ProRail

Cloud Security Beleid

Informatie beveiligingsbeleid

Autorisatie

	paraaf	datum
Auteur / BIA: Maurice Endhoven		April 2020
Project manager: N,V,T,		
Security/Privacy Officer: Stoffel Bos		Mei 2020

Eigenaar	ICT CIO Office
Auteurs	Maurice Endhoven e.a.
Kenmerk	IBB 1.8
Versie	1.1
Datum	Mei 2020
Bestand	IBB 1.8 Cloud Security Beleid ProRail v1.1.docx
Status	Goedgekeurd

Inhoudsopgave

1. Inleiding 3
1.1 Doel 3
1.2 Bereik 3
1.3 Opbouw van het document 3

2. Introductie van Azure Cloud 4
2.1 Inleiding 4
2.2 Gebruik Azure Cloud binnen ProRail 4
2.3 Rollen en verantwoordelijkheden 4

3. Leeswijzer richtlijnen 6

4. Richtlijnen 7
4.1 Beveiligingszones en segregatie 7
4.2 Monitoring 9
4.2.1 Logverzameling en -analyse 9
4.2.2 Incidentmanagement 10
4.3 Identiteit en toegangsbeheer 12
4.3.1 Azure Console toegangsbeleid 12
4.3.2 Toegangsbeleid Azure 14
4.3.3 Verhoogde toegangsrechten Azure-console 15
4.3.4 Toegang tot virtuele machines 16
4.3.5 Toegang voor derde partijen 18
4.4 Security-technologie 20
4.5 Naleving, retentie en archivering 21
4.6 Beschikbaarheid 23
4.7 Back-up 24
4.8 Netwerkbeveiliging 26
4.9 Verstoringen en updates 28
4.10 Encryptie 29
4.11 Dataclassificatie 30

5. Woordenlijst 32

1. Inleiding

1.1 Doel

Het doel van dit document is het beschrijven van het beleid omtrent gebruik en inrichting van Azure Cloud-omgevingen, zodat deze conform het informatiebeveiligingsbeleid van ProRail ontworpen en geïmplementeerd worden. Het document beschrijft de vereiste architectuur, de beveiligingseisen en de processen voor Azure Cloud-oplossingen.

Dit document vult de volgende interne referentiedocumenten van ProRail aan met betrekking tot Azure Cloud-architectuur:

- *Cloud – Richtlijnen en voorwaarden.pdf*
- *IBB-2.3 Risicobeheersing en classificatie bij Informatievoorziening Prorail.pdf*
- *IBB-1.2 Handboek voor Informatiebeveiliging ProRail.pdf*
- *IBB-1.6 Eisen Informatieveiligheid aan de Ondernemer.pdf*
- *IBB-1 Informatie beveiliging ProRail*
- *IBB-2.4 Logische Toegangsarchitectuur en wachtwoordbeleid*
- *IBB-2.5 Externe connectie standaarden*

1.2 Bereik

De afdeling ProRail ICT CIO Office is eigenaar van dit document. Het beleidsstuk is van toepassing op ontwerpers, (project)architecten en (interne en externe) auditors.

1.3 Opbouw van het document

De richtlijnen in dit document zijn als volgt ingedeeld:

- **Rood (V)**: Verplichte richtlijn voor alle Microsoft Azure Cloud-omgevingen van ProRail.
- **Oranje (G)**: Gewenste richtlijn, deze dienen waar mogelijk geimplementeerd te worden en uitzonderingen volgen het interne afwijkingsproces.
- **Groen (O)**: Optionele richtlijn, bestaande uit best practices die wenselijk maar niet verplicht zijn.

2. Introductie van Azure Cloud

2.1 Inleiding

Microsoft Azure Cloud is een IaaS-dienst, die verschillende PaaS-, CaaS-, FaaS- en SaaS-diensten omvat. Zo zijn er bijvoorbeeld PaaS-diensten beschikbaar in Azure:

- Azure SQL Database en Azure Cosmos DB zijn respectievelijk een SQL en een NoSQL Database die rechtstreeks door Azure worden beheerd.
- Azure Web Apps voor het publiceren van webapplicaties in Azure Cloud, deze dienst beheert load balancing en virtuele machines die aan de applicatie zijn toegewezen.
- Azure Search, waarmee zoekdiensten op een siteapplicatie kunnen worden aangeboden zonder dat een Lucene- of Solr-zoekserver hoeft te worden beheerd.

2.2 Gebruik Azure Cloud binnen ProRail

Alle Azure Cloud-omgevingen binnen ProRail zijn onderdeel van de ProRail tenant. Het is niet toegestaan om buiten de ProRail Azure omgeving om te werken. Het is mogelijk om publieke of private diensten aan te bieden binnen de Azure Cloud-omgeving, de maatregelen beschreven in dit beleid gelden voor beide typen diensten.

