



universität
wien

BACHELORARBEIT / BACHELOR'S THESIS

Titel der Bachelorarbeit / Title of the Bachelor's Thesis

„Resilient deployments with Istio“

verfasst von / submitted by

Ruslan Jelbuldin 01407036

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Bachelor of Science

Wien, 2021 / Vienna, 2021

Studienkennzahl lt. Studienblatt /
degree programme code as it appears on
the student record sheet:

A 033 521

Studienrichtung lt. Studienblatt /
degree programme as it appears on
the student record sheet:

Bachelor Computer Science UG2002

Betreut von / Supervisor:

Amine El Malki BSc. MSc.
Research Group Software Architecture

Contents

1	Introduction	3
2	Monolithic vs. Distributed Approach	4
3	Microservices	5
3.1	Microservices & Containerization	7
3.2	Microservices & Cloud Computing	8
3.3	Microservices & Kubernetes	9
4	Service Meshes	10
4.1	Consul Connect	11
4.2	Istio	11
4.3	Linkerd	11
4.4	Comparison of Istio, Linkerd and Consul	11
5	Implementation	13
5.1	Technology stack	13
5.2	Distributed Calculation Cloud	13
5.3	How to run	19
6	Evaluation	20
6.1	Canary deployment with Istio as part of Routing	20
6.2	Fault Injection	23
6.3	Fault Injection - Timeout	23
6.4	Fault Injection - HTTP 5XX	27
6.5	Problems with testing and outlier detection	29
7	Conclusion	31
8	Future Work	31

Abstract

The purpose of this thesis is to demonstrate on a practical example, how service meshes could be integrated into a complex distributed system. We will briefly cover how modern software engineering came to the point, where such an approach became necessary and why. To do so, we will need to scratch and analyse the surface of the topic distributed systems, cloud computing, containerisation and container orchestration and understand how each of these concepts are related. This will consequently bring us to the understanding of the concept of service mesh and shed light on its purpose and application area. Thereafter, we will get acquainted with ISTIO (open source service mesh platform) and integrate it to the distributed system on a practical example. To sum it all up, we will analyse the results and observe how ISTIO is gathering metrics and discuss and analyse it.

Keywords: Microservices, Distributed Systems, Software Architecture, Service Mesh, Cloud Computing, Docker, Kubernetes, ISTIO

1 Introduction

Since the first appearance of programming languages in the middle of 20th century and since the level of abstraction had started to increase, the process of building software systems started to gain in complexity. Nonetheless, these systems were still relatively simple when compared to modern super complex one's. At the beginning of software engineering times, there was no such thing as internet. Every built system was created to work locally on a single machine. Those machines had very limited data processing abilities. Nonetheless, this all was still sufficient enough for the tasks of that time.

With the lapse of time technologies evolved: machines became more advanced and were able to process larger amounts of data within shorter periods, new programming paradigms were introduced, which opened new doors for research and improvement. Programming languages started to slowly morph from 0, 1 and punch card gibberish to a text that could have been read by people. They became more high-level. Very slowly, the steepness of the learning curve began to decline, introducing more people to computer science. These factors influenced those small systems too and they consequently started to grow. Simple scripts turned into more complex and more abstract programming code. Tasks became more complex too due to increased power of computers.

In 1966 - 1967 the US computer scientist Allen Kay first introduced the concept of Object Oriented Programming at grad school. He mentioned that - "The big idea was to use encapsulated mini-computers in software which communicated via message passing rather than direct data sharing — to stop breaking down programs into separate "data structures" and "procedures"" [14]. Code pieces started to decouple into separate files, where each file had served it's own purpose. Although programs were split into file chunks, they still were running on one single machine and as a single instance and couldn't be accessed from elsewhere. It was one of the ceilings that computer science faced before invention of the internet and its worldwide spreading and overall integration.

But even before internet computer scientists were thinking on how to handle growing system complexity. The concept of Software Architectures, that started to emerge in early sixties was aimed to solve the problem. The idea was to systematize and cleverly decouple program components into an understandable structure that would make sense to anyone who is ever going to work with it. More complex systems started to appear. Development teams were growing. Depending on system application area, different architectures patterns were created with the laps of time. The most widely used are Layered (n-tier), Event Driven, Microkernel and with worldwide internet spreading - Microservices patterns. The first 3 were and still are great for their application area and each is actively used nowadays. However, back in time growing software complexity made it harder and harder to scale programs that were based on them. They were monolithic.

In nineties internet started it's world conquer and created new opportunities for software development and new challenges. It was spreading at an extreme pace and data transmission speed was increasing. In 2005 Dr. Peter Rogers first used the term "Web Micro Service". He described it as a way to split monolithic designs into multiple components/Processes. thereby making the codebase more granular and manageable [13]. As the time passed the pattern was widely adopted especially with appearance of cloud computing. Microservices and Cloud Computing became indivisible. However, the progress didn't stop and industry faced the new ceiling. Distributed systems were becoming more complex and it became harder to track data flow between services. It

became difficult to determine what has failed and where. Especially in containerized services in Kubernetes nodes. Demand for tracking tools appeared and one of these tools is ISTIO.

But let's first have a closer look at Architectures, containerization and orchestration concepts before diving into ISTIO and sum up why we ended up needing service meshes at all.

2 Monolithic vs. Distributed Approach

In modern software engineering Architectures could be split into 2 main types:

- Monolithic
- Distributed

Over time and with appearance of internet and cloud technologies some monolithic systems were replaced by distributed systems. This happened because some huge enterprise applications mainly relied on big number of features that were all part of a single program and failure of one part could cause failure of entire application, which could result in huge losses for the company. After 2010 big players started to migrate their legacy systems to cloud. However, this does not mean that monolithic approach is dead. It's alive and feeling well in smaller applications. On the other hand, big systems, like bank chains, government, military sector and IT giants shifted their sights on distributed approach, where microservices play bigger role.

Back in time applications were smaller and there were neither demand in decoupling services nor available means and infrastructure for building them. Therefore, monolithic apps were mostly dominating until the end of last century. Distributed systems, on the other hand, first appeared the mainstream stage in 1998, when the term Service-Oriented Architecture was first introduced. Not so long after, in 2005, the Microservice architecture, the ideological successor of SOA, entered the stage and became the backbone of modern cloud computing.

Comparison of Architectures	
Monolithic	Microservices
- Application is a single, integrated software instance	- Application is broken into modular components. This makes the application easier to understand, develop, test, and become more resilient to architecture erosion.[3] It can be considered as main advantage of microservices and this benefit is often argued in comparison to the complexity of monolithic architectures. [20]
- Application instance resides on a single server or VM	- Application can be distributed across the clouds and datacenter
- Updates to an application feature require reconfiguration of entire app	- Adding new features only requires those individual microservice to be updated
- Network services can be hardware based and configured specifically for the server	- Network services must be software-defined and run as a fabric for each microservice to connect to
-	- Scalability - Microservices can be implemented and deployed independently namely they run in independent processes and can be scaled, monitored and maintained independently. [5]
-	- Legacy migration: Microservices is considered as an effective solution for migrating existing monolithic software application.[15] [19]

3 Microservices

Microservices as an architectural style originate from Service-Oriented Architecture or SOA. The idea behind SOA is to create reusable and specialized components that work independently from one another. Key difference between two approaches is scope. SOA is enterprise oriented whereas Microservices' scope is application .

