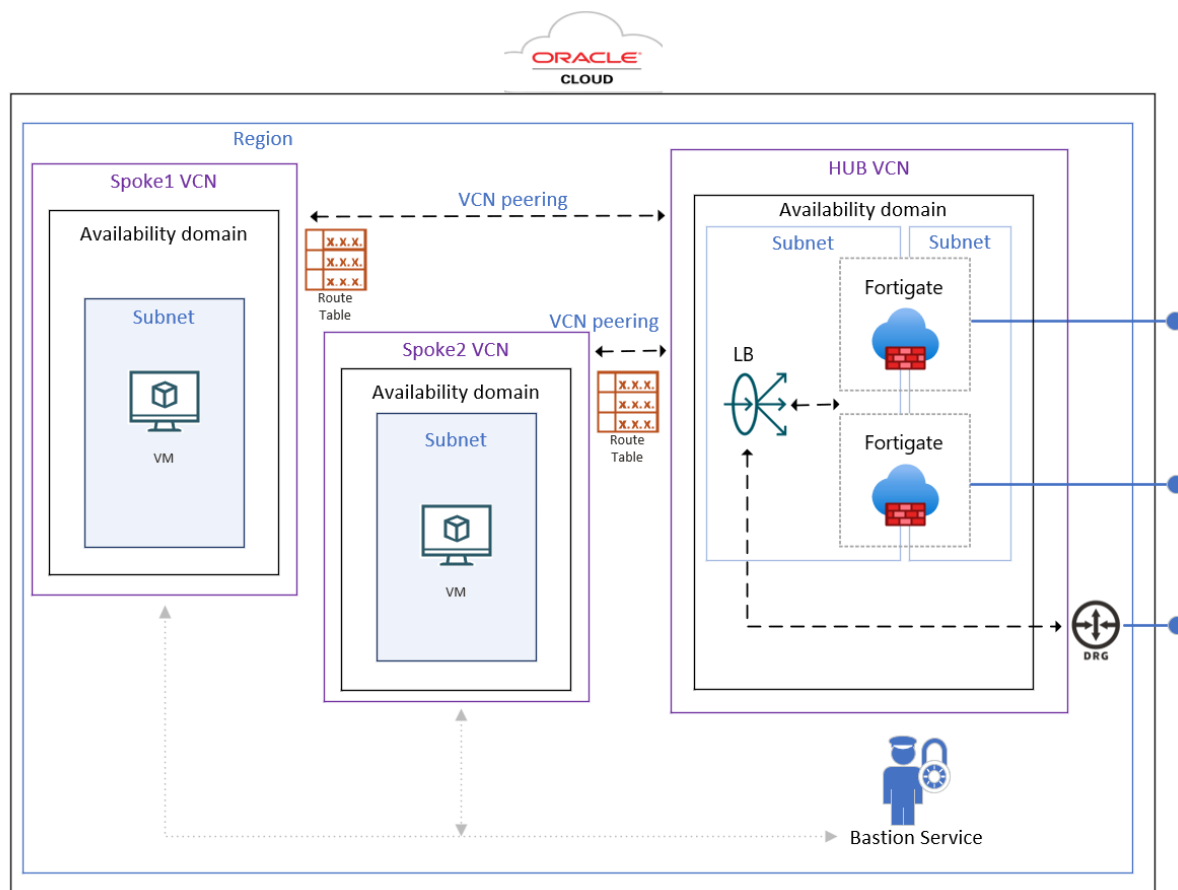
Effective routes

Source	↑↓	State	↑↓	Address Prefixes	↑↓	Next Hop Type	↑↓	Next Hop IP Address	↑↓	User Defined Route Name	↑↓
Default		Active		10.1.0.0/16		Virtual network		-		-	
Default		Active		10.0.0.0/16		VNet peering		-		-	
Default		<u>Invalid</u>		<u>0.0.0.0/0</u>		Internet		-		-	
User		<u>Active</u>		<u>0.0.0.0/0</u>		Virtual appliance		10.0.1.132		allTraffic	

Figuur 13 Door de gebruiker gedefinieerde route die de standaardroute in Azure overschrijft

4.3. Infrastructuur in OCI

In deze sectie worden het ontwerp en de implementatie van de OCI-omgeving beschreven. Zoals weergegeven in Figuur 14, werden dezelfde principes gevolgd als in Azure, met een hub-and-spokesmodel. Andere belangrijke elementen zijn de virtuele cloudnetwerken, het firewallcluster en de VPN-connectiviteit.



Figuur 14 OCI-cloudarchitectuur met een hub-and-spokesmodel

4.3.1. VCN's , subnetten en FortiGate-cluster

In OCI volgde het netwerkontwerp een vergelijkbare hub-and-spoke-aanpak als in Azure. Er werd een speciaal HUB VCN gecreëerd om te fungeren als centraal punt voor connectiviteit, routing en verkeersinspectie, eveneens met een WAN- en LAN-subnet toegewezen voor extern en intern verkeer. In tegenstelling tot Azure is de Dynamic Routing Gateway (DRG) in OCI echter niet gekoppeld aan een specifiek subnet. In plaats daarvan is het een resource op regioniveau waaraan meerdere VCN's, IPsec-tunnels, externe peerings en meer services kunnen worden gekoppeld. Het kan fungeren als centraal punt voor connectiviteit tussen OCI-regio's, andere cloudnetwerken en on-premises netwerken. Daarom was er geen speciaal subnet nodig voor VPN-connectiviteit.

