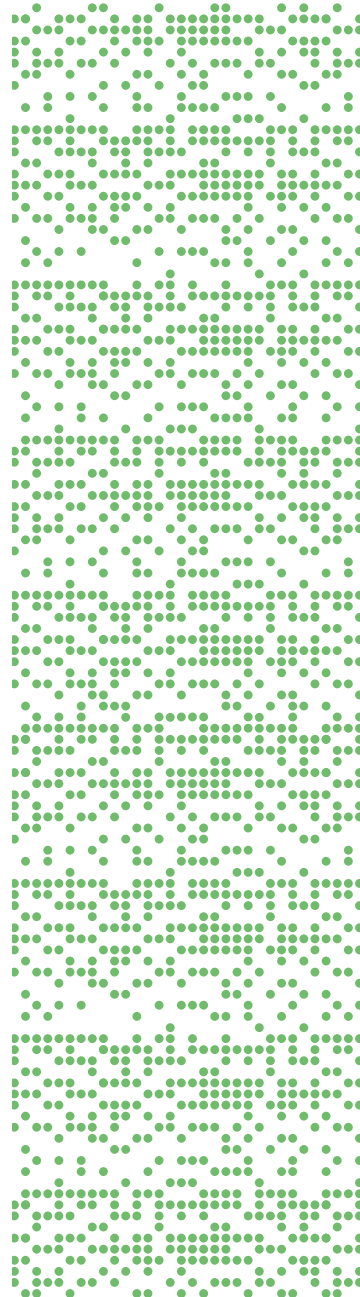


WHITE PAPER
**CLOUD,
CONNECTIVITEIT EN
AUTOMATION**

EEN PRAKTISCHE HANDLEIDING VOOR
STRATEGIEONTWIKKELING

(VISION TO DATE JANUARI 2022)

[ROUTZ.NL](https://www.routz.nl)



INDEX

	Inleiding	5
1	Cloud: een introductie	7
2	Connectiviteit	13
3	Cloud automation	27
4	Tot slot: Routz helpt u graag!	35



ROUTZ GROUP

- NETWORK EXECUTIVES
- NETWORK SERVICES
- NETWORK OPERATIONS
- BUSINESS CONSULTANCY

INLEIDING

De cloud biedt meerwaarde én uitdaging ...

Veel bedrijven willen met de cloud waarde toevoegen aan hun business. Logisch ook, want de voordelen van werken in de cloud zijn groot. Het biedt organisaties meer schaalbaarheid, snelheid en eenvoud. Maar in de praktijk is de integratie van cloud in de bestaande technische architectuur en IT-organisatie vaak een uitdaging.

... maar integratie blijft een uitdaging

Een goede netwerkachitectuur in de cloud is essentieel voor de performance van de hele IT-dienstverlening, net als in traditionele ICT-infrastructuren. Niet alleen voor verkeer binnen de cloud, maar ook tussen de cloud en de eigen locatie (on-premises omgeving). En de cloud biedt weliswaar met een paar muisklikken een IT-infrastructuur die voorheen maanden aan doorlooptijd en ontwikkeling kostte, meer er komen ook nieuwe uitdagingen mee. Bijvoorbeeld op het gebied van connectiviteit en security, en juist dáár is de integratie van bijzonder groot belang. De moeizame integratie maakt het voor veel organisaties uitdagend om de theoretische voordelen van werken in de cloud in de praktijk te ervaren.

Dit whitepaper helpt u op weg ...

Dit whitepaper is een praktische leidraad voor de cloud-initiatieven van uw organisatie. Het behandelt verschillende cloud-modellen en laat zien wat hun specifieke eigenschappen en nuances zijn. Zo krijgt u ook inzicht in de overeenkomsten en verschillen met uw bestaande infrastructuur. En vooral: in wat de cloud betekent voor uw architectuur en uw (IT-)organisatie.

... óók als het gaat om automation en orchestration

Cloud kan niet los gezien worden van de ontwikkelingen op het gebied van automation en orchestration. Een infrastructuur die bij uitstek geschikt en ontworpen is om snel en flexibel op te schalen, kan immers niet effectief handmatig geconfigureerd en bediend worden. Enige vorm van automation en orchestration is daarom essentieel voor het slagen van uw cloud-strategie. Ook daar gaat dit whitepaper op in.

1

CLOUD: EEN INTRODUCTIE

CLOUD: EEN INTRODUCTIE

‘De cloud’ wordt vaak gebruikt als een containerbegrip. Voor het bepalen van een strategie is het belangrijk dat dit begrip concreter wordt. In dit hoofdstuk geven we daarom een definitie van de cloud, en beschrijven we de belangrijkste opties.

1.1 De definitie van cloud computing

Cloud computing is - eenvoudig gezegd - een model om snelle, eenvoudige netwerktoegang tot een gedeelde pool van configureerbare resources mogelijk te maken. Die resources zijn bijvoorbeeld netwerken, servers, opslag, applicaties en diensten. Dit cloudmodel bestaat uit vijf essentiële kenmerken, drie servicemodellen en vier implementatiemodellen (National Institute of Standards and Technology, 2011).

Die vijf kenmerken, drie servicemodellen en vier implementatiemodellen beschrijven we hieronder.

1.2 De vijf essentiële kenmerken van cloud-services

1. On-demand selfservice

De mogelijkheid om geautomatiseerd, dus zonder dat menselijk handelen nodig is, de beschikking te krijgen over compute, netwerk en storage resources.

2. Broad network access

De eerder genoemde resources zijn via het (internet-)netwerk te bereiken op verschillende devices, zoals PC, tablet of smartphone.

3. Resource pooling
De resources van de cloud provider worden gedeeld met andere gebruikers in aparte, logisch gescheiden omgevingen (tenants). Daarbinnen krijgt een gebruiker bepaalde resources toegewezen. Ook kan de gebruiker er in zekere mate de locatie van de resources bepalen (bijvoorbeeld op het niveau van regio, land of datacenter).
4. Rapid elasticity
De capaciteit van de resources groeit of krimpt mee met de gebruikersbehoefte.
5. Measured service
Het gebruik van resources kan gemonitord, gecontroleerd en gerapporteerd worden. In de praktijk betekent dit dat resources ook apart afgerekend kunnen worden. Dat biedt afnemers een hoge mate van transparantie.

