smart applications. for business.

enigmatry

Applicatie architectuur

trAPP

Het Waterschapshuis

November 2020

Versie 1.1

Enigmatry BV
Stationsplein 45, Unit C8.070
3013 AK Rotterdam

Postbus 84
3000 AB Rotterdam

t 010-2409929
info@enigmatry.com
www.enigmatry.com

KVK 27265056
BTW NL819566263B01
IBAN NL73RABO035823324

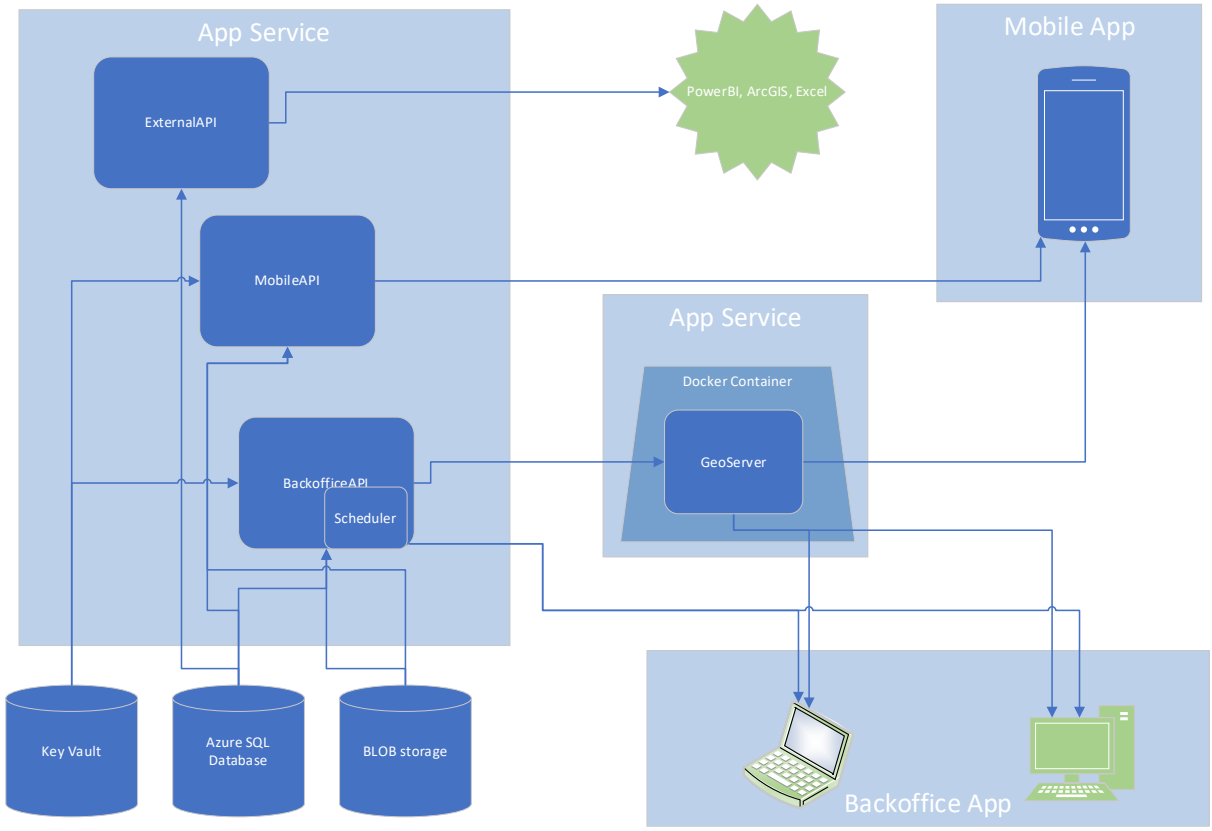
Inhoudsopgave

1 Architectuur

In dit hoofdstuk wordt een overzicht gegeven van de componenten op hoog niveau die deel uitmaken van de trAPP-applicatie.

1.1 Overzichtsschema

De volgende afbeelding toont een overzicht van componenten die deel uitmaken van de trAPP-applicatie.



1.2 Componentenoverzicht

Alle componenten worden geïmplementeerd in Azure. Azure is een cloudplatform van Microsoft dat allerlei diensten levert voor de moderne applicatieontwikkeling.

