# Abstract

This is a Release Management Plan for Blood Pressure Monitoring Web Application. The Plan covers architecture updates for the creation of loosely coupled microservices, and continuous build, test, and release plans as part of the Automated DevOps Cycle.

# Introduction

The Blood Pressure Monitoring Web Application, previously deployed will undergo architectural transformation to a microservice architecture, supporting de-coupled and independent services. Release, Delivery, and Deployment solution will embrace DevOps techniques to deliver Continuous Build, Test, Release, and Deployment pipeline. The Release plan will leverage from Blue-Green Deployment strategy to accomplish zero downtime in deployment.

Using a microservices approach application transformation will deliver a highly scalable, available solution, accommodating high traffic as business need expands.

The overall solution, which includes both Microservices and DevOps approach, will be robust, reliable, and scalable as the business need at a lower effective cost.

The approach also promotes vulnerability checks during build and deployment, which will guarantee the software in production is of higher quality and risk-free.

# Decompose to Microservices

## Current Application Design

The current Application is designed in 2-Tier service. A Front-End UI Service and a Backend Web Service, with Mongo Database working as a persistence data store. Though the solution design followed basic Microservices techniques of being de-couples and independent to some extent, further decomposition will be needed.

Diagram

Description automatically generated

Figure : Current Design

## Architecture Changes

1. Frontend UI service should not communicate with Database directly.
   1. The UI Service should delegate the complexity of data query from the database to other services.
   2. Connecting to Database also created complexity for security where the connection and distribution of credentials should be restricted to backend services only.
2. Separate Microservice for calculating the Category.
   1. Calculation of Category is a business process, which can be made independent.
   2. This reduces the load on Backend services.
   3. Enhances the solution making it an independent service.
3. Data Recording Service to record Blood Pressure Readings.
   1. Enhance flexibility in accepting reading from other sources.
   2. Separate channel for writing to the database.
4. Backend Service is transformed to Data Service only responsible to read historical data from the database.
   1. Reduced responsibility, only in reading historical data from the database.
   2. Enhances flexibility, due to different channels for reading and writing to the database.

The flow results in Microservices designed by separation of concern. Each Microservices has its responsibility, has its lifecycle, and can scale independently. The Independence of Microservices increases testability, it can be patched and upgraded without downtime.

Each microservices is built, deployed, and tested independently. All Microservices is packaged as independent services, deployed as one solution.

Diagram

Description automatically generated

Figure : Updated Microservices

## Implementation

The new design consists of 3 Microservices and a UI Service

1. Info Service: Calculates the category of Blood Pressure.
2. Recording Service: Saves the Blood Pressure Reading to Database.
3. Data Services: Reads the historical Blood Pressure data from Database.

* UI Service: Provides the User Interface, accepting BP reading using a Web Application. It processes by calling the above 3 microservices.

To reduce the technology stack, it is better to stick with one programming language. NodeJS is perfectly suitable for all purposes. It is powerful, fast, scalable, robust, functional, and reactive.

## Code Updates

Choosing NodeJS reduces the technology stack, which will also reduce the complexity in build and testing infrastructure. NodeJS is reactive by design and has many libraries which support REST communication and E2E Testing. We also cannot ignore the fact that NodeJS has larger community support and are actively releasing new libraries. As such transforming all the functions of the previous Blood Pressure Monitoring backend Java-based Web Services to a NodeJS application will be good for the product.

### Express JS

For REST-based communication we Express JS is now considered the most accepted module for NodeJS applications. It supports all JSON-based content types by default, reducing the conversion complexity.

### Cypress

Cypress is an automated Test Tool, with the capability to test E2E, Components, and User Interface. Various reporters can be added to report the result.

## Cloud Infrastructure

The application is delivered as a cloud solution. This affects how the application is packaged, released, and deployed. The process also requires the handling of credentials and runtime properties. The application must be deployed as a solution with complete automation from build to deployment.

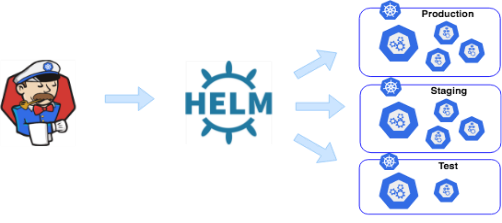
### Cloud Deliverables

Application is delivered as a cloud solution on a Kubernetes cluster rather than composing them on an independent virtual machine(s). Kubernetes is a vendor-agnostic solution, which can run on any cloud provider. It also creates its private network with its own isolated, security networking, and scalability rules. Kubernetes scales the application unit, across its cluster which is composed of its nodes. This reduces the effort in provisioning new VMs for scaling up.

