



Uitvoeringsorganisatie
Bedrijfsvoering Rijk
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

Samenvatting architectuurvisie Logius platform

UBR|HIS

Bezoekadres

Rijkskantoor Beatrixpark
Wilhelmina van Pruisenweg 52
2595 AN Den Haag

Postbus 20011
2500 EA Den Haag

Bijlage A2 Behorend bij

Europese aanbesteding Uitbesteden Infrastructuurdiensten en SIEM/SOC diensten

ten behoeve van het

ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Datum	08 juli 2019
Kenmerk	201850054.011.018

Inhoud

Inhoud	2
1 Doel van dit document	4
1.1 Doel	4
1.2 Doelgroep	4
1.3 Opbouw van het document	4
2 Huidige inrichting en uitdagingen	5
2.1 Inleiding.....	5
2.2 Kenmerken van technische inrichting	5
2.3 Ontwikkelingen gedurende de afgelopen jaren	6
2.4 Wijzigingen in de omgeving van Logius	6
3 Randvoorwaarden en afhankelijkheden	8
3.1 Inleiding.....	8
3.2 Verwerving Infrastructuur en Digipoort	8
3.3 Ondersteuning voor nieuwe applicaties en voorzieningen.....	8
3.4 Ondersteuning voor huidige applicaties en voorzieningen	9
3.5 Introductie van SAFe	9
4 Doelplatform	10
4.1 Inleiding.....	10
4.2 Schets van het doelplatform	10
4.3 Beschrijving van de onderdelen van het platform	10
4.3.1 Housing	10
4.3.2 Fysieke opslag, netwerkapparatuur en hardware	11
4.3.3 Containerinfra	11
4.3.4 Storage services	11
4.3.5 Virtual machines	11
4.3.6 Containers	11
4.3.7 Virtual Private Cloud	12
4.3.8 Logius Cloud	12
4.3.9 GMP / DBK.....	12
4.3.10 Service	12
4.3.11 Koppelvlak	12
4.3.12 Regietooling	13
4.3.13 SIEM/SOC	13
4.3.14 Identity en Access Management.....	13
4.3.15 Centrale logging en monitoring	13
4.4 Verdere toekomst.....	13

5	Onderdelen van SP Cloud	14
5.1	<i>Inleiding.....</i>	<i>14</i>
5.2	<i>Verplicht gebruik.....</i>	<i>14</i>
5.2.1	CI/CD pipeline.....	14
5.2.2	Source repo	14
5.2.3	Monitoring en logging	14
5.2.4	Netwerk	14
5.2.5	Bibliotheek.....	15
5.2.6	Identity	15
5.3	<i>Facultatief gebruik.....</i>	<i>15</i>
5.3.1	Data services	15
5.3.2	Middleware en appserver	15
5.3.3	Centraal aansluitpunt	15

1 Doel van dit document

1.1 Doel

Dit document bevat de samenvatting van de Architectuurvisie Logius Platform. Het document beschrijft op hoofdlijnen de platformarchitectuur van de Logius infrastructuur (de "containerinfra") en het bovenliggende platform (CI/CD en applicaties).

1.2 Doelgroep

De doelgroep van het document bestaat uit architecten en managers op strategisch en tactisch niveau, zowel aan de kant van Logius als bij toeleverende partijen (zoals leveranciers en system integrators). Voor iedere andere stakeholder is dit document ter kennisname.

1.3 Opbouw van het document

In dit document wordt een korte samenvatting gegeven van de huidige, technische inrichting van de Logius dienstverlening en de hierbij behorende uitdagingen, met name voor wat betreft snelheid en efficiëntie van opleveren van functionaliteit, garanderen van beschikbaarheid en continuïteit van die dienstverlening. Het document beschrijft vervolgens de manier waarop het mogelijk is met een combinatie van containerinfra en platform deze uitdagingen aan te gaan. Tenslotte geeft het document een kort overzicht van hoe deze ontwikkeling vorm heeft gekregen in de sourcingstrategie van Logius en de resulterende verkaveling.

2 Huidige inrichting en uitdagingen

2.1 Inleiding

In dit hoofdstuk is de huidige technische inrichting van de Logius dienstverlening geschetst.

