POLITECHNIKA WROCŁAWSKA
WYDZIAŁ ELEKTRONIKI

KIERUNEK: INFORMATYKA
SPECJALNOŚĆ: SYSTEMY I SIECI KOMPUTEROWE

PRACA DYPLOMOWA INŻYNIERSKA

Projekt strony internetowej do recenzji albumów muzycznych w technologii ASP.NET Core oraz grafowej bazie danych

Design of an internet website for music albums reviewing based on ASP.NET Core and graph database

AUTOR:
Marcin Kotas

PROWADZĄCY PRACĘ:
dr inż. Mariusz Topolski, W4/K2

OCENA PRACY:

WROCŁAW, 2019

Spis treści

Skróty

IT (ang. *Information Technology*)
RPC (ang. *Remote Procedure Call*)
JSON (ang. *JavaScript Object Notation*)
SOAP (ang. *Simple Object Access Protocol*)
XML (ang. *Extensible Markup Language*)
WSDL (ang. *Web Services Description Language*)
REST (ang. *Representational state transfer*)
API (ang. *Application Programming Interface*)
CRUD (ang. *Create Read Update Delete*)
HTTP (ang. *HyperText Transfer Protocol*)
DTO (ang. *Data Transfer Object*)
HTML (ang. *HyperText Markup Language*)
CSS (ang. *Cascading Style Sheets*)
RDBMS (ang. *Relational Database Management System*)
JWT (ang. *JSON Web Token*)

Rozdział 1

Wprowadzenie

1.1. Cel pracy

Celem pracy była implementacja strony internetowej pozwalającej dodawać recenzje albumów muzycznych, wykorzystując najnowsze technologie z tej dziedziny zgodne z obecnymi trendami. Główny nacisk nałożony zostanie na stworzenie architektury stanowiącej solidną bazę do dalszego rozwijania aplikacji. Projekt wykorzystywać będzie tylko oprogramowanie open source.

1.2. Zakres pracy

W pierwszym rozdziale przedstawiono cel oraz zakres pracy. Kolejny rozdział zawiera informacje na temat technologii, które zostały wykorzystanie w projekcie. Porównane zostały one do alternatywnych rozwiązań, które również spełniają wymagania projektu. Rozdział 3 opisuje wymagania projektowe: wymagania funkcjonalne i niefunkcjonalne, przypadki użycia oraz założenia projektowe. W następnym rozdziale przedstawiono projekt aplikacji. Zawarte w nim są projekty architektury poszczególnych warstw aplikacji oraz bazy danych. Rozdział 5 zawiera opis implementacji projektu. Podzielony został na podrozdziały, które opisują po kolei implementację każdego dockerowego kontenera aplikacji.

dokończyć strukturę pracy jak będą wszystkie rozdziały

Rozdział 2

Przegląd technologii

2.1. Paradygmaty komunikacji z usługami sieciowymi

Powstało wiele sposobów komunikacji z usługami sieciowymi. W tym rozdziale opisane zostaną najpopularniejsze z nich.

2.1.1. RPC

RPC to prosty protokół zdalnego wywołania procedury. Klient wysyła do serwera potrzebne dane do wywołania akcji: nazwę metody oraz parametry. W podstawowej wersji całość komunikacji odbywa się za pomocą jednego punktu dostępowego (ang. *endpoint*). Zwykle wykorzystywane są wariacje protokołu np. JSON-RPC, które przesyłają dane w formacie JSON.

Przykładowe wywołanie oraz odpowiedź:

```
{
  "jsonrpc": "2.0",
  "method": "divide",
  "params": {
    "dividend": 32,
    "divisor": 4
  },
  "id": 5
}
```

```
{
  "jsonrpc": "2.0",
  "result": 8,
  "id": 5
}
```

2.1.2. SOAP

SOAP to ustandaryzowany protokół służący do opakowywania przesyłanych danych. Często porównywany do wkładania danych do „koperty”, definiuje sposób kodowania i dekodowania danych do formatu XML [8]. Paczka z danymi zawiera również informacje opisujące dane oraz w jaki sposób mają być przetworzone. Wykorzystuje przez to więcej zasobów niż czysty JSON z danymi – zarówno w kwestii rozmiaru przesyłanych danych jak i czasu ich przetworzenia.

Opcjonalny lecz zalecany jest dokument WSDL, który w ustandaryzowany sposób określa punkty dostępowe usług serwisu. Umożliwia automatyczne generowanie testów serwisu oraz funkcji wywołujących usługi.

Zapytanie w SOAP jest zawsze typu POST, a więc odpowiedź nie jest zapisywana przez przeglądarkę i za każdym razem wywoływana jest procedura w Api. Jest jednak dzięki temu bardziej zaawansowany - zapewnia wsparcie dla transakcji spełniających ACID oraz posiada

rozszerzone mechanizmy bezpieczeństwa – oprócz SSL, implementuje również WS-Security. Te właściwości są istotnymi zaletami wykorzystywanymi w aplikacjach typu enterprise.
Przykładowa budowa zapytania SOAP [5]:

```
<?xml version="1.0"?>

<soap:Envelope
xmlns:soap="http://www.w3.org/2003/05/soap-envelope/"
soap:encodingStyle="http://www.w3.org/2003/05/soap-encoding">

<soap:Body xmlns:m="http://www.example.org/stock">
  <m:GetStockPrice>
    <m:StockName>IBM</m:StockName>
  </m:GetStockPrice>
</soap:Body>

</soap:Envelope>
```

oraz odpowiedź:

```
<?xml version="1.0"?>

<soap:Envelope
xmlns:soap="http://www.w3.org/2003/05/soap-envelope/"
soap:encodingStyle="http://www.w3.org/2003/05/soap-encoding">

<soap:Body xmlns:m="http://www.example.org/stock">
  <m:GetStockPriceResponse>
    <m:Price>34.5</m:Price>
  </m:GetStockPriceResponse>
</soap:Body>

</soap:Envelope>
```