For deploying the application in a Kubernetes cluster:

* Individual Microservice applications must be delivered as a Docker Image.
* Finally packing all as Helm Charts and pushed to docker registry.
* All Credentials and Environment properties must be injected at runtime.
* All deployable artifacts (i.e. docker image and helm charts) must be pushed to the cloud provider’s Container Registry.
* Application should be disposable, it can be destroyed and started without any side-effect.
* All deployment, configuration, scaling and networking requirements should be configured in a manifest file.

### Helm Chart

 A Helm chart can be thought of as a Kubernetes package. Charts contain the declarative Kubernetes resource files required to deploy an application. Similar to an RPM, it can also declare one or more dependencies that the application needs in order to run.

(Andrew Block, JUNE 2020)

Advantages of Helm Chart:

* Helm chart provided reusable templates for Kubernetes deployment, which allowed us to update the configuration during the deployment phase for different environments.
* Helm provides a dependency option, which allows us to integrate with another dependent application deployment. Using Helm dependency, we now package and deploy the entire solution as one single chart or deployment.
* Helm also manages application version and lifecycle (Install, Upgrade and Rollback and Uninstall)

## Code Repositories

#### Code Structure

The code is structured keeping in mind the NodeJS requirements, NPM requirements, Helm packaging, and Cypress Test. The Helm folder contains the Kubernetes manifest, services, and value files. The code repository also contains Azure Test and Build Pipeline file, which is executed in the Azure DevOps pipeline. Cypress Test specification is available in the “cypress” folder.

Text

Description automatically generated

azure-end-2-end-test.yaml : Contains azure pipeline code for building and testing docker image.

azure-pipeline.yaml: Contains azure pipeline code for creation of docker image and Helm chart. Both Helm chart and docker image is published to Azure Container Registry

Figure :Source Code Structure

### Code Repositories

Each Microservice has its repository. This allows us to control the build, versioning, and release independently.

|  |  |
| --- | --- |
| Repository Name | Purpose |
| EAD\_CA2\_BP\_INFO\_SERVICE | Business function, which accepts blood pressure readings and computes the Level. |
| EAD\_CA2\_BP\_DATA\_SERVICE | Provides historical blood pressure readings based on ID like email |
| EAD\_CA2\_BP\_RECORDING\_SERVICE | Service which records the blood pressure reading to the database |
| EAD\_CA2\_BP\_FE\_SERVICE | Front End UI service Blood Pressure reading |
| EAD\_CA2\_BP\_DEPLOYMENT | Provides the Solution as Helm Chart packaging all the above services as dependencies. The repository also contains deployment pipeline code for Mongo Database and Ingress-nginx configuration. |

# Architectural Challenges

## High Scalability and Availability

The application is deployed in the Kubernetes cluster as a POD. A pod is a basic deployment unit, which is orchestrated by the Kubernetes engine to distribute and scale in their clustered nodes. Kubernetes will handle scalability, and maintain SLA, security, communication, and high availability.

Each Microservices application is deployed with a minimum of 2 replicas, to support High Availability.

Kubernetes manages the load balancing between the replicas.

Kubernetes will ensure each replica resides on different nodes, to keep application redundancy when any node suffers a failure.

Kubernetes will respect the SLA, which means it will maintain a minimum number of replica sets in the cluster for each Microservices.

# Networking, Exposing Services

A picture containing text

Description automatically generatedMicroservices deployed in Kubernetes expose their container port, using a service. Kubernetes assign a virtual IP to that service, which is known as “ClusterIP”. The service with virtual IP and the Port number becomes a communication endpoint for the application.

Figure 4 : Sample Service YAML

The deployment manifest file contains the configuration for the creation of the service. The Blood Pressure Web Application microservices will expose their service as default, “ClusterIP”, restricting pod accessibility within the cluster.

The client will access the Front-End UI of the web application using a Public IP.

The service type for the Front-End UI remains as “ClusterIP”. The external traffic will be proxied to the Front-End UI Service using the “Ingress-Nginx” Kubernetes Load-Balancer.

## Nginx Ingress Controller (expose service to Web)

Diagram

Description automatically generated*An Ingress Controller is a Kubernetes controller that is deployed manually to the cluster, most often as a Daemon Set or a Deployment object that runs dedicated Pods for handling incoming traffic load balancing and smart routing. It is responsible for processing the Ingress objects (which specify that they especially want to use the Ingress Controller) and dynamically configuring real routing rules. A commonly used Ingress controller for Kubernetes is* ***ingress-nginx***

(McKendrick, 2022)

Ingress-Nginx controller scans all namespaces for resources of the kind “Ingress”, which contains routing information based on the path prefix. The routing information maps the URL’s path prefix with a Kubernetes service name and port, thus routing traffic to the respective service in the backend.

