ASSIGNMENT 2:

USE GCP CLOUD TO CREATE A VM TO LEVERAGE AUTO SCALING AND SECURITY

B Mugundhan
G24AI1051
24ai1051@iitj.ac.in

TABLE OF CONTENTS

Introduction

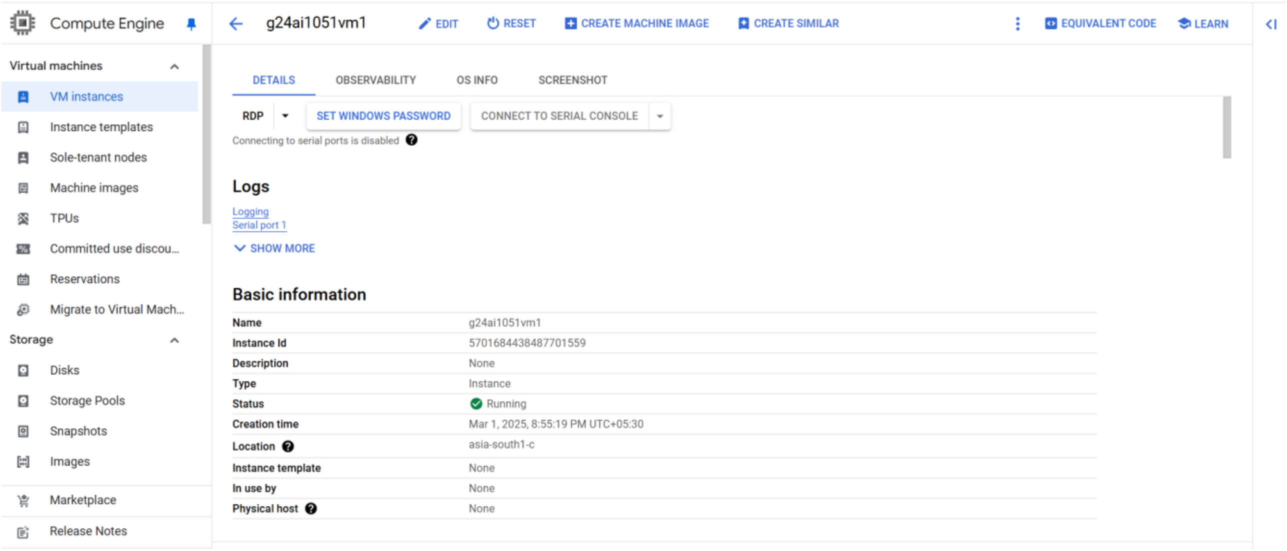
THIS ASSIGNMENT AIMS TO SET UP A VIRTUAL MACHINE (VM) IN THE GOOGLE CLOUD PLATFORM (GCP), IMPLEMENT AUTO-SCALING POLICIES BASED ON WORKLOAD, AND CONFIGURE SECURITY MEASURES SUCH AS FIREWALL RULES AND IAM ROLES. THIS REPORT GIVES A PROCESS OF VM CREATION IN CGP, ALONG WITH AN ARCHITECTURE DESIGN AND REFERENCES TO RELEVANT RESOURCES.

DELIVERABLES

1. STEP-BY-STEP INSTRUCTIONS FOR IMPLEMENTATION

1.1 CREATION OF A VM INSTANCE ON GCP

1. **Sign in to GCP Console:**
   - Navigate to GCP Console.
   - Giving necessary permission to VM instance.
2. **Create a New VM Instance:**
   - Go to the **Compute Engine** section.
   - Click on **VM instances** => **Create Instance**.
   - Creating with the following details:
     - **Name**: g24ai1051-vm1.
     - **Region & Zone**: as we are located in INDIA, choosing Mumbai and zones.
     - **Machine Type**: choosing E2 CPU and memory configuration.
     - **Boot Disk**: Select an operating system such as Windows Server
     - **Firewall Rules**: Enable HTTP/HTTPS traffic if required.
   - **Create** to launch the VM instance.