Er zijn aparte 'spoke' VCN's gecreëerd om privé-workloads te hosten. Deze VCN's bevatten één subnet met één test-VM die wordt gebruikt om de interne routing en connectiviteit met andere netwerken te valideren.

Ook vergelijkbaar met de omgeving van Azure, werden twee FortiGate-firewalls in een active-active configuratie geïmplementeerd. Deze firewalls zijn verantwoordelijk voor al het verkeer tussen de spoke-VCN's, het internet en de externe cloudomgevingen. Om de lastverdeling over het cluster te beheren, werd een Network Load Balancer (NLB) geconfigureerd in de hub-VCN. De configuratie is nauw verwant aan die in Azure, wat zorgt voor uniform gedrag op alle platforms.

4.3.2. VPN-connectiviteit en DRG

In OCI wordt verbinding met externe omgevingen mogelijk gemaakt via DRG, waaraan de HUB VCN is gekoppeld. Er is een IPSec VPN-tunnel tot stand gebracht tussen de DRG en de Azure VPN-gateway om veilige, versleutelde communicatie mogelijk te maken.

Statische routes werden geconfigureerd om verkeer van het OCI-spoke VCN via de FortiGate naar de Network Load Balancer (NLB) te leiden, vervolgens via de DRG en uiteindelijk via de VPN-tunnel naar Azure. Verkeer van Azure wordt op dezelfde manier teruggeleid naar OCI.

De keuze voor site-to-site VPN in OCI is om dezelfde redenen gemaakt als in Azure: flexibele, kosteneffectieve connectiviteit en volledige compatibiliteit met multicloudomgevingen. Hoewel OCI ook FastConnect ondersteunt voor dedicated, snelle privéverbindingen, was dit geen vereiste voor de PoC.

4.3.3. Routing en VCN-peering

Om de verkeersstroom te beheren, werden routetabellen geconfigureerd op zowel subnet- als DRG-koppelingsniveau. Al het verkeer van de spoke-VCN's werd via het interne IP-adres van de NLB naar het FortiGate-firewallcluster geleid, zodat het verkeer werd gecontroleerd voordat het de bestemming bereikte. Lokale VCN-peering werd gebruikt om de spoke-VCN's te verbinden met de HUB-VCN, waardoor connectiviteit met de HUB als centraal punt mogelijk werd, vergelijkbaar met Azure.

4.4. Bewijs van implementatie

Om het ontwerp te valideren en te garanderen dat de multicloudarchitectuur naar behoren functioneert, werden verschillende connectiviteitstests uitgevoerd. De test

richtte zich op interne routing, VPN-connectiviteit, firewallinspectie en NAT-gedrag in Azure, OCI en het on-premises datacenter. Elk scenario werd getest met echt netwerkverkeer, met firewallsessielogs om een correcte verkeersstroom te bevestigen.

4.4.1. Connectiviteit in Azure

Om de interne routing en firewallintegratie binnen Azure te verifiëren, probeerde de virtuele machine in spoke VNet 1 een andere virtuele machine in spoke VNet 2 te bereiken. Figuur 15 toont de succesvolle ICMP-verkeersdoorvoer (ping) en toont aan dat VNet-peering operationeel is. Figuur 16 Vervolgens wordt aangetoond dat het verkeer correct door het FortiGate-cluster gaat voor inspectie en doorsturen. Dit bevestigt dat de interne communicatie tussen spoke-netwerken functioneert via het hub-and-spoke-model. Bovendien bevestigde de FortiGate-sessietabel dat al het verkeer de firewall passeerde, wat valideert dat de routing en inspectie in de hele omgeving consistent zijn.

```

2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state
link/ether 00:22:48:5a:fa:f8 brd ff:ff:ff:ff:ff:ff
inet 10.1.0.4/24 metric 100 brd 10.1.0.255 scope global eth0
    valid_lft forever preferred_lft forever
inet6 fe80::222:48ff:fe5a:faf8/64 scope link
    valid_lft forever preferred_lft forever
lepoc@UBUNTUS-P1-LE-POC:~$ ping -c 3 10.2.0.4
PING 10.2.0.4 (10.2.0.4) 56(84) bytes of data.
64 bytes from 10.2.0.4: icmp_seq=1 ttl=63 time=7.87 ms
64 bytes from 10.2.0.4: icmp_seq=2 ttl=63 time=5.71 ms
64 bytes from 10.2.0.4: icmp_seq=3 ttl=63 time=2.47 ms

--- 10.2.0.4 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 2.472/5.351/7.871/2.218 ms
lepoc@UBUNTUS-P1-LE-POC:~$

```

Figuur 15 Connectiviteitstest tussen twee virtuele machines in Azure

Time		Source	Device	Destination	Application Name	Result	Policy ID
i:52		10.1.0.4		10.2.0.4	PING	✓ Accept (252 B / 252 B)	AzureIntern(4)

