Module: ITS 4243 Microservices and Cloud Computing
Assignment: 2
Index No: ICT/18/820
Name: H.M.G.C Herath

Part 1 - A

01)

Microservices are an architectural style that structures an application as a collection of services that are independent of each other and communicate over well-defined APIs. Each service performs a single function and is built for business capabilities. Microservices allow a large application to be separated into smaller independent parts, with each part having its own realm of responsibility.

02)

Container Runtime Platform

A container runtime platform is a software component that can run containers on a host operating system. It is responsible for loading container images from a repository, monitoring local system resources, isolating system resources, and creating and running containers. A container engine is a general software platform that supports container use. Typical container engines include Docker, CRI-O, RKT, and LXD.

Container Image

A container image is a lightweight, standalone, executable package of software that includes everything needed to run an application: code, runtime, system tools, libraries, and settings. It is a file that contains all the necessary components to run an application in a container.

03).

Container Orchestration Tools

Container orchestration tools are used to automate the deployment, management, scaling, and networking of containers. They provide a framework for managing containers and microservices architecture at scale. Container orchestration tools automate many tasks such as provisioning and deployment of containers, redundancy and failover, load balancing, and traffic routing, monitoring container health, configuring applications based on the container in which they will run, keeping interactions between containers secure, and more.

Container Registry

A container registry is a repository used to store and access container images. It is a place for developers to save, share, and access container images as they are created.

Infrastructure Monitoring Tools

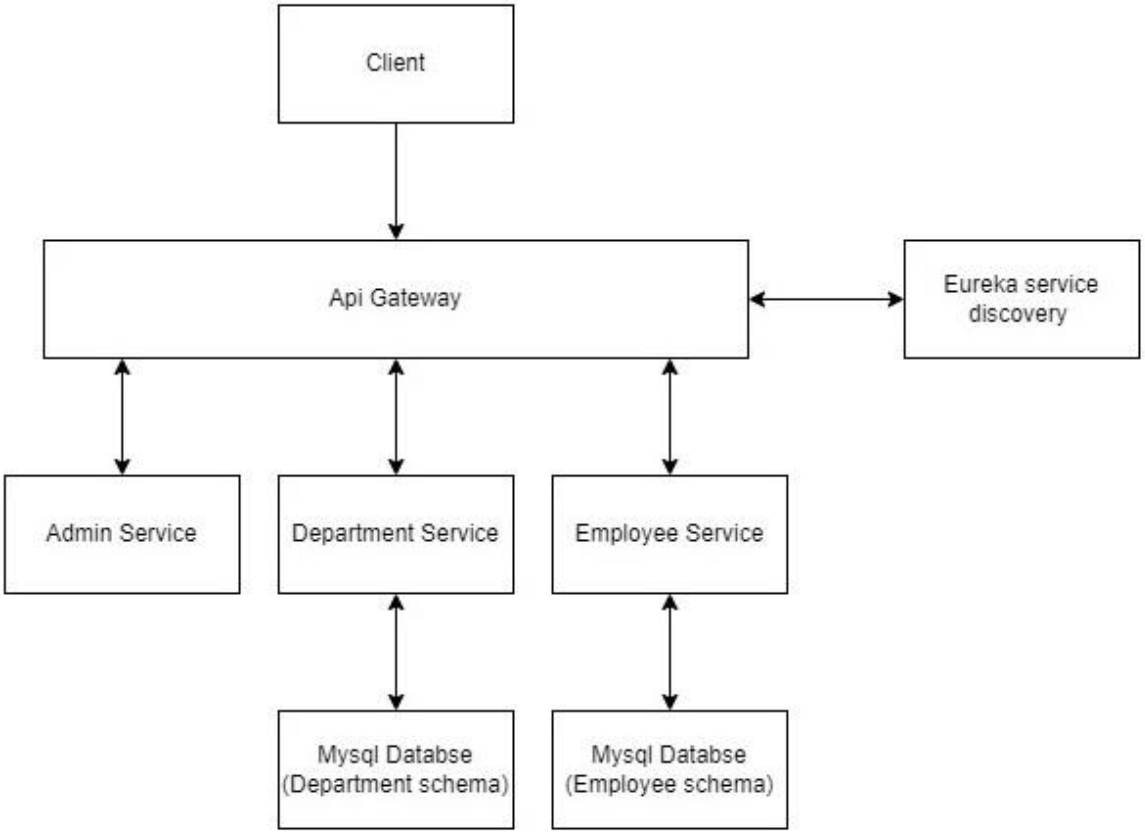
These tools provide insights into the performance and health of your microservices running inside containers.

Network Infrastructure

Network infrastructure is an essential component of containerization. Containers are a streamlined way to build, test, deploy, and redeploy applications on multiple environments from a developer's local laptop to an on-premises data center and even the cloud. Container orchestration automates the deployment, management, scaling, and networking of containers. It enables developers to easily build containerized applications and services, as well as scale, schedule, and monitor those containers.

Part 1 - B

The following is a high-level design diagram for the given scenario.