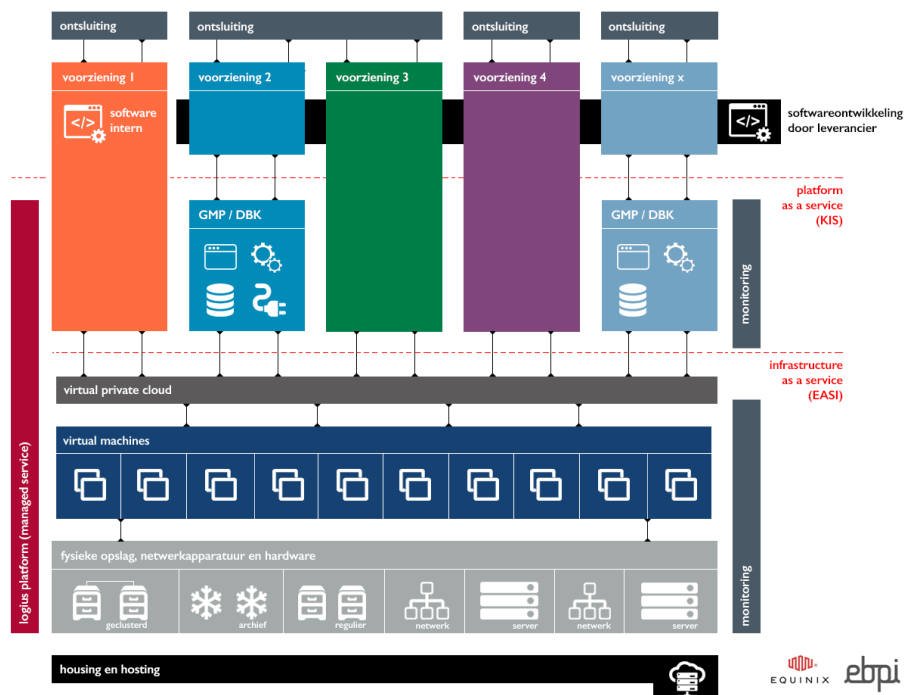
2.2 Kenmerken van technische inrichting

De huidige inrichting van de Logius dienstverlening kenmerkt zich als volgt:

1. Een grote hoeveelheid systemen en applicaties;
2. Een combinant (Equinix – EBPI) op infrastructuur en middleware;
3. Dienstverlening verdeeld over twee datacenters (ODC RWS/DJI);
4. Meerdere betrokken dienstverleners en integrators op de voorzieningen;
5. Verschillen in technische opbouw en ontwikkelaanpak;
6. Veel koppelingen met systemen in de ketens;
7. Feitelijke beschikking over assets (toegangsmiddelen, code, configuratie, data) ligt bij externe partijen;
8. Auteursrecht van code, data en ontwerp ligt bij Logius.

De dienstverlening vanuit het consortium bestaat primair uit technische bouwstenen, aangeboden via een productcatalogus. Applicatieontwikkelaars en beheerders stellen op basis van (een combinatie van) deze bouwstenen zelf een omgeving samen.

In de afbeelding hieronder is een overzicht gegeven van de huidige dienstverlening. De “as a service” aanduidingen zijn nu niet als dienstverlening ingeregeld, maar geven een logische scheiding aan.



Afbeelding 1: Huidige architectuur Logius voorzieningen. De afkortingen GMP en DBK staan voor het Generiek Middleware Platform en Dienst Beveiligd Koppelvlak, twee middleware producten die als dienst worden geleverd door Equinix/EBPI.

2.3 Ontwikkelingen gedurende de afgelopen jaren

In de afgelopen jaren is de situatie binnen en buiten Logius veranderd, namelijk:

- Vanuit de business neemt de vraag naar functionaliteit (en met name het sneller opleveren hiervan) toe. Deze tendens is kenmerkend voor de veranderingen die de verregaande digitalisering van de samenleving met zich meebrengt en daarmee niet geïsoleerd voor Logius van toepassing;
- In het verlengde hiervan heeft Logius, maar ook de afnemers en eindgebruikers van haar dienstverlening steeds meer behoefte aan de schaalvoordelen en flexibiliteit die de Cloud biedt;
- In toenemende mate wordt hergebruik (in de vorm van kennis en kunde, maar ook functionaliteit van applicaties en diensten) een vereiste bij de inrichting van de informatievoorziening van de overheid. Logius zet hier stevig op in;
- Deze functionaliteitsvraag en flexibiliteitsbehoefte zijn alleen te realiseren middels een innovatiever platform dan de huidige infrastructuur biedt.