2.1.3. REST

REST nie jest protokołem lecz stylem architektury. Nie narzuca konkretnej implementacji ani specyfikacji. Definiuje za to wymagania, które powinno spełnić Api typu RESTful [7]:

1. Klient-Serwer: podział ról i odpowiedzialności – klient i serwer mogą być rozwijane niezależnie, o ile interfejs pozostanie bez zmian.
2. Bezstanowość: wszystkie informacje potrzebne to wykonania żądania zawarte są w zapytaniu – jego wykonanie jest niezależne od poprzedniego stanu serwera.
3. Pamięć podręczna: klient jest w stanie zapisać odpowiedź serwera w pamięci podręcznej aby ograniczać zapytania do serwera.
4. System warstwowy: klient nie musi mieć bezpośredniego połączenia z serwerem – pomiędzy może być zaimplementowany load-balancer, proxy lub inny serwis, który jest niewidoczny ani dla serwera ani klienta.
5. Kod na żądanie (opcjonalne): Serwer jest w stanie przesłać wykonywalny kod na żądanie klienta, np. skrypty w języku JavaScript.
6. Jednolity interfejs: określa wymagania dotyczące interfejsu między klientem a serwerem:
   - zasoby są identyfikowane unikalnym URI
   - serwer opisuje dane w postaci reprezentacji, klient modyfikuje dane poprzez przesłanie reprezentacji
   - każda wiadomość zawiera informacje, w jaki sposób przetworzyć dane
   - HATEOAS (ang. *Hypermedia as the Engine of Application State*) – serwer przesyła linki do akcji, które mogą zostać wykonane dla danego stanu zasobu

Większość developerów pomija jednak implementowanie HATEOAS, ponieważ wymaga dużego nakładu pracy zarówno po stronie serwera jak i klienta i często nie jest potrzebne dla prostych zapytań typu CRUD.

Przykładowa odpowiedź na zapytanie `GET /accounts/12345` [3]:

```
{
    "account": {
        "account_number": 12345,
        "balance": {
            "currency": "usd",
            "value": 100.00
        },
        "links": {
            "deposit": "/accounts/12345/deposit",
            "withdraw": "/accounts/12345/withdraw",
            "transfer": "/accounts/12345/transfer",
            "close": "/accounts/12345/close"
        }
    }
}
```

W odpowiedzi zawarta jest lista `links` — są to akcje dostępne dla danego stanu konta. Jeśli stan konta byłby na minusie, część z tych akcji nie pojawiła by się w odpowiedzi. Takie działanie API wymaga jednak zaimplementowania maszyny stanów na serwerze.

2.1.4. GraphQL

GraphQL to język zapytań dla API oraz środowisko do wykonywania tych zapytań na istniejących danych [1]. Specyfikacja nie określa w jaki sposób ma być zbudowane Api ale oferuje następujące zasady projektowania[2]:

- hierarchiczna struktura zapytań — pola są zagnieżdżone, a zapytanie ma taki sam kształt jak dane które zwraca
- budowa GraphQL jest determinowana potrzebami aplikacji klienckiej
- silne typowanie — w schemacie każde pole ma zdefiniowany typ, który jest walidowany
- zapytania określane przez klienta — serwer GraphQL określa schemat wszystkich możliwych zapytań, a klient sam określa, które pola ma zwrócić
- introspekcyjny — język GraphQL umożliwia odpytywanie serwera o jego schemat i typy

Język zapytań GraphQL (ang. *Query Language*) znacznie różni się od SQL. Do pobierania danych zamiast *SELECT* używany jest typ *Query*, natomiast *INSERT*, *UPDATE* oraz *DELETE* zawierają się w jednym typie: *Mutatation*. Dodatkowo zdefiniowany jest typ *Subscription*, który używany jest do nasłuchiwania zmian przez gniazda (ang. *socket*). Przykładowe zapytanie GraphQL pokazano poniżej:

```
query getAlbum($id: ID!) {
  album(id: "7803c5ee938249daa7ed67574c13e389") {
    id
    title
    albumArtist {
      name
    }
  }
}
```

Odpowiedź z serwera na takie zapytanie ma analogiczną strukturę:

```
{
  "data": {
```

```
    "album": {
      "id": "7803c5ee938249daa7ed67574c13e389",
      "title": "Until the Quiet Comes",
      "albumArtist": {
        "name": "Flying Lotus"
      }
    }
  }
}
```

Aby wykonanie takiego zapytania było możliwe, serwer musi zadeklarować odpowiednie typy. Typ reprezentuje obiekt odpowiadający jakiejś funkcji aplikacji [6]. W kontekście strony muzycznej do typami byłyby między innymi albumy czy artyści. Typ składa się z pól, które odpowiadają danym obiektu. Każde pole zwraca określony typ danych.

Typy mogą być skalarne lub obiektowe: typ skalarny zawsze zwraca wartość, natomiast typ obiektowy złożony jest z kolejnych pól. Wbudowane typy skalarne to Int, Float, String, Boolean, ID. Możliwe jest tworzenie dodatkowych typów skalarnych np. DateTime, aby zapewnić odpowiednie formatowanie i walidację danych. Dodatkowo typy mogą zostać oznaczone wykrzyknikiem, co znaczy że zawsze zwrócą wartość (ang. *non-nullable*).

