Gemeente Sittard-Geleen

DELIVERY/DEPLOYMENT CONTRACT





I N H O U D S O P G A V E

1. INFRASTRUCTUUR OMSCHRIJVING 3

1.1 Cloud resource provider 3
1.2 Subscriptions AKS 3
1.3 Azure resources 4
1.4 Open source infra tools 4
1.5 Documentatie platform 5

2. DEFINITIES IN KADER VAN DEPLOYMENT 6

3. WAT VOOR EEN SOFTWARE ZETTEN WE WEL/NIET OP DE HAVEN OMGEVING 7

3.1 Op Haven: ontwikkeld vanuit Common Ground 7
3.2 Op Haven: Geheel open source die doorontwikkeld wordt in lijn met CG 7
3.3 Niet op Haven 7

4. CONNECTIVITEIT EN INTEGRATIECOMPONENTEN 8

5. BESCHIKBAAR MAKEN APPLICATIE VOOR GEBRUIKERS 11

6. WELKE RECHTEN KRIJGT U ALS COMPONENT DIENSTVERLENER 12

6.1 Deployment orkestratie via gitversiebeheersysteem 12
6.2 Kubernetes API 12

7. WAT VERWACHTEN WIJ VAN EEN COMPONENT DIENSTVERLENER 13

7.1 Kwalitatief/onderhouden software 13
7.2 Containers & software image 14
7.3 Veiligheidsmaatregelen leveringsketen 15
7.4 Schaalbaarheid en starts/stops 16
7.5 Helm charts 17
7.6 Namespaces 17
7.7 100% Automatisering 17
7.8 Adressering van componenten 18
7.9 Deployment orkestratie (Gitversiebeheersysteem) 18
7.10 Bij gebruik van een mailservice 19
7.11 Communicatie tussen componenten 19
7.12 Communicatie met andere omgevingen van de gemeente 20
7.13 Communicatie met diensten van derden 20
7.14 Database migraties 20
7.15 Concurrency/stateless 20
7.16 Configuratie/secrets 21
7.17 Versleutelen (encryptie) 22
7.18 SBOM (Software Bill Of Materials) & IBOM (Interface Bill of Materials) 22
7.19 Probes 22
7.20 Logging 23
7.21 Metrics 23
7.22 Resource requirement 24
7.23 Release notes 24
7.24 Documentatie & gegevensoverdracht 24
7.25 Backward compatibel 25

1. Infrastructuur omschrijving

1.1 Cloud resource provider

We maken momenteel gebruik van Microsoft Azure Kubernetes Service (AKS). Desalniettemin moet de gemeente te allen tijde kunnen overstappen naar een alternatief cloud Kubernetes-platform. Om deze reden vertrouwen we, naast de Haven-standaard, op een samenhangende set open source beheertools en proberen we zo min mogelijk afhankelijk te zijn van Azure-services. Een externe marktpartij zorgt ervoor dat deze beheertools altijd up-to-date zijn, kwetsbaarheden worden opgelost, en door de samenhang te waarborgen kunnen we gemakkelijk naar een nieuwe Kubernetes-versie migreren.

De gemeente koos voor een Kubernetes-service van een public cloudprovider bij de opstart, omdat op deze manier het snelst een werkende Kubernetesomgeving te realiseren is. Specifiek koos de gemeente voor AKS vanwege de bestaande contracten met Microsoft, waardoor aparte aanbestedingen niet nodig waren.

De gemeente gaat anders om met zeer gevoelige/geheime gegevens. De gemeente overweegt hiervoor een aparte Havenomgeving op te zetten of (tijdelijk) te werken met confidential computing binnen Azure. Bij een aparte Haven omgeving levert een Nederlands of Europees moederbedrijf dat valt onder de Nederlandse jurisdictie die Kubernetesomgeving. De Kubernetes-omgeving die zij aanbieden, mag niet gebaseerd zijn op publieke cloudproviders. De CI/CD straat van beide omgevingen (Azure Haven en Haven gevoelige gegevens) blijft één entiteit.

De gemeente volgt de ontwikkelingen en aanbevelingen van de IBD, VNG en NCSC nauwlettend. Ook ontwikkelingen met betrekking tot een Europese cloud worden gevolgd. Op basis van de ontwikkelingen kan de gemeente besluiten om de Havenomgeving, die momenteel op Azure draait, over te zetten naar een andere Kubernetes-omgeving.

1.2 Subscriptions AKS

Op dit moment biedt team IM & ICT van de gemeente Sittard-Geleen alleen aan haar eigen gemeente een Havenomgeving aan. Er zijn echter ook andere gemeenten en semi-overheidsinstanties die graag ICT-dienstverlening bij de gemeente Sittard-Geleen willen afnemen en daarmee uiteindelijk ook een Havenomgeving.

De volgende insteek hanteert de gemeente:

- Elke gemeente/ semi-overheidsinstantie maakt gebruik van eigen Azure subscriptions. Dit vereenvoudigt de facturering omdat Azure per subscriptie grafisch inzicht geeft in de kosten. Daarnaast zorgt deze aanpak voor een beveiligingsafbakening tussen de omgevingen van de organisaties.
- Eén Azure subscription voor elk van de OTAP-omgevingen. Dit zorgt voor een beveiligingsafbakening tussen de verschillende omgevingen.
- Niet elke gemeente/semi-overheidsinstantie heeft de volledige set aan OTAP omgevingen nodig.

1.3 Azure resources

Hieronder vindt u de huidige lijst (Q2 2024) aan Azure resources. Deze kan natuurlijk met de tijd wijzigen.

Soort	Azure resource	Opmerking
Kubernetes (k8s)	Azure Kubernetes Services (AKS)	Kubernetesversies worden maandelijks bijgewerkt. Eerst op test dan acceptatie en vervolgens productie. Het tijdsbestek tussen de omgevingen bedraagt 2 weken.
SQL DBMS	Azure Database voor PostgresSQL	• PostgreSQL14 is Q2 2024 in gebruik • Database Tijdzone is UTC • Upgrades worden tijdig aangegeven.
Storage	Azure Storage Accounts	Gebruikt AKS standaard
Identity Management	Active Directory/ Entra ID	Azure Entra ID gebruiken bij identiteitsbeheer. Als een andere identiteitsoplossing wordt gebruikt, moet er een ontheffing worden verkregen met een plan voor toekomstige migratie naar Entra.
Load balancer	TCP native Kubernetes load balancer. In het geval van een load balancer gaat het om het verwerken van inkomend verkeer op basis van verzoeken van een applicatie buiten het cluster. Het is niet van toepassing wanneer een applicatie binnen het cluster een service buiten het cluster bevraagt.	• Wanneer de gemeente (of de Haven-partner) een Kubernetes Service van het type LoadBalancer creëert, zorgt AKS ervoor dat een Azure Load Balancer wordt geconfigureerd om het verkeer naar de service te routeren. • Bevindt zich op Layer 4 (Transport). • In elke omgeving wordt één publieke load balancer en één privé load balancer ingezet.