Component	Omschrijving
Azure SQL Database	Applicatiegegevens worden bewaard in een Azure SQL Database. Azure SQL Database is een relationele database die tabellen, views, stored procedures en functions bevat. De databasestructuur wordt gegenereerd op basis van code met behulp van Entity Framework Code First Migrations. Zie voor een gedetailleerde beschrijving het “trAPP Datamodel en Database.docx”
Azure BLOB storage	Het Azure Storage-account wordt gebruikt om grote bestanden op te slaan in een BLOB-opslag. trAPP-applicaties slaan daar afbeeldingen van waarnemingen en offline OSM-kaarten op.
Azure Key Vault	Azure Key Vault wordt gebruikt om cryptografische sleutels en andere secrets te beveiligen die worden gebruikt door cloud-apps en -services. De trAPP-applicatie slaat account credentials op die nodig zijn voor de Backoffice en Mobile API.
Backoffice API	De API wordt uitgevoerd in een Azure App Service. De API bevat modellen, controllers en services voor de backoffice-applicatie. Er wordt een reeks restful API's ontsloten die door de Backoffice-app worden gebruikt om gegevens van en naar de database te lezen en te schrijven. Het gedetailleerde overzicht en de beschrijving van de services is online gedocumenteerd in de OpenAPI-documentatie. (https://trapp.hetwaterschapshuis.nl/api) Binnen de Backoffice API draait ook een scheduler. De scheduler is verantwoordelijk voor het uitvoeren van periodieke taken zoals het verzenden van overzichtsmail, het vernieuwen van rapportgegevens, het annonimiseren van gebruikers, enz.
Mobile API	De API wordt uitgevoerd in een Azure App Service. De API bevat modellen, controllers en services voor de mobiele applicatie. Er wordt een reeks restful API's ontsloten die door de mobiele app worden gebruikt om gegevens van en naar de database te lezen en te schrijven. Het gedetailleerde overzicht en de beschrijving van de diensten is online gedocumenteerd in de OpenAPI-documentatie (https://trapp-mob.hetwaterschapshuis.nl/api)
External API	De API wordt uitgevoerd in een Azure App Service. De API bevat modellen, controllers en services voor externe applicaties. Het ontsluit een aantal restful API’s en een OData-interface. De OData-interface wordt gebruikt door externe toepassingen zoals PowerBI, Excel of ArcGIS om gegevens uit de trAPP-database te lezen. Deze toepassingen maken geen deel uit van de trAPP-oplossing.

	Het gedetailleerde overzicht en de beschrijving van de services is online gedocumenteerd in de OpenAPI-documentatie. (https://trapp-api.hetwaterschapshuis.nl)
GeoServer	GeoServer is een open source-applicatie voor het ontsluiten van geografische entiteiten. Het wordt uitgevoerd als een Docker-container in een Azure App Service. Het biedt WMS- en WFS-services voor gebruik in de Backoffice en Mobile APP met content en overlay-lagen.
Backoffice App	De Backoffice APP is een applicatie die in een browser op een desktop of laptop draait. De app bestaat uit een single page application (SPA).
Mobile App	De mobiele app is een applicatie die op een mobiel apparaat draait. Het is ontwikkeld met behulp van het Ionic-framework voor zowel de iOS- als Android-platforms.

1.3 Software bibliotheken

Hier is een overzicht van de belangrijkste bibliotheken die in de trAPP-componenten worden gebruikt.

APIs:

- AspNetCore.HealthChecks
- Autofac
- AutoMapper
- Azure.Storage.Blobs
- BeatPulse
- DevExtreme.AspNet.Data
- FakeItEasy
- FluentAssertions
- FluentValidation
- MailKit
- MediatR
- Microsoft.ApplicationInsights
- Microsoft.AspNetCore
- Microsoft.Azure.Services.AppAuthentication
- Microsoft.EntityFrameworkCore
- Newtonsoft.Json
- Npgsql.NetTopologySuite
- NSwag.AspNetCore
- NUnit
- Polly
- ProjNET4GeoAPI
- Quartz
- Refit

- Serilog

Backoffice Single Page Application:

- angular
- angular/material
- azure/msal-browser
- devextreme
- ol
- proj4

Mobile:

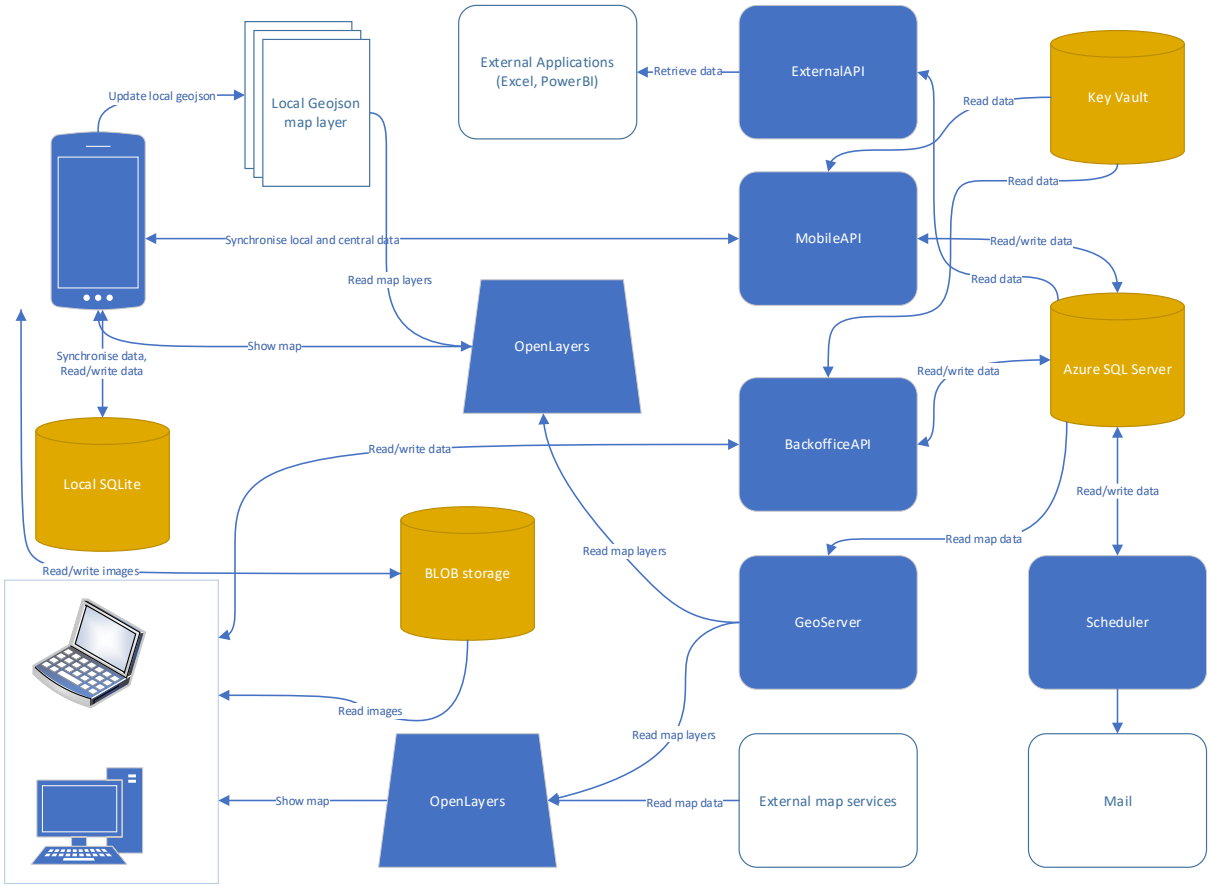
- angular
- ionic-native
- cordova
- ol
- proj4

2 Interactie

In dit hoofdstuk wordt de interactie tussen trAPP-componenten geïllustreerd.

2.1 Interactie diagram

De volgende afbeelding toont de interactiestromen tussen de componenten van de trAPP-toepassing.



2.2 Interactie

In de volgende tabel wordt alleen de afwijkende of specifieke interactie beschreven die van toepassing is op de trAPP-applicatie. De gebruikelijke interacties die in een moderne Single Page Application worden gedefinieerd, worden niet verder uitgewerkt.