Przykładowy schemat, który umożliwi wykonanie powyższego zapytania wygląda następująco:

```
type Album {
  id: ID!
  title: String!
  albumArtist: Artist!
  releaseDate: DateTime
  averageRating: Float
}

type Artist {
  id: ID!
  albums: [Album!]!
  name: String!
}

type Query {
  album(id: ID!): Album
  artist(id: ID!): Artist
}
```

Wszystkie zapytania wywoływane są na jednym punkcie dostępowym (np. `/api/graphql`), przez co nie jest możliwe proste zapisywanie odpowiedzi HTTP serwera. Wymusza to implementację bardziej zaawansowanych mechanizmów cache po stronie klienta, np. poprzez identyfikacje częściowych obiektów po ID i uzupełnianie ich danych w pamięci podręcznej.

2.1.5. Porównanie

Żaden z tych protokołów nie jest najlepszy pod każdym aspektem i wszystkie wciąż mają swoje zastosowania.

RPC jest najczęściej używane w API nastawionych na akcje. W sytuacjach, gdzie często wywołanie metody nie wpływa na stan zasobu RPC jest wystarczające.

SOAP rozbudowuje RPC zapewniając bezpieczeństwo i transakcje. Istnieją jednak nowsze rozwiązania takie jak OData bazujące na REST, które mają znacznie lepszą wydajność i kompatybilność.

REST jest najbardziej zaawansowaną architekturą (jeśli zaimplementowana w pełni) i jednocześnie najczęściej spotykaną. Pozwala na szybkie operacje typu CRUD oraz zaawansowaną

nawigację przez HATEOAS. Dodatkowo dzięki unikalnym URI dla każdego zasobu umożliwia łatwe stworzenie skutecznego cache.

GraphQL umożliwia stworzenie uniwersalnego API dla wielu klientów zapewniając wysoką wydajność. Definiuje jednoznaczną specyfikację zapewniającą silne typowanie oraz introspekcję w przeciwieństwie do REST, do którego powstało mnóstwo różniących się implementacji.

2.2. Platformy do tworzenia SPA

Powstało mnóstwo bibliotek i frameworków do tworzenia stron internetowych i choć różnią się implementacją, to zasada działania pozostaje podobna. Oto trzy najpopularniejsze obecnie platformy:

Angular to framework stworzony przez Google, napisany w języku TypeScript. Zawiera w sobie pełen zestaw narzędzi i bibliotek do stworzenia strony wspierającej również urządzenia mobilne. Definiuje wzorce projektowe, które określają strukturę projektu i dobre praktyki.

React to biblioteka do tworzenia UI opracowana przez Facebooka. Do stworzenia pełnej, zaawansowanej strony wymaga użycia dodatkowych bibliotek do zarządzania stanem, trasowania czy interakcji z API. Nie narzuca żadnej struktury projektu, przez co każdy projekt może być zbudowany inaczej. Wymaga więc osoby doświadczonej, która kieruje projektem.

Vue nie jest zarządzany przez jedną korporację, lecz przez społeczność. Jest najbardziej przystępny, pozwala na stworzenie zarówno prostych stron, jak i złożonych poprzez rozszerzanie infrastruktury. Jest to osiągalne dzięki wysoce modularnej i elastycznej strukturze.

2.3. Platformy do tworzenia API

Serwer Api można stworzyć w większości istniejących języków programowania. Najczęściej wykorzystywane są frameworki zbudowane w PHP (Laravel), Javie (Spring), Pytonie (Django), C# (ASP.Net Core), Ruby (Rails) i Node.js (Express). W tym projekcie zdecydowano się użyć ASP.Net Core 3.0 ze względu na wieloplatformowość (wsparcie dla kontenerów linuksowych), wbudowany system wstrzykiwania zależności (ang. *Dependency Injection*), nowoczesny język C# 8 oraz wysoki stopień zaawansowania bibliotek implementujących GraphQL. Ważnym aspektem była również oficjalna biblioteka *Identity*, która zapewnia bezpieczną obsługę kont użytkowników.

Rozdział 3

Analiza wymagań projektowych

3.1. Wymagania funkcjonalne

Wymagania funkcjonalne określają wymagania dotyczące pożądanego zachowania systemu. Definiują, jakie usługi ma oferować i jak ma reagować na określone dane wejściowe. Wyszczególniono następujące wymagania funkcjonalne:

1. System zawiera katalog albumów
2. Albumy da się wyświetlać wraz ze szczegółami
3. Każdy album można oceniać oraz dodawać recenzję
4. Istnieje możliwość dodawania nowych albumów
5. Wyszukiwanie albumów korzysta z bazy zewnętrznego serwisu
6. Możliwość rejestracji i logowania
7. Wybór pomiędzy ciemnym i jasnym motywem aplikacji

3.2. Wymagania niefunkcjonalne

Wymagania te określają właściwości systemu, jego ograniczenia i standardy w jakich pracuje. Wymagania systemu spełniającego założenia projektowe są następujące:

1. Aplikacja powinna być obsługiwana przez obecne wersje przeglądarek
2. Do poprawnego działania wymagane jest połączenie z Internetem
3. Aplikacja powinna być napisana w sposób umożliwiający łatwe dodawanie nowej funkcjonalności
4. Dane użytkowników są przechowywane w bezpieczny sposób