Text

Description automatically generated

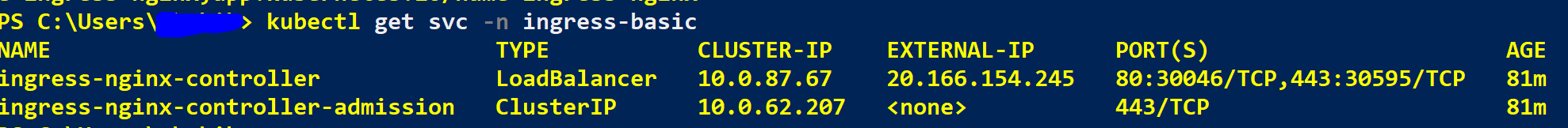
Figure : Ingress YAML file

## Deploying Ingress Controller

Ingress controller is not available by default in many Cloud Infrastructure, it can be deployed using minimum effort. The details are provided in [Installation Guide - NGINX Ingress Controller (kubernetes.github.io)](https://kubernetes.github.io/ingress-nginx/deploy/) and [Create an ingress controller in Azure Kubernetes Service (AKS) - Azure Kubernetes Service | Microsoft Learn](https://learn.microsoft.com/en-us/azure/aks/ingress-basic?tabs=azure-cli#create-an-ingress-controller)

Ingress Controller is delivered as Helm chart, which starts an Ingress Nginx POD and provisions a Service of type “LoadBalancer”. When a service is exposed as type “LoadBalancer” in the cluster, Kubernetes assign a Public IP to this service, which is visible as “EXTERNAL-IP”.

Figure 6: ingress-nginx-controller

External Traffic is received on the Public IP by the Ingress controller. The routing rules prepared using configuration will route the traffic to the configured service based on the path prefix.

# DevSecOps Delivery Pipeline

## Delivery Pipeline

The Blood Pressure Web Application is divided into 4 independent deliverable services or applications. All applications are NodeJS Applications, it will use NPM (Node Package Manager) to assemble their dependencies at runtime. Dockerfile is provided in every repository to package a Docker image and pushed to ACR (Azure Container Registry).

Finally, the application is packed as a Helm Chart. The helm chart contains the Kubernetes Manifest file that defines the pod (, Kubernetes basic processing unit). Pod will download and compose a docker image on startup. Helm chart also contains the Service YAML file, which specifies the ports to be exposed, which is a service name.

### Azure Pipeline

Azure DevOps provides the infrastructure for developing and running the Pipeline. It has options to connect to ACR, AKS, and external GitHub Repository. The pipeline has credentials, authorizations, and service connections to facilitate the build, release, and deployment of the application.

### Build Stages

Diagram

Description automatically generated

Figure : Build Stages

**Build Pipeline**

The build and release pipeline is stored as a YAML file in our code repository. Azure Pipeline provisions these files, and executes them when code change is triggered.

### List of all Build and Release pipelines

|  |  |  |
| --- | --- | --- |
| Name | Pipeline File | Purpose |
| Data-Service-Test | [azure-end-2-end-test.yaml](https://github.com/AINULX00159358/EAD_CA2_BP_DATA_SERVICE/blob/main/azure-end-2-end-test.yaml) | Build Docker image, Check Vulnerability, Integration Test for bpDataService app |
| Data-Service-Build | [azure-pipeline.yaml](https://github.com/AINULX00159358/EAD_CA2_BP_DATA_SERVICE/blob/main/azure-pipeline.yaml) | Package Docker Image and Helm Chart to Azure Container Registry for bpDataService app |
| INFO-SERVICE-TEST | [azure-end-2-end-test.yaml](https://github.com/AINULX00159358/EAD_CA2_BP_INFO_SERVICE/blob/main/azure-end-2-end-test.yaml) | Build Docker image, Check Vulnerability, Integration Test for bpInfoService app |
| INFO-SERVICE-BUILD | [azure-pipeline.yaml](https://github.com/AINULX00159358/EAD_CA2_BP_INFO_SERVICE/blob/main/azure-pipeline.yaml) | Package Docker Image and Helm Chart to Azure Container Registry for bpInfoService app |
| Recording-service-test | [azure-end-2-end-test.yaml](https://github.com/AINULX00159358/EAD_CA2_BP_RECORDING_SERVICE/blob/main/azure-end-2-end-test.yaml) | Build Docker image, Check Vulnerability, Integration Test for bpRecordingService app |
| Recording-service-build | [azure-pipeline.yaml](https://github.com/AINULX00159358/EAD_CA2_BP_RECORDING_SERVICE/blob/main/azure-pipeline.yaml) | Package Docker Image and Helm Chart to Azure Container Registry for bpDataService app |
| FE-Service-Test | [azure-end-2-end-test.yaml](https://github.com/AINULX00159358/EAD_CA2_BP_FE_SERVICE/blob/main/azure-end-2-end-test.yaml) | Build Docker image, Check Vulnerability, Integration Test for bpFEService app |
| FE-Service-Build | [azure-pipeline.yaml](https://github.com/AINULX00159358/EAD_CA2_BP_FE_SERVICE/blob/main/azure-pipeline.yaml) | Package Docker Image and Helm Chart to Azure Container Registry for bpFEService app |
| SOLUTION-BUILD | [helm-build-pipeline.yaml](https://github.com/AINULX00159358/EAD_CA2_BP_DEPLOYMENT/blob/main/Pipelines/helm-build-pipeline.yaml) | Package all above applications as Helm Chart Dependency and publish a common Helm Chart to Azure Container Registry |

