Systems Advanced Docker Containers

Compose Secrets

DE HOGESCHOOL MET HET NETWERK

Elfde-Liniestraat 24, 3500 Hasselt, www.pxl.be

Secrets in Compose

Een Docker Secret is een blob van data, zoals een password, een SSH private key, een SSL certificate of een ander stuk data dat niet over een netwerk mag worden verzonden of unencrypted mag worden opgeslagen in een Dockerfile of in de source code van je applicatie.

Je kan Docker secrets gebruiken om deze gegevens centraal te beheren en veilig te verzenden naar alleen die containers die er toegang toe moeten hebben. Een secret in Docker Compose is alleen toegankelijk voor die services die er expliciet toegang toe hebben gekregen, en alleen zolang die services runnen.

Secrets werken niet in gewone Dockerfiles, enkel in Compose.

Secrets gebruiken in Compose

Dit voorbeeld maakt een eenvoudige WordPress site met behulp van twee secrets in een compose file. Zie secret-vb-1/ directory in de docker-lessen repo.

Het keyword `secrets:` definieert twee secrets `db_password:` en `db_root_password:`.

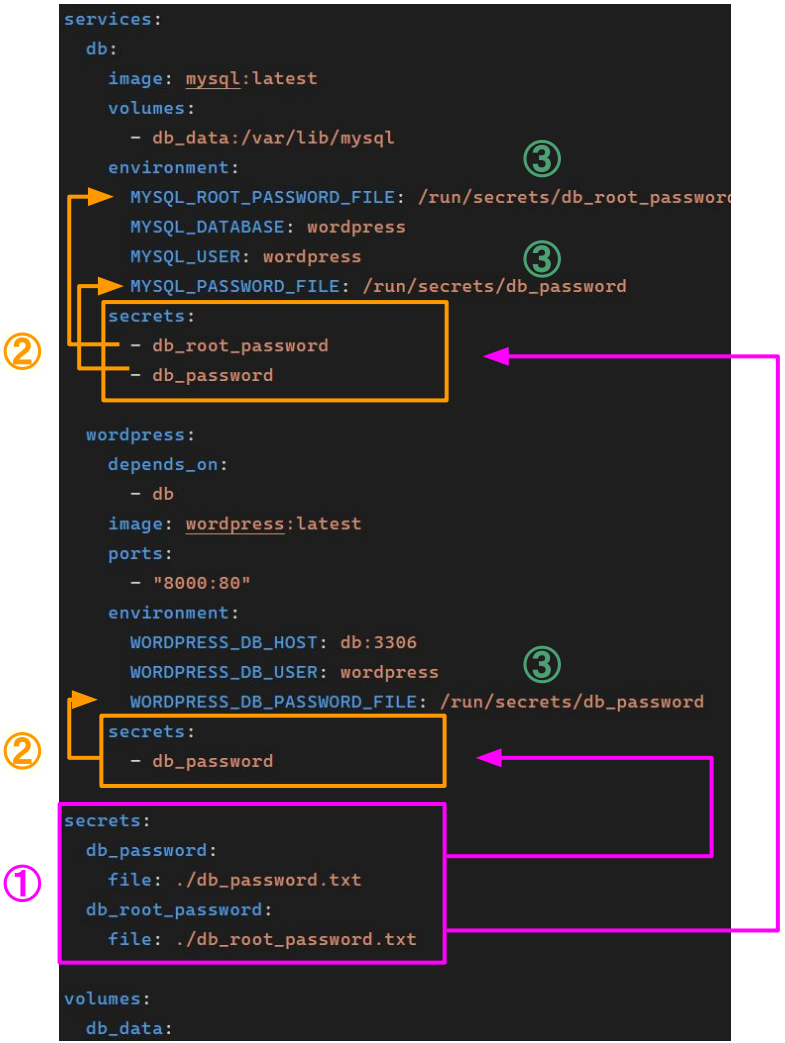
Bij het deployen maakt Docker deze twee secrets aan en vult het met de inhoud van de files die in de compose file beschreven staan.

①
- Het secret `db_password:` krijgt de inhoud van de file `./db_password.txt` dat op de host staat.
- Het secret `db_root_password:` krijgt de inhoud van de host file `./db_root_password.txt` dat op de host staat.

② De **db** service gebruikt beide secrets, en **wordpress** gebruikt er één. Als een service een secret wil gebruiken moet dat vermeld worden onder `secrets:` in de service definitie, met de naam van de secret.

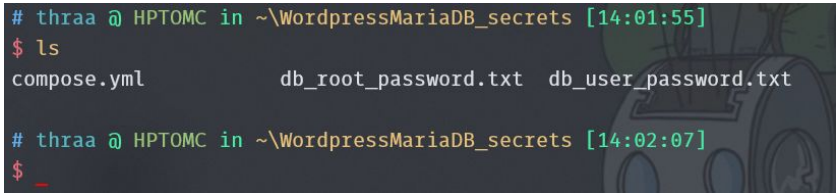
③ Bij het deployen koppelt Docker 'auto-magisch' een bestand onder `/run/secrets/<secret_name>` in de services, per secret. Deze bestanden worden nooit in de container op schijf bewaard, maar worden in het geheugen beheerd.

Elke service gebruikt environment variables om aan te geven waar de service moet zoeken naar die geheime gegevens. Je kan die environment variabelen gewoon toewijzen aan `/run/secrets/<secret_name>` zoals in het voorbeeld hiernaast.



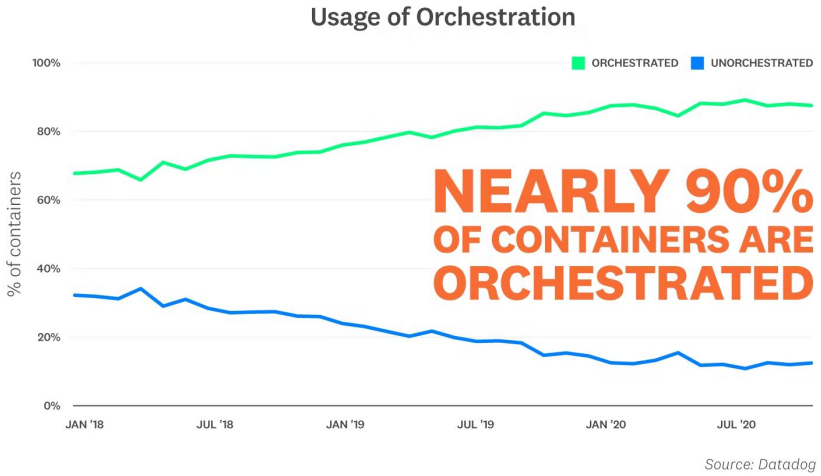
Oefening 1: docker compose met secrets

- Maak een nieuwe directory "WordpressMariaDB_secrets" aan.
  - Kopieer de file "docker-compose.yml" uit de directory "WordpressMariaDB"
  - Zorg er voor dat de paswoorden via secrets aan de containers worden doorgegeven
    - db_root_password
      - gebruik jouw voornaam als wachtwoord
    - db_user_password
      - gebruik jouw achternaam als wachtwoord



Indien het niet werkt
→ nogmaals proberen nadat je de directories van de volumes opnieuw hebt verwijderd
→ check met **`docker-compose ps`** en **`docker-compose logs`**

We hebben containers gezien - What's next?



Source: Datadog