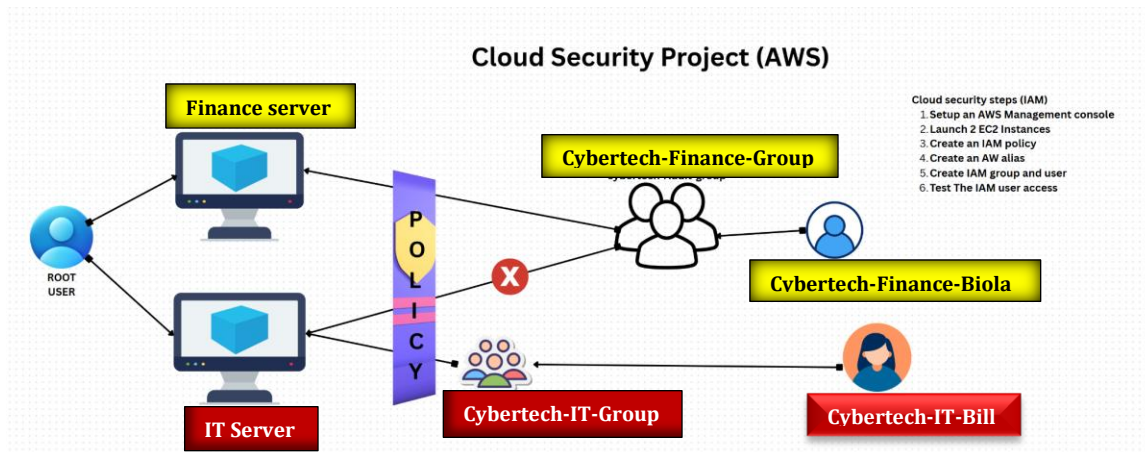


AWS IAM Cloud Security Project

1. Project Overview

I completed this project on cloud security controls in Amazon Web Services (AWS), focusing on Identity and Access Management (IAM). The goal was to create a least-privilege policy, attach it to a user group, and verify that the policy correctly restricts actions on two Amazon EC2 instances (audit and sales).



2. Tools & Concepts

- AWS IAM – users, groups, policies, account alias
- Amazon EC2 – instance tagging and lifecycle actions
- JSON policy syntax – Effect, Action, Resource
- Principle of least privilege and policy testing

3. Tagging Strategy

I applied a descriptive tag to each EC2 instance:

Instance | Tag Key| Tag Value

Finance| Environment| Finance

IT| Environment | IT

Instances (1/2) [Info](#) [Refresh](#) [Connect](#) [Instance state](#) [Actions](#) [Launch instances](#)

Find Instance by attribute or tag (case-sensitive) [All states](#) [< 1 >](#) [Settings](#)

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
<input checked="" type="checkbox"/>	Cybertech-IT-...	i-08f77e6dd78df9cd0	Running	t3.micro	Initializing	View alarms +
<input type="checkbox"/>	Cybertech-Fin...	i-0d6327c95e16b3aa2	Terminated	t3.micro	-	View alarms +

i-08f77e6dd78df9cd0 (Cybertech-IT-Server) [Settings](#) [Dropdown](#)

[Details](#) [Status and alarms](#) [Monitoring](#) [Security](#) [Networking](#) [Storage](#) [Tags](#)

▼ **Instance summary** [Info](#)

4. Creating the IAM Policy

I authored the following JSON policy to block instance stop/start actions on the Finance server but allow those actions on the IT server:

aws [Search](#) [Alt+S] [Account ID: 0010-9288-1997](#) [Cybertech-Finance-Biola](#)

[IAM](#) > [Policies](#) > Create policy [Info](#) [Help](#)

Step 1 **Specify permissions**
Step 2 Review and create

Specify permissions [Info](#)
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor [Visual](#) [JSON](#) [Actions](#) [Add](#)

