

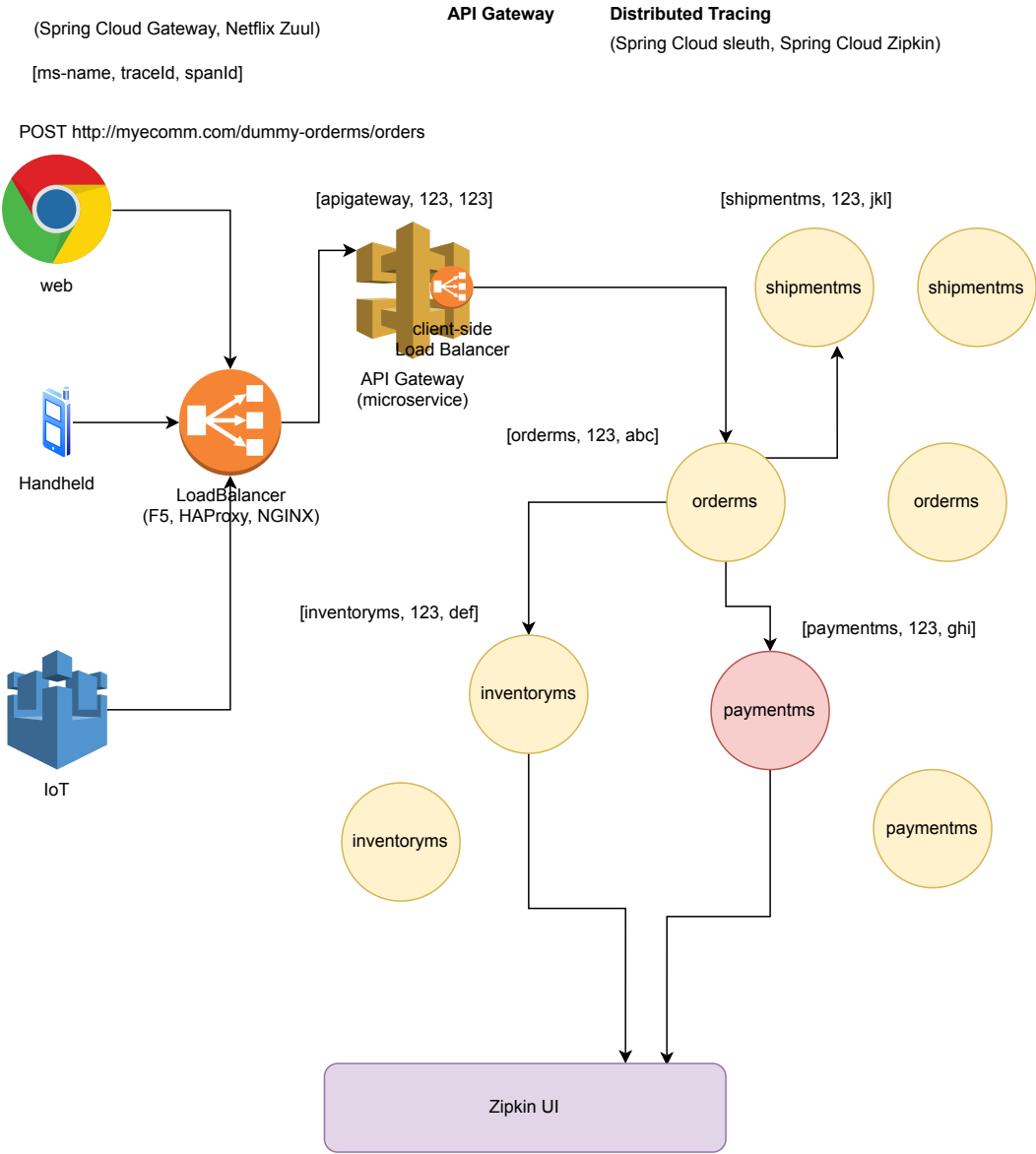
APIGateway Cross Cutting Concerns:

- 1. Security(Authn/Authz)
- 2. URL Hiding
- 3. Routing
- 4. Reverse Proxy
- 5. Distributed Tracing
- 6. Audit(API usage, durationOfRequest)
- 7. Enrich/Remove some info (add header/drop tIs)
- 8. client-device-specific response
- 9. RateLimit/Throttle

Pre-Filter:
request: addHeader("startTime",currentTime);

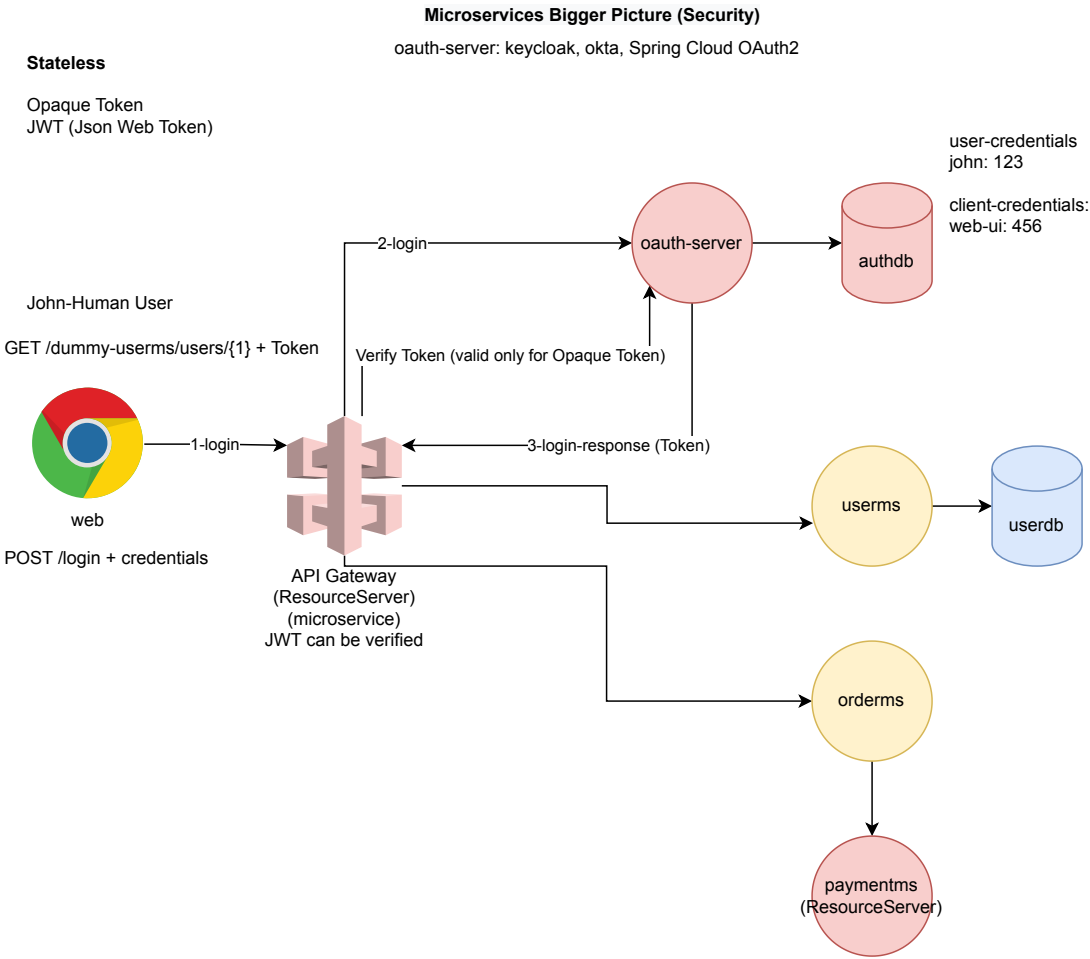
Post-Filter:
request: startTime = getHeader("startTime")
durationOfRequest = currentTime - startTime