De mate van innovatie is daarbij echter wel onderwerp van discussie: Logius zal niet in één keer al haar applicatiefunctie kunnen vertalen naar bijvoorbeeld een ontwikkelmethode op basis van microservices en onderliggende containerinfra, maar kan wel de randvoorwaarden invullen voor een dergelijke transitie.

2.4 Wijzigingen in de omgeving van Logius

Naast de uitdagingen die de huidige inrichting van de voorzieningen van Logius hebben, is in de omgeving van Logius veel veranderd. Deze veranderingen zijn in een drietal documenten, een wet en een beleidsstuk verwoord, namelijk:

- *Logius 2020*
Een initiatief om een aantal strategische organisatieveranderingen – zoals portfoliomanagement, architectuur en informatievoorziening) te adresseren;
- *Always On*
Een onderzoek naar de toegenomen complexiteit en daarmee het risicoprofiel van de voorzieningen van Logius en een schets van de benodigde veranderingen, met name op het gebied van de inzet van nieuwe technologie;
- *Maak Waar*
Rapport van de studiegroep Informatiesamenleving over het functioneren van de digitale overheid met daarin onder andere de vermelding dat de Logius voorzieningen behoren tot de vitale digitale overheidsinfrastructuur;
- *Wet GDI*
Nieuwe wet, die een overheidsinfrastructuur (voor een belangrijk deel in beheer van Logius) schetst die speciaal is toegespitst op de digitale inrichting van primaire processen van overheidsorganisaties;
- *Digitale Agenda 2020*
Beleids-ondersteuningsvoorstel voor gemeenten bij de digitalisering van hun dienstverlening met behulp van onder andere voorzieningen die in beheer zijn van Logius.

Ook in andere rapporten (zoals 'Aan de slag') wordt gesteld dat Logius niet langer voorzieningen centraal zou moeten stellen, maar de dienstverlening aan klanten. Het

begrip “voorziening” komt in de toekomst van de Logius informatievoorziening niet meer voor: er wordt slechts gesproken van (hergebruik van) functionaliteit en services.

Het antwoord van Logius op deze verander(en)de omgeving moet uiteraard meer omvattend zijn dan alleen het bieden van een nieuwe technische infrastructuur en platform. Zoals al eerder vermeld biedt deze Architectuurvisie echter alleen een blik op de mogelijke (technische) realisatie van het platform dat onder een Logius-brede informatievisie ligt.

3 Randvoorwaarden en afhankelijkheden

3.1 Inleiding

In dit hoofdstuk wordt op hoofdlijnen een viertal randvoorwaarden en afhankelijkheden bij de verdere ontwikkeling van het Logius Platform geschetst, die voortvloeien uit of impact hebben op de huidige ontwikkelingen in de Logius-omgeving.

3.2 Verwerving Infrastructuur en Digipoort

De contracten die ten grondslag liggen aan de dienstverlening van Logius rondom de Infrastructuur en Digipoort, lopen in de komende jaren af. Om deze reden is gestart met de selectie van een nieuwe dienstverlener. De selectie heeft – alleen al vanuit technisch perspectief – invloed op de toekomst van Logius (want de keuze voor een dienstverlener geldt voor meerdere jaren), maar wordt er ook door bepaald (want de mate waarop de dienstverlener invulling geeft aan de dienstverlening bepaalt mede de toekomstige inrichting van het Logius Platform).

3.3 Ondersteuning voor nieuwe applicaties en voorzieningen

Op dit moment vindt binnen een aantal proof-of-concepts realisatie van nieuwe functionaliteit plaats. De manier van ontwikkelen verschilt op drie manieren van traditionele softwareontwikkeling (binnen Logius):