Table : Build Pipelines

#### Text Description automatically generatedSolution Build

Figure 8 : Helm Chart Dependency

The “SOLUTION-BUILD” prepares the Helm charts for the solution, packing all microservices as its dependent Charts, and a common value file. The Helm chart is published to Azure Container Registry as “charts/bpwebapp”.

The Helm chart from the Solution-build also packages a service manifest for the Mongo Database service of type “ExternalName”.

Diagram

Description automatically generated

Figure 9 : Service Type as External Name

Services of type ExternalName can be used to proxify applications that are not actually running on your cluster, while still keeping the Service as a layer of abstraction that can be updated at any time.

(Raul, 2021)

Mongo Database service is deployed in the “mongo” namespace. Application in other namespaces like “blue” or “green” can access the service FQDN. But instead using an ExternalName allows us to update the service dynamically without updating the running application consuming it.

Text

Description automatically generated

Figure 10 : MongoDB ExternalName Service

#### Packaging the Solution

Diagram

Description automatically generated

Figure : Helm Chart Packaging Solution

### Vulnerability Scan

Software vulnerability scan must be carried on the deployable artifacts and container images, before releasing the software for production.

Trivy Scan is an open-source tool that can scan docker images for various vulnerabilities and breaches. The scanner is integrated into the Azure Build Pipeline stages so that vulnerability scanning is done in every build pushing it to the Azure Container Registry.

The vulnerability report will be published in the build pipeline.

To use Trivy Scan, it is first installed on the build VM machine. After the docker image is built, the Trivy scan is executed for the vulnerability scan. The image build is passed as a parameter to the Trivy scanner.

Text

Description automatically generated

Figure : Trivy Scanner script

Trivy Scan, by default, exits with exit code of 0. If the build must be broken in case of Critical and High vulnerabilities, “*--exit-code 1*” option will be added to the Trivy scan command.

### Automation in E2E Testing

Cypress provides an E2E Test framework. It is capable of testing application that uses web UI or REST interface. It is specifically designed for NodeJS applications capable of doing live testing of UI components. The reporting tool is added to consume to test result and publish it to the test pipeline. Cypress Test process is integrated into the Azure Build Pipeline, which provides the capability to perform End to End Test during the build process, before pushing the docker image to ACR.

To run the Cypress test, the NodeJS application should be running. The application’s docker image is executed in the local docker environment, along with its dependencies. Cypress Test will perform an “End to End” test, calling the application’s exposed endpoints.

Cypress test is executed using NPM command, with reporting format as JUNIT. The test report is piped to a file, which is published to the Build Pipeline Result.

A screenshot of a computer

Description automatically generated with medium confidence

Figure : Cypress E2e Testing pipeline config

#### Sample Test Report

Graphical user interface, text, application

Description automatically generated

Figure : Sample test report

### Deployment Pipeline

The Blood Pressure Web Application is deployed to the Azure Kubernetes cluster. The deployment will require “Service Connection”, which acts like authorization for the pipeline to deploy on Azure Kubernetes. The Service connection is created using a Service Account. There will be a service connection per namespace.

The Release Pipeline deploys the Helm Chart created and pushed by the build pipeline to the Kubernetes cluster.

Diagram

Description automatically generated

Figure : Deployment Pipeline high-level view

### Deployment Strategy (Blue Green Deployment)

The deployment process starts by creating a Release Branch. The docker image and helm chart version are tagged by REL-*version-number.*  (REL stands for Release. All deployments are triggered manually using a dedicated release pipeline for different namespaces. All security and authorization are injected into the pipeline, reducing any user entry.

