



Uitvoeringsorganisatie
Bedrijfsvoering Rijk
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

Extract baseline architectuur Logius

UBR|HIS

Bezoekadres

Rijkskantoor Beatrixpark
Wilhelmina van Pruisenweg 52
2595 AN Den Haag

Postbus 20011
2500 EA Den Haag

Bijlage A1 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. Inleiding	3
1.1. Doel van dit document	3
1.1 Doelgroep	3
1.2 Organisatiecontext	3
1.3 Documentindeling	3
2 Context	4
2.1 Achtergrond van Logius.....	4
2.2 Doel van Managed Services	4
2.3 Scope van de dienstverlening	4
2.4 Afbakening verantwoordelijkheden	5
3 Eisen en kaders.....	6
3.1 Wet- en regelgeving	6
3.2 Beleid van de Rijksoverheid	6
3.3 Strategie en beleid van Logius	7
4 Logische en technische opzet	8
4.1 Basisopzet diensten (VM, VPC etc).....	8
4.1.1 Bundeling van diensten in VPC's	8
4.1.2 Basisbouwsteen VM.....	8
4.1.3 Gegevensopslag	8
4.1.4 Lokale netwerken	8
4.1.5 Firewalls binnen de VPC's.....	9
4.1.6 Proxy	9
4.1.7 OS-image	9
4.1.8 Rackspace	9
4.2 Beheertoegang en beheeromgevingen	9
4.3 Externe connectiviteit en beveiliging	9
4.4 Generieke diensten.....	9
4.5 Aanvullende diensten.....	10
4.5.1 Hardware Security Module (HSM)	10
4.5.2 Load balancer.....	10
4.6 Beheerondersteunende diensten	10
4.6.1 MSP	10
4.6.2 Vulnerability scanner.....	10
4.6.3 Back-up diensten.....	10
4.7 Fysiek ontwerp.....	11
5 Bijlage A: Overzicht kentallen	12

Inleiding

1.1. Doel van dit document

Dit document beschrijft de architectuur van de huidige Logius Managed Services dienstverlening op hoofdlijnen. Dit betreft de baseline architectuur. De doelarchitectuur is beschreven in andere documenten.

Het doel van dit document is om in de selectiefase van de verwerving van de nieuwe infrastructuur voor Logius de potentiële inschrijvers voldoende inzicht te geven in de huidige dienstverlening, die in de nieuwe situatie wordt voortgezet. In deze fase van de verwerving is gekozen voor een samenvattend document om niet onnodig details aan een brede, openbare verspreiding bloot te stellen.

1.1 Doelgroep

De doelgroep van dit document bestaat uit (potentiële) inschrijvers op de verwerving voor Logius Managed Services.

1.2 Organisatiecontext

Met ingang van 1 januari 2019 is Logius gekanteld naar een organisatie waarin agile werken volgens de SAFe methodiek centraal staat. De invulling hiervan bij Logius is nog in ontwikkeling. In de nieuwe organisatie zal de sturing op het beheer van de infrastructuur anders worden belegd dan voorheen. Dit document is daarop nog niet aangepast en geeft de sturing op de infrastructuur uit de voorgaande periode weer, op basis van de situatie uit 2018. In de doelarchitectuur voor de infrastructuur zal wél rekening gehouden worden met de nieuwe organisatie-indeling.

1.3 Documentindeling

Dit document geeft de huidige (baseline) architectuur weer van de Managed Services dienstverlening van Logius. Het is globaal in 3 delen verdeeld:

- Hoofdstukken 1 t/m 3 geven een inleiding, context en kaders;
- Hoofdstuk 4 beschrijft de service view van de architectuur en geeft een kort beeld van de fysieke architectuur.

2 Context

2.1 Achtergrond van Logius

Logius is een beheerorganisatie die valt onder het Ministerie van BZK met als taak het beheer van een aantal belangrijke voorzieningen van de digitale overheid. Deze hebben een onontbeerlijke rol in de communicatie tussen de overheid en het bedrijfsleven (zoals Digiport), de communicatie tussen de overheid en de burger (zoals MijnOverheid) en authenticatie en machtiging bij digitale interactie met overheidsinstellingen (zoals PKIoverheid, eHerkenning, DigiD en DigiD-Machtigen).

