Planung und Erstellung einer Backend-Microservices-Architektur aus den Anforderungen durch das Spiel Stirnraten.

Michael Rothkegel

24. Juni 2019

Inhaltsverzeichnis

1 Glossar

Das ist der:
enter

Begriff	Erklärung
Deployen	Ein Softwareprodukt updaten.
Hosten	Ein Softwareprodukt auf einem Server bereitstellen. Dafür stehen heutzutage viele Möglichkeiten bereit, vom eigenen Server, gemieteten Servern oder Cloudlösungen (Azure, AWS, Google Cloud)
CI/CD	Continuous Integration/Continuous Delivery beschreibt den kontinuierlichen Prozess ein Softwareprodukt von der Entwicklung bis zur tatsächlichen Veröffentlichung zu begleiten. Dies sollte automatisch funktionieren, schnell gehen und leicht auszuführen sein.
User Interface	Oberfläche für Benutzer
VM	Virtuelle Maschine, Kapselung eines Rechnersystems innerhalb eines anderen
Legacy	Es handelt sich um Altsysteme, die eine Erneuerung benötigen oder abgelöst werden müssen. Das kann verschiedene Gründe haben, wie z.B. schlechte Programmierung, Fehlentscheidungen oder technologische Veraltung
Technologiestack	
Overhead	
Downtime	Zeitpunkt, die eine Anwendung benötigt, bis sie neugestartet ist. Während der Downtime ist eine Anwendung nicht erreichbar.
technische Schuld	
Monolith	monolitsche Struktur
Microservice	Service
Domain Driven Design (DDD)	
Bounded Contexts	
up-stream	
down-stream	
Pattern	
REST	
Monitoring	
Deployment	
Logging	
Traffic	
Timeout	
Fallback	
Route	

Eventbus
Subscriber/subscribe
publish
Message Broker
Load Balancer
REST
Backend
Performance
Latenz
Middleware

Tabelle 1: Glossar

2 Einleitung

- Ziel: Muss erwähnt werden: Lokale Datenhaltung in den Apps ablösen.

3 Grundlagen

Hier erklären was kommt

3.1 Microservices

Für den Begriff Microservices existiert keine einheitlich anerkannte Definition. Während Wolff unter Microservices unabhängig, deploybare Module versteht[30], spricht Newman von kleinen, autonomen Services, die zusammenarbeiten. Cockcroft verwendet den Begriff Microservice gekoppelt mit einem Architekturbegriff: Eine Microservice Architektur sind gekoppelte Services, welche für einen gewissen Kontextbereich zuständig sind.[9] D.h. jeder Service behandelte gewisse, fachliche Aufgaben und kann genau für diese genutzt werden. Eine Vielzahl von solchen Services bildet dann die gesamte Anwendung.

Amudsen schreibt dem Microservice an sich die Eigenschaft zu, dass er unabhängig zu anderen Microservices sein muss, d.h. ein Microservice kann losgelöst von anderen geupdated (deployed) werden. Weiter ist ein Microservice wie schon bei Cockcroft für einen gewissen Aufgabenbereich zuständig. Eine Microservice-Architektur ist ein zusammenschluss von miteinander kommunizierenden Microservices.[9]

In *Flexible Software Architecture*[31] werden Microservices zu den bisherigen noch weitere, teils technische Eigenschaften zugeschrieben: Microservices sind technologisch unabhängig, d.h. eine Microservice Architektur ist beispielsweise nicht an eine bestimmte Programmiersprache oder Datenbank gebunden. Weiter müssen Microservices einen privaten Datenspeicher haben und sie kommunizieren mit anderen Services über das

Netzwerk (z.B. über REST). Ebenfalls werden Microservices verwendet, um große Programme in kleine Teile zu unterteilen. Diese kleine Teile lassen sich automatisch bauen und deployen.

Basierend auf den folgenden Definitionen wird der Microservice Begriff wie folgt verwendet: Microservices sind

- klein in der Größe
- kommunizieren mit anderen Services über Netzwerkschnittstellen (z.B. REST) sind unabhängig voneinander deploybar
- können unabhängig voneinander entwickelt werden (d.h. Microservice A muss nicht auf B,C,D ... warten und/oder umgekehrt)
- eingeschränkt in ihrer Geschäftslogik, d.h. ein Microservice kümmert sich immer um einen speziellen Kontext, der im vorhinein definiert werden muss
- dezentral, d.h. sie können auf unterschiedlichsten Plattformen gehosted werden werden automatisch gebaut und deployed

Abschließend handelt es sich um eine Microservice-Architektur, wenn viele Microservices nach Definition verwendet werden.

3.2 Monolithische Struktur

Eine monolithische Struktur ist ein einziges Softwareprogramm (Monolith), welches in sich geschlossen ist. Dies bedeutet im Detail, dass ein Monolith aus mehreren Ebenen besteht auf die über Schnittstellen zugegriffen werden kann. Innerhalb der Ebenen werden Komponenten wie z.B. Frameworks oder selbstgeschriebene Klassen eingebunden und verwendet.[1] Durch die sich aufeinander aufbauenden Ebenen folgt daraus, dass sämtliche Geschäftslogiken, User Interfaces sowie die Datenbank und Datenbankzugriffe Abhängigkeiten haben. All dies ist in einem Programm vereint.[1] Natürlich kann die monolithische Struktur innerhalb noch einmal Modular sein. In einem Monolithen existierten also ggf. mehrere Module, welche verschiedene Geschäftslogiken abbilden oder ein Modul, welches nur zum Erstellen einer grafischen Oberfläche verwendet wird. Dennoch können diese Module nicht unabhängig von der gesamten Anwendung deployed werden.[14]

Abbildung 1 zeigt eine vereinfachte Gegenüberstellung der beiden Architekturen. Die App 1 ist in drei klassische Funktionen (Web, Business und Data) unterteilt. Die Skalierung (2) kann durchgeführt werden, in dem App 1 über mehrere Server oder VMs geklont wird.

Bei der Microservice Architektur werden die Funktionen auf unterschiedliche Dienste aufgeteilt. Konkreter könnte dies bedeuten, dass App 1 bei (3) zuständig für eine Benutzerkontoverwaltung ist und App 2 für ein Abrechnungssystem. Die Microservices (4) werden nicht geklont, sondern können unabhängig voneinander bereitgestellt werden.

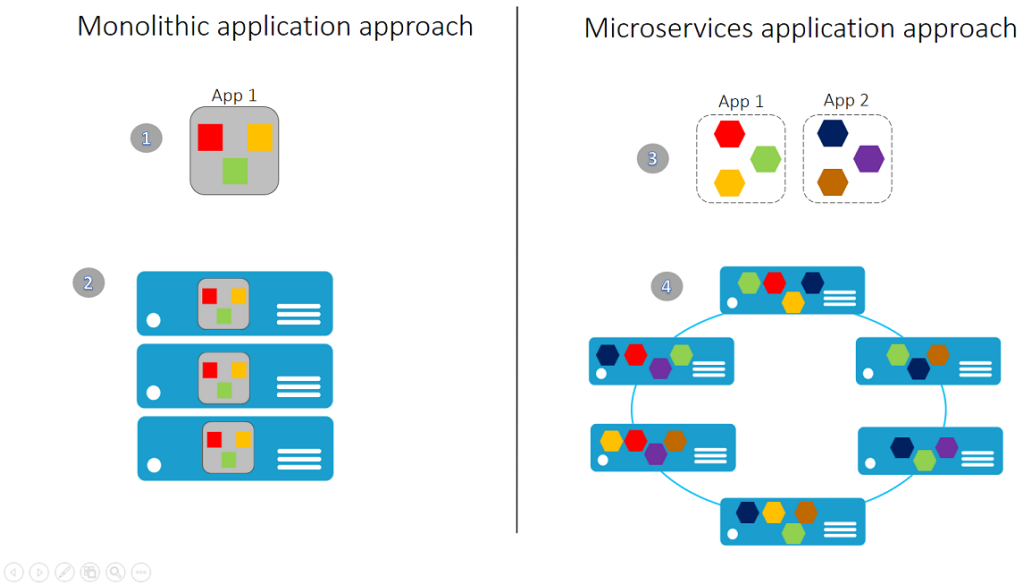

Abbildung 1: Monolith und Microservice-Architektur.[1]

3.3 Monolith vs. Microservices

Aus den vorherigen Abschnitten sind diverse Unterschiede zwischen den Architekturen erkennbar. Nun gilt es festzustellen, für welche Problemstellungen, welche Architektur sinnvoller ist. [31] [3]

Aus der Tabelle ergeben sich verschiedene Punkte: Der Monolith eignet sich besonders dann sehr gut, wenn die Projekt- sowie Teamgrößen absehbar sind und auch die Technologie entschieden ist. Zusätzlich kann es beim Projektanfang ein Vorteil sein, da die Abhängigkeiten innerhalb des Projektes liegen und so Entwicklungsgeschwindigkeit nicht durch komplizierte Infrastrukturen blockiert wird. Ist die Projektgröße allerdings nicht absehbar, treten früher oder später mehrere Schwierigkeiten auf: Zum einen bindet der am Anfang des Projektes festgelegte Technologiestack und die Nutzung oder der Austausch neuer Technologien sind in der Regel mit sehr viel Arbeit verbunden. Des Weiteren führen die anfangs eingegangen Abhängigkeiten zu problemenen im Deployment (A kann erst updaten, wenn B soweit ist) und einem erhöhten Aufwand in der Kommunikation zwischen den Teams (A kann erst beginnen, wenn B xy erledigt hat).

Zusätzlich ist die Skalierung von Microservices unabhängiger. Es können sich feingranular Services gesucht werden, welche skaliert werden sollen. Diese benötigen nicht zwingend mehr Hardware (vertikale Skalierung), sondern könnten z.B. auch auf verschiedene Server verteilt werden (horizontale Skalierung). Dies ist bei einem Monolithen natürlich auch möglich, dennoch muss immer der ganze Monolith skaliert werden, welcher zum einen immer mehr Hardware als einzelne Microservices benötigt und zum anderen auch durch die Komplexität in der Regel auch schwerer zu skalieren ist.[30] Als abschließender Punkt ist die Robustheit zu erwähnen: Wenn ein Microservice einen Fehler enthält,

	Monolithische Architektur	Microservice-Architektur
Abhängigkeiten	alles in einer Anwendung	entkoppelt, da Prinzip von Modularisierung verwendet wird
Größe	linear steigend	einzelne Services sind klein
Geschwindigkeit Zugriffe	schnell, da alles in einer Anwendung	Zugriffe können länger dauern
Deployment	schwieriger desto größer das Projekt, aufgrund von • Abhängigkeiten • Größe	einfach, da Microservices • klein und • modular sind
Organisation	leichter, da alles an einem Ort	schwerer, da mehr Domänenlogik (wer macht was?) beachtet werden muss
Legacy-Systeme ablösen	ggf. schwierig, da System sehr verzahnt miteinander	leicht, da Microservices durch neue abgelöst werden können
Technologie	beschränkt	vielfältig
Nachhaltige Entwicklung	wartbar mit Einschränkungen	leicht wartbar
Robustheit	weniger, da ganzes System bei schweren Fehlern abstürzt	sehr, da im Zweifel immer nur ein Service abstürzt
Skalierung	horizontale und vertikale Skalierung, Umsetzung kann sehr komplex werden	horizontale und vertikale Skalierung
Betrieb	nur ein System	komplex, da mehr Services verwaltet werden müssen

Tabelle 2: Monolitih vs. Mircoservice-Architektur

stürzt dieser im schlechtesten Fall ab. Im besten Fall übernimmt dieser Service eine weniger wichtige Funktion und der Nutzer bemerkt den Ausfall noch nicht einmal. Beim Monolithen dagegen stürzt die gesamte Anwendungen ab. In der Regel startet so eine Anwendung automatisch neu, jedoch ist betrifft die Downtime alle Nutzer.

Aus den genannten Punkten lässt sich schließen, dass eine generelle Aussage, ob eine monolithische oder Microservice-Architektur besser oder schlechter ist, sich nicht treffen lässt. Es kommt immer drauf an, welche Zielsetzung und wie viele Ressourcen für das Projekt festgelegt sind. REWE Digital beispielsweise hat ihr Produkt zuerst als Monolithen gestartet und ist erst später auf eine Microservice-Architektur umgeschwenkt.[7] Zwei mögliche Gründe könnten dafür sein, dass zum einen ein lauffähiges Produkt schneller mit einer monolithischer Struktur zu erreichen ist, zum anderen ist nicht gegeben, ob ein entwickeltes Projekt überhaupt die Nachfrage erzeugt, so dass eine Microservice-Architektur notwendig ist. Dementsprechend muss abgewogen werden, welche Architektur für welchen Anwendungsfall besser geeignet ist.[30]

3.4 Architektur von Micrsoservices

Wie bereits erwähnt, ist die Entkopplung von Microservices ein großer Vorteil gegenüber dem Monolithen. Dennoch ist es sinnvoll Richtlinien, Regeln und/oder Festlegungen zu schaffen, damit die Microservices nicht blockierend oder technologisch unnötig gegensätzlich arbeiten. Die Entscheidungsebene kann global (Makroarchitektur) oder nur für einen einzelnen Services (Mikroarchitektur) gelten.[31] Welche Festlegungen und mit welcher Strenge diese eingehalten werden müssen, hängt von verschiedenen Faktoren ab, welche technologisch, organisatorisch oder wirtschaftlich motiviert sein können.[7]

In dem folgenden Abschnitt wird das Grundprinzip der Software-Modellierungs-Methodik Domain Driven Design untersucht. Zusätzlich wird erläutert, welche Fälle makro- oder microarchitektonisch einzuordnen sind.