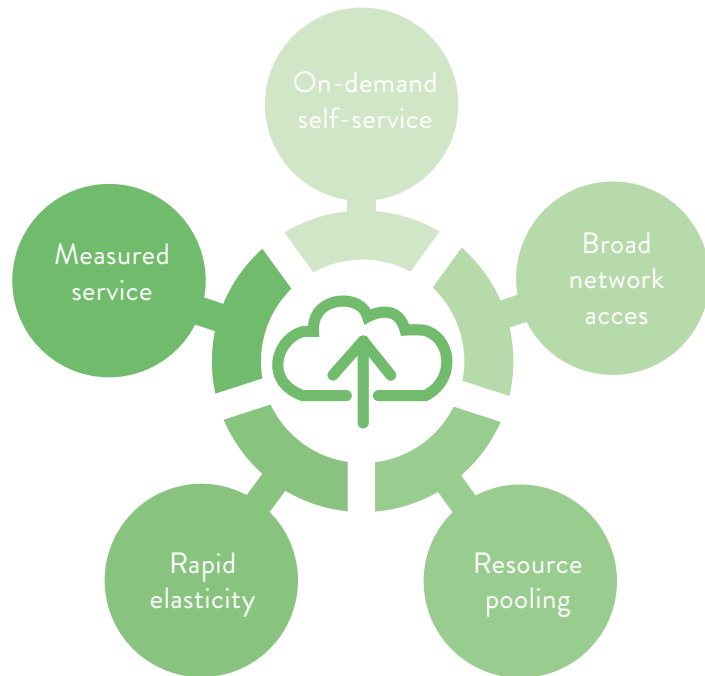


Figure 1: Essentiële kenmerken cloud

1.3 De drie servicemodellen voor cloud-services

Automation can be seen as a subset of orchestration. The table below shows some characteristics of automation and orchestration.

1. Infrastructure as a Service (IaaS)

Bij IaaS levert de leverancier van de cloud-service (de CSP, of cloud service provider) uitsluitend de compute, network en storage resources. De configuratie van het operating system en de bovenliggende applicaties en services laat hij over aan de gebruiker. *Amazon EC2* is hier een voorbeeld van.

2. Platform as a Service (PaaS)

In dit servicemodel levert de CSP de benodigde infrastructuur, het operating system én services, maar laat de configuratie van de applicaties over aan de gebruiker. *Azure IIS* is een voorbeeld van dit model.

3. Software as a Service (SaaS)

In het SaaS-model wordt de gebruiker totaal ontzorgd. Hij consumeert de dienst als applicatie en hoeft zich daarbij over de infrastructuur of platformdiensten niet druk te maken. Hiervan is het product van *Salesforce* een bekend voorbeeld.

1. Cloud provider levert hardware en virtualisatielaag
2. Afnemer is verantwoordelijk voor OS, applicatie en diensten

1. Cloud provider levert hardware-, virtualisatie- en middlewarelaag
2. Afnemer is verantwoordelijk voor configuratie applicatie en diensten

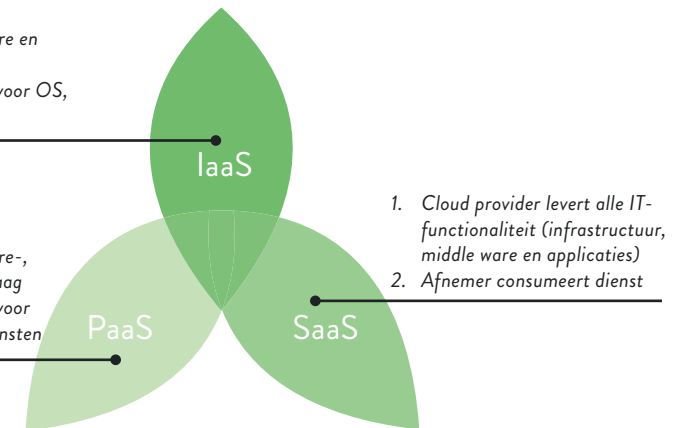


Figure 2: Servicemodellen cloud

1.4 De vier implementatiemodellen voor cloud-services

1. Public cloud

De public cloud is voor iedere internetgebruiker beschikbaar. De ontwikkeling en het beheer ervan liggen bij een externe partij. Voorbeelden van public clouds zijn Amazon Web Services (AWS) en Azure Cloud van Microsoft. Gebruikt een organisatie meerdere public clouds? Dan spreken we van een multi cloud.

2. Community cloud

Een community cloud wordt gebruikt door meerdere organisaties die vanwege compliance, security of andere beperkende maatregelen een eigen omgeving willen gebruiken. Een voorbeeld is de Rijkscloud. Die wordt door verschillende overheidsorganisaties gebruikt, en voldoet aan specifieke eisen op het gebied van compliance en security waar een public cloud niet aan voldoet.

3. Private cloud

In een private cloud is de cloud-infrastructuur uitsluitend bedoeld voor één organisatie. Aanschaf, beheer en gebruik liggen dan ook bij één entiteit. De locatie kan in een eigen datacenter zijn (on-premises) of off-premises bij een co-locatieprovider (bijvoorbeeld Equinix).

4. Hybrid cloud

Een hybrid cloud bestaat uit een combinatie van bovenstaande modellen. Er is bijvoorbeeld sprake van een hybrid cloud als een organisatie een private cloud heeft, en daarnaast gebruik maakt van een public cloud.

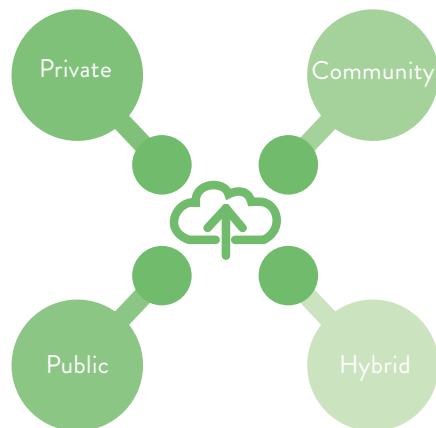


Figure 3: Deploymentmodellen cloud

2

CONNECTIVITEIT

CONNECTIVITEIT

In dit hoofdstuk gaan we in op de connectiviteit van de verschillende implementatiemodellen. De community cloud behandelen we niet apart, omdat die qua infrastructuur en netwerkaspecten nauwelijks afwijkt van public clouds.

2.1 Public cloud

Voor- en nadelen van de public cloud

Er is een aantal belangrijke verschillen tussen connectiviteit in een public cloud en connectiviteit in traditionele architecturen. In de eerste plaats hebben gebruikers in public clouds geen inzicht in de onderliggende infrastructuur. De opties voor beheer of troubleshooting zijn dus beperkt. Daarnaast vindt communicatie in de cloud standaard plaats op basis van gerouteerd IP-verkeer. Dat kan gevolgen hebben voor het koppelen van virtuele machines of databaseclusters. Die zijn vaak gebaseerd is op niet-gerouteerd verkeer.

Verder vereisen netwerk appliances (zoals firewalls) in de cloud ook dedicated resources in de cloud. Dat heeft vaak impact op de kosten. Tot slot geldt voor de meeste public clouds dat tenants alleen via aparte gateways te koppelen zijn. Ze zijn IP-technisch immers aparte, gescheiden omgevingen. Verkeer tussen deze omgevingen wordt beschouwd als extern verkeer, en moet ook als zodanig worden afgerekend.