The above figure clearly shows us the scope difference between two approaches. In SOA we are speaking about multiple monolithic applications interconnected via enterprise network. The system itself is way bigger. Each application is a separate module that consists of various pieces that build it up as a single monolithic program. All these pieces are tightly coupled and entire application depends on the healthiness

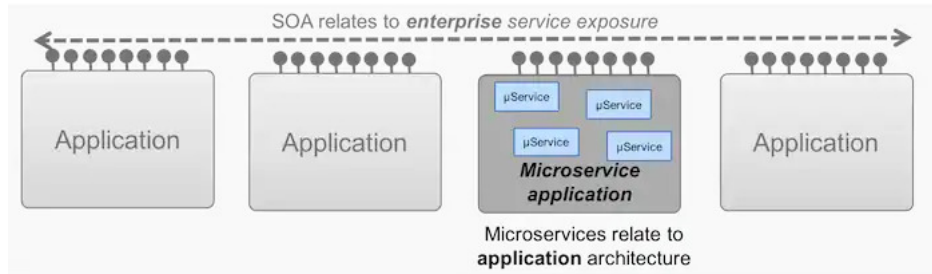


Figure 1: SOA vs. Microservice

of each piece. Because it can easily happen that if one fails, the entire application can collapse as a house of cards, but not necessarily.

Microservice application, on the other hand, has these pieces decoupled. This loose coupling isolates each piece and makes them independent even on technology stack level. For instance, if we have an IOT app that monitors weather measurements, we could have sensors software written in C, calculations module written in C++, messaging service in Java and UI could be an Electron/Web/Mobile app written in Flutter. Each of the services could be run from different location and doesn't require enterprise network. Interservice communication usually happens via exposed API endpoints. A common practice of deployment of microservices apps is containerization.

However, there are few moments to think about when considering microservices as architecture of choice. Although, it offers great scalability and encapsulation capabilities, it is considered to be way slower than monolithic approach. In monolithic apps, since each module is located and run on one machine, it has direct access to machines' computing power. Delays are minimal. Whereas, microservice based systems are distributed, hence could, theoretically, be run on different servers, that could even be located in different countries. The data between processes flows over the network with all the ensuing consequences like longer transfer time and possible security issues. Figure below sums up pros and cons of microservice architecture[?].

Advantages and disadvantages of Microservice Architecture	
PRO	CON
<ul style="list-style-type: none"> - Versatile — microservices allow for the use of different technologies and languages - Easy to integrate and scale with third-party applications - Microservices can be deployed as needed, so they work well within agile methodologies - Solutions developed using microservice architecture allow for fast and continuous improvement of each functionality - Maintenance is simpler and cheaper — with microservices you can make improvements or amendments one module at a time, leaving the rest to function normally - The developer can take advantage of functionalities that have already been developed by third parties — you don't need to reinvent the wheel here, simply use what already exists and works - A modular project based on microservices evolves more naturally, it's an easy way to manage different developments, utilising the resources available, at the same time 	<ul style="list-style-type: none"> - Because the components are distributed, global testing is more complicated - It's necessary to control the number of microservices that are being managed, since the more microservices that exist in one solution, the more difficult it is to manage and integrate them - Microservices require experienced developers with a very high level of expertise - Thorough version control is required - Microservice architecture can be expensive to implement due to licensing costs for third party apps

3.1 Microservices & Containerization

Another important concept is containerization. One of the biggest problems with traditional development is that when we try to run our app on another machine, a high chance exists, that app will not run properly/at all because of version inconsistency of some packages, libraries, OS, programming languages, compilers and many many more other small things. Containerization solves this huge problem.

If we put it simple, containerization is packaging the source code of the app into a bare minimal OS setup with minimal set of libraries and dependencies that are required to launch the application. This package is called a container. Containers weigh less and are more resource-efficient than Virtual Machines, which makes it much faster to deploy and which also reduces overall costs including licensing. According to IBM's

latest survey¹ - "61% of container adopters reported using containers in 50% or more of the new applications they built during the previous two years; 64% of adopters expected 50% or more of their existing applications to be put into containers during the next two years." [?] The massive popularization of containerization began with introduction of Docker engine in 2013 which became industry standard. Other popular solutions are: LXC (Linux), Hyper-V and Windows Containers, Podman & others.

One of the most promoted conceptual advantages of containerization is that the code they contain could be "written once and run everywhere". It gives it the following advantages:

- improved development speed
- prevention of cloud vendor lock-in
- fault isolation
- ease of management
- simplified security and many more [?]

This already makes containers ideal companions for microservices. By building our entire distributed system on containers we can avoid database bottlenecks and enable Continuous Integration / Continuous Delivery (CI/CD) pipelines. As consequence system scalability is also greatly improved, since each service can be individually updated without influencing other ones. If necessary, we could even rewrite existing service using entirely different technology stack. Furthermore, containers are more secure, since they have less entry points that should be observed, making them easier to monitor.

3.2 Microservices & Cloud Computing

Cloud computing became integral part of modern software engineering and for a good reason. As already mentioned previously, with the lapse of time systems had become more complex and old-school server-client approach can not handle the growing codebases and data flow. Cloud computing brought application decoupling to the next level. Now we don't need expensive servers that will host our backend. We can just rent them and not only deploy our entire app there but also deliver entire storages, databases, servers, analytics etc. over the internet. Service providers like Google, Amazon and Microsoft provide developers with power of their data centers. Basically speaking, we delegate computation to these server providers. They provide us with "clouds" where we can manage our systems the way we want. Pricing is based on how much computing power is used. So it's relatively cheap to start. Clouds could be public, private and hybrid. Depending on how much control we need over our project we can choose over the following types² of cloud services:

- Infrastructure as a service (IaaS)
- Platform as a service (PaaS)
- Serverless computing
- Software as a service (SaaS)

Cloud computing caused the appearance of new software concept - Cloud native applications that entirely reside in clouds. Microservices wrapped in containers are naturally fitting into this concept, as they are made of independent modules, each of which can be deployed to the cloud and leverage its functionality and computation power.

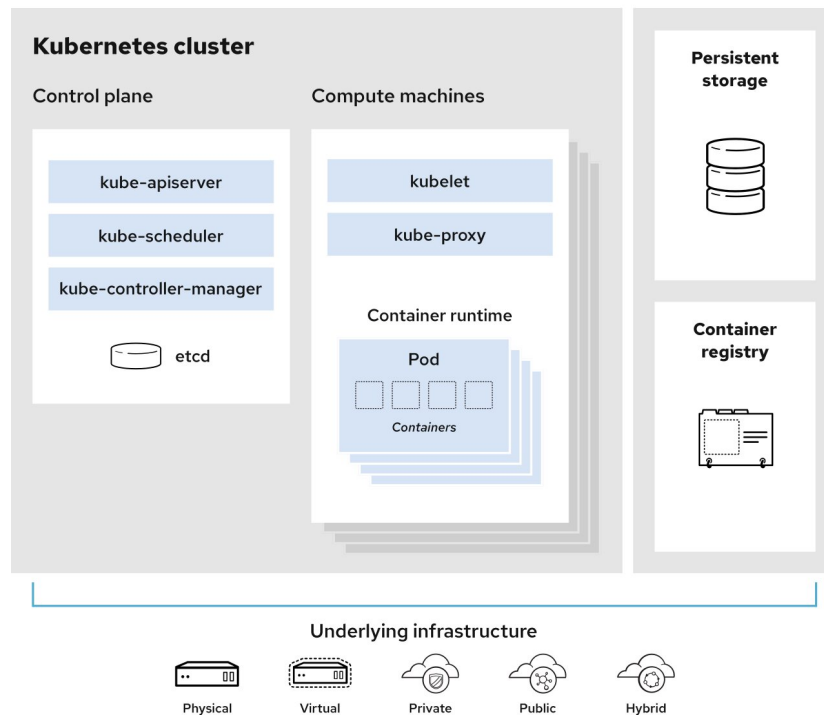
¹<https://www.ibm.com/downloads/cas/VG8KRPRM>

²<https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/#benefits>

3.3 Microservices & Kubernetes

However, industry is not stopping there. The number of containers that are being deployed to cloud grows, and it's getting harder and harder to operate them. In 2014 Google introduced Kubernetes also known as k8s and "kube", an open-source container orchestration tool that manages clusters of Virtual machines and Schedules container deployment. It will take an entire thesis to describe Kubernetes in detail, but in a nutshell its main objective is to keep deployed containers up and running by automating many of the manual processes involved in deploying. Containers are being run in nodes that are organized in clusters. Nodes are the instances where our microservices are running. Clusters contain control pane that is responsible for node state management. Clusters can be used as development, testing and production environments.

