Systeem en Netwerkbeheer

Thomas Van Hecke

December 20, 2025

Contents

1 Inleiding

Een bedrijf wil elk kwartaal de verkoopsresultaten opslaan en vergelijken met vorige kwartalen. De IT-dienst stelt voor om een computer aan te schaffen die deze resultaten kan opslaan en verwerken. Het bedrijf is nog in volle ontwikkeling waardoor ze de middelen niet hebben om dure hardware-infrastructuur aan te kopen en te onderhouden. Hoe kan er nu een computer aangeschaft worden zonder grote instapkosten en onderhoudt? Om dit probleem op te lossen kan de men gebruik maken van de Cloud.

2 De Cloud

De cloud is een verzameling van computermiddelen [10]. Enerzijds wordt er opslagruimte aangeboden zoals OneDrive van Microsoft, anderzijds worden er ook diensten aangeboden zoals extra rekenkracht en databases. Om deze computermiddelen aan te vragen bestaat er een online platform zoals het Google Cloud Platform 1.

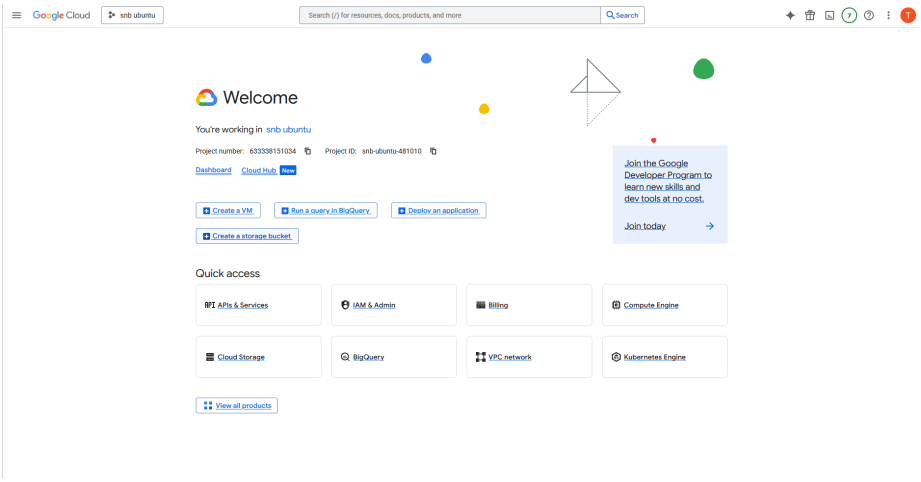


Figure 1: Google Cloud Platform

Computers in de cloud worden virtuele machines genoemd omdat deze machines in de realiteit niet echt bestaan, maar geëmuleerd worden in software d.m.v. een hypervisor. Een hypervisor is een besturingssysteem dat virtuele machines beheert. Zoals op de ontvangstpagina in 1 te zien is, kan er een virtuele machine worden aangemaakt met de (create a VM)-knop.

3 Virtuele Machine: Configuratie

3.1 Compute Engine API

Om bekend te geraken met het aanvragen van een VM, wordt de tutorial doorlopen die het platform aanbiedt. Om via het platform middelen aan te vragen, uit te lezen, bij te werken of te verwijderen moet de Compute Engine API geactiveerd worden. Deze API laat toe dat het platform geldige API calls maakt naar de corresponderende endpoints, deze API is noodzakelijk omdat het alle functionaliteit voorziet voor het aanmaken en opstarten van VM's [4]. Wanneer alle VM's ook wel instances (entiteiten) genoemd, moeten opgelijst worden zal het platform een API methode zoals: `compute.v1.instances.aggregatedList` gebruiken [5]. Deze methode maakt onderliggend een HTTP GET request naar `https://compute.googleapis.com/compute/v1/projects/{project}/aggregated/instances`. Dit is maar één method, in realiteit worden een tientallen gemaakt.