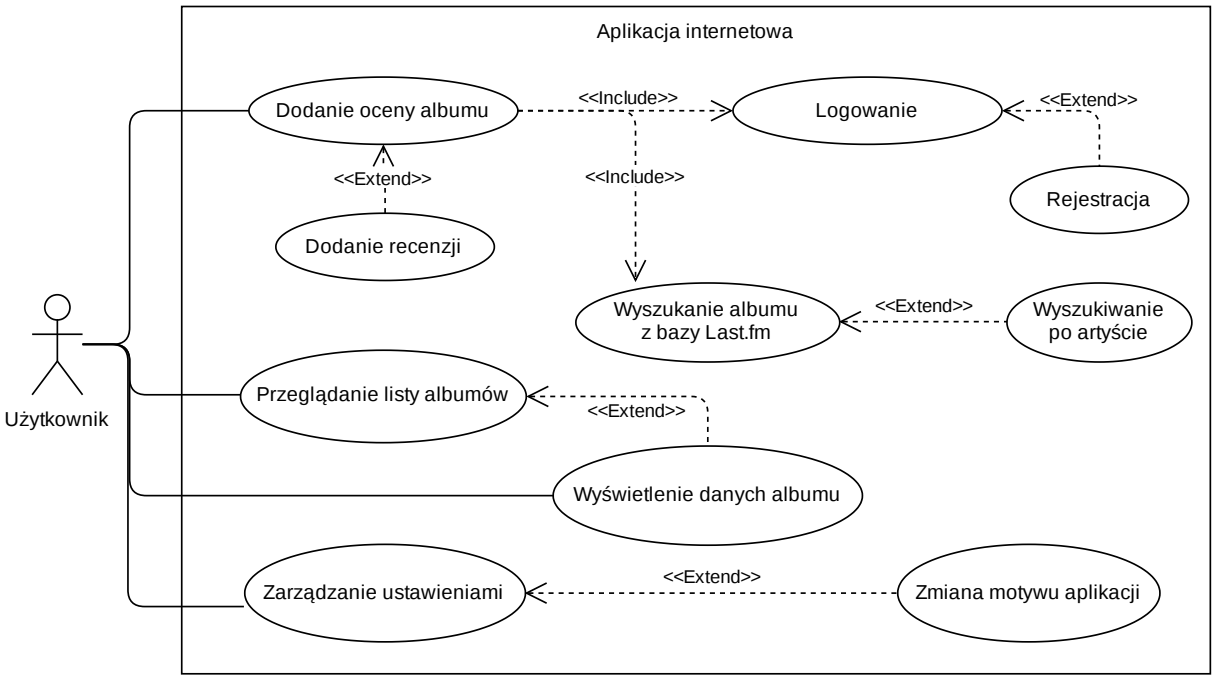
3.3. Przypadki użycia

Na rysunku 3.1 przedstawiono diagram przypadków użycia użytkownika aplikacji. Zawarte zostały główne funkcjonalności skupiające się na przeglądaniu albumów i dodawaniu recenzji. W ten sposób wyszczególniono następujące przypadki użycia:

1. Dodanie oceny albumu
   Przypadek użycia dotyczy akcji dodania oceny do albumu. Dodawanie opisowej recenzji jest opcjonalne, dlatego ujęte zostało jako opcjonalny, rozszerzający przypadek użycia.
2. Wyszukanie albumu z bazy Last.fm
   Aby dodać ocenę do albumu należy wyszukać odpowiedni album wpisując jego nazwę

lub wybrać z najpopularniejszych albumów podanego artysty. Wyszukiwarka korzysta z API Last.fm, jednak nie wymaga konta na tym serwisie.

3. Logowanie
   Dodawanie ocen dostępne jest tylko dla zalogowanych użytkowników. Przeglądanie albumów i recenzji nie wymaga konta.
4. Rejestracja
   Jeśli użytkownik nie ma jeszcze utworzonego konta, a chce dodawać oceny to może się zarejestrować.
5. Przeglądanie listy albumów
   Użytkownik może przeglądać wszystkie albumy, do których zostały dodane oceny. Po kliknięciu w album przenoszony zostaje do widoku wyświetlającego wszystkie dane albumu.
6. Zarządzanie ustawieniami
   Przypadek użycia opisujący zmianę ustawień aplikacji, które są unikalne dla każdego użytkownika. Na chwilę obecną możliwa jest zmiana motywu głównego aplikacji (jasny/ciemny).



Rys. 3.1: Diagram przypadków użycia

3.4. Założenia projektowe

Całość aplikacji zaprojektowana zostanie ze wsparciem platformy Docker. Każda odrębna część systemu zamknięta będzie we własnym wirtualnym kontenerze:

1. strona internetowa typu Single-Page Application:
   Architektura SPA pozwala tworzyć strony, które w swoim działaniu bardziej przypominają tradycyjne aplikacje komputerowe. Podczas interakcji użytkownika ze stroną fragmenty widoku są dynamicznie odświeżane zamiast przeładowywania całej strony. Dodatkowo strona powinna przechowywać w pamięci zapytania do serwera aby minimalizować czas oczekiwania na dane.

2. serwer uwierzytelniający użytkowników:
   Strona internetowa działa po stronie klienta, przez co możliwa jest znaczna ingerencja w dane. Aby minimalizować zagrożenia, zaimplementowane zostanie uwierzytelnianie użytkowników wykorzystujące bezpieczny protokół. Wykorzystany standard powinien zapewnić zarówno uwierzytelnianie jak i autoryzację.
3. serwer dostępowy do danych aplikacji:
   Grafowy dostęp do bazy danych zaimplementowany zostanie za pomocą GraphQL. Serwer umożliwiać będzie pobieranie danych stosując zapytania w języku GraphQL. Dzięki temu relacje między danymi przedstawione są w postaci grafu, co pozwala formować skompilowane zapytania bez potrzeby tworzenia dedykowanych kontrolerów i modeli DTO po stronie API.
4. baza danych:
   Baza danych powinna umożliwiać przechowywanie relacji między obiektami w taki sposób, aby możliwe było reprezentowanie danych w postaci grafu.
5. serwer dostarczający odwrócone proxy:
   Z racji tego, że użytkownicy będą przekierowywani między główną stroną, a stroną do uwierzytelniania, adresy serwerów zarejestrowane będą w odwróconym proxy. Będzie to również główny punkt dostępu do aplikacji, który będzie kierował ruchem. Dodatkowo, będzie obsługiwał szyfrowanie przesyłanych danych protokołem HTTPS.

