Proposed Microservices Architecture

esm_logo.jpg

Nexelus USA  
New York, NEW YORK (NY)  
646-558-1950 ext.128

**11/1/2023**

# Document Information

The following table shows the details for document creation, review, approval, and effective date.

| **Category** | **Information** |
| --- | --- |
| Work Product: | Proposed Microservices Architecture |
| Product Name: | Nexelus |
| Function Name: | SOC 1 Type II Document |
| Version: | 1.0 |
| Status: | Draft |
| Author(s): | Tauseef Shahzad |
| Reviewer(s): | Asim Jameel |
| Approver(s): | Imran Rahman |
| Control Status: | CONTROLLED, PROTECTED |
| Disclaimer: | This document contains confidential information. Do not distribute this document without prior approval from Nexelus. |

# Revision History

The following table is used for revision details of this document.

| **Author(s)** | **Date** | **Version** | **Description of Change** |
| --- | --- | --- | --- |
| Tauseef Shahzad | Nov 1, 2023 | 1.0 | Initial Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

Contents

[Document Information ii](#_Toc149742291)

[Revision History iii](#_Toc149742292)

[Table of Contents i](#_Toc149742293)

[Scope 1](#_Toc149742294)

[Terms and Definitions 2](#_Toc149742295)

[Technologies 5](#_Toc149742296)

[Nexelus Micro Frontend 7](#_Toc149742297)

[Micro-Frontend Application - Inter-Communication 7](#_Toc149742298)

[State Management 7](#_Toc149742299)

[Global Store 8](#_Toc149742300)

[Nexelus Microservice Architecture 9](#_Toc149742301)

[API Gateway 9](#_Toc149742302)

[MicroService - Messaging 10](#_Toc149742303)

[Database Connectivity 11](#_Toc149742304)

[Authentication Service 11](#_Toc149742305)

[Cache 12](#_Toc149742306)

[Logging 12](#_Toc149742307)

[Multi-Tanent System 13](#_Toc149742308)

## Scope

Nexelus Application has been developed using Microsoft .Net Webforms. Some newer modules have been created using Microsoft .Net Core platform. .Net Core application is created as separate application, however both applications share the session/state information managed in Web Forms application.

The scope of this document is to outline Microservices architecture for Nexelus, and to propose high level architecture, technology, and application components. The document also covers proposed mechanism to integrate with existing application as well as how to implement Multi-Tenant Architecture.

## Terms and Definitions

At their cores, API gateways, Ingress controllers, and service meshes are each a type of proxy, designed to get traffic into and around your environments.

**Monolithic Applicaton Architecture**

A monolithic architecture is a traditional model of a software program, which is built as a unified unit that is self-contained and independent from other applications. A monolithic application may or may not consume external APIs and services.

**Microservice Application Architecture**

A microservices architecture is a type of application architecture where the application is developed as a collection of services. It provides the framework to develop, deploy, and maintain microservices architecture diagrams and services independently.

**Rest API**

REST API, or application programming interface, is a set of rules that define how applications or devices can connect to and communicate with each other. A REST API is an API that conforms to the design principles of the REST, or representational state transfer architectural style.

**Micro-Frontends**

Micro-frontend architecture is a design approach in which a front-end app is decomposed into individual, semi-independent “microapps” working loosely together. The micro-frontend concept is vaguely inspired by, and named after, microservices.

**API Gateway**

An API gateway routes API requests from a client to the appropriate services. But a big misunderstanding about this simple definition is the idea that an API gateway is a unique piece of technology. It’s not. Rather, “API gateway” describes a set of use cases that can be implemented via different types of proxies – most commonly an ADC or load balancer and reverse proxy, and increasingly an Ingress controller or service mesh.