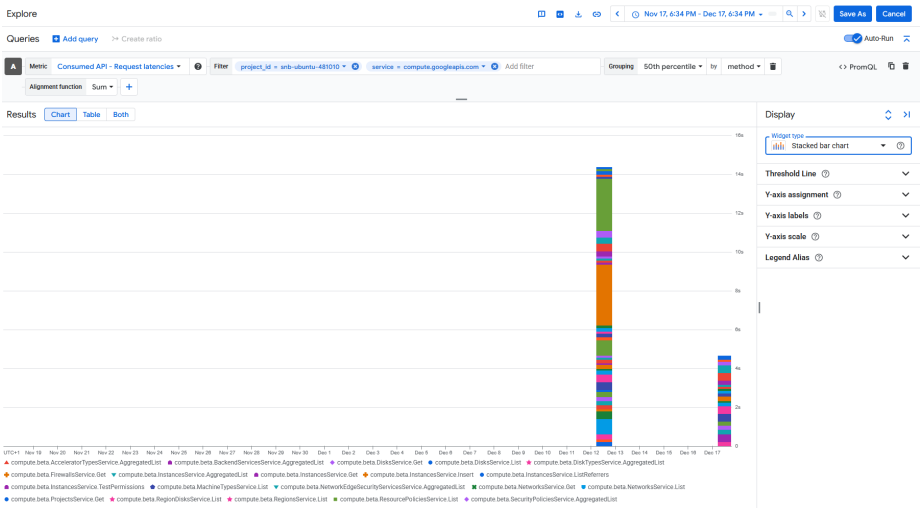


Figure 2: Compute Engine API Bar Chart

Elke kleur in 2 stelt een andere methode voor.

3.2 Machine Configuratie

Om een VM gestructureerd op te bouwen biedt het Google Cloud Platform verschillende secties.

De eerste sectie is de configuratie 3 van de machine. Deze sectie omvat:

1. Een naam geven aan de VM
2. Een regio kiezen voor de resources

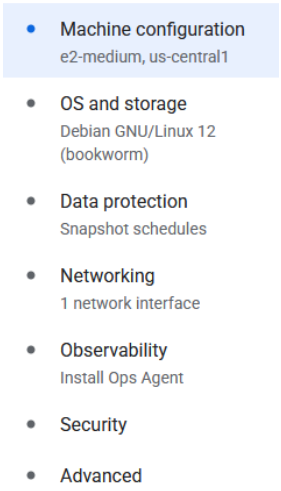


Figure 3: VM Different Sections

3. Een zone in de gekozen regio kiezen
4. Een machine series kiezen
5. Een machine type kiezen
6. Een provisie model kiezen

De regio is een individuele geografische plaats waar de resources plaatsvinden bv. europa-west1 [8]. Een regio bestaat uit verschillende zones zoals bv. europa-west1-a. Sommige resources zijn zone specifiek zoals compute engine instances (bv. VM's) andere resources zijn regio specifiek bv. statische externe IP-adressen. Een zone bepaalt dus welke computing resources er ter beschikking zijn en waar de data opgeslagen wordt [8]. Om redundantie op te bouwen kan het dus interessant zijn om meerdere VM's te verspreiden over verschillende regio's en zones. Om latency te verminderen kan het interessant zijn om de primaire regio (belangrijkste regio) zo dicht mogelijk bij de doelgroep te plaatsen. In het voorbeeld van het bedrijf kan het dus interessant zijn om twee VM's aan te maken in twee verschillende regio's en om deze regio's geografische zo dicht mogelijk te kiezen bij de locatie van het bedrijf. Een machine series zijn machine types met soortgelijke CPU's en geheugen mogelijkheden [7]. Er bestaan verschillende groepen van series bv. deze voor algemeen gebruik. Elke series biedt een bereik met virtuele CPU's (vCPU's) en een bereik van geheugen die beschikbaar is binnen die serie. Elke series is bedoeld voor een bepaald gebruik, enerzijds zijn er series bedoeld voor een gebalanceerde prijs en performantie, anderzijds zijn er die bedoeld zijn voor continue performantie. Voor het bedrijf kan het dus interessant zijn om voor een algemene series bv. een N-series te

kiezen die een balans aanbiedt tussen kost en performantie. Een bepaalde series biedt verschillende machine types aan, elk met een aantal vCPU's en een hoeveelheid geheugen. Een type kan ook zelf samengesteld worden. Een provisie model is een model dat bepaalt wanneer de virtuele machine moet stoppen met draaien.