Having containers with microservices deployed to Kubernetes nodes and grouped into appropriate clusters, it becomes relatively easy to test, scale and update each of the individual services. Moreover, Kubernetes is able to perform health-checks, failovers, networking, service discoveries, load balancing, container life cycle management and many other useful operations. This all makes Kubernetes play a giant role in CI-CD and a very useful tool for complex applications. Cloud platforms like Google, AWS, MS Azure provide access to Kubernetes. Red-Hat also provides an alternative called Open Shift. Below figure shows the example Kubernetes cluster. ³



³https://www.redhat.com/cms/managed-files/kubernetes_diagram-770x71700v2.svg?itok=Z6bFR9q1

4 Service Meshes

A service mesh is a dedicated infrastructure layer that facilitates communication between (micro)services using a proxy.[12] This infrastructure level provides some benefits, such as providing observability into communications, secure connections or automating retries and backoff for failed requests.[1]

Even though Kubernetes helps to orchestrate containers, it is still hard to track how individual microservices interact with each other. Kubernetes can handle failovers, but it doesn't provide comprehensive tools for monitoring interservice communication. If we think about that, we can build microservices in such a way that this monitoring is possible, but the more complexer becomes communication, the harder it is to monitor it. Here is where service meshes come to rescue.

Basically a service mesh is abstraction to which we delegate monitoring duties. No new functionality is being added to service runtime. What's different about a service mesh is that it takes the logic governing service-to-service communication out of individual services and abstracts it to a layer of infrastructure[?].

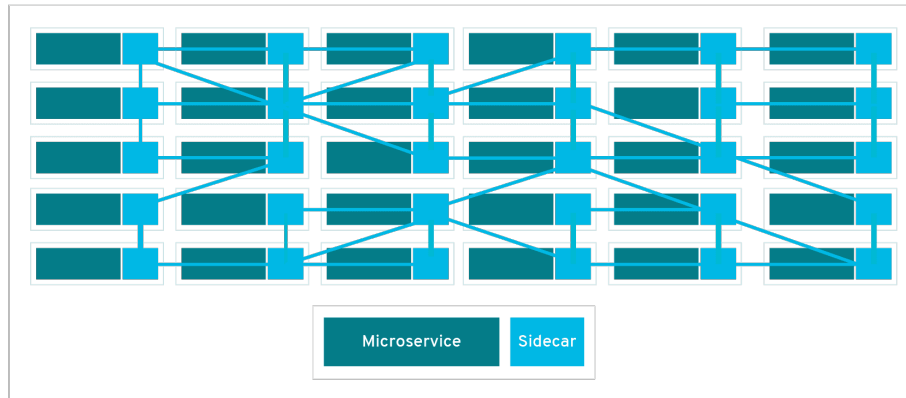


Figure 2: Proxy network [17]

We build it in to an app as an array of proxies. Requests are routed between microservices through proxies in their own infrastructure layer. These proxies are also called "sidecars" since they run not within but alongside microservices. All together these meshes form a mesh network. Every time a new service is added the new proxy instance is assigned to it. Proxies will monitor every aspect of service-to-service communication and create metrics report.

Istio is such a service mesh solution. It provides necessary functionality to manage traffic, security and observability of microservices. In below sections we will discuss how it works in greater detail on practical example.

There are three leading, open source solutions in the Kubernetes ecosystem for Service Mesh. As number of microservices grows, it creates challenges around figuring out how to enforce and standardize things like routing between multiple services/versions, authentication and authorization, encryption, and load balancing within a Kubernetes cluster. [16] Each service mesh solution has its benefits and drawbacks.

4.1 Consul Connect

Consul is a solution providing a full featured control plane with service discovery, configuration, and segmentation functionality. Each of these features can be used individually as needed, or they can be used together to build a full service mesh. [4] Consul Connect uses an agent installed on every node as a DaemonSet which communicates with the Envoy sidecar proxies that handles routing and forwarding of traffic. [16]

4.2 Istio

Istio is a kubernetes native solution, which is discussed in details in this thesis. Istio has separated its data and control planes by using a sidecar loaded proxy which caches information so that it does not need to go back to the control plane for every call. The control planes are pods that also run in the Kubernetes cluster, allowing for better resilience in the event that there is a failure of a single pod in any part of the service mesh.[16]

4.3 Linkerd

Linkerd is the 2nd popular service mesh on Kubernetes, which architecture mirrors Istio's closely, with an initial focus on simplicity instead of flexibility. Linkerd is a part of the Cloud Native Foundation (CNCF), which is the organization responsible for Kubernetes.[16]

4.4 Comparison of Istio, Linkerd and Consul




	 Istio	 LINKERD Linkerd v2	 Consul
Supported Workloads	Does it support both VMs-based applications and Kubernetes?		
Workloads	Kubernetes + VMs	Kubernetes only	Kubernetes + VMs
Architecture	The solution's architecture has implications on operation overhead.		
Single point of failure	No – uses sidecar per pod	No	No. But added complexity managing HA due to having to install the Consul server and its quorum operations, etc., vs. using the native K8s master primitives.
Sidecar Proxy	Yes (Envoy)	Yes	Yes (Envoy)
Per-node agent	No	No	Yes

Figure 3: Comparison by workloads and architecture [16]

Traffic Management			
Blue/Green Deployments	Yes	Yes	Yes
Circuit Breaking	Yes	No	Yes
Fault Injection	Yes	Yes	Yes
Rate Limiting	Yes	No	Yes

Figure 4: Comparison by traffic management [16]

Chaos Monkey-style Testing			
Traffic management features allow you to introduce delays or failures to some of the requests in order to improve the resiliency of your system and harden your operations			
Testing	Yes- you can configure services to delay or outright fail a certain percentage of requests	Limited	No
Observability			
In order to identify and troubleshoot incidents, you need distributed monitoring and tracing.			
Monitoring	Yes, with Prometheus	Yes, with Prometheus	Yes, with Prometheus
Distributed Tracing	Yes	Some	Yes

Figure 5: Comparison by testing and observability [16]

5 Implementation

5.1 Technology stack

Technologies used: Java 11, Gradle, Python 3.7, Docker, Kubernetes, Istio, java script, canvasJS.