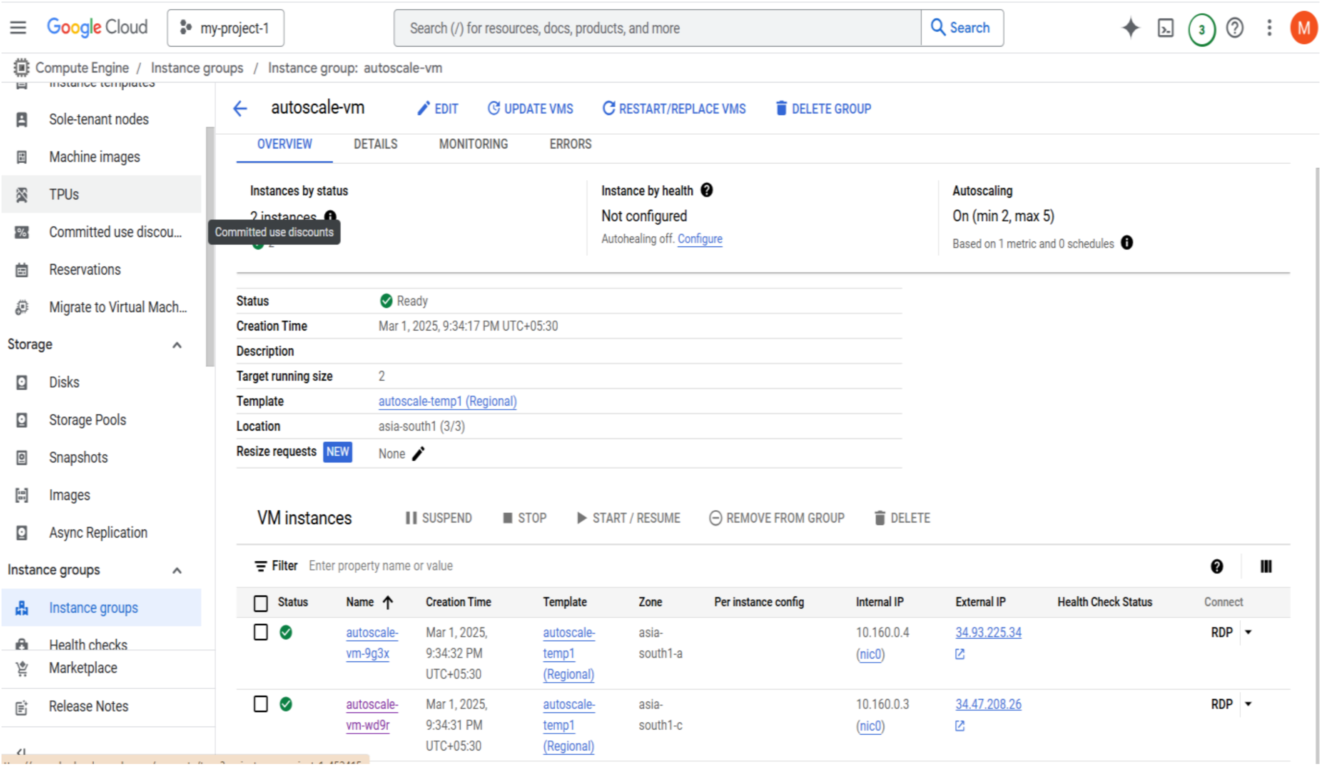
Connecting to serial ports is disabled

Basic information

Name	g24ai1051vm1
Instance Id	5701684438487701559
Description	None
Type	Instance
Status	✓ Running
Creation time	Mar 1, 2025, 8:55:19 PM UTC+05:30
Location	asia-south1-c
Instance template	None
In use by	None
Physical host	None

1.2 CONFIGURATION OF AUTO-SCALING POLICIES

1. **Create an Instance Template:**
   - Navigate to **Compute Engine** > **Instance Templates** > **Create Instance Template**.
   - Configure the machine as we require, I created the same as the VM1.
   - Click **Create**.
2. **Create a Managed Instance Group (MIG):**
   - Go to **Compute Engine** > **Instance Groups** > **Create Instance Group**.
   - Select **Managed instance group**.
   - Choose the instance template created earlier.
   - Define Autoscaling policies:
     - Enable autoscaling.
     - Set up metrics such as CPU utilization (e.g., increase instances when CPU usage exceeds 60%).
     - Define minimum and maximum instances to ensure scalability limits as minimum as 2 and maximum as 5.
   - Click **Create**.