3.3 Besturingssyteem & Opslag

Deze sectie omvat:

1. De keuze van het besturingssysteem
2. De versie van het gekozen besturingssysteem
3. De keuze van de boot disk type
4. De keuze van de opslaggrootte

Tot op heden bestaan er drie veel gebruikte besturingssystemen elk met hun voor- en nadelen. Deze drie zijn Windows OS, Mac OS en alle Linux gebaseerde OS'es. Voor de keuze van het besturingssysteem heeft de tutorial gekozen voor Ubuntu 24.04 LTS, dit is een linux gebaseerd OS. Elk besturingssysteem heeft verschillende versies, nieuwere versies zijn bedoeld om problemen van oudere versies op te lossen. Desondanks kunnen ze ook nieuwe kwetsbaarheden introduceren. Een boot disk type is het type van het opslagmedium waarop het besturingssysteem staat van de virtuele machine. Tijdens het doorlopen van de tutorial kun je kiezen uit vier boot disk types: balanced persistent disk, extreme persistent disk, SSD persistent disk en standard persistent disk. Een persistent disk type is een network storage device, dit is geen fysiek storage medium dat verbonden is met de host waarop de instance draait. Elk type gebruikt een Solid State Drive (SSD) als opslagmedium, uitgezonderd het standard persistent type wat een Hard Disk Drive (HDD) gebruikt [9]. SSD's en HDD's hebben beide hun voor- en nadelen. In het algemeen is een SSD beter voor performantie en een HDD beter voor kostenreductie [15]. In het voorbeeld van het bedrijf zou een SSD persistent disk geschikt zijn omdat het een goede balans levert tussen performantie en kost. Een opslag medium heeft ook een bepaalde grootte bv. 512 GB. In de cloud worden VM's aangemaakt met cloud image's die geschreven worden naar de boot disk van die VM. Volgens de officiële Ubuntu website is er een minimum van 4 GB nodig voor cloud images, maar het minimum op het platform is 10 GB. Voor het doorlopen van de tutorial is 10 GB voldoende. Om een besturingssysteem te kiezen is het ook mogelijk om zelfgemaakte images, snapshots of bestaande disks te gebruiken.

3.4 Data bescherming

Deze sectie omvat:

1. De keuze van het type back-up

2. De keuze van het type replicatie

Om de data van de VM te beschermen biedt Google drie types back-ups: een back-up plan, snapshot schedules en no back-ups. Een back-up plan kopieert de data van de volledige VM, dit kan meerdere disks omvatten. Een snapshot kopieert de data van één enkele disk [14]. Naast back-ups biedt Google ook drie types van replicatie aan: synchrone replicatie, asynchrone replicatie en excludeer boot disk van data replicatie. Synchrone replicatie houdt in dat er één regio boot disk bestaat die wordt gerepliceerd naar twee zones. Asynchrone replicatie houdt in dat data van één regio disk gekopieerd wordt naar een andere regio disk. Het excluderen van boot disk data replicatie houdt in dat enkel data gerepliceerd wordt van non-boot disks. Dit zijn disks waarop geen besturingssysteem staat. In het voorbeeld van het bedrijf zou het interessant zijn twee disks te gebruiken. Enerzijds een boot disk anderzijds een disk bedoeld om data op te slaan. Op die manier kan de boot disk al geëxcludeerd worden voor data replicatie en dan hangt het af van hoe belangrijk de data is op de non-boot disk.