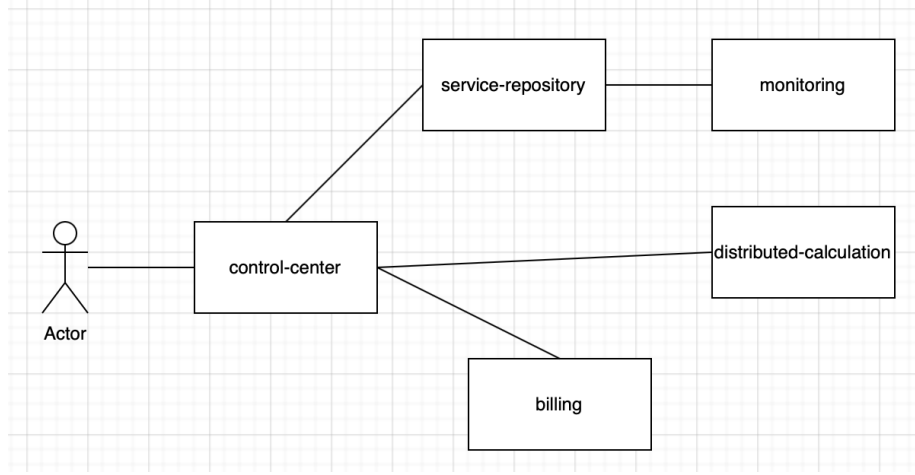


Figure 6: Distributed Calculation Cloud

5.2 Distributed Calculation Cloud

The goal of the study is testing of resilience features of Istio, understanding of how microservices can be managed and also how useful is this service mesh. To be able to test it, the distributed application was created and deployed with kubernetes and Istio. The distributed calculation cloud application is a simple version of Google Genomics or the LHC Computation Grid.[6] The solution provided in this paper allow users to perform "long" running calculations in asynchronous and multi-threaded fashion. To prevent the uneven and excessive utilization of calculation services a billing service is created [6], so users can create their bank accounts and pay for the requested calculations. As hundred of calculation and billing services can be deployed, the service repository was implemented. It is a main microservice which enable other services to simply ask which microservice supports a desired task.

1. Service Repository. The crucial microservice that contains information about all registered microservices, supports dynamically querying and registering any microservices and their endpoints. All other microservices know the main endpoint of the service repository MS. It is possible to register microservice's information such as description, endpoint path and its functionality. The service repository keeps all the information about registered microservices up-to-date. If there is a microservice that does not respond or not active anymore, it will be immediately removed from the list of registrations. It is also possible to query a list of microservices which support a requested job. Up to N Microservices' instances,

that provide the same functionality can be registered. For example 3 calculation services can be registered, so a user can choose which one is better for his/her purposes.

HTTP	Path	Request Body	Request Parameters	Consumes
POST	/register	msName: String, msPort: Integer, msDescription: String, msFunction: String, msType: String	-	application/json
GET	/getRegisteredServices	-	-	
GET	/findServiceByFunction	-	function	
GET	/getMetrics	-	-	

Figure 7: Service Repository API

2. Distributed Calculation Service. This service simulates long running calculations such as, data analysis tasks or machine learning jobs. The service supports following calculations: addition of two numbers, calculation of two numbers, calculation of prime and Fibonacci numbers. Each calculation operation has its own endpoint, that is registered at the service repository.

HTTP	Path	Request Body	Request Parameters	Consumes
POST	/add	decimalOne: Double, decimalTwo: Double	-	application/json
POST	/multiply	decimalOne: Double, decimalTwo: Double	-	application/json
POST	/prime	-	n	-
POST	/fibonacci	-	n	-
GET	/health	-	-	-
GET	/getWorkloadByType/{type}	-	-	-
POST	/timeout	-	n	-
POST	/responseCode	-	n	-

Figure 8: Distributed Calculation Service API

3. Billing Service. The microservice implements a simple billing service, where users can create their accounts, deposit them, get account information and pay for the requested calculations. A price for a calculation is based on the workload

of each distributed calculation service instance and is changed dynamically, so if one of the calculation services is idle and the other one is loaded, the price for the last will be higher. For the sake of simplicity, a user can create/delete an account only with the first name, which is unique in this case.

HTTP	Path	Request Body	Request Parameters	Consumes
POST	/createAccount	-	user: String	-
POST	/depositAccount	-	user: String, amount: Double	-
POST	/chargeAccount	-	user: String, amount: Double	-
GET	/getAccountInfo	-	user: String	-
DELETE	/deleteAccount	-	user: String	-
GET	/health	-	-	-

Figure 9: Billing Service API

4. Service Control Center. The control center for the whole application and its main entry point. With this service users can request calculations, account information, deposit, charge and delete their accounts. It interacts with all microservices in the system and all incoming requests are redirected to a corresponding MS. The logic for calculation price is also implemented here. In Figure 6 is shown the communication between microservices after calculation is requested.

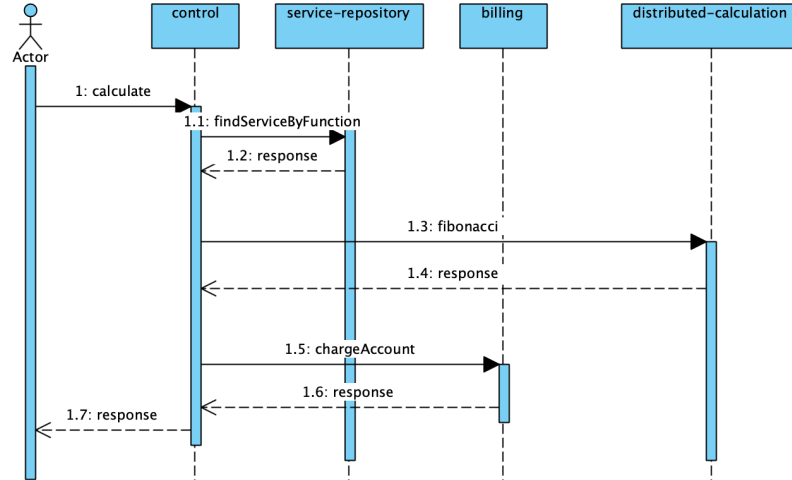


Figure 10: Successful calculation flow

- 1. A user requested a calculation via control panel. The requirement

includes the description about calculation type, price that the user is able to pay.

- 1.1. Control center requested a list of microservices and its endpoints, which are active and support the required calculation. The information about billing service was also requested.
- 1.2 All requested information was provided by service repository.
- 1.3 Control panel sends a calculation request to distributed calculation service.
- 1.4 The result of calculation is returned to control panel.
- 1.5 The User is charged.
- 1.6 OK from the billing service
- 1.7 The result of calculation is returned to the user.

HTTP	Path	Request Body	Request Parameters	Consumes
POST	/createAccount	-	user: String	-
POST	/depositAccount	-	user: String, amount: Double	-
POST	/chargeAccount	-	user: String, amount: Double	-
GET	/getAccountInfo	-	user: String	-
DELETE	/deleteAccount	-	user: String	-
POST	/calculate	user: String, calculationType: String, price: Double, firstNumber: Double, secondNumber: Double	-	-

Figure 11: Service Control Center API

5. Fake Behaviour Application. This application is connected to the control panel and replaces/simulates the frontend, from which customers can request the calculations, create and deposit their accounts.
6. Service Dashboard. The service provides a minimalistic website, where a user can monitor the service availability and workload. The service can access the service repository via ingress gateway, so it is an external html page. It can be considered as frontend for analytics service. But in this paper it was only used to control the workload of calculation services, hence it was not even deployed with kubernetes.
7. Analytics. The service provides information about estimated calculation time and has a simple API. It collects the information about registered microservices from service-repository and calculates the estimated time for the requested calculation type. It can be used as backend for monitoring applications.