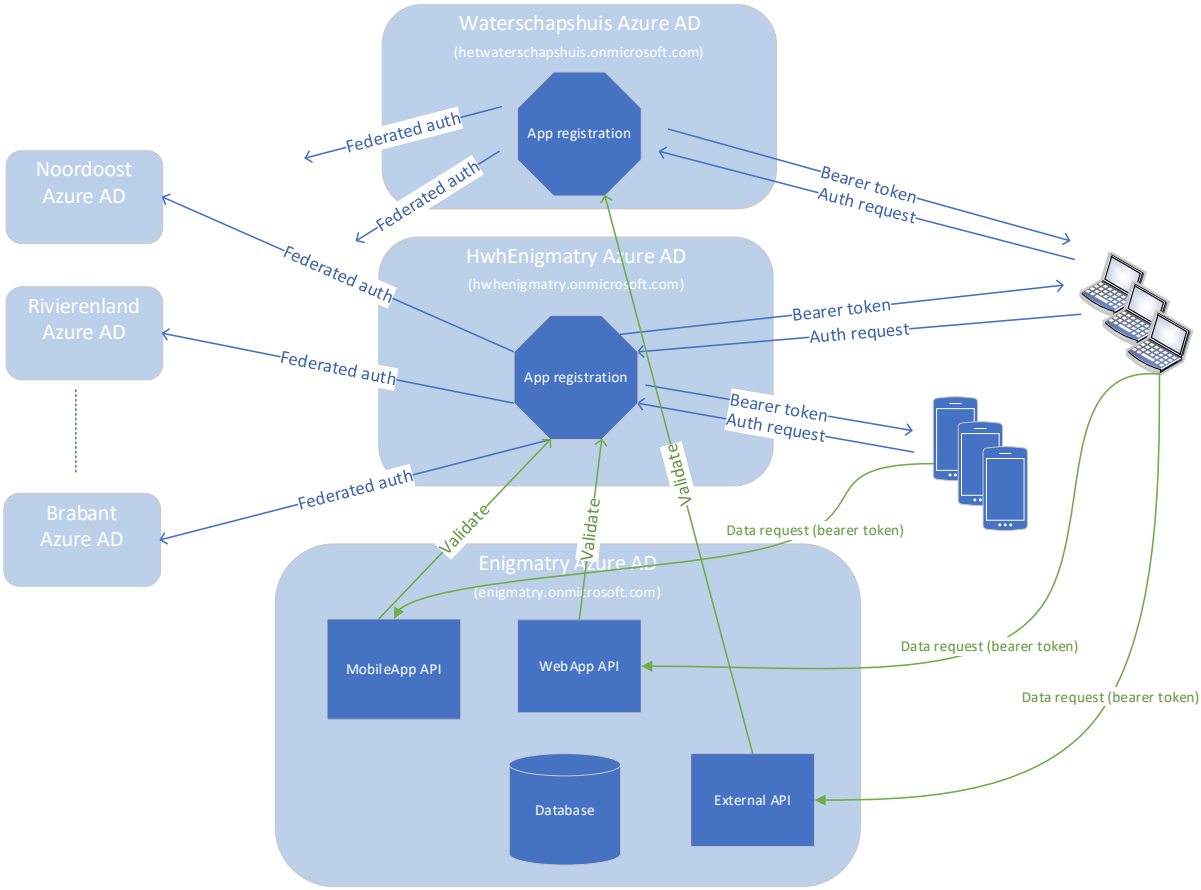
Component	Omschrijving
GeoServer	GeoServer is een op Java gebaseerde softwareserver waarmee gebruikers geospatial gegevens kunnen bekijken en bewerken. Door gebruik te maken van open standaarden die uiteengezet zijn door het Open Geospatial Consortium (OGC), biedt GeoServer grote flexibiliteit bij het maken van kaarten en het delen van gegevens. (http://geoserver.org/) GeoServer vormt het hart van de trAPP-applicatie. Het is verantwoordelijk voor het aanbieden van kaartinhoud aan de mobiele telefoon en aan de backoffice-applicatie. Alle gegevens worden opgehaald uit de Azure SQL-database. Beschikbare functies bij de inhoud zijn: TrapDetails, TrackingLines, TrackingLinesByTrapper, TrackingLinesByUser en Observations. Beschikbare functies met overlay zijn: SubAreas, CatchAreas, Rayons, WaterAuthorities, Organisations, Provinces, SubAreaHourSquares en HourSquares. Beschikbare functies voor rapportagedoeleinden zijn: SubAreaCatches, CatchAreaCatches, SubAreaHourSquareCatches, OrganizationCatches, WaterAuthorityCatches, RayonCatches en HeatMapOfCatches. De achterliggende stored procedures zijn beschreven in het “trAPP Datamodel en Database.docx”
OpenLayers	OpenLayers is een open source-bibliotheek, waarmee u eenvoudig een dynamische kaart in elke webpagina kunt plaatsen. Het kan kaarttegels, vectorgegevens en markeringen weergeven die vanuit elke bron zijn geladen. (https://openlayers.org/) Als zodanig dient het als een brug tussen de GeoServer en de trAPP-applicatie.
External Map Services	De trAPP-applicatie haalt achtergrondkaarten op uit externe bronnen. Door gebruik te maken van externe bronnen zijn de kaarten altijd up-to-date. De belangrijkste bron is de pdok.nl-site waar de volgende drie achtergrondkaarten worden onderhouden: • Top10NL • OpenTopo • Luchtfoto, inclusief straatnamen Voor de offline kaartfunctionaliteit gebruikt trAPP Open Street Maps.
Local GeoJson layer	De trAPP-applicatie kan ook offline functioneren. Dit betekent dat er geen actieve internetverbinding nodig is om de trAPP-applicatie in het veld te kunnen gebruiken. De Open Street Map (OSM) wordt offline gedownload vanuit Azure BLOB-opslag.