- *Andere methoden voor softwareontwikkeling*
Logius is overgestapt op SAFe en past SCRUM toe binnen de ontwikkelwerkzaamheden. Het (applicatie-) voortbrengingsproces wordt gemoderniseerd en is gericht op snelle, continue doorvoer van wijzigingen en de daaraan gekoppelde nauwe samenwerking tussen ontwikkeling en beheer (DevOps). Ontwikkeling van software vindt soms in-house, soms bij een softwareleverancier plaats. Dit heeft consequenties voor de manier waarop SCRUM-teams zijn samengesteld;
- *Innovatief deliverymechanisme*
Bij de ontwikkeling van nieuwe software wordt gebruik gemaakt van het architectuurpatroon microservice, waarbij functionaliteit wordt opgesplitst in zo klein mogelijke, isoleerbare brokken die beter schaalbaar en onderhoudbaar zijn. Ondersteunende software zoals operating system, database of webserver dan wel applicatieserver zijn generiek (gemaakt) en weg-geabstraheerd naar het onderliggende platform. Het beschikbaar stellen van deze brokken functionaliteit geschiedt via een delivery pipeline, een mechanisme dat verregaande automatisering mogelijk maakt;
- *Aflevering op containers in een containerplatform*
De gerealiseerde functionaliteit wordt afgeleverd op een containerplatform. Een container is een technisch construct dat primair is bedoeld om een applicatie of applicatiefunctie zo te verpakken dat ze overal kan draaien, ongeacht de onderliggende infrastructuur. Een containerplatform wordt als product door verschillende leveranciers aangeboden en kan in zowel een publieke als private (cloud)omgeving draaien. Een belangrijk verschil tussen containers en virtuele machines (het construct dat in het huidige Managed Services contract wordt gebruikt als basis van het applicatieplatform) is dat een containerplatform efficiënter omgaat met het onderliggende systeem en meer portabiliteit biedt, hetgeen vooral van belang is bij situaties waarin meerdere partijen gezamenlijk aan software werken – zoals bij Logius. Daarnaast biedt een containerplatform veel

meer mogelijkheden voor het hoog beschikbaar, schaalbaar en performant opleveren en draaien van applicaties, bijvoorbeeld door de ingebouwde (softwarematige) voorzieningen rondom load balancing en de inrichting van een dergelijk platform met behulp van beschikbaarheidszones (in plaats van stretched VPCs, zoals in het huidige platform).

3.4 Ondersteuning voor huidige applicaties en voorzieningen

Ongeacht de ontwikkelingen zoals geschetst in paragraaf 3.2.2 zal Logius nog gedurende langere periode (naar verwachting zeker een aantal jaren) delen van de huidige dienstverlening beschikbaar moeten houden. Iedere nieuwe oplossingsrichting dient hiermee rekening te houden.

3.5 Introductie van SAFe

Gerelateerd aan wat is beschreven in paragraaf 3.2.2 geldt dat Logius per 1 januari 2019 is gekanteld naar een organisatie die is vormgegeven conform de inrichtingsprincipes van het Scaled Agile Framework. Dit betekent bijvoorbeeld (ook in het verlengde van wat in paragraaf 3.2.1 is beschreven) dat de aansturing van en relatie tot leveranciers wijzigt.