3.4.1 Domain Driven Design

Domain Driven Design (DDD) ist ein Vorgehen mit dem ein Softwaresystem modelliert werden kann. Im Sinne einer Microservice-Architektur kann dies als Werkzeug genutzt werden, um Microservices fachlich einzuteilen.[20] Beim sogenannten *Strategic Design* wird dafür das Softwaressytem in verschiedene *Bounded Contexts* eingeteilt, welche an ein *Domänenmodell* gebunden sind. Ein Domänenmodell bildet die Geschäftslogik ab, d.h. inwiefern einzelne Objekte innerhalb des Kontexts in Relation zueinander stehen, welche Eigenschaften sie haben und wie sich verhalten. Dabei kann ein Domänenmodell - je nach Entwurfsmuster - von einem oder mehreren Bounded Contexts genutzt werden.[30]

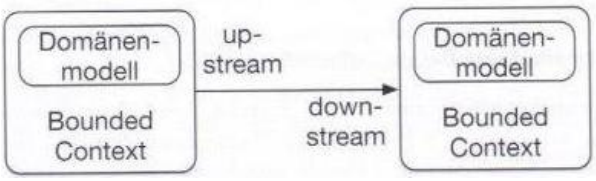

Abbildung 2: Bounded Contexts mit eigenständigem Domänenmodell.[30]

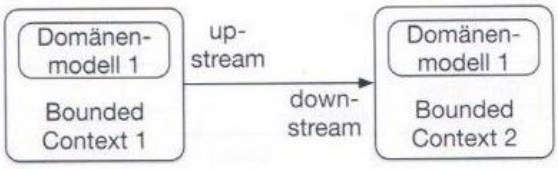

Abbildung 3: Bounded Context 2 adaptiert das Domänenmodel von Bounded Context 1.[30]

Wolff verdeutlicht das Prinzip von Bounded Contexts mit Hilfe von vier Microservices, welche einen Onlineshop repräsentieren: *Suche*, *Check Out*, *Inkasso* und *Lieferung*. Während das Datenmodell der Suche detaillierte Informationen über die Produkte enthält, reicht es im Warenkorb (hier Check Out), wenn ggf. nur der Produktname gespeichert wird. Bei Inkasso ist es ähnlich: An dieser Stelle sind Zahlungsdaten des Benutzers relevant, während bei Lieferung die ggf, nur Adresse notwendig ist.[30] An diesem Beispiel wird deutlich, dass zwar von selben Begrifflichkeiten wie Benutzer, Produkt usw. gesprochen wird, allerdings jeder Service sein eigenes Domänenmodell hat. Durch diese Technik, was dabei hilft, eine saubere Microservice-Architecktur zu erstellen.[30] [20]

Neben der fachlichen Trennung bildet DDD auch die Kommunikation zwischen Kontexten ab. Dabei wird grundsätzlich vom *up-stream* (vorgeschaltet) und dem *down-stream* (nachgeschaltet) gesprochen.[30]. Der up-stream stellt dem down-stream Informationen bereit. Wie dies technisch umgesetzt ist, also ob der down-stream nachfragt oder der up-stream aktiv Daten schickt, ist frei wählbar.

Nach dem Anwenden von DDD sollte die Struktur der Software erkennbar sein: D.h. welche Art Microservices werden benötigt und iwiefern sie mit anderen in Abhängigkeiten bzw. Kommunikation stehen.

3.4.2 Macro- und Mikroarchitektur

Wenn durch das DDD entworfen wird, welche Microservices voraussichtlich benötigt werden, ist es sinnvoll einen Art Bauplan zu verfassen, welcher impliziert, an welche Regeln sich ein Microservice halten muss. Diese Regeln können wie bereits erwähnt auf globaler Ebene getroffen werden, d.h. sie gelten für alle Services (Makroarchitektur) oder sie gelten nur im Microservice selber (Microarchitektur). REWE Digital unterscheidet dabei zwischen *Must*, *Should*, *Could*. D.h. es gibt Regeln, die Microservices erfüllen müssen wie

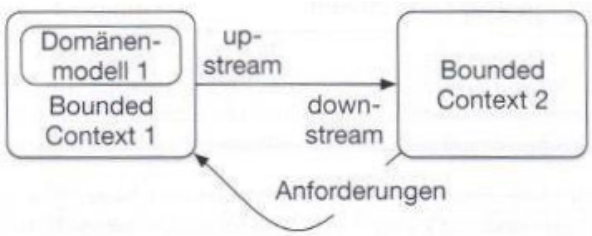

Abbildung 4: Bounded Context 2 erhält ein auf ihn zugeschnittenes Domänenmodel von Bounded Context 1.[30]

z.B. das Kommunzieren über REST oder das Implementieren eine einheitlicher Autorisierung.[7] Andere Regeln dagegen sind viel mehr Richtlinien (should) oder komplett optional (could). Das Ziel ist stets, dass durch die makroarchitektonischen Entscheidungen nicht die Vorteile von Microservices beschnitten werden.[30][9].

Es gibt verschiedene Einflussfaktoren wie sich die Makroarchitektur für ein Unternehmen definiert: Zum einen empfiehlt es sich ein Gremium zu gründen, welches sich stetig mit den Regeln der Makroarchitektur auseinandersetzt, sie entsprechend erweitert, überarbeitet und die getroffenen Entscheidungen auch immer begründen kann.[30] Zum anderen besteht immer ein technischer Einfluss[30]:

- Gewählte Technologien müssen in die Infrastruktur des Unternehmens passen: Angenommen die Auslastung eines Microservices muss überwacht werden und dies wird firmenweit mit Tool A erledigt, dann wäre es sehr aufwendig, wenn der besagte Service nur eine Schnittstelle für Tool B anbietet und der nächste Service nur für Tool C. Dies würde einerseits sehr unübersichtlich werden und andererseits viel Aufwand bedeuten.

- Technologien sind immer von dem Personal abhängig: Gerade wenn Unternehmen klein bis mittelständig sind, emphielt es sich Technologien zu nutzen, die mehrere Entwickler beherrschen, um Inselwissen zu reduizieren.

- Ebenfalls können gezielt strategische Entscheidungen getroffen werden, z.B. wenn ein Unternehmen die Dateninfrastruktur zu einem Cloudanbieter auslagern möchte, hat dies entsprechende makroarchitekonisches Auswirkungen.

Basierend auf Wolff und Nadareishvili ist folgende Tabelle entstanden, welche einen Überblick darüber gibt, wie gängige Entscheidungspunkte einzuordnen sind. [30][9][7]

In der Tabelle sieht man, dass gerade die ersten Punkten sehr von der Unternehmenskultur und den technischen sowie personellen Freiheiten abhängt. In der Theorie sollte die Programmiersprache sinnvoll für jeden Microservices gewählt werden, dennoch ergibt es auch Sinn einen Pool an Programmiersprachen auf Makroebene zu definieren, um Inselwissen zu reduzieren und nachhaltige Codequalität zu gewährleisten. Ähnliches gilt beispielsweise für die Wahl der Datenbank: Ist bereits eine globale Infrastruktur für Datenbank X geschaffen, sollte diese nicht ohne weiteres aufgebrochen werden, nur weil

	Mikroarchitektur	Makroarchitektur
Programmiersprache	x	x
Datenbank	x	x
Look and Feel (UI)	x	x
Dokumentation	x	x
Datenformat		x
Kommunikationsprotokoll		x
Authentifizierung		x
Integrationtests		x
Autorisierung	x	
Unittests	x	
Continuous-Delivery-Pipeline	x	

Tabelle 3: Entscheidungen Micro- und Macroarchitektur

es technisch möglich ist.

Bei der Dokumentation sowie beim Look & Feel ist es sinnvoll, globale Richtlinien zu definieren, damit klar ist, wo bei jedem Microservices die Dokumentation zu finden ist oder wie ein User Interface grundsätzlich angeordnet und gestaltet werden soll. Dennoch können diese Punkte im Detail je nach Microservice abweichen.

Ein Kommunikationsprotokoll (z.B. REST) sowie Datenformate (z.B. JSON) sollten festgeschrieben werden.[7] [30] Als Grund wird zum einen das Vermeiden von technischen Mehraufwand angegeben, zum anderen sind Microservices zwar eigenständig deploybare Einheiten, dennoch sollten sie technisch zum Gesamtsystem passen und nicht dagegen arbeiten.

Während die Authentifzierung (um wen handelt es sich) einmalig festgelegt werden sollte, liegt die Überprüfung der Autorisierung (was darf der Benutzer) in jedem Microservice selbst. Die Alternative wäre, dass jede eingehende Anfrage noch einmal geprüft wird, was zu unnötig hohem Traffic und Verzögerungen führen würde.

Die hier erarbeitete Tabelle ist an dieser Stelle nicht als feststehendes Manfifest für alle Unternehmen zu verstehen, sondern als neutral betrachtete, sinnvolle Einordnung. Natürlich können architektonische Entscheidungen stark vom jeweiligen Anwendungszweck abhängen.

Die Tabelle zeigt lediglich allgemeine Beispiele und ist nicht als vollständig zu betrachten. Nicht aufgeführt ist beispielsweise der Umgang mit Konfigurationsdateien, Monitoring oder Logging. Dies liegt unter anderem daran, weil es auf Projekte oder von dem

Microservice abhängt: Beim Monitoring könnte zum Beispiel global entschieden werden, *wo* Metriken abgelegt werden bzw. mit *welcher* Technologie gearbeitet wird. Aus microarchitektonischer Sicht könnten die Services selbst entscheiden, *was* gemessen wird.

Ebenso beim Deployment: Es gibt zahlreiche Methoden, um neue Updates bereitzustellen wie z.B. mittels Docker, Kubernetes oder indivudelle Installationsskripte.[30] Welche Technologie sich durchsetzt, muss anhand der Anforderung entschieden werden.

Aus den erarbeitenten Punkten lassen sich Vor- und Nachteile ableiten, zwischen denen abgewogen werden muss. Vorteile für microarchitektonische Entscheidungen sind ein sehr hohes Maß an Flexibilität und eine hohe Unabhängigkeit im Gesamtsystem, was grundsätzlich das Ziel von Microservices ist. Dies wiederum kann dazu führen, dass Entwicklungsoverhead oder Inselwissen entsteht. Ebenfalls könnten Punkte wie z.B. das *Look & Feel* oder die *Dokumentation* darunter leiden.

Macroarchitektonische Entscheidungen haben zum Vorteil, dass es Regeln gibt, welche die Entwicklung vereinfachen sollen und gegebenfalls die Nachteile der Microarchitektur kompensieren können. Auf der anderen Seite schränken macroarchitekonische Entscheidungen ein. Zusätzlich müssen sie organisch, z.B durch ein extra dafür geschaffenes Gremium, durchgesetzt und werden.[30] Im Gesamten lässt sich daraus schließen, dass sehr genau abgewogen werden muss, welche Entscheidungen global oder individuell entschieden werden. Grundsätzlich gilt, dass jede Entscheidung begründbar sein muss.

3.5 Kommunikation

Bei einem Monolithen wird eine Abfrage über eine Route gestellt, woraufhin die Anwendung entsprechend mit der Bearbeitung beginnt. Da die gesamte Datenhaltung an einer Stelle ist, sind alle Daten bekannt und abrufbar. Wichtiger noch: Die Daten sind konsitent.

Microservices sind diesbezüglich herausfordernder. Es müssen verschiedene architektonische Entscheidungen getroffen werden, wie z.B. ob es einen zentralen Service gibt, welcher alle Anfragen weiterleitet (**API Gateway**) oder ob jeder Service einzeln erreichbar ist. Ebenfalls sollte auch begründbar entschieden werden, ob eine synchrone, asynchrone oder möglicherweise eine hybride Kommunikation verwendet wird.

In den folgende Unterkapiteln werden Vor- und Nachteile der verschiedenen Kommunikationsarten für Microservices mit einem Schwerpunkt auf Unabhängigkeit (Entkopplung) und Datenkonsitenz untersucht.

3.5.1 Synchrone Kommunikation

Wenn ein Microservice bei der Bearbeitung einer Anfrage selbst eine weitere Anfrage an einen anderen Microservice stellen muss und auf das Ergebnis wartet, spricht man von synchroner Kommunikation.[30]

Anhand dieser Definition lässt sich folgendes Szenario darstellen (siehe Abbildung 5).