Logius besteedt in veel gevallen het werk voor het beheer van de voorzieningen uit en voert daarbij de regie over de dienstverlening van de leveranciers en stuurt op architectuur en integratie. Logius heeft te maken met de coördinatie van verschillende beheerpartijen voor verschillende delen van de dienstverlening.

2.2 Doel van Managed Services

Logius Managed Services biedt een gemeenschappelijke hosting infrastructuur voor de voorzieningen die Logius beheert. Daarnaast omvat de dienstverlening cluster-, middleware- en platformbouwstenen en applicatiediensten.

Logius heeft er bewust voor gekozen de verschillende applicaties niet elk te laten (voort)bestaan als volledig gescheiden kolom met eigen infrastructuur, maar deze te plaatsen op een gemeenschappelijke infrastructuur. Dit heeft een aantal doelen:

- Integratie van applicaties eenvoudiger te maken door standaardisatie en gebruik van gemeenschappelijke infrastructuur;
- Op- en afschalen van individuele applicaties eenvoudiger te maken door gebruik van standaard infrastructuurdiensten;
- Meer greep te houden op de applicaties door de applicaties en het beheer ervan in een omgeving te plaatsen waarover Logius zeggenschap heeft;
- Efficiency te bereiken door standaardisatie en het creëren van schaalgroottes.

2.3 Scope van de dienstverlening

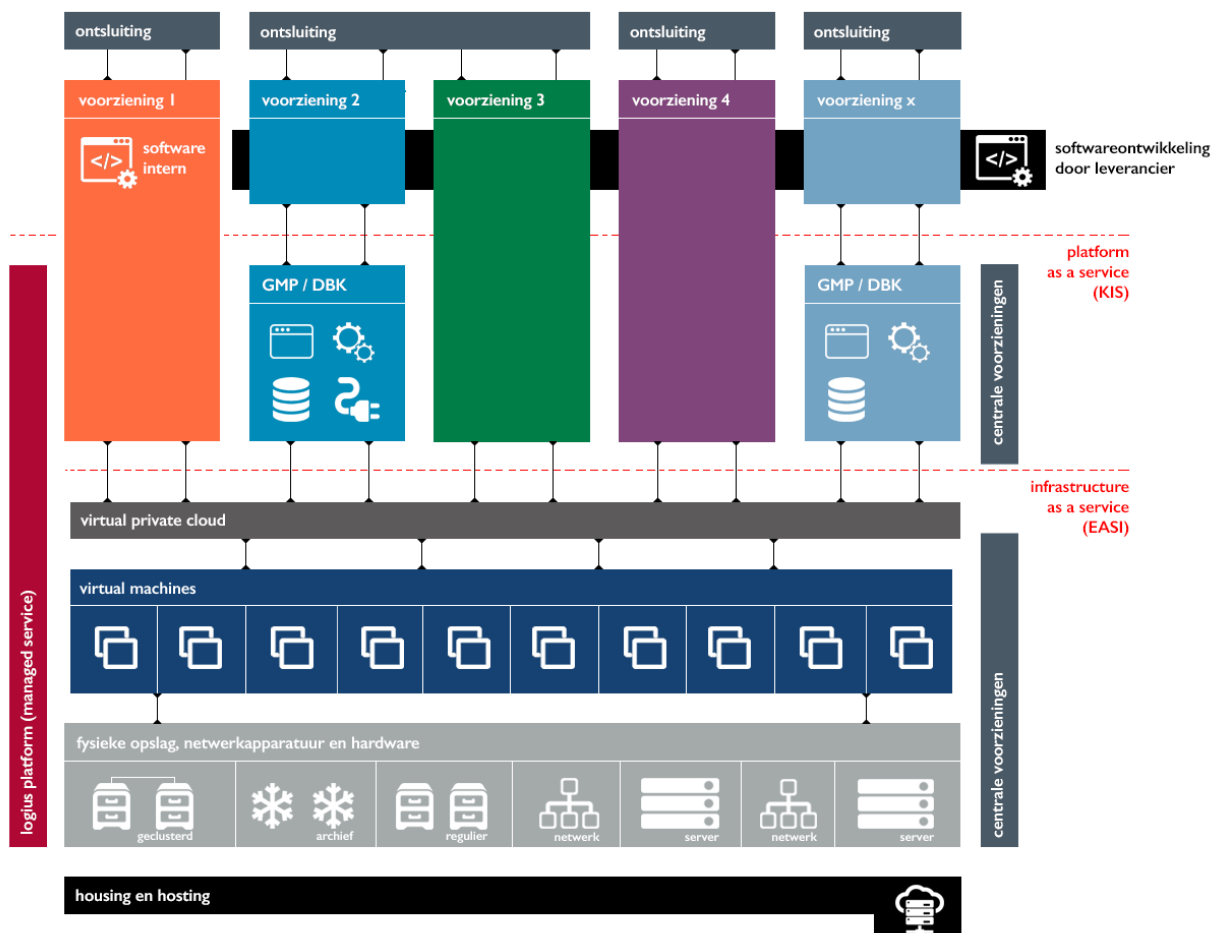
De kern van de Managed Services omvat:

- Hosting diensten op basis van virtual machines;
- Opslagcapaciteit met back-up en restore;
- Interne connectiviteit: lokale netwerkvoorzieningen en – bekabeling binnen datacenters;
- Verbinding tussen datacenters;
- Gemeenschappelijke ondersteunende diensten;
- Externe connectiviteit en DDoS protectie.

Conform I-Strategie Rijk is *housing* van het Logius platform ondergebracht bij een Overheidsdatacentrum (ODC), meer specifiek ODC RWS/DJI. Housing omvat apparatuurkasten in een eigen kooi, stroomvoorziening inclusief UPS en koeling.

Bovenop de infrastructurele diensten biedt Managed Services ook middlewarediensten.

Naast de op virtual machines gebaseerde hosting biedt de infrastructuur sinds kort ook containerservices als bestelbare optie. In de huidige opzet worden deze behandeld als een applicatie-omgeving draaiend in een eigen VPC. In onderstaande figuur is weergegeven hoe applicaties en middleware landen op de Managed Services infrastructuur.



2.4 Afbakening verantwoordelijkheden

Zoals aangegeven heeft Logius te maken met verschillende beheerpartijen die verschillende delen van de Logius voorzieningen beheren:

- Applicatiebeheerpartijen, die de applicaties van e-overheid voorzieningen beheren en doorontwikkelen;
- De infrabeheerpartij, die de onderliggende infrastructuur beheert;
- De middlewarebeheerpartij, die de gemeenschappelijke middleware beheert.

Managed Services is zo ingericht dat de applicatiebeheerpartijen en de middlewarebeheerpartij elk verantwoordelijk zijn voor de beheerde diensten en de machines en omgeving waarop deze draaien. Bemoeienis van de infrabeheerpartij wordt beperkt tot die gevallen waar technische eisen of functiescheiding dit nodig maken. Dit wordt bereikt door hen een eigen domein te bieden *binnen* het domein van de Logius Managed Services infrastructuur. Daarbij moeten zij zich houden aan de algemene regels van het domein van de Logius Managed Services infrastructuur.

3 Eisen en kaders

Het beleid van Logius wordt naast wet- en regelgeving bepaald door het algemene beleid van de (rijks)overheid voor informatievoorziening en beveiliging daarvan. De onderstaande opsomming is niet volledig, maar geeft een goed beeld van de belangrijkste onderdelen.

3.1 Wet- en regelgeving

Algemene wet bestuursrecht

De algemene wet bestuursrecht verplicht bestuursorganen die elektronisch berichten verzenden, dit op een voldoende betrouwbare en vertrouwelijke wijze te doen. Modernisering van het elektronisch bestuurlijk verkeer geeft burgers en bedrijven het recht gegevens elektronisch aan te leveren.

Wetboek van Strafvordering

Dit bevat een mogelijke verplichting tot verstrekking van gegevens aan politie en Openbaar Ministerie in het kader van strafrechtelijk onderzoek.