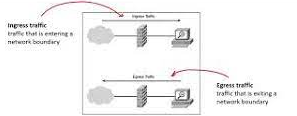
There isn’t a lot of agreement in the industry about what capabilities are “must haves” for a tool to serve as an API gateway. We typically see customers requiring the following abilities (grouped by use case):

* Resilience Use Cases
  + A/B testing, canary deployments, and blue‑green deployments
  + Protocol transformation (between JSON and XML, for example)
  + Rate limiting
  + Service discovery
* Traffic Management Use Cases
  + Method‑based routing and matching
  + Request/response header and body manipulation
  + Request routing at Layer 7
* Security Use Cases
  + API schema enforcement
  + Client authentication and authorization
  + Custom responses
  + Fine‑grained access control
  + TLS termination

Almost all these use cases are commonly used in Kubernetes. Protocol transformation and request/response header and body manipulation are less common since they’re generally tied to legacy APIs that aren’t well‑suited for Kubernetes and microservices environments.

**Ingress Controller**

An Ingress controller (also called a Kubernetes Ingress Controller – KIC for short) is a specialized Layer 4 and Layer 7 proxy that gets traffic into Kubernetes, to the services, and back out again (referred to as ingress‑egress or north‑south traffic). In addition to traffic management, Ingress controllers can also be used for visibility and troubleshooting, security, and identity, and all but the most advanced API gateway use cases.



**Service Mesh**

A service mesh handles traffic flowing between Kubernetes services (referred to as service-to-service or east‑west traffic) and is commonly used to achieve end-to-end encryption (E2EE). Service mesh adoption is small but growing as more organizations launch advanced deployments or have requirements for E2EE. A service mesh can be used as a distributed (lightweight) API gateway very close to the apps, made possible on the data plane level by service mesh sidecars.

**Container**

Containers are lightweight packages of your application code together with dependencies such as specific versions of programming language runtimes and libraries required to run your software services. Containers are packages of software that contain all the necessary elements to run in any environment. In this way, containers virtualize the operating system and run anywhere, from a private data center to the public cloud or even on a developer’s personal laptop.

**Docker**

Docker is an open platform for developing, shipping, and running applications. Docker enables you to separate your applications from your infrastructure so you can deliver software quickly. With Docker, you can manage your infrastructure in the same ways you manage your applications. By taking advantage of Docker's methodologies for shipping, testing, and deploying code, you can significantly reduce the delay between writing code and running it in production.

**Kubernetes**

Kubernetes automates operational tasks of container management and includes built-in commands for deploying applications, rolling out changes to your applications, scaling your applications up and down to fit changing needs, monitoring your applications, and more making it easier to manage applications.