Instances by status
2 instances

Instance by health
Not configured
Autohealing off. Configure

Autoscaling
On (min 2, max 5)
Based on 1 metric and 0 schedules

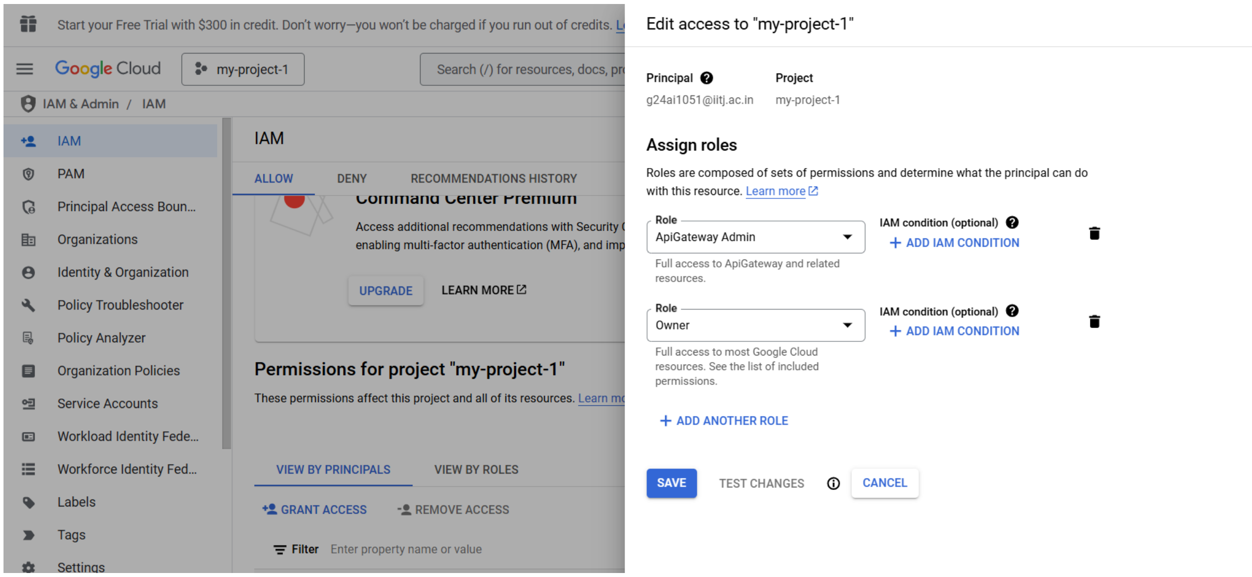
Status	✓ Ready
Creation Time	Mar 1, 2025, 9:34:17 PM UTC+05:30
Description	
Target running size	2
Template	autoscale-temp1 (Regional)
Location	asia-south1 (3/3)
Resize requests NEW	None

VM instances

□	Status	Name ↑	Creation Time	Template	Zone	Per instance config	Internal IP	External IP	Health Check Status	Connect
□	✓	autoscale-vm-9g3x	Mar 1, 2025, 9:34:32 PM UTC+05:30	autoscale-temp1 (Regional)	asia-south1-a		10.160.0.4 (nic0)	34.93.225.34		RDP ▾
□	✓	autoscale-vm-wd9r	Mar 1, 2025, 9:34:31 PM UTC+05:30	autoscale-temp1 (Regional)	asia-south1-c		10.160.0.3 (nic0)	34.47.208.26		RDP ▾

1.3 IMPLEMENTATION OF SECURITY MEASURES

1. **Setting Up IAM Roles:**
   - Navigate to **IAM & Admin** > **IAM**.
   - Click **Add** to assign roles to users or service accounts.
   - Select the appropriate roles such as:
     - **Compute Viewer** (Read-Only Access)
     - **Compute Admin** (Full Access)
     - Custom roles based on specific permissions.
   - Click **Save** to apply changes.
2. **Configuring Firewall Rules:**
   - Navigate to **VPC Network** > **Firewall** > **Create Firewall Rule**.
   - Provide the following details:
     - **Name**: Name as auto-scalling- firewall.
     - **Direction**: Choose **Ingress** (incoming traffic) or **Egress** (outgoing traffic).
     - **Targets**: Specify whether the rule applies to all instances or specific tags.
     - **Source/Destination**: Define the IP range (e.g., allow only internal traffic 10.0.0.0/16).
     - **Protocol and Ports**: Allow or deny traffic for specific protocols (e.g., TCP: 22 for SSH, TCP: 80 for HTTP).
     - Click **Create** to enforce the rule.



Start your Free Trial with $300 in credit. Don't worry—you won't be charged if you run out of credits. L

Access additional recommendations with Security C enabling multi-factor authentication (MFA), and imp

Permissions for project "my-project-1"

These permissions affect this project and all of its resources. Learn mo

Edit access to "my-project-1"

Principal: g24ai1051@iitj.ac.in

Project: my-project-1

Assign roles

Roles are composed of sets of permissions and determine what the principal can do with this resource. Learn more

Role: ApiGateway Admin — IAM condition (optional) + ADD IAM CONDITION

Full access to ApiGateway and related resources.