Toegang tot de public cloud

De toegang tot een public cloud kan op vier manieren worden ingericht:

1. Via het internet, waarbij de public cloud-diensten direct worden afgenomen. In de meeste gevallen is dit op basis van HTTPS/TLS: een beveiligde verbinding via de webbrowser, gebaseerd op certificaten.
2. Via een VPN-connectie over het internet. Een VPN is een virtueel private network: een beveiligde verbinding tussen twee punten over een onbeveiligd netwerk. In dit geval wordt er in de afgesloten tenant van de gebruiker een VPN-gateway opgezet, die toegang geeft tot de public cloud. Dit kan bijvoorbeeld met een zogenoemde client VPN-oplossing. De gebruiker zet dan vanaf een eigen device een beveiligde verbinding op.

3. Een alternatief voor optie 2 is een site-to-site VPN. Daarbij wordt vanaf een firewall in de eigen omgeving een VPN naar de public cloud opgezet. In beide gevallen verzorgt de internetkoppeling de connectie met de public cloud.
4. Via een directe verbinding vanaf de on-premises locatie naar de co-locatie van de CPS. Dit type connectie staat bij verschillende cloud-providers bekend onder verschillende namen:
 - Azure (Microsoft): ExpressRoute
 - AWS (Amazon): DirectConnect
 - GCP (Google): Cloud Interconnect

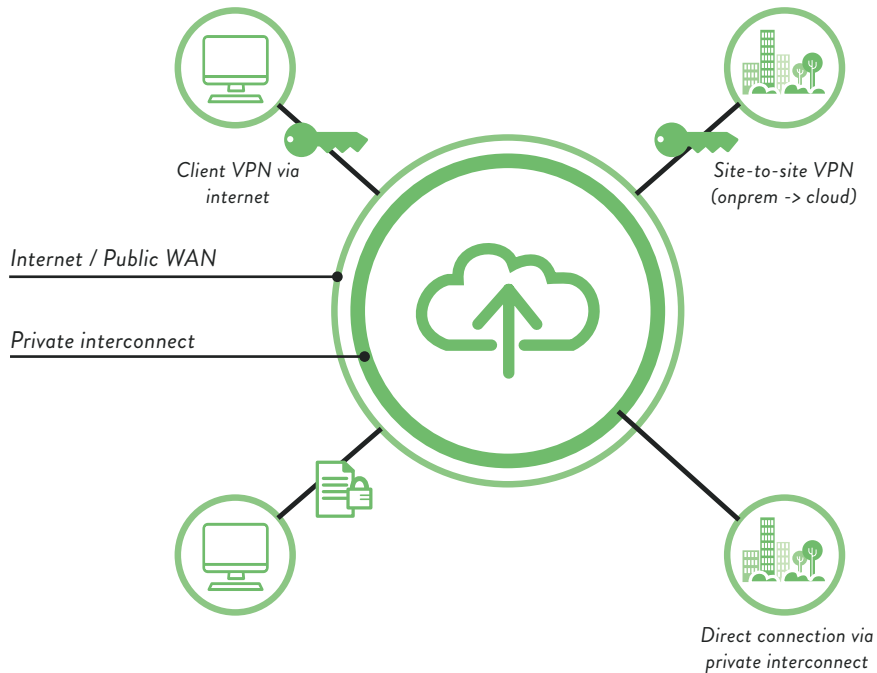


Figure 4: Toegangsmodellen public cloud

Kiezen voor een toegangsmodel

Welk toegangsmodel het meest geschikt is voor een organisatie, hangt af van verschillende factoren. Het gebruikte servicemodel (IaaS, PaaS of SaaS) is daar één van, net als het type internet-ontsluiting in een organisatie, en het aandeel van hybride cloud-diensten in de gehele IT-strategie. Als de cloud direct via internet wordt afgenomen, is ook nog van belang of dat via HTTPS (TLS) kan. Het flowdiagram in Figuur 5 toont de samenhang tussen die factoren, en kan helpen om een toegangsmethode te kiezen.

