

Richtlijnen en voorwaarden Cloud

Eigenaar	ProRail ICT Cloud Center of Excellence
Auteur	Maurice Endhoven
Reikwijdte	ProRail breed (inclusief Leveranciers)
Kenmerk	Richtlijnen en voorwaarden Cloud
Versie	1.1
Datum	18 mei 2020
Bestand	Richtlijnen en voorwaarden Cloud 1.1
Status	Goedgekeurd

Dit document heeft een beperkte houdbaarheid. De laatste goedgekeurde versie is te vinden op: https://prorailbv.sharepoint.com/teams/dc2015_0001/Documenten/Forms/AllItems.aspx

Informatieclassificatie Intern + Contractpartners

Inhoudsopgave

1	Inleiding	3
2	Richtlijnen, uitgangspunten, eisen	3
2.1	“SaaS boven PaaS boven IaaS”	3
2.2	Gebruik ProRail Azure Cloud	3
2.3	Alles is code en uitrol is geautomatiseerd	4
2.4	ProRail Azure DevOps en ontwikkelomgeving (OTAP)	4
2.5	Beheer van de cloudoplossing	5
2.6	Security richtlijnen	5
2.7	Connectiviteit	6
3	ProRail Azure Cloud	8
3.1	Subscriptions	8
3.2	Netwerk	8
3.3	Naamconventie	10

1 Inleiding

Dit document beschrijft de richtlijnen waar aanbieders van cloudoplossingen rekening mee moeten houden en de voorwaarden waaraan de technische oplossing moet voldoen om te kunnen worden opgenomen in de ProRail public cloudomgeving.

Het doel van dit document is in een zo vroeg mogelijk stadium te waarborgen dat cloudoplossingen veilig en beheersbaar binnen het applicatielandschap van ProRail kunnen worden opgenomen.

Onder “cloudoplossing” wordt verstaan het geheel aan applicatiefunctiealiteit en alle daarbij gebruikte clouddiensten (app hosting, opslag, database etc) dat als één geheel wordt geleverd en als één geheel in productie en onder beheer gebracht moet worden.

Dit is een levend document en zal regelmatig geactualiseerd worden door het ProRail Cloud Center of Excellence (CCoE) en worden gepubliceerd op IV plaza.

2 Richtlijnen, uitgangspunten, eisen

2.1 “SaaS boven PaaS boven IaaS”

Er zijn drie delivery modellen van Cloud Computing te onderscheiden, te weten:

- Software as a service (SaaS)
- Platform as a service (PaaS)
- Infrastructure as a service (IaaS)

Voor de keuze volgens welk model de cloudoplossing wordt geleverd hanteert ProRail het uitgangspunt “SaaS boven PaaS boven IaaS”.

De cloudoplossing dient bij voorkeur als SaaS te worden aangeboden, waarbij er dus geen maatwerk en technische regie/beheer door ProRail nodig is. Dit betreft dus ook de configuratie van de SaaS dienst t.b.v. ProRail gebruik.

Indien er sprake is van maatwerk en SaaS dus geen optie is, moet de cloudoplossing zoveel mogelijk middels PaaS diensten geleverd worden.

Het gebruik van IaaS diensten, zoals virtual machines, heeft niet de voorkeur, gezien de extra beheerlast t.o.v PaaS dat IaaS met zich meebrengt.

IaaS kan wel worden toegepast voor applicaties die niet continue in gebruik zijn (b.v. in het weekend) of uitgezet kunnen worden totdat ze daadwerkelijk nodig zijn, zoals bijvoorbeeld in een ontwikkel- en testomgeving.

2.2 Gebruik ProRail Azure Cloud

De ProRail Azure Cloud is de public cloudomgeving van waaruit ProRail publieke clouddiensten intern aanbiedt. Op dit moment zijn dat diensten die vanuit Microsoft Azure aangeboden worden.

De ProRail Azure Cloud valt onder de Microsoft Enterprise Agreement van ProRail.

