

Applicatie analyse API-gateway

Inhoudsopgave

Samenvatting	3
Huidige situatie	3
Datastromen schematische weergave.....	3
Weergave tbv Spoke inrichting, technische componenten	4
Operationele aspecten.....	4
Beschikbaarheid.....	4
Beheerprocessen (logging, monitoring).....	4
Disaster Recovery inrichting	4
Operating Model.....	5
Ontwikkel Test Acceptatie	5
Gewenste doelarchitectuur en migratie.....	5
User Story.....	6
Definition of Done.....	6

Samenvatting

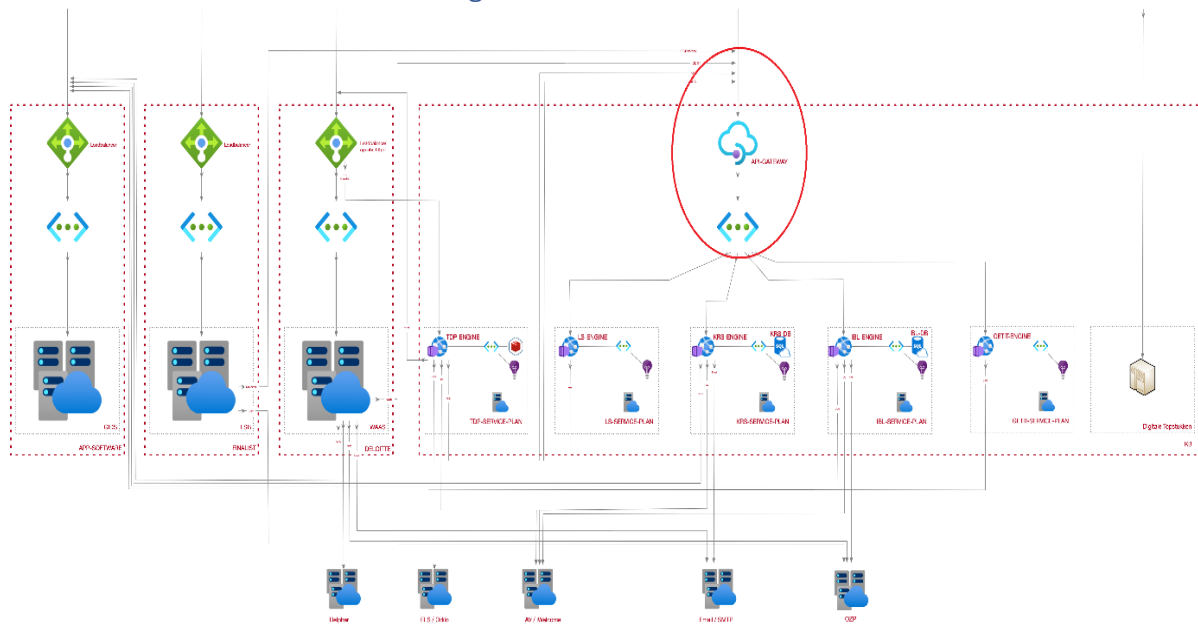
De API gateway is een spil in het Koninklijke Bibliotheek backend netwerk. Deze verzorgt de toegang tot bronsystemen van de KB en de buitenwereld. De API-gateway voegt additionele authenticatie en beveiliging toe aan de bronsystemen.

In de nieuwe situatie, op het Azure platform, wenst de KB het Functioneel Applicatie Beheer te continueren en het technische applicatiebeheer als PaaS dienst van Azure af te nemen.

Huidige situatie

De API gateway wordt momenteel ingezet om (bijna) alle datastromen van en naar de backend applicaties in goed banen te leiden. De gateway gebruikt open standaarden en voegt beveiliging, toegangs policies, IP-filtering en authenticatie toe aan de datastroom.