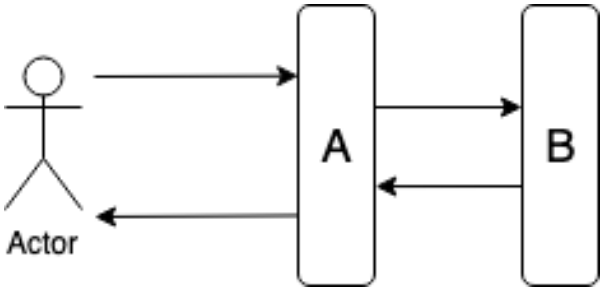

Abbildung 5: Synchrone Kommunikation

Der Actor fragt bei Microservice A an, welcher diese Anfrage bearbeitet und schließlich an B weiterleitet. B verarbeitet die Anfrage und antwortet, schließlich kann auch A antworten. Aus diesem Ablauf lässt sich festhalten, dass die übertragenden Daten aktuell sind. D.h. der Actor erhält definitiv konsistente Daten, was positiv zu vermerken ist. Problematischer dagegen ist die Abhängigkeit, welche entsteht. Sollte B nicht erreichbar sein, läuft A in einen Timeout und ist blockiert. Einerseits ließe sich argumentieren, dass genau dies passieren soll, schließlich scheint es einen Fehler zu geben. Aber angenommen A wäre ein Service zum Erstellen von Rechnungen und B ein Service zum Sammeln von Daten. A möchte B infomieren, dass eine Rechnung erstellt wurde, ist aber blockiert. Die Operation eine Rechnung zu erstellen hätte höhere Priorität als es statisch zu erfassen. Nach den aufgestellen Definitionen aus 3.3 für Microservices wird die Entkopplung, Modularität und Robustheit des Systems verletzt, da A nicht weiterarbeiten kann.[30] [12]

Bläht man das Beispiel auf, so dass weitere Services statistische Daten erfassen wollen, würden zahlreiche Microservices ausfallen (siehe Abbildung 6).

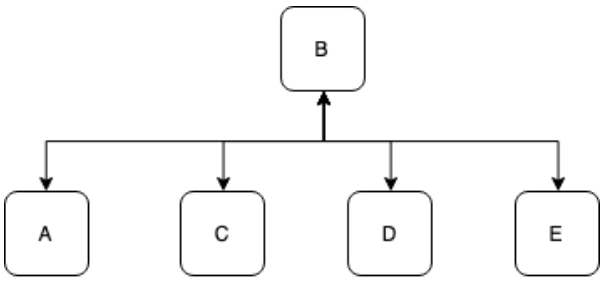

Abbildung 6: Abhängigkeiten in synchroner Kommunikation

Die Microservices können auch nicht auf eine Notfallstrategie (**Fallback**) zurückgreifen. Angenommen wenn Serivce B nach x Sekunden nicht erreichbar ist, wird die ursprüngliche Abfrage durch A weiter abgearbeitet, um nicht zu blockieren. Nun müsste eine andere Logik dafür sorgen, dass die Daten, die nicht übertragen werden konnten,

zu einem anderen Zeitpunkt übertragen werden. In diesem Moment herrscht keine Konsistenz mehr vor, was aber ein großer Vorteil an synchroner Kommunikation ist.

Betrachtet man das Beispiel andersherum und nimmt an, dass jeder Service seine Datenhaltung soweit aufspreizt, dass jeder Service die Statistiken führt, ist es nur eine Frage der Zeit, bis weitere Felder gespeichert werden müssen. Überspitzt formuliert, würde jeder Service alles speichern, was gegen die Absicht von Bounded Contexts arbeiten würde.[30]

Auch nicht zu vernachlässigen, ist die Geschwindigkeit mit der die Abfragen abgearbeitet werden können. Möglicherweise muss B in einem anderen Szenario noch mit C kommunizieren. Die Anfrage würde sich über drei Services erstrecken, was zusätzliche Latenzzeiten mit sich bringt.[30]

Ebenfalls entsteht durch jede Schnittstelle eine fachliche Abhängigkeit geschaffen.[12] Die Anfragen von den Microservices A, C, D, E müssen der Schnittstellendefinition von B entsprechen. Änderungen führen gegebenenfalls zu Fehlern und weiteren Abhängigkeiten. Wie diese Problematik gelöst werden könnte, wird 3.5.2 beschrieben.

3.5.2 Asynchrone Kommunikation

Wie bereits beschrieben, wird bei der synchronen Kommunikation auf weiterführende Abfragen gewartet. Die asynchrone Kommunikation wartet nicht auf Antworten von weiteren Services, sondern trifft Annahmen über etwaige Systemzustände.[30] Um Annahmen zu treffen, existieren je nach Anwendungsfall verschiedene Strategien:

1. Ein Microservice kann replizierte Daten vorhalten. Angenommen ein Artikel soll rausgeschickt werden: Der dafür verantwortliche Service benötigt die Anschrift des Kundens, aber nicht weitere Daten wie Geburtsdatum, Zahlungsmethode oder ähnliches. Dementsprechend werden nur relevante Daten repliziert vorgehalten. Eine Herausforderung ist es, dass diese replizierten Daten stets mit den Originaldaten übereinstimmen. Schließlich kann sich eine Anschrift ändern.[30]

2. Ggf. muss nur ein weiterer Service informiert werden wie der Service B aus Abschnitt 3.5.1, welcher Statistiken erfasst. In dem Szenario der asynchronen Kommunikation würde die Abfrage gestellt werden ohne das Ergebnis abzuwarten, da es schlichtweg nicht relevant ist. Die Herausforderung hier ist, zu gewährleisten, dass die Abfrage auch in Fehlerfehlen früher oder später zugestellt wird.

Aus den Strategien ergeben sich Anforderungen an die Kommunikationsstruktur: Es muss gewährleisten sein, dass fehlerhafte Abfragen erneut übermittelt werden und ebenfalls wird eine Struktur benötigt, die dafür sorgt, dass replizierte Datensätze stets mit aktuellen Daten befüllt sind. Dies lässt sich durch sogenannte Events erreichen.[12].[30]

Die folgende Abbildung 7 verdeutlich das Prinzip von Events und deren Infrastruktur:

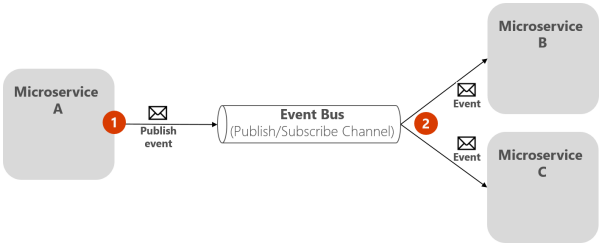

Abbildung 7: Eventbus mit Events[22]

In dieser Abbildung haben Microservice B und C das Event x beim Ergeinisbus (**Event Bus**) abonniert (**subscribed**). D.h. Microservice A veröffentlicht (**published**) eine Änderung, woraufhin B und C informiert werden. B und C können nun ihren Datenbestand aktualisieren und halten so die aktuellen Daten vor. Parallel kann der Microservice A seine Abfrage ganz normal weiterführen. Der Eventbus ist dementsprechend ein Vermittler (**Message Broker**), welcher garantiert, dass die Nachrichten übertragen werden. Dieser sollte mit etwaigen Fehlerfällen (z.B. C ist nicht erreichbar) umgehen können und eine spätere Übertragung garantieren. [22][30]

Aus diesem Modell ergibt sich ein weiterer Vorteil, nämlich dass die Microservices entkoppelt sind. Es wird keine REST-Schnittstelle definiert, welche eine gewissen Fachlogik vorgibt. Ebenfalls können mehrere Services auf ein Event hören. Wolff warnt allerdings davor Events unnötig aufgebläht zu gestalten: Zum einen werden schnell Daten übermittelt, die nicht für alle Abonnenten (**Subscriber**) relevant sind und zum anderen entspräche dies nicht dem Prinzip vom DDD.

Zusätzlich sollte beachtet werden, dass Microservices so gestaltet werden, dass sie idempotent sind. In diesem Zusammenhang bedeutet dies, dass falls ein selbes Event zweimal übertragen wird, der Microservice die Aktion nicht zweimal ausführt. D.h. eine Mehrfachausführung führt zu dem selben Ergebnis wie eine einzige Ausführung. Wenn z.B. eine Rechnung versendet werden soll, ist garantiert, dass diese nur ein einziges Mal versendet wird.[30]

3.5.3 Abwägung asynchrone vs. synchrone Kommunikation

Aus den zwei vorherigen Abschnitten ergibt sich folgende Aufstellung (siehe Tabelle 4).

	synchrone Kommunikation	asynchrone Kommunikation
Vorteile		
	• Jederzeit Konsitent • Paradigma ist Entwicklern bekannt[30]	• Entkoppelt durch Events • Flexibilität, da ein Event mehre Services erreichen kann • Nachrichtenempfang garantiert (ggf. mit Verzögerung) • Absicherung gegen Ausfall
Nachteile		
	• Anfälligkeit durch Abhängigkeiten • Erweiterbarkeit ist schwerer, da fachliche Abhängigkeiten • Ggf. lange Netzwerkzeiten	• nicht jederzeit garantiert konsistent • Idempotenz muss beachtet werden

Tabelle 4: synchrone vs. asynchrone Kommunikation

Es lässt sich feststellen, dass die Vorteile einer asynchrone Kommunikation für Microservices überwiegen und auch diese wird empfohlen.[30][12] Allerdings ist die Kommunikation nicht dogamtisch zu betrachten, sondern sollte je nach Projekt und Anwendungsfall entschieden werden. Synchrone Kommunikation bietet sich nämlich gerade dann an, wenn der Datenbestand definitiv konsistent sein sollen.

Das sogenannte CAP-Theoreom beschreibt die Abwägung, welche man in verteilten Systemen bei der Auswahl der Kommunikation treffen muss. CAP bedeutet:

- Consistency (Konsistenz): Die Daten in einem verteilten System sind konsistent.
- Availability (Verfügbarkeit): Die Verfügbarkeit für alle Systeme ist gegeben.
- Partition Tolerance (Partitionstoleranz): Das Gesamtsystem arbeitet auch weiter, wenn Teile davon ausfallen.

In einem verteilten System können immer nur zwei von den drei Bedinungen erfüllt sein.[30]. Sofern Konsistenz gewährleistet soll, müssen alle dienste stets verfügbar sein. Damit kann der Punkt Partitionstoleranz nicht erfüllt sein. Umgekehrt: Wenn die Partitionstoleranz garantiert ist, z.B. dadurch dass Services ihre eigene Datenhaltung besitzen, ist zwar prinzipiell auch die Verfügbarkeit gegeben, aber nicht die Konsistenz.

Dementsprechend ist es sinnvoll sich die Anforderungen, welches man an sein System hat zu überlegen und sich aufgrund dieser Grundlage zu entscheiden, welche Kommunikationsart implementiert werden soll.

3.5.4 API-Gateway

Umso mehr Services aufgesetzt werden, desto komplexer ist es, die Übersicht über alle zu behalten. Eine Abhilfe im Routing bietet ein sogeanntes API-Gateway. Ein API-Gateway ist der einzige Einstiegspunkt für den Nutzer (**Client**). Von dort wird er weitergeleitet, ohne die Routen von einzelnen Services zu kennen.

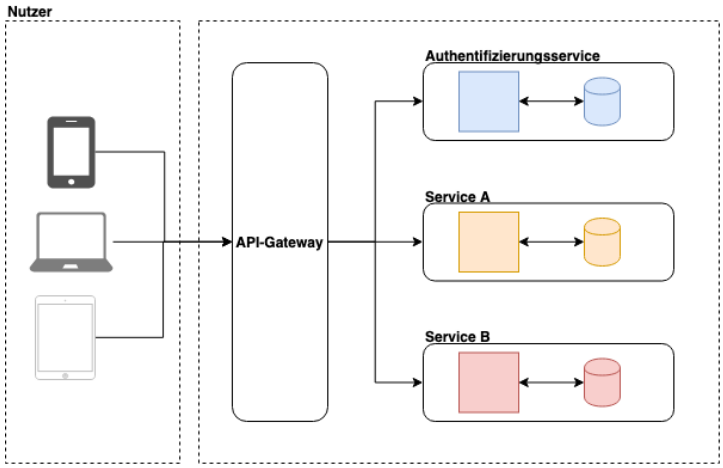

Abbildung 8: Prinzip API-Gateway

Abbildung 8 zeigt deutlich wie die Clients über das Gateway kommunizieren, welches anschließend an die entsprechenden Services weiterleitet. Wenn APIs eine hohe Auslastung haben, würde man mehrere Instanzen von einem API-Gateway erstellen. Ein sogenannter Load Balancer wäre der Einstiegspunkt für die Clients. Dieser würde die Anfragen sinnvoll an die API-Gateway-Instanzen verteilen, so dass keine Überlastung entsteht.[28]

API-Gateways haben neben dem einzelnen Einstiegspunkt noch weitere Vorteile:

- Höhere Sicherheit, das einzelne Services nicht sichtbar und nur über das Gateway zu erreichen[12]
- Authentifizierung kann bereits im Gateway ausgeführt werden, dies führt zu weniger Last für einzelne Microservices.[30]

- Zentralisiertes Logging, Caching, Monitoring, Mocking sowie eine zentralisierte Dokumentation ist möglich.[30]

Ein Nachtteil in der Struktur des API-Gateways ist, dass die Abfragen länger sind, da sie immer erst über das Gateway gehen.