Figuur 16 FortiGate Firewall-sessielogboek

4.4.2. Connectiviteit in Azure met internet

Om de uitgaande internettoegang vanuit Azure's spoke-VNets te valideren, werd een test uitgevoerd door ICMP-verkeer van een virtuele machine in een spoke-VNet naar google.com te sturen, zoals weergegeven in Figuur 17. Het antwoord bevestigde dat de uitgaande internetconnectiviteit functioneerde. Het toont ook aan dat er geen openbaar IP-adres vereist is op de virtuele machine zelf, omdat al het verkeer centraal via de FortiGate-firewall wordt gerouteerd.


```

lepoc@UBUNTUS-P1-LE-POC:~$ ping -c 3 google.com
PING google.com (142.250.181.238) 56(84) bytes of data.
64 bytes from fra16s56-in-f14.1e100.net (142.250.181.238): icmp_seq=1 ttl=112 time=4.06 ms
64 bytes from fra16s56-in-f14.1e100.net (142.250.181.238): icmp_seq=2 ttl=112 time=3.14 ms
64 bytes from fra16s56-in-f14.1e100.net (142.250.181.238): icmp_seq=3 ttl=112 time=3.85 ms

--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 3.135/3.681/4.060/0.395 ms
lepoc@UBUNTUS-P1-LE-POC:~$

```

Figuur 17Connectiviteitstest van een virtuele machine in Azure naar internet

Naast het pingresultaat moest de FortiGate-sessietabel opnieuw verifiëren of het verkeer de firewall passeerde, zoals te zien is in Figuur 18. Afbeelding 19 REF_Ref200120300 \h toont de uitvoer van de opdracht `diagnose sys session list | grep 10.1.0.4` op de FortiGate-firewall en laat zien dat het interne bron-IP van de virtuele machine is vertaald (SNAT) naar het privé-WAN-interface-IP van de FortiGate, voordat het de publieke bestemming van het IP-adres van Google bereikte. Het retourverkeer werd ook correct verwerkt met DNAT, waarbij de respons werd teruggekoppeld naar de oorspronkelijke bron. Dit bevestigde dat FortiGate actief uitgaand verkeer verwerkt, NAT correct is toegepast en routing en sessieafhandeling naar behoren functioneren.

Date...	Source	Device	Destination	Application Name	Result	P...
2025/0...	10.1.0.4		 142.250.185.78	PING	✓ Accept (2.44 kB / 2.44 kB)	ping(5

Figuur 18FortiGate Firewall-sessielogboek

```

lepoc-fgt-1 # diagnose sys session list | grep 10.1.0.4
hook=post dir=org act=snat 10.1.0.4:2->142.250.186.46:8(10.0.1.69:5118)
hook=pre dir=reply act=dnat 142.250.186.46:5118->10.0.1.69:0(10.1.0.4:2)

```

Figuur 19FortiGate CLI-uitvoer: vertaalde sessie van 10.1.0.4 naar internet

4.4.3. Connectiviteit tussen Azure en het datacenter

De connectiviteit met het on-premises datacenter werd getest met behulp van een ping van de Azure VM naar een bekende bereikbare host in het datacenter, in Figuur 20. De bronping van de host in het datacenter is 172.22.20.65 en komt binnen in Azure als 192.168.0.65. Dit komt door de NAT-regels die worden toegepast op de VPN-gateway, zoals uitgelegd in een eerder hoofdstuk. De succesvolle respons, in Figuur 22, bevestigde dat de IPsec site-to-site VPN-tunnel actief was, dat het verkeer correct werd gerouteerd via de FortiGate en Azure VPN Gateway, en dat NAT toegepast op de gateway de bereikbaarheid of retourpaden niet verstoort. Figuur 21 En Figuur 23 tonen opnieuw aan dat het verkeer effectief de benodigde firewalls passeert.

```

CLI Console (1)
649.697860 192.168.0.65 -> 10.1.0.4: icmp: echo request
649.697860 192.168.0.65 -> 10.1.0.4: icmp: echo request
649.697864 192.168.0.65 -> 10.1.0.4: icmp: echo request
649.697864 192.168.0.65 -> 10.1.0.4: icmp: echo request
649.699806 10.1.0.4 -> 192.168.0.65: icmp: echo reply
649.699806 10.1.0.4 -> 192.168.0.65: icmp: echo reply
649.699826 10.1.0.4 -> 192.168.0.65: icmp: echo reply
649.699826 10.1.0.4 -> 192.168.0.65: icmp: echo reply
649.699829 10.1.0.4 -> 192.168.0.65: icmp: echo reply
649.699829 10.1.0.4 -> 192.168.0.65: icmp: echo reply

^C
--- 10.1.0.4 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 13.6/17.6/23.0 ms

FGT-CGK-FORTI # execute ping-options source 172.22.20.65
FGT-CGK-FORTI # execute ping 10.1.0.4
PING 10.1.0.4 (10.1.0.4): 56 data bytes
64 bytes from 10.1.0.4: icmp_seq=0 ttl=63 time=14.5 ms
64 bytes from 10.1.0.4: icmp_seq=1 ttl=63 time=13.8 ms
64 bytes from 10.1.0.4: icmp_seq=2 ttl=63 time=14.0 ms
^C
--- 10.1.0.4 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 13.8/14.1/14.5 ms

```

Figuur 20Connectiviteitstest vanuit on-premises datacenter en Azure

Da...	Source	Device	Destination	Application Name	Result	Policy ID
2025...	192.168.0.65		10.1.0.4	PING	✓ Accept (252 B / 252 B)	testvpn (6)