1.4 Open source infra tools

Hieronder vindt u een beschrijving van de open source infra tools (Q2 2024) die voor u als component dienstverlener relevant zijn.

Soort	Toelichting
Secret en certificaatmanagement	We gebruiken Sealed Secrets. De secrets worden via Kubeseal CLI versleuteld en veilig opgeslagen in de deployment orkestratie tool (gitversiebeheersysteem). In de POD ontsleuteld de Sealed Secrets Controller de secrets. https://fluxcd.io/flux/guides/sealed-secrets/ Als u een PKI overheidscertificaat nodig heeft, vraagt de gemeente dit voor u aan. Het aanmaken van self signed certificaten via de certificaatmanager in Haven gebeurt Q2 2024 door de platformbeheerder. Dit zijn SAN certificaten. We gebruiken geen

	wildcard voor componenten. De gemeente moet nog overwegen of het aanmaken van certificaten bij platformbeheer blijft liggen of dat de mogelijkheid voor het aanmaken tevens bij de component dienstverlener wordt neergelegd.
Deployment orkestratie	De gemeente zet Gitlab in als gitversiebeheersysteem. De gemeente zet Flux in voor continous delivery. https://fluxcd.io/ De combinatie van Gitlab en Flux zetten we in voor de implementatie van Kubernetes resources. De documentatie die specifiek is voor de gemeente Sittard-Geleen neemt u op in de wiki van het gitversiebeheersysteem van de gemeente. Mogelijk dat de gemeente in de toekomst toch de keuze maakt voor Azure DevOps ivm kosten.
Ingress controller (reverse proxy binnen Kubernetes ecosysteem)	De gemeente zet NGINX in als Ingress Controller. Een ingress controller bevindt zich op Layer 7 (applicatie). In elke omgeving wordt één privé en één publieke Ingress Controller ingezet. De ingress controller wordt alleen ingezet als de APIgateway niet wordt ingezet.
Analyseren logdata	De gemeente zet Grafana Loki in voor het analyseren van logdata.
Omgevingsspecifieke documentatie	De gemeente bekijkt nog of ze voor deze documentatie bookstack inzet of gebruikt wil maken van de wiki binnen Gitlab.

1.5 Documentatie platform

Gedetailleerde documentatie van het platform is op het gitversiebeheersysteem (gitlab) van de gemeente terug te vinden. Tot deze documentatie krijgt u na het verlenen van de juiste rechten toegang.

2. Definities in kader van Deployment

OTAP omgevingen
Ontwikkel-, Test-, Acceptatie-, Productieomgeving(en).

Infrastructuurplatform 'Haven'
Het infrastructuurplatform 'Haven' fungeert als de basisinfrastructuur voor het platformecosysteem. Op deze infra installeren en beheren we onze microservices in het kader van de Common Ground.

Platformecosysteem (applicatieniveau)
Het platformecosysteem op applicatieniveau bestaat uit een set van componenten (microservices) die in samenhang een oplossing bieden, zoals Openzaak en Zaak Afhandel Component. Het ecosysteem bevordert samenwerking tussen verschillende ontwikkelaars, leveranciers en gebruikers.

Installatie
Het deployen van een component (bijv. Helm chart uitvoeren zodat Open Zaak, Appsemble, Zaak Afhandel Component, ApiSix technisch draaien).

Configuratie
Parameters zodat de component kan doen wat het moet doen (bijv. API parameters of de instellingen op de PODS om componenten met elkaar uit te laten wisselen).

Inrichting
Functionele vulling van het component evt. met hele specifieke configuratie (bijv. zaaktypen, processen, translaties van Stuf naar API, routing binnen integratiecomponenten).

Platformbeheerder
De beheerder van het infrastructuurplatform 'Haven'.

Component dienstverlener (opdrachtnemer voor deployen CG component)
De beheerder van het Common Ground Component op de Haven-omgeving van de gemeente:

- Installeren, up to date houden en oplossen problemen Common Ground Component.
- Het configureren van een Common Ground Component.

Op deze dienstverlener is het Delivery Deployment Contract van toepassing.

Dienstverlener functionele inrichting
De dienstverlener die invulling geeft aan de functionele inrichting van het common ground component.

3. Wat voor een software zetten we wel/niet op de Haven omgeving

3.1 Op Haven: ontwikkeld vanuit Common Ground

We nemen alleen een bestaand Common Ground component in gebruik als één of meerdere andere gemeenten hierin investeren en het aansluit bij de kaders van regieorganisatie Common Ground. Ook een Common Ground component waarin we (samen met anderen) investeren en die succesvol is nemen we in gebruik.

3.2 Op Haven: Geheel open source die doorontwikkeld wordt in lijn met CG

Bestaande open source software zetten we ook op de Haven als:

- Deze geheel open source is of nu en in de toekomst de gemeenschapsversie in gebruik is.
- In lijn met de Common Ground door te ontwikkelen valt en wordt.
- Het een kwalitatief en goed onderhouden open source project is
    - Het project heeft regelmatige en consistente ontwikkelingsactiviteit. Dit betekent dat er nieuwe functies worden toegevoegd, bugs/kwetsbaarheden worden opgelost en pull requests worden beoordeeld en samengevoegd.
    - Het project heeft een actieve community die bijdraagt aan discussies, het indienen van bugrapporten/kwetsbaarheden, het maken van pull requests etc.
    - Het project heeft geplande en stabiele releases met duidelijke releasenotes en update-instructies.
    - De code maintainers (diegene die die de bijdragen van contributors accepteren) een belang blijven hebben bij goedwerkende software omdat ze er zelf dienstverlening op bieden.
- Software met persistente opslag van verwerkingsgegevens aansluit of aan te sluiten is bij een microservice-architectuur.