AVG (Algemene verordening Gegevensbescherming, 2016)

De privacywetgeving vereist van Logius dat het zich kan verantwoorden over het gebruik van persoonsgegevens, de opgeslagen persoonsgegevens goed beveiligt en melding maakt van eventuele datalekken. Ook relatief kleine registraties als die van (applicatie)beheerders moeten in beeld zijn. Op niveau van de infrastructuur leidt dit tot de eisen aan beveiliging van de opgeslagen gegevens van voorzieningen en monitoring van gebruik en beveiliging.

3.2 Beleid van de Rijksoverheid

I-Strategie Rijk (2017 en eerder)

De rijksoverheid streeft naar consolidatie van datacenters, realisatie van rijksbrede netwerken (RON) en verbeteren van de samenwerking van ICT-dienstverleners om tot een beter interoperabiliteit van hun clouddiensten te komen. In de eerdere I-strategie agenda's is aangegeven dat het Rijk streeft naar een private cloud, waarbij voor de overheid belangrijke gegevens in eigen datacenters worden opgeslagen.

BIR 2012, BIR 2017 en BIO

De Baseline Informatiebeveiliging Rijksdienst uit 2012 is toegepast op de Managed Services dienstverlening. De BIR streeft naar een voldoende hoog en interoperabel niveau van informatiebeveiliging bij alle rijksdiensten. De BIR is herzien in 2017, dit heeft niet geleid tot grote aanpassingen van de maatregelen. De BIR is overheidsbreed geadopteerd als Baseline Informatiebeveiliging Overheid (BIO).

Digitale Agenda 2020

Ondersteuningsvoorstel voor gemeenten bij de digitalisering van hun dienstverlening met behulp van onder andere voorzieningen die in beheer zijn van Logius.

Normen Bureau Forum Standaardisatie

De Rijksoverheid past in principe de open normen en standaarden op de 'pas-toe-of-leg-uit-lijst' van het Forum Standaardisatie toe.

Normen ICT-beveiligingsassessments DigiD

Aan het gebruik van DigiD voor authenticatie wordt als voorwaarde gesteld, dat organisaties en websites die van DigiD gebruik maken, voldoen aan de Normen ICT-beveiligingsassessments DigiD. Dit om misbruik van (de aansluiting op) DigiD te voorkomen. Elke website die van DigiD gebruik maakt, dient regelmatig hierop geaudit te worden.

NCSC richtlijnen

Het NCSC (Nationaal Cyber Security Centrum) brengt aanbevelingen uit voor de toepassing van beveiligingsmaatregelen. De bekendste hiervan zijn de "ICT-Beveiligingsrichtlijnen voor Webapplicaties" en de "ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)".

3.3 Strategie en beleid van Logius

Logius heeft als beleidsdoelen:

- **Bruikbaarheid**
Diensten zijn altijd toegankelijk, doelmatig, samenhangend, beschikbaar en persoonlijk;
- **Genericiteit en flexibiliteit**
Diensten zijn standaard, voor iedereen, herbruikbaar, op meerdere manieren bereikbaar, multi-channel, en multi-tenant;
- **Betrouwbaarheid en Veiligheid**
Diensten zijn veilig, 24x7, compliant, vertrouwelijk, modulair, herleidbaar en verantwoordelijkheden zijn gescheiden;
- **Efficiency**
Kosteneffectiviteit en standaardisatie bereiken door gebruik van één gemeenschappelijk hosting platform.

4 Logische en technische opzet

4.1 Basisopzet diensten (VM, VPC etc)

In onderstaande paragrafen is de basisopzet van de verschillende diensten binnen Managed Services beschreven.

4.1.1 *Bundeling van diensten in VPC's*

De diensten worden aangeboden in de vorm van VPC's (Virtual Private Cloud), virtuele datacentra met virtuele servers, netwerken en opslag. Servers en daarbij behorende opslag en netwerken worden niet buiten een VPC aangeboden.

Een VPC is opgezet conform het drie tier model.

4.1.2 *Basisbouwsteen VM*

De basisbouwsteen voor de Managed Services dienstverlening is de Virtual Machine (VM) waarop de verwerking plaatsvindt.

De architectuur is gecompartmenteerd waarbij beheer en productieverkeer van elkaar gescheiden is.

Aanmaken van VM's, monitoring op VM niveau en ander technisch beheer van de VM's wordt uitgevoerd door de leverancier van Managed Services. De inrichting hiervan is buiten scope van dit document.

