**Hands-On Lab: Practicing Cloud Concepts**

**1. Setting Up the Environment**

* **Objective:** Set up accounts in AWS, Azure, and GCP.
* **Steps:**
  + Create free tier accounts on AWS, Azure, and GCP if not already done.
  + Familiarize yourself with the management consoles of each provider.

**2. Creating and Managing Virtual Machines (VMs)**

* **Objective:** Deploy and manage virtual machines in AWS, Azure, and GCP.
* **Steps:**
  + **AWS:**
    - Navigate to the EC2 Dashboard.
    - Launch a new EC2 instance (e.g., Amazon Linux 2).
    - Configure the instance type, security group, and key pair.
    - Connect to the instance via SSH.
    - Terminate the instance after testing.
  + **Azure:**
    - Navigate to the Azure Portal.
    - Create a new Virtual Machine (e.g., Ubuntu Server).
    - Configure the size, networking, and security settings.
    - Connect to the VM using SSH or RDP.
    - Delete the VM after testing.
  + **GCP:**
    - Navigate to the Google Cloud Console.
    - Create a new VM instance in Compute Engine.
    - Configure machine type, firewall rules, and SSH keys.
    - Connect to the VM using SSH.
    - Delete the VM after testing.

**3. Implementing Security Groups and Firewalls**

* **Objective:** Secure virtual machines by configuring security groups or firewalls.
* **Steps:**
  + **AWS:**
    - Create a new Security Group with custom rules (e.g., allowing HTTP and SSH traffic).
    - Attach the Security Group to an EC2 instance.
    - Test connectivity based on the rules.
  + **Azure:**
    - Configure Network Security Groups (NSG) to control inbound and outbound traffic.
    - Attach the NSG to a Virtual Machine.
    - Test connectivity and access.
  + **GCP:**
    - Set up firewall rules in the VPC network to allow specific traffic (e.g., TCP:22, TCP:80).
    - Apply the firewall rules to a VM instance.
    - Test connectivity and access.

**4. Configuring IAM Roles and Permissions**

* **Objective:** Manage user access and permissions using IAM.
* **Steps:**
  + **AWS:**
    - Create a new IAM user with specific permissions (e.g., S3 access).
    - Assign a role to the user and test access to resources.
  + **Azure:**
    - Create a new user in Azure Active Directory.
    - Assign roles and permissions (e.g., Contributor role to a resource group).
    - Test access and verify role functionality.
  + **GCP:**
    - Create a new IAM user.
    - Assign a predefined role (e.g., Compute Admin).
    - Test user access and permissions on GCP resources.

**5. Monitoring and Logging**

* **Objective:** Set up monitoring and logging for cloud resources.
* **Steps:**
  + **AWS:**
    - Enable CloudWatch monitoring for an EC2 instance.
    - Set up an alarm for instance metrics (e.g., CPU utilization).
    - Review logs and metrics in the CloudWatch console.
  + **Azure:**
    - Enable monitoring in Azure Monitor.
    - Create an alert rule for a specific metric (e.g., disk space).
    - Review logs in Azure Log Analytics.
  + **GCP:**
    - Set up Stackdriver (now known as Cloud Monitoring) for a VM instance.
    - Create an alerting policy for instance health.
    - Review logs and alerts in the Monitoring console.

**6. Deploying a Simple Web Application (Optional)**

* **Objective:** Deploy a basic web application to understand deployment and management in the cloud.
* **Steps:**
  + **AWS:**
    - Use Elastic Beanstalk to deploy a simple Node.js or Python application.
  + **Azure:**
    - Deploy a web app using Azure App Service.
  + **GCP:**
    - Deploy an application on Google App Engine.

**7. Cleaning Up Resources**

* **Objective:** Ensure that all resources are properly terminated to avoid unnecessary charges.
* **Steps:**
  + Go through each cloud provider and delete all resources created during the lab (VMs, Security Groups, IAM roles, etc.).
  + Verify that there are no lingering resources that could incur costs.