3.3 Niet op Haven

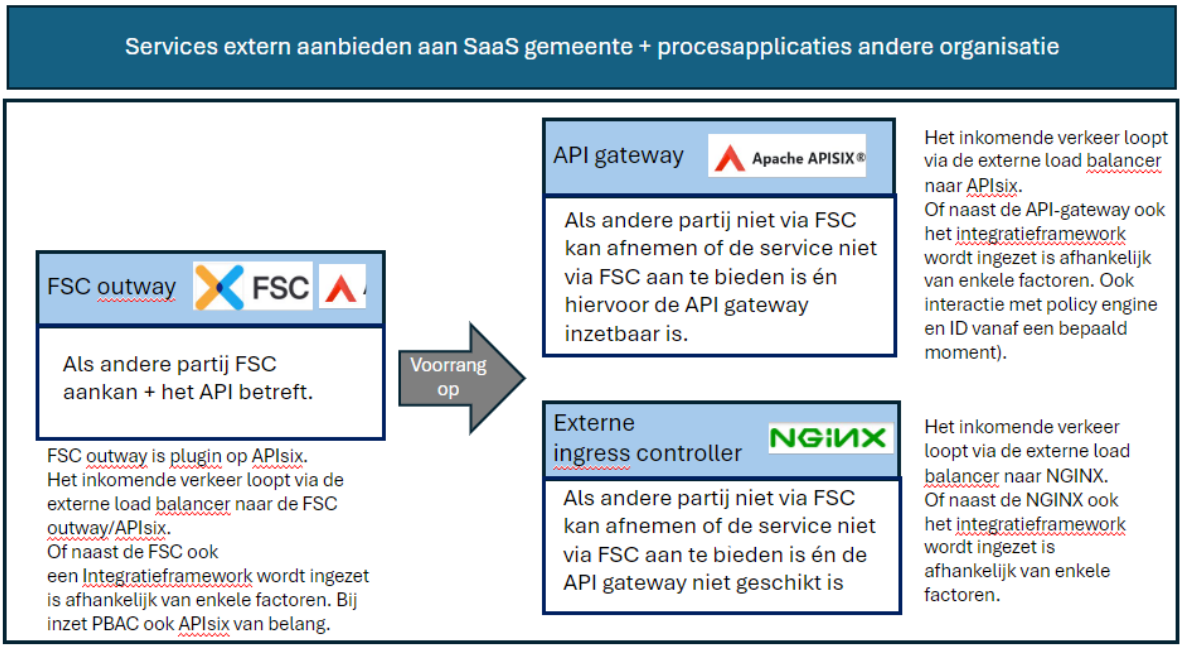
We zetten geen software op Haven die:

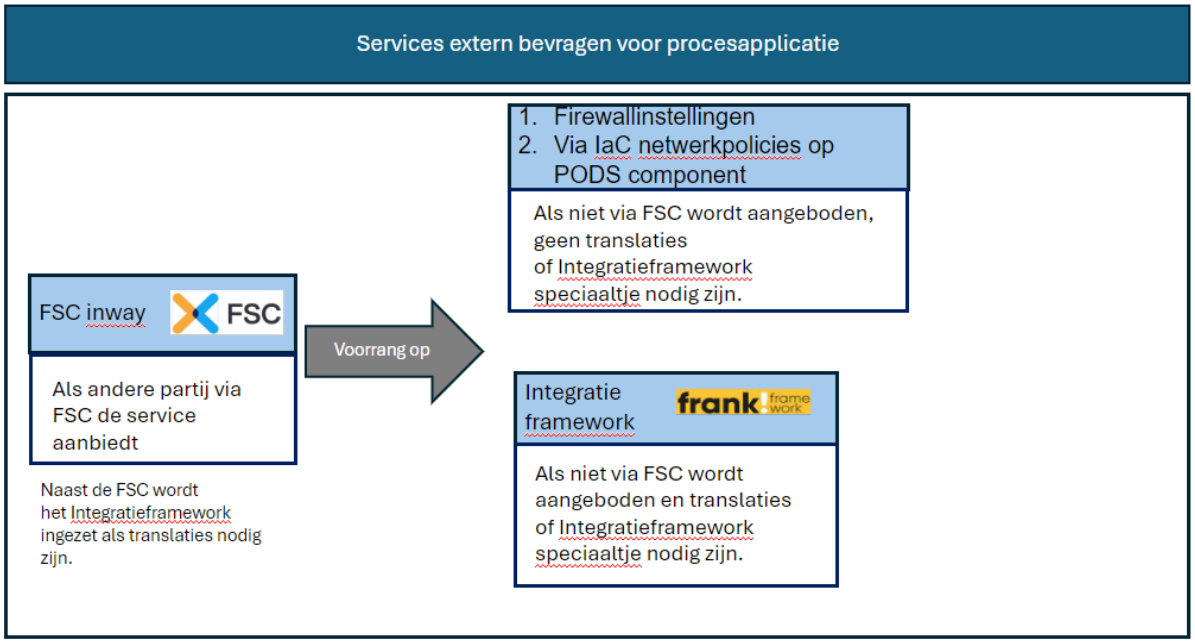
- Closed source is, een closed source deel bevat of een andere beperking heeft.
- Verwerkingsgegevens zelf opslaat en deze niet direct kan doorgeven aan of ophalen van een andere microservice.
- Wel in lijn met de Common Ground door te ontwikkelen is, maar niet wordt doorontwikkeld.

4. Connectiviteit en integratiecomponenten

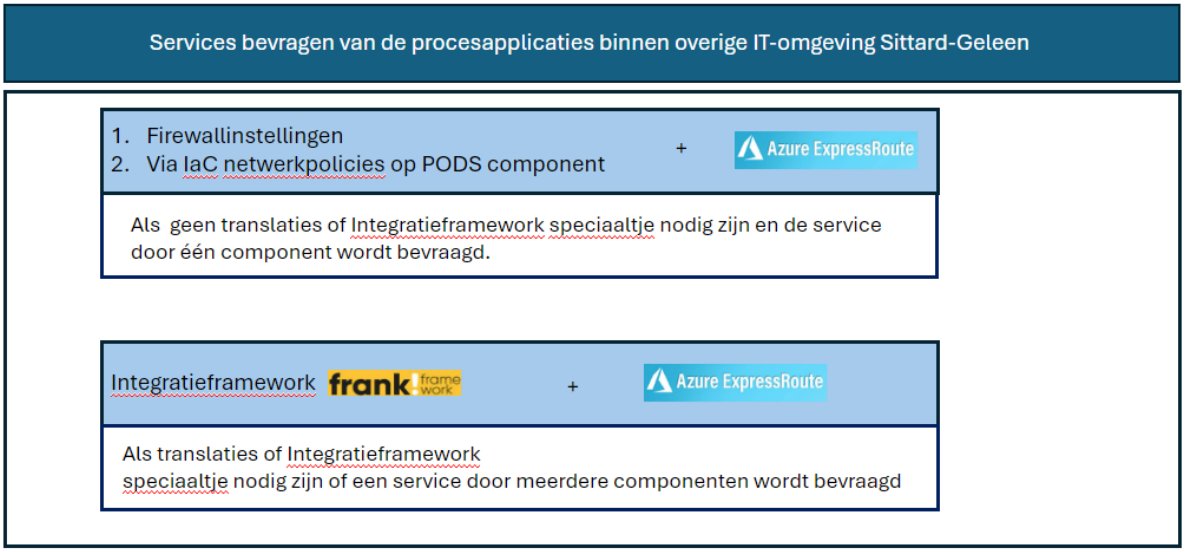
Voor procesondersteunende systemen beschikt de gemeente een gestandaardiseerde aanpak wat betreft het gebruik van applicatie integratievoorzieningen. Deze aanpak omvat richtlijnen omtrent de inzet van verschillende integratiemiddelen, waaronder integratieframework, API-gateway, FSC-NLX en service mesh. Voor BI/data science systemen beschikt de gemeente over een gestandaardiseerde aanpak voor het bepalen van de communicatie tussen databronnen en het datavirtualisatiecomponent, evenals andere datapreparatietools voor BI, GIS, data science & digital twin (denk onder andere aan ETL/ELT). Dit omvat richtlijnen voor wanneer het gebruik van databaseadapters of databaseconnecties geprefereerd wordt boven API's. Voor BI/data science systemen beschikt de gemeente over een gestandaardiseerde aanpak voor het bepalen van de communicatie tussen BI/datascience tooling en datavirtualisatie. Deze aanpak omvat richtlijnen omtrent de inzet van API's, ODBC, JDBC, specifieke toolings connector.