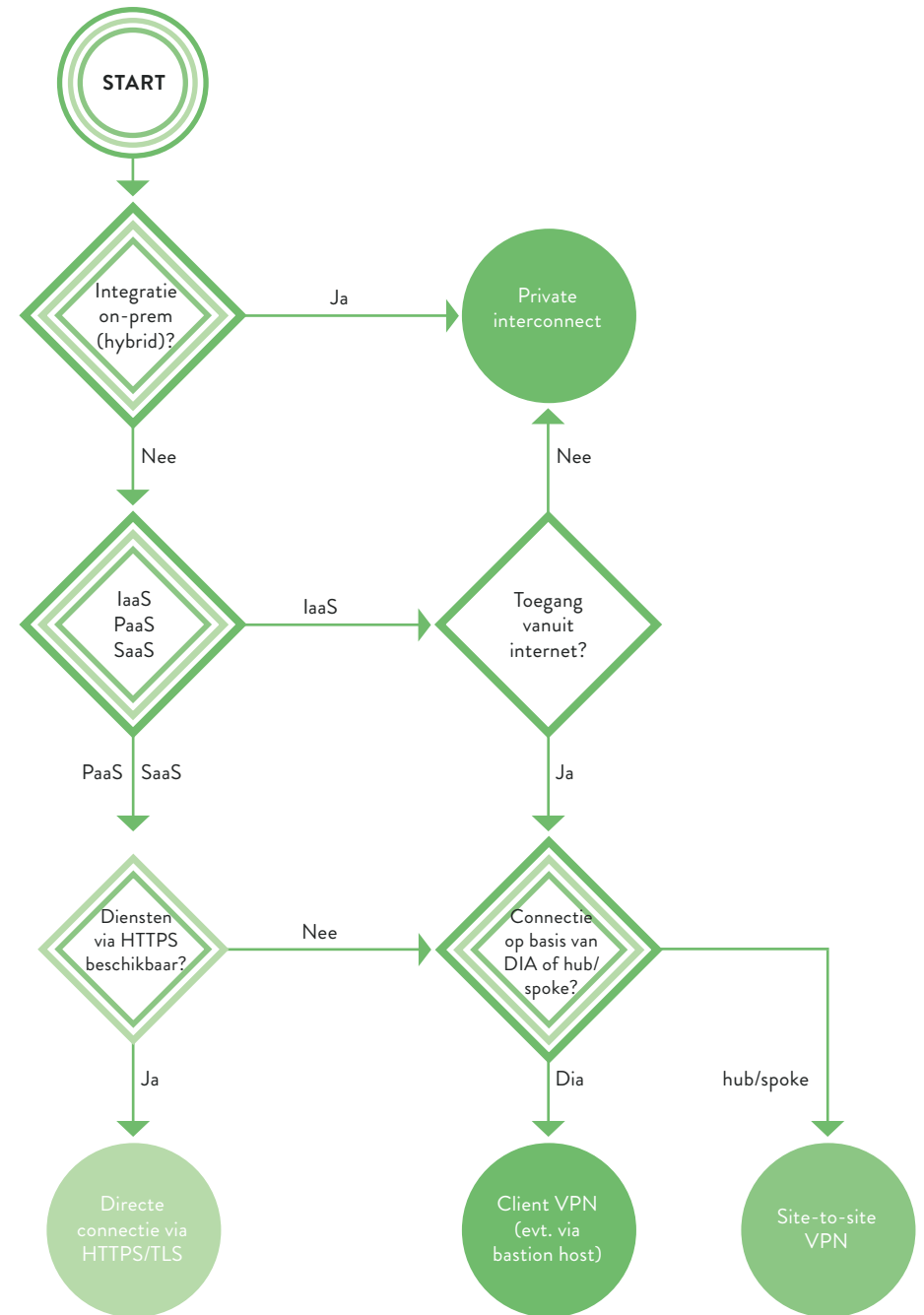


Figure 5: Flow diagram toegangsmethode public cloud

Connectiviteit binnen de public cloud

Binnen de public cloud is het uitgangspunt de tenant. Daar worden de netwerk- en connectiviteitspolicy bepaald. Verschillende aanbieders gebruiken verschillende termen voor de tenant, maar in essentie is de 'virtual private cloud' het basis-compartiment waarbinnen IP-adressering, DNS en (netwerk-)security geconfigureerd worden. Tabel 1 geeft een overzicht van de belangrijkste eigenschappen van de belangrijkste connectiviteit elementen.

Connectiviteitservices	
IP-adressering	<ul style="list-style-type: none"> • Publieke reeksen (via internet bereikbare IP-adressen) worden gealloceerd door de cloud provider. • RFC1918 (private) reeksen (IP-adressen voor intern gebruik) worden door de gebruiker geconfigureerd in de tenant-configuratie. In beide gevallen regelt de cloud-provider de daadwerkelijke toewijzing.
DNS	<ul style="list-style-type: none"> • Bij publieke IP-adressen verzorgt de cloud-provider vaak de DNS-diensten. • Het is ook mogelijk om publieke en interne services beschikbaar te stellen onder een domeinnaam in eigen beheer. • Een andere optie is het gebruik van een DNS-server in eigen beheer, in een public cloud.
Firewalling	<ul style="list-style-type: none"> • Security op IaaS niveau is over het algemeen geregeld met zogenoemde security groups. Het belangrijkste verschil met traditionelere segmentering is dat dit per workload, VM of applicatie is geregeld - en niet per IP-netwerk. Dit zorgt voor een fijnmaziger beveiliging. • Ook in de public cloud is het mogelijk om traditionele firewalls van vendors als Checkpoint, Palo Alto of Fortinet in te zetten. De firewall wordt dan in gevirtualiseerde vorm aangeboden, en kan als gateway worden ingezet in een tenant. Dit heeft soms de voorkeur omdat zo alle firewalls in een organisatie (zowel on-premises als off-premises) via één managementlaag beheerd kunnen worden.

Connectiviteitservices

Loadbalancing

- Als er meer opslagruimte of rekenkracht gevraagd wordt in de organisatie, schaalde de cloud automatisch op. Bijvoorbeeld door extra servers in te schakelen. Het inkomende verkeer moet dan natuurlijk nog wel op een effectieve manier verdeeld worden. Dat is de rol van de loadbalancer. Cloud-providers bieden standaard loadbalancers aan, die in de meest basale variant zelfs gratis zijn. Voor geavanceerdere moet vaak wel betaald worden.
- Traditionele vendors als F5 Networks leveren ook cloud-gebaseerde varianten van hun loadbalancers. Daarnaast zijn er ook cloud-only vendors, zoals AVI Networks. Er is dus een keuze te maken: gebruikt u een eigen product van de cloud-provider? Of een product van een aparte vendor? Verschillende factoren kunnen een rol spelen bij die afweging. Zo zijn de gebruiksmogelijkheden bij specifieke loadbalancing vendors over het algemeen uitgebreider. Daar staat tegenover dat daar vaak ook hogere kosten bijhoren. En net als bij firewalls, is het soms handiger om het management van meerdere loadbalancers in één overzichtelijke beheersuite te hebben.

2.2 Multi cloud

De voordelen van multi cloud

Organisaties kiezen er geregeld voor om gebruik te maken van meerdere public cloud providers. Daar kunnen verschillende redenen voor zijn. Dit zijn de belangrijkste:

- Best of breed

Het kan zo zijn dat voor verschillende onderwerpen de oplossingen van verschillende cloud-providers het beste bij een organisatie passen. Door niet voor één provider te kiezen, houden organisaties toegang tot de best mogelijke oplossing op elk gebied.

- Minimaliseren van vendor lock-in

Het afnemen van alle cloud-applicaties bij één leverancier verhoogt het risico op vendor lock-in. Een organisatie kan dan niet meer makkelijk van leverancier veranderen omdat dat teveel kosten of ongemak met zich meebrengt. Dat kan de flexibiliteit en de innovatiekracht van een organisatie op lange termijn schaden.

- Redundantie

Als de systemen van één cloud-provider uitvallen, is het prettig als uw organisatie moeiteloos over kan schakelen op een andere provider. Cloudgebaseerde applicaties zijn daar ook bij uitstek geschikt voor. Ze kunnen prima autonoom en over meerdere IT-domeinen en cloud-omgevingen functioneren.

