15-6-2017

Installatiehandleiding Database

Omgevingswet

Database Factory 5

Database Factory 5

Inhoudsopgave

1. Inleiding

Deze installatiehandleiding beschrijft wat er nodig is om de aangeleverde Omgevingswet database te installeren.

2. Benodigdheden

Voordat de database geïnstalleerd kan worden, moet er eerst worden voldaan aan enkele randvoorwaarden. Een server waarop een MSSQL database draait en de bestanden aangeleverd door DatabaseFactory5.

3. Installatiestappen

Na het opzetten van de server kunnen de database scripts worden uitgevoerd. Allereerst moet het DDL bestand worden uitgevoerd. Hiermee worden de tabellen gecreëerd. Vervolgens moeten de beperkingsregels op de database van kracht worden. Dit kan gedaan worden door middel van de bestanden in de map “constraints”. Daarna is het verstandig om alle testscripts uit te voeren, zodat automatisch gecontroleerd kan worden of alles goed is gegaan. Als alles correct is verlopen, is er nu een lege database.

Na het opzetten van de database kan het handig zijn om alvast enige data toe te voegen. Denk bijvoorbeeld aan verschillende soorten vergunningstypen. Ook is het van belang dat de configuratiegegevens van de database worden aangepast in de beheer- en webapplicatie. Het ip-adres/hostname, poortnummer, database gebruiker en het daarbij behorende wachtwoord moeten allemaal naar alle waarschijnlijkheid aangepast worden.

Met betrekking tot het ip-adres zijn er in principe twee opties. Het is mogelijk om de database (tijdelijk) lokaal te hosten, dan zou het ip-adres er als volgt uit kunnen zien:

- Localhost;
- 127.0.0.1;
- Of, indien de database op een lokaal netwerk draait, 192.168.x.x.

Hiervoor hoeven geen poorten open te worden gezet. Aanbevolen is om ervoor te kiezen de database op het lokale netwerk te draaien. Hierdoor kunnen aanvallers van buitenaf er alleen in als ze ook toegang hebben tot ditzelfde lokale netwerk.

Voor de webserver zou het geen probleem moeten vormen als de database slechts vanuit het lokale netwerk beschikbaar is, mits de webserver zelf op hetzelfde lokale netwerk draait. Voor de beheerapplicatie zou dit wel een probleem kunnen vormen, zeker als beheerders vanuit thuis zouden willen werken, maar om veiligheidsredenen wordt dit afgeraden.

Er kan ook voor gekozen worden om de database poort wél open te zetten. In MSSQL is dit standaard poort 1433. Dit heeft als gevolg dat iedereen waar dan ook ter wereld verbinding kan maken met de database, mits ze over de juiste inloggegevens beschikken. Dit maakt dat er een reële kans is op bruteforcing en phishing aanvallen.

Tenslotte nog de database gebruiker. Het wordt ten strengste afgeraden om de beheer- en webapplicatie zodanig te configureren dat deze gebruikmaken van de door de database standaard aangemaakte accounts. Denk hierbij aan bijvoorbeeld “root” of “sa”. De voorkeur gaat over het algemeen uit naar een nieuw aangemaakt account, die een sterk wachtwoord heeft en zo min mogelijk privileges.

Mocht er worden besloten om de database poort open te zetten, dan wordt ook ten strengste aangeraden om alle accounts te beschermen met een sterk wachtwoord.