In geval dat de aangeboden cloudoplossing gebaseerd is op Azure PaaS en/of eventuele IaaS diensten, dient de leverancier de oplossing binnen een door ProRail toegewezen en beheerde subscription/resource groep in de ProRail Azure Cloud op te leveren.

ProRail

2.3 Alles is code en uitrol is geautomatiseerd

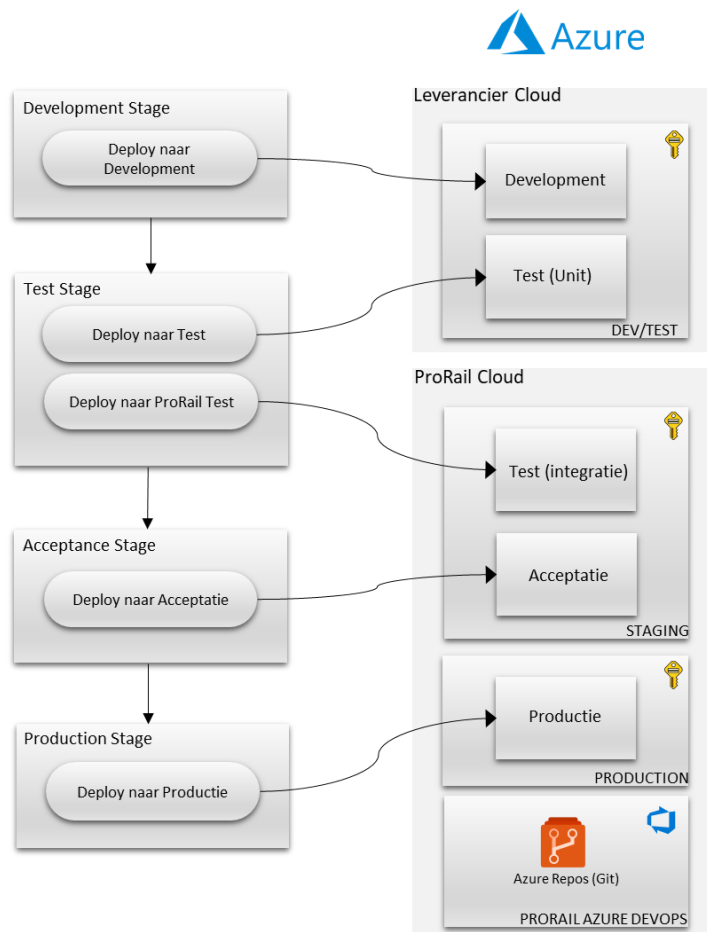
De uitrol van de clouddiensten en de applicatie en diens configuratie is beschreven als code (zoals in scripts en ARM templates) en dient in de productie omgeving volledig geautomatiseerd plaats te vinden.

2.4 ProRail Azure DevOps en ontwikkelomgeving (OTAP)

Als onderdeel van een ontwikkelomgeving biedt Microsoft Azure DevOps ondersteuning aan ontwikkelteams. Deze Cloud service zorgt voor een naadloze integratie met Azure ten behoeve van het uitrollen van applicaties op het Azure platform en zorgt ervoor dat alle informatie centraal opgeslagen staat.

ProRail vereist het gebruik van een door ProRail beheerde instantie van Azure DevOps. ProRail zal binnen deze omgeving een “project” aanmaken voor de leverancier, waarbinnen de ontwikkelactiviteiten kunnen plaatsvinden. Azure Repos is daarbij de centrale plek waar de broncode en ARM templates bewaard worden.

Het is geen vereiste dat de hele ontwikkelstraat binnen de ProRail Azure Cloud wordt gehost. Het is toegestaan dat de leverancier er een eigen development/test omgeving op na houdt. De voortbrenging van applicatie releases door OTAP heen zal dan plaatsvinden volgens onderstaande afbeelding.