DoS: Denial of Service



about:blank

2/8



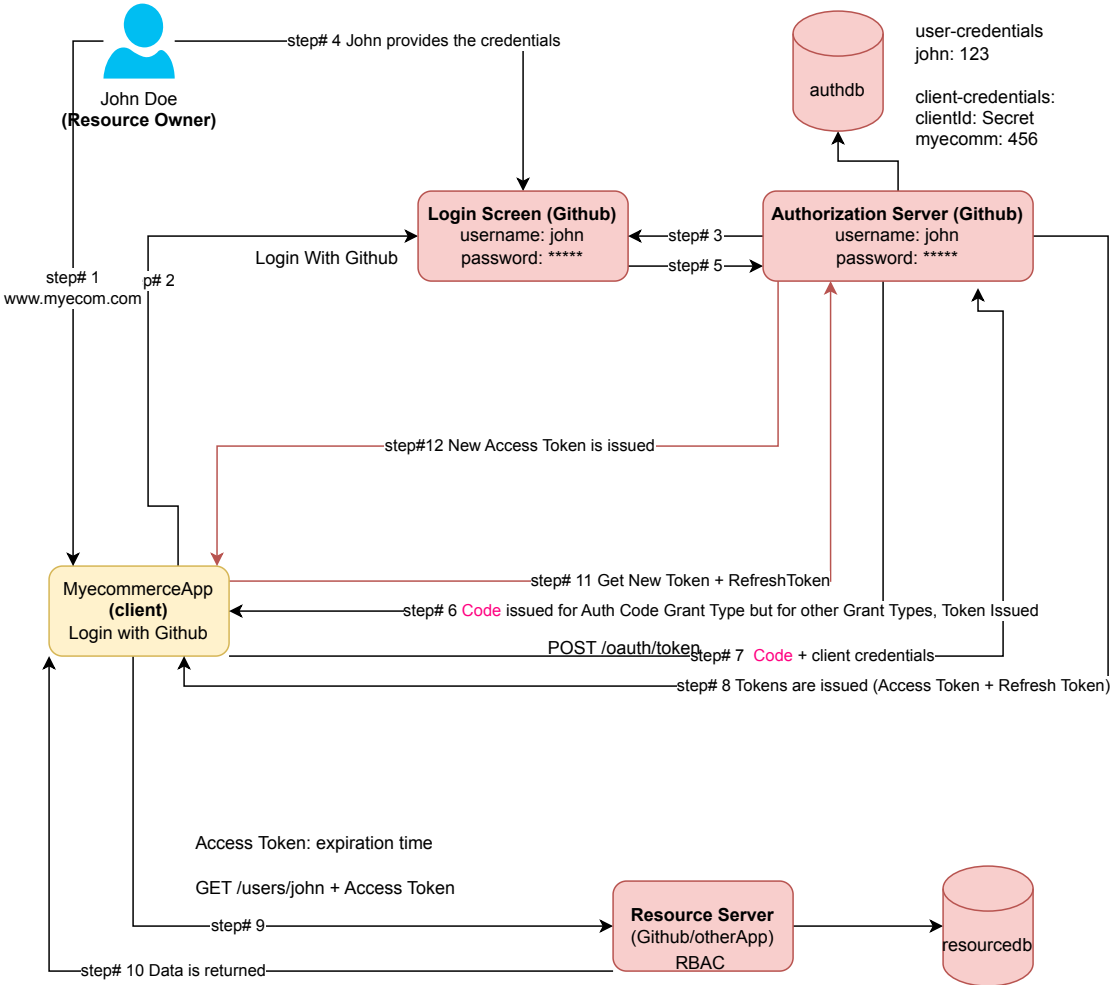
oAuth2

oAuth2 Players:

- 1. Resource Owner (Human User)
- 2. Client (Application/Non-Human User)
- 3. Authorization Server (Issues Tokens)
- 4. Resource Server (Secured data is kept)