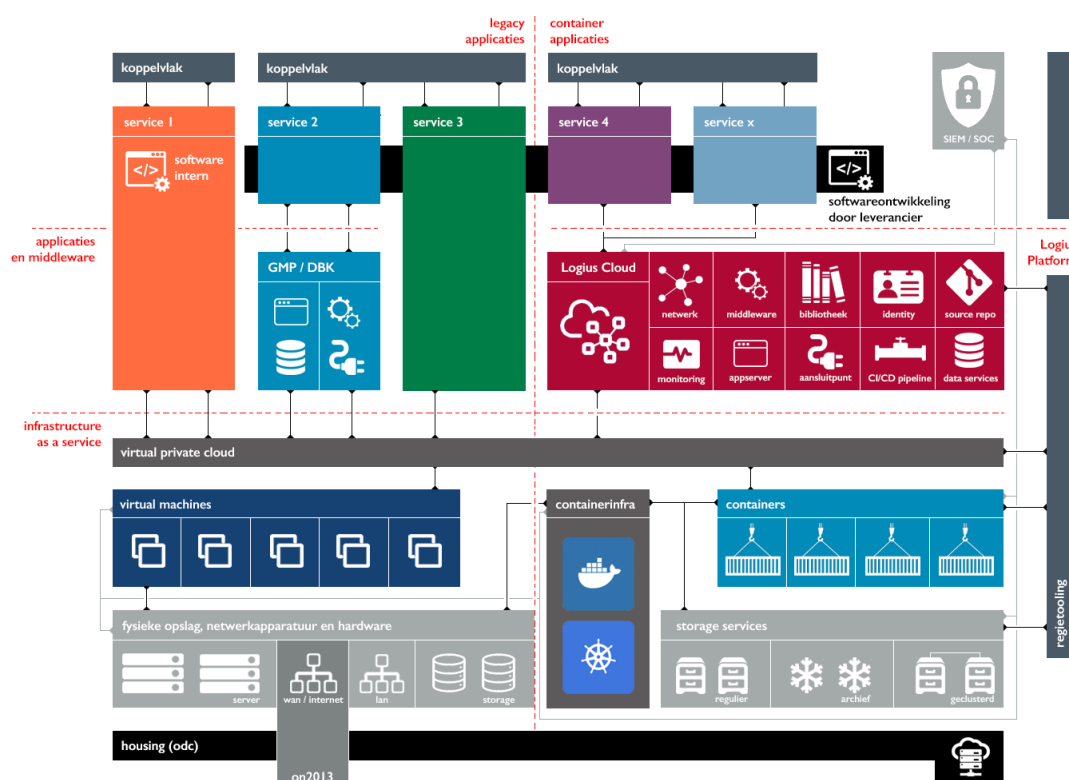
4 Doelplatform

4.1 Inleiding

In dit hoofdstuk is een korte schets en beschrijving opgenomen van het doelplatform dat Logius als het resultaat van de verwerving van de infrastructuur ziet.

4.2 Schets van het doelplatform

In de afbeelding hieronder is het doelplatform afgebeeld:



Afbeelding 2: doelplatform verwerving infrastructuur

4.3 Beschrijving van de onderdelen van het platform

In de onderstaande paragrafen zijn de verschillende onderdelen van het platform nader beschreven.

4.3.1 Housing

Conform I-Strategie Rijk (2017, 2019-2021) is *housing* van het Logius platform ondergebracht bij een Overheidsdatacentrum (ODC), meer specifiek ODC RWS/DJI. Het is waarschijnlijk dat in de toekomst de dienstverlening rondom het Logius platform vanuit een van de andere ODCs zal plaatsvinden, als uitbreiding op dan wel vervanging van ODC RWS/DJI.

De inrichting is volgens het principe van beschikbaarheidszones, waarbij iedere locatie van het ODC als een zone geldt. Een zone biedt een volledig op zichzelf staande versie van het Logius platform, waarmee een nog hogere beschikbaarheid mogelijk wordt. Uitwijk naar

een ander datacenter is eenvoudig en in principe snel (afhankelijk van de overdrachtssnelheid tussen de datacentra).

4.3.2 *Fysieke opslag, netwerkkapparatuur en hardware*

Het onderdeel *fysieke opslag, netwerkkapparatuur en hardware* vormt samen de hosting van het Logius platform, die is belegd bij een te selecteren marktpartij die haar diensten vanuit het ODC zal aanbieden. De inrichting van dit onderdeel (zoals keuze voor specifieke hardware en vormen van beheer) wordt overgelaten aan die marktpartij, binnen door Logius te schetsen kaders (zoals informatiebeveiliging) en serviceniveaus.

Hierbij geldt overigens dat Logius voor een gedeelte van de inrichting van connectiviteit gebruik maakt van het overheidsbrede raamcontract ON2013 (zie <https://on2013.nl/>).

4.3.3 *Containerinfra*

Een specifiek onderdeel van de hosting van het Logius platform is de zogenaamde *containerinfra*. Dit is de combinatie van hard- en software tot een enterprise containerplatform, bijvoorbeeld Kubernetes. De term *enterprise* betekent hier dat de versie van het containerplatform die door de marktpartij wordt geboden, wordt ondersteund door een door de Cloud Native Computing Foundation (CNCF, een leverancier-neutrale stichting die is opgericht om de verdere verspreiding van containers te bewerkstelligen) gecertificeerde leverancier. Deze leverancier biedt officiële ondersteuning op het geleverde product.

De software waarop de containerinfra is gebaseerd wordt zodanig gespecificeerd dat deze door meerdere leveranciers is te bieden. Hiermee wordt het overstappen van de ene naar de andere leverancier (bijvoorbeeld bij hernieuwde verwerving na afloop van de contracttermijn) eenvoudiger.