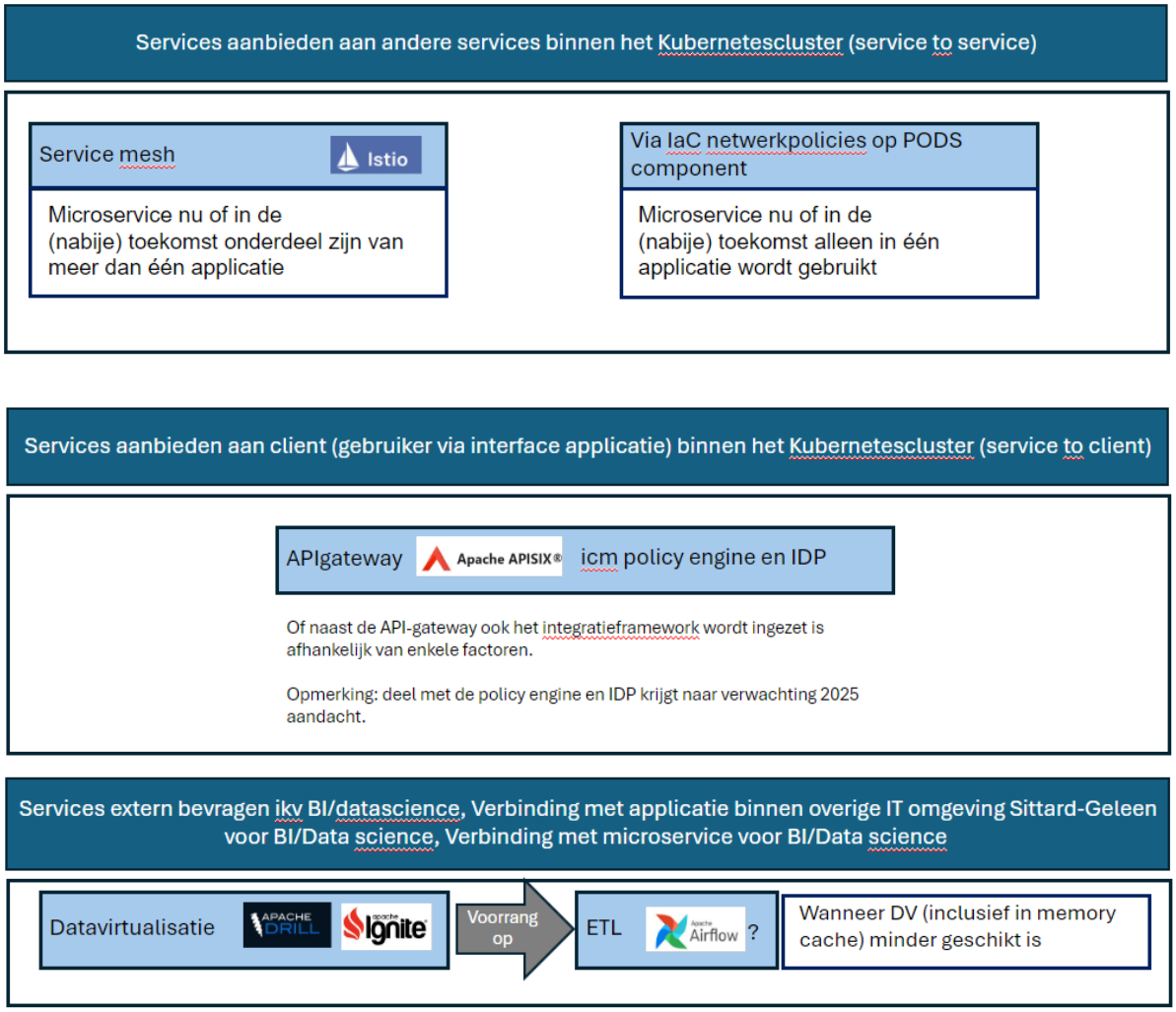
De thema IM-adviseur bepaalt op basis van de architectuur of en wanneer een integratiecomponent in te zetten is. De integratiespecialisten/data engineers stellen de integratievoorzieningen (waar nodig met externe hulp) in. Om een indruk te geven, volgt hieronder enkel het rechtlijnige deel. Het onderstaande is de situatie van Q2 2024, maar is nog aan enige verandering onderhevig. De thema IM-adviseur bekijkt allerlei elementen, die hieronder niet verwoord zijn en die uiteindelijk bepalen of en welk(e) integratiecomponent(en) uiteindelijk in te zetten zijn.




Services extern bevragen voor procesapplicatie
1. Firewallinstellingen
2. Via IaC netwerkpolicies op PODS component
Als niet via FSC wordt aangeboden, geen translaties of Integratieframework speciaaltje nodig zijn.
FSC inway
FSC
Als andere partij via FSC de service aanbiedt
Voorrang op
Integratie framework
frank framework
Als niet via FSC wordt aangeboden en translaties of Integratieframework speciaaltje nodig zijn.
Naast de FSC wordt het Integratieframework ingezet als translaties nodig zijn.


Services aanbieden aan procesapplicaties binnen overige IT-omgeving Sittard-Geleen
API gateway
Apache APISIX®
icm policy engine en IDP
+
Azure ExpressRoute
Het inkomende verkeer loopt via de externe load balancer naar APIsix.
Of voorafgaande aan het aanbieden van de service ook het integratieframework wordt ingezet is afhankelijk van enkele factoren.
Opmerking: deel met de policy engine en IDP krijgt naar verwachting 2025 aandacht.


Services bevragen van de procesapplicaties binnen overige IT-omgeving Sittard-Geleen
1. Firewallinstellingen
2. Via IaC netwerkpolicies op PODS component
+
Azure ExpressRoute
Als geen translaties of Integratieframework speciaaltje nodig zijn en de service door één component wordt bevraagd.
Integratieframework
frank framework
+
Azure ExpressRoute
Als translaties of Integratieframework speciaaltje nodig zijn of een service door meerdere componenten wordt bevraagd



Momenteel heeft de gemeente geen rechtstreekse verbinding met Diginetwerk. De toegang tot Diginetwerk verloopt via Gemnet. Gemnet ontsluit de gemeente richting de Haven omgeving via de express route.