Figuur 21FortiGate Firewall-sessielogboek

```
lepoc@UBUNTUS-P1-LE-POC:~$ ping -c 3 192.168.0.65
PING 192.168.0.65 (192.168.0.65) 56(84) bytes of data.
64 bytes from 192.168.0.65: icmp_seq=1 ttl=254 time=15.6 ms
64 bytes from 192.168.0.65: icmp_seq=2 ttl=254 time=14.7 ms
64 bytes from 192.168.0.65: icmp_seq=3 ttl=254 time=14.3 ms

--- 192.168.0.65 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 14.293/14.869/15.611/0.550 ms
lepoc@UBUNTUS-P1-LE-POC:~$
```

Figuur 22Connectiviteitstest van Azure naar on-premises datacenter

Source	Device	Destination	Application Name	Result	Policy ID
202...	10.1.0.4	192.168.0.65	PING	✓ Accept (252 B / 252 B)	testvpn (6)

Figuur 23FortiGate Firewall-sessielogboek

4.4.4. Connectiviteit tussen OCI en Azure

Figuur 24 Om de connectiviteit tussen de cloudomgevingen te bevestigen, werd een pingtest uitgevoerd vanaf een Azure VM naar een VM die in OCI werd gehost en terug. De respons bevestigde dat de IPsec VPN-tunnel tussen de Azure VPN-gateway en OCI DRG actief was en dat de routes en firewallregels aan beide kanten correct waren geconfigureerd. De test valideerde het multicloudaspect van de PoC en bevestigde dat het verkeer tussen de clouds zowel versleuteld als geïnspecteerd is. Figuur 25 geeft aan dat het verkeer via de FortiGate-firewalls verloopt.

```
lepoc@UBUNTUS-P1-LE-POC:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOW
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq s
    link/ether 00:22:48:9a:fa:f8 brd ff:ff:ff:ff:ff:ff
    inet 10.1.0.4/24 metric 100 brd 10.1.0.255 scope global et
        valid_lft forever preferred_lft forever
    inet6 fe80::222:48ff:fe5a:faf8/64 scope link
        valid_lft forever preferred_lft forever
lepoc@UBUNTUS-P1-LE-POC:~$ ping 172.22.20.68
PING 172.22.20.68 (172.22.20.68) 56(84) bytes of data.
64 bytes from 172.22.20.68: icmp_seq=1 ttl=59 time=14.2 ms
64 bytes from 172.22.20.68: icmp_seq=2 ttl=59 time=12.0 ms
64 bytes from 172.22.20.68: icmp_seq=3 ttl=59 time=11.9 ms
^C
--- 172.22.20.68 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 11.904/12.725/14.241/1.072 ms
lepoc@UBUNTUS-P1-LE-POC:~$

ubuntu@spoke3-vnic:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOW
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9000 qdisc pfifo_fast st
    link/ether 02:00:17:03:b3:a5 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet 172.22.20.68/28 metric 100 brd 172.22.20.79 scope global ens3
        valid_lft forever preferred_lft forever
    inet6 fe80::17ff:fe03:b3a5/64 scope link
        valid_lft forever preferred_lft forever
ubuntu@spoke3-vnic:~$ ping 10.1.0.4
PING 10.1.0.4 (10.1.0.4) 56(84) bytes of data.
64 bytes from 10.1.0.4: icmp_seq=1 ttl=60 time=15.1 ms
64 bytes from 10.1.0.4: icmp_seq=2 ttl=60 time=12.0 ms
64 bytes from 10.1.0.4: icmp_seq=3 ttl=60 time=14.6 ms
^C
--- 10.1.0.4 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 12.017/13.917/15.130/1.360 ms
ubuntu@spoke3-vnic:~$
```

Figuur 24Connectiviteitstest tussen OCI en Azure

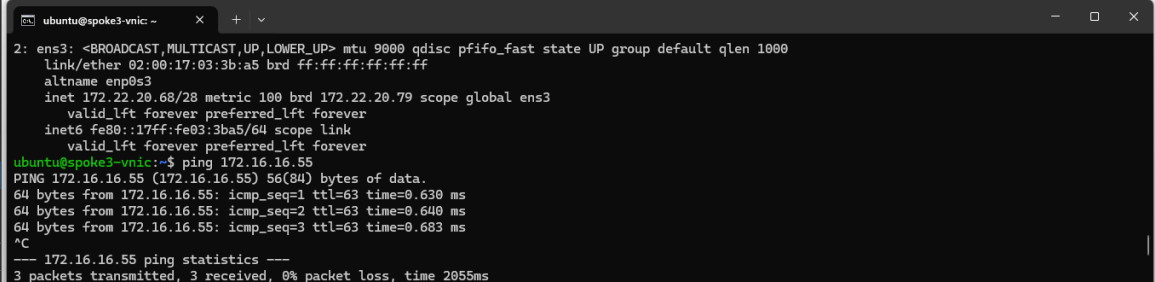
Source	D...	Destination	Application Name	Result	Policy ID
/0...	10.1.0.4	172.22.20.68	PING	✓ Accept (252 B / 252 B)	testvpn (6)

Figuur 25FortiGate Firewall-sessielogboek

4.4.5. Connectiviteit in OCI

Om de interne werking binnen de OCI-omgeving te valideren, werd een pingtest uitgevoerd tussen twee virtuele machines in twee verschillende subnetten over peered VCN's, zoals te zien is in Figuur 26. De succesvolle respons, samen met de sessietabel van de FortiGate, bevestigde dat het verkeer succesvol door het firewallcluster werd geleid, waardoor werd gegarandeerd dat intern verkeer ook het HUB VCN passeerde.

