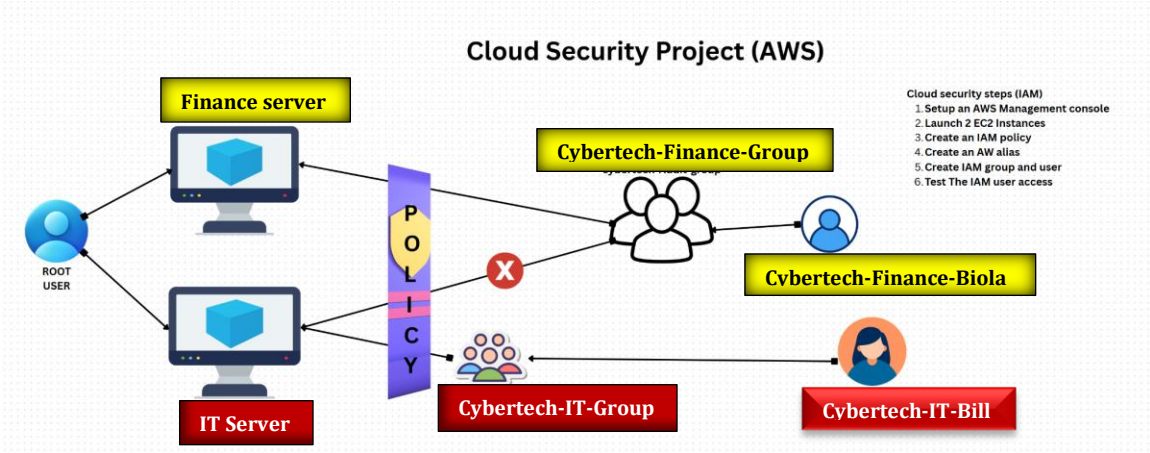
AWS IAM Cloud Security Project

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).