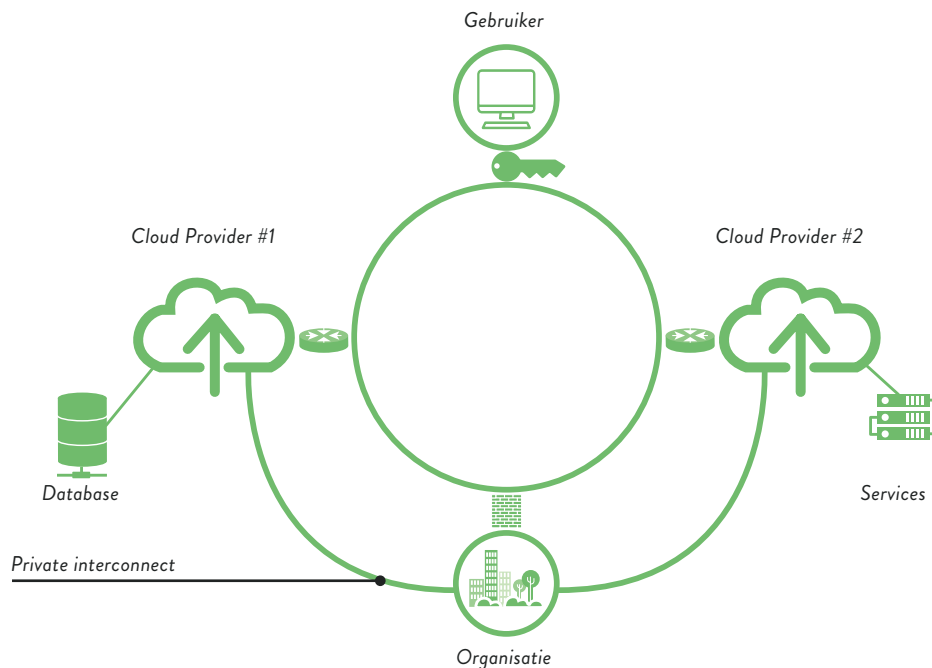


Figure 6: Multi cloud omgeving

De nadelen van multi cloud

- Kosten

Meer betekent vaak duurder - en dat is in de cloud niet anders. Zeker als modules van applicaties over meerdere cloud-omgevingen verdeeld worden, kunnen de kosten voor verkeer van en naar de cloud oplopen. Daarnaast kunnen er extra kosten verbonden zijn aan private interconnects naar meerdere cloud-omgevingen.

- Latency

De belangrijkste cloud-providers zijn onderling optimaal verbonden, blijkt uit performancemetingen van ThousandEyes uit 2019. Toch is het in een multi cloud belangrijk om applicaties zó te ontwikkelen, dat tijdelijke verbindingproblemen geen negatieve impact op de performance van de hele applicatie hebben.

- Beheer

Het gebruik van een multi cloud maakt het automatisch complexer om de netwerktopologie, de eventuele interconnects en de bijbehorende security policies beheersbaar te houden. Er zijn wel partijen (zoals Aviatrix en Alkira) die dit probleem kunnen oplossen met een integrale toepassing.

2.3 Private cloud

De voordelen van een private cloud

Een private cloud biedt dezelfde voordelen als andere cloud-vormen, maar mét extra zekerheid, beheer in eigen hand en voorspelbare kosten. Het platform draait immers op een eigen (co-)locatie, en de data staat dus in een gecontroleerde omgeving. In sommige use-cases is dat een vereiste. Organisaties met een streng security-beleid willen of mogen soms absoluut geen gebruik van maken van de public cloud. Voor veel andere organisaties is de inzet van een private cloud de eerste stap naar een hybride model, waarbij ze zowel public als private cloud-diensten gebruiken. AWS en Azure bieden zelfs producten aan met dezelfde look-and-feel als hun publieke diensten, maar dan in een private vorm. Zo is een mogelijke latere migratie naar de public varianten van deze providers makkelijk te maken.

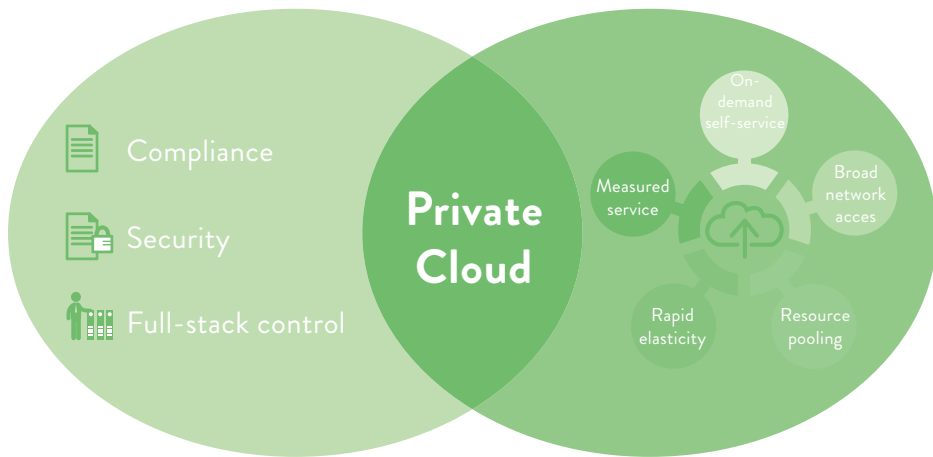


Figure 7: Private cloud; Combinatie van on-premises zekerheid en cloud voordelen

Connectiviteit in de private cloud

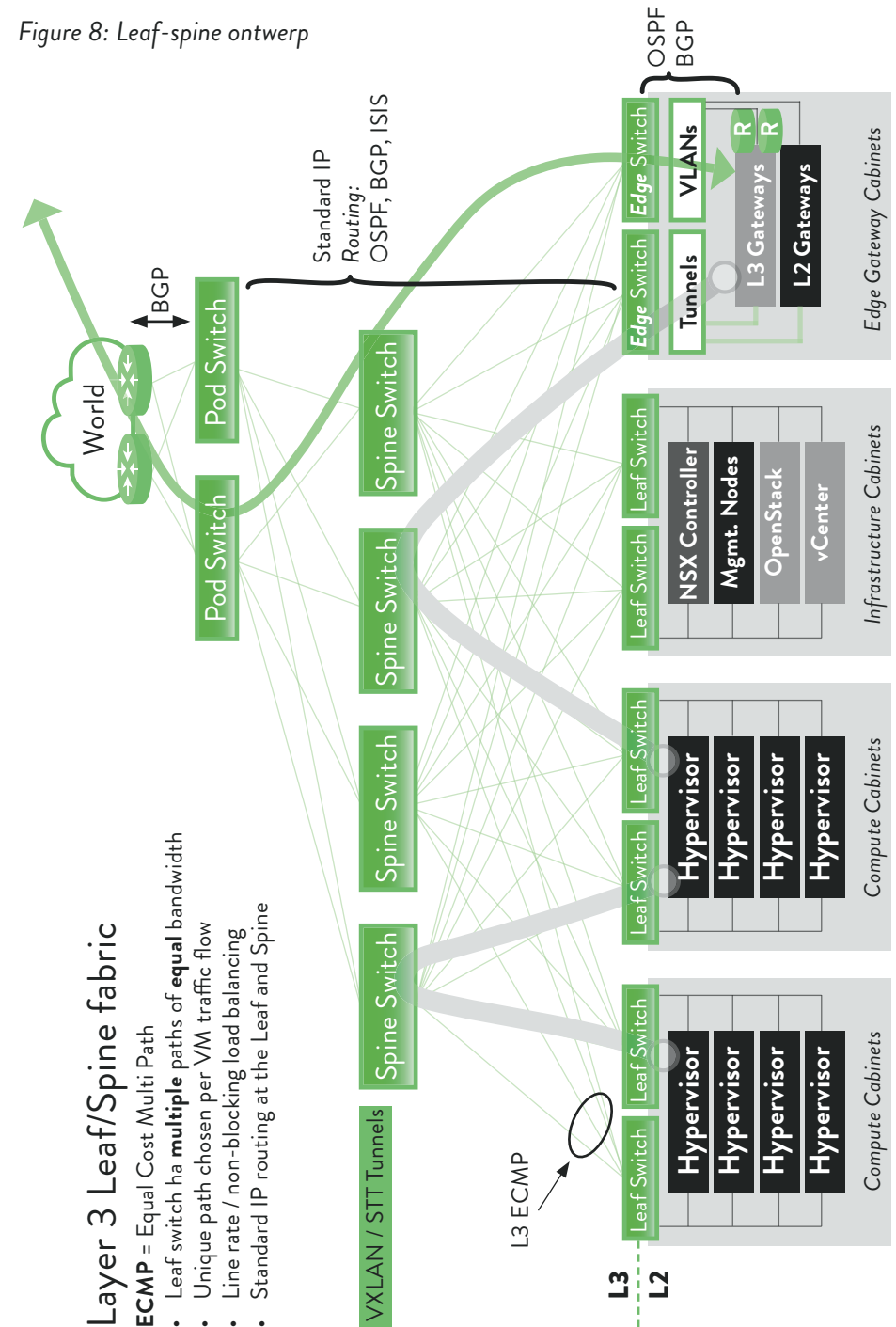
In een private cloud heeft de gebruiker veel controle. Hij bepaalt in sterke mate zelf hoe de omgeving opgebouwd is. Dat geldt zowel voor de fysieke topologie (underlay) als de virtuele netwerkinfrastructuur (overlay). Het underlay-netwerk is er vaak op gericht om zoveel mogelijk bandbreedte te bieden, en geoptimaliseerd voor oost-westverkeersstromen. In de praktijk is hiervoor een leaf-spine ontwerp (Figuur 8) het meest geschikt. Dat biedt de meeste schaalbaarheid en doorvoersnelheid.