3.5 Netwerkbeer

Deze sectie omvat:

1. Het instellen van de firewall
2. Het kiezen van een netwerk tag
3. Het kiezen van een hostname
4. Het toestaan van IP-forwarding
5. Het toestaan van een verhoogde bandbreedte
6. Het kiezen van de netwerk interfaces

De firewall bepaalt welk type inkomend netwerkverkeer toegelaten wordt en welke geweigerd wordt. Het platform biedt drie mogelijkheden: HTTP verkeer toelaten, HTTPS verkeer toelaten en load balancer health checks. Om de tutorial te volgen selecteer je enkel HTTP verkeer toelaten. Een netwerk tag is een string (naam) die een VM toegewezen krijgt, daarna is het mogelijk om firewall regels op te leggen op een tag. Elke VM met een tag krijgt dan de firewall regels van die tag [3]. Dit kan interessant zijn om repetitieve taken te vermijden en grotere groepen VM's te beheren. Een hostname is fully qualified DNS-naam, ook wel fully qualified domain name (FQDN) genoemd, die je aan de VM kan geven. Een hostname bestaat uit minimaal twee labels die samengevoegd zijn met puntjes bv. bedrijf.com is een FQDN [6]. Zelfgekozen hostname's kunnen handig zijn om conventies aan te houden of indien er applicaties een specifieke hostname verwachten. In beide gevallen (wel/geen hostname) zal Google Cloud automatisch een interne DNS-naam genereren voor de VM, alsook een interne DNS A record. Om een bruikbare hostname aan te maken moet er zelf nog

een interne DNS-record aangemaakt worden voor de correcte zone, dit kan met Cloud DNS. IP-forwarding is het proces waarbij een device netwerk pakketjes op één interface ontvangt en op een andere interface plaatst richting de bestemming van dat pakketje. Een voorbeeld van zo'n device is een router. Een verhoogde bandbreedte zorgt voor een verhoogde throughput wat voor een snellere communicatie zorgt. De meeste huishoudens hebben een bandbreedte van 150 Mbps downlink en 30 Mbps uplink. De Compute Engine's verhoogde bandbreedte biedt een maximum uplink (outbound) van 2 Gbps, de downlink is niet gespecifieerd maar is meestal hoger dan de uplink. Deze asymmetrie komt vaak voor omdat over het algemeen meer data gedownload wordt dan geüpload. Een netwerk interface is de verbinding tussen een device en een netwerk. Deze interfaces kunnen in hardware geïmplementeerd zijn zoals Netwerk Interface Cards (NIC's) of in software. Indien deze interfaces in software zijn geïmplementeerd wordt ook wel van Virtuele Netwerk Interfaces gesproken. Een VM kan meerdere netwerk interfaces hebben, alsook dynamische netwerk interfaces. Dynamische netwerk interfaces zijn interfaces die toegevoegd of verwijderd kunnen worden zonder dat de VM moet gereboot worden. In het voorbeeld van het bedrijf is het voldoende om HTTP en HTTPS verkeer toe te staan.

4 Virtuele Machine: Verbinding

De laatste drie secties zijn: waarneembaarheid, veiligheid en gevorderd. Deze worden niet doorgenomen in de tutorial. Nu kan de VM aangemaakt worden door op create-knop te drukken. Eens de status van VM groen is wil dat zeggen dat VM up-and-running is, nu is het mogelijk om met de VM te verbinden. Om te verbinden biedt het platform meerdere opties: via een ssh-in-browser verbinding, via een ssh-in-browser op een custom poort, via ssh-in-browser gebruikmakend van een gegeven private ssh key, via een gcloud command en via een andere ssh client. Tijdens het verbinden met ssh-in-browser zal Compute Engine een ephemeral ssh-key genereren, dit is een tijdelijke ssh-key die automatisch vervalt na een bepaalde periode [13]. Het voordeel hiervan is dat er geen nood is aan het zelf genereren van ssh-keys en het zelf overbrengen van de publieke key. Het nadeel hiervan is dat er vertrouwd wordt op een derde partij die dit ephemeral certificaat uitreikt, in dit geval Compute Engine. Om dit te vermijden kan een ssh key gegenereed worden op de eigen computer. Controleer eerst of er al geen bestaande ssh keys zijn in de map ¡gebruiker¿/.ssh (Windows) of /.ssh (Linux). Indien er al ssh-key pair bestaat van het type rsa, ecdsa of ed25519 kan deze hergebruikt worden. Een nieuwe ssh key pair van hetzelfde type is overbodig voor deze toepassing. Secure shell verbindingen zijn veilige verbindingen dankzij asymmetrische encryptie. Zolang de private key van een ssh key pair niet wordt verspreidt kan de publieke key blijven gedistribueerd worden zonder veiligheids risico's [16]. Om via een OpenSSH client te verbinden, klik in de console op de VM waarmee een verbinding moet gesloten worden, klik daarna op edit en onderaan de pagina is er een sectie genaamd `Security and Access`. In die sectie kan de publieke ssh key