2.3 Rollen en verantwoordelijkheden

Om de Azure Cloud-omgeving van ProRail effectief te beheren, is het van belang dat rollen en verantwoordelijkheden gedefinieerd zijn. Met betrekking tot beheersing van cloud zijn er specifieke aspecten die aandacht verdienen:

- Wie kan beslissen over in welke mate een Azure Cloudoplossing voldoet aan de vereisten en doelen van ProRail? Welke zaken worden meegenomen in deze beslissing?
- Wie beslist wat het budget is voor Azure?
- Hoe worden bestaande systemen geïntegreerd binnen de cloudarchitectuur, en welke impact heeft dit op de systemen?
- Wie heeft welke toegang tot specifieke gegevens? Hoe wordt deze toegang verleend en beheerd?
- Welke data wordt bewaard, en waar wordt deze bewaard?
- Wie definieert beleid met betrekking tot informatie-, applicatie- en servergebruik?

De RACI-structuur van rollen en verantwoordelijkheden met betrekking tot Azure Cloud binnen ProRail is in onderstaande tabel weergegeven:

Stap	CIO Office	PROJECT TEAM	TRANSITION TEAM	CCOE	ITSM	SECURITY	IT ARCHITECTURE
Nieuw verzoek of project	A	R	C	I	-	I	I
Haalbaarheidsstudie en dataclassificatie	I	A/R	C	I	-	C	C
Budget verzoek (boven €150k)	A/R	C	I	I	I	I	I
Budget verzoek evaluatie	A/R	C	I	I	I	I	I

Selectie van dienst	I	A/R	C	C	C	C	C
Selectie van leverancier	I	A/R	I	I	C	I	I
Aanvragen account nieuwe gebruiker	I	A/R	I	C	-	I	I
Evaluatie van account verzoeken	C	C	C	I	A/R	I	I
Aanmaken en goedkeuren van nieuwe accounts	C	C	C	I	A/R	I	I
Ontwerp	I	A/R	C	I	-	I	I
Aanpassen van ontwerp	I	A/R	C	I	-	I	I
Aanmaken van diensten	I	I	A	I	R	I	I
Beveiligen van gegevens in de Cloud	I	A/R	I	C	-	C	C
Ontwikkeling en integratie van systemen	I	A/R	I	C	-	C	C
Indienen van architectuur assessments	I	A/R	I	I	-	I	C
Evalueren van architectuur assessments	I	C	I	I	-	I	A/R
Aanpassen van architectuur	I	A/R	I	C	-	C	C
Delivery	-	A/R	C	I	-	I	I
Continue monitoring	-	c	C	C	-	A/R	C

NB, Deze matrix is onderhevig aan organisatiewijzigingen

3. Leeswijzer richtlijnen

In de volgende hoofdstukken van dit document zijn de richtlijnen opgenomen die ProRail stelt met betrrekking tot inrichting en gebruik van de Azure-omgeving.

Deze richtlijnen zijn als volgt opgezet:

Beschrijving

Korte beschrijving van de maatregel.

Aanvullende informatie

Optioneel: aanvullende informatie ter verduidelijking van de maatregel.

4. Richtlijnen

4.1 Beveiligingszones en segregatie

Routering van netwerkverkeer [SEG1]	V	IaaS ☑ PaaS/CaaS/FaaS ☑ SaaS ☐

Beschrijving

Uitgaand netwerkverkeer van IaaS- en PaaS-componenten moet gerouteerd worden via een centrale firewall voordat het lokale netwerk of internet bereikt kan worden.

Aanvullende informatie

Door verkeer via een centrale firewall te leiden is het mogelijk om centraal beheersmaatregelen en monitoring in te richten, alsmede forensisch onderzoek uit te voeren wanneer nodig.

Beheersmaatregelen voor clouddiensten [SEG2]	G	IaaS ☑ PaaS/CaaS/FaaS ☐ SaaS ☐

Beschrijving

Verkeer tussen het lokale netwerk en clouddiensten moet voorzien zijn van beheersmaatregelen om ongeautoriseerd(e) toegang, gebruik en aanpassingen te voorkomen.

Aanvullende informatie

Door het gebruik en de ontwikkeling van lokale en clouddiensten steunend op hetzelfde autorisatiesysteem kunnen nieuwe aanvalspaden gecreëerd worden. Bij de ontwikkeling en inrichting van zowel lokale als clouddiensten moet rekening gehouden worden met deze mogelijke aanpassingen aan het securitypostuur van ProRail. Maatregelen moeten getroffen worden om op passende wijze de bijkomende risico’s van deze aanpassingen te beheersen.

Routeren via besloten verbindingen [SEG3]	G	IaaS ☑ PaaS/CaaS/FaaS ☑ SaaS ☑

Beschrijving

Vertrouwd verkeer tussen private clouddiensten en het lokale netwerk moet via een besloten verbinding gerouteerd worden. Als dit niet mogelijk is, moet het verkeer als regulier internetverkeer behandeld worden en dienen de daarbij behorende beheersmaatregelen toegepast te worden.