Rozdział 4

Projekt aplikacji

4.1. Architektura fizyczna

Zgodnie z założeniami projektowymi, całość aplikacji serwowana będzie z platformy dockerowej. Podczas tworzenia aplikacji uruchamiana ona będzie na systemie *Ubuntu 18.04* przy użyciu *Windows Subsystem For Linux*. Umożliwia to jednoczesne korzystanie z narzędzi dostępnych tylko pod systemem Windows (Visual Studio) i uruchamianie w docelowym systemie (Linux). Wersja produkcyjna aplikacji umieszczona zostanie na serwerze z systemem Linux.

Na schemacie 4.1 przedstawiono architekturę aplikacji z podziałem na poszczególne kontenery. Aby zapewnić najwyższe bezpieczeństwo, porty kontenerów nie są mapowane na zewnątrz dockera. Wyjątkiem jest kontener z odwróconym proxy (*revProxy*), który obsługuje całą komunikację ze światem zewnętrznym. Kieruje on odpowiednio ruchem w zależności od adresu zapytania. Na przykładzie lokalnego adresu zapytania obsługiwane będą w następujący sposób:

localhost/ domyślnie cały ruch kierowany jest do strony internetowej serwowanej z kontenera *spa*

auth.localhost/ zapytania z subdomeną *auth* kierowane są do kontenera *authServer* obsługującego zapytania związane z OpenID

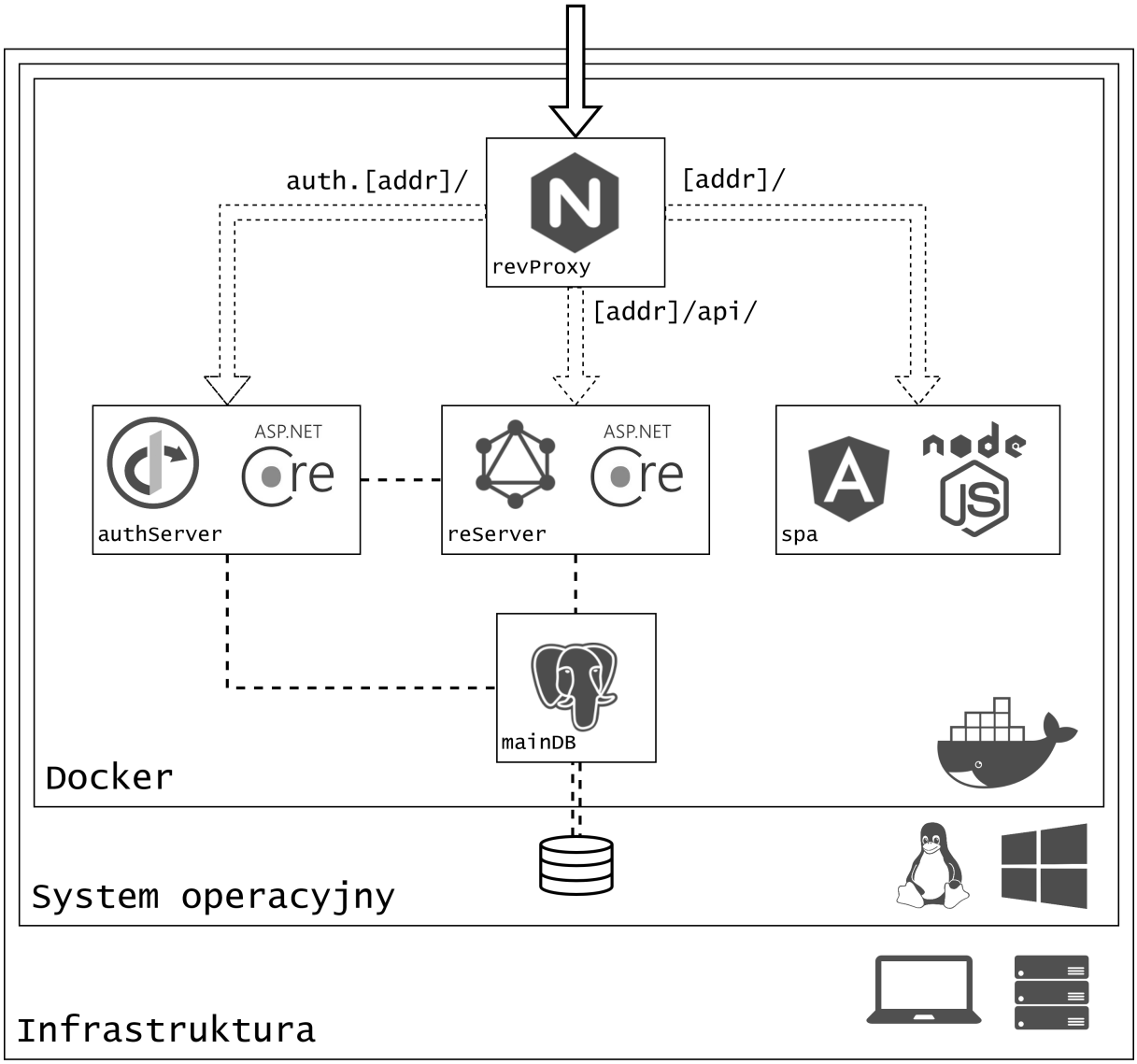
localhost/api/ jeśli zapytanie odnosi się do katalogu */api/* to zostaje obsłużone przez kontener *reServer*