Date/Time		Source	Device	Destination	Application Name	Result
2025/05/08 10:44:47		172.22.20.68		172.16.16.55	PING	✓ Accept (252 B / 252 B)



The screenshot shows a terminal window titled 'ubuntu@spoke3-vnic ~'. It displays the configuration of the 'ens3' network interface, including its IP address (172.22.20.68) and other settings. Below the configuration, a ping command is executed: 'ping 172.16.16.55'. The output shows three successful ping attempts with a time of approximately 0.630 ms each. At the bottom, the ping statistics are shown: '3 packets transmitted, 3 received, 0% packet loss, time 2055ms'.

Figuur 26 FortiGate-sessielogboek en connectiviteitstest in OCI

5. Conclusie

In dit proefschrift werd de vraag onderzocht hoe een multicloudomgeving kan worden geïmplementeerd en wanneer een dergelijke strategie gerechtvaardigd is. Door een combinatie van theoretisch onderzoek en een technische PoC werden zowel de strategische motivaties als de praktische uitdagingen van de adoptie van multicloud geanalyseerd en gedemonstreerd in een realistische opzet.

Vanuit theoretisch oogpunt werd duidelijk dat alle cloudproviders, AWS, Azure en OCI, een grotendeels vergelijkbare set kernservices aanbieden, zoals computing, opslag, netwerken en IAM. De manier waarop deze services worden geïmplementeerd, beheerd en geprijsd, verschilt echter aanzienlijk. Azure blinkt uit in hybride integraties en enterprise-ecosystemen, AWS loopt voorop in de breedte van services en wereldwijde schaal, terwijl OCI zich positioneert als een kosteneffectief en krachtig platform voor data-intensieve workloads. Deze verschillen creëren een strategische kans om de sterke punten van elke provider te benutten in een multicloudarchitectuur.

De PoC valideerde dat een dergelijke integratie technisch mogelijk is. Door een hub-and-spoke-architectuur te ontwerpen en te implementeren in zowel Azure als OCI, en deze te verbinden via een VPN-verbinding, toonde de PoC aan dat cloudomgevingen van verschillende providers veilig en betrouwbaar met elkaar verbonden kunnen worden. De routing werd gecentraliseerd via firewallclusters om volledige inspectie en controle van het verkeer te garanderen. Bovendien toonde de PoC aan dat de integratie van een derde omgeving, zoals een on-premises datacenter, mogelijk is met dezelfde principes en technologieën. Dit brengt echter wel extra uitdagingen met zich mee, zoals overlappende VPN IP-bereiken, die werden ondervangen door NAT-strategieën.

In het proefschrift werden de voordelen van multicloud bevestigd: flexibiliteit, minder vendor lock-in, workloadoptimalisatie, de mogelijkheid van verhoogde veerkracht en snellere innovatie. Tegelijkertijd kwamen er tal van uitdagingen naar voren. Het beheer van IAM over verschillende cloudplatforms vereist meerdere configuraties en federaties met tools van derden, monitoring mist integratie tussen providers zonder externe tools en het inzicht in de kosten kan beperkt zijn. Deze uitdagingen maken duidelijk dat multicloud geen standaardpad is, maar een weloverwogen strategie moet zijn die aansluit bij de behoeften en mogelijkheden van de organisatie.

Wat de kosten betreft, lieten de analyse en de kostenoverwegingen zien dat multicloud-implementaties vaak een hogere operationele en financiële last met zich meebrengen in vergelijking met singlecloud-configuraties. Hoewel theoretische kostenbesparingen mogelijk zijn door servicespecialisatie, worden deze gemakkelijk tenietgedaan door indirecte kosten zoals personeel, training, certificering en governance-overhead. Deze bevindingen bevestigen dat multicloud het meest geschikt is voor organisaties die al cloudvolwassen zijn en duidelijk gedefinieerde zakelijke of technische motivaties hebben, zoals workloadspecialisatie, compliancebeperkingen of klantgedreven vereisten.

We kunnen er gerust van uitgaan dat een multicloudomgeving effectief kan worden geïmplementeerd, mits de organisatie beschikt over de technische expertise, de juiste capaciteit en een geldige strategische reden om dit te doen. De beslissing om een multicloudstrategie te implementeren mag nooit lichtvaardig of puur gebaseerd zijn op een vergelijking van providers; deze moet worden gestuurd door de daadwerkelijke

bedrijfsbehoeften, workloadkenmerken en flexibiliteitsdoelen op de lange termijn. Hoewel theoretische kostenvoordelen kunnen bestaan, betekenen de verborgen operationele kosten dat multicloud in de praktijk bijna altijd duurder is dan een enkele cloudopstelling. Er zijn echter scenario's waarin deze extra kosten gerechtvaardigd zijn: bijvoorbeeld wanneer platformspecifieke sterke punten moeten worden gecombineerd, compliance dit vereist of de verwachtingen van klanten ondersteuning over meerdere providers vereisen.

Voor een dienstverlener als Cegeka vormen deze complexiteiten eerder een kans dan een belemmering. Door expertise op te bouwen in meerdere cloudomgevingen kan Cegeka een breder scala aan klantomgevingen ondersteunen, inspelen op de steeds diversere klantvraag en zich onderscheiden in een competitieve IT-markt. Uiteindelijk draagt dit vermogen niet alleen bij aan technische innovatie, maar ook aan commerciële groei, uitbreiding van het klantenbestand en het verhogen van de potentiële omzet uit geleverde clouddiensten. Het proefschrift toont aan dat zowel de kansen als de risico's aanwezig zijn. Het vinden van een evenwicht daartussen vereist meer dan alleen technische kennis; het vereist een goed doordachte, goed onderbouwde architectuurvisie.

