Experiment Title:
Identity and Access Management #1

Aim/Objective:

The goal of this lab is to familiarize with setting up a CloudWatch Billing Alarm to monitor AWS usage costs and implementing basic Identity and Access Management (IAM) policies to control access.

Description:

The CloudWatch Billing Alarm is used to monitor AWS usage costs. This involves creating an alarm that triggers when estimated charges exceed a predefined threshold. Additionally, participants will configure actions such as sending notifications via SNS to stay informed about cost fluctuations. The Identity and Access Management (IAM) portion of the lab focuses on securing AWS resources. Participants will create an IAM user with programmatic access and attach a policy defining specific permissions.

Pre-Requisites:

- AWS account
- Administrative Privileges
- AWS Management Console Access
- Basic Understanding of AWS Services

Pre-Lab:

1) What is the primary purpose of creating a budget in AWS?

Ans:- the Primary Purpose of creating a budget in AWS is to effectively manage and control costs associated with cloud resources by setting limits, tracking expenses, and against insights into usage Patterns.

2) What is the primary purpose of setting up a CloudWatch Billing Alarm in AWS?

Ans:- the Primary Purpose of setting up a cloudWatch Billing Alarm in AWS is to receive notifications when your AWS costs exceed specified threshold this helps you monitor and control your expenses. your cloud spending.

3) What is the least privilege principle in AWS IAM?

Ans:- The Principle of least Privilege in AWS IAM means granting users and entities the minimum Permissions required for their tasks to enhances Security.

4) What is the purpose of an AWS IAM policy?

Ans: - the purpose of an AWS IAM Policy is to define and grant permissions for users, groups or roles, specifying what actions they are allowed or denied on AWS resources.

5) What AWS service can be used for monitoring and auditing IAM user activity?

Ans: - AWS cloud Trail : captures API calls and events, including IAM actions.
AWS cloud Watch Logs : collects and stores logs for analysis.
AWS config : Monitors and records configuration changes, including IAM.
Amazon cloudWatch Events : Triggers automated response based on IAM events.

Lab:

(a) Create CloudWatch Billing Alarm/budget

Procedure/Program:

- Set up a CloudWatch Billing Alarm to monitor AWS usage costs.
- Configure actions such as sending notifications via SNS.
- Test the alarm by deliberately exceeding the specified billing threshold.

(b) IAM user, role and policy creation

Procedure/Program:

Task 1: IAM User Setup and Permissions

- Create an IAM user with programmatic access.
- Attach an existing IAM policy that grants read-only access to a specific AWS service.
- Test the IAM user's access using AWS CLI or SDK.

Task 2: IAM Role and EC2 Instance Attachment

- Create an IAM role with a custom policy.
- Launch an EC2 instance and attach the IAM role during instance creation.
- Verify the EC2 instance has the permissions defined in the IAM role.

Task 3: Custom IAM Policy Creation and Attachment

- Create a custom IAM policy that grants specific permissions.
- Attach the custom policy to an existing IAM user or group.
- Verify that the IAM user or group inherits the permissions defined in the custom policy.

1. open the Google search box aws.amazon.com and the right corner we can see the top right corner we see the console and there we can sign in our account.
2. After signing into account then there ask the mail and we can appear the home page.
3. In the home page the right corner appear account details then click on it.
4. After billing and cost management clicked then left side Preference and setting we can select the Billing Preference.
5. then there appear a one home page in that Alert Preference we can give our Personal mail id then click the update.
6. After click on the Budgets and Planning in that click on the budgets then home page will be appear then we give email recipts we can give Personal mail create budget.
7. In search bar cie cloudwatch and click on a create alarm.

Step-2:-

1. In IAM search go to the ~~course~~ users and next create users select the S3 Access then user will be created and download the css.
2. After Signout again Signinto the console with IAM user or id number.
3. After login in search box S3 than click on it, after that create a bucket.
4. Again Signout the root account and sign in to the console b using Personal mail id.

Step : 3 :-

After sign into the console go to IAM then click the roles and create a role.

→ after click on the create role select the service EC2 and amazon full access.