Kontener obsługujący zapytania API musi być dostępny z zewnątrz, ponieważ strona internetowa jest typu SPA, a więc jest wszystkie zapytania będą wysyłane bezpośrednio z przeglądarki użytkownika. Z tego samego powodu kontener *spa* nie komunikuje się z resztą kontenerów, co ukazane zostało na schemacie. Pozostałe kontenery korzystają z wewnętrznej sieci do komunikacji z bazą danych. Dodatkowo, kontener *reServer* komunikuje się z kontenerem *authServer* do walidacji tokenów JWT oraz do pobierania danych zalogowanego użytkownika.

Dane nie mogą być zapisywane bezpośrednio w kontenerze, ponieważ mogły by zostać łatwo utracone jeśli istniała by potrzeba zresetowania kontenerów. Z tego powodu baza danych zapisuje dane do folderu zmapowanego na dysk systemu operacyjnego. Ogranicza to ryzyko utraty danych jednak w środowisku produkcyjnym baza powinna znajdować się w dedykowanym do tego serwerze.

4.2. Strona internetowa

Do stworzenia strony zdecydowano się użyć frameworku Angular 8. Serwowana będzie ze środowiska uruchomieniowego Node.js. Projekt zbudowany jest z osobnych modułów dla każdej funkcjonalności. Widoki składane są z komponentów — są to elementy zawierające szablon



Legenda:

Połączenie z zewnątrz

Połączenie korzystające z wewnętrznej sieci dockerowej

Komunikacja pomiędzy kontenerami

Połączenie pomiędzy dockerem a systemem operacyjnym

Rys. 4.1: Architektura fizyczna aplikacji

HTML, style CSS oraz logikę i dane w klasie napisanej w języku typescript. Dodatkowo komponenty mogą korzystać z serwisów. Serwisy to specjalne klasy, które są wstrzykiwane jako zależności (ang *Dependency injection*). Zawierają się w nich dane oraz logika dzielone między wieloma komponentami. Nawigacja pomiędzy poszczególnymi widokami odbywa się przy pomocy dedykowanego routera, który przechwytuje nawigację przeglądarki. Dzięki temu nawet

nawigacja do tyłu nie powoduje przeładowania całej strony tylko poszczególnych zmienionych elementów.

Do budowy widoków użyta zostanie biblioteka Angular Material, która zawiera często wykorzystywane elementy zbudowane zgodnie z oficjalną specyfikacją *Material design*.

Taka modularna architektura pozwala na wielokrotne używanie tych samych komponentów oraz na zachowanie czytelnej struktury kodu.

4.3. Serwis API

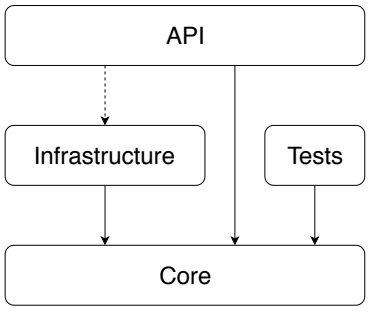
Projekt podzielony zostanie na trzy warstwy:

Api warstwa obsługująca zapytania GraphQL

Core warstwa domenowa definiująca modele encji, serwisy oraz interfejsy, z których korzysta warstwa Api

Infrastructure warstwa implementująca interfejsy oraz obsługująca dostęp do bazy danych

Podział ten znany jest jako „czysta architektura" (ang. *Clean architecture*). Schemat ten przedstawiony został na rysunku 4.2, gdzie linie ciągłe oznaczają zależności na etapie budowania, natomiast linia przerywana oznacza zależność po uruchomieniu. Taki układ umożliwia umieszczenie logiki biznesowej oraz modelu aplikacji w centrum (Core). W ten sposób infrastruktura oraz szczegóły implementacji są zależne od Core, a nie na odwrót — odwrócenie zależności. Warstwa API pracuje na interfejsach zdefiniowanych w Core i nie zna ich implementacji w Infrastructure. Implementacje te są podłączane dopiero po uruchomieniu poprzez wstrzykiwanie zależności. Istotną zaletą takiej architektury jest również możliwość testowania każdej funkcjonalności z osobna.



Rys. 4.2: Schemat czystej architektury użyta w projekcie

Na platformie .Net Core dostępne są dwie aktywnie rozwijane biblioteki implementujące GraphQL: *GraphQL .NET* oraz *Hot Chocolate*. Mimo znacznie mniejszej popularności wybrana została biblioteka *Hot Chocolate*, ponieważ prezentuje wiele możliwości automatyzacji generowania schematu GraphQL oraz analizowania zapytań.