REFERENTIELIJST

Abandy, R. (24 augustus 2022). *De geschiedenis van Microsoft Azure*. Microsoft. Geraadpleegd op 8 april 2025 van <https://techcommunity.microsoft.com/blog/educatordeveloperblog/de-geschiedenis-van-microsoft-azure/3574204>

Appvia. (19 februari 2024). *Hoe een multicloudstrategie compliance kan vereenvoudigen*. Appvia. Geraadpleegd op 12 maart 2025 via <https://www.appvia.io/blog/how-a-multi-cloud-strategy-can-simplify-compliance>

AWS. (2025). *AWS Global Infrastructure*. AWS Amazon. Geraadpleegd op 19 maart 2025 via <https://aws.amazon.com/about-aws/global-infrastructure/>

AWS. (2025). *Hoe betaal je voor AWS?* AWS Amazon. Geraadpleegd op 28 maart 2025 via https://aws.amazon.com/pricing/?nc2=h_ql_pr_ln&aws-products-pricing.sort-by=item.additionalFields.productNameLowercase&aws-products-pricing.sort-order=asc&awsf.Free%20Tier%20Type=*all&awsf.tech-category=*all

AWS. (sa). *Identiteitsproviders en federatie*. AWS Amazon. Geraadpleegd op 13 mei 2025 via https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers.html

AWS. (2025). *Onze oorsprong*. AWS Amazon. Geraadpleegd op 8 april 2025 via <https://aws.amazon.com/about-aws/our-origins/>

AWS. (2025). *Regio's en beschikbaarheidszones*. AWS Amazon. Geraadpleegd op 15 april 2025 via https://aws.amazon.com/about-aws/global-infrastructure/regions_az/?p=ngi&loc=2

Barr, J. (2024, 18 november). *AWS Lambda bestaat tien jaar – een terugblik en een vooruitblik*. AWS. Geraadpleegd op 27 februari 2025 via <https://aws.amazon.com/blogs/aws/aws-lambda-turns-ten-the-first-decade-of-serverless-innovation/>

Bell, H. (31 januari 2019). *Wat is het verschil tussen multicloud en hybride cloud?* Nutanix. Geraadpleegd op 4 maart 2025 via https://www.nutanix.com/en_gb/blog/hybrid-cloud-vs-multi-cloud-whats-difference

Brophy, M. (2025, 19 mei). *Trends in de cloudcomputingmarkt om in de gaten te houden in 2025*. AlphaSense. Geraadpleegd op 21 mei 2025 via <https://www.alpha-sense.com/blog/trends/cloud-computing-market-trends/>

Chen, M. (2025, 20 februari). *Wat is multicloud? Toepassingen en voordelen*. Oracle. Geraadpleegd op 11 maart 2025 via <https://www.oracle.com/cloud/multicloud/what-is-multicloud/>

Dua, A. (23 februari 2024). *IaaS versus PaaS versus SaaS: de belangrijkste verschillen uitgelegd*. Turing. Geraadpleegd op 18 maart 2025 van <https://www.turing.com/blog/iaas-vs-paas-vs-saas-belangrijkste-verschillen>

F5. (sa). *Wat is multicloudnetwerkarchitectuur?* F5. Geraadpleegd op 19 februari 2025 via <https://www.f5.com/glossary/multi-cloud-network-architecture>

Gartner, Magic Quadrant voor Integration Platform as a Service, Guttridge, K., Comes, A., Pasricha, S., van den Berk, M. & Humphreys, A. (2024, 19 februari). *Oracle Restricted IT Executive's Guide to Oracle Cloud Infrastructure* . Oracle. Geraadpleegd op 8 april 2025 via <https://www.oracle.com/a/ocom/docs/cloud/oracle-cloud-infrastructure-platform-overview-wp.pdf>

Google Cloud. (sa). *Voordelen en nadelen van cloudcomputing* . Google Cloud. Geraadpleegd op 5 maart 2025 via <https://cloud.google.com/learn/advantages-of-cloud-computing?hl=en>

Google Cloud. (sa). *Wat is multicloud?* . Google. Geraadpleegd op 13 maart 2025 via <https://cloud.google.com/learn/what-is-multicloud>

IBM. (20 oktober 2021). *Wat zijn Iaas, Paas en Saas?* IBM. Geraadpleegd op 18 maart 2025 via <https://www.ibm.com/think/topics/iaas-paas-saas>

Krishnakumar, V. (2025, 11 april). *Azure Arc: Vereenvoudiging van hybride en multi-cloudbeheer* . Cloudoptimo. Geraadpleegd op 24 april 2025 via <https://www.cloudoptimo.com/blog/azure-arc-simplifying-hybrid-and-multi-cloud-management>

MarketsandMarkets. (2023, december). *Cloud Computing Market* . MarketsandMarkets. Geraadpleegd op 5 maart 2025 via <https://www.marketsandmarkets.com/Market-Reports/cloud-computing-market-234.html>

Microsoft. (2025). *Microsoft Datacenters* . Microsoft. Geraadpleegd op 19 maart 2025 via <https://datacenters.microsoft.com/globe/explore?view=map>