4.3.4 *Storage services*

Een volgend specifiek onderdeel van de hosting van het Logius platform zijn de *storage services*. Dit is een verzamelnaam voor alle diensten die betrekking hebben op de opslag van gegevens. Een storage service is een logische laag die is gebaseerd op fysieke opslag en deze opslag via onderliggende fysieke hardware (inclusief containerinfra) beschikbaar stelt aan virtual machines en containers. De storage services (block, file en object) zijn daarnaast de basis voor bovenliggende data services, onderdeel van het SP Cloud platform (zie 4.3.8).

Daarnaast zijn storage services (zoals NFS en S3) beschikbaar voor de ondersteuning van (legacy) applicaties.

4.3.5 *Virtual machines*

Bestaande applicaties en services binnen het Logius platform draaien uiteindelijk binnen virtual machines, technologie voor de virtualisatie van hardware. De virtual machines vormen een laag tussen de fysieke hardware en deze applicaties. Ook virtual machines maken deel uit van de hosting van het Logius platform.

4.3.6 *Containers*

Logius streeft ernaar nieuwe applicatie(functionaliteit) zonder uitzondering binnen containers te draaien. Een container is software waarbinnen (gecompileerde) applicatiecode en bijbehorende libraries en frameworks zijn verpakt tot een geïsoleerd geheel dat onafhankelijk van de onderliggende infrastructuur is uit te rollen. Containers kunnen naast virtual machines bestaan. Waar een virtual machine zich richt op het zo waarheidsgetrouw als mogelijk nabootsen van een volledig computersysteem, bestaat een container uit een computersysteem waaruit de onderdelen die niet noodzakelijk zijn om de erin ondergebrachte applicatiefunctie te laten werken zo verregaand als mogelijk zijn geabstraheerd. Containers zijn onderdeel van de hosting van het Logius platform en verbonden met de containerinfra uit paragraaf 4.3.3.

4.3.7 *Virtual Private Cloud*

Een virtual private cloud (VPC) is een orderingsprincipe, gevormd door een virtueel netwerk dat in de context van Logius uit drie VLANs (zogenaamde tiers) bestaat die gescheiden zijn door firewalls: een extern, productie en backend VLAN. Voor zowel virtual machines als containers geldt dat zij zich conformeren aan dit model. Dit betekent dat binnen de verschillende tiers zowel virtual machines als containers kunnen bestaan, maar wil niet zeggen dat de VPC-architectuur één-op-één wordt overgenomen naar de containerarchitectuur.

4.3.8 *Logius Cloud*

De containerinfra bestaat uit al die software die nodig is voor het beschikbaar stellen en houden van containers zodat ontwikkelaars en beheerders daarmee kunnen werken. Logius Cloud is de omgeving waarin configuratie en beheer van die software plaatsvindt. Logius Cloud wordt gebaseerd op het Standaard Platform, op dit moment onderdeel van het Ministerie van Infrastructuur en Waterstaat (IenW). Dit platform kent verschillende klanten bij verschillende ministeries, waaronder ook Logius zelf. Door Logius wordt een verregaande samenwerking onderzocht, waarbij in-sourcing niet wordt uitgesloten.

Logius Cloud is een private cloudplatform dat is opgebouwd uit herbruikbare bouwstenen, zoals voor monitoring, applicatieservers, databases en CI/CD pipelines. Logius is zelf verantwoordelijk voor de toolkeuze rondom deze bouwstenen en geeft ook invulling aan functioneel- en applicatiebeheer ervan. Concreet betekent dit dat bijvoorbeeld de tooling die samen de CI/CD pipeline vormt door Logius wordt vastgesteld, geïnstalleerd en beheerd. De containerinfra waarop Logius Cloud wordt geplaatst, dient dit mogelijk te maken. Het moet dus mogelijk zijn om specifieke componenten van de containerinfra te vervangen door eigen tools, voor zover deze componenten niet noodzakelijk zijn voor de inherente werking van die containerinfra.

Hierbij geldt als uitzondering dat monitoring en logging van Logius Cloud zelf onderdeel is van de uitgevraagde dienstverlening bij de containerinfra.

4.3.9 *GMP / DBK*

Het *Generiek Middleware Platform (GMP)* en de *Dienst Beveiligd Koppelvlak (DBK)* zijn onderdeel van de huidige dienstverlening van Logius. Op deze diensten zijn onder andere gedeelten van MijnOverheid en Digipoort gerealiseerd. Voor beide onderdelen geldt dat de bestaande dienstverlening wordt uitgefaseerd (middels herbouw). Totdat de uitfasering is afgerond, dient het Logius platform de huidige GMP en DBK dienstverlening te ondersteunen.