Aanvullende informatie

Verkeer tussen het interne (virtuele) netwerk en clouddiensten wordt standaard via het publieke internet gerouteerd en is hiermee blootgesteld aan de gebruikelijke risico's die daarmee gepaard gaan. Sommige clouddiensten bieden routering via een besloten verbinding aan waardoor het verkeer niet het netwerk van de clouddienst verlaat. Hierdoor is het verkeer in mindere mate blootgesteld aan de risico's van het publieke internet.

4.2 Monitoring

4.2.1 Logverzameling en -analyse

Centrale opslag van logbestanden [LOG1]	V	IaaS ☑ PaaS/CaaS/FaaS ☑ SaaS ☑

Beschrijving

Indien mogelijk moeten logbestanden verzameld worden in een gecentraliseerde opslag, waar deze regelmatig gearchiveerd worden en in overeenstemming met bijbehorende retentietermijnen verwijderd worden.

Aanvullende informatie

De centrale opslag van logbestanden draagt bij aan de vereenvoudiging van het monitoren van de geschiktheid, opzet en operationele effectiviteit van beheersmaatregelen, alsmede het verbeteren van de effectiviteit van forensische onderzoeksmogelijkheden. De centrale opslag van logbestanden bevordert de mogelijkheden om gegevens te importeren naar loganalyse-oplossingen of 'Security Information en Event Management' (SIEM)-oplossingen voor verdere verwerking en afhandeling.

Door doorvoerbeperkingen tussen zowel lokale infrastructuur als cloudomgevingen, is het gebruikelijk om logbestanden dicht bij de bron op te slaan, dat wil zeggen logbestanden van lokale infrastructuur in het lokale netwerk en logbestanden van clouddiensten in de clouddienst.

Voor de effectiviteit van loganalyse- of SIEM-oplossingen is het bevorderlijk om, indien mogelijk, zo veel mogelijk logbestandsbronnen te aggregeren, zodat correlaties tussen incidenten eerder gevonden kunnen worden.

Vastlegging van logbestanden [LOG2]	G	IaaS ☑ PaaS/CaaS/FaaS ☑ SaaS ☑

Beschrijving

Voor alle lokale en cloudoplossingen en de daarbij behorende data moet beoordeeld worden of deze afhankelijkheden of implicaties hebben op de doelstellingen en eisen voor beveiliging, beschikbaarheid, integriteit, vertrouwelijkheid en privacy van processen of data. In opvolging van deze beoordeling moet de vastlegging en retentie van logging ingericht worden zodat doelstellingen en eisen nageleefd kunnen worden.

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

Toegang tot logbestanden [LOG3]	G	IaaS ☑ PaaS/CaaS/FaaS ☑ SaaS ☐

Beschrijving

Alle verzamelde logs moeten enkel leesbaar zijn voor services en individuen indien deze strikt nodig zijn voor een legitiem doeleinde. Waar mogelijk dienen toegangsmaatregelen ingericht te worden zodat toegang tot logbestanden beperkt is tot een vooraf gedefinieerde periode.

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

4.2.2 Incidentmanagement

Training voor cloud-incidentmanagement [INC1]	G	IaaS ☑ PaaS/CaaS/FaaS ☑ SaaS ☑

Beschrijving

Het team dat verantwoordelijk is voor afhandeling van beveiligingsincidenten met betrekking tot clouddiensten moet op gepaste wijze getraind zijn om deze adequaat en tijdig af te kunnen handelen.

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

Incidentmanagement [INC2]	G	IaaS ☑ PaaS/CaaS/FaaS ☑ SaaS ☑

Beschrijving

De afhandeling van beveiligingsincidenten gebeurt in dezelfde omgeving en volgens dezelfde incidentmanagementprocessen voor zowel clouddiensten als het lokale netwerk.

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

4.3 Identiteit en toegangsbeheer

4.3.1 Azure Console toegangsbeleid

Azure Cloud-account wachtwoordmanagement [IAM1]	V	IaaS ☑ PaaS/CaaS/FaaS ☑ SaaS ☑

Beschrijving

De toekenning van administratieve privileges moet periodiek beoordeeld worden. Wachtwoorden voor accounts aangemaakt voor specifieke services (service-accounts) binnen Azure, moeten jaarlijks gewijzigd worden.

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

Noodtoegang tot Microsoft Azure Subscription Administrator Account [IAM2]	V	IaaS ☑ PaaS/CaaS/FaaS ☑ SaaS ☑

Beschrijving

Het ‘Subscription Administrator Account’ mag niet gebruikt worden voor gebruikersbeheer. Dit account dient te fungeren als noodtoegangaccount. Het account moeten worden voorzien van een lang en complex wachtwoord, opgedeeld in twee of meer delen, en bewaard op een veilige manier (bijvoorbeeld middels een kluisprocedure).