toegevoegd worden, de publieke key begint met het type daarna de key zelf en eindigt met een gebruikersnaam. Zorg ervoor dat de gebruikersnaam dezelfde naam is van de gebruiker op VM. In een shell naar keuze op de eigen computer kan nu een verbinding gesloten worden met het volgende commando: ssh -i `<PATH_NAAR_PRIVATE_KEY> <GEBRUIKERSNAAM>@<EXTERN_IP_ADDRESS>`. Indien er nog geen ssh-key pair bestaat, kan er een aangemaakt worden met het volgende commando `ssh-keygen -t <TYPE_KEY> -f <PAD_NAAR_.ssh> -C <GEBRUIKERSNAAM>`. Als de ssh verbinding geslaagd is zouden de commando's `cat /etc/os-release` en `who` gelijkaardige resultaten als in 4a en 4b moeten weergeven.

5 Praktijkvoorbeeld: MongoDB

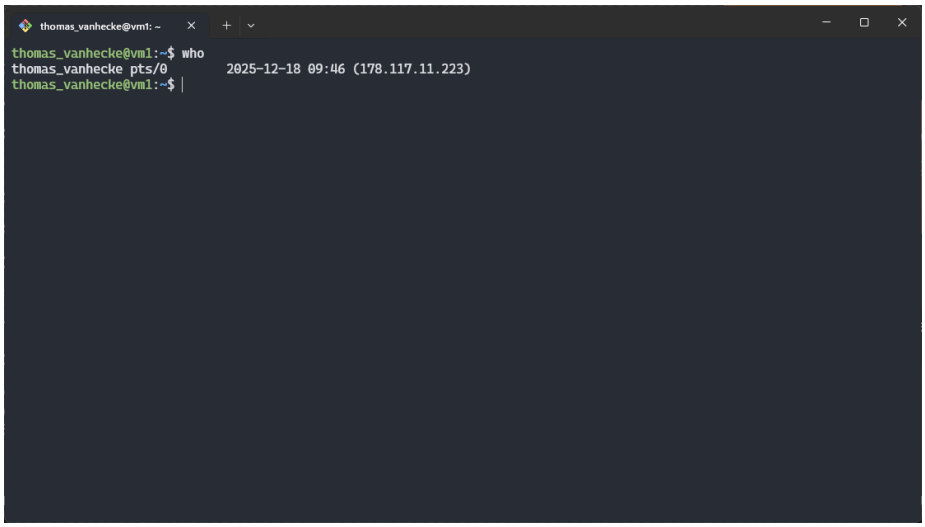
5.1 MongoDB

De tutorial heeft duidelijk gemaakt hoe VM's kunnen aangemaakt worden, maar de VM zelf moet nog ingesteld worden om bruikbaar te zijn. Om de VM bruikbaar te maken wordt een mongodb cluster gehost op de VM, die door middel van een ssh tunnel bruikbaar wordt gesteld aan de buiten wereld. Eerst moet een nieuwe VM aangemaakt worden met de image: `Rocky Linux 10 Optimized for GCP | x86/64`. Voor de correcte keuze van de resources zie `Virtuele Machine: Configuratie`. Eens de VM aangemaakt is moet een ssh verbinding gemaakt worden op basis van een zelf toegevoegde public key, voor meer informatie zie `Virtuele Machine: Verbinding`. Een goede gewoonte is om regelmatig alle packages bij te werken en zeker op een nieuw besturingssysteem. Dit kan door middel van het commando `sudo dnf update -y` gevolgd door `sudo dnf upgrade -y`. Rocky Linux is een Red-Hatt gebaseerd besturingssysteem en gebruikt daarom de Dandified YUM (DNF) package manager [12]. MongoDB maakt initieel geen deel uit van Rocky Linux's 10 dnf repository door licentie conflicten. MongoDB valt onder de Server Side Public License (SSPL) wat niet onder een Open Source Initiatief valt. Daarom is beslist om de MongoDB