Datastromen schematische weergave

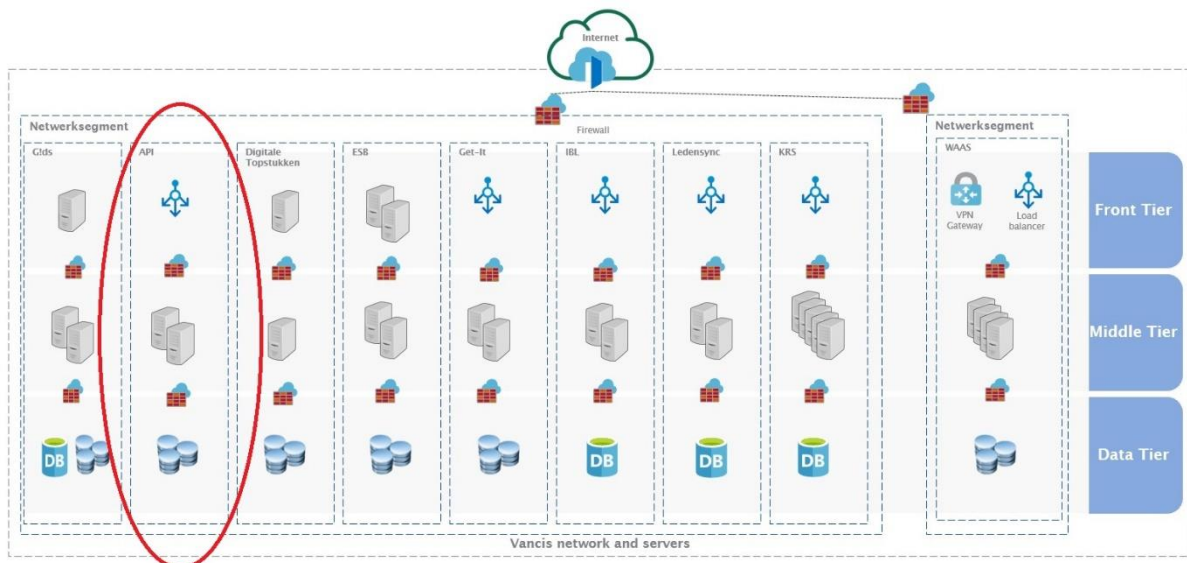


Zoals aangegeven in bovenstaand schema lopen alle datastromen, komende vanaf het internet (bovenzijde) naar de achterliggende producten door de API gateway, met uitzondering van Digitale Topstukken, GIDS, WAAS en ESB.

Alle verbonden applicaties die toegang willen hebben tot de bronsystemen achter de API-gateway authenticeren met behulp van API-keys, bij de migratie naar Azure zullen deze gemigreerd moeten worden vanuit de oude omgeving naar de nieuwe omgeving. Het precieze aantal API-keys is niet bekend, maar ingeschat wordt dat dat getal tussen de 50 en 100 ligt.

Alle lagen, zoals deze schematisch zijn weergegeven, worden gescheiden middels een, door Vancis beheerde, firewall.

Weergave tbv Spoke inrichting, technische componenten



De Front tier wordt door Vancis geleverd. Het is een Shared Service Loadbalancer configuratie die zorg draagt voor de verdere distributie van de API requests.

De Middle tier bestaat uit 2 servers. Hierop is TYK software geïnstalleerd. Deze servers zijn gekoppeld aan een management server die bij TYK in de cloud staat.

Alleen configuratie van de TYK gateway wordt opgeslagen. Deze staat in de VM op het VSAN.

Operationele aspecten

Beschikbaarheid.

De beschikbaarheidseisen aan de applicatie zijn niet heel scherp gedefinieerd. Vancis heeft wel servicelevels, deze gelden aan de onderliggende infrastructuur componenten:

Servers zijn standaard servers, (2 vCPU, 4 GB en 50G OS storage) deze hebben een beschikbaarheidspercentage van 99,8 % (conform Vancis SLA)

In de praktijk heeft zich nog nooit een calamiteit en/of grote verstoring voorgedaan. Voor deze applicatie geldt dan ook dat dit niveau als voldoende worden ervaren.

Beheerprocessen (logging, monitoring)

Logging op de infrastructuur componenten (tot en met OS laag) wordt uitgevoerd door Vancis.

Indien relevant genereren zij ook incidentmeldingen welke worden geregistreerd bij de Service Desk van de KB. De KB gebruikt op dit moment hiervoor Topdesk.

Daarnaast monitort de Service Desk van de KB ook de systemen, op ongeveer dezelfde parameters (disk, CPU, processen etc.).

Er is een rudimentair SIEM proces, maar nog geen volledige security implementatie. Er vindt geen proactieve Informatie Beveiliging plaats.

Disaster Recovery inrichting

Er zijn geen RTO's en RPO's voor de API gateway gedefinieerd. Deze worden echter wel verwacht in de Azure omgeving.

De servers worden geleverd op een virtuele omgeving in een Active-Passive cluster configuratie en middels snapshots continue geborgd. Vancis heeft hier geen contractuele KPI's op afgesloten.

Alle overige zaken die bij DR horen (bijvoorbeeld gebruikersoefeningen, of applicatie beschikbaarheidsgarantie) zijn niet ingericht.

Operating Model

Het Functioneel Beheer van de applicatie wordt door de KB uitgevoerd. Voor het technisch beheer van de API Gateway wordt TYK gebruikt, met deze kanttekening dat de primaire verantwoordelijkheid van het technische beheer bij de KB ligt. Het beheer van de OS laag wordt door Vancis uitgevoerd.