2.5 Beheer van de cloudoplossing

De leverancier van de cloudoplossing verzorgt het volledige beheer, inclusief het ontwikkelen van nieuwe functionaliteit, het installeren van nieuwe versies en updates en de beveiliging van de diensten. Gebruikersbeheer kan zowel bij de leverancier als bij ProRail liggen.

2.6 Security richtlijnen

De leverancier van de cloudoplossing moet voldoen aan de volgende security eisen.

- **Aanbieder cloud service moet voldoen aan het ProRail Informatiebeveiligingsbeleid (IBB)**
In IBB-1.6 staan eisen genoemd op het gebied van beveiliging en privacy waaraan een aanbieder van cloud services moet voldoen.
- **Geschiktheid toepassing in de cloud obv risico-analyse (BIV/PIA)**
Voordat een toepassing in de cloud gezet kan worden, dient eerst een risico-analyse uitgevoerd te worden waarin o.a. de risico's met betrekking tot beschikbaarheid, integriteit, vertrouwelijkheid en privacy-waarborgen geanalyseerd moeten worden.
- **Identificatie/Authenticatie/Autorisatie obv ProRail logische toegangsarchitectuur**
Voor de identificatie, authenticatie en autorisatie moet voldaan worden aan ProRail beleid: Logische Toegangsarchitectuur en wachtwoordbeleid, zoals beschreven in de aansluitvoorwaarden ProRail ICT KA.
- **Interne communicatie van en naar internet valt onder de verantwoordelijkheid van ProRail**
Communicatie van en naar Internet dient daardoor via een ProRail entiteit (on-premise of cloud) uitgevoerd te worden. Een uitzondering hierop zijn SAAS diensten, aangezien ProRail daar geen controle op kan uitvoeren.
- **Overeenkomsten afsluiten met leverancier ivm privacy (verwerkers-overeenkomst)**
In het kader van de AVG wetgeving is ProRail te allen tijde verantwoordelijk voor de bescherming van de privacy. Met de cloud-leverancier dienen de benodigde verwerkers-overeenkomsten afgesloten te worden indien er sprake is van verwerking van persoonsgegevens.

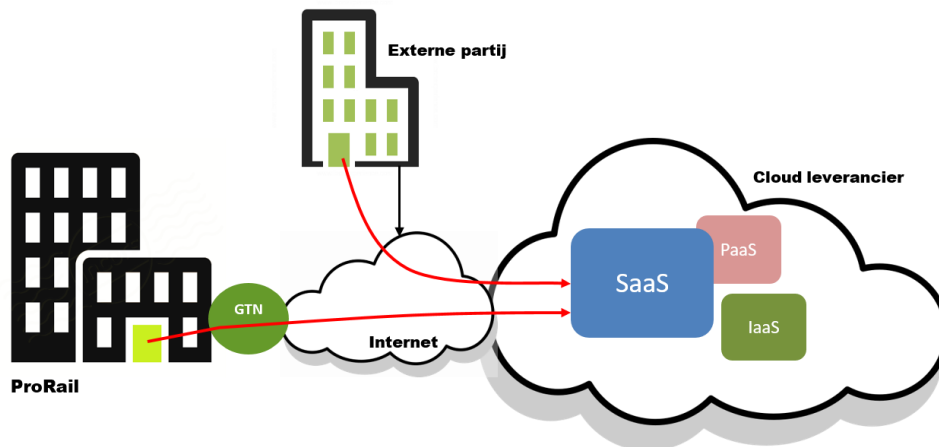
2.7 Connectiviteit

Binnen ProRail ICT onderscheiden we 3 varianten van cloudconnectiviteit. Het gaat hierbij om de netwerkconnectiviteit tussen de locatie waar de afnemer zich bevindt (ProRail kantoor of datacenter) en de locatie waar de clouddienst wordt aangeboden. Hieronder worden de richtlijnen voor gebruik beschreven.

Public Connect

Met name bedoeld voor connectiviteit naar SaaS en PaaS diensten buiten het beheer en netwerkdomein van ProRail.

Gebruikers maken hierbij gebruik van een standaard voorziening voor internet toegang. Voor ProRail gebruikers is dat het Generieke Toegang Netwerk (GTN).