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "ec2:*",
7       "Resource": "*",
8       "condition": {
9         "stringEquals": {
10          "ec2:ResourceTag/Env": "Finance"
11        }
12      }
13    },
14    {
15      "Effect": "Deny",
16      "Action": [
17        "ec2:DeleteTags",
18        "ec2:CreateTags"
19      ],
20      "Resource": "*"
21    }
22  ]
23 }

```

Edit statement [Remove](#)

Add actions

Choose a service [Search services](#)

Included [EC2](#)

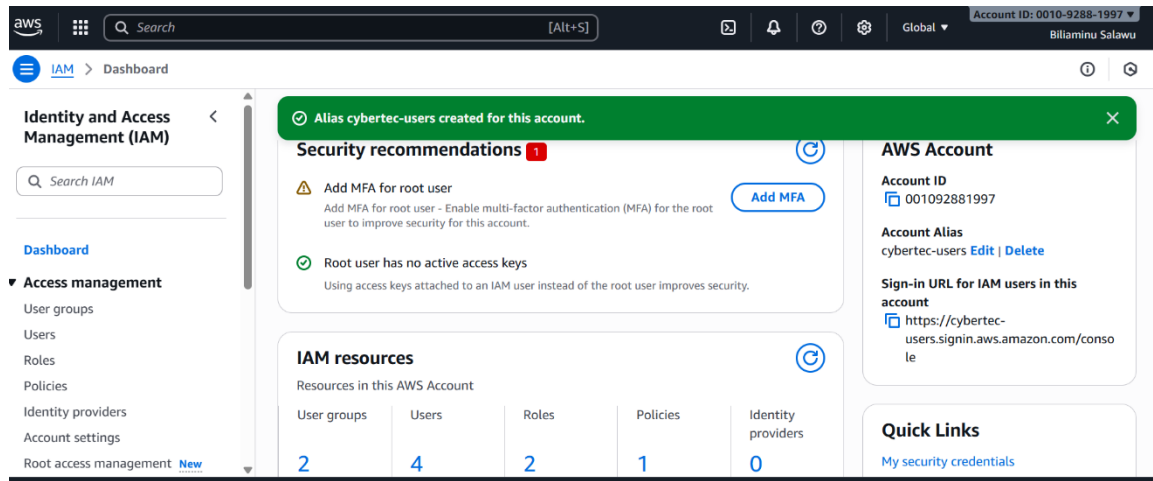
[+ Add new statement](#)

[+ Add new statement](#)

CloudShell [Feedback](#) © 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

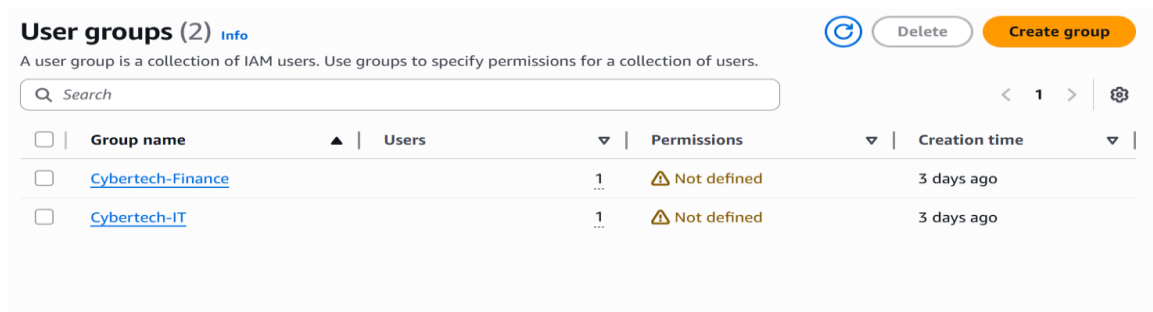
5. Account Alias

I set a memorable account alias to replace the default numeric URL, making sign-in easier for team members.

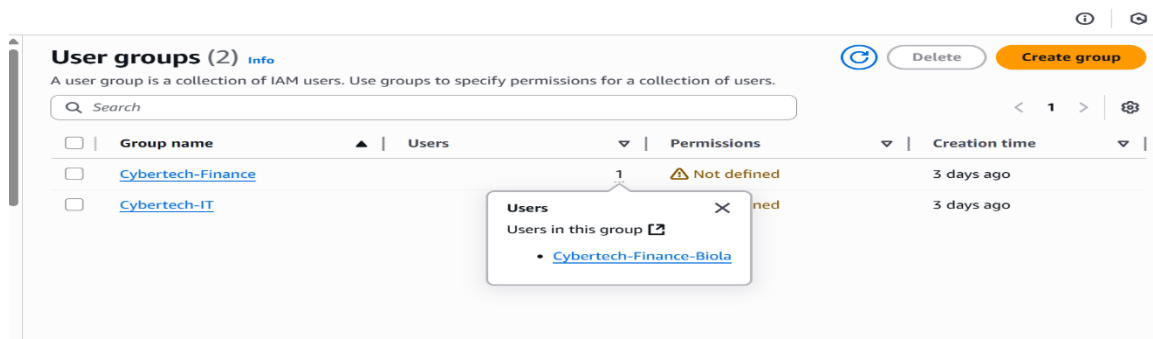


6. IAM Users & Groups

1. Created an IAM user group called Cybertech-Finance and Cybertech-IT Group respectively.
2. Attached the **CybertechFinancePolicy** policy to the group.
3. Added



individual IAM users who require controlled EC2 Access.



User groups (2) [Info](#)

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Search

<input type="checkbox"/>	Group name	Users	Permissions	Creation time
<input type="checkbox"/>	Cybertech-Finance	1	Not defined	3 days ago
<input type="checkbox"/>	Cybertech-IT	1	Not defined	3 days ago

Users

Users in this group

- [Cybertech-IT-Bill](#)

7. Logging in as an IAM User

IAM users can sign in through:

- AWS Management Console (using the new alias URL)
- AWS CLI via programmatic keys

8. Testing the Policy

Test Action | Expected Result | Actual Result

Stop Finance instance | Denied | Access denied error displayed

Stop sales instance | Allowed | Instance stopped successfully

Start IT instance | Denied | Access denied error displayed

Start sales instance | Allowed | Instance started successfully

The screenshot shows the AWS IAM Dashboard for Account ID: 0010-9288-1997. The left sidebar contains navigation links for Identity and Access Management (IAM), including a search bar and a list of resources: Dashboard, Access management, User groups, Users, Roles, Policies, Identity providers, Account settings, and Root access management. The main content area is divided into three sections: Security recommendations (with a warning to add MFA for the root user), IAM resources (showing 2 user groups, 4 users, 2 roles, 1 policy, and 0 identity providers), and AWS Account details (highlighted with a yellow circle). The AWS Account details section includes the Account ID (001092881997), Account Alias (Create), and Sign-in URL for IAM users in this account (https://001092881997.signin.aws.amazon.com/console). A Quick Links section at the bottom right provides a link to 'My security credentials'.