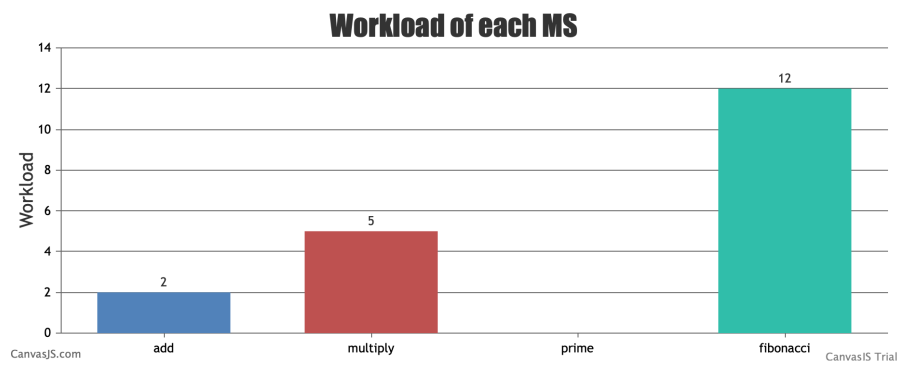


Figure 12: Service Dashboard

```
{
  "estimatedTime": 8.356241694424522,
  "msDescription": "Addition of two numbers.",
  "msFunction": "add",
  "msName": "172.17.0.11",
  "msPort": 8080,
  "msType": "calculation",
  "workload": 0
}
```

Figure 13: Analytics service response

HTTP	Path	Request Body	Request Parameters	Consumes
GET	/getAnalytics	-	function: String	-
GET	/version	-	-	

Figure 14: Analytics/Advanced Analytics API

- Advanced Analytics. It is an improved version of analytics, that can additionally predict estimated price in euro and dollars for requested type of calculation. The service was created for testing canary deployments with Istio.

```
{
  "estimatedPriceInDollar": 20.797515604090364,
  "estimatedPriceInEur": 21.797515604090364,
  "estimatedTime": 17.986259693769114,
  "msDescription": "Addition of two numbers.",
  "msFunction": "add",
  "msName": "172.17.0.11",
  "msPort": 8080,
  "msType": "calculation",
  "workload": 0
}
```

Figure 15: Advanced Analytics service response

The implementation of services was a part of DSE (Distributed Systems Engineering) course, where I implemented the distributed calculation service. However I had completely rewritten all other microservices, so it is a different communication logic withing the whole application. Moreover, I decided to implement microservices in different programming languages such as Java and Python, to have a polyglot stack, what is a common practice in distributed systems. I also added additional functionalities and endpoints to each microservice, so it will be easier to test istio resiliency features:

- The distributed calculation service was implemented in two versions, the first one with a standard set of endpoints and the second version has additional multiplication endpoint. It allows to demonstrate the canary deployment with help of Istio.
- Additional endpoints in the distributed calculation service were added: Now it is possible to set a response code, with which the MS should answer and also it is possible to set a response timeout for the microservice.

3. Health-checks were added to each MS.
4. New simple application for generating behaviour of users/clients was implemented.
5. New analytics service, that can predict estimated time of calculation.
6. New advanced analytics service, that can predict estimated time of calculation and price in euro and dollars.

5.3 How to run

There are following requirements for Linux and MacOS: Be sure that Istio supports the version of Kubernetes. The version of kubernetes - v.1.18.1. The version of Istio - 1.10.3. Minikube must be installed. At least 16GB of RAM, otherwise problems with running services. Deployment with Kubernetes and Istio:

- Clone the project from github:

```
git clone https://github.com/troublemaker92/resilient-microservices-with-istio.git
```

- Change directory:

```
cd resilient-microservices-with-istio
```

- start minikube:

```
minikube start
```

- Move to the Istio package directory.

```
cd istio/istio-1.10.3/
```

- Add the istioctl client to your path (Linux or macOS):

```
export PATH=$PWD/bin:$PATH
```

- Set default istio profile:

```
istioctl install --set profile=demo -y
```

- Add a namespace label to instruct Istio to automatically inject Envoy sidecar proxies for future application deployments: [11]

```
kubectl label namespace default istio-injection=enabled
```

- Deploy all applications with kubernetes:

```
kubectl apply -f k8s/service-repository-deployment.yaml;
kubectl apply -f k8s/calculation-1-deployment.yaml;
kubectl apply -f k8s/billing-deployment.yaml;
kubectl apply -f k8s/control-center-deployment.yaml;
kubectl apply -f k8s/analytics-deployment.yaml;
```

- Set the ingress ports:


```
export INGRESS_PORT=$(kubectl -n istio-system get service istio-ingressgateway -o jsonpath='{.spec.ports[0].port}')
export SECURE_INGRESS_PORT=$(kubectl -n istio-system get service istio-ingressgateway -o jsonpath='{.spec.ports[1].port}')
```
- Apply ingress gateway and virtual service


```
kubectl apply -f istio/ing_gateway.yaml;
kubectl apply -f istio/virt_svc.yaml;
```
- For monitoring be sure, that kiali and grafana are installed:


```
kubectl apply -f https://raw.githubusercontent.com/istio/istio/release-1.11/samples/addons/grafana.yaml
kubectl apply -f https://raw.githubusercontent.com/istio/istio/release-1.11/samples/addons/kiali.yaml
```
- Be sure that all services are up and running:


```
kubectl get all -A
```
- Start the python simulation app to mimic behaviour of customers:


```
python3 microservices/app-driver/calculation-driver.py
```

In the provided postman collection run `simulator_simulate` request
To stop the simulation run `simulator_stop` request in postman

NAMESPACE	NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
default	service/analytcs	ClusterIP	10.103.126.214	<none>	8080/TCP	128m
default	service/analytcs-advanced	ClusterIP	10.99.121.10	<none>	8080/TCP	128m
default	service/billing	ClusterIP	10.103.158.79	<none>	8080/TCP	128m
default	service/control	NodePort	10.111.43.55	<none>	8080:30000/TCP	128m
default	service/distributed-calculation-1	NodePort	10.100.77.75	<none>	8080:30002/TCP	128m
default	service/distributed-calculation-2	NodePort	10.100.121.88	<none>	8080:30003/TCP	128m
default	service/kubermates	ClusterIP	10.96.0.1	<none>	443/TCP	11d
default	service/service-repository	NodePort	10.99.185.67	<none>	8080:30005/TCP	128m
istio-system	service/grafana	ClusterIP	10.105.112.88	<none>	3000/TCP	8d
istio-system	service/istio-egressgateway	ClusterIP	10.110.165.206	<none>	80/TCP, 443/TCP	15d
istio-system	service/istio-ingressgateway	LoadBalancer	10.107.214.145	<pending>	15021:30909/TCP, 80:30439/TCP, 443:32457/TCP, 31400:30774/TCP, 15443:30504/TCP	15d
istio-system	service/istiod	ClusterIP	10.107.241.255	<none>	15010/TCP, 15012/TCP, 443/TCP, 15014/TCP	15d
istio-system	service/kiali	ClusterIP	10.100.93.35	<none>	20001/TCP, 9090/TCP	14d
istio-system	service/prometheus	ClusterIP	10.101.143.159	<none>	9090/TCP	14d
kube-system	service/kube-dns	ClusterIP	10.96.0.10	<none>	53/UDP, 53/TCP, 9153/TCP	16d

Figure 16: Services

Important is, that all the services are up and running. From the default namespace we can see, that all deployments are there and available. Be sure, that all needed services from istio-system namespace are also available. Ingressgateway allows you to define entry points into the mesh that all incoming traffic flows through[9]. Egress gateway is a symmetrical concept; it defines exit points from the mesh. Egress gateways allow you to apply Istio features, for example, monitoring and route rules, to traffic exiting the mesh. [9] Grafana, kiali and prometheus are needed for visualization.