Kenmerken:

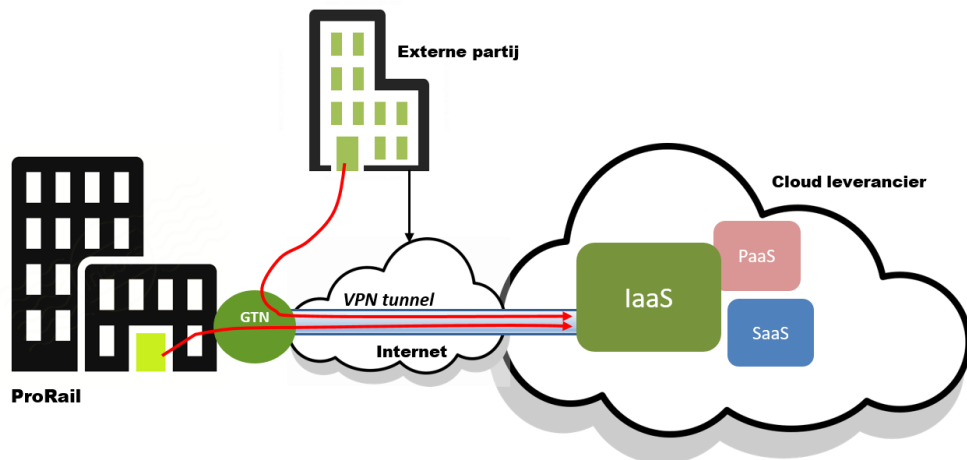
- Verwerking voornamelijk in de cloud
- Eindgebruikers, intern en extern
- Geen of zo weinig mogelijk systeemkoppelingen naar ProRail
- Alleen https
- Maakt gebruik van Internet
- Geen SLA over beschikbaarheid, latency

VPN Connect

Met name bedoeld voor connectiviteit naar IaaS/PaaS diensten die niet via Direct Connect (zie 3) ontsloten kunnen worden.

Deze connectiviteitsvariant staat ook bekend als site-to-site (S2S) VPN verbinding.

ProRail

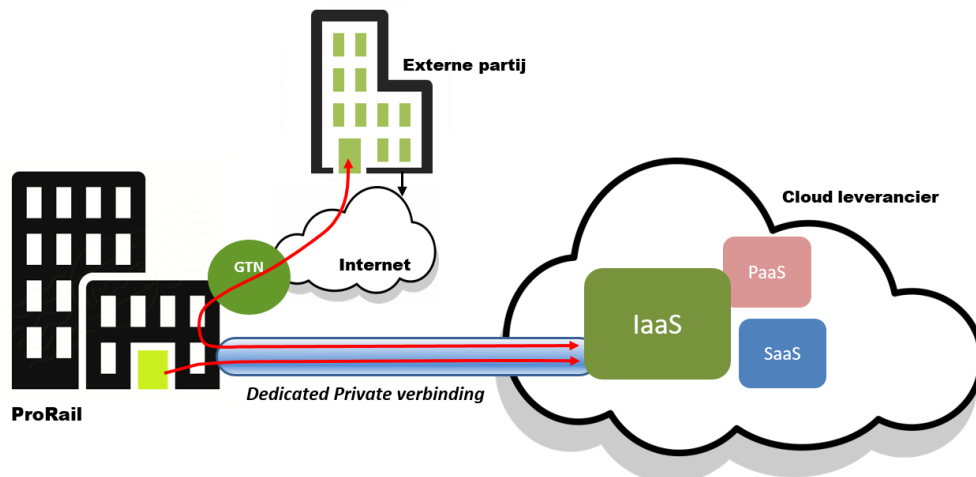


Kenmerken:

- Verwerking in de cloud en bij ProRail
- Eindgebruikers, intern en extern én
- systeemkoppelingen via VPN verbinding
- https en andere protocollen
- Maakt gebruik van Internet
- Geen SLA over beschikbaarheid, latency
- Communicatie van en naar Internet via GTN

Direct Connect

Met name bedoeld voor connectiviteit naar IaaS/PaaS diensten die binnen het beheer en netwerkdomein van ProRail vallen en als verlengstuk van de ProRail datacenter infrastructuur kunnen worden beschouwd.