5. Beschikbaar maken applicatie voor gebruikers

De URL van een interactiecomponent komt via de interne ingress controller en interne load balancer beschikbaar voor gebruikers, zodat gebruikers vanuit de omgeving van de gemeente Sittard-Geleen de applicatie kunnen starten. Alleen als de URL van het interactiecomponent via de externe ingress controller en externe load balancer beschikbaar komt, kunnen gebruikers de applicatie starten buiten de omgeving van de gemeente Sittard-Geleen (via het internet).

Vanuit beveiligingsoogpunt heeft dit laatste voor medewerkers van de gemeente niet de voorkeur. De gemeente biedt momenteel (Q2 2024) nog hun applicaties aan via een Citrix omgeving. Voor medewerkers die niet achter een werkplek thuis of het gemeentehuis zitten, maar vooral onderweg zijn is het opstarten van applicaties via de huidige Citrix omgeving niet geschikt voor telefoons en tablets.

Zolang er nog geen nieuwe digitale werkplekomgeving is, bekijkt de gemeente per interactiecomponent voor medewerkers of deze wel of niet via een URL extern benaderbaar moet zijn. De gemeente past sowieso multifactor authenticatie toe. Daarnaast zijn dan nog andere maatregelen nodig zoals ip whitelisting, het enkel beschikbaar maken van de app via een VPN (alleen is die soms traag en te onhandig), via Azure AD applicatie proxy of anderzijds. De gemeente moet dat Q2 2024 nog nader onderzoeken.

6. Welke rechten krijgt u als component dienstverlener

6.1 Deployment orkestratie via gitversiebeheersysteem

U krijgt toegang tot de repositories op het gitversiebeheersysteem voor de applicatie(componenten) die u voor ons beheert.

6.2 Kubernetes API

Geheime sleutels (secrets)

U heeft geen directe toegang tot de opslagplaats van de secrets. Toegang tot de secrets wordt alleen verleend aan de applicatie zelf voor de benodigde functionaliteit. Via sealed secrets maakt u de secrets voor de applicatie aan en bewerkt deze.

Testomgeving

U krijgt lees- en schrijfrechten voor de namespaces binnen de testomgeving van het Kubernetescluster voor de applicatie(componenten) die u voor ons beheert. Portforward-rechten verleend de gemeente op deze omgeving alleen bij legitieme redenen en moet u aanvragen bij het change board van ICT via de daarvoor aangewezen contactpersoon.

Acceptatieomgeving

Alleen voor componenten op laag 1 en 2 van de Common Ground krijgt u schrijfrechten op de acceptatieomgeving. Voor componenten op de andere lagen beschikt u op de acceptatieomgeving alleen over leesrechten. Portforward-rechten verleend de gemeente op deze omgeving alleen bij legitieme redenen en moet u aanvragen bij het change board van ICT via overkoepelend functioneel beheer.

Productieomgeving

Op de productieomgeving krijgt u alleen leesrechten. In noodgevallen krijgt u via een verzoek aan functioneel beheer en uitleg aan technisch applicatiebeheer tijdelijk schrijfrechten op de productieomgeving. Portforward-rechten verleend de gemeente op deze omgeving alleen bij legitieme redenen en moet u aanvragen bij het change board van ICT via overkoepelend functioneel beheer.

Centraal loggingsysteem (Grafana Loki)

U kunt op het centrale loggingsysteem de logging die betrekking heeft op de applicatie(componenten) die u beheert inzien.

7. Wat verwachten wij van een component dienstverlener

Hieronder staan onze verwachtingen van een component dienstverlener per categorie gegroepeerd. Elk item per categorie geeft aan of het een kwaliteitseis aan software betreft, een werkwijzeafspraak of een dienstverleningseis. Bij kwaliteitseisen aan software worden niveaus gehanteerd en bij elke kwaliteitseis staat het bijbehorende niveau vermeld. Dit is gedaan om te voorkomen dat bij een experiment de focus eerst ligt op het voldoen aan de kwaliteitseisen in plaats van te kijken hoe het past. Bovendien, om te voorkomen dat het lang duurt voordat we naar productie kunnen met de software, hoeft de software pas na ingebruikname aan specifieke kwaliteitseisen te voldoen. De volgende niveaus worden gehanteerd:

1. Minimale set aan kwaliteitseisen voor een experiment.
2. Aanvullend op niveau 1, de minimale set aan kwaliteitseisen voor een test om een versie van een (applicatie)component daarna in productie te nemen.
3. Aanvullend op niveau 2, de minimale set aan kwaliteitseisen voor een (applicatie)component dat naar de acceptatieomgeving of productieomgeving wordt gebracht.
4. Aanvullend op niveau 3, een extra set aan kwaliteitseisen waar de gemeente naartoe wil werken met de marktpartijen. Hierover maakt de gemeente afspraken met de dienstverlener.

7.1 Kwalitatief/onderhouden software

Wat	Omschrijving
Kwaliteitseis software *Vanaf test om uiteindelijk in productie te nemen (niveau 2)*	Een open source project maakt regelmatig gebruik van andere open source projecten. Op dat moment is sprake van afhankelijkheden. De gemeente neemt alleen een Common Ground/open source oplossing in gebruik als deze enkel afhankelijkheden kent naar kwalitatieve en onderhouden software: • Een goed onderhouden project heeft regelmatige en consistentie ontwikkelingsactiviteit. Dit betekent dat er nieuwe functies worden toegevoegd, bugs worden opgelost en pull requests worden beoordeeld en samengevoegd. • een goed onderhouden project heeft een actieve community die bijdraagt aan discussies, het indienen van bugrapporten, het maken van pull requests etc. • een goed onderhouden project heeft geplande en stabiele releases met duidelijke releasenotes en update-instructies.
Dienstverleningseis	Op het moment dat een onderliggend project niet meer kwalitatief en onderhouden wordt, kijkt u naar alternatieven en verwerkt u het alternatief. Wanneer dit niet mogelijk is, bespreekt u dit met de gemeente.

7.2 Containers & software image

Wat	Omschrijving
Werkwijze-afspraak	Passend bij de Common Ground architectuur wordt elk component van een laag gehost in een afzonderlijke container, terwijl de applicatie als geheel wordt geleverd als een reeks containers die elk een specifieke laag vertegenwoordigen. Niet Common Ground applicaties worden geleverd als één of een reeks containers.
Kwaliteitseis aan software *Vanaf niveau 2*	Het image van de applicatie(component) in de container moet beschikbaar zijn op een publiek bereikbaar Docker register zoals Docker Hub.
Kwaliteitseis aan software *Vanaf niveau 2*	Containerlabels moeten semantisch versienummering gebruiken. Het semantische versienummer is terug te vinden het Docker register als tag.
Werkwijze-afspraak	Voorlopige versies mogen worden geïmplementeerd met versie + trefwoord (bijv. 1.2.3-snapshot).
Werkwijze-afspraak	De dienstverlener geeft aan wat de vertrouwde locatie is van de docker image.
Kwaliteitseis aan software *Vanaf niveau 4*	Docker images worden ondertekend met een ondertekenvoorziening (bijvoorbeeld Cosign). Op deze wijze kan de gemeente verifiëren of het van de juiste marktpartij komt. Zie https://www.sigstore.dev/ en https://docs.sigstore.dev/signing/quickstart/.
Kwaliteitseis *Vanaf niveau 1*	Er staan geen geheime sleutels (zoals API-keys) in de docker-image.
Dienstverleningseis	De component dienstverlener herkent malifide software binnen de eigen docker images en voert de juiste vervolgacties uit bij het ontdekken hiervan.
Dienstverleningseis	Bij een oplossing die gebruik maakt van andere open source projecten, moet de dienstverlener: -bij updates, bugfixes e.d. van deze andere open source vulnerability management toepassen. -bij gebruik van een docker image van een andere open source project de kwaliteit van het docker image toetsen om te voorkomen dat deze malafide is.
Kwaliteitseis aan software *Vanaf niveau 1*	De Docker image is zo samengesteld dat ze niet onder root draait (er is sprake van non-root container).