3.6 Authentifizierung und Autorisierung

Beim Monolithen ist architektonisch klar, dass die Authentifizierung und Autorisierung innerhalb des Monolithen stattfindet. Im Bereich der Microservice Architektur existieren verschiedene Szenarien, wie man eine Authentifizierung sowie Autorisierung gestalten kann.[12]

Authentifizierung: Identifiziert, wer jemand ist. Z.B. Nutzer A, der sich durch Benutzername und Passwort registriert hat.[12] **Autorisierung**: Bestimmt, wie viel ein Nutzer darf. Nutzer A hat eine Rolle, welche ihn berechtigt gewisse Aktionen durchzuführen.[12]
Es emphielt sich die Autorisierung in den Microservices ansich zu überprüfen, da diese den entsprechenden Datenbestand haben. Um unnötige Last zu verhindern, kann die Validität - ob es sich überhaupt um einen gültigen Request handelt - bereits im API-Gateway überprüft werden. Die Authentifizierung dagegen sollte in einem eigenen Service oder ins API-Gateway verlagert werden.[7][19] Zu empfehlen ist, dass die Authentifizierung an einer zentralen Stelle durchgeführt wird, um Redundanz und fehlerhafte Implementierungen zu verhindern.

Die Idee ist, dass der Benutzer nach dem Anmelden ein Security-Token erhält, welches verwendet wird, um sensible Anfragen zu verifizieren. Zum einen gibt es die Möglichkeit ein Token auszustellen, welches beim Auslesen verschlüsselt ist (opaque Token) und zum anderen auf ein offenen Standard namens Json Web Token (JWT, transparent Token) zu setzen. Das opaque Token hat den großen Nachteil, dass es zusätzliche Performance sowie Latenz verursacht und nur synchron entschlüsselt werden kann.[19]

Das JWT wird beim Ausstellen signiert, um die Echtheit zu gewährleisten. Während die Nachteile des opaque Token hier nicht auftreten, ist ein anderes Problem, dass ein JWT nach Ausstellung nicht widerrufen werden kann. Theoretisch wäre es dauerhaft gültig, weshalb Ablauflaufzeiten gesetzt werden. Dies wiederum impliziert, dass der Client dafür sorgen muss, immer rechtzeitig ein neues Token anzuforden. Für solche und weitere Logiken exisitiert bereits ein Sicherheitsstandard namens OAuth2, welcher empfohlen wird zu verwenden.[19]

Ziel bei OAuth2 ist unter anderem Autorisierungen zwischen verschiedene Anwendungen zu erlauben. Ursprünglich wurde das Authentifizierungsprotokoll so entworfen, dass Drittanwendungen Zugang zu Informationen erhalten, ohne dass Passwörter weitergelei-

tet werden müssen.[19] Beispielsweise wird OAuth2 verwendet, wenn Benutzer sich über ihren Facebook-Account bei Drittplattformen anmelden. Die Drittplattformen können natürlich nicht das Facebook-Passwort einsehen, erhalten aber je nach Anwendungsfall Zugriff auf verschiedene Ressourcen (z.B. Lesezugriff auf die E-Mail-Adresse und/oder Konakte, Schreibzugriffe zum Teilen von Nachrichten usw.).

Da OAuth2 ein sehr komplexes und umfangreiches Thema ist, wird im Folgenden nur ein häufig verwendetes Grundprinzip erklärt.

Um die Abbildung 9 besser zu verstehen, sind folgende Definitionen hilfreich:[19]

Authorization Server: Authentifiziert den Benutzer und gibt ein Access sowie Refresh Token raus.

Access Token: Durch ein Access Token erhält man Zugriff auf den Resource Server. Das Format ist Abhängig von der jeweiligen Implementierung, eine bereits genannte Möglichkeit wäre JWT. Der Access Token ist zeitlich begrenzt gültig.

Refresh Token: Ein Token welches langlebig ist, also eine lange Gültigkeit besitzt. Dieses kann allerdings im Gegensatz zum Access Token widerrufen werden. Ebenfalls wird es verwendet, um ein neues Access Token vom Authorization Server anzufordern. Dafür ist keine Übergabe der Benutzerdaten nötig.

Resource Server: Eine Resource auf die nur zugegriffen werden kann, wenn ein valides Access Token vorliegt, dies könnte z.B. ein Micoservice sein.

Client: Ein Client möchte Zugriff auf den Resource Server. Clients können beispielsweise Drittanwendungen, Webanwendungen oder mobile Applikationen sein.

Client: Ein Client möchte Zugriff auf den Resource Server. Clients können beispielsweise Drittanwendungen, Webanwendungen oder mobile Applikationen sein. Sie werden auch Resource Owner genannt.

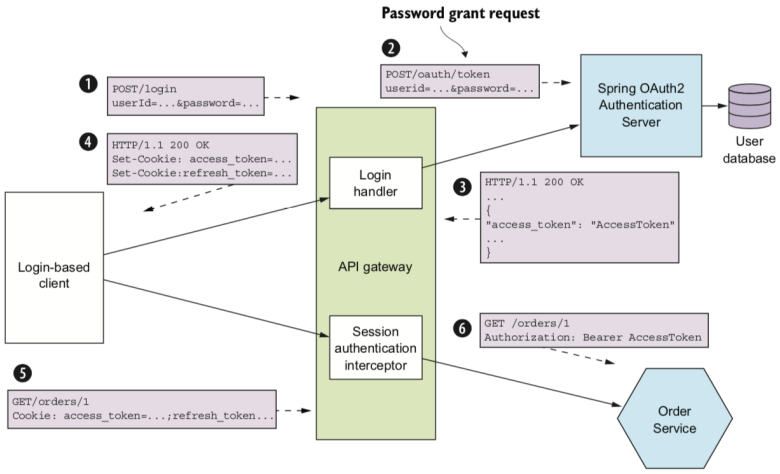

Abbildung 9: Ablauf eines sogenannten ‘password grant‘[19]

Die Abbildung 9 zeigt einen Ablauf, bei dem ein Client sein Usernamen und Passwort übermittelt (1). Diese Anfrage wird von dem API-Gateway weitergeleitet an einen Authorization Server (2). Wurde der Nutzer gefunden, wird ein Access und Refresh Token über das API-Gateway (3) an den Nutzer übermittelt (4). Mit der entsprechenden Authorisierung ruft der Client seine Bestellungen (5) ab. Dieser Request wird entsprechend von dem API-Gateway weitergeleitet (6).

Neben dem *password grant Flow* existiert auch der sogenannte *client credentials grant Flow*. Dieser funktioniert ähnlich, nur dass nicht Username und Passwort übertragen werden, sondern der Anwendungen durch gemeinsam bekannte Daten zwischen Anwendungen und Authorization Server vertraut wird. Den *client credentials grant Flow* sollte man verwenden, wenn eine Applikation Ressourcen aufrufen möchte, die außerhalb eines User-Kontextes liegen, d.h. es handelt sich in der Regel um recht allgemeine Daten.[16][19]

Aufgrund dieser Grundlage wird im Konzept 4.5 herausgearbeitet, welche Möglichkeiten zur technischen Umsetzung von OAuth2 bereitstehen.

3.7 Docker

Über Docker können Anwendungen innerhalb eines Containers laufen. Ein Container ist vergleichbar mit einer sehr leichtgewichtigen, modularen virtuellen Maschine.[29] Docker in der Tiefe aufzuarbeiten, würde den Umfang dieser Arbeit überschreiten. Dennoch wird im Folgenden erläutert, warum speziell Docker sich sehr gut für Microservices eignet und wie das grundsätzliche Wirkungsprinzip von Docker funktioniert.

Anfangs wurden Microservices so definiert, dass sie als möglichst eigenständige, deploybare Einheiten zu betrachten sind. Beim Hosten - also dem Bereitstellen des Services

- sollte dies ebenfalls berücksichtigt werden. Nimmt man an, man hostet alle Services auf einer Maschine, läuft man Gefahr, dass die Microservices sich z. B. durch Portkonfigurationen oder dem Zugriff auf selbe Ressourcen behindern.[31]

Bisherige Lösungen - und je nach Anwendungsfall auch sinnvoll - bieten sich an dieser Stelle virtuelle Maschinen (**VM**) an. D.h. auf einem Host könnten mehrere Betriebssysteme laufen, die sich die Hardwareressourcen vom Host teilen. Die angestrebte Isolation zwischen den Microservices wäre erreicht und individuelle Konfigurationsmöglichkeiten wie z.B. Portfreigeben könnten sich gegensetitig nicht mehr stören. Durch die VMs entstehen allerdings eine Performanceeinbußen, welche nicht im Verhältnis zum Nutzen stehen und zusätzlich ein höherer Verbrauch der Hardwareressourcen.[31] Gesucht ist dementsprechend eine Technologie, die es schafft Services zu isolieren und dabei gleichzeitig leichtgewichtig zu sein: Docker.

Startet man einen Microservice über Docker ist dies damit gleichzusetzen, als würde im Betriebssystem der Service als Prozess gestartet werden. Es entsteht kein deutlich sichtbarer Overhead in Bezug auf Ressourcenverbrauch.[31]

Um den Docker-Aufbau (siehe Abbildung 10) besser zu verstehen, ist folgendes Vokabular nützlich:[31]

Docker-Image: Aus einer Anwendung kann man ein Image erzeugen, so dass es im Docker-Container gestartet werden kann.

Docker-Container: Wenn ein Image ausgeführt wird, läuft es in einem Container, welcher verschiedene Eigenschaften hat, wie z.B. ein eigenes Netzwerk-Interface und ein Dateisystem.

Dockerfile: Ein Dockerfile ist ähnlich einem Bauplan. Er beschreibt, wie das Image gebaut werden muss, damit es in einem Docker-Container laufen kann.

Repository: Ein Repository speichert Images. In der Regel hält ein Repository mehrere Images von derselben Anwendung mit verschiedenen Versionen bereit.[29]

Docker-Registry: Eine Docker-Registry verwaltet mehrere Repositories.

Docker-Host: Ein Docker-Host unterstützt die Docker-Technologie, d.h. es können entsprechend Images ausgeführt werden. Zusätzlich ist es möglich, Images von einem Repository auszuführen. D.h. man muss die Images nicht extra auf den Host laden, um sie auszuführen.

Bei genauerer Betrachtung der Abbildung 10 fällt auf, dass Container in einem Netzwerk sind und sich denselben Kernel teilen. Dateisysteme, Netzwerk-Interface und containereigene Prozesse sind voneinander isoliert. D.h. Portfreigaben oder ähnliches behin-

dern sich nicht.

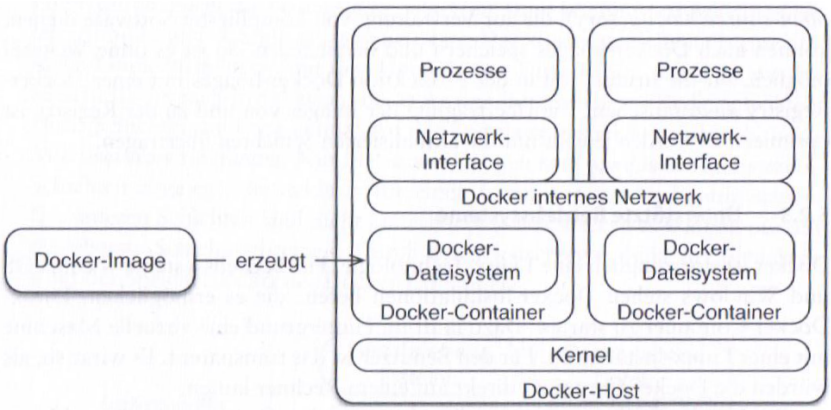

Abbildung 10: Docker Architektur[31]

Zusammenfassend lässt sich sagen, dass durch das Nutzen von Docker eine isolierte und ressourcenvertretbare Trennung von Microservices auf einem Host erreichen lässt.

4 Konzept

Das ist die Konzepteinleitung

4.1 Anforderungen definieren

Um die Anforderungen für das Spiel *Stirnraten* zu erfassen, sollten zwei verschiedene Aspekte berücksichtigt werden:

- der **IST-Stand**, was muss mindestens erfüllt werden und
- welche möglichen **Erweiterungen** entstehen durch eine API.