4.1.3 *Gegevensopslag*

Gegevensopslag binnen het platform wordt aangeboden in 2 varianten:

1. Block storage
Een hoeveelheid "ruwe" diskruimte (LUN) op het SAN, aangeboden via de virtualisatie van VMware;
 2. File storage
Toegang tot een file share op een NFS file server. Deze is virtueel geïsoleerd en wordt exclusief aan één VPC aangeboden. Het storage netwerk is opgezet als private VLAN, zodat VM's die dit gebruiken, alleen met de NFS server en niet met andere VM's kunnen communiceren.
- Extra: Objectstorage
In een aantal gevallen wordt aanvullende opslag buiten de Managed Services infrastructuur gebruikt.

4.1.4 *Lokale netwerken*

Binnen het platform worden laag-2 virtuele netwerken (VLAN's) gedefinieerd die alleen die VM's met elkaar verbinden die rechtstreeks met elkaar mogen communiceren. In voorkomende gevallen zijn deze gestretcht.

4.1.5 *Firewalls binnen de VPC's*

De VPC heeft firewalls. Deze reguleren het verkeer met de netwerken buiten de VPC's, tussen de VPC's en tussen de tiers.

4.1.6 *Proxy*

Aan een VPC kunnen proxy servers worden toegevoegd die zowel forward (uitgaand) als reverse (inkomend verkeer) proxies worden aangeboden.

4.1.7 *OS-image*

In de image repository worden de diskimages van elke VM opgeslagen. De infrabeheerpartij heeft de taak te zorgen dat de images goed integreren met de VM omgeving. Er zijn twee soorten images:

1. *Golden Image*
2. *Custom Image*

4.1.8 *Rackspace*

De dienst Rackspace of "appliance" biedt de mogelijkheid om specifiek voor een applicatie benodigde apparatuur die geen onderdeel uitmaakt van het dienstenaanbod van de leverancier in het datacenter onder te brengen en met de netwerken te verbinden.

4.2 **Beheertoegang en beheeromgevingen**

Bij de toegang tot het Managed Services platform zijn de volgende uitgangspunten gehanteerd:

1. Gebruikers (applicatiebeheerders) krijgen toegang via een jumphost constructie;
2. Gebruikers krijgen beperkte toegangsmogelijkheden;
3. Beheermiddelen bevinden zich binnen het platform;
4. Uitgaand verkeer wordt beperkt.

4.3 **Externe connectiviteit en beveiliging**

De externe connectiviteit van het Managed Services platform is essentieel voor het gebruik ervan. Het Managed Services platform heeft twee externe verbindingen:

1. Internet: hierover hebben burgers, bedrijven en organisaties verbinding met de voorzieningen/applicaties die draaien op Managed Services;
2. Diginetwerk: een besloten netwerk van netwerken dat verbinding biedt met overheidsinstellingen, gemeenten, provincies en partnerorganisaties van de overheid.

De verbindingen zijn redundant uitgevoerd.

4.4 **Generieke diensten**

Applicaties in de VPC's worden ondersteund door een aantal generieke (netwerk)diensten. Deze bieden:

1. Tijdsynchronisatie met NTP (network time protocol). Dit maakt het mogelijk alle servers dezelfde systeemtijd te geven;
2. Domeinnaamresolutie en interne domeinnaam-hosting met DNS (domain name system);
3. Login en gebruikersinformatie (applicatiebeheerders) met LDAP en 2-factor authenticatie;
4. Afleveren van log-informatie bij een centrale logserver;
5. Verzenden en ontvangen van e-mail met SMTP resp. POP en IMAP; Dit maakt het mogelijk verzenden en ontvangen van mail met een eenduidig niveau van beveiliging (virusscanning, spamfiltering, DKIM, SPF en DMARC);
6. 2FA-Web is een 2-factor authenticatievoorziening die gebruik maakt van de eigenschappen van webbrowsers en die geïntegreerd wordt met webapplicaties

4.5 Aanvullende diensten

Naast de generieke diensten is er een aantal aanvullende diensten die naar keuze kunnen worden afgenomen. Sommige diensten worden opgenomen in het communicatiepad tussen eindgebruiker en applicatie. Andere diensten worden gebruikt voor verwerking of opslag van gegevens.