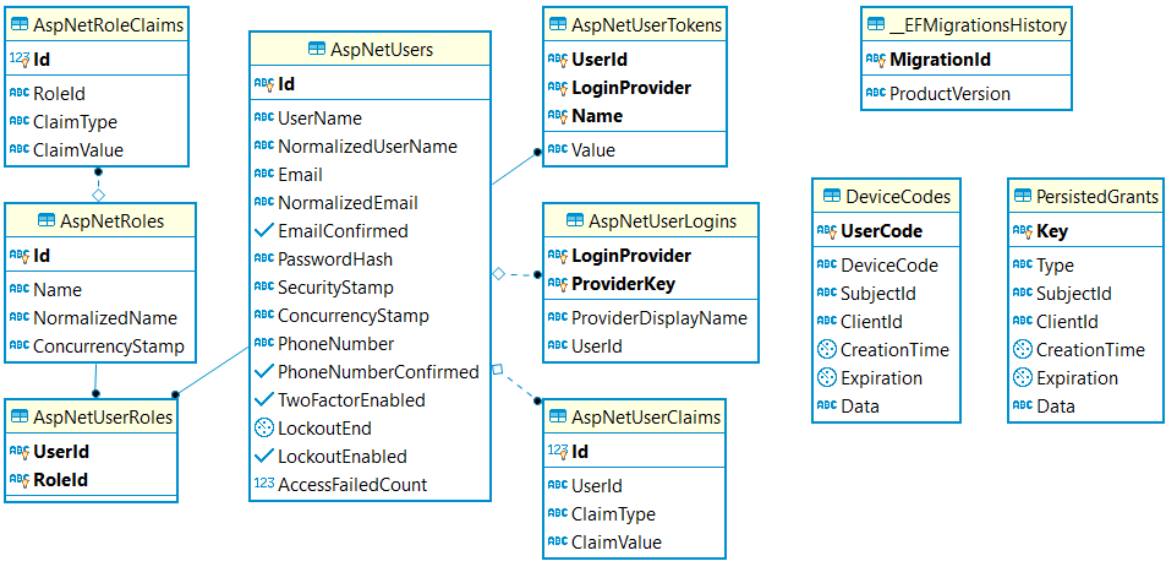
Z racji tego, że GraphQL jest protokołem służącym do przesyłania danych, jest on zaimplementowany w najwyższej warstwie serwisu – Api. W związku z tym nie zawęża sposobu implementacji zapisu danych w warstwie infrastruktury, a więc nic nie stoi na przeszkodzie, aby użyć relacyjnej bazy SQL. Takie rozwiązanie umożliwia wykorzystanie zalet relacyjnych baz - integralność i niezależność danych, jednocześnie oferując grafowy odczyt danych poprzez GraphQL.

4.4. Baza danych

Baza danych stworzona zostanie w systemie zarządzania relacyjną bazą danych PostgreSQL. Jest to open source'owe oprogramowanie, obecnie jeden z najlepiej rozwiniętych RDBMS-ów.

Baza z kontami użytkowników (rys. 4.3) zostanie wygenerowana za pomocą platformy Identity. Tabele te przechowują podstawowe dane kont użytkowników takie jak login, hasz hasła czy email. Zawierają się tu również role oraz ich upoważnienia (opisane szerzej w rozdziale). Oprócz danych użytkowników zapisywane są również dane związane z migracjami bazy zarządzane przez *Entity Framework* oraz dwie pomocnicze tabele biblioteki *IdentityServer4* (*DeviceCodes* i *PersistedGrants*).

Dodać ref do rozdziału o Identity



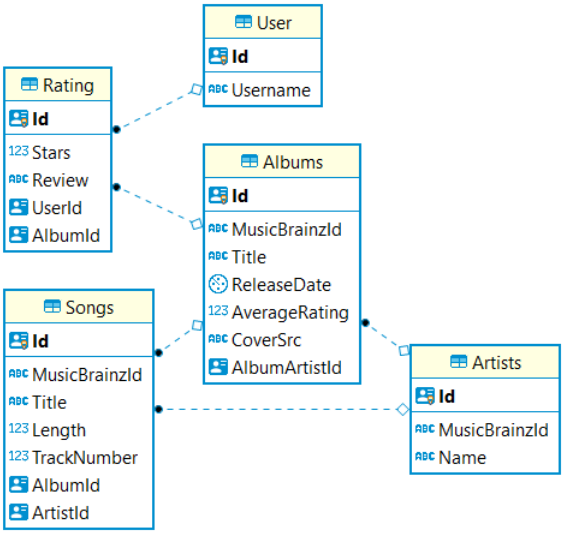
Rys. 4.3: Schemat ERD bazy z kontami użytkowników

Rysunek 4.4 przedstawia bazę przechowującą główne dane aplikacji. Przechowywana jest minimalna ilość danych wymagana do zaimplementowania wersji konceptualnej aplikacji. Jeśli aplikacja miałaby zostać wdrożona, z konieczne byłoby dodanie większej ilości danych. Tabele połączone są relacjami umożliwiającymi grafową reprezentację. Baza ta również została wygenerowana metodą code first za pomocą *Entity Framework*.

4.5. Uwierzytelnianie i autoryzacja

Jako protokół uwierzytelniania wybrano OpenID Connect. Standard ten rozszerza OAuth2 (służący do autoryzacji) o warstwę identyfikacji użytkowników. Jest obecnie jednym z najbezpieczniejszych standardów uwierzytelniania. Zaimplementowany zostanie przy pomocy biblioteki *IdentityServer4* na platformie *ASP.Net Core 3.0*. Użytkownik po zalogowaniu otrzyma token JWT, który będzie zawierał cyfrową sygnaturę. Dzięki temu jakakolwiek ingerencja w jego strukturę sprawi, iż jego walidacja zakończy się niepowodzeniem.

Dla zapewnienia najwyższego standardu bezpieczeństwa zaimplementowany zostanie proces logowania z wykorzystaniem kodu PKCE (ang. *Proof Key for Code Exchange*), opisany w dokumencie RFC 7636 [4]. Stanowi on udoskonalenie przepływu wykorzystującego kod autoryzacji (ang. *Authorization Code Flow*). Zabezpiecza przed próbami przechwycenia kodu autoryzacji przez złośliwą aplikację, która mogła by za pomocą tego kodu uzyskać token dostępowy (ang. *Access Token*).