Um die Anforderungen greifbarer zu gestalten, wird auf das Prinzip von User Story Mapping zurückgegriffen. D.h. jede Anforderung ergibt sich aus einer sogenannte User Story. Diese ist so aufgebaut, dass beschrieben wird **wer** möchte **was** und **aus welchem Grund**.[17]

Im Folgenden gelten die zwei Definitionen: Ein Nutzer ist eine Person, welche die App spielt. Der Betreiber ist der Besitzer von Stirnraten. Ein User kann ein Nutzer oder Betreiber sein.

Ein Beispiel für eine User Story könnte lauten: Als Nutzer (*wer*) möchte ich mein Spielprofil teilen (**was**), um mich besser mit meinen Freunden messen zu können (**warum**).

Wie diese User Story nun umgesetzt wird, muss abgewogen werden. Zum einen sollten User Stories konkret genug formuliert werden, so dass klar ist, was der User möchte. Zum anderen bleibt bei der Entwicklung ein agiler Handlungsspielraum.[17] Eine Teile-Funkion beispielweise kann unterschiedlich aufwendig umgesetzt werden. Der Nutzer könnte ein Text teilen, ein extra aufbereitets Bild oder einen Link, welcher auf ein mögliches Online-Profile verweist. All diese Möglichkeiten bedeuten unterschiedliche Aufwände. Alternativ könnte man aus dieser einen User Story drei erstellen, welche entsprechend unterschiedlich priorisiert werden.

Exkurs - Spielprinzip Stirnraten: Die Spieleranzahl muss mindestens zwei betragen. Ein Spieler wählt aus verschiedenen Kategorien aus und hält sich das Telefon an die Stirn. Es erscheint Begriff, welchen der Gegenüber erklären muss. Errät der Spieler den Begriff, neigt er das Telefon nach vorne und ein neuer Begriff erscheint. Weiß er ihn nicht, kann er diesen überspringen, in dem er das Telefon nach hinten neigt. Ziel ist es, innerhalb einer frei wählbaren Zeit (z.B. 60 Sekunden), so viele Begriffe wie möglich zu erraten.

4.1.1 Erfassung Stirnratens IST-Stand

In der folgenden Tabelle 5 wird gezeigt, welche Funktionen die App bereits auf dem Gerät bereitstellt, welche aber zukünftig serverseitig erledigt werden sollen.

Funktion	Beschreibung
Profil/Statistik	Nach jedem Spiel werden verschiedene Daten erfasst, z.B. die Dauer des Spiels oder richtig geratene Wörter. Löscht man die App, ist dieses Profil unwiederbringlich.
Bereitstellung Begriffe	Die über 6000 verschiedenen Begriffe liegen nur offline zur Verfügung. Editieren, Hinzufügen und Löschen geht nur über das Updaten der App.
Zweisprachigkeit	Die App wird für den deutschen sowie den englischen Sprachraum angeboten. Es ist gewährleistet, dass je nach Nutzer, auf die sprachlich richtige Datenbank zugegriffen wird.

Tabelle 5: bestehende Funktionen in Stirnraten

Aus dem IST-Zustand ergeben sich bereits folgende User Stories:

- Als Betreiber möchte ich neue Begriffe über eine Schnittstelle hinzufügen, editieren und löschen können, um die Datenbank schneller und leichter zu pflegen

- Als Betreiber möchte ich eine Datenbank, um nicht für zwei Apps (iOS und Android) den Datenbestand zu pflegen
- Als Betreiber möchte ich entscheiden können, in welcher Sprache (englisch oder deutsch) ich Begriffe manipuliere, um sinnvolle Daten zu gewährleisten
- Als Nutzer möchte ich das Spiel immer offline spielen können, da ich auf Reisen häufiger kein stabiles Internet habe
- Als Nutzer möchte ich mein Spielerprofil online speichern, um es auf anderen Geräten oder nach einer Neuinstallation abrufen zu können
- Als Nutzer möchte ich automatisch die Sprache angezeigt kriegen, welche für mich relevant ist, weil es mir sonst zu kompliziert ist

4.1.2 Erweiterungen mittels User Story Mapping

Durch das Einführen einer API bieten sich folgende Erweiterungsmöglichkeiten an:

- Als Betreiber möchte ich neue Kategorien hinzufügen, editieren und löschen können, um das Nutzerangebot zu vergrößern
- Als Betreiber möchte ich Bilder pro Kategorie hinzufügen, editieren und löschen können, um ein sprechendes Bild für die Nutzer zu hinterlegen
- Als Betreiber möchte ich eine Kategorie als Premium kennzeichnen können, um Angebotsaktionen zu schalten
- Als Betreiber möchte ich eine Kategorie (de)aktivieren können, um sie immer zu einem sinnvollen Zeitpunkt anbieten zu können
- Als Betreiber möchte ich eine Registrierfunktion anbieten, um die Nutzer stärker an mich zu binden.
- Als Betreiber möchte ich die Nutzer abrufen, welche sich bei mir registriert haben, um einen Nutzerstamm aufzubauen
- Als Betreiber möchte ich Nutzer aus Datenschutzgründen löschen können
- Als Nutzer möchte ich mich in einer Rangliste mit anderen Nutzern vergleichen können, um zu sehen, wer in dem Spiel besser ist.
- Als Nutzer möchte ich die Spielerprofile von anderen Nutzern detailliert ansehen, um zu sehen, was ihnen gefällt
- Als Betreiber möchte ich die Ranglisten-Namen der Nutzer manipulieren können, um unflätige Namen/Missbrauch zu verhindern.

- Als Betreiber möchte ich kummulitierte Daten aus den Nutzerstatistiken sehen, um Marktentscheidungen besser treffen zu können
- Als Betreiber möchte ich die Kategorien sortieren können, um die Anordnung für die Nutzer bestmöglich zu gestalten
- Als Betreiber möchte ich sehen, wenn ein Begriff bereits in der Kategorie ist, um die Datenqualität zu gewährleisten
- Als Nutzer möchte ich eigene Begriffe einreichen können, weil mir manche Begriffe oder Kategorien im Spiel fehlen
- Als Nutzer möchte ich sehen, wenn ein eingereichter Begriff bereits in einer Kategorie existiert, um Bescheid zu wissen
- Als Betreiber möchte ich eingereichte Begriffe zulassen oder ablehnen können, um den Datenbestand zu vergrößeren bzw. die Qualität zu gewährleisten
- Als Betreiber möchte ich sehen, wann meine Nutzer zuletzt online waren, um ggf. Marketingmaßnahmen zu unternehmen
- Als Betreiber möchte ich, dass Nutzer-Zugangsdaten entsprechend gut verschlüsselt sind, um die Datensicherheit zu gewährleisten

Die folgende Auflistung sind User Stories, welche auch als Anforderungen entstanden sind, aber im Rahmen der Projektarbeit aufgrund von Aufwänden nicht umgesetzt werden können.

- Als Betreiber möchte ich eine Newsletter-Funktion anbieten, um die Nutzer über Neuigkeiten zu informieren
- Als Nutzer möchte ich ein Profilbild hochladen, um mein Profil zu indiviualisieren
- Als Nutzer möchte ich mein Passwort zurücksetzen können, wenn ich es vergessen habe.
- Als Betreiber möchte ich individuelle Animationen vom Server an den Nutzer weiterreichen können, um die Verspieltheit der App zu unterstreichen.
- Als Betreiber möchte ich Themes und Farbcodes online bereitstellen, um den Nutzern Individualsierungsmöglichkeiten schneller und leichter bereitzustellen
- Als Betreiber möchte ich automatisiert, individuelle (Push)Nachrichten senden, um den Nutzer stärker zu binden

Aus den User Stories ergeben sich konkrete Abhängigkeiten zwischen den Microservices sowie klare Vorlagen für die Datenhaltung, z.B. benötigt der Nutzer mindestens einen eindeutigen Namen sowie ein Passwort. Die konkrete Umsetzung ist in FIGURE-VERLINKEN-AUF-KAPITEL-5.

4.2 Macroarchitektonische Festlegungen von Technologien

Wie bereits in 3.4.2 erwähnt, können durch makroarchitektonische Entscheidungen gewisse Vorteile erzielt werden, wie z.B. dass die Technologien zur Infrastruktur des Unternehmens und zu den Kompetenzen der Mitarbeiter passen. Ebenfalls können strategische Entscheidungen (z.B. ausschließlich Nutzen von Cloudtechnologien) die Makroarchitektur beeinflussen. Im Folgenden werden einige Technologien für 'Stirnraten' makroarchitektonisch festgelegt.

4.2.1 Wahl der Datenbank

Bei der Entscheidung, ob eine relationale oder schemalose (NoSQL) Datenbank verwendet wird, wurde sich für eine relationale entschieden. NoSQL Datenbanken sind häufig für spezielle Anwendungsfälle sinnvoll, z.B. wenn das Datenbankmodell sich häufig ändert oder ein hohes Maß an Skalierung notwendig ist. Diese Fälle sind für Stirnraten nicht absehbar, weshalb auf den etablierten Standard einer relationalen Datenbank gesetzt wird.[11]

Im Bereich der relationalen Datenbanken können verschiedene Technologien zur Umsetzung genutzt werden. Es wurde sich auf die derzeit (Stand Mai 2019) vier Populärsten Technologien konzentriert: Oracle (Rang 1), MSSQL (2), MySQL (Rang 3) und Postgres (Rang 4).[10] Oracle und MSSQL wurden für das Projekt ausgeschlossen, da diese kommerziell betrieben werden. Für Postgres und MqSQL wurde ein sogenanntes Proof of Concept erstellt, d.h. es wurde in einem einfachen Szenario eine Machbarkeit überprüft. Die Grundanforderungen war, dass MySQL und Postgres in verschiedenen Docker-Containern auf einer Maschine laufen können. Bei dem Proof of Concept hat sich gezeigt, dass es deutlich komplizierter ist, multiple Postgres Instanzen auf einer Maschine zu starten, da zusätzlich individuelle Scripts ausgeführt werden müssen.[18]

Beim Erstellen von multiplen MySQL-Instanzen kam es zu keinerlei Problemen. Aufgrund des Rankings und der einfacheren technischen Implementierung durch das Proof of Concept wurde, sollen makroarchitektonisch die Microservices MySQL verwenden.

4.2.2 Programmiersprachen, Darstellungsart, REST und Docker

Programmiersprachen: Anfangs wurde erwähnt, dass aufgrund unternehmensstrategischer Gründe Entscheidungen darüber getroffen werden, welcher Technologiestack verwendet wird. In Hinblick auf die Programmiersprachen wird deshalb festgelegt, dass die Microservices im .net Framework in c# entwickelt werden. Diese Sprache wird am besten von dem Entwickler beherrscht, so dass Wartbarkeit, Nachhaltigkeit und Pflege des Codes langfristig garantiert sind. Als zusätzliche Alternative ist kotlin ebenfalls erlaubt.

Darstellungsart: Das verwendete Datenformat beim Austausch von Daten ist JSON (JavaScript Object Notation). Alternativ wäre auch die Extensible Markup Language

(XML) möglich, allerdings ist XML deutlich aufgeblähter und damit weniger leichtgewichtig. Zusätzlich lässt JSON sich leichter von den Programmiersprachen weiterverarbeiten.[13]

REST: Die Kommunikation zwischen den Microservices wird so festgelegt, dass sie dem Representational State Transfer-Paradigma (REST) unterliegen. Eine Alternative zu REST wäre SOAP (Simple Object Access Protocol) in Kombination mit WSDL (Web Services Description Language). Da WSDL allerdings auf der Basis von XML arbeitet und SOAP deutlich komplexer und schwerer skalierbar ist als REST, wird es nicht verwendet. [2]

Die Prinzipien von REST sind bereits aus dem *Modul Mobile Application Development* bekannt und werden deshalb nicht weiter erwähnt.