Dit ontwerp heeft als groot voordeel dat het geoptimaliseerd is voor oost-westverkeer, wat zich kenmerkt door veel intra-host verkeer in hetzelfde segment. Het aantal hops tussen hosts is op elke plek in de topologie gelijk (equidistant), daardoor levert dit model de beste performance voor oost-westverkeersstromen.

De meeste private cloud-architecturen zijn op basis van dit model gebouwd. Alhoewel er geen technische beperking is om een private cloud-omgeving op basis traditionelere architecturen te bouwen, is met name de schaalbaarheid een belangrijke beperking van klassiekeren ontwerpen.

Over het algemeen gedraagt een private cloud zich qua netwerkdiensten vrijwel hetzelfde als een traditionele omgeving. De private cloud-omgeving kan ingericht worden als een aparte 'pod': een module van waaruit (netwerk) diensten worden geleverd. Die pod heeft dan een eigen architectuur, die uitgangspunten als schaalbaarheid, flexibiliteit en elasticiteit ondersteunt.

Figure 8: Leaf-spine ontwerp



2.4 Hybrid Cloud

De voordelen van een hybrid cloud

Een hybrid cloud is een combinatie van een private cloud en een public cloud infrastructuur. Wij weten uit ervaring: de meeste organisaties maken gebruik van de hybrid cloud. En met reden. De public cloud wordt vaak gebruikt om nieuwe workloads te activeren (deze vorm is dan ook populair bij ontwikkelaars die snel iets willen activeren in de public cloud). Ook wordt de public cloud vaak gebruikt als extra capaciteit voor de private cloud, die on-demand kan worden op- en afgeschaald.

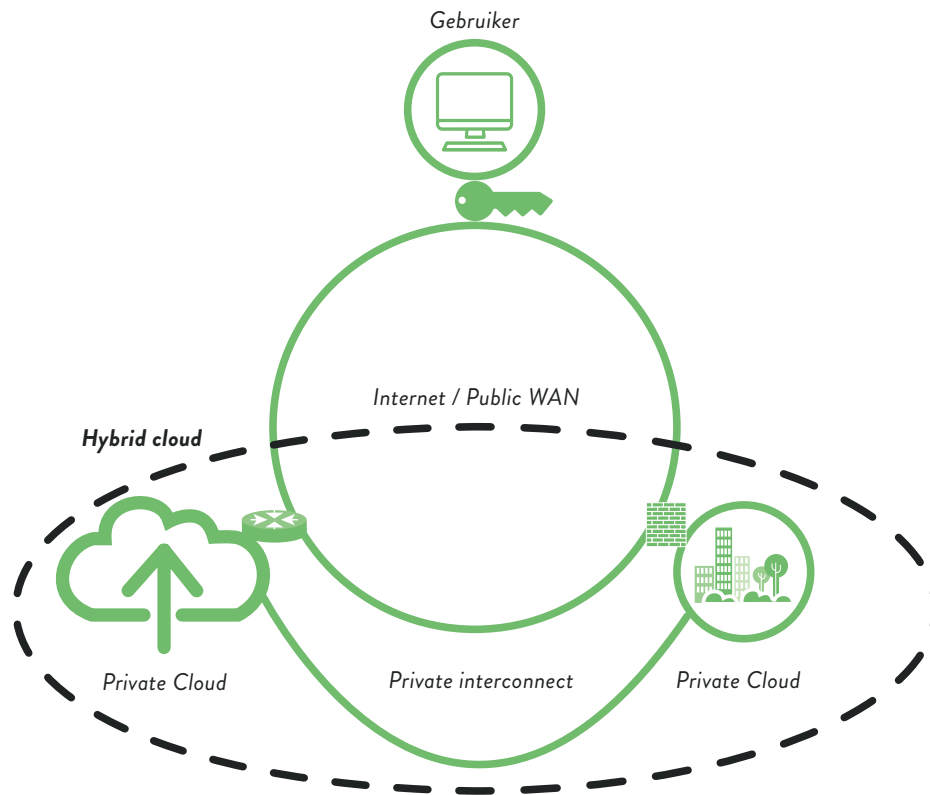


Figure 9: Hybrid Cloud

Connectiviteit in de hybrid cloud

De hybrid cloud biedt grote voordelen, maar is qua connectiviteit wel complex. We benoemen een aantal complicerende factoren:

- Intern of extern?
Organisaties met een private én een public cloud-omgeving moeten heel helder hebben wat als 'intern' of als 'extern' beschouwd wordt. En vooral: welke beveiligingsmaatregelen daarvoor gelden. Vaak beschouwen organisaties de public cloud als een extensie van hun eigen infrastructuur. In dat geval moeten er vaak flinke beveiligingsmaatregelen getroffen worden in de public cloud.
- Sommige organisaties kiezen ervoor om de public cloud als een apart security domein te zien, en leggen een demarcatie aan tussen private en public cloud. Verkeersstromen die via deze demarcatie lopen, moeten dan wel expliciet gefilterd worden. Dat kan de flexibiliteit van de cloud negatief beïnvloeden.
- Door de laagdrempeligheid van de cloud is het risico op onbedoelde internettoegang aanzienlijk. De internettoegang voor cloud workloads moet dan ook helder en veilig geïmplementeerd worden. Alleen zo is te voorkomen dat er via cloud workloads security-incidenten ontstaan.

