

**connectiviteit   
IBIS-GeoMatch**

|  |  |
| --- | --- |
| **Datum** | 21-02-2024 |
| **Status** | Concept |
| **Versie** | 1.0 |
| **Auteur(s)** | Baars, Paul |
| **Project** |  |

# Inhoudsopgave

[Inhoudsopgave 2](#_Toc159419687)

[1. Inleiding 3](#_Toc159419688)

[2. Berichtstromen 4](#_Toc159419689)

[2.1 In scope 4](#_Toc159419690)

[2.2 Out-of-scope 5](#_Toc159419691)

[2.3 Typering van de berichtstromen 5](#_Toc159419692)

[3. Authenticatie/Authorisatie 6](#_Toc159419693)

[4. Netwerk koppeling 7](#_Toc159419694)

[Bijlage: sFTP verbinding voor monitoring data 9](#_Toc159419695)

# Inleiding

Dit document is niet bedoeld als HLD of LLD. Doel van dit document is alle informatie te verzamelen die nodig is om de connectiviteit met COA en partner applicaties in te richten. In de meeste gevallen vindt de connectie plaats via Azure API Management. Dat betekent dat er connectie van en naar de zogenaamde Trusted Cloud nodig is. Het tot stand brengen van de connectiviteit is een belangrijke voorwaarde voor het realiseren van integratie oplossingen door het cloud integratie team.

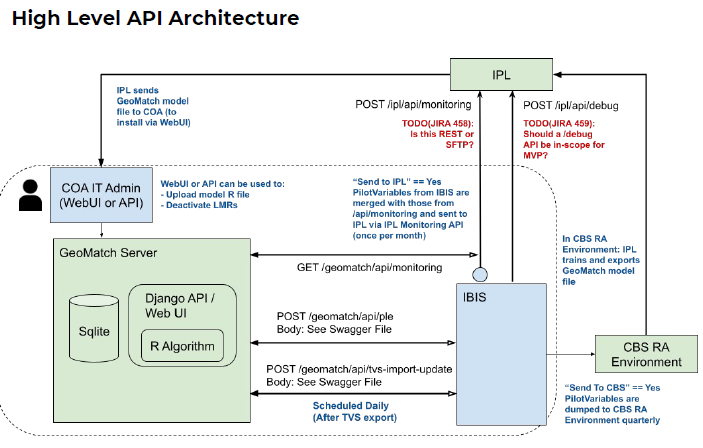
De GeoMatch koppeling wordt door IBIS gebruikt voor regio advies ten aanzien van het toewijzen van asielzoekers aan gemeenten.

**Er moet een netwerk koppeling worden opgezet voor Productie en Niet-Productie (A).**

# Berichtstromen

Swagger definitie Geomatch API: geomatch-server-0.1.2-20240112.yml

## In scope



Gegevensstromen tussen IBIS en GeoMatch:

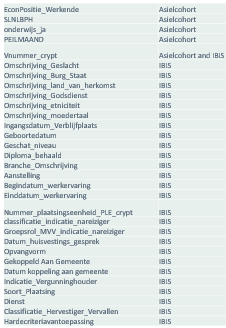
* POST /geomatch/api/ple
  + Request GeoMatch advice for a PLE given a list of individuals in that PLE
* GET /geomatch/api/ple/{ple\_id}/advice/
  + Retrieve advice for given PLE
* POST /geomatch/tvs-import-update.
  + Update GeoMatch with (1) taakstelling from TVS and (2) linkings made since the last TVS import.

Monitoring gegevens van IBIS naar IPL (zie bijlage):

* Csv bestand via sFTP. sFTP heeft de voorkeur van IPL (mail 12-1-2024). Het is wel de vraag of dit een geautomatiseerde aanlevering wordt. Frequentie: maandelijks.
* De monitoring data die IBIS verstuurt bevatten monitoring data van IBIS en GeoMatch. De monitoring data van GeoMatch kunnen ook oopgehaald worden via de API:

GET /geomatch/api/monitoring/

In het PSA Kansrijke koppelingen zijn de monitoring data gespecificeerd die nu bekend zijn. De lijst van monitoring data is nog in bewerking, maar geeft een indruk van de monitoring data die IPL graag wil ontvangen. IPL gebruikt de monitoring data om te kunnen bepalen of de regio advies oplossing en het ML algoritme goed functioneren.