6 Evaluation

6.1 Canary deployment with Istio as part of Routing

A canary deployment is a deployment strategy that releases an application or service incrementally to a subset of users [2]. A canary deployment has the lowest risk

NAMESPACE	NAME	READY	UP-TO-DATE	AVAILABLE	AGE
default	deployment.apps/analytics	1/1	1	1	128m
default	deployment.apps/analytics-advanced	1/1	1	1	128m
default	deployment.apps/billing	1/1	1	1	128m
default	deployment.apps/control	1/1	1	1	128m
default	deployment.apps/distributed-calculation-1	1/1	1	1	128m
default	deployment.apps/distributed-calculation-2	1/1	1	1	128m
default	deployment.apps/service-repository	1/1	1	1	128m
istio-system	deployment.apps/grafana	1/1	1	1	8d
istio-system	deployment.apps/istio-egressgateway	1/1	1	1	15d
istio-system	deployment.apps/istio-ingressgateway	1/1	1	1	15d
istio-system	deployment.apps/istiod	1/1	1	1	15d
istio-system	deployment.apps/kiali	1/1	1	1	14d
istio-system	deployment.apps/prometheus	1/1	1	1	14d
kube-system	deployment.apps/coredns	1/1	1	1	16d

Figure 17: Deployments

jelbuldinr87@jelbuldinr87		resilient-microservices-with-istio/istio		main	kubectl get all -A	
NAMESPACE	NAME	READY	STATUS	RESTARTS	AGE	
default	pod/analytics-7b9485c488-w8hvq	2/2	Running	0	128m	
default	pod/analytics-advanced-57bd4dbbf9-9d84g	2/2	Running	0	128m	
default	pod/billing-6bddb9c7df-zlpcq	2/2	Running	0	128m	
default	pod/control-75b8f687-78tn5	2/2	Running	0	128m	
default	pod/distributed-calculation-1-5ddd49d747-trxkd	2/2	Running	1	128m	
default	pod/distributed-calculation-2-6848b85b85-mcjbx	2/2	Running	1	128m	
default	pod/service-repository-5fb8894566-jbv82	2/2	Running	0	128m	
istio-system	pod/grafana-556f8998cd-rwm89	1/1	Running	14	8d	
istio-system	pod/istio-egressgateway-7bfdcc9d86-p2wnk	1/1	Running	8	15d	
istio-system	pod/istio-ingressgateway-565bff4d-8jnv	1/1	Running	8	15d	
istio-system	pod/istiod-5c6d886bd8-hzgzk	1/1	Running	8	15d	
istio-system	pod/kiali-85c8cd5b5-2lkm2	1/1	Running	35	14d	
istio-system	pod/prometheus-69f7f4d689-pd68d	2/2	Running	42	14d	
kube-system	pod/coredns-74ff55c5b-25l5h	1/1	Running	14	16d	
kube-system	pod/etcd-minikube	1/1	Running	23	16d	
kube-system	pod/kube-apiserver-minikube	1/1	Running	24	16d	
kube-system	pod/kube-controller-manager-minikube	1/1	Running	28	16d	
kube-system	pod/kube-proxy-l5586	1/1	Running	9	16d	
kube-system	pod/kube-scheduler-minikube	1/1	Running	20	16d	
kube-system	pod/storage-provisioner	1/1	Running	42	16d	

Figure 18: All pods are up and running.

compared to other release strategies, because it can be controlled very easily. With Istio can be configured, that N-percent of the traffic should be forwarded to one or another service. In our case we have analytics service, that predicts the estimated time of calculations and then a new version of the analytics was implemented, now it can predict the price of calculation in dollars and euro. To test this feature in production 10 percent of all traffic fill be redirected to a new advanced analytics service and 90 percent to the old one. In case of failure the rollback scenario is pretty simple, a couple of parameters needs to be changed to direct all requests to the old service, that works correctly. To apply the deployment do the following:

- Apply canary deployment

```
kubectl apply -f istio/virt_svc_10_90_canary.yaml
```

After it is applied, we can see from the Kiali, that only 13 percent of requests are forwarded to the new service and the rest to the old one.

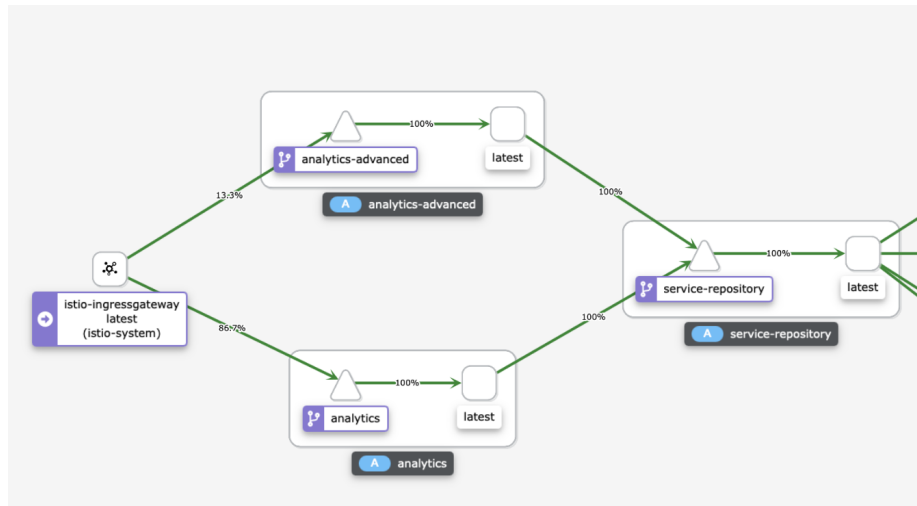


Figure 19: Requests distribution between services

```

- match:
  - uri:
    | prefix: "/getAnalytics"
    route:
  - destination:
    | host: analytics.default.svc.cluster.local
    | port:
    | | number: 8080
    weight: 90
  - destination:
    | host: analytics-advanced.default.svc.cluster.local
    | port:
    | | number: 8080
    weight: 10

```

Figure 20: Canary deployment

6.2 Fault Injection

While architecting the cloud calculation application, I assumed that it should be designed for resiliency. An application can fail at some point, so I have designed it with failure in mind. Intentionally additional endpoints were added to distributed calculation service such as /timeout and /errorCode for testing istio resiliency features. At that point of time I didn't even know, that Istio provides such a feature. Chaos Testing is a practice to intentionally introduce failures into your system to test the resiliency and recovery of microservices architecture. The Mean Time to Recovery (MTTR) needs to be minimized in modern day architectures. Hence, it is beneficial to validate different failure scenarios ahead of time and to take the necessary steps to stabilize the system and make it more resilient.[7] With Istio it is possible to inject failures at application layer, it can be different HTTP-Errors or delays. It is even possible to create a fault injection rule to delay traffic coming from the specific user. [10]

6.3 Fault Injection - Timeout

Note that the service repository has a 15 seconds hard-coded connection timeout for any calls. With this timeout the end-to-end flow should work normally, but with delay. It can be seen from Postman pictures, that the normal response time before fault injection was < 100ms and after > 15s. From the provided config file we can see that the timeout was set to 30 percent of requests. The timeout was set for service repository, and since it is a central service in the ecosystem, the control center will not be able to communicate with the repository in a normal way. We can see on the Kiali graph after timeout injection, that there is no errors, but the control panel can't access the service repository, so the delay there is more than 50s.