package te verwijderen uit de repository [2]. Deze package kan wel manueel toegevoegd worden door in de `/etc/yum.repos.d/` folder een `mongodb-org-RELEASE_SERIES.repo` bestand aan te maken [11] [1]. De volledige tutorial is hier te vinden. Nu kan de package geïnstalleerd worden met het commando `sudo dnf install mongodb-org`. Nadat de package geïnstalleerd is moet de service opgestart worden met het commando `sudo systemctl start mongod.service`. Indien de service automatisch moet opstarten als de VM opstart, moet de service ook geënabled worden. Dit kan met het commando `sudo systemctl enable mongod.service`.

5.2 SSH Tunnel

De service die verantwoordelijk is voor ssh-connecties zou by default al moeten lopen, om te dit te controleren voer het volgende commando uit `sudo systemctl`

(a) Commando cat /etc/os-release



(b) Commando who

`status sshd`. Om de ssh tunnel te openen wordt het volgende commando gebruikt `ssh -N -L POORT:HOST:HOSTPOORT GEBRUIKERSNAAM@EXTERN_IP_ADRESS`. De `-N` optie vertelt de ssh verbinding om geen remote commando's uit te voeren, dit zijn commando's die worden uitgevoerd op de VM. De `-L` optie wordt gebruikt voor port forwardings, in het commando wordt alle data op poort `POORT` geforward naar de host met ip adres `HOST` op poort `HOSTPOORT`. Dit geldt ook in de omgekeerde richting. Als bij het uitvoeren van het commando bv. `ssh -N -L 8080:127.0.0.1:27017 thomas_vanhecke@34.76.154.33` geen foutmelding gegenereerd wordt is de tunnel succesvol aangemaakt. Dan kan een GUI zoals MongoDB

Compass gebruikt worden om te interageren met de cluster. De GUI moet volgens het voorbeeld luisteren op poort 8080 van host 127.0.0.1 ookwel localhost genoemd (eigen computer). Nu kan met de database geïnterageerd worden vanaf de eigen computer. MongoDB Compass biedt ook de mogelijkheid om zelf een ssh tunnel aan te maken, daardoor is er geen nood aan een aparte shell die deze tunnel onderhoudt.