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

Wachtwoordbeleid [IAM3]	V	IaaS ☑ PaaS/CaaS/FaaS ☑ SaaS ☑

Beschrijving

Wachtwoorden moeten worden ingesteld in lijn met het ProRail-wachtwoordbeleid.

Aanvullende informatie

Refereer voor gedetailleerde eisen naar IBB2.4.

Multi Factor Authenticatie (MFA) [IAM4]

V	IaaS	☑
	PaaS/CaaS/FaaS	☑
	SaaS	☑

Beschrijving

Alle accounts met verhoogde rechten (zoals bijvoorbeeld administrator-accounts) moeten gebruikmaken van multifactor-authenticatie.

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

4.3.2 Toegangsbeleid Azure

Beperking gebruikersrechten [IAM5]	V	IaaS ☑ PaaS/CaaS/FaaS ☑ SaaS ☑

Beschrijving

Aanpassingen op de Azure-productieomgeving mogen enkel worden uitgevoerd via beheerde automatische *pipelines*, met de juiste goedkeuring. Indien er geen *pipeline* voor de specifieke wijziging beschikbaar is, moet deze worden aangevraagd bij het verantwoordelijke team (zie RACI matrix). Indien noodzakelijk zullen zij deze *pipeline* aanmaken.

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

Microsoft Azure-resourcevergrendeling [IAM6]	G	IaaS ☑ PaaS/CaaS/FaaS ☑ SaaS ☑

Beschrijving

Om onbedoelde verwijdering van Azure-resources te voorkomen, moet Resource Lock worden ingeschakeld voor kritieke cloud-resources.

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

4.3.3 Verhoogde toegangsrechten Azure-console

Tijdsgebonden verhoogde toegangsrechten [IAM7]	V	IaaS ☑ PaaS/CaaS/FaaS ☑ SaaS ☑

Beschrijving

Waar mogelijk binnen Azure moet gebruikgemaakt worden van tijdelijk verhoogde toegangsrechten, in plaats van permanente accounts met hoge rechten.

Aanvullende informatie

Dit kan door gebruik te maken van Azure Active Directory (Azure AD) Privileged Identity Management (PIM), een service waarmee toegang tot belangrijke resources kan worden beheerd, gecontroleerd en bewaakt.

Azure AD-beheer [IAM8]	G	IaaS ☑ PaaS/CaaS/FaaS ☑ SaaS ☑

Beschrijving

Beheer van Azure AD moet worden gedaan via specifieke Cloud Azure AD Administrator-accounts. Beheer van Azure-resources dient met een apart account te gebeuren.

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

Aanmaken van een Service Principal [IAM9]	G	IaaS ☑ PaaS/CaaS/FaaS ☑ SaaS ☑

Beschrijving

Indien er een nieuwe Service Principal wordt aangemaakt, moet dit worden gesplitst in het aanmaken van het object en het aanmaken van de relaties. Om de kans op compromitatie van de Service Principal te minimaliseren, moeten deze taken worden belegd bij twee verschillende teams.

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

Beheer van beveiligingsgegevens [IAM10]	V	IaaS ☑ PaaS/CaaS/FaaS ☑ SaaS ☑

Beschrijving

Beveiligingsgegevens (bijvoorbeeld geheimen, wachtwoorden, sleutels en certificaten) gebruikt in ontwikkelde cloudapplicaties moeten per applicatie worden opgeslagen in een gecentraliseerde ‘Key Vault’.

Aanvullende informatie

De centrale opslag van beveiligingsgegevens staat controle toe op hoe en wanneer er toegang tot sleutels en geheimen is gezocht.

Gebruik van Cloud-only accounts [IAM11]	V	IaaS ☑ PaaS/CaaS/FaaS ☑ SaaS ☑

Beschrijving

Waar mogelijk dient gebruik te worden gemaakt van gefedereerde of gesynchroniseerde AD-accounts, in plaats van Azure-specifieke accounts.

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

4.3.4 Toegang tot virtuele machines

Lokale administrator-accounts op virtuele machines [IAM12]	V	IaaS ☑ PaaS/CaaS/FaaS ☐ SaaS ☐

Beschrijving

Lokale administrator-accounts zijn niet toegestaan op virtuele machines in de test- en productie-omgevingen.

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

Beheer van sleutelparen [IAM13]

V

IaaS	☑
PaaS/CaaS/FaaS	☐
SaaS	☐

Beschrijving

Sleutelparen die gebruikt worden om verbindingen tot stand te brengen met een virtuele machine (bijvoorbeeld via SSH or RDP) moeten op een veilige manier bewaard worden. Hierbij kan gebruik worden gemaakt van een oplossing buiten Azure, of Azure Key Vault.