Kwaliteitseis aan software *Vanaf niveau 2*	De Docker image is zo samengesteld dat deze met een read-only filesystem draait. Hierdoor kan niemand de inhoud van het bestandssysteem wijzigen nadat de container is gestart. Directories of bestanden die tijdens de uitvoering van de container aanpasbaar moeten blijven, niet zijn opgenomen in het read-only bestandssysteem van de container. In plaats daarvan zijn deze directories of bestanden gekoppeld aan externe volumes of zijn tijdelijke volumes aangevraagd via Kubernetes.
Kwaliteitseis aan closed source software *Mits de gemeente toch besluit deels closed source toe te staan*	Niet open source Docker images staan ook een op Docker register. Ze zijn daar beveiligd met een sleutel/token.

7.3 Veiligheidsmaatregelen leveringsketen

Wat	Omschrijving
Werkwijze afspraak	Elke medewerker van de dienstverlener die toegang krijgt tot het gitversiebeheersysteem en kubernetes api heeft een eigen inlog met wachtwoord en: • maakt verplicht gebruik van multi factor authenticatie. • laat unieke wachtwoorden automatisch genereren via een wachtwoordmanager voor het gitversiebeheersysteem. Het wachtwoord wordt door automatische generatie regelmatig aangepast en gebruikt alleen sterke wachtwoorden. • Het wachtwoord is alleen bij de gebruiker bekend. • Wijzigt onmiddelijke het wachtwoord indien het vermoeden bestaat dat het bekend is geworden aan een derde. • Gebruikt geen wachtwoorden in automatische inlogprocedures (bijvoorbeeld opgeslagen onder een functietoets of in een marcro).
Dienstverleningseis	Een component dienstverlener van een component wat gegevens opslaat & ontsluit, verzorgt het roteren van de wachtwoorden van de databases één keer per jaar (in lijn met beste practices zou het normaal hoger zijn). Wat betreft de wachtwoorden voor de database gelden dezelfde eisen als bij de hiervoor genoemde werkwijze afspraak.
Dienstverleningseis	De gemeente krijgt meldingen van de IBD en NCSC tav mogelijke kwetsbaarheden. U beantwoordt de vragen conform het afgesproken Service Level Agreement.
Dienstverleningseis	Oplossingen afkomstig van de IBD met betrekking tot beveiligingsissues worden 1 op 1 overgenomen.

Dienstverleningseis	Een component dienstverlener ontdekt zelf kwetsbaarheden. De component dienstverlener informeert de gemeente (en een partij die het Haven beheer namens de gemeente doet) van een high impact kwetsbaarheid binnen 8 uur.
Dienstverleningseis	Een component dienstverlener beschikt of één of twee vaste aanspreekpartners die de gemeente buiten kantoortijden kan benaderen op het moment dat er sprake is van urgente beveiligingsissues.
Dienstverleningseis	De gemeente (of een partij die dit namens de gemeente doet) scant op een reguliere basis de containers op kwetsbaarheden met behulp van een Security scanner (Trivy). De scanner geeft tevens aan welke problemen direct oplosbaar zijn door het installeren van een bepaalde softwareversie. U lost deze problemen conform het afgesproken Service Level Agreement op.
Dienstverleningseis	Vanaf het moment dat de applicatie(component) in de acceptatieomgeving staat, scant u minimaal maandelijks geautomatiseerd op kwetsbaarheden en nieuwe versies van bibliotheken en publiceert updates in nieuwe versies van de software. Dit doet u ook voor alle open source software waar de hoofdsoftware gebruik van maakt.

7.4 Schaalbaarheid en starts/stops

Wat	**Omschrijving**
Kwaliteitseis aan software *Vanaf niveau 1*	De applicatie(component) gaat, waar dat passend is, soepel om met het op- en afschalen van containers op basis van de belasting.
Kwaliteitseis aan software *Vanaf niveau 2*	De applicatie(component) moet grotendeels bestand zijn tegen plotselinge stops en starts (bijvoorbeeld als een node uitvalt of bij een container-node migratiegebeurtenis). NB: De gemeente realiseert zich dat niet voor alle situaties mogelijk is.

7.5 Helm charts

Wat	Omschrijving
Kwaliteitseis aan software *Vanaf niveau 2*	Om de applicatie(component) eenvoudig te installeren op een Kubernetescluster, levert u deze met een Helm chart.
Werkwijze-afspraak	De dienstverlener geeft aan wat de vertrouwde locatie is van de helm chart.
Werkwijze-afspraak	We ondersteunen niet het gebruik van applicaties en componenten die worden ingezet door middel van Kubernetes Operators.
Werkwijze-afspraak	Implementaties moeten worden uitgevoerd als een rollende update, tenzij er een ontheffing is verleend. Implementaties en upgrades die database-wijzigingen met zich meebrengen, zijn momenteel vrijgesteld van deze vereiste.
Werkwijze-afspraak	U schrijft netwerkpolicies voor de deployments om netwerksegmentatie op POD-niveau toe te passen en verankerd deze in de helm-chart.
Kwaliteitseis aan software *Vanaf niveau 1*	Er staan geen geheime sleutels (zoals API-keys) in de helm-chart.

7.6 Namespaces

Wat	Omschrijving
Werkwijze afspraak	De gemeente gebruik één enkel k8s-namespace per herkenbaar functioneel component (datavirtualisatie, generiek zaakafhandelcomponent, etc). Componenten moeten worden ingezet in hun eigen namespace in het Kubernetescluster.

7.7 100% Automatisering

Wat	Omschrijving
Werkwijze afspraak	Alle componenten van de applicatie moeten, muv de configuratie, volledig via de helm chart te deployen zijn. In dit geval betekent een volledige implementatie dat de containers correct draaien binnen de K8s-cluster met de juiste implementatieparameters en secrets, verbonden met andere bronnen zoals databases.