Implementation and source code :
https://github.com/Gayan1998/Microservice_Assignment-2.git

Necessary steps are required if the client further requires to containerize the above solution.

1. Install Docker
2. Create Dockerfiles
3. Build Docker Images
4. Create Docker Compose File
5. Start the Services
6. Test the Services
7. Push Docker Images to the Repository
8. Deploy the Services

Part 2

1).

Cloud Service Model

- **IaaS (Infrastructure as a Service)**
  Infrastructure as a Service (IaaS) is a form of cloud computing that provides virtualized computing resources over the Internet. In an IaaS service model, a cloud provider hosts the infrastructure components that are traditionally present in an on-premises data center, including servers, storage, and networking hardware, as well as the virtualization or hypervisor layer.

- **PaaS (Platform as a Service)**
  Platform as a Service (PaaS) is a cloud computing model where a third-party provider delivers hardware and software tools to users over the internet1. PaaS combines servers, storage, and network infrastructure with the software you need to deploy apps.

- **SaaS (Software as a Service)**
  Software as a Service (SaaS) is a software licensing model that allows access to software on a subscription basis, where the software is located on external servers rather than on servers located in-house.

Cloud Deployment Model

- **Public Cloud**
  A public cloud is a third-party managed platform that uses the standard cloud computing model to make resources and services available to remote users around the world. It is a pool of virtual resources developed from hardware owned and managed by a third-party company that is automatically provisioned and allocated among multiple clients through a self-service interface.

- **Private Cloud**

A private cloud is a cloud computing environment that is exclusively dedicated to a single entity or service1. It runs on the organization's premises or in a third-party data center and is not shared with other organizations.

- **Hybrid Cloud**
  A hybrid cloud is a cloud computing environment that uses a mix of on-premises, private cloud, and third-party public cloud services with orchestration between these platforms.

02).

Total Cost of Ownership (TCO) is an estimation of the expenses associated with purchasing, deploying, using, and retiring a product or piece of equipment. TCO is a management accounting concept that derives an asset's total cost during its useful life. It includes the purchase price, maintenance, and operational cost that will incur during the asset's lifespan.TCO can be calculated as the initial purchase price plus costs of operation across the asset lifespan. The overall TCO includes direct and indirect expenses, as well as some intangible ones that may be assigned a monetary value. The components of TCO depend on the item but should always include the initial purchase price, costs associated with installation and deployment, maintenance and support costs, energy consumption costs, and disposal costs.

03).

As a cloud solution architect, the following steps can be taken to handle a cloud migration project:

1. Establish the Cloud Migration Architect Role: The migration architect is a system architect-level position responsible for planning and completing all aspects of the migration.

2. Define Business Purpose for Migration: Define the business purpose for migration and assess your migration costs and needs.

3. Assess Your Organization's Readiness: Evaluate your organization's readiness for cloud migration.

4. Estimate the Costs and ROI: Estimate the costs and return on investment (ROI) of cloud migration.
5. Assess the Environment and Applications: Assess the environment and applications to determine which ones are suitable for cloud migration.

6. Choose Cloud Environment: Choose a cloud environment that suits your organization's needs, whether it is a single or multi-cloud environment.

7. Determine Deployment Model: Determine the deployment model that suits your organization's needs, whether it is Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS).

8. Choose a Strong Cloud Partner: Choose a strong cloud partner that can provide the necessary support and expertise throughout the migration process.

9. Choose the Right Architecture: Choose the right architecture that suits your organization's needs, whether it is a lift-and-shift approach or refactoring.

10. Conduct Security Testing: Conduct security testing to ensure no vulnerabilities exist before migrating to the cloud.

11. Execute the Migration: Implement the migration plan and migrate the workload, dependencies, and related data to the prepared cloud infrastructure. This process also involves making network changes such as configuring domain and IP environments.

12. Ongoing Support: Provide ongoing support after migration to ensure that everything runs smoothly in the new environment.

04).

Positives	Negatives
Cost Efficiency: Cloud computing is generally cheaper than traditional IT approaches and can significantly lower the overall technology-related expenses of a business.	**Lack of Knowledge**: One of the challenges of moving to the cloud is whether an organization has the ability to move to the cloud successfully.
Increased Storage Capacity: The cloud is known for being able to store much more data than classic servers or personal computers.	**Security Risks**: Cloud computing poses security risks as data is stored on third-party servers, which can be vulnerable to cyber-attacks.
Better Uptime and Convenience: Cloud computing provides better uptime and convenience as it allows users to access their data from anywhere with an internet connection.	**Dependence on Internet Connection**: Moving to the cloud means that an organization's operations are dependent on a stable Internet connection, which can be a challenge in areas with poor connectivity.
Improved Recovery and Backup: Cloud computing provides improved recovery and backup options as data is stored in multiple locations.	
Increased Flexibility for Employees: Moving to the cloud can increase flexibility for employees as they can access their work from anywhere with an internet connection.	
Increased Collaboration and Flexible Scalability: Migrating data to the cloud can increase collaboration and flexibility scalability as it allows multiple users to access the same data from different locations.	