Role: Owner — IAM condition (optional) + ADD IAM CONDITION

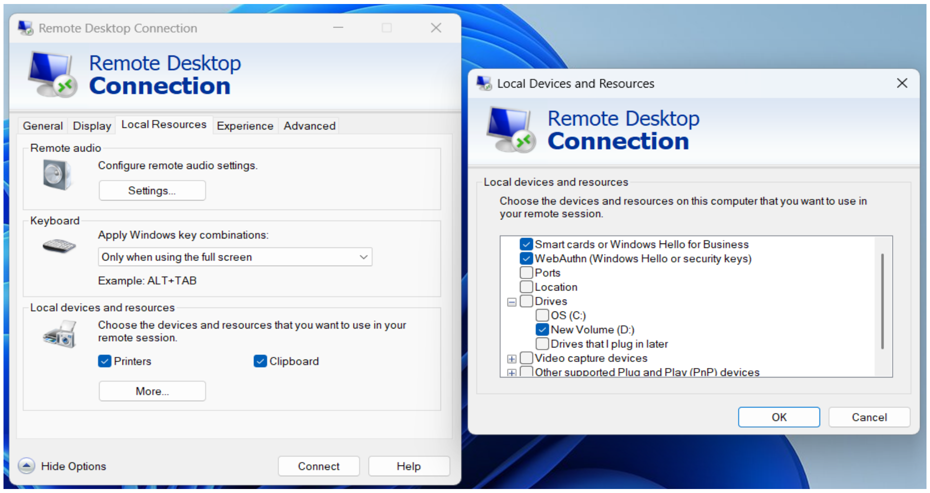
Full access to most Google Cloud resources. See the list of included permissions.

+ ADD ANOTHER ROLE

SAVE   TEST CHANGES   CANCEL

2. ACCESSING VIRTUAL MACHINE FROM PHYSICAL SYSTEM

1. **Setting Up remote desktop:**
   - Navigate to **Remote desktop**.
   - Paste the external IP from the VM that was created early.
   - Select the location pathway to share the files in the VM.
   - Get the password from the GCP – VM that we created.
   - And connect.


Remote Desktop Connection
Remote Desktop Connection
General
Display
Local Resources
Experience
Advanced
Settings...
More...
Hide Options
Connect
Help
Local Devices and Resources
Remote Desktop Connection
OK
Cancel

Remote audio

Configure remote audio settings.

Keyboard

Apply Windows key combinations:

Only when using the full screen

Example: ALT+TAB

Local devices and resources

Choose the devices and resources that you want to use in your remote session.

☑ Printers ☑ Clipboard

Local devices and resources

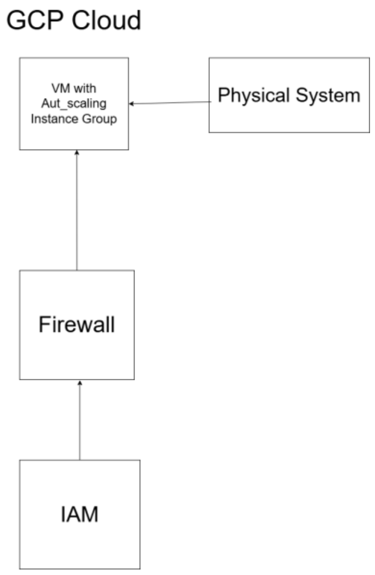
Choose the devices and resources on this computer that you want to use in your remote session.

☑ Smart cards or Windows Hello for Business
☑ WebAuthn (Windows Hello or security keys)
□ Ports
□ Location
□ Drives
  □ OS (C:)
  ☑ New Volume (D:)
  □ Drives that I plug in later
□ Video capture devices
□ Other supported Plug and Play (PnP) devices

   - After connecting we can access VM we can see there is one shared drive that connects the local system and the VM.

3. ARCHITECTURE DESIGN

1. Below is an overview of the GCP architecture:
   - VM Instance: A virtual machine hosted in GCP.
   - Managed Instance Group (MIG): Handles auto-scaling of VMs based on CPU utilization.
   - Firewall Rules: Defines inbound and outbound traffic control.
   - IAM Roles: Restricts access to specific users or service accounts.



3. GITHUB LINK AND VIDEO LINK

1. Git hub repo - https://github.com/Mugundh97B/Weather_application.git
2. Video Link – https://drive.google.com/drive/folders/152Q_55YLL20lat6LMgSjZpfJ1YjoTRcC?usp=sharing

CONCLUSION

This report can successfully deploy a virtual machine in GCP, implement auto-scaling based on workload demands, and enforce security measures to protect the infrastructure. This setup ensures efficient resource utilization and robust security control in a cloud environment.

REFERENCES

- Compute Engine (VMs) Overview: https://cloud.google.com/compute/docs
- Managed Instance Groups and Auto-Scaling: https://cloud.google.com/compute/docs/instance-groups
- Google Cloud Load Balancer (If used): https://cloud.google.com/load-balancing/docs
- Firewall Rules in GCP: https://cloud.google.com/vpc/docs/firewalls
- IAM Roles and Permissions: https://cloud.google.com/iam/docs/roles-overview