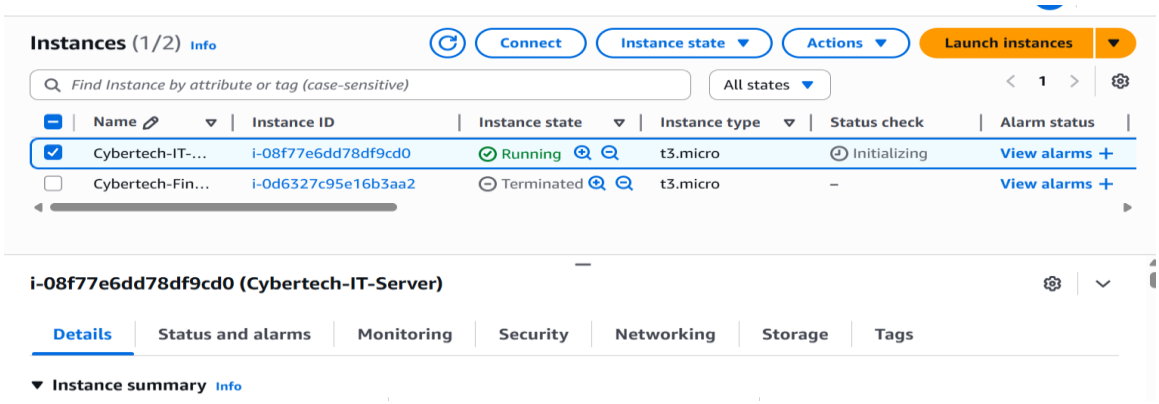


2. Tools & Concepts

- 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

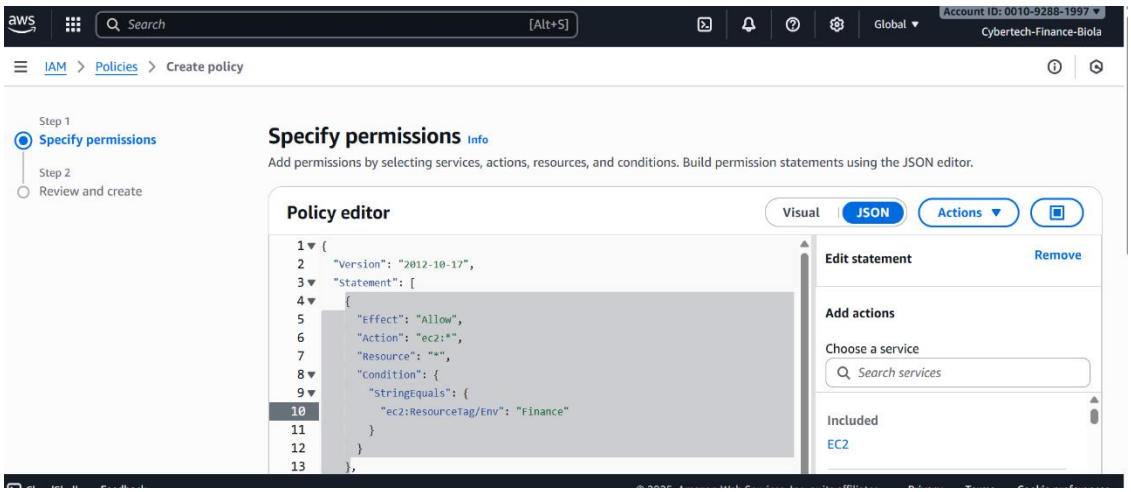
3. Tagging Strategy

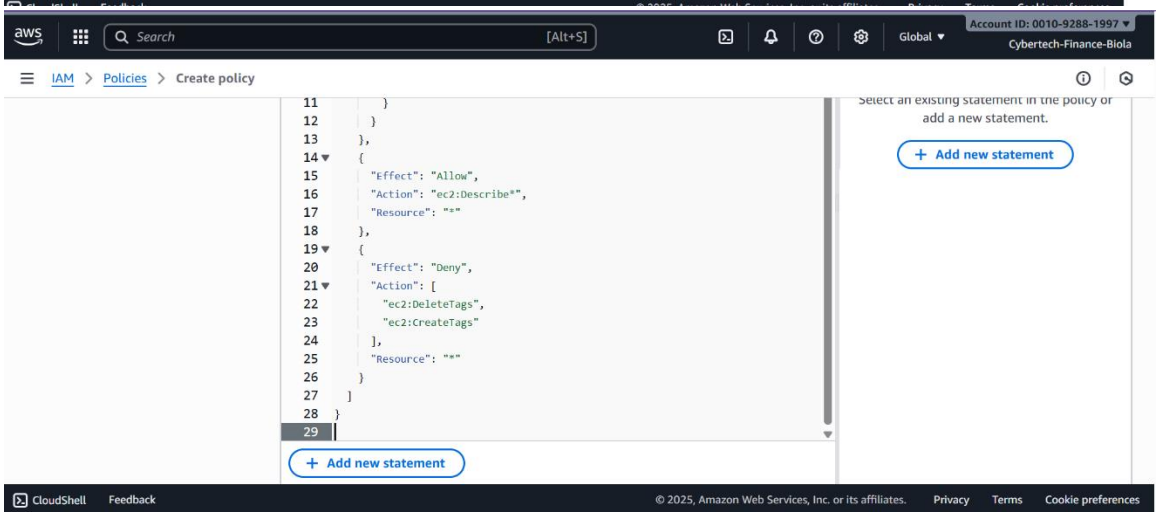
I applied a descriptive tag to each EC2 instance:
Instance | Tag Key| Tag Value
Finance| Environment| Finance
IT| Environment | IT