Docker: Neben Docker als Containerisierung existieren einige Alternativen wie Podman, Rocket, LXD, Flockport, Windocks oder Boxfuse. Sie unterscheiden sich teils in Sicherheitsaspekten, Preis, Kompatibilität zum Betriebssystem oder der Anbindung zu Kubernetes (Programm zum Bereitstellen, Skalieren und Verwalten von Container-Anwendungen).[4][23] Es wurde sich für Docker entschieden. Zum einen da dies - wie bereits bei den Programmiersprachen - eine beherrschte Technologie ist. Zum anderen - gemessen am Google Trend - ist Docker die bevorzugt gesuchte Technologie für Containerisierung:

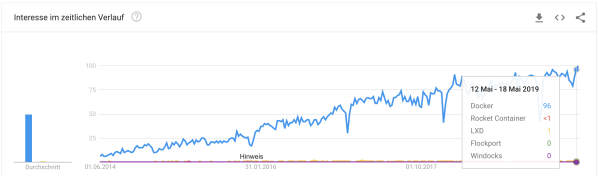

Abbildung 11: Trends bei den Suchworten: Docker, Rocket Container, LXD, Flockport und Podman

4.2.3 Bounded Contexts - Architektur des Projektes

Aus den Abschnitt 3.4.1 lassen sich folgende Bounded Contexts erstellen:

Durch die verschiedenen Kontexte lassen sich entsprechende Microservices abbilden. Zusätzlich wird definiert, was unter welchen Fachtermini im entsprechenden Context zu verstehen ist. Zum Beispiel stellt der *Identity Context* dem Nutzer ein Token aus mit dem er weitere Aktionen ausführen darf. Dafür speichert der *Identity Context* sich in seinem Customer-Modell (Domänenmodell) einen Namen und ein Passwort. Der Customer im *Profile Context* dagegen enthält noch weitere Informationen wie z.B. Anzahl der gespielten Spiele, geratene Begriffe, Lieblingskategorie und Spielminuten. Der Customer im *Rank Context* benötigt dagegen nur den Customer-Namen und noch zu definierende Parameter aus denen Customer-Punkte generiert werden können, um eine Bestenliste

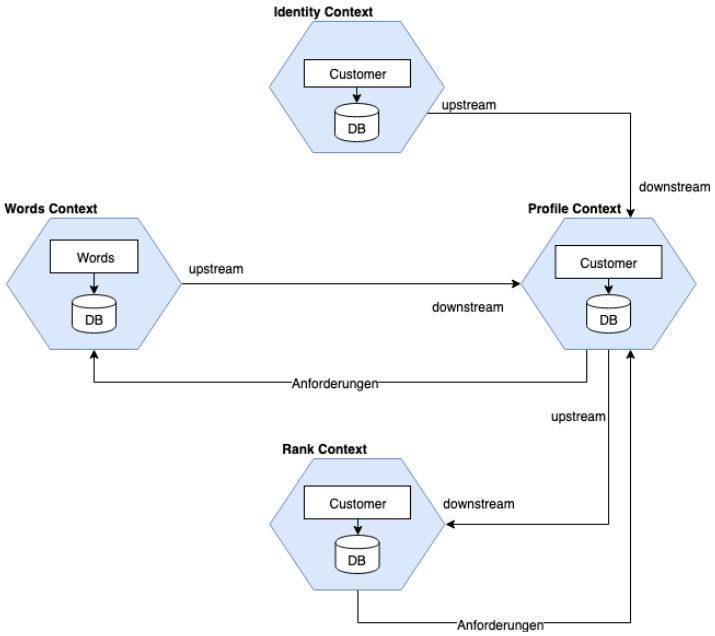

Abbildung 12: Bounded Contexts für die Stirnraten API.

darzustellen.

Es wurde bereits erwähnt, dass der *upstream* dem *downstream* Informationen bereitstellt. Zusätzlich können Anforderungen gestellt werden, damit mit den Daten, die der *downstream* erhält, entsprechend gerarbeitet werden kann. In der Abbildung 12 fordert der *Profile Context* Informationen vom *Words Context* sowie der *Rank Context* vom *Profile Context*

Um die aus den User Stories entstanden Anforderungen zu erfüllen, werden im Folgenden die Domainmodels konzeptioniert. Diese können während der Implementierungsphase noch abweichen.

Words-Context: Words Domainmodel
id: Dient als unique identifier
category_name: Name der Kategorie
subtitle: Optionale Beschreibung der Kategorie
image_name: Name des Bildes, welches für eine Kategorie hinterlegt werden soll
premium_key: Notwendig für die Kaufabwicklung zum Identifizieren, um welchen In-App-Kauf es sich handelt
is_premium: Markiert, ob eine Kategorie kostenpflichtig ist oder nicht
selected: Definiert, ob die Kategorie in der App vorausgewählt ist oder nicht
words: Die Begriffe pro Kategorie, welche erraten werden können
sort: Definiert, an welcher Stelle in der Sortierung die Kategorie ist
is_activ: Definiert, ob die Kategorie in der App angezeigt wird oder nicht

updated_ at: Zeitpunkt, wann die Kategorie das letzte mal verändert worden ist

Identiy-Context: Customer-Domainmodel:
id: Dient als unique identifier
name: Name des Benutzers
password: Passwort des Benuzters

Profile-Context: Customer-Domainmodel:
id: Dient als unique identifier
name: Name des Benutzers (kommt aus dem Identiy-Context)
mail: E-Mail-Adresse des Benutzers (optional)
played_ games: Zeigt die Anzahl absolvierter Spiele
most_ right_ words: Zeigt die Anzahl der Wörter, die während einer Runde geraten worden sind
most_ skipped_ words: Zeigt die Anzahl der Wörter, die während einer Runde übersprungen worden sind
right_ words: Zeigt Anzahl aller Wörter, die richtig geraten worden sind
skipped_ words: Zeigt Anzahl aller Wörter, die übersprungen worden sind
time: Zeigt, wie lange der Benutzer gespielt hat
top_ categories: Speichert, welche Kategorien der Benutzer favorisiert

Rank-Context: Customer-Domainmodel:
id: Dient als unique identifier
name: Name des Benutzers (kommt aus dem Identiy-Context)
played_ games: Zeigt die Anzahl absolvierter Spiele (kommt aus Profile-Context)
right_ words: Zeigt Anzahl aller Wörter, die richtig geraten worden sind (kommt aus Profile-Context)
skipped_ words: Zeigt Anzahl aller Wörter, die übersprungen worden sind (kommt aus Profile-Context)
time: Zeigt, wie lange der Benutzer gespielt hat (kommt aus Profile-Context)
points: Punkte, die sich aus played_games, right_words, skipped_words und time berechnen

Es lässt sich feststellen, dass es Überschneidungen zwischen dem Customer-Domainmodel gibt, je nach dem in welchem Kontext man sich befindet. Natürlich verändert dieses Konzept sich noch im Laufe der Produktentwicklung und muss iterativ an den Stand der Entwicklung angepasst werden. Ebenfalls gilt zu erwähnen, dass es an dieser Stelle im Domain Driven Design nicht zwangsweise ein richtig oder falsch gibt. Dies ist ein Konzeptentwurf, aber natürlich nicht die einzige mögliche Lösung.

4.3 Wahl des API-Gateway

Bei der Wahl des API-Gateways existieren verschiedene Technologien, die gegeneinander abgewogen werden müssen. Dabei werden unterschiedliche Aspekte betrachtet: Zum

einen sollte das API-Gateway etabliert und leichtgewichtigsowie leicht zu implementieren sein, d.h. der Projektgröße angemessen. Zusätzlich muss das Gateway ein OAuth2 Token verarbeiten können. Um das Gateway umzusetzen, könnte es selbst entwickelt werden, auf ein Library zurückgegriffen oder ein Clouddienst (z.B AWS, Azure oder Google Cloud) verwendet werden.

Eigenentwicklung: Die eigene Entwicklung eines Gateways ist kritisch zu betrachten, da viele aktuelle, umfangreiche und bereits etablierte Libraries für diesen Einsatzzweck existieren. Schätzungsweise kostet es viel Zeit und Energie die Funktionen, die ein Gateway erfüllen muss, technisch sauber umzusetzen. Beispiele für Funktionen eines Gateways sind: Routing, Caching, Load Balancing, Headers/Query String/Claims Transformation, Logging ...

Libraries: Eine etablierte und leichtgewichtige Lösung ist das API-Gateway Zuul zu verwenden, welches allerdings auf Java basiert und dementsprechend aus macroarchitektonischer Sicht nicht bevorzugt wird.

Eine weitere Möglichkeit ist ein Gateway mit **Istio** in Kombination mit Kubernetes aufzubauen. Das hätte unter anderem den großen Vorteil, dass die Services sich untereinander kennen und die Kommunikation sehr wenig händische Konfigurationen benötigt. Allerdings erfordert Kubernetes sowie Istio jeweils ein hohes Maß an technischem Verständnis und erscheint nicht lohnenswert für ein verhältnismäßig kleines Projekt zu implementieren.[21][26]

Von Microsoft empfohlen wir das Open Source Gateway **Ocelot**. Es ist leichtgewichtig und überschneidet sich mit gesuchten Anforderungen (Routing, Load Balancing, Authorization usw.). Zusätzlich ist es explizit desigend für ASP .NET Core und bietet so eine überschaubare Implementierung vom Aufwand her.[5]

Cloudanbieter: AWS, Azure und Google Cloud bieten alle Gateways an, die auch einen entsprechend großen Funktionsumfang garantieren. Ein weiterer Vorteil ist die Skalierbarkeit, die jeder Cloud-Anbieter verspricht. Ebenfalls wird die Programmiersprache c# im .net Kontext unterstützt.[25][24] Ein Nachteil dagegen ist die preisliche Komponentene. Es ist nicht absehbar, wie sich die Stirnraten API bezüglich der Last entwickelt, weshalb unsicher ist, wie viele Kosten entstehen werden. Auch wenn eine selbstgehoste Lösung andere Nachtteile mit sich bringt, ist ein Festpreis garantiert, welcher für eine Projektarbeit bevorzugt wird.

Aufgrund der Rercheren wird sich weder für eine Eigenentwicklung (zu aufwendig) noch für eine Cloudlösung (unsichere Kostenfrage) entschiedene. Betrachtet man die Vor- und Nachteile der Libraries bietet Ocelot den größten Mehrwert, weshalb ein Gateway via Ocelot implementiert wird.

Die Architektur erweitert sich wie folgt:

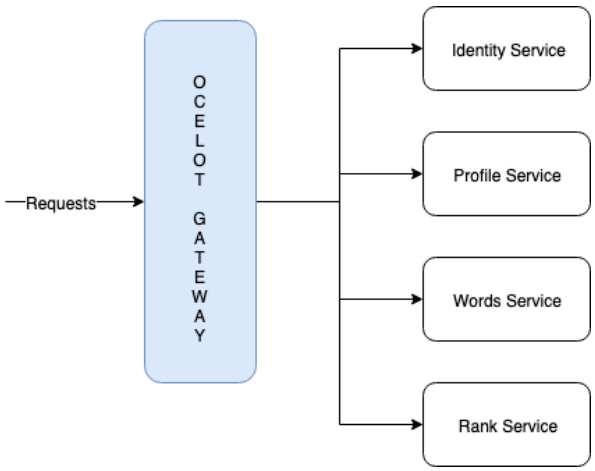

Abbildung 13: Struktur mit dem API Gateway Ocelot

4.4 Wahl der Kommunikation

Um die in den VERLINKEN_GRUNDLAGEN ausgearbeitete asynchrone Kommunikation zu gewährleisten, werden sogenannte Message Broker (kurz: Broker) verwendet. Diese empfangen Nachrichten und senden diese ggf. an mehrere Empfänger weiter. Die folgenden Message Broker sind in der Selbstbeschreibung schnell, robust, zuverlässig und einfach zu implementieren: *RabbitMQ*, *Kafka*, *RocketMQ*, *Artemis* oder *NSQ*.

Bevor die Message Broker jedoch im Detail gegeneinander abgewogen werden, wird untersucht, ob es bereits vorherige Ausschlusskriterien gibt. Zum Beispiel weist die *RocketMQ* (Apache Projekt) noch über 130 Github Issues auf, weshalb davon auszugehen ist, dass dieser Message Broker sich noch in der Entwicklung befindet. *Artemis* verwendet noch ältere Technologien wie XML und *NSQ* bietet nicht den Funktionsumfang wie andere Broker (z.B. Haltbarkeit der Nachrichten oder Clustering).[6] Deshalb werden diese Message Broker von vorneherein ausgeschlossen.

Im Folgenden wird der von LinkedIn entwickelte Broker *Kafka* mit dem *RabbitMQ* Broker verglichen.

Auch wenn beide Broker in unterschiedlichen Sprachen entwickelt worden sind, können sie mittels C# verwendet werden und sind Open Source.

Architektonisch arbeitet RabbitMQ mit einer Entkopplung, da die Produzenten ihre Nachrichten in eine sogenannte Börse (exchange) übermitteln (publish). Die Konsumenten entnehmen die Nachrichten aus einer Queue. So liegt das Routing zwischen Exchange und Queue nicht bei den Produzenten bzw. Konsumenten. Kafka dagegen ist für ein höheres Volumen auslegt. Im Gegensatz zur RabbitMQ merken die Consumer sich, ob sie bereits eine Nachricht gelesen haben oder nicht. D.h. die Nachrichten werden

in einem Kafka Cluster zeitlich begrenzt gespeichert, unabhängig ob sie schon gelesen oder ungelesen sind. Kafka könnte diesbezüglich sinnvoll für Event Sourcing sein, also in einem System, wo der Zustand eines Systems durch Sequenzen von Events abgebildet werden kann.[19] Kafka benötigt im Gegensatz zur RabbitMQ einen externen Dienst (häufig Zookeper verwendet) durch den vereinfacht ausgedrückt mit Kafka kommuniziert werden kann.[8][27] Typische Anwendungsfälle werden bei Kafka beim Messaging, Webseiten-Aktivitäts-Tracking, erfassen von Metriken, Log Aggregationen und Event Sourcing gesehen.[27] RabbitMQ setzt dagegen mehr auf sehr zuverlässige Zustellung der Nachrichten und unterstützt eine Vielzahl von Kommunikationsprotokollen. Zusätzlich lassen sich viele Kafka-Anwendungsfälle (z.B. Event Sourcing) mit Hilfe von Drittsoftware (z.B. Cassandra) in Kombination mit der RabbitMQ abbilden.[8]

Es ist schwierig zu entscheiden, welcher Broker der besser geeinete ist. Beide Technologien sind sehr umfangreich und decken gerade in Kombination mit Drittsoftware viele selbe Anwendungsfälle ab. Ebenfalls sind die in *Stirnraten* zu erwartetenden Anwedungsfälle im Gegensatz zu den Möglichkeiten, die die Broker bieten, eher trivial. Da Kafka allerdings wie bereits erwähnt ein zusätzliches Programm für die Verwaltung benötigt und im Gesamten größer sowie umfangreicher erscheint, wird auf eine schlankere Implementierung mittels RabbitMQ gesetzt.