## Out-of-scope

* ML-model vanuit IPL importeren in GeoMatch. Dit is nu een handmatig proces dat een keer per jaar plaatsvindt.
  + /geomatch/api/import/model/
    - Uploads an Rdata model trained in the CBS RA environment.
* De gegevens naar CBS zijn tot nu toe (2 of 3 keer) handmatig geupload via het portaal van CBS. In de toekomst moet het elke kwartaal. Deze koppeling heeft niet de eerste prio.
* Koppeling PLE aan gemeente in TVS. Geomatch advies kan aangeleverd worden vanuit IBIS aan TVS, maar hoeft niet gevolgd te worden.

## Typering van de berichtstromen

* Er is geen sprake van grote berichten.
* Er zijn geen grote pieken in het berichtenverkeer.
* Er worden geen bijlagen meegestuurd.

# Authenticatie/Authorisatie

Er wordt voor authenticatie/authorisatie gebruik gemaakt van de OAuth2 client credentials flow.

Het OAuth2 token kan worden opgehaald door aanroep van het token endpoint van GeoMatch:

<https://geomatch.coa.eminjenv.nl/api/oauth/token>

Informatie over dit token endpoint is onderin het service contract geomatch-server-0.1.2-20240112.yml te vinden:

securitySchemes:

oauth2:

type: oauth2

flows:

clientCredentials:

tokenUrl: /api/oauth/token/

scopes:

read: Read scope

write: Write scope

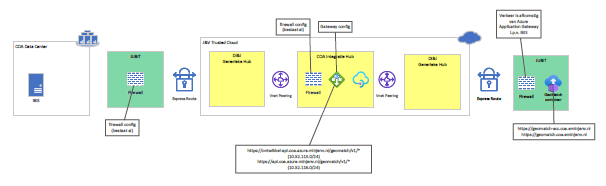
Voor de Acceptatie omgeving kunnen de onderstaande gegevens worden gebruikt:

* grant\_type=client\_credentials
* scope=read+write
* ClientId: IBIS
* Clientsecret: [doorgegeven aan Michel]

ClientId en ClientSecret zijn opgenomen in de environment variabelen van de GeoMatch container image. Solvinity kan de info voor Acceptatie en Productie aanleveren.

# Netwerk koppeling

* IBIS wordt gehost in het COA Data Center
* GeoMatch maakt gebruik van een Docker container. Container image wordt aangeleverd door IPL (gelieerd aan Stanford University). De GeoMatch container wordt gehost in JUBIT.



Voor deze koppeling wordt gebruik gemaakt van de JUBIT Reverse Proxy (Solvinity).

Hostnames, URLs en firewall rules zijn al eerder gespecificeerd in Technisch ontwerp Geomatch 231017.pdf. De firewall rules zullen moeten worden aangepast omdat de verbinding via Azure API Management moet lopen en niet rechtstreeks van IBIS naar GeoMatch.

Hieronder staan de aangepaste firewall rules die met Solvinity zijn afgestemd:

PRD

1. COA IBIS (10.51.109.136) à COA application gateway (10.52.116.0/24) – URL [https://api.coa.azure.minjenv.nl/geomatch/v1/\*](https://api.coa.azure.minjenv.nl/geomatch/v1/*) - vrijwel zeker dat dit pad technisch al mogelijk/gebouwd is.
2. COA application gateway (10.52.116.0/24) à Geomatch vm (10.48.197.10 = vip op Geomatch load balancer) – URL <https://geomatch.coa.eminjenv.nl>
3. Geomatch vm (10.68.197.234) à COA application gateway (10.52.116.0/24) – URL [https://api.coa.azure.minjenv.nl/geomatch/v1/\*](https://api.coa.azure.minjenv.nl/geomatch/v1/*)
4. COA application gateway (10.52.116.0/24) à COA IBIS (10.52.191.13 = vip op de COA load balancer) – URL <https://ibis.coa.minjenv.nl>