**End-to-end encryption**

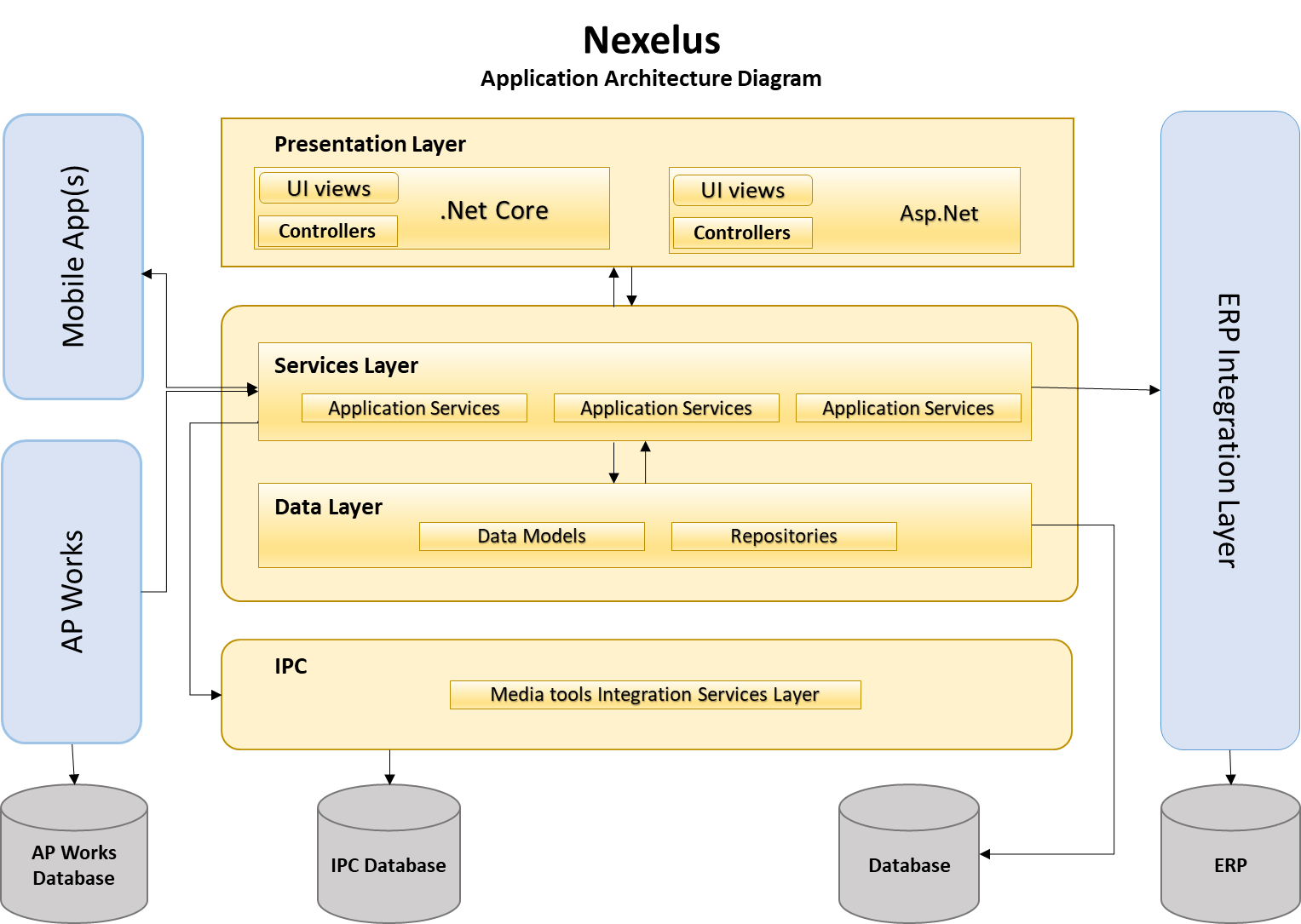
End-to-end encryption (E2EE) is a method of secure communication that prevents third parties from accessing data while it's transferred from one end system or device to another.

In E2EE, the data is encrypted on the sender's system or device, and only the intended recipient can decrypt it. As it travels to its destination, the message cannot be read or tampered with by an internet service provider (ISP), application service provider, hacker or any other entity or service.

## Technologies

#### Existing Architecture

Nexelus has been designed as dotNet Webforms Monolithic application. The application is divided in Presentation, Service and Database Layer. Some of its business functions are deployed as Rest services, such as IPC, etc. However, it is deployed as a Monolithic application that includes all business functions.



#### Proposed Architecture - (Micro Services with Micro Front Ends)

Microservices are a set of services that act together to make a whole application operate. This architecture utilizes APIs to pass information, such as user queries or a data stream, from one service to another.

How the underlying software works, or which hardware the service is built upon, depends solely on the team who built the service. This makes both communicating between teams and upgrading services very dynamic—even reactive—allowing a software company or team to be more resilient in its development.

React provides state-of-the-art functionality and is an excellent choice for developers looking for an easy-to-use and highly productive JavaScript framework. Using React, you can build complex UI interactions that communicate with the server in record time with JavaScript-driven pages.



## Nexelus Micro Frontend

Nexelus application will be segregated between loosely coupled Micro Frontends and Microservices. The Micro Frontends will be developed primarily using Node and React.

