1. Tematem pracy był Projekt i implementacja aplikacji wspomagającej zarządzanie finansami domowymi. Tematyka pracy posłużyła przy tym głownie do zaprezentowania możliwości jakie oferują wykorzystane techonologie.

Aplikacja składa się z trzech warstw:

* warstwy aplikacji klienckiej napisanej w języku TypeScript z wykorzystaniem środowiska Angular
* warstwy serwerowej zbudowanej w oparciu o architekturę mikrousług, składającą się z 3 niezależnych mikroserwisów
* Warstwy danych. W tym przypadku wykorzystano bazę danych MongoDB dosttępną w modelu SaaS.

Aplikacja kliencka komunikuje się z warstwą serwerową za pomocą interfejsu REST API, natomiast komunikacja poiędzy poszczególnymi mikrousługami może być zrealizowana na dwa sposoby: synchronicznie – z wykorzystaniem interfejsu REST API oraz asynchronicznie z wykorzystaniem brokera wiadomości RABBIT MQ.

1. Na kolejnym slajdzie zaprezentowano wykorzystane w aplikacji technologie.

Technologie podzielono na 3 grupy, tj technologie wykorzystane w implementacji mikroserwisów: m.in. język Java, biblioteki Spring Boot oraz bibliotek reaktywne Reactor.

Technologie wykorzystane do stworzenia aplikacji klienckiej, m.in. TypeScript, Angular oraz biblioteki reaktywne RxJS.

Oraz technologie wykorzystane do wdrożenia aplikacji czyli oprogramowanie do konteneryzacji Docker, oraz platform Okteto umożliwiającą uruchamianie aplikacji z wykorzystaniem systemu do zarządzania kontenerami jakim jest Kubernetes.

--------

Poszczególne mikroserwisy zostały zbudowane z wykorzystaniem architektury warstwowej. Najwyższą warstwę stanowi tutaj warstwa API, na którą składają się punkty końcowe REST API oraz klasy odpowiedzialne za odbieranie i wysyłanie wiadomości asynchronicznych.

Środkową warstwę stanowi warstwa serwisów zawierających logikę biznesową.

Najniższą warstwę stanowią klasy odpowiedzialne za obsługę dostęp do bazy danych (repozytoria danych).

1. W celu umożliwienia logowania się użytkowników oraz zapewnienia bezpiecznego sposobu uwierzytelniania i autoryzacji wykorzystano zewnętrzną aplikację Keycloak która pełni funkcję dostarczyciela tożsamości użytkowników. Uwierzytelnianie i autoryzacja możliwa jest dzięki wykorzystaniu protokołu OAuth 2.0 oraz Open ID connect.

Na slajdzie pokazano diagram sekwencji ilustrujący proces logowania użytkownika na który składa się m.in. uzyskanie tokenu JWT oraz wysłanie żądania zawierającego token w nagłówku.

1. Na kolejnym slajdzie przedstawiono diagram sekwencji dla jednego z wybranych przypadków użycia, którym jest konkretnie przypadek „Dodaj przychód/wydatek”.

W celu obsłużenia tego przypadku użycia jak widać na diagramie wykorzystane zostaną dwa mikroserwisy: Transaction management oraz Planning aplikacja kliencka oraz broker wiadomości.

POKAZ

1. Na następnym slajdzie z kolei przedstawiono diagram przypadku użycia „Dodaj Depozyt”. W tym przypadku komunikacja pomiędzy mikroserwisami odbywa się nie tylko asynchronicznie, ale również synchronicznie. Jak widać na diagramie mikroserwis Asset management, wykonuje serie synchronicznych żądań do serwisu Planning w celu pobrania aktualnego stanu środków oraz sprawdzenia czy kategoria Asset jest utworzona (w przypadku jej braku wysłane zostanie żądanie utworzenia, co zostało pominięte na schemacie).

Następnie wykonywane jest synchroniczne żądanie do serwisu Transaction management w celu utworzenia transakcji. Serwis transaction Management z kolei w w trakcie przetwarzania żądania wysyła asynchroniczną wiadomość do serwisu planing, z informacją o szczegółach utworzonej transakcji.

1. W celu sprawdzenia poprawności działania poszczególnych funkcji zaimplementowano testy jednostkowe. W tym celu wykorzystano środowisko testowe Spock oraz język Groovy.