Kenmerken:

- Verwerking in de cloud en bij ProRail
- Eindgebruikers, intern en extern én
- systeemkoppelingen via eigen private verbinding
- https en andere protocollen
- Maakt gebruik van service provider voor de private verbinding
- SLA af te sluiten over beschikbaarheid, latency
- Communicatie van en naar Internet via GTN

3 ProRail Azure Cloud

Voor cloudoplossingen binnen de ProRail Azure Cloud zijn de volgende voorwaarden van toepassing:

3.1 Subscriptions

Subscriptions worden gebruikt om een logische scheiding van clouddiensten aan te brengen voor o.a. beheer en doorbelasting van kosten. ProRail hanteert een subscription per applicatie of applicatiegroep voor zowel productie als staging (ontwikkeling, test en acceptatie). Op deze wijze zijn de kosten per applicatie eenvoudig inzichtelijk te maken en de toegang voor behorende partijen te regelen.

- **Staging Subscription**

Binnen een staging subscription vinden alle ontwikkel-, test- en acceptatie activiteiten plaats. Hier wordt de applicatie-functionaliteit gebouwd, getest en gereed gemaakt voor productie. Dit omvat dus o.a. ook het maken van de scripts (ARM templates) om de applicatie en Azure PaaS/IaaS diensten automatisch te kunnen installeren in productie. Gebruikers zoals ontwerpers, ontwikkelaars en testers krijgen hier voldoende rechten om deze werkzaamheden uit te voeren.

- **Production Subscription**

Een production subscription omvat de productieomgeving waar de applicatiefunctie als beheersbaar geheel aan de afnemers/eindgebruikers wordt geleverd. Toegang tot een production subscription is beperkt tot die rollen/processen die nodig zijn voor de automatische deployment en het beheer van de toepassing. Voor dat laatste krijgen persoonlijke accounts hier enkel leesrechten.