7.8 Adressering van componenten

Wat	Omschrijving
Kwaliteitseis aan software *Vanaf niveau 2*	De applicatie(component) kan worden toegewezen aan een "verfraaide" DNS-hostnaam van de volgende vorm: https://mooietoepassingsnaam.gemeente.nl

7.9 Deployment orkestratie (Gitversiebeheersysteem)

Wat	Omschrijving
Werkwijze afspraak	De gemeente gebruikt één of twee repositories per herkenbaar functioneel component (datavirtualisatie, generiek zaakafhandelcomponent, etc). Er bestaat altijd één repository voor de software zelf. Op het moment dat (een deel) van de inrichting (zie bijlage 1 voor uitleg over de term inrichting) via het gitversiebeheersysteem verloopt is dit een aparte repository. De Infrastructur as a Code van de applicatie(component) moeten worden ondergebracht in de eigen repository gekoppeld aan de software zelf. Op het moment dat de dienstverlener naast de software(versie) installatie, configuratie, oplossen van softwarematige problemen ook nog inrichtingswerk verricht via het gitversiebeheersysteem, doet hij dit in de andere repository die bedoeld is voor inrichtingswerkzaamheden.
Werkwijze afspraak	De software wordt altijd eerst op de testomgeving geïnstalleerd en getest. Daarna op de acceptatieomgeving en tot slot naar productie gebracht.
Werkwijze afspraak	In de testomgeving werkt u bij voorkeur met wijzigingsverzoeken. Voor wijzigingen bij een ontwikkeltraject (als deze plaatsvindt in test) is dit niet nodig.
Werkwijze afspraak	In de acceptatie en productomgeving werkt u met wijzigingsverzoeken via het gitversiebeheersysteem. U brengt geen rechtstreekse wijzigingen aan via het gitversiebeheersysteem.
Werkwijze afspraak	Via git dwingt de gemeente vanaf de acceptatieomgeving en productieomgeving reviewflows af. Dat betekent dat altijd een goedkeuring van een andere medewerker werkzaam bij de u nodig is om het wijzigingsverzoek in te dienen.
Werkwijze afspraak	Het semantische versienummer van de software is terug te vinden in het versiebeheersysteem.

7.10 Bij gebruik van een mailservice

De mailservice van een POD verloopt via de centrale mailomgeving van de gemeente Sittard-Geleen.

Wat	Omschrijving
Kwaliteitseis aan software *Vanaf niveau 2*	De applicatie(component) moet standaard e-mailprotocollen ondersteunen zoals SMTPS, SMTP in combinatie met OAuth 2.0 of de Microsoft GraphAPI.

7.11 Communicatie tussen componenten

Standaard staat via netwerk policies ingesteld dat een service standaard geen toegang heeft tot een andere namespace.

Wat	Omschrijving
Werkwijze afspraak	Voorafgaande aan het inrichten van de communicatie stelt de thema IM-adviseur een logisch ontwerp op.
Werkwijze afspraak	Communicatie tussen componenten binnen hetzelfde k8s cluster vindt binnen het cluster plaats.
Kwaliteitseis software	Voor procesondersteunende systemen: De communicatie en datatransport vindt bij uitwisseling tussen componenten op laag 2 (services) met laag 4 (procesinrichting) en 5 (interactie) plaats via API's.
Werkwijze afspraak	Welke services elkaar binnen het cluster mogen benaderen verloopt via netwerk policies. De component dienstverlener stelt via Infrastructure as a Code in welke service zijn service mag benaderen of welke hij wil benaderen, maar kan zichzelf geen toegang verlenen tot een andere service. Een component dienstverlener verleent alleen toegang aan een andere service als de functioneel beheerder van het component daartoe opdracht verleent.
Kwaliteitseis software *Vanaf niveau 2*	De applicatie(component) moet soepel kunnen omgaan met de encryptie en decryptie van communicatie, zonder dat dit de normale werking van de applicatie(component) verstoort.
Werkwijze afspraak	We werken met rate limitting om het aantal verzoeken van één entiteit of IP-adres te beperken om overbelasting en aanvallen zoals DDoS te voorkomen. Bij inzet van de service mesh, ingress controller of API-gateway stellen we rate limiting in op deze tool. Anders wordt in overleg met de gemeente rate limiting op een andere wijze ingesteld.

7.12 Communicatie met andere omgevingen van de gemeente

De gemeente zet tussen het Haven platform en andere omgevingen van de gemeente (zoals on premise) een express route in. De gegevens worden automatisch in transit versleuteld.

Wat	Omschrijving
Werkwijze afspraak	De gemeente wil het minimaal nodige openzetten per vraagstuk. Per vraagstuk is duidelijk wat het bron applicatie(component) is die het initieert, wat het ontvangende applicatie(component) is, welk soort verkeer (poort) voor welke doeleinden. Functioneel beheer haalt bij de component dienstverlener (Haven) en bij functioneel beheer van de applicatie in de andere omgeving de informatie op en dient het verzoek in bij ICT.

7.13 Communicatie met diensten van derden

Wat	Omschrijving
Werkwijze afspraak	Voorafgaande aan het inrichten van de communicatie stelt de thema IM-adviseur een logisch ontwerp op.

7.14 Database migraties

Wat	Omschrijving
Kwaliteitseis aan software *Vanaf niveau 2*	Een applicatie(component) die gegevens opslaat, moet over ingebouwde databasemigratieopties beschikken of het bieden van configuratiescripts voor een DB migratietool zoals Flyway of Liquibase.

7.15 Concurrency/stateless

Wat	Omschrijving
Kwaliteitseis *Vanaf niveau 1*	De software is ontwikkeld voor een container-infrastructuur en kan worden uitgevoerd als een of meerdere *stateless* processen. Alle persistente informatie wordt opgeslagen in externe services (database, cache, queue, bestandsopslag).

Werkwijze afspraak	Bestanden schrijft het applicatie(component) weg naar een objectopslag zoals Azure Blob Storage.
Werkwijze afspraak	Bestanden mag het applicatie(component) wegschrijven naar cloudbestandsshares.
Werkwijze afspraak	Persistente bestanden die gegevens bevatten mogen niet worden geschreven naar lokale opslag op de container.

7.16 Configuratie/secrets

Wat	**Omschrijving**
Kwaliteitseis aan software *Vanaf niveau 3*	De gehele applicatie(configuratie) gebeurt via omgevingsvariabelen.
Kwaliteitseis aan software *Vanaf niveau 3*	Voor de omgevingsvariabelen voor de configuratie bestaat documentatie.
Kwaliteitseis aan software *Vanaf niveau 3*	Het instellen van omgevingsvariabelen gebeurt via config maps in de helm-chart.
Kwaliteitseis aan software *Vanaf niveau 1*	Secrets/gevoelige informatie (zoals wachtwoorden, tokens en andere geheime gegevens) worden weggeschreven naar de K8s secrets store.
Kwaliteitseis aan software *Vanaf niveau 1*	Secrets worden opgehaald en gelezen uit Sealed secrets gedurende de deployment.
Kwaliteitseis aan software *Vanaf niveau 2*	Het is mogelijk om de logging van de applicatie uit te breiden door een debug-omgevingsvariabele in te stellen en de container opnieuw op te starten.