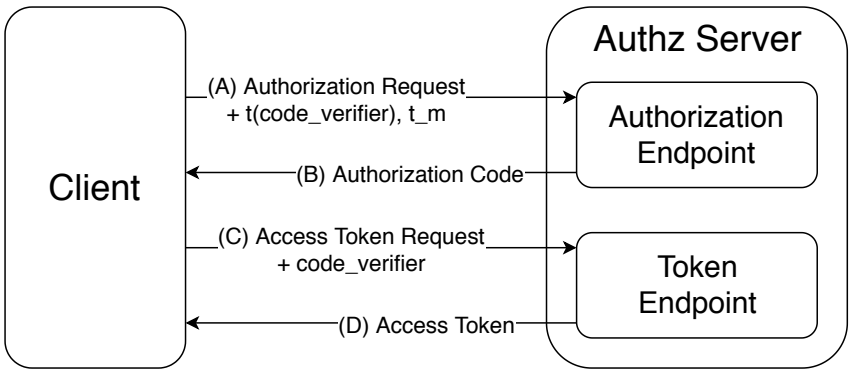


Rys. 4.4: Schemat ERD bazy z głównymi danymi

Proces uzyskania tokenu dostępowego, przedstawiony na schemacie 4.5, jest następujący:

A. Klient tworzy losowy klucz `code_verifier` i przekształca go za pomocą metody transformacji `t_m`. Następnie przesyła przekształcony klucz wraz z metodą transformacji w żądaniu autoryzacji OAuth 2.0.
B. Jeśli użytkownik zalogował się poprawnymi danymi, serwer zapisuje parametry weryfikacji i zwraca kod autoryzacji.
C. Aby uzyskać token dostępowy, klient przesyła kod autoryzacji wraz z oryginalną wartością `code_verifier` wygenerowaną w punkcie (A).
D. Serwer autoryzacji przekształca `code_verifier` za pomocą metody `t_m` i porównuje z wartością `t(code_verifier)` otrzymaną w punkcie (B). Jeśli są równe, serwer zwraca token dostępowy.

W ten sposób nawet jeśli kod autoryzacji w punkcie (B) zostanie przechwycony, nie będzie mógł zostać wykorzystany bez znajomości klucza `code_verifier`.



Rys. 4.5: Schemat procesu logowania z użyciem PKCE

Rozdział 5

Implementacja

5.1. Docker

5.2. Strona internetowa

5.2.1. Zastosowane technologie

Zgodnie z projektem, strona stworzona została w Angularze. Oprócz podstawowych bibliotek Wykorzystane zostały następujące biblioteki:

apollo — wiodący klient GraphQL. Oprócz implementacji protokołu GraphQL, zapewnia również zarządzanie pamięcią podręczną (ang. *cache*) oraz stanem aplikacji (ang. *state management*). Dzięki temu wszystkie wszystkie odpowiedzi z serwisu Api są zapamiętywane, co pozwala na stworzenie aplikacji działającej szybko nawet przy słabym połączeniu z internetem.

flex-layout — biblioteka stworzona przez zespół tworzący Angulara, umożliwiająca stworzenie responsywnego interfejsu. Dostarcza API, które pozwala na definiowanie struktury elementów HTML zależnej od rozmiaru ekranu. Dzięki temu interfejs automatycznie dostosowuje się np. do ekranu telefonu komórkowego.

oidc-client — biblioteka implementująca protokół OpenID Connect oraz OAuth2. Zapewnia klasy obsługujące proces logowania oraz zarządzania tokenami.

rxjs — ReactiveX

5.2.2. Klient GraphQL

5.2.3. Połączenie z Last.fm

5.2.4. Responsive design

5.2.5. Przykładowy moduł

dodawanie recenzji

5.3. GraphQL API

5.3.1. Zastosowane technologie

Hot Chocolate
Autofac

Entity Framework Core
Namotion.Reflection
Serilog

5.3.2. Warstwa Api

5.3.3. Warstwa domenowa

5.3.4. Warstwa infrastrukturalna

5.4. Serwis uwierzytelniający

5.4.1. Zastosowane technologie

Oprócz opisanych wcześniej *Entity Framework Core* oraz *Serilog* wykorzystane zostały:

IdentityServer4
AspNetCore.Identity

5.4.2. Proces rejestracji i logowania

5.4.3. Autoryzacja dostępu do API

5.5. Baza danych

5.6. Odwrócone proxy

Literatura

[1] GraphQL | A query language for your API. https://graphql.org. dostęp dnia 17 listopada 2019.

[2] GraphQL Spec, Czwerwiec 2018. https://graphql.github.io/graphql-spec/June2018. dostęp dnia 17 listopada 2019.

[3] HATEOAS - Wikipedia. https://en.wikipedia.org/wiki/HATEOAS. dostęp dnia 17 listopada 2019.

[4] RFC 7636 - Proof Key for Code Exchange by OAuth Public Clients. https://tools.ietf.org/html/rfc7636. dostęp dnia 17 listopada 2019.

[5] XML Soap. https://www.w3schools.com/xml/xml_soap.asp. dostęp dnia 17 listopada 2019.

[6] E. Porcello, A. Banks. *Learning GraphQL.* O'Reilly Media, 2018.

[7] L. Richardson, M. Amundsen. *RESTful Web APIs*. O'Reilly Media, 2013.

[8] D. Tidwell, J. Snell, P. Kulchenko. *Programming Web Services with SOAP*. O'Reilly Media, 2001.

Spis rysunków

Dodatek A

Opis załączonej płyty CD/DVD

Tutaj jest miejsce na zamieszczenie opisu zawartości załączonej płyty. Należy wymienić, co zawiera.