VIRTUAL MACHINE CREATION USING GCP

Virtualization and Cloud Computing

Subject: Virtualization and Cloud Computing

Assignment No: II

Submitted By: Purusothaman S

Student Id: G24AI1042

e-mail: g24ai1042@iitj.ac.in

Institute: Indian Institute of Technology Jodhpur

Submitted To: Assistant Professor, Dr. Sumit Karla

Table of Contents

1. Introduction

This Assignment report deals with a step-by-step guide to setting up a virtual machine (VM) in Google Cloud Platform (GCP), implementing auto-scaling policies based on workload, and configuring security measures such as firewall rules and IAM roles.

2. Creating a VM Instance on GCP

1. ***Sign in to GCP Console:***
    - Navigate to https://console.cloud.google.com/
    - Ensure you have the necessary permissions to create a VM instance.
2. ***Create a New VM Instance****:*
    - Go to the Compute Engine section.
    - Click on VM instances => Create Instance.
    - Provide the following details:
        - Name: Specify a unique name for the instance.
        - Region & Zone: Select the preferred location.
        - Machine Type: Choose the appropriate CPU and memory configuration.
        - Boot Disk: Select an operating system (e.g., Ubuntu, Debian, or Windows Server).
        - Firewall Rules: Enable HTTP/HTTPS traffic if required.
    - Click Create to launch the VM instance.

3. Configuring Auto-Scaling Policies

1. ***Create an Instance Template:***
    - Navigate to Compute Engine > Instance Templates > Create Instance Template.
    - Configure machine type, boot disk, and startup script as per your requirements.

- 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 70%).
  - Define minimum and maximum instances to ensure scalability limits.
- Click Create.

4. Implementing Security Measures

1. Setting Up IAM Roles

1. Navigate to IAM & Admin > IAM.
2. Click Add to assign roles to users or service accounts.
3. Select the appropriate roles such as:
   - Compute Viewer (Read-Only Access)
   - Compute Admin (Full Access)
   - Custom roles based on specific permissions.
4. Click Save to apply changes.

2. Configuring Firewall Rules

1. Navigate to VPC Network > Firewall > Create Firewall Rule.
2. Provide the following details:
   - Name: Unique firewall rule name.
   - Direction: Choose Ingress (incoming traffic) or Egress (outgoing traffic).

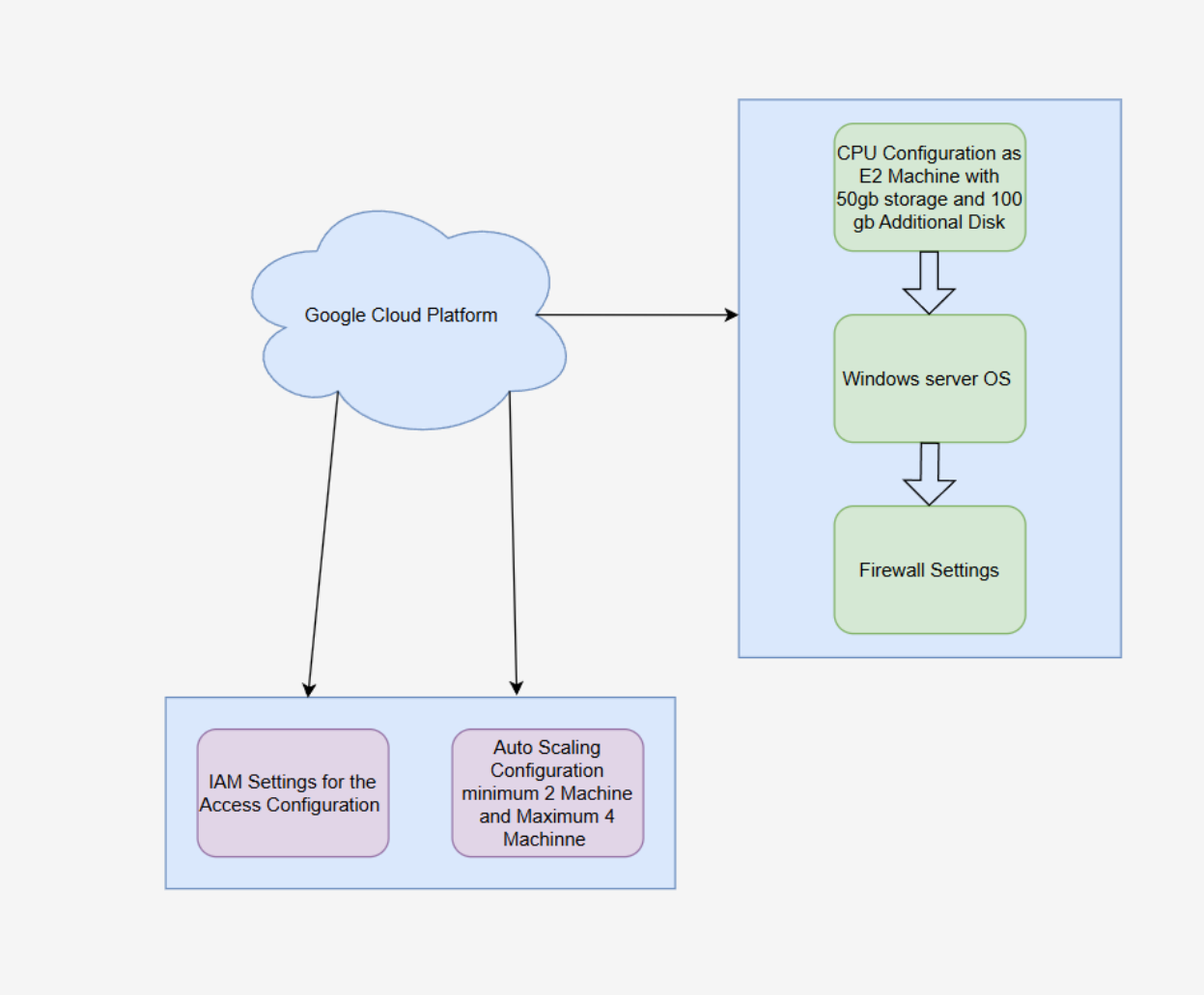
- Targets: Specify whether the rule applies to all instances or specific tags.
- Source/Destination: Define the IP range (e.g., allow only internal traffic 10.0.0.0/16).
- Protocol and Ports: Allow or deny traffic for specific protocols (e.g., TCP: 22 for SSH, TCP: 80 for HTTP).

3. Click Create to enforce the rule.

5. Architecture Design

Below is a high-level overview of the GCP architecture:

Diagram Overview:



- VM Instance: A virtual machine hosted in GCP.
- Managed Instance Group (MIG): Handles auto-scaling of VMs based on CPU utilization.
- Load Balancer (Optional): Distributes traffic among instances.
- Firewall Rules: Defines inbound and outbound traffic control.
- IAM Roles: Restricts access to specific users or service accounts.

6. Conclusion

By following these steps, you 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.

7. 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

https://cloud.google.com/compute/docs/autoscaler

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