### Micro-Frontend Application - Inter-Communication

Micro frontend application comprises of multiple smaller apps running independently and embedded in a single Micro Frontends container application. The architecture with its whole list of advantages comes up with a set of complexities also and one of those is inter-communication of micro frontend applications. In this section, we are going to discuss five different techniques for micro frontend communications and the pros and cons of each one.

#### Props

This is the most basic technique for cross micro frontend communication where the container app is maintaining the state and passing it further to the required micro frontends.

* Pros
  + One of the very well-known techniques of data passing in component-based architecture.
  + Most of the frameworks support this way.
  + One can always use framework structs to avoid prop drilling issues e.g. React Context etc.
* Cons
  + Adds a lot of coupling between the micro frontends and the container app.
  + Hard to achieve if two micro frontends are not using the same framework
  + It can impact the overall performance of the application as multiple unwanted layers will be re-rendered with every state change.

#### Platform Storage Apis

In this technique, we can leverage the platform's built-in storage APIs like Local Storage in browsers and Async Storage in cross-platform solutions like react native for mobile micro frontends also.

We can create a simple storage utility library exposing setter and getter from storage APIs. Now, instead of making micro frontends communicate via container app, each different micro frontend can set as well as read the data directly using the utility.

* Pros
  + Available for browsers as well as mobile devices. Local storage for browsers and Async storage for mobile apps.
  + Less coupling compares to passing props between the App and micro frontend but hard to debug which micro frontend is setting the data.
* Cons
  + Not a scalable solution for bigger applications. But can be used for a small set of data. It is always good to namespace the data set into platform storage according to the app name to avoid ambiguity.
  + Not a secure technique for saving protected data.

#### Custom Events

This technique is more suitable for web micro frontends and a more scalable technique for run-time micro frontends. The main idea here is to utilize the browser-inbuilt custom events APIs to publish the events with the data from one micro frontend and the other micro frontends subscribe to the events to get the data. This technique is closest to the events-driven architecture in the microservices world.

* Pros
  + The inbuilt solution in-browser platform.
  + Very much close to asynchronous event-based architecture in the microservices world. Easy for the backend developers to understand as well.
  + High setup cost but easy to scale.
  + Build a generic mechanism that all the micro frontend teams can follow.
* Cons
  + Not achievable in the case of mobile micro frontends

#### Custom Message bus

This technique is almost similar to the above one but instead of relying on the browser custom events API, we can build our pub-sub mechanism.

The message bus library can expose methods to publish, subscribe and unsubscribe the events. The publish event needs to make sure that all the subscribed handlers are invoked once the event is published.

* Pros
  + A custom-made solution equivalent to message bus in microservices implementation.
  + High setup cost but easy to scale.
  + Libraries like Postal.js (<https://github.com/postaljs/postal.js>) are available in the market.
* Cons
  + Similar to the custom events technique, it can be hard to make all the micro frontends teams follow the same pattern.

#### Post Message passing in iFrames

This technique is only relevant if you are building runtime micro frontends using iFrames. I feel that there is a better integration pattern for building micro frontends than using iFrames, but this technique can be very much useful when you need to inject a micro frontend inside another running app.

This technique is prone to hacking and brings up a lot of security concerns and hence it is not recommended.

#### Proposed Inter-Communication Technique:

It is proposed to use the **Custom Message Bus** for inter-application communication.

### State Management

Utilizing state management mechanisms in micro frontends is generally considered an unfavorable practice as it may result in the coupling of disparate applications, consequently undermining the benefits of adopting micro frontends. However, in certain scenarios where state sharing among micro frontends is unavoidable, it is recommended to keep the state as simple as possible to mitigate the potential drawbacks.