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

Gebruik van een Bastion-server [IAM14]

V

IaaS	☑
PaaS/CaaS/FaaS	☐
SaaS	☐

Beschrijving

Indien een account met verhoogde rechten toegang wil verkijgen tot een virtuele machine van buiten het ProRail-netwerk, moet toegang tot de virtuele machine enkel via een ‘Bastion server’ verlopen.

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

PaaS-authenticatie [IAM15]

V

IaaS	☐
PaaS/CaaS/FaaS	☑
SaaS	☐

Beschrijving

Toegang tot PaaS-services moet waar mogelijk gebruikmaken van Azure AD.

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

4.3.5 Toegang voor derde partijen

Toegang voor derde partijen [IAM16]	V	IaaS ☑ PaaS/CaaS/FaaS ☑ SaaS ☑

Beschrijving

Toegang tot de ProRail Azure Cloud-omgeving voor derde partijen wordt gefaciliteerd door Azure B2B-accounts. Indien dit niet mogelijk is, kan gekozen worden voor Active Directory-accounts gecreëerd door ProRail, die gefedereerd of gesynchroniseerd zijn met de cloud-omgeving.

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

Multi Factor Authenticatie (MFA) voor derde partijen [IAM17]	V	IaaS ☑ PaaS/CaaS/FaaS ☑ SaaS ☑

Beschrijving

Alle accounts voor derde partijen moeten gebruikmaken van multifactor-authenticatie.

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

Toegang tot virtuele machines voor derde partijen [IAM18]	G	IaaS ☑ PaaS/CaaS/FaaS ☐ SaaS ☐

Beschrijving

Toegang tot systeemaccounts op virtuele machines voor derde partijen dient te worden voorzien van aanvullende beveiligingsmaatregelen. Hierbij kan bijvoorbeeld gedacht worden aan het gebruik van MFA, en een stepping stone server. Toegang dient te worden aangevraagd en goedgekeurd door de verantwoordelijke persoon binnen ProRail.

Aanvullende informatie

Door gebruik te maken van ‘Just-In-Time’-toegang (JIT) voor virtuele machines kunnen specifieke poorten aanvullend worden beschermd. Dit is onder andere relevant voor poorten die gebruikt worden voor:

- SSH
- RDP
- WinRM

4.4 Security-technologie

Security-oplossingen voor Virtual Machines [SEC1]	V	IaaS ☑ PaaS/CaaS/FaaS ☐ SaaS ☐

Beschrijving

Alle virtuele machines die gebruikt worden in preproductie- en productie-omgevingen moeten voorzien zijn van de monitoring- en antivirus-oplossingen zoals beschreven in de Technologie Roadmap.

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

DevOps-beveiliging [SEC2]	G	IaaS ☑ PaaS/CaaS/FaaS ☑ SaaS ☑

Beschrijving

Voordat wijzigingen aan applicaties of infrastructuur worden gepubliceerd, moet de kwaliteit en veiligheid van de code beoordeeld worden, door middel van:

- Statische en dynamische code-analyse
- Pull requests met als onderdeel beoordeling door een medeontwikkelaar
- Onderscheid tussen versies door gebruik van ‘branches’
- Documenteren van testresultaten in een gedeelde omgeving

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

4.5 Naleving, retentie en archivering

Continuïteit van cloudapplicaties [COM1]

G

IaaS ☑
PaaS/CaaS/FaaS ☑
SaaS ☑

Beschrijving

Een continuïteitsplan moet worden opgesteld voor cloudapplicaties die kritiek zijn voor ProRail. Dit plan dient jaarlijks getest en bijgewerkt te worden.

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

Dataretentie [COM2]

G

IaaS ☑
PaaS/CaaS/FaaS ☑
SaaS ☑

Beschrijving

De binnen ProRail gehanteerde data-retentietermijnen gelden ook voor data die wordt bewaard in cloudomgevingen. Data-retentietermijnen moeten worden gehanteerd bij beëindiging van contracten met cloudleveranciers.

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

Ontbindende voorwaarden [COM3]

G

IaaS ☑
PaaS/CaaS/FaaS ☑
SaaS ☑

Beschrijving

In contracten met cloudserviceproviders moeten ontbindende voorwaarden voor de dienstverlening worden opgenomen.

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

Exit strategie per cloudapplicatie [COM4]	O	IaaS ☑ PaaS/CaaS/FaaS ☑ SaaS ☑

Beschrijving

Voor elke cloudapplicatie stelt ProRail een exitstrategie op, in geval van beëindiging van de dienstverlening of migratie van de applicatie.

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

Inventarisatie van cloudmiddelen [COM5]	O	IaaS ☑ PaaS/CaaS/FaaS ☐ SaaS ☐

Beschrijving

Cloudcomponenten (zoals IaaS-componenten in preproductie- en productieomgevingen) worden automatisch bijgehouden in de wijzigingsbeheerdatabase (CMDB).