This following report outlines the implementation of the Identity and Access Management (IAM) service on cloud infrastructure, specifically focusing on the creation of an Amazon S3 bucket and the associated access control measures.

S3 Bucket Creation

The screenshot displays the Amazon S3 console interface. At the top, a green notification bar states "Successfully edited bucket policy." Below this, a JSON policy is shown, which includes a "Deny" statement for the "s3:DeleteBucket" action on the resource "arn:aws:s3::deployment.bucket1".

Below the policy editor, another green notification bar states "Successfully created bucket 'deployment.bucket1'". To the right of this bar is a "View details" button. Below the notification, the "General purpose buckets (1)" section is visible. It includes a search bar, a table of buckets, and two summary cards: "Storage Lens" and "External access summary - new".

Name	AWS Region	Creation date
deployment.bucket1	Europe (London) eu-west-2	October 3, 2025, 10:29:30 (UTC+01:00)

The "Storage Lens" card provides a "View dashboard" link and states "Storage Lens provides visibility into storage usage and activity trends." The "External access summary - new" card also provides a "View dashboard" link and states "External access findings help you identify bucket permissions that allow public access or access from other AWS accounts."

Bucket Name: deployment.bucket1

Service Used: Amazon S3 (Simple Storage Service)

The S3 bucket was created to facilitate secure storage and management of deployment artifacts and Access Control Lists (ACLs) have been enabled for the S3 bucket to manage

permissions at the bucket level. This ensures that only authorized users and groups can access or modify the bucket's contents.

Policy Implementation: A specific policy was generated and implemented to enhance security by preventing unauthorized deletions.

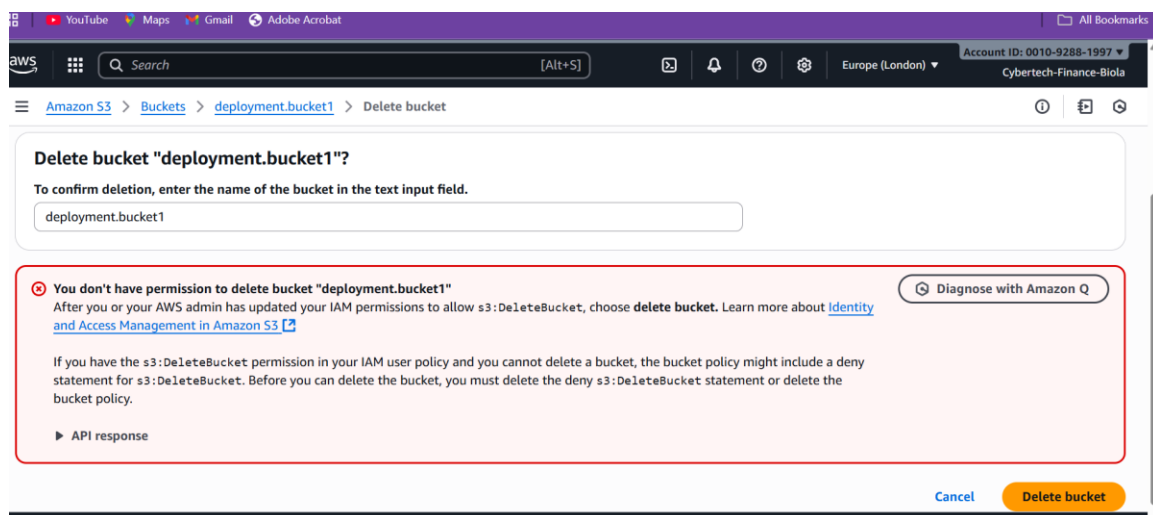
Policy Details:

Objective: Deny the deletion of the bucket.

Affected Groups and USERS: -

Finance Users in Cybertech and IT Users in Cybertech

This policy ensures that even users with broader access cannot delete the bucket, thereby protecting critical deployment data from potential accidental or malicious deletions.



Conclusion: The creation of the S3 bucket and the implementation of ACLs and restrictive policies reflect a commitment to maintaining a secure cloud environment. By restricting deletion permissions for specific user groups, the integrity and availability of deployment resources are safeguarded.