De Nederlandse Digitaliseringsstrategie

Onze referentie
Aanjaagteam NDS Cloud NDS-cloud@minbzk.nl

Datum 24 augustus 2026
Betreft Oplegger Het Ontwerp versie 0.9 Soevereine Overheidscloud

Beste,

De ontwikkeling van de overheidscloud vordert gestaag. In de afgelopen maanden heeft een groep architecten uit verschillende overheidsorganisaties gezamenlijk dit Ontwerp voor de Soevereine Overheidscloud opgesteld.

Deze publicatie is de volgende mijlpaal na de Kamerbrief *Stand van zaken Verkenning soevereine overheidsclouddienst*, die voor de zomer aan de Tweede Kamer is aangeboden. Met deze publicatie nodigen wij marktpartijen en overheden uit om vanuit hun kennis en ervaring te reageren op het concept. Minstens zo belangrijk als het document zelf is de samenwerking die is gegroeid. Tijdens dit traject is veel meer kennis gedeeld dan uiteindelijk op papier terecht is gekomen. Experts van publieke dienstverleners, gemeenten, waterschappen, provincies, overheidsdatacenters en het Rijk hebben gezamenlijk bijgedragen aan de totstandkoming van dit ontwerp. Dat was een proces van luisteren, herschrijven, afwegen en opnieuw beoordelen.

Dit Ontwerp beschrijft de hoofdlijnen van de beoogde oplossing. Het biedt een introductie op de verdere uitwerking en de bijbehorende Proof-of-Concept en schetst hoe de soevereine clouddienst eruit zal zien, welke voorzieningen deze biedt en hoe de technische keuzes samenhangen.

Tegelijkertijd realiseren wij ons dat een ontwerp voor een ambitie als deze nooit in één keer volledig is. Onderdelen zullen moeten worden aangescherpt en verrijkt. Wij geloven dat open samenwerking belangrijk is voor soevereiniteit. De kennis, ervaring en feedback van marktpartijen, overheidsorganisaties, kennisinstituten en onafhankelijke experts zijn daarom van grote waarde voor de verdere ontwikkeling van dit ontwerp.

Wij kijken uit naar de reacties.

Ron Kolkman
Namens het aanjaagteam NDS Cloud

De Nederlandse Digitaliseringsstrategie

NDS
Prioriteit Cloud

Overheidsbrede Soevereine clouddienst
Het Ontwerp

Versienummer 0.9

Datum 17 augustus 2026
Status Definitief concept

Colofon

Programmanaam Projectnaam	NDS prioriteit Cloud Overheidsbrede Soevereine Clouddienst
Document	Het Ontwerp
Versienummer	0.9
Prioriteit, Versneller	NDS Cloud – 4. Overheidsbrede Soevereine Clouddienst
Contactgegevens	NDS-cloud@minbzk.nl
Bijlage(n)	Zie hoofdstuk Bijlagen.
Auteur(s)	Programmateam NDS Cloud

Inhoud

Lijst van figuren en tabellen

1 Inleiding

Dit document beschrijft Het Ontwerp dat is ontwikkeld onder de Nederlandse Digitaliseringsstrategie (NDS), voor de Prioriteit 1 Cloud. Die staat bekend als de overheidsbrede soevereine clouddienst, in dit document genoemd 'Clouddienst'. Het Ontwerp beschrijft de gewenste start- en eindsituatie, met primaire focus op technologie, voor het mogelijk maken van de Clouddienst. De organisatieinrichting die hierbij hoort wordt in een ander traject uitgewerkt[1], waar uitgebreider wordt ingegaan op de organisatiekant van het leveren van een clouddienst.

De NDS is een samenwerking van Rijk, provincies, gemeenten, waterschappen, publieke dienstverleners (VDP) en uitvoeringsorganisaties (ZBO). Deze samenwerking was ook een belangrijk onderdeel van de totstandkoming van Het Ontwerp. Door middel van *pressurecooker*-sessies, schrijfdagen en feedbackrondes is met delegaties uit verschillende overheidslagen en organisaties gewerkt aan Het Ontwerp.

Aan de gemaakte keuzes ligt een Cloudmanifesto (zie § 2.2) en de Verkenning ten grondslag. Hierin staat onder andere de visie op de Clouddienst beschreven, volgens de kernwaarden soeverein, overheidsbreed (samen), veilig, privacy, open, betrouwbaar, continuïteit, transparantie, controle.

1.1 Scenario's

Kabinetsbrief
Met de kabinetsbrief van 1 juli 2026 heeft het kabinet de Tweede Kamer geïnformeerd over de Verkenning naar de soevereine overheidscloud en daarin een duidelijke voorkeur uitgesproken: "Het kabinet geeft de voorkeur aan een zo soeverein mogelijk ingerichte cloudomgeving die waar mogelijk wordt gehuisvest in de overheidsdatacenters (ODC's) van het Rijk. [...] Deze keuze sluit aan bij wat Gartner heeft beschreven als scenario A: een nieuwe soevereine overheidsclouddienst die onder centrale regie wordt neergezet."

Ontwerp
Over Het Ontwerp van deze Clouddienst, waarvan dit document de architectuurbasis vormt, schrijft het kabinet: "Samen met experts vanuit de overheid wordt een eerste ontwerp van soevereine clouddienst opgesteld. De focus van Het Ontwerp ligt op een containerplatform dat voldoet aan de Haven-standaard. Het Ontwerp is opgesteld op basis van open source (open en vrij beschikbare broncode), waardoor de leveranciersafhankelijkheid afneemt."

Vervolg
En over het vervolg: "Het Ontwerp van deze soevereine clouddienst wordt doorontwikkeld en zal binnenkort openbaar gemaakt worden zodat andere partijen kunnen bijdragen aan de doorontwikkeling en er zelf gebruik van kunnen maken. De regie blijft bij de overheid, maar marktpartijen en anderen, zoals onderwijs- en kennisinstellingen, worden nadrukkelijk uitgenodigd om bij te dragen."[2]

[1] De niet-technologie aspecten, die relevant kunnen zijn voor sourcings- en aanbestedingskeuzes, zijn in deze versie voor openbare review weggelaten. Daarover heeft nog geen besluitvorming plaatsgevonden
[2] Overheid zet in op eigen, veilige soevereine cloud - Digitale Overheid

Notitie verkenning
De kabinetsbrief is nader uitgewerkt in de Notitie Verkenning Overheidsbrede Soevereine Clouddiensten[3], die de voorkeursrichting als volgt samenvat: "Samengevat betekent de hiervoor opgebouwde richting een keuze voor scenario A, een nieuwe soevereine overheidsclouddienst die greenfield en vanuit centrale regie naast bestaande aanbod binnen de rijksoverheid (ODC's) en vanuit markt wordt neergezet. De beoordeling vanuit het NDS cloudprogramma van de door Gartner geschetste beelden maakt duidelijk dat dit het meest kansrijke scenario is."

De genoemde scenario's zijn afkomstig uit het onderzoek dat Gartner in opdracht van het NDS Cloudprogramma heeft uitgevoerd (Bijlage 1 – Gartner rapport Verkenning Soevereine Cloud). Gartner heeft de relevante soevereine cloudontwikkelingen in kaart gebracht en vier mogelijke scenario's voor de realisatie van de soevereine overheidscloud geïdentificeerd. Scenario A wordt in de notitie omschreven als "een volledig nieuwe, centraal aangestuurde overheidscloud die los van de bestaande systemen wordt opgebouwd".

Het Ontwerp is geschreven voor voorkeursscenario A: greenfield, centraal.

1.2 Uitgangspunt Ontwerp

1.2.1 Schaalbaarheid

Om alle betrokken partijen bij Het Ontwerp van de Clouddienst uit te dagen op de juiste schaal te denken, is gewerkt met een architectuur die moet kunnen schalen tot een ordegrootte van 50.000 fysieke servers[4]. Dit getal is een bewust globaal gekozen toetssteen, geen vraagprognose of beoogd afnamevolume: het dient uitsluitend om ontwerpkeuzes te toetsen aan een potentieel grote, overheidsbrede omgeving. De primaire focus in deze eerste fase ligt op het realiseren van een overheidsbreed soeverein containerplatform.

1.2.2 Soevereiniteit
In de context van de Clouddienst betekent soeverein dat de overheid volledige zeggenschap heeft over de technologiestack, de data, en de operatie. Deze zeggenschap moet aantoonbaar zijn en niet enkel een contractuele verplichting.

De definitie van een soevereine clouddienst en operationele autonomie volgens Cloud definities en begrippenlijst[5] is als volgt:

> **Soevereine clouddienst**
> Verzameling clouddiensten binnen het eigen rechtsgebied die voldoet aan de eisen voor datalocalisatie en operationele autonomie. De soevereine cloud moet ervoor zorgen dat de data, activiteiten, infrastructuurcomponenten en technologie niet kunnen worden beïnvloed door andere rechtsgebieden en beschermd moeten worden tegen directe invloed of toegang door overheden uit derde landen.
>
> **Operationele autonomie**

[3] Notitie Verkenning Overheidsbrede Soevereine Clouddiensten, NDS Cloudprogramma, 11 juni 2026 (bijlage bij de kabinetsbrief).
[4] Dit aantal is een educated-guess, op basis van statistische analyse en extrapolatie van de beleidsdoelstellingen, van het aantal servers dat nodig zou kunnen zijn voor de Clouddienst.
[5] https://pgdi.nl/files/cloud_definities_en_begrippenlijst_v1.0 16.04.2025 (vastgesteld door OBDO).pdf

Mogelijkheid van een afnemer om zelfstandig en zonder ongewenste afhankelijkheden beslissingen te kunnen nemen over het gebruik, beheer en de ontwikkeling van digitale technologieën ter ondersteuning van eigen processen.

Dit omvat tenminste:

- technologische keuzevrijheid,
- voldoende interne kennis hebben en onderhouden om zelf de interactie tussen eigen systemen en afgenomen Clouddiensten te begrijpen en aan te sturen,
- screening van eigen personeel,
- beperken van toegang tot cruciale onderdelen,
- controle van de *supply chain* van cruciale onderdelen en
- het borgen van bovengenoemde aspecten.

Het Ontwerp heeft betrekking op de infrastructuur voor de Clouddienst. Ook daarvoor is operationele autonomie van belang, om SEAL-4 te kunnen behalen. Borging van de daarvoor relevante controls worden elders verder uitgewerkt in het operating model, zie ook §1.9 Scope.

1.2.3 De mate van soevereiniteit

Software
De Notitie verkenning geeft sturing aan de mate van soevereiniteit voor de Clouddienst. Notitie § 2.3 adopteert het EU Cloud Sovereignty Framework (EUCSF). Het EUCSF hanteert meetbare niveaus van SEAL-0 tot SEAL-4. De afkorting SEAL staat voor Sovereignty Effectiveness Assurance Levels. De doelstelling voor de Clouddienst is het **SEAL-4** niveau met specifieke scope vanuit de Notitie.

"Daarbij kiest het NDS Cloudprogramma voor een duidelijke focus: eerst de basisclouddienst realiseren en inclusief bijbehorende dienstverlening opschalen.”
In technische termen: een open source containerplatform. Voor dat gedeelte is schaalgrootte het meest van belang en de focus op dat deel maakt de kennisopbouw realistischer. In de Nederlandse markt is hiervoor voldoende kennis aanwezig. De combinatie van SEAL4 en duidelijke focus vergroot haalbaarheid, beperkt de benodigde voorinvestering en reduceert de complexiteit."

Hardware
De Notitie kadert het ambitieniveau voor hardware van de Clouddienst als volgt.
"Een kanttekening daarbij is dat SEAL4 op een aantal punten genuanceerd moet worden. Met name op het gebied van hardware en de direct daarop werkende besturingssoftware is de wereldwijde toeleveringsketen een feit dat voorlopig niet verandert. Het EU Cloud Sovereignty Framework geeft voldoende richting om omtrent deze aspecten mitigerende maatregelen te nemen."

Voor de hardware stack geldt SEAL3 met de ambitie dit zo hoog mogelijk te krijgen. Op dit moment is SEAL4 voor de hardware stack nog niet mogelijk door het ontbreken van Europese leveranciers van CPU, GPU, ASIC’s, etc. Hiervoor volgen we nauwlettend en continue de ontwikkelingen vanuit de European Sovereign Tech Package, zoals de EU Cloud & AI Development Act, de EU Chips Act 2.0, en EU Open Source Initiative.

1.2.4 Open Source

In dit hoofdstuk duiden wij Open Source in de context van de Clouddienst.

De Cloud and AI Development Act (CADA)[6] en EU Open Source Strategy[7] zijn onderdeel van het EU Sovereign Tech Package. Het kabinet heeft daarop gereageerd[8] in het *Fiche: Cloud & AI Development Act*[9] en het *Fiche: Mededeling Europese Tech Soevereiniteit, inclusief Open Source Strategie*[10]. Belangrijke kanttekening hierbij is wel dat onderhandelingen over CADA nog moeten beginnen, waardoor de uitkomst vooralsnog onzeker is. Uit het Fiche:

"Het kabinet verwelkomt de Open Source Strategie en ondersteunt maatregelen die bijdragen aan open standaarden, interoperabiliteit, digitale gemeenschapsgoederen en de ontwikkeling van Europese open source alternatieven. Daarbij zal het kabinet verduidelijking vragen over de reikwijdte van het voorgestelde open-source-first-principe."

Ook Nederlandse Marktpartijen roepen op tot Open Source[11]. Het kabinet heeft daar op 3 juli jl. op gereageerd[12] en schrijft "het platform is zoveel als mogelijk gebaseerd op open source software.".

Om SEAL4 te kunnen halen schrijft het EUCSF het volgende voor, vertaald naar de Nederlandse context.

- SOV-4: "volledige beschikbaarheid van technische documentatie, broncode, en operationeel digitaal vakmanschap borgen lange-termijn autonomie"
- SOV-5: "oorsprong van software: waar en door wie de software architectuur en implementatie is bedacht, de locatie en jurisdictie waar de software governance (lifecycle management) is geborgd incl. packaging, distributie, en updates", en "mate van afhankelijkheid van niet-EU leveranciers, faciliteiten, of proprietary technologie", en "zichtbaarheid in de leverancier en leverancierskeketen, incl. auditeerbaarheid".
- SOV-6: "of de software toegankelijk is onder open licenties, met rechten om te auditen, aanpassen, herdistribueren, om transparantie en aanpasbaarheid te borgen".

Momenteel is er echter nog geen vastgesteld Overheidsbreed Open Source beleid. Wel staat in de Handleiding Wet hergebruik van overheidsinformatie (Who)[13]: "...dienen voorwaarden zo veel mogelijk gesteld te worden via standaardlicenties...". Er is wel een Overheidsbreed standpunt voor de inzet van generatieve AI[14], waarin specifiek voor Open Source gekozen wordt voor het hanteren van de Open Source Definitie van het Open Source Initiative.

Voor de Clouddienst wordt (ADR-003) ook de OSI-definitie gehanteerd met aanvullend criterium dat alle software *OSI-approved* is, niet (slechts) *OSI-compatible*, zodat kan worden voldaan aan SOV-4, SOV-5, en SOV-6. Hierbij citeren we uit het BNC-fiche:

---

[6] https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada
[7] https://digital-strategy.ec.europa.eu/en/policies/open-source-strategy
[8] Zie de volgende beschrijving hoe het kabinet de Beoordeling van Nieuwe Commissievoorstellen (BNC) vanuit de EU doet, via BNC-fiches: https://www.kcbr.nl/ontwikkelen-beleid-en-regelgeving/handleiding-wetgeving-en-europa/3-module-3-procedures/33-fase-voorstel-eu-regeling/3310-coordinatie-nederlandse-inbreng/3310b-bnc
[9] https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2026D33068&did=2026D33068
[10] https://www.tweedekamer.nl/kamerstukken/detail?id=2026D36414&did=2026D36414
[11] Zie bijvoorbeeld https://www.opencloudalliantie.nl/wp-content/uploads/2026/04/OCA%E2%80%94Manifest%E2%80%94Digitaal-2026.pdf
[12] https://www.tweedekamer.nl/downloads/document?id=2026D35322, 26643-1542
[13] https://minbzk.github.io/publicatie/hl/hwho/#voorwaarden
[14] https://www.rijksoverheid.nl/documenten/2025/04/16/het-overheidsbrede-standpunt-voor-de-inzet-van-generatieve-ai

"Het kabinet onderschrijft het belang van open source als fundamenteel middel ter versterking van technologische soevereiniteit".

1.3 Technologiestack

Het Ontwerp beslaat de volledige technologiestack, die uitgewerkt is in hoofdstukken 4 tot en met 7. Van de lagen datacenter en compute tot netwerk, basisfunctionaliteit, (generieke) platformservices, managed diensten en technische afhankelijkheden. Doorsnijdende thema's zoals security, doorbelasting, schaalbaarheid, en koppelvlakken op basis van open standaarden zijn voor elke laag uitgewerkt.

Het Operating Model wordt nog uitgewerkt, en bevat o.a. het Leveringsmodel. Dat betekent dat de Producten en Diensten, en daarmee de lagen van de technologiestack (en de interfaces) nog kunnen wijzigen. Dat wordt verwerkt in de volgende versie (2.0) van Het Ontwerp.

Met Het Ontwerp wordt zo goed mogelijk invulling gegeven aan de soevereiniteit onderdelen uit het EU Cloud Sovereignty Framework[15], de Haven standaard, de NIS2/Cyberbeveiligingswet, BIO2, de GDRP/Algemene Verordening Gegevensbescherming (AVG), CER/Wet weerbaarheid kritieke entiteiten (Wwke), ISO 42010.

1.4 Architectuurkeuzes

De gemaakte architectuurkeuzes liggen vast in zogenoemde Architectural Decision Records (ADR's). Deze set van ADR’s vormt een geheel met Het Ontwerp. Samen geven zij de nadere concretisering die nodig is om realisatie te sturen van de Clouddienst. Zij gaan een stap dieper dan de Domeinarchitectuur Overheidsclouddiensten[16].

Het Ontwerp wordt openbaar gemaakt, zodat ook marktpartijen hier gebruik van kunnen maken voor hun eigen dienstenaanbod, en hun diensten toetsen aan Het Ontwerp. Daarmee bundelt de overheid kennis en waarborgt zij interoperabiliteit tussen eventuele decentrale[17] implementaties, hoewel de Clouddienst vanuit de Notitie verkenning "scenario A" greenfields centraal wordt gerealiseerd.

Status van publicatie
De ADR's zelf worden op dit moment nog niet openbaar gepubliceerd. De set is nog in ontwikkeling: een deel van de besluiten is vastgesteld, terwijl een ander deel nog in bespreking is of nog moet worden genomen. Om te voorkomen dat het beeld ontstaat dat conceptkeuzes al definitief zijn, wordt terughoudend omgegaan met publicatie. Geïnteresseerden kunnen de actuele set opvragen bij het NDS Cloudprogramma[18]. Zodra de ADR's voldoende zijn uitgekristalliseerd, worden deze alsnog formeel gepubliceerd.

[15] https://commission.europa.eu/Cloud Sovereignty Framework, v1.2.1, oktober 2025
[16] https://pgdi.nl/Domeinarchitectuur overheidsclouddiensten v061.pdf, 04.06.2026
De Domeinarchitectuur Overheidsclouddiensten is onderdeel van de Architectuur Digitale Overheid (ADO), voor de Generieke Digitale Infrastructuur (GDI).
[17] De Clouddienst gaat uit van Open Architectuur, Open Standaarden, en Open Source. Dat maakt eventuele decentrale implementaties in principe mogelijk. Daar is echter niet voor gekozen voor realisatie van de Clouddienst. Zie de Notitie verkenning voor details.
[18] Via Postbus NDS-Cloud: NDS-cloud@minbzk.nl

1.5 Doelgroepen

Dit document is voor iedereen die betrokken is bij Het Ontwerp, de bouw, en de beoordeling van de Clouddienst. En voor de ontwikkelteams en andere gebruikers van de IaaS-diensten bij overheidsorganisaties. Het Ontwerp is opgesteld voor gebruik door:

- Chief Information Officers (CIO's) en Chief Technology Officers (CTO's) van overheidsorganisaties die inzicht willen in wat de Clouddienst gaat bieden, qua diensten en service niveaus (richten);
- Leden van het NDS Cloud Aanjaagteam die architectuurbesluiten willen toetsen aan de opdrachtdoelstellingen (richten);
- IT-architecten en technisch ontwerpers van overheidsorganisaties die willen aansluiten op de Clouddienst (inrichten);
- Clouddienstteam met DevSecOps-engineers die het platform en bijbehorende Clouddienst bouwen, leveren, beheren en doorontwikkelen (inrichten);
- Platformteams die het containerplatform afnemen en gebruiken (verrichten);
- Marktpartijen die willen aansluiten bij de implementatie van de Clouddienst, of het bestaande portfolio willen toetsen aan Het Ontwerp zoals vastgelegd in dit document.