Microsoft. (2025). *Wat zijn publieke, private en hybride clouds?* Azure Microsoft. Geraadpleegd op 13 mei 2025 via <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-are-private-public-hybrid-clouds>

Microsoft Learn. (28 mei 2025). *Aanbevolen procedures voor Azure Identity Management en toegangscontrolebeveiliging* . Microsoft. Geraadpleegd op 13 mei 2025 via <https://learn.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices>

Microsoft Learn. (21 maart 2025). *Wat zijn Azure-regio's?* Microsoft. Geraadpleegd op 26 februari 2025 via <https://learn.microsoft.com/en-us/azure/reliability/regions-overview>

Microsoft Learn. (25 februari 2025). *Wat zijn beschikbaarheidszones?* Microsoft. Geraadpleegd op 28 februari 2025 via <https://learn.microsoft.com/en-us/azure/reliability/availability-zones-overview?tabs=azure-cli>

Mishra, S. (2024, 9 september). *Multicloud Masterclass: OCI, Azure en AWS vergeleken* . Rainfocus. Geraadpleegd op 13 maart 2025 via https://static.rainfocus.com/oracle/ocw24/sess/1721138693474001PhzP/finalsessionfile/09.03.24%20OCW%20Multicloud%20Masterclass%20Oracle%20Cloud%20Infrastructure%2C%20Azure%2C%20and%20AWS%20Compared%20V1_1725356172709001XH2m.pdf

Oracle. (mei 2023). *Best practices voor identiteits- en toegangsbeheer (IAM) in Oracle Cloud Infrastructure* . Oracle. Geraadpleegd op 13 mei 2025 via <https://docs.oracle.com/en-us/iaas/Content/Resources/Assets/whitepapers/best-practices-for-iam-on-oci.pdf>

Oracle. (31 oktober 2024). *Vergelijk OCI met AWS, Azure en Google Cloud* . Oracle. Geraadpleegd op 6 maart 2025 via <https://www.oracle.com/cloud/service-comparison/>

Oracle. (23 oktober 2024). *Oracle opnieuw erkend als leider in de Gartner Magic Quadrant™-rapporten van 2024 voor strategische cloudplatformservices en gedistribueerde hybride infrastructuur* . Oracle. Geraadpleegd op 27 maart 2025 via <https://www.oracle.com/news/announcement/oracle-again-recognized-as-a-leader-in-the-2024-gartner-magic-quadrant-reports-for-strategic-cloud-platform-services-and-distributed-hybrid-infrastructure-2024-10-23/>

Oracle. (2025). *Public Cloud Regions* . Oracle. Geraadpleegd op 19 maart 2025 via <https://www.oracle.com/be/cloud/public-cloud-regions/>

Oracle. (21 mei 2025). *Regio's en beschikbaarheidsdomeinen* . Oracle. Geraadpleegd op 17 april 2025 via <https://docs.oracle.com/en-us/iaas/Content/General/Concepts/regions.htm?>

Richter, F. (27 februari 2025). *Cloudinfrastructuurmarkt: Amazon en Microsoft blijven koploper op de wereldwijde cloudmarkt* . Statista. Geraadpleegd op 8 april 2025 van <https://www.statista.com/chart/18819/wereldwijd-marktaandeel-van-leidende-cloud-infrastructuur-serviceproviders/>

Sasovets, I., & Teres, K. (2025, 11 februari). *Multi-cloudbeveiliging: belangrijkste uitdagingen en effectieve werkwijzen van experts* . Techmagic. Geraadpleegd op 8 mei 2025 via <https://www.techmagic.co/blog/multi-cloud-security>

Susnjara, S. & Smalley, I. (2025, 10 februari). *Wat is cloudcomputing?* IBM. Geraadpleegd op 19 februari 2025 via <https://www.ibm.com/think/topics/cloud-computing>

Tata Communications. (11 april 2025). *Multicloud versus singlecloud: welke is geschikt voor uw bedrijf?* Tatacommunications. Geraadpleegd op 2 april 2025 via <https://www.tatacommunications.com/knowledge-base/multi-cloud-vs-single-cloud/>

Teske, K. (2024, 17 juni). *Multicloudstrategie: Beveiligde data en compliance* . Veeam. Geraadpleegd op 14 mei 2025 via <https://www.veeam.com/blog/multi-cloud-strategy.html>

BIJLAGE S

AWS Pricing Calculator > My Estimate

My Estimate [Edit](#) [Info](#) Export Share

Estimate summary [Info](#)

Upfront cost	Monthly cost	Total 12 months cost
0.00 USD	754.96 USD	9,059.52 USD
		Includes upfront cost

Getting Started with AWS

[Get started for free](#)

[Contact Sales](#)

My Estimate Duplicate Delete Move to Create group Add support Add service

< 1 > [Settings](#)

☐	Service Name		Status	Upfron...	MonthL...	Descrip...	Region	Con
☐	Amazon Simple Storage Service (S3)	Edit	-	0.00 USD	1.28 USD	-	US East (...)	S3 S
☐	AWS Lambda	Edit	-	0.00 USD	0.20 USD	-	US East (...)	Inve
☐	Amazon API Gateway	Edit	-	0.00 USD	32.10 USD	-	US East (...)	HTT
☐	Amazon QuickSight	Edit	-	0.00 USD	510.00 USD	-	US East (...)	SPIC
☐	Amazon Virtual Private Cloud (VPC)	Edit	-	0.00 USD	66.50 USD	-	US East (...)	Wor
☐	Amazon Simple Storage Service (S3)	Edit	-	0.00 USD	0.92 USD	-	US East (...)	S3 S
☐	Amazon RDS for SQL server	Edit	-	0.00 USD	143.96 USD	-	US East (...)	Stor