Przykładowy prosty test jednostkowy służący do testowania statycznej metody pokazany jest na slajdzie. Wykorzystano tutaj metodę DDA, pozwalającą na sprawdzenie wielu przypadków w jednej metodzie testowej.

Testy jednostkowe wykorzystano także do testowania bardziej skomplikowanych funkcji systemu wymagających zbudowania kontekstu aplikacji oraz stworzenia protez (mocków) m.in. dla metod które zwracają dane z zewnętrznych systemów.

1. W aplikacji zastosowano także testy integracyjne których celem jest sprawdzenie prawidłowości współpracy aplikacji z zewnętrznymi systemami takimi jak bazy danych czy też zewnętrzne interfejsy API.

Aby przetestować łączność z zewnętrznymi systemami w tym przypadku z bazą danych MongoDB oraz brokerem wiadomości RabbitMQ skorzystano z bibliotek umożliwiających uruchamianie tych systemów w tymczasowych kontenerach testowych z wykorzystaniem Dockera.

Prezentowany slajd przedstawia klasę bazową zawierającą konfigurację kontenerów Dockera. Jak widać powyższy kod odpowiedzialny jest za uruchomienie kontenerów zawierających instancje bazy danej MongoDb oraz brokera RabbitMQ, dynamiczną podmianę zmiennych przechowujących informacje o adresach obu systemów oraz za usunięcie kontenerów po zakończeniu testów.

1. Na kolejnym slajdzie przedstawiono natomiast przykładowy, stosunkowo prosty test integracyjny którego celem jest sprawdzenie punktu końcowego służącego do pobierania transakcji o konkretnym identyfikatorze.

Metoda umieszczona pod klauzylą given: populateDataBase() odpowiada za przygotowanie i zapisanie danych testowych w bazie danych.

Następnie przygotowywane jest zapytanie http.

Po klauzuli when wykonywane jest zapytanie

Klauzula then z kolei służy do sprawdzenia warunków testowych, m.in. sprawdzenia statsu http, a także kategorii oraz kwoty transakcji.

1. Ostatnim etapem pracy było wdrożenie aplikacji. W tym celu skorzystanio z platformy Okteto która oferuje możliwość uruchamiania aplikacji z wykorzystaniem systemu Kubernetes. Platforma Okteto wspiera przy tym możliwość uruchamiania/wdrażania aplikacji z wykorzystaniem plików Docker Compose.   
     
   Na platformie okteto uruchamiane są wszystkie aplikacjie w tym aplikacja kliencka oraz 3 mikroserwisy. Oprócz tego na platformie Oketeto uruchamiana jest aplikacja RabbitMQ.  
     
   Jak pokazuje diagram wdrożenia, baza danych znajduje się na zewnętrzym systemie. W tym przypadku skorzystano z bazy danych MongoDB w modelu Software as a Service.  
     
   Dodatkowo na serwerze zewnętrznym również z wykorzystaniem Docker Compose uruchamiana jest aplikacja Keycloak pełniąca funkcję dostarczyciela tożsamości.
2. Na następnym slajdzie przedstawiono głowny plik docker Compose pozwalający na uruchomienie wszystkich aplikacji w osobnych kontenerach. Plik zawiera odniesienia do plików Dockerfile które z kolei umożliwiają zbudowanie obrazów dockera bezpośrednio z kodu źródłowego. Plik pozwala na skorzystanie również z obrazów dostępnych online. Taki obraz który jest dostępny online wykorzystano do wdrożenia brokera wiadomości RabbitMQ.

Plik zawiera także odniesienia do plików ze zmiennymi systemowymi które tworzone są w kontenerach. Plik zawiera również odniesienia do zmiennych zawierające hasła i dane poufne. Jednak hasła te nie są bezpośrednio umieszczone w pliku, są one zapisane w sposób bezpieczny bezpośrednio na platformie okteto.

1. Następny slajd przedstawia widok panelu administracyjnego platformy Okteto.

Na panelu znajduje się podgląd wszystkich uruchomionych kontenerów oraz aplikacji w nich uruchomionych. System umożliwia także podgląd logów dla poszczególnych aplikacji.

Ostatecznym efektem pracy jest działający system o podstawowej funkcjonalności, który jednak dzięki modułowej budowie może być łatwo rozbudowany. Dzięki zastosowaniu architektury mikroserwisowej, nierelacyjnej bazy danych oraz komunikacji asynchronicznej, system taki może być w łatwy sposób skalowalny, przez co nadaje się do obsługi ruchu o zróżnicowanym nasileniu.