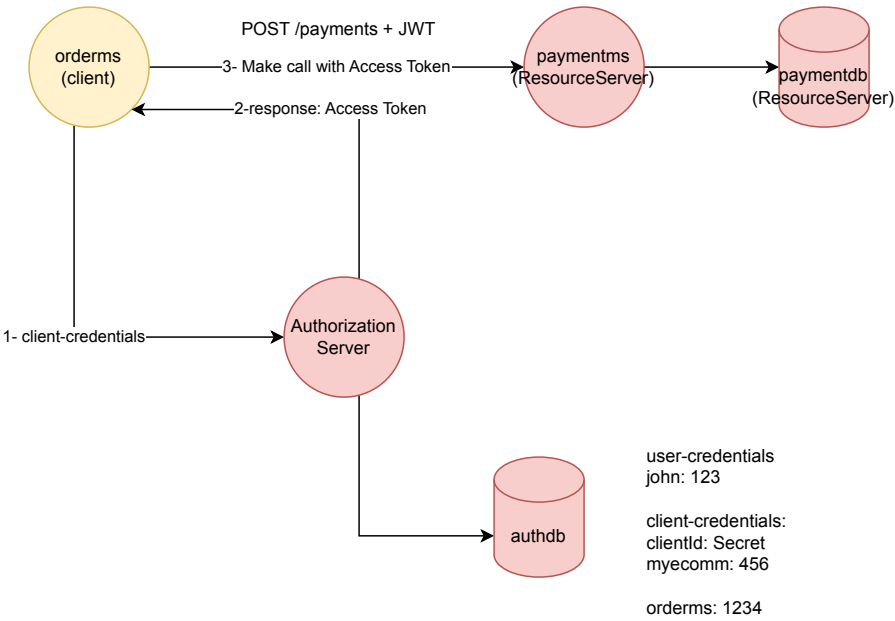
Grant Types:

- 1. Authorization Code (third party login)
- 2. Implicit (Deprecated)
- 3. Password (we own client and auth-server)
- 4. Client Credentials (Non-Human User)
- 5. Refresh