Bijlage 1 Prijsberekening in een enkele cloudopstelling in AWS

OCI
About Services Solutions Pricing Partners Resources
Search
Sign in to Oracle Cloud

My Estimate
Configure and estimate costs for OCI services (Learn more)
Send to Sales
Start for Free
EUR - Euro
Estimated Monthly Cost
€628.80

Add configuration

Object Storage ...
Estimated Monthly Cost €2.09

Virtual Cloud Networks ...
Estimated Monthly Cost €0.00

Oracle Analytics Cloud - Enterprise ...
Estimated Monthly Cost €502.34

Autonomous Database ...
Estimated Monthly Cost €122.84

OCI Functions ...
Estimated Monthly Cost €0.03

Object Storage ...
Estimated Monthly Cost €1.50

Bijlage 2 Prijsberekening in een enkele cloudopstelling in OCI

single cloud

Static Web Apps	Standard tier, 1 app, 100 GB of Bandwidth...	Upfront: \$0.00	Monthly: \$9.00
Azure Functions	Consumption tier, Pay as you go, 512 MB...	Upfront: \$0.00	Monthly: \$0.20
Storage Accounts	Block Blob Storage, General Purpose V2, ...	Upfront: \$0.00	Monthly: \$4.84
Power BI Embedded	1 node(s) x 176 Hours, Node type: A2, 2 ...	Upfront: \$0.00	Monthly: \$353.43
Bandwidth	Internet egress, 300 GB outbound data tr...	Upfront: \$0.00	Monthly: \$16.00
VPN Gateway	VPN Gateways, VpnGw1 tier, 730 gateway...	Upfront: \$0.00	Monthly: \$138.70
Azure SQL Database	Single Database, vCore, Hyperscale, Provi...	Upfront: \$0.00	Monthly: \$213.43

Support
SUPPORT:
Basic (Included)
\$0.00

Select your program/offer
LICENSING PROGRAM:
Microsoft Customer Agreement (MCA)
Log in to see your Azure agreement pricing.
Show Dev/Test Pricing

Estimated upfront cost \$0.00
Estimated monthly cost \$735.60

Bijlage 3 Prijsberekening in een enkele cloudopstelling in Azure

[AWS Pricing Calculator](#) > My Estimate

My Estimate [Edit](#)

[Export](#) [Share](#)

Estimate summary [Info](#)

Upfront cost	Monthly cost	Total 12 months cost
0.00 USD	198.74 USD	2,384.88 USD
		Includes upfront cost

Getting Started with AWS

[Get started for free](#)

[Contact Sales](#)

My Estimate

[Duplicate](#) [Delete](#) [Move to](#) [Create group](#) [Add support](#) [Add service](#)

☐	Service Name	Status	Upfront...	Monthl...	Descrip...	Region	Confi
☐	Amazon Simple Storage Service (S3)	-	0.00 USD	1.28 USD	-	US East (...)	S3 St
☐	AWS Lambda	-	0.00 USD	0.20 USD	-	US East (...)	Invok
☐	Amazon API Gateway	-	0.00 USD	32.10 USD	-	US East (...)	HTTP
☐	Amazon Virtual Private Cloud (VPC)	-	0.00 USD	165.16 USD	-	US East (...)	Work

Bijlage 4 Prijsberekening in een multicloud-opstelling in AWS

multicloud

↺

↻

↻

🗑

✓ Power BI Embedded	ⓘ	1 node(s) x 176 Hours, Node type: A2, 2 Vi...	⊕ 🗑	Upfront: \$0.00	Monthly: \$353.43
✓ Storage Accounts	ⓘ	Block Blob Storage, General Purpose V2, F...	⊕ 🗑	Upfront: \$0.00	Monthly: \$5.88
✓ VPN Gateway	ⓘ	VPN Gateways, VpnGw1 tier, 730 gateway ...	⊕ 🗑	Upfront: \$0.00	Monthly: \$138.70
✓ Bandwidth	ⓘ	Internet egress, 1000 GB outbound data tr...	⊕ 🗑	Upfront: \$0.00	Monthly: \$72.00

Support

SUPPORT:

Basic (Included) [Info](#)

\$0.00

Select your program/offer

LICENSING PROGRAM:

Microsoft Customer Agreement (MCA) [Info](#)

[Log in](#) to see your Azure agreement pricing.

☐ Show Dev/Test Pricing [Info](#)

Estimated upfront cost

\$0.00

Estimated monthly cost

\$570.01

Bijlage 5 Prijsberekening in een multicloud-opstelling in Azure

My Estimate

Configure and estimate costs for OCI services ([Learn more](#))

Send to Sales

Start for Free

EUR - Euro

Estimated Monthly Cost

€119.66

Add configuration

Object Storage

Estimated Monthly Cost €1.25

Autonomous Database

Estimated Monthly Cost €118.41

Bijlage 6 Prijsberekening in een multicloud-opstelling in OCI

Stage – Wolken verbinden – Bachelorscriptie

44