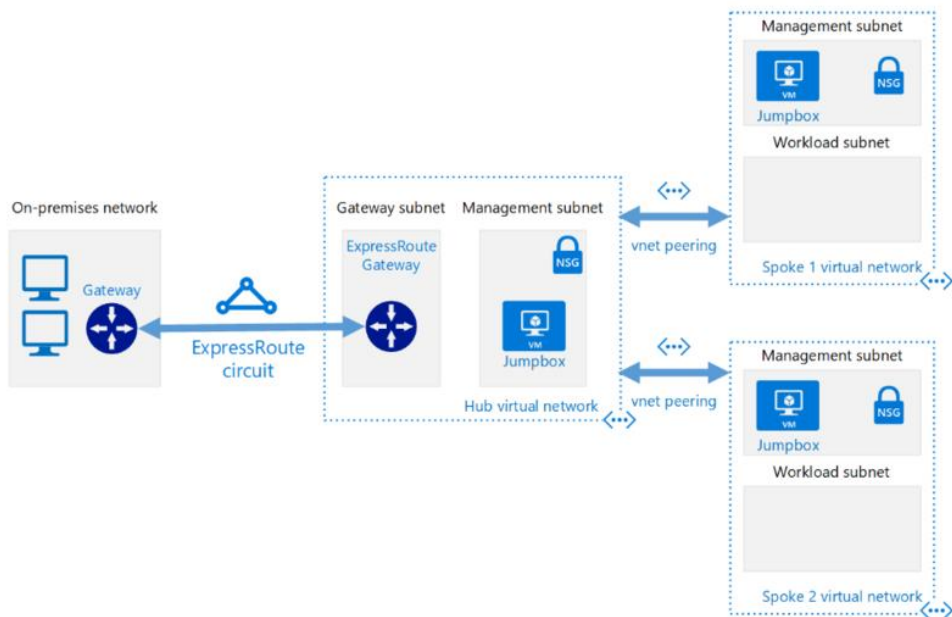
3.2 Netwerk

Binnen de Azure subscriptions waar IaaS clouddiensten worden gebruikt, worden één of meer Virtual Networks (VNet) gehost. Elk VNet heeft veelal een verbinding (peering) met een andere VNet of met het on-premises netwerk van ProRail. Om deze connectiviteit gecontroleerd in goede banen te leiden maakt ProRail gebruik van een 'Hub-Spoke' topologie.

- **Hub-Spoke Model**

De Hub fungeert als centraal punt van connectiviteit naar het ProRail on-premises netwerk. De Spokes zijn VNets die via peering zijn verbonden met de hub en die kunnen worden gebruikt om workloads te isoleren. Netwerkverkeer stroomt tussen de ProRail on-premises datacenters en de hub via een ExpressRoute gateway verbinding.

ProRail

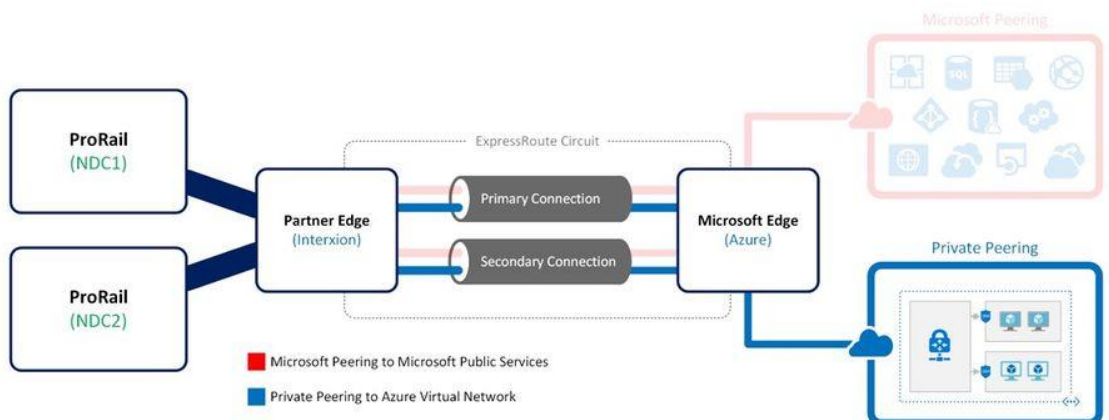


▪ On-premises connectiviteit

Voor de verbinding tussen het ProRail on-premises network en de virtuele netwerken in de ProRail Azure cloud wordt gebruik gemaakt van ExpressRoute. ExpressRoute maakt gebruik van een netwerk service provider voor de private verbinding. ExpressRoute ondersteunt de volgende routing domeinen:

- Microsoft Peering voor de verbinding met Microsoft online services (Office 365, Azure PaaS-services) die worden aangeboden op openbare IP-adressen
- Azure Private Peering voor de verbinding met Azure compute-services, namelijk virtuele machines (IaaS) en clouddiensten (PaaS), die zijn geïmplementeerd in een virtueel netwerk

Op dit moment is voor ProRail alleen de Azure Private Peering geïmplementeerd als vertrouwde uitbreiding van het KA-netwerk domein in Microsoft Azure.



3.3 Naamconventie

Binnen de ProRail Azure Cloud zijn de volgende naamconventies van toepassing:

▪ Subscriptions

Voor subscriptions geldt de volgende naamconventie:

{AFD}-{TYPE}-{OMGEVING}-{Uniek Nummer}

- AFD = IV (infravoorzieningen), A&B (Assets en Bedrijfsvoering) of LOG (Logistiek)
- TYPE = HUB of APP of {Applicatie naam}
- OMGEVING = Production of Staging (Ontwikkel/Test/Acceptatie)

Voorbeeld:

IV-HUB-Production-01
A&B-BDAP-Staging-01
LOG-APP-Production-03

▪ Resource groups

Voor resource groepen geldt de volgende naamconventie:

{AFD}-{APPLICATIE}-{OMGEVING}-RG

- AFD = IV (infravoorzieningen), AB (Assets en Bedrijfsvoering) of LOG (Logistiek)
- APPLICATIE= Applicatie naam
- OMGEVING = Production of Staging (Ontwikkel/Test/Acceptatie)
- TYPE = RG

Note: "&" is niet toegestaan.