**Redux-Thunk Vs Redux-Saga**: Redux Thunk and Redux Saga take care of dealing with side effects. In very simple terms, applied to the most common scenario (async functions, specifically AJAX calls) Thunk allows Promises to deal with them, Saga uses Generators. Thunk is simple to use and Promises are familiar to many developers, Saga/Generators are more powerful but you will need to learn them. When Promises are just good enough, so is Thunk, when you deal with more complex cases on a regular basis, Saga gives you better tools.

As an example, what happens when you start an AJAX call in a route/view and then the user moves to a different one? Can you safely let the reducer change the state anyway? Saga makes it trivial to cancel the effect, Thunk requires you to take care of it, with solutions that don't scale as nicely.

// simple usage of redux-thunk:

export const asyncApiCall = values => {

return dispatch => {

return axios.get(url)

.then(response =>{

dispatch(successHandle(response));

})

.catch(error => {

dispatch(errorHandle(error));

});

};

};

// async/await usage of redux-thunk:

export const asyncApiCall = values => {

return async dispatch => {

try {

const response = await axios.get(url);

dispatch(successHandle(response));

}

catch(error) {

dispatch(errorHandle(error));

}

};

};

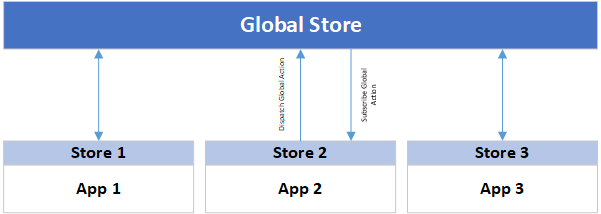
For managed, scalable, and controlled code, proposed solution is to use Redux-Saga.

### Global Store

The Global Store is not an actual store, rather it's a collection of multiple isolated Redux Stores. Each physical Redux Store here refers to the isolated store that each app uses. Micro frontends having access to the Global Store would be able to perform all operations that are allowed on an individual Redux Store including getState(), dispatch() and subscribe().

**Global Actions**

The concept of Global Action is available which allows other apps to dispatch actions to stores registered by other Micro Frontends. Each Micro Frontend has the capability to register a set of global actions along with the store. These sets of global actions can be dispatched in this Micro Frontend's store by other Micro Frontends. This enables cross-application communication.



**Cross-state callbacks**

Cross-application communication can also be achieved by subscribing to change notifications in other Micro Frontend's state. Since each micro-frontend has read-only permission to other states, they can also attach callbacks for listening to state changes. The callbacks can be attached either at an individual store level or at a global level (this would mean that state change in any store would invoke the callback).

### User Interface Libraries

#### Material-UI <https://mui.com/material-ui/>

[blurbs]

[More to be added]

## Nexelus Microservice Architecture

### API Gateway

The following API gateways are considered for Nexelus API Gateway.

**DAPR**<https://dapr.io/>

The Distributed Application Runtime (Dapr) provides APIs that simplify microservice connectivity. Whether your communication pattern is service to service invocation or pub/sub messaging, Dapr helps you write resilient and secured microservices. By letting Dapr’s sidecar take care of the complex challenges such as service discovery, message broker integration, encryption, observability, and secret management, you can focus on business logic and keep your code simple.

**Ocelot**<https://ocelot.readthedocs.io/>

A modern fast, scalable API gateway built on ASP.NET core. It is aimed at people using .NET running a micro services / service oriented architecture that need a unified point of entry into their system. However it will work with anything that speaks HTTP and run on any platform that ASP.NET Core supports. It manipulates the HttpRequest object into a state specified by its configuration until it reaches a request builder middleware where it creates a HttpRequestMessage object which is used to make a request to a downstream service.

**Proposed Architecture**:

API Gateway is a pivotal technology for Microservices application. Each of the above mentioned API Gateways has its own advantages.

Ocelot is an API gateway written in C# and is easiest to implement for dotNet Core applications.

DAPR is Microsoft developed and backed API Gateway that is actively developed and evolving platform.

ISTIO is most popular and has more deployments than the other two platforms.

