CHAROTAR UNIVERSITY OF SCIENCE AND TECHNOLOGY
CHANDUBHAI S PATEL INSTITUTE OF TECHNOLOGY
K. D. PATEL DEPARTMENT OF INFORMATION TECHNOLOGY
ACADEMIC YEAR: 2022-23

List of Experiments

===

Subject Name: Cloud Computing   **Semester:** 7
Subject Code: IT449   **Academic Year:** 2022-23

===

Sr. No.	Practical	Hrs
1.	Understanding and Analyzing Your Costs with Google Cloud Billing Reports. Google Cloud cost management tools provide greater visibility, accountability, control, and intelligence so that you can scale your business in the cloud with confidence. Tailored to meet the needs of organizations of all sizes, these tools help reduce complexity and increase the predictability of your cloud costs. Google Cloud Billing reports is a cost management tool that provides built-in reporting within the Google Cloud Console. In this lab, you familiarize yourself with Billing reports and understand how to answer fundamental cost management questions, such as: How much am I spending? What are my cost trends? What are my cost drivers?	02
2.	Google Cloud Computing Foundations: Discuss what the cloud is and why it's a technological and business game changer. Describe the different ways a user can interact with Google Cloud. Discover the different compute options in Google Cloud. 2.1 Getting Started with Cloud Shell and gcloud 2.2 Creating a Virtual Machine 2.3 App Engine: Qwik Start – Python 2.4 Cloud Functions: Qwik Start - Command Line 2.5 Kubernetes Engine: Qwik Start 2.6 Set Up Network and HTTP Load Balancers	04
3.	Google Cloud Computing Foundations: Infrastructure in Google Cloud. Implement a variety of structured and unstructured storage models. Discuss the different application managed service options in the cloud. Outline how security in the cloud is administered in Google Cloud. 3.1 Cloud Storage: Qwik Start - CLI/SDK 3.2 Cloud SQL for MySQL: Qwik Start 3.3 Cloud Endpoints: Qwik Start 3.4 Google Cloud Pub/Sub: Qwik Start – Python 3.5 User Authentication: Identity-Aware Proxy 3.6 Cloud IAM: Qwik Start	04
4.	Google Cloud Computing Foundations: Networking and Security in Google Cloud. Demonstrate how to build secure networks in the cloud. Identify cloud automation and management tools. 4.1 Multiple VPC Networks 4.2 VPC Networks - Controlling Access 4.3 HTTP Load Balancer with Cloud Armor 4.4 Create an Internal Load Balancer 4.5 Cloud Monitoring: Qwik Start	06
5.	Kubernetes in Google Cloud: Kubernetes is the most popular container orchestration system and the Google Kubernetes Engine was designed specifically to support managed Kubernetes deployments in the Google Cloud. In this advanced-level quest, you will get hands-on practice configuring Docker images and containers, and deploying fully-fledged Kubernetes Engine applications. This quest lab will teach you the practical skills needed for integrating container orchestration into your own workflow.	06

6.	Google Cloud Certificate Authority Service (CAS) is a highly available & scalable service that enables you to simplify, automate, and customize the deployment, management, and security of private certificate authorities (CA). In this hands-on lab you'll learn how to enable the service API, create a root, a subordinate CA and eventually issue a certificate.	02
7.	Building a VPN Between Google Cloud and AWS with Terraform. This lab will show you how to use Terraform by HashiCorp to create secure, private, site-to-site connections between Google Cloud and Amazon Web Services (AWS) using virtual private networks (VPNs). This is a multi-cloud deployment. In this lab, you will deploy virtual machine (VM) instances into custom virtual private cloud (VPC) networks in Google Cloud and AWS. You then deploy supporting infrastructure to construct a VPN connection with two Internet Protocol security (IPsec) tunnels between the Google Cloud and AWS VPC networks. The environment and tunnel deployment usually completes within four minutes.	02
8.	Troubleshooting Workloads on GKE for Site Reliability Engineers. Site Reliability Engineers (SRE) have a broad set of responsibilities, and managing incidents is a critical part of their role. You will learn how to take advantage of the integrated capabilities of Google Cloud's operations suite that includes logging, monitoring, and rich, out-of-the-box dashboards.	02
9.	Using Role-based Access Control in Kubernetes Engine. While RBAC resource definitions are standard across all Kubernetes platforms, their interaction with underlying authentication and authorization providers needs to be understood when building on any cloud provider. RBAC is a powerful security mechanism that provides great flexibility in how you restrict operations within a cluster. This lab will cover two use cases for RBAC: Assigning different permissions to user personas, namely owners and auditors. Granting limited API access to an application running within your cluster.	02