4. Creating the IAM Policy

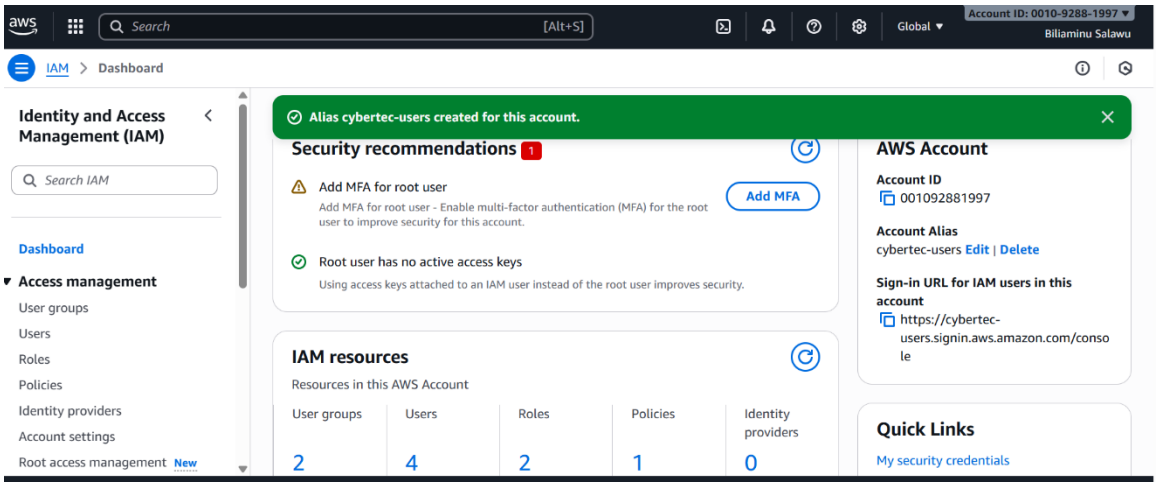
I authored the following JSON policy to block instance stop/start actions on the Finance server but allow those actions on the IT server:





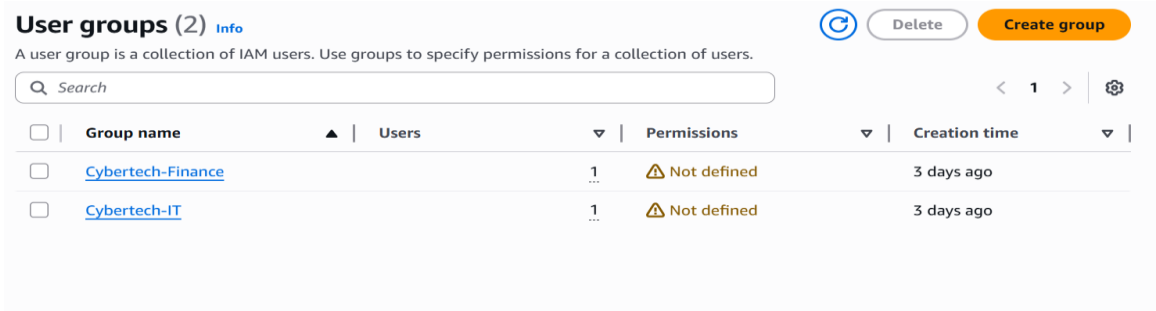
5. Account Alias

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

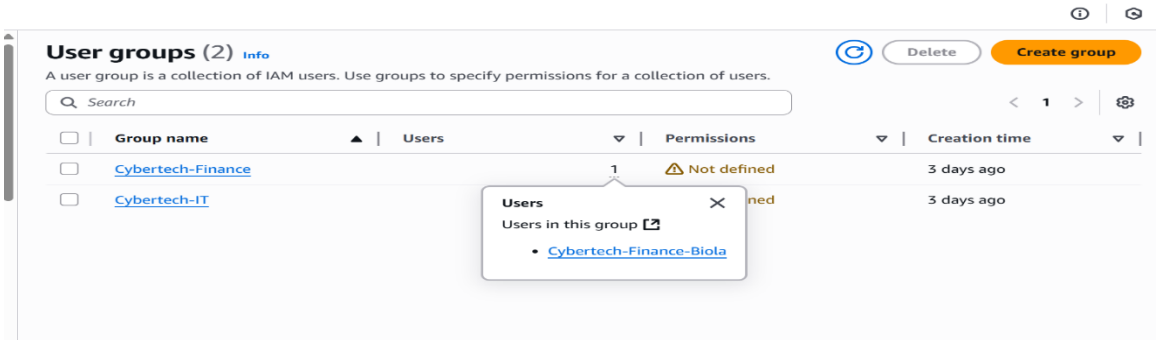


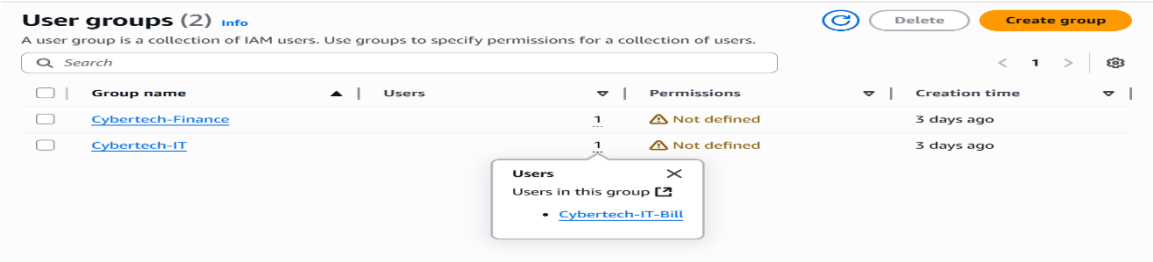
6. IAM Users & Groups

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.





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

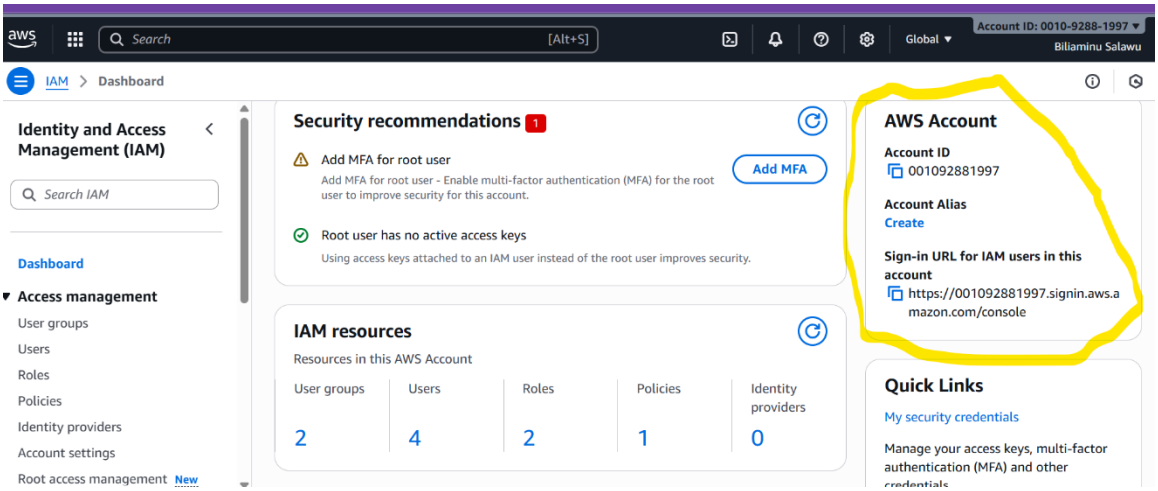
Test Action | Expected Result | Actual Result

Stop Finance instance | Denied | Access denied error displayed

Stop sales instance | Allowed | Instance stopped successfully

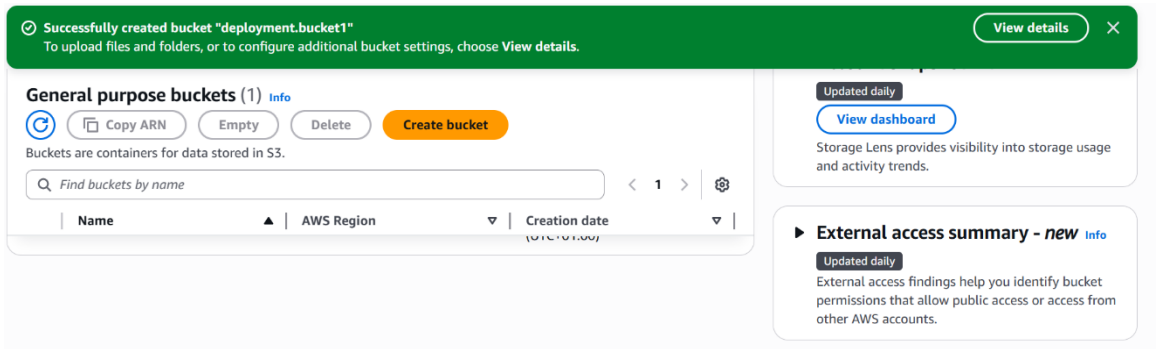
Start IT instance | Denied | Access denied error displayed

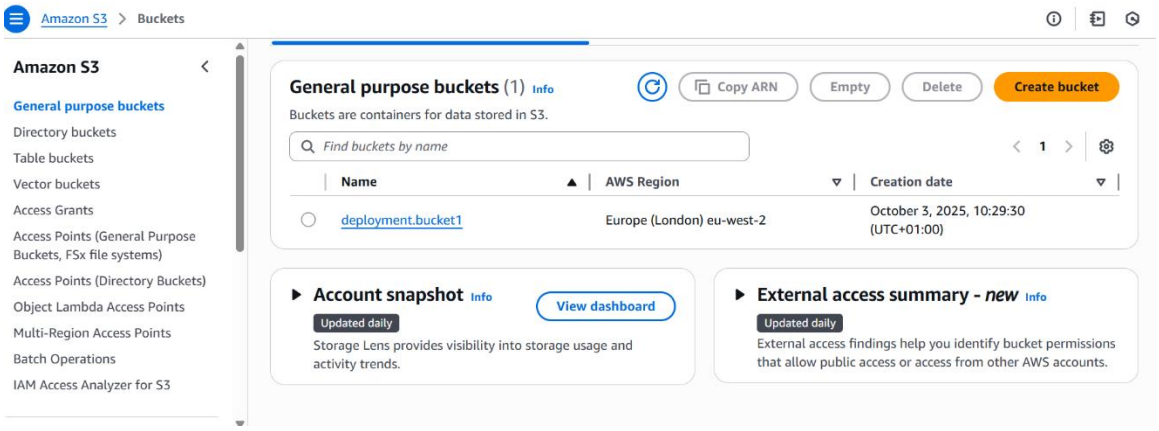
Start sales instance | Allowed | Instance started successfully



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





Bucket Name: deployment.buckett1

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.

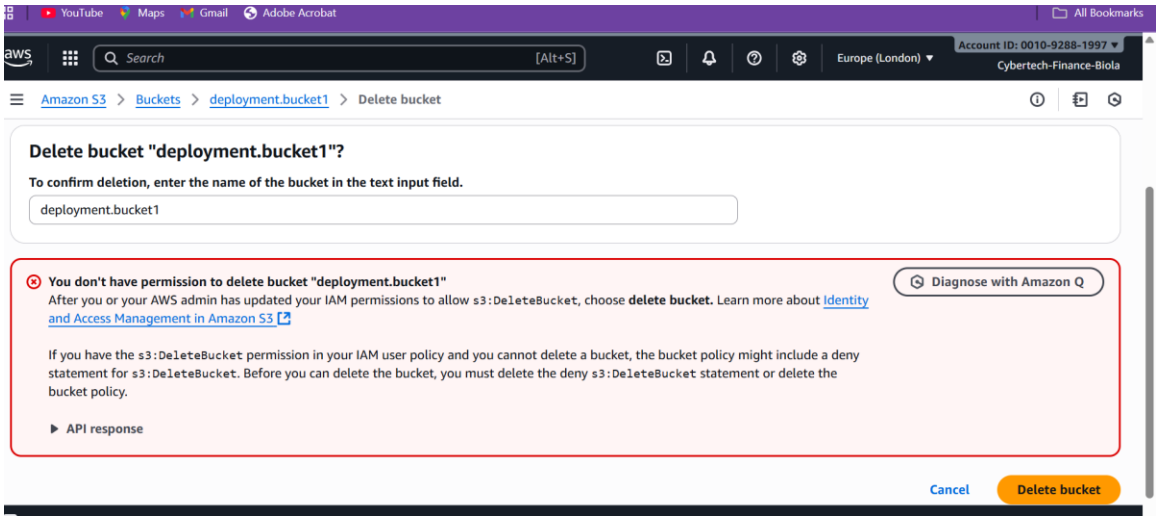
Policy Details:

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.