Deployment voor MB Ontdekt

# Inleiding

MB Ontdekt moet uiteindelijk openbaar gehost worden, zodat deze gebruikt kan worden door het brede publiek. Van de opdrachtgevers mag dit pas als de applicatie bepaalde functies heeft, namelijk:

* Een heatmap naar wens
* Een account-functionaliteit waarbij meetstationhouders de optie hebben hun meetstation te verbergen op de kaart.

Momenteel voldoet de applicatie alleen deels aan de eerste eis en mag deze dus nog niet officieel gehost worden, echter is er nog steeds een wens om de applicatie ergens online te hebben staan. Daarom is het besluit genomen om de applicatie te hosten in een develop-omgeving.

Er is gekozen om het te hosten via een [DMZ fhict account](https://portal.fhict.nl/Studentenplein/ISSD/SitePages/Netlab.aspx). Dit DMZ-account is gekoppeld aan een publiek IP-adres, in dit geval is dat: <http://145.220.74.224/>.

Om het project verder op weg te helpen wordt nu beschreven hoe de app staat gehost en wat de complicaties hiervan zijn.

# Hosting

Allereerst bevat het DMZ-account 2 VM’s:

1. **pfSense router –** dit is wat het netwerk scheidt van de boze buitenwereld, en dus de beveiliging van het netwerk regelt. Wanneer onzeker hoe alles werkt, is het advies om hier van de instellingen af te blijven!

2. **Ubuntu workstation** – dit is een Ubuntu (Linux) desktop omgeving, waarop de daadwerkelijke servers virtueel gehost worden.

Op het moment is de router zo ingesteld dat alle bezoekers die het publieke IP-adres in de browser bezoeken de front-end van de applicatie te zien krijgen. Dit gebeurt via poort 80, de standaard poort voor HTTP-verkeer, welke door de router doorgestuurd wordt (portforwarding/NAT) naar het interne netwerk, specifiek poort 80 van het Ubuntu workstation.

Op poort 80 van het Ubuntu workstation draait de webserver in een docker container. Ook draait op deze machine de API-server (poort 8082) en de MariaDB database (poort 3306), dit is via docker-compose gedaan. Deze zijn nu nog niet beschikbaar voor browser access buiten de VM-omgeving.

# Complicaties

Hiervoor werd al even kort gezegd dat de back-end niet bereikbaar is buiten de VM-omgeving. Dit komt omdat alleen poort 80 doorgestuurd wordt naar het interne netwerk. Om poort 8082 open te stellen naar de buitenwereld lijkt ons geen goed plan. Dit maakt de api-server namelijk kwetsbaar voor cyberaanvallen. Men kan zich afvragen wat de kans is dat dit daadwerkelijk uitgevoerd wordt, maar de keuze is gemaakt om dit niet te riskeren.

Het advies is tweedelig:

1. Beveilig de api-server met access-tokens (JWT’s) of een andere vorm van authenticatie. Zo kunnen kwetsbare endpoints niet bereikt worden zonder de juiste autorisatie. Mocht dit doel bereikt worden kan op de pfSense router ingelogd worden om zo een nieuwe portforwarding in te stellen van poort 8082 op het DMZ IP-adres naar poort 8082 van het Ubuntu workstation.

2. Op dit moment draait de front-end in NGINX als webserver, maar NGINX kan ook ingesteld worden als ‘reverse-proxy’. Dit wil zeggen dat NGINX, endpoints van de api-server die op poort 80 van het DMZ IP-adres bereikt willen worden kan doorsturen naar een andere poort, specifiek poort 8082 van het Ubuntu workstation, want hier draait de api-server op.

# Network Diagram