7.17 Versleutelen (encryptie)

Wat	Omschrijving
Kwaliteitseis aan software *Vanaf niveau 1*	De applicatie(component) is beschikbaar middels het unencryptet HTTP-protocol via een poort op de container. De encryptie via SSL certificaten verloopt via de ingress controller of de APIgateway
Kwaliteitseis aan software *Vanaf niveau 3*	De gegevens die een API (laag 2) doorzendt zijn versleuteld.
Werkwijze afspraak	Onze publiek-toegankelijke Ingress controller NGINX voert bij inkomend verkeer SSL-terminatie uit en garandeert een veilige verbinding naar het Kubernetes-cluster. De NGINX Ingress listeners worden gevuld met certificaten die door de gemeente worden verstrekt.
Werkwijze afspraak	Onze publiek-toegankelijke APIgateway APIsix voert bij inkomend verkeer SSL-terminatie uit en garandeert een veilige verbinding naar het Kubernetes-cluster. De APIgateway wordt gevuld met certificaten die door de gemeente worden verstrekt.

7.18 SBOM (Software Bill Of Materials) & IBOM (Interface Bill of Materials)

Wat	Omschrijving
Kwaliteitseis aan software *Vanaf niveau 4* *Als wettelijk verplicht (via Cyber Resilience Act) wordt dan vanaf niveau 3.*	De versie van een applicatie(component) beschikt over een gesigneerde machine leesbare SBOM in een veelgebruikt formaat (SPDX of Cyclon DX) en bevat tenminste de top-level afhankelijkheden van het product. De SBOM is onderdeel van de technische documentatie die de gemeente ontvangt. https://www.ncsc.nl/documenten/publicaties/2023/juli/5/sbom-startersgids

7.19 Probes

Wat	Omschrijving
Kwaliteitseis aan software *Vanaf niveau 2*	De applicatie(component) moeten ervoor zorgen dat probe-endpoints beschikbaar zijn om correcte afhandeling van het starten, draaien en falen van containers mogelijk te maken. Zie Configure Liveness, Readiness and Startup Probes | Kubernetes

7.20 Logging

Wat	Omschrijving
Kwaliteitseis aan software *Vanaf niveau 2*	De applicatie(component) schrijft alle logging weg naar de standard output (STDOUT). Deze logs worden vastgelegd en naar het juiste logging-eindpunt gestuurd.
Kwaliteitseis aan software *Vanaf niveau 2*	Applicatielogging moet configureerbaar zijn via een Loglevel-omgevingsvariabele volgens standaardgebruik voor debug, info, warn, error en fatal logniveaus.
Kwaliteitseis aan software *Vanaf niveau 4*	Applicatielogs moeten worden geschreven in JSON-indeling om correcte parsing in het Logging-systeem mogelijk te maken. (zie https://betterstack.com/community/guides/logging/json-logging/).
Kwaliteitseis aan software *Vanaf niveau 4*	Logregels worden geschreven met tijdstempels in UTC-indeling, zonder tijdzone.

7.21 Metrics

Wat	Omschrijving
Kwaliteitseis aan software Vanaf niveau 3	Een applicatie(component) moet de metrieken verstrekken die relevant zijn voor de betreffende toepassing, zoals: • Aantal transacties • Transactievertraging • Onvolledige transacties • Mislukte transacties • Eventuele andere relevante metrieken per applicatie(component) Metrieken zijn een doorlopende discussie en zullen gedurende de levenscyclus van de toepassing voortdurend worden bijgewerkt en verbeterd. Het volgende artikel biedt een grondige bespreking van het gebruik van metrieken in Kubernetes: https://sysdig.com/blog/golden-signals-kubernetes/
Kwaliteitseis aan software Vanaf niveau 4	Óf de metrieken kunnen worden verzameld door een onafhankelijke centrale monitoringoplossing (bijvoorbeeld Prometheus) om ze in grafiekvorm weer te geven, voor analyse- en waarschuwingsdoeleinden. Óf voor het uitwisselen van metrieken met de centrale monitoringoplossing hanteert u Open Telemetry.

7.22 Resource requirement

Wat	Omschrijving
Werkwijze afspraak	Als onderdeel van het Helm-diagram geeft u een schatting van CPU-/Schijf-/Geheugenvereisten voor een bepaalde basislijn, met de benodigde resources om het component te laten werken. ***Bijvoorbeeld:*** Om component X in staat te stellen Y transacties per minuut te verwerken, raden we aan: • 2000 milliCPU • 1 GB RAM • 3 containerreplica's • Opslagtype Z

7.23 Release notes

Wat	Omschrijving
Kwaliteitseis aan software *Vanaf niveau 2*	Technisch beheer krijgt bij wijzigingen tijdig via release notes de relevante informatie.
Kwaliteitseis aan software *Vanaf niveau 2*	De volgende informatie voor functioneel beheer moet minimaal in de release notes staan: -Beschrijvingen van nieuwe functionaliteiten of verbeteringen -Welke bugs of kwetsbaarheden worden opgelost -Veranderingen die backwards incompatibel zijn -aanpassingen die tot een verandering leiden in de externe communicatie (samenwerking met andere componenten). Dit kan gaan over de ontvangstverwerking als de wijze van versturen. De release notes worden voorafgaande aan de wijziging verstrekt.
Kwaliteitseis aan software *Vanaf niveau 2*	De wijzigingen in de software worden bijgewerkt conform de conventie 'Keep a changelog'. Meer informatie op https://keepachangelog.com/en/1.1.0/

7.24 Documentatie & gegevensoverdracht

Wat	Omschrijving
Dienstverlening eis	De externe services (database, cache, queue en bestandsopslag) zijn beschreven in de software architectuurdocumentatie.
Werkwijze afspraak	Documentatie die specifiek betrekking heeft op de omgeving van de gemeente Sittard-Geleen, is alleen beschikbaar op de daarvoor aangewezen locatie, namelijk intern bij de gemeente.

Werkwijze afspraak	Gegevensoverdracht tussen de component dienstverlener en de gemeente vindt alleen plaats over beveiligde kanalen. “Beveiligde kanalen” worden gedefinieerd door de afdeling Security binnen gemeente Sittard-Geleen en wordt mogelijk gewijzigd naarmate technologie vordert.

7.25 Backward compatibel

Wat	Omschrijving
Kwaliteitseis aan software *Vanaf niveau 2*	Communicatie met andere Common Ground componenten moet bij een update/upgrade/patch/bugfix backward compatibel zijn. Dit om te voorkomen dat: • Na een update/upgrade de dienstverlening of bedrijfsvoering niet meer (naar behoren) werkt. • De gegevenshuishouding van de gemeente in gevaar komt. • Een update langdurig niet kan worden uitgevoerd, omdat één component niet compatibel is met de meest recente standaardversie.