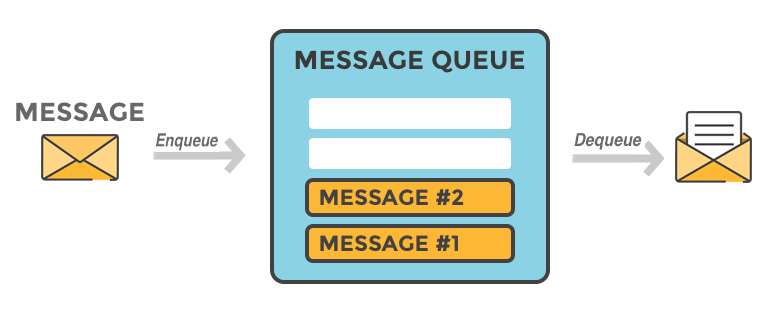
It is proposed to use Istio, however it is open for debate before we start actual development.

### MicroService - Messaging

We have multiple options to use for Messaging inside Microservice (Rabbit MQ, Azure Bus) ,

**RabbitMQ**<https://www.rabbitmq.com/>

RabbitMQ is a message-queueing software also known as a message broker or queue manager. Simply said; it is software where queues are defined, to which applications connect to transfer a message or messages.



**Azure Service Bus**<https://learn.microsoft.com/en-us/azure/service-bus-messaging/service-bus-messaging-overview>

Azure Service Bus is a fully managed enterprise message broker with message queues and publish-subscribe topics (in a namespace). Service Bus is used to decouple applications and services from each other, providing the following benefits:

* Load-balancing work across competing workers
* Safely routing and transferring data and control across service and application boundaries
* Coordinating transactional work that requires a high degree of reliability

**Saga design pattern**

<https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/saga/saga>

The Saga design pattern is a way to manage data consistency across microservices in distributed transaction scenarios. A saga is a sequence of transactions that updates each service and publishes a message or event to trigger the next transaction step. If a step fails, the saga executes compensating transactions that counteract the preceding transactions.

A diagram of a service

Description automatically generated

**Proposed Messaging Architecture**

Need more R&D to propose messaging architecture.

### Database Connectivity

Nexelus Web Forms application uses ADO.net for database connectivity. Nexelus .Net core application is currently using Dapper as ORM.

It is proposed to use Entity Framework for the new Microservices Application.

An ORM or Object Relational Mapping is an object-oriented programming technique that is used to map data between two incompatible types. Dapper is called micro ORM as it does not provide the full functionality and features like Entity Framework does. Dapper provides you with an ability to fetch the data from a relational database. It does not support code first support approach and can work with the querying and update through raw SQL. It cannot be used to configure classes and has a set of extension methods for ADO.NET. Entity Framework is an open source ORM that is available as a part of .NET framework. It is responsible to handle the interactions  
between the relational databased and .NET applications. It simplifies the programming code by generating the model classes for the database schema automatically. It allows you to have the database first and create the entities from it or alternatively, the application code can be initiated before the designing of database. In this way, any manual changes to the database, needs to be updated or copied to the code level because the changes will be lost.