→ Search for EC2 in EC2 click the launching instance and go to the launch instance click on it browser in first and go to the next and give the instance name and give the instance name and scroll down select launch instances.

→ If we get the key pairs option then we can go the without key pair option then launch it then successfully created.

Step 4 :-

→ Again signout and again sign into the console with IAM user.

→ After signin into the console go to the Policies and select it.

→ Click on create role Policy and attach the files and after that detach the files what we created.

Experiment #	TO BE FILLED BY STUDENT	Student ID	7002
Date	TO BE FILLED BY STUDENT	Student Name	Thoyasi. R.

Sample VIVA-VOCE Questions (In-Lab):

1. **What is the purpose of CloudWatch Logs?**

Amazon cloud watch logs is used for collecting, storing, and monitoring logs from various AWS services and applications. It Provides a centralized location for log data.

2. **What is the purpose of AWS Cost Explorer?**

AWS cost explorer is used for analyzing and visualizing AWS usage and cost data. It helps user understand their AWS Spending Patterns, identify cost drivers.

3. **Which type of access does an IAM user with "Programmatic access" have?**

An IAM user with Programmatic access to Aws services and resources through the AWS Command Line interface, AWS SDK, or both other tools that use AWS APIs.

4. **What is the primary purpose of an IAM user in AWS?**

IAM users in Aws server the Primary Purpose of Providing authentication, authorization, accountability and resource for individuals or applications to interact securely with AWS services.

5. **How are IAM policies typically attached to IAM users, roles, or groups?**

IAM Policies are typically attached to IAM user, role or Group by associating the Policy directly with the user, role or Group. The attachment is done through the Aws management console, AWS CLI or API.

Experiment #		Student ID	
Date		Student Name	

Post-Lab:

- **Perform the following task**

  Task: Cross-Account IAM Role Setup

  - ✓ **Create an IAM role in Account A.**
  - ✓ **Assume the IAM role from an IAM user in Account B**
  - ✓ **Test access to resources in Account A from Account B.**

- **Data and Results:**

1. open the IAM console, Log in to the AWS management console for Account A.
2. In the AWS Management console, Go to the IAM service.
3. click on Roles in the left navigation pane.
4. click the create role button.
5. Choose "Another AWS account" and enter the Account ID of Account B.
6. on the Permissions Page, attach Policies that define the Permissions the role will have. You can choose from existing Policies or create custom ones.
7. Enter a meaningful name and description for the role to distinguish it.
8. In the Review step, review the settings and click "create role". Ensure that the relationship allows the IAM user in Account B to assume this role.

Date

Experiment Title: Create custom VPC and display user data #2

Aim/Objective:

Create a custom VPC in AWS, launch an EC2 instance within the VPC, and display user data on the instance.

Description:

The ABC Corporation, a leading tech company, is undergoing a digital transformation and has decided to migrate its applications to the cloud. The company aims to leverage the scalability and flexibility offered by cloud services to enhance its overall operational efficiency. As part of this initiative, the IT team is tasked with creating a custom Virtual Private Cloud (VPC) on Amazon Web Services (AWS) and displaying user data during the launch of Elastic Compute Cloud (EC2) instances. Establish a secure and isolated network environment for ABC Corporation's cloud infrastructure. Customize the initialization process of EC2 instances to streamline application deployment and configuration.

Pre-Requisites:

- AWS account
- Knowledge on virtualization
- Knowledge on Key-Pair
- Knowledge on Networking

Pre-Lab:

1) What is VPC?

Ans:- VPC stands for virtual Private cloud. It is a virtual network dedicated to your AWS account. In the context of cloud computing a VPC allows you to create a logically isolated section of the AWS cloud where you launch resources.

2) What are the components of Amazon VPC?

Ans:- the main components of amazon VPC include subnets, internet Gateway, Route tables, Network Acls, Security Groups, Elastic IP Adresses, VPC Peering, VPN Connection and direct connect.

3) What is a subnet in VPC?

Ans:- A subnet in Amazon VPC is a range of IP addresses within the VPC's address space. It acts as a segmented network inside the vpc and is associated with a specific availability zone.