4.3.10 *Service*

Onder de verzamelnaam *service* valt iedere (applicatie)functionaliteit die binnen Logius wordt gebruikt om specifieke diensten te ontsluiten richting afnemers (waaronder burgers en bedrijven). In de traditionele Logius omgeving is dergelijke (applicatie)functionaliteit beschikbaar in de vorm van voorzieningen die specifieke en geïsoleerde functies hebben, zoals bijvoorbeeld DigiD of MijnOverheid. Logius stelt voor de komende jaren verservicing van deze functionaliteit echter centraal, met als doel functionaliteit te ontvlechten uit voorzieningen en hergebruik mogelijk te maken. Daarmee is een service voor het Logius platform van de toekomst een richtinggevende eenheid: functionaliteit is beschikbaar als een herbruikbare, aan de buitenwereld ontsluitbare service.

4.3.11 *Koppelvlak*

Het ontsluiten van de services zoals beschreven in paragraaf 4.3.10 gebeurt via een koppelvlak. Voor zowel bestaande als nieuwe applicatie(functionaliteit) is het mogelijk dat er meerdere koppelvlakken bestaan, maar voor nieuwe applicatie(functionaliteit) die specifiek in de vorm van services wordt aangeboden is koppelvlak in de vorm van een

(REST-gebaseerde) API-gateway preferent. Het Logius platform dient beide manieren van ontsluiting te ondersteunen.

4.3.12 *Regietooling*

Onder regietooling wordt die software verstaan die nodig is voor het ondersteunen van samenwerken, vastleggen van afspraken en het planningsproces rondom (software)ontwikkeling.

4.3.13 *SIEM/SOC*

Logius maakt gebruik van een gescheiden Security Operations Center (SOC) met bijbehorende SIEM (Security Information and Event Management) tooling. Alle logging van het Logius platform wordt apart opgeslagen en is beschikbaar voor het SOC.

4.3.14 *Identity en Access Management*

Bij het platform hoort één voorziening voor Identity en Access Management (IAM) waarmee het mogelijk is om de juiste mensen tot de juiste functionaliteit van het platform te geven (op basis van rollenscheiding). Er wordt single sign on (SSO) gerealiseerd voor alle delen van het platform.

4.3.15 *Centrale logging en monitoring*

Monitoring en logging van het platform gebeurt op basis van een set componenten die onderdeel uitmaken van het platform. Het is mogelijk om deze monitoring en logging zodanig uit te breiden dat het ook mogelijk is om hiermee applicaties en services die op het platform draaien, te monitoren.

Er is een centraal dashboard beschikbaar dat actuele inzichten biedt over de beschikbaarheid van het platform en de bovenliggende applicaties en services, op basis van rollenscheiding toegankelijk.

4.4 **Verdere toekomst**

Voor de verdere toekomst wordt ingezet op het uitfaseren van alle applicatie(functionaliteit) die is gebaseerd op virtual machines en wordt daarmee een overstap gemaakt naar volledige verservicing en containerisatie van het Logius applicatielandschap. Deze transitie en migratie wordt echter door de (beheerders, ontwikkelaars, architecten en eigenaars van) applicaties en voormalige voorzieningen zelf vormgegeven. Uitspraken over tijdslijnen en stappen zijn daarmee aan (de productmanagers van) die applicaties, maar de koers is wel degelijk op niveau van het Logius Directieteam bepaald. Wel is het belangrijk aan te geven dat de eerste voorzichtige migraties al zijn gestart en dat tijdens de komende jaren een intensivering van de activiteiten wordt verwacht.

Van het Logius platform wordt verwacht dat het gevraagde tempo van verandering moeiteloos kan bijbenen en in staat is om gedurende de komende jaren een omslag te maken van hosting op basis van virtual machines naar hosting op basis van containers.

5 Onderdelen van SP Cloud

5.1 Inleiding

In deze paragraaf zijn de verschillende onderdelen van het SP Cloud kort omschreven. Van deze onderdelen is aangegeven of ze bij gebruik van het Logius platform verplicht zijn af te nemen. Hierbij geldt wel dat het portfolio van SP Cloud nog sterk in ontwikkeling is.