ACC

1. COA IBIS (10.52.48.97) à COA application gateway (10.52.113.0/24) – URL [https://ontwikkel-api.coa.azure.minjenv.nl/geomatch/v1/\*](https://ontwikkel-api.coa.azure.minjenv.nl/geomatch/v1/*) - vrijwel zeker dat dit pad technisch al mogelijk/gebouwd is.
2. COA application gateway (10.52.113.0/24) à Gemoatch vm (10.48.197.11 = vip op Geomatch load balancer) - <https://geomatch-acc.coa.eminjenv.nl>
3. Geomatch vm (10.68.198.26) à COA application gateway (10.52.113.0/24) – URL [https://ontwikkel-api.coa.azure.minjenv.nl/geomatch/v1/\*](https://ontwikkel-api.coa.azure.minjenv.nl/geomatch/v1/*)
4. COA application gateway (10.52.113.0/24) à COA IBIS (10.52.213.13 = vip op de COA load balancer) – URL <https://ibis-acc.coa.minjenv.nl>

Opmerking: Waarschijnlijk zijn er hierboven te veel firewall rules gespecificeerd. In deze usecase wordt het verkeer altijd geïnitieerd vanuit IBIS en nooit vanuit GeoMatch. In geval van een request-response patroon (geinitieerd vanuit IBIS) verloopt de communicatie via dezelfde sessie. Om die reden zijn alleen de firewall rules 1 en 2 nodig.

In principe moet COA ook de firewall configureren in Azure en DCA (naar IBIS). Omdat het verkeer vanuit IBIS ook al nodig was voor MyCOA, is geen actie nodig. De firewall rules bestaan al.

Outbound verkeer vanuit APIM verloopt net als inbound verkeer via het Application Gateway subnet, omdat je een routeerbaar subnet nodig hebt.

# Bijlage: sFTP verbinding voor monitoring data

In order to provide monthly monitoring data, we need a solution to communicate from COA to IPL.

Previously, this was Biztalk, but SFTP would provide a longer term solution that can integrate with

existing AWS infrastructure easily. This document outlines a basic solution.

IPL could set up an SFTP server using AWS Transfer Family. This supports Secure Shell (SSH) File

Transfer Protocol (SFTP) Version 3. The server is exposed over the public internet via a Server Name /

Port shared with COA. It would be located in an EU region, and would be dedicated entirely to

receiving COA monitoring data.

Uploads to this IPL SFTP server are stored in AWS S3 before being processed and cleaned for the

purposes of monitoring.

Authentication

IPL could support SFTP authentication via SSH key pairs, passcode or both. Please see the BizTalk

send adapter documentation for an example client setup.

[Preferred] Asymmetric SSH Key Pairs

For this method, COA would generate a key pair (by using *ssh-keygen* for example) and send the

GeoMatch team the public key, which can then be installed on the IPL SFTP server.

This corresponds to “Client Authentication Mode” of “PublicKeyAuthentication” in a Biztalk client.

AWS Transfer Family accepts RSA, ECDSA, and ED25519 keys.

Symmetric Passcode

In a less ideal scenario, IPL and COA could share a well-known passcode that would be used to

authenticate requests to the SFTP server.

This corresponds to “Client Authentication Mode” of “Password” in a Biztalk client.

Other Optional Security Features

Fingerprinting

The IPL SFTP server fingerprint will be communicated to COA IT to verify they are contacting the

correct IPL server.

This corresponds to “SSH Server Host Key Finger Print” in the Biztalk client setup.

COA Well-Known IP Range

If COA’s cloud environment has a well-known IP range from which it connects to other machines, we

can configure the IPL server to only accept connections from this range (via an AWS security group).

Key Rotation

If required, we can schedule the update of the COA public key / passcode installed on the IPL SFTP

server. We are open to other methods of rotating the public key / passcode as required.

(Michael Maurer, Stanford University, 21-02-2024)