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

Installatie van extensies [COM6]	G	IaaS ☑ PaaS/CaaS/FaaS ☑ SaaS ☑

Beschrijving

Extensies die gebruikt worden binnen de cloudomgeving van ProRail mogen enkel worden geïnstalleerd na expliciete goedkeuring van het verantwoordelijke team (zie RACI matrix).

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

4.6 Beschikbaarheid

Beschikbaarheid van interne kritieke applicaties [AVA1]	G	IaaS ☑ PaaS/CaaS/FaaS ☑ SaaS ☐

Beschrijving

Applicaties die van kritiek belang zijn voor ProRail moeten worden ingericht op een wijze waarmee voldaan kan worden aan een beschikbaarheidspercentage gelijk aan dat van het interne verkeer.

Aanvullende informatie

ProRail's interne verkeer is afhankelijk van Microsoft Azure ExpressRoute-beschikbaarheid, waarbij de SLA een beschikbaarheidspercentage van 99,9% voorschrijft.

Beschikbaarheid van extern bereikbare kritieke applicaties [AVA2]	G	IaaS ☑ PaaS/CaaS/FaaS ☑ SaaS ☐

Beschrijving

Extern bereikbare applicaties die van kritiek belang zijn voor ProRail moeten worden ingericht op een wijze waarmee voldaan kan worden aan beschikbaarheidspercentage hoger dan dat van het interne verkeer.

Aanvullende informatie

ProRail's interne verkeer is afhankelijk van Microsoft Azure ExpressRoute beschikbaarheid, waarbij de SLA een beschikbaarheidspercentage van 99,9% voorschrijft.

Een hoger beschikbaarheidspercentage kan bereikt worden door gebruik te maken van verschillende '*availability zones'* in Azure.

4.7 Back-up

Back-up van servers [BAC1]	G	IaaS ☑ PaaS/CaaS/FaaS ☐ SaaS ☐

Beschrijving

Zodra een server wordt opgezet, moet er een back-up gemaakt worden – door middel van een ‘snapshot’. Na elke wijziging of upgrade van de server moet er een incrementeel ‘snapshot’ worden gemaakt. Deze snapshots dienen bewaard te worden volgens de binnen ProRail geldende retentietermijnen.

Aanvullende informatie

Binnen Azure is het mogelijk om snapshots te bewaren in een Azure Cool Blob-storage. Dit is een generieke dienst die door het verantwoordelijke team (zie RACI matrix) voor elke server in Azure moet worden geïmplementeerd.

Back-up van data [BAC2]	G	IaaS ☑ PaaS/CaaS/FaaS ☑ SaaS ☐

Beschrijving

Zodra een service geinitialiseerd wordt, moet er een back-up gemaakt worden van de data – door middel van een ‘snapshot’. Een incrementeel ‘snapshot’ moet periodiek worden gemaakt, in overeenstemming met de SLA van de specifieke dienst. Deze snapshots dienen bewaard te worden volgens de binnen ProRail geldende retentietermijnen.

Aanvullende informatie

Binnen Azure is het mogelijk om snapshots te bewaren in een Azure Cool Blob-storage. Dit is een generieke dienst die door het verantwoordelijke team (zie RACI matrix) voor elke server in Azure moet worden geïmplementeerd.

Office 365 data-replicatie [BAC3]	G	IaaS ☐ PaaS/CaaS/FaaS ☐ SaaS ☑

Beschrijving

Data die bewaard wordt in Office 365 moet dagelijks gerepliceerd worden naar een back-up-omgeving. Hierbij kan gekozen worden voor een cloudomgeving of een lokale omgeving.

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

4.8 Netwerkbeveiliging

Netwerkconnectiviteit [NET1]

O	IaaS	☑
	PaaS/CaaS/FaaS	☑
	SaaS	☐

Beschrijving

Voor gepland onderhoud mag de verstoring van de connectiviteit van het netwerk niet langer duren dan 15 seconden. Voor onverwachte storingen mag de verstoring van connectiviteit van het netwerk niet langer duren dan 1,5 minuut.

Aanvullende informatie

De Azure VPN Gateway is opgezet in een active-standby-configuratie. Dit betekent dat bij onderhoud of storingen aan de actieve instance, er automatisch overgeschakeld wordt naar de stand-by instance.

DDoS-bescherming [NET2]

G	IaaS	☑
	PaaS/CaaS/FaaS	☑
	SaaS	☐

Beschrijving

Om de Azure-omgeving van ProRail te beschermen tegen Distributed Denial of Service (DDoS)-aanvallen moet op elke publieke verbinding Azure DDoS Protection Standard worden ingeschakeld. De meldingen en alerts over DDoS-aanvallen moeten worden geïntegreerd met de bestaande SIEM-oplossingen.

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

ExpressRoute agent monitoring [NET3]

V	IaaS	☑
	PaaS/CaaS/FaaS	☑
	SaaS	☐

Beschrijving

Netwerkconnectiviteit van ExpressRoute-circuits moet gemonitord worden.