Ontwikkel Test Acceptatie

Naast de hierboven beschreven productie omgeving kent de applicatie een Ontwikkel-, Test- en Acceptatieomgeving welke gebruikt worden voor implementatie van nieuwe API functionaliteit. De Test en Ontwikkel omgeving zijn gecombineerd en verschilt qua dimensionering van de Acceptatie- en Productieomgeving (minder servers met minder capaciteit). De functionele eis aan de Acceptatieomgeving is dat deze representatief voor de productie omgeving is.

OTA en P omgevingen zijn ook gescheiden middels een, door Vancis beheerde, firewall.

Er is geen standaard test- en acceptatieproces geïdentificeerd. Hiermee bedoelen we een standaardproces van wie welke aanpassing mag testen en goedkeuren voordat deze naar de volgende acceptatiestap gaat. Dit proces wordt onder begeleiding van de KB aangestuurd.

Gewenste doelarchitectuur en migratie

- De KB vraagt van de leverancier een oplossing die gebaseerd is op de API technologie zoals deze in Azure als PaaS dienst ("Azure API Management") wordt geleverd.
- Het gebruik van een developer portal moet ook worden gerealiseerd. De developer portal moet aansluiten op de gebruikersadministratie van de KB, voorzien in documentatie voor de afnemers van de API gateway, versiebeheer en in het algemeen automatiseren van de deployment van de code.
- De KB vraagt tevens van de nieuwe leverancier de migratie van de bestaande, (in TYK geconfigureerde) API's naar de nieuwe Azure oplossing te realiseren.
- Omdat de API gateway de spil in het web is van alle backend applicaties gaan bijna alle datastromen van aangesloten partijen over deze API gateway. Hiervoor zijn alle aangesloten systemen voorzien van een API-key voor authenticatie. Het gewenste migratie scenario is dan ook gebaseerd op geen verstoring voor alle aangesloten partijen. Hiervoor moeten de API-keys (zoals deze nu in TYK staan) in de nieuwe Azure API gateway worden opgenomen.

Profiel

De KB is primair op zoek naar een leverancier die helder communiceert wat er nodig is om succesvol in de Cloud te landen, hierbij proactief adviseert op gebied van best practises, en de KB actief ondersteunt in de implementatie van Azure API management en het verankeren hiervan in de organisatie. De KB verwacht dan ook van de leverancier dat deze de KB ook wijst op haar eigen taken en verantwoordelijkheden, op gebied van organisatie inrichting of anderszins, terwijl zij volledig invulling geeft aan de aan haar gestelde eisen.

Uiteraard heeft de nieuwe leverancier de mogelijkheid om met een alternatief migratie scenario te komen.

User Story

In mijn rol als **API ontwikkelaar voor de API gateway** verwacht ik dat de Cloud diensten mij gaat ontzorgen in de ontwikkeling en deployment, door automatiseren of toepassen van best practices, van de uitrol van nieuwe API's zonder afbreuk te doen aan de beveiligingseisen die de Koninklijke Bibliotheek aan mij oplegt. In mijn rol als **API ontwikkelaar van backend systemen** verwacht ik dat de Cloud diensten (API-management) het mogelijk dat los van de applicatie, zelfstandig nieuwe API's kunnen toevoegen en/of te beheren vanuit 'Infrastructure as code' (bij voorkeur Terraform).

In mijn rol als **Productowner API management platform** verwacht ik dat Azure API management wordt ingericht volgens de best practices. Tevens verwacht ik dat de governance rondom het bouwen, aansluiten en beheren van API's goed wordt ingericht, zodat de API's van de KB goed gedocumenteerd ontsloten kunnen worden voor netwerkpartners. Als hiervoor organisatieaanpassingen nodig zijn, verwacht ik dat de leverancier dit signaleert en de KB hierbij begeleidt.

Definition of Done

De generieke eisen gesteld aan deze applicatie en de migratie naar de Cloud zijn de volgende:

- De applicatie levert in de nieuwe, gemigreerde, situatie dezelfde functionaliteiten als in dit document beschreven.
- Beschikbaarheid, monitoring en rapportage functionaliteiten voor deze applicatie zijn in de nieuwe, gemigreerde, situatie minimaal van hetzelfde niveau als voor de migratie.
- Logging en monitoring voor deze applicatie levert, na migratie, direct inzicht in de gemaakte kosten voor deze applicatie.
- Alle betrokken partijen, benodigd voor het goed functioneren van de applicatie, zijn bekend en op de hoogte van elkaars rol en verantwoordelijkheden.
- De rol en verantwoordelijkheden van alle betrokken partijen, benodigd voor het goed functioneren van de applicatie, zijn beschreven en overeengekomen.
- De gemigreerde applicatie is op zijn minst getest en geaccepteerd door de leverancier (Technische Applicatie Test), in dit geval de Koninklijke Bibliotheek.
- De gemigreerde applicatie is op zijn minst getest en geaccepteerd door de gebruiker (Functionele Applicatie Test), nog nader te bepalen door de product owner van de API gateway.