	Inhoud en overlay-lagen worden gedownload van de GeoServer.
Local SQL Lite	De mobiele applicatie bevat een SQL lite-database om te dienen als cachemechanisme wanneer de verbinding tijdelijk niet beschikbaar is. Trackinginformatie wordt lokaal opgeslagen en periodiek (momenteel 2 min.) Gesynchroniseerd met de backoffice om prestatieredenen. Verder dient het voor het cachen van wijzigingen, die gemaakt worden terwijl de applicatie in offline modus is (het bewerken van traps, catches en observaties).
BLOB storage	De Azure BLOB-opslagcontainer maakt deel uit van de Azure Cloud-omgeving. Het dient als opslag voor afbeeldingen van waarnemingen van de trapper. Bovendien wordt het gebruikt als opslag voor de OSM-kaart.
Scheduler	De Scheduler wordt uitgevoerd binnen de Backoffice API in dezelfde Azure App Service. Het is verantwoordelijk voor het uitvoeren van periodieke taken die als CRON-taken zijn gepland. Deze taken omvatten het verzenden van overzichtsmail, het vernieuwen van rapportgegevens, het annonimiseren van gebruikers, het aanmaken van volgregels en het voltooien van tijdregistraties. Voor het versturen van mail wordt als mailserver Office365 gebruikt. Voor de overzichtmail wordt als afzender trapp@hetwaterschapshuis.nl gebruikt.
Key Vault	De trAPP-applicatie slaat account credentials op die nodig zijn voor de Backoffice en Mobile API.

3 Authenticatie

Voor authenticatie gebruikt trAPP een Azure Active Directory (AD). Alle gebruikersaccounts worden beheerd door de waterschapsorganisaties in hun eigen Azure AD-tenant. trAPP autoriseert alleen toegang tot de applicatie en wijst een rol toe aan een gebruiker.

3.1 Azure AD-authenticatie schema



De mobiele en desktoptoepassing vraagt om AD-authenticatie van de HWH Enigmatry AD met behulp van het standaard OAuth 2.0-protocol. HWH Enigmatry bundelt deze verzoeken aan de volgende AD van de verschillende waterschappen. De response is een geldige of ongeldige authenticatie. Bij een geldige authenticatie ontvangen we een bearer-token.

Azure herkent de aanvragende gebruiker op basis van zijn UPN. Het authenticatieverzoek wordt verder gefedereerd met de corresponderende Azure AD van een waterschapsorganisatie.

Na een succesvolle validatie worden de data en andere koppelingen direct afgehandeld door de WebApp API of MobileApp API. In de API-aanroep sturen we een bearer-token om een geautoriseerd verzoek te identificeren. Bearer-tokens worden gevalideerd op basis van de HWH Enigmatry Azure AD. WebApp API, MobileApp API en de database worden gehost in de Azure-omgeving van Enigmatry.

3.2 App registraties

Het is noodzakelijk om de trAPP applicatiecomponenten te registreren in de Azure AD's van de waterschappen. Zodat elke individuele organisatie toegang kan verlenen tot de trAPP-applicatie. Dit is een workflow die is geïnstrueerd door Azure.

De Backoffice-API en mobiele API-app-registraties worden gedefinieerd in de trAPP Azure AD beheerd door Enigmatry (hwhenigmatry.onmicrosoft.com). De External API app-registratie wordt echter beheerd in de HWH Azure AD (hetwaterschapshuis.onmicrosoft.com). Dit komt door het feit dat de API beschikbaar is op het hetwaterschapshuis.nl domein en de OData interface het niet mogelijk maakt om de app te registreren in andere domeinen (noch hwhenigmatry.onmicrosoft.com noch enigmatry.onmicrosoft.com).

4 Back-up

De volgende storage componenten worden geback-upt:

- Azure SQL database: hiervoor wordt de standaard point-in-time-restore van Azure SQL Databases voor gebruikt
- Blob storage: hiervoor wordt de standaard retentie faciliteit en soft delete van Azure Blob storage gebruikt
- Key Vault: hiervoor wordt de soft delete en purge protection van Azure gebruikt.

De Local SQLLite database op de mobiele devices wordt niet geback-upt, maar deze bevat enkel caching data.