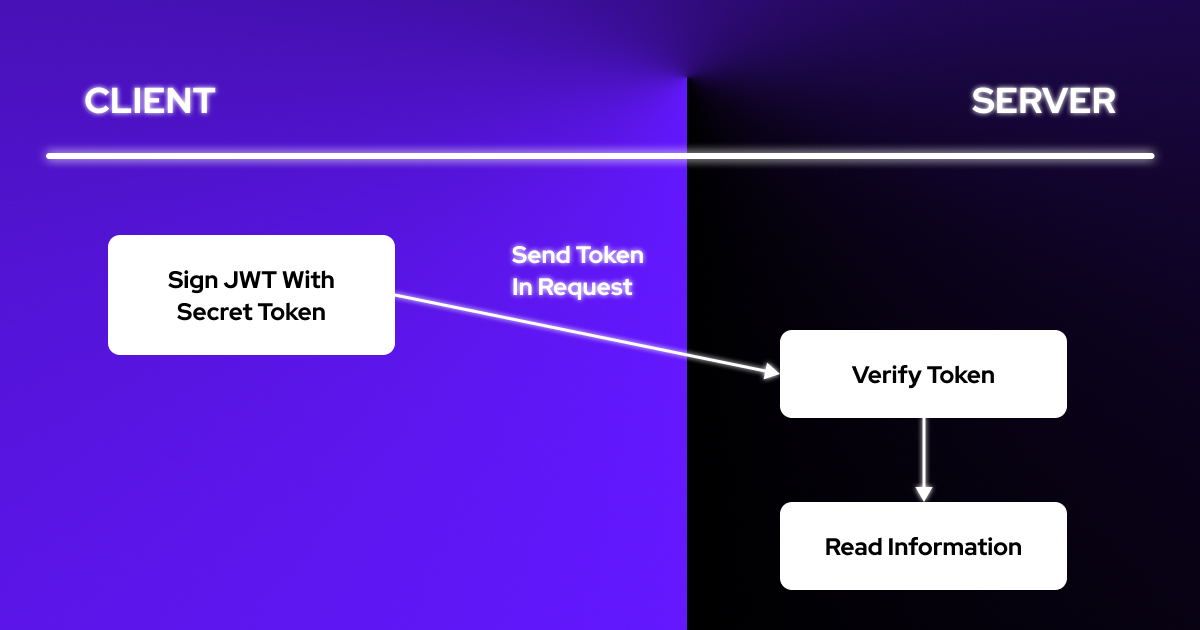
Reference: https://www.chubbydeveloper.com/entity-framework-vs-dapper/

### Authentication Service

* JWT
* OAuth OpenID
* Identity Server

[ Write a little details on each]

JWT is proposed for token base authentication.



JWT, or JSON Web Token, is a web protocol used to share security information between client and server. In a standard web application, private API requests contain JWT that is generated because of the verification of the user information, thus allowing these users to reach protected data and access services.

### Cache

Radis Cache

### Logging

This section covers logging of Microsoft Core Logging components.

##### log4net

The Apache log4net library is a tool to help the programmer output log statements to a variety of output targets. log4net is a port of the excellent Apache log4j™ framework to the Microsoft® .NET runtime, keeping the framework similar in spirit to the original log4j while taking advantage of new features in the .NET runtime. Over the years, development continued under the Apache Logging Services project.

##### NLog Overview

NLog is legacy project that is used in existing Nexelus Application. Version 1.0 was released back in 2006, but it is still under active development with the latest version having been released in December of 2017. log4net hasn’t seen a release in 18 months, which isn’t necessarily bad as the project is stable. The latest release of NLog adds structured logging and support for .NET Standard.

##### Serilog

Reference URL : <https://stackify.com/nlog-vs-log4net-vs-serilog/>

The API is modern, it is easier to set up, it is better maintained, and it does structured logging by default. The ability to add enrichers give you the ability to intercept and modify the messages is useful.

##### Grafana Loki <https://grafana.com/oss/loki/>

Loki is a horizontally scalable, highly available, multi-tenant log aggregation system inspired by Prometheus. It is designed to be very cost effective and easy to operate. It does not index the contents of the logs, but rather a set of labels for each log stream.

**Proposed Logging Tool**: Logging is an important aspect to any application and shouldn’t be treated as an afterthought. Grafana Loki is more suitable for Docker applications as it allows viewing logs through portal using Kubernetes.

### Multi-Tanent System

We are going to have our Microservice to get requests from the Application and decide which DB (enterprise) going to use depending on the URL provided by the Frontend Application.

## Infrastructure and Monitoring

### Docker Desktop

It provides a straightforward GUI (Graphical User Interface) that lets you manage your containers, applications, and images directly from your machine. You can use Docker Desktop either on its own or as a complementary tool to the CLI.