#### Blue Green Deployment Strategy

Graphical user interface, diagram

Description automatically generatedBlue-green deployment is a technique to reduce the downtime associated with the release. It concerns having two identical production environments, one called **green**, the other called **blue**.

If we want to make a new release, then we deploy everything to the green environment and, at the end of the release process, change the load balancer to the green environment. (Leszko, 2017)

To accomplish Blue Green Deployment, the Blood Pressure Application is deployed in two different namespaces, blue and green. Nginx Ingress configuration will be used to expose the application to public IP. As per the norm, an application that is marked as blue is considered Live. The green namespace is reserved for application staging.

Diagram, schematic

Description automatically generatedFigure : Blue Green Deployment High Level View

## 

## Azure Release Pipelines

Link to Releases: <https://dev.azure.com/AINULX001593580081/EAD_CA2/_release>

### Deployment Pipelines

|  |  |
| --- | --- |
| Release Pipeline Name | JSON File |
| Application Deployment BLUE | [Application Deployment BLUE.json](https://github.com/AINULX00159358/EAD_CA2_BP_DEPLOYMENT/blob/main/Pipelines/Application%20Deployment%20BLUE.json) |
| Application Deployment GREEN | [Application Deployment GREEN.json](https://github.com/AINULX00159358/EAD_CA2_BP_DEPLOYMENT/blob/main/Pipelines/Application%20Deployment%20GREEN.json) |

Table : Deployment Pipeline

## Blue Green Pipelines

|  |  |
| --- | --- |
| Release Pipeline Name | JSON File |
| BlueToGreen | [BlueToGreen.json](https://github.com/AINULX00159358/EAD_CA2_BP_DEPLOYMENT/blob/main/Pipelines/BlueToGreen.json) |
| GreenToBlue | [GreenToBlue.json](https://github.com/AINULX00159358/EAD_CA2_BP_DEPLOYMENT/blob/main/Pipelines/GreenToBlue.json) |

Table : Blue Green Traffic Pipelines

## Monitoring and Logging

### Kubernetes Cluster Metrics

Kubernetes has a dedicated service, called “kube-state-metrics”, which listens to the Control Plane and generates metrics about resources. These metrics provide valuable insight about the health of the cluster, resource utilization and deployed artefacts. Alerts is also configured using the Kubernetes monitoring and metrics.

Azure provides in-house monitoring tools for Kubernetes, which analyse logs, generate metrics, and configure alerts. External cloud-based monitoring and logging solution is popular in enterprise world. Some popular examples are Datadog, Splunk, Dynatrace, etc. These solutions requires a light weight agent or jobs in the cluster, which scrapes logs and metrics to the cloud server.

Monitoring solution is also provided using Prometheus and Grafana. Both are added using Azure Portal to the monitoring workspace.

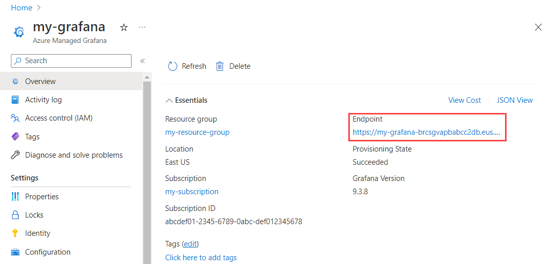
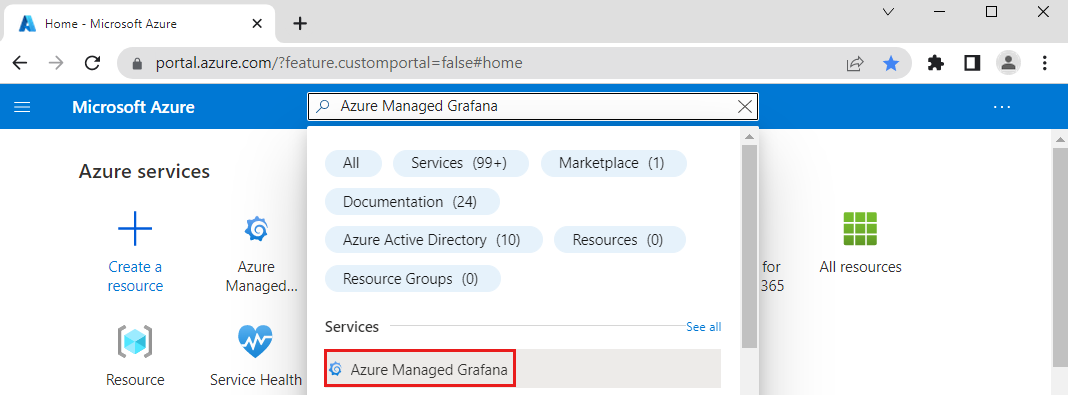
### Prometheus Integration