3

CLOUD AUTOMATION

CLOUD AUTOMATION

De flexibiliteit is één van de grootste voordelen van de cloud. Maar om daar maximaal van te kunnen profiteren, moet een cloud-strategie wel gepaard gaan met een duidelijk plan op het gebied van standaardisering én automatisering.

Automatisering speelt een steeds grotere rol binnen IT-organisaties. Logisch, want geautomatiseerde productie is sneller en minder foutgevoelig dan handmatige acties. Bovendien biedt ze een goede basis voor verdere innovatie. Bijvoorbeeld door het versnellen van kernactiviteiten of door het aanbieden van diensten via volledige selfservice portals.

Zo is automatisering ook een krachtige methode om de flexibiliteit en schaalbaarheid van een cloud-omgeving maximaal in te zetten. Het dynamische consumptiemodel van een cloud leent zich bij uitstek voor het inzetten van automatisering. Met verschillende tools en producten kunt u de cloud aanspreken als één grote resource pool. En kunt u binnen die omgeving netwerken, servers en applicaties automatisch implementeren, configureren en beheren.

Hieronder gaan we in op het kiezen van de juiste tools, de voordelen van Infrastructure as Code, en op het creëren van consistentie in de werkomgeving – ook als ontwikkelingen snel gaan.

3.1 Toolselectie: wat past bij uw organisatie?

Er zijn legio tools beschikbaar die kunnen assisteren bij het automatiseren van de huidige business-logica. De grootste cloud-providers hebben deze automation tooling zelfs al ingebouwd. Zo biedt Amazon bijvoorbeeld CloudFormation, en heeft Azure op zijn beurt Resource Templates. Cloud-specifieke tools bieden logischerwijs het hoogste niveau van integratie met hun platforms, maar ze zijn moeilijker inzetbaar bij een multi cloud-strategie. Daarnaast zijn er ook tools als Terraform en Pulumi, die er juist op gericht zijn om infrastructuur onafhankelijk van de onderliggende cloud-provider te implementeren.

De werkwijze van iedere tool is ongeveer hetzelfde. De infrastructuur wordt eerst gedefinieerd in een template. Vervolgens berekent de tool de benodigde

stappen om de gewenste infrastructuur uit te rollen, aan te passen of zelfs te verwijderen. Vervolgens voert de tool zo optimaal mogelijk de wijzigingen uit. Het gros van de producten definieert een eigen Domain Specific Language (DSL) waarin de gewenste configuratie (desired state) wordt vastgelegd, een concept dat Infrastructure as Code wordt genoemd. Hierover later meer. Deze desired state wordt vervolgens naar de devices of de cloud gestuurd.

Stateless of stateful tooling?

Natuurlijk zijn er ook verschillen tussen tools. Sterker: er is een duidelijke fundamentele tweedeling. Zo werken reguliere tools voor configuratiemanagement als Ansible, Chef en Puppet op basis van een stateless model, terwijl tooling als Terraform op basis van een stateful model werkt. Het belangrijkste verschil is dat stateless tools geen data bewaren, en dus bij iedere deployment de infrastructuur moeten bevragen op de huidige 'state'. Deze tools hebben dus niet voortdurend een totaalbeeld van de infrastructuur. Dat maakt vooral rollbacks lastig. Daarbij worden delen van de infrastructuur of configuratie verwijderd, en zonder een volledig overzicht is het moeilijk om te beoordelen welke componenten afhankelijk zijn van elkaar.

Bij stateful tools wordt de huidige staat van de infrastructuur helemaal vastgelegd in een bestand. Toekomstige wijzigingen zijn dus verschillen met de al bekende state, en alle afhankelijkheden tussen componenten zijn bekend. Daardoor gaat het uitrollen van nieuwe infrastructuur sneller, én zijn er voordelen bij een rollback. Een bijkomend voordeel in een stateful scenario is dat een configuratie over meerdere devices, toch vastgelegd is op één centrale plek. Dat kan van belang zijn bij deployments die uit meerdere componenten bestaan.

Ons advies: kies de combinatie

Hoewel stateful tooling dus veel voordeliger lijkt, zijn het met name stateless tools die uitblinken in het in detail configureren van één component. En hoewel beide soorten producten ingezet kunnen worden om de totale infrastructuur uit te rollen, adviseren we vrijwel altijd een combinatie. Gebruik bijvoorbeeld stateful tooling om de infrastructuurcomponenten uit te rollen, en stateless tools voor het beheer van de configuratie van individuele devices. Ter illustratie: in Figuur 10 is de tweedeling van deze tools weergegeven.

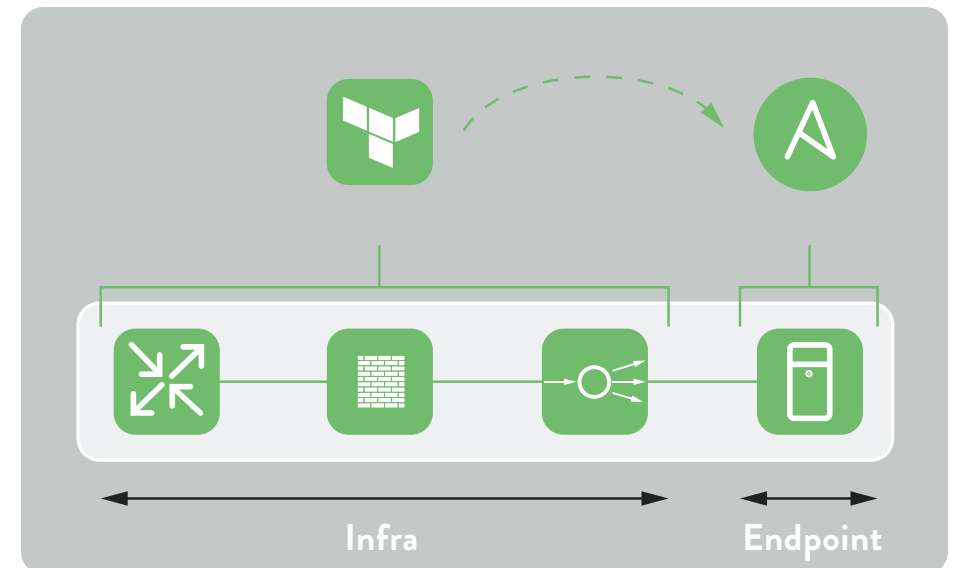


Figure 10: Stateful tooling is bij uitstek geschikt voor het configureren van infra-ketens, waar stateless tooling juist uitblinkt in endpoint configuratie

Naast de eerdergenoemde verschillen zijn er drie zaken die de moeite van het afwegen waard zijn bij de keuze voor tooling. In de eerste plaats is het wijs om te verdiepen in de support vanuit de vendor. Daarnaast is vooral het draagvlak van het product in de online community van belang. Hoe meer het product ingezet wordt, hoe meer kant-en-klare oplossingen er publiekelijk beschikbaar zijn op internet. En tot slot is het draagvlak voor een tool binnen uw eigen organisatie natuurlijk belangrijk. Want hoewel vrijwel iedere tool een eigen taal (DSL) definieert, is er wel een duidelijk verschil in de moeilijkheidsgraad én in de initiële leercurve.