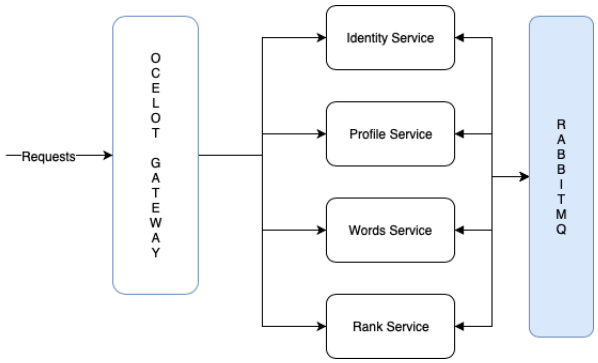

Abbildung 14: Architektur mit Hilfe der RabbitMQ

4.5 Wahl der Authenfizierung/Authorisierung

In 3.6 wurde bereits argumentiert, dass OAuth2 für die Authentifizierung und Autorisierung verwendet wird. Ebenfalls wurde festgelegt, dass jeder Microservices die Autorisierung durchführt, die Authentifizierung allerdings in einem eigenen Service liegen muss. Damit ein Microservice die Autorisierung durchführen kann, muss ein Request vom API-Gateway entsprechend aufbereitet werden. Im Detail sieht dies wie folgt aus[19]:

1. Ein Request mit JWT wird vom Gateway empfangen

2. Das Gateway prüft die Signatur. Ist der Request valide, werden Informationen (z.B. Schreibrecht um neues Wort zu hinterlegen) in den Header vom Request geparst.

3. Das Gateway leitet den Request angereichert mit entpackten Daten im Header weiter an den Microservice.

4. Der Microservice liest die Daten aus und überprüft, ob die nötigen Rechte für die entsprechende Aktion vorliegen.

Während der strukturelle Ablauf nun festgelegt ist, stellt sich die Frage, wie OAuth2 implementiert wird. Dafür stehen verschiedene Möglichkeiten zur Verfügung: Auth0 (Drittanbieter), IdentityServer4 oder Owin (jeweils Frameworks für ASP .net) sowie Clouds.

Auth0: Bei Auth0 (http://auth0.com) handelt sich um einen Drittanbieter, welcher laut eigenen Angaben alle gängigen Authenifizierungsmöglichkeiten abbildet. Die Dienste, welche bereitgestellt werden (z.B. Social Login, Zwei-Faktor-Authentifizierung, E-Mail-Verfication, Forget Password usw.) würden laut eigenen Angaben um die 90 Tage Eigenentwicklung beanspruchen. Mit Auth0 benötigt man zum Implementieren wenige Stunden und hat Zugriff auf gute gepflegte Dokumenation. Der Nachteil ist, dass Auth0 ab einer gewissen Last (über 7000 aktive Nutzer im Monat) kostenpflichtig wird. Zusätzlich ist das Angebot z.B. Zwei-Faktor-Authentifizierung für Stirnraten nicht notwendig.

.net OWIN: Allgemein ist OWIN eine von Microsoft für ASP .net core entwickelt und hat den Vorteil, dass Webanwendung und Webserver voneinander entkoppelt sind. Durch OWIN sitzt eine Middleware vor dem Webserver. Dort bietet OWIN die Möglichkeit Autorisierungsserver basierend auf OAuth2 zu implementieren. Der Dienst ist kostenfrei und auf ASP .net core zugeschnitten, leider ist die Dokumentation sehr rudimentär. Es ist schwer herauszufinden, welche Möglichkeiten OWIN genau bietet und wie man diese implementiert.[15]

IdentityServer4: Der IdentityServer4 ist ein OAuth2 Framework für ASP.NET Core, welches in ASP.NET Core 3.0 (derzeitige produktivversion ist 2.2 - Stand 2.6.2019) künftig vorhanden sein soll. Derzeit muss es noch über Libraries installiert werden. Es vereinfacht die Handhabung mit OAuth2, bietet eine umfangreiche Dokumenation und arbeitet unterstützend mit Ocelot zusammen. Es bietet natürlich nicht so eine leichte Implementierung an wie Auth0, ist allerdings kostenfrei.

Clouds: Die Clouddienste Google, AWS und Azure bieten ebenfalls eigene Lösungen an. Auf diese wird allerdings nicht weiter eingegangen, da bei dem Gateway und Hosting bereits auf eine Cloudlösung verzichtet worden ist.

Aus den genannten Möglichkeiten wird sich für das Frsamework IdentityServer4 entschieden, da es kostenlos ist (im Gegensatz zu Auth0), besser dokumentiert als OWIN

und mit Ocelot kompatibel ist. Zusätzlich spart man sich gegenüber der kompletten Eigentlichentwicklung Zeit.

5 Implementierung

Das ist der Implementierungspart

5.1 Authentifizierung und Autorisierung

Ein zentraler Teil bei Microservices ist die Authentifizierung sowie die Autorisierung. Es wurde sich für eine Identity Server mit OAuth2 entschieden. Die MySQL-Datenstruktur ergibt sich aus dem Datenmodell:

```
public class User
{
    [Required] public int Id { set; get; }
    public string Name { set; get; }
    public string Password { set; get; }
    public bool Active { set; get; }
    public string Role { set; get; }
}
```

Als eindeutiger Identifier ist eine ‘Id‘ notwendig. Zusätzlich besitzt jeder User einen Namen, ein Passwort, ist im Standaradfall aktiviert und es wird zwischen zwei Rollen unterschieden: ‘customer‘ und ‘admin‘. Wie zu erwarten hat die ‘admin‘-Rolle mehr Berechtigung als ein Customer.

Um den Identity Server einzurichten, müssen sogenannte NuGet-Pakete heruntergeladen werden. NuGet ist ein System, mit welchem Softwarebibliotheken bereitgestellt werden können. Diese Verweise werden zur Projektdatei hinzugefügt.

```
<PackageReference Include="IdentityServer4" Version="2.3.0" />
<PackageReference Include="IdentityServer4.AccessTokenValidation" Version="2.7.0" />
```

In der ‘Startup.cs‘, welche standardmäßig bei C# .net vorliegt, werden grundsätzlich Serverkonfigurationen initialisiert. Dies muss für den Identity Server ebenfalls getan werden.

```
(1)
var builder = services.AddIdentityServer()
.AddInMemoryIdentityResources(Config.GetIdentityResources()) //check below
.AddInMemoryApiResources(Config.GetApis())
.AddInMemoryClients(Config.GetClients())
```

```
.AddProfileService<ProfileService>();

services.AddTransient<IResourceOwnerPasswordValidator, ResourceOwnerPasswordValidator
services.AddTransient<IProfileService, ProfileService>();

(2)
services.AddAuthentication("Bearer")
.AddJwtBearer("Bearer", options =>
{
   options.Authority = "http://identity_server_service";
   [...]
   options.Audience = "srapi";
});
```

Wie man feststellen kann, sind diese Konfigurationen schon recht umfangreich, obwohl es sich in dieser Version schon um eine sehr leichtgewichtige Implementierung von OAuth2 handelt. In (1) wird der Identity Server zum Projekt hinzugefügt. Zusätzlich wird auf den ‘ProfileService‘ sowie den ‘ResourceOwnerPasswordValidator‘ verwiesen, welche anschließend initialisiert werden müssen. In (2) wird noch die ‘Authority‘ und die ‘Audience‘ gesetzt. Die ‘Authority‘ garantiert zusätzlich, dass das Token nicht von einem anderen Identity Server ausgestellt wird. Die ‘Audience‘ gibt noch einmal an, dass das ausgestellte Token nur Zugriff auf eine entsprechende ‘srapi‘(Stirnraten-API) Ressource hat.

```
new ApiResource("srapi", "Stirnraten API")
{
    ApiSecrets = new List<Secret>()
    {
    new Secret(CustomClientSecret.Sha256())
    }
}
```

Zusätzlich müssen noch die beiden in den Grundlagen erwähnten Flows (‘ClientCredentials‘ und ‘ResourceOwnerPassword‘) implementiert werden.

```
{
[...]
new Client
{
    ClientId = CustomClientId,
    AllowedGrantTypes = GrantTypes.ClientCredentials,
    ClientSecrets =
    {
    new Secret(CustomClientSecret.Sha256())
```

```
    },
    AllowedScopes =
    {
    "srapi"
    }
},

new Client
{
    ClientId = "sr.client",
    AllowedGrantTypes = GrantTypes.ResourceOwnerPassword,
    ClientSecrets =
    {
    new Secret("secret".Sha256())
    },
    AllowedScopes =
    {
    "srapi"
    }
}
```

Durch diese Flows ist garantiert, dass die API grundsätzlich geschützt ist, d.h. auch dann wenn Benutzer keine Benutzerdaten hinterlegt haben. Werden allerdings benutzerspezifische Zugänge hinterlegt, erhalten diese noch mehr Zugriffsrechte auf die API. Dies wird im Bereich 5.2 deutlich.

Wenn eine Anfrage mit Benutzernamen und Passwort gestellt wird, ruft der Identity Server in seinem Abarbeitungszyklus folgende Methode ab:

```
public async Task ValidateAsync(ResourceOwnerPasswordValidationContext context)
{
(1)
var user = await _unitOfWork.UserRepository.GetUserByNameAndPasswordAsync(context.Use
context.Password);

(2)
if (user == null)
{
context.Result = new GrantValidationResult(
TokenRequestErrors.InvalidGrant,
"invalid custom credential");
return;
}
```

```
if (!user.Active)
{
context.Result = new GrantValidationResult(
TokenRequestErrors.InvalidClient,
"User was deactivated by admin");
return;
}

(3)
context.Result = new GrantValidationResult(
subject: user.Id.ToString(),
authenticationMethod: "custom",
claims: GetUserClaims(user)); //get user claims
}
```

In (1) wird ein Benutzer gesucht, welcher mit dem übergebenen Namen und Passwort übereinstimmt. In (2) wird dieser validiert und in (3) das Token anhand der 'Claims' generiert. 'Claims' sind vereinfacht ausgedrückt, zusätzlich Informationen, welche man in dem Token übergeben möchte.

```
return new[]
{
new Claim("user_id", user.Id.ToString() ?? ""),
new Claim(JwtClaimTypes.Name, user.Name),
new Claim(JwtClaimTypes.Role, user.Role)
};
```

In der umgesetzten API wird eine 'user_id', der 'Name' sowie die 'Role' übergeben. Alles wird ggf. von anderen Microservices benötigt, um eine entsprechende Autorisierung zu gewährleisten.

Abbildung 15 und 16 zeigen wie über eine POST Abfrage die entsprechenden Token ausgestellt werden können.

Enkodiert sieht so ein ausgestellter Benutzer-Token wie folgt aus:

```
[...]
"iss": "http://identity_server_service",
"aud": [
"http://identity_server_service/resources",
"srapi"
],
```

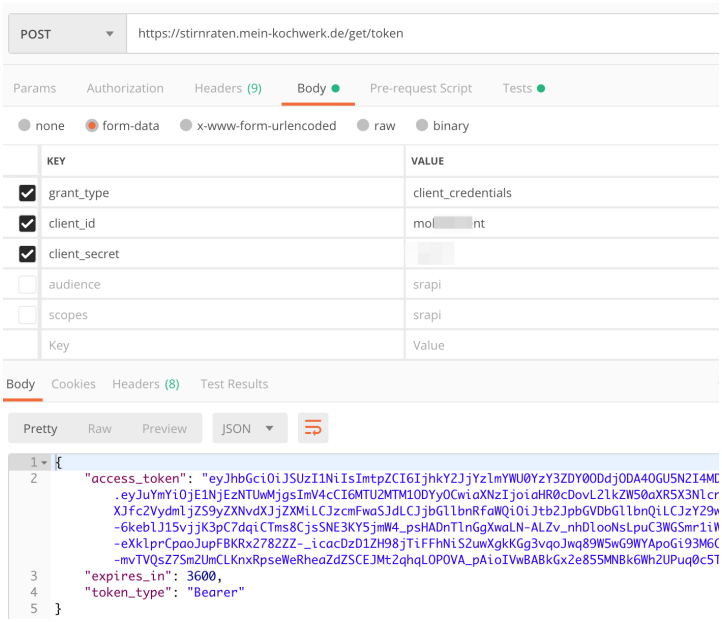

Abbildung 15: Über Postman gesendeter Client Credential Flow. Mit Hilfe dieses Tokens erhält man für 3600 Sekunden (eine Stunde) beschränkten Zugang zur API, um z.B. Kategorien abzurufen, neue Wörter einzusenden oder ein Benutzerkonto anzulegen.