4) What are Internet Gateways in VPC?

Ans:- Internet Gateways in amazon VPC are horizontally scable, redundant components that enable communication between instances in the VPC and the internet.

5) What are inbound and outbound rules in security group?

Ans:- In a Security Group, inbound rules control incoming traffic specifying the allowed sources, IP Protocols, and Ports. outbound rules on the other hand manage outgoing traffic for allowed communications

Lab:

- **Procedure/Program:**

VPC Creation & Configuration

a. Create a VPC
b. Create Subnets
c. Create an Internet Gateway
d. Create a Routing Table
e. Associate Subnets with the Routing Table
f. Add a Route to the Internet

EC2 Instance Launch & Testing

g. Configure Instance Details
h. Attach custom VPC
i. Create Security Group
j. Feed the user data
k. Test the connectivity keeping the https://public_ipv4 in browser

1. Login into the console With root user and search for VPC.
2. click on create vpc.
3. Next select vpc only and fill their IPV4 CIDR.
4. Then go to the next then successfully created VPC.
5. Then go to next items subnets.
6. create subnets and fill the details of the subnets.

7. Successfully created the Subnet.
8. Go to the internet Gateways and create internet Gateway.
9. Give the name for internet Gateway.
10. create internet Gateway click on it and successfully created the internet gateway.
11. Attach to a VPC and give Available VPCs.
12. then Attach to it. then successfully created a internet Gateway.
13. Select the Routetables and create route table and give to Name for that. then click on the create route table.
14. After that created route table successfully.
15. then Edit routes and give the internet Gateway after click on the save changes.
16. then updated the routes. and click on subnet associations
17. And give the Name to the Launch instance.
18. After launch instances then go down click the view all instances.
19. Then click on the created instance open the Ip address then the required output will be come. appear.
20. After terminate the Internet Gateway and your VPC's.

Experiment #		Student Name	
Date			

Sample VIVA-VOCE Questions (In-Lab):

1. **What is the purpose of VPC flow logs?**

VPC flow logs capture network traffic metadata within an amazon virtual Private cloud, Providing insights into communication Patterns, aiding in security analysis, and facilitating trouble shooting.

2. **What is the purpose of a NAT Gateway in AWS?**

A NAT Gateway in AWS enables instances in a Private subnet to initiate outbound traffic to the internet while Preventing inbound traffic from reaching them, and allowing for controlled external communication.

3. **What are the differences between Private, Public & Elastic IP Addresses?**

A Private and Public IP addresses is used within a local network and routable on the internet and an Elastic IP in AWS is a static Public IP that can be associated with external access.

4. **Illustrate what is CIDR Routing in VPC?**

CIDR in VPC allows efficient IP address allocation and routing by aggregating address ranges, Simplifying network management and improveme -nt routing table efficiency in Amazon Virtual Private cloud.

5. **What is the default VPC?**

In AWS, the default VPC is a Pre-configured VPC Provided in each region, automatically created for user convenience, with default settings for routing subnets.

Post-Lab:

- **Perform the following task**

VPC Peering

- **Establish VPC peering between two VPCs within the same AWS account.**
- **Establish VPC peering between VPCs in different AWS accounts.**

- **Data and Results:**

VPC Peering between different AWS Accounts.

1. Sender Account initiates Peering request.
2. Accept Peering Request in receiver account.
3. update route tables in Both Accounts.
4. Configure cross-Account IAM Role.
5. Adjust Security Groups and Networks Acls.

VPC Peering within the same AWS account:

1. open the VPC Dashboard, Navigate to the AWS Management Console. and open the
2. Choose "Peering connections" in the VPC Dashboard.
3. click create Peering connection and specify the necessary details, such as the VPC IDs of both Peering VPCs.
4. In the target VPC's console, go to "peering connections." find the Pending connection, and accept it.
5. Update the route tables of both VPCs to include routes for each other's CIDR blocks.
6. Ensure that Security Groups and networks ACLs allow the desired traffic between the Peered VPCs.