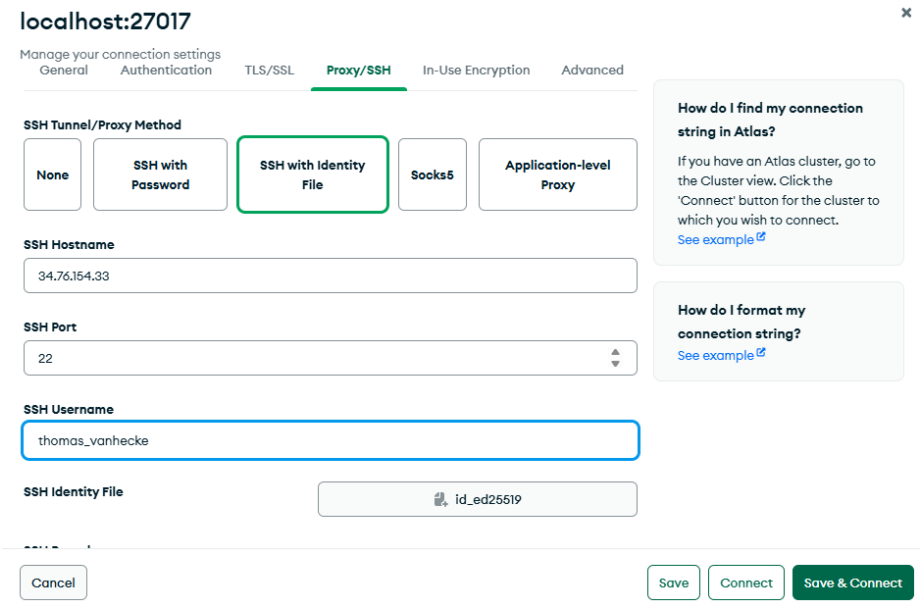


Figure 5: MongoDB Compass SSH Tunnel

Als de VM opnieuw opgestart wordt, bestaat er een kans dat de SSH hostname (extern ip adres) veranderd, deze moet dan aangepast worden in de configuratie. Als test is het interessant om een nieuwe database aan te maken, een nieuwe collectie en een document toe te voegen aan de nieuwe connectie. In 6 is het resultaat van de test zichtbaar met een compass ssh tunnel alsook een tunnel in een externe shell.

Indien er authenticatie is ingesteld voor de interactie met MongoDB vergeet de authenticatie database en credentials dan niet toe te voegen aan de configuratie in MongoDB Compass.

6 Besluit

Voor start-ups kan het interessant zijn om in het begin alles dat te maken heeft met hardware-infrastructuur te outsourcen naar de cloud. Hierdoor kan de meerderheid van de energie gespendeerd worden aan het uitwerken van het bussinesmodel. Eens bedrijven groeien en meer resources ter beschikking hebben

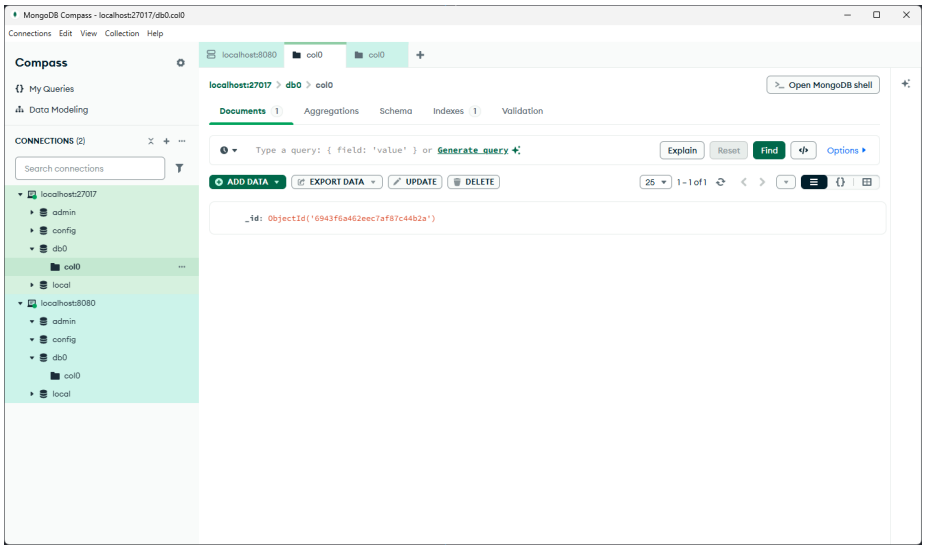


Figure 6: MongoDB Compass Test Connection

is het voordeliger om ook de hardware-infrastructuur zelf te gaan beheren, omdat dit op lange termijn goedkoper zal uitkomen. Het voordeel dat de cloud biedt, is dat het `ready-to-go` is, er is een kleine leercurve om bekend te worden met de verschillende termen en configuratie mogelijkheden. Het internet is hiervoor een goede startplaats. Het nadeel is de afhankelijkheid van de cloud provider. Voor bedrijven die werken met geklassificeerde data zou het veiliger zijn om de hardware-infrastructuur niet te outsourcen. In het besproken praktijkvoorbeeld zou MongoDB atlas kunnen gekozen worden in plaats van een Cloud VM die lokaal een cluster host. MongoDB Atlas is een vorm van Internet as a Service (IaaS) en is biedt een cloud infrastructuur aan die gespecialiseerd is voor het opzetten van clusters. In het besproken praktijkvoorbeeld zou dit een betere keuze zijn.