Prometheus is deployed from [GitHub](https://prometheus-community.github.io/helm-charts) using Helm Command. This deploys Prometheus “Node Exporter”, “Operator” and “State-Metrics”. Prometheus server is exposed as “Load Balancer” using a Configuration YAML file <https://github.com/AINULX00159358/EAD_CA2_BP_DEPLOYMENT/blob/main/monitoring/prometheus-loadbalancer.yaml>

This exposes the Prometheus server to external traffic, using a public IP passed in the YAML file.

### Add Grafana using Azure Portal

Azure portal provides a deployment Wizard to add the resource named “Azure Managed Grafana”. The wizard deploys a basic Grafana web application, using subscription ID, Resource Group and location. The basic deployment creates a Grafana workspace with a public endpoint.

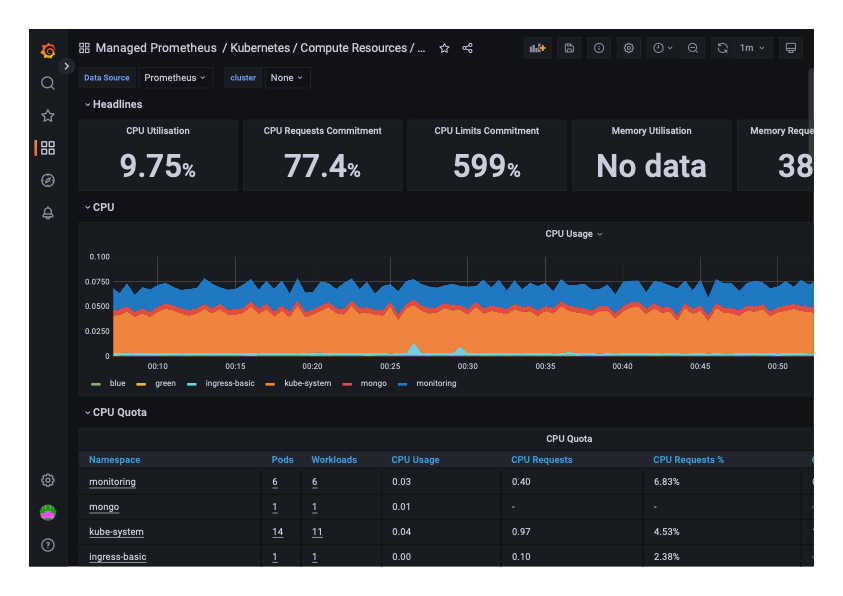


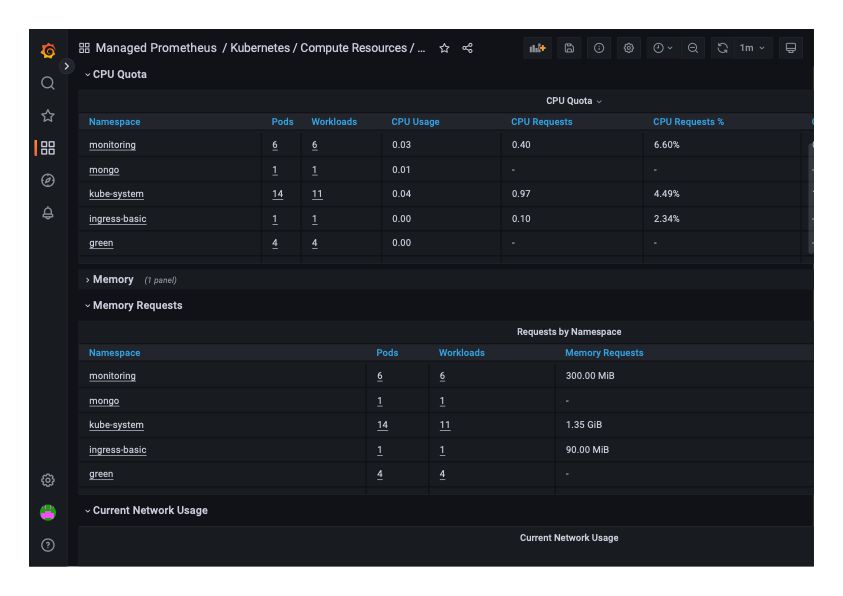
Connect to Prometheus server deployed in previous steps with Grafana.

