



Voorgestelde besluiten

Technische inrichting Data.OD

Voor de realisatie van Data.OD moeten enkele fundamentele keuzes worden gemaakt over de technische inrichting van het platform. Deze keuzes bepalen hoe het platform wordt gebouwd, beveiligd, beheerd en later kan doorgroeien. Het projectteam heeft verschillende alternatieven onderzocht en deze verwoord in het document 'Voorstel technische inrichting basisomgeving en data-architectuur Data.OD'. Dit document is technisch diepgaand.

In voorliggende notitie zijn de essentiële keuzes uit dit document samengevat en beschreven. De stuurgroep kan zich daarmee richten op de inhoudelijke afwegingen in plaats van de onderliggende techniek. We vragen de Stuurgroep een besluit te nemen over onderstaande 7 punten.

Voorgestelde besluiten

Besluit 1. Kies voor een PaaS-architectuur op basis van Azure Database Services

Voorgesteld besluit

Data.OD wordt ingericht met Azure Database Services (PaaS) en niet met Microsoft Fabric.

Toelichting

Deze oplossing:

- sluit het beste aan op de huidige werkwijze met EasyMorph;
- biedt betere prestaties en lagere kosten;
- geeft meer controle over beveiliging;
- voorkomt afhankelijkheid van één leverancier;
- blijft geschikt om later alsnog door te groeien naar Microsoft Fabric.

Hiermee ontstaat een toekomstvaste basis zonder onnodige investeringen.

Besluit 2. Richt het platform in met een Data Lake en een centrale SQL-database

Voorgesteld besluit

Data wordt opgeslagen in twee lagen:

- een Data Lake voor onbewerkte brongegevens;
- een centrale Azure SQL-database voor verwerkte gegevens.

Toelichting

Hierdoor blijven brongegevens altijd beschikbaar, kunnen gegevens efficiënt worden verwerkt en kunnen meerdere omgevingsdiensten dezelfde gegevens veilig gebruiken. \

Besluit 3. Plaats Data.OD in een eigen Azure Subscription binnen de ODDV-tenant

Voorgesteld besluit

Data.OD krijgt een volledig eigen Azure Subscription binnen de bestaande Azure-tenant van ODDV.

Toelichting

Hiermee:

- blijven kosten volledig afzonderlijk inzichtelijk;
- zijn data en beheer logisch gescheiden van andere systemen;
- kan gebruik worden gemaakt van de bestaande beheerorganisatie;
- blijft verhuizing naar een andere organisatie later mogelijk.

Dit combineert snelheid met een goede mate van onafhankelijkheid.

Besluit 4. Gebruik Microsoft Entra ID met gastaccounts

Voorgesteld besluit

Gebruikers van deelnemende omgevingsdiensten krijgen toegang via Microsoft Entra ID met gastaccounts.

Toelichting

Deze oplossing:

- voorkomt extra licentiekosten;
- maakt nieuwe deelnemers eenvoudig aan te sluiten;
- houdt het beheer centraal;
- biedt voldoende beveiliging.

Een federatieve inrichting is onderzocht maar levert meer complexiteit en hogere kosten op.

Besluit 5. Kies voor centrale opslag met veilige gegevensscheiding

Voorgesteld besluit

Alle deelnemende omgevingsdiensten maken gebruik van één centrale database, waarbij iedere organisatie uitsluitend haar eigen gegevens kan raadplegen.

Toelichting

De gegevens worden logisch gescheiden door autorisaties. Hierdoor ontstaat één gezamenlijke voorziening zonder dat organisaties elkaars gegevens kunnen inzien. Dit maakt uitbreiding naar meerdere omgevingsdiensten eenvoudig.

Besluit 6. Richt de omgeving veilig in volgens de voorgestelde beveiligingsarchitectuur

Voorgesteld besluit

De Azure-omgeving wordt ingericht met:

- Multifactor Authenticatie;
- Microsoft Entra ID;
- beveiligde beheerverbindingen;
- firewall- en IP-beveiliging;
- versleutelde opslag;
- autorisaties op basis van rollen.

Toelichting

Hiermee voldoet het platform aan de gangbare beveiligingseisen en ontstaat een goede basis voor verdere groei naar een volledig Zero Trust-model.

Besluit 7. Start pragmatisch zonder volledige OTAP-omgeving

Voorgesteld besluit

Voor de MVP wordt nog geen volledige OTAP-straat ingericht.

Toelichting

Ontwikkel-, test- en productieomgevingen worden logisch gescheiden binnen dezelfde Azure-omgeving. Dit verlaagt de kosten en versnelt de realisatie. Wanneer het platform verder groeit, kan alsnog een volledige OTAP-omgeving worden ingericht.

Financiële consequenties

De gekozen inrichting leidt tot een overzichtelijke Azure-omgeving met transparante kosten. De grootste kostenposten zijn de ETL-server, de SQL-database en de beveiligingscomponenten. Door gebruik te maken van serverless-technologie en een eigen subscription blijven de kosten beheersbaar, passend binnen de opgestelde begroting in het projectplan en volledig toewijsbaar aan Data.OD.

Gevraagd besluit

De stuurgroep wordt gevraagd in te stemmen met:

1. de keuze voor een PaaS-gebaseerde architectuur op basis van Azure Database Services;
2. de inrichting met Azure Data Lake Storage en Azure SQL;
3. de inrichting van een eigen Azure Subscription binnen de ODDV-tenant;
4. het gebruik van Microsoft Entra ID met gastaccounts voor toegang;
5. een centrale dataopslag met logische scheiding van gegevens per omgevingsdienst;
6. de voorgestelde beveiligings- en toegangsarchitectuur;
7. een gefaseerde ontwikkeling waarbij OTAP en verdere netwerkisolatie in een latere fase worden gerealiseerd.