- Apply fault injection with delay using istio


```

apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: service-repository
spec:
  hosts:
  - service-repository.default.svc.cluster.local
  http:
  - fault:
      delay:
        fixedDelay: 15s
        percentage:
          value: 30
      route:
      - destination:
          host: service-repository.default.svc.cluster.local

```

Figure 21: Fault injection - Timeout configuration

```
kubectl apply -f istio/fault_injection_delay.yaml
```

- Set timeout directly

```
curl http://192.168.64.3:30002/timeout?n=15000
```

```

apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: service-repository
spec:
  hosts:
  - service-repository.default.svc.cluster.local
  http:
  - fault:
      delay:
        fixedDelay: 15s
        percentage:
          value: 30
      route:
      - destination:
          host: service-repository.default.svc.cluster.local

```

Figure 22: Canary deployment

ms4_getAccountInfo Examples

GET 192.168.64.3:30439/getAccountInfo?user=ruslan

Params Authorization Headers (8) Body Pre-request Script Tests Settings

Query Params

KEY	VALUE	DESCRIPTION
<input checked="" type="checkbox"/> user	ruslan	

Body Cookies Headers (5) Test Results Status: 200 OK Time: 15.05 s

Pretty Raw Preview Visualize JSON Copy

```

1 {
2   "balance": 9260,
3   "name": "ruslan"
4 }

```

Figure 23: Postman - normal response time

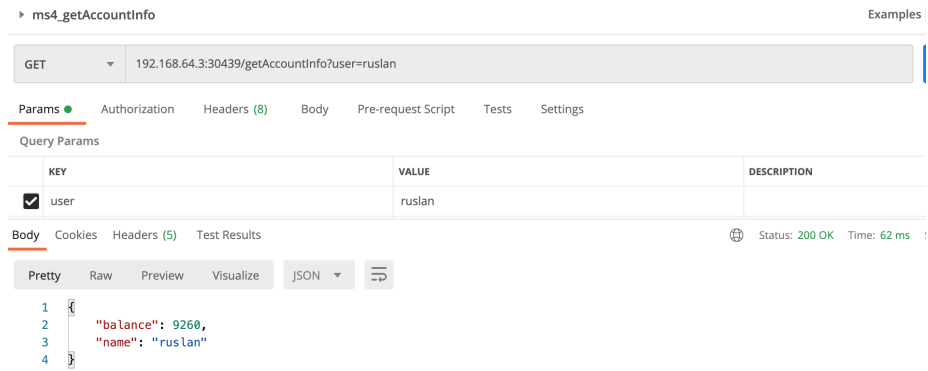


Figure 24: Postman - response time after fault injection

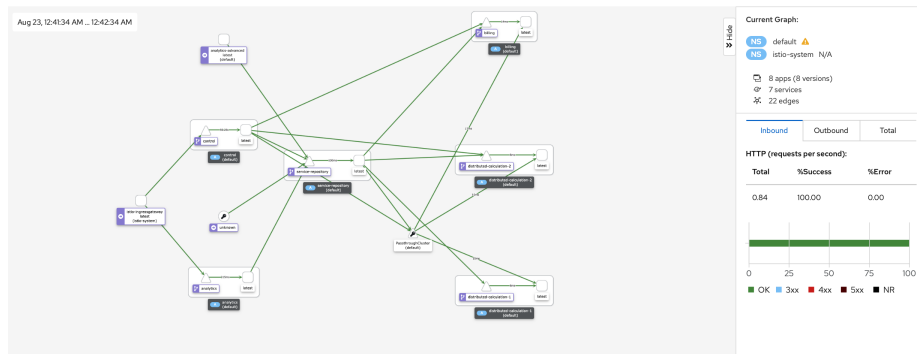


Figure 25: Kiali - Response time after timeout fault injection

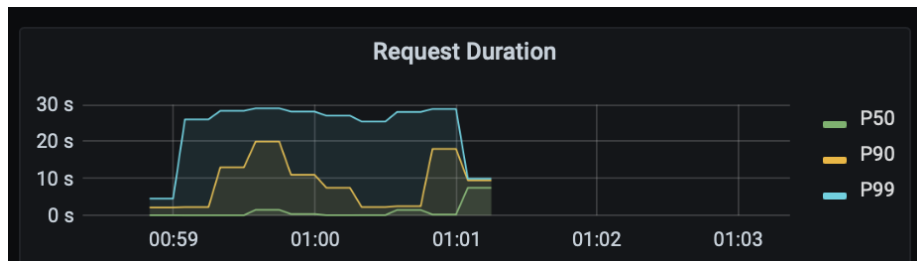


Figure 26: Grafana - Request duration after fault injection

6.4 Fault Injection - HTTP 5XX

For testing this feature, do the following:

- Apply fault injection with HTTP 500

```
kubectl apply -f istio/fault_injection_calculation_500.yaml
```

On the Kiali graph is the expected results shown. The control center can't access service repository in a success case. For most of the requests (80 percent) it is failed. Right after injecting the http 500, we can see on grafana dashbord, that the success rate is 84%, that means, that compared to the normal success rate of 100 % it decreases.

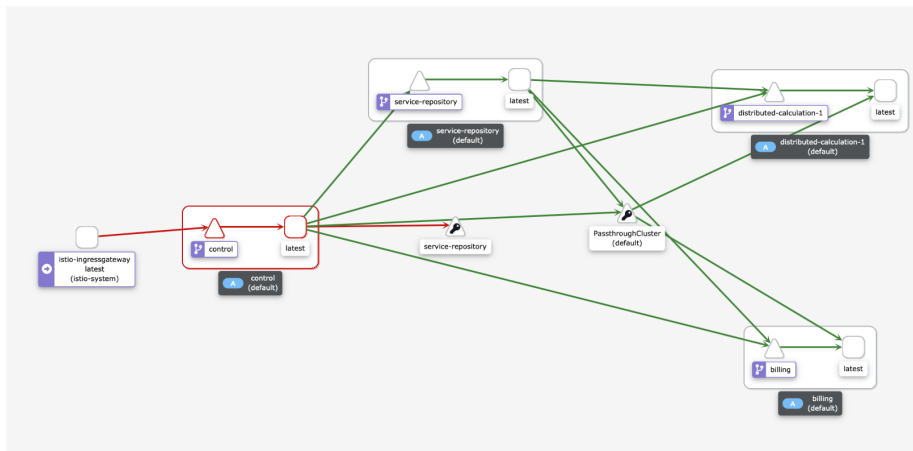


Figure 27: Kiali graph with fault injection - HTTP 500

```

apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: service-repository
spec:
  hosts:
  - service-repository.default.svc.cluster.local
  http:
  - fault:
      abort:
        httpStatus: 500
        percentage:
          value: 80
      route:
      - destination:
          host: service-repository.default.svc.cluster.local

```

Figure 28: Fault injection configuration - HTTP 500

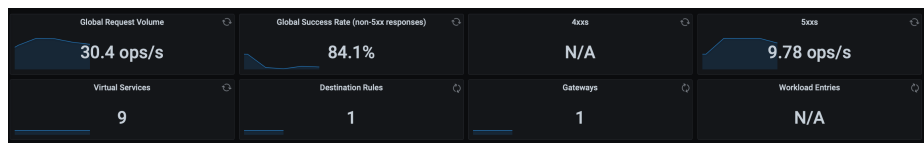


Figure 29: Grafana - success rate with fault injection

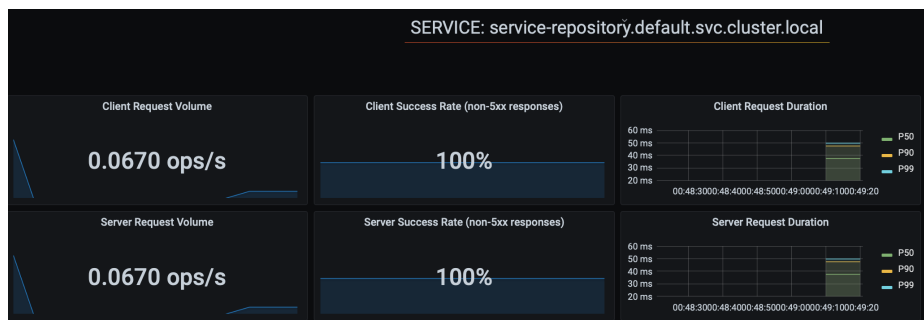


Figure 30: Grafana - Service Repository

6.5 Problems with testing and outlier detection

For people, who never used Istio and who has no idea about its main features and functions should be interesting to learn and try out all provided mechanisms. It was not easy to test some Istio features for me, cause I designed the applications in a traditional fashion. As example, there is a retry implementation in calculation service written on Java with Spring framework. If a request is failed, there are 3 attempts with interval of 100 milliseconds. The Spring Cloud Netflix Ribbon library was used for this purposes. While designing the applications for the bachelor thesis I wanted it to be fault tolerant and it worked perfect, but this approach has some disadvantages:

1. It should be a part of application and for each endpoint it should be implemented additionally. There is no possibility to change the retry policy globally.
2. There are different implementations for each programming language and the library should be up to date. But for microservice approach, especially in polyglot stack it is not a good solution.
3. If any changes are needed, it is not possible to change the application configuration file and restart the service. Adaption of existing code is needed, which can be difficult in some cases.

```
@Service
public class RetryService {

    @Autowired
    private IFeignClient iFeignClient;

    @Retryable(value = {Exception.class}, maxAttempts = 3, backoff = @Backoff(100))
    public String retryWhenError(URI uri) {
        return iFeignClient.health(uri);
    }
}
```

Figure 31: Retry with Spring Netflix Ribbon

But with Istio it can be configured on a global level without changing the source code. Another fault tolerant decision is implemented between services. The service repository make health checks of every registered service in 100ms interval, if one of the services is not reachable it will be ejected from the list of registered services. Each registered microservice checks the status of the service repository, and if there is no response within 2 minutes the service will be switched off. Here we can use a feature of Istio such as outlier detection - is an istio resiliency strategy that is used to detect unusual behaviour of a service and if a host is unhealthy, it will be evicted from the list. This feature of Istio can track the status of each service and check metrics like consecutive errors and latency associated with service calls. If it finds outliers, it will automatically evict them. [8] The following features for outlier detection provided in Istio:

1. BaseEjectionTime - The maximum ejection duration for a host. For example, in the config provided below the host will be ejected for 60 seconds before it is evaluated again for processing requests. [8]

2. **ConsecutiveErrors** - Number of errors before a host is ejected from the connection pool. For example, if you have 3 consecutive errors while interacting with a service, Istio will mark the pod as unhealthy.[8]
3. **Interval** - The time interval for ejection analysis. For example, the service dependencies are verified every 5 seconds.[8]
4. **MaxEjectionPercent** - The max percent of hosts that can be ejected from the load balanced pool. For example, setting this field to 100 implies that any unhealthy pods throwing consecutive errors can be ejected and the request will be rerouted to the healthy pods.[8]

If a request fails namely returns 5XX code or response time is too long, a service will be ejected from the load balancing pool for a defined time, so only healthy hosts will be loadbalanced, which can increase availability of services. In the following configuration

```
apiVersion: networking.istio.io/v1alpha3
kind: DestinationRule
metadata:
  name: distributed-calculation-1
spec:
  host: distributed-calculation-1.default.svc.cluster.local
  trafficPolicy:
    outlierDetection:
      baseEjectionTime: 60s
      consecutiveErrors: 3
      interval: 5s
      maxEjectionPercent: 100
```

Figure 32: Outlier Detection config

7 Conclusion

Different open source solutions such as Linkerd, Istio and Consul in the Kubernetes ecosystem for service meshes were discussed in the bachelor's thesis. Each of them has its own benefits and minuses. We have also discussed the difference between monolithic and microservice architecture. However, the goal of the thesis was deploying distributed application with Kubernetes and testing the resiliency features of Istio.

Using any of the above mentioned service meshes will put your DevOps teams in a better position to thrive as they develop and maintain more and more microservices. [16] Various features such as fault injection, canary deployment and outlier detection were tested and results of the testing was introduced above. From the demonstrated tests we can see, that istio provides a lot of useful features. As part of the thesis the distributed calculation service was implemented and deployed with kubernetes and Istio. Fault injection, canary deployment and outlier detection features were tested. The expected results were achieved, what we can see from provided screenshots of monitoring systems such as Kiali and Grafana. Istio is a new technology, which is great, but not mature. There are a lot of open bugs there. Distributed calculation service contains at most 10 simple microservices connected with each other, but sometimes 16 GB of RAM was not enough to handle it.

8 Future Work

In this bachelor thesis simple, basic Istio resiliency features were tested and documented. In the future work more resiliency features can be tested and discussed. As mentioned above there are at least 3 open source solutions of service meshes with its features, pros and cons. A future work could contain a practical comparison of service meshes by following parameters:

- Traffic Management
- Monitoring and Observability
- Architecture
- Testing

It is interesting to see how Istio will be implemented and integrated in existing production solutions to understand the difference between theory and practice.

The community is focused on continuing to make Istio easy to use and as transparent as possible, with little or zero configuration [18]. Istio is promising.

References

- [1] CALCOTE, L., AND BUTCHER, Z. *Istio: Up and Running: Using a Service Mesh to Connect, Secure, Control, and Observe*. O'Reilly Media, 2019.
- [2] <https://harness.io/blog/continuous-verification/blue-green-canary-deployment-strategies/>.
- [3] CHEN, L. Microservices: Architecting for continuous delivery and devops. In *2018 IEEE International Conference on Software Architecture (ICSA)* (2018), pp. 39–397.
- [4] <https://www.consul.io/docs/intro>.
- [5] DRAGONI, N., LANESE, I., LARSEN, S. T., MAZZARA, M., MUSTAFIN, R., AND SAFINA, L. Microservices: How to make your application scale. In *Perspectives of System Informatics* (Cham, 2018), A. K. Petrenko and A. Voronkov, Eds., Springer International Publishing, pp. 95–104.
- [6]
- [7] <https://dzone.com/articles/chaos-testing-your-microservices-with-istio>.
- [8] <https://dzone.com/articles/istio-circuit-breaker-with-outlier-detection>.
- [9] <https://istio.io/latest/docs/tasks/traffic-management/egress/egress-gateway/>.
- [10] <https://istio.io/latest/docs/tasks/traffic-management/fault-injection/>.
- [11] <https://istio.io/latest/docs/setup/getting-started/>.
- [12] KHATRI, A., KHATRI, V., NIRMAL, D., PIRAHESH, H., AND HERNES, E. *Mastering Service Mesh: Enhance, secure, and observe cloud-native applications with Istio, Linkerd, and Consul*. Packt Publishing, 2020.
- [13] <https://medium.com/microservicegeeks/an-introduction-to-microservices-a3a7e2297ee0>.
- [14] [https://medium.com/javascript-scene/the-forgotten-history-of-oop-88d71b9b2d9f?text=%E2%80%9CObject%2DOriented%20Programming%E2%80%9D%20\(,his%20Sketchpad%20](https://medium.com/javascript-scene/the-forgotten-history-of-oop-88d71b9b2d9f?text=%E2%80%9CObject%2DOriented%20Programming%E2%80%9D%20(,his%20Sketchpad%20)
- [15] NEWMAN, S. *Building Microservices: Designing Fine-Grained Systems*, 1st ed. O'Reilly Media, February 2015.
- [16] <https://platform9.com/blog/kubernetes-service-mesh-a-comparison-of-istio-linkerd-and-consul/>.
- [17] <https://www.redhat.com/en/topics/microservices/what-is-a-service-mesh>.
- [18] <https://sdtimes.com/softwaredev/guest-view-5-reasons-to-be-excited-about-istios-future/>.
- [19] WOLFF, E. *Microservices: Flexible Software Architecture*. Always learning. Addison-Wesley, 2017.
- [20] YOUSIF, M. Microservices. *IEEE Cloud Computing* 3, 5 (2016), 4–5.