3.2 Infrastructure as code: weg met menselijke fouten

Bij het overstappen naar nieuwe tooling om de infrastructuur aan te spreken past ook een nieuwe manier van werken. En wel een waarbij de IT-omgeving op een logische wijze in code is gedefinieerd. Dat is wat Infrastructure as Code (IaC) inhoudt. Een belangrijke eigenschap daarvan is dat de set commando's of procedures om een omgeving uit te rollen, is vastgelegd in code. Dat maakt het mogelijk om relatief eenvoudig, aan de hand van enkele regels, en herhaaldelijk een volledige infrastructuur te implementeren. En dat is weer efficiënt voor het aanmaken van identieke ontwikkel-, acceptatie- en productieomgevingen. Of bijvoorbeeld voor het realiseren van een migratie tussen cloudproviders.

Bij IaC worden infrastructuurcomponenten letterlijk beschreven als objecten met individuele eigenschappen. Ter illustratie: in het voorbeeld in Figuur 11 wordt een netwerk binnen Azure gespecificeerd.

```
resource "azure_virtual_network" "example" {
  name          = "virtualNetwork1"
  location      = azure_resource_group.example.location
  resource_group_name = azure_resource_group.example.name
  address_space = ["10.0.0.0/16"]
  dns_servers   = ["10.0.0.4", "10.0.0.5"]

  [...]

  subnet {
    name          = "subnet1"
    address_prefix="10.0.1.0/24"
  }
}
```

Figure 11: Voorbeeld Terraform resource

Door deze resource vast te leggen in code, en hem geautomatiseerd uit te rollen, verdwijnt de kans op menselijke fouten bij het uitvoeren van configuraties of updates. Daarnaast is het veel eenvoudiger om het totaaloverzicht van de infrastructuur te houden.

Eenvoudiger, sneller en altijd te herstellen

IaC maakt ook versiebeheer eenvoudiger. Door de code op te nemen in versiebeheerssoftware als Git of SCM zijn wijzigingen immers traceerbaar en herhaalbaar. Ook gaat de snelheid van nieuwe implementaties aanzienlijk omhoog. Het aanmaken van een nieuw netwerk is immers slechts een relatief kleine wijziging op de al bestaande configuratie. En het verwijderen van een hele omgeving vraagt slechts het weghalen van enkele regels code. Zijn de wijzigingen uiteindelijk toch niet naar wens? Dan kunt u altijd terug in de tijd door de code weer te herstellen in zijn originele staat. Die optie ontbreekt bij handmatig beheer vrijwel altijd.

3.3 CI/CD: gegarandeerde consistentie

Wie infrastructuur behandelt als code, kan ook de best practices van softwareontwikkeling toe gaan passen. Denk bijvoorbeeld aan automatische tests, versiebeheer, build automation en automated deployments. Hiermee kunt u de kwaliteit en voorspelbaarheid van de omgeving beter waarborgen. Veel van die concepten vinden hun oorsprong in de softwarewereld. Ze worden vaak gecombineerd in geautomatiseerde stappen. Deze reeks aan geautomatiseerde stappen wordt ook wel een Continuous Integration/Continuous Delivery (CI/CD) pipeline genoemd.

Zo'n pipeline is over het algemeen een lineair proces, dat de code voorafgaand aan een nieuwe release test (CI), en als de tests goed bevonden zijn, de wijziging klaarzet voor productie (CD). Zodra een team codewijzigingen in de infrastructuur heeft doorgevoerd in versiebeheer, gaat automatisch een pipeline draaien die alle stappen doorloopt. Over het algemeen zijn CI/CD-platforms self-hosted óf een SaaS-product. Tools als Jenkins en Gitlab CI zijn bijvoorbeeld populaire self-hosted producten om pipelines in te definiëren. Cloudproviders als AWS en Azure bieden ook een eigen SaaS-oplossing.

De overtreffende trap van CI/CD is Continuous Deployment. Hierbij worden de geteste wijzigingen ook direct doorgevoerd in de productieomgeving. Toch is het zeker voor bedrijven die net starten met IaC en CI/CD raadzaam om deze laatste stap in de keten handmatig door te voeren. Zo zit er altijd nog een menselijke check op het eindproduct.

De kwaliteit van een deployment hangt natuurlijk wel af van de kwaliteit van de tests. En hoewel het uitrollen van nieuwe infrastructuur dus niet meer handmatig gebeurt, verschuift de werklast van troubleshooting achteraf, dus naar testontwikkeling vooraf. Dat is arbeidsintensief, maar wel veiliger op de lange termijn. En het grootste voordeel is dat consistentie in de omgeving gegarandeerd is.

4

TOT SLOT: ROUTZ
HELPT U GRAAG!

TOT SLOT: ROUTZ HELPT U GRAAG!

Zaken als werken in de cloud, automation en CI/CD pipelines zijn niet meer weg te denken uit moderne IT-organisaties. De uitdaging is om gefundeerde keuzes te maken over de manier waarop u uw bedrijfsdoelstellingen, en daarmee ook uw IT-doelstellingen, wilt realiseren. Nu, en in de toekomst.

De kans is groot dat uw IT-landschap bestaat uit een traditionele architectuur, die op een slimme en effectieve manier met de cloud gekoppeld moet worden. Of wellicht wilt u maximaal inzetten op het afnemen van clouddiensten, en zal dus een gedeelte van uw huidige landschap moeten verdwijnen. In alle gevallen geldt: het fundament is van vitaal belang.

Routz is dé kennisorganisatie op het gebied van netwerk- en ICT-infrastructuren. Wij weten als geen ander dat het bepalen van de juiste cloud-strategie geen eenvoudige opgave is. Als onafhankelijke en neutrale partij ondersteunen we u daar graag bij, en helpen we u de juiste keuzes voor uw organisatie te maken. Als u wilt, ontzorgen we uw organisatie naar een beheerde en beheersbare infrastructuur. Zowel in uw eigen omgeving, als in de cloud. En altijd vanuit de business, via design én implementatie.



Praecellenti
The Network Academy