4.5.1 Hardware Security Module (HSM)

Een aantal applicaties heeft behoefte aan een zeer hoog niveau van bescherming van de gebruikte cryptografische sleutels.

4.5.2 Load balancer

Om de werklast te verdelen over verschillende VPC's of servers is er een behoefte aan load balancers die het netwerkverkeer (en daarmee werklast) op een aan de applicaties aangepaste manier verdelen.

4.6 Beheerondersteunende diensten

Daarnaast zijn er diensten gericht op de medewerkers van Logius en applicatiebeheerpartijen ter ondersteuning van beheer of beveiliging.

4.6.1 MSP

Ter ondersteuning van de dienstverlening biedt de huidige dienstverlener een Managed Services Portaal (MSP), dat vanuit Logius en voor applicatiebeheerders toegankelijk is.

4.6.2 Vulnerability scanner

Op het platform is een verplichting van geautomatiseerd vulnerability scanning t.b.v. vulnerability management proces.

4.6.3 Back-up diensten

Onderdeel van de geleverde diensten zijn back-ups en restore mogelijkheden.

4.7 Fysiek ontwerp

De dienstverlening van de infraleverancier bestaat uit gevirtualiseerde servers en netwerken. De verantwoordelijkheid voor de kwaliteit hiervan ligt bij de infraleverancier, maar Logius heeft wel een aantal eisen gesteld aan de technische en fysieke opzet van de onderliggende infrastructuur.

- **Gesloten**
Als belangrijkste eis geldt dat de fysieke locatie en de afbakening van de fysieke infrastructuur nauwkeurig bekend en afgebakend moeten zijn;
- **Exclusief**
Het is niet toegestaan componenten van de kern van de dienstverlening te delen met andere klanten van de infrabeheerder. Dit omvat de servers, de storage, LAN componenten, netwerkkaparaatuur voor de verbindingen die de twee datacenterlocaties verbinden en de Centrale firewall;
- **Binnen Nederlandse jurisdictie**
De apparatuur en opgeslagen gegevens moeten zich op een plaats bevinden die onder Nederlandse jurisdictie valt;
- **Fysiek gescheiden beheeromgeving**
De applicaties waarmee direct de werking en configuratie van de systemen onder de Managed Services diensten wordt beheerst, alsmede de LDAP directory, dienen gescheiden te zijn van apparatuur die dergelijke functies voor andere klanten vervult;
- **Beveiliging beheeromgeving**
Toegang tot de beheeromgeving van waaruit de infraleverancier de Managed Services dienstverlening beheert, dient sterk beveiligd te zijn en te voldoen aan de eisen van de BIR en de best practices voor een kritieke omgeving;
- **Redundant**
Alle kritieke apparatuur (apparatuur waarvan uitval zou leiden tot uitval van een aanzienlijk deel van de dienstverlening) moet dubbel uitgevoerd zijn en voorzien van een mechanisme om de taak van uitgevallen apparatuur (vrijwel) ongemerkt over te nemen.

5 Bijlage A: Overzicht kentallen

Onderstaande tabellen geven een beeld van de volumes van de applicaties binnen de Logius-dienstverlening.

	Voorzieningen				
	DigiD	DigiD Machtigen	Digilevering	Digimelding	Mijn Overheid
Containergebruik	ja	deels	nee	nee	nee
VM's	272	42	58	63	251
Cores	1389	178	189	186	830
RAM (GB)	5338	804	770	740	2808
SAN (GB)	201520	25990	51250	9760	103330
NAS (GB)	13000	1160	0	30	1000

	Voorzieningen					
	BSNK	eHerkenning	PKIo	Beheer-omgeving	Digipoort OTP	Digipoort
Containergebruik	nee	nee	nee	nee	nee	nee
VM's	244	20	8	156	252	272
Cores	399	42	9	548	1166	1256
RAM (GB)	810	110	18	2271	4572	4880
SAN (GB)	19160	690	280	83570	469740	70850
NAS (GB)	0	110	0	20000	11640	1000

Deze gegevens zijn indicatief, hieraan kunnen geen rechten ontleend worden.