Aanvullende informatie

De bereikbaarheid van ExpressRoute-circuits kan worden gemonitord zodat netwerkproblemen vroegtijdig kunnen worden geïdentificeerd.

Aanmaken van virtuele netwerken [NET4]

G

IaaS ☑
PaaS/CaaS/FaaS ☐
SaaS ☐

Beschrijving

Bij het aanmaken van een nieuw virtueel netwerk (VNet) en bijbehorende CIDR-blokken moet worden geverifieerd dat er geen overlap bestaat tussen de netwerken. De gebruikte CIDR-blokken moeten opgenomen worden in het centrale IP-managementsysteem. Aanmaken van nieuwe netwerken en uitgifte van CIDR-blokken dient centraal te gebeuren, en wordt beheerd door het verantwoordelijke team (zie RACI matrix).

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

4.9 Verstoringen en updates

Publicatie van een nieuwe wijziging [RES1]

V

IaaS ☑
PaaS/CaaS/FaaS ☐
SaaS ☐

Beschrijving

Waar mogelijk dienen wijzigingen aan cloudapplicaties en –componenten op een geautomatiseerde wijze gepropageerd te worden.

Aanvullende informatie

Door de propagatie van wijzigingen te automatiseren is het minder waarschijnlijk dat menselijke fouten plaatsvinden. Daarnaast introduceert het automatiseren van wijzigingenmanagement de mogelijkheid om ook beheersmaatregelen te automatiseren.

Wijzigingen bij verstoring van diensten [RES2]

V

IaaS ☑
PaaS/CaaS/FaaS ☐
SaaS ☐

Beschrijving

Bij verstoring van actieve diensten moet een wijziging binnen gepaste tijd kunnen worden gepubliceerd volgens vooraf gedefinieerde stappen en beheersmaatregelen. Indien er een back-up beschikbaar is, kan ervoor worden gekozen om een herstel van de meest recente back-up terug te zetten.

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

Impactanalyse voor een wijziging [RES3]

V

IaaS ☑
PaaS/CaaS/FaaS ☐
SaaS ☐

Beschrijving

Voor updates of aanpassingen aan applicaties of componenten (zie RES1) moet alvorens deze uitgevoerd wordt, een impactanalyse gedaan worden met daarin ten minste een analyse van de impact op andere applicaties of componenten.

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

4.10 Encryptie

Encryptie van getransporteerde gegevens naar Azure [ENC1]	V	IaaS ☑ PaaS/CaaS/FaaS ☑ SaaS ☑

Beschrijving

Alle data die ontvangen wordt vanaf een publiek netwerk (bijvoorbeeld het internet), moet worden versleuteld.

Aanvullende informatie

Er kan gekozen worden voor end-to-end encryptie (indien de data via Microsoft FrontDoor of de Application Gateway binnenkomt), of encryptie tot aan de Microsoft Azure Firewall.

TLS-implementatie [ENC2]	G	IaaS ☑ PaaS/CaaS/FaaS ☐ SaaS ☐

Beschrijving

Alle gegevensstromen door Azure moeten worden verzonden over een versleutelde verbinding met een TLS-versie gelijk aan of hoger dan de TLS-versie opgenomen in de Technologie Roadmap van ProRail.

Aanvullende informatie

Refereer naar de laatste versie van de Technologie Roadmap voor de actuele vereisten.

4.11 Dataclassificatie

Dataclassificatie en -autorisatie [DAT1]	O	IaaS ☑ PaaS/CaaS/FaaS ☑ SaaS ☑

Beschrijving

ProRail kan ervoor kiezen om export van gegevens naar de cloud stop te zetten, indien de juiste autorisaties of licenties niet beschikbaar zijn. Het verantwoordelijke team (zie RACI matrix) kan de classificatieniveaus van data naar eigen behoefte controleren.

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

Toegang tot en beveiliging van data [DAT2]	G	IaaS ☑ PaaS/CaaS/FaaS ☑ SaaS ☑

Beschrijving

Toegang tot de data in Azure en beveiliging van data in Azure volgen de beheersmaatregelen voorschreven door ProRail op basis van classificatie. Deze zijn gelijk aan de beheersmaatregelen voor lokaal opgeslagen data.

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

Dataretentie [DAT3]	G	IaaS ☑ PaaS/CaaS/FaaS ☑ SaaS ☑

Beschrijving

Voor data bewaard in Azure Cloud moet een retentieperiode worden gespecificeerd, op basis van de classificatie van de data.

Aanvullende informatie

Geen aanvullende informatie beschikbaar.

5. Woordenlijst

Afkorting / Term	*Definitie*
CaaS	Container as a Service (CaaS) is een cloud-servicemodel dat gebruikers in staat stelt om containers, applicaties en clusters te beheren en uit te rollen door middel van container gebaseerde virtualisatie. CaaS is zeer nuttig voor IT-afdelingen en ontwikkelaars bij het bouwen van veilige en schaalbare container gestuurde applicaties. Met CaaS kan dit worden bereikt met behulp van on-premise datacenters of via de cloud.
FaaS	Function as a Service (FaaS) is een cloud-servicemodel dat een platform biedt waarmee klanten applicatie-functionaliteiten kunnen ontwikkelen, uitvoeren en beheren zonder de complexiteit van het bouwen en onderhouden van de infrastructuur die normaal gesproken gepaard gaat met het ontwikkelen en lanceren van een app. Het bouwen van een applicatie volgens dit model is een manier om een 'serverloze' architectuur te bereiken en wordt typisch gebruikt bij het bouwen van microservice toepassingen.
Hybrid Cloud (Hybride Cloud)	De cloudinfrastructuur is een samenstelling van twee of meer verschillende cloud-infrastructuren (privé, gemeenschappelijk of publiek) die uniek blijven, maar met elkaar verbonden zijn door gestandaardiseerde technologie die data- en applicatieportabiliteit mogelijk maakt (bijv. cloud bursting voor het in evenwicht brengen van de belasting tussen de verschillende clouds).
IaaS	Infrastructure as Service (IaaS) is de mogelijkheid die aan de consument wordt geboden om verwerking, opslag, netwerken en andere fundamentele computerhulpmiddelen te leveren, waarbij de consument in staat is om willekeurige software, waaronder besturingssystemen en applicaties, in te zetten en te laten draaien. De consument beheert of controleert de onderliggende cloud-infrastructuur niet, maar heeft controle over besturingssystemen, opslag en ingezette applicaties; en mogelijk beperkte controle over geselecteerde netwerkcomponenten (bijvoorbeeld host firewalls).
PaaS	Platform as a Service (PaaS) is de mogelijkheid die aan de consument wordt geboden om door de consument gemaakte of aangeschafte applicaties te implementeren op de cloudinfrastructuur die zijn gemaakt met behulp van programmeertalen, bibliotheken, diensten en tools die door de aanbieder worden ondersteund. De consument beheert of controleert de onderliggende cloud-infrastructuur niet, inclusief netwerk, servers, besturingssystemen of opslag, maar heeft de controle over de ingezette applicaties en eventueel de configuratie-instellingen voor de applicatie-hostingomgeving.

Afkorting / Term	*Definitie*
Private Cloud (Privé Cloud)	De cloud-infrastructuur wordt exclusief gebruikt door één organisatie met meerdere consumenten (bijv. business units). De infrastructuur kan eigendom zijn van, beheerd worden door en geëxploiteerd worden door de organisatie, een derde partij of een combinatie daarvan, en kan on- of off-premise bestaan.
Public Cloud (Publieke Cloud)	De cloudinfrastructuur is opgezet voor open gebruik door het grote publiek. Het kan eigendom zijn van, beheerd worden door en geëxploiteerd worden door een bedrijf, een academische of een overheidsorganisatie, of een combinatie daarvan. Het bestaat on-premises van de cloudaanbieder.
SaaS	Software as a Service (SaaS) is de mogelijkheid voor de consument om gebruik te maken van de applicaties van de provider, toegankelijk vanaf verschillende client-apparaten via een thin client-interface, zoals een webbrowser (bijv. webgebaseerde e-mail), of een programma-interface. De consument beheert of controleert de onderliggende cloud-infrastructuur niet, inclusief netwerk, servers, besturingssystemen, opslag of zelfs individuele applicatiemogelijkheden, met de mogelijke uitzondering van beperkte gebruikersspecifieke applicatieconfiguratie-instellingen
Tenant (huurder)	Een tenant (huurder) is een groep gebruikers die een gemeenschappelijke toegang delen met specifieke privileges voor een software-instantie. In het verlengde daarvan is de tenant (huurder) verbonden aan de afnemer van de cloud-dienstverlener. Met een multi-tenant architectuur is een softwareapplicatie ontworpen om elke tenant (huurder) een specifiek deel van de instance te bieden - inclusief de gegevens, de configuratie, het gebruikersbeheer, de individuele functionaliteit van de tenant (huurder) en de niet-functionele eigendommen. Multi-tenancy staat in contrast met multi-instance-architecturen, waarbij afzonderlijke software-instanties voor verschillende tenants (huurders) werken.
TLS	Transport Layer Security (TLS) is een encryptie-protocol om de communicatie tussen computers (bijvoorbeeld op het internet) te beveiligen.
SIEM	Met Security Information and Event Management (SIEM) worden security alerts voortdurend gemonitord, gecombineerd en gecorreleerd, om vervolgens analyses op relevante dreigingen uit te kunnen voeren.
SLA	Service Level Agreement (SLA) bevat afspraken tussen afnemer en aanbieder van een product of dienst.