Docker Desktop reduces the time spent on complex setups so you can focus on writing code. It takes care of port mappings, file system concerns, and other default settings, and is regularly updated with bug fixes and security updates.

### Kubernets

Kubernetes works by managing a cluster of compute instances and scheduling containers to run on the cluster based on the available compute resources and the resource requirements of each container. Containers are run in logical groupings called pods and you can run and scale one or many containers together as a pod.

Kubernetes control plane software decides when and where to run your pods, manages traffic routing, and scales your pods based on utilization or other metrics that you define. Kubernetes automatically starts pods on your cluster based on their resource requirements and automatically restarts pods if they or the instances they are running on fail. Each pod is given an IP address and a single DNS name, which Kubernetes uses to connect your services with each other and external traffic.

Kubernetes is required for local development and deployment of microservice infrastructure for development.

Kubernetes manages clusters of Amazon Elastic Compute Cloud (EC2) compute instances and runs containers on those instances with processes for deployment, maintenance, and scaling. Using Kubernetes, you can run any type of containerized applications using the same toolset on-premises and in the cloud.

### Service Mesh

**ISTIO**<https://istio.io/>

Istio is an open-source service mesh that layers transparently onto existing distributed applications. Istio’s powerful features provide a uniform and more efficient way to secure, connect, and monitor services. Istio is the path to load balancing, service-to-service authentication, and monitoring – with few or no service code changes. Its powerful control plane brings vital features, including:

* Secure service-to-service communication in a cluster with TLS encryption, strong identity-based authentication, and authorization
* Automatic load balancing for HTTP, gRPC, WebSocket, and TCP traffic
* Fine-grained control of traffic behavior with rich routing rules, retries, failovers, and fault injection.
* A pluggable policy layer and configuration API supporting access controls, rate limits and quotas.

Automatic metrics, logs, and traces for all traffic within a cluster, including cluster ingress and egress.

## Configure Docker, Kubernetes and Istio

A service mesh is a configurable infrastructure layer. It has capabilities to handle service-to-service communication, resilience, and many cross-cutting concerns. Proxy is a key component of service mesh. Sidecar proxy is injected in each service in this concept. Here I will show you service mesh communication using Istio with asp.net core applications on Kubernetes environment.

Istio is an open platform for providing a uniform way to integrate microservices, manage traffic flow across microservices, enforce policies and aggregate telemetry data. Istio uses following tools-

|  |  |
| --- | --- |
| Tool | Description |
| Prometheus | It monitors everything in the cluster. |
| Grafana | Data visualization tools |
| Jaeger | It’s used for distributed tracing. |

### Istio Configurations

Please follow the following steps to download, install, and configure Istio

|  |  |
| --- | --- |
| Step | Description |
| 1 | * Download Istio from following link:   <https://github.com/istio/istio/releases/tag/1.12.2>   * Extract zip file in a folder (e.g., d:\software\istio) * Add d:\software\istio\bin folder to Path |
| 2 | * Verify Istio using following command   Istioctl |
| 3 | * Install Docker Desktop <https://docs.docker.com/desktop/install/windows-install/> |
| 4 | * Enable Kubernetes in Docker Desktop Settings:     It will install Kubernetes in Docker Desktop |
| 5 | * For installation, we use the demo configuration profile. It’s selected to have a good set of defaults for testing, but there are other profiles for production or performance testing. Use below command to install Istio.   istioctl install --set profile=demo -y |
| 6 | * Use the following command to verify Istio.   kubectl get all -n istio-system  You will see response similar to following |
| 7 | * Configure for auto proxy injection   Add a namespace label to instruct Istio to automatically inject Envoy sidecar proxies when you deploy your application later. Use below command to configure default namespance with Istio sidecar proxy.  kubectl label namespace default istio-injection=enabled |
| 8 | * Check label by using below command   kubectl describe namespace default |

## Sample Application and Deployment Guidelines