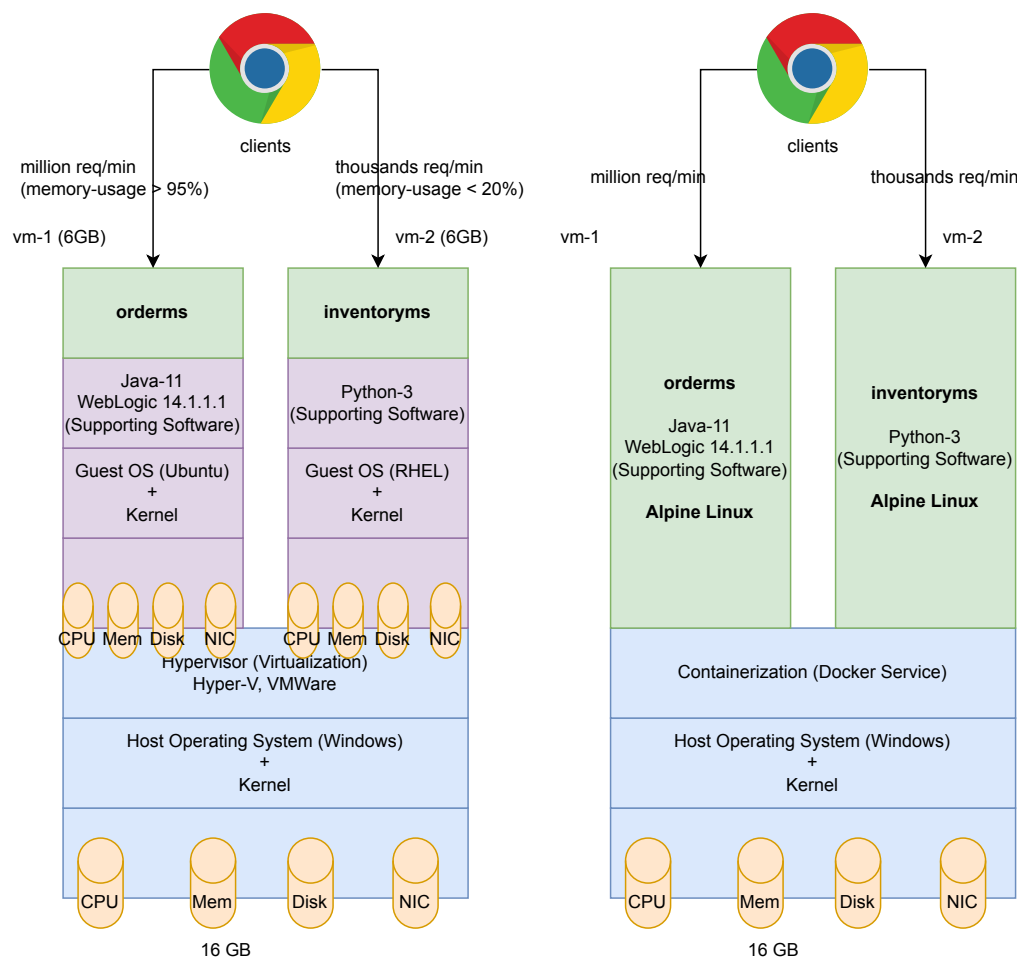


client credentials

No Refresh Token

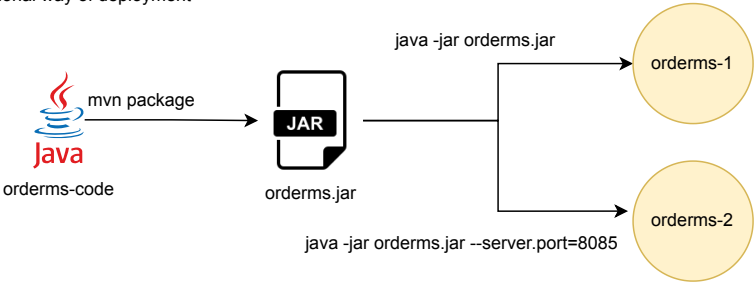


VM vs Container



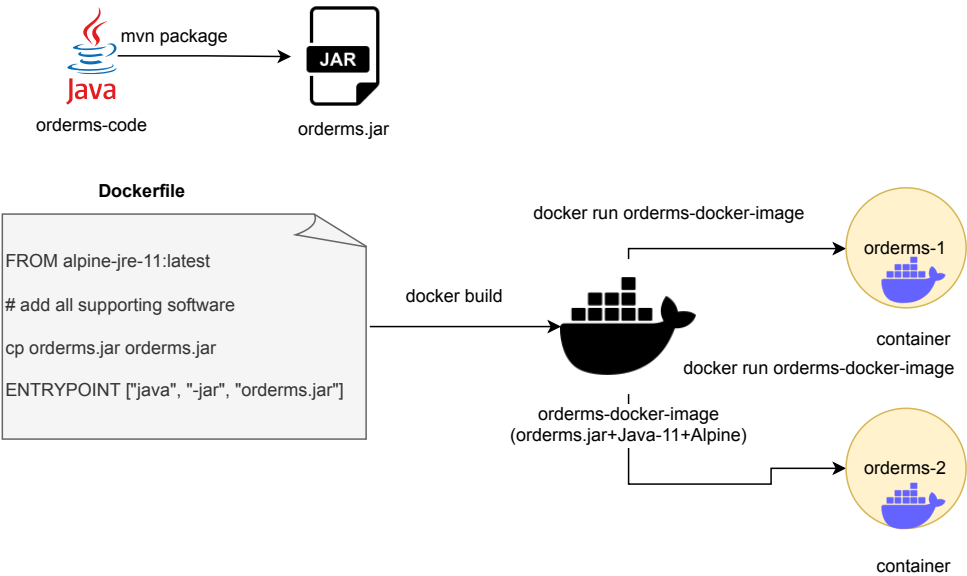
Deploy JAR vs Docker Image

Traditional way of deployment



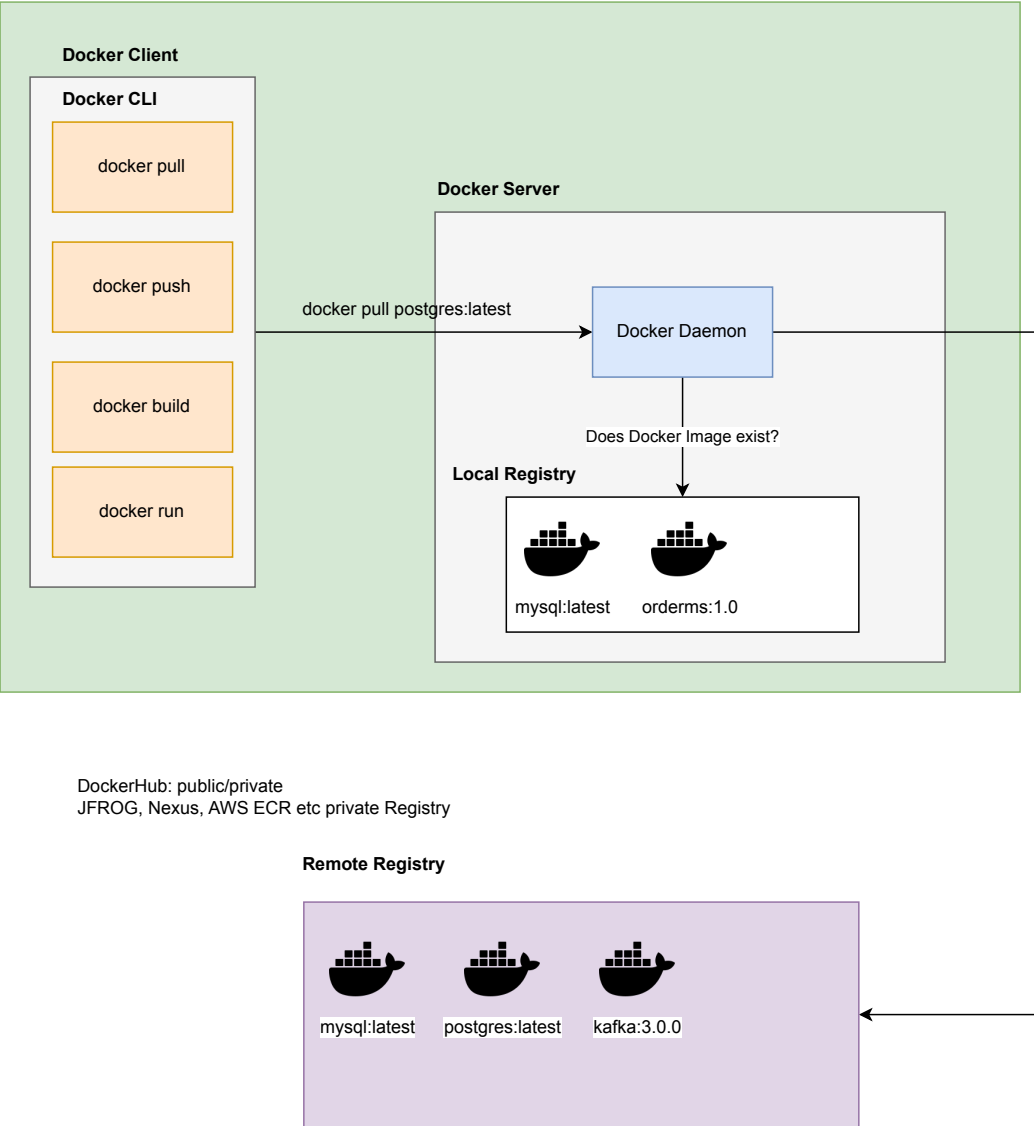
Deployment through Docker Image and Container

Docker Images are immutable
Running instance of Docker Image is a Container



Ubuntu machine where Docker Service is installed

Docker (Client-Server)



DockerHub: public/private
JFROG, Nexus, AWS ECR etc private Registry