Voorbeeld:

IV-Jira-Production-RG
IV-Confluence-Production-RG
IV-Bitbucket-Production-RG

▪ Virtual Networks

Voor een Virtual Network binnen een Hub of Spoke geldt de volgende naamconventie:

{AFD}-{Applicatie}-VNET

- AFD = IV (infravoorzieningen), AB (Assets en Bedrijfsvoering) of LOG (Logistiek)
- SOORT = Type (applicatie is dan APP)
- TYPE = VNET

NOTE: Per Hub of Spoke (lees subscriptions) is één Virtual Network toegestaan.

Voorbeeld:

IV-OntwikkelTools-VNET

Subnets

Voor Subnets geldt de volgende naamconventie:

{NAME}{Volgnummer}

- NAME = Een omschrijving waar het subnet voor dient zoals GatewaySubnet, FrontEnd, BackEnd, etc...
- VOLGNUMMER = 1

Volgnummer is niet toegestaan voor de GatewaySubnet.
Hieronder voorbeelden van subnet namen.

GatewaySubnet
FrontEndSubnet1
BackEndSubnet1

▪ **Network Security Groups**

Voor Network Security Groups geldt de volgende naamconventie:

{AFD}-{APPLICATIE}-{OMGEVING}-NSG

- AFD = IV (infravoorzieningen), AB (Assets en Bedrijfsvoering) of LOG (Logistiek)
- APPLICATIE = Applicatie naam (conform naamgeving Resource Group)
- OMGEVING = Production of Staging (Ontwikkel/Test/Acceptatie)
- TYPE = NSG

Voorbeeld:

IV-Jira-Production-NSG
IV-Confluence-Production-NSG
IV-Bitbucket-Production-NSG

▪ **Virtual Machines**

Voor virtual machines die binnen de ProRail Azure tenant aangemaakt worden, geldt de volgende naam conventie:

{AFD}-{TYPE}{Volgnummer}-{OMGEVING}-VM

- AFD = IV (infravoorzieningen), AB (Assets en Bedrijfsvoering) of LOG (Logistiek)
- SOORT = Applicatie server is dan APP, SQL server is SQL, etc...
- VOLGNUMMER = Begin 101
- OMGEVING = P voor Productie, O voor ontwikkel, S voor staging, etc...
- TYPE = VM

Voorbeeld:

IV-APP101-P-VM
IV-APP102-P-VM
IV-APP103-P-VM

NOTE: Maximum is 15 karakters voor een Virtual Machine.

▪ **Storage Accounts**

Voor Storage Accounts geldt de volgende naam conventie:

ProRail

{afd}{applicatie}{omgeving}sa

- AFD = iv (infravoorzieningen), ab (Assets en Bedrijfsvoering) of log (Logistiek)
- APPLICATIE= Applicatie naam (conform naamgeving Resource Group)
- OMGEVING = prod of stag (Ontwikkel/Test/Acceptatie)
- TYPE = sa

Voorbeeld:

ivjiraprodsa

ivconfluencestagsa

ivbitbucketprodsa

▪ Overig

Voor alle overige resources de bovenstaande naamconventies gebruiken als richtlijn.

Hieronder een aantal voorbeelden:

- IV-Jira-Production-SQLSRV (SQL server)
- IV-Jira-Production-SQLDB (SQL database)
- IV-Jira-Production-AS (App Service)
- IV-Jira-Production-CR (Container Registry)
- IV-Jira-Production-ASP (App Service Plan)