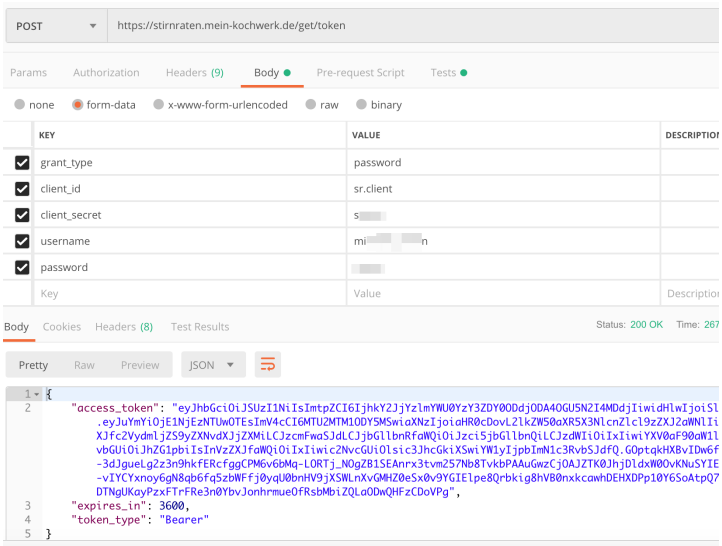

Abbildung 16: Über Postman gesendeter Password Flow. Er ist ebenfalls 3600 Sekunden lang gültig und hat mehr Berechtigung, wie z.B. das Speichern eines Benutzerprofils.

```
"client_id": "sr.client",
[...]
"role": "admin",
```

```
"user_id": "1",
"scope": [
"srapi"
],
"amr": [
"custom"
]
[...]
```

Durch diese Informationen kann das API-Gateway bereits eine Autorisierung vornehmen. Wie dies im Detail funktioniert, wird im Abschnitt **??** deutlich.

5.2 Umsetzung API-Gateway

Ähnlich wie bei dem Identity Server müssen für Ocelot auch gewisse Bibliotheken über NuGet hinterlegt werden.

```
 <PackageReference Include="IdentityServer4.AccessTokenValidation" Version="3.0.0-pre
<PackageReference Include="IdentityServer4" Version="2.4.0" />
<PackageReference Include="Ocelot" Version="11.0.2" />
<PackageReference Include="Microsoft.AspNetCore.Authentication.JwtBearer" />
```

Durch diese Pakete wird zum einen das Ocelot Gateway eingebunden, zum anderen wird der Authentifizierungsmechanismus zum Identity Server vereinfacht. Des Weiteren müssen Verbindungsdaten hinterlegt werden, die garantieren, dass das Gateway den Identity Server erreichen kann. Diese werden in der Startup.cs hinterlegt.

```
(1)
var authenticationProviderKey = "NTT9N7MXLJN9";

(2)
void Options(IdentityServerAuthenticationOptions o)
{
   o.Authority = "http://identity_server_service";
   o.ApiName = "srapi";
   o.RequireHttpsMetadata = false;
   o.SupportedTokens = SupportedTokens.Both;
   o.ApiSecret = "xxxxxx";
}
services.AddAuthentication()
.AddIdentityServerAuthentication(authenticationProviderKey, Options);

[...]
(3)
await app.UseOcelot();
[...]
```

In (1) muss ein sogenannter ‘Authentication Provider Key‘ gesetzt werden. Dies ist obligatorisch vorgegeben von Ocelot und notwendig, um weitergeleitete Requests eindeutig zuzuordnen. In (2) werden die Optionen für die Verbindung zum Identity Server definiert. Diese Konfigurationen müssen mit den Einstellungen aus dem zuvor erwähnten Identity Server übereinstimmen. In (3) wird noch einmal explizit ausgedrückt, dass Ocelot auch verwendet werden soll.

Um eingehende Request zu verarbeiten, verwendet Ocelot eine JSON, in dem sogenannte ReRoutes (Weiterleitungen) hinterlegt werden.

```
"ReRoutes": [
 {
 (1)
 "DownstreamPathTemplate": "/api/customers",
 (2)
 "DownstreamScheme": "http",
 "DownstreamHostAndPorts": [
    {
    (3)
    "Host": "customer_service",
    "Port": 80
    }
  ],
  (4)
  "UpstreamPathTemplate": "/api/stats",
  (5)
  "AuthenticationOptions": {
  "AuthenticationProviderKey": "NTT9N7MXLJN9",
  "AllowedScopes": [
    "srapi"
  ]
  },
  (6)
  "RouteClaimsRequirement": {
  "role": "admin"
  }
 },
[...]
]
```

Diese dargestellte ReRoute zeigt bereits viele Vorteile von Ocelot. Durch (1) wird das ‘DownstreamPathTemplate‘ definiert. D.h. das Gateway präsentiert über das ‘UpstreamPathTemplate‘ (5) die öffentlichen Schnittstellen, welche man als Client anspricht. Dadurch lässt sich das Weiterleiten flexibel gestalten. Zusätzlich ist es nicht zwingend

notwendig, dass wenn das ‘DownstreamPathTemplate‘ seine Route ändert, die Clienten davon betroffen sind, da das ‘UpstreamPathTemplate‘ gleichgeblieben ist.

Das ‘DownstreamScheme‘ (2) ist http, da die Microservices zu denen weiterleitet wird, nur in einem lokalen Netz befinden. Das hat den Vorteil, dass die Microservices nur über das Gateway zu erreichen sind. So kann garantiert werden, dass kein Dritter Zugriff auf die Services hat ohne über das Gateway zu gehen.

In (3) wird definiert an welchen Microservice weitergeleitet werden soll. In diesem Beispiel der ‘customer_service‘.

In (5) findet die Authentifizierung statt: Jeder Request welcher eingeht, muss im Token als Scope die ‘srapi‘ enthalten. In diesem Beispiel wird bereits auch autorisiert. Denn es wird die Rolle ‘admin‘ erwartet. D.h. wenn ein Request kein gültiges Token oder die entsprechende Rolle hat, wird der Request abgelehnt.

5.3 Asynchrone Kommunikation

// ieine Queue umsetzen (RabbitMQ, Kafka...)

5.4 Service Architektur

// nginx vom Hoster // deployment // Grafik erstellen, welche Services es gibt und wie diese Kommunizieren // Docker erwähnen und Beispiel einfügen

6 Fazit

Gelungen, weil

6.1 Ausblick

- Loadbalancing - ELK Stack - Service Mash - Kubernetes (Orchestrierung) - Sichtbarkeit von Microservices (was soll alles erreichbar sein): Also nur das Gateway und/oder auch die Microservices

Tabellenverzeichnis

Abbildungsverzeichnis

Literatur

[1] Mark Fussel (msfussell). *Einführung in Microservices in Azure - Microsoft-Dokumentation*. abgerufen am 9.4.2019. 2017. URL: `https://docs.microsoft.com/de-de/azure/service-fabric/service-fabric-overview-microservices`.

[2] Amine El Ayadi. *Webservices: REST vs. SOAP*. Hochschule für Angewandte Wissenschaften Hamburg. 2008.

[3] Ferdinand Birk. „Microservices - Eine State-of-the-Art Bestandsaufnahme und Abgrenzung zu SOA“. Universität Ulm, 2016.

[4] Björn Bohn. *Podman*. abgerufen am 27.5.2019. 2019. URL: `https://www.heise.de/developer/meldung/Die-Docker-Alternative-Podman-erreicht-Version-1-0-4281333.html`.

[5] Cesar. *Designing and implementing API Gateways with Ocelot in .NET Core containers and microservices architectures*. abgerufen am 29.5.2019. 2018. URL: `https://devblogs.microsoft.com/cesardelatorre/designing-and-implementing-api-gateways-with-ocelot-in-a-microservices-and-container-based-architecture/`.

[6] Antoine Duprat. *How to choose a Message Queue*. abgerufen am 2.6.2019. 2018. URL: `https://medium.com/linagora-engineering/how-to-choose-a-message-queue-247dde46e66c`.

[7] Sebastian Gauder. „A competitive food retail architecture with microservices“. 2019.

[8] PIETER HUMPHREY. *Understanding When to use RabbitMQ or Apache Kafka*. abgerufen am 2.6.2019. 2017. URL: https://content.pivotal.io/blog/understanding-when-to-use-rabbitmq-or-apache-kafka.

[9] Matt McLarty Irakli Nadareishvili Ronnie Mitra und Mike Amundsen. *Microservice Architecture - Aligning Principels, Practices, and Culture*. O Reilly, 2016.

[10] solid IT gmbh. *DB-Engines Ranking*. abgerufen am 21.5.2019. 2019. URL: https://db-engines.com/de/ranking.

[11] Kevin Klöckner. *Im Vergleich: NoSQL vs. relationale Datenbanken*. Universität Siegen. 2015.

[12] Paulo A. Pereira Morgan Bruce. *Microservices in Action*. Manning, 2019.

[13] Sven Neuhaus. *Betont schlank*. abgerufen am 21.5.2019. 2016. URL: https://www.heise.de/ix/artikel/Betont-schlank-506574.html.

[14] Dennis Peuser Nhiem Lu Gert Glatz. *Moving mountains – practical approaches for moving monolithic applications to Microservices*. University of Applied Science und Arts, Dortmund, Germany, adesso AG, Dortmund, Germany. 2017.

[15] olprod hongyes olprod. *OWIN-OAuth 2.0-Autorisierungsserver*. abgerufen am 2.6.2019. 2019. URL: https://docs.microsoft.com/de-de/aspnet/aspnet/overview/owin-and-katana/owin-oauth-20-authorization-server.

[16] Aaron Parecki. *OAuth 2.0 Client Credentials Grant*. abgerufen am 11.5.2019. o. J. URL: https://oauth.net/2/grant-types/client-credentials/.

[17] Jeff Patton. *User Story Mapping - Die Technik für besseres Nutzerverständnis in der agilen Produktentwicklung*. O Reilly, 2015.

[18] phlegx. *Create multiple users and databases*. abgerufen am 21.5.2019. 2016. URL: https://github.com/docker-library/postgres/issues/151.

[19] Chris Richardson. *Microservice Pattern*. Manning, 2019.

[20] Golo Roden. *Domain-driven Design erklärt*. abgerufen am 15.3.2019. 2016. URL: https://www.heise.de/developer/artikel/Domain-driven-Design-erklaert-3130720.html?seite=all.

[21] Heiko Rupp. *Das Service Mesh für verteilte Systeme*. abgerufen am 29.5.2019. 2018. URL: https://www.heise.de/developer/artikel/Istio-Das-Service-Mesh-fuer-verteilte-Systeme-4153426.html.

[22] Cesar de la Torre (cesardelatorre). *Implementieren ereignisbasierter Kommunikation zwischen Microservices*. abgerufen am 16.4.2019. 2018. URL: https://docs.microsoft.com/de-de/dotnet/standard/microservices-architecture/multi-container-microservice-net-applications/integration-event-based-microservice-communications.

[23] o. V. *App-Container: 5 professionelle Docker-Alternativen im Überblick*. abgerufen am 27.5.2019. 2017. URL: https://t3n.de/news/docker-alternativen-container-783741/.

[24] o. V. *AWS SDK für .NET*. abgerufen am 28.5.2019. o. J. URL: https://aws.amazon.com/de/sdk-for-net/.

[25] o. V. *Erste Schritte mit Endpoints in einer flexiblen App Engine-Umgebung (.NET)*. abgerufen am 28.5.2019. o. J. URL: https://cloud.google.com/endpoints/docs/openapi/get-started-app-engine-dotnet.

[26] o. V. *Istio Quickstart*. abgerufen am 29.5.2019. o. J. URL: https://istio.io/docs/setup/kubernetes/install/kubernetes/.

[27] o. V. *Kafka - A distributed stream platform*. abgerufen am 2.6.2019. o. J. URL: https://kafka.apache.org/uses.

[28] o. V. *Plan an API Gateway system*. abgerufen am 1.5.2019. o. J. URL: https://docs.oracle.com/cd/E55956_01/doc.11123/administrator_guide/content/admin_planning.html.

[29] o. V. *Was ist Docker?* abgerufen am 11.5.2019. o. J. URL: https://www.redhat.com/de/topics/containers/what-is-docker.

[30] Eberhard Wolff. *Das Microservice Praxisbuch - Grundlagen, Konzepte und Rezepte*. dpunkt.verlag, 2018.

[31] Eberhard Wolff. *Flexible Software Architectures*. Leanpub, 2016.