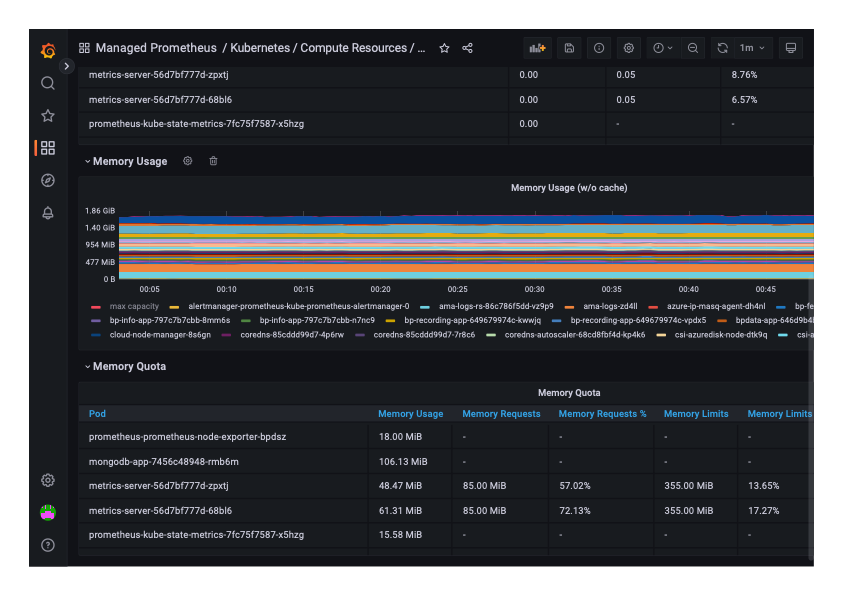
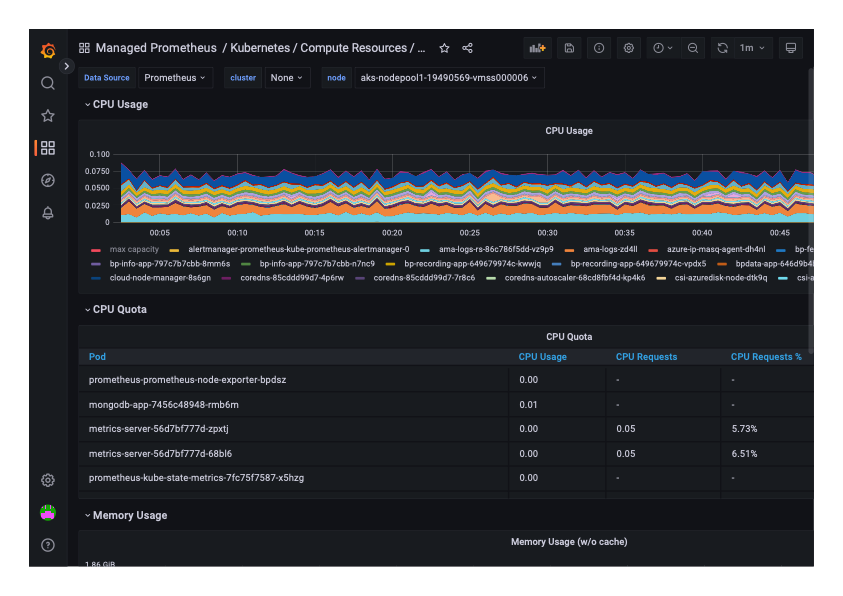
Prometheus is added as a “Data Source” in Grafana using Prometheus Server Load Balancer IP, exposed in previous steps. After Prometheus “Data Source” is synced, Kubernetes Dashboards starts populating the metrics after few seconds.

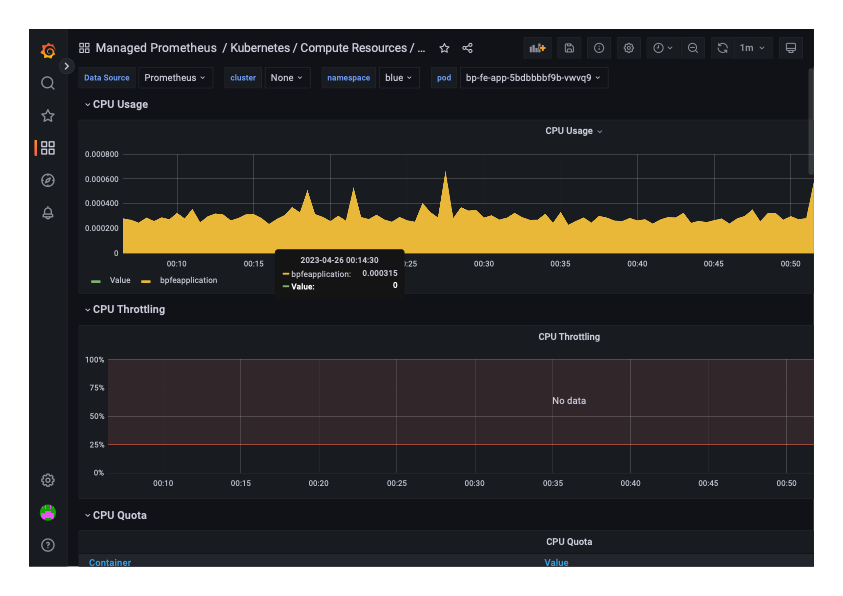
Prometheus Agents collect all the metrics from Kubernetes “metric-server” and “control pane”, scrapes it to Prometheus server. Grafana pulls these metrics to populate the graphs and user interfaces.