5.2 Verplicht gebruik

De volgende onderdelen van SP Cloud zijn verplicht te gebruiken. Dit betekent dat indien een afnemer gebruik maakt van het Logius platform, dit specifieke onderdeel beschikbaar wordt gesteld vanuit SP Cloud.

5.2.1 *CI/CD pipeline*

Een *pipeline* bestaat uit de processen en tooling die wordt gebruikt om software (geautomatiseerd) van code naar productie te krijgen. Voor het Logius platform geldt dat de ontwikkelaar van software zelf verantwoordelijk is voor het binnen kaders¹ realiseren en opleveren van geteste, veilige broncode aan de staging repository en niet verantwoordelijk is voor het in productie brengen van deze code.

5.2.2 *Source repo*

Er is een *sourcecode-repository* - een opslagplaats voor broncode - ingericht die voor alle applicaties binnen Logius beschikbaar is. De repository is in beheer van Logius en wordt verplicht gebruikt door leveranciers, integrators en software-ontwikkelpartijen. Voor Logius leidt dit tot meer grip op versiebeheer, de kwaliteit en het uitrolproces van software.

5.2.3 *Monitoring en logging*

Vanuit SP Cloud zijn bouwstenen beschikbaar voor het inrichten van *monitoring en logging*, bestaande uit een gestandaardiseerd koppelvlak (met eenduidige aanlever- en berichtenspecificatie, ook richting het SOC), opslagmechanisme en specifieke tooling voor monitoring en logging. Daarnaast is er een Logius-breed dashboard ingericht waarop de beschikbaarheid van de applicatie(functionaliteit) en services die op SP Cloud draait zichtbaar is.

5.2.4 *Netwerk*

Binnen het SP Cloud zijn meerdere *netwerken* gerealiseerd, conform de best practice inrichting van de onderliggende containerinfra en in lijn met de huidige indeling van netwerken in het Logius platform². Alle netwerkcomponenten binnen het Logius platform zijn software defined.

¹ Deze kaders, die onder andere bestaan uit richtlijnen voor veilige applicatieontwikkeling en inrichtingsprincipes voor pipelines zijn op het moment van schrijven van dit document nog niet vastgesteld.

² Dit is verder uitgewerkt in de netwerkarchitectuur van Logius, die tijdens de inschrijvingsfase beschikbaar is.

5.2.5 *Bibliotheek*

Er is een *bibliotheekvoorziening* beschikbaar waarin het mogelijk is om containerimages, binaries en configuratiebestanden (zoals Helm charts en Dockerfiles) op te slaan. Voor ieder software-defined onderdeel van het Logius platform is het gebruik van deze bibliotheek verplicht. Dit borgt dat de volledige configuratie van het platform op een locatie is opgeslagen en terug te vinden.

5.2.6 *Identity*

Toegang tot SP Cloud is ingericht op basis van Role Based Access Control (RBAC). Er is single sign-on (SSO) ingericht voor alle onderdelen van het platform. Ook autorisatie en authenticatie in relatie tot het koppelvlak tussen applicaties en buitenwereld (zoals de API gateway) zijn in SP Cloud ingericht.

5.3 **Facultatief gebruik**

De onderstaande onderdelen zijn niet verplicht in gebruik of niet verplicht af te nemen van SP Cloud.

5.3.1 *Data services*

Er zijn *data services* beschikbaar voor de opslag van drie verschillende soorten gegevens (waarbij voor elke categorie de persistentie en beschikbaarheid is ingericht die er het beste bij past), namelijk relationeel (aangeduid met SQL), niet-relationeel (aangeduid met NoSQL) en tijdsgebonden (zoals loggegevens).

5.3.2 *Middleware en appserver*

Door SP Cloud wordt de mogelijkheid geboden om applicatie(functionaliteit) op een volledig ingericht *integratieplatform* te draaien³. Hiervoor is de suite van WSO2 beschikbaar, bestaande uit onder andere een oplossing voor API management, enterprise integration en identity en access management.

5.3.3 *Centraal aansluitpunt*

Het SP Cloud beschikt over een specifieke voorziening die het *centraal aansluitpunt* wordt genoemd, ingericht volgens de standaarden van Digikoppeling, Digimelding en Digilevering. Hiermee wordt onder andere een aantal centrale overheidsbronnen (zoals basisregistraties) ontsloten.

³ Op dit moment is deze suite nog niet beschikbaar in containervorm. De verwachting is dat dit in de nabije toekomst wel zal gebeuren.