In het algemeen ging het aanmaken van VM's op het GCP redelijk vlot. De enige verwarring was het toevoegen van een publieke key voor key-based authenticatie. Als de publiek key toegevoegd wordt aan de VM Configuratie moet de gebruikersnaam die zijn van de gebruiker op VM, anders kan er geen connectie gesloten worden. Normaal biedt het platform ssh-in-browser aan waarbij zelf een publiek key file van op de computer kan geselecteerd worden, dit bleek niet te werken.

References

[1] Atlantic.Net. *How to Install and Use MongoDB on Rocky Linux 10*. URL: https://www.atlantic.net/dedicated-server-hosting/how-to-install-and-use-mongodb-on-rocky-linux-10/ (visited on 12/18/2025).

[2] Fedora Project. *About MongoDB and SSPL licensing*. URL: https://developer.fedoraproject.org/tech/database/mongodb/about.html (visited on 12/18/2025).

[3] Google Cloud. *Adding and removing network tags*. URL: https://docs.cloud.google.com/vpc/docs/add-remove-network-tags (visited on 12/18/2025).

[4] Google Cloud. *Compute Engine API: Overview*. URL: https://docs.cloud.google.com/compute/docs/reference/rest/v1 (visited on 12/20/2025).

[5] Google Cloud. *Compute Engine API: Rest Resource Instances*. URL: https://docs.cloud.google.com/compute/docs/reference/rest/v1#rest-resource:-v1.instances (visited on 12/18/2025).

[6] Google Cloud. *Configuring a custom hostname for a VM instance*. URL: https://docs.cloud.google.com/compute/docs/instances/custom-hostname-vm (visited on 12/18/2025).

[7] Google Cloud. *Machine families resource and comparison guide*. URL: https://docs.cloud.google.com/compute/docs/machine-resource (visited on 12/20/2025).

[8] Google Cloud. *Regions and zones documentation*. URL: https://docs.cloud.google.com/compute/docs/regions-zones (visited on 12/18/2025).

[9] Google Cloud. *Storage options: Persistent disks*. URL: https://docs.cloud.google.com/compute/docs/disks/persistent-disks (visited on 12/18/2025).

[10] Microsoft Azure. *Wat is de cloud? - Cloud-woordenlijst*. URL: https://azure.microsoft.com/nl-nl/resources/cloud-computing-dictionary/what-is-the-cloud/ (visited on 12/18/2025).

[11] RedSwitches. *How to Install MongoDB on Rocky Linux*. URL: https://medium.com/@redswitches/how-to-install-mongodb-on-rocky-linux-f3f266d60bd0 (visited on 12/18/2025).

[12] Rocky Linux. *DNF package manager*. URL: https://docs.rockylinux.org/10/guides/package_management/dnf_package_manager/ (visited on 12/20/2025).

[13] SSH Academy. *Ephemeral Certificates and Access*. URL: https://www.ssh.com/academy/iam/ephemeral-certificates-and-access (visited on 12/18/2025).

[14] StarWind Software. *Snapshots vs Backups: Key Differences*. URL: https://www.starwindsoftware.com/blog/snapshots-vs-backups-key-differences/ (visited on 12/18/2025).

[15] Stellar Data Recovery. *SSD vs HDD: Which is better for you?* URL: https://www.stellarinfo.co.in/kb/ssd-vs-hdd.php (visited on 12/18/2025).

[16] Wikipedia. *SSH protocol*. URL: https://en.wikipedia.org/wiki/Secure_Shell (visited on 12/20/2025).