Some screen shorts of the Dashboard is provided below









## Code Repositories

### EAD\_CA2\_BP\_RECORDING\_SERVICE (https://github.com/AINULX00159358/EAD\_CA2\_BP\_RECORDING\_SERVICE)

Bottom of Form

### EAD\_CA2\_BP\_FE\_SERVICE (https://github.com/AINULX00159358/EAD\_CA2\_BP\_RECORDING\_SERVICE)

### EAD\_CA2\_BP\_DEPLOYMENT ( https://github.com/AINULX00159358/ EAD\_CA2\_BP\_DEPLOYMENT)

Bottom of Form

### EAD\_CA2\_BP\_INFO\_SERVICE ( https://github.com/AINULX00159358/ EAD\_CA2\_BP\_INFO\_SERVIDE)

### EAD\_CA2\_BP\_DATA\_SERVICE (( https://github.com/AINULX00159358/ EAD\_CA2\_BP\_DATA\_SERVICE))

# List of Figures

[Figure 1: Current Design 1](#_Toc133319140)

[Figure 2: Updated Microservices 2](#_Toc133319141)

[Figure 3:Source Code Structure 4](#_Toc133319142)

[Figure 4 : Sample Service YAML 5](file:///C:\Users\ahabib\Desktop\MSC-DevOPS_Reaserch\ReleaseManagementPlan_EADCA2.docx#_Toc133319143)

[Figure 5 : Ingress YAML file 6](#_Toc133319144)

[Figure 6: ingress-nginx-controller 6](file:///C:\Users\ahabib\Desktop\MSC-DevOPS_Reaserch\ReleaseManagementPlan_EADCA2.docx#_Toc133319145)

[Figure 7 : Build Stages 8](#_Toc133319146)

[Figure 8 : Helm Chart Dependency 9](file:///C:\Users\ahabib\Desktop\MSC-DevOPS_Reaserch\ReleaseManagementPlan_EADCA2.docx#_Toc133319147)

[Figure 9 : Service Type as External Name 9](file:///C:\Users\ahabib\Desktop\MSC-DevOPS_Reaserch\ReleaseManagementPlan_EADCA2.docx#_Toc133319148)

[Figure 10 : MongoDB ExternalName Service 9](file:///C:\Users\ahabib\Desktop\MSC-DevOPS_Reaserch\ReleaseManagementPlan_EADCA2.docx#_Toc133319149)

[Figure 11: Helm Chart Packagig Solution 10](#_Toc133319150)

[Figure 12: Trivy Scanner script 10](#_Toc133319151)

[Figure 13 : Cypress E2e Testing pipeline config 11](#_Toc133319152)

[Figure 14: Sample test report 11](#_Toc133319153)

[Figure 15 : Deployment Pipeline high level view 12](#_Toc133319154)

[Figure 16 : Blue Green Deployment High Level View 13](#_Toc133319155)

# List of Tables

[Table 1: Build Pipelines 9](#_Toc133319186)

[Table 2 : Deployment Pipeline 13](#_Toc133319187)

[Table 3 : Blue Green Traffic Pipelines 13](#_Toc133319188)

# References

Andrew Block, A. D., JUNE 2020. *Learn Helm.* s.l:PACKT.

Leszko, R., 2017. *Continuous Delivery with Docker and Jenkins.* s.l.:Packt.

McKendrick, N. K. a. R., 2022. *The Kubernetes Bible: The Definitive Guide to Deploying and Managing Kubernetes Across Major Cloud Platforms.* s.l.:Packt.

Raul, A., 2021. *Cloud Native with Kubernetes: Deploy, configure, and run modern cloud native applications on Kubernetes.* s.l.:Packt.