De architectuur is bewust geschreven om een goede inhoud te representeren zonder te veel technische details te verliezen. Deze details staan verder uitgewerkt in de onderliggende ADR’s, ABB’s en andere bijlages. Meer beleidsmatige keuzes zijn vastgelegd in de Verkenning Clouddienst en de MIDO Domeinarchitectuur overheidsclouddiensten; dit document werkt daarop verder voor de Clouddienst.

1.6 Koppeling Proof of Concept

Het eerste ontwerp van de Clouddienst wordt "in een Proof of Concept gerealiseerd", met gebruik van "bestaande innovatie-voorzieningen"[19]. Het Ontwerp en de Proof of Concept (PoC) worden bewust parallel ontwikkeld: Het Ontwerp legt de keuzes vast die "voor soevereiniteit nodig zijn", de PoC toetst diezelfde keuzes in de praktijk "op een schaalgrootte die net groot genoeg is voor beproeving"[20]. Samen vormen zij het eerste ontwerp: geen "detailontwerp of in beton gegoten blauwdruk". Maar een levend document dat iteratief wordt doorontwikkeld.

Inzichten uit de beproeving werken namelijk door in de architectuur, en omgekeerd. Ontwerp en PoC kunnen daardoor op onderdelen tijdelijk van elkaar afwijken; ontwerpen en beproeven zijn hier bewust een leerproces. Signaleringen van inconsistenties tussen beide zijn in de review dan ook uitdrukkelijk welkom.

1.7 Leeswijzer

De inhoud van dit document is sturend geformuleerd en bedoeld om richting te geven aan Het Ontwerp en de bouw van de Clouddienst. Het document combineert architectuurprincipes, uitgangspunten, en een bouwsteenoverzicht per laag van de technologiestack en kan op twee manieren worden gelezen:

- Van voor naar achter: voor een volledig beeld van visie, producten, bouwblokken en kwaliteitseisen;
- Per laag: hoofdstuk 4 Producten en diensten is zo opgezet dat elke laag zelfstandig leesbaar is voor lezers met een specifiek vakgebied.

[19] Kamerbrief 'Stand van zaken verkenning soevereine overheidscloud', 1 juli 2026, https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2026D34379&did=2026D34379
[20] Notitie Verkenning Overheidsbrede Soevereine Clouddiensten, 11 juni 2026 (§ 2.6 en 2.7), https://www.tweedekamer.nl/kamerstukken/detail?did=2026D34382&id=2026D34382

Dit document is als volgt opgebouwd:

Hoofdstuk 2: Gaat in op de vragen waarom de Nederlandse overheid aan een overheidsbrede soevereine clouddienst werkt en waarom gekozen is voor de huidige aanpak.
Hoofdstuk 3: beschrijft de architectuurvisie, principes en uitgangspunten, (wettelijke) kaders, referentiekaders en -architecturen.
Hoofdstuk 4: beschrijft de producten- en dienstencatalogus die de Clouddienst levert, inclusief aansluitvoorwaarden en serviceniveau-afspraken.
Hoofdstuk 5: geeft het lagenoverzicht van de volledige technologiestack, per laag voorzien van een diagram, architectuurprincipes en conformiteitseisen.
Hoofdstuk 6: beschrijft hoe wordt voldaan aan de benodigde garanties, de niet-functionele eisen op het gebied van prestatie, beschikbaarheid, security, onderhoudbaarheid en portabiliteit.

1.8 Definities van architectuurdocumenten

Om de samenhang tussen de verschillende architectuurniveaus te borgen, hanteren we binnen dit document een vaste set definities. Deze documenten vormen samen het normatieve en richtinggevende kader voor de ontwikkeling van de Clouddienst.

Hieronder volgt het overzicht van de gehanteerde definities en hun specifieke rol binnen het architectuurlandschap:

- **Architectuur Digitale Overheid (ADO):** De ADO biedt het algemene architectuurkader waarbinnen de architectuur van de Clouddienst wordt ontwikkeld. De ADO verbindt bestuurlijke en maatschappelijke doelen met de inrichting van de digitale overheid. Dit is het hoogste niveau van architecturen binnen de overheid met daarin de domeinen Dienstverlening/ Interactie, Toegang, Gegevensuitwisseling en Infrastructuur.

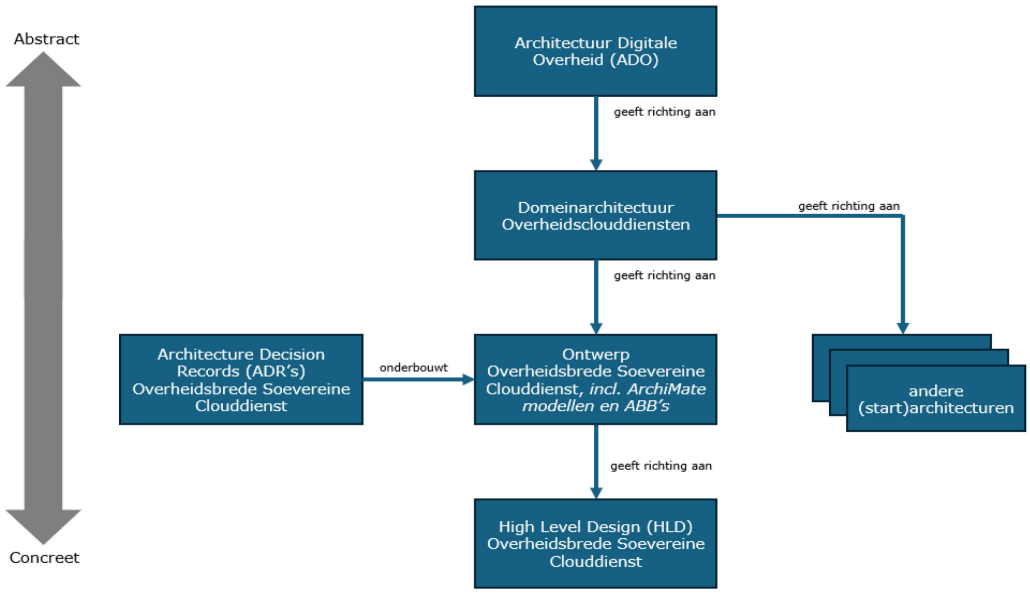
- **Generieke Digitale Infrastructuur (GDI):** De Generieke Digitale Infrastructuur is het stelsel van afspraken, standaarden en voorzieningen dat publieke dienstverleners gebruiken voor digitale dienstverlening aan burgers, ondernemers en andere publieke organisaties. De GDI is opgedeeld in vier hoofdomeinen: Toegang; Interactie; Gegevensuitwisseling; Infrastructuur.

- **Domeinarchitectuur Overheidsclouddiensten:** Deze domeinarchitectuur beschrijft het centrale overheidsmarktplaatsmodel voor clouddiensten en de kaders die gelden voor alle cloudaanbieders. Technologieneutraal en breed. De Overheidsbrede Soevereine Clouddienst (waar dit Het Ontwerp voor is) is één type cloudaanbod.

- **Globaal Ontwerp Overheidsbrede Soevereine Clouddienst:** Beschrijft wat de Clouddienst is in principes, uitgangspunten, bouwblokken en kwaliteitseisen van de Clouddienst als referentie-implementatie. Geeft richting aan het High Level Design.

- **Architecture Decision Records (ADR's) NDS Overheidsbrede Soevereine Clouddienst:** Vastgelegde architectuurbesluiten per technologielaag. Elke ADR beschrijft context, alternatieven, besluit en motivatie. De ADR's onderbouwen de keuzes in zowel Het Ontwerp als het HLD.

1.8.1 Samenhang architectuurdocumenten



Figuur 1-1 Samenhang tussen ADR's, Domeinarchitectuur, Ontwerp en HLD

1.9 Scope

Het Ontwerp beschrijft de architectuur van de Clouddienst. In de eerste fase ligt de focus op de bouw van een containerplatform met VM-ondersteuning voor gebruik door de hele Nederlandse overheid. Met behulp van feedback vanuit de markt en een (of meer) Proof of Concept(s) kan dit architectuurontwerp, en de ontwerpkeuzes die daarbij zijn gemaakt, getoetst en doorontwikkeld worden.

In de tweede fase wordt gekeken naar uitbreiding met Overheidsbrede Soevereine PaaS-diensten (Platform-as-a-Service). Dit kan leiden tot uitbreiding van de managed diensten van de Clouddienst die in deze versie beschreven zijn. Hiervoor zal door prioriteit 1. Cloud samengewerkt gaan worden met NDS prioriteit 2. Data en 3. AI om de roadmap op te stellen voor de dienstontwikkeling, die de deze sporen nodig hebben. Bovendien nemen we in deze fase de geprioriteerde behoefte mee die vanuit de NDS Cloud vraagarticulatie binnen de overheid wordt opgehaald.

In de derde fase wordt het mogelijk om uit te breiden naar Overheidsbrede Soevereine clouddiensten op applicatieniveau (Overheidsbrede Soevereine SaaS, Software-as-a-Service), i.e. gebruikmakend van de Clouddienst voor de onderliggende infrastructuur.

Op dit moment zijn de volgende onderdelen expliciet **buiten scope** van dit ontwerpdocument:

- Governance, organisatie inrichting, budgettering en dergelijke voor levering van de Clouddienst. Dit wordt nader uitgewerkt als onderdeel van het Operating Model. Voor de voortgang verwijzen we naar de Kabinetsbrief en de Verkenning.
- We halen de overheidsbehoefte (vraag) op via de NDS Cloud vraagarticulatie. Het Ontwerp heeft als doel richting te geven aan de realisatie van de Clouddienst (toekomstig aanbod). Het verwerken van input uit de vraagarticulatie is op dit moment out of scope. Dat doen we tijdens de doorontwikkeling van Het Ontwerp, dus bij de volgende versie (2.0).
- De centrale overheidsmarktplaats voor clouddiensten, zoals bedoeld in doelstelling 2 van de NDS Cloud en beschreven in het Globaal Ontwerp

Overheidsbrede Soevereine Clouddienst. De soevereine overheidsbrede clouddienst is één onderdeel, dat in de centrale overheidsmarktplaats voor clouddiensten terecht kan komen, naast andere aanbieders van soevereine clouddiensten. Dit is niet hetzelfde als het selfserviceportaal die in Het Ontwerp beschreven wordt, welke alleen diensten aanbiedt die gebruikt kunnen worden in de Clouddienst zelf.
    - De Clouddienst is niet bedoeld voor Hoog Gerubriceerde Informatie (HGI[21]).
    - SaaS-dienstverlening: aanvullende clouddiensten (applicaties), die gebruik kunnen gaan maken van de Clouddienst voor de onderliggende infrastructuur ("hosting") om Overheidsbrede Soevereine SaaS-diensten te gaan leveren.
    - Een digitale werkomgeving voor onder andere digitaal samenwerken (specifieke aanvullende SaaS-diensten, waarvoor grote behoefte is aan digitaal soevereinere oplossingen).
    - Data-analyse-, en AI PaaS-capabilities (bijvoorbeeld een data-/businessintelligence- /AI-Platform). De eisen en hiervoor benodigde doorontwikkeling wordt opgenomen op de Roadmap 2027 voor de Clouddienst, in afstemming met de NDS Prioriteiten 2. Data, en 3. AI.
- Oplossingen voor Identity & Access Management (IAM) als Tenant-IDP. Er is nu nog geen soevereine IAM oplossing beschikbaar die alle functionaliteiten uit de bekende IAM suites dekt. Daarom wordt tenant IAM federatief opgelost *(zie ADR-G06).* Afnemers gebruiken in eerste instantie hun eigen Identity Provider via een federatief koppelvlak (e.g. via SSO-Rijk/GovConext). Dat biedt hen bovendien een groeipad om de eigen IAM dienst/oplossing soeverein te maken op een tijdschaal die past bij de voor hen relevante lifecycle(s).

Relatie van Het Ontwerp tot NORA PSA

Op dit moment volgen we de NORA PSA Template niet volledig, omdat de governance (voor de leveringsorganisatie) en het operating model (hoe we de dienst leveren) nu buiten de scope van dit ontwerp vallen *(zie 1.9.2 Operationeel model en governance)*. Komend kwartaal wordt het operating model ontworpen. Daarna kunnen ook de invalshoeken Organisatie (NORA §4.2) en Beheer (NORA §7) verder worden uitgewerkt en toegevoegd.

1.9.1 Operationeel model en governance

De Clouddienst leveren vraagt om een uitgewerkt operationeel model: de inrichting van beheer, exploitatie, dienstverleningsprocessen en de bijbehorende besturing. Dit model is sterk afhankelijk van de nog te maken keuze over *build, run & maintain*. Oftewel, wie bouwt het platform, wie exploiteert en beheert het en onder welke afspraken? Zolang het in de Notitie Verkenning aangegeven voorkeursscenario op dit punt nog niet is uitgewerkt, blijft dat aspect ook in dit ontwerpdocument nog open. Het Ontwerp beschrijft daarom bewust geen operationeel model.

Ook governance, financiering, organisatie inrichting en exploitatie van de dienst vallen buiten de scope van dit document en worden op een later moment onder een ander mandaat uitgewerkt. Wat Het Ontwerp wél levert, is de technische basis voor een toekomstig operationeel model: een Cloud-native[22] architectuur die voldoet aan de vijf karakteristieken van Cloud computing. Dat zijn op afroep beschikbare selfservice, breed beschikbare netwerktoegang[23], gedeelde resources, snelle schaalbaarheid, en gebruik gebaseerde dienstverlening[24]. De architectuur stelt daarmee de operationele randvoorwaarden, zonder het operationeel model in te vullen.

[21] Dit betreft staatsgeheime of uiterst gevoelige data, waarvan openbaarmaking grote schade toebrengt aan de nationale veiligheid. Zie ook Figuur 2 van de Gartner-verkenning.
[22] Zie definitie in de "Cloud definities en begrippenlijst", https://www.tweedekamer.nl/downloads/document?id=2026D34380
[23] Breed beschikbare netwerktoegang betekent dat de clouddienst vanaf elke locatie, op elk moment en via elk type apparaat toegankelijk is via standaard netwerkverbindingen.
[24] Zie toelichting bij Gebruiksgebaseerde dienstverlening in 6.2 Prestatie-efficiëntie (prestatie en capaciteit).

2 Motivatie/ Ontwerp-keuzes

De keuzes die het NDS Cloudprogramma heeft gemaakt om tot Het Ontwerp te komen, hebben hun basis in de antwoorden op twee vragen. Waarom werkt de Nederlandse overheid aan een eigen Clouddienst? En waarom is gekozen voor de huidige aanpak? De antwoorden op beide vragen hebben te maken met afhankelijkheid, risico's en versnippering.

Deze afhankelijkheid is ook het vertrekpunt van de Verkenning[25]: "De afhankelijkheid van een klein aantal grote, niet Europese cloud- en softwareleveranciers creëert risico's die steeds moeilijker te negeren zijn." De notitie Verkenning benadrukt dit met de casussen van het afgesloten e-mailaccount van de hoofdaanklager van het Internationaal Strafhof en het faillissement van de Amsterdam Trade Bank, beide mede als gevolg van Amerikaanse sancties.

2.1 Risico's

De Nederlandse overheid is sterk afhankelijk van digitalisering voor het uitvoeren van haar kerntaken. Daarbij verwerkt zij dagelijks grote hoeveelheden informatie van en over burgers en bedrijven. Om al die informatie veilig op te slaan en te verwerken is de overheid in toenemende mate afhankelijk geraakt van een beperkt aantal grote, niet-Europese cloudaanbieders (*hyperscalers*). Deze afhankelijkheden brengen drie soorten risico's met zich mee.

- **Extraterritoriale risico's**
  Juridische en economische risico's die ontstaan wanneer de wet- en regelgeving van een ander land van toepassing wordt op activiteiten in Nederland. De Amerikaanse CLOUD Act (2018)[26] verplicht Amerikaanse technologiebedrijven om op verzoek van Amerikaanse autoriteiten toegang te verlenen tot data die zij beheren, ook als die data zich in Europa bevinden *(zie ook Bijlage 3 – Wetgeving)*. Voor Europese overheidsdata die op Amerikaans-beheerde cloudinfrastructuur staan, is deze wet direct van toepassing. Vergelijkbare wetgeving bestaat in andere landen. Juridische bescherming via contracten of datalocatie-afspraken is niet afdoende zolang het technologiebedrijf buiten EU-jurisdictie valt.

- **Geopolitieke continuïteitrisico's**
  Recente geopolitieke ontwikkelingen tonen aan dat toegang tot commerciële technologie-infrastructuur niet vanzelfsprekend is. Exportrestricties, handelsconflicten en sancties kunnen de beschikbaarheid van cloudinfrastructuur beïnvloeden. Bijvoorbeeld niet-Europese techreuzen die onder druk van nationale veiligheidswetgeving verplicht worden om diensten aan bepaalde landen per direct te ontzeggen. Ook hybride oorlogsvoering en gerichte sabotage zijn een risico. Vitale cloud- en netwerkinfrastructuur kunnen worden aangevallen of ontregeld tijdens geopolitieke conflicten.

- **Marktconsolidatierisico's**
  De cloudmarkt is sterk geconcentreerd. Een klein aantal aanbieders heeft een dominantie positie verworven. Dat leidt tot prijszettingsmacht, lock-in via propriëtaire (private) diensten en beperkte onderhandelingsruimte. Er zijn diverse recente voorbeelden met abrupte licentiewijzigingen en extreme

[25] https://www.tweedekamer.nl/downloads/document?id=2026D34382
[26] https://www.govinfo.gov/content/pkg/PLAW-115publ141/html/PLAW-115publ141.htm

kostenstijgingen als gevolg. Overheidsorganisaties die voor vitale bedrijfsprocessen afhankelijk zijn van één aanbieder zijn, zonder reële uitwijkmogelijkheid op de korte termijn, structureel kwetsbaar op dit punt.

Naast deze drie risicocategorieën is er bij de Nederlandse overheid ook sprake van zeer grote versnippering van clouddiensten en kennis. Een soeverein cloudplatform ontsluit kennis voor alle overheden, maakt de ontwikkeling van meer clouddiensten efficiënter en biedt betere controle op de locaties waar data wordt verwerkt en opgeslagen voor risicovolle processen.

Deze risico's en de versnippering maken van digitale soevereiniteit geen abstracte ambitie, maar een strategische noodzaak. Het uitvoeren van de kerntaken van de overheid en het leveren van veilige en betrouwbare dienstverlening aan burgers en bedrijven mogen niet verstoord worden. Om dit waar te maken is zeggenschap over de infrastructuur waarop deze diensten draaien, absoluut noodzakelijk.

2.2 Cloudmanifesto

Voor Het Ontwerpen en realiseren van de Clouddienst hanteerden we acht Architectuuruitgangspunten en vier Strategische en Governance uitgangspunten, samengebracht in een Cloudmanifesto.

Acht architectuuruitgangspunten

1. **De Clouddienst is aantoonbaar soeverein**, dit realiseren we door gebruik te maken van het EU Cloud Sovereignty Framework. SEAL-4 voor de software, SEAL-3 voor de hardware.

2. **De Clouddienst is een échte clouddienst**, die aan de vijf essentiële karakteristieken van een cloud[27] voldoet:

   - Op afroep beschikbare selfservice;
   - Breed beschikbare netwerktoegang;
   - Gedeelde resources;
   - Snelle schaalbaarheid;
   - Gemeten dienstverlening.

3. **De Clouddienst is secure by design**, security is een basis voor elke component van de Clouddienst.

4. **De Clouddienst is schaalbaar**, zodanig dat wordt voorzien in de cloudvraag van de gehele overheid.

5. **De Clouddienst is gebaseerd op Open Architectuur, Open Standaarden én Open Source oplossingen,** ook de architectuur en aanverwante documenten zijn zoveel mogelijk open source.
   - We vermijden afhankelijkheid van software met één leverancier, en accepteren géén niet-OSI-licenties, zoals onderbouwd in 1.2.4
   - We bouwen voort op bestaande open-source-implementaties in plaats van opnieuw uitvinden.

6. **De Clouddienst is een modern (cloud-native) platform**, ook als dit betekent dat op dag één nog niet alle bestaande (legacy) workloads naar dit

[27] Cloud definities en begrippenlijst v1.0 d.d. 25.03.2026 (definitief)

platform kunnen migreren.

7. **De Clouddienst is gebaseerd op eenvoud boven volledigheid**. Een kleine, goed werkende set bouwblokken vinden we belangrijker dan een platform dat alle mogelijke functionaliteit bevat.

8. **De Clouddienst wordt incrementeel gerealiseerd**, we realiseren allereerst een basisfunctionaliteit, die we vervolgens verbeteren en uitbreiden.

Vier strategische en governance-uitgangspunten

1. **De overheid heeft de regie en bepaalt de maatvoering**
   Omdat soevereiniteit niet stopt bij techniek gaat de overheid meer regie nemen, en de aanwezige kennis binnen de overheid en in Nederland (beter) bundelen en benutten. De overheid bepaalt de richting, de architectuur en de regels en bepaalt de 'maatvoering' inzake de technische standaarden, specificaties, omvang en inrichting van de systemen.

2. **Eerst een soeverein platform**
   We willen allereerst IaaS-containerdiensten beschikbaar maken en werken daarom aan het realiseren van een technisch uitvoerbaar Ontwerp. Het Ontwerp gebruiken we, om in nauwe samenwerking met overheidspartijen en marktpartijen deze soevereine Clouddienst te bouwen.

3. **Zo hoog mogelijke mate van digitale soevereiniteit**
   De NDS heeft een soevereiniteitsambitie geformuleerd die gericht is op een zo hoog mogelijke mate van digitale soevereiniteit, waarbij eigenaarschap, controle, onafhankelijkheid, continuïteit en vertrouwelijkheid van overheidsdienstverlening geborgd zijn.

4. **Nieuw naast bestaand**
   Op dit moment hanteren we als uitgangspunt voor Het Ontwerp dat we een nieuwe Clouddienst bouwen naast de al bestaande initiatieven in overheidsland.

2.3 Modelkeuze

In de Verkenning Soevereine Clouddienst van 30 april 2026 (Bijlage 1 – Gartner rapport Verkenning Soevereine Cloud) beschrijft onderzoeksbureau Gartner vier mogelijke scenario's. Parallel in een sessie met een brede vertegenwoordiging van architecten uit overheidsorganisaties, is op 9 maart 2026 gekozen voor model 3 (zie onder): Het Ontwerpen op basis van losse opensource-oplossingen. Deze keuze biedt maximale keuzevrijheid en de hoogste onafhankelijkheid. Deze keuze is gedreven door scenario A uit het Gartneronderzoek dat in de Verkenning is gekozen als scenario.

Tabel 1: Keuze architectuurmodel voor de Clouddienst (ADR-001)

Model	Omschrijving	Afweging
1. OpenStack IaaS	Bewezen platform, gedragen door de OpenStack Foundation. Breed ingezet bij telecombedrijven en overheden.	**Afgevallen.** OpenStack is een monolithische stack die sterk is gericht op virtualisatie-paradigma's uit het pre-container tijdperk. Hoge integratielast, beperkte Kubernetes-native integratie.

Model	Omschrijving	Afweging
2. Europees geïntegreerd product	Aanbod van Europese cloudleveranciers (OVHcloud, IONOS, Exoscale e.a.) of geïntegreerde platformproducten.	**Afgevallen.** Beperkt aanbod op de vereiste schaal, leveranciersafhankelijkheid van een ander soort maar niet minder. Onvoldoende controle over de technologiestack.
3. CNCF-componenten op bare-metal	Samenstelling van losse opensource CNCF-componenten (Europese opensourceprojecten zoals NeoNephos zijn ook in scope) tot een Kubernetes-platform dat rechtstreeks op fysieke servers draait, zonder onderliggende virtualisatie laag (bare-metal) en zonder afhankelijkheid van één leverancier of product.	**Gekozen.** Maximale leveranciersonafhankelijkheid, volledig auditeerbare opensource stack, CNCF-community biedt continuïteitsgaranties, aansluiting op internationale industriestandaard.

Tijdens de eerste sessie verwees dit model naar CNCF[28]-componenten (Cloud Native Compute Foundation). Inmiddels is geconstateerd dat vanwege soevereiniteit focus op Europese opensourceprojecten en in het bijzonder NeoNephos[29] van belang is.

Het gevolg van deze keuze is dat werken met deze bouwblokken substantiële investering vereist in expertise. Dat kost tijd en vraagt om een andere aanpak, die van kennis investeringen binnen de overheid. Hierin zit ook een kans om samen met de markt de kennispositie van Nederland op het gebied van Cloud te versterken.

2.3.1 De invulling: incrementeel en nieuw naast bestaand

De richting voor de invulling is vastgelegd in de Notitie. De Notitie kiest voor de Clouddienst die "greenfield en vanuit centrale regie naast bestaande aanbod binnen de rijksoverheid (ODC's) en vanuit markt wordt neergezet" (Notitie § 1.1) en stelt als randvoorwaarde centrale regie op vraagbundeling en fasering, "zodanig dat sprake is van minimum gegarandeerde afname en gecoördineerde opschaling in de periode 2027 – 2030 (met verdere groei daarna)" (Notitie § 3.4).
Het Ontwerp voegt daar de architectuurconsequenties aan toe:

Start met de kern: de Clouddienst begint met IaaS voor containers met mogelijkheid voor virtuele machines via KubeVirt (ADR-C03). Daarna wordt incrementeel uitgebreid naar een breder managed-dienstenaanbod, op basis van bewezen vraag. Een "big-bang"-migratie is operationeel en bestuurlijk niet realistisch gezien bestaande IT-investeringen en lopende contracten.

Nieuw naast bestaand: de Clouddienst wordt gebouwd als nieuwe infrastructuur naast de bestaande cloud omgevingen. Nieuwe workloads kunnen direct van de Clouddienst gebruikmaken; bestaande workloads migreren op een logisch moment in de eigen contract- en levenscyclus, binnen de centraal geregisseerde vraagbundeling en fasering.

[28] https://www.cncf.io/
[29] https://neonephos.org/

Deze aanpak maakt de Clouddienst productierijp op een realistisch tijdpad, terwijl de architectuur is ontworpen voor de volledige beoogde schaal: tienduizenden servers, tientallen tot honderden tenants (overheidsorganisaties), meerdere regio's.

2.4 Succesfactoren voor de Clouddienst

Voor succesvolle positionering en adoptie van de Clouddienst zijn o.a. tijdens de *pressurecooker*-sessies de kritieke succesfactoren opgehaald. Deze lijst is te lezen in Bijlage 4 – Lijst van succesfactoren Overheidsbrede Soevereine clouddienst. Daarin is een prioritering aangebracht. Voor succesvolle levering van de Clouddienst onderkennen we de volgende drie pijlers.

2.4.1 Organisatie-onafhankelijkheid en gestandaardiseerde dienstverlening

De basisdienstverlening moet vanaf de start een volwassen en onafhankelijk karakter hebben om drempels voor afnemers te minimaliseren.

- **Positionering buiten bestaande structuren:** Exploitatie en beheer van de Clouddienst worden losgekoppeld van bestaande overheidsorganisaties om duidelijke rolverdeling te borgen. Hoewel dit als succesfactor is aangemerkt, is dit niet verder beschreven in Het Ontwerp omdat het Operating Model en de Governance nog nader worden uitgewerkt.
- **Hoge toegankelijkheid:** De Clouddiensten zijn via laagdrempelige, gestandaardiseerde mechanismen en interfaces afneembaar voor de doelgroep.

2.4.2 Solide en duurzaam financieringsmodel

Het financieringsmodel moet de adoptie stimuleren en de continuïteit van het platform op de lange termijn borgen.

- **Centrale basisfinanciering (Vaste kosten):** Vaste infrastructuur-, platform-, en organisatiekosten worden centraal en overheidsbreed gefinancierd. Dit voorkomt *first mover disadvantage*, waarbij de eerste afnemers onevenredig zwaar worden belast met initiële opstartkosten.
- **Variabele kosten op basis van verbruik:** Het operationele gebruik wordt transparant inzichtelijk gemaakt op basis van daadwerkelijk verbruik conform een nader op te stellen financieringsmodel (e.g. *pay-per-use,* volgt uit Operating Model).
- **Structureel innovatiebudget:** In de centrale bekostiging is een structureel, langjarig innovatiecomponent opgenomen. Dit garandeert de financiële ruimte voor continue doorontwikkeling en *lifecyclemanagement* van de Clouddienst.

2.4.3 Generieke randvoorwaarden, security & transparantie

- **Voldoende aansluittijd:** overheidsorganisaties dienen voldoende tijd te hebben om in te stappen, op een logisch moment van hun eigen relevante levenscycli (e.g. de contractuele levenscyclus, infra platform levenscyclus, etc.).
- **Brede overheidsbeschikbaarheid:** de Clouddienst is ontworpen om beschikbaar en toegankelijk te zijn voor álle Bestuurslagen van de overheid en overheidsorganisaties. Dit moet leiden tot duidelijkheid vooraf welke organisaties afnemer mogen zijn zodat een complex onboardingsproces vermeden wordt.
- **Overheidsbreed vertrouwd securitybeleid:** Privacy- en security kaders, richtlijnen, standaarden, policies, en audits worden uitgevoerd op basis van overheidsbreed vastgesteld beleid en de auditrapportages zijn te allen tijde inzichtelijk voor alle gebruikers van de Clouddienst. Dit voorkomt dat afnemers individuele audits moeten uitvoeren voorafgaand aan gebruik van de Clouddienst.
- **Transparantie en auditeerbaarheid (SEAL):** Het platform biedt volledige transparantie en auditeerbaarheid ten aanzien van de Sovereignty Evaluation and Assurance Levels (SEAL) over alle dieperliggende componenten.

3 Architectuurkaders

3.1 Referentiearchitecturen

Omdat de Clouddienst alle overheden bedient, gelden alle standaarden en afspraken voor de verschillende bestuurslagen en overheidsorganisaties. Het Ontwerp is daarom gebaseerd op de volgende referentie architecturen en afgeleiden daarvan.

NORA	Nederlandse Overheid[30]	https://www.noraonline.nl/NORA
RORA	Rijksoverheid	https://www.roraonline.nl/RORA
PETRA	Provincies	https://petra.wikixl.nl/PETRA
WILMA	Waterschappen	https://www.wilmaonline.nl/WILMA
GEMMA	Gemeentes	https://www.gemmaonline.nl/GEMMA

RORA conformeert aan NORA en heeft naast definities ook handreikingen met betrekking tot leveranciersafhankelijkheid en exitstrategie. De definities van RORA zijn gebruikt in het vastgestelde begrippenkader cloud[31], versneld door het NDS Cloudprogramma. De waterschappen en provincies hebben voor hun cloudbeleid aangegeven WILMA en PETRA te conformeren aan de NDS en NORA[32].

GEMMA hanteert andere uitgangspunten naast NORA. Waar NORA alleen refereert aan het gebruik van open standaarden en de Pas-toe-of-leg-uit-lijst, gaat GEMMA verder met de principes van Common Ground en het gebruik van de HAVEN-standaard. Dat stimuleert cloudnative ontwikkelen en portabiliteit om leveranciersafhankelijkheid en *vendor lock-in* te voorkomen[33]. Deze standaard is meegenomen in Het Ontwerp.

3.2 Standaarden

De Clouddienst adopteert de standaarden van Forum Standaardisatie. De ABB's en ADR's beschouwen op detailniveau voor elke standaard welke specifiek op de betreffende ADR's en/of ABB's van toepassing is. Een wisselwerking hiervan met de ABB's en Het Ontwerp is voorzien vanuit het nader op te stellen High Level Design, zodra de Solution Bouw Blokken (SBB's) verder worden uitgewerkt. Dat wordt meegenomen in de volgende versie van Het Ontwerp (2.0).

Daarnaast zijn diverse standaarden nog niet opgenomen door Forum Standaardisatie, die wel voorzien in een behoefte, zoals:

- De cloud standaarden ISO27017 en ISO27018;
- HAVEN/HAVEN+[34]standaarden en "de facto" commerciële dataportabiliteits-standaarden;
- European Cloud Sovereignty Framework SEAL;
- NIST-standaarden en richtlijnen.

Voor de lijst van gehanteerde standaarden in Het Ontwerp, zie Bijlage 6 – Relevante standaarden en toetsingskaders.

[30] NORA is, per kabinetsbesluit, van toepassing op de gehele overheid.
[31] Samen versnellen is dezelfde 'cloudtaal' spreken | Digitale Overheid
[32] In de formele bestuurlijke reactie van de Unie van Waterschappen wordt verklaard dat cloudinzet van de Waterschappen volledig aansluit bij de prioriteiten van de NDS. Op noraonline.nl, wilmaonline.nl en petra.wikixl.nl is vastgelegd dat WILMA en PETRA dochters zijn van NORA
[33] Bron: GEMMA Online en Haven Commonground)
[34] HAVEN+ is nog geen standaard vastgesteld door het OBDO, HAVEN is dat wel.

3.3 Architectuur Digitale Overheid (ADO)

De Architectuur Digitale Overheid (ADO) vormt de architectuurvisie op de Digitale Overheid en geeft richting aan de ontwikkeling van de gemeenschappelijke basis[35]. Het is hiermee een toekomstgericht stuurinstrument voor de meerjarenprogrammering en het richten van investeringen. Het zorgt voor herkenbare elementen waarmee overheidsorganisaties hun eigen dienstverleningsprocessen en interne processen kunnen opbouwen en stelt ons gezamenlijk in staat om wendbaar te blijven en in te kunnen spelen op toekomstige ontwikkelingen.

De ADO is gestructureerd volgens domeinen. De Clouddienst is gepositioneerd in het domein Infrastructuur. Daarbij zijn er afhankelijkheden met andere domeinen voorzien, zoals Toegang, Gegevensuitwisseling, Interactie en met toekomstige ontwikkelgebieden zoals AI en Digitale Werkomgeving.

Centraal in de ADO is het denken in functionele bouwblokken: Waartoe de digitale overheid in staat moet zijn wordt per domein functioneel omschreven zonder meteen over specifieke voorzieningen te spreken. Dit geeft ruimte om nationaal en internationaal aan te haken op wat er al ontwikkeld wordt, en voorkomt dat de architectuur vastzit aan de voorzieningen van vandaag.

Niet ieder denkbaar Functioneel Bouwblok heeft een plaats in de Architectuur Digitale Overheid, het gaat uitsluitend om die bouwblokken waarvoor geldt dat we deze als overheid gemeenschappelijk invullen: omdat samenwerking wettelijk vereist of voor interoperabiliteit noodzakelijk is, omdat een gezamenlijke aanpak de dienstverlening aan burgers, ondernemers of ambtenaren verbetert, of omdat samen optrekken substantieel bespaart of een ander publiek belang dient.

3.3.1 Generieke Digitale Infrastructuur (GDI)

De Generieke Digitale Infrastructuur (GDI) is de daadwerkelijke operationele ruggengraat.

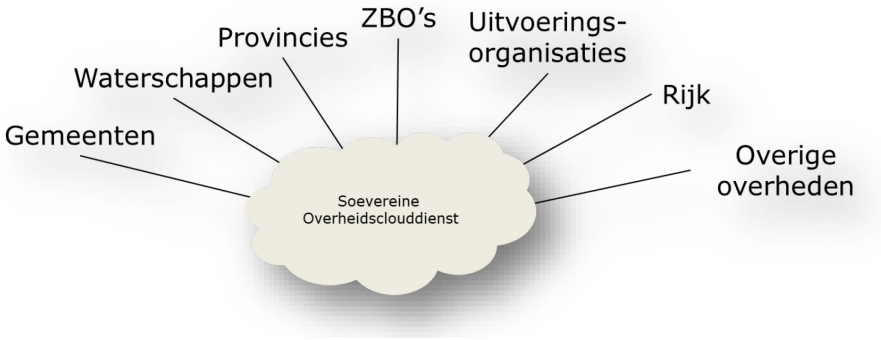
De Clouddienst wordt zodanig ontworpen dat deze zou kunnen passen binnen de GDI-systematiek van afspraken, standaarden en voorzieningen. Daarmee zou de dienst dan niet alleen technisch bruikbaar zijn, maar ook bestuurlijk, financieel, juridisch en operationeel kunnen passen binnen de governance-, financierings- en besluitvormingskaders van het Meerjarenprogramma Infrastructuur Digitale Overheid (MIDO). Nadere besluitvorming daarover is buiten scope van Het Ontwerp en wordt in een ander gremium onder een ander mandaat genomen.

Dit betekent dat de Clouddienst een samenhangend geheel kan worden van:

- **Afspraken:** een overeengekomen, vastgelegde en gepubliceerde regel over inrichting, gebruik, governance, financiering, levering, beveiliging of doorontwikkeling van de Clouddienst.
- **Standaarden:** een vastgestelde norm, specificatie of werkwijze die voorschrijft hoe diensten, technologieën, processen, interfaces of gegevensuitwisseling worden ingericht en beheerd.
- **Voorzieningen**: een concrete groepering van services, platformcomponenten, beheerfuncties of hulpmiddelen die aan afnemers of beheerorganisaties wordt aangeboden.

[35] Er wordt momenteel gewerkt aan de 2026 herziening van de ADO.

De Clouddienst zal door álle Bestuurslagen van de Overheid en Overheidsorganisaties te gebruiken zijn.



Figuur 3-1 Gebruikers van de nieuwe Overheidsbrede Soevereine Clouddienst

Dat vraagt om generieke, Overheidsbrede voorzieningen met een combinatie van eigenschappen die op dit moment door geen van de bestaande voorzieningen volledig wordt geboden (zoals GDI, tot nog toe primair gericht op dienstverlening aan burgers en ondernemers, of het ICBR (Interdepartementale Commissie Bedrijfsvoering Rijksdienst, gericht op Rijksbrede bedrijfsvoering). Voor de Overheidsbrede Clouddienst moet daarom nog beoordeeld worden of dit een nieuwe voorziening wordt, of een variant die groeit vanuit een van de bestaande voorzieningen.

3.3.2 ADO Domein Infrastructuur

Voor Het Ontwerp zijn de Functionele Bouwblokken voor het domein Infrastructuur verder uitgewerkt naar wat nodig is om de Clouddienst te kunnen leveren en beheren. De gedefinieerde Functionele Bouwblokken voor het domein infrastructuur zijn:

Cloudinfrastructuur	*Het vermogen om cloud-technologie in te zetten met behoud van regie over data, diensten en leverancierskeuze - zodat de overheid niet afhankelijk wordt van één platform of aanbieder.* Cloudinfrastructuur wordt hier breed opgevat: niet alleen als technische platformlaag, maar als het geheel van capabilities waarmee clouddiensten worden bestuurd, geleverd en bewaakt. Het omvat de capabilities voor regie, levering en kwaliteitsbewaking van clouddiensten. Onderdelen daarvan worden nader uitgewerkt in het Operating Model.

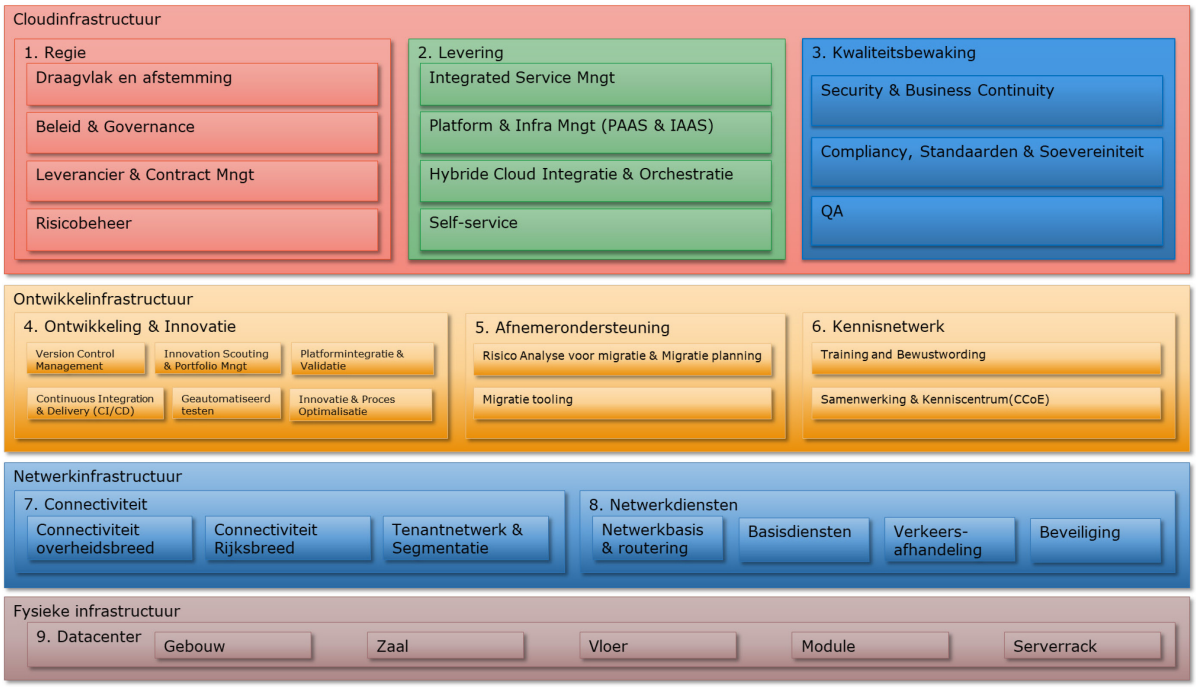
Ontwikkelinfrastructuur	*Het vermogen om ontwikkelteams te ondersteunen bij het ontwikkelen en beheren van software zonder ongewenste platformafhankelijkheden. Dit omvat maar is niet beperkt tot platform engineering.* Omvat de capabilities voor doorontwikkeling van de Clouddienst en ondersteuning van afnemers, zoals ontwikkelstraat, test- en automatiseringstooling, de platformintegratie en validatie van software en hardware op het platform, migratieondersteuning, templates, kennisnetwerk en platformengineering[36].
Netwerkinfrastructuur	*Het vermogen om een vertrouwde en betrouwbare overheidsinfrastructuur met connectiviteits- en toegankelijkheidsdiensten te gebruiken, voor het gebruik van clouddiensten en breder.* Meer toegespitst gaat het hierbij om het vermogen om de Clouddienst bereikbaar en koppelbaar te maken[37]. Dit wordt nader onderzocht en verder uitgewerkt in de volgende versie van Het Ontwerp.
Fysieke infrastructuur	Omvat datacenterfaciliteiten zoals racks, stroom, koeling, fysieke beveiliging, bekabeling en gebouwgebonden continuïteit.

[36] Platformengineering: het standaardiseren en automatiseren van ontwikkel- en beheerpatronen voor platformteams en afnemers

[37] De technische uitwerking daarvan in ABB's staat in de Netwerklaag van hoofdstuk 5.

3.3.3 Domein Infrastructuur capability map

Onderstaand figuur toont de capabilities die in Het Ontwerp zijn geïdentificeerd als noodzakelijk voor het leveren, beheren en doorontwikkelen van de Clouddienst. Herijking volgt na oplevering van het Operating Model. De capability map is een ontwerp-uitwerking op basis van het ADO-domein Infrastructuur en vormt de brug naar de ABB's in hoofdstuk 4 en 5.



Figuur 3-2 Capability map Domein Infrastructuur

Zie Bijlage 7 – Toelichting § 3.3 ADO domein Infrastructuur, paragraaf *ADO Level 3 Domein Infrastructuur*.

3.3.4 Architectural Building Blocks (ABB's) en capabilities

Capabilities beschrijven wat het ADO domein Infrastructuur moet kunnen om de Clouddienst te leveren. Architectural Building Blocks beschrijven vervolgens met welke logische bouwblokken deze capabilities worden gerealiseerd.

De ABB-capabilitymatrix in Bijlage 8 – Het Ontwerp Artefacten maakt deze relatie expliciet en laat zien welke ABB's primair of ondersteunend bijdragen aan welke capability.

4 Producten en diensten

Dit hoofdstuk toont de producten en diensten zoals gedefinieerd voor de Clouddienst. De scope hiervan is de Clouddienst zelf, niet (voortbrenging van) applicaties/oplossingen die ervan gebruikmaken. Dit hoofdstuk beschrijft louter de diensten zoals de afnemer van die diensten deze ervaart en niet de onderliggende technologiestack waarmee de technologiediensten worden gerealiseerd.

Leeswijzer ArchiMate-diagrammen
De in dit hoofdstuk opgenomen ArchiMate-diagrammen dienen primair ter visuele herkenning en ter ondersteuning van de tekstuele beschrijvingen. De volledige en interactief leesbare modellen zijn beschikbaar als ArchiMate export *(Bijlage 8 – Het Ontwerp Artefacten)*. Geadviseerd wordt deze export in een ArchiMate-tool te laden en daar de platen te raadplegen voor detailanalyses.

4.1 Productenoverzicht

De productenportefeuille bestaat in de basis uit twee producten:

1. Product **Soevereine Cloud-native Hosting** als NDS-clouddienst voor het ontwikkelen en hosten van container-gebaseerde applicaties door de afnemer

2. Product **Soevereine Virtual Machine Hosting** als NDS-clouddienst voor het hosten van Virtual Machines (virtuele servers) met middleware en applicatiesoftware beheerd door de afnemer

In het ecosysteem van dienstenaanbieders en –afnemers wordt daarnaast voorzien in het volgende product:

3. Product **Robuuste Datazaal** voor het realiseren van de benodigde technologiestack voor bovenstaande producten. Voor de *afnemer* van NDS Clouddiensten is dit product niet relevant.

Tot slot wordt in dit ecosysteem geanticipeerd op een Selfserviceportaal van soevereine clouddiensten geleverd door marktpartijen die gebruikmaken van het product Soevereine Cloud-native Hosting:

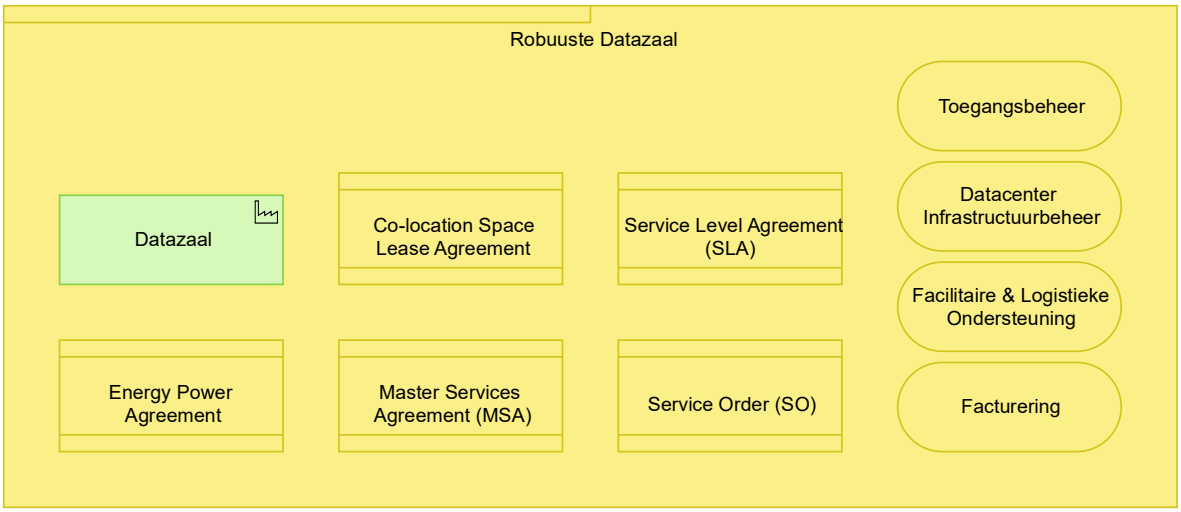
4. Product **Selfserviceportaal Soevereine PaaS Dienst** (in verschillende verschijningsvormen) die de afnemer verder faciliteert in applicatieontwikkeling en –beheer.

5. Product **Selfserviceportaal Soevereine SaaS Dienst** (in verschillende verschijningsvormen) waarbij complete applicaties worden geleverd die door de afnemer alleen nog maar geconfigureerd dienen te worden.

Elk product is opgebouwd uit de geleverde technologiediensten, de bijbehorende ondersteunende diensten en contractuele afspraken. Deze zijn uitgewerkt in de volgende paragrafen.

4.2 Robuuste Datazaal

Het product Robuuste Datazaal wordt door een nationale aanbieder of meerdere lokale aanbieders verhuurd aan de aanbieder van de Soevereine Hostingproducten.



Figuur 4-1 Decompositie Robuuste Datazaal

Fysieke beveiliging is onderdeel van toegangsbeheer zodat alleen personeel van de aanbieder van Soevereine Hostingproducten toegang heeft tot de gehuurde ruimte. De aanbieder van Soevereine Hostingproducten is zelf verantwoordelijk voor het kiezen van geschikte locaties waarmee voldoende beschikbaarheid kan worden gerealiseerd.

4.3 Soevereine Cloud-native Hosting

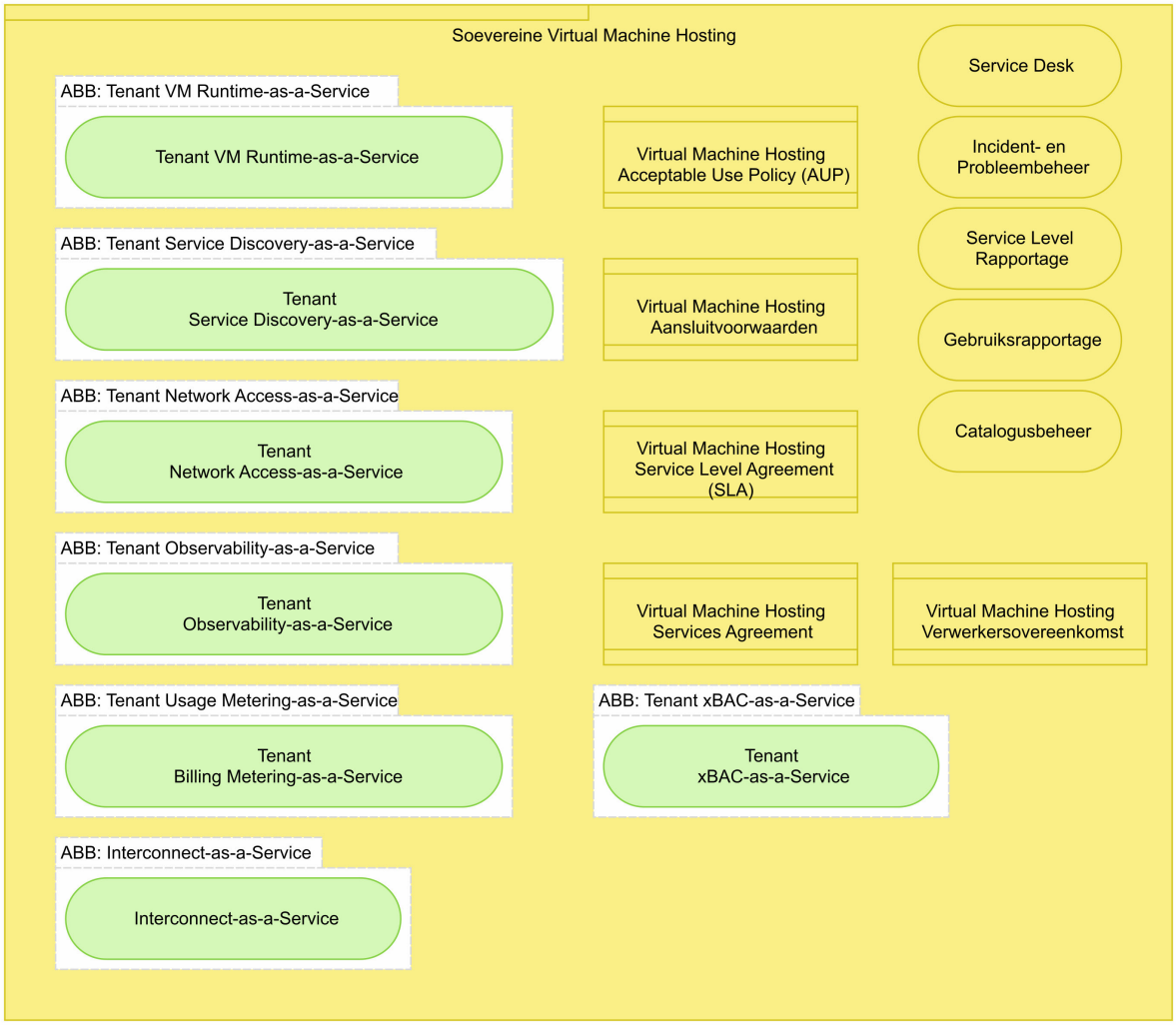
Het product Soevereine Cloud-native Hosting vormt de kern van de NDS-productenportefeuille.

Figuur 4-2 Decompositie Soevereine Cloud native Hosting

De afnemer van dit product krijgt een of meerdere eigen Tenant Kubernetesclusters inclusief Kubernetes control plane voor clusterbeheer. Daarnaast worden extra technologiediensten aangeboden om het eigen cluster effectief als platform te kunnen inzetten. Ondersteuning wordt geboden op basis van standaard ITSM-processen.

4.4 Soevereine Virtual Machine Hosting

Het product Soevereine Virtual Machine Hosting wordt aangeboden door dezelfde aanbieder die het product Soevereine Cloud-native Hosting aanbiedt.

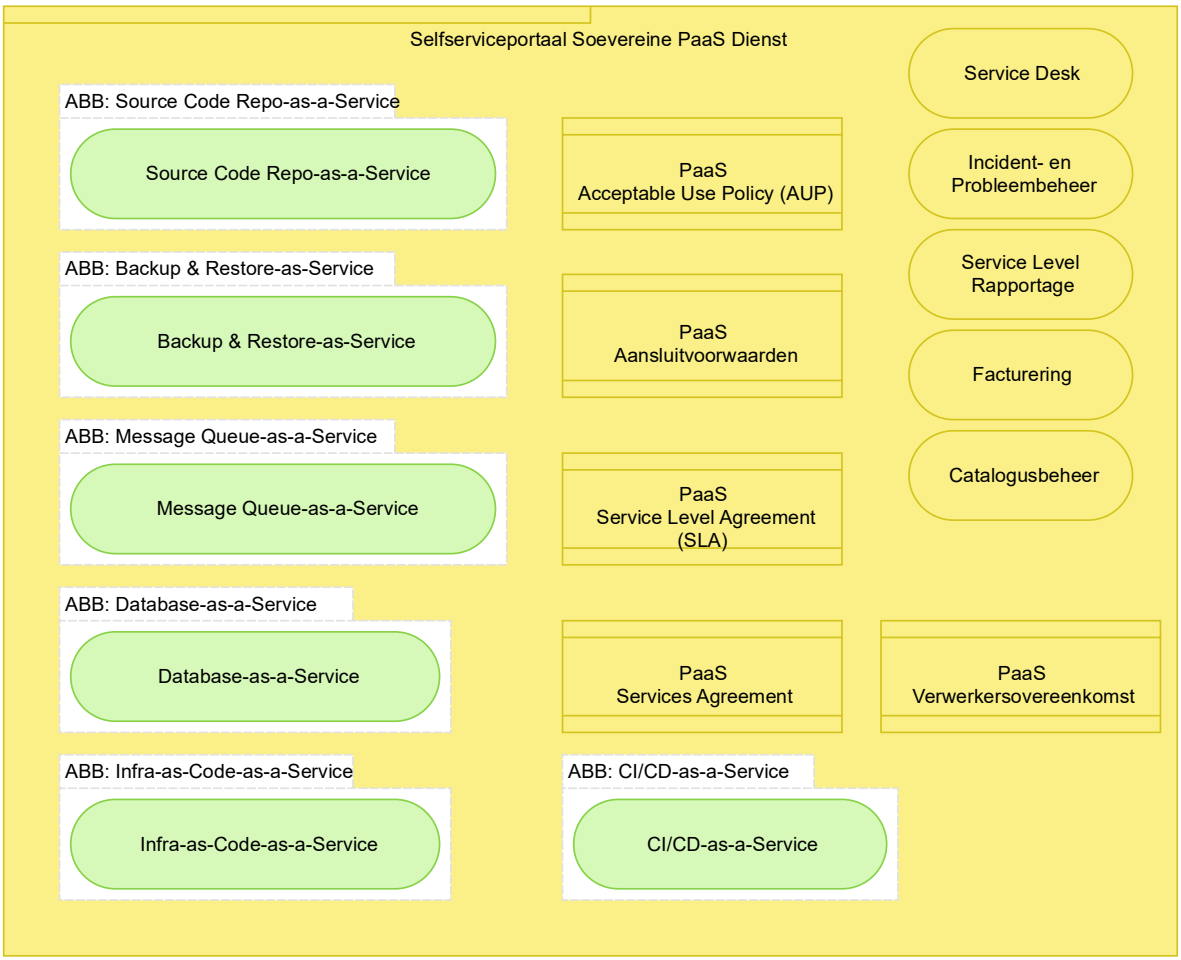


Figuur 4-3 Decompositie Soevereine Virtual Machine Hosting

Dit product is gericht op afnemers die nog niet in staat zijn tot *replatforming* van traditionele server-based applicaties naar een cloud-native variant maar wel de voorkeur geven aan *rehosting* naar een soeverein platform.

4.5 Selfserviceportaal Soevereine PaaS Dienst

Het product Selfserviceportaal Soevereine PaaS Dienst is strikt genomen geen onderdeel van Het Ontwerp (zie 1.9 Scope) maar is hier opgenomen voor een heldere duiding en demarcatie van de soevereine hostingproducten.

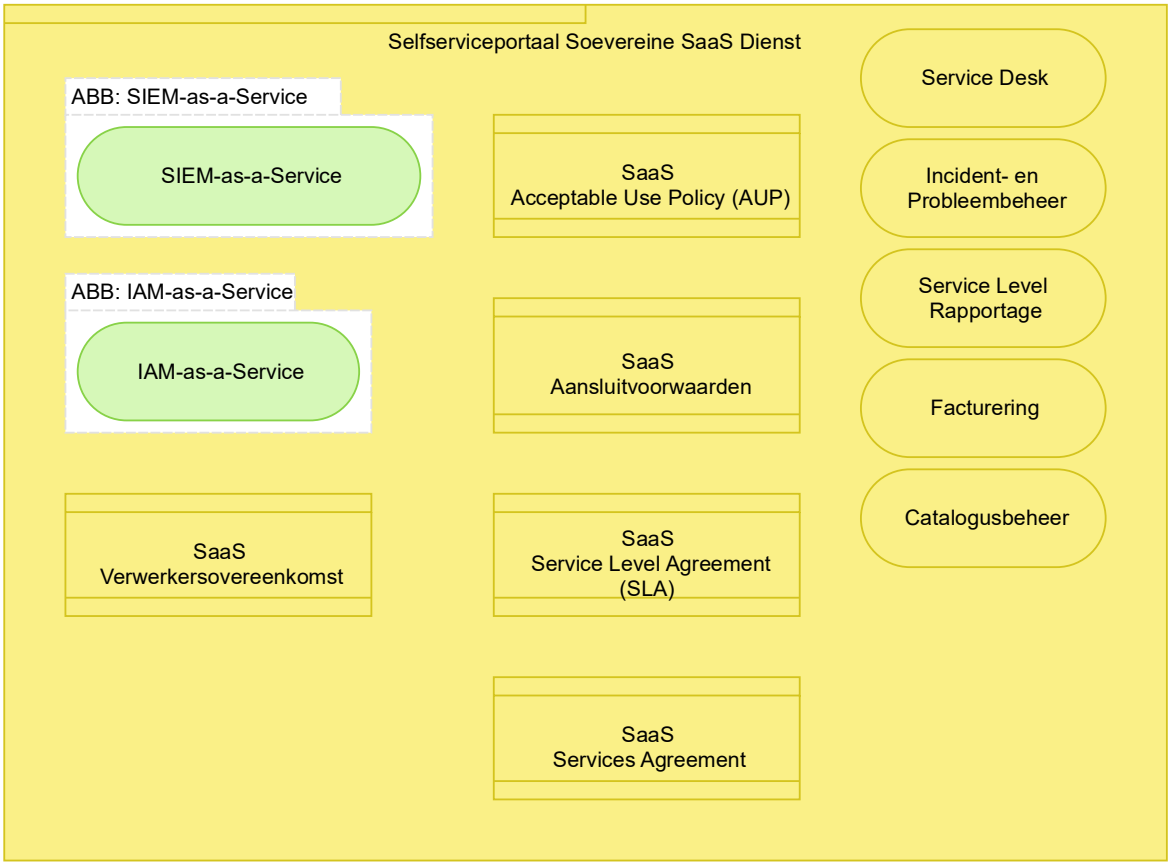


Figuur 4-4 Decompositie Selfserviceportaal Soevereine PaaS Dienst

Het Selfserviceportaal voorziet in meerdere partijen die PaaS-producten gaan leveren gebruikmakend van het product Soevereine Cloud-native Hosting. Omdat het om PaaS gaat, zal zo'n partij typisch gebruikmaken van het Tenantcluster van de afnemer van het PaaS-product. De technologiediensten gemodelleer*d* in *Figuur 4-4 Decompositie Selfserviceportaal Soevereine PaaS Dienst,* zijn voorbeelden en vormen geen uitputtende opsomming.

4.6 Selfserviceportaal Soevereine SaaS Dienst

Het product Selfserviceportaal Soevereine SaaS Dienst is strikt genomen geen onderdeel van Het Ontwerp (zie 1.9 Scope) maar is hier opgenomen voor een heldere duiding en demarcatie van de soevereine hostingproducten.



Figuur 4-5 Decompositie Selfserviceportaal Soevereine SaaS Dienst

Het Selfserviceportaal voorziet in meerdere partijen die SaaS-producten gaan leveren gebruikmakend van het product Soevereine Cloud-native Hosting. Omdat het om SaaS gaat, zal zo'n partij typisch gebruikmaken van een eigen Tenantcluster en niet het Tenantcluster van de afnemer van het SaaS-product. De technologiediensten gemodelleerd in *Figuur 4-5 Decompositie Selfserviceportaal Soevereine SaaS Dienst*, zijn voorbeelden en vormen geen uitputtende opsomming.

4.7 Voortbrenging

Het gebruik van Open Source Software betekent dat (systeem)integratie tussen de gebruikte open source bibliotheken, componenten, en/of applicaties noodzakelijk is. Besluitvorming over het Operating Model en rol van de markt volgt nog. Daaruit zal nader blijken welke organisatie(s) de dienst gaat/gaan leveren. Wat in ieder geval noodzakelijk is voor de dienstverlening is Voortbrenging van de gebruikte software (e.g. Platform Engineering). Daarvoor is hoogwaardige kwaliteit/automatisering van de software integratie- en ontwikkelprocessen nodig. Randvoorwaarden daarvoor worden nader uitgewerkt in de volgende versie van Het Ontwerp.

5 Systeemperspectief

Dit hoofdstuk beschrijft de technologiestack van de Clouddienst in een model met Architectural Building Blocks (ABB's) en relaties met andere ABB's. De ABB's zijn gemodelleerd als ArchiMate Technology Services.

De weergegeven ABB's bevatten bewust geen implementatie-details zoals de gekozen open source componenten of producten om ze te realiseren. Per ABB zal er minstens één Solution Bouw Blok (SBB) zijn dat deze implementatiedetails beschrijft. Deze uitwerking volgt in het nader op te stellen High Level Design. Daarin wordt aangegeven welke (externe) open source software componenten daarbij benut worden en welke eigen software nodig is.

De technologiestack heeft zes architectuurlagen, conform de opdracht voor Het Ontwerp. Op basis van het Operating Model wordt verwacht dat deze lagen herijkt worden in de volgende versie van Het Ontwerp (2.0).

1. **Datacenterlaag:** de fysieke datacentra en bijbehorende faciliteiten, de locaties, availibility zones, redundantie, eisen aan stroomtoevoer naar de racks, eisen aan de koelingstechniek.

2. **Netwerklaag**: de relevante Wide Area Netwerken (WAN) en de onderliggende netwerken (*underlay*) gebruikt in het datacenter. Deze laag is *exclusief* de bovenliggende netwerkconnectiviteit (*overlay*) die wordt gerealiseerd in het Kubernetes-cluster. Bandbreedte-eisen noord-zuid/oost-west en naar de servers inclusief (toekomstige) GPU-nodes, integraties met Diginetwerk/NAFIN/Rijksoverheidsnetwerk, netwerkhardware.

3. **Computelaag:** de hardware voor het hosten van de Kubernetes-clusters inclusief fysieke servers, opslag en netwerk (routers & switches). Eisen aan certificering van de hardware, integratie met software/netwerk, integratie met koeling van het DC, stroomcapaciteit.

4. **Basisfunctionaliteitlaag**: de inrichting van de storagesystemen en integratie met het onderliggend netwerk, inrichting van de fysieke en virtuele Kubernetes-clusters, de integratie met de bovenliggende netwerkconnectiviteit en de inrichting van de (KubeVirt) Virtual Machine-dienst.

5. **Platformlaag**: de systemen die aanvullend nodig zijn om virtuele Kubernetes-clusters en de (KubeVirt) Virtual Machine-dienst als onderdeel van de Clouddienst te leveren.

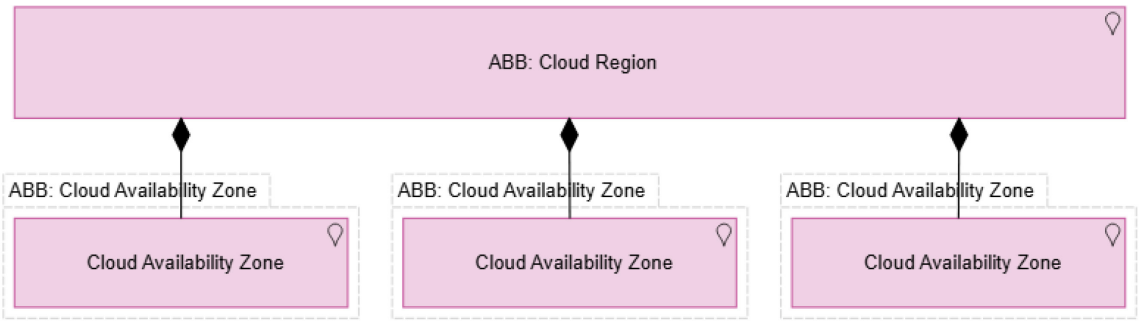
6. **Managed Dienstenlaag**: voorbeelden van managed diensten als mogelijke extra dienst van de Clouddienst.

Leeswijzer Architectuurlagen en ArchiMate-diagrammen
De paragrafen hieronder tonen voor elke architectuurlaag views die laten zien hoe de ABB's van de betreffende architectuurlaag zijn gepositioneerd ten opzichte van andere ABB's.

De in dit hoofdstuk opgenomen ArchiMate-diagrammen dienen primair ter visuele herkenning en ter ondersteuning van de tekstuele beschrijvingen. De verdere uitwerking van de verschillende ABB's is niet opgenomen in Het Ontwerp. De volledige en interactief leesbare modellen zijn beschikbaar als ArchiMate export *(Bijlage 8 – Het Ontwerp Artefacten)*. Geadviseerd wordt deze export in een ArchiMate-tool te laden en daar de platen te raadplegen voor detailanalyses.

5.1 Datacenterlaag
Dit beschrijft de Architectural Building Blocks (ABB) van het fysieke datacenter (hierna: datacentergebouw) en de bijbehorende faciliteiten.

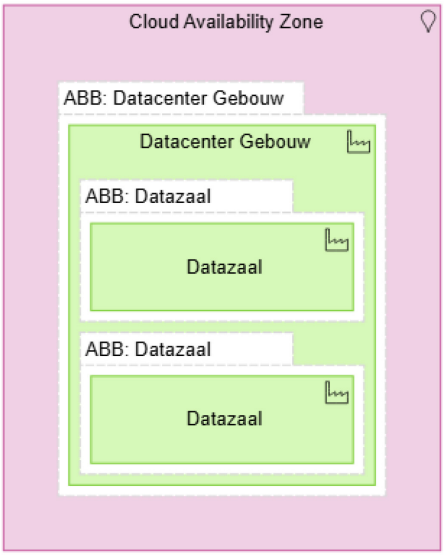
5.1.1 Datacenteroverzicht
Het Datacenteroverzicht toont hoe datacenters voor de Clouddienst zich verhouden tot Cloud Availability Zones en Cloud Regions[38]. In Nederland worden meerdere Cloud Regions ingericht (elk gebaseerd op bestaande ODC's) die volgens hyperscaler *best practices*[39] bestaat uit verschillende Cloud Availability Zones die onafhankelijk van elkaar kunnen falen bij een grote calamiteit. Een Cloud Availability Zone bestaat in de gewenste eindsituatie uit één datacenter.



Figuur 5-1 Decompositie ABB Cloud Region

Samenvatting uitgangspunten, architectuurkeuzes en aandachtspunten:
- Minimumafstand tussen Cloud Availability Zones bepaald door insluiting grootschalige calamiteiten;
- Minimaal twee verschillende stroomverdeelsubstations;
- Impact aardbeving blijft beperkt tot één Cloud Availability Zone;
- Gestart kan worden met zelfstandige datazalen als Availability Zones.

[38] Cloud regions zijn specifieke geografische locaties voor datacenters. Een availability zone (AZ) is een onafhankelijke datazaal, datacenter, of groep datacenters binnen zo'n regio, voorzien van eigen stroom, koeling en netwerk.
[39] Bronnen: AWS Global Infrastructure, Microsoft Azure Availability Zones Overview en Google Cloud Compute Engine Regions and Zones.



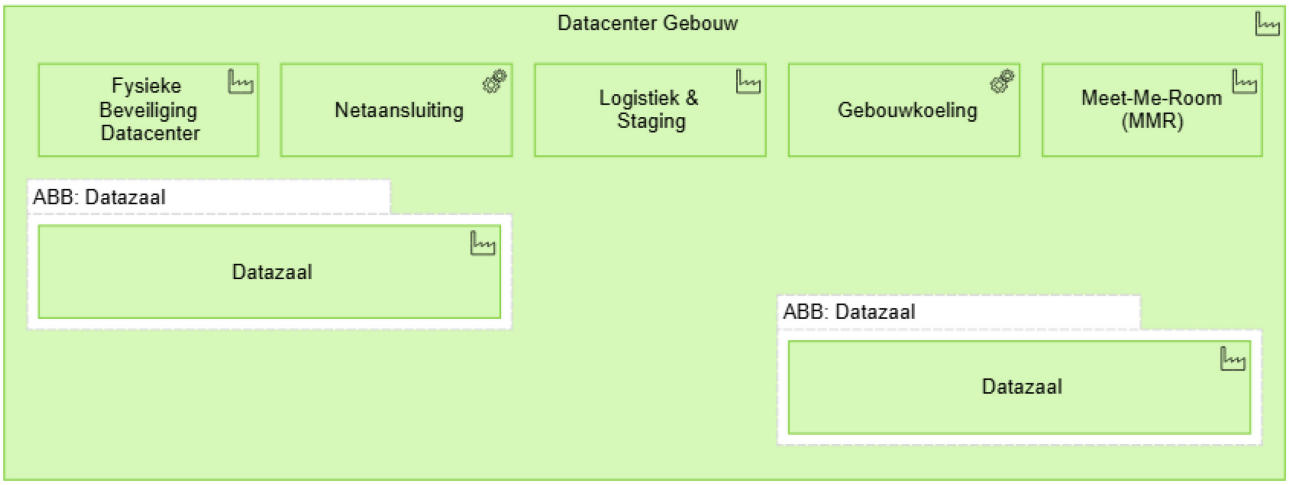
Figuur 5-2 Decompositie ABB Cloud Availability Zone

Samenvatting uitgangspunten, architectuurkeuzes en aandachtspunten:

- Het datacenter staat fysiek op Nederlandse grondgebied en valt onder Nederlandse jurisdictie;
- Het datacenter voldoet minimaal aan de ANSI/TIA-942 eisen voor tier-3 datacenters;
- Het datacenter beschikt over eigen watervoorziening en back-up-generatoren.

5.1.2 Decompositie ABB "Datacenter Gebouw"

Een datacentergebouw heeft een of meerdere datazalen, met daarin generieke voorzieningen als fysieke toegangsbeveiliging, stroomvoorziening, koeling en fysieke koppelingen met externe netwerken.



Figuur 5-3 Decompositie ABB Datacenter Gebouw

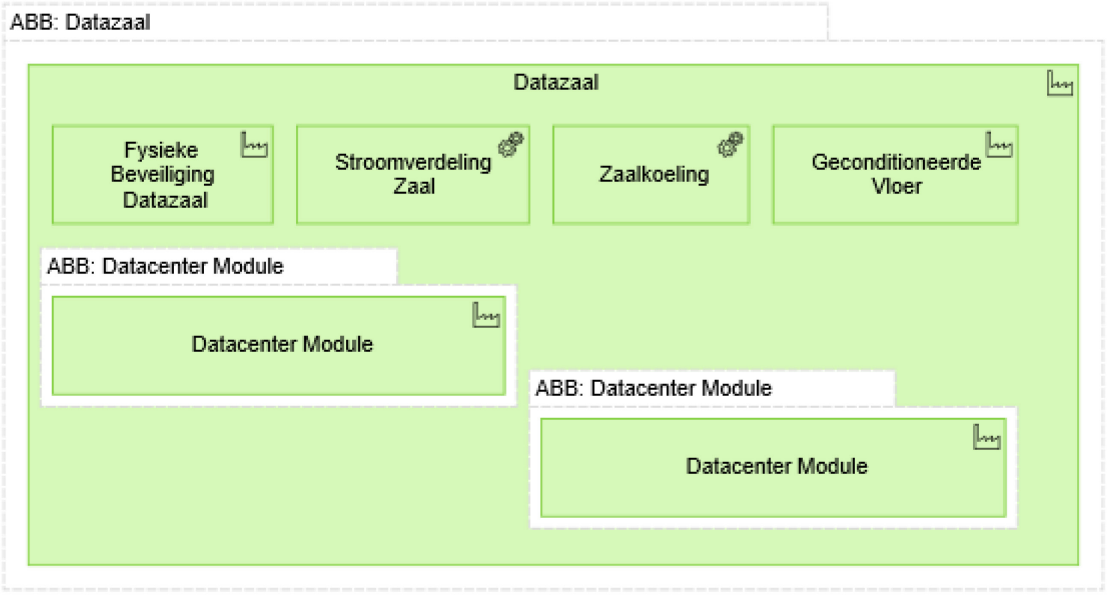
Attribuut	Invulling
ABB#	**DC01**
Naam ABB	Datacentergebouw
Eigenaar	Rijksvastgoedbedrijf (RVB)
Architectuurdomein/Capability	3.1 Security & Business Continuity 9. Datacenter
Beschrijving	De fysieke buitenstructuur die de IT-infrastructuur huisvest. Het gebouw moet voldoen aan strikte eisen wat betreft constructieve veiligheid, beveiliging (fysieke barrières), brandveiligheid en de toegang tot externe nutsvoorzieningen zoals hoogspanningselektriciteit en water voor koelsystemen.
Functionele scope	• *In scope*: stroommanagement, warmtemanagement, toegangsbeveiliging, SCADA (efficiëntie/CO_2), geografische, locatiegebonden en fysieke risico's, capaciteit, beschikbaarheid. • *Out of scope*: nutsvoorzieningen etc.
Onderliggende ADR	ADR-G01
Relaties met andere ABB	NE01, i.v.m. extern koppelvlak (pop)
Relaties met GDI-bouwblokken	Infra bouwblokken GDI
Interfaces en integratiepunten	Fysieke toegang met vrachtverkeer, paddock, hulpdiensten, stroom.
Dataopslag	Volledig lokaal, persistent
SEAL-Level afwijkingen	• Apparatuur voor gebouwbeheer kent externe afhankelijkheden. • Fysiek gescheiden "meet me room" noodzakelijk bij afname externe leverancier (ter voorkoming van wiretapping)
Dataclassificatie	Dep-V/BBN2
Risico's	• Nuts-management en brandveiligheid • Fysieke beveiliging van het pand en toegangsbeveiligingssysteem mogen geen externe afhankelijkheid kennen • Vaak cloud-gebaseerd • Vendor lock-in • AI-integratie • GPU's
Kandidaat-SBB's	• ODC's / leverancier • TIA-942 – tier III

Tabel 1: Attributen van ABB-DC01

Voor het ABB Datacentergebouw zijn hierboven (Tabel 1), als voorbeeld, de bijbehorende attributen ingevuld. Bijlage 8 – Het Ontwerp Artefacten, ABB per architectuurlaag view**.pdf** bevat de gehele set aan ABB's met decompositie en voor de meest relevante ABB's de bijbehorende attributen

5.1.3 Decompositie ABB "Datazaal"

De datazaal is een fysiek afgescheiden datacenterruimte met voorzieningen zoals stroomvoorziening en koeling. De datazaal wordt geëxploiteerd door de aanbieder van de NDS Clouddienst.



Figuur 5-4 Decompositie ABB Datazaal

Samenvatting uitgangspunten, architectuurkeuzes en aandachtspunten:

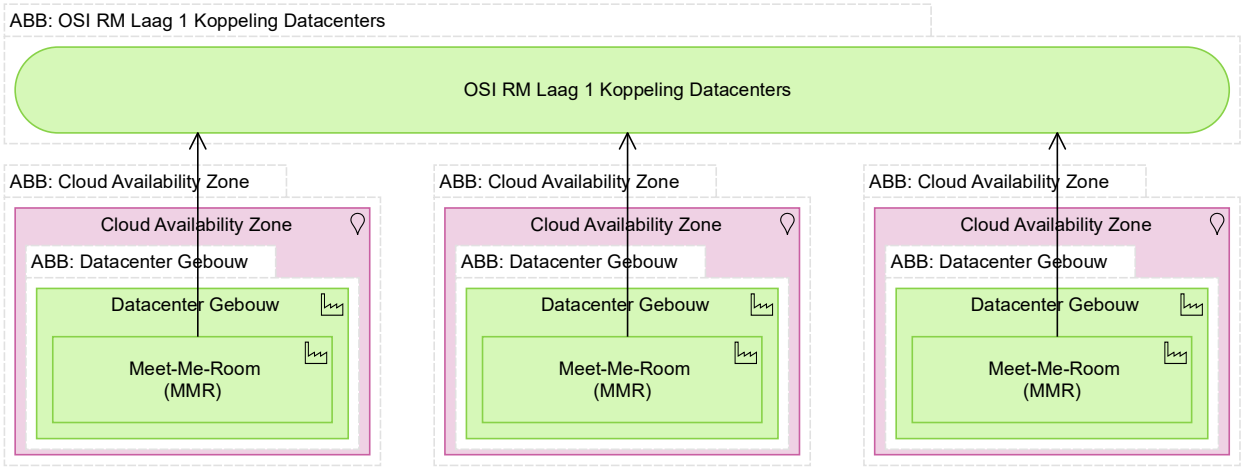
- Wholesale-model: de aanbieder NDS Cloud huurt een lege datazaal;
- De aanbieder datazaal zorgt ook voor fysieke toegangsbeveiliging;
- De aanbieder NDS Cloud zorgt voor hardware;
- Fit-out: extra datazaal als 1e datazaal 80% vol is;
- De aanbieder NDS Cloud bedingt opties voor datacenterruimte en stroomgebruik.

5.2 Netwerklaag

Deze laag betreft alle netwerklagen van het platform, inclusief netwerkhardware, underlay- en overlaynetwerken. Minimaal: inrichting underlay- en overlaynetwerken, bandbreedte-eisen noord-zuid/oost-west en naar de servers inclusief de GPU-nodes, integratie met het Diginetwerk/NAFIN/Rijksoverheidsnetwerk (DC-i, WAN-i, etc.), inrichting van de automatisering van het netwerk, multi-vendorstrategie voor netwerkhardware.

5.2.1 Positionering ABB "OSI RM Laag1 Koppeling Datacenters"

De datacenters die samen een Cloud Region vormen, worden onderling gekoppeld door een OSI RM Laag-1 netwerk.



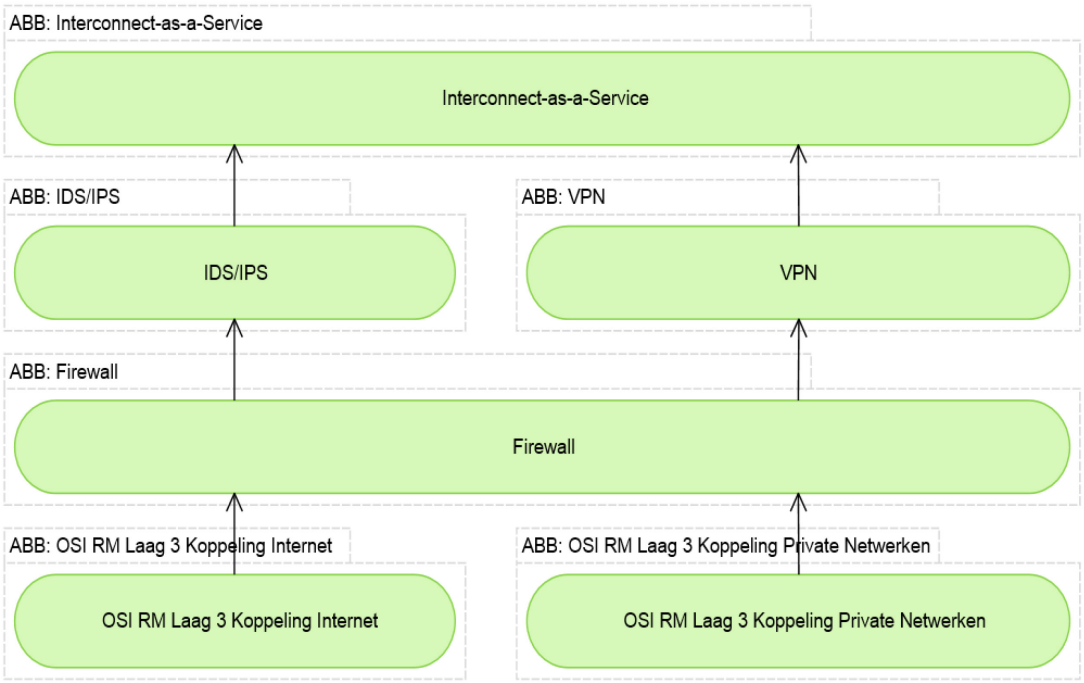
Figuur 5-5 Positionering ABB OSI RM Laag1 Koppeling Datacenters

Samenvatting uitgangspunten, architectuurkeuzes en aandachtspunten:

- Maximum afstand tussen datacenters binnen Cloud Region bepaald door synchrone storage-replicatie.

5.2.2 Positionering ABB's koppelnetwerken

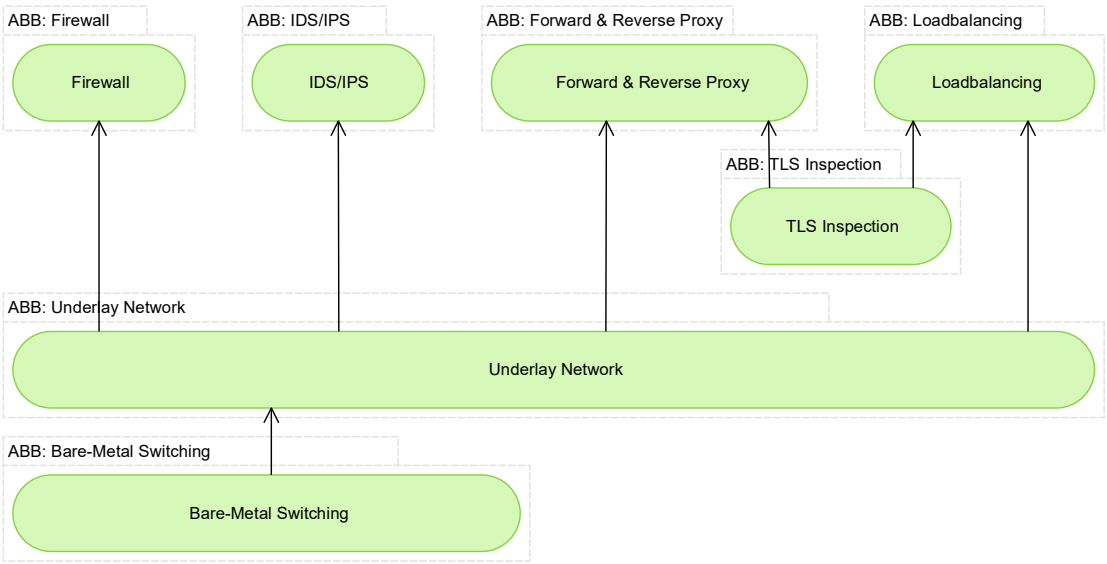
Elk datacenter moet worden ontsloten naar zowel publieke (Internet) als private (overheids-) OSI RM Laag 3-netwerken. Hierbij kan eventueel gebruik worden gemaakt van VPN-technologie om bijvoorbeeld SD-WAN te realiseren.
Deze interconnectiviteit wordt als technologiedienst beschikbaar gesteld aan de afnemer.



Figuur 5-6 Positionering ABB's koppelnetwerken

5.2.3 Positionering ABB "Underlay Network"

Binnen de gehuurde datazalen wordt netwerkconnectiviteit gerealiseerd met meerdere gescheiden OSI RM Laag-3 routeringsdomeinen. De benodigde netwerkswitches kunnen hiervoor softwarematig als bare-metal worden toegewezen.



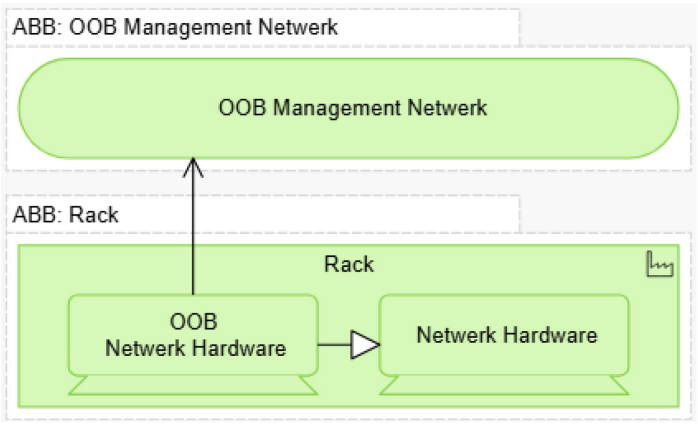
Figuur 5-7 Positionering ABB Underlay Network

Samenvatting uitgangspunten, architectuurkeuzes en aandachtspunten:

- Het Underlay netwerk biedt basisconnectiviteit voor het overlay netwerk *(niet expliciet gemodelleerd)* dat connectiviteit biedt tussen individuele Kubernetes Pods en typisch via de CNI-interface ontsloten wordt.

5.2.4 Positionering ABB "OOB Management Network"

Om fysieke servers en netwerkswitches als bare-metal softwarematig toe te wijzen, is een fysiek gescheiden ("Out-of-band") netwerk nodig met eigen hardware (switches).



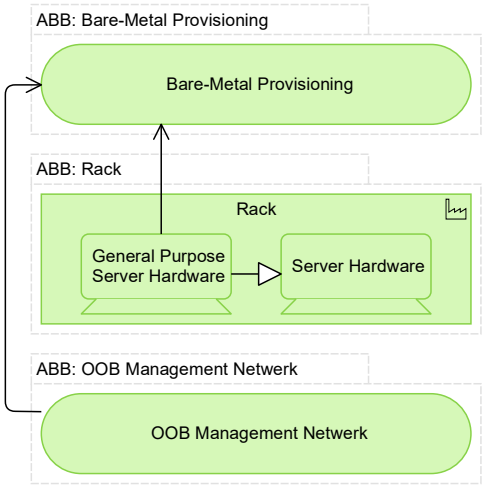
Figuur 5-8 Positionering ABB OOB Management Network

5.3 Computelaag

De Computelaag betreft de hardware en storage die wordt gebruikt voor het hosten en leveren van de Clouddienst. De uitwerking betreft (onder andere) de inrichting van diverse typen nodes, integratie met koeling van het datacenter, inrichting specifiek voor AI (soorten inrichting van GPU-clusters), eisen aan certificering van de hardware en integratie met software/netwerk, multi-vendorstrategie en de effecten ervan, stroomcapaciteit.

5.3.1 Positionering ABB "Bare-Metal Provisioning"

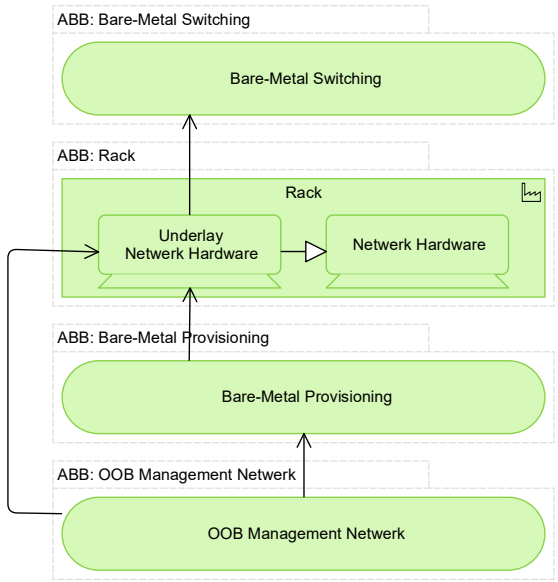
De software benodigd om bare-metal (fysieke servers en netwerkswitches) softwarematig toe te kunnen wijzen, heeft zijn eigen server nodig.



Figuur 5-9 Positionering ABB Bare-Metal Provisioning

5.3.2 Positionering ABB "Bare-Metal Switching"

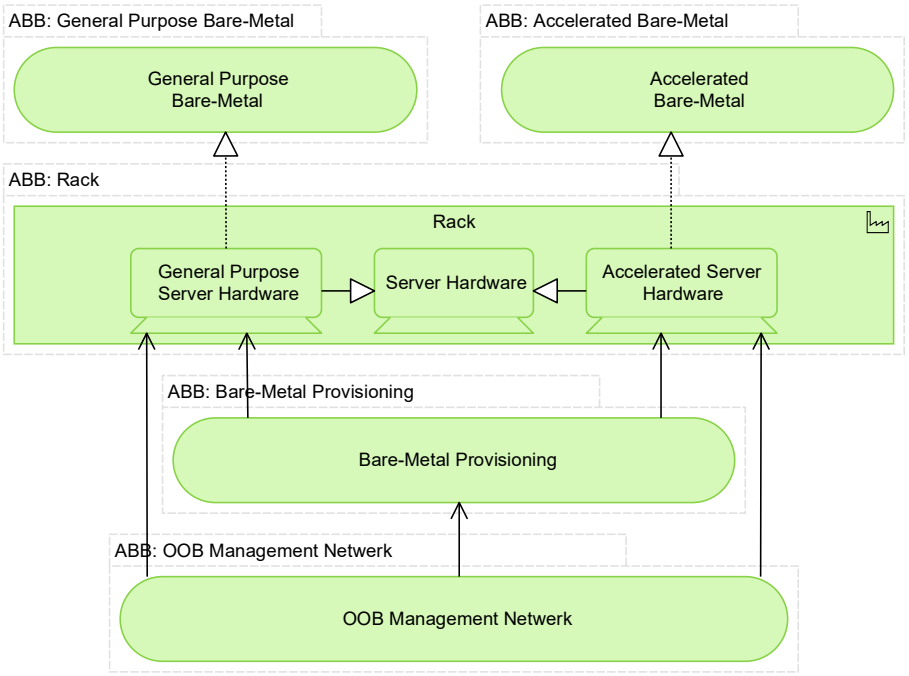
Fysieke netwerkswitches kunnen softwarematig worden toegewezen als bare-metal.



Figuur 5-10 Positionering ABB Bare-Metal Switching

5.3.3 Positionering ABB "Server Bare-Metal"

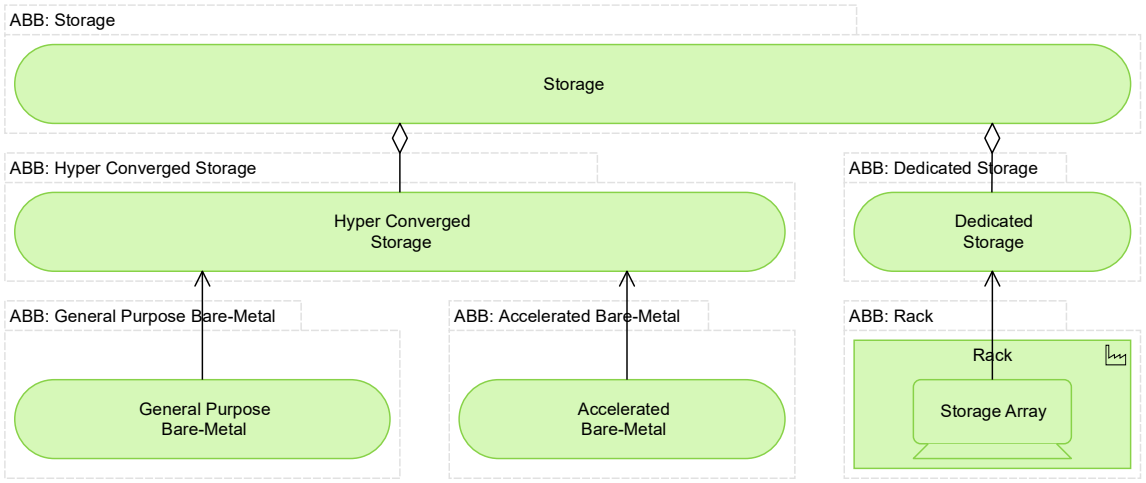
De fysieke servers die worden als bare-metal worden toegewezen, bestaan naast algemeen inzetbare bare-metal servers ook uit bare-metal servers met opgevoerde hardware (GPU-technologie).



Figuur 5-11 Positionering ABB Server Bare-Metal

5.3.4 Positionering ABB "Storage"

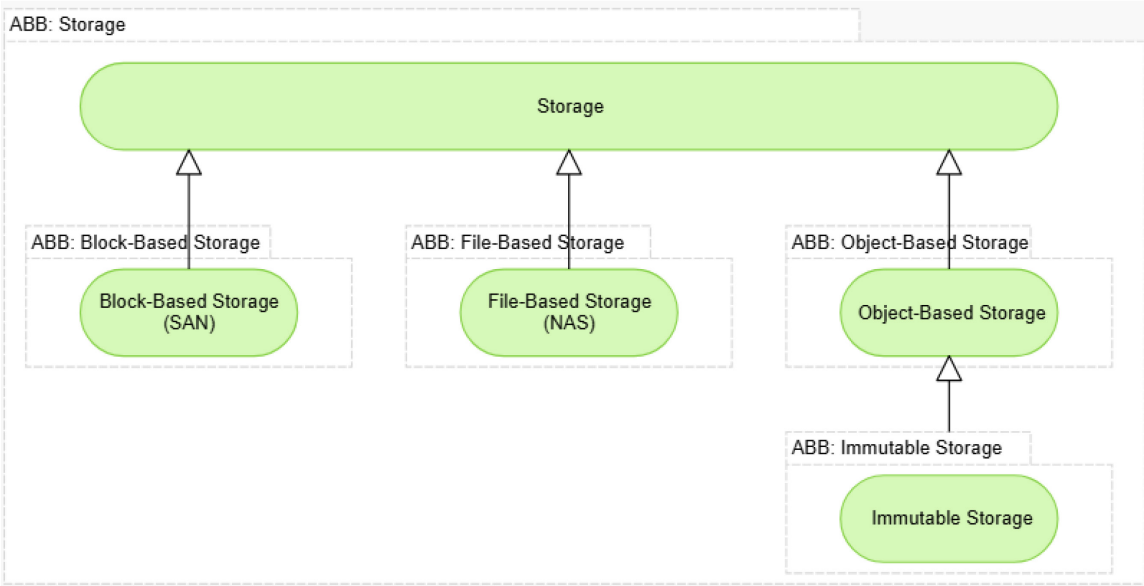
Storage wordt afhankelijk van de benodigde schaalgrootte op twee manieren aangeboden: op basis van Hyper Converged Infrastructure (HCI) gebruikmakend van de storage op de fysieke servers of op basis van een storage array.



Figuur 5-12 Positionering ABB Storage

5.3.5 Decompositie ABB "Storage"

Storage wordt op 3 verschillende manieren ingezet: block-based, files-based en object-based.



Figuur 5-13 Decompositie ABB Storage

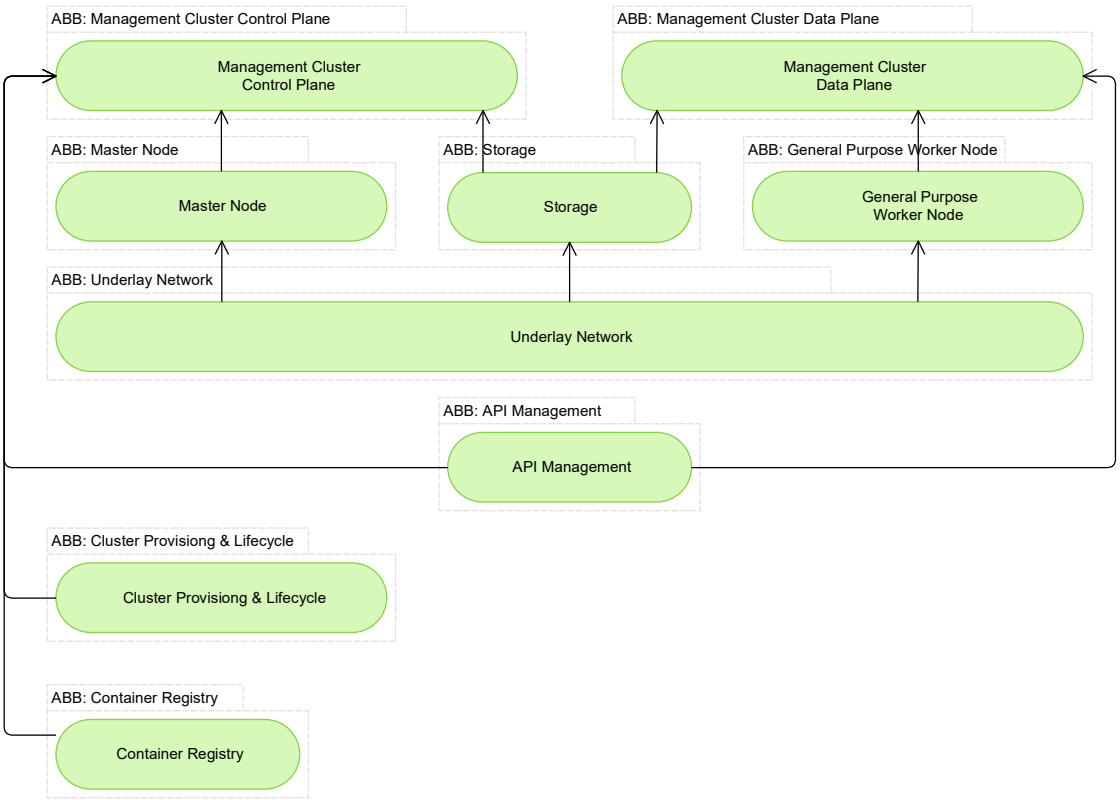
5.4 Basisfunctionaliteitlaag

Betreft de basisfunctionaliteit die voor elk cloudplatform nodig is, zoals:

- **Containers:** inrichting van de technologie om containers te hosten, integratie met externe oplossingen die gebruik willen maken van deze functionaliteit;
- **Virtualisatie:** inrichting van de technologie om VM's te hosten en te beheren, inrichting van de oplossing voor managed/unmanaged diensten, integratie met externe oplossingen die afhankelijk zijn van deze functionaliteit;
- **Managementplatform:** inrichting van het geautomatiseerd aansturen en coördineren van VM's en containers, uitwerking van de wijze waarop *security policies* worden gedefinieerd en afgedwongen, uitwerking van belangrijke functionaliteit voor afnemers (zoals autoscaling van services), inrichting van koppeling met publieke clouddiensten.

5.4.1 Positionering ABB "Management Cluster"

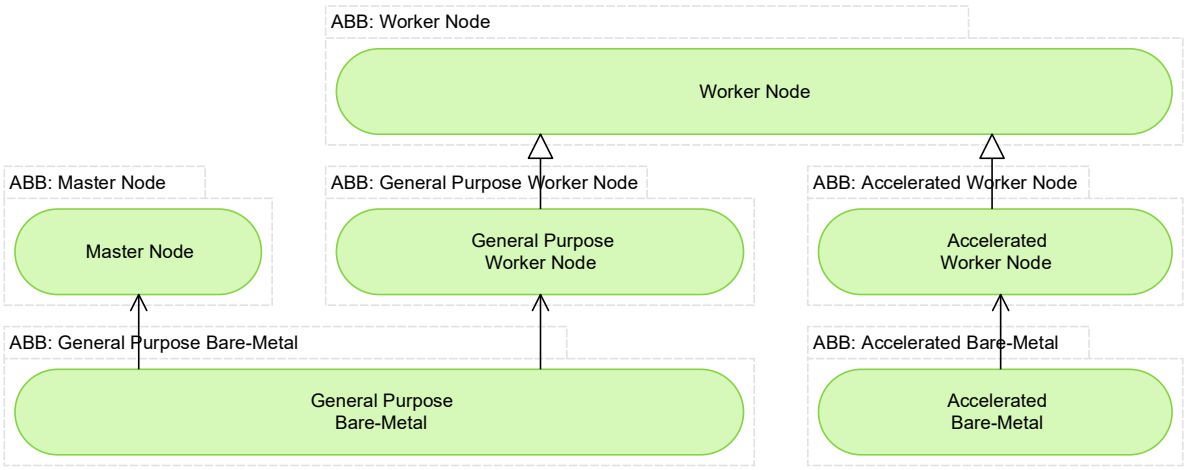
De technologiestack bestaat uit één Kubernetes managementcluster die gebruikt wordt voor het beheer van meerdere tenantclusters.



Figuur 5-14 Positionering ABB Management Cluster

5.4.2 Positionering Nodes

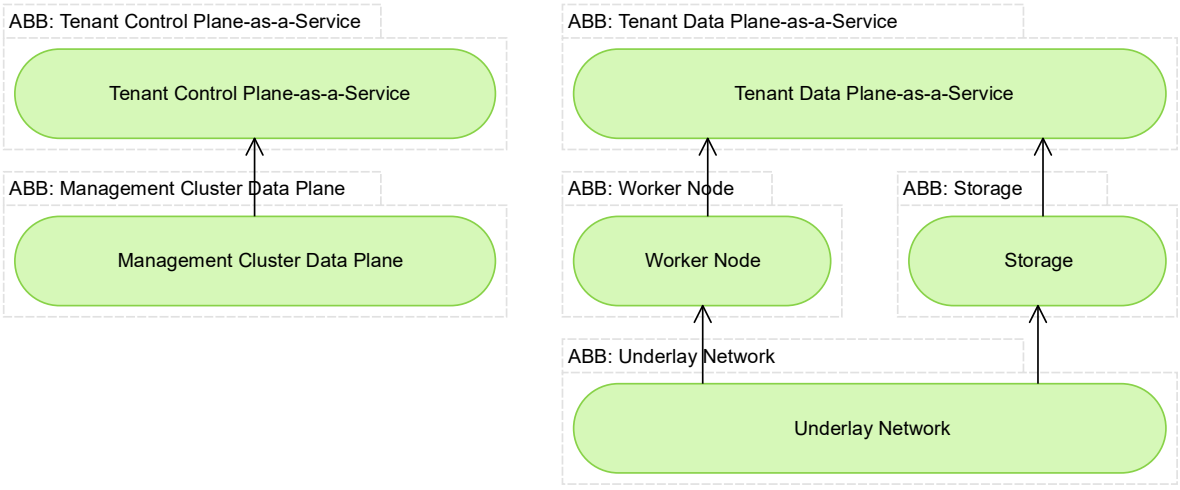
De Kubernetes Master Node is altijd gebaseerd op algemeen-inzetbare hardware. Voor Worker Nodes kan naar keuze eventueel ook opgevoerde hardware worden ingezet.



Figuur 5-15 Positionering Nodes

5.4.3 Positionering ABB "Tenant Cluster"

Elk Tenant Cluster bestaat uit Worker Nodes met eigen hardware. De Kubernetes control plan van elk Tenant Cluster maakt wel gebruik van gedeelde hardware (Hosted Control Plane).



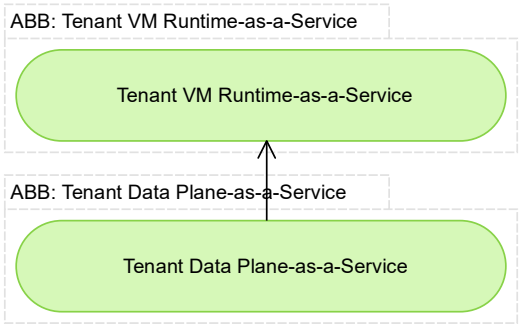
Figuur 5-16 Positionering ABB Tenant Cluster

Samenvatting uitgangspunten, architectuurkeuzes en aandachtspunten:

- De afnemer kan één of meerdere tenantclusters afnemen die zowel onderling als van tenantclusters van andere afnemers fysiek gescheiden zijn;
- Elke tenantcluster kan logisch verder opgedeeld worden in projecten die elk weer bestaan uit Kubernetes namespaces.

5.4.4 Positionering ABB "Tenant VM Runtime-as-a-Service"

Voor het hosten van Virtual Machines (gevirtualiseerde servers) draait de hypervisortechnologie niet direct op de fysieke hardware maar als een container op het tenantcluster.



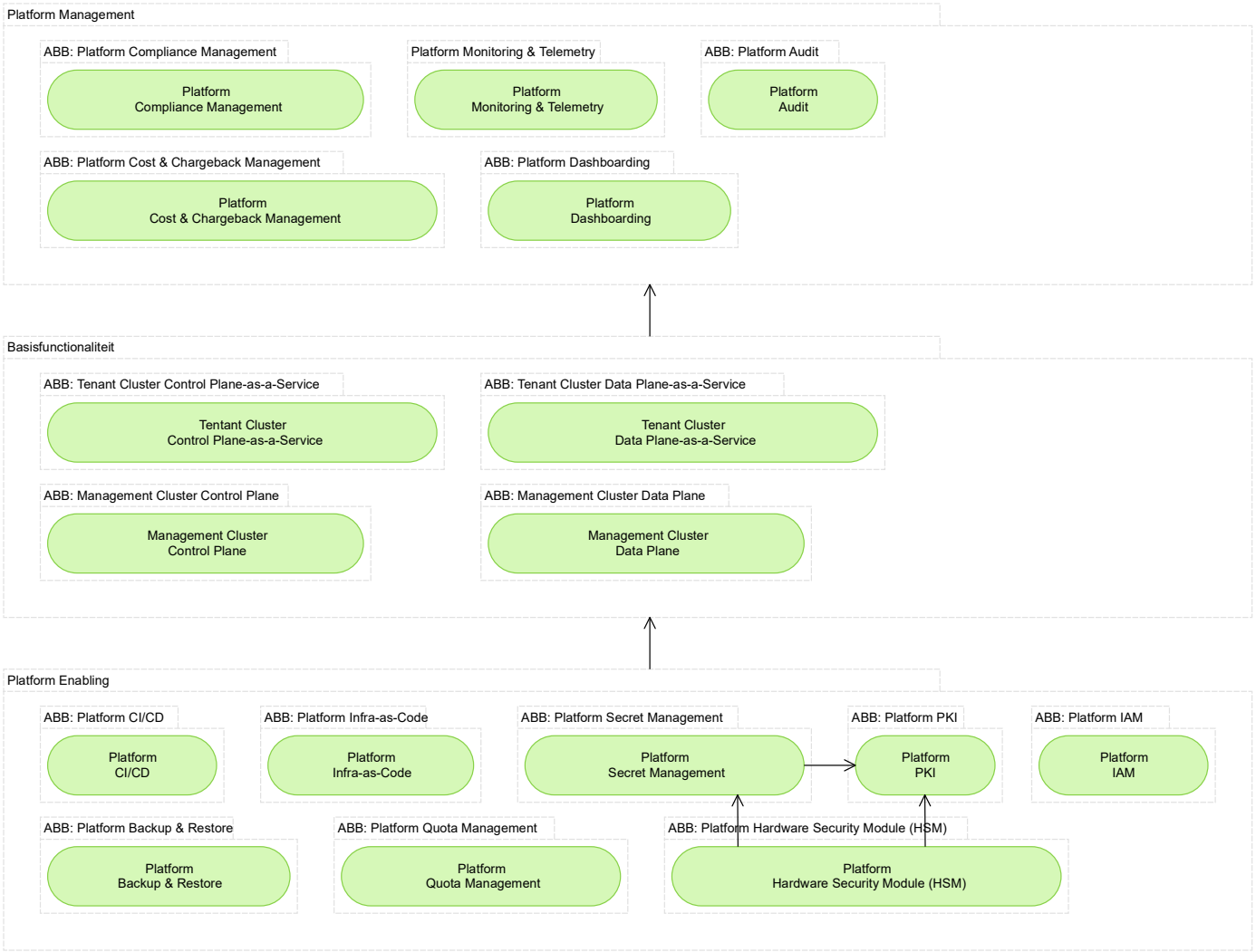
Figuur 5-17 Positionering ABB Tenant VM Runtime-as-a-Service

5.5 Platformservicelaag

Betreft de diensten die nodig zijn om het platform te leveren. De uitwerking betreft (onder andere) de inrichting van het bootstrapproces en -techniek, inrichting Git-omgeving en IAM (KMS, IDP, IGA), inrichting reportingservice voor het faciliteren van financiële inzichten.

5.5.1 Decompositie Containerplatform

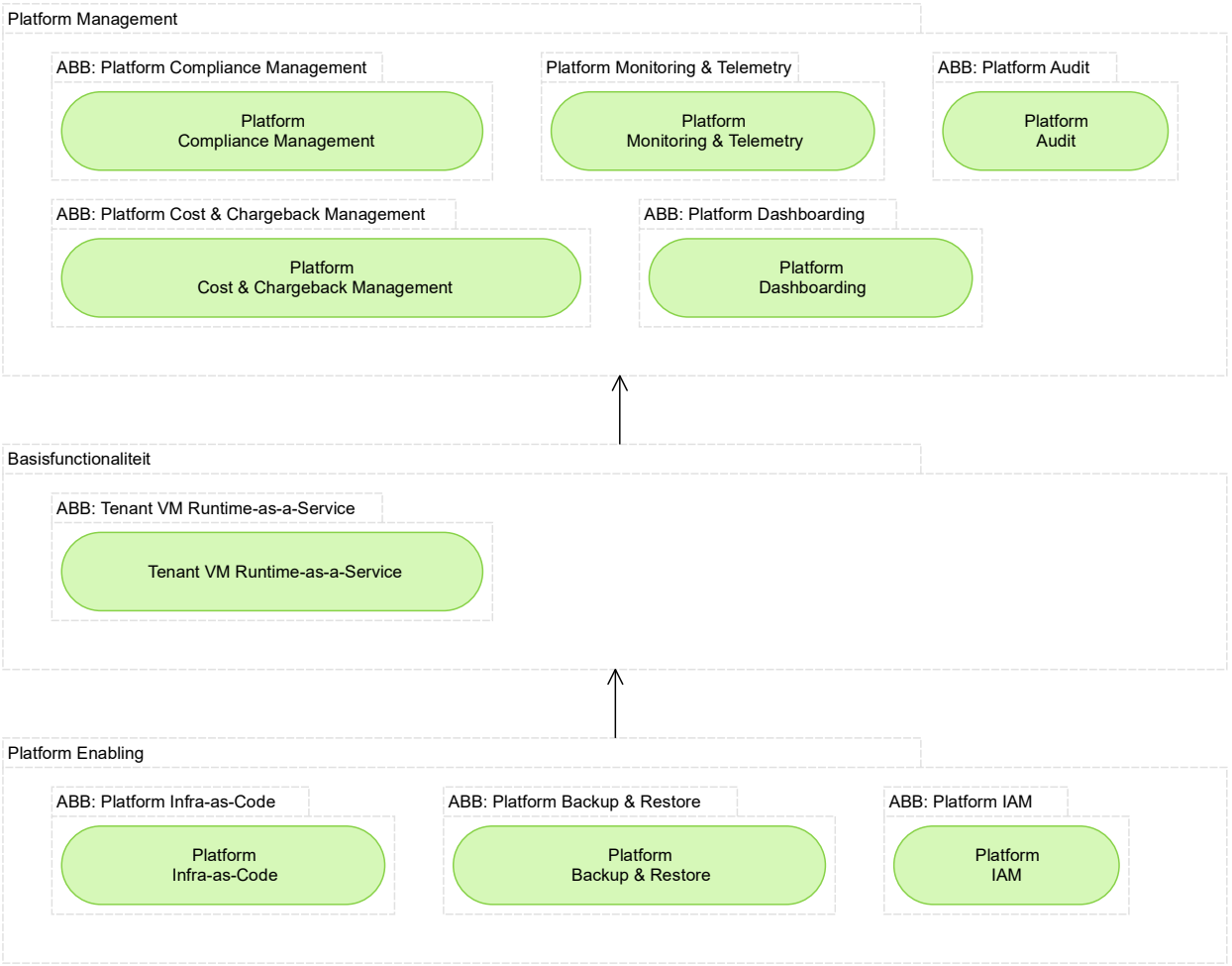
Om tenantclusters als platform beschikbaar te stellen aan afnemers, is aanvullende technische functionaliteit nodig zoals bijvoorbeeld cost & chargeback management, CI/CD en quota management.



Figuur 5-18 Decompositie Containerplatform

5.5.2 Decompositie Virtual Machine Platform

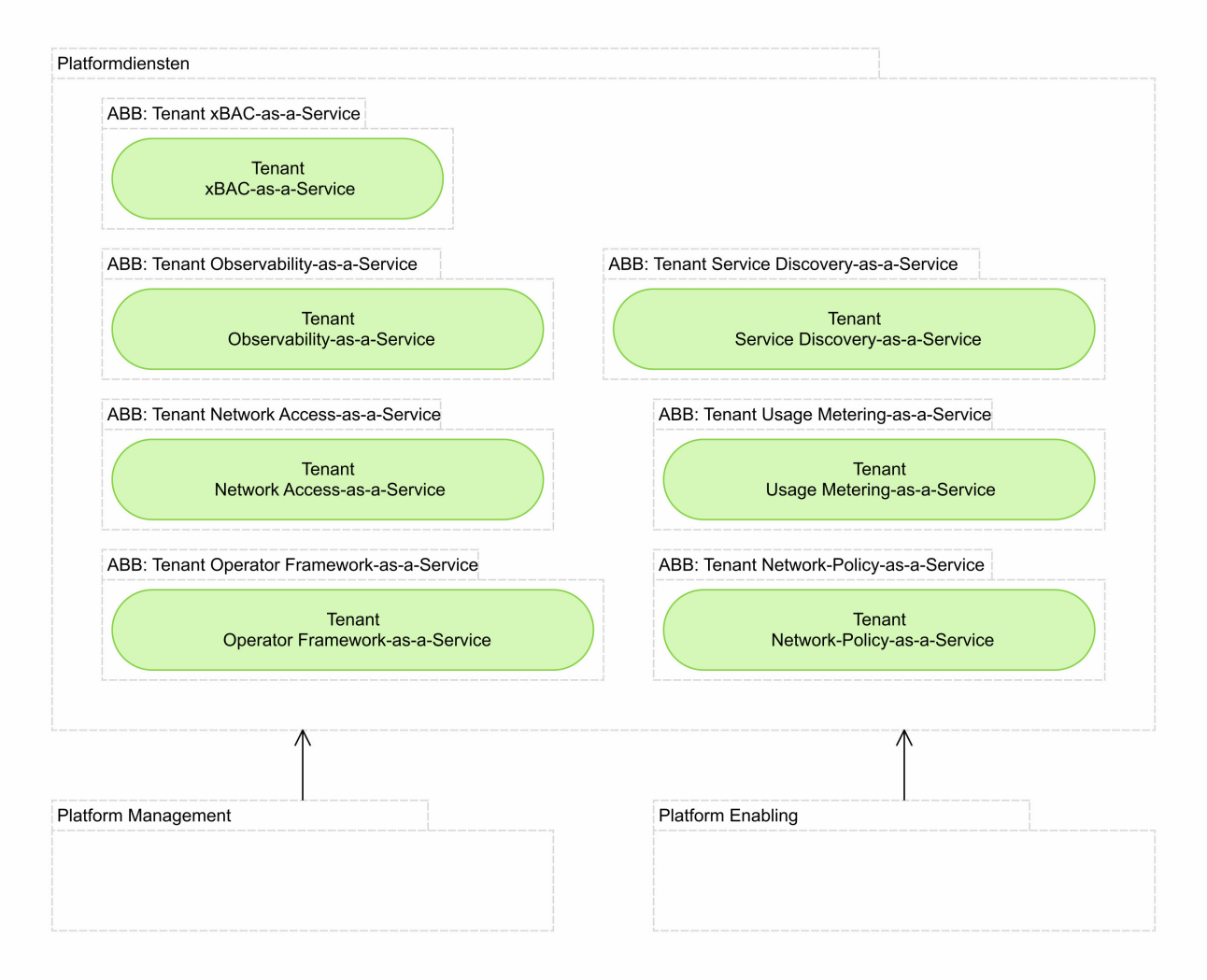
Ook voor het aanbieden van runtime-omgevingen als platform is extra technische functionaliteit nodig die deel overlapt met die van het containerplatform.



Figuur 5-19 Decompositie Virtual Machine Platform

5.5.3 Positionering Platformdiensten

De afnemer zal zelf ook gebruik moeten maken van extra technische functionaliteit om het tenantcluster als platform in te kunnen zetten.



Figuur 5-20 Positionering Platformdiensten

5.6 Managed dienstenlaag

Betreft het systeem/framework dat het mogelijk maakt om managed diensten op basis van het platform te leveren, zoals databases, *message queueing* en data-analytics. De uitwerking betreft (onder andere) inrichting van het systeem voor het leveren van managed diensten (moet continuous delivery en IaC ondersteunen), inzet van het operatorframework, basisarchitectuur waarop managed services draaien, aansluiting op externe diensten.

5.6.1 Positionering Managed Diensten

Managed diensten vallen uiteen in PaaS-diensten die typisch in het tenantcluster van de PaaS-afnemer worden gehost en SaaS-diensten die in het tenantcluster van de SaaS-aanbieder (dus niet tenantcluster van de afnemer) worden gehost.

Figuur 5-21 Positionering Managed Diensten

Samenvatting uitgangspunten, architectuurkeuzes en aandachtspunten:

- Interface voor infra-as-code zou typisch via zowel een GUI (handmatig) als API (t.b.v. geautomatiseerde uitrol van applicaties) kunnen worden aangeboden

6 Kwaliteitsperspectief

Waar hoofdstuk 2 de architectuurprincipes en uitgangspunten beschrijven en hoofdstukken 5 de technologiestack, vertaalt dit hoofdstuk die beide naar toetsbare kwaliteitseisen per kwaliteitsattribuut: de eisen en wensen, de randvoorwaarden om daaraan te kunnen voldoen, en (waar relevant) de complicaties die het NDS Cloudprogramma bewust accepteert. De eisen zijn sturend geformuleerd en herleidbaar naar de onderliggende ADR's. Ze vormen de basis voor de serviceniveau-afspraken (hoofdstuk 4) en de conformiteitseisen per bouwsteen.

De kwaliteitseisen worden beheerd als één integraal kwaliteits-, beveiligings- en compliancekader. Dit kader brengt de toepasselijke wetgeving, beleidskaders, standaarden en architectuurkeuzes samen en vertaalt deze naar concrete controls, acceptatiecriteria en bewijsvoering voor de Clouddienst en de onderliggende ABB’s.

Het kader omvat ten minste:
- Digitale soevereiniteit;
- Prestatie-efficiëntie (prestatie en capaciteit)
- Uitwisselbarheid, overdraagbaarheid en exit;
- Bruikbaarheid;
- Betrouwbaarheid, continuïteit en herstelbaarheid;
- Informatiebeveiliging en privacy;
- Compliance, standaarden en audit;
- Onderhoudbaarheid, lifecycle en operationele beheerbaarheid;
- Kwaliteitsborging, observability en continue verbetering.

De inrichting van het operationeel model en de bijbehorende processen valt buiten de scope van Het Ontwerp. Het ontwerp stelt wel de technische en architectonische voorwaarden waarmee deze processen later eenduidig, geautomatiseerd en aantoonbaar kunnen worden ingericht.

6.1 Digitale Soevereiniteit

Binnen Het Ontwerp wordt gebruik gemaakt van de definitie van soevereiniteit zoals vastgelegd in de begrippenlijst[40].

Voor de Clouddienst vertaalt dit zich in de volgende eisen (grondslag: ADR-002):

Datalocalisatie	Alle data, back-ups en beheeractiviteiten bevinden zich in Nederland en vallen uitsluitend onder Nederlandse en Europese jurisdictie.
Operationele autonomie	Het platform wordt beheerd door gescreend personeel, toegang tot cruciale onderdelen is beperkt en de supply chain van cruciale componenten wordt gecontroleerd.
Aantoonbaarheid	De mate van soevereiniteit wordt periodiek en onafhankelijk getoetst aan het EU Cloud Sovereignty Framework; de toetsingsresultaten zijn beschikbaar voor Afnemers.

[40] https://pgdi.nl/files/cloud_definities_en_begrippenlijst_v1.0 16.04.2025 (vastgesteld door OBDO).pdf

6.1.1 EU Cloud Sovereignty Framework

Bij Het Ontwerpen van de Clouddienst streven we naar **SEAL-4** voor de volledige softwarestack: alle software is volledig open source, auditeerbaar en wordt beheerd onder EU-controle, operationeel op infrastructuur in Nederland. Voor de hardwarestack geldt SEAL-3, omdat Europese leveranciers van CPU's, GPU's en ASIC's vooralsnog ontbreken.

Complicatie: we accepteren voorlopig een restafhankelijkheid van niet-Europese hardware leveranciers. Dit risico beheersen we via controle van de supply chain en we volgen nauwlettend de ontwikkelingen vanuit het European Sovereign Tech Package, zoals de EU Cloud & AI Development Act, de EU Chips Act 2.0 en het EU Open Source Initiative, met de ambitie ook voor de hardware SEAL-4 te bereiken.

6.2 Prestatie-efficiëntie (prestatie en capaciteit)

Prestatie-efficiëntie beschrijft de mate waarin de Clouddienst presteert in verhouding tot de ingezette middelen, en of er voldoende capaciteit is voor de cloudvraag van de gehele overheid.

Voor de Clouddienst vertaalt dit zich in de volgende eisen:

Schaalbaarheid	Het platform schaalt automatisch mee met het actuele gebruik, zonder onderbreking van de dienstverlening. De capaciteit is berekend op de cloudvraag van de gehele overheid.
Geautomatiseerde levering	Standaarddiensten worden via selfservice volledig geautomatiseerd geleverd, om wachttijden zo kort mogelijk te houden.
Gebruiksgebaseerde dienstverlening	Het verbruik wordt per afnemer gemeten en is voor de afnemer inzichtelijk. Afnemer betaalt alleen voor gebruikte diensten, zodat er een drijfveer is om ongebruikte resources vrij te geven voor anderen in ruil voor lagere kosten.
Prestatie	Per dienst worden meetbare eisen vastgesteld voor onder meer responstijd, latency, doorvoercapaciteit en verwerkingstijd. De Clouddienst maakt zichtbaar in welke mate aan deze eisen wordt voldaan.
Capaciteitsmanagement	Capaciteit van compute, storage, netwerk, energie en koeling wordt gemeten, voorspeld en tijdig uitgebreid. Afhankelijkheden tussen deze capaciteitssoorten worden gezamenlijk bewaakt.
Quota en begrenzing	Resources kunnen per tenant en dienst worden begrensd en geprioriteerd, zodat één tenant de dienstverlening aan andere tenants niet nadelig beïnvloedt.
Resource-optimalisatie	Ongebruikte of structureel overgedimensioneerde resources worden inzichtelijk gemaakt en kunnen worden afgeschaald of vrijgegeven.
Energie-efficiëntie	Energiegebruik, koeling en hardware benutting worden meetbaar gemaakt. Bij ontwerp- en vervangingskeuzes wordt naast performance en kosten ook energie-efficiëntie meegewogen.
Schaaltesten	Schaalbaarheid wordt niet alleen theoretisch ontworpen, maar periodiek gevalideerd door load-, performance- en capaciteitstesten.

6.3 Uitwisselbaarheid, overdraagbaarheid en exit

Uitwisselbaarheid beschrijft de mate waarin de Clouddienst en de daarop draaiende workloads gegevens en diensten kunnen uitwisselen met andere systemen, binnen en buiten de overheid.

Voor de Clouddienst vertaalt dit zich in de volgende eisen:

Open standaarden voor API's	Koppelvlakken gebruiken universele, platformonafhankelijke protocollen zoals HTTP/JSON (REST). De standaarden van Pas-toe-of-leg-uit van Forum Standaardisatie zijn verplicht, waaronder OAuth 2.0 voor autorisatie en Digikoppeling voor berichtenverkeer binnen de overheid.
Open bestandsformaten	Gegevens workloads, images en configuraties worden opgeslagen en uitgewisseld in open, universele formaten (zoals JSON, XML, CSV en de open geostandaarden) of volgens de standaarden uit het Federatief Datastelsel (FDS).
Gestandaardiseerde koppelvlakken	De Clouddienst koppelt via gestandaardiseerde koppelvlakken met bestaande overheidsvoorzieningen (zoals IAM, DNS en PKI) en met andere cloudomgevingen.

Voor de volledige lijst van standaarden en toetsingskaders: zie Bijlage 6 – Relevante standaarden en toetsingskaders.

Overdraagbaarheid en exit beschrijft de mate waarin workloads, gegevens, configuraties en operationele kennis naar een andere omgeving of implementatie kunnen worden overgebracht.

Voor de Clouddienst vertaalt dit zich in de volgende eisen:

Workloadportabiliteit	We gebruiken de HAVEN-standaard om de portabiliteit van een workload te garanderen, containerworkloads worden geleverd via gestandaardiseerde Kubernetes- en OCI-koppelvlakken. Platformspecifieke afhankelijkheden worden zichtbaar gemaakt en beperkt.
Data-export	Tenants kunnen hun gegevens in gedocumenteerde, gangbare en machineleesbare formaten exporteren.
Configuratie-export	Relevante tenantconfiguraties, policies, deploymentdefinities en Infrastructure-as-Code kunnen worden geëxporteerd en opnieuw worden toegepast.
Geen verborgen afhankelijkheden	Afhankelijkheden van specifieke hardware, software, licenties, operators, beheerinterfaces of leveranciers worden expliciet vastgelegd.
Exitondersteuning	De dienstbeschrijving bevat voorwaarden, verantwoordelijkheden en technische mogelijkheden voor migratie en beëindiging.
Exitvalidatie	Kritieke export-, restore- en migratiemogelijkheden worden periodiek getest. Alleen het bestaan van documentatie geldt niet als voldoende bewijs van portabiliteit.

Continuïteit tijdens migratie	Waar nodig wordt gedurende een overgangsperiode parallelle werking of gegevenssynchronisatie ondersteund.
Portabiliteit van observabilitydata	Relevante logs, metrics, traces en auditgegevens zijn overdraagbaar in gestandaardiseerde formaten.

6.4 Bruikbaarheid

Bruikbaarheid beschrijft het gemak waarmee afnemers de Clouddienst leren kennen, gebruiken en beheren. Voor een cloudplatform betekent dit vooral eenvoudig aansluiten, selfservice en consistente, goed gedocumenteerde diensten.

Voor de Clouddienst vertaalt dit zich in de volgende eisen:

Selfservice via portaal én API	Alle standaarddiensten zijn afneembaar via een selfserviceportaal en via volledig gedocumenteerde API's. Wat via het portaal kan, kan ook geautomatiseerd via de API.
Documentatie en voorbeelden	Elke aangeboden dienst heeft actuele documentatie, quickstarts en referentievoorbeelden, zodat een afnemer zonder tussenkomst van de beheerorganisatie kan aansluiten (zie de aansluitvoorwaarden in hoofdstuk 4).
Consistentie	Diensten volgen dezelfde ontwerp- en interactiepatronen, zodat kennis van de ene dienst herbruikbaar is bij de andere.
Toegankelijkheid	Het selfserviceportaal voldoet aan de overheidsbrede eisen voor digitale toegankelijkheid (WCAG, conform het Besluit digitale toegankelijkheid overheid). 100% score op internet.nl en volledig AI vindbaar. Voorwaarde: de capabilities Afnemerondersteuning en Kennisnetwerk ondersteunen afnemers bij het leren kennen en goed gebruiken van de Clouddienst. Complicatie: de afnemers omvatten alle Bestuurslagen, met sterk uiteenlopende cloudvolwassenheid. Selfservicekennis van cloudwerkwijzen wordt verondersteld; afnemers die deze kennis nog niet hebben worden via het kennisnetwerk ondersteund, in plaats van met maatwerk bediend.
Onboarding en offboarding	Afnemers kunnen via een gestandaardiseerd en zoveel mogelijk geautomatiseerd proces worden aangesloten en afgesloten.
Dienstconfiguratie	De mogelijke configuraties, kwaliteitsniveaus, afhankelijkheden, kosten en verantwoordelijkheden zijn vooraf inzichtelijk.
Ondersteuning	Afnemers hebben toegang tot actuele documentatie, trainingsmateriaal, een kennisnetwerk en ondersteuning bij migratie en ingebruikname.
Voorspelbaarheid	Dezelfde begrippen, interactiepatronen en aanvraagprocessen worden voor alle diensten gebruikt.
Foutpreventie:	Het portaal en de API's voorkomen waar mogelijk onveilige, niet-conforme of technisch ongeldige configuraties door middel van vooraf ingestelde guardrails en validaties.

6.5 Betrouwbaarheid, continuïteit en herstelbaarheid

Betrouwbaarheid beschrijft de mate waarin de Clouddienst onder normale en verstoorde omstandigheden correct blijft functioneren en zich na verstoring kan herstellen.

Voor de Clouddienst vertaalt dit zich in de volgende eisen:

Beschikbaarheidsklassen	De Clouddienst hanteert drie beschikbaarheidsklassen. Per dienst worden beschikbaarheid, onderhoudsvensters, incidentrespons, RTO en RPO vastgesteld. De gekozen klasse en de daarbij behorende verantwoordelijkheidsverdeling worden bij onboarding vastgelegd en vormt de basis voor de SLA.
Beschikbaarheid	De Clouddienst garandeert beschikbaarheid op infrastructuurniveau; de beschikbaarheid van de applicatie die van de Clouddienst gebruikmaakt is de verantwoordelijkheid van de tenant.
Redundantie	Kritieke componenten hebben geen single point of failure en worden waar nodig gespreid over foutdomeinen, availability zones en regio's *(zie 5.1.1 Datacenteroverzicht)*.
Afhankelijkheden	De beschikbaarheid en herstelbaarheid van netwerkverbindingen, datacenters, identityproviders, DNS, PKI en andere externe voorzieningen worden meegenomen in de beschikbaarheid van de gehele keten.
Backup en restore	Voor daarvoor geschikte data en configuraties worden geautomatiseerde backup- en restorevoorzieningen aangeboden. Herstelbaarheid wordt periodiek daadwerkelijk getest.
Disaster recovery	Voor kritieke diensten zijn uitwijk- en herstelprocedures beschikbaar en aantoonbaar beproefd. Zowel processen als technische procedures worden ten minste jaarlijks geoefend en getest.
Gecontroleerde degradatie	Bij een gedeeltelijke storing blijft waar mogelijk een beperkte dienstverlening beschikbaar, in plaats van volledige uitval.
Storingsdetectie	Storingen, capaciteitsproblemen en het in werking treden van redundantiemechanismen worden automatisch gedetecteerd en gemeld.
Continuïteit bij leveranciersuitval	Voor kritieke componenten is bekend welke alternatieven, broncode, kennis en herstelmiddelen beschikbaar zijn wanneer een leverancier of community wegvalt. Het moet mogelijk zijn direct naar een andere leverancier over te stappen in geval van uitval of bedreiging van kritieke componenten, dit is het "rode knop-scenario".

De Clouddienst garandeert de kwaliteit van de aangeboden infrastructuur- en Platformdiensten binnen de overeengekomen servicegrens. De tenant blijft verantwoordelijk voor de beschikbaarheid en herstelbaarheid van de eigen workload voor zover deze niet als onderdeel van de afgenomen dienst wordt geleverd.

6.6 Informatiebeveiliging en privacy

Informatiebeveiliging en privacy worden vanaf ontwerp, bouw en ingebruikname als integraal onderdeel van iedere component en dienst meegenomen. De beveiliging wordt ingericht volgens de principes security by design, zero trust, en defence in depth. De security posture bestaat dus uit meerdere, elkaar aanvullende beveiligingslagen.

Voor de Clouddienst vertaalt dit zich in de volgende eisen:

Tenantisolatie	Gegevens, workloads, netwerkverkeer, beheerfuncties en resources van tenants zijn logisch en waar vereist fysiek van elkaar geïsoleerd.
Identity & Access Management	Toegang is gebaseerd op sterke authenticatie, least privilege, functiescheiding en periodieke beoordeling van rechten. Beheertoegang en tenanttoegang zijn van elkaar gescheiden.
Privileged access	Toegang tot cruciale beheerfuncties is beperkt, tijdelijk waar mogelijk, volledig gelogd en achteraf controleerbaar.
Encryptie	Gevoelige gegevens worden tijdens transport en opslag versleuteld. Sleutels, certificaten en secrets worden centraal en gecontroleerd beheerd en periodiek geroteerd.
Sleuteleigenaarschap	Waar het risicoprofiel dit vereist, kan een tenant eigen of exclusief toegewezen cryptografische sleutels gebruiken.
Netwerkbeveiliging	Netwerkverkeer wordt standaard beperkt tot expliciet toegestane verbindingen. Firewalling, netwerksegmentatie, DDoS-bescherming, IDS/IPS en beveiligde ingress en egress worden risicogestuurd toegepast.
Kwetsbaarhedenbeheer	Software, images, firmware en configuraties worden continu gecontroleerd op kwetsbaarheden. Voor het oplossen of mitigeren van kwetsbaarheden worden termijnen op basis van ernst en risico vastgesteld.
Software supply chain	Herkomst, afhankelijkheden, integriteit en licenties van softwarecomponenten zijn inzichtelijk en controleerbaar. Softwarepakketten en deploybare componenten kunnen worden gescand, ondertekend en op herkomst worden gevalideerd.
Incidentrespons en forensics	Securityincidenten kunnen worden gedetecteerd, onderzocht en gereconstrueerd. Relevante gegevens worden veilig en volgens vastgestelde bewaartermijnen opgeslagen.
Privacy by design	Verwerking van persoonsgegevens wordt beperkt tot wat noodzakelijk is. Datalocatie, bewaartermijnen, toegang en verwijdering zijn beheersbaar en aantoonbaar.
Dataclassificatie	De toegestane dataclassificatie en het maximale beveiligingsniveau worden per dienst en ABB vastgelegd

De precieze inrichting van security operations en incidentprocessen wordt onderdeel van het operationeel model. Het Ontwerp vereist wel dat de benodigde monitoring & telemetry (inclusief logs, metrics en traces), toegangsbeheersing en technische responsmogelijkheden vanuit systemen, applicaties, netwerken en infrastructuur beschikbaar zijn.

6.7 Compliance, standaarden en audit

Compliance beschrijft de mate waarin aantoonbaar wordt voldaan aan toepasselijke wetgeving, beleidskaders, standaarden, architectuurafspraken en contractuele eisen.

Voor de Clouddienst vertaalt dit zich in de volgende eisen:

Integraal control framework	Toepasselijke eisen uit onder meer BIO2, AVG, Cyberbeveiligingswet/NIS2, ISO 27001/27002/27017/27018/22301, SEAL, Haven en de Pas-toe-of-leg-uit-lijst worden gemapt op concrete controls.
Traceerbaarheid	Iedere control is herleidbaar naar de relevante eisen, ADR's, ABB's, implementaties en bewijsstukken.
Control ownership	Voor iedere control wordt vastgelegd welke rol verantwoordelijk is voor implementatie, uitvoering, toetsing en rapportage.
Continuous compliance	Naleving wordt waar mogelijk automatisch en continu gecontroleerd, in plaats van uitsluitend tijdens periodieke audits.
Audit evidence	Loggegevens, configuratiestatus, testresultaten, wijzigingen, kwetsbaarheden, uitzonderingen en andere bewijsstukken kunnen gecontroleerd worden verzameld en beschikbaar gesteld.
Onafhankelijke toetsing	Voor relevante delen van de Clouddienst worden periodieke interne en externe audits, penetratietesten of certificeringstrajecten uitgevoerd.
Afwijkingenbeheer	Afwijkingen van kaders en standaarden worden expliciet vastgelegd, risicogestuurd beoordeeld, voorzien van een eigenaar en einddatum en periodiek herbeoordeeld.
Transparantie voor afnemers	Afnemers krijgen inzicht in de relevante compliance- en auditstatus en in de verdeling van verantwoordelijkheden tussen provider en tenant.
Standaardisatie	Technische en functionele standaarden worden centraal beheerd en waar nodig vertaald naar herbruikbare configuraties, templates en policies
Normenkaders	De normenkaders worden niet als losstaande en mogelijk overlappende eisenverzamelingen beheerd. Het integrale control framework vormt de gemeenschappelijke ingang voor implementatie, toetsing en verantwoording.

6.8 Onderhoudbaarheid, lifecycle en operationele beheerbaarheid

Onderhoudbaarheid beschrijft de mate waarin de Clouddienst veilig, voorspelbaar en met beperkte verstoring kan worden aangepast, hersteld, vervangen en doorontwikkeld. De organisatorische inrichting van deze processen valt buiten scope van Het Ontwerp. De Clouddienst moet de uitvoering ervan wel technisch ondersteunen en waar mogelijk automatiseren.

Voor de Clouddienst vertaalt dit zich in de volgende eisen:

Codegestuurde en reproduceerbare inrichting	We kiezen ervoor alles te automatiseren om menselijke fouten uit te sluiten en altijd een herhaalbaar resultaat te krijgen. Infrastructuur en platformconfiguraties worden zoveel mogelijk als code vastgelegd, onder versiebeheer, gereviewd en geautomatiseerd uitgerold.
Reproduceerbaarheid	Platformcomponenten en omgevingen kunnen op basis van vastgelegde code, configuratie en artefacten opnieuw worden opgebouwd
Immutable infrastructure	Wijzigingen aan beheerde infrastructuur worden bij voorkeur door vervanging en geautomatiseerde heruitrol uitgevoerd, niet door handmatige aanpassing van productiecomponenten.
Configuratiebeheer	De actuele en gewenste configuratie, versies, afhankelijkheden en relaties van componenten zijn inzichtelijk. Afwijkingen en configuratiedrift worden automatisch gesignaleerd.
Lifecyclebeleid	Voor iedere component en dienst zijn ondersteunde versies, patchbeleid, upgradefrequentie, end-of-life en uitfaseringsvoorwaarden bekend.
Veilige upgrades	Updates kunnen gefaseerd, getest en waar mogelijk zonder onderbreking van tenantdiensten worden uitgevoerd. Terugval naar een werkende versie is mogelijk.
Modulariteit en vervangbaarheid	Componenten hebben duidelijke verantwoordelijkheden en koppelvlakken, zodat zij met beheersbare impact kunnen worden vervangen.
Kennis en documentatie	architectuur, configuratie, operationele procedures en herstelhandelingen zijn actueel gedocumenteerd en niet uitsluitend bekend bij individuele personen of leveranciers.
Servicemanagementondersteuning	de architectuur ondersteunt event-, incident-, problem-, change-, release-, configuratie- en servicelevelmanagement met gestandaardiseerde gegevens en interfaces.

6.9 Kwaliteitsborging, observability en continue verbetering

Quality Assurance borgt dat wijzigingen en nieuwe diensten aantoonbaar aan de vastgestelde functionele en niet-functionele eisen voldoen voordat zij beschikbaar worden gesteld.

Voor de Clouddienst vertaalt dit zich in de volgende eisen:

Teststrategie	Per dienst en ABB worden relevante testsoorten, kwaliteitsdoelen, verantwoordelijkheden en acceptatiecriteria vastgesteld.
Geautomatiseerde tests	Unit-, integratie-, end-to-end-, performance-, security-, herstel- en compliancetests worden waar mogelijk onderdeel van CI/CD-pipelines.
Releasecriteria	Een release kan alleen worden uitgerold wanneer aan vastgestelde kwaliteits-, security- en compliancecriteria is voldaan of een expliciete risicoacceptatie is vastgelegd.
Code- en configuratiereview	Wijzigingen in code, configuratie en Infrastructure-as-Code worden door minimaal een tweede bevoegde persoon beoordeeld.
Observability	Alle kritieke onderdelen leveren gestandaardiseerde metrics, logs en traces waarmee functioneren, prestaties, beveiliging en afhankelijkheden inzichtelijk zijn.
Auditlogging	Beheerhandelingen, wijzigingen, toegang en securityrelevante gebeurtenissen worden herleidbaar en manipulatiebestendig vastgelegd.
Dashboarding en rapportage	Provider en afnemers krijgen passend inzicht in beschikbaarheid, performance, verbruik, incidenten, security en compliance.
Proactieve detectie (trendanalyse)	Trends in capaciteit, foutmeldingen, beveiligingsincidenten en degradatie worden tijdig gesignaleerd voordat zij tot uitval leiden.
Defect- en probleemanalyse	Structurele fouten worden onderzocht op grondoorzaak; verbetermaatregelen worden geregistreerd en gevolgd.
Continue verbetering	Testresultaten, incidenten, audits, kwetsbaarheden, gebruiksgegevens en feedback van afnemers worden gebruikt om dienstverlening en architectuur iteratief te verbeteren.

Kwaliteitsbewijs per ABB

De acceptatiecriteria en verificatiemethode van iedere ABB maken zichtbaar hoe wordt aangetoond dat het bouwblok aan de relevante kwaliteitseisen voldoet. Observability is daarmee geen afzonderlijke beheerfunctie achteraf, maar een ontwerpvereiste voor iedere relevante component en dienst.

Bijlagen

N.B. De bijlagen van Het Ontwerp staan in aparte documenten.

Hieronder de bijlagen die in het document NDS Overheidsbrede Soevereine Clouddienst Ontwerp BIJLAGEN 1 t/m 7 bij v0.9 zijn opgenomen:

Bijlage 1 – Gartner rapport Verkenning Soevereine Cloud
Versie 1.0, d.d. 30 april 2026

Bijlage 2 – NDS Cloud Notitie Verkenning Overheidsbrede Soevereine Clouddienst
Versie 1.0, d.d. 11 juni 2026

Bijlage 3 – Wetgeving
Subhoofdstukken: Internationale wetgeving; Europese wetgeving; Nederlandse wetgeving; Nederlandse wetgeving i.v.m. het Overheidsbrede karakter van de Clouddienst; Cloud wetgeving

Bijlage 4 – Lijst van succesfactoren Overheidsbrede Soevereine clouddienst
De bijlage toont de lijst van succesfactoren zoals op 20 mei 2026 verzameld bij een brede groep vertegenwoordigers van verschillende overheidspartijen en/of -dienstverleners.

Bijlage 5 – Afkortingen
Het Ontwerp is voor een Overheidsbrede dienst. Daarom zijn in deze bijlage de afkortingen hier opgenomen zodat het document opzichzelfstaand leesbaar is voor alle overheidslagen. Voor domein-specifieke (cloud) definities verwijzen wij naar de Cloud definities en begrippenlijst[41].

Bijlage 6 – Relevante standaarden en toetsingskaders
Deze bijlage bevat de set van relevante standaarden en toetsingskaders.

[41] https://pgdi.nl/files/cloud_definities_en_begrippenlijst_v1.0 16.04.2025 (vastgesteld door OBDO).pdf

Hieronder de bijlagen die in het document NDS Overheidsbrede Soevereine Clouddienst Ontwerp BIJLAGEN 7 en 8 bij v0.9 zijn opgenomen:

Bijlage 7 – Toelichting § 3.3 ADO domein Infrastructuur

Bijlage 8 – Het Ontwerp Artefacten

1. **Capability-realisatie diagram**
   Voor management/architectuurraad. Laat zien welke ABB-clusters capabilities realiseren.

2. **ABB-capabilitymatrix**
   Voor traceerbaarheid en koppeling met ADO domein Infrastructuur.

3. **ABB's per architectuurlaag view**

   ABB Modellen
   Voor de nadere technische uitwerking richting het toekomstige High Level Design van de Clouddienst.
   Deze informatie is beschikbaar in twee formaten:

   a. Als **ArchiMate export** van de gemodelleerde ABB's;
   b. Als **.pdf document** met daarin zowel de ABB postioneringsmodellen als de ABB decomposities.

   Attributenlijst ABB's
   c. Deze bijlage toont de lijst van attributen voor de ABB's per architectuurlaag en is beschikbaar als **.pdf